Nortel Communication Server 1000

Nortel Communication Server 1000 Release 4.5

IP Peer Networking

Installation and Configuration

Document Number: 553-3001-213
Document Release: Standard 11.00
Date: May 2007

Produced in Canada

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Revision history

May 2007

Standard 11.00. This document is up-issued for CR Q01624041, with information on ring burst in Adaptive Network Bandwidth Management.

April 2007

Standard 10.00. This document is up-issued for: (1) CR Q01454475, revising the configuration rules for Bandwidth Management. See page 140. (2) CR Q01524156, revising the description of loop limitations on a large system. See page 303. (3) CR Q01583690, revising the default value of the FOPT (Flexible Orbit Prevention Timer) from 14 to 6 seconds. See page 363. (4) CR Q01524220, specifying that a user password can be up to 24 characters in length. See page 480.

December 2006

Standard 9.00. This document is up-issued for CR Q01453520, specifying that the Primary, Alternate and (optional) Failsafe Network Routing Servers must host the same major software release. See page 384.

November 2006

Standard 8.00. This document is up-issued for CR Q014694590-01, specifying that at least 768 MByte of memory is required on the Signaling Server to obtain 1200 H.323 Virtual Trunks. See Table 1: “Virtual Trunk limits for each Signaling Server” on page 29.

October 2006

Standard 7.00. This document is up-issued for CR Q01461442, specifying in the Procedure for Adding a Collaborative Server that the TLAN IP address of the server must be entered in the Server address text box. See page 445

August 2006

Standard 6.00. This document is up-issued for CR Q01374118, adding a note that Data calls are not supported on Virtual Trunks. See page 28

April 2006

Standard 5.00. This document is upissued for CR Q01256567-01, adding a statement that Nortel does not support a modem in IP networks. See pages 27 and 182.

January 2006

Standard 4.00. This document is up-issued for CR Q01202736, with information on reconfiguring Call Server alarm notification levels if necessary when configuring Adaptive Network Bandwidth Management. See pages 158 and 166.

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 NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: IP Peer Networking (553-3023-220).

Contents

List of procedures

About this document

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

Subject

This document describes the IP Peer Networking feature, and how to implement IP Peer Networking as part of your system.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5 software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)

- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

Note: When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

Intended audience

This document is intended for administrators responsible for configuring the IP Peer Networking feature and managing the Network Routing Service database.

Conventions

Terminology

In this document, the following systems are referred to generically as "system":

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Meridian 1

The following systems are referred to generically as "Small System":

- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

The following systems are referred to generically as "Large System":

- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)

- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

Unless specifically stated otherwise, the term “Element Manager” refers to the CS 1000 Element Manager.

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Converging the Data Network with VoIP* (553-3001-160)
- *Electronic Switched Network: Signaling and Transmission Guidelines* (553-3001-180)
- *Dialing Plans: Description* (553-3001-183)
- *Signaling Server: Installation and Configuration* (553-3001-212)
- *Branch Office: Installation and Configuration* (553-3001-214)
- *System Management* (553-3001-300)
- *Features and Services* (553-3001-306)
- *Communication Server 1000: System Redundancy* (553-3001-307)
- *Software Input/Output: Administration* (553-3001-311)
- *Optivity Telephony Manager: System Administration* (553-3001-330)
- *IP Trunk: Description, Installation, and Operation* (553-3001-363)
- *IP Line: Description, Installation, and Operation* (553-3001-365)
- *Basic Network Features* (553-3001-379)
- *Software Input/Output: System Messages* (553-3001-411)
- *Software Input/Output: Maintenance* (553-3001-511)

- *Simple Network Management Protocol: Description and Maintenance* (553-3001-519)
- *Communication Server 1000M and Meridian 1: Small System Planning and Engineering* (553-3011-120)
- *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210)
- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258)
- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120)
- *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* (553-3021-258)
- *Communication Server 1000S: Planning and Engineering* (553-3031-120)
- *Communication Server 1000S: Installation and Configuration* (553-3031-210)
- *Communication Server 1000S: Upgrade Procedures* (553-3031-258)
- *Communication Server 1000E: Planning and Engineering* (553-3041-120)
- *Communication Server 1000E: Installation and Configuration* (553-3041-210)
- *Communication Server 1000E: Upgrade Procedures* (553-3041-258)
- *Communication Server 1000E: Maintenance* (553-3041-500)
- *Multimedia Portfolio Communication (MCP) Interworking Basics NTP (NN10372-111)*
- *CallPilot Planning and Engineering Guide (553-7101-101)*
- *CallPilot Installation and Configuration Part 3: T1/SMDI and CallPilot Server Configuration (553-7101-224)*
- *CallPilot Administrator’s Guide (553-7101-301)*

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Overview

Contents

This section contains information on the following topics:

IP Peer Networking overview

IP Peer Networking enables the customer to distribute the functionality of the CS 1000 systems over a Wide Area Network (WAN), using either Nortel

Session Initiation Protocol (SIP) or H.323 Gateways or other third-party SIP or H.323 Gateways.

Key advantages of IP Peer Networking are as follows:

- Provides global coverage of standard Voice over Internet Protocol (VoIP) signaling interfaces.
- Enables the networking of multiple systems across an IP network.
- Enables the customer to provision IP Phones anywhere on the connected network (LAN/MAN/WAN) and also enables them to provide LAN-connected modules (such as a router, Layer 2 switch, Layer 3 switch, bridge, or hub).
- Enables the CS 1000 systems to provide an industry-leading PBX feature set on an IP PBX that can be distributed throughout a customer's IP network.
- Consolidates voice and data traffic on a single Quality of Service (QoS)-managed network. Network-wide feature transparency is provided using the Nortel Meridian Customer Defined Network (MCDN) protocol.
- Enables Call Servers to work together in a network, over IP facilities, without using circuit switching.

  IP Peer Networking uses direct IP media paths for connections that involve two IP devices. Media streams route directly between the IP Phones and Gateways over the IP network, using Virtual Trunks. This minimizes voice quality issues caused by delay and transcoding between circuit-switched voice and IP packets. For more information on Virtual Trunks, see page 28.

SIP and the modified IP Peer Networking feature achieves a direct SIP interface used to interwork with other SIP-enabled Nortel products, such as Multimedia Communication Server 5100 (MCS 5100) and Communication Server 2000 (CS 2000).

SIP is a protocol standard used for establishing, modifying, and terminating conference and telephony sessions in IP networks. A session can be a simple two-way telephone call or it can be a collaborative multimedia conference session. SIP initiates real-time, multimedia sessions which can integrate voice, data, and video. The protocol’s text-based architecture speeds access to new services with greater flexibility and more scalability.

IP Peer overlap signaling using the H.323 protocol is also supported.

Nortel does not support the use of a modem in IP networks.

Assumptions

An existing system must be upgraded with CS 1000 Release 4.5 software for IP Peer Networking, and a Signaling Server must be installed and configured to provide SIP or H.323 signaling for Virtual Trunks. SIP and H.323 on the same Signaling Server platform is supported.

The Signaling Server is an industry-standard PC-based server that provides a central processor to drive SIP and H.323 signaling for IP Phones and IP Peer Networking. For more information on the Signaling Server, refer to page 31 and *Signaling Server: Installation and Configuration* (553-3001-212).

To use the Network Routing Service (NRS), a Succession 3.0 H.323 Gatekeeper database must be converted to a CS 1000 Release 4.0 (or later) NRS database. The NRS interface is provided when the Signaling Server is upgraded to CS 1000 Release 4.0 (or later) software. For more information on the NRS, see page 37 and page 201.

A brief overview of the migration procedures is described in “GK/NRS Data Upgrade” on page 471. However, refer to the following NTPs for detailed migration procedures:

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258)
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* (553-3021-258)
- *Communication Server 1000S: Upgrade Procedures* (553-3031-258)

Note: With the introduction of the NRS, the old Gatekeeper CLI commands are no longer available.

Virtual Trunk

Virtual Trunks are software components configured on virtual loops, similar to IP Phones. A Virtual Trunk acts as the bridge between existing call processing features and the IP network. It enables access to all trunk routing and access features that are part of the MCDN networking feature set. Virtual Trunks do not require dedicated Digital Signal Processor (DSP) resources to provide these features. Virtual Trunks include all the features and settings available to ISDN Signaling Link (ISL)-based TIE trunks, and are configured within trunk routes. Voice Gateway Media Card resources are only allocated for Virtual Trunks when it is necessary to transcode between IP and circuit-switched devices.

> ***Note:*** Voice Gateway Media Card is a generic term used when referencing both the ITG-P 24-port Card (dual-slot card) and the 32-port Media Card (single-slot) running the IP Line application. For more information about Voice Gateway Media Cards, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

> ***Note:*** Data calls are not supported on Virtual Trunks.

Both SIP and H.323 Virtual Trunks are supported. Up to 1800 Virtual Trunks can be configured on a Signaling Server.

Table 1 on page 29 lists the maximum number of Virtual Trunks that can be configured on a Signaling Server.

Table 1
Virtual Trunk limits for each Signaling Server

Protocol	Maximum number of Virtual Trunks
H.323	less than or equal to 1200 (see Note 1)
SIP	1800
Combination of both H.323 and SIP	less than or equal to 1800 (see Note 2)

Note 1: At least 768 MByte of memory is required on the Signaling Server to obtain 1200 H.323 Virtual Trunks.

Note 2: See Table 3 on page 34.

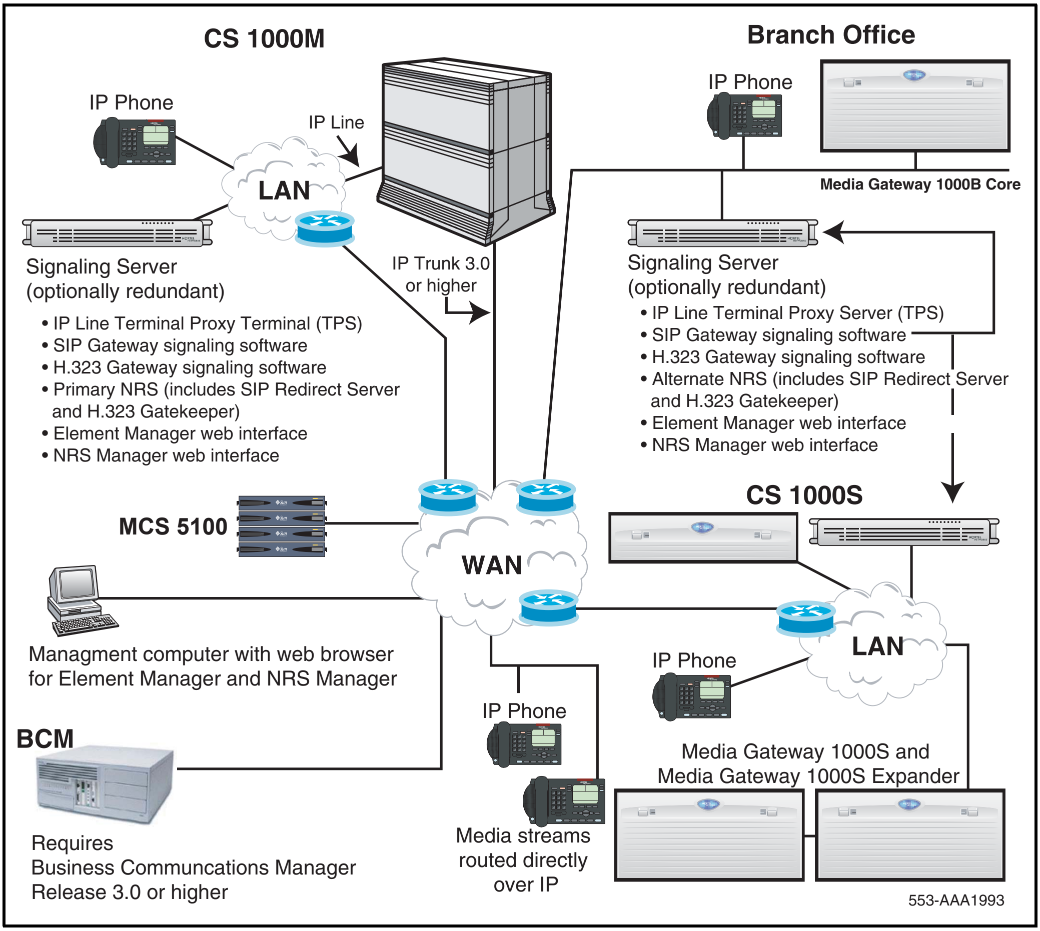
SIP and H.323 Virtual Trunks can reside on the same Signaling Server platform. This is achieved by configuring the Virtual Trunks on separate routes; however, the Virtual Trunks must use the same IP D-channel ID. Each SIP Trunk Gateway occupies one Virtual Trunk route.

Use the Signaling Server Resource Capacity (SSRC) prompt in LD 17 to configure the number of Virtual Trunks on a Signaling Server.

For more information, refer to “Scalability” on page 32 and the Planning and Engineering NTPs.

Figure 1 on page 30 illustrates an example of an IP Peer Networking configuration.

Figure 1
An example of IP Peer Networking


CS 1000M
Branch Office
IP Phone
IP Line
LAN
IP Phone
Media Gateway 1000B Core
Signaling Server
(optionally redundant)
• IP Line Terminal Proxy Terminal (TPS)
• SIP Gateway signaling software
• H.323 Gateway signaling software
• Primary NRS (includes SIP Redirect Server and H.323 Gatekeeper)
• Element Manager web interface
• NRS Manager web interface
IP Trunk 3.0 or higher
Signaling Server
(optionally redundant)
• IP Line Terminal Proxy Server (TPS)
• SIP Gateway signaling software
• H.323 Gateway signaling software
• Alternate NRS (includes SIP Redirect Server and H.323 Gatekeeper)
• Element Manager web interface
• NRS Manager web interface
CS 1000S
MCS 5100
WAN
Managment computer with web browser for Element Manager and NRS Manager
LAN
IP Phone
IP Phone
BCM
Media Gateway 1000S and Media Gateway 1000S Expander
Requires
Business Communcations Manager
Release 3.0 or higher
Media streams routed directly over IP
553-AAA1993

Signaling Server

IP Peer Networking uses a Signaling Server. The Signaling Server provides a central processor to drive SIP and H.323 signaling for IP Phones and IP Peer Networking. The Signaling Server is an industry-standard PC-based server that provides signaling interfaces to the IP network, using software components that operate on the VxWorks™ real-time operating system.

At least one Signaling Server is required for each CS 1000 system. Additional Signaling Servers can be installed in a load-sharing redundant configuration for higher scalability and reliability.

> ***Note:*** The load-sharing redundancy applies only to IP Phones and not to Virtual Trunks.

For more information, refer to *Signaling Server: Installation and Configuration* (553-3001-212).

Applications running on the Signaling Server

The following software components can operate on the Signaling Server:

- IP Line application (UNIStim), including the Line Terminal Proxy Server (LTPS)
- IP Phone Application Server which includes Personal Directory, Callers List, Redial List, and Password administration.

  Note: For detailed information on the IP Line application and the IP Phone Application Server, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

- SIP Gateway signaling software, including IP Peer access and SIP Converged Desktop Service
- H.323 Gateway signaling software for IP Peer access
- Network Routing Service (NRS) comprised of the following components:
  - SIP Redirect/Registrar Server
  - H.323 Gatekeeper
  - Network Connection Service (NCS)

- CS 1000 Element Manager and NRS Manager

  Note 1: All the software elements can coexist on one Signaling Server or reside individually on separate Signaling Servers, depending on traffic and redundancy requirements for each element. For details, refer to the *Planning and Engineering* NTPs.

  Note 2: If the Signaling Server is running applications other than H.323 or SIP Virtual Trunks, then the maximum number of Virtual Trunks is reduced. If all possible applications are running on the Signaling Server, the maximum number is 382 Virtual Trunks.

  Note 3: Refer to the *Planning and Engineering* NTPs for details on the applications that can co-reside on the Signaling Server. There can be limitations to the number of applications that can reside on the Signaling Server at the same time.

The software components are described in the sections that follow.

Scalability

Table 2 shows the capacity limits for each Signaling Server in the network.

Table 2
Signaling Server limits

Signaling Server component	Limit
Network Routing Service (NRS)	100 000 calls per hour 20 000 dialing plan entries 5000 H.323 and/or SIP endpoints
Virtual Trunks	1800 See Table 3: “Maximum number of Virtual Trunk on each Signaling Server” on page 34.

Note: Performance degradation occurs if the number of endpoints supported by the NRS exceeds 5000. Degradation, in this case, refers to the increased time required to complete actions such as the following:

- Synchronization between the Primary NRS and the Alternate NRS, and synchronization between the Active NRS and the Failsafe NRS
- Database actions (such as Commit, Rollback, Automatic Backup, and Restore)
- Boot-up

However, the ability of the H.323 Gatekeeper to resolve Admission Requests (ARQ) is not affected by an increased number of endpoints.

Both SIP and H.323 Virtual Trunks are supported.

For detailed information on scalability and capacity engineering, refer to the Planning and Engineering NTPs.

- *Communication Server 1000M and Meridian 1: Small System Planning and Engineering* (553-3011-120)
- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120)
- *Communication Server 1000S: Planning and Engineering* (553-3031-120)
- *Communication Server 1000E: Planning and Engineering* (553-3041-120)

Maximum number of SIP and H.323 Virtual Trunks

The maximum number of SIP and H.323 channels available on each Signaling Server depends on the number of available File Descriptors (FD) for Virtual Trunks. The maximum number of FDs for Virtual Trunks is 1800.

- Each SIP call uses one File Descriptor.
- Each incoming H.323 call uses two File Descriptors.
- Each outgoing H.323 call uses one File Descriptor.

When no more File Descriptors are available (available FD = 0), new channels added on the Call Server will not be able to register on the Signaling Server. Each Signaling Server supports up to 1800 Virtual Trunks. The maximum number of SIP and H.323 trunks depends on traffic patterns, both the split between SIP and H.323 calls and the split between incoming and outgoing H.323 calls. Table 3 on page 34 gives examples of the maximum number of Virtual Trunks supported for different configurations.

Table 3
Maximum number of Virtual Trunk on each Signaling Server

	H.323 (see Note)			Total Virtual Trunks
SIP	Incoming	Outgoing	Total H.323	
1800	0	0	0	1800
0	600	600	1200	1200
0	900	0	900	900
600	0	1200	1200	1800
600	300	600	900	1500
Note: Assumes H.245 tunneling is enabled.				

The formula to calculate the maximum number of Virtual Trunks is:

(Num_of_SIP × 1 FD) + (Num_of_Incoming_H323 × 2 FD) +
(Num_of_Outgoing_H323 × 1 FD) <= Max_Num_of_FDs

where Max_Num_of_FDs = 1800

Impact of H.245 tunneling

By default, H.245 tunneling is enabled. Unless there is a specific reason to disable tunneling, such as for maintenance, it should always be enabled. When tunneling is disabled, the handling capacity of the Signaling Server is reduced to a maximum of 900 H.323 Virtual Trunks. See ““H.245 tunneling” on page 49”.

Terminal Proxy Server

The Terminal Proxy Server (TPS) is a SIP/ H.323 signaling proxy software component for IP Phones. The TPS supports up to 5000 IP Phones on each Signaling Server. The TPS, in conjunction with the Call Server, delivers a full suite of telephone features.

IP Peer Networking supports the following telephones for IP telephony:

- Nortel IP Phone 2001
- Nortel IP Phone 2002
- Nortel IP Phone 2004
- Nortel IP Phone 2007
- Nortel IP Audio Conference Phone 2033
- Nortel IP Softphone 2050
- Nortel Mobile Voice Client 2050
- Nortel WLAN Handset 2210
- Nortel WLAN Handset 2211
- Nortel WLAN Handset 2212

You can configure each IP Phone to use the Dynamic Host Configuration Protocol (DHCP) to register with a Call Server for feature control.

SIP Gateway Signaling software

The SIP Gateway offers an industry-standard SIP-based IP Peer solution. SIP Gateway delivers a SIP interface for interoperability with Nortel SIP products and other industry SIP-based products.

SIP Gateway is a generic term used to refer to the SIP IP Peer networking application. The SIP Trunk Gateway provides a direct trunking interface between the CS 1000 systems and a SIP domain. The SIP Trunk Gateway application resides on a Signaling Server and has two functions:

- acts as a SIP User Agent, which services one or more end users in making/receiving SIP calls

- acts as a signaling gateway for all CS 1000 telephones (IP Phones, analog [500/2500-type] telephones, and digital telephones), which maps ISDN messages to and from SIP messages

As the call-signaling gateway, the SIP trunking application does the following:

- maps telephony numbers to and from SIP Uniform Resource Identifiers (URIs)
- performs client registration
- maps ISDN messages to and from SIP messages
- establishes the speech path between the desktop and SIP endpoints

  Note: SIP endpoints are also known as SIP User Agents that service one or more endpoints. This document uses the term “SIP endpoints”.

The SIP Trunk Gateway is implemented according to SIP standards. The SIP Trunk Gateway can connect two CS 1000 nodes and can also connect CS 1000 systems to other Nortel or third-party SIP-enabled products. This direct SIP interface is used to interwork with products such as MCS 5100.

The direct SIP interface provides the following:

- removes the requirement for a SIP/PRI gateway between the CS 1000 and the MCS 5100 systems
- improves voice quality through peer-to-peer communication of IP devices

SIP connectivity (also known as SIP trunking) provides a direct media path (trunk interface) between a user in the CS 1000 domain and a user in a SIP domain.

SIP Converged Desktop Service

The SIP Converged Desktop Service (SIP CDS) is a CS 1000 Release 4.0 (or later) and MCS 5100 Release 3.0 (or later) feature. SIP CDS brings multimedia features to CS 1000 users. SIP CDS allows a user to have access to multimedia features on MCS 5100 and voice features on CS 1000 systems at the same time. SIP CDS allows users to use their existing telephony system for voice communication and to use their PC for multimedia communication.

H.323 Gateway Signaling software

H.323 Gateway Signaling software provides the industry-standard H.323 protocol, to provide connectivity to H.323 Gateways and circuit switches that act as H.323 Gateways. H.323 Gateway Signaling software uses an H.323 Gatekeeper to resolve addressing for systems at different sites. The H.323 Gateway uses Virtual Trunks to enable direct, end-to-end voice paths between two IP devices.

Direct IP media paths provide the following benefits:

- elimination of multiple IP Telephony to circuit-switched conversions
- improved voice quality
- simplified troubleshooting

See “Interworking protocols” on page 41 for further information.

Overlap Signaling

Overlap signaling over IP is supported using the H.323 protocol.

> ***Note:*** Overlap signaling is not supported using the Session Initiation Protocol (SIP).

In the H.323 network, dialed digits can be sent out or received in either en bloc (normal dialing) or overlap modes. Overlap signaling is sending some digits of the called-party number in the first signaling message (SETUP messages) followed by further digits in subsequent signaling messages (INFORMATION messages). Overlap signaling improves call setup time.

For detailed information, refer to “Overlap signaling” on page 487.

Network Routing Service

IP Peer Networking uses the NRS to simplify the configuration of IP component addressing. The NRS (which is optionally redundant) manages a centralized numbering plan for the network. The NRS allows customers to manage a single network dialing plan for SIP, H.323, and mixed SIP/H.323 networks.

Note: Within each Call Server, configure the numbering plan information required for the Call Server software to internally route calls, such as routing information for locally accessible numbers.

The IP Peer Networking feature provides the NRS where all CS 1000 systems in the network can register. This eliminates the need for manual configuration of IP addresses and numbering plan information at every site.

The NRS combines the following:

- SIP Redirect Server (see page 39) and SIP Registrar (see page 39)
- H.323 Gatekeeper (see page 40)
- Network Connection Service (NCS) (see page 40)

The SIP Redirect Server and H.323 Gatekeeper can reside on the same Signaling Server. The data entry for the dialing plan is common for both SIP and H.323. The Network Routing Service (NRS) Manager includes both the SIP Redirect Server and the H.323 Gatekeeper.

The NRS can operate in two modes:

- Stand-alone mode — The host Signaling Server does not have an attached Call Server. During installation of a stand-alone Signaling Server, the Call Server IP address defaults to 0.0.0.0.
- Co-resident mode — The host Signaling Server has an attached Call Server. The Signaling Server is running the NRS as well as other applications such as the IP Line TPS and Gateway Signaling Software. Refer to “Applications running on the Signaling Server” on page 31.

For more information, see“Enabling and configuring the NRS server” on page 384.

The Alternate NRS is supported only on a Leader Signaling Server. Nortel recommends that, for network reliability, the Alternate NRS be located in a physical location separate from the Primary NRS.

For more information about stand-alone NRS, see “Stand-alone NRS support for Meridian 1 and BCM nodes” on page 250.

For detailed information, see “Network Routing Service overview” on page 201.

SIP Redirect Server software

Building on the H.323 Gatekeeper, the SIP Redirect Server is used to facilitate centralized dialing plan management and the configuration of the network routing information for the SIP domain.

Nortel has many products with a SIP interface. A SIP Redirect Server translates telephone numbers recognized by Enterprise Business Network (EBN) voice systems to IP addresses in the SIP domain. As a result, the SIP Redirect Server interfaces with SIP-based products.

The SIP Redirect Server resides on the Signaling Server. The SIP Redirect Server is used to interconnect with other Nortel communication servers using SIP. Along with the H.323 Gatekeeper application, the SIP Redirect Server has access to the endpoint/location database. The SIP Redirect Server has the ability to access the CS 1000 system's location database in order to direct SIP Trunk Gateways and SIP Phones within the networked environment.

SIP Registrar

The SIP Registration Server is also known as the SIP Registrar. Registration is one way that the server can learn the location of a user (SIP client). The SIP Registrar accepts registration requests from SIP Phones, SIP Trunk Gateways, and other certified compatible third-party SIP user agents that are supported.

Upon initialization, and at periodic intervals, a user's telephone sends REGISTER messages to the SIP Registrar in the same domain. The contact information from the REGISTER request is then made available to other SIP servers, such as proxies and redirect servers, within the same administrative domain. The registration process precedes the call setup.

The SIP Registrar is collocated with the SIP Redirect Server on the Signaling Server.

By storing information mapping device addresses on a SIP Registrar, communication can be addressed to a person's name instead of a complex number scheme. A person simply registers one or more SIP devices (for example, a SIP Phone) with the network and becomes reachable, wherever he or she may be, independent of the details of the networks and devices involved.

For more information, refer to “SIP Registrar” on page 205.

H.323 Gatekeeper software

The H.323 Gatekeeper manages a centralized numbering plan for the H.323 network. This enables simplified management of the CS 1000 network. The H.323 Gatekeeper software identifies the IP addresses of H.323 Gateways, based on the network-wide numbering plan, in the CS 1000 systems and third-party systems.

Network Connection Server

The NRS also includes the Network Connection Service (NCS). The NCS is used for the Branch Office (including the Survivable Remote Gateway [SRG]), IP Line Virtual Office, and Geographic Redundancy features. The NCS allows the Line TPS (LTPS) to query the NRS using the UNIStim protocol. For more information, refer to “Network Connection Service” on page 208.

Element Manager web interface

Element Manager is a simple and user-friendly web-based interface that supports a broad range of system management tasks, including:

- configuration and maintenance of IP Peer and IP telephony features
- configuration and maintenance of traditional routes and trunks
- configuration and maintenance of numbering plans
- configuration of Call Server data blocks (such as configuration data, customer data, Common Equipment data, D-channels) maintenance commands, system status inquiries, backup and restore functions
- software download, patch download, patch activation

Element Manager has many features to help administrators manage systems with greater efficiency. For example:

- Web pages provide a single point-of-access to parameters that were traditionally available through multiple overlays.
- Parameters are presented in logical groups to increase ease-of-use and speed-of-access.

- The "hide or show information" option enables administrators to see information that relates directly to the task at hand.
- Full-text descriptions of parameters and acronyms help administrators reduce configuration errors.
- Configuration screens offer pre-selected defaults, drop-down lists, check boxes, and range values to simplify response selection.

The Element Manager web server resides on the Signaling Server and can be accessed directly through a web browser or Optivity Telephony Manager (OTM). The OTM navigator includes integrated links to each network system and their respective instances of Element Manager.

NRS Manager web interface

The NRS Manager is the web interface for the NRS. The web interface is common to both the H.323 Gatekeeper and the SIP Redirect Server. NRS Manager is used for populating the location and registration database. For detailed information, refer to “Configuring and managing the Network Routing Service” on page 379.

Interworking protocols

Peer-to-peer call and connection control at the IP level requires peer-to-peer protocol. IP Peer Networking uses the SIP and H.323 protocols.

To support traditional PBX signaling on an IP network, it can be necessary to transport non-IP peer signaling information from peer to peer. This is achieved by “tunneling” the legacy protocol in the IP peer protocol.

SIP, H.323, and MCDN tunneling is supported.

Session Initiation Protocol

Session Initiation Protocol (SIP) is supported by CS 1000, which complies with the standards described in the following Request for Comments (RFC) Internet Engineering Task Force (IETF) standards documents:

- RFC 3261 – SIP: Session Initiation Protocol

- RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 2806 – URLs for Telephone Calls
- RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3265 – Session Initiation Protocol (SIP)-Specific Event Notification
- RFC 3311 – The Session Initiation Protocol (SIP) UPDATE Method
- RFC 2976 – The SIP INFO Method

SIP is an Application Layer (Layer 7 of the OSI Reference Model) protocol used for establishing, modifying, and terminating real-time conference and telephony sessions over IP-based networks. SIP uses text-based messages, much like Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). SIP also uses Session Description Protocol (SDP) for media description.

A SIP session is any interactive communication that takes place between two or more entities over the IP network, from a simple two-way telephone call or instant message to a collaborative multimedia conference session.

SIP is a simple, transport-independent, text-based protocol used for multimedia call control and enhanced telephony services. SIP has only six different method types. These methods, when combined, allow for complete control over a multimedia call session while limiting complexity. SIP is transport-layer independent. Both TCP and UDP can be used as the transport protocol for SIP; however, TCP is the default mechanism.

> ***Note:*** Nortel recommends that customers use TCP as the transport protocol for SIP traffic.

SIP is text-based in that a method is formed using a textual header with fields that contain call properties. This text-based approach is easy to parse, has small packet overhead, and is flexible.

SIP clients are also known as SIP User Agents. These clients communicate with SIP servers in a client-server fashion. User Agents also act as servers when the SIP request reaches its final destination. These user agents contain the full SIP state machine and can be used without intermediate servers.

Table 4 lists and describes the SIP components.

Table 4
SIP components

Component	Description
SIP User Agent	The end system component for the call
SIP Network Server	The network device that handles the signaling associated with multiple calls

SIP User Agent

The User Agent has a client and server element.

- User Agent Client — the client element initiates the calls
- User Agent Server — the server element answers the calls

Peer-to-peer calls can, therefore, be made using a client-server protocol.

SIP Network Server

The main function of the SIP Network Server is to provide name resolution and user location, as the caller is unlikely to know the IP address or host name of the called party.

An “e-mail-like” address or a telephone number is usually associated with the called party. Using this information, the caller’s User Agent identifies with a specific server to resolve the address information.

Three forms of SIP Network Server can exist in a network: the SIP stateful proxy server, the SIP stateless proxy server, and the SIP redirect server. The three forms function as follows:

- A SIP proxy server (both stateful and stateless) receives requests, determines where to send the requests, and passes them on to the next server.
  - stateful proxy — a proxy server in a stateful mode remembers the incoming requests it receives, along with the responses it sends back and the outgoing requests it sends on
  - stateless proxy — a proxy server acting in a stateless mode forgets all information once it has sent a request

  Note: CS 1000 does not support SIP proxy servers. CS 1000 interoperates with other SIP Proxy servers, such as the MCS 5100 system.

- A SIP redirect server receives requests, but does not pass the requests onto the next server. Instead, the SIP redirect server sends a response back to the caller, indicating the address for the called user. Because the response includes the address of the called user, the caller can then directly contact the called party at the next server.

The NRS provides a SIP Redirect Server, but does not support SIP proxy servers.

SIP addressing is built around either a telephone or a web host name. For example, the SIP address can be based on a URL such as the following: SIP:john.doe@companyabc.com. The format makes it very easy to guess a SIP URL based on an e-mail address. The URL is translated into an IP address through a Domain Name Server (DNS).

SIP negotiates the features and capabilities of the session at the time the session is established. With SIP, a common set of audio and video compression algorithms negotiate prior to establishing the SIP session. This advance negotiation reduces the call setup time (compared to the time required for H.323 sessions). The Session Description Protocol (SDP) is used for this advance negotiation process. Once the session is established, the designated capabilities can be modified during the call. For example, additional features can be added if both terminals are capable and can negotiate a common compression algorithm.

SIP supports both unicast (one-to-one) sessions and multicast (one-to-many) communication.

SIP/MCDN

SIP services also implement tunneling of MCDN messages. Tunneling enables preservation of MCDN features if calls between two CS 1000 systems are over a SIP trunk or the call is redirected back to the CS 1000 systems from MCS 5100.

If MCS 5100 tunnels MCDN messages, Trunk Route Optimization (TRO) removes the unnecessarily used DSP/Virtual Trunk channels between CS 1000 and MCS 5100 systems. The result is a significant cost reduction and voice quality improvement for the converged desktop users.

MCDN tunneling is supported over SIP Virtual Trunks. However, if calls are connected between two CS 1000 systems using the MCS 5100, then the SIP trunk between two CS 1000 systems does not support the full set of MCDN features unless the proxy that connects the two systems can tunnel the MCDN messages.

> ***Note 1:*** While the MCDN protocol is supported by MCDN tunneling in SIP, QSIG is not supported by CS 1000 in terms of Q.SIG over SIP.
>
> ***Note 2:*** SIP uses a subset of the MCDN content in UIPE format and carries it like H.323 does; however, this is only for information that does not have standardized transport mechanisms.

For detailed information about SIP, refer to RFC 3261.

H.323 protocol

CS 1000 systems support H.323 version 4.0.

H.323 is the leading standard in the Voice over IP (VoIP) area. The term VoIP stands for more than only voice transmission in IP networks. It covers an abundance of applications that are now being successively integrated due to the universality and ubiquity of the IP networks. Enhanced performance of IP and Ethernet networks, as well as the improved manageability of the bandwidth, allow traditional switched-network applications — such as Automatic Call Distribution, Real-time Messaging and Teleworking — to be offered in IP networks.

In addition to voice applications, H.323 provides mechanisms for video communication and data collaboration, in combination with the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) T.120 series of standards. The H.323 standard (published in 1996 by the ITU-T) represents the basis for data, voice, and video communication over IP-based LANs and the Internet.

The H.323 standard refers to many other standards such as H.245, H.225, H.450. H.323 regulates the technical requirements for visual telephony, which means the transmission of audio and video in packet-based networks. Because IP is the prevailing protocol in packet-based networks (with about 90 percent market share), the H.323 standard is interpreted as a standard for multimedia communication in IP networks.

By definition, H.323 focuses on IP packet-based networks that do not provide any guaranteed service quality. For example, packets can be lost and real-time (voice and video) traffic does not take precedence over non-real-time, and therefore delay-insensitive, data traffic.

Recent developments in IP networking technology introduce Quality of Service (QoS) mechanisms that lead to improved voice/video quality. However, because the majority of IP networks today still do not have QoS capabilities, the H.323 mechanisms help provide reliable communication.

Because IP runs on any existing Layer 2 technologies, H.323 can be used over:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- FDDI
- Token-Ring

Recent implementation proves that H.323 can also be used beyond LANs, in multisite configurations over Wide Area Networks (WANs) based on T1, Frame Relay, and ATM technology.

H.323 is often characterized as an "umbrella specification" because it refers to various other ITU standards. The topology and its parts, as well as the protocols and standards, are specified in H.323.

Table 5 lists and describes the H.323 components.

Table 5
H.323 components

Component	Description
Terminal	Terminals represent the end devices of every connection.
Gateway	Gateways establish the connection in other networks. That is, gateways connect the H.323 network with the switched network of PBXs and Central Office switches.
Gatekeeper	Gatekeepers take over the task of translating between telephone numbers (for example, in accordance to the E.164 numbering standard) and IP addresses. Gatekeepers also manage the bandwidth and provide mechanisms for terminal registration and authentication.
Multipoint Control Units (MCUs)	MCUs are responsible for establishing multipoint conferences. The H.323 standard makes the distinction between callable and addressable end devices: all components are addressable; gatekeepers are, however, not callable.

The four components communicate by exchanging information flows among each other. The information flows are split into five categories:

- Audio (digitized and coded) voice
- Video (digitized and coded full-motion image communication)
- Data (files such as text documents or images)

- Communication control (such as exchange of supported functions and controlling logical channels)
- Controlling connections (such as connection setup and connection release)

H.323/MCDN

MCDN tunneling in H.323 is supported.

Internet-enabled Meridian 1 Systems also support MCDN tunneling in H.323, using IP Trunk 3.0 (or later), which supports H.323 Gatekeeper operation, as well as non-call associated signaling.

Wireless LAN interworking (802.11 Wireless IP Handsets)

802.11 Wireless IP Handsets use H.323 as a protocol to access a Call Server, as opposed to using H.323 to access an H.323 network. For the 802.11 Wireless IP Handset, the H.323 network consists of the 802.11 Wireless IP Gateway to which it terminates, instead of the entire H.323 network. The Call Server sees 802.11 Wireless IP Handsets as ordinary telephones.

802.11 Wireless IP Handsets can access Virtual Trunk routes like any other terminal device; however, indirect media paths are used. Also, no direct media connection occurs between 802.11 Wireless IP Handsets and IP Phones or Media Gateways (the media stream from the 802.11 Wireless IP Handset terminates at its IP Line/Trunk).

Call independent signaling connection and connectionless transport

With IP Peer Networking, signals cannot be sent directly from endpoint to endpoint without first determining the signaling IP address of the remote endpoint, using standard Gatekeeper procedures. This requires setting up an end-to-end path or connection to support the messaging. However, the base MCDN Peer-to-Peer signaling, used to provide supplementary service signaling independently of any established calls, uses connectionless signaling; it does not use a path.

Therefore, connectionless MCDN Non-Call Associated Signaling (NCAS) is transported as though it is a virtual, path-oriented connection (virtual call) using the H.323 call-independent call-signaling connection. Because this call is essentially an H.323 call with no media, standard H.323 Gatekeeper procedures apply. As a direct result, MCDN services using connectionless transport between the Call Server and the Signaling Server are not transported over the IP network using H.323 connectionless transport.

Alternate routing is not supported for NCAS messages over IP Peer. Services such as Network Ring Again, Network ACD and Centralized CallPilot that rely on NCAS may not work over alternate routes if the primary IP Peer route fails.

H.245 tunneling

H.245 tunneling is supported, and is enabled by default. This conserves resources, synchronizes call signaling and control, and reduces call setup time. If required, the user has the option to turn the tunneling on and off. This is done using CLI commands through the VxWorks shell on the Signaling Server.

H.245 specifies the signaling protocol which is used to:

- establish a call
- determine the capabilities of a call
- issue the commands necessary to open and close media channels

The H.245 control channel is responsible for control messages governing the operations of H.323 terminals.

H.245 tunneling enables the reuse of socket FDs used for H.323 call signaling. The H.245 control messages are sent on the same TCP link that was opened for the H.225 call control message exchange with the peer node. This halves the number of sockets used for each call.

Number of supported Virtual Trunks with H.245 tunneling enabled

If H.245 tunneling is enabled (the default), then the following are supported on the Signaling Server:

- up to 1200 H.323 Virtual Trunks
- up to 1800 SIP Virtual Trunks

- a combination of both H.323 and SIP Virtual Trunks

  If there is a combination of H.323 and SIP trunks, then the available number of Virtual Trunks is shown in the following calculation:

  1800 - [(1 x H.323 channels) + SIP channels]
  (where 1800 is the maximum number of Virtual Trunks)

  Example 1: 1200 H.323 and 600 SIP

  1800 - [(1 x 1200 H.323 channels) + 600 SIP channels]
  = 0 available Virtual Trunks

  Example 2: 900 H.323 and 900 SIP

  1800 - [(1 x 900 H.323 channels) + 900 SIP channels]
  = 0 available Virtual Trunks

  Example 3: 0 H.323 and 1800 SIP

  1800 - [(1 x 0 H.323 channels) + 1800 SIP channels]
  = 0 available Virtual Trunks

  Example 4: 1200 H.323 and 0 SIP

  1800 - [(1 x 1200 H.323 channels) + 0 SIP channels]
  = 600 available Virtual Trunks

  Note: The 600 available trunks must be SIP trunks, as the number of H.323 channels is already at the maximum limit of 1200.

Number of supported Virtual Trunks with H.245 tunneling disabled

If H.245 tunneling is disabled, then the following are supported on the Signaling Server:

- up to 900 H.323 Virtual Trunks
- up to 1800 SIP Virtual Trunks
- a combination of H.323 and SIP trunks

  If there is a combination of H.323 and SIP trunks, then the available number of Virtual Trunks is shown in the following calculation:

  1800 - [(2 x H.323 channels) + SIP channels]
  (where 1800 is the maximum number of Virtual Trunks)

  Example 1: 900 H.323 and 0 SIP

  1800 - [(2 x 900 H.323 channels) + 0 SIP channels]
  1800 - [(1800 H.323 channels) + 0 SIP channels]
  = 0 available Virtual Trunks

  Example 2:. 600 H.323 and 600 SIP

  1800 - [(2 x 600 H.323 channels) + 600 SIP channels]
  1800 - [(1200 H.323 channels) + 600 SIP channels]
  = 0 available Virtual Trunks

  Example 3: 0 H.323 and 1800 SIP

  1800 - [(1 x 0 H.323 channels) + 1800 SIP channels]
  = 0 available Virtual Trunks

SIP signaling

Contents

This section contains information on the following topics:

Introduction

The SIP Trunk Gateway offers an industry-standard SIP-based IP Peer solution. A SIP Trunk Gateway delivers a SIP interface for interoperability with Nortel SIP products and other industry SIP-based products.

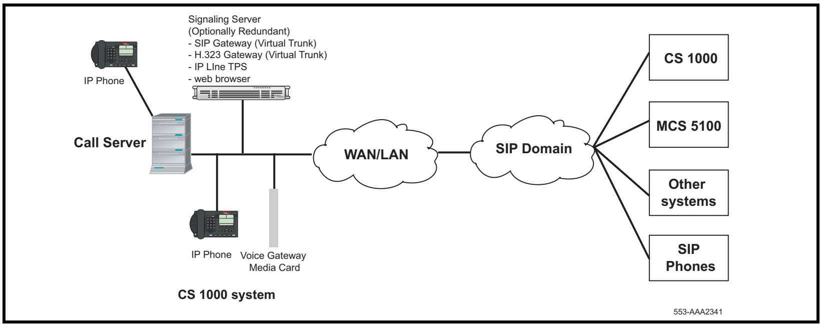
The SIP Trunk Gateway is implemented according to SIP standards. The SIP Trunk Gateway can connect two CS 1000 nodes and can also connect CS 1000 systems to other Nortel or third-party SIP-enabled products. This SIP Trunk Gateway interworks with the MCS 5100 system.

The SIP trunking application resides on the Signaling Server. The SIP Trunk Gateway provides a direct trunking interface between the CS 1000 systems and a SIP domain.

For information, see “SIP Trunk Gateway software — trunk route redundancy” on page 187.

Figure 2 shows the CS 1000 SIP Trunk Gateway interworking.

Figure 2
CS 1000 SIP Trunk Gateway interworking



The direct SIP interface provides the following:

- removes the requirement for a SIP/PRI gateway between the MCS 5100 and the CS 1000 systems
- improves voice quality through peer-to-peer communication of IP devices

SIP connectivity (also known as SIP trunking) provides a direct media path (trunk interface) between a user in the CS 1000 domain and a user residing in a SIP domain.

SIP trunking (the SIP Trunk Gateway) acts as a SIP User Agent and a call-signaling gateway for the telephones (analog [500/2500-type] telephones, digital telephones, and IP Phones).

- As a SIP User Agent, it services one or more end users in making and receiving SIP calls.
- As a call-signaling gateway, the SIP trunking application does the following:
  - maps telephony numbers to and from SIP Uniform Resource Identifiers (URIs)
  - performs client registration
  - maps ISDN messages to and from SIP messages

— establishes the speech path between the desktop and SIP endpoints

SIP requests and responses

Table 6 shows the SIP request methods.

Table 6
SIP request methods (Part 1 of 2)

Method	Description
INVITE	Indicates a user or service is being invited to participate in a call session. A re-INVITE message is an INVITE message that is used after a call is answered.
ACK	Confirms that the client has received a final response to a request.
BYE	Terminates a call and can be sent by either the caller or the called party.
CANCEL	Cancels any pending searches but does not terminate a call that has already been accepted.
OPTIONS	Queries the capabilities of servers.
REFER	Provides a mechanism allowing the party sending the message to be notified of the outcome of the referenced request. This can be used to enable many applications, including call transfer.
UPDATE	Allows a client to update parameters of a session (such as the set of media streams and their codecs) but has no impact on the state of a dialog. In that sense, it is like a re-INVITE message, but unlike re-INVITE, it can be sent before the initial INVITE has been completed.
INFO	Carries session-related control information during a session.

Table 6
SIP request methods (Part 2 of 2)

Method	Description
PRACK	Provides reliable provisional response messages.
SUBSCRIBE/ NOTIFY	Requests notification from remote nodes indicating that certain events have occurred.

Table 7 shows the SIP response methods.

Table 7
SIP response methods

Response numbers	Type of response
SIP 1xx	Informational responses
SIP 2xx	Successful responses
SIP 3xx	Redirection responses
SIP 4xx	Client Failure responses
SIP 5xx	Server Failure responses
SIP 6xx	Global Failure responses

Format of a SIP message

A SIP message consists of the following components:

- start line
- one or more header fields
- an empty line indicating the end of message header
- an optional message body

A start line can be either a request line or a response line:

- A request line distinguishes a request message.
- A response line distinguishes a response message.

Request line

A request line is defined as follows:

Method <space> Request-URI <space> SIP-Version <CRLF>

For example: INVITE sip:john@myServiceProvider.com SIP/2.0

In this example, INVITE is the method, followed by user URI sip:john@myServiceProvider.com, and followed by SIP version.

Response line

A response line is defined as follows:

SIP-Version <space> Status-Code <space> Reason-Phrase <CRLF>

For example: SIP/2.0 100 Trying

In this example, SIP/2.0 is the version string, 100 is the status code, and "Trying" is the text description of status code.

Direct IP Media Paths

With IP Peer Networking, the SIP Trunk Gateway signaling software enables direct IP voice paths to IP devices. An endpoint is the SIP Trunk Gateway that terminates a SIP signaling stream. A SIP Trunk Gateway that terminates SIP signaling registers at the NRS (specifically the SIP Redirect Server in the NRS) as an endpoint. IP Phones interact with the SIP Trunk Gateway software to appear as SIP devices that support Direct IP Media Paths.

> ***Note 1:*** IP Peer Networking supports both Media Gateways and third-party Gateways that have been tested for compatibility. Use the Gateway to enable communication between an H.323 or SIP network and circuit-switched equipment. Interfaces provided by Media Gateways operate in H.323/SIP standard mode and support MCDN feature capabilities. They operate autonomously in the network.
>
> ***Note 2:*** A Media Gateway is a gateway that uses a protocol similar to the Media Gateway Control Protocol (MGCP). The Media Gateway houses peripheral cards. Media Gateways are controlled directly by the

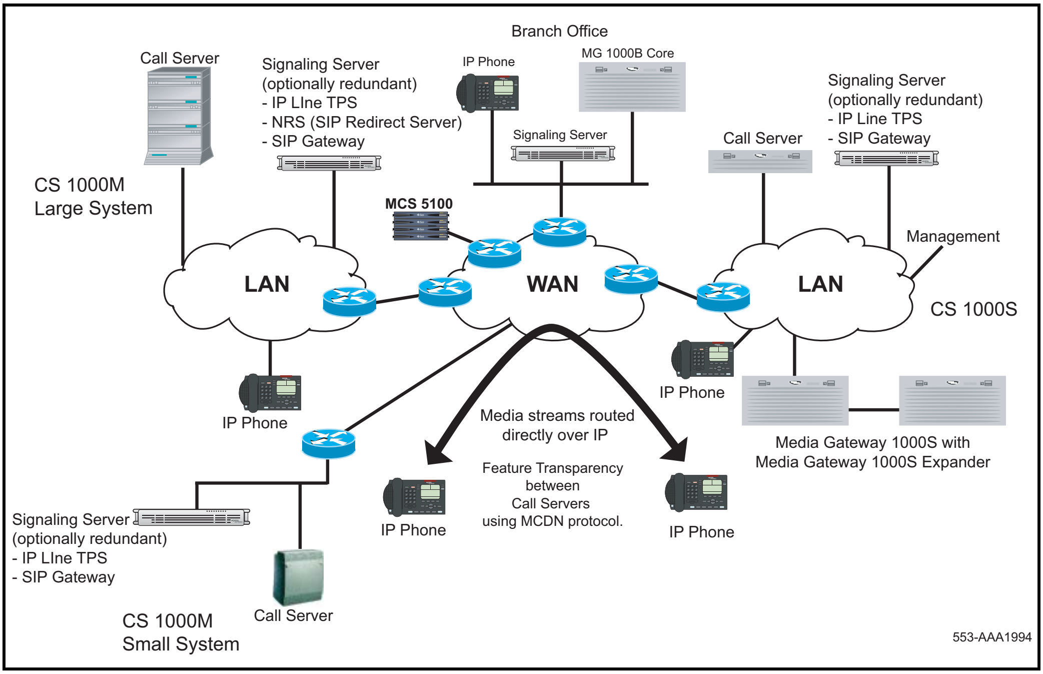
Call Server. Peripheral cards are housed in the Intelligent Peripheral Equipment (IPE) shelf in CS 1000M Systems.

The Direct IP Media Path functionality ensures that when any IP device in the network (for example, an IP Phone) connects to another IP address (for example, an IP Phone), the media path uses direct IP connections and does not pass through a central circuit-switched PBX. When the connection is made between a Virtual Trunk and a circuit-switched device (for example, a PRI trunk), a Digital Signal Processor (DSP) resource on the Voice Gateway Media Card is allocated to transcode the media stream from IP to circuit-switched.

When the network address of the local IP device or DSP resource is determined, the address is signaled over standard SIP to the far end so a direct media path can be established. If a call-modification operation is involved (for example, Call Transfer), further signaling of the address information occurs using the SIP re-INVITE or UPDATE methods.

Figure 3 on page 59 shows a media path routed directly over IP, not using a circuit switch.

Figure 3
An example of IP Peer Networking using Virtual Trunk and direct media paths



IP Phone to IP Phone (on separate Call Servers)

An IP Phone at Site A calls an IP Phone at Site B (see Figure 4 on page 61). When the user presses a key on the IP Phone, a signaling message is carried over the IP network.

The Call Server on the originating node selects an ISDN route and a virtual IP trunk, based on the dialed digits translation. After terminating on a Virtual Trunk, D-channel signaling occurs over IP. This includes basic call setup signals (ISDN over IP, as well as Nortel MCDN signaling over IP, which is used for networking features). The ISDN signaling is converted to a SIP message by the SIP Trunk Gateway on the Signaling Server. MCDN messages are carried within the SIP message, using proprietary SIP message-body extensions.

On the terminating node, the SIP signaling is received at the SIP Trunk Gateway on the Signaling Server. The SIP message is converted to an ISDN message which is then sent to the Call Server. The terminating Call Server translates the received digits to an IP Phone DN. When the terminating IP Phone answers the call, the terminating node returns an ISDN CONNECT message, then converts the ISDN message to the SIP 200 OK message. The Signaling Servers complete the exchange of the IP media information required to establish the IP media path. The originating and terminating Call Servers establish a direct two-way IP media path between the two IP Phones.

Basic network call walk-through

When a user makes a call on a CS 1000 system, the dialed digits are translated to determine if the user is attempting to reach an internal or external telephone.

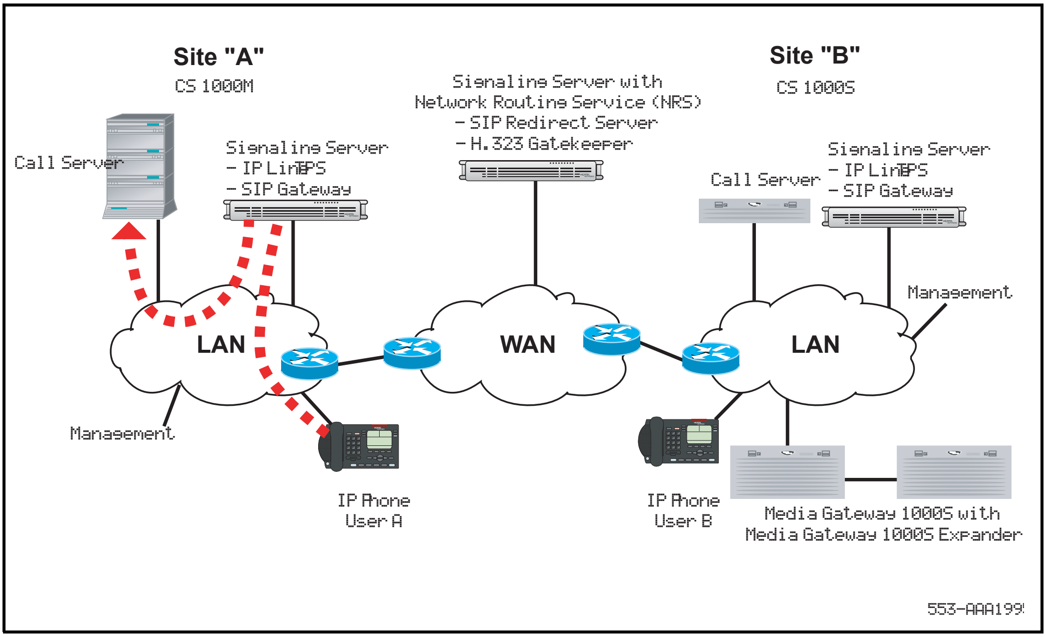
If the user is attempting to reach an internal telephone, the call is terminated on the internal device. When the system determines that the user is attempting to reach a telephone or service using the IP network, the call routes to the SIP Trunk Gateway software. The SIP Trunk Gateway software uses the NRS, specifically the SIP Redirect Server, to help with call routing.

> ***Note:*** Only the primary messages are illustrated in the following call flows.

The following scenario describes the Direct IP Media Path functionality for a basic network call:

1 User A on Call Server A dials the DN of User B on Call Server B. Call Server A collects the digits through the Terminal Proxy Server (TPS) on Signaling Server A. See Figure 4.

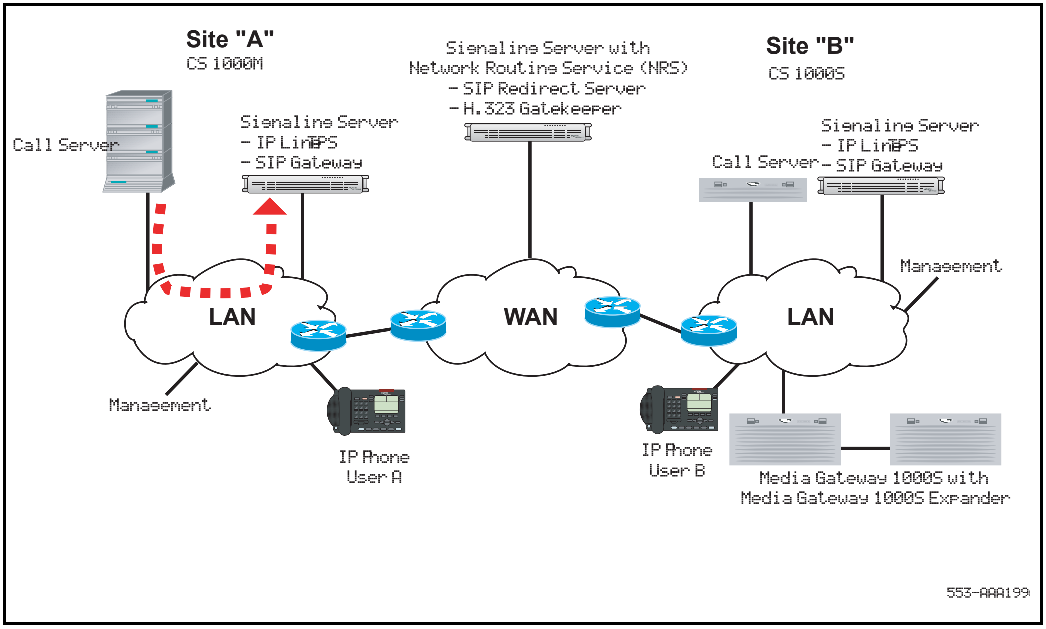
Figure 4
User A dials User B



2 Call Server A determines that the dialed DN is at another site. Call Server A selects the codec list, allocates bandwidth, and routes the call to the SIP Trunk Gateway using the Virtual Trunk. See Figure 5.

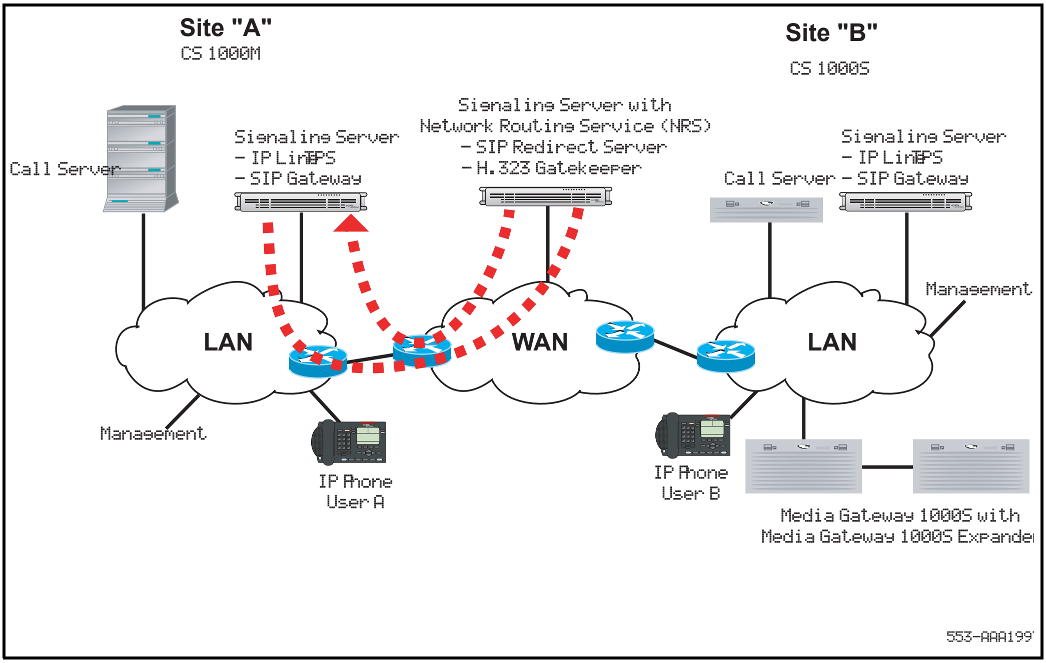
Note: To select which Virtual Trunk to use for routing, Call Server A examines the number dialed, and uses various trunk routing and signaling features (for example, ESN and MCDN).

Figure 5
Call Server A routes the call to the IP network



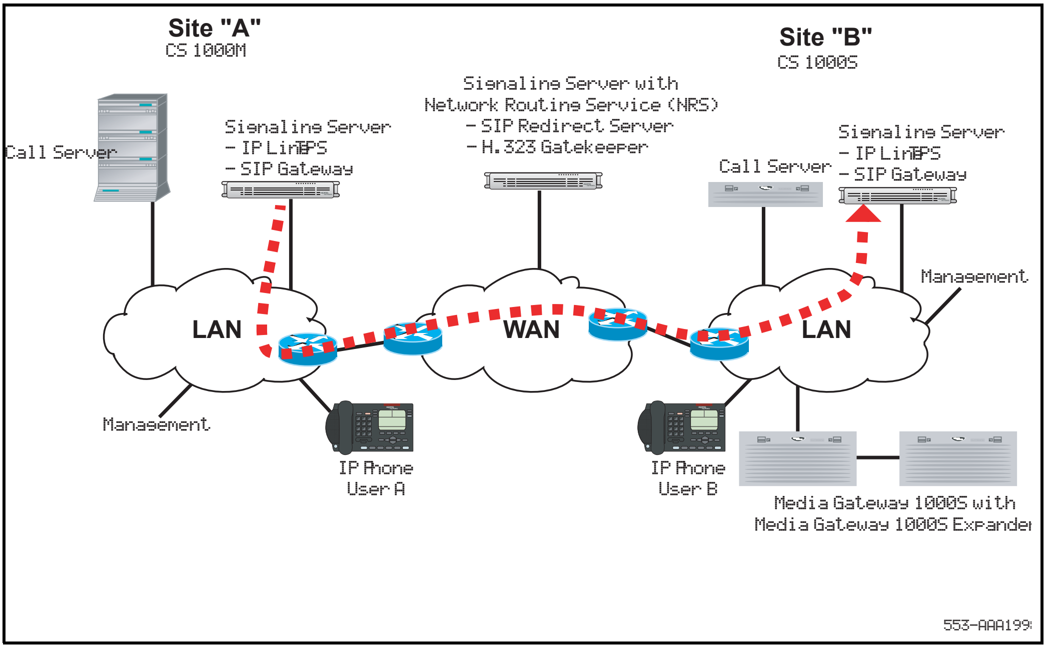
3 SIP Trunk Gateway A asks the NRS to search for the dialed DN in the database (for example, within the appropriate CDP domain). The NRS (SIP Redirect Server) sends the IP address of the SIP Trunk Gateway B to SIP Trunk Gateway A. See Figure 6.

Figure 6
The NRS sends the IP address of SIP Trunk Gateway B to SIP Trunk Gateway A



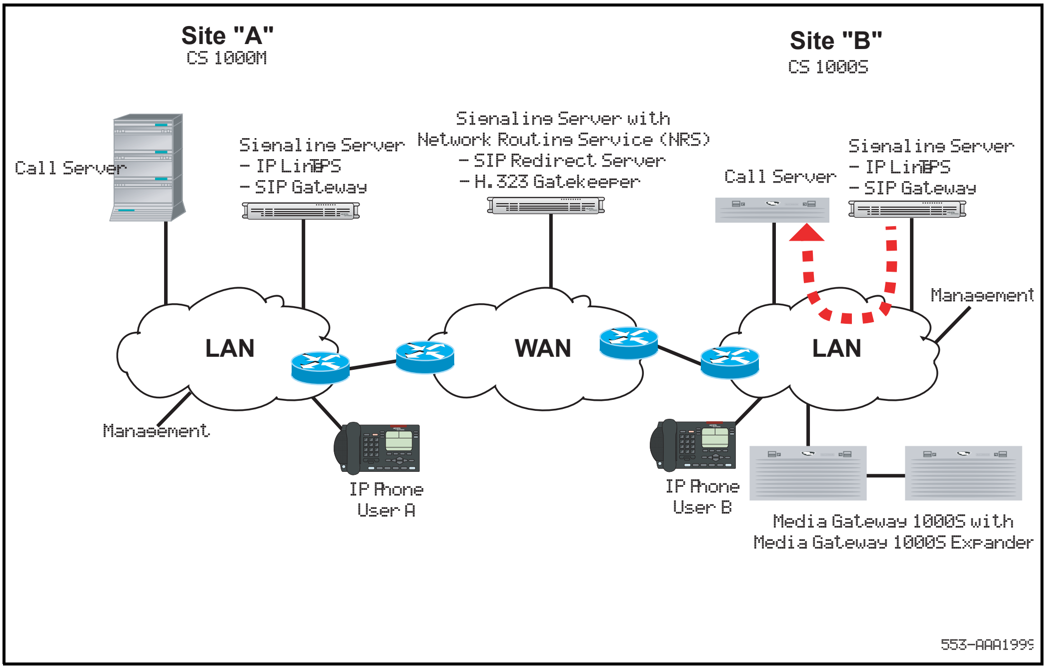
4 SIP Trunk Gateway A sends an INVITE message to SIP Trunk Gateway B, including the DN information. See Figure 7.

Figure 7
SIP Trunk Gateway A sends an INVITE message to SIP Trunk Gateway B



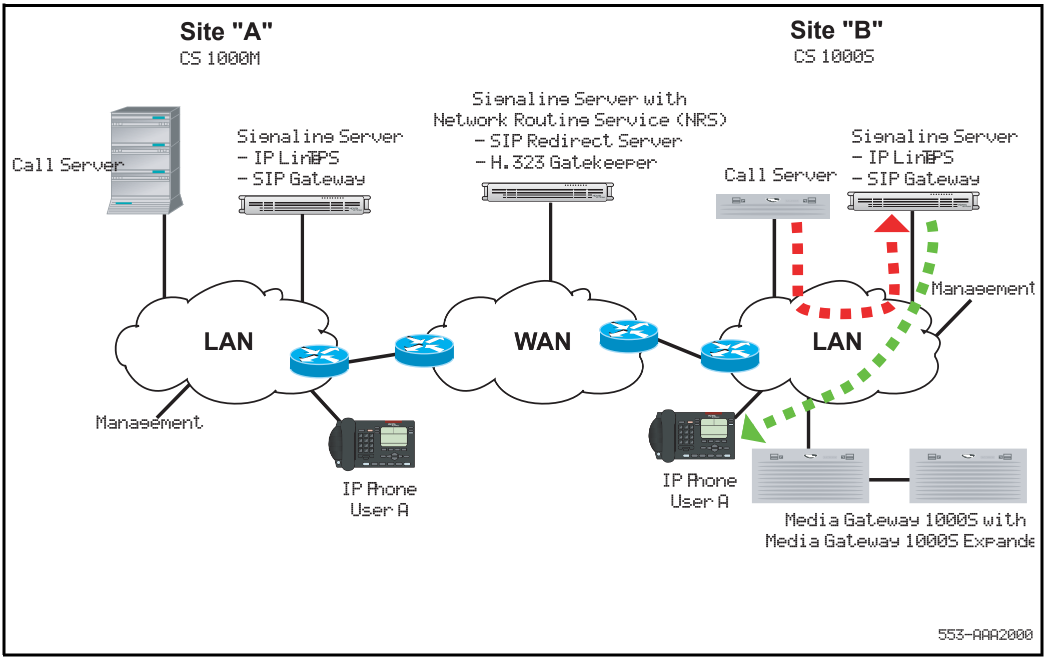
5 SIP Trunk Gateway B treats the incoming call from SIP Trunk Gateway A as an incoming Virtual Trunk call. SIP Trunk Gateway B sends the call to Call Server B over a Virtual Trunk. Call Server B also treats the call as an incoming call from a Virtual Trunk. See Figure 8.

Figure 8
SIP Trunk Gateway B sends the call to Call Server B over a Virtual Trunk



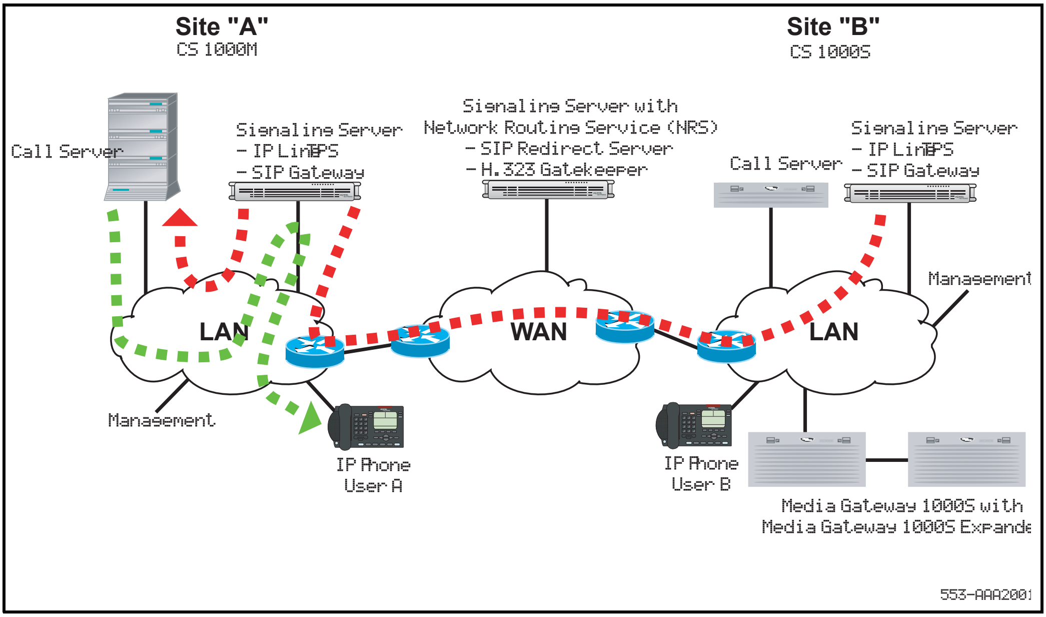
6 Call Server B selects the codec, allocates bandwidth, rings the telephone, and sends an ISDN Alert message to SIP Trunk Gateway B over the Virtual Trunk. See Figure 9.

Figure 9
Call Server B sends an Alert message to SIP Trunk Gateway B



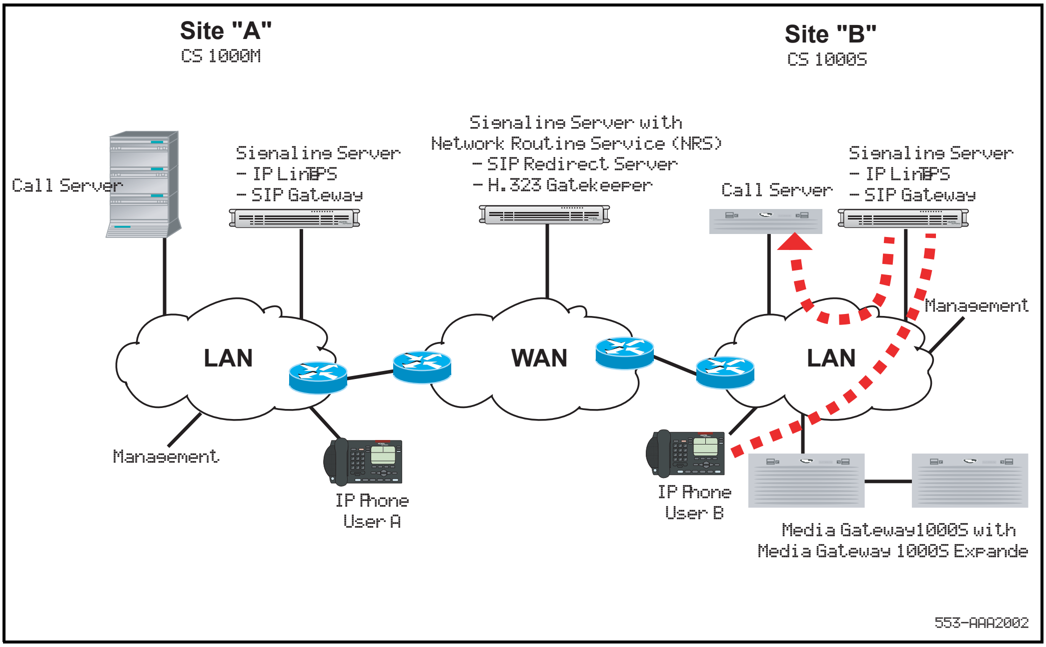
7 SIP Trunk Gateway B converts the ISDN Alert message to a SIP 180 response message. SIP Trunk Gateway B sends the SIP message to SIP Trunk Gateway A. SIP Trunk Gateway A converts the SIP 180 message back to the ISDN Alert message. SIP Trunk Gateway A then sends the message to Call Server A. Call Server A requests that the IP Phone play ringback tone. See Figure 10.

Figure 10
SIP Trunk Gateway B sends an Alert message to Call Server A



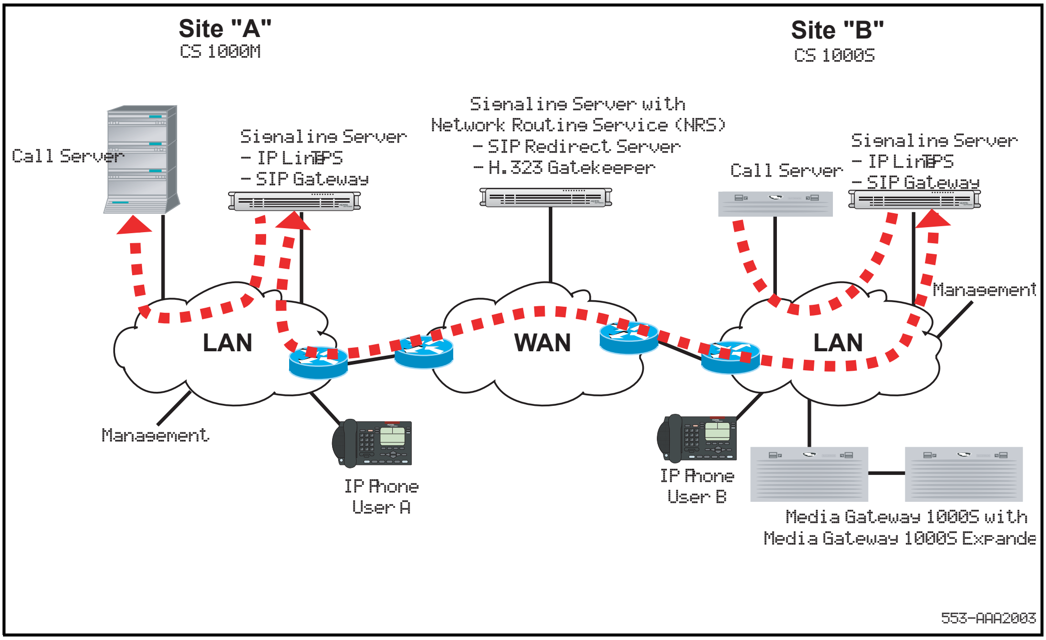
8 User B answers the call. A message is sent to Call Server B through the TPS on Signaling Server B. See Figure 11.

Figure 11
User B answers the call



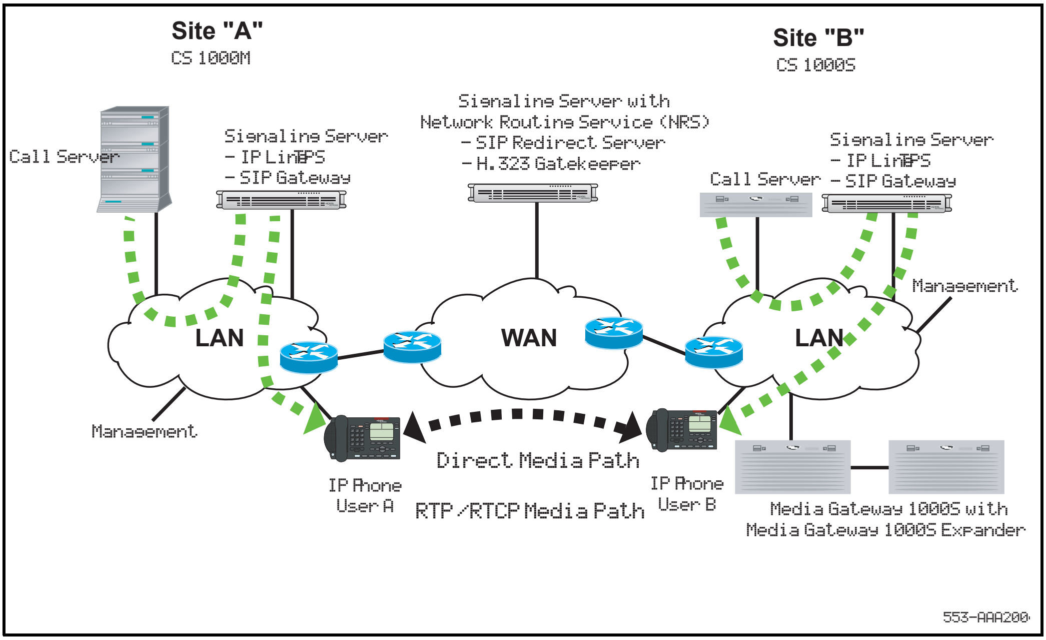
9 Call Server B sends an ISDN CONNECT message to SIP Trunk Gateway B. SIP Trunk Gateway B converts the CONNECT message to the SIP 200 OK message. SIP Trunk Gateway B sends the SIP 200 OK message to SIP Trunk Gateway A. SIP Trunk Gateway A sends an ACK message back to SIP Trunk Gateway B to acknowledge the SIP 200 OK message. SIP Trunk Gateway A converts the SIP 200 OK message back to the ISDN CONNECT message and sends the message to Call Server A over the Virtual Trunk. See Figure 12.

Figure 12
Call Server B sends an ACK message to SIP Trunk Gateway B



10 The Call Servers tell the IP Phones to start the direct IP media paths. The IP Phones then begin to transmit and receive voice over the IP network. See Figure 13.

Figure 13
IP Phones start the direct IP media paths



Call scenarios

In the sections that follow, direct IP-media-path operation is described for a number of call scenarios. Each scenario uses IP Peer Networking to provide a direct IP media path between the peers taking part in the call. In all cases, the IP signaling path separates from the IP media path. Depending on the originating and terminating terminal types, the media path is between one of the following:

- IP Phone and IP Phone
- IP Phone and circuit-switched gateway
- circuit-switched gateway and circuit-switched gateway

- SIP Phone and SIP Phone (see page 528)
- SIP Gateway and SIP Phone (see page 533)

In each case, the IP signaling path is the same; the trunk is virtual instead of physical.

IP Phone to circuit-switched telephone (on separate Call Servers)

An IP Phone on Node A calls a circuit-switched telephone (for example, an analog [500/2500-type] telephone) on Node B.

The Call Server on the originating node selects an ISDN route and Virtual Trunk, based on the dialed digits translation. The ISDN signaling routes through the Signaling Server and encodes using SIP.

On the terminating node, the SIP signaling is received at the Signaling Server, and converts the SIP message to an ISDN message. The ISDN message is forwarded to the Call Server. The terminating Call Server translates the received digits to the DN of a circuit-switched device. The Call Server determines that the call is incoming on a Virtual Trunk and terminating on a circuit-switched device, and selects a DSP resource on a Voice Gateway Media Card. The DSP performs IP-to-circuit-switched conversion when the call is established.

When the terminating circuit-switched party answers the call, the terminating Call Server returns an ISDN CONNECT message. The message is sent to the SIP Trunk Gateway on the Signaling Server. The SIP Trunk Gateway on the Signaling Servers converts the ISDN CONNECT message to a SIP 200 OK message and the Signaling Server completes the exchange of IP media information required to establish the IP media path. The originating and terminating Call Servers establish a direct two-way IP media path between the IP Phone and the DSP. The terminating node also establishes a circuit-switched speechpath between the DSP and the circuit-switched telephone.

> ***Note:*** If a Voice Gateway Media Card channel is not available when required for IP to circuit-switched connections, call processing treats the scenario the same way current traffic timeslot blocking is handled. If all Virtual Trunks in a route are busy when call routing is attempted, the

routing operates the same way as physical trunks by routing the call to the next available route selection.

IP Phone to Recorded Announcement or Music

In certain call scenarios, an IP Phone requires a Recorded Announcement (RAN) or Music treatment from a remote node. For example, an IP Phone is placed on hold by a party on a remote node that has Music on Hold configured.

When the IP Phone is placed on hold by the holding party, the direct IP media path that had been established between the two parties is torn down. A new IP media path is established between the IP Phone and a circuit-switched gateway on the node providing the Music.

The media path, in this case, is one way only (from the circuit-switched gateway to the IP Phone). This media-path redirection is initiated by the node providing the Music, using the SIP re-INVITE or UPDATE methods. No ISDN signaling is exchanged between the nodes, and the call state on the originating node is unchanged.

IP Peer Networking supports RAN Broadcast and Music Broadcast. The RAN and Music Broadcast features enable multiple listeners to share the same RAN and Music trunks to listen to a recorded announcement or music. However, one DSP channel is required for each user. IP Peer Networking does not support IP broadcast/multicast of RAN or Music.

When the holding party retrieves the held call, the media path is torn down, and a two-way IP media path is reestablished between the parties.

Virtual Trunk to Virtual Trunk

An incoming call to a node over a Virtual Trunk is routed over another Virtual Trunk based on the translation of digits in the SIP INVITE message. A call between two parties on remote nodes is tandemed through this node.

The call originates on the incoming Virtual Trunk. ISDN signaling is converted and exchanged between the originating node and the tandem node using SIP. The call terminates on the outgoing Virtual Trunk, and ISDN signaling is converted and exchanged between the tandem node and the terminating node using SIP.

The ISDN signaling generated at the end node is sent through the tandem node and processed by the Call Server. The Call Server processes the call as it does a normal tandem call. The exchange of IP call parameters between the end nodes is sent through the tandem node's Signaling Server and Call Server, so each end node can establish a direct IP media path between end parties.

The IP media path is established directly between the originating and terminating parties on the end nodes. No media resources are used on the tandem switch. When trunks are not optimized, signaling continues to be handled in a tandem manner, even though the media path is direct.

Tandem operations

All media paths route directly over IP networks. However, to maintain proper control points and billing records for a call, sometimes signaling must be indirect. The following sections describe indirect signaling operations for these scenarios.

Direct tandem calls

Because SIP IP Peer Networking uses the NRS (specifically the SIP Redirect Server) for address resolution, there is minimal requirement for tandem calls. With an NRS (SIP Redirect Server), each node can obtain the IP address of the terminating node. Therefore, calls route directly to the terminating node and not through a tandem node.

Feature modification (for example, Call Transfer) can cause calls to tandem. Tandem calls also occur when routing is configured as tandem, so accounting records can generate during calls from a third-party gateway.

Tandem feature calls

When a tandem call occurs due to a transfer operation, the IP media paths between the originating party and the "transferred-to" party must be redirected to each other. This redirection is initiated by the transferring (tandem) node.

This scenario describes a form of the Trunk Route Optimization (TRO)/ MCDN feature.

When a tandem call occurs due to a Call Forward operation, it attempts to use TRO to optimize the route between the originating and "transferred-to" parties. In the event packaging or user provisioning selections mean that TRO is not supported, the tandem node initiates media path redirection for both parties.

TRO is used when a call from Node A to Node B forwards to Node C. Node B sends a TRO facility message to Node A. The message contains the digits of the "forwarded-to" party. Node A resolves these digits to a route and determines whether it has a direct route configured to Node C.

IP Peer handling of TRO differs slightly from the PRI handling at this point. With PRI, each destination has a dedicated route and ISDN link. With IP Peer, in the Node A routing configuration, all remote locations are reached using the same Virtual Trunk (the SIP Redirect Server subsequently translates the digits to separate IP nodes). When TRO is attempted at Node A, the call processing finds that the new destination is accessed through the same Virtual Trunk route, and accepts the TRO even though the call does not have an alternate direct route to Node C. The tandem call routing through Node B is cleared. Node A places a new call through the same Virtual Trunk route and IP D-channel that was used for the original call to Node B. The SIP Redirect Server translation identifies the correct destination, Node C, and the call is placed directly to that node.

In cases where the TRO feature does not optimize trunks, the Virtual Trunks must remain busy at Nodes A, B, and C until the call is released. A direct media path between Node A and Node C supports the connection; Node B is not on the media path. This eliminates voice quality problems caused by multiple transcoding steps.

Circuit-switched tandem calls

The IP Peer Networking feature supports circuit-switched tandem calls by configuring a circuit-switched TIE trunk on a CS 1000 system or gateway which routes calls across the IP network. The signaling over the circuit-switched trunk can use any of the TIE trunks supported in traditional MCDN circuit-switched networks.

Virtual Trunk calls in conference

A party on Node A calls a party on Node B. The party on Node B creates a three-party conference with a party on Node C. A circuit-switched conference circuit is used on Node B. Each party has their media path redirected to a separate circuit-switched gateway on Node B. Circuit-switched speech paths are established between each circuit-switched gateway and the conference bridge.

Virtual Trunk to circuit-switched party transferred to an IP Phone

The following occurs in this scenario:

- A call is established between a party on a remote node (the caller) and a circuit-switched party on the local node (the called party) using a Virtual Trunk.

  A media path exists between the caller (which can be an IP Phone or a circuit-switched gateway) and a circuit-switched gateway on the local node.

- The called party transfers the call to an IP Phone on the local node.

  When the called party initiates the transfer operation, the caller is placed on hold, using the re-INVITE message. The existing media path remains allocated. A local call (called a consultation call) is set up between the transferring called party and the local IP Phone to which the call is to be transferred.

- When the transfer is complete, the consultation call is released, and a call is set up between the caller and the IP Phone to which the call was transferred. The original media path between the caller and the called party is redirected using the SIP re-INVITE or UPDATE methods. Because the IP Phone to which the call was transferred is not a circuit-switched telephone, the circuit-switched gateway resource is released.

- A direct media path is set up between the caller and the IP Phone.

Virtual Trunk to a circuit-switched party “transferred before answer” to an IP Phone

The following occurs in this scenario:

- A call is established between a party on a remote node (the caller) and a circuit-switched party on the local node (the called party) over a Virtual Trunk.

  A direct IP media path exists between the caller (for example, an IP Phone or circuit-switched gateway) and a circuit-switched gateway on the local node.

- The called party initiates a transfer to an IP Phone on the local node before answering the call. While the IP Phone is ringing, the called party completes the transfer by disconnecting or pressing the Transfer key. The caller receives ringback tone.

  When the called party initiates the Transfer operation, the incoming Virtual Trunk (and indirectly, the caller) is placed on hold, and the direct IP media path between the caller and the circuit-switched gateway is torn down. If Music or RAN is configured, a new IP media path is established between a circuit-switched gateway and the caller.

- When the called party completes the “transfer before answer”, ringback tone is provided to the caller. A new one-way IP media path is established between a circuit-switched gateway on the node providing the ringback tone and the caller. The node providing the ringback tone initiates this media path “redirection” using the SIP re-INVITE or UPDATE methods. It does not use ISDN signaling for this purpose.

- When the party on the transferred-to IP Phone answers, another media path redirection occurs. The media path between the circuit-switched gateway and the caller is released, and a new two-way IP media path is established between the caller and the party answering the IP Phone to which the call was transferred. This uses the SIP re-INVITE or UPDATE methods.

IP Phone to local IP Phone transferred to a Virtual Trunk

A call is established between two IP Phones on the same node. A direct media path exists between the two telephones. One of the parties initiates a transfer to a party on a remote node.

When the IP Phone party initiates the transfer, call processing on the local node places the other party on hold. The media path between the two IP Phones is torn down. A call is set up between the transferring IP Phone and the remote party (this could be an IP Phone or circuit-switched telephone). See "IP Phone to IP Phone (on separate Call Servers)" on page 59.

When the transferring IP Phone completes the transfer before answer, the consultation call between the IP Phone and the remote party is torn down and a call is set up between the transferred IP Phone and the remote party. The media path that existed between the remote party and the transferring IP Phone is redirected using the SIP re-INVITE or UPDATE methods. No ISDN signaling is exchanged between the nodes, and the call state on the terminating node is unchanged. A direct IP media path is established between the transferred IP Phone and the remote party.

H.323 signaling

Contents

This section contains information on the following topics:

Direct IP Media Paths

With IP Peer Networking, the H.323 Gateway Signaling software enables direct IP voice paths to IP devices. An endpoint is the H.323 Gateway that terminates an H.323 signaling stream. An H.323 Gateway that terminates H.323 signaling registers at an H.323 Gatekeeper as an endpoint. IP Phones interact with the Gateway software to appear as H.323 devices that support Direct IP Media Paths.

Note 1: IP Peer Networking supports both Media Gateways and third-party Gateways that have been tested for compatibility. Use the Gateway to enable communication between an H.323 or SIP network and circuit-switched equipment. Interfaces provided by Media Gateways operate in H.323/SIP standard mode and support MCDN feature capabilities. They operate autonomously in the network.

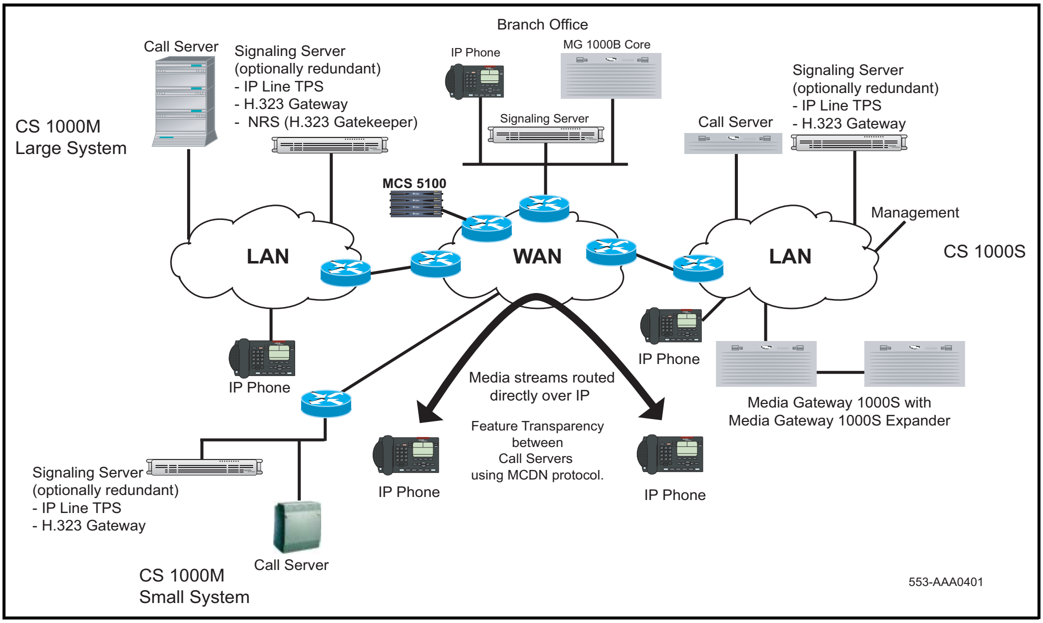
Note 2: A Media Gateway is a gateway that uses a protocol similar to the Media Gateway Control Protocol (MGCP). The Media Gateway houses peripheral cards. Media Gateways are controlled directly by the Call Server.

Direct IP Media Path functionality ensures that, when any IP device in the network (for example, an IP Phone) connects to another IP address (for example, an IP Phone), the media path uses direct IP connections and does not pass through a central circuit-switched PBX. When the connection is made between a Virtual Trunk and a circuit-switched device (for example, a PRI trunk), a DSP resource is allocated to transcode the media stream from IP to circuit-switched.

When the network address of the local IP device or DSP resource is determined, the address is signaled using standard H.323 protocol to the far end so a direct media path can be established. If a call modification operation is involved (for example, Call Transfer), further signaling of the address information occurs using standard H.323 Pause and Reroute protocol.

Figure 14 shows a media path routed directly over IP, not using a circuit switch.

Figure 14
An example of IP Peer Networking using Virtual Trunk and direct media paths



IP Phone to IP Phone (on separate Call Servers)

An IP Phone at Site A calls an IP Phone at Site B (see Figure 15 on page 82). When the user presses a key on the IP Phone, a signaling message is carried over the IP network.

The Call Server on the originating node selects an ISDN route and a virtual IP trunk, based on the dialed digits translation. After terminating on a Virtual Trunk, D-channel signaling occurs over IP. This includes basic call setup signals (Q.931 over IP, as well as Nortel MCDN signaling over IP, which is used for networking features). The ISDN Q.931 signaling is routed using the Signaling Server and encoded using the H.323 protocol. MCDN messages are carried within the H.323 protocol, using standard H.323 facilities for proprietary extensions.

On the terminating node, the H.323 signaling is received at the Signaling Server, and the ISDN Q.931 messages are forwarded to the Call Server. The terminating Call Server translates the received digits to an IP Phone DN. When the terminating IP Phone answers the call, the terminating node returns a Q.931 CONNECT message, and the Signaling Servers complete the exchange of the IP media information required to establish the IP media path. The originating and terminating Call Servers establish a direct two-way IP media path between the two IP Phones.

Basic network call walk-through

When a user makes a call on a CS 1000 system, the dialed digits are translated to determine if the user is attempting to reach an internal or external telephone.

By default, H.323 on CS 1000 systems uses en bloc signaling. For overlap signaling, refer to “Overlap signaling” on page 487.

If the user is attempting to reach an internal telephone, the call is terminated on the internal device. When the system determines that the user is attempting to reach a telephone or service using the IP network, the call routes to the H.323 Gateway software. The H.323 Gateway software uses the NRS (specifically the H.323 Gatekeeper) to help with call routing.

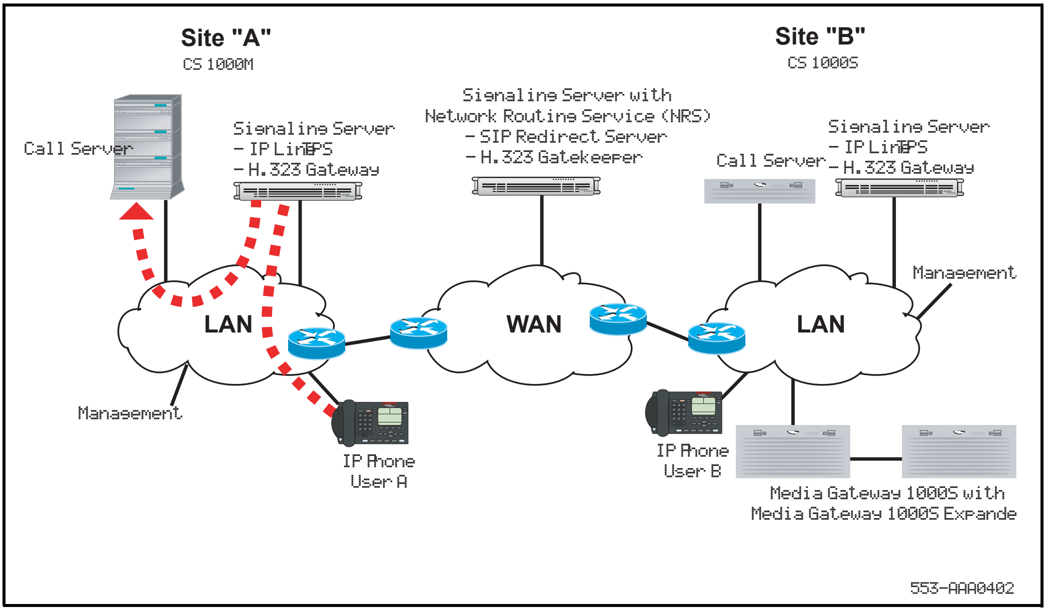
Note 1: Configure Virtual Trunk routes as circuit-switched routes. Use CS 1000 Element Manager or LD 14 and LD 16 in the Command Line Interface (CLI). See “Configuring the Virtual routes and trunks” on page 298.

Note 2: Only the primary messages are illustrated in the following call flows.

The following scenario describes the Direct IP Media Path functionality for a basic network call using en bloc signaling:

1 User A on Call Server A dials the DN of User B on Call Server B. Call Server A collects the digits through the Terminal Proxy Server (TPS) on the Signaling Server A. See Figure 15.

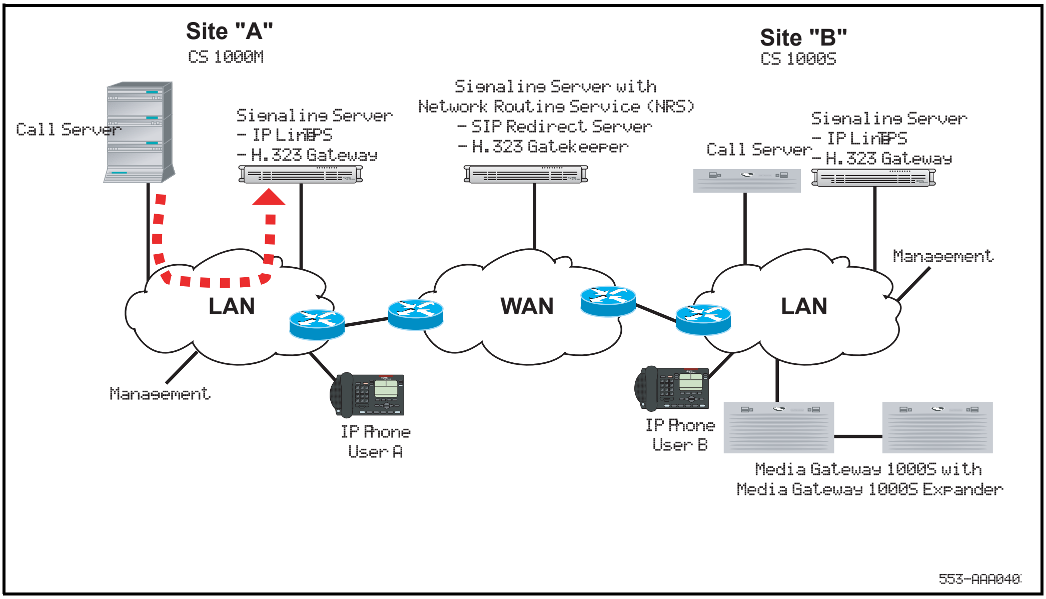
Figure 15
User A dials User B



2 Call Server A determines that the dialed DN is at another site. Call Server A selects the codec list, allocates bandwidth, and routes the call to the IP network using a Virtual Trunk and an H.323 Gateway. See Figure 16.

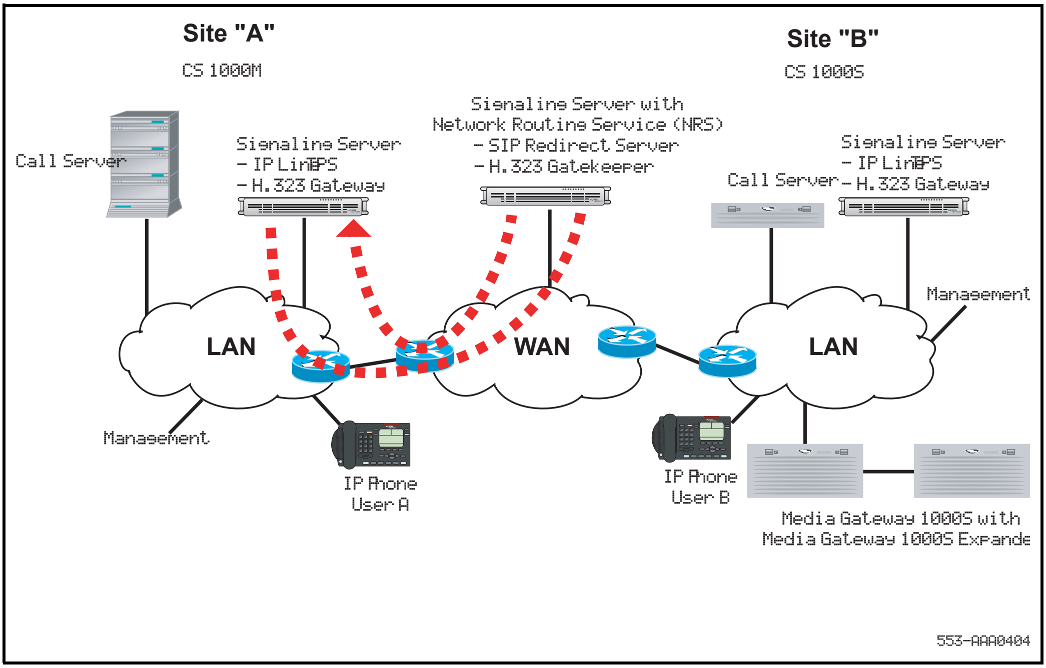
Note: To select which Virtual Trunk to use for routing, Call Server A examines the number dialed and uses various trunk routing and signaling features (for example, ESN and MCDN).

Figure 16
Call Server A routes the call to the IP network



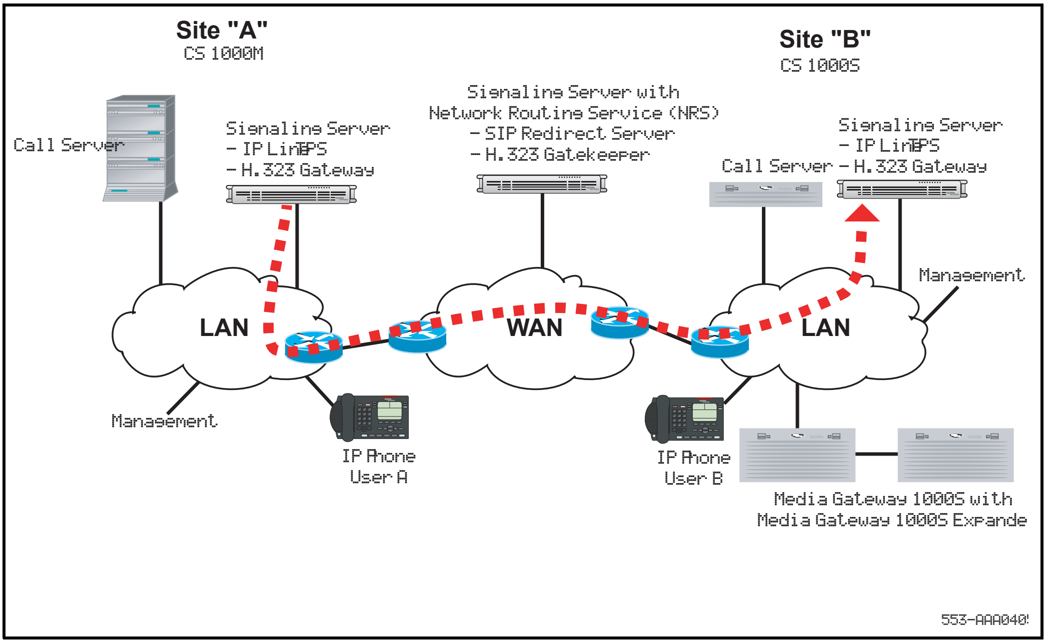
3 H.323 Gateway A asks the NRS (specifically the H.323 Gatekeeper) to search for the dialed DN in the database (for example, within the appropriate CDP domain). The NRS (H.323 Gatekeeper) sends the IP address of H.323 Gateway B to H.323 Gateway A. See Figure 17.

Figure 17
The H.323 Gatekeeper sends the IP address of H.323 Gateway B to H.323 Gateway A



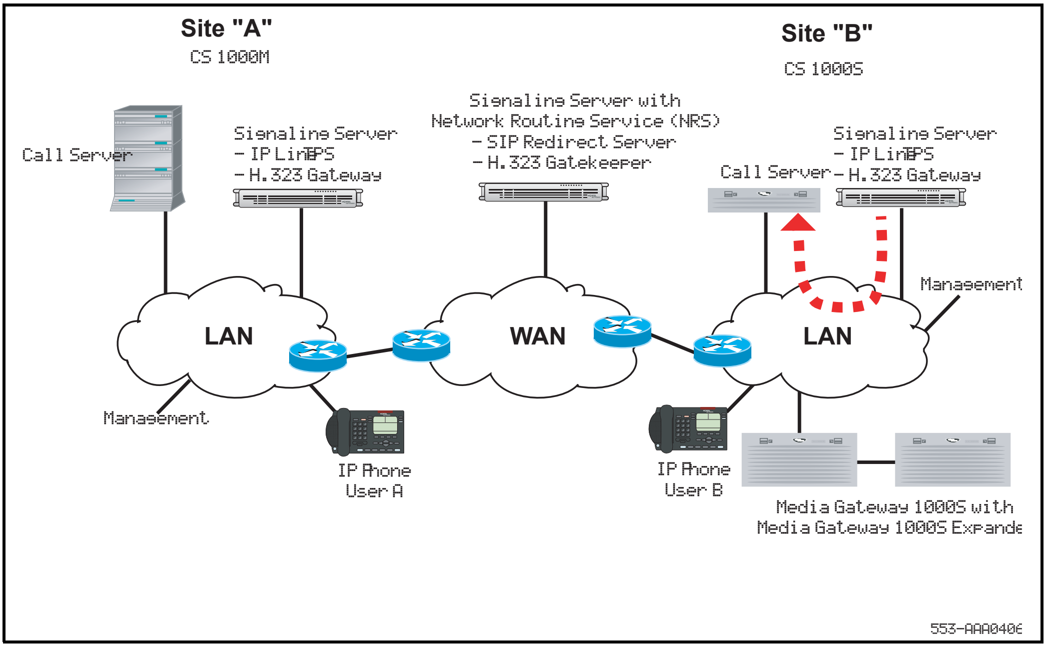
4 H.323 Gateway A sends a SETUP message to H.323 Gateway B, including the DN information. See Figure 18.

Figure 18
H.323 Gateway A sends a SETUP message to H.323 Gateway B



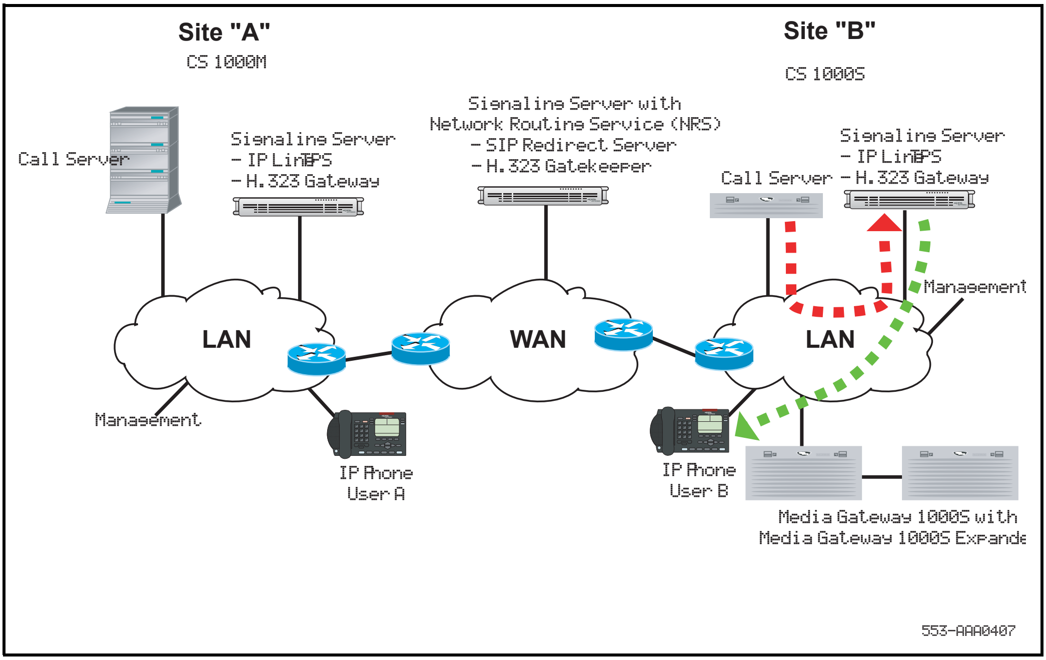
5 H.323 Gateway B treats the call as an incoming call from a Virtual Trunk. H.323 Gateway B sends the call to Call Server B over a Virtual Trunk. Call Server B also treats the call as an incoming call from a Virtual Trunk. See Figure 19.

Figure 19
Gateway B sends the call to Call Server B over a Virtual Trunk



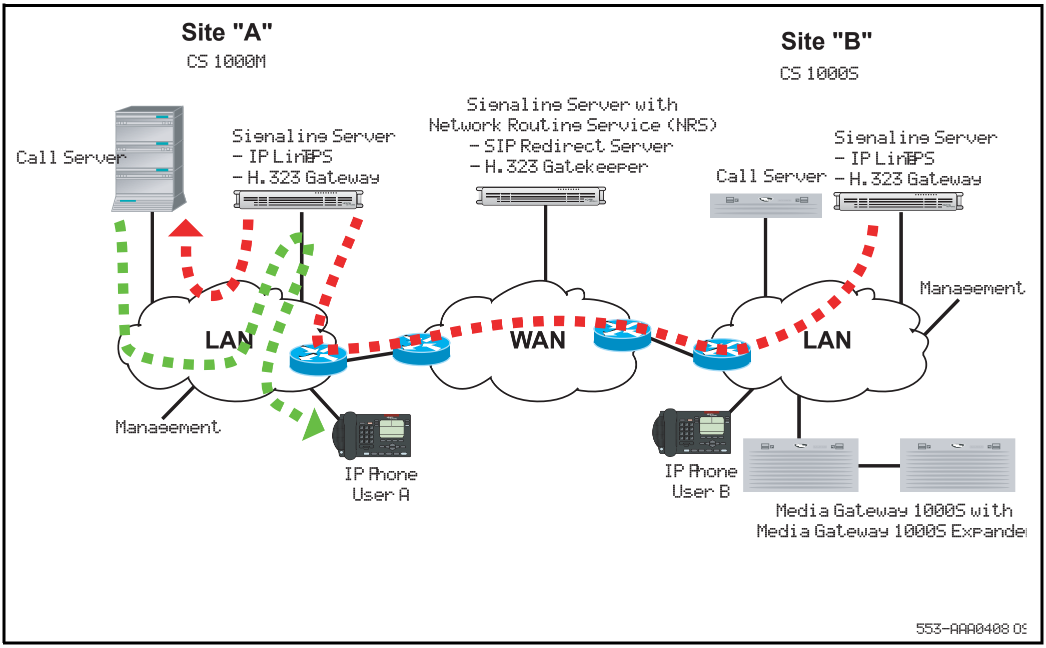
6 Call Server B selects the codec, allocates bandwidth, rings the telephone, and sends an alerting message to H.323 Gateway B. See Figure 20.

Figure 20
Call Server B sends an alerting message to H.323 Gateway B



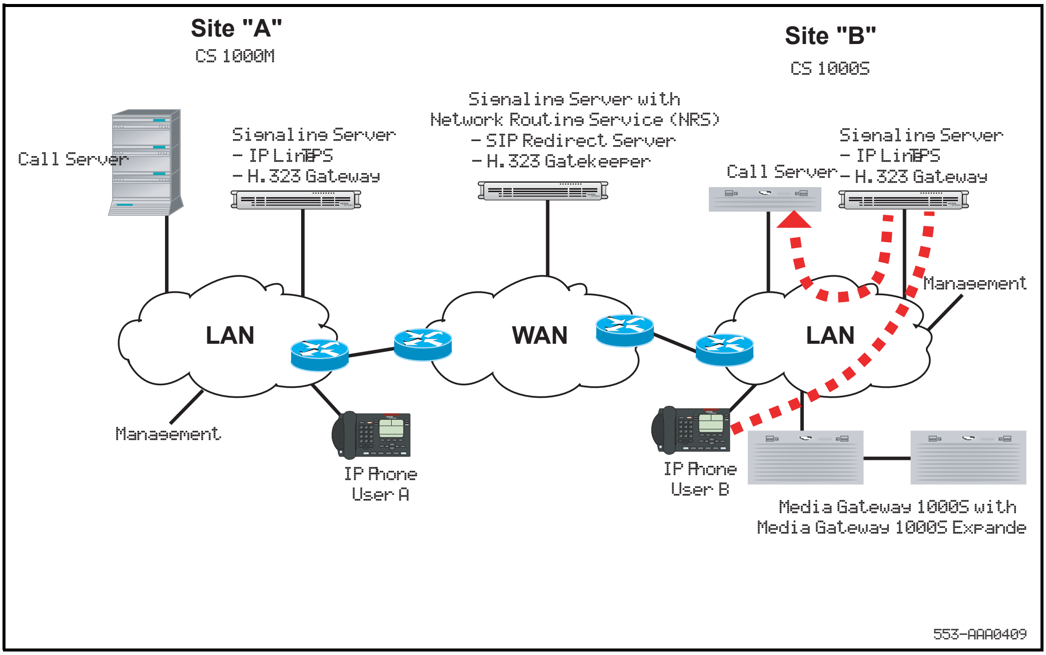
7 H.323 Gateway B sends an alerting message to Call Server A. Call Server A requests that the IP Phone play ringback tone. See Figure 21.

Figure 21
H.323 Gateway B sends an alerting message to Call Server A



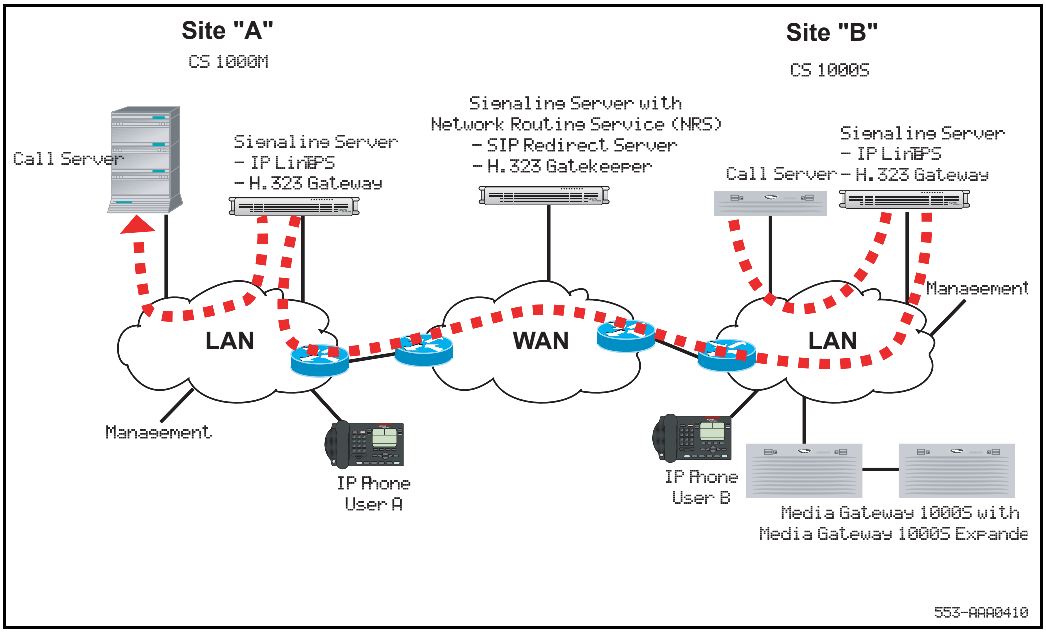
8 User B answers the call. A message is sent to Call Server B through the TPS on the Signaling Server. See Figure 22.

Figure 22
User B answers the call



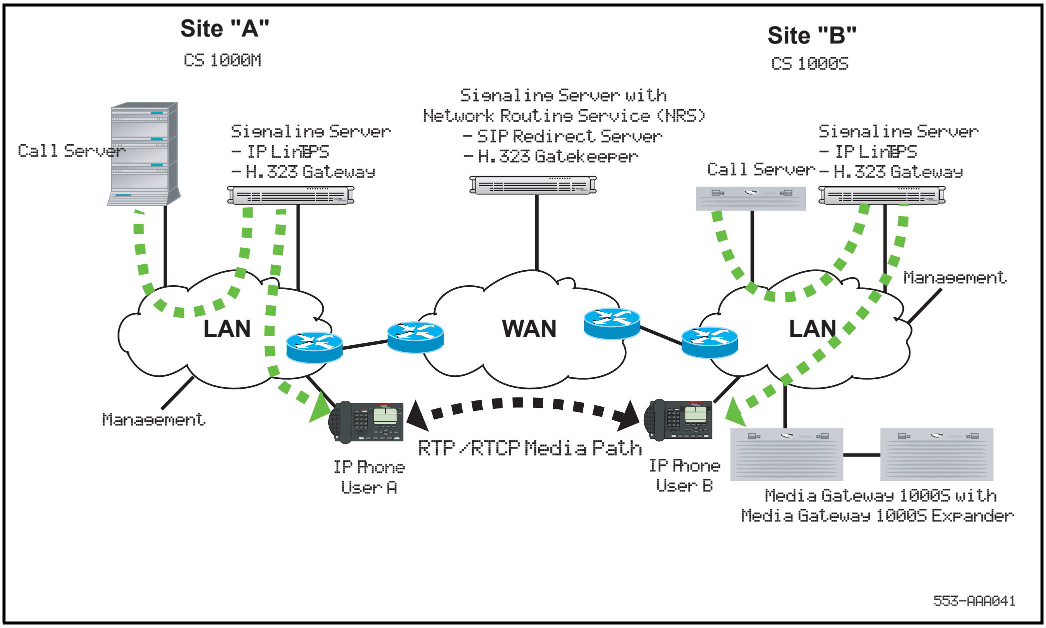
9 Call Server B sends a CONNECT message to H.323 Gateway B. H.323 Gateway B sends an H.323 CONNECT message to H.323 Gateway A and Call Server A. See Figure 23.

Figure 23
Call Server B sends a CONNECT message to Gateway B



10 The Call Servers tell the IP Phones to start the direct IP media paths. The IP Phones then begin to transmit and receive voice over the IP network. See Figure 24.

Figure 24
IP Phones start the direct IP media paths



Call scenarios

In the sections that follow, direct IP media path operation is described for a number of call scenarios. Each scenario uses IP Peer Networking to provide a direct IP media path between the peers taking part in the call. In all cases, the IP signaling path separates from the IP media path. Depending on the originating and terminating terminal types, the media path is between one of the following:

- IP Phone and IP Phone
- IP Phone and circuit-switched gateway
- circuit-switched gateway and circuit-switched gateway

In each case, the IP signaling path is the same; the trunk is virtual instead of physical.

IP Phone to circuit-switched telephone (on separate Call Servers)

An IP Phone on Node A calls a circuit-switched telephone (for example, an analog [500/2500-type] telephone) on Node B.

The Call Server on the originating node selects an ISDN route and Virtual Trunk, based on the dialed digits translation. The ISDN Q.931 signaling messages that route through the Signaling Server are encoded using the H.323 protocol.

On the terminating node, the H.323 signaling is received at the Signaling Server, and the ISDN Q.931 messages forward to the Call Server. The terminating Call Server translates the received digits to the DN of a circuit-switched device. The Call Server determines that the call is incoming on a Virtual Trunk and terminating on a circuit-switched device, and selects a DSP resource on a Voice Gateway Media Card. The DSP performs IP-to-circuit-switched conversion when the call is established.

When the terminating circuit-switched party answers the call, the terminating node returns a Q.931 CONNECT message, and the Signaling Servers complete the exchange of IP media information required to establish the IP media path. The originating and terminating Call Servers and Media Gateway SSC establish a direct two-way IP media path between the IP Phone and the DSP. The terminating node also establishes a circuit-switched speechpath between the DSP and the circuit-switched telephone.

> ***Note:*** If a Voice Gateway Media Card channel is not available when required for IP to circuit-switched connections, call processing treats the scenario the same way current call blocking is handled. If all Virtual Trunks in a route are busy when call routing is attempted, the routing operates the same way as physical trunks by routing the call to the next available route selection.

IP Phone to Recorded Announcement or Music

In certain call scenarios, an IP Phone requires a Recorded Announcement (RAN) or Music treatment from a remote node. Such a scenario could occur, for example, if an IP Phone is placed on hold by a party on a remote node that has Music on Hold configured.

When the IP Phone is placed on hold by the holding party, the direct IP media path that had been established between the two parties is torn down. A new IP media path is established between a circuit-switched gateway on the node providing the Music and the IP Phone.

The media path, in this case, is one way only (from the circuit-switched gateway to the IP Phone). This media path redirection is initiated by the node providing the Music, using the H.323 third-party initiated pause and re-routing mechanism. No ISDN Q.931 signaling is exchanged between the nodes, and the call state on the originating node is unchanged.

IP Peer Networking supports RAN Broadcast and Music Broadcast. The RAN and Music Broadcast features enable multiple listeners to share the same RAN and Music trunks to listen to a recorded announcement or music. However, one DSP channel is required for each user. IP Peer Networking does not support IP broadcast/multicast of RAN or Music.

When the holding party retrieves the held call, the media path is torn down, and a two-way IP media path is reestablished between the parties.

Virtual Trunk to Virtual Trunk

An incoming call to a node over a Virtual Trunk is routed over another Virtual Trunk based on the translation of digits in the Q.931 SETUP message. A call between two parties on remote nodes is tandemed through this node.

The call originates on the incoming Virtual Trunk. ISDN Q.931 signaling is exchanged between the originating node and the tandem node using the H.323 protocol. The call terminates on the outgoing Virtual Trunk, and ISDN Q.931 signaling is exchanged between the tandem node and the terminating node using the H.323 protocol.

The ISDN Q.931 signaling generated at the end node is sent through the tandem node and processed by the Call Server. The Call Server processes the call as it does a normal tandem call. The exchange of IP call parameters between the end nodes is sent through the tandem node's Signaling Server and Call Server, so each end node can establish a direct IP media path between end parties.

The IP media path is established directly between the originating and terminating parties on the end nodes. No media resources are used on the tandem switch. When trunks are not optimized, signaling continues to be handled in a tandem manner, even though the media path is direct.

Tandem operations

All media paths route directly over IP networks. However, to maintain proper control points and billing records for a call, sometimes signaling must be indirect. The following sections describe indirect signaling operations for these scenarios.

Direct tandem calls

Because IP Peer Networking uses an NRS (H.323 Gatekeeper) for address resolution, the requirement for tandem calls is minimal. With an NRS (H.323 Gatekeeper), each node can obtain the IP address of the terminating node. Therefore, calls route directly to the terminating node and not through a tandem node.

Feature modification (for example, Call Transfer) can cause calls to tandem. Tandem calls also occur when routing is configured as tandem, so accounting records can generate during calls from a third-party gateway.

Tandem feature calls

When a tandem call occurs due to a transfer operation, the IP media paths between the originating party and the “transferred-to” party must be redirected to each other. This redirection is initiated by the transferring (tandem) node.

This scenario describes a form of Trunk Route Optimization (TRO).

When a tandem call occurs due to a Call Forward operation, it attempts to use TRO to optimize the route between the originating and “transferred-to” parties. If packaging or user provisioning selections mean that TRO is not supported, the tandem node initiates media path redirection for both parties.

TRO is used when a call from Node A to Node B forwards to Node C. Node B sends a TRO facility message to Node A. The message contains the digits of the “forwarded-to” party. Node A resolves these digits to a route and determines whether it has a direct route configured to Node C.

IP Peer handling of TRO differs slightly from the PRI handling at this point. Unlike the Primary Rate case where each destination has a dedicated route and ISDN link, for IP Peer, in Node A’s routing configuration, all remote locations are reached using the same Virtual Trunk (the H.323 Gatekeeper subsequently translates the digits to separate IP nodes). When TRO is attempted at Node A, the call processing finds that the new destination is accessed through the same Virtual Trunk route, and accepts the TRO even though the call does not have an alternate direct route to Node C. The tandem call routing through Node B is cleared. Node A places a new call through the same Virtual Trunk route and IP D-channel that was used for the original call to Node B. H.323 Gatekeeper translation identifies the correct destination, Node C, and the call is placed directly to that node.

In cases where the TRO feature does not optimize trunks, the Virtual Trunks must remain busy at Nodes A, B and C until the call is released. A direct media path between Node A and Node C supports the connection; Node B is not on the media path. This eliminates voice quality problems caused by multiple transcoding steps.

Circuit-switched tandem calls

The IP Peer Networking feature supports circuit-switched tandem calls by configuring a circuit-switched TIE trunk on a CS 1000 system, or gateway which routes calls across the IP network. The signaling over the circuit-switched trunk can use any of the TIE trunks supported in traditional MCDN circuit-switched networks.

Virtual Trunk calls in conference

A party on Node A calls a party on Node B. The party on Node B creates a three-party conference with a party on Node C. A circuit-switched conference circuit is used on Node B. Each party has their media path redirected to a separate circuit-switched gateway on Node B. Circuit-switched speech paths are established between each circuit-switched gateway and the conference bridge.

Virtual Trunk to circuit-switched party transferred to an IP Phone

A call is established between a party on a remote node and a circuit-switched party on the local node using a Virtual Trunk. A media path exists between the remote party (the remote party can be an IP Phone or a circuit-switched gateway) and a circuit-switched gateway on the local node. The local circuit-switched party transfers the call to an IP Phone on the local node.

When the circuit-switched party initiates a transfer operation, call processing on the local node places the remote party on hold, according to existing functionality. H.323 signaling places the remote party in a "paused" state, and the existing media path remains allocated. A local call is set up between the transferring circuit-switched party and the local IP Phone.

When the circuit-switched party completes the transfer, the consultation call is released, and a call is set up between the remote party and the transferred-to party. The media path (that existed between the remote party and the transferring circuit-switched party) is redirected using the H.323 pause and re-routing mechanism. As the transferred-to party is not a circuit-switched telephone, the circuit-switched gateway resource is released. The call scenario completes with a direct media path between the remote party and the IP Phone on the local node.

Virtual Trunk to a circuit-switched party "transferred before answer" to an IP Phone

A call is established between a party on a remote node and a circuit-switched party on the local node over a Virtual Trunk. A direct IP media path exists between the remote party (for example, an IP Phone or circuit-switched gateway) and a circuit-switched gateway on the local node. The local circuit-switched party initiates a transfer to an IP Phone on the local node. While the IP Phone is ringing, the transferring party completes the transfer by disconnecting or pressing the Transfer key. The originating party receives ringback tone.

When the circuit-switched party initiates the Transfer operation, the incoming Virtual Trunk (and indirectly, the originating party) is placed on hold and the direct IP media path between the originating party and the circuit-switched gateway is torn down. If Music or RAN is configured, a new IP media path is established between a circuit-switched gateway and the originating party.

When the transferring party completes the “transfer before answer”, ringback tone must be provided to the originating party. A new IP media path is established between a circuit-switched gateway on the node providing the ringback tone and the originating party. The media path is one way only, from the circuit-switched gateway to the originating party. The node providing the ringback tone initiates this media path “redirection” using the H.323 “Third-party initiated pause and re-routing” mechanism. It does not use ISDN Q.931 signaling for this purpose.

When the party on the IP Phone answers, another media path redirection occurs. The media path between the circuit-switched gateway and the originating party is released, and a new two-way IP media path is established between the originating party and the IP Phone party. This uses the H.323 “Third-party initiated pause and re-routing” mechanism.

IP Phone to local IP Phone transferred to a Virtual Trunk

A call is established between two IP Phones on the same node. A direct media path exists between the two telephones. One of the parties initiates a transfer to a party on a remote node.

When the IP Phone party initiates the transfer, call processing on the local node places the other party on hold. The media path between the two IP Phones is torn down. A call is set up between the transferring IP Phone and the remote party (this could be an IP Phone or circuit-switched telephone). See “IP Phone to IP Phone (on separate Call Servers)” on page 81.

When the transferring IP Phone completes the transfer before answer, the consultation call between the IP Phone and the remote party is torn down and a call is set up between the transferred IP Phone and the remote party. The media path that existed between the remote party and the transferring IP Phone is redirected using the H.323 third-party initiated pause and re-routing mechanism. No ISDN Q.931 signaling is exchanged between the nodes, and the call state on the terminating node is unchanged. A direct IP media path is established between the transferred IP Phone and the remote party.

H.323-to-SIP signaling

Contents

This section contains information on the following topics:

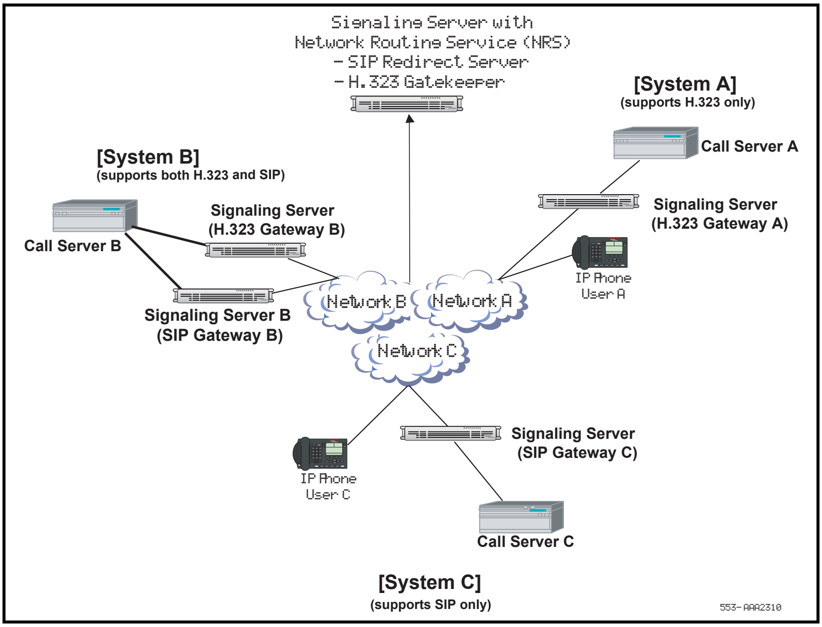
Introduction

H.323 is used to set up and tear down H.323 calls, while SIP is used to set up and tear down SIP calls. If a network uses both the SIP and H.323 protocols, then an H.323-to-SIP “bridge” must exist between the H.323 domain and the SIP domain.

H.323-to-SIP signaling (coexistence of both H.323 and SIP)

This section describes a call flow example of an H.323 incoming trunk call to a SIP trunk. In the following example, System A supports only H.323, System B supports both SIP and H.323, and System C supports only SIP. See Figure 25 on page 100.

Figure 25
Sample network for H.323-to-SIP call



In this example, System B shows two Signaling Servers:

- one serves the H.323 Virtual Trunk
- another serves the SIP Virtual Trunk

The Signaling Servers in System B are shown as two separate servers for clarity. Both the H.323 Gateway and the SIP Trunk Gateway can be configured on the same Signaling Server. Each Signaling Server has its own D-channel IP, and both are connected to the same Call Server.

> ***Note:*** This statement does not imply that H.323 and SIP cannot coexist on one Signaling Server. If both applications are enabled, then the two Signaling Servers in Figure 25 will collapse into one Signaling Server.

In this example, System C (which is the SIP domain) is a CS 1000 system. However, System C could be any type of SIP endpoint such as a SIP Phone or MCS 5100 system.

The implementation of H.323-to-SIP basic call flow is similar to an H.323 Virtual Trunk-to-Virtual Trunk tandem call (see“Virtual Trunk to Virtual Trunk” on page 72 for SIP and “Virtual Trunk to Virtual Trunk” on page 93 for H.323).

The difference is in the SIP Network Protocol Module (NPM) (that is, the SIP Trunk Gateway, where the ISDN messages are converted to the corresponding SIP messages).

Call scenarios — summary

Using the configuration shown in Figure 25 on page 100, the following call scenarios exist:

- Calls between System A (H.323) and System C (SIP) are not possible, because each system supports a different protocol.
- H.323 calls between System A and System B are possible. SIP calls between System A and System B are not possible, because System A does not support SIP.
- SIP calls between System B and System C are possible. H.323 calls between System B and System C are not possible, because System C does not support H.323.
- Call between System A and System C are possible when routed through System B, because the Call Server in System B can convert H.323 calls to SIP and SIP calls to H.323. Therefore, a SIP call from System C is converted to H.323 in System B and terminates at System A. Similarly, an H.323 call from System A is converted to SIP in System B and terminates at System C. This scenario is a genuine SIP/H.323 network.

Call walk-through

IP Phone A (which has H.323-only configuration) wants to talk to IP Phone C (which has SIP-only configuration).

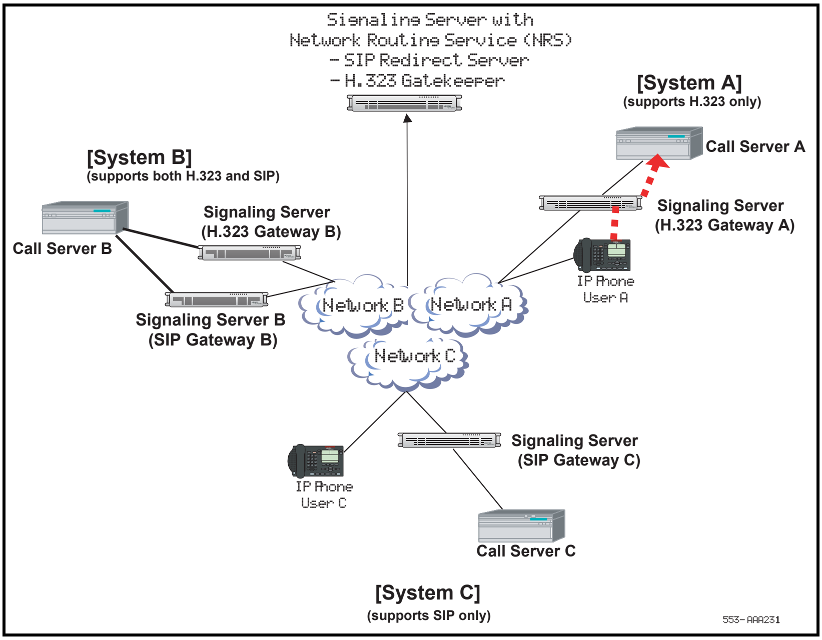
The following scenario describes the Direct IP Media Path functionality for a basic network call.

Note: Only the primary messages are illustrated in the following call flows.

1 User A on Call Server A dials the DN of User C on Call Server C. In order to get to User C, the call must go through System B for digit manipulation. See Figure 26.

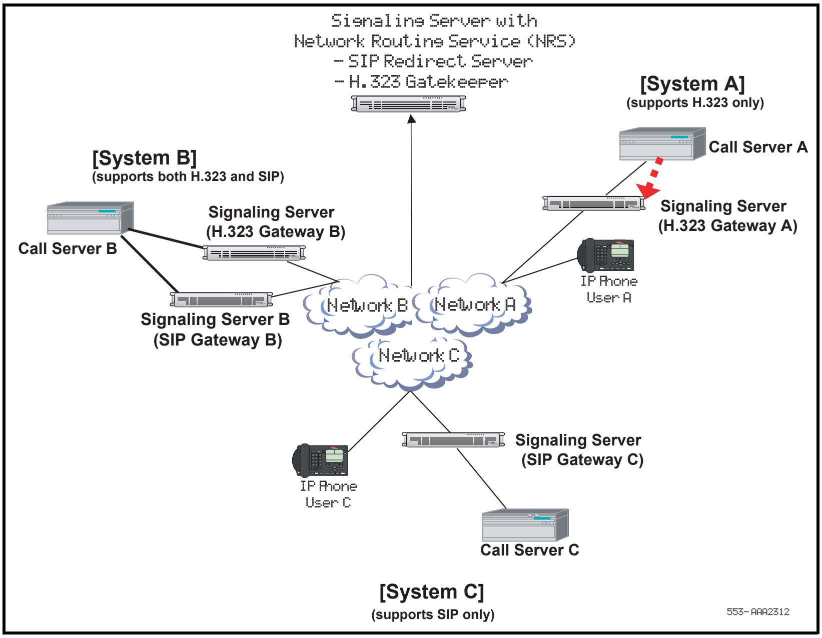
Note: The following call walk-through assumes that System A is using an H.323 Gateway only, System C is using a SIP Trunk Gateway only, and System B has both an H.323 Gateway and a SIP Trunk Gateway.

Figure 26
User A dials User C



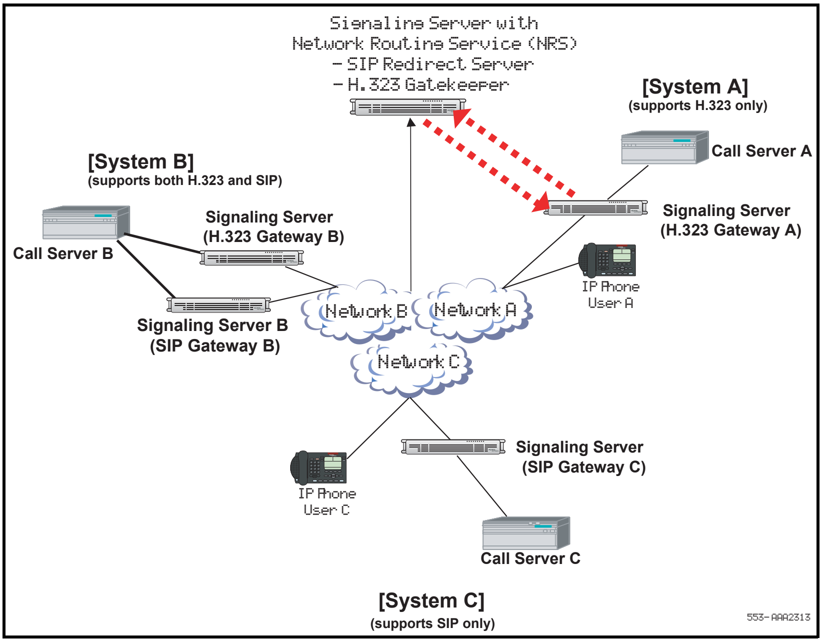
2 Call Server A determines that the dialed digits are at another site. Call Server A select the codec list, allocates bandwidth, and routes the call to the IP network using a Virtual Trunk and H.323 Gateway A. See Figure 27.

Figure 27
Call Server A routes the call to the IP network



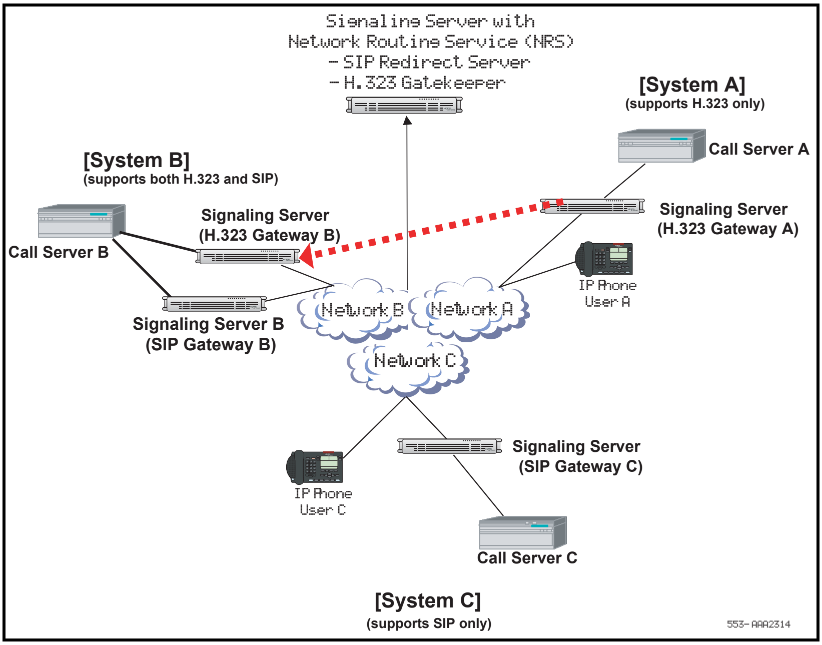
3 H.323 Gateway A asks the NRS (H.323 Gatekeeper) to search for the dialed DN in its database, as System A cannot go directly to System C because System A is using H.323 only and System C is using SIP. The NRS (H.323 Gatekeeper) responds back to H.323 Gateway A with the IP address of the H.323 Gateway B in System B. See Figure 28.

Figure 28
H.323 Gateway A communicates with the NRS (H.323 Gatekeeper)



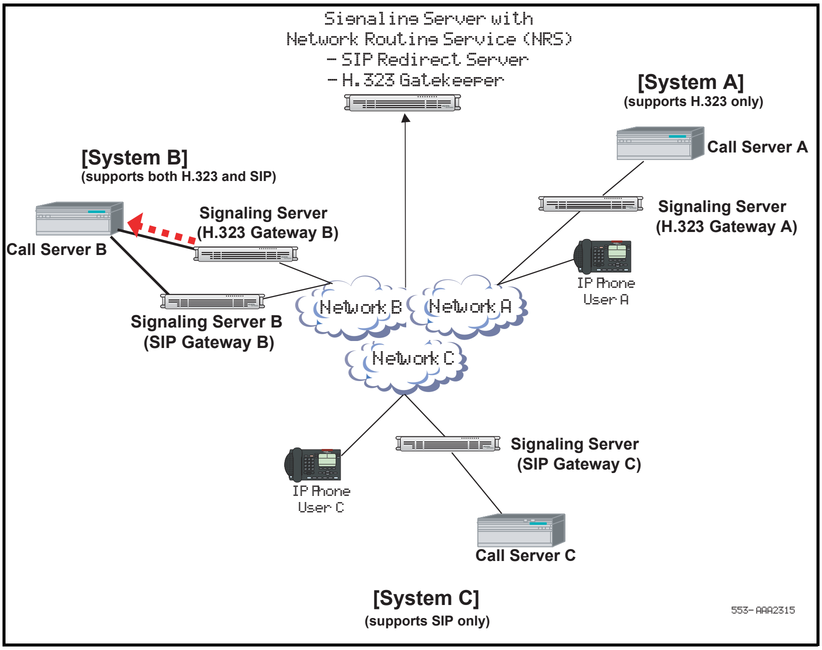
4 H.323 Gateway A sends an H.323 SETUP message to H.323 Gateway B including the DN information and IP Phone information (IP address and port number) for User A. See Figure 29.

Figure 29
H.323 Gateway A sends information to H.323 Gateway B



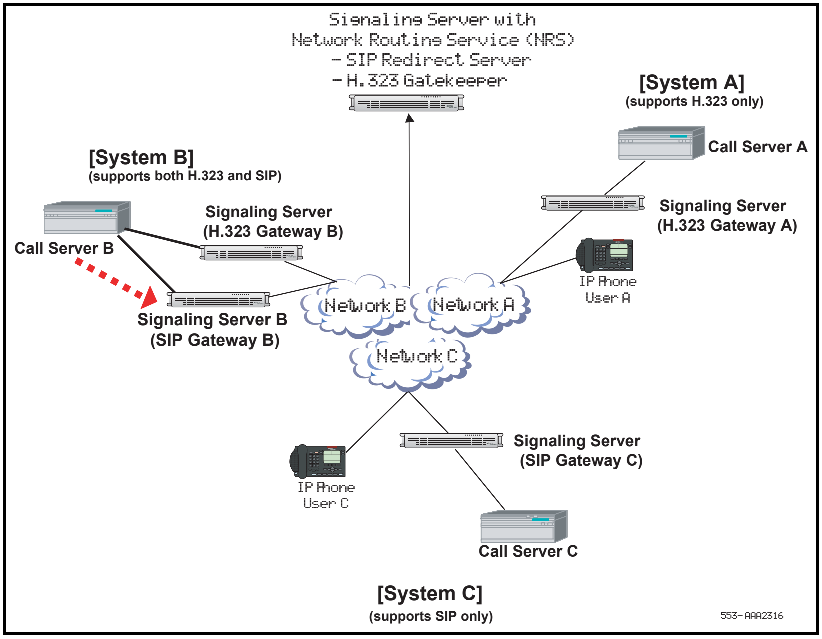
5 H.323 Gateway B receives the message from H.323 Gateway A and sends the call to Call Server B over a Virtual Trunk. Call Server B also treats the call as an incoming call from a Virtual Trunk. See Figure 30.

Figure 30
H.323 Gateway B sends calls to Call Server B



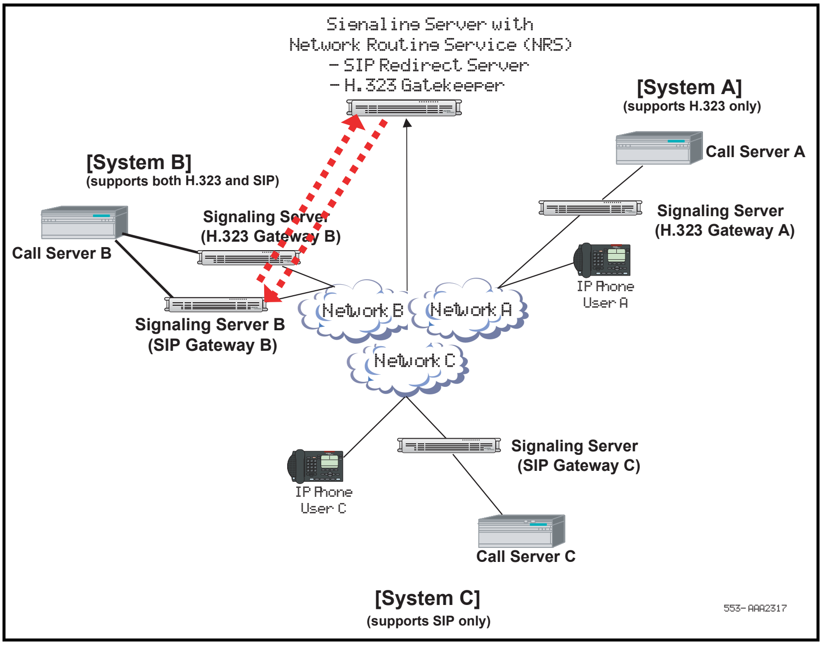
6 Call Server B processes the incoming message and determines that the call should go to System C through SIP Trunk Gateway B. Call Server B routes the call to SIP Trunk Gateway B. See Figure 31.

Figure 31
Call Server B sends calls to SIP Trunk Gateway B



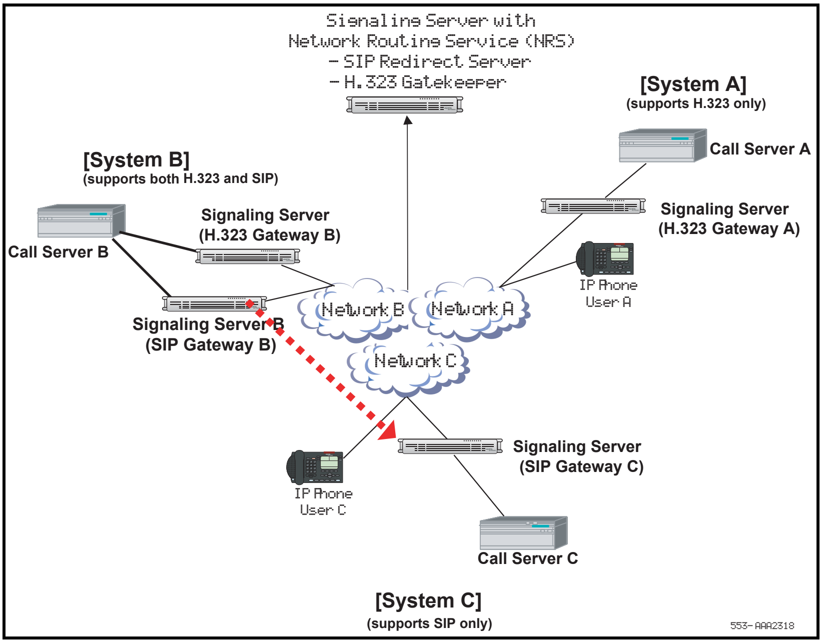
7 SIP Trunk Gateway B asks the NRS (SIP Redirect Server) to do a search for the DN of User C. The NRS (SIP Redirect Server) sends the IP address of SIP Trunk Gateway C to SIP Trunk Gateway B. See Figure 32.

Figure 32
SIP Trunk Gateway B communicates with the NRS (SIP Redirect Server)



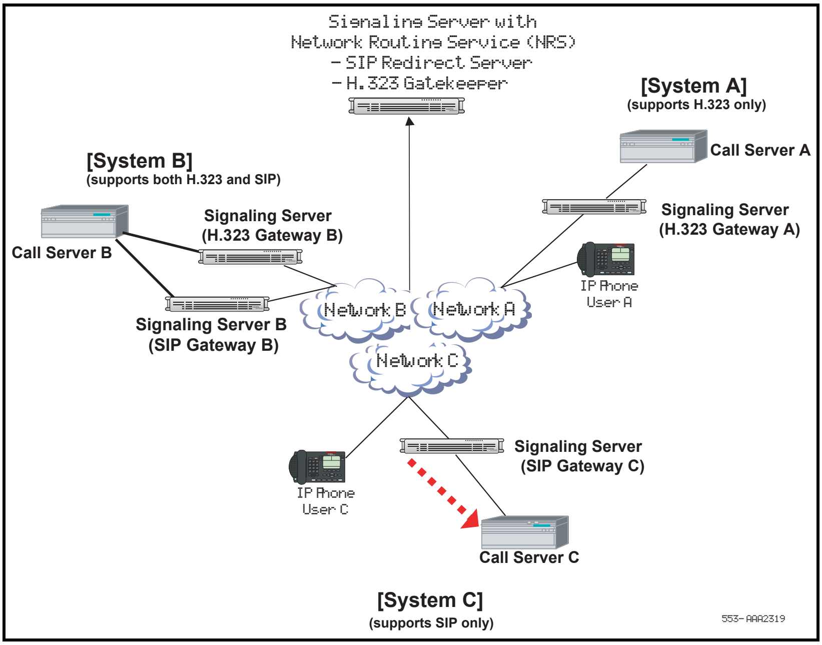
8 SIP Trunk Gateway B sends an INVITE message to SIP Trunk Gateway C. See Figure 33.

Figure 33
SIP Trunk Gateway B sends INVITE message to SIP Trunk Gateway C



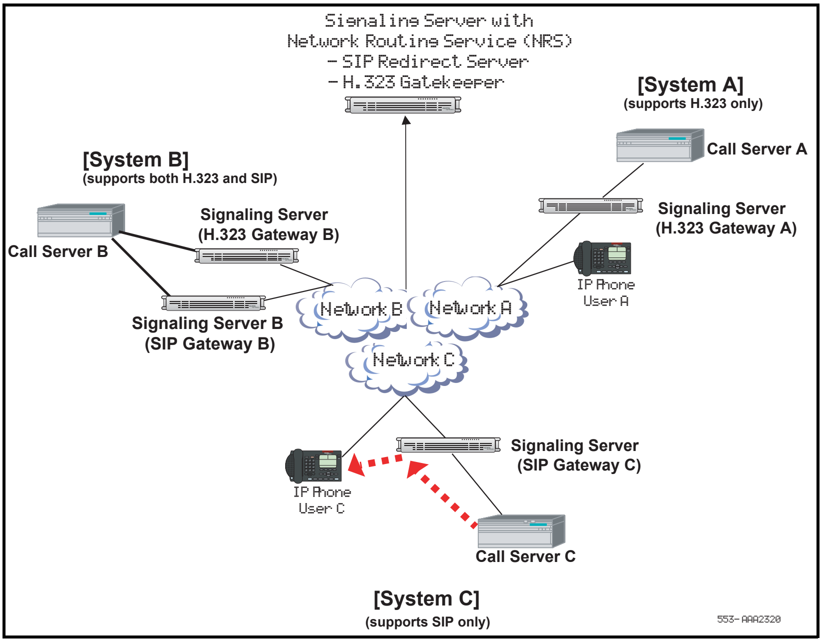
9 SIP Trunk Gateway C sends the call to Call Server C. See Figure 34.

Figure 34
SIP Trunk Gateway C sends call to Call Server C



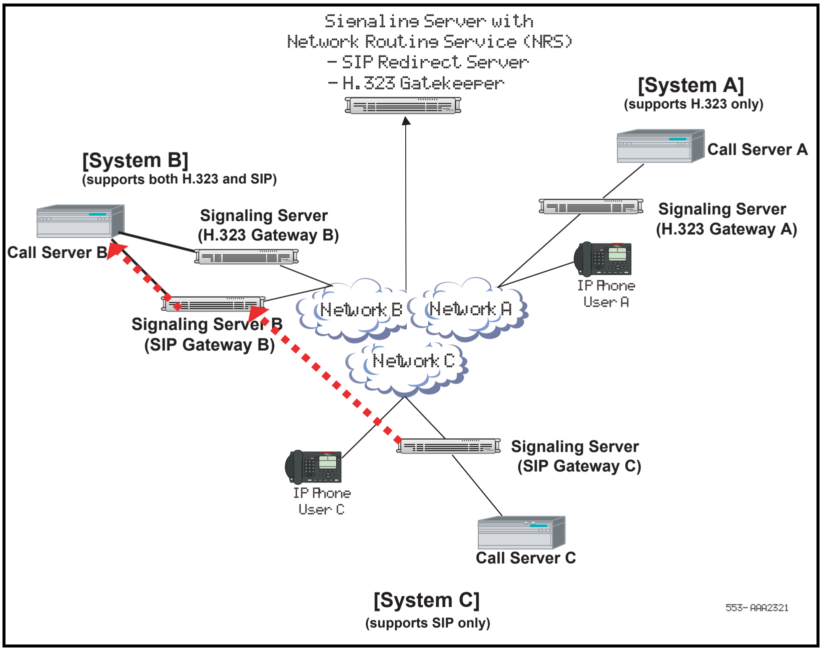
10 Call Server C selects the codec, allocates bandwidth, rings the telephone, and sends an ISDN Alert message to SIP Trunk Gateway C. See Figure 35.

Figure 35
Call Server C sends Alert message to SIP Trunk Gateway C



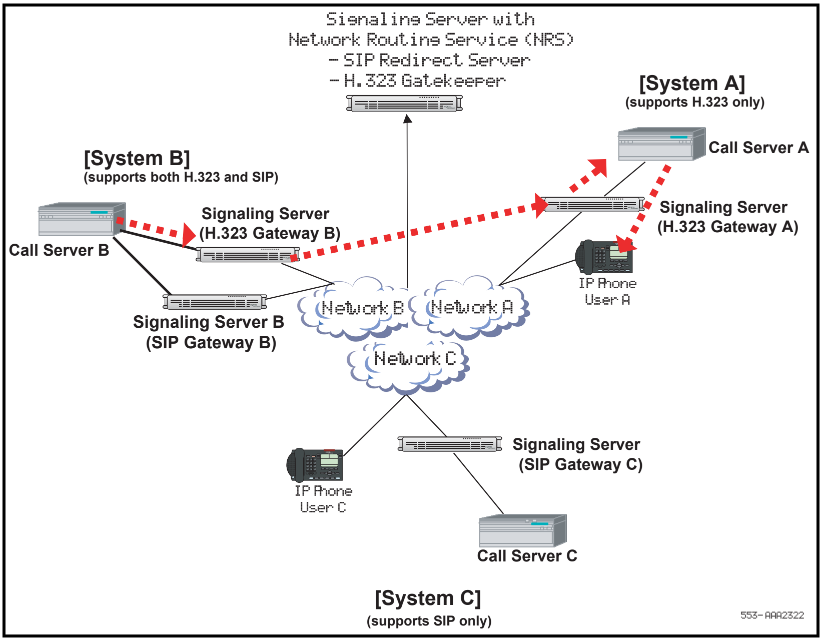
11 SIP Trunk Gateway C converts the ISDN Alert message to a SIP 180 response message. SIP Trunk Gateway C sends the SIP message to SIP Trunk Gateway B. SIP Trunk Gateway B converts the incoming SIP 180 response message back to the ISDN Alert message. SIP Trunk Gateway B then sends the message to Call Server B. See Figure 36.

Figure 36
SIP Trunk Gateway B sends ISDN Alert message to Call Server B



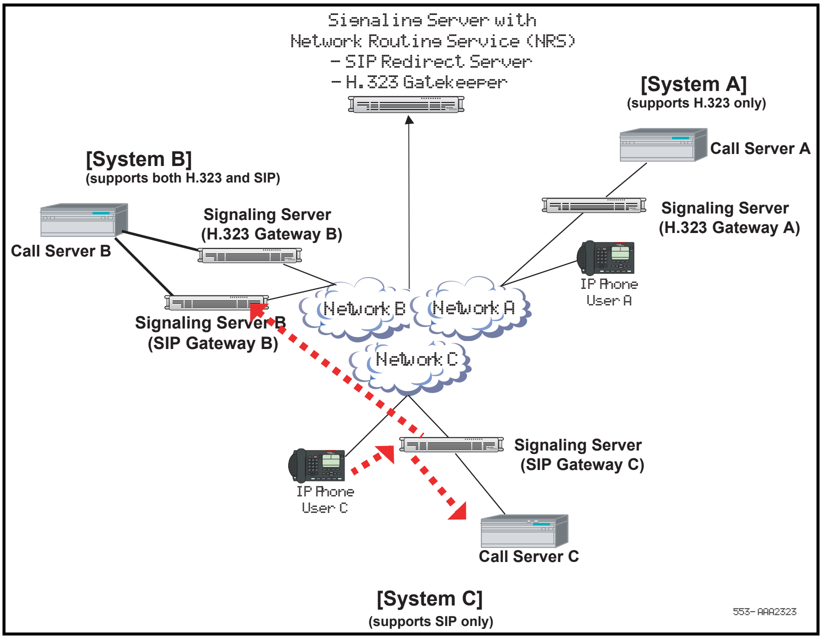
12 Call Server B forwards the ISDN Alert message to H.323 Gateway B. H.323 Gateway B sends the message to H.323 Gateway A. H.323 Gateway A sends the message to Call Server A. Call Server A requests that IP Phone User A play ringback tone. See Figure 37.

Figure 37
H.323 Gateway B sends Alert message to H.323 Gateway A



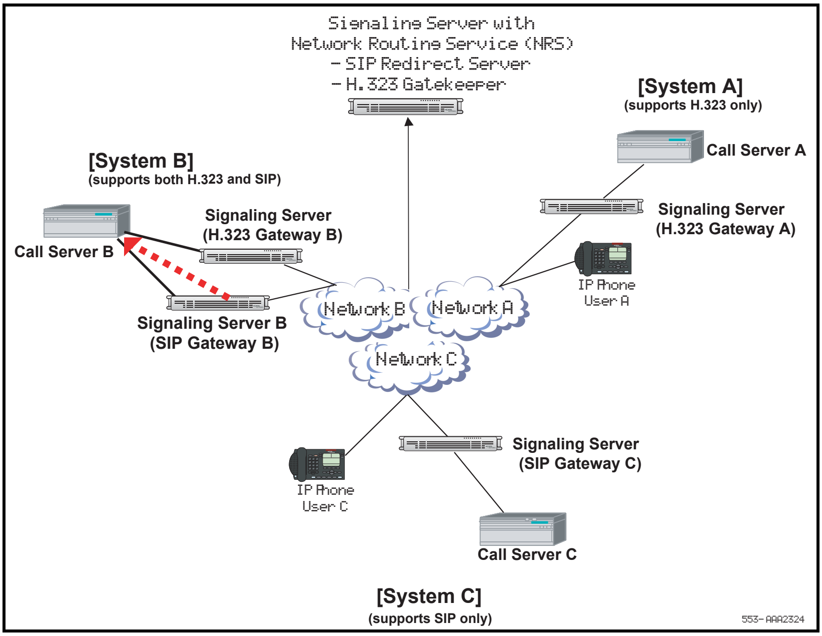
13 IP Phone User C answers the call. A message is sent to Call Server C on SIP Trunk Gateway C. SIP Trunk Gateway C sends a SIP 200 OK message along with the IP Phone information (IP address, port numbers, and codec) to SIP Trunk Gateway B. See Figure 38.

Figure 38
User C answers the call



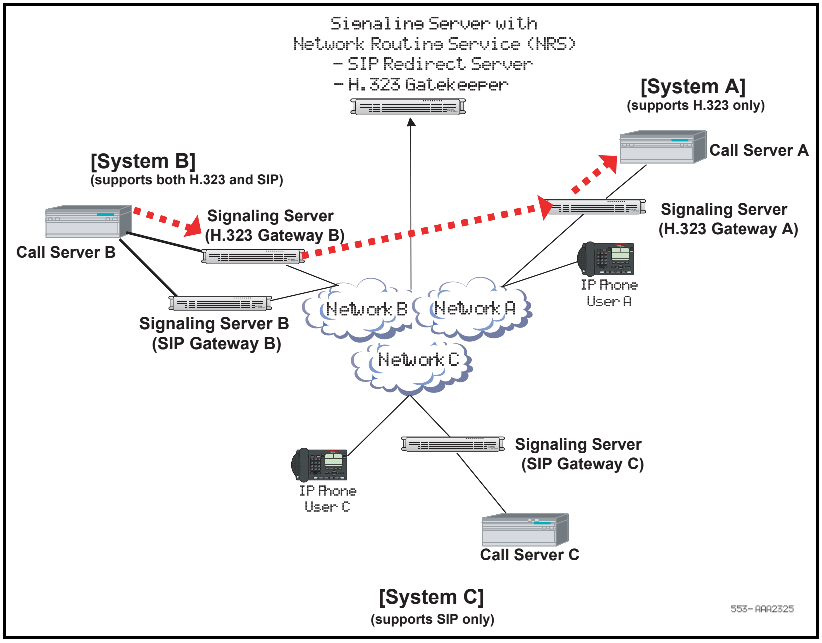
14 SIP Trunk Gateway B converts the SIP 200 OK message to an ISDN CONNECT message and sends the message to Call Server B. See Figure 39.

Figure 39
SIP Trunk Gateway B sends message to Call Server B



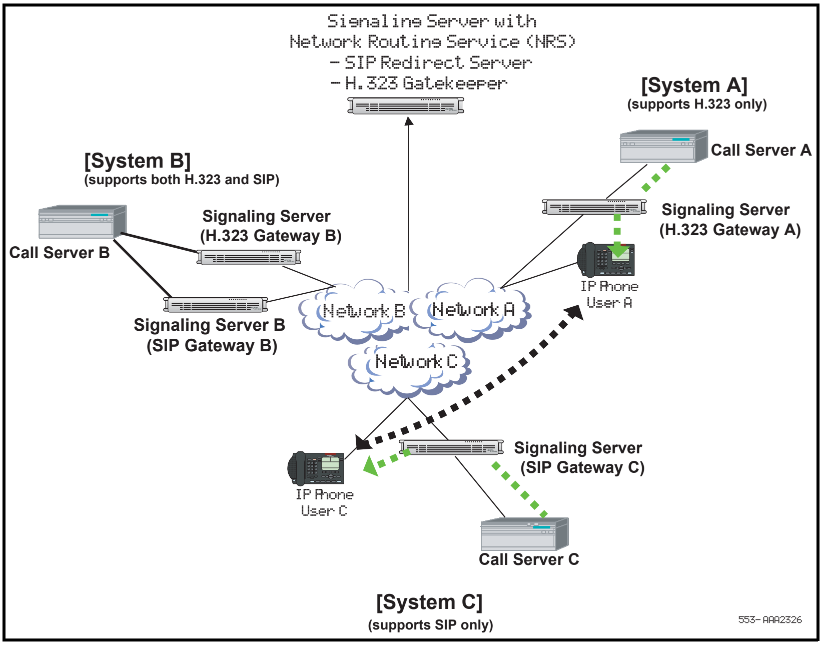
15 Call Server B forwards the ISDN CONNECT message to H.323 Gateway B. H.323 Gateway B then sends a message to H.323 Gateway A. H.323 Gateway A sends the message to Call Server A. See Figure 40.

Figure 40
H.323 Gateway B sends message to H.323 Gateway A



16 Call Server A tells IP Phone A to set up the direct IP media path with IP Phone C. The IP Phones then begin to transmit and receive voice over the IP network. See Figure 41.

Figure 41
IP Phones start the direct media paths



Fallback to PSTN

Contents

This section contains information on the following topics:

Introduction

It is possible to automatically Fallback to PSTN, if calls cannot be completed due to loss of connectivity between sites over the IP network. This is achieved using the standard MCDN Alternate Routing feature when:

- the IP network is down
- the destination IP Peer endpoint is not responding
- the destination IP Peer endpoint responds that there are no available IP Peer trunk resources
- the destination IP Peer endpoint is not registered with the NRS
- there are address translation errors
- all Virtual Trunks are busy at the originating sites

- all bandwidth configured for a bandwidth zone has been allocated
- Quality of Service (QoS) metrics cause a reduction in available bandwidth (see "Fallback to PSTN" on page 119)

Fallback to PSTN can be configured by programming an alternate route entry after the virtual IP trunk route entry in RLB in LD 86 and entering RRA at the SBOC prompt for the virtual IP trunk entry. Refer to the *Software Input/ Output: Administration* (553-3001-311) for the configuration of RLB in LD 86.

Fallback to PSTN for IP Peer Networking refers to the use of the MCDN Alternate Routing feature to step back to any alternate switched-circuit trunk route to the destination that the call first attempted to reach by the IP Peer virtual IP trunk route.

The alternate switched-circuit trunk route can be any of the following:

- a direct ISDN PRI tie trunk route
- a Virtual Private Voice Network tie trunk route using a common carrier voice network
- a PSTN trunk route

  Note 1: If Fallback to PSTN uses PSTN trunks as the alternate route, then the appropriate ESN digit manipulation features must be implemented to convert the dialed number from on-net to off-net, or from private to public E.164 format.

  Note 2: If Fallback to PSTN uses PSTN trunks as the alternate route, Nortel recommends that you configure both the original and alternate trunk routes as en bloc-capable or overlap-capable. See "Overlap signaling" on page 487 for more information.

A similar feature, Alternative Call Routing for Network Bandwidth Management, is available to provide alternate routing between a branch office (or Survivable Remote Gateway [SRG]) and a main office. Refer to *Branch Office: Installation and Configuration* (553-3001-214) for more information.

Engineering practices

Best IP network engineering practices for IP Telephony

In general, the best IP network engineering practices for IP Telephony tend to remove the requirement for QoS Fallback to PSTN. Best practices include:

- implementing network QoS features such as DiffServ and 802.1Q to give priority to real-time voice traffic
- fragmenting large data frames to limit the maximum frame size on low speed WAN links and limiting the quantity of voice traffic that is transmitted over low speed links

When QoS Fallback to PSTN is required for certain network locations (in an IP Peer network) because WAN links have not been engineered according to best practices, IP Trunk 3.0 (or later) can be used to achieve QoS Fallback to PSTN between those locations and an IP Peer node located on the IP network backbone. An IP Trunk 3.0 (or later) node must be configured in the same CS 1000 system with the IP Peer node.

Engineering considerations for using IP Trunk to achieve QoS Fallback to PSTN

Using IP Trunk 3.0 (or later) nodes to provide QoS Fallback to PSTN in an IP Peer network imposes certain engineering and network management trade-offs that must be carefully considered:

- QoS Fallback to PSTN only works between symmetrically-configured pairs of IP Trunk nodes. QoS Fallback to PSTN does not work between an IP Trunk node and an IP Peer node. Each IP Trunk node in a symmetrically-configured pair must have QoS Fallback to PSTN enabled for the opposite destination node.
- A pair of symmetrically-configured IP Trunk nodes must each have a local Dialing Plan entry in the IP Trunk node that points to these opposite IP Trunk nodes. The Gatekeeper cannot be used for any IP Trunk destinations that are symmetrically configured to enable QoS Fallback to PSTN.

- An IP Trunk node configured in a CS 1000 system with an IP Peer node does not support the Direct Media Path feature of IP Peer Networking. Therefore all IP Trunk calls originating or terminating at the network location that require QoS Fallback to PSTN must have a tandem media path connection through the CS 1000 IP Peer node. The tandem media path can occasionally cause voice quality degradation due to multiple transcoding and higher end-to-end latency of the voice conversation.

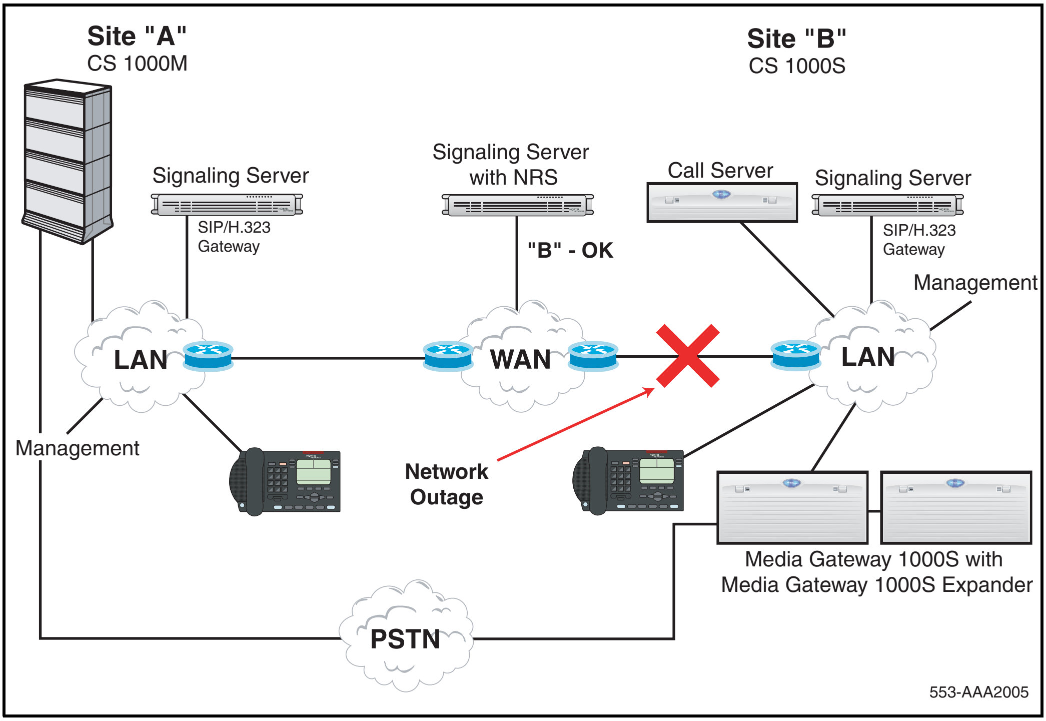
For more information, refer to *IP Trunk: Description, Installation, and Operation* (553-3001-363) and *Basic Network Features* (553-3001-379).

Alternate circuit-switched routing

The following scenario describes alternate circuit-switched routing when there is an IP network outage:

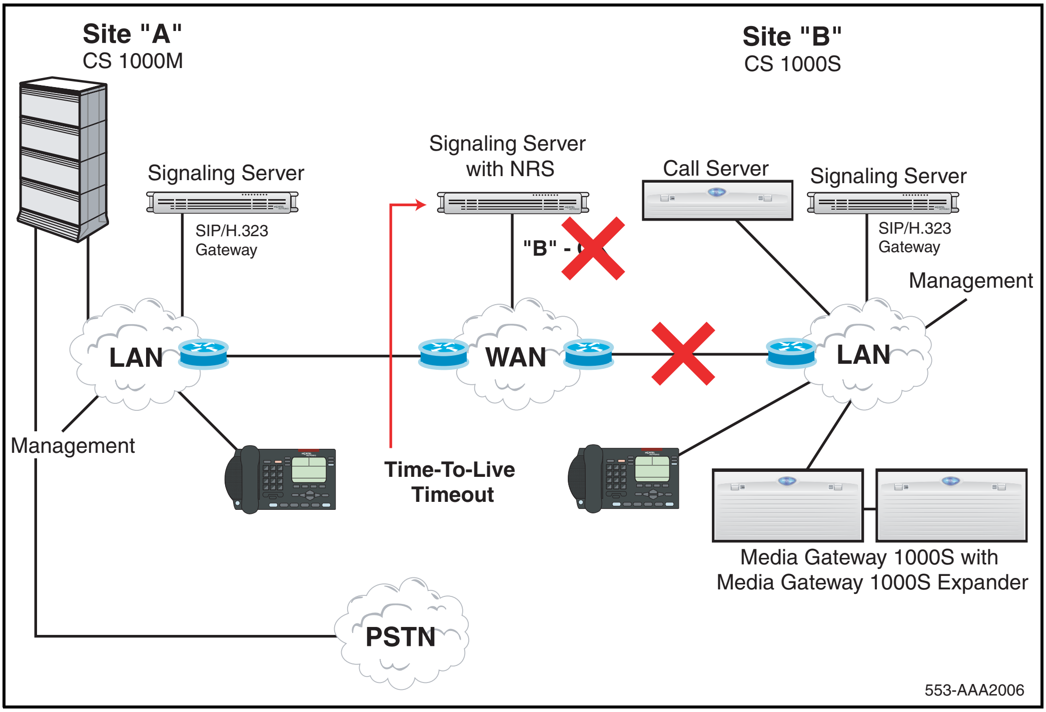
1 An IP network outage occurs at Site B. See Figure 42.

Figure 42
IP network outage at Site B



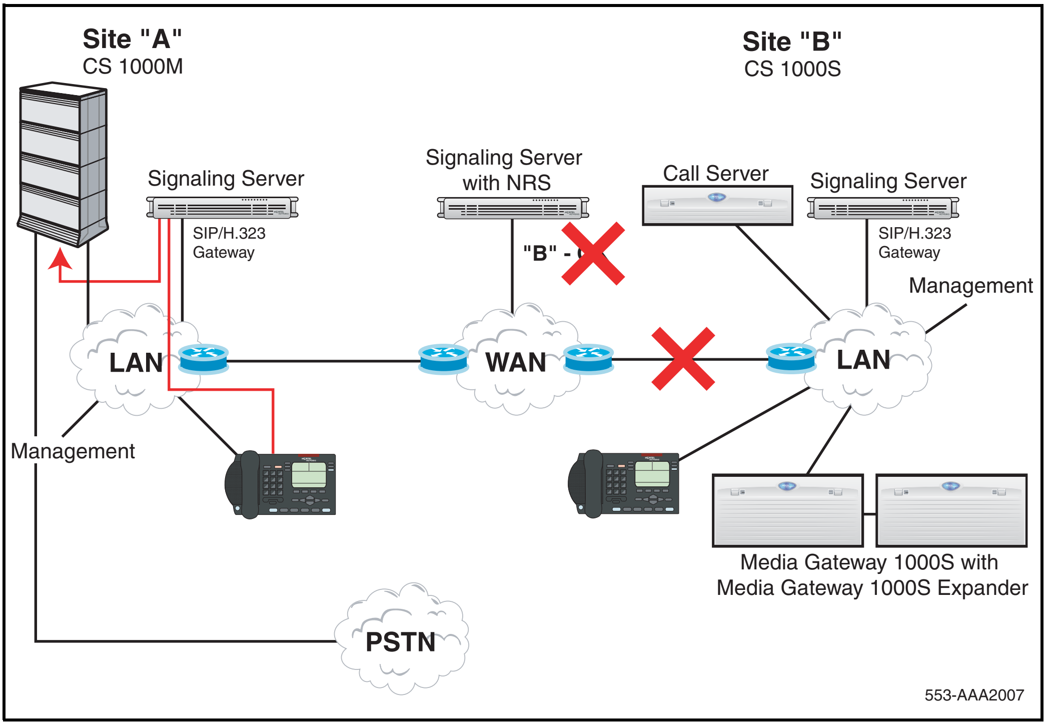
2 The registration of Site B times out at the NRS; the status updates. See Figure 43.

Figure 43
Registration at Site B times out



3 User A on Call Server A dials the DN of User B on Call Server B. Call Server A collects the dialed digits through the Terminal Proxy Server (TPS) on the Signaling Server. See Figure 44.

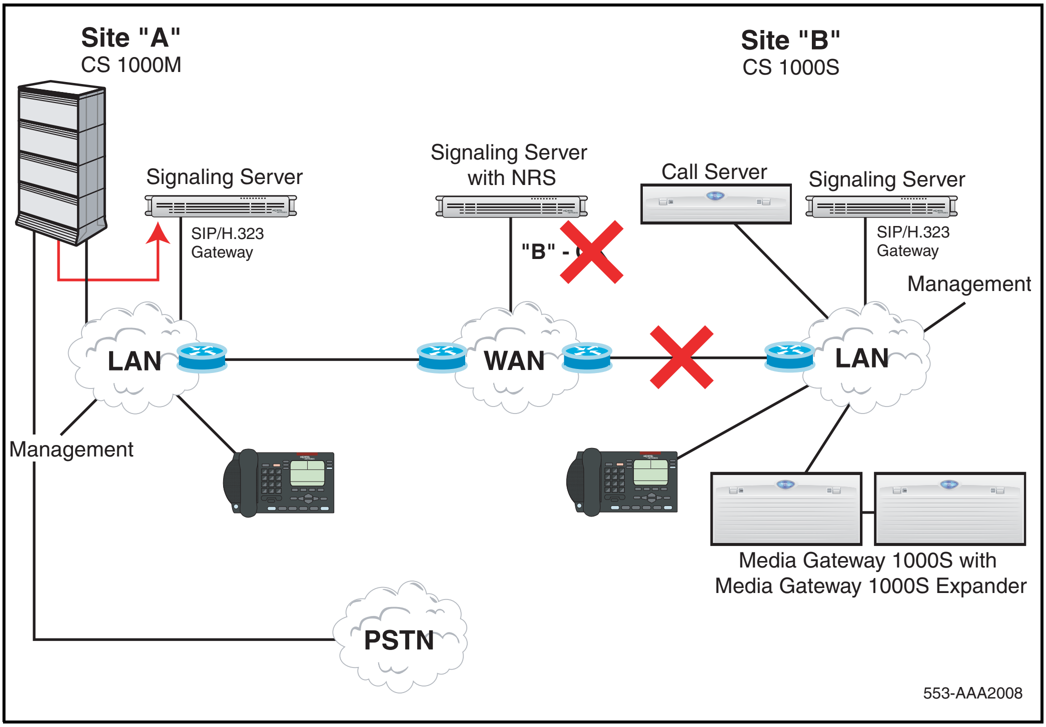
Figure 44
User A dials User B



4 Call Server A determines that the DN is at another site. Call Server A selects the codec list, allocates bandwidth, and routes the call to the IP network, using a Virtual Trunk and the SIP/H.323 Gateway. See Figure 45.

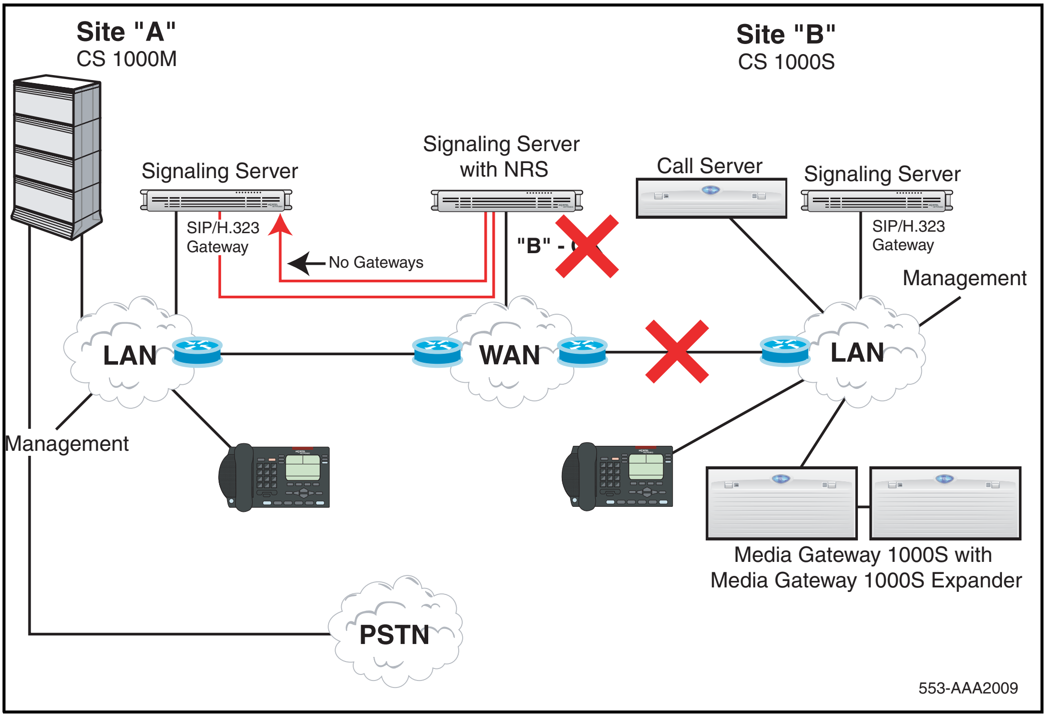
Note: To select which Virtual Trunk to use for routing, Call Server A examines the number dialed and uses various trunk routing and signaling features (for example, ESN and MCDN).

Figure 45
Call Server A routes the call to the IP network



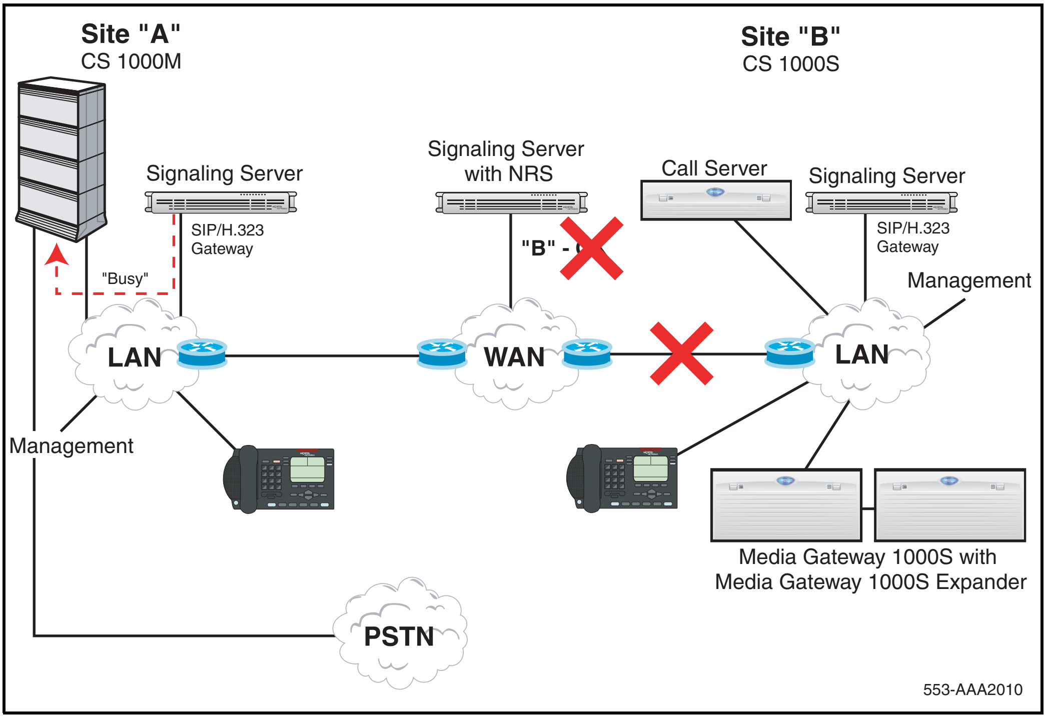
5 SIP/H.323 Gateway A asks the NRS to search for a dialed DN in the database (for example, within the appropriate CDP domain).
The NRS replies that no SIP/H.323 Gateways are available for the dialed number. See Figure 46.

Figure 46
No SIP/H.323 Gateways are available for the dialed DN



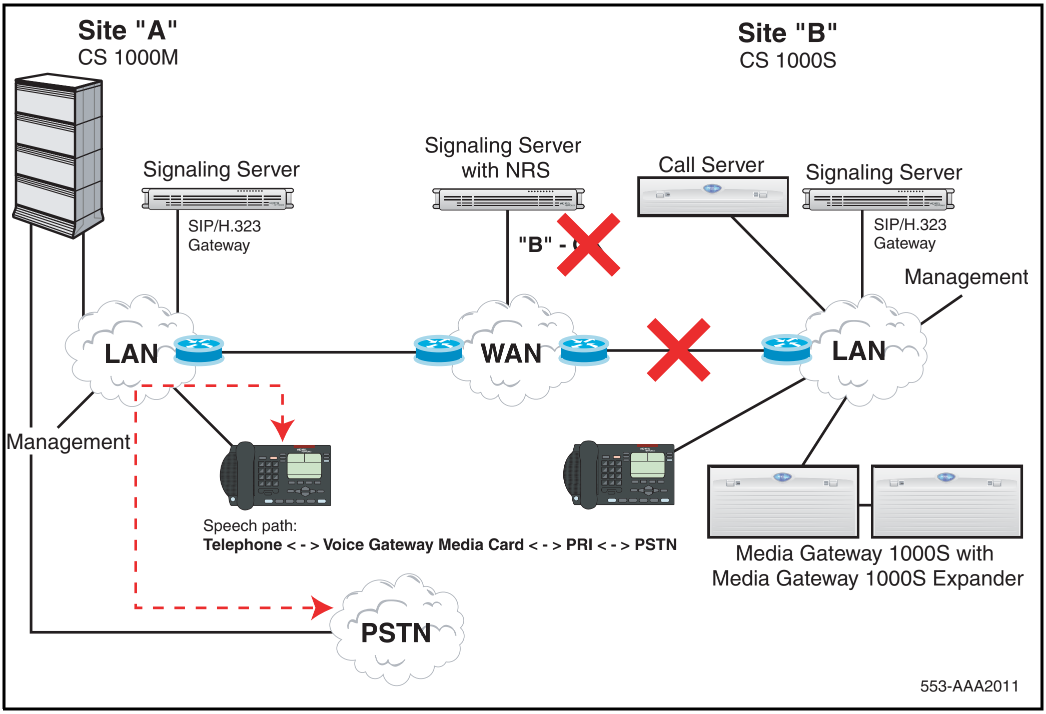
6 SIP/H.323 Gateway A replies to Call Server A with a message that all IP trunks are busy for the dialed DN. See Figure 47.

Figure 47
SIP/H.323 Gateway A replies to Call Server A



7 Call Server A chooses the next route in the Route List Data Block. The next route is a local PSTN trunk route. Call Server A allocates a Voice Gateway Media Card and PRI channel. Digit manipulation is applied to the route using the local PSTN. A successful call is made. See Figure 48.

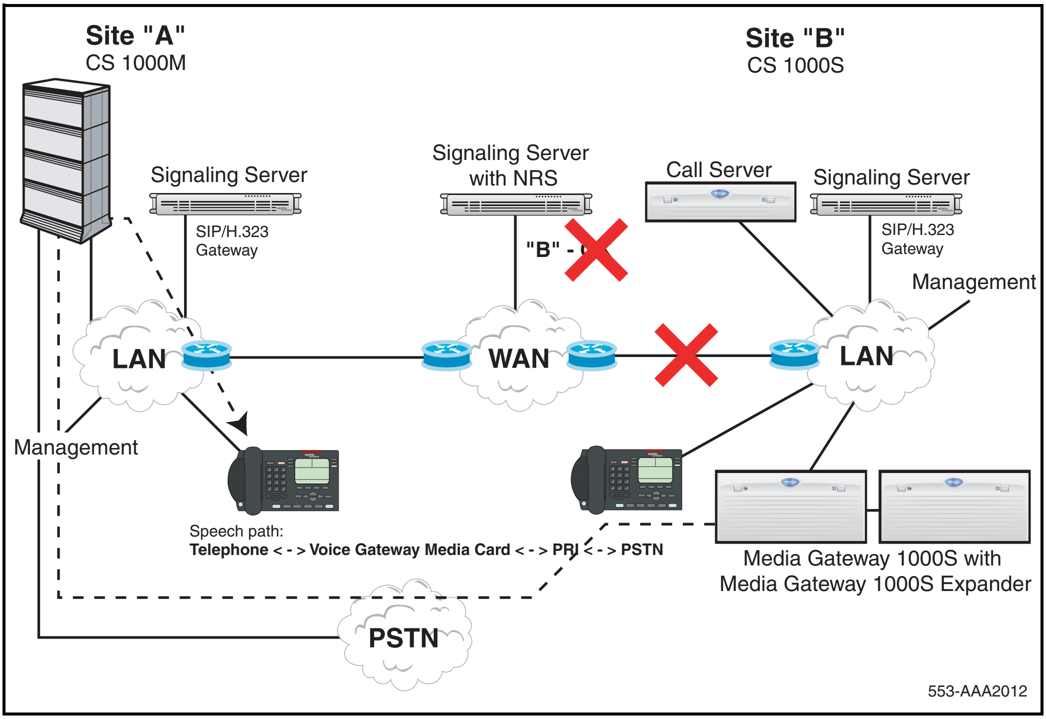
Figure 48
Call Server A chooses the next route in the Route List Data Block



Speech path:
Telephone < - > Voice Gateway Media Card < - > PRI < - > PSTN

8 The call is routed across PSTN and enables the users to talk to each other. The call is terminated over PSTN to Site B. See Figure 49.

Figure 49
Call is terminated over PSTN



Bandwidth Management

Contents

This section contains information on the following topics:

Introduction

CS 1000 supports Bandwidth Management on a network-wide basis so that voice quality can be managed between multiple Call Servers.

Bandwidth management allows for codec selection and bandwidth limitations to be placed on calls, depending on whether the calls are intrazone or interzone.

Adaptive Network Bandwidth Management is an enhancement of Bandwidth Management in which Quality of Service (QoS) metrics are used to automatically lower available bandwidth.

IMPORTANT!

Once all bandwidth is used, any additional calls are blocked or rerouted. Keep this in mind when designing and implementing Network Bandwidth Management.

Codec negotiation

Codec refers to the voice coding and compression algorithm used by DSPs. Each codec has different QoS and compression properties.

IP Peer Networking supports the per-call selection of codec standards, based on the type of call (interzone or intrazone). IP Peer Networking supports the following codecs (with supported payload sizes in parentheses, with the default value in bold):

- G.711 A/mu-law (10 ms, **20 ms**, and 30 ms)
- G.729 A (10 ms, **20 ms**, 30 ms, 40 ms, and 50 ms)
- G.729 AB (10 ms, **20 ms**, 30 ms, 40 ms, and 50 ms)
- G.723.1 (**30 ms**) (though it can limit the number of DSP channels available)
- T.38 for fax

  Note: The G.XXX series of codecs are standards defined by the International Telecommunications Union (ITU).

By default, the G.711 codec must be supported at both ends of a call. Codec configuration is performed for each node and is independent of the signaling gateway (SIP or H.323) that is used on the node.

If more than one codec is configured, then the minimum payload size among the configured codecs is used for the SIP Trunk Gateway codec negotiation.

> ***Note:*** Nortel recommends configuring the same payload size for all codecs in the same node.

SIP example

If a G.711 20ms codec and G.729 30ms codec are configured, then codec negotiation uses the minimum payload size of 20 ms. That is, the G.711 20ms codec and the G.729 20ms codec are used. Instead, Nortel recommends that both G.711 and G.729 codecs be configured as 20ms.

> ***Note:*** When a G.729 30ms codec is configured, then the G.729 10ms/20ms/30ms codecs are supported.

IP Peer Networking performs codec negotiation by providing a list of codecs that the devices can support. Use CS 1000 Element Manager to configure the list of codec capabilities. See Procedure 13 “Configuring codecs” on page 319.

The codec preference sequence sent over SIP/H.323 depends on the bandwidth policy selected for the Virtual Trunk zone and the involved telephones. For “Best Quality”, the list is sorted from best to worst voice quality. For “Best Bandwidth”, the list is sorted from best to worst bandwidth usage.

The G.711 codec delivers “toll quality” audio at 64 kbit/s. This codec is optimal for speech quality, as it has the smallest delay and is resilient to channel errors. However, the G.711 codec uses the largest bandwidth.

The G.729A codec provides near toll quality voice at a low delay. The G.729A codec uses compression at 8 kbit/s. The G.729AB codec also uses compression at 8 kbit/s.

The G.723.1 codec provides the greatest compression.

> ***Note 1:*** Payload default values need to be changed if the customer wants to communicate with a third-party gateway that does not support the

above default payload sizes. Otherwise, IP Peer calls to or from the third-party gateway are not successful.

Note 2: If the payload sizes are set higher than the default values (for example, to support a third-party gateway), then the local IP calls are affected by higher latency. This is because the codec configuration applies to both IP Peer calls and local IP (IP Line) calls.

G.711 A-law and mu-law interworking

In case the far end uses a different Pulse Code Modulation (PCM) encoding law for its G.711 codec, systems that are configured as G.711 A-law also include G.711 mu-law on their codec preferences list. Systems configured as G.711 mu-law include G.711 A-law as their last choice. Therefore, encoding law conversion is performed between systems with different laws.

Bandwidth management and codecs

Bandwidth management defines which codecs are used for intrazone call and interzone calls.

Bandwidth management enables administrators to define codec preferences for IP Phone-to-IP Phone calls controlled by the same CS 1000 system within the same zone. These calls are known as intrazone calls. This is different than the codec preferences for calls between an IP Phone on the CS 1000 system to a Virtual Trunk (potentially an IP Phone on another CS 1000 system) or calls to IP Phones is another zone. These calls are known as interzone calls.

For example, you may prefer high quality speech (G.711) over high bandwidth within one system, and lower quality speech (G.729 AB) over lower bandwidth to a Virtual Trunk. Such a mechanism can be useful when a system is on the same LAN as the IP Phones it controls, but the other systems are on a different LAN (connected through a WAN).

Virtual Trunks' usage of bandwidth zones is different than IP Phone bandwidth usage. For Virtual Trunks, a zone number is configured in the Route Data Block (LD 16). The zone number determines codec selection for interzone and intrazone calls (that is, Best Bandwidth or Best Quality). See "Configuring IP Peer Networking" on page 281 for information on configuring the RDB zone.

Bandwidth usage for Virtual Trunks is accumulated in its zone to block calls that exceed the bandwidth availability in a specific zone. However, the amount of bandwidth that is required to complete a given call is not known until both call endpoints have negotiated which codec to use. The bandwidth used for calculating the usage of a Virtual Trunk call is determined by the preferred codec of the device that connects to the Virtual Trunk. If the device is an IP Phone, the bandwidth calculations use the preferred codec of the IP Phone, based on the codec policy defined for the zones involved (that is, Best Bandwidth or Best Quality). Likewise, the bandwidth calculations use the preferred codec of the Voice Gateway Media Card for connections between a circuit-switched device (for example, a PRI trunk) and a Virtual Trunk.

Codec selection

For every Virtual Trunk call, a codec must be selected before the media path can be opened. When a call is set up or modified (that is, media redirection), one of two processes occurs:

- The terminating node selects a common codec and sends the selected codec to the originating node.
- The codec selection occurs on both nodes.

Each node has two codec lists: its own list and the far end’s list. In order to select the same codec on both nodes, it is essential to use the same codec selection algorithm on both nodes. Before the codec selection occurs, the following conditions are met:

- Each codec list contains more than one payload size for a given codec type (it depends on the codec configuration).
- Each codec list is sorted by order of preference (the first codec in the near end’s list is the near end’s most preferred codec, the first codec in the far end’s list is the far end’s preferred codec).

Codec selection algorithms

Once the codec lists meet the above conditions, one of the following codec selection algorithms selects the codec to be used:

- H.323 Master/Slave algorithm

- SIP Offer/Answer model
- "Best Bandwidth" codec selection algorithm

Note: If a SIP trunk call is between a CS 1000 system and other third-party gateway/SIP clients (for example, MCS 5100), then the codec selection does not guarantee that the same codec is selected for a call from endpoint A to endpoint B and for a call from endpoint B to endpoint A. This different codec selection makes it difficult for bandwidth management. However, calls between two CS 1000 systems have the same codec selection decision regardless of who originated the call.

H.323 Master/Slave algorithm

In the case of a Virtual Trunk call between Nortel and third-party equipment, the H.323 Master/Slave algorithm is used.

The codec selection algorithm proposed by the H.323 standard involves a Master/Slave negotiation. This is initiated each time two nodes exchange their capabilities (TCS message). The Master/Slave information decides that one node is Master and the other node is Slave. The outcome of the Master/Slave negotiation is not known in advance; it is a random result. One node could be Master then Slave (or vice versa) during the same call.

Algorithm details

The H.323 Master/Slave algorithm operates in the following manner:

- The Master node uses its own codec list as the preferred one and finds a common codec in the far end's list. In other words, the Master gets the first codec in its list (for example, C1), checks in the far end's list if it is a common codec; if it is, C1 is the selected codec. Otherwise, it gets the second codec in its list and verifies it against the far end, and so on.
- The Slave node uses the far end's list as the preferred one and finds in its own list the common codec.

Issues caused by the H.323 Master/Slave algorithm

The issues caused by the Master/Slave algorithm are due to the random nature of the Master/Slave information. In other words, one cannot predetermine the codec that is used during a Virtual Trunk call.

The following are the issues associated with the H.323 Master/Slave algorithm:

- After an on-hold and off-hold scenario (which triggers Master/Slave negotiation), the codec used for the restored call might be different than the one used before on-hold, because the Master/Slave information could have been changed.
- When using "Fast Start" codec selection, a call from Telephone 1 (node1) to Telephone 2 (node2) can use a different codec than a call from Telephone 2 (node2) to Telephone 1 (node1), because the terminating end is always Master.
- For tandem calls, the Master/Slave information is not relevant. The Master/Slave information is designed for use between two nodes only, not between three or more nodes. It makes the codec selection for tandem calls more complex and inefficient.

To solve the issues, another codec selection algorithm, not based on the unpredictable Master/Slave information, is needed. Since any change to the Master/Slave algorithm implies a change to the H.323 standard, the new codec algorithm is used for Virtual Trunk calls between Nortel equipment.

SIP Offer/Answer model

The SIP codec negotiation is based on the Offer/Answer model with Session Description Protocol (SDP).

The following three cases of codec negotiation are supported:

- The calling user agent sends an SDP offer with its codec list in the INVITE message with a "sendrecv" attribute. In this case, the called user agent selects one codec and sends the selected codec in an SDP answer. The SDP answer is included in the 200 OK message (which is the response to the INVITE) with the "sendrecv" attribute.

  This is the preferred method of operation.

- The calling user agent sends an SDP offer with its codec list in the INVITE message with a "sendrecv" attribute. The called user agent returns more than one codec in the SDP answer. In the case that many codecs are included in the response, the calling user agent picks the first compatible codec from the called user agent's list, and sends a new SDP offer with a single codec to lock it in.

- If the SDP of the calling user agent is not present in the INVITE message, then the called user agent sends its codec list in an SDP offer in the 200 OK message, with the "sendrecv" attribute. The calling user agent selects one codec and sends the selected codec in an SDP answer inside the ACK message, with "sendrecv" attribute.

For more information on this algorithm, refer to RFC 3264 – An Offer/ Answer Model with the Session Description Protocol (SDP).

'Best Bandwidth' codec selection algorithm

The "Best Bandwidth" codec selection algorithm solves the issues caused by the H.323 Master/Slave algorithm. The "Best Bandwidth" algorithm selects one common codec based on two codec lists. Every time the selection is done with the same two lists, the selected codec is the same.

The "Best Bandwidth" codec decision is based on the codec type only, it does not take into account the fact that some codecs, while generally using less bandwidth, can consume more bandwidth than others at certain payload sizes.

"Best Bandwidth" is also applicable to SIP.

Algorithm details

The selected codec is the type considered as the best bandwidth codec type. To know whether one codec type has better bandwidth than another, see the rule as summarized in Table 8 on page 139.

Table 8
"Best Bandwidth" algorithm — codec type

	G.711 A law	G.711 mu-law	G.729 A	G. 729 AB	G. 723.1
G.711 A-law	G.711 A-law	G.711 mu-law	G.729 A	G. 729 AB	G. 723.1
G.711 mu-law	G.711 mu-law	G.711 mu-law	G.729 A	G. 729 AB	G. 723.1
G.729 A	G.729 A	G.729 A	G.729 A	G. 729 AB	G.729 A
G. 729 AB	G. 729 AB	G. 729 AB	G. 729 AB	G. 729 AB	G. 729 AB
G. 723.1	G. 723.1	G. 723.1	G.729 A	G. 729 AB	G. 723.1

Interoperability between CS1000 and SRG

The SRG is designed to interoperate with this feature in a manner similar to MG 1000B, but with a limitation with respect to codec selection policy.

Calls between branch IP Phones and the branch PSTN or between branch IP Phones and branch analog phones are based on the interzone policy rather than the intrazone policy defined in the CS 1000 main office. The zone table is updated based on the intrazone policy.

The net result of this limitation is that calls between branch IP Phone users and the branch PSTN, or between branch IP Phones and branch analog telephones, always use a Best Bandwidth codec. However, the calls are accounted for as Best Quality. This can impact the perception of call quality in this scenario, but it does not result in early call blocking. There are no impacts to codec selection or bandwidth usage tracking for calls that require WAN bandwidth.

Configuring Bandwidth Management

The following sections describe how to configure Bandwidth Management in a CS 1000 network. Nortel recommends that you read the Bandwidth Management section in *Converging the Data Network with VoIP* (553-3001-160) before using the following configuration information.

Zones

Bandwidth Management Zones are configured for each endpoint on a Call Server. The Network Bandwidth Zone number determines if a call is an intrazone call or an interzone call. Once that is determined, the proper codec and bandwidth limit is applied to the call.

All of the endpoints on one Call Server are configured with Zone number to identify all of the endpoints as being in a unique geographic location in the network. In addition, Virtual Trunks are configured with a Zone number that is different from the endpoint Zone numbers in the Call Server.

Codec selection occurs as described in “Codec selection” on page 135.

Configuration rules

There are three configuration rules for Bandwidth Management, as follows:

1. Each Call Server in the network must be configured with a unique VPNI, with the only exception noted in point 2, next.
2. Branch office (MG 1000B and SRG) Call Servers must be configured with the same VPNI as that of the main office Call Server with which they register.
3. Virtual Trunks must be configured with a different Zone number than the endpoints.

Network Planning

Before configuring Bandwidth Management in a CS1000 network, follow these steps:

1. Choose unique VPNIs for all Call Servers in the network.
2. Choose unique Bandwidth Zone numbers for all Call Servers in the network. These are used when configuring the endpoints (telephones and gateways) on the Call Server.
3. Choose unique Bandwidth Zone numbers for the Virtual Trunks in the network.
4. Choose the codecs that will be enabled on each Call Server.

5. Identify what the interzone codec strategy will be (BB-Best Bandwidth or BQ-Best Quality) for each zone in the network.
6. Identify what the intrazone codec strategy will be (BB-Best Bandwidth or BQ-Best Quality) for each zone in the network.
7. Calculate the bandwidth available for intrazone calls for each zone in the network.
8. Calculate the bandwidth available for interzone calls for each zone in the network.
9. Calculate the bandwidth available for intrazone calls

Enabling codecs

In Element Manager, select the codecs that will be enabled for calls on the Call Server, and define the associated parameters, such as payload size.

Use Procedure 13 on page 319 to view available codecs, and configure existing or new codecs.

Configuring Bandwidth Management parameters

The steps to configure Bandwidth Management on the Call Server are as follows:

1. Define a VPNI number in LD 15.
2. Configure the Bandwidth Management parameters for each zone on the Call Server using either Element Manager (see “Configuration using CS 1000 Element Manager” on page 142) or LD 117 (see “Configuration using LD 117” on page 143):
   - Call Server zones that will be used for endpoints (telephones and gateways) with the following properties:
     - — Intrazone Preferred Strategy = Best Quality (BQ)
     - — Intrazone Bandwidth = default (1000000)
     - — Interzone Preferred Strategy = Best Bandwidth (BB)
     - — Interzone Bandwidth = maximum bandwidth usage allowed between peer Call Servers

- Call Server zones that will be used for Virtual Trunks with the following properties:
  - — Intrazone Preferred Strategy = Best Quality (BQ)
  - — Intrazone Bandwidth = default (1000000)
  - — Interzone Preferred Strategy = Best Bandwidth (BB)
  - — Interzone Bandwidth = default (1000000)

3 Configure the IP Phone, DSP and Virtual Trunk data with the corresponding zone numbers.

For example, for an IP Phone 2004 telephone in zone 8:

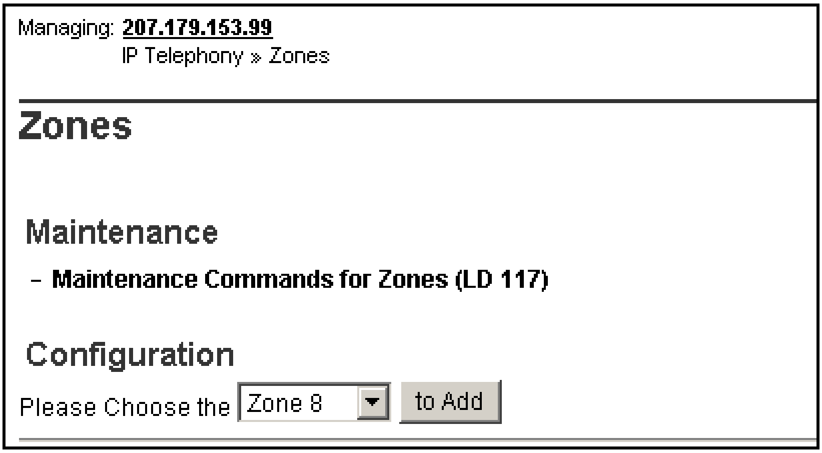
```
LD 11
REQ NEW
TYPE i2004
...
ZONE 8
...
```

Configuration using CS 1000 Element Manager

Zones are configured from the Zones web page, shown in Figure 50.

Use Procedure 6 on page 295 to configure a Network Bandwidth Management zone, using the values given on page 141.

Figure 50
Zones web page



Managing: 207.179.153.99
IP Telephony » Zones

Zones

Maintenance

- Maintenance Commands for Zones (LD 117)

Configuration

Please Choose the Zone 8 to Add

Configuration using LD 117

A new Bandwidth Management zone is configured in LD 117 using the NEW ZONE command. An existing zone can be modified using the CHG ZONE command.

LD 117 Configure a new or existing Bandwidth Management zone.

Command	Description
NEW | CHG ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneIntent> <zoneResourceType>]	
	Configure a new zone (NEW) or change (CHG) an existing zone, where: • zoneNumber = 0-255 • intraZoneBandwidth = Available intrazone bandwidth (Kbit/s); Nortel recommends this value be set to the maximum value. • intraZoneStrategy = BB (Best Bandwidth) or BQ (Best Quality); Nortel recommends this value be set to BQ. • interZoneBandwidth = — For Call Server zone = Maximum bandwidth usage (in Kbit/s) allowed between peer Call Servers — For Virtual Trunk zones = 1000000 (Kbit/s) • interZoneStrategy = BB (Best Bandwidth) or BQ (Best Quality); Nortel recommends this value be set to BB to conserve interzone bandwidth. • zoneIntent = type of zone, where: — MO = Main office (Call Server) zone — BMG = Branch Media Gateway (for branch office zones) — VTRK = Virtual Trunk zone • zoneResourceType = resource intrazone preferred strategy, where: — shared = shared DSP channels (default) — private = private DSP channels ***Note:*** In CS 1000 Release 4.5, the zones that were described with BMG designator stay with BMG one, all the other zones are provided with MO designator. It is possible to update ZoneIntent using CHG ZONE command.

Maintenance commands

Maintenance commands can be run from Element Manager or LD 117.

Maintenance using Element Manager

The PRT INTRAZONE and PRT INTERZONE commands are available in Element Manager from the Zones web page, shown in Figure 50 on page 143. To access these commands, follow the steps in Procedure 1 on page 145.

Procedure 1
Printing intrazone and interzone statistics for a zone

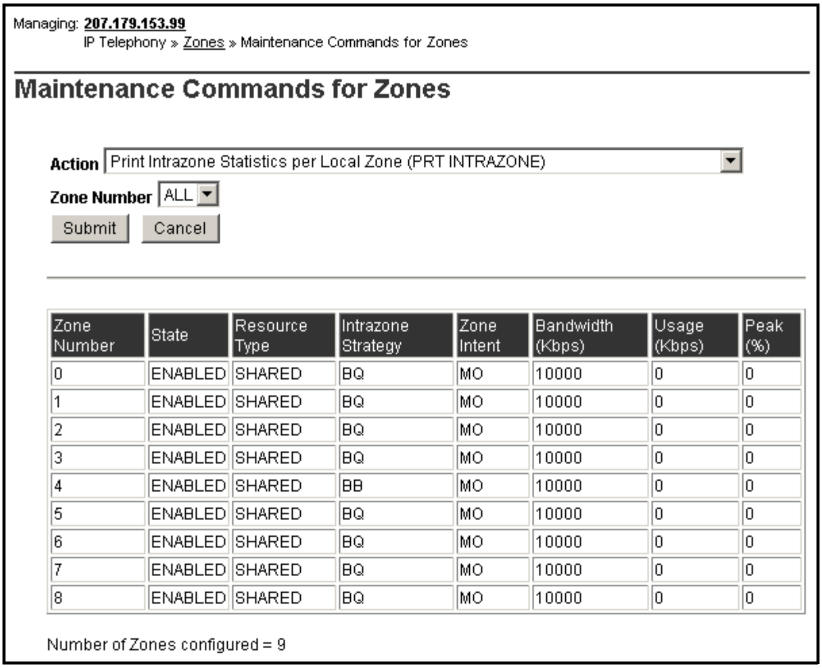
1 Select **IP Telephony > Zones** from the navigator.

The **Zones** web page opens, as shown in Figure 50 on page 143.

2 Click **Maintenance Commands for Zones (LD 117)**.

The **Maintenance Commands for Zones** web page opens, as shown in Figure 51 on page 146. This page lists all the configured zones.

Figure 51
Maintenance Commands for Zones web page



Managing: **207.179.153.99**
IP Telephony » Zones » Maintenance Commands for Zones

Maintenance Commands for Zones

Action Print Intrazone Statistics per Local Zone (PRT INTRAZONE)

Zone Number ALL

Zone Number	State	Resource Type	Intrazone Strategy	Zone Intent	Bandwidth (Kbps)	Usage (Kbps)	Peak (%)
0	ENABLED	SHARED	BQ	MO	10000	0	0
1	ENABLED	SHARED	BQ	MO	10000	0	0
2	ENABLED	SHARED	BQ	MO	10000	0	0
3	ENABLED	SHARED	BQ	MO	10000	0	0
4	ENABLED	SHARED	BB	MO	10000	0	0
5	ENABLED	SHARED	BQ	MO	10000	0	0
6	ENABLED	SHARED	BQ	MO	10000	0	0
7	ENABLED	SHARED	BQ	MO	10000	0	0
8	ENABLED	SHARED	BQ	MO	10000	0	0

Number of Zones configured = 9

3 Do one of the following:

- To display interzone statistics:

  i. Select **Print Interzone Statistics (PRT INTERZONE)** from the **Action** drop-down list.

  ii. Select a zone from the **Zone Number** drop-down list, by doing one of the following:

  — Select **ALL** to print statistics for all zones.

  — Select a specific zone number to display statistics for a specific zone.

- To display intrazone statistics:

  i. Select **Print Intrazone Statistics per Local Zone (PRT INTRAZONE)** from the **Action** drop-down list.

ii. Select a zone from the **Near End Zone Number** drop-down list, by doing of the following:

— Select **ALL** to print statistics for all zones.

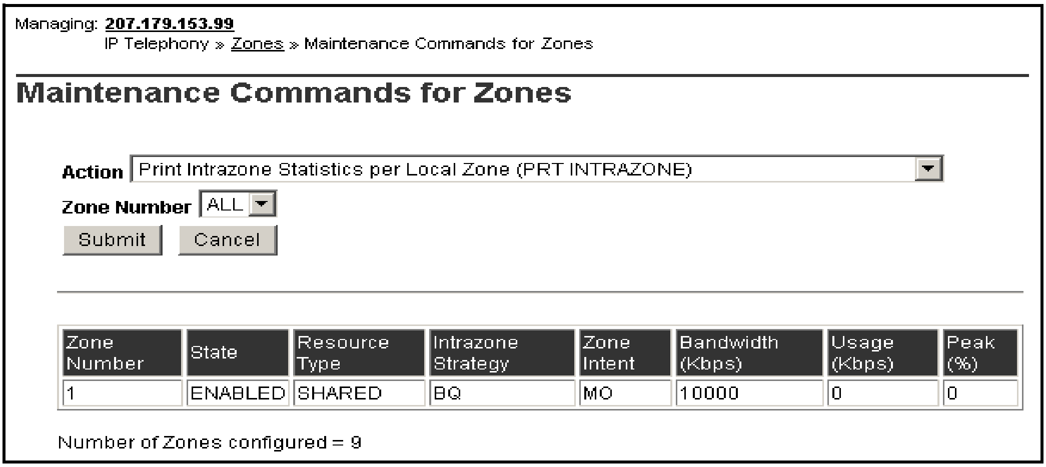
— Select a specific zone number to display statistics for a specific zone.

4 Click **Submit**.

The **Maintenance Commands for Zones** web page reopens, displaying the statistics for the specified zone or zones. A blank field indicates that that statistic is either not available or not applicable to that zone.

Figure 52 shows an example of intrazone statistics for a sample Zone 1. Figure 53 on page 148 shows an example of interzone statistics for the same Zone 1.

Figure 52
Element Manager — intrazone statistics



Managing: 207.179.153.99
IP Telephony » Zones » Maintenance Commands for Zones

Maintenance Commands for Zones

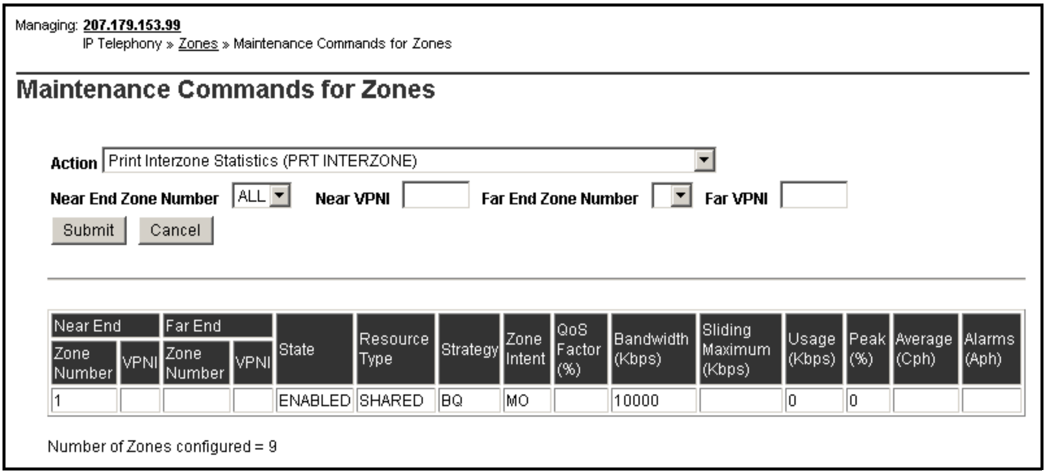
Action: Print Intrazone Statistics per Local Zone (PRT INTRAZONE)

Zone Number: ALL

Zone Number	State	Resource Type	Intrazone Strategy	Zone Intent	Bandwidth (Kbps)	Usage (Kbps)	Peak (%)
1	ENABLED	SHARED	BQ	MO	10000	0	0

Number of Zones configured = 9

Figure 53
Element Manager — interzone statistics



Managing: 207.179.153.99
IP Telephony » Zones » Maintenance Commands for Zones

Maintenance Commands for Zones

Action Print Interzone Statistics (PRT INTERZONE)

Near End Zone Number ALL **Near VPNI** **Far End Zone Number** **Far VPNI**

Near End		Far End		State	Resource Type	Strategy	Zone Intent	QoS Factor (%)	Bandwidth (Kbps)	Sliding Maximum (Kbps)	Usage (Kbps)	Peak (%)	Average (Cph)	Alarms (Aph)
Zone Number	VPNI	Zone Number	VPNI											
1				ENABLED	SHARED	BQ	MO		10000		0	0		

Number of Zones configured = 9

End of Procedure

Maintenance using LD 117

Use the PRT INTRAZONE or PRT INTERZONE commands in LD 117 to view the intrazone or interzone statistics for specified zones.

> ***Note:*** Do not use the PRT ZONE command — it has been replaced by the PRT INTRAZONE and PRT INTERZONE commands.

LD 117 Print zone statistics.

Command	Description
PRT INTRAZONE {<zone>}	
	Print intrazone statistics for the identified zones, where: • zone = ALL or 0-255 The output of this command displays the following information: • Zone • Type = PRIVATE/SHARED • Strategy = BB/BQ • ZoneIntent = MO/BMG/VTRK • Bandwidth = number of Kbps • Usage = number of Kbps • Peak = %
PRT INTERZONE {<nearZone>} [{<nearVPNI>} {<farZone>} {<farVPNI>}]	
	Print interzone statistics for the specific VPNI zone; where: • nearZone = ALL or 0-255 The output of this command displays the following information: • Zone number = 0-255 • Zone VPNI = 1-16283 • Type= PRIVATE/SHARED • Strategy = BB/BQ • ZoneIntent = MO/VTRK

Adaptive Network Bandwidth Management

Description

The Adaptive Network Bandwidth Management feature enhances the performance of Voice over Internet Protocol (VoIP) networks based on real-time interaction. It provides the means to automatically adjust bandwidth limits and take corrective action in response to Quality of Service (QoS) feedback. This dynamic bandwidth adjustment maintains a high level of voice quality during network degradation.

The Adaptive Network Bandwidth Management feature dynamically adapts to QoS in the network and reduces the bandwidth available for interzone calls if QoS degrades. Typically, each Call Server in the network has a zone assigned to it. The Call Server keeps track of the bandwidth being used between its own zone and zones belonging to other Call Servers. If the QoS degrades between the Call Server zone and a zone belonging to another Call Server, the available bandwidth is reduced automatically between those two zones. When the QoS between the two zones improves, then the bandwidth limit is allowed to return to normal.

When an IP Phone encounters degradation of the network, it informs the Call Server through various QoS alarms. These QoS alarms (packet loss, jitter, delay, and, for phase 2 IP Phones, R value) get reported to the Call Server. Depending upon the rate of the incoming alarms and the value of the alarms, the Call Server reduces the available bandwidth available to make new calls. The Call Server will lower/limit the number of new calls allowed, based on the available bandwidth. This prevents excessive calls being placed on a network with limited bandwidth (resulting in poor voice quality). Once the adjusted (lowered) bandwidth reaches its full capacity, new calls are either routed to an alternate route (if available) using Network Alternate Routing Service (NARS) or the Alternative Routing for NBWM feature (see *Branch Office: Installation and Configuration* (553-3001-214)), or new calls are blocked. The Call Server continues to monitor the network throughout the network degradation period. When the degradation is removed or the performance of the network improves, the allowable bandwidth returns to provisioned levels and the Call Server gradually starts allowing new calls.

Essentially, Adaptive Network Bandwidth Management provides a fallback to PSTN on QoS degradation for new calls. As a result, bandwidth is managed and quality measured between all the zones across the entire network, and when necessary corrective action is taken. Due to the real-time interaction with the network, less maintenance is required for the network since the system reacts automatically to network conditions.

With Adaptive Network Bandwidth Management, it is not necessary to provision bandwidth parameters between every zone in the network. Rather, the Call Server automatically learns of new zones in the network and applies

Adaptive Network Bandwidth Management to these new zones as required. Therefore, as new Call Servers are added to the network, it is not necessary to re-provision all the other Call Servers on the network to take into account this new Call Server. Conversely, when Call Servers are removed from the network, the remaining Call Servers age out the old Call Server information and therefore, provide only up to date bandwidth information.

This feature operates between all IP Peer CS 1000 systems, including the Media Gateway 1000B and Survivable Remote Gateway 50.

Call scenario

A call is requested from a telephone in VPNI 1/Zone 2 on Call Server A to a telephone in VPNI 3/Zone 3 on Call Server B. Both zones have Adaptive Network Bandwidth Management enabled.

1 Call Server A contacts the Network Redirect Server to obtain the address of Call Server B.

2 Call Server A sends a call setup message to Call Server B, identifying the calling telephone's VPNI and zone.

3 Call Server B determines if there is sufficient bandwidth for the call, and sends back the VPNI and zone of the called telephone.

4 Call Server A checks its bandwidth table to determine if there is sufficient bandwidth available for the call from Call Server A to Call Server B.

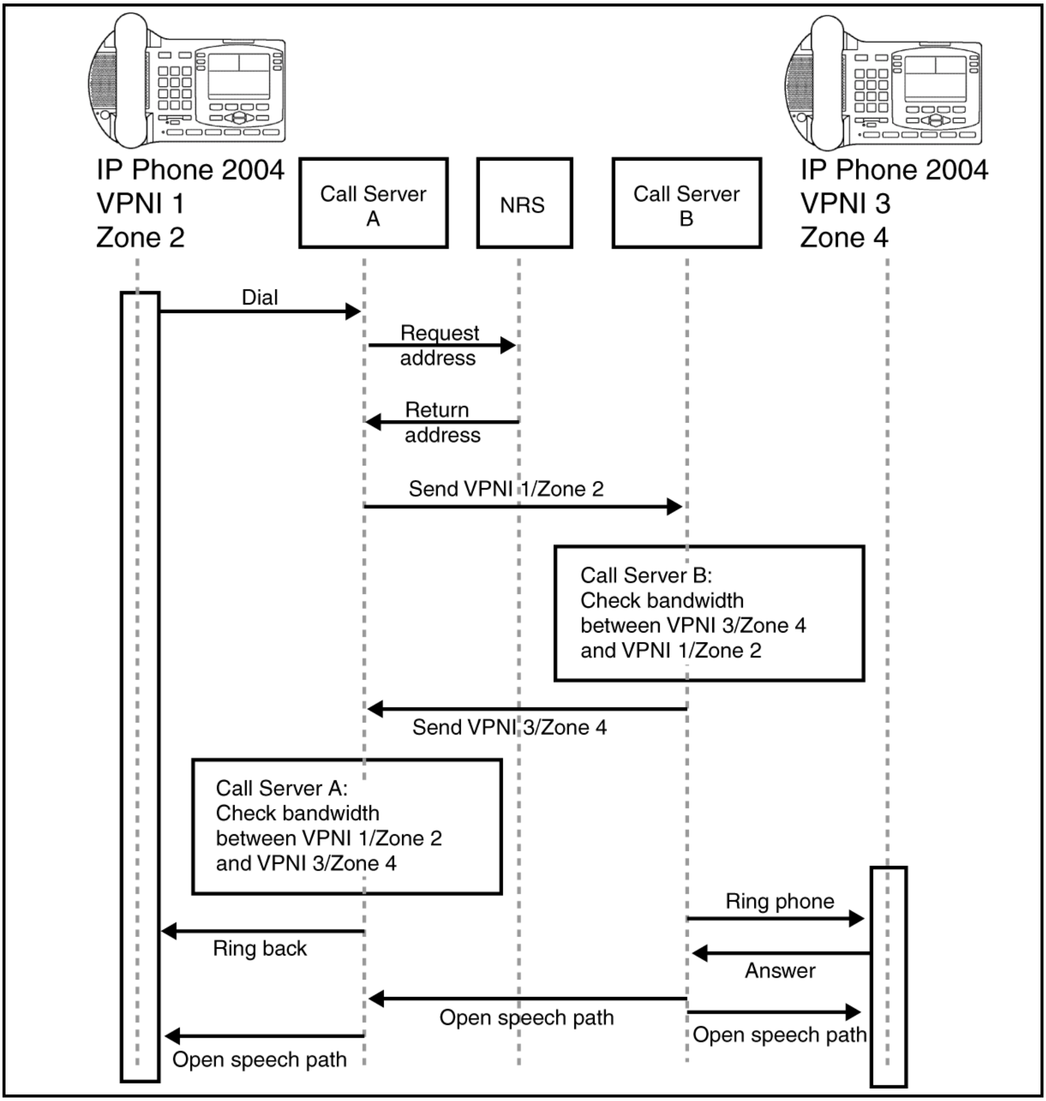
5 If Call Server A determines there is enough bandwidth available, the call is established; otherwise, alternate treatment is provided in the form of blocking or rerouting the call.

Both Call Server A and Call Server B must consult their own bandwidth tables to determine if there is enough bandwidth for the call to proceed. Figure 54 on page 152 shows this scenario.

Limitations

The far-end set experiences a short ring burst if the bandwidth limit between the two zones is reached and a call is made between these two zones. The call is rejected after the Call Server realizes that the bandwidth limit is reached but the far-end set rings temporarily until the call is rejected.

Figure 54
Call Progress with Adaptive Network Bandwidth Management



Zone bandwidth management and Adaptive Network Bandwidth Management

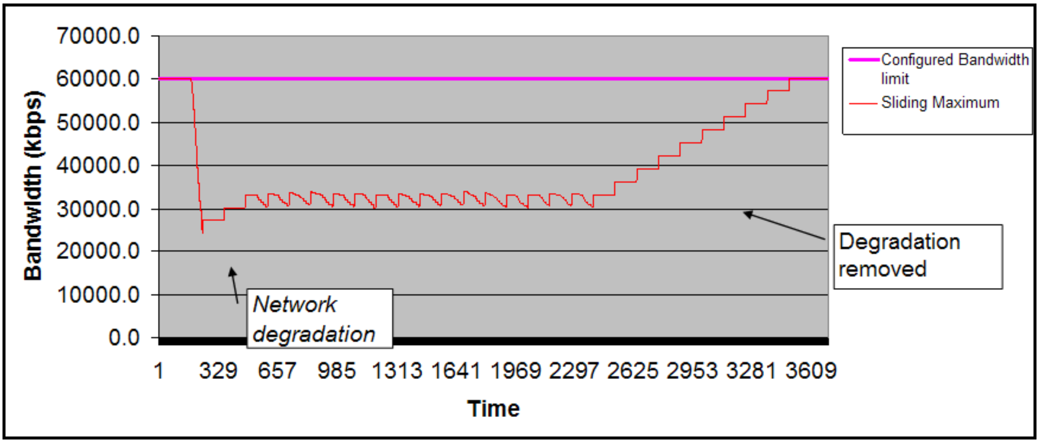
Using Element Manager or the Command Line Interface (CLI), previously configured zones (except Zone 0) can have the Adaptive Network Bandwidth Management feature turned on or off. Once turned on, alarm threshold levels and the QoS coefficients can be adjusted from the default values. Adaptive Network Bandwidth Management cannot be enabled for Zone 0.

When Adaptive Network Bandwidth Management is enabled for a particular zone on the Call Server, the zone appears in the zone table. The zone table can be displayed using Element Manager or LD 117. When a call is made from the configured zone to another zone, the bandwidth used appears in the zone table.

When a call is made from a zone with Adaptive Network Bandwidth Management enabled, to a third party gateway, which has no zone, then the zone of the Virtual Trunk (VTRK) is used and appears in the zone table.

Figure 55 shows an example of the bandwidth changes.

Figure 55
Adaptive Network Bandwidth Management graph



When a Call Server receives a QoS alarm, the two zones that originated the alarm are determined. Using this information, the Call Server reduces the bandwidth limit between the two zones. This zone-to-zone bandwidth limit (in effect at any particular time) is known as the Sliding Maximum Bandwidth Limit and is a percentage of the Configured Interzone bandwidth limit. The Sliding Maximum Bandwidth Limit value is displayed using the command `prt interzone` command. The `QoS Factor %` value, also displayed by this command, is a ratio of the Sliding Maximum Bandwidth Limit and the configured allowable bandwidth expressed as a percentage. The Call Server checks the Network Bandwidth zone management tables for the originating and terminating zones of the new call to determine the available bandwidth for the call.

For more information about alarms, refer to *Software Input/Output: System Messages* (553-3001-411).

When feedback indicates a significant QoS change in a zone, the Call Server reduces the available bandwidth (Sliding Maximum Bandwidth Limit) in the zone until the QoS reaches a satisfactory level. Once satisfactory QoS is reached, the bandwidth is slowly raised until either the full bandwidth is available or until QoS degrades again. Bandwidth changes can be configured to be gradual (to reduce rapid swings and variations) or rapid.

Multiple Appearance Directory Numbers (MADN) can exist on different zones. Calls to an MADN are handled the same as other IP Phone calls, and are subject to the same bandwidth limitations.

New SNMP alarms are provided to monitor the system. When the bandwidth limit between zones is reduced below configured levels, an alarm is raised. A Warning alarm and an Unacceptable alarm, each corresponding to a drop below a configured threshold, are used. When the bandwidth returns to normal, the alarm is cleared. If the bandwidth limit reaches zero, an additional Unacceptable alarm is raised. These alarms allow the system administrator to monitor the system and take corrective action when required.

Adaptive Network Bandwidth Management configuration parameters

Packet Loss (pl), Jitter (j) and Delay (d) measurements, along with the R factor (r) in IP Phone 200x Phase II telephones, are used to calculate the QoS level for the zones. The coefficients for these QoS measurements — packet loss (Cpl), jitter (Cj), delay (Cd), and the R factor (Cr) — can be configured and are used to calculate the rate of bandwidth change. Increasing them from their default values causes the Sliding Maximum to decrease faster in response to the specific QoS alarm.

The QoS Coefficient (CQoS) can be varied from its default value. Increasing this value causes the Sliding Maximum to change more rapidly in response to QoS alarms. However, making this value too large will result in loss of overall bandwidth, as shown in Figure 56 below and Figure 57 on page 156.

Figure 56
Effect of the default CQos Coefficient

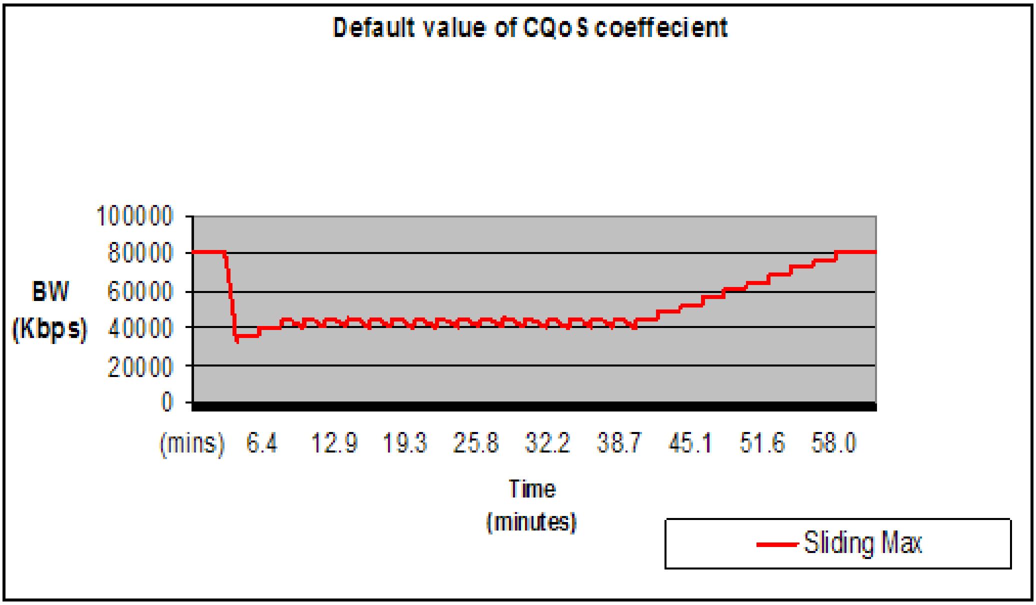
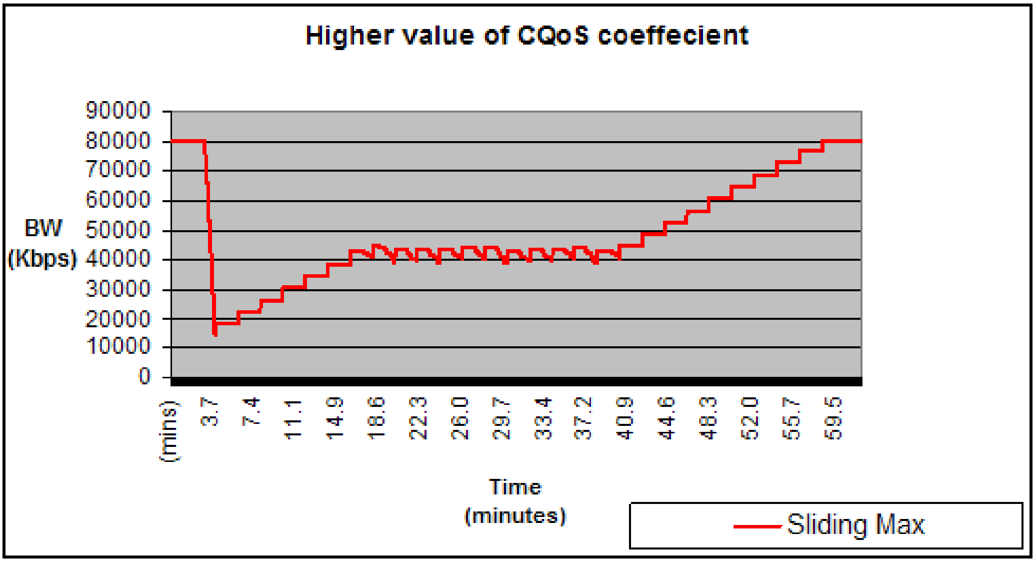


Figure 57
Effect of a higher CQoS Coefficient



Other configurable coefficients used in the calculation are the QoS Coefficient (CQoS), QoS Response Time Increase (ZQRT), and QoS Response Time Interval (ZQRTI). CQoS, Cr, Cd, Cpl, and Cj control the rate of bandwidth decrease, while ZQRT and ZQRTI control the rate of bandwidth increase.

The Call Admission Control (CAC) Validity Time Interval (CACVT) is used to control the length of time that records from a Call Server are saved in the Bandwidth Management table. If no calls occur between two Call Servers within the configured time, the Call Server is removed from the table. For example, if Call Server A has Call Server B in the table, and no call is placed between A and B for the CACVT time, then Call Server A removes all Call Server B records in the table.

Limitations

Virtual Office IP Phones are not subject to bandwidth limitations. They may not have the correct zone information configured. They can also be controlled by a Call Server that is not responsible for the particular zone. Thus, bandwidth management is not possible for these phones.

Feature packaging

The Adaptive Network Bandwidth Management feature requires the following packages:

- QoS Enhanced Reporting (PVQM) package 401

  Note: Package 401, QoS Enhanced Reporting (PVQM), is required if the R value from the Phase II IP Phones is to be reported and used in the calculations.

- Call Admission Control (CAC) package 407

Configuration rules

The configuration rules for Adaptive Network Bandwidth Management are as follows:

- Each main office Call Server in a network must have a unique non-zero VPNI.
- All branch offices (MG1000B or SRG) associated with a particular main office must have the same VPNI as the main office Call Server.
- All IP Phones (other than specific IP SoftPhone 2050s) and DSP endpoints on a Call Server must be configured for the same zone.
- IP SoftPhone 2050s being used remotely must be configured for Zone 0.
- Branch office systems (MG 1000B or SRG) should tandem all calls through the main office Call Server to allow bandwidth monitoring and control. In this case, the media path is direct between the branch office and any point in the network.
- Trunk Route Optimization (TRO) must be disabled between the main office Call Server and the MG 1000B Core or SRG. In this case, the media path is direct between the branch office and any point in the network.
- Adaptive Network Bandwidth Management parameters are configured on the main office only and must not be configured at the branch offices.

Configuring Adaptive Network Bandwidth Management

The following is a summary of the tasks necessary to configure Adaptive Network Bandwidth Management in the network.

1 Enable the Call Admission Control (CAC) package.

2 Configure CAC in Element Manager or LD 117:

  a Configure the VPNI on the main office and branch offices.

  b Configure both the main office and branch office zones at the main office.

  c Configure the branch office zone on the MG 1000B Core or SRG.

  d Configure the interzone and intrazone bandwidth limits at the main office and MG 1000B Core or SRG.

  e Enable Adaptive Network Bandwidth Management for the zones on the main office Call Server.

  f If required, alter the Adaptive Network Bandwidth Management parameters in keeping with the information in "Advanced Configuration Notes" below.

3 Tandem the outbound branch office calls by configuring the NRS.

4 Tandem the inbound branch office calls by creating a dialing plan which routes all calls destined for the branch office through the main office.

Advanced Configuration Notes

1 The default values for Cpl, Cj, Cd, Cr and CQos can be increased to increase the response time for Sliding Maximum changes. However, increasing them can cause the Sliding Maximum to temporarily decrease to a lower value then necessary, resulting in the needless blocking of interzone calls.

2 Increasing the value of ZQRT will increase the speed at which the Sliding Maximum increases. The same effect can be achieved by decreasing ZQRTI. However, changing these values can cause the Sliding maximum to oscillate until the network degradation is removed.

3 It may be necessary to change the notification level (ZQNL) of the Call Server so it can react to the QoS alarms. Use LD 117 to change this level.

Refer to *Converging the Data Network with VoIP* (553-3001-160) for information on notification levels for alarms.

Configuration using Element Manager

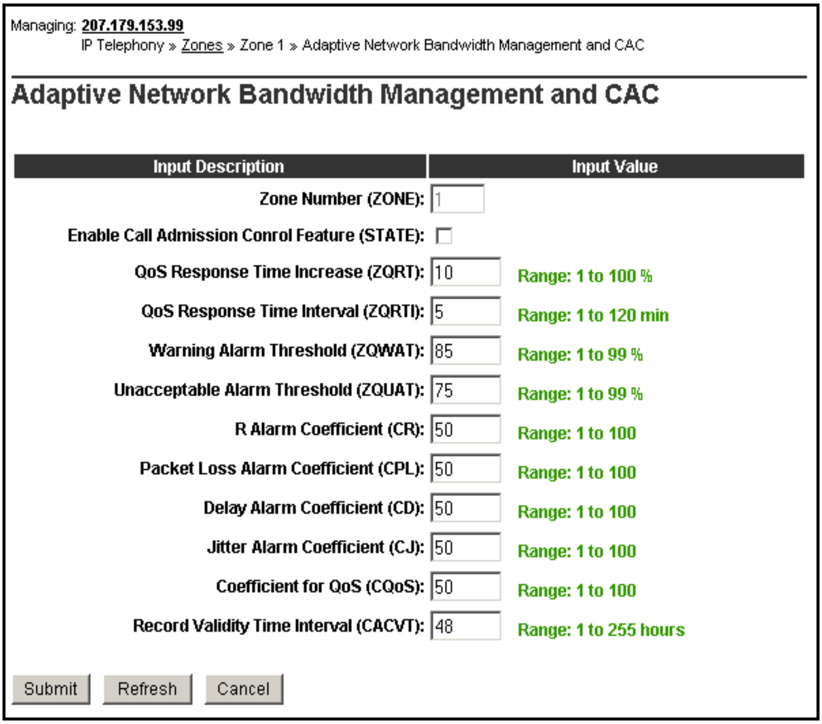
Element Manager can be used to enable and configure the feature.

The zone must exist before it can be configured for Adaptive Network Bandwidth Management. Use Procedure 6 on page 295 to create and configure basic properties of the zone.

To configure the Adaptive Network Bandwidth Management feature, select a zone on the Zones web page (see Figure 50 on page 143) and click **Adaptive Network Bandwidth Management and CAC**. The **Adaptive Network Bandwidth Management and CAC** web page opens, as shown in Figure 58 on page 160.

> ***Note:*** Do not configure Adaptive Network Bandwidth Management for Zone 0 or Virtual Trunk zones.

Figure 58
Adaptive Network Bandwidth Management and CAC web page



Managing: 207.179.153.99
IP Telephony » Zones » Zone 1 » Adaptive Network Bandwidth Management and CAC

Adaptive Network Bandwidth Management and CAC

Input Description	Input Value	
Zone Number (ZONE):	1	
Enable Call Admission Conrol Feature (STATE):	□	
QoS Response Time Increase (ZQRT):	10	Range: 1 to 100 %
QoS Response Time Interval (ZQRTI):	5	Range: 1 to 120 min
Warning Alarm Threshold (ZQWAT):	85	Range: 1 to 99 %
Unacceptable Alarm Threshold (ZQUAT):	75	Range: 1 to 99 %
R Alarm Coefficient (CR):	50	Range: 1 to 100
Packet Loss Alarm Coefficient (CPL):	50	Range: 1 to 100
Delay Alarm Coefficient (CD):	50	Range: 1 to 100
Jitter Alarm Coefficient (CJ):	50	Range: 1 to 100
Coefficient for QoS (CQoS):	50	Range: 1 to 100
Record Validity Time Interval (CACVT):	48	Range: 1 to 255 hours

If the Adaptive Network Bandwidth Management feature is enabled using the **Enable Call Admission Control feature** (**ZCAC**) check box, then the other parameters can be adjusted as required.

Table 9 on page 161 shows the fields in the **Adaptive Network Bandwidth Management and CAC** web page, the field definitions, and their LD 117 command equivalent.

Table 9
Adaptive Network Bandwidth Management and CAC fields

Field Title	Field Definition	LD 117 equivalents
Enable Call Admission Control Feature (CAC)	Control the CAC feature for the zone • Enable (check box selected) • disable (clear the check box)	ENL ZCAC DIS ZCAC
QoS Response Time Increase (ZQRT)	Bandwidth limit increment, as a percentage of the QoS factor for the zone	CHG ZQRT
QoS Response Time Interval (ZQRTI)	Time (in minutes) between bandwidth limit increments	CHG ZQRTI
Warning Alarm Threshold (ZQWAT)	A QoS value, which is lower than this value, but higher than the Critical (Unacceptable) Alarm Threshold, triggers a Major Alarm.	CHG ZQWAT
Critical Alarm Threshold (ZQUAT)	A QoS value, which is lower than this value, triggers an Unacceptable (Critical) Alarm.	CHG ZQUAT
R Alarm Coefficient (CR)	The R (Cr) coefficient is used to calculate the QoS value for the zone.	CHG CR
Packet Loss Alarm Coefficient (CPL)	The Packet Loss (Cpl) coefficient is used to calculate the QoS value for the zone.	CHG CPL
Delay Alarm Coefficient (CD)	The Delay (Cd) coefficient is used to calculate the QoS value for the zone.	CHG CD
Jitter Alarm Coefficient (CJ)	The Jitter (Cj) coefficient is used to calculate the QoS value for the zone.	CHG CJ
Coefficient of QoS (CQoS)	The Coefficient of QoS (CQoS) is used to calculate the overall QoS value for the zone.	CHG CQOS
Recent Validity Time Interval (CACVT)	Amount of time (in hours) for zone-to-zone record validity. Once this interval expires, records for unused zones are purged from the tables.	CHG CACVT

Configuration using Command Line Interface

You can also configure the Adaptive Network Bandwidth Management feature using LD 117.

LD 117 — Configure Adaptive Network Bandwidth Management. (Part 1 of 6)

Command	Description
CHG CACVT <Zone> <Interval>	
	Configure the zone-to-zone record validity time interval, where: • Zone = 1-255 • Interval = 1-(48)-255
CHG CD <Zone> <Cd>	
	Change the Cd coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where: • Zone = 1-255 • Cd = Cd coefficient = 1-(50)-100
CHG CPL <Zone> <Cpl>	
	Change the Cpl coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where: • Zone = 1-255 • Cpl = Cpl coefficient = 1-(50)-100
CHG CJ <Zone> <Jitter>	
	Change the Cj coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where: • Zone = 1-255 • Jitter = Jitter coefficient = 1-(50)-100

LD 117 — Configure Adaptive Network Bandwidth Management. (Part 2 of 6)

Command	Description
CHG CQOS <Zone> <QoS>	
	Change the QoS coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where: • Zone = 1-255 • QoS = QoS coefficient = 1-(50)-100
CHG CR <Zone> <Cr>	
	Change the Cr coefficient in the formula that determines how quickly an alarm reduces the Sliding Maximum bandwidth for the identified zone, where: • Zone = 1-255 • Cr = Cr coefficient = 1-(50)-100

LD 117 — Configure Adaptive Network Bandwidth Management. (Part 3 of 6)

Command	Description
CHG ZONE <zoneNumber> <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> [<zoneIntent> <zoneResourceType>]	
	Change the parameters of an existing zone, where: • zoneNumber = 1-255 • intraZoneBandwidth = 1000000 (Mbit/s) • intraZoneStrategy = intrazone preferred strategy — Best Quality = BQ — Best Bandwidth = BB • interZoneBandwidth = 100000 (Mbit/s) • interZoneStrategy = intrazone preferred strategy — Best Quality = BQ — Best Bandwidth = BB • zoneIntent = type of zone, where: — MO = Main office zone — BMG = Branch Media Gateway (branch office) zone — VTRK = Virtual Trunk zone • zoneResourceType = resource intrazone preferred strategy — shared DSP channels (default) = shared — private DSP channels = private ***Note:*** In CS 1000 Release 4.5, the zones that were described with BMG designator stay with BMG one, all the other zones are provided with MO designator. It is possible to update ZoneIntent using the CHG ZONE command.
CHG ZQRT <Zone> <Incr>	
	Change ZQRT, which is Response time increase by percentage. It is used to determine the increase to the Sliding Maximum for the identified zone, where: • Zone = 1-255 • Incr = increase value in percentage = 1-(10)-100

LD 117 — Configure Adaptive Network Bandwidth Management. (Part 4 of 6)

Command	Description
CHG ZQRTI <Zone> <Interval>	
	Change the QoS Response Time Interval while alarms are not coming, in order to increase the Sliding Maximum for the identified zone, where: • Zone = 1-255 • Interval = interval in minutes = 1-(5)-120
CHG ZQUAT <Zone> <Thres>	
	Change the QoS Unacceptable Alarm Threshold value for the identified zone, where: • Zone# = 1-255 • Thres = threshold value = 1-(75)-99 ***Note:*** When the zone-to-zone QoS value drops below the threshold value, the alarm is presented. This value must be below the value of ZQWAT.
CHG ZQWAT <Zone> <Thres>	
	Change the QoS Warning Alarm Threshold value for the identified zone, where: • Zone = 1-255 • Thres = threshold value = 1-(85)-99 ***Note:*** When the zone-to-zone QoS value drops below the threshold value, the alarm is presented. The value for ZQWAT must be higher than the value of ZQUAT.

LD 117 — Configure Adaptive Network Bandwidth Management. (Part 5 of 6)

Command	Description
CHG ZQNL <ZoneNumber> <level>	
	Change the Notification Level for the specified zone, where: • Zone = 1-255 • Level = 0-(2)-4, where: — Level 0 = All voice quality alarms are suppressed. — Level 1 = All zone-based Unacceptable alarms. — Level 2 = Allow all level 1 alarms PLUS zone-based Warning alarms. — Level 3 = Allow all level 1 and 2 alarms PLUS per-call Unacceptable alarms. — Level 4 = Allow all level 1, 2, and 3 alarms PLUS per-call Warning alarms.
NEW ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <zoneIntent> <zoneResourceType>]	
	• zoneNumber = 1-255 • intraZoneBandwidth = 1000000 (Mbit/s) • intraZoneStrategy = BQ (Best Quality) • interZoneBandwidth = 1000000 (Mbit/s) • interZoneStrategy = intrazone preferred strategy — Best Quality = BQ — Best Bandwidth = BB • zoneIntent = type of zone, where: — MO = Main office zone — BMG = Branch Media Gateway (branch office) zone — VTRK = Virtual Trunk zone • zoneResourceType = resource intrazone preferred strategy — shared DSP channels (default) = shared — private DSP channels = private

LD 117 — Configure Adaptive Network Bandwidth Management. (Part 6 of 6)

Command	Description
DIS ZCAC <Zone>	
	Disables the Call Admission Control (CAC) feature for the specified zone, where: • Zone = 1-255 ***Note:*** Disables the feature on a zone-by-zone basis.
ENL ZCAC <Zone>	
	Enables the Call Admission Control (CAC) feature for the specified zone, where: • Zone = 1-255 ***Note:*** Enables the feature on a zone-by-zone basis.

Maintenance commands

The Adaptive Network Bandwidth Management feature can be maintained using Element Manager or LD 117.

Maintenance using Element Manager

The CAC parameters, intrazone statistics, and interzone statistics for one of more zones are available in Element Manager from the Zones web page, shown in Figure 50 on page 143. To view the intrazone or interzone statistics, use Procedure 1 on page 145. To display the CAC parameters, follow the steps in Procedure 2.

Procedure 2
Displaying CAC parameters for one or more zones

1 Select **IP Telephony > Zones** from the navigator.

The **Zones** web page opens (see Figure 50 on page 143).

2 Click **Maintenance Commands for Zones (LD 117)**.

The **Maintenance Commands for Zones** web page opens, as shown in Figure 51 on page 146. This page lists all the configured zones and their intrazone statistics by default.

3 Select **Print Adaptive Network Bandwidth Management and CAC Parameters (PRT ZCAC)** from the **Action** drop-down list.

4 Select a zone from the **Zone Number** drop-down list, by doing one of the following:

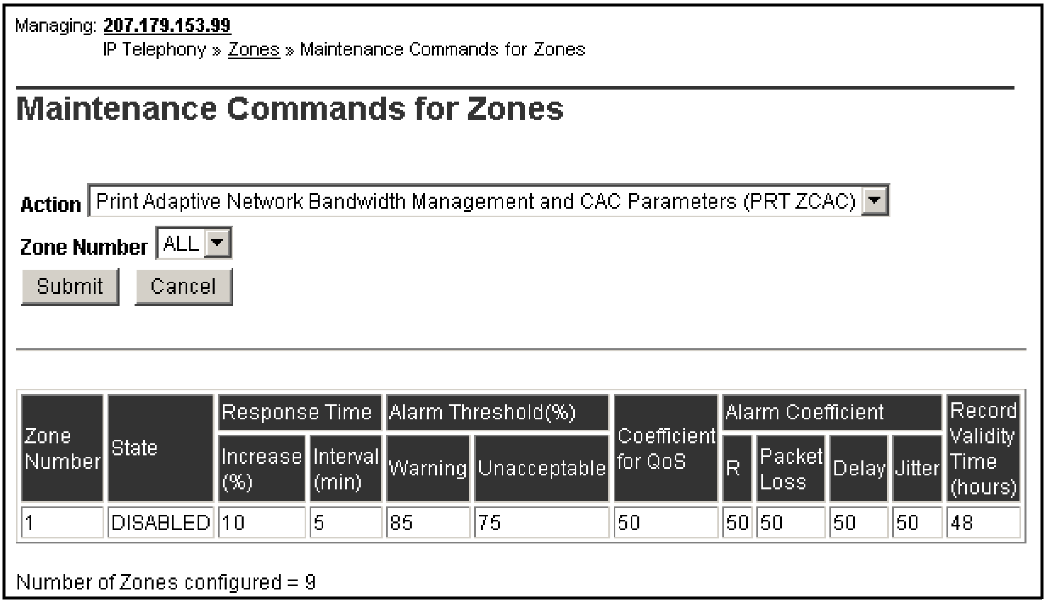
- Select **ALL** to print statistics for all zones.
- Select a specific zone number to display statistics for a specific zone.

5 Click **Submit**.

The **Maintenance Commands for Zones** web page reopens, displaying the statistics for the specified zone or zones. A blank field indicates that that statistic is either not available or not applicable to that zone.

Figure 59 on page 169 shows an example of the CAC parameters for sample Zone 1.

Figure 59
Element Manager — CAC parameters



Managing: **207.179.153.99**
IP Telephony » Zones » Maintenance Commands for Zones

Maintenance Commands for Zones

Action Print Adaptive Network Bandwidth Management and CAC Parameters (PRT ZCAC)

Zone Number ALL

Zone Number	State	Response Time		Alarm Threshold(%)		Coefficient for QoS	Alarm Coefficient				Record Validity Time (hours)
		Increase (%)	Interval (min)	Warning	Unacceptable		R	Packet Loss	Delay	Jitter	
1	DISABLED	10	5	85	75	50	50	50	50	50	48

Number of Zones configured = 9

End of Procedure

Maintenance using LD 117

The same information can be displayed using commands in LD 117.

LD 117 — Display Adaptive Network Bandwidth Management information (Part 1 of 3)

Command	Description
CLR CACR <Near Zone> [<Near VPNI>] [<Far Zone>] [{<Far VPNI>]	
	Clear zone-to-zone record for near (VPNI-Zone) for far (VPNI-Zone), where: • Near Zone = 1-255 • Near VPNI = 1-16383 • Far Zone = 1-255 • Far VPNI = 1-16383
PRT INTRAZONE [<zone>]	
	Print intrazone statistics for the identified zones, where: • zone = ALL or 1-255 The output of this command displays the following information: • Zone • State = ENL/DIS • Type = PRIVATE/SHARED • Strategy = BB/BQ • MO/BMG/VTRK = ZoneIntent • Bandwidth = Kbps • Usage = Kbps • Peak = % Figure 60 on page 173 shows an example of the output for this command.

LD 117 — Display Adaptive Network Bandwidth Management information (Part 2 of 3)

Command	Description
PRT INTERZONE [<nearZone>] [<nearVPNI>] [<farZone>] [<farVPNI>]	
	Print interzone statistics for the specific VPNI zone; where: • nearZone = ALL or 1-255 • nearVPNI = 1-16383 • farZone = 1-255 • farVPNI = 1-16383 The output of this command displays the following information: • Near end Zone • Near end VPNI • Far end Zone • Far end VPNI • State = ENL/DIS • Type = PRIVATE/SHARED • Strategy = BB/BQ • MO/BMG/VTRK = Zone Intent • QoS factor = % • Bandwidth configured = Kbps • Sliding max = Kbps • Usage = Kbps • Peak = % • Call = Cph • Alarm = Aph The report rows are grouped as: • First row = summary bandwidth usage per near zone • Next rows = bandwidth usage per near (VPNI- Zone) and far (VPNI - Zone) Figure 61 on page 174 shows an example of the output for this command.

LD 117 — Display Adaptive Network Bandwidth Management information (Part 3 of 3)

Command	Description
PRT ZCAC {<zone>}	
	Print CAC parameters for the specified zone, or for all zones, where: • zone = ALL or 1-255 The output of this command displays the following information: • Local ZONE = 1-255 • State = ENL/DIS • CR = 1-100 • CPL = 1-100 • CD = 1-100 • CJ = 1-100 • CQOS = 1-100 • ZQRT = 1-100 • ZQRTI = 10-120 • ZQUAT = 1-99 • ZQWAT =1-99 • CACVT = 1-255

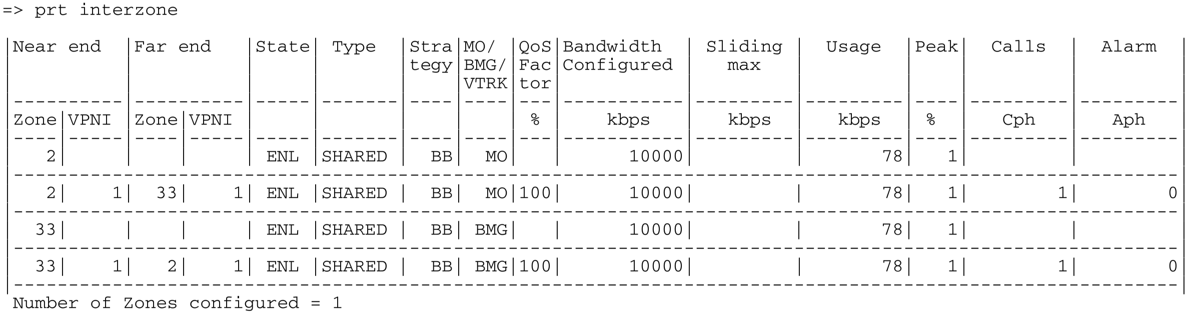
Sample outputs for PRT commands

Figure 60 on page 173 shows an example of the output of the PRT INTRAZONE command. Figure 61 on page 174 shows an example of the output of the PRT INTERZONE command.

Figure 60
Sample output for PRT INTRAZONE command

```
=> prt intrazone
_______________________________________________________________
|Zone|State| Type  |Strategy|MO/ | Bandwidth |  Usage  | Peak |
|    |     |       |        |BMG/|   kbps    |   kbps  |  %   |
|    |     |       |        |VTRK|           |         |      |
|----|-----|-------|--------|----|-----------|---------|------|
|   2| ENL |SHARED |   BQ   |  MO|      10000|      190|   3  |
|-------------------------------------------------------------|
|  44| ENL |SHARED |   BQ   | BMG|      10000|        0|   1  |
|-------------------------------------------------------------|
 Number of Zones configured = 2
```

Figure 61
Sample output for PRT INTERZONE command



```
=> prt interzone
|Near end  |Far end   |State|  Type  |Stra|MO/ |QoS|Bandwidth  | Sliding  |   Usage  |Peak|  Calls   |  Alarm   |
|          |          |     |        |tegy|BMG/|Fac|Configured |   max    |          |    |          |          |
|          |          |     |        |    |VTRK|tor|           |          |          |    |          |          |
|----------|----------|-----|--------|----|----|---|-----------|----------|----------|----|----------|----------|
|Zone|VPNI |Zone|VPNI |     |        |    |    | % |   kbps    |   kbps   |   kbps   | %  |   Cph    |   Aph    |
|----|-----|----|-----|-----|--------|----|----|---|-----------|----------|----------|----|----------|----------|
|   2|     |    |     | ENL |SHARED  |  BB|  MO|   |      10000|          |        78|   1|          |          |
|------------------------------------------------------------------------------------------------------------|
|   2|    1|  33|    1| ENL |SHARED  |  BB|  MO|100|      10000|          |        78|   1|         1|         0|
|------------------------------------------------------------------------------------------------------------|
|  33|     |    |     | ENL |SHARED  |  BB| BMG|   |      10000|          |        78|   1|          |          |
|------------------------------------------------------------------------------------------------------------|
|  33|    1|   2|    1| ENL |SHARED  |  BB| BMG|100|      10000|          |        78|   1|         1|         0|
|------------------------------------------------------------------------------------------------------------|
 Number of Zones configured = 1
```

Note: The Far end and VPNI fields are displayed only when Adaptive Bandwidth Management is enabled in LD 117.

Features

Contents

This section contains information on the following topics:

Tone handling

Progress tones

The IP Phone or Gateway can generate call-progress tones locally. IP Peer Networking supports both in-band and out-of-band generated tones. For example, simple calls between IP Phones rely exclusively on out-of-band locally generated tones. A call from an IP Phone to an analog Gateway (or to an ISDN Gateway that terminates on an analog line) can rely exclusively on in-band tones. The state of the terminating side is not always known by the originating end through the H.323 protocol or SIP. Therefore, some scenarios require generating in-band tones from the terminating side.

Dial tone is always the responsibility of the originating side. The call is not setup with the far end as long as the digits are gathered for en-bloc transmission, or for overlap signaling until the provisioned minimum number of required digits is met on the Call Server. Other tones are provided by the originating side when the call cannot proceed to the far end.

For calls that terminate within a private network of CS 1000 systems, ringback tone is provided locally at the originating Call Server. This is based on the tone definition within that Call Server. Calls terminating on analog trunk gateways relay the tone generated from the PSTN through to the originator of the call.

Call modification scenarios, after a call has been answered, result in the provision of in-band tones. In this case, the generated tones are determined by the flexible tone configuration at that Call Server (that is, where the modification occurred).

In-band tones are generated by connecting a Tone circuit to a DSP channel so that the tone samples can be transported across the IP network within standard RTP streams.

For call center limitations on tone handling, see the “Limitations” on page 199.

End-to-end DTMF signaling

Dual Tone Multifrequency (DTMF) signaling represents the pressing of dialpad keys (0-9, *, #) on a telephone during a call. IP Peer Networking supports the sending and receiving of DTMF signaling during speech.

DTMF signaling can be received from the following:

- analog (500/2500-type) telephones
- digital telephones
- IP Phones
- Virtual Trunk (SIP/H.323 trunks)
- analog trunks
- PRI trunks

Standard SIP and H.323 protocols are used to transmit DTMF tones.

> ***Note:*** IP Peer Networking does not support long DTMF tones over Virtual Trunks. Long-digit duration is not supported.

Tone handling methods

DTMF tones must be transmitted using out-of-band signaling, because sources of delay and distortion caused by IP media streams can cause invalid tone detection when transmitted in-band.

- The out-of-band method uses H.245 channel signaling messages to represent the DTMF tones for H.323.
- The out-of-band method uses INFO methods to represent the DTMF tones for SIP.

Out-of-band signaling

Out-of-band DTMF tones are generally used for Virtual Trunks. The DTMF tones are sent as messages over the signaling channels. The messages are then converted to tones on the receiving side. This is a reliable way of sending DTMF tones over the Virtual Trunk.

SIP

End-to-end DTMF signaling is carried out-of-band by the SIP INFO message. The message does not include information about the duration of DTMF tones, and, as a result, long DTMF tones are not supported.

The INFO format is the same as MCS 5100 implementation. However, third-party gateways may use a different INFO format or even a different method to implement the out-of-band DTMF, which might lead to an interoperability issue. For more information, refer to RFC 2976 – The SIP INFO Method.

H.323

Out-of-band DTMF tones are transmitted using H.245 UserInputIndication messages. The content of each message represents the key that generated the tone. The message can represent the key value using a string indication, a signal indication, or both. If the signal indication is used, the message can also include a parameter to represent the tone method duration (that is, how long the key was pressed).

The endpoints negotiate which method is used. This negotiation occurs during H.323 call setup signaling.

On receipt of a UserInputIndication message, the receiving H.323 Signaling proxy signals the appropriate entity to generate the corresponding tone. This depends on whether the call involves a circuit-switched party or an IP party. DTMF Tone Detection is a configurable codec parameter.

> ***Note:*** In-band DTMF tones that originate from an analog (500/2500-type) telephone or incoming trunk are filtered out of the media stream by the DSP of the Voice Gateway Media Card. This is so that double detection of the DTMF digits does not occur. This causes additional delay in the speech path due to the buffering required to ensure that no DTMF tones get through the filter.

In-band signaling

In-band DTMF tones are sent as RTP packets over the RTP channels. This method of transporting DTMF tones is inherently unreliable as RTP packets can be lost over the network. However, this method is quite reliable if a G.711 codec is used for the transmission.

For CS 1000 systems, the in-band DTMF tones can be sent only from an analog (500/2500-type) telephone with tone detection turned off for the Voice Gateway Media Card.

IP Phone End-to-End Signaling (EES)

An IP Phone uses UNISTIM messages to signal digits. These messages are received by the telephone's Terminal Proxy Server (TPS), which translates the messages into SSD format for existing call processing.

IP Phones EES to H.323 trunks

On receipt of a message that represents a key press on an IP Phone, the Call Server relays it to the H.323 Signaling Proxy. The H.323 Proxy generates the appropriate H.245 UserInputIndication message.

Circuit-switched device DTMF and EES

Circuit-switched devices can transmit DTMF tone using the circuit-switched switching fabric or using SSD messages in the case of EES. When a circuit-switched device connects to a remote party over an H.323 trunk, the circuit-switched gateway (DSP) detects the DTMF tone and informs the Call Server. The Call Server signals the H.323 Signaling Proxy to generate an H.245 UserInputIndication message to represent the tone. When a digital telephone is operating the EES feature, the Call Server receives the input message and behaves as described below.

DTMF signaling for a circuit-switched trunk and analog (500/2500-type) telephones using H.323 trunks

During call setup, a Digitone Receiver (DTR) is connected to the circuit-switched trunk or analog (500/2500-type) telephone if DTMF is used for dialing. Digits detected for call setup are handled the same way as traditional call processing.

After a call has been established, circuit-switched trunks (for example, PRI trunks) or 2500 lines can carry DTMF tones in-band. When a circuit-switched trunk or analog (500/2500-type) telephone is connected to an H.323 trunk, tones are passed through the circuit-switched switching fabric to the circuit-switched gateway (DSP). The DSP detects the DTMF tone and informs the Call Server. The Call Server signals the H.323 Signaling Proxy to generate an H.245 UserInputIndication message to represent the tone.

DTMF out-of-band signals from H.323 trunk

For calls incoming from an H.323 trunk, DTMF signals are indicated using the H.245 UserInputIndication message.

Calls from H.323 trunks to circuit-switched trunks/analog (500/2500-type) telephones/digital telephones

On receipt of an H.245 UserInputIndication message, the H.323 Proxy signals the circuit-switched gateway (DSP) that supports the circuit-switched call. This is to generate the appropriate DTMF tone through the circuit-switched switching fabric to the terminating circuit-switched device.

> ***Note:*** Out-of-band DTMF signals received when a Virtual Trunk is connected to an IP Phone are ignored and not sent to the IP Phones.

Tandem H.323 trunks to H.323 trunks

On receipt of an H.245 UserInputIndication message on a given signaling proxy, the proxy transmits an appropriate UserInputIndication message on the connected outgoing H.323 signaling channel.

DTMF out-of-band signals from SIP trunk

For calls incoming from a SIP trunk, DTMF signals are indicated using the SIP INFO message.

Calls from SIP trunks to circuit-switched trunks/analog (500/2500-type) telephones/digital telephones

On receipt of a SIP INFO message on a given SIP Trunk Gateway, the SIP Trunk Gateway transmits an appropriate message to the Call Server. The Call

Server then relays the message to the other SIP Trunk Gateway, which then sends out a SIP INFO message.

This generates the appropriate DTMF tone through the circuit-switched switching fabric to the terminating circuit-switched device.

> ***Note:*** Out-of-band DTMF signals received when a Virtual Trunk is connected to an IP Phone are ignored and not sent to the IP Phones.

Tandem SIP trunks to SIP trunks

On receipt of a SIP INFO message on a given signaling SIP Trunk Gateway, the SIP Trunk Gateway transmits an appropriate SIP INFO message on the connected outgoing SIP signaling channel.

Fax calls

SIP

T.38 UDP fax is supported. The switchover procedure in T.38 ANNEX D (D.2.2.4) is used to establish a fax channel.

A SIP INVITE is made to the called party requesting a voice connection using the basic call setup flow. A voice connection is then established. Upon the detection of the fax tone (V.21) at the terminating end, the voice channel is replaced by a fax channel using the offer/answer SDP exchange.

H.323

IP Peer Networking supports the voice-to-fax switchover protocol for T.38 fax, by using the mode select signaling in H.323.

First, a voice call is established. When the DSP detects the fax tone, H.245 signaling is exchanged to request the far end node to change from voice mode to T.38 mode. The existing voice channels are closed and new channels for T.38 are opened. The fax call then proceeds.

The CS 1000 systems comply with H.323 version 3.0 with the H.323 version 4.0 extensions necessary for voice-to-fax switchover. This version standardizes the procedures in switching from voice mode to fax mode. Some third-party H.323 gateways can use different implementations of protocols to switch from voice to fax. Using a third-party gateway requires fax interoperability testing of the system. The end result can be that fax is not supported, due to the complexity of the H.323 protocol and other factors. Check with your Nortel sales representative for approved third-party gateways.

Nortel does not recommend using a modem on the CS 1000 network, due to the variety of modems available and the issues of packet loss and delay. For more information about fax and modem support and limitations, see *IP Trunk: Description, Installation, and Operation* (553-3001-363).

Reliability and redundancy

CS 1000 systems provide levels of redundancy to ensure that telephony services can withstand single hardware, software, and network failures. Table 10 on page 183 shows each reliability and redundancy feature and the systems that support the feature. The reliability and redundancy features include:

- "Alternate Call Server" on page 183
- "Signaling Server software redundancy" on page 186 (including H.323/SIP Trunk Gateway and IP Phone software)
- "H.323 Gateway software — trunk route redundancy" on page 187 (H.323 Gateway interface to Gatekeeper redundancy [Failsafe Gatekeeper])
- "SIP Trunk Gateway software — trunk route redundancy" on page 187
- "NRS redundancy" on page 188
- "Campus-distributed Media Gateway in survival mode" on page 193
- "CS 1000M Large System CPU redundancy" on page 195
- "Survivable IP Expansion" on page 197

Table 10 on page 183 shows the features and the systems that support the feature.

Table 10
Reliability and redundancy features by system type

Reliability and Redundancy Features		CS 1000M Small Systems		CS 1000M Large Systems	
	CS 1000S	CS 1000M Cabinet	CS 1000M Chassis	CS 1000M Single Group	CS 1000M Multi Group
Alternate Call Server	X	X	X		
Signaling Server software redundancy	X	X	X	X	X
NRS redundancy	X	X	X	X	X
SIP Trunk Gateway	X	X	X	X	X
H.323 Gateway	X	X	X	X	X
Campus distributed Media Gateway in survival mode	X	X	X		
CPU redundancy				X	X
Survivable IP Expansion (SIPE)	X	X	X		

Note: For CS 1000E redundancy, refer to *Communication Server 1000E: Planning and Engineering* (553-3041-120).

Note: For Geographic Redundancy, refer to *Communication Server 1000: System Redundancy* (553-3001-307).

Alternate Call Server

All Media Gateways have a full set of call-processing software components and maintain a configuration database that is periodically synchronized with the primary Call Server.

During normal operation, the processor in the Media Gateway handles low-level control of the interface cards in the gateway slots and communicates with the Call Server for feature operation. If the Media Gateway processor loses communication with the Call Server due to Call Server or IP network component failure (for example, cabling and L2 switch), one Media Gateway, configured as the Alternate Call Server, assumes Call Server responsibilities. The Signaling Server registers with that Alternate Call Server. Other Media Gateways can access only local Gateway hardware and local non-IP Phones, and are not under the control of the Alternate Call Server.

The Alternate Call Server IP address must be in the same ELAN subnet as the Primary Call Server IP address.

The Alternate Call Server is applicable only to the CS 1000S system and CS 1000M Small Systems.

As an example, Figure 62 shows the normal mode of operation for a CS 1000S system.

Figure 62
Example — Normal mode of operation for a CS 1000S system

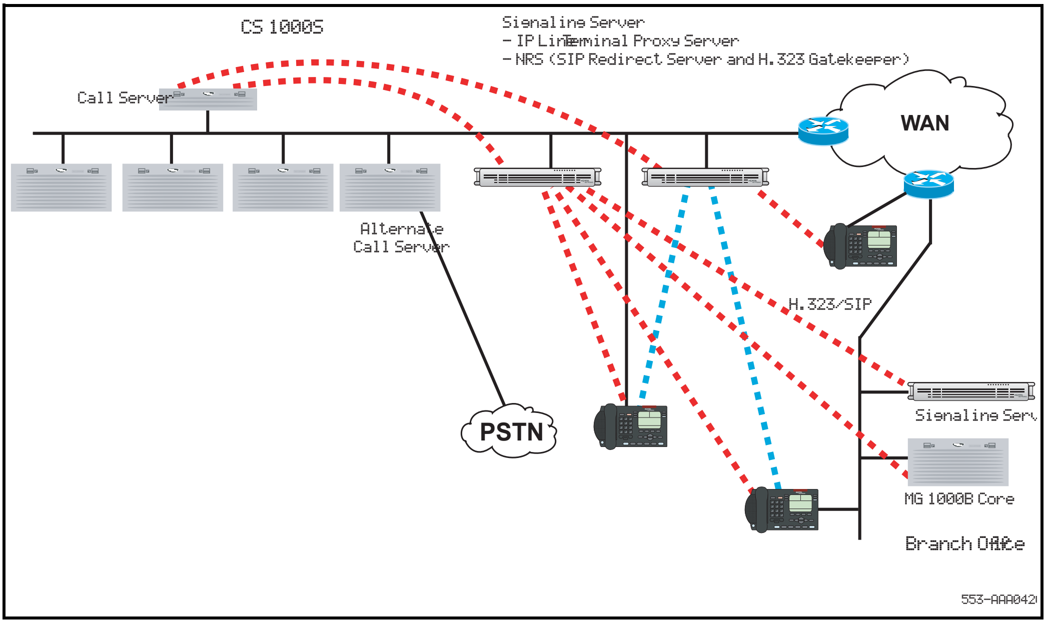


Figure 63 illustrates what occurs when the Call Server in a CS 1000S system fails:

1 The Call Server database periodically synchronizes at the Alternate Call Server.

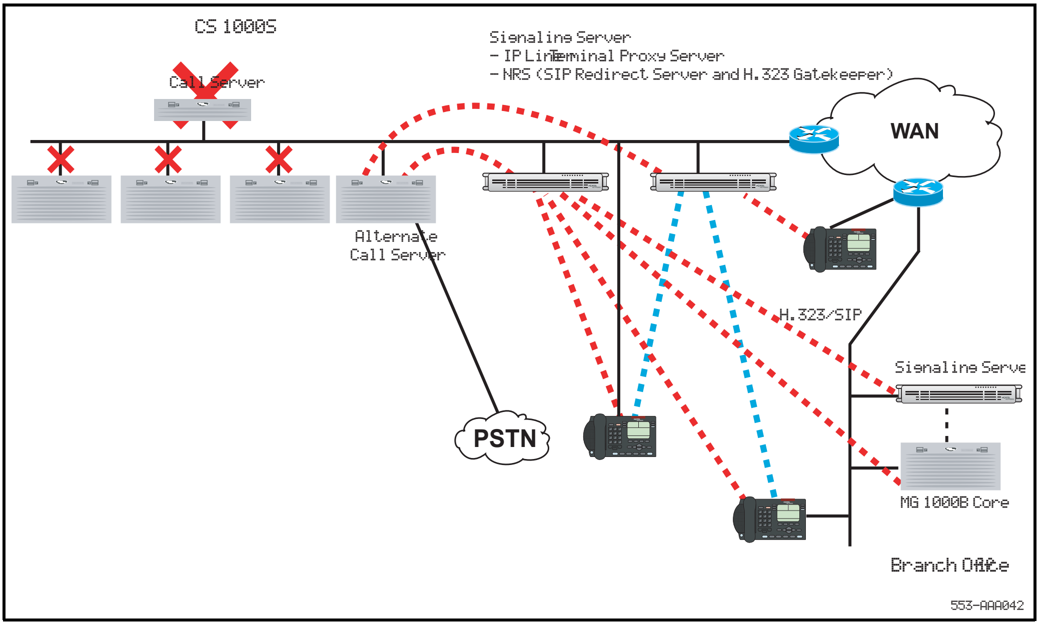
2 The Primary Call Server fails.

3 The Alternate Call Server assumes the role of Primary Call Server for IP Phones.

4 The Signaling Server registers at the Alternate Call Server.

5 Operation resumes with all Media Gateways, but the Signaling Server registers only with the Alternate Call Server.

Figure 63
Call Server failure and redundancy in a CS 1000S system



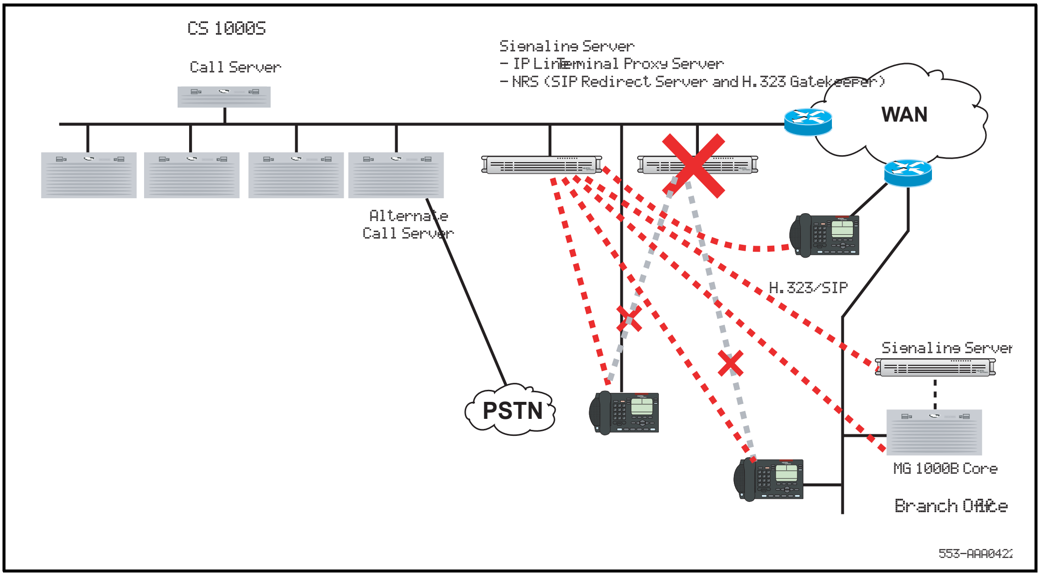
Signaling Server software redundancy

Signaling Server redundancy is provided on a load-sharing basis for the TPS. The Follower Signaling Server is the platform for the SIP/H.323 Gateway software if the Leader Signaling Server fails. The NRS (Primary, Alternate, or Failsafe) cannot reside on a Follower Signaling Server. It must reside on a Leader Signaling Server.

As an example, Figure 64 on page 187 shows Signaling Server redundancy in a CS 1000S system. In the example, the following occurs:

1. The IP Phones are distributed between the two Signaling Servers. The SIP/H.323 Gateway software runs on the Primary Signaling Server.
2. The Primary Signaling Server fails.
3. The Alternate Signaling Server assumes the Connection Server IP address, if necessary.
4. The IP Phones Time-to-Live time-out causes the IP Phones to reset and register to the Alternate Signaling Server. Active calls are dropped.
5. The Alternate Signaling Server assumes responsibility for the SIP/H.323 Gateway software.
6. Operation resumes.

Figure 64
Signaling Server redundancy in a CS 1000S system



H.323 Gateway software — trunk route redundancy

The H.323 Gateway software runs on the Node Master. The Signaling Server is normally configured as the Leader. If the Primary (Leader) Signaling Server fails, an Alternate (Follower) Signaling Server can take over the Node IP address. The Gateway software then runs on the Signaling Server with the Node IP address.

Existing calls are kept when the Primary Signaling Server fails. This situation applies to IP Phones that are not registered with the Primary Signaling Server, and for all circuit-switched telephones. IP Phones that are registered with the Primary Signaling Server restart after the Time-to-Live time-out, so active calls on those telephones are lost.

SIP Trunk Gateway software — trunk route redundancy

Each Call Server can have one or more SIP nodes; however, at any time each node has only one active gateway. A separate Signaling Server can be configured to run the SIP Trunk Gateway application as a backup (or alternate SIP Trunk Gateway). SIP Trunk Gateway redundancy is similar to the H.323 Gateway redundancy implementation. That is, the Leader and Follower Signaling Servers are configured in the same node. If the Leader Signaling Server fails, the Follower Signaling Server with the Alternate SIP Trunk Gateway becomes the master and takes over the node IP.

All active calls remain active during switchover; however, a near-end call is completely released using Scan and Signal Distributor (SSD) messages when the near-end party hangs up the call.

If the Leader (Primary) SIP Trunk Gateway comes back up during active calls, the following occurs:

- The busy channels stay busy in the Alternate SIP Trunk Gateway.
- The idle channels register with the Primary SIP Trunk Gateway.
- The near-end calls are released from the Alternate SIP Trunk Gateway when the near-end party hangs up. The SIP Virtual Trunk channels then register with the Primary SIP Trunk Gateway.

Each SIP Trunk Gateway occupies one Virtual Trunk route. To have SIP and H.323 Virtual Trunks co-residing on the same Signaling Server platform, the Virtual Trunks must be configured in separate routes, but must use the same IP D-channel ID.

NRS redundancy

The NRS provides address translation services for all endpoints in the network zone; therefore, redundancy is important. If an endpoint cannot reach an NRS over the network for address translation, calls cannot be placed. Nortel recommends that a backup or Alternate NRS be installed and configured on the network.

The CS 1000 networks have at least one NRS to provide network numbering plan management for private and public numbers. An optionally redundant NRS can be installed in the network. The Alternate NRS periodically synchronizes its database with the Primary NRS.

Primary, Alternate, and Failsafe NRS databases are supported. The H.323 or SIP Trunk Gateway software attempts to recover system functionality if a failure occurs at the NRS. The two types of NRS redundancy are:

- Alternate NRS
- Failsafe NRS

The Alternate NRS is optional but recommended for all networks. The Failsafe NRS is also optional but is recommended for selected critical IP Peer H.323 and SIP Trunk Gateways.

Only one of the servers in the pair is active at one time — the other is on standby. A heartbeat mechanism between servers is implemented. When a failure of the heartbeat from the active server is detected, the standby server takes over. Another mechanism ensures that both servers have up-to-date configuration.

For NRS/H.323 Gatekeeper redundancy, see below.

For NRS/SIP Redirect Server redundancy, see page 192.

NRS H.323 Gatekeeper redundancy

Alternate H.323 Gatekeeper

The H.323 Gateway software runs on the Signaling Server and communicates with both a Primary and Alternate (optional) H.323 Gatekeeper. If the Gateway software loses communication with its Primary H.323 Gatekeeper, it automatically registers at the Alternate H.323 Gatekeeper to resume operation.

To enable the Alternate H.323 Gatekeeper to provide H.323 Gatekeeper redundancy, the CS 1000 systems can accept a prioritized list of Alternate NRSs in the Gatekeeper Confirmation (GCF) and Registration Confirmation (RCF) messages returning from the Primary Gatekeeper at the Gatekeeper Discovery and Gatekeeper Registration times respectively.

Note: The list of Alternate Gatekeepers in the registration confirmation message takes precedence over the list in the Gatekeeper confirmation message. At any time, if the system detects that it is not registered, or if the Gatekeeper does not respond (for example, because it receives an Unregister Request (URQ) message or because the Time-to-Live messages are not answered), it reattempts registration to its Primary Gatekeeper (the address that was returned by the GCF). The value of the Time-to-Live timer is determined by the Gatekeeper in the RCF, and obeyed by the endpoint. If the timer fails, the system sequentially attempts to register with the Alternate Gatekeepers until registration succeeds.

Polling and switchover

A Time-to-Live timer is provided to ensure that if a Gatekeeper stops responding for a specified amount of time, the H.323 Gateway software registers at the Alternate Gatekeeper to resume operation. This ensures Gatekeeper redundancy across the network. For more information about endpoint registration and Time-to-Live, refer to “Time-to-Live” on page 235.

The Alternate Gatekeeper is inactive and in standby mode by default. It constantly polls the Primary Gatekeeper by sending Information Response Request (IRR) messages to the Primary Gatekeeper. The default for the poll interval is configured to approximately 30 seconds and can be configured through NRS Manager (see “Configuring system-wide settings” on page 402). The endpointType.gatekeeper field of the IRR message is configured to indicate that the IRR is coming from a Gatekeeper and not an endpoint. If the Primary Gatekeeper is currently in-service and accepting registrations, then it returns an Information Request Negative Acknowledgement (INAK) message with nakReason set to notRegistered.

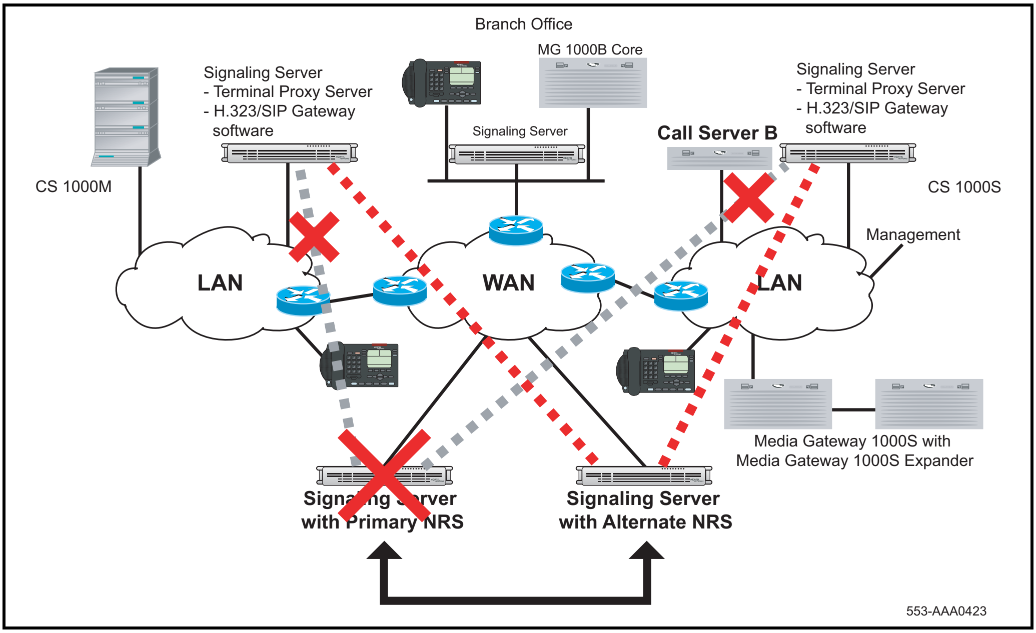
Figure 65 on page 191 shows the handling of the Gateway interface and the Alternate Gatekeeper in the event of Primary Gatekeeper failure:

1. The Alternate Gatekeeper periodically synchronizes with the Primary Gatekeeper.
2. The Primary Gatekeeper fails.
3. The Alternate Gatekeeper assumes the role of the Primary Gatekeeper and generates a Simple Network Management Protocol (SNMP) alarm.

4 The Gateways time out and register at the Alternate Gatekeeper.

5 The network calls resume.

Figure 65
Primary NRS failure and redundancy



In addition to Gatekeeper redundancy, the H.323 Gateway interfaces can withstand communication loss to both Gatekeepers by reverting to a locally cached copy of the Gateway addressing information. Since this cache is static until one of the Gatekeepers becomes accessible, it is intended only for a brief network outage.

Failsafe H.323 Gatekeeper

For additional redundancy, provide a Failsafe Gatekeeper at each endpoint in the network.

When configuring the Gatekeeper, the administrator must configure whether the Gatekeeper is the Primary Gatekeeper (GKP) or the Alternate Gatekeeper (GKA). If the Gatekeeper is the Primary Gatekeeper, the administrator can statically configure the IP address of the GKA (if an Alternate Gatekeeper is used on the network). If the H.323 Proxy Server application on the Signaling Server cannot contact the Primary or Alternate Gatekeepers, it can fall back on its local Failsafe Gatekeeper. Failsafe Gatekeepers are used only by local Signaling Server components. Failsafe Gatekeepers reject all Registration, Admission, and Status signaling (RAS) messages received over the network from remote entities. The Failsafe Gatekeeper provides a Security Denied messages.

The Primary Gatekeeper returns the IP address of the Alternate Gatekeeper (if an Alternate Gatekeeper is configured) in the alternateGatekeeper field of GCF and RCF messages. The Alternate Gatekeeper returns the IP address of the Primary Gatekeeper in the alternateGatekeeper field of GCF and RCF messages.

> ***Note:*** If the endpoints are configured with the IP addresses of Primary and Alternate Signaling Servers, the IP addresses, which are returned in the GCF and RCF messages, take precedence over configured IP addresses.

NRS SIP Redirect Server redundancy

Alternate SIP Redirect Server

Normally only the Primary SIP Redirect Server is the active SIP Redirect Server. The Primary SIP Redirect Server has the master database while the Alternate SIP Redirect Server and Failsafe SIP Redirect Server have a replica of the database.

If the master database is changed, the Primary SIP Redirect Server creates a publication for the replica. The replica database automatically synchronizes the database from the master.

> ***Note:*** A user can also force a manual database synchronization.

The database synchronization success and failure messages are logged in the RPT report log.

Polling and switchover

A polling message is sent out between Primary and Alternate SIP Redirect Servers and between Primary and Failsafe SIP Redirect Servers.

If the Alternate SIP Redirect Server determines that the Primary SIP Redirect Server is unreachable, it automatically switches to become the active SIP Redirect Server and its database becomes the master database. At the same time, the Failsafe SIP Redirect Server also determines that Primary is no longer available and it automatically switches to contact the Alternate SIP Redirect Server. The replica database on the Failsafe synchronizes with the master database on the Alternate SIP Redirect Server, if required.

Once the Primary SIP Redirect Server become inactive, no configuration changes are allowed. Only maintenance operations can be performed.

Switch-over messages are logged in the RPT report log.

Failsafe SIP Redirect Server

If the Failsafe SIP Redirect Server loses its connection with both the Primary and Alternate SIP Redirect Servers, then it becomes the active SIP Redirect Server.

Campus-distributed Media Gateway in survival mode

In addition to having an Alternate Call Server, you can have Survivable Media Gateways (each of the Media Gateways can be survivable).

The Media Gateway survival modes applies to the following systems:

- CS 1000S System
- CS 1000M Small System

Media Gateways can be configured as survivable when distributed throughout a campus environment. In this case, basic telephony services are provided in the event of a network outage. Figure 66 on page 194 illustrates how such an outage is handled.

The following list indicates the steps to a call in the survival mode scenario:

1 The Call Server database periodically synchronizes at the campus-distributed Media Gateway.

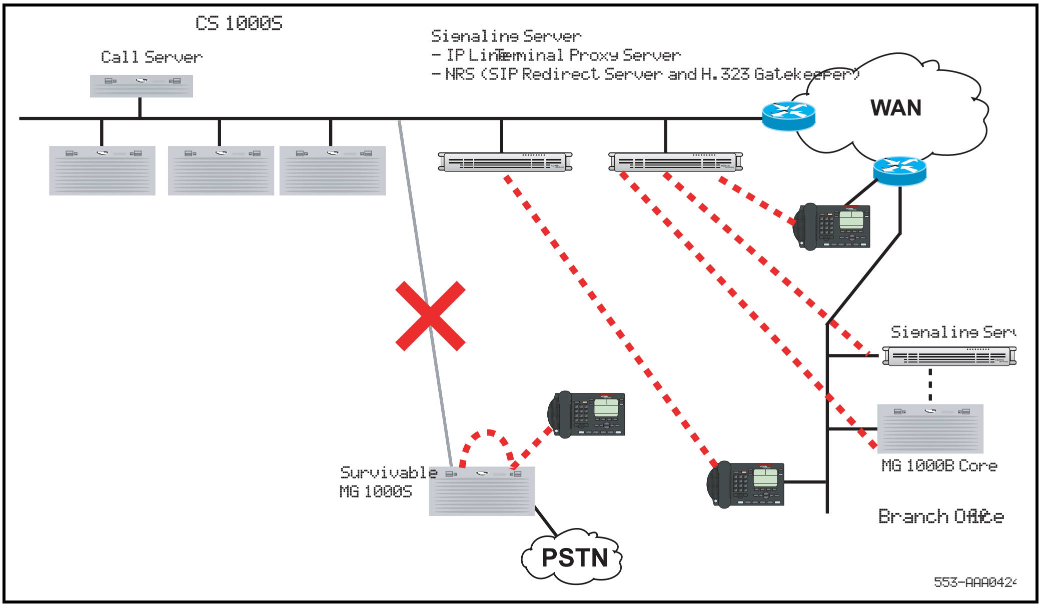
2 The Primary Call Server fails.

3 The campus-distributed Media Gateway assumes the role of the Primary Call Server for IP Phones.

4 The Signaling Server registers at the campus-distributed Media Gateway.

5 Operation resumes with the single Media Gateway.

Figure 66
Network failure with Survivable Media Gateways



Note: To facilitate the survival mode operation below, the IP address configured in the IP Phones (for example, through DHCP) must be the Node IP address of the Voice Gateway Media Cards in the Survivable Media Gateway.

CS 1000M Large System CPU redundancy

The CS 1000M Large Systems have dual hot standby CPU redundancy to handle failure of the Call Server. IP Peer Networking supports the following Large System redundancy features:

- Health Monitoring
- Virtual Trunk redundancy
- Graceful switch-over
- Ungraceful switch-over

Health Monitoring

The health of the dual CPUs are monitored such that the active CPU switches over to the standby CPU when the standby CPU is healthier than the active CPU. The health of a CPU is calculated based on the conditions of various system components. For IP Peer Networking, the Signaling Server is one of the monitored components. If a CPU switch-over occurs, the Signaling Server registers with the new CPU.

The Signal Server uses the IP Line scheme for health monitoring. This scheme has a minimum threshold of two (that is, at least two IP Line connections) must exist before the health count is initiated. As a result, two Signaling Servers are required for health monitoring to work.

Table 11 shows the health count scheme.

Table 11
Health count

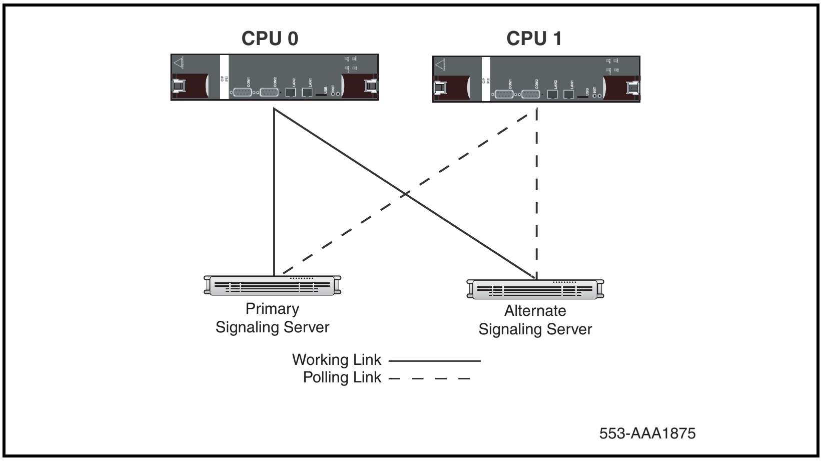
Number of cards	Health count
2 or 3 cards	1 health count
4 or 5 cards	2 health counts
6 or 7 cards	3 health counts
8 or 9 cards	4 health counts
...	...

Under normal operation, the following occurs:

- The primary Signaling Server works with the active CPU (CPU 0) over a working link and also keeps contact with the standby CPU (CPU 1) over a polling link.
- The alternate Signaling Server keeps contact with the active CPU (CPU 0) over a working link and the standby CPU (CPU 1) over a polling link.

Figure 67 illustrates health monitoring under normal operation.

Figure 67
Health Monitoring



When all the links are up and running there is no CPU switch-over. However, if the ELAN network interface in the active CPU (CPU 0) stops working, both Signaling Servers cannot communicate with the active CPU, and the health count on the active CPU is decreased. The health count of the standby CPU remains the same because both Signaling Servers can communicate with it.

Therefore, the standby CPU is healthier. A CPU switch-over takes place, and the standby CPU becomes the active CPU. The primary Signaling Server registers with the new active CPU.

Virtual Trunk redundancy

If the ELAN network interface on the Primary Signaling Server fails or the server itself fails, no CPU switch-over occurs, because both the active and the standby CPU lose contact with the Primary Signaling Server. As a result, they have the same health count.

The Virtual Trunk Redundancy mechanism is initiated. If a Virtual Trunk is unavailable, the call-processing software selects an alternate route. The alternate Signaling Server becomes the master and registers to the active CPU to resume the Virtual Trunk operation. The transient calls are dropped, while the established calls remain. The alternate Signaling Server becomes active in approximately 30 seconds, but calls cannot be initiated during that time.

Graceful switch-over

During a graceful switch-over, both established calls and transient calls survive the CPU switch-over. When the connection between the Signaling Servers and the active CPU goes down, a graceful switch-over occurs so that the Signaling Servers can register to the standby CPU that has become active. There is no impact to the calls; however, the report log file shows that graceful switch-over has taken place.

Ungraceful switch-over

During an ungraceful switch-over, the standby CPU sysloads and then everything returns to a normal state. For IP Peer Networking, the Signaling Server registers to the standby CPU. The report log file shows that ungraceful switch-over has taken place.

Survivable IP Expansion

Survivable IP Expansion (SIPE) cabinets are available for the CS 1000M Small Systems:

- CS 1000M Cabinet
- CS 1000M Chassis

CS 1000M Small Systems can be configured to be survivable in the event of a link failure or a failure of the Main cabinet. Based on the system configuration, if IP connectivity to the Main is lost or a manual command is issued, an IP Expansion cabinet can enter survival mode in which it acts as a fully functional stand-alone system. Each CS 1000M Small System has the capability to make and take calls independent of the state of the Main cabinet. This provides each cabinet with the ability to operate as a stand-alone unit when required.

A Survivable IP Expansion cabinet is able to restart after it loses communication with the Main cabinet due to an outage of the Main cabinet or a failure of the link between the cabinets. During the restart procedure, the Survivable IP Expansion cabinet attempts to register with the Main cabinet. If a connection cannot be made with the Main cabinet within approximately two minutes, the IP Expansion cabinet switches to survival mode and acts as a stand-alone system.

Least Cost Routing

IP Peer Networking supports the traditional methods of managing costs in a circuit-switched environment (for example, through BARS/NARS). See *Basic Network Features* (553-3001-379).

IP Peer Networking also supports a method to manage costs at the NRS. This is done in an IP environment using Least Cost Routing. With Least Cost Routing, you can assign a cost factor to the routes using NRS Manager. You can also use Least Cost Routing to identify the preferred SIP/H.323 Gateways for specific numbering plan entries. See "Adding a Routing Entry" on page 432.

Licenses

For each Virtual Trunk configuration, you must purchase a License. The number of trunks must match those that are enabled with the installation keycode.

The following packages are available for IP Peer Networking:

- H.323 Virtual Trunk (H323_VTRK) package 399
- SIP Gateway and Converged Desktop Package (SIP) package 406

The following Licenses are available for IP Peer Networking:

- SIP Access Port License
- H.323 Access Port License

For more information, refer to the following NTPs.

- *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210)
- *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)
- *Communication Server 1000S: Installation and Configuration* (553-3031-210)
- *Communication Server 1000E: Installation and Configuration* (553-3041-210)

Limitations

The NRS (Primary, Alternate, or Failsafe) cannot reside on an Alternate Signaling Server. It must reside on a Primary (Leader) Signaling Server.

Circuit capacity can provide a maximum of 60 simultaneous channels for tone generation and handling. Some queuing is provided when a channel becomes available. In order to alleviate the number of tone channels required for call center applications, Music trunks in broadcast mode are recommended.

The Radius protocol that is supported on IP Trunk software is not provided for IP Peer Networking.

The use of G.723 codec can limit the number of DSP channels available on the 32-port Media Card to 24. For ITG-P Line cards, all 24 ports can be used. The use of codec G.729A/AB and G.723 impacts the voice quality, including music provided to the user.

H.323 and SIP do not support NAT. If address translation is required, it needs H.323-aware or SIP-aware NAT or VPN facilities. IP Phones (which use the proprietary UNIStim protocol) have a limited implementation of NAT.

While the CS 1000 systems supports MCDN, the systems do not support H.450 supplementary services, which is the industry-standard form of signaling used by H.323, which is equivalent to the feature transport aspect of MCDN.

Network Routing Service overview

Contents

This section contains information on the following topics:

Description

The Network Routing Service (NRS) is a web-based application that runs on the Signaling Server.

The NRS is the Enterprise Business Network (EBN) solution for providing routing services to both H.323- and SIP-compliant devices. The NRS allows customers to manage a single network dialing plan for SIP, H.323, and mixed H.323/SIP networks.

The NRS allows for the configuration of multiple customers.

The NRS is a database of gateway and terminal (SIP Phone) endpoints, and routes to these endpoints. The NRS also includes three interface methods: SIP Redirect Server, H.323 Gatekeeper, and Network Connection Service (NCS).

The advantages of the NRS database are:

- simplicity of administration
- troubleshooting
- capacity enhancements
- synchronization
- authentication
- maintenance
- new web interface (NRS Manager)

The user can configure the H.323 Gatekeeper application for routing services for H.323 endpoints and the SIP Redirect Server for SIP routing services for SIP endpoints. The NCS is used for the Branch Office (including the SRG), Virtual Office, and Geographic Redundancy features.

The H.323 Gatekeeper and the SIP Redirect Server can coexist on the same Signaling Server.

The NRS can support 5000 endpoints. The endpoints can include Gateway Endpoints (SIP and H.323) and SIP Phone User Endpoints. The NRS also supports 20 000 routing entries.

Examples of H.323- and/or SIP-compatible endpoints needing the services of the NRS are CS 1000E System and IP Trunk 3.0 (or later) endpoints. The NRS also supports endpoints that do not support H.323 Registration, Admission, and Status (RAS) or SIP registration with the NRS, such as ITG Trunk 1.0 and 2.x.

> ***Note:*** Systems that do not support H.323 RAS procedures and H.323 Gatekeeper procedures are referred to as non-RAS endpoints or static endpoints.

When you define the physical network and you are configuring the gateways, you must define whether the gateway is a SIP Trunk Gateway or an H.323 Gateway. Calls are directed differently depending on the protocol.

The NRS is designed to operate with both phone-context and NPI/TON qualified numbers. As a result, basic calls and services are provided to SIP Trunk Gateways and SIP Phones (if the SIP Phones register by name/number and dial by a number).

The purposes of the NRS are as follows:

- It populates the location and registration database.
- It adds the appearance of the proxy in the customer network.
- It facilitates a translation database for telephone numbers contained within the SIP Uniform Resource Identifier (URI) in order to present a well-formed, syntactically-correct telephone number to the location service within the proxy.

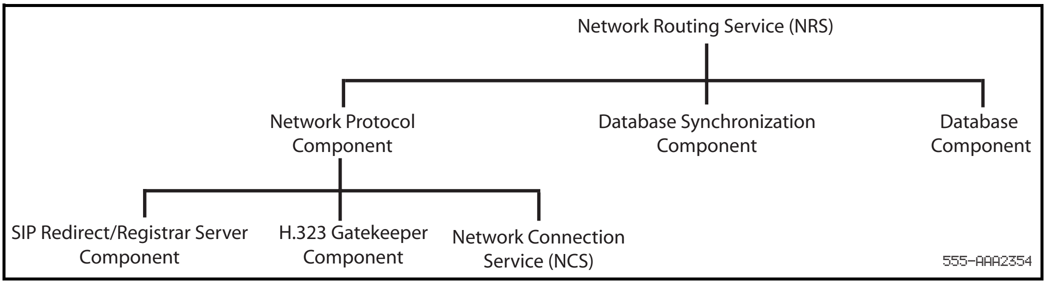
> ***Note:*** The location service is used by the SIP Redirect Server to locate the SIP Trunk Gateway that serves the target of the request. A SIP Trunk Gateway has a number of non-SIP lines and trunks behind it which do not have their own identity in the SIP domain. These non-SIP endpoints are accessed by mapping SIP URIs based on telephony DNs to one or more SIP Trunk Gateways. The location service is effectively a matching mechanism that allows a fully-qualified telephone number to be associated with a range of telephone numbers and the SIP Trunk Gateway that provides access to that DN range.

The NRS is comprised of the following three components:

- network protocol component
- database synchronization component
- database component

Figure 68 shows a graphical view of the NRS.

Figure 68
NRS components


Network Routing Service (NRS)
Network Protocol Component
Database Synchronization Component
Database Component
SIP Redirect/Registrar Server Component
H.323 Gatekeeper Component
Network Connection Service (NCS)
555-AAA2354

Network protocol component

The NRS combines the following components into a single application for network-based routing:

- SIP Redirect Server – Provides central dialing plan management/routing for SIP-based solutions. The SIP Redirect Server is an NRS software component (see page 205).
- SIP Registrar – Accepts SIP REGISTER requests from users (see page 205).
- H.323 Gatekeeper – Provides central dialing plan management/routing for H.323-based solutions. The H.323 Gatekeeper is an NRS software component (see page 207).
- Network Connection Service (NCS) – The NCS is required for the IP Line Virtual Office, Branch Office (including the SRG), and Geographic Redundancy features (see page 208). The NCS allows the Line TPS (LTPS) to query the NRS using the UNIStim protocol.

SIP Redirect Server

The SIP Redirect Server facilitates centralized dialing plan management and the configuration of network routing information for the SIP domain.

A SIP Redirect Server translates telephone numbers recognized by Enterprise Business Network (EBN) voice systems to IP addresses in the SIP domain. Therefore, the SIP Redirect Server interfaces with SIP-based products.

The SIP Redirect Server resides on the Signaling Server. The SIP Redirect Server is used to interconnect with other Nortel Communication Servers using SIP.

Along with the H.323 Gatekeeper application, the SIP Redirect Server has access to the endpoint/location database. The server has three functions:

- acts as a redirect server for SIP-initiated sessions
- acts as a location service for SIP-initiated sessions
- acts as a registrar for a SIP node within a trusted domain

The SIP Redirect Server has the ability to access the CS 1000 system's location database in order to direct SIP gateways within the networked environment.

SIP Registrar

A SIP Registrar is a server that accepts REGISTER requests and places the information it receives in those requests into a location service for the domain it handles. The registration process precedes call setup. The SIP Registrar accepts registration requests from SIP Phones, SIP Trunk Gateways, and other certified compatible third-party SIP endpoints.

The SIP registrar does the following:

- removes the need to statically configure an endpoint's IP address
- allows the NRS to be aware of or detect the presence of an endpoint in the network, as the endpoint must register and reregister with the NRS

A SIP Phone registers against a provisioned RAS endpoint. The endpoint name is the username of a registered subscriber and is used to authenticate the telephone at registration. An endpoint route entry contains an assigned telephone number at which the SIP Phone can be reached. An IP address of the SIP endpoint is learned from the Contact header of a REGISTER message.

The SIP Registrar is co-resident with the SIP Redirect Server on the Signaling Server. Co-resident SIP Registrar and SIP Redirect Servers accept only the following SIP messages/requests:

- REGISTER (for registering contact information)
- INVITE, ACK, and CANCEL (for setting up sessions)
- BYE (for terminating sessions)
- OPTIONS (for terminating services for their capabilities)
- NOTIFY
- REFER (for MWI, Transfer, and Conference)

All other requests (such as INFO, SUBSCRIBE, and PRACK) return the 501 “Not Implemented” response. Registration is used for routing incoming SIP requests. Registration has no role in authorizing outgoing requests.

Authorization and authentication

A SIP Registrar requires a registering User Agent to be authorized and authenticated.

Authentication is handled in SIP on a request-by-request basis using a challenge-response authentication mechanism. The SIP Registrar provides this challenge-response authentication mechanism. The mechanism is used by:

- the SIP Registrar (server) to challenge a client request
- the client to provide authentication information

Authorized users are authenticated using the challenge-response mechanism. When the server receives a request, it can challenge the initiator of the request to provide assurance of its identity. This process is called authentication.

Users must prove they are who they claim to be. Authentication is password-based. Both the client and server must know the username and the password. Password validation ensures that the User Agent knows the password.

The SIP Registrar/Redirect Server authenticates the originator of a SIP request. If the request does not contain credentials or the credentials fail to authenticate the originator, then the SIP Registrar/Redirect Server returns a 401 (Unauthorized) response for REGISTER request and a 407 (Proxy Authentication Required) response for other requests containing a challenge. Once the originator has been identified or authenticated, the server can determine if the user is authorized to make the request in question. Authorization grants the user permission to perform the requested action.

The SIP Registrar assesses the identity of the User Agent domain by checking a URL in the REGISTER message. The SIP Registrar assesses the identity of a request sender by checking the username in the REGISTER message.

Authentication is configured using NRS Manager. Authentication can be configured at two levels in the NRS: at the Level 1 Domain and at gateway endpoints. For more authentication information, see “SIP authentication” on page 214. For more configuration information, see “Configuring and managing the Network Routing Service” on page 379.

H.323 Gatekeeper

The H.323 Gatekeeper Network Protocol Module (NPM) interfaces with the H.323 stack and is responsible for sending and receiving all H.323 RAS messaging. When a RAS request message arrives over the network, the H.323 stack informs the H.323 Gatekeeper NPM of the incoming request. The H.323 Gatekeeper NPM uses H.323 Application Programming Interfaces (APIs) to retrieve the relevant data. For example, if the incoming request is an ARQ, the H.323 Gatekeeper NPM extracts the originator’s endpointIdentifier and the desired terminator’s destinationInfo fields from the ARQ message. After all relevant information is extracted from the incoming RAS request, the H.323 Gatekeeper NPM passes the request to the Database Module (DBM) for resolution. The DBM consults its numbering plan configuration and informs the H.323 Gatekeeper NPM of the result. The H.323 Gatekeeper NPM then sends the relevant RAS response to the RAS request originator.

Network Connection Service

The Network Connection Service (NCS) is used with the IP Line Virtual Office, Branch Office (including the SRG), and Geographic Redundancy features. The NCS allows the Line TPS (LTPS) to query the NRS using the UNIStim protocol.

There are four areas in CS 1000 Element Manager and in NRS Manager for configuring the NCS:

- In Element Manager, the H.323 Gateway Settings contains the NCS configuration. See **IP Telephony > Node: Servers, Media Cards > Configuration > Edit > Signaling Servers > Signaling Server Properties > H323 GW Settings** (see Procedure 18 on page 367).
- In NRS Manager, NCS is configured in the following areas:
  - For configuration of the NRS server to support the NCS, see **Home > NRS Server Settings > NCS Settings** (see "Configuring NRS Server Settings" on page 405).
  - Configuration of Virtual Office and branch office (including the SRG) user redirection to the main office, see **Configuration > Gateway Endpoints** (see "Adding a Gateway Endpoint" on page 424).
  - Configuration of the Virtual Office Login, see **Configuration > Collaborative Servers** (see "Viewing the Collaborative Servers" on page 447).

Database component

The database component of the NRS is responsible for the following:

- configuring the numbering plan
- reading and updating the active and standby databases on disk
- resolving all registrations and requests which the NRS passes to the database

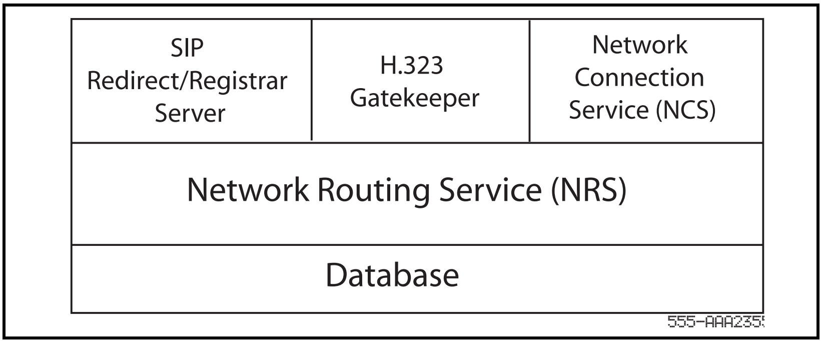
The NRS numbering plan configuration is stored in XML format in two databases on disk. The active database is used for call processing and the standby database is used for configuration changes.

The database component interfaces with the active and standby databases on disk. All call processing requests that the NRS passes to the database are resolved using the active database. The database uses the information that the NRS extracted from the request to search its database. For example, in the case of an H.323 ARQ message, the database attempts to find a registered endpoint that can terminate the call.

The NRS Manager web server interfaces with the database for viewing, adding, deleting, or modifying numbering plan configuration data. All changes to the numbering plan database are carried out on the standby database. Changes that the administrator makes to the numbering plan database do not affect call processing immediately. The database must first be cut over to the main active database.

The NRS database provides a central database of addresses that are required to route calls across the network. The NRS database resides on the Signaling Server with the other NRS applications (see Figure 69).

Figure 69
NRS database and network protocol components


SIP Redirect/Registrar Server
H.323 Gatekeeper
Network Connection Service (NCS)
Network Routing Service (NRS)
Database
555-AAA235

Both the SIP Redirect Server and H.323 Gatekeeper have access to the endpoint/location database.

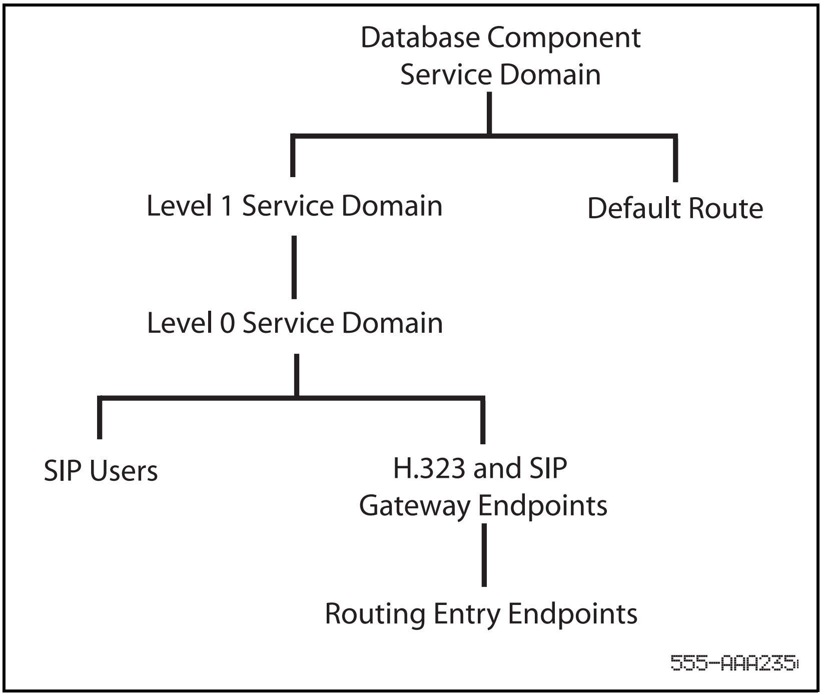
- The SIP Redirect Server accesses the location database on CS 1000 systems to direct SIP Trunk Gateways within a networked environment.
- The H.323 Gatekeeper also accesses the central location database, but to direct H.323 Gateways.

Both the SIP Redirect Server and the H.323 Gatekeeper provide the address-resolution functionality.

The routing data is the same for SIP and H.323. As a result, both the SIP Redirect Server and H.323 Gatekeeper provide address resolution for the CS 1000 Call Server.

Figure 70 shows a hierarchical view of the database. The data is stored and organized in the database as described in “Hierarchical model of the Network Routing Service” on page 211. The data is used by both the SIP Redirect Server and the H.323 Gatekeeper.

Figure 70
Hierarchy of the NRS database components



Hierarchical model of the Network Routing Service

The NRS can support multiple customers and can provide routing services to several service provider networks. To do this, the NRS server uses a hierarchical model as outlined in Table 12. This model outlines how information is stored and organized in the database. The data stored in the database is common to both H.323 and SIP.

Table 12
Hierarchical model of the Network Routing Service (Part 1 of 2)

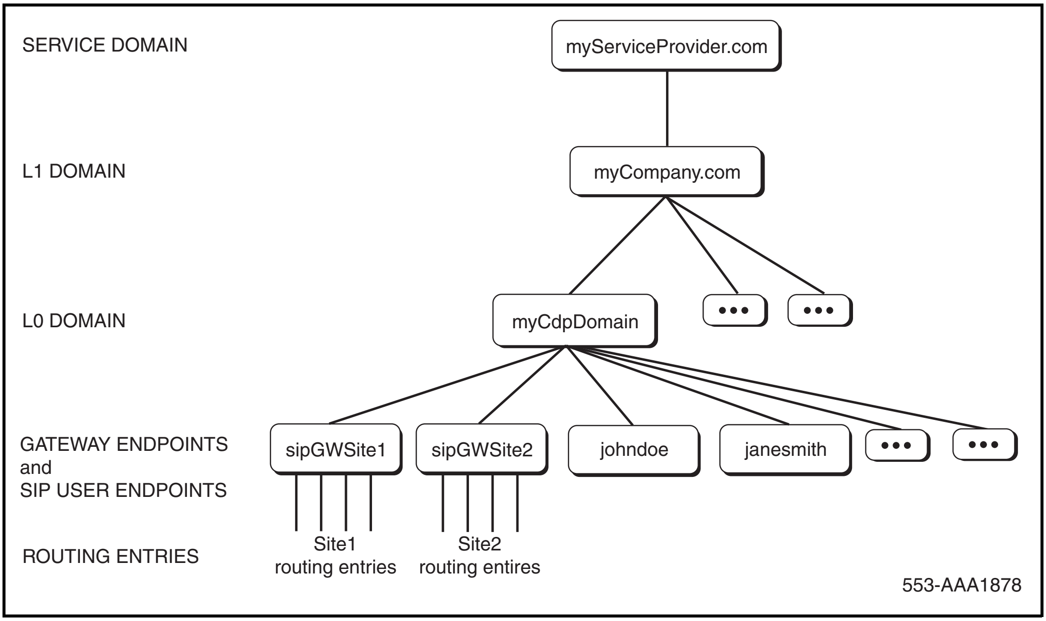
Level	Description
Service Domain	Represents a service provider network. A service domain maps into a SIP-domain. Example: myServiceProvider.com
Level 1 Regional Domain	Represents a subdomain in a Service Domain. ***Note 1:*** The Level 1 Regional Domain is also referred to as the L1-domain (in the context of the Network Routing Service). An L1-domain maps into an enterprise/customer network as well as a Meridian Uniform Dialing Plan (UDP) domain. The L1-domain should match across the UDP domain including E.164. Example: myCompany.com ***Note 2:*** UDP means all the call types in the dialing plan which include private (special numbers) and public (national, international, subscriber, and special numbers).
Level 0 Regional Domain	Represents a subdomain in a Level 1 Regional Domain. ***Note 1:*** The Level 0 Regional Domain is also referred to as the L0-domain (in the context of the Network Routing Service). An L0-domain maps to a site level as well as a Meridian Coordinated Dialing Plan (CDP) domain. The L0-domain should match across the CDP domain. Example: myCdpDomain ***Note 2:*** A site can be a street address, a campus, or a metropolitan area.

Table 12
Hierarchical model of the Network Routing Service (Part 2 of 2)

Level	Description
Gateway Endpoint	Represents a gateway. It exists within an L0 Domain. A site can have many endpoints. Example: sipGWSite1, sipGWSite2
User Endpoints	Represents a SIP Phone. It exists with the L0 domain. A site can have many SIP Phones. Example: johndoe, janesmith
Routing Entry	Represents a range of addresses (URIs) where a gateway can terminate calls. A routing entry exists within a gateway. These are the routing entries that the gateway supports.

Figure 71 on page 213 shows the hierarchical structure of the Network Routing Service.

Figure 71
Hierarchical structure of the Network Routing Service



> ***Note:*** If there is no Service Domain, the Service Domain must be configured the same as the Level 1 Regional Domain.

For example:

- Bell Canada is the Service Provider.
- Nortel is the Level 1 Domain.
- Sites within Canada can make up the Level 0 Domains (such as Belleville or Ottawa).
- Switches at the sites are the Gateway Endpoints.

SIP authentication

The data that the SIP Registrar/Redirect Server needs to successfully perform authentication is configured on the SIP Registrar/Redirect Server in two ways:

- Group identity
  - against an enterprise network (that is, the Level 1 Regional domain)
  - against a site in the enterprise network (that is, the Level 0 Regional (CDP) Domain)
- Individual endpoint identity
  - against a Gateway Endpoint
  - against a SIP User Endpoint

If a gateway endpoint does not have individual identity configured, then the L0 Domain group identity data is used by the SIP Registrar/Redirect/Proxy Server during the authentication procedure.

If neither the individual endpoint identity nor the L0 identity is provided, then L1 Domain identity is used.

Configuring authentication in the NRS

Authentication is configured using NRS Manager. Authentication can be configured at the following levels in the NRS:

Level 1 Domain and Level 0 Domain

Authentication can be turned on or off at this level. If authentication is turned on, then all Gateway Endpoints and SIP User Endpoints require authentication.

Gateway Endpoints and SIP User Endpoints

Authentication can also be turned on or off at the Gateway Endpoint and SIP User Endpoint levels. This level provides three authentication options:

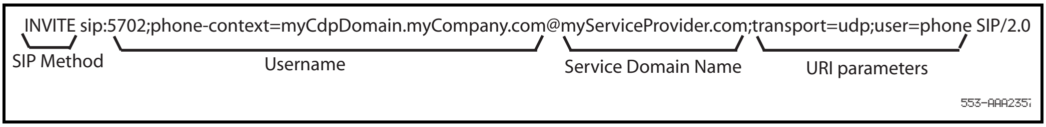
- Not configured — If this option is selected, then the endpoint uses the Level 1 or Level 0 Domain authentication (if Level 1 authentication is enabled).

- Authentication off — If authentication is turned off, then authentication is off for this endpoint even if Level 1 or Level 0 Domain authentication is enabled. This endpoint authentication setting overrides the Level 1 and Level 0 Domain authentication setting.
- Authentication on — If authentication is turned on, then authentication is on for this endpoint and the authentication overrides the Level 1 and Level 0 Domain authentication (if it is enabled). This endpoint authentication setting overrides the Level 1 and Level 0 Domain authentication setting.

SIP Uniform Resource Identifiers

The NRS supports SIP URIs (see Figure 72). A SIP URI is a user's SIP identity.

Figure 72
SIP URI example



```
INVITE sip:5702;phone-context=myCdpDomain.myCompany.com@myServiceProvider.com;transport=udp;user=phone SIP/2.0
```

Where:

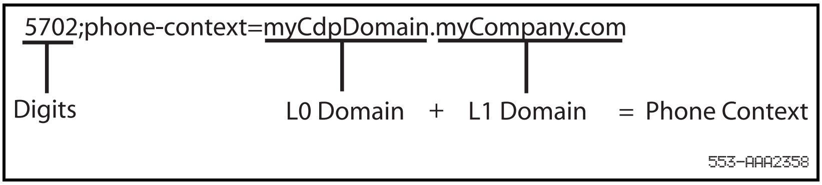
- **Username**: Specifies the actual subscriber information, which is used by the SIP Trunk Gateway to map to and from the NPI/TON field. The username field is parsed into a name and phone context (see Figure 73 on page 216).

  The subscriber information or the "username" part of the SIP URI (that is, the field before the @ symbol) is formatted as:

  digits;phone-context=[L0 subdomain name.L1 subdomain name]

  Where digits is the telephone number digits.

Figure 73
Username example



- **Service Domain Name**: Each SIP domain is a collection of a group of users either within the same region or within the same organization. All users within the same domain share the same domain name, and each has a unique username within the domain. The domain name is well known by all SIP proxies. Typically, this is the host name after the @ symbol (for example, myServiceProvider.com).
- **user=phone**: Indicates that the URI is for a telephone user.

Address lookup is based on the digits, phone context, and domain name:

> sip:[number];phone-context=[L0 subdomain name.L1 subdomain name]
> @[service domain];user=phone

The subdomain names are preconfigured data on both the SIP Trunk Gateway and SIP Redirect Server. The name explicitly maps a dialing plan to and from a SIP URI.

The ISDN NPI/TON field explicitly maps to the SIP phone-context attribute. The public numbering plans map to SIP URI by rules specified in RFC 2806 and RFC 3261. The exception is TON = unknown and TON = special number.

The private numbering plans, public/unknown numbers, and public/special numbers also have explicit one-to-one mappings to SIP URI. They must be defined by preconfigured subdomain names. The subdomain name must be defined on both Gateway and proxy/registrar.

The NRS also facilitates a translation database for phone numbers contained within the SIP URI, in order to present a well formed, syntactically correct phone number to the location service. Therefore, the NRS is designed to operate with both the phone-context and NPI/TON qualified numbers.

Example

Table 13 on page 217 provides an example of the numbering plan mapping to clarify how different dialing plans are mapped to a SIP URI. Two methods can be used to configure the URI map — one for the NRS and one for the MCS 5100. Table 13 provides examples for both the NRS and MCS 5100.

Assume the following:

- The SIP Trunk Gateway has registered at a domain called myServiceProvider.com.
- A telephone user resides at sipGWSite1 and has ESN Location Code 343 with extension 3756. The Direct Inward Dialing (DID) number is 1-613-967-3756.

Refer to Figure 71 on page 213 for the SIP address hierarchy tree.

Table 13
Numbering plan mapping (Part 1 of 3)

NPI/TON/DN	SIP URI
E.164/ International/ 1-613-967-3756	NRS example: sip:+16139673756@myServiceProvider.com;user=phone MCS 5100 example: sip:+16139673756@myServiceProvider.com;user=phone ***Note:*** Public international numbers do not have a phone context, as these numbers are globally unique within a domain. A "+" sign is automatically added by the gateway before the digits to indicate that the number is an international number.
E.164/National/ 613-967-3756	NRS example: sip:6139673756;phone-context=+1@myServiceProvider.com;user=phone MCS 5100 example: sip:6139673756;phone-context=mynation.national.e164.myrootdomain @myServiceProvider.com;user=phone

Table 13
Numbering plan mapping (Part 2 of 3)

NPI/TON/DN	SIP URI
E.164/Subscriber/ 967-3756	NRS example: sip:9673756;phone-context=+1613@myServiceProvider.com;user=phone MCS 5100 example: sip:9673756;phone-context=myarea.mynation.local.e164.myrootdomain @myServiceProvider.com;user=phone
E.164/Unknown/ 9-1-613-967-3756	Not supported for the NRS. MCS 5100 example: sip:916139673756;phone-context=myarea.mynation.unknown.e164. myrootdomain@myServiceProvider.com;user=phone
E.164/ Special Number/ 911	Not supported for the NRS. MCS 5100 example: sip:911;phone-context=myarea.mynation.special.e164.myrootdomain @myServiceProvider.com;user=phone
Private/UDP/ 343-3756	NRS example: sip:3433756;phone-context=myCompany.com@myServiceProvider.com; user=phone MCS 5100 example: sip:3433756;phone-context=level1.private.myenterprise @myServiceProvider.com;user=phone
Private/CDP/ 3756	NRS example: sip:3756;phone-context=myCdpDomain.myCompany.com @myServiceProvider.com;user=phone MCS 5100 example: sip:3756;phone-context=mylocation.level0.private.myenterprise @myServiceProvider.com;user=phone

Table 13
Numbering plan mapping (Part 3 of 3)

NPI/TON/DN	SIP URI
Private/ Special Number/ 911	NRS example: sip:911;phone-context=special.myCdpDomain.myCompany.com @myServiceProvider.com;user=phone MCS 5100 example: sip:911;phone-context=mylocation.special.private.myenterprise @myServiceProvider.com;user=phone
Private/ Unknown (Vacant Number Routing)/ 343-3756	No configuration is required for NRS. MCS 5100 example: sip:3433756; phone-context=mylocation.unknown.private.myenterprise @myServiceProvider.com;user=phone
Unknown/ Unknown/ 6-343-3756	No configuration is required for NRS. MCS 5100 example: sip:63433756; phone-context=mylocation.unknown.unknown. myrootdomain@myServiceProvider.com;user=phone

Database synchronization/operation component

The NRS database has two schemas — an active schema and a standby schema.

- The active database is used for runtime queries.
- The standby database is used for administrator modifications. A user can only make changes to the standby database.

Cutover and revert

Figure 74 on page 220 shows both the active and standby database when a cutover and a revert occur.

1. Both the active and standby databases are synchronized.
2. A change is made to the standby database.

3 The standby database is changed and the active database is unchanged, so the databases are not synchronized.

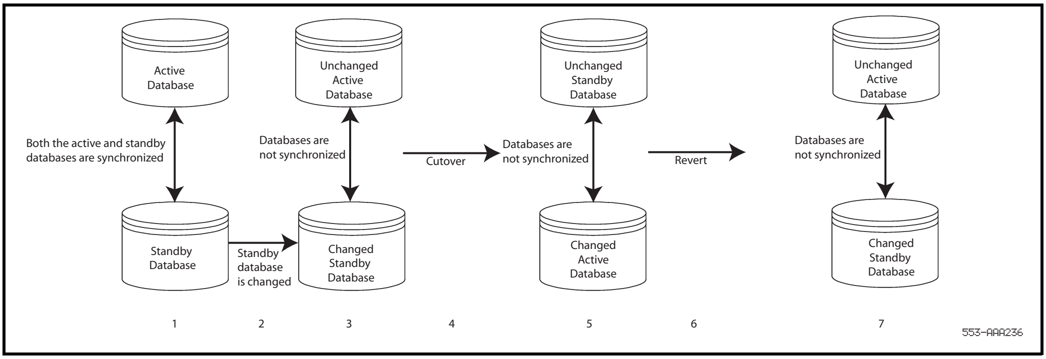
4 The database cutover command is issued.

5 The changed database becomes the active database.

6 The database revert command is issued (perhaps the user wants to make more changes to the database).

7 The changed database becomes the standby database.

Figure 74
NRS database actions — cutover and revert


Active Database
Unchanged Active Database
Unchanged Standby Database
Unchanged Active Database
Both the active and standby databases are synchronized
Databases are not synchronized
Cutover
Databases are not synchronized
Revert
Databases are not synchronized
Standby Database
Standby database is changed
Changed Standby Database
Changed Active Database
Changed Standby Database
1
2
3
4
5
6
7
553-AAA236

Cutover and commit

Figure 75 on page 221 shows both the active and standby database when a cutover and a commit occur.

1 Both the active and standby databases are synchronized.

2 A change is made to the standby database.

3 The standby database is changed and the active database is unchanged, so the databases are not synchronized.

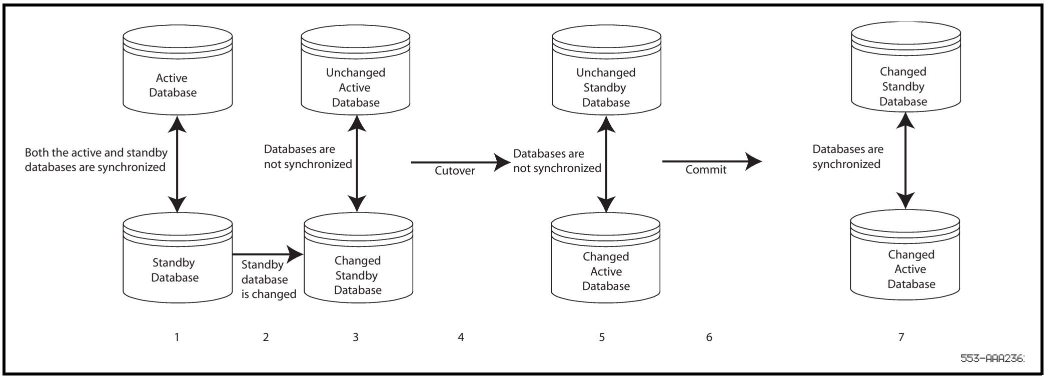
4 The database cutover command is issued.

5 The changed database becomes the active database.

6 The database commit command is issued (the user wants to submit the changes made to the database).

7 Both databases are changed.

Figure 75
NRS database actions — cutover and commit


Active Database
Both the active and standby databases are synchronized
Standby Database
Standby database is changed
Unchanged Active Database
Databases are not synchronized
Changed Standby Database
Cutover
Unchanged Standby Database
Databases are not synchronized
Changed Active Database
Commit
Changed Standby Database
Databases are synchronized
Changed Active Database
1
2
3
4
5
6
7
553-AAA236

Single-step cutover and commit

Figure 76 on page 222 shows both the active and standby database when a single-step cutover and commit occur:

1 Both the active and standby databases are synchronized.

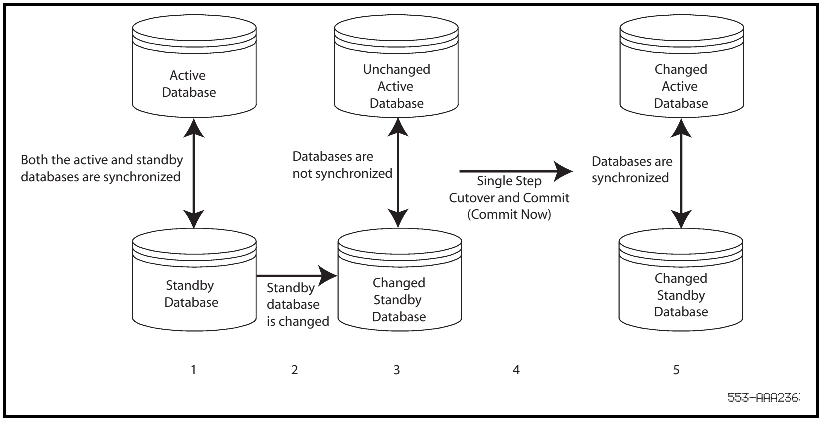
2 A change is made to the standby database.

3 The standby database is changed and the active database is unchanged, so the databases are not synchronized.

4 The database single-step cutover and commit command is issued.

5 Both databases are changed.

Figure 76
NRS database actions — single-step cutover and commit


Active Database
Unchanged Active Database
Changed Active Database
Both the active and standby databases are synchronized
Databases are not synchronized
Single Step Cutover and Commit (Commit Now)
Databases are synchronized
Standby Database
Standby database is changed
Changed Standby Database
Changed Standby Database
1
2
3
4
5
553-AAA236

Rollback

Figure 77 on page 223 shows both the active and standby database when a single-step cutover and commit occur:

1 Both the active and standby databases are synchronized.

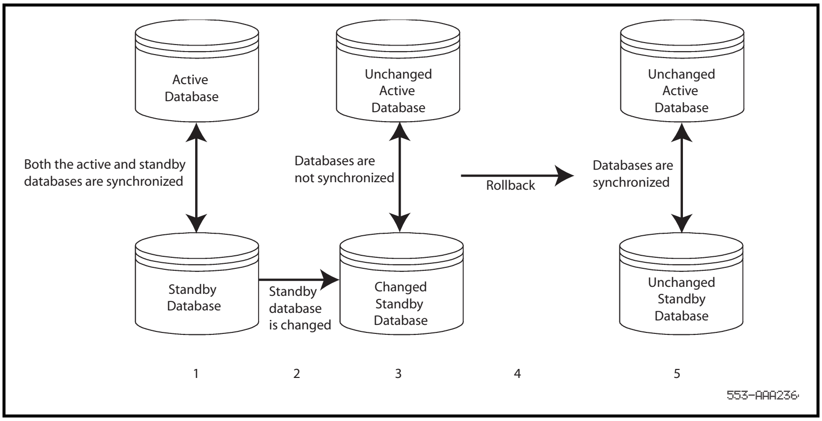
2 A change is made to the standby database.

3 The standby database is changed and the active database is unchanged, so the databases are not synchronized.

4 The database rollback command is issued (the user wants to undo the changes to the database).

5 Neither database is changed.

Figure 77
NRS database actions — rollback


Active Database
Both the active and standby databases are synchronized
Standby Database
Standby database is changed
Unchanged Active Database
Databases are not synchronized
Changed Standby Database
Rollback
Unchanged Active Database
Databases are synchronized
Unchanged Standby Database
1
2
3
4
5
553-AAA236

To perform database actions using NRS Manager, refer to “Performing NRS database actions” on page 454.

Web server — NRS Manager

NRS configuration and maintenance is performed using a recommended web browser. NRS Manager is used to configure and maintain aspects of the Network Routing Service through a web interface.The NRS Manager web server is on the Signaling Server. The NRS Manager web client application supports Microsoft Internet Explorer 6.0 (or later).

For detailed information about NRS Manager, refer to “Configuring and managing the Network Routing Service” on page 379.

vxWorks shell

The Wind River vxWorks shell provides access to the operating system for maintenance and debug operations.

NRS functionality

Contents

This section contains information on the following topics:

Introduction

All systems in the IP Peer network must register with the NRS.

The primary function of the NRS is to provide the following services:

- endpoint and Gateway registration
- call admission control
- address translation and telephone number-to-IP lookup
- centralized numbering plan administration

> ***Note:*** The NRS can operate in stand-alone mode, without being connected to the Call Server.

The NRS is SIP- and H.323-compliant. It can provide NRS features to other SIP-compliant and H.323-compliant Nortel endpoints (for example, CS 1000 systems and IP Trunk 3.0 (or later) endpoints). A static IP address must be configured for these endpoints, as well as the telephone numbers that the endpoints can terminate.

> ***Note:*** Systems that do not support H.323 RAS procedures and H.323 Gatekeeper procedures are referred to as non-RAS endpoints.

Network overview

With IP Peer Networking, each network zone contains one active NRS. The NRS can run on any of the Signaling Server platforms on any of the CS 1000 nodes in the network. The NRS is configured with numbering plan information for every node in the network zone.

Coordinated endpoint configuration across multiple NRS zones

IP Peer Networking supports multiple SIP and H.323 zones. Separate NRS databases must be managed for each zone in a 1:1 relationship. Each NRS zone contains a Primary NRS, optionally an Alternate NRS, and multiple

Gateway Endpoints or User Endpoints. The reasons for implementing multiple NRS zones are:

1. to scale up to very large networks with hundreds of registered endpoints
2. to divide a network of any size into convenient administration zones (for example, Western Europe and North America)

When a CS 1000 system places an IP call to another node, the originating Gateway signaling server sends a message to the NRS, specifying the destination telephone number. The NRS consults its internal numbering plan database and determines which node is the correct destination node.

SIP operation

The SIP Redirect Server allows SIP Trunk Gateways to communicate with other SIP Trunk Gateways across an enterprise. The SIP Trunk Gateway must keep information only about various lines and applications for which it is responsible, and it must have enough knowledge to contact the SIP Redirect Server. The SIP Redirect Server then redirects the SIP Trunk Gateway to where it needs to send its signaling.

A SIP Redirect Server receives requests but, rather than passing these requests onto another redirect server, it sends a response back to the originator of the request.

SIP Trunk Gateways, SIP Proxy Servers (for example, the MCS 5100), and SIP Phones forward calls to the contact address returned by the SIP Redirect Server. For instance, a SIP Trunk Gateway sends an INVITE message to the SIP Redirect Server. The SIP Redirect Server then sends a redirect message back to the originator with the addressing information for the destination node. The originator then sends an INVITE message directly to the SIP Trunk Gateway destination node.

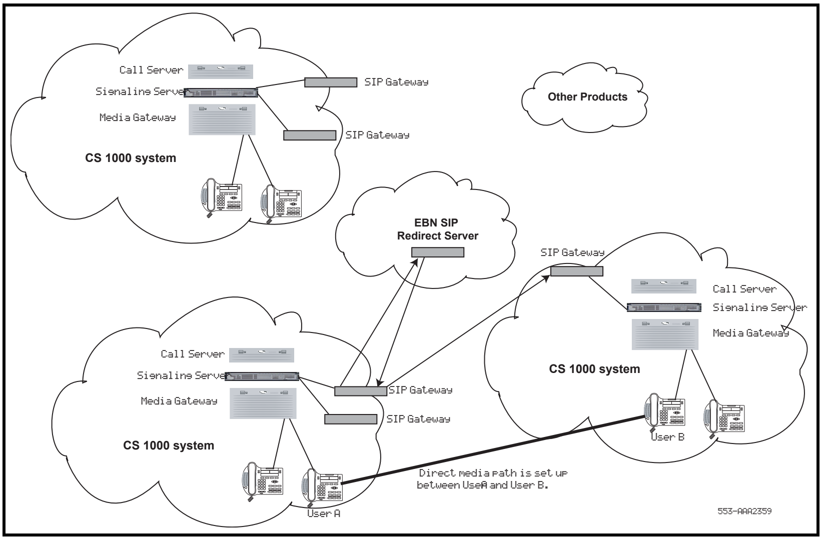
For example, User A would like to contact User B across the enterprise network. The following sequence occurs:

- User A contacts its SIP Trunk Gateway. (That is, User A sends an address-resolution request to the SIP Trunk Gateway.)
- User A’s SIP Trunk Gateway contacts the EBN SIP Redirect Server.

- The EBN SIP Redirect Server executes a location look-up to see if its database contains an address match for the domain of User B.
- If a match is found, the SIP Redirect Server returns a response back to User A indicating the contact address required for User A to call the called party. (That is, the EBN SIP Redirect Server redirects User A’s SIP Trunk Gateway to User B’s SIP Trunk Gateway.)
- User A’s SIP Trunk Gateway uses the provided contact address and directly communicates with User B’s SIP Trunk Gateway.
- A direct media path is then set up between User A and User B.

Figure 78 shows how the SIP Redirect Server accepts a request from a SIP Trunk Gateway and sends the response back to the SIP Trunk Gateway. The SIP Trunk Gateway can then contact the called party’s SIP Trunk Gateway directly. Once the SIP Trunk Gateway contacts the called party's SIP Trunk Gateway, a direct media path is set up between the caller and the called party.

Figure 78
SIP Signaling and SIP Redirect Server



If the SIP Redirect Server does not find any matching numbering plan entries, (a NULL entry is returned by the database), then the SIP Redirect Server transmits a SIP 404 (Not Found) response.

Similarly, if a request fails due to registration failure, a SIP 401 (Unauthorized) response is transmitted.

> ***Note:*** All redirect server logs use the existing RPT report log facility.

H.323 operation

An H.323 Gateway sends an ARQ message to the H.323 Gatekeeper. If a match is found for the called-party number digits in the ARQ, then the H.323 Gatekeeper sends an ACF message to the call originator and includes addressing information for the destination node.

If no numbering plan entries are found, the H.323 Gatekeeper queries all the H.323 Gatekeepers on its list, using H.323 LRQ/LCF (Location Request/ Location Confirm) multicast protocol.

For example, a caller located at Node A places a call and sends an ARQ message to the H.323 Gatekeeper. The H.323 Gatekeeper consults its numbering plan database, determines that Node B is the correct destination, and returns the addressing information for Node B in an ACF message. Node A then sends the SETUP message directly to the H.323 Gateway Signaling Proxy Server on Node B.

If an H.323 Gatekeeper cannot resolve the destination address received in an incoming ARQ message, then it sends a LRQ message to other network zone H.323 Gatekeepers in order to resolve the number.

> ***Note:*** The H.323 Gatekeeper sending the LRQ message includes its own identification in the LRQ message and does not include the H323-ID of the gateway that sent the original ARQ message.

The peer H.323 Gatekeeper that resolves the number sends an LCF message with the destination Call Signaling address.

If an H.323 Gatekeeper cannot resolve the destination address in an incoming LRQ, it sends a Location Reject (LRJ) message to the originator of the LRQ message.

The behavior of the H.323 Gatekeeper (that sent the LRQ messages) depends on the responses from the remote H.323 Gatekeepers. When an LCF is received from a remote H.323 Gatekeeper, the local H.323 Gatekeeper immediately sends the ACF to the gateway at Node A. If an ARJ is received indicating "incomplete number", further digits are required. An immediate ARJ indicating the need for further digits is sent to Node A. Node A retries on receiving more digits. Otherwise, the local H.323 Gatekeeper waits until either all the remote Gateways have responded, or a timer expires indicating that one or more Gatekeepers could not reply. At this time, either an ARJ indicating call failure is returned, or an ACF indicating the default route is returned.

Incoming LRQ messages

When an H.323 Gatekeeper receives an incoming LRQ message, it checks to see if the H.323 Gatekeeper that sent the request is configured in its database. The information received in the **sourceInfo** field is used for authentication.

Table 14
How the H.323 Gatekeeper authenticates incoming LRQ messages

If the H.323 Gatekeeper sending the LRQ is a...	Then its sourceInfo field contains...	And the H.323 Gatekeeper has to check...
CS 1000 Release 4.0 (or later) H.323 Gatekeeper or Succession 3.0 H.323 Gatekeeper	the alias address of the peer H.323 Gatekeeper that sent the LRQ message	(not applicable)
CS 1000S Release 2.0 H.323 Gatekeeper	the alias address of the H.323 Gateway	for the alias in the • network zone H.323 Gatekeeper list • endpoints list

If the information in the sourceInfo field cannot be authenticated, then the H.323 Gatekeeper rejects the incoming LRQ.

On receiving the incoming LRQ, the H.323 Gatekeeper parses the sourceInfo field. It searches for the source alias address as a URL ID type or an H323-ID type.

The H.323 Gatekeepers send the gatekeeper alias address along with the CDP domain information as a URL string. The format of the URL string is:

```
h323:gkH323ID;phone-context=cdpDomain
```

This URL string contains two variables that are configured at the far end:

- gkH323ID
- cdpDomain

This URL string is parsed for incoming LRQs and is used to extract the H.323 Gatekeeper alias name and the CDP domain information.

- The H.323 Gatekeeper alias name is used for gatekeeper authentication.
- The CDP domain information is used to search in the same CDP domain if the destination info was private.level0 type of number.

  Note: The cdpDomain is a string of characters that can be of any format. Typically, it would be something like the following to ensure uniqueness: “CDP-TorontoOntarioCanada.cdp.corporateTitle.com”.

Outgoing LRQ messages

An H.323 Gatekeeper can be configured with a list of IP addresses of alternate H.323 Gatekeepers in different network zone. The H.323 Gatekeeper can then send LRQ requests in an attempt to resolve ARQ requests for which it cannot find registered matches in its own numbering plan database.

The configuration of H.323 Gatekeepers Collaborative Servers includes:

- an IP address

- an H.323 ID
- a CDP domain (Level 0 Domain)

See “Adding a Collaborative Server” on page 442.

This information is used for incoming LRQs and is also used to determined the H.323 Gatekeepers in which to send outgoing LRQs. If a Network Zone H.323 Gatekeeper is configured with a CDP domain, then it is sent an LRQ only if the endpoint sending the ARQ is also in the same CDP domain. If an ARQ request arrives, and there is no matching numbering plan entry for the destination telephone number or there is a match but the matching entry (plus any alternates) is not currently registered, then the H.323 Gatekeeper sends an LRQ to all other H.323 Gatekeepers on the network whose IP addresses have been configured.

Each H.323 Gatekeeper is configured with an H.323 Gatekeeper alias name which is an H323-ID. The outgoing LRQ message contains the H.323 Gatekeeper alias name in the sourceInfo field instead of the H323-ID received in the incoming ARQ message.

NRS purpose

IP Peer Networking uses optionally redundant NRSs to support a centralized Network Numbering Plan. Each NRS has a zone that administers its own numbering plan and requests other NRSs for the numbering plan in their respective zones. A numbering plan specifies the format and structure of the numbers used within that plan. A numbering plan consists of decimal digits segmented into groups to identify specific elements used for identification, routing, and charging capabilities. A numbering plan does not include prefixes, suffixes, and additional information required to complete a call. The Dialing Plan contains this additional information. The Dialing Plan is implemented by the endpoints in a network. A Dialing Plan is a string or combination of digits, symbols, and additional information that defines the method by which the numbering plan is used. Dialing Plans are divided into the following types:

- Private (on-net) dialing
- Public (off-net) dialing

For more information about numbering plans and dialing plans, see "Numbering plans" on page 255.

H.323 Gatekeeper discovery

Endpoints that require admission to the IP network and address translation must discover their NRS. Endpoints can be configured with the static IP address of the NRS running on the network's Primary NRS. This ensures that the IP address stays constant across restarts, and, therefore, the endpoints with statically configured NRS IP addresses can always discover the NRS. These endpoints send a message directly to the NRS over the User Datagram Protocol/Internet Protocol (UDP/IP). This is the recommended approach; however, endpoints not configured with the IP address of the NRS can use multicast to discover the IP address of their NRS.

The message requesting the IP address of the H.323 Gatekeeper contains the endpoint alias and the RAS signaling transport address of the endpoint. This is so the H.323 Gatekeeper knows where to send return messages. The message from the endpoint to the H.323 Gatekeeper also contains vendor information. Thus, the H.323 Gatekeeper determines the specific product and version that is attempting discovery. The H.323 Gatekeeper only uses this information if the request for discovery is rejected.

Nortel recommends that endpoints use the endpoint Alias.h323-ID alias types.

The Gatekeeper contains a list of predefined endpoint aliases. The Gatekeeper attempts to match the H323-ID in the message from the endpoint with one of the endpoint aliases in the list. If it cannot find a match, it rejects the discovery request.

The Gatekeeper returns its RAS signaling transport address to any endpoints that are allowed to register, so the endpoints know where to send RAS messages. The Gatekeeper also returns a list of Alternate Gatekeepers, if any are configured. Therefore, if the Gatekeeper is removed from service gracefully or if it cannot be reached by an endpoint, the endpoints can attempt to register with the Gatekeepers in the Alternate Gatekeepers list.

> *Note:* Gatekeeper Discovery using the Multicast approach is not recommended over large networks, because all routers between the endpoint requesting Gatekeeper discovery and the Gatekeeper must support Internet Group Management Protocol (IGMP).

H.323 Endpoint registration

After Gatekeeper discovery is complete, endpoints must register with the Gatekeeper. The Signaling Server platform, on which the H.323 Proxy Server for the node runs, has an IP address. This IP address is both the RAS signaling transport address and the call-signaling transport address. The endpoints register with the Gatekeeper by sending a registration-request message to the Gatekeeper.

Registering endpoints must provide vendor information, as well as its alias name in the registration-request message. The Gatekeeper tracks the vendor information for management purposes. The administrator can determine the exact product and version of all registered endpoints using NRS Manager or the CLI. The Gatekeeper also uses this information if registration fails.

If the Gatekeeper accepts the registration request, it responds with a registration confirmation message. In this message, the Gatekeeper can include the IP address of an Alternate Gatekeeper (if one is configured). Endpoints also provide call signaling and RAS transport addresses in the registration-request message. The Gatekeeper supports the receipt of multiple transport addresses and gives priority to the first address in each list.

> *Note 1:* IP Trunk 3.0 (or later) nodes always register multiple IP addresses due to the load-balancing architecture of the IP Trunk 3.0 (or later) nodes. The first IP address in the registration request is the node IP address and the remaining IP addresses are the IP addresses of the individual trunk cards in the node. When a call terminates on an IP Trunk 3.0 (or later) node, the Gatekeeper returns only the node IP address. The Gatekeeper knows that the endpoint is an IP Trunk 3.0 (or later) node, as its vendor information is provided in the request for registration message.

> *Note 2:* IP Trunk 3.0 (or later) nodes use multiple IP addresses when sending admission requests to the Gatekeeper. The card that is the RTP endpoint for the call uses its own IP address for the ARQ. However, to

ensure that the node can carry out load-balancing, the node "Leader" IP address is sent to the Gatekeeper in the registration request; no other IP addresses are provided, to allow the IP Trunk node to control load balancing.

The Gatekeeper knows that the IP Trunk 3.0 (or later) IP address used in the ARQ belongs to the node, since the Gatekeeper provides an endpoint identifier in the registration sequence, and this is included in all ARQs.

The Gatekeeper extracts the H323-ID from the incoming request for registration message and attempts to match it with one of the preconfigured endpoint H323-ID aliases in its internal database. If no match is found, the Gatekeeper rejects the registration request. If a match is found, the Gatekeeper accepts registration and extracts the call signaling and RAS transport addresses from the registration-request message. The Gatekeeper updates its internal database with this information and then sends a registration confirmation message to the endpoint. If an Alternate Gatekeeper is configured, the Gatekeeper also returns the Alternate Gatekeeper's IP address.

The Gatekeeper assigns the endpoint a unique Endpoint Identifier and returns this identifier in the registration confirmation message. This Endpoint Identifier is included in all subsequent RAS requests that the endpoint sends to the Gatekeeper. The Gatekeeper tracks the value of the assigned Endpoint Identifier for the duration of the endpoint's registration. The Gatekeeper can then match any incoming RAS request with the registration confirmation sent previously.

> ***Note:*** The Gatekeeper accepts registration-request messages from an endpoint even if the Gatekeeper has not received a Gatekeeper discovery request from that particular endpoint.

Time-to-Live

The registration message includes Time-to-Live information. Endpoints periodically send registration-request messages to the NRS in order to remain registered and so that the NRS knows that the endpoints are alive.

An endpoint's registration with the NRS can expire. Registering endpoints must include Time-to-Live information in their registration-request messages. The NRS responds with the same Time-to-Live information or the Time-to-Live information currently configured on the NRS if the NRS timer is shorter. This is a time-out in seconds. After this time, the registration expires. Before the expiration time, the endpoint sends a registration-request message with the "Keep Alive" bit configured. When the NRS receives this request, it extends the endpoints registration and resets the Time-to-Live timer.

If the Time-to-Live timer expires, the NRS unregisters the endpoint. The endpoint's entry in the internal database is updated to indicate that it is no longer registered and that the associated transport addresses are no longer valid.

Configure the Time-to-Live timer using NRS Manager. Nortel recommends that the timer be configured to 30 seconds. Refer to "Configuring system-wide settings" on page 402 (specifically, Procedure 31: step 4 on page 403).

Multiple registration requests

The NRS supports re-registration requests by an endpoint, provided that the information contained in the registration request is identical to that in the initial registration request. For example, if an endpoint crashes and then restarts after the boot sequence, it attempts to reregister with the NRS by sending another registration-request message. The NRS accepts this registration by sending a confirmation message to the endpoint.

Registration requests when the NRS is out-of-service

The NRS can be taken out-of-service through NRS Manager. If the NRS receives a registration-request message from an endpoint while it is out-of-service, it rejects the registration request. However, the NRS sends the IP address of the Alternate NRS in the reject message.

Unregistration

An endpoint should be taken out-of-service prior to changing its IP address or performing software upgrades. Once out-of-service, an endpoint unregisters from the NRS by sending an unregister message. The NRS updates the endpoint's entry in the internal database to indicate that it is no longer registered and that the associated transport addresses are no longer valid.

If the endpoint does not send an unregister message to the NRS, the NRS automatically unregisters the endpoint when the Time-to-Live timer expires.

SIP registration

The SIP Registrar accepts REGISTER requests. A request is a SIP message sent from a client to a server to invoke a particular operation.

> ***Note:*** A response is a SIP message sent from a server to a client to indicate the status of a request sent from the client to the server.

Registration entails sending a REGISTER request to the SIP Registrar. The SIP Registrar acts as the front end to the location service (database) for a domain, reading and writing mappings based on the contents of REGISTER requests. This location service is then typically consulted by a SIP Redirect or Proxy Server that is responsible for routing requests for that domain.

The SIP Registrar places the information it receives (in the requests) into the location service for the domain it handles. The location service is used by the SIP Redirect and Proxy Servers to locate the SIP Trunk Gateway that serves the target of the request. A SIP Trunk Gateway has a number of non-SIP lines and trunks behind it which do not have their own identity in the SIP domain. These non-SIP endpoints are accessed by mapping SIP URIs based on telephony DNs to one or more SIP Trunk Gateways. The location service is a matching mechanism that allows a fully-qualified telephone number to be associated with a range of telephone numbers and the SIP Trunk Gateway that provides access to that DN range.

SIP endpoints are also known as User Agents. User Agents have two functions:

- act as User Agent Clients — initiate request
- act as User Agent Servers — process requests and generate responses to the requests

The SIP Registrar is a special type of User Agent Server.

The REGISTER request

A REGISTER request is used for registering contact information. The REGISTER request is used by SIP clients to notify a SIP network of its current IP address and the URLs for which it would like to receive a call. This SIP mechanism is used by called parties to register in order to receive incoming calls from proxies that serve that domain.

Dynamic registration

Dynamic registration facilitates the creation of a contact list for the authorized SIP Trunk Gateway Endpoints and SIP Phones (SIP User Endpoints).

Dynamic registration of SIP Trunk Gateway Endpoints

SIP Trunk Gateway dynamic registration facilitates the creation of the contact list for the authorized Gateway endpoints. The gateways dynamically register their IP address with the SIP Redirect/Proxy Server (that is, with the SIP Registrar component). This eliminates some manual provisioning at the SIP Redirect Server. It also reduces the potential for error when manually entering the IP address of the SIP Trunk Gateway in the SIP Redirect Server.

Dynamic registration of SIP Phones (SIP User Endpoints)

SIP Phone dynamic registration facilitates the creation of the contact list for the authorized SIP Phones. For more information about SIP Phone registration, refer to “SIP Phone dynamic registration” on page 540.

Database synchronization

Database synchronization treats dynamically registered data the same way as the H.323 Gatekeeper:

- If the Alternate NRS database takes over, then registrations are lost.
- If the Failsafe NRS database takes over, then registrations are kept.

NRS Manager

NRS Manager is a web-based configuration interface. Use NRS Manager to configure the NRS. You can use NRS Manager to view, add, modify, or delete all numbering plan configuration data.

You can perform the following NRS configuration functions using NRS Manager:

- configure a numbering plan
- add, modify, or delete preconfigured endpoint data
- add, modify, or delete numbering plan entries on a per-endpoint basis
- retrieve the current configuration database
- interwork with a preconfigured database
- revert to the standby database
- change system passwords

Security

NRS Manager is password-protected.

The NRS has two access levels:

- Administrator level
- Monitor level

Administrator access

A user with administration-level access can view and modify the NRS. Administrator-level access is the highest authority level. An administrator has the authority to manage the entire NRS.

The administrator has the ability to view, create, and modify the login names and passwords that are used for configuration and maintenance.

If you log in to NRS Manager as an administrator, you have full administrative access. You can update all configuration entries, and you have full write access to the database, including the ability to change all NRS passwords.

The NRS administrator username and password are used only when accessing NRS Manager. Changing the NRS administrator username and password does not change the username and password for the Signaling Server shell.

IMPORTANT!

Nortel recommends that default usernames and passwords be changed for increased network security.

Changing username and passwords

The usernames and passwords used to access the NRS can be changed under the Administration tab in NRS Manager. See "Configuring and administering users" on page 479.

All user login names and passwords are recorded in the NRS database. The passwords are stored in an encrypted format.

Monitor access

A user with monitor-level access can only view existing NRS configuration data. The user cannot modify any NRS configurations or settings. A user with monitor access can only change their own password.

NRS Manager blocks certain navigation operations for monitor-access level users. If a user is a monitor-level user, then NRS Manager does not allow the user to change NRS provisioning operations.

If you log in to the NRS as a monitor, you can:

- view configuration data
- execute H.323 and SIP routing tests
- review reports

  Note: CS 1000 Element Manager includes performance and traffic monitoring functions.

NRS operating parameters

The NRS can co-reside on the Signaling Server with other applications (co-resident mode). For large networks, if the Signaling Server does not have enough capacity to support the NRS functionality in conjunction with other applications, a dedicated Signaling Server can be required for the NRS (stand-alone mode). The NRS (Primary, Alternate, or Failsafe) cannot reside on an Alternate Signaling Server. It has to be on a Primary (Leader) Signaling Server.

The NRS has no knowledge of dialing plans implemented on endpoints. The NRS only has knowledge of numbering plans and deals only with fully-qualified E.164/International numbers, fully-qualified E.164/National numbers, and fully-qualified Private numbers.

The NRS can use prefix routing as long as the prefix is qualified. That is, you do not need 1-613-969-7944; 1-613-969 may be enough.

Endpoints do not have to register the telephone numbers or range of telephone numbers that they support with the NRS. If endpoints register with this information, it is not used but can be made available for management purposes to Element Manager.

Information regarding the numbers which an endpoint can terminate must be configured in the NRS. This ensures that the numbering plan for the entire network is managed from a central location and that endpoints cannot support numbers which are not preconfigured on the NRS. If an endpoint provides this number information when registering with the NRS, it is ignored.

H.323 endpoints which register using RAS messages must provide an H323-ID or a similar alias (for example, URL-ID or e-mail ID).

The NRS supports only direct-routed call signaling and RAS messaging for call control.

- All H.323 endpoints registered with the H.323 Gatekeeper must use the ARQ mechanism and must consult with the H.323 Gatekeeper for admission and address translation. The H.323 Gatekeeper does not pre-grant an ARQ for the call originator, but does pre-grant for the call terminator. This is because the H.323 Gatekeeper does not track call state, and has no easy way of correlating the ARQ between call originators and terminators.
- All SIP endpoints registered with the SIP Redirect Server must use the SIP INVITE message.

All H.225/Q.931 call-signaling messages and all H.245 call-control messages are not directed to the NRS and are passed directly between endpoints. This approach enables the NRS to be more scalable and to handle a larger number of simultaneous calls.

Each NRS supports up to 100 000 calls per hour.

The IP Peer Networking feature uses direct-routed call signaling; therefore, use of the NRS has no impact on MCDN or QSIG tunneling. For example, if MCDN or QSIG is tunneled between a CS 1000 node and an IP Trunk 3.0 (or later) node, then the tunneling takes place in the H.225/Q.931 call signaling. The tunneling is completely independent of the RAS which is routed to the NRS.

The NRS (H.323 Gatekeeper only) supports Overlap Sending according to H.323; however, allowable configuration items on the H.323 Gatekeeper must be taken into consideration. For more information about overlap signaling, refer to "Overlap signaling" on page 487.

The NRS (stand-alone mode only) generates SNMP traps and sends them to a configured SNMP host. The NRS uses the SNMP services provided by the Signaling Server platform.

The NRS supports IP multicast for discovery and location-request messages.

> ***Note:*** NRS/H.323 Gatekeeper Discovery using the Multicast approach is not recommended over large networks, because all routers between the endpoint requesting NRS discovery and the NRS must support Internet Group Management Protocol (IGMP).

The NRS supports multiple customers. Multiple customers can be configured with each customer having their own unique dialing or numbering plan.

The NRS does not track the state of active calls, keep count of the total number of active calls, or generate Call Detail Recording (CDR) records. Therefore, all Disengage Request (DRQ) messages are automatically confirmed. The NRS does not have traffic management capabilities, such as maximum calls allowed for each endpoint or maximum bandwidth allowed for each endpoint or zone.

Alternate routing based on the geographical zone of the call originator is not supported. This has implications for 911 handling. In order to provide different routing for 911 calls from different originating CS 1000 nodes, some form of digit manipulation is required. In the case of two nodes, for example, one node could prefix 911 with 1, and the other node could prefix 911 with 2. The NRS could have two different numbering plan entries, one for 1911 and one for 2911 and provide different routing in this fashion.

Zone management on the Call Server provides an alternate mechanism for routing 911 calls, based on the branch office or SRG zone. For more information, refer to *Branch Office: Installation and Configuration* (553-3001-214).

The NRS, like all CS 1000 components, does not support the H.235 security protocol.

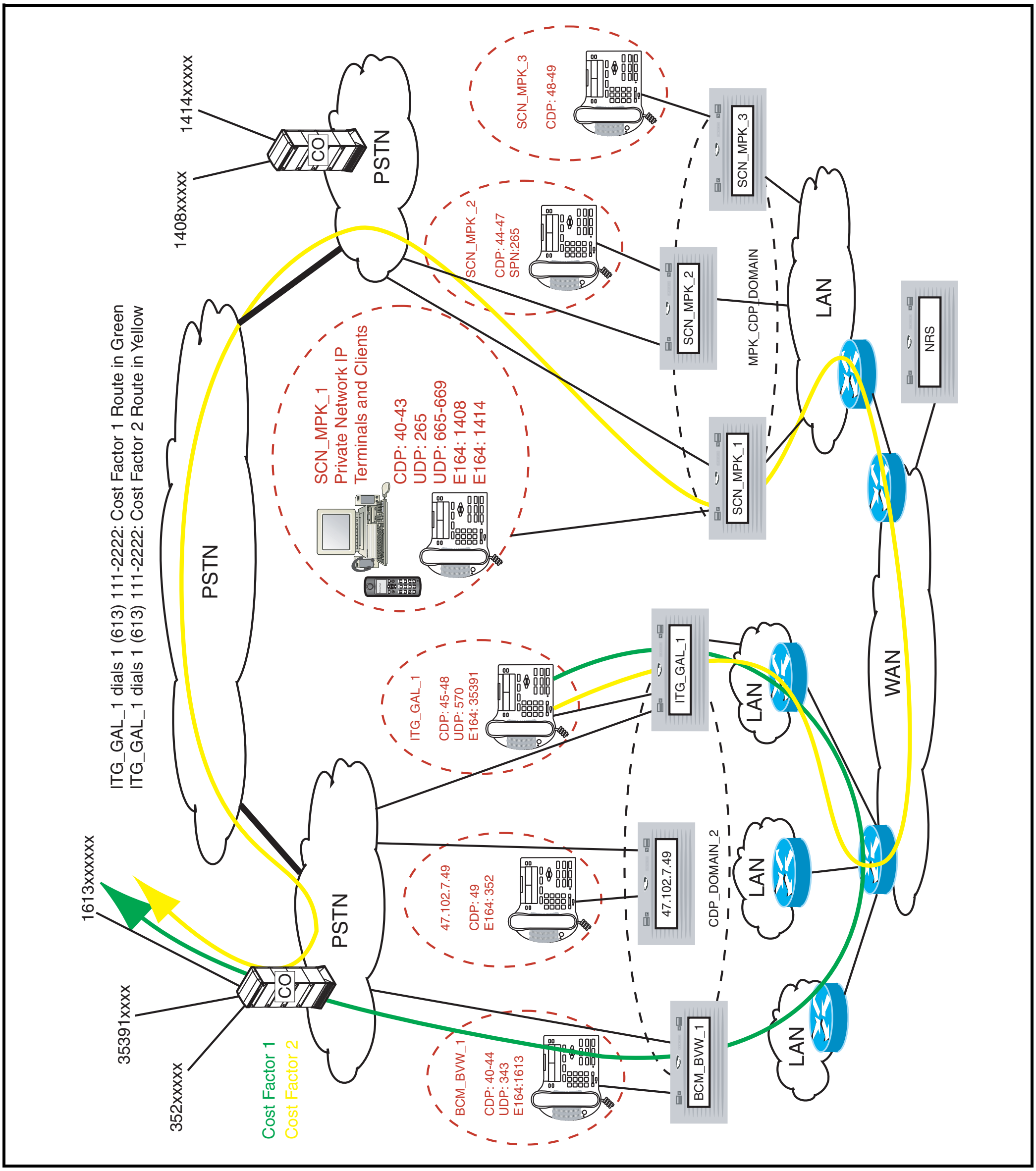
All number and cost factor pairs within a numbering plan table are unique for private numbering plans. When adding an H.323 alias for a predefined H.323 endpoint, the request is rejected if the administrator specifies an alias type and provides a number string and cost factor that is already in the numbering plan table for that alias type.

For example, Figure 79 on page 244 illustrates the configuration of a CS 1000S System.

- SCN_MPK1 terminates privateNumber.level1RegionalNumber 265 with cost factor 1.
- BCM_BVW_1 also terminates this number but with a different cost factor, 2.

If the administrator had attempted to configure this number on BCM_BVW_1 and had specified a cost factor of 1, the request would be rejected.

Figure 79
Example of all call routing plans



Number and cost factor pairs can be the same across different numbering plan tables. The numbering plan tables shown have only three columns for terminating route H323-ID and cost factor pairs. These are for illustrative purposes and in practice there can be as many alternate routes with different cost factors as required.

Similarly, configure the default routes according to alias type and CDP domain, as many alternate routes and associated cost factors can be required.

The NRS places the numbers in the numbering plan tables in ascending order. This accelerates the search when performing address translations.

When additional numbering plan entries are added using NRS Manager, they are inserted in the middle of the table. For example, if an entry with publicNumber.internationalNumber alias type and numbering plan digits 1514 is added, it is inserted in the table between the 1414 and 1613 entries.

If an alias is added whose leftmost digits match an existing alias of the same type, it is placed below the existing entry in the table. For example, in the privateNumber.level1RegionalNumber table, the 2651 entry is below the 265 entry. This is similar to the ordering of entries in IP network routing tables, with more specific entries appearing below more general entries.

> ***Note:*** Tables generated in this example are represented in "Example – generated tables" on page 247.

When the NRS is resolving the IP address, if the number to be resolved begins with 2651XXX, the IP address of SCN_MPK_3 is returned (if it is registered). If the number to be resolved begins with 2652XXX, the IP address of SCN_MPK_1 is returned (if it is registered).

Ranges of leading digits can be configured (for example, a privateNumber.level1RegionalNumber entry of 665-669). This means that any numbers of this type beginning with 665, 666, 667, 668, or 669 are resolved to the IP address of SCN_MPK_1.

Leading digit ranges can be overridden by configuring more precise numbering plan entries or numbers with a greater number of leading digits. For example, a privateNumber.level1RegionalNumber of 6651200# takes precedence over an entry of 665-669.

This means that the number 6651299 would resolve to the IP address of SCN_MPK_1, but 6651200 would resolve to the IP address of BCM_BVW_1. Note that due to the '#' character length requirement, 66512001 would not match the 6651200# numbering plan table entry and would resolve to SCN_MPK_1.

Endpoints that do not support RAS procedures have their IP address entered directly into the numbering plan table entry H323-ID field or the default route H323-ID field.

All H323-IDs are included in alphabetical order in the endpoint status table. This includes default endpoints.

The IP address field in the endpoint status table is only updated if it is known (that is, if the endpoint with the associated H323-IDs has registered).

CDP numbering plan entries can be the same provided that the terminating endpoints belong to different CDP domains. For example, the CDP entries 40-43 for SCN_MPK_1 and 40-44 for BCM_BVW_1.

No special configuration items are present for ESN5 or Carrier Access Code support. If the Signaling Server is unable to provide a fully-qualified number in ARQ to the H.323 Gatekeeper and the number is prefixed with ESN5 prefix 100, then this prefix is placed before the existing entry in the numbering plan table.

National numbers are inserted into the publicNumber.internationalNumber table with the country code prefixed.

Example – generated tables

The configuration shown in Figure 79 on page 244 would result in Table 15 through Table 22 on page 250.

Table 15
privateNumber.level1RegionalNumber numbering plan

Digits	Terminating Routes			
	H323-ID	Cost Factor	H323-ID	Cost Factor
265	SCN_MPK_1	1	BCM_BVW_1	2
2651	SCN_MPK_3	1		
343	BCM_BVW_1	1	SCN_MPK_1	2
570	ITG_GAL_1	1	47.102.7.49	2
665-669	SCN_MPK_1	1		
6651200#	BCM_BVW_1	1		

Table 16
privateNumber.pISNSpecificNumber numbering plan

Digits	Terminating Routes	
	H323-ID	Cost Factor
265	SCN_MPK_2	1

Table 17
publicNumber.internationalNumber numbering plan

	Terminating Routes					
Digits	H323-ID	Cost Factor	H323-ID	Cost Factor	H323-ID	Cost Factor
1408	SCN_MPK_1	1	BCM_BVW_1	2		
1414	SCN_MPK_1	1	SCN_MPK_2	2	ITG_GAL_1	3
1613	BCM_BVW_1	1	SCN_MPK_1	2		
352	47.102.7.49	1				
35391	ITG_GAL_1	1	47.102.7.49	2	SCN_MPK_1	3

Table 18
CDP domain table

	Default Routes	
CDP Domain Name	H323-ID	Cost Factor
CDP_DOMAIN_2	47.85.2.100	1
MPK_CDP_DOMAIN		

Table 19
CDP_DOMAIN_2 numbering plan

	Terminating Routes			
Digits	H323-ID	Cost Factor	H323-ID	Cost Factor
40-44	BCM_BVW_1	1		
45-48	ITG_GAL_1	1		
49	47.102.7.49	1	47.102.7.50	2

Table 20
MPK_CDP_DOMAIN numbering plan

	Terminating Routes	
Digits	H323-ID	Cost Factor
40-43	SCN_MPK_1	1
44-47	SCN_MPK_2	1
48-49	SCN_MPK_3	1

Table 21
Default route table

	Default Routes			
Alias Type	H323-ID	Cost Factor	H323-ID	Cost Factor
publicNumber.internationalNumber	INTN_GW_1	1	INTN_GW_2	2
privateNumber.level1RegionalNumber	PRIV_GW	1		

Table 22
Endpoint Status Table

H323-ID	IP
BCM_BVW_1	
SCN_MPK_1	47.82.33.47
SCN_MPK_2	47.82.33.50
SCN_MPK_3	
INTN_GW_1	
INTN_GW_2	47.50.10.20
ITG_GAL_1	47.85.2.201
PRIV_GW	

Stand-alone NRS support for Meridian 1 and BCM nodes

Nortel supports the use of an NRS for Meridian 1 Release 25.40 and Business Communications Manager (BCM) 3.6 nodes using H.323 endpoints that use use IP Trunk 3.0 (or later).

The NRS in a stand-alone configuration can be used to migrate numbering plans from node-based numbering plans to centralized NRS-based numbering plans. This provides increased functionality as well as the flexibility to migrate a traditional Meridian 1 or BCM-based network to a CS 1000 network.

To illustrate how the NRS fits into a Meridian 1/BCM network using IP Trunks, it is useful to first look at how the Meridian1/BCM handles call admission control and numbering plan resolution.

Meridian 1/BCM node-based numbering plan

Figure 80 illustrates how the Meridian1/BCM handles call admission control and numbering plan resolution.

Figure 80
Meridian 1/BCM node-based numbering plan

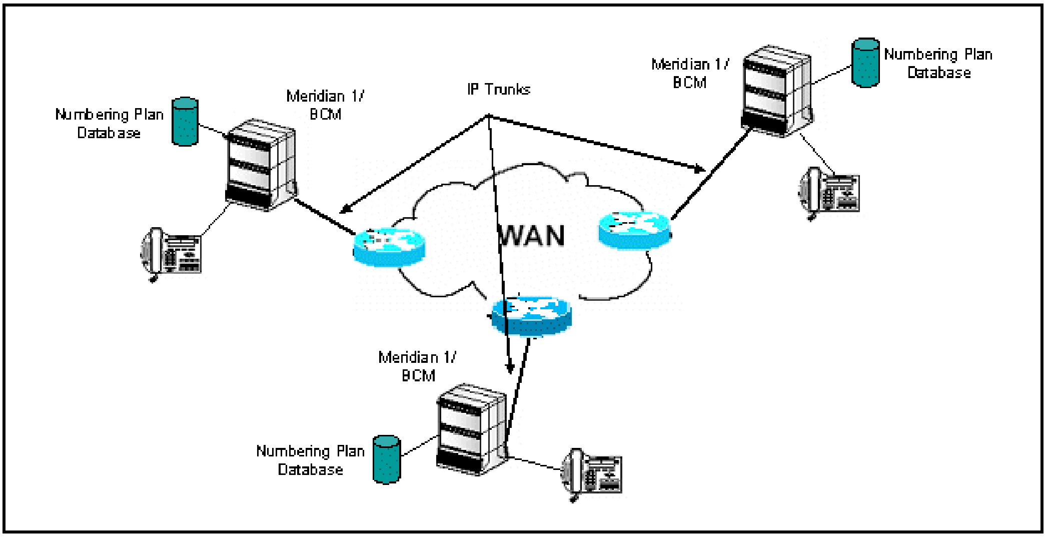


Figure 80 shows a Meridian 1/BCM network with the Meridian 1/BCM nodes equipped with IP Trunks. The IP Trunk routes are point-to-multipoint. Regardless of where the terminating node is located, all calls can be sent out over the same route. The calls can be routed to the correct destination over the packet-based IP network by the IP Trunk.

Every IP Trunk node in the network has its own numbering plan database. All IP Trunk nodes are configured with the following:

- The static IP address of every other IP Trunk node on the network.
- The numbering plan to route calls to the correct destination node.

When the Meridian 1/BCM wishes to make an IP Trunk call, the following occurs:

1 The node consults its numbering plan.

2 The node determines where the destination is located.

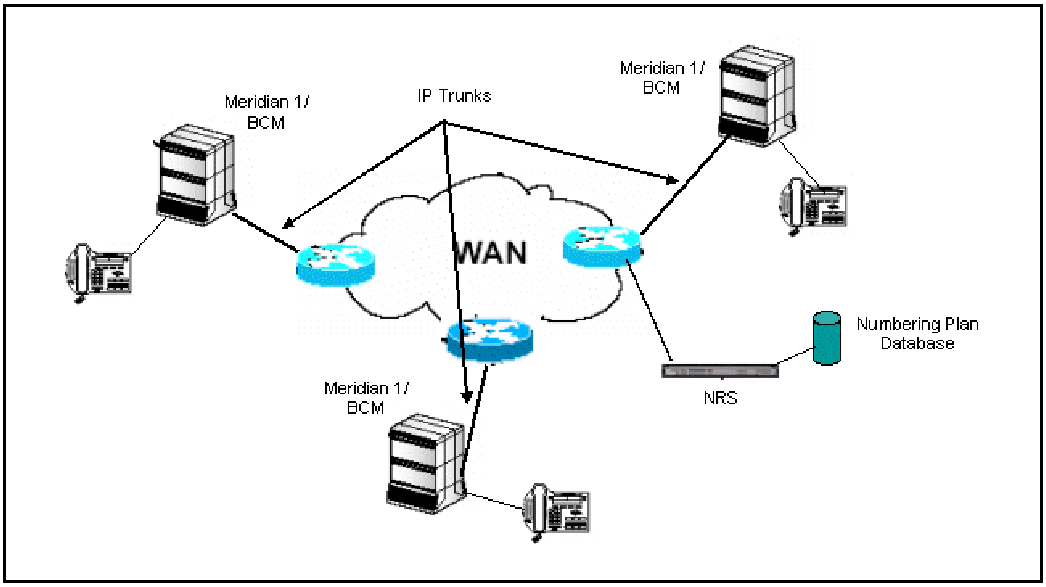
3 The node retrieves the statically configured destination IP address.

4 The node routes the call directly to the destination node.

NRS-based numbering plan

In a Meridian 1/BCM network running IP Trunks and a stand-alone NRS, the network numbering plan is centrally administered by the NRS, as shown in Figure 81.

Figure 81
NRS-based numbering plan



The NRS is configured with numbering plan information for every Meridian 1/BCM node in the network zone.

The typical Meridian 1/BCM network is configured to use H.323 Gatekeeper Resolved signaling. With H.323 Gatekeeper Resolved signaling, the H.323 Gatekeeper provides address resolution; however, call setup is performed directly between the nodes.

When a node wishes to place an IP call to another IP Trunk-enabled node, the originating node looks at its internal dialing plan table for address translation. If the originating node cannot find a match, it then sends ARQ (Admission Request) to the H.323 Gatekeeper specifying the destination phone number. When configured to use H.323 Gatekeeper, the node automatically sends the ARQ to the H.323 Gatekeeper. The H.323 Gatekeeper consults its internal numbering plan database and determines which Meridian 1/BCM node is the correct destination node. The H.323 Gatekeeper then sends an Admission Confirm (ACF) to the call originator and includes addressing information for the destination node. Standard call setup is then performed between the two nodes.

Numbering plan information is stored centrally on the NRS for the entire network zone which greatly reduces the administrative overhead.

> ***Note:*** For customers using a stand-alone NRS, note that QoS Fallback to PSTN is not supported for IP Trunk destination nodes whose called telephone numbers are resolved by the NRS. Meridian 1 IP Trunk nodes that must use QoS Fallback to PSTN must continue to use the node-based dialing plan table entries to resolve each other's telephone numbers. NRS number resolution can be used concurrently for any IP Trunk destination nodes that do not use QoS Fallback to PSTN.
>
> In order to eliminate a single point of failure in their network, Nortel recommends the deployment of both a Primary and an Alternate NRS.

Numbering plans

Contents

This section contains information on the following topics:

Introduction

When configuring a CS 1000 network, several numbering plans can be used. The numbering plan depends on customer preferences for dialing and configuration management requirements.

> ***Note:*** The numbering plan information required for the Call Server software to internally route calls, such as routing information for locally accessible numbers, must be configured within each Call Server.

“Numbering plan entry overview” on page 268 describes the implementation of the numbering plans. The sections below describe the following types according to their use:

- Uniform Dialing Plan
  - North American Numbering Plan
  - Flexible Numbering Plan
- Coordinated Dialing Plan
  - Transferable Directory Number
  - Group Dialing Plan
- Vacant Number Routing
- Special Numbering Plan

Private (on-net) numbering plans

Private (on-net) dialing refers to the dialing situations that occur when dialing telephones located within a local (private) network.

Uniform Dialing Plan

A Uniform Dialing Plan (UDP) enables users to dial all calls in a uniform manner, regardless of the location of the calling party or the route that the call takes. When using a Uniform Dialing Plan (UDP) to address private numbers, each location is assigned a Location Code (LOC). Each telephone has a Directory Number (DN) that is unique within the Call Server (and Customer).

To reach a user, you must know the user’s Location Code and DN. To reach an on-net location, the user dials the following:

Network Access Code (AC1 or AC2) + LOC + DN

For example, if:

- Network Access Code (AC1 or AC2) = 6
- LOC = 343
- DN = 2222

The user dials: 6 343 2222

The NRS must keep the Home Location (HLOC) code of every Gateway that is registered for UDP routing. To route a call, the Gateway passes the LOC and DN to the NRS to determine the IP addressing information of the desired Gateway. The NRS searches for the LOC within its database and returns the IP addressing information for the site. Then, the Gateway software can directly set up a call to the desired Gateway.

For more information on UDP, refer to *Basic Network Features* (553-3001-379).

For call routing information, see “UDP call-routing operation” on page 278.

Coordinated Dialing Plan

With a Coordinated Dialing Plan (CDP), each location is allocated one or more Steering Codes that are unique within a CDP domain. Steering Codes are configured within a dialing plan and are part of the DN itself. They route calls on the network by a DN translator. The NRS has a list of Distant Steering Codes to route a call, while the Call Server has a list of Local Steering Codes, which act like an HLOC.

Steering Codes enable you to reach DNs on a number of Call Servers with a short dialing sequence. Each user’s DN (including the Steering Code) must be unique within the CDP domain.

For example, a number of Call Servers can be coordinated so that five-digit dialing can be performed within a campus environment. For example:

- **Call Server A:** Steering codes 3 and 4 (that is, DNs in the range 3xxxx and 4xxxx)
- **Call Server B:** Steering code 5 (that is, DNs in the range 5xxxx)

Within this group of Call Servers, users can reach each other by dialing their unique DNs. However, all DNs on Call Server A must be in the range 3xxxx or 4xxxx, whereas all DNs on Call Server B must be in the range 5xxxx.

> ***Note:*** If a user moves from one Call Server to another, the user's DN must change in the CDP numbering plan (see "Transferable Directory Number" on page 259).

You can use CDP in conjunction with UDP. You use UDP by dialing AC1 or AC2 to reach UDP Location Codes, but use CDP by dialing CDP DNs within a CDP domain.

For a detailed description, refer to *Dialing Plans: Description* (553-3001-183).

For call routing, see "CDP call routing operation" on page 276.

Group Dialing Plan

Group Dialing Plan (GDP) enables coordinated dialing within a network using LOCs. Each group is assigned a LOC. From outside the group, you must dial the LOC as a prefix to the group CDP. In this case, the telephone's dialed number can be different when dialed from different locations.

For example, if:

- Network Access Code (AC1 or AC2) = 6
- LOC = 343
- DN = 3861

The user dials: 6 343 3861 from anywhere on the network, or the user dials only the DN (3861) from within the same CDP group.

Group Dialing Plans are part of Flexible Numbering Plans. For more detailed information, refer to *Dialing Plans: Description* (553-3001-183).

Transferable Directory Number

With Transferable Directory Numbers, each user is provided with a unique DN that does not change if the user moves to a different Call Server. The NRS must keep track of each Transferable Directory Number in the network so that it knows which Gateway(s) to return when asked to resolve a Transferable Directory Number address.

For call routing information, see “Transferable DN call routing operation” on page 274.

Vacant Number Routing

Vacant Number Routing (VNR) is supported in order to keep the Transferable Numbering Plan at a manageable level. As a result, small sites, such as the branch office, require minimal configuration to route calls through other Call Servers or through the NRS. Instead of changing the numbering trees and steering codes at each location, all the routing information can be kept at one central location.

If a vacant number is dialed, the call is routed to the NRS. The NRS decides where the terminal is located. If the terminal cannot be located, then vacant number treatment at the terminating location is given. The DN is not treated as invalid at the location where vacant number dialing is in effect.

Vacant Number Routing must be configured on the Media Gateway 1000B (MG 1000B) Core Small System Controller (SSC). Refer to *Branch Office: Installation and Configuration* (553-3001-214) for more information.

VNR enables data manipulation index (DMI) numbers for all trunk types so that an alternate route can be used for the VNR route. The VNR enhancement increases the flexible length of UDP digits from 10 to 19 and as a result, international calls can be made.

Based on the analysis of the dialed digits sets, TON/NPI for Virtual Trunk calls removes the NARS access code and the national or international prefix (dialed after NARS access code) so the NRS can route the call correctly.

This process minimizes the configuration on the branch office. Only CDB NET data must be defined on the originating node (the branch office). There is no need to define NET data (in LD 90) and all UDP calls (International, National, NXX LOC) are working using VNR route.

> ***Note:*** LOC and NXX must use different NARS access codes. That is, if LOC is using AC2 then NXX must be defined for AC1. When defining CDB, you must only define dialing plans which use AC2. All others default to use AC1.

For more information on the VNR enhancement, refer to page 358.

Public (off-net) numbering plans

Public (off-net) dialing refers to dialing situations that occur when dialing a telephone that is not part of the local (private) network.

Uniform Dialing Plan

An off-net call using UDP is a call that does not terminate within the local (private) network; although, some on-net facilities can be used to complete a portion of the call routing. UDP uses network translators AC1 and AC2 to route calls. UDP uses Special Numbers (SPNs) to enable users to dial numbers of varying lengths.

For example, a UDP call is considered off-net if a user at LOC 343 dials the following:

AC1 or AC2 +1 + NPA +NXX + XXXX

For example, if:

- Network Access Code (AC1 or AC2) = 6
- NPA = 416
- NXX = 475
- XXXX = 7517

The user dials: 6 + 1 (416) 475-7517.

For call routing information, see “UDP call-routing operation” on page 278.

North American Numbering Plan

The Call Server supports North American Numbering Plan routing. The North American Numbering Plan is used to make North American public network calls through the private network. The North American Numbering Plan accommodates dialing plans based on a fixed number of digits. A user can dial AC1 or AC2 + NXX + XXXX for local calls or AC1 or AC2 + 1 + NPA + NXX + XXXX for toll calls.

For example, if:

- Network Access Code (AC1 or AC2) = 9
- NPA = 506
- NXX = 755
- XXXX = 8518

The user dials: 9 + 1 (506) 755-8518

Flexible Numbering Plan

Flexible Numbering Plan (FNP) accommodates dialing plans that are not based on a fixed number of digits (for example, International numbers). FNP uses SPNs to enable users to dial numbers of varying lengths. Also, the total number of digits dialed to reach a station can vary from station to station. FNP also enables flexibility for the length of location codes from node to node. An FNP can be used to support country-specific dialing plans. For example, to reach an international number from North America, a user can dial: AC1 or AC2 + 011 + Country Code + City Code + XXXXXX.

For example, if:

- Network Access Code (AC1 or AC2) = 9
- Country Code = 33
- City Code = 1
- XXXXXX = 331765

The user dials: 9 + 011 + 33 + 1 + 331765

For information on FNP operation and package dependencies, refer to *Dialing Plans: Description* (553-3001-183).

Special Numbering Plan

SPNs exist for each country's dialing plan. In North America, the recognizable SPNs are 411, 611, 0, and 011 for international calling. The circuit switch or NRS recognizes the digits that are not part of, or do not comply with, the regular dialing plan, such that further dialing-string analysis is rarely possible (this is referred to as a catch-all configuration).

Europe uses SPN dialing plans almost exclusively, because European numbering plans are not as rigid as North American plans.

Address translation and call routing

H.323

When an H.323-compliant entity on the network wants to place a call, it sends an admission request (ARQ) to the H.323 Gatekeeper. The endpoint includes the destination telephony number in this message. The destination information is an H.323 alias. The H.323 Gatekeeper extracts the destination alias and ensures that it is one of the supported types. The H.323 Gatekeeper then searches its numbering plan database to determine which endpoints on the network can terminate the telephone number and whether or not these endpoints are registered. The H.323 Gatekeeper returns the IP address of any endpoints which can terminate this number and are registered to the endpoint.

> ***Note:*** Endpoints that do not support RAS messaging do not register with the H.323 Gatekeeper.

SIP

When a SIP-compliant entity on the network wants to place a call, it sends an INVITE message to the SIP Redirect Server by way of the SIP Trunk Gateway. The endpoint includes the destination telephony number in this message. The destination information is a SIP URI (see “SIP Uniform Resource Identifiers” on page 215). The SIP Redirect Server searches its numbering plan database to determine which endpoints on the network can terminate the telephone number and whether or not these endpoints are registered. Address lookup is based on the digits, phone context, and domain name.

The SIP Redirect Server returns the IP address of any endpoints that can terminate this number and that are registered to the endpoint.

Basic call routing

The routing of calls within the CS 1000 networks depends on the type of numbering plan in use and the number dialed. "Transferable DN call routing operation" on page 274 provides a description of how a call is routed from the call originator to the desired desktop or PSTN using the Transferable DN type of numbering plan. This is the most flexible numbering plan. It illustrates the configuration and operation of the routing software. The operation for "Private (on-net) numbering plans" on page 256 and "Public (off-net) numbering plans" on page 260 are described in "Numbering plans and routing" on page 272.

The NRS plays a key role in configuring numbering plans in a network. It provides IP address resolution based on dialed numbers.

Supported alias types (for H.323)

The H.323 Gatekeeper performs address translations on H.323 partyNumber alias types and on E.164 alias types. The partyNumber alias can be one of several subtypes according to the H.323 standard. The only partyNumber subtypes that the H.323 Gatekeeper supports are partyNumber.publicNumber and partyNumber.privateNumber. These also have subtypes. See Table 23.

Table 23
H.323 term explanations (Part 1 of 2)

H.323 signaling protocol	CS 1000 term
publicNumber.internationalNumber (Note 1)	E.164 International (UDP)
publicNumber.nationalNumber (Note 1)	E.164 National (UDP)
publicNumber.subscriber	See Note 2.

Table 23
H.323 term explanations (Part 2 of 2)

H.323 signaling protocol	CS 1000 term
publicNumber.unknown	See Note 3.
privateNumber.level1RegionalNumber (Note 1)	Uniform Dialing Plan Location Code (UDP LOC)
privateNumber.pISNSpecificNumber (Note 1)	Special Numbers (SPN)
privateNumber.localNumber (Note 1)	Coordinated Dialing Plan (CDP)
privateNumber.unknown	Unknown (UKWN) (Note 4)
e164	See Note 5.
Note 1: Only these alias types can be entered as numbering plan table entries using the web browser interface. The other alias types have no Type Of Number (TON) information.	
Note 2: Not supported by the H.323 Gatekeeper. The Call Server algorithmically converts any public subscriber number to a supported type (for example, converts a publicNumber.internationalNumber by adding the country code and area code).	
Note 3: Not supported by the Call Server, but is supported by the H.323 Gatekeeper for third-party interoperability. This is treated as a publicNumber.internationalNumber.	
Note 4: Not supported by the Call Server, but is supported by the NRS for third-party interoperability. The Call Server can generate privateNumber.unknown types with the limitation that INAC does not work. The NRS attempts to convert the number to privateNumber.localNumber (that is, CDP) or privateNumber.level1RegionalNumber (that is, UDP LOC) by analyzing the digits. If the NRS cannot determine which type to use based on digit analysis, it assumes that privateNumber.localNumber (that is, CDP) should be used.	
Note 5: Not supported by the Call Server, but is supported by the NRS for third-party interoperability. A default prefix can be configured on a per-NRS basis to distinguish between public and private numbers. For example, a prefix of “9” can be configured as the public number prefix. A prefix of “6” can be configured as the private default prefix. The NRS looks at the first digit. If it matches the public prefix (for example, “9”), it treats the subsequent digits as a publicNumber.internationalNumber. If the first digit matches the private prefix (for example, “6”), it treats the subsequent digits as a privateNumber.localNumber (that is, CDP) or privateNumber.level1RegionalNumber (that is, UDP LOC), depending on its digit examination.	

If the H.323 Gatekeeper receives an admission-request message requesting translation for any other alias type (for example, publicNumber.subscriberNumber), it rejects the request.

The H.323 Proxy Server, which sends the admission request to the H.323 Gatekeeper, is responsible for mapping Numbering Plan Indicator (NPI)/ Type of Number (TON) values in the ISDN SETUP Called Party Number Information Element to one of the eight H.323 alias types listed in Table 23 on page 263.

Mapping between CS 1000 NPI/TON and H.323 alias types

The CS 1000 system supports the NPI and TON values shown in Table 24 and Table 25. These values are for Universal ISDN Protocol Engine (UIPE)-formatted NPI/TON numbers.

Table 24
NPI values

NPI on Call Server	UIPE-formatted description
0	UNKNOWN
1	E164
2	PRIVATE
3	E163

Table 25
TON values (Part 1 of 2)

TON	UIPE-formatted description
0	UNKNOWN
1	INTERNATIONAL
2	NATIONAL
3	SPECIAL
4	SUBSCRIBER

Table 25
TON values (Part 2 of 2)

TON	UIPE-formatted description
5	UNIFIED (UDP location code).
6	COORDINATED (CDP distant/trunk steering code)
Note: The H.323 Gatekeeper sees a trunk steering code as privateNumber.unknown. The H.323 Gatekeeper then converts the code to privateNumber.localNumber in CDP.	

Table 26 shows the NPI/TON pairs, the corresponding call types, and their corresponding H.323 alias types for which the H.323 Gatekeeper accepts translation requests. The call type for outgoing routes is manipulated by configuring a DMI in LD 86 and specifying the Call Type (CTYP).

If the H.323 Proxy Server receives a Q.931 SETUP message for an NPI/TON pair not included in Table 26, it must map the number according to one of the NPI/TON pairs/H.323 alias types which the H.323 Gatekeeper supports. This process can require modifications to the called number dialing string.

CTYP is the mnemonic in the ESN overlays.

Table 26
NPI/TON to H.323 alias mapping (Part 1 of 2)

NPI UIPE	TON UIPE	CTYP	H.323 alias
E164 or E163	INTERNATIONAL	INTL	publicNumber.internationalNumber
	NATIONAL	NPA	publicNumber.nationalNumber
	UNKNOWN		publicNumber.unknown

Table 26
NPI/TON to H.323 alias mapping (Part 2 of 2)

NPI UIPE	TON UIPE	CTYP	H.323 alias
PRIVATE	SPECIAL	SPN	privateNumber.pISNSpecificNumber
	UNIFIED (see Table 25 on page 265)	LOC	privateNumber.level1RegionalNumber
	COORDINATED (see Table 25 on page 265)	CDP	privateNumber.localNumber
	UNKNOWN	UKWN	privateNumber.unknown

The endpoints must correctly map the UIPE NPI/TON pairs to a valid partyNumber type that the H.323 Gatekeeper supports. The administrator must coordinate the numbering plan on the H.323 Gatekeeper with the mapping carried out by the endpoints.

LD 96 shows NPI/TON and ESN call types for D-channel monitoring. Calling and Called number information for level 0 D-channel tracing includes the TON and ESN call types.

Table 27 shows Q.931 TON mapping.

Table 27
Q.931 TON mapping (Part 1 of 2)

NPI	TON
x000xxxx	Unknown
x001xxxx	International Number
x010xxxx	National Number
x011xxxx	Network Specific Number
x100xxxx	Subscriber Number

Table 27
Q.931 TON mapping (Part 2 of 2)

NPI	TON
x110xxxx	Abbreviated Number
x101xxxx x111xxxx	Reserved for Extension

Table 28 shows the NPI/TON to ESN Call type mapping.

Table 28
NPI/TON to ESN Call type mapping

NPI	TON	ESN
0001 - E.164	010 - National	NPA
0001 - E.164	100 - Subscriber	NXX
1001 - PRIVATE	011 - Network Specific	SPN
1001 - PRIVATE	101 - Reserved	LOC
1001 - PRIVATE	110 - Abbreviated	CDP

Numbering plan entry overview

A numbering plan entry can be private or public. Private numbers can be configured using CDP, or UDP Location Code (LOC) entries. Public numbers can be configured using E.164 International or E.164 National entries.

When configuring a predefined endpoint on the NRS, the administrator must add the required numbering plan entries. The administrator adds the numbers or number ranges that the endpoint can terminate. For every numbering plan entry, the administrator must specify the DN type, the default route, the DN prefix, and the cost factor associated with the route. See “Adding a Routing Entry” on page 432.

Using the cost factor to determine the entry or the path and endpoint, the NRS can match multiple entries to a dialed number. This enables alternate routing based on the cost of facilities. The NRS matches the number string with the most matching digits. For example, the following are defined as entries:

- 1613
- 161396
- 1613967

If a user dials “1613966”, the NRS matches entries with “161396”. See Table 29 for the cost factors associated with these entries.

Table 29
Cost factors

Entry	Cost factor
1613	1
161396	1
161396	2
1613967	1

In this case, the NRS first returns the entries with the lowest cost entry.

The administrator must also specify if the endpoint belongs to a CDP domain. If the endpoint does belong to a CDP domain, the administrator must specify the CDP domain name. However, before specifying an endpoint’s CDP domain membership, the administrator must configure the CDP domain. The administrator does this by adding a new CDP domain and specifying its name. The alias type privateNumber.localNumber corresponds to a CDP number. When configuring a numbering plan entry for this alias type, the administrator must have previously specified the CDP domain to which the endpoint belongs.

Default endpoints can also be configured for each of the supported numbering plan types. These entries are configured by entering the DN type, the default route, the DN prefix, and their associated cost factors.

> *Note:* For alias type privateNumber.localNumber (for example, CDP numbers), multiple default routes for each CDP domain can be configured. Each CDP domain must have its own default routes.

The NRS has one standard numbering plan table for each of the publicNumber.internationalNumber (CTYP = INTERNATIONAL), privateNumber.pISNSpecificNumber (CTYP = COORDINATED), and privateNumber.level1RegionalNumber (CTYP = UNIFIED) supported alias types.

> *Note:* Although publicNumber.nationalNumber aliases can be configured, there is no numbering plan table associated with this alias type, as these aliases are inserted in the publicNumber.internationalNumber table.

The NRS also has one numbering plan table for each CDP domain configured. Therefore, there are multiple numbering plan tables configured for the privateNumber.localNumber alias type. Each table contains lists of numbering plan entries with each entry containing the following information:

- leading digit string
- cost factor associated with the route to this endpoint

The NRS has a table for each of the standard alias types (internationalNumber.pISNSpecificNumber and level1RegionalNumber) which provides the default routes associated with each type. The tables contain the H323-ID of the default routes or the IP address if the default route does not support RAS procedures and the cost factor associated with the route. There is also a table of default routes for each CDP domain.

Number Type support

The NRS enables address-translation requests for publicNumber.nationalNumber and publicNumber.internationalNumber types. The NRS can be used for address translation across several countries; therefore, the NRS must be able to identify from which country the request came. The NRS must also be able to handle country codes correctly.

A system-wide configuration variable specifies the default country code. For example, this variable could be configured as “1” if the majority of the NRS traffic is within North America. There is also the option to configure a country code for every endpoint that overrides the default system-wide country code. For example, if one CS 1000 node is in Galway, Ireland and all other nodes are in North America, the default system-wide country code could be configured as "1" and the country code for the node in Galway could be configured as "353".

When configuring numbering plan table entries, the administrator can configure national number entries. When configuring a national number entry, either the system-wide country code or the endpoint-specific country code must be configured first. The NRS automatically prefixes the national numbering plan entry with the country code and then inserts this entry in the international numbering plan table. No table exists for national numbers. All national numbers are converted to international. When the NRS receives an admission request for a national number, the NRS determines the originator of the request, extracts the destination telephony number, prefixes the number with the relevant country code (either the country code for the endpoint or the system-wide country code), and resolves the number by searching in the international number table.

Note that the numbering plan entries in the NRS conform strictly to the E.164 International standard. Calls on Virtual Trunks that access the NRS must be tagged correctly.

For example, an endpoint can make an international call to 1-416-xxxxxxx. If this digit sequence is sent to the NRS, it must have a Call Type of "International", because the country Code ("1") is included. The same endpoint can make a call to 416-xxxxxxx, but in this case the Call Type must be "National", because the country code is not included. Both of these scenarios work correctly, as the NRS is set up to process both 416/National and 1416/International.

However, it is not valid to send digits 1-416-xxxxxx with a Call Type of "National"; the NRS cannot recognize this, and the call is not routed.

Numbering plans and routing

When users attempt to make calls on a CS 1000 system, they use dialed digits to indicate which telephone or service they would like to reach. Within the Call Server, these digits are translated to determine whether the user is attempting to reach an internal telephone or service, or trying to reach another user or service outside of the CS 1000 system. This is the first level of routing.

If the user is trying to reach a device that is internal to the CS 1000 system, the Call Server terminates the call as appropriate on the internal device. If the user is trying to reach a device outside the CS 1000 system, several options can be configured within the system.

The system administrator can choose to use one of the PBX Networking numbering plans, such as CDP, to help route the call to the appropriate trunk route, or the administrator can choose to use Vacant Number Routing (VNR), where any number that is not known to the Call Server is routed out a specified trunk route. An NRS can therefore determine the final destination of the call from a central database.

Refer to *Dialing Plans: Description* (553-3001-183) for information on VNR operation.

Using an NRS for routing

Once the system determines that a user is attempting to reach a telephone or service using the IP network, the call is routed to the Gateway software, which uses the NRS to help with the routing of the call.

The basic role of an H.323 Gatekeeper is to perform address translation from an alias (in this case, a telephone number) to an IP signaling address, and to authorize the call in the H.323 network.

The basic role of a SIP Redirect Server is to perform address translation from a SIP URI to an IP signaling address and to authorize the call in the SIP network.

The NRS is the central location where the numbering plan information is configured. The identity of each endpoint (for example, a CS 1000 system) is configured in the NRS with the numbers it can reach. For example, an entry could look like the following:

“Santa Clara-01”

PublicNumber = +1 408 XXX XXXX

PrivateNumber = Electronic Switched Network (ESN) 265 XXXX, ESN 655 XXXX

At power-up, an H.323 endpoint performs Gatekeeper Discovery using a configured H.323 Gatekeeper address. The endpoint then registers with its primary H.323 Gatekeeper at the address returned by the Gatekeeper Discovery process using the H.225.0 (RAS) protocol by sending its H323-ID and its IP address. In the example above, it would use the following:

“Santa_Clara-01”

Signaling IP address = 47.0.1.2

Upon receipt of the registration, the H.323 Gatekeeper matches the name “Santa_Clara-01” in the registration with the configured information in its database, and adds the IP address.

When a user behind an H.323 proxy wants to reach another user, its H.323 proxy sends a call request to its H.323 Gatekeeper. The H.323 Gatekeeper determines any endpoint(s) that are responsible for that particular user and returns its signaling IP address(es) in the direct-routed model, which is the preferred model.

Using the same example, the user dials “62653756”. The Call Server at the originating end determines that this call is destined to ESN 265 3756, based on the dialing prefix, and routes the call to the H.323 Gateway. The H.323 Gateway sends an admission request to the H.323 Gatekeeper for PrivateNumber ESN 265 3756. The H.323 Gatekeeper then consults its database and performs the closest match (that is, “ESN 265 XXXX” in the “Santa_Clara-01” entry) and returns the IP address that was previously provided by “Santa_Clara-01” at registration time (that is, 47.0.1.2).

Transferable DN call routing operation

With the Transferable Directory Number type of CDP numbering plan, networks provide the ability to enable users to move from location to location while retaining their Directory Number. This capability is provided by a combination of Network Management and the call routing capabilities of the Call Server software. The NRS must be updated to reflect the current location of the DNs.

> ***Note:*** Transferable Directory Numbers are usually used in conjunction with Vacant Number Routing (VNR).

Figure 82 on page 275 shows a network of CS 1000 Systems in which each user wants to retain their unique seven-digit Directory Number. Table 30 on page 275 provides a summary of the DNs in Figure 82, as well as their associated Call Server.

Each user in the network is associated with a Call Server and its group of SIP Trunk and/or H.323 Gateways. The Gateways provide call-processing features and redundancy. The NRS in Figure 82 on page 275 is aware of the location of any user with a given Directory Number within the network. In this case, the user with Directory Number 22221 is located at Call Server A. When a user dials the last digit of this number, their Call Server determines whether the user is within its local database, and if so, handles the call directly.

For example, if the user with Directory Number 22222 dials 22221, Call Server A handles the call directly.

However, if the Directory Number is not within the local database of the initial Call Server, the call is routed through the Gateway software on the Signaling Server in order to locate the user. This routing uses a feature called Network Number Resolution. Because the NRS knows where to locate any user with a Transferable Directory Number, it directs the call to the proper Call Server.

For example, if the user with DN 22224 dials DN 22221, Call Server B routes the call to the Gateway software, which requests the location of the desired Call Server from the NRS. The NRS responds with the address information of Call Server A, at which time Call Server B attempts a call setup to Call Server A and completes the call.

Figure 82
Transferable DN routing

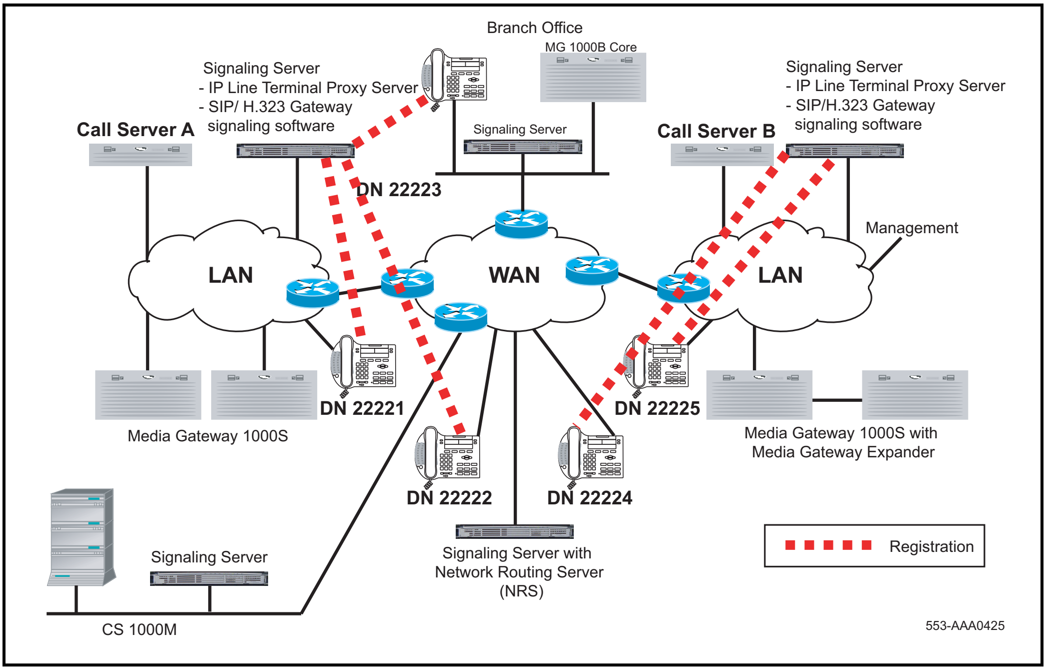


Table 30
DNs with their associated Call Servers (Part 1 of 2)

DN	Call Server
22221	A
22222	A
22223	A

Table 30
DNs with their associated Call Servers (Part 2 of 2)

DN	Call Server
22224	B
22225	B

CDP call routing operation

The routing of calls in a CDP-type of numbering plan is the same as that for Transferable Directory Number, with the following exceptions:

- Only the Steering Codes must be stored in the NRS, because entire ranges of DNs are located within the same Call Server.
- With CDP, Call Servers and MG 1000B platform systems can be grouped into CDP domains, all sharing a CDP. This enables more convenient number dialing within a complex, such as a campus with several Call Servers. When configuring CDP numbers at the NRS, administrators must also specify to which CDP domain they belong.

Figure 83 on page 277 shows an example of CDP routing. Table 31 on page 277 shows the DNs with their associated Call Servers and CDP domains.

Figure 83
CDP call routing

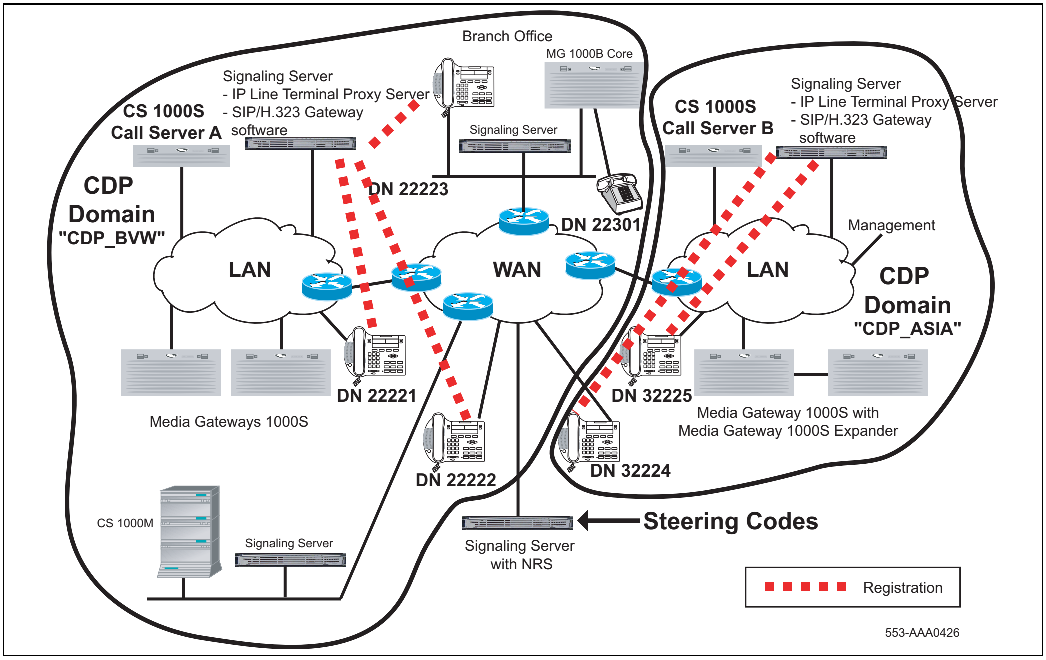


Table 31
DNs with their associated Call Servers and CDP domains

DN	Call Server	CDP domain
22221	A	“CDP_BVW”
22222	A	“CDP_BVW”
22223	A	“CDP_BVW”
22301	MG 1000B	“CDP_BVW”
32224	B	“CDP_ASIA”
32225	B	“CDP_ASIA”

UDP call-routing operation

The routing of calls in a UDP private numbering plan is basically the same as that for Transferable Directory Number, except that only the Location Codes must be stored in the NRS because the user uniquely identifies the specific location by dialing this code.

CDP and Transferable Directory Number numbering plans can coexist within the same network. The dialing of a network access code (AC1 or AC2) enables the Call Server to differentiate between calls that must be resolved using the UDP Type of Number (TON) and those that must be resolved using the CDP TON.

> ***Note:*** Transferable Directory Numbers are considered CDP numbers.

Off-net call routing operation

When dialing calls to PSTN interfaces, the Call Server determines that the call is destined off-net, based on digit analysis that must be configured at major Call Servers in the network. This determination enables the Gateway software to request the location of public E.164 numbers from the NRS. The NRS is configured with a list of potential “alternate routes” that can be used to reach a certain number, each of which is configured with a Cost Factor to help determine the least-cost route for the call.

When an NRS replies to the Gateway with the address information for E.164 numbers, it provides a list of alternate gateways, sorted in order of cost. If a Gateway is busy when a call attempt is made, the originating Gateway tries the next alternative in the list. If none of the alternatives are available over the IP network, the originating Call Server can be configured to step to the next member of its route list, which could be a PSTN or TIE alternate route.

For example, in the event of an IP network outage that does not enable voice calls to terminate over the IP network, calls are rerouted to any alternate PSTN or TIE routes.

Routing to and from a branch office or SRG

Because IP Phone users can be located at a branch office equipped with an MG 1000B Core or SRG, the routing of calls to the local gateway is important (especially when toll charges are applicable to calls made from the central Call Server that is controlling the telephone). The administrator can configure digit manipulation for IP Phones that are located near an MG 1000B Core or SRG, selecting a gateway that provides PSTN access local to the telephone.

> ***Note:*** The Branch Office feature (which includes the SRG) supports the various PSTN interfaces. Refer to *Electronic Switched Network: Signaling and Transmission Guidelines* (553-3001-180) for further information.

Calls from the PSTN to users within the network can be routed either using the various ESN numbering plan configurations or using the Vacant Number Routing (VNR) feature. This process enables small sites, such as those using the MG 1000B Core, to require minimal configuration to route calls through other Call Servers or through the NRS.

Outgoing calls to access local PSTN resources can be routed using ESN, as well as zone parameters that enable digit insertion. The zone parameters enable calls made by a branch office or SRG user to be routed to the desired local PSTN facilities. Refer to *Branch Office: Installation and Configuration* (553-3001-214) for further information.

Configuring IP Peer Networking

Contents

This section contains information on the following topics:

Overview

You use the following interfaces for configuring various components of IP Peer Networking:

- CS 1000 Element Manager
- Command Line Interface (CLI)
- NRS Manager
- Optivity Telephony Manager (OTM)

  Note: You can use OTM to launch Element Manager. Refer to *Optivity Telephony Manager: System Administration* (553-3001-330) for detailed information on OTM.

This chapter provides instructions on how to implement IP Peer Networking in your IP network using overlays and Element Manager. Once you implement IP Peer, you must then configure data in the NRS, as described in "Configuring and managing the Network Routing Service" on page 379.

For information on how to install system components and how to perform basic configuration, refer to the following NTPs:

- *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210)
- *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)
- *Communication Server 1000S: Installation and Configuration* (553-3031-210)
- *Communication Server 1000E: Installation and Configuration* (553-3041-210)

For a description of system management, refer to *System Management* (553-3001-300). For a detailed description of Element Manager, refer to *Element Manager: System Administration* (553-3001-332).

Once you install the various components and configured the basic information, you then implement the IP Peer Networking feature. Implementing IP Peer Networking in a CS 1000 network is similar to configuring a traditional circuit-switched network that uses a "star" topology. All CS 1000 systems form the outer points of the star, with respect to address resolution (the systems form a grid with respect to media paths). These systems are configured to route network-wide calls into the IP network over a route configured with Virtual Trunks. The Virtual Trunks are configured to use the NRS. The NRS, in conjunction with the SIP/H.323 Gateway software at each site, acts as the center of the "star".

Element Manager and NRS Manager enable you to configure and maintain certain aspects of the system through a web browser.

> ***Note 1:*** Element Manager must be installed on each Signaling Server within the system.
>
> ***Note 2:*** Element Manager requires Internet Explorer 6.0 (or later).

In addition to Element Manager and NRS Manager, you can perform a number of configuration functions through the Command Line Interface (CLI). You can access the CLI from a serial port, or by using the Telnet or rlogin commands over a network connection.

You can also use OTM to access the web server running on the Signaling Server.

Task summary

You must configure the following data when setting up a IP network:

1 Plan your Network Numbering Plan. Refer to *Dialing Plans: Description* (553-3001-183).

   a Are you using Uniform Dialing Plan (UDP) or Coordinated Dialing Plan (CDP), or both?

   b Are you also using Group Dialing Plan (GDP), North American Numbering Plan (NANP), or Flexible Numbering Plan (FNP)?

2 Perform basic installation, setup, and configuration of the various components, including the Signaling Server. Refer to:

— *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210)

— *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)

— *Communication Server 1000S: Installation and Configuration* (553-3031-210)

— *Communication Server 1000E: Installation and Configuration* (553-3041-210)

— *Signaling Server: Installation and Configuration* (553-3001-212).

3 Configure the Primary, Alternate, and Failsafe NRS at installation and initial setup of the Signaling Server. See *Signaling Server: Installation and Configuration* (553-3001-212).

Note: The NRS requires IP telephony node configuration files. These files are installed and configured during the Signaling Server software installation (basic configuration step).

4 Configure the Customer Data Block with any desired networking settings and options, including ISDN. Use Element Manager or the Command Line Interface (LD 15). See "Configuring the Customer Data Block" on page 289 and "Feature Implementation of IP Peer Networking" on page 341.

5 Configure the D-channel using Element Manager or the Command Line Interface (LD 17). See"Configuring D-channels" on page 292 and "Feature Implementation of IP Peer Networking" on page 341.

6 Configure the zones.

7 Configure the SIP and/or H.323 Virtual Trunk routes using Element Manager or the Command Line Interface (LD 16). Configure the Route Data Blocks and associate the Virtual Trunk routes with the IP network by configuring the following parameters:

a route information

- **b** network management information (for example, Access Restrictions)
- **c** bandwidth zone
- **d** protocol identifier
- **e** associated Node ID

For the Element Manager procedure, see "Configuring the Virtual routes and trunks" on page 298. For the CLI procedure, see "Feature Implementation of IP Peer Networking" on page 341.

8 Configure the Virtual Trunks using Element Manager (see "Configuring the Virtual routes and trunks" on page 298) or the Command Line Interface (LD 14) and "Feature Implementation of IP Peer Networking" on page 341.

9 Use Element Manager or the Command Line Interface (CLI) to configure networking ("Configuring networking" on page 310) and numbering plan features ("Configuring call routing" on page 315) within the Call Server, such as routing calls based on digits dialed. For example, CDP configuration for the dialing plan used on the Call Server includes:

- **a** ESN control block basics (LD 86): configure the dialing plan
- **b** Network Control Block (LD 87): configure network access
- **c** Route List Block (LD 86): create an entry for Virtual Trunk route
- **d** Network Control Block (LD 15): enter CDP steering codes or UDP steering codes

10 Configure the codecs using Element Manager (see "Configuring codecs" on page 319).

11 Configure dialing plan information for calls that must be routed to circuit-switched trunks (for example, PSTN interfaces). See *Dialing Plans: Description* (553-3001-183) and *IP Trunk: Description, Installation, and Operation* (553-3001-363).

12 Configure the gateways. See"Configuring the Gateways" on page 364.

- — See"Enabling and configuring the H.323 Gateway" on page 364
- — "Enabling and configuring the SIP Trunk Gateway" on page 369

13 Configure the NRS. See “Configuring and managing the Network Routing Service” on page 379.

Launching Element Manager

To log in to Element Manager, follow the steps in Procedure 3. Element Manager supports Microsoft® Internet Explorer 6.0 (or later) for the Windows® operating systems.

Procedure 3
Launching Element Manager

1 Open the web browser.

2 Enter the **Signaling Server Node IP address** in the Address Bar of the browser window and press **Enter** on the keyboard.

Note: The ELAN network interface IP address may be required, instead of the Node IP address, to access to the Element Manager login web page in secure environments.

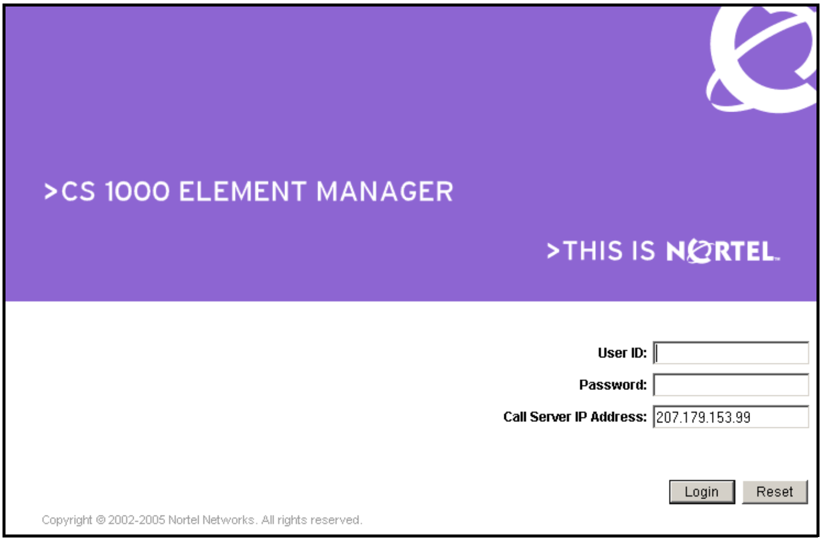
3 Element Manager launches and the **Login** web page opens (see Figure 84 on page 287).

a. Enter the **User ID** and **Password** of the Call Server.

The IP address of the Call Server is auto-filled in the **CS IP Address** field.

b. Click **Login**.

Figure 84
Element Manager – Login web page



User ID:

Password:

Call Server IP Address: 207.179.153.99

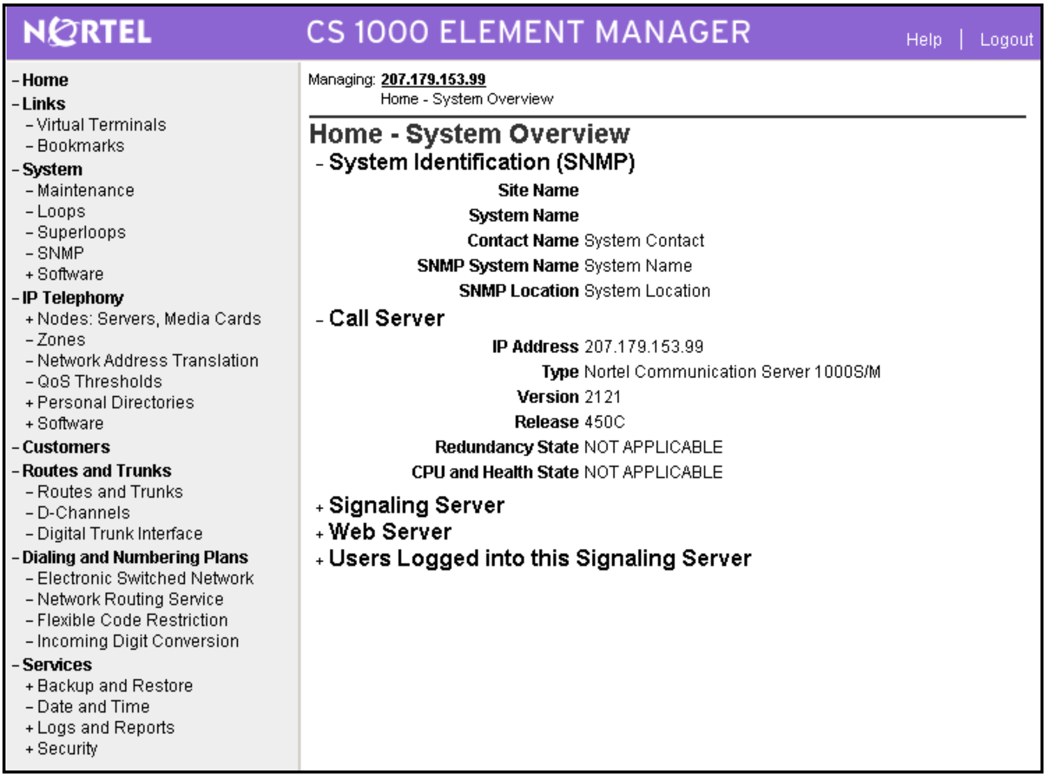
Copyright © 2002-2005 Nortel Networks. All rights reserved.

4 The **System Overview** web page opens (see Figure 85 on page 288).

The navigator is located on the left side of the browser window.

The **System Overview** web page contains information about the system. The web page shows that the Call Server is a central component of the system and also lists other components in the system.

Figure 85
Element Manager – System Overview



Managing: **207.179.153.99**
Home - System Overview

Home - System Overview

- System Identification (SNMP)

Site Name
System Name
Contact Name System Contact
SNMP System Name System Name
SNMP Location System Location

- Call Server

IP Address 207.179.153.99
Type Nortel Communication Server 1000S/M
Version 2121
Release 450C
Redundancy State NOT APPLICABLE
CPU and Health State NOT APPLICABLE

+ Signaling Server
+ Web Server
+ Users Logged into this Signaling Server

Note 1: To log out of Element Manager, click **Logout** at the right in the Element Manager banner at the top of any Element Manager web page (for example, see Figure 85 on page 288). The **Login** web page (see Figure 84 on page 287) is displayed again. If you need to log back in to Element Manager, repeat step 3 on page 286.

Note 2: Element Manager times out after a period of inactivity.

Users are logged out without any warning in all Element Manager web pages, with the exception of the **Edit** web page (see Figure 117 on page 321). When you are working in the Edit web page, a message opens that warns of the impending time-out action. Click **OK** (on the warning message) within the remaining time-out period (5 minutes) to reset the timer. If you do not respond within the 5 minute warning period, your session is canceled and you must log in again. Any data modifications made on screen, but not submitted to the system, are lost.

Note 3: For additional information about Element Manager, refer to the following NTPs:

— *Signaling Server: Installation and Configuration* (553-3001-212)

— *Element Manager: System Administration* (553-3001-332)

End of Procedure

Using Element Manager for configuration

Read the following sections and follow the procedures in the order given.

Configuring the Customer Data Block

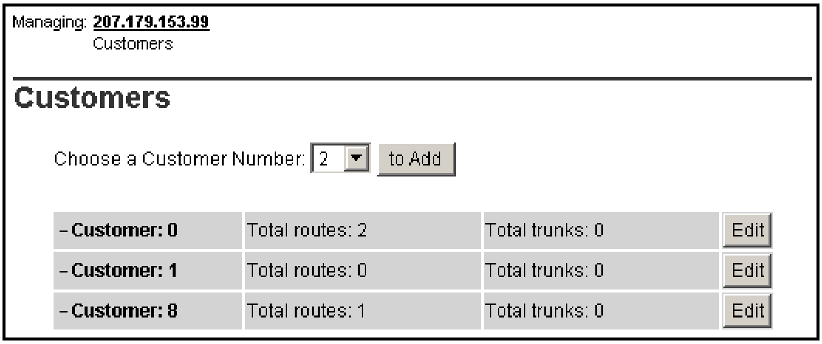
Procedure 4
Configuring the Customer Data Block and enabling ISDN

To configure the Customer Data Block with network settings and options, you can use Element Manager or LD 15 of the Command Line Interface.

1 Click **Customers** in the navigator.

The **Customers** web page opens (see Figure 86).

Figure 86
Customers web page



Managing: 207.179.153.99
Customers

Customers

Choose a Customer Number: 2 ▼ to Add

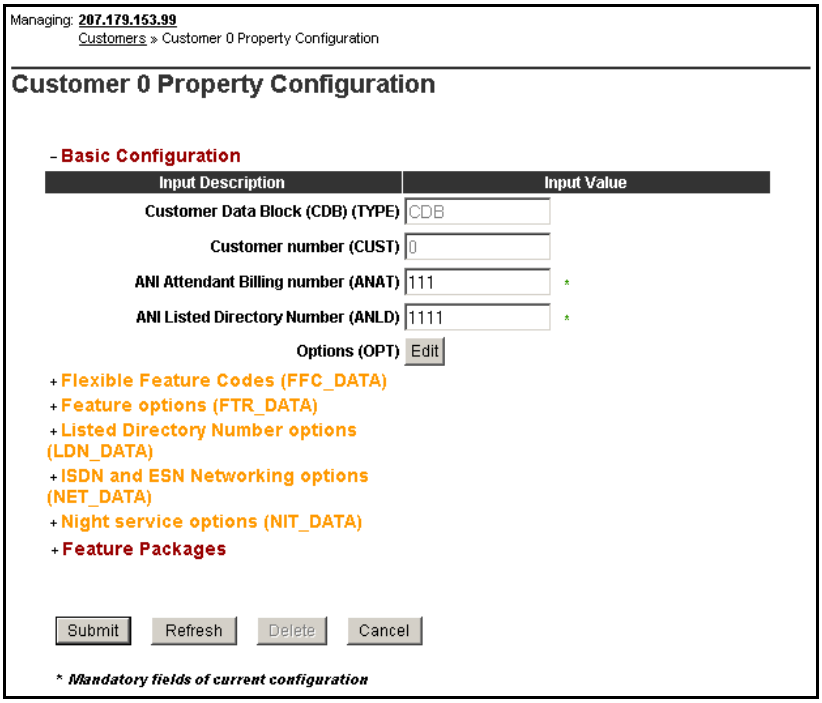
- Customer: 0	Total routes: 2	Total trunks: 0	Edit
- Customer: 1	Total routes: 0	Total trunks: 0	Edit
- Customer: 8	Total routes: 1	Total trunks: 0	Edit

2 Click **Edit** associated with the customer (not the route) to open the **Customer xx Property Configuration** web page, where xx is the Customer number.

Figure 87 on page 290 shows the **Customer xx Property Configuration** web page.

Use the **Customer Property Configuration** web page to configure Customer data.

Figure 87
Customer xx Property Configuration web page



Managing: 207.179.153.99
Customers » Customer 0 Property Configuration

Customer 0 Property Configuration

- Basic Configuration

Input Description	Input Value	
Customer Data Block (CDB) (TYPE)	CDB	
Customer number (CUST)	0	
ANI Attendant Billing number (ANAT)	111	*
ANI Listed Directory Number (ANLD)	1111	*
Options (OPT)	Edit	

+ Flexible Feature Codes (FFC_DATA)
+ Feature options (FTR_DATA)
+ Listed Directory Number options (LDN_DATA)
+ ISDN and ESN Networking options (NET_DATA)
+ Night service options (NIT_DATA)
+ Feature Packages
Submit
Refresh
Delete
Cancel

* *Mandatory fields of current configuration*

3 Click **Feature Packages**.

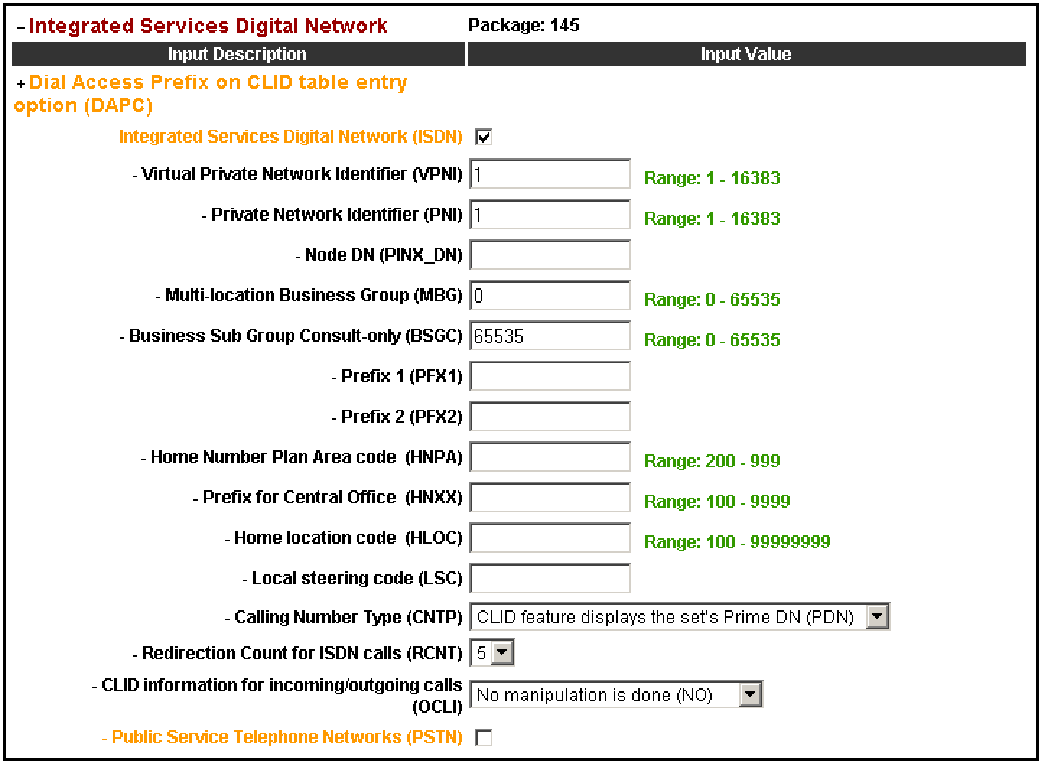
The Feature Packages list expands.

4 Scroll down the page and select **Integrated Services Digital Network Package:145**.

5 Click **Integrated Services Digital Network (ISDN)**.

The ISDN list expands to show the ISDN package options, as shown in Figure 88.

Figure 88
ISDN package options



– Integrated Services Digital Network Package: 145

Input Description	Input Value	
+ Dial Access Prefix on CLID table entry option (DAPC)		
Integrated Services Digital Network (ISDN)	☑	
- Virtual Private Network Identifier (VPNI)	1	Range: 1 - 16383
- Private Network Identifier (PNI)	1	Range: 1 - 16383
- Node DN (PINX_DN)		
- Multi-location Business Group (MBG)	0	Range: 0 - 65535
- Business Sub Group Consult-only (BSGC)	65535	Range: 0 - 65535
- Prefix 1 (PFX1)		
- Prefix 2 (PFX2)		
- Home Number Plan Area code (HNPA)		Range: 200 - 999
- Prefix for Central Office (HNXX)		Range: 100 - 9999
- Home location code (HLOC)		Range: 100 - 99999999
- Local steering code (LSC)		
- Calling Number Type (CNTP)	CLID feature displays the set's Prime DN (PDN)	
- Redirection Count for ISDN calls (RCNT)	5	
- CLID information for incoming/outgoing calls (OCLI)	No manipulation is done (NO)	
- Public Service Telephone Networks (PSTN)	□	

6 Scroll to the bottom of the page and click **Submit**.

End of Procedure

Configuring D-channels

Procedure 5
Configuring D-channels

To configure D-channels, use Element Manager or LD 17 of the Command Line Interface.

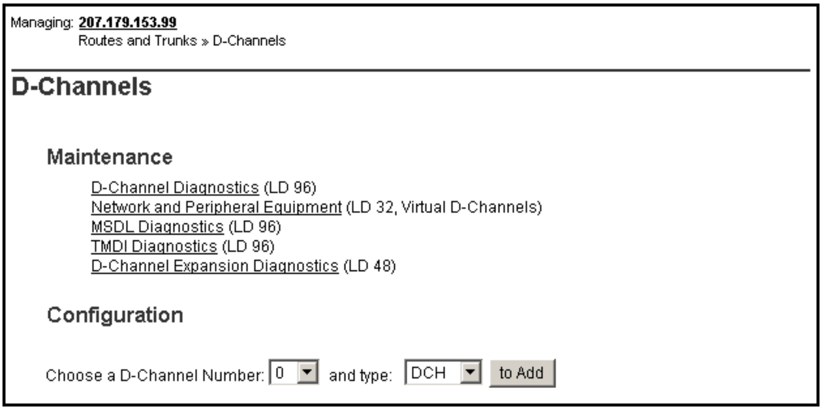
Figure 89 on page 292 and Figure 90 on page 293 show the **D-Channel Configuration** web pages in Element Manager. Use these web pages to configure D-channels.

1 Select **Routes and Trunks > D-Channels** from the navigator.

Note: The first time you access this web page, a message indicates that no D-channels have been configured.

The **D-Channels** web page opens as shown in Figure 89. This window also contains links to D-Channel maintenance and diagnostic pages.

Figure 89
D-Channels web page



Managing: 207.179.153.99
Routes and Trunks » D-Channels

D-Channels

Maintenance

D-Channel Diagnostics (LD 96)
Network and Peripheral Equipment (LD 32, Virtual D-Channels)
MSDL Diagnostics (LD 96)
TMDI Diagnostics (LD 96)
D-Channel Expansion Diagnostics (LD 48)

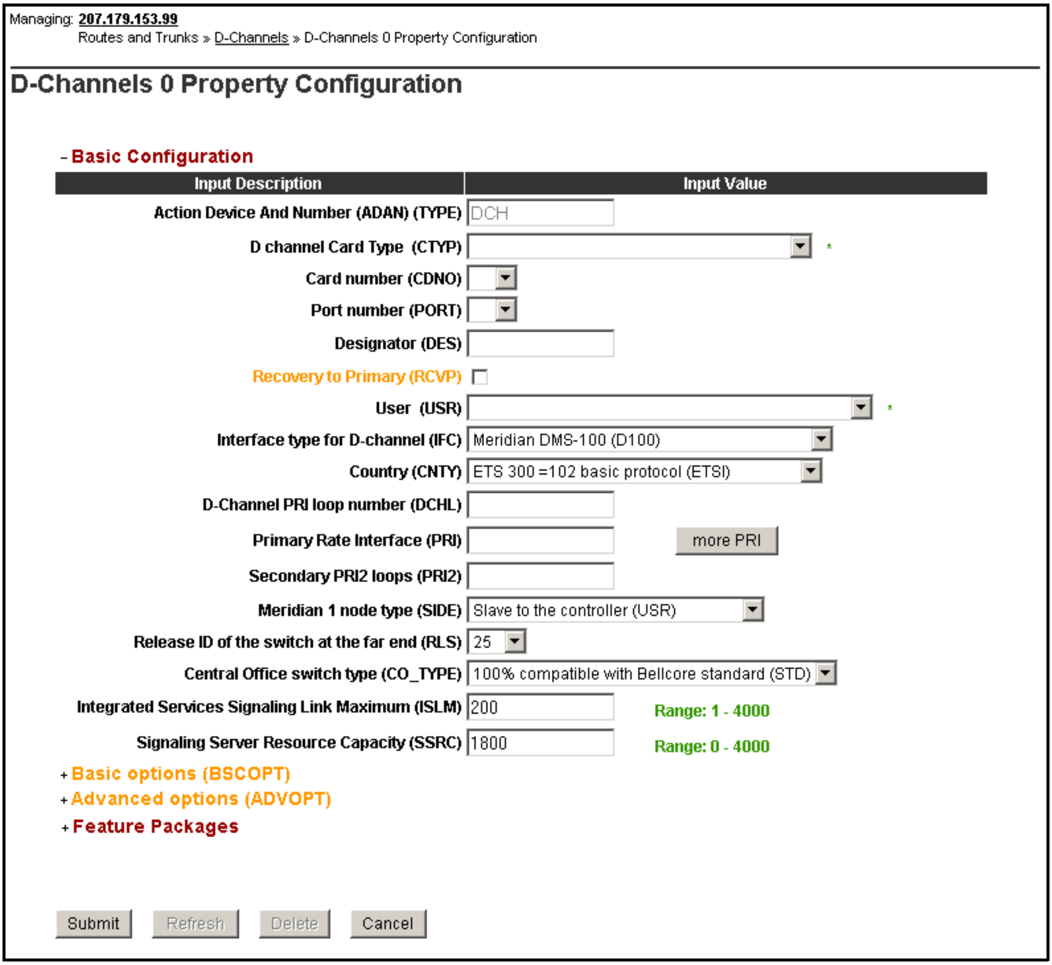
Configuration

Choose a D-Channel Number: 0 and type: DCH

2 In the **Configuration** section, input the D-channel number and click **to Add**.

The **D-Channels xx Property Configuration** web page opens, as shown in Figure 90. The D-channel number is denoted by xx. Required fields are indicated with a green asterisk.

Figure 90
D-channels xx Property Configuration web page



Managing: 207.179.153.99
Routes and Trunks » D-Channels » D-Channels 0 Property Configuration

D-Channels 0 Property Configuration

- Basic Configuration

Input Description	Input Value	
Action Device And Number (ADAN) (TYPE)	DCH	
D channel Card Type (CTYP)		*
Card number (CDNO)		
Port number (PORT)		
Designator (DES)		
Recovery to Primary (RCVP)	□	
User (USR)		*
Interface type for D-channel (IFC)	Meridian DMS-100 (D100)	
Country (CNTY)	ETS 300 =102 basic protocol (ETSI)	
D-Channel PRI loop number (DCHL)		
Primary Rate Interface (PRI)		more PRI
Secondary PRI2 loops (PRI2)		
Meridian 1 node type (SIDE)	Slave to the controller (USR)	
Release ID of the switch at the far end (RLS)	25	
Central Office switch type (CO_TYPE)	100% compatible with Bellcore standard (STD)	
Integrated Services Signaling Link Maximum (ISLM)	200	Range: 1 - 4000
Signaling Server Resource Capacity (SSRC)	1800	Range: 0 - 4000

+ Basic options (BSCOPT)
+ Advanced options (ADVOPT)
+ Feature Packages

3 Configure the following fields with the following values:

a. **D channel Card Type (CYTP)** = D-Channel is over IP (DCIP)

b. **User (USR)** = Integrated Services Signaling Link Dedicated (ISLD)

c. **Interface type for D-channel (IFC)** = Meridian Meridian1 (SL1)

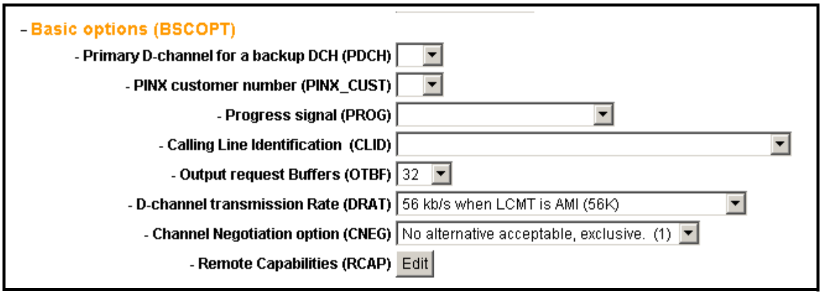
4 If you are defining the Network Name Display:

a. Select the **Release ID of the switch at the far end (RLS)** from the drop-down list.

b. Click **Basic options (BSCOPT)** tab.

The **Basic options** list expands, as shown in Figure 91.

Figure 91
D-channel — Basic options



- Basic options (BSCOPT)
- Primary D-channel for a backup DCH (PDCH)
- PINX customer number (PINX_CUST)
- Progress signal (PROG)
- Calling Line Identification (CLID)
- Output request Buffers (OTBF): 32
- D-channel transmission Rate (DRAT): 56 kb/s when LCMT is AMI (56K)
- Channel Negotiation option (CNEG): No alternative acceptable, exclusive. (1)
- Remote Capabilities (RCAP): Edit

c. Configure **Remote Capabilities (RCAP)** by clicking **Edit**.

The **Remote Capabilities Configuration** web page opens.

d. Scroll down the page and click the check box for **Network name Display method 2 (ND2)**.

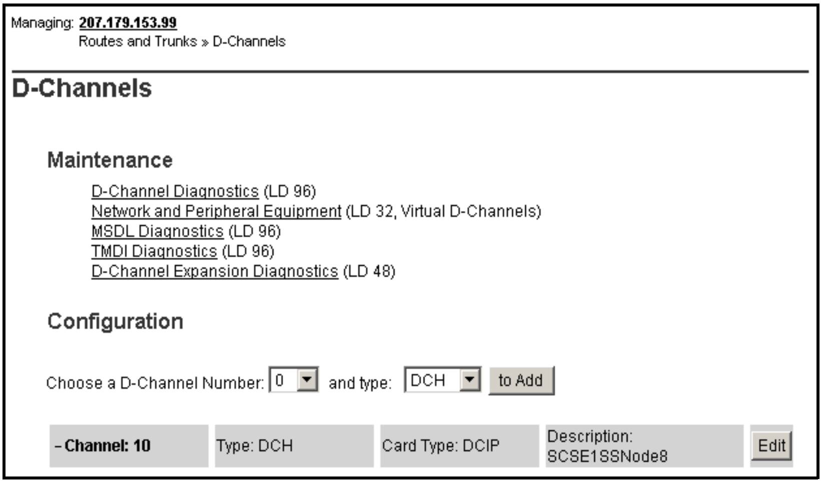
e. Click **Return - Remote Capabilities** at the bottom of the page.

The **D-Channel xx Property Configuration** web page reopens.

5 Click **Submit** to save the changes.

The **D-Channel**s web page reopens (Figure 92 on page 295) with the changes.

Figure 92
D-channel configuration results



Managing: 207.179.153.99
Routes and Trunks » D-Channels

D-Channels

Maintenance

D-Channel Diagnostics (LD 96)
Network and Peripheral Equipment (LD 32, Virtual D-Channels)
MSDL Diagnostics (LD 96)
TMDI Diagnostics (LD 96)
D-Channel Expansion Diagnostics (LD 48)

Configuration

Choose a D-Channel Number: 0 and type: DCH

- **Channel: 10**	Type: DCH	Card Type: DCIP	Description: SCSE1SSNode8	Edit

End of Procedure

Configuring zones

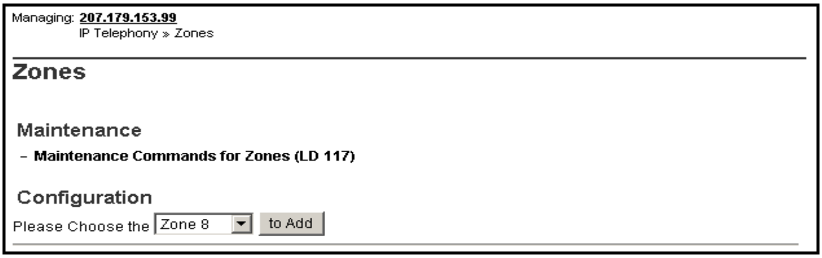
A zone is an area of a network that can be treated as a single entity with respect to the use of bandwidth for voice and signaling. Zones must be configured before the configuration of virtual routes.

Procedure 6
Configuring zones

1 Select **IP Telephony > Zones** from the navigator.

The **Zones** web page opens (see Figure 93 on page 296). This page also contains a link to Maintenance Commands for Zones, using LD 117.

Figure 93
Zones web page



Managing: 207.179.153.99
IP Telephony » Zones

Zones

Maintenance

- Maintenance Commands for Zones (LD 117)

Configuration

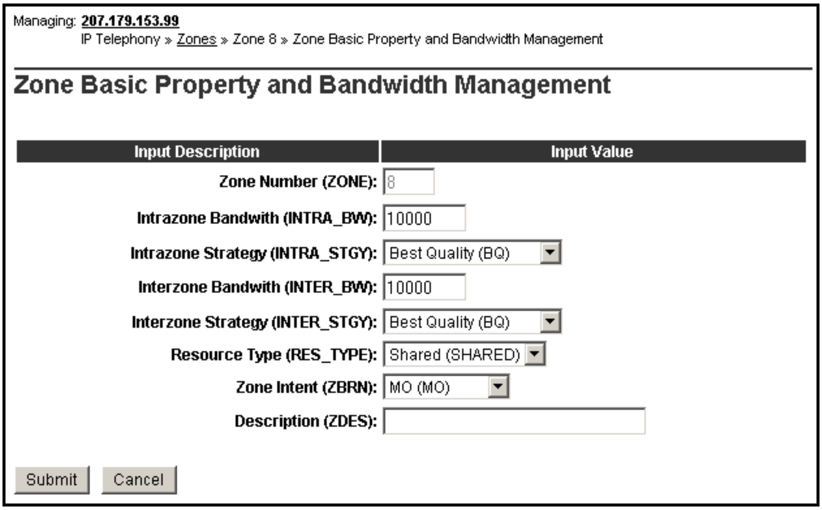
Please Choose the Zone 8 to Add

2 Choose a zone number from the drop-down list.

3 Click **to Add**.

4 The **Zone Basic Property and Bandwidth Management** web page opens (see Figure 94).

Figure 94
Zone Basic Property and Bandwidth Management web page



Managing: 207.179.153.99
IP Telephony » Zones » Zone 8 » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	8
Intrazone Bandwith (INTRA_BW):	10000
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwith (INTER_BW):	10000
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	

Note: The **Zone Number (ZONE)** field is auto-filled based on the number selected on the Zone List web page.

5 Enter the **Intrazone Bandwidth (INTRA _BW)**.

6 Select the **Intrazone Strategy (INTRA _STGY)** from the drop-down list.

7 Enter the **Interzone Bandwidth (INTER _BW)**.

8 Select the **Interzone Bandwidth (INTER _BW)** from the drop-down list.

9 Select the **Resource Type (RES_TYPE)** from the drop-down list.

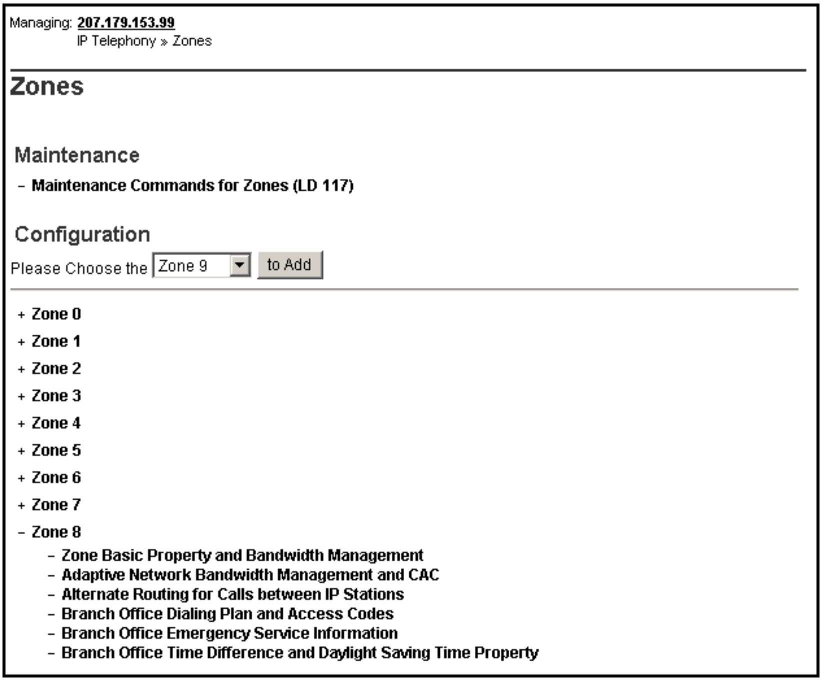
10 Select the **Branch Office Support (ZBRN)** from the drop-down list.

11 Enter a description of the zone in the **Description (ZDES)** text box.

12 Click **Submit**.

The **Zones** web page reopens with the new zone added (see Figure 95).

Figure 95
Zones web page with newly added zone



Managing: 207.179.153.99
IP Telephony » Zones

Zones

Maintenance

- Maintenance Commands for Zones (LD 117)

Configuration

Please Choose the Zone 9 to Add

+ Zone 0
+ Zone 1
+ Zone 2
+ Zone 3
+ Zone 4
+ Zone 5
+ Zone 6
+ Zone 7
- Zone 8
  - Zone Basic Property and Bandwidth Management
  - Adaptive Network Bandwidth Management and CAC
  - Alternate Routing for Calls between IP Stations
  - Branch Office Dialing Plan and Access Codes
  - Branch Office Emergency Service Information
  - Branch Office Time Difference and Daylight Saving Time Property

End of Procedure

Configuring the Virtual routes and trunks

Procedure 7
Configuring Virtual Trunk routes

To configure Virtual Trunk routes, you can use Element Manager or LD 16 of the Command Line Interface.

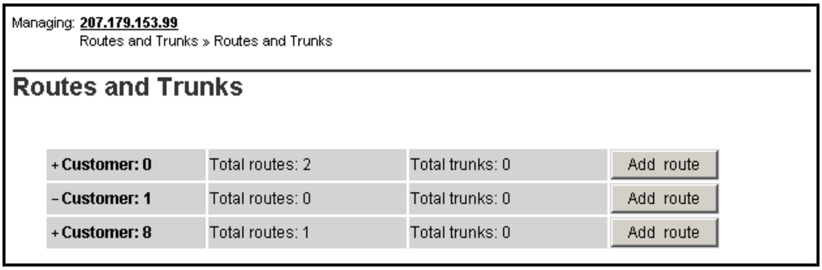
Figure 97 on page 299 shows the **New Route Configuration** web page in Element Manager. Use this web page to configure Virtual Trunk routes.

> ***Note:*** The zone parameter makes the codec selections and calculates the bandwidth usage for calls to the trunk members of a given route.

1 Select **Routes and Trunks > Routes and Trunks** from the navigator.

The **Routes and Trunks** web page opens, as shown in Figure 96.

Figure 96
Routes and Trunks web page



Managing: **207.179.153.99**
Routes and Trunks » Routes and Trunks

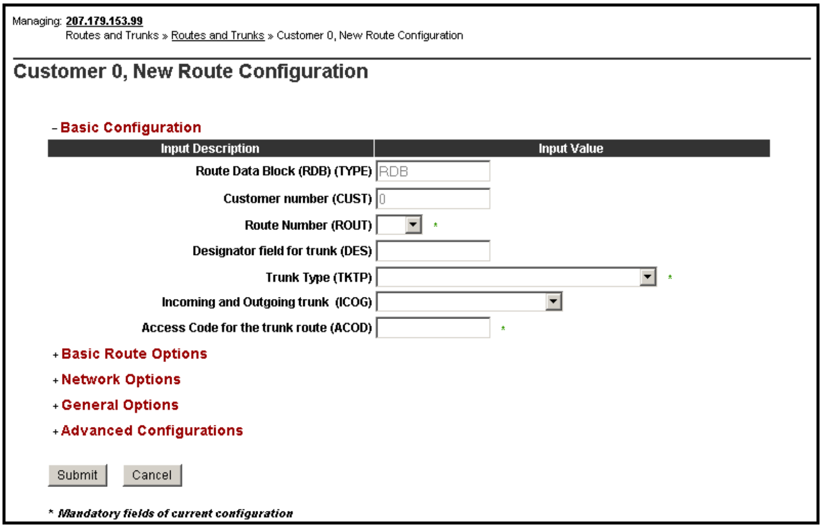
Routes and Trunks

+ **Customer: 0**	Total routes: 2	Total trunks: 0	Add route
- **Customer: 1**	Total routes: 0	Total trunks: 0	Add route
+ **Customer: 8**	Total routes: 1	Total trunks: 0	Add route

2 Click **Add route** associated with the customer.

The **Customer xx, New Route Configuration** web page opens (where xx is the customer number). See Figure 97 on page 299.

Figure 97
New Route Configuration web page



Managing: 207.179.153.99
Routes and Trunks » Routes and Trunks » Customer 0, New Route Configuration

Customer 0, New Route Configuration

- Basic Configuration

Input Description	Input Value
Route Data Block (RDB) (TYPE)	RDB
Customer number (CUST)	0
Route Number (ROUT)	*
Designator field for trunk (DES)	
Trunk Type (TKTP)	*
Incoming and Outgoing trunk (ICOG)	
Access Code for the trunk route (ACOD)	*

+ Basic Route Options

+ Network Options

+ General Options

+ Advanced Configurations

* Mandatory fields of current configuration

3 Under **Basic Configuration**, fill in the required fields to create a new Virtual Trunk Route:

a. Select a **Route Number (ROUT)** from the drop-down list.

b. Select the **Trunk Type (TKTP)** = TIE trunk data block (TIE).

When **Trunk Type (TKTP)** is selected, the following three options appear (see Figure 98 on page 300):

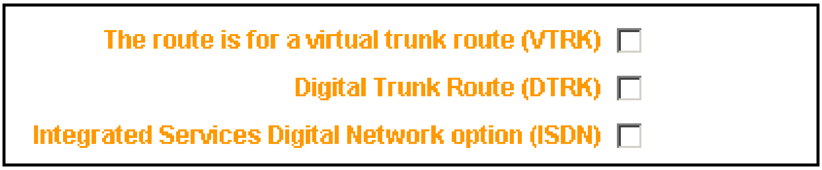
— **The route is for a virtual trunk route (VTRK)** (see step 4 on page 300)

— **Digital Trunk Route (DTRK)**

— **Integrated Services Digital Network option (ISDN)** (see step 5 on page 300)

c. Enter the **Access Code for the trunk route (ACOD)**.

Figure 98
Options available when TIE is selected



The route is for a virtual trunk route (VTRK) □

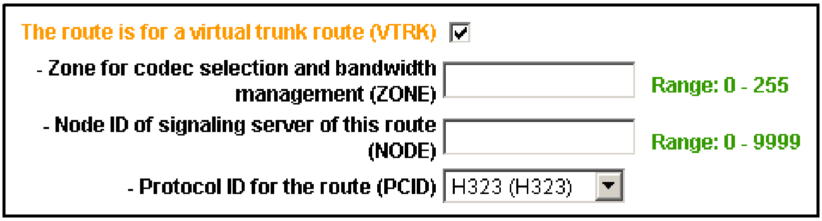
Digital Trunk Route (DTRK) □

Integrated Services Digital Network option (ISDN) □

4 Select **The route is for a virtual trunk route (VTRK)** check box.

Three fields display as shown in Figure 99.

Figure 99
Virtual trunk route



The route is for a virtual trunk route (VTRK) ☑

- Zone for codec selection and bandwidth management (ZONE) Range: 0 - 255

- Node ID of signaling server of this route (NODE) Range: 0 - 9999

- Protocol ID for the route (PCID) H323 (H323)

a. Enter a **ZONE** number.

b. Enter the **NODE** ID (the node served by this Signaling Server).

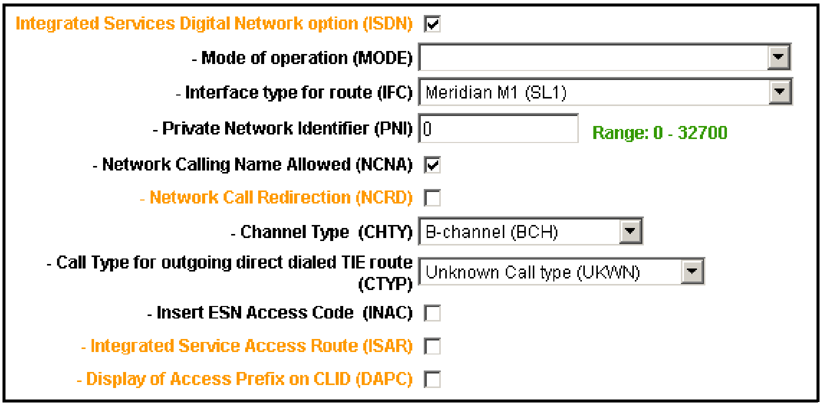
c. Select the **Protocol ID for the route** (**PCID**). H323 (H323) and SIP (SIP) are two of the available options.

Note: If SIP is selected as the protocol ID for the route (PCID), then the **Print Correlation ID in CDR for the route (CRID)** check box is displayed. CRID only appears if VTRK is YES and PCID is SIP and CDR is turned on for the route.

5 Select the **Integrated Services Digital Networks option (ISDN)** check box.

The ISDN section expands as shown in Figure 100 on page 301.

Figure 100
ISDN option



Integrated Services Digital Network option (ISDN) ☑

- Mode of operation (MODE)
- Interface type for route (IFC) Meridian M1 (SL1)
- Private Network Identifier (PNI) 0 Range: 0 - 32700
- Network Calling Name Allowed (NCNA) ☑
- Network Call Redirection (NCRD) □
- Channel Type (CHTY) B-channel (BCH)
- Call Type for outgoing direct dialed TIE route (CTYP) Unknown Call type (UKWN)
- Insert ESN Access Code (INAC) □
- Integrated Service Access Route (ISAR) □
- Display of Access Prefix on CLID (DAPC) □

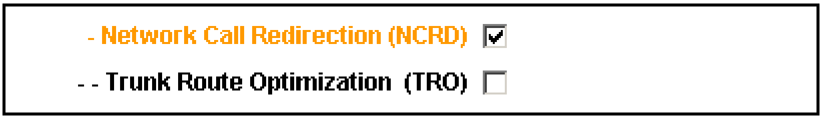
a. Choose **Mode of operations (MODE)** = Route uses ISDN Signaling Link (ISLD).

b. Choose **Interface type for route (IFC)** = Meridian M1 (SL1).

c. Select the **Network Calling Name Allowed (NCNA)** check box.

6 Select the **Network Call Redirection (NCRD)** check box (see Figure 101).

Figure 101
NCRD



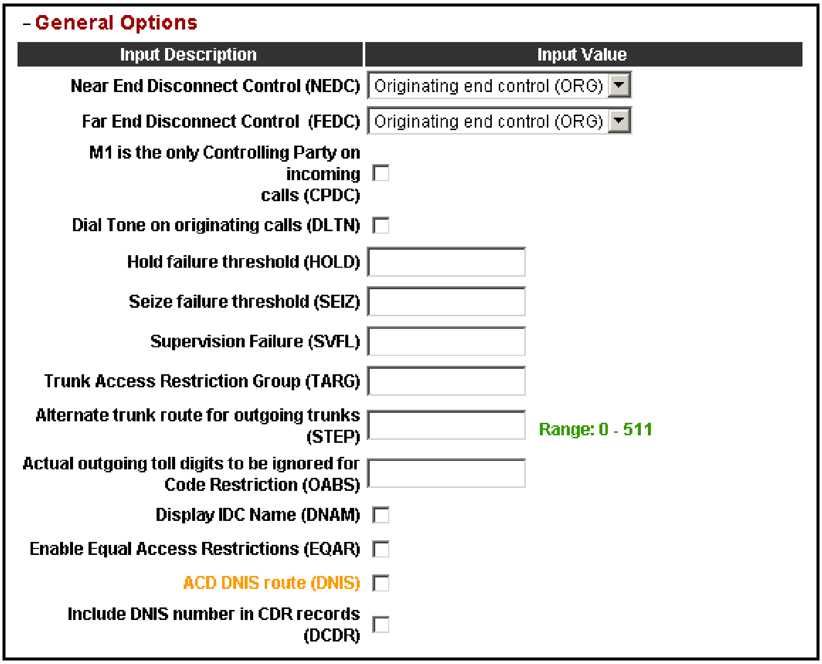
- Network Call Redirection (NCRD) ☑

- - Trunk Route Optimization (TRO) □

7 Click **General Options**.

The General Options list expands, as shown in Figure 102 on page 302.

Figure 102
General Options



- General Options

Input Description	Input Value
Near End Disconnect Control (NEDC)	Originating end control (ORG) ▾
Far End Disconnect Control (FEDC)	Originating end control (ORG) ▾
M1 is the only Controlling Party on incoming calls (CPDC)	☐
Dial Tone on originating calls (DLTN)	☐
Hold failure threshold (HOLD)	
Seize failure threshold (SEIZ)	
Supervision Failure (SVFL)	
Trunk Access Restriction Group (TARG)	
Alternate trunk route for outgoing trunks (STEP)	Range: 0 - 511
Actual outgoing toll digits to be ignored for Code Restriction (OABS)	
Display IDC Name (DNAM)	☐
Enable Equal Access Restrictions (EQAR)	☐
ACD DNIS route (DNIS)	☐
Include DNIS number in CDR records (DCDR)	☐

8 Enter the **Trunk Access Restriction Group (TARG)** value if you are configuring a single customer.

9 Enter the appropriate information in the text boxes and in **Basic Route Options**, **Network Options**, **General Options**, and **Advanced Configurations**.

10 Click **Submit**.

The **Trunks and Routes** web page opens and the newly configured route is displayed for the customer.

End of Procedure

Configure virtual superloops for IP Phones (LD 97)

One or more virtual superloops must be configured to support IP Phone Virtual TNs (VTNs).

Large Systems

In Large Systems, virtual superloops contend for the same range of loops with phantom, standard and remote superloops, digital trunk loops and all service loops. Virtual superloops can reside in physically-equipped network groups or in virtual network groups.

A 61c is a sinlge group machine and can have physical loops 0-31 and virtual loops up to 159.

An 81c is a multi-group machine and can have physical and virtual loops 0-159. An 81c with the FIBN package and FIBN hardware can have physical and virtual loop 0-255.

Virtual superloops have 1024 TNs and are non-blocking. Therefore all 1024 TNs can be configured on a virtual superloop and still be a non-blocking configuration. Virtual Superloops are configured in LD 97.

.

LD 97 – Configure virtual superloop for Large Systems. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change
TYPE	SUPL	Superloop

LD 97 – Configure virtual superloop for Large Systems. (Part 2 of 2)

Prompt	Response	Description
SUPL	Vxxx	V stands for a virtual superloop and xxx is the number of the virtual superloop xxx = 0 – 156 in multiples of four for a Large System without Fiber Network Package (FIBN) package 365 xxx = 0 – 252 in multiples of four for a Large System with Fiber Network Package (FIBN) package 365 xxx = 0 – 252 in multiples of four for a CS 1000E system xxx = 96 – 112 in multiples of four for a Small System and CS 1000S system

Small Systems

In Small Systems, virtual superloops contend for the same range of superloops, 96 – 112, with phantom superloops.

Up to 128 VTNs can be configured on a single virtual superloop for a Small System, for a maximum number of 640 VTNs in each system.

In a Small System, mapping virtual superloops to virtual cards is the same as mapping phantom superloops to phantom cards. See Table 32.

Table 32
Virtual superloop/virtual card mapping for Small Systems

SUPL	Card
96	61-64
100	65-68
104	69-72
108	73-76
112	77-80

CS 1000S systems

Table 33 lists the virtual superloop and virtual card mapping for the CS 1000S system.

Table 33
Virtual superloop/virtual card mapping for CS 1000S Systems

SUPL	Card	
96	61-64	81-84
100	65-68	85-88
104	69-72	89-92
108	73-76	93-96
112	77-80	97-99

LD 97 PRT TYPE SUPL prints the implicit virtual, phantom, or DECT cards for a virtual, phantom, or DECT superloop.

LD 21 LUU allows the user to list unused units of a specified type (iset, vtrk, phantom, DECT) in a specified range of (virtual, and so on) TNs. Similarly, LUC of a specified type (virtual, phantom, or DECT) prints a list of unused cards on configured superloops.

Procedure 8
Configuring Virtual Trunks

To configure Virtual Trunks in Element Manager, use the “New Member Property” pages.

Figures 104 to 106 show the New Member Property web page in Element Manager. Use this web page to configure Virtual Trunks.

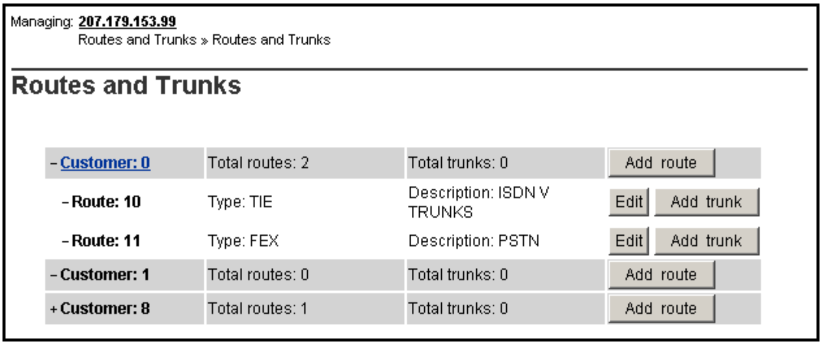
1 Select **Routes and Trunks > Routes and Trunks** from the navigator.

The **Routes and Trunks** web pages opens (see Figure 96 on page 298).

2 Select the **Customer** for which you are configuring Virtual Trunks.

The customer list expands showing a list of configured routes, as shown in Figure 103 on page 306.

Figure 103
Customer routes



Managing: 207.179.153.99
Routes and Trunks » Routes and Trunks

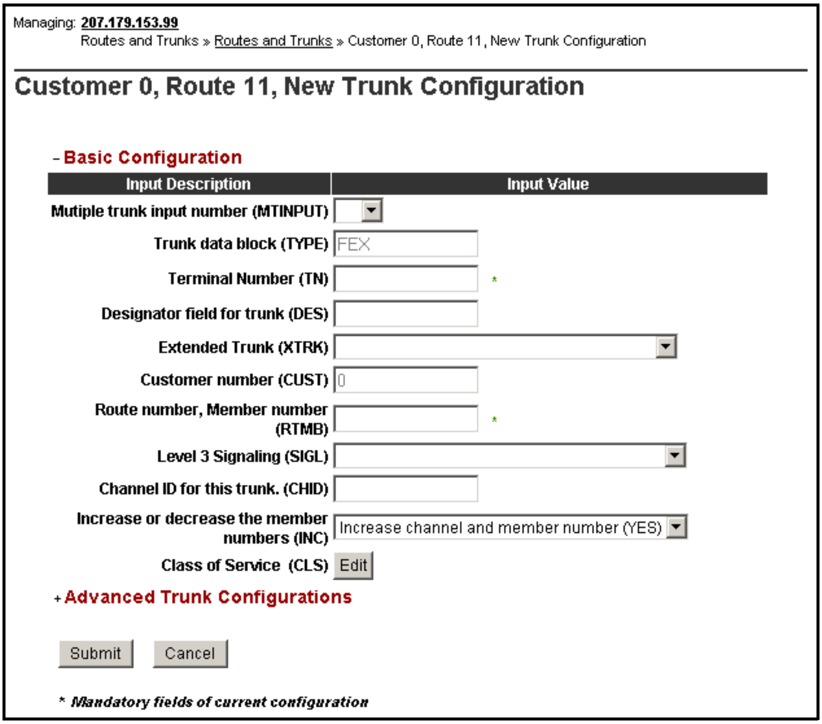
Routes and Trunks

- Customer: 0	Total routes: 2	Total trunks: 0	Add route
- Route: 10	Type: TIE	Description: ISDN V TRUNKS	Edit Add trunk
- Route: 11	Type: FEX	Description: PSTN	Edit Add trunk
- Customer: 1	Total routes: 0	Total trunks: 0	Add route
+ Customer: 8	Total routes: 1	Total trunks: 0	Add route

3 Click **Add trunk** associated with the route listing to add new trunk members.

The **Customer xx, Route yy, New Trunk Configuration** web page opens, as shown in Figure 104 on page 307. The customer number is represented by xx and the route number by yy.

Figure 104
New Trunk Configuration web page



Managing: 207.179.153.99
Routes and Trunks » Routes and Trunks » Customer 0, Route 11, New Trunk Configuration

Customer 0, Route 11, New Trunk Configuration

- Basic Configuration

Input Description	Input Value
Mutiple trunk input number (MTINPUT)	
Trunk data block (TYPE)	FEX
Terminal Number (TN)	*
Designator field for trunk (DES)	
Extended Trunk (XTRK)	
Customer number (CUST)	0
Route number, Member number (RTMB)	*
Level 3 Signaling (SIGL)	
Channel ID for this trunk. (CHID)	
Increase or decrease the member numbers (INC)	Increase channel and member number (YES)
Class of Service (CLS)	Edit

+ Advanced Trunk Configurations

Submit Cancel

* *Mandatory fields of current configuration*

4 Choose **Multiple trunk input number (MTINPUT)** if you are using more than one trunk.

5 Select **Trunk data block (TYPE)** = IP Trunk (IPTI).

6 **Terminal Number (TN)**.

7 (Optional) **Designator field for trunk (DES)** is a text string only, and has no impact on functionality.

8 Select **Extended Trunk (XTRK)** = Virtual trunk (VTRK).

9 Enter a **Route number, Member number (RTMB)**.

10 Enter a **Trunk Group Access Restriction (TGAR)** value.

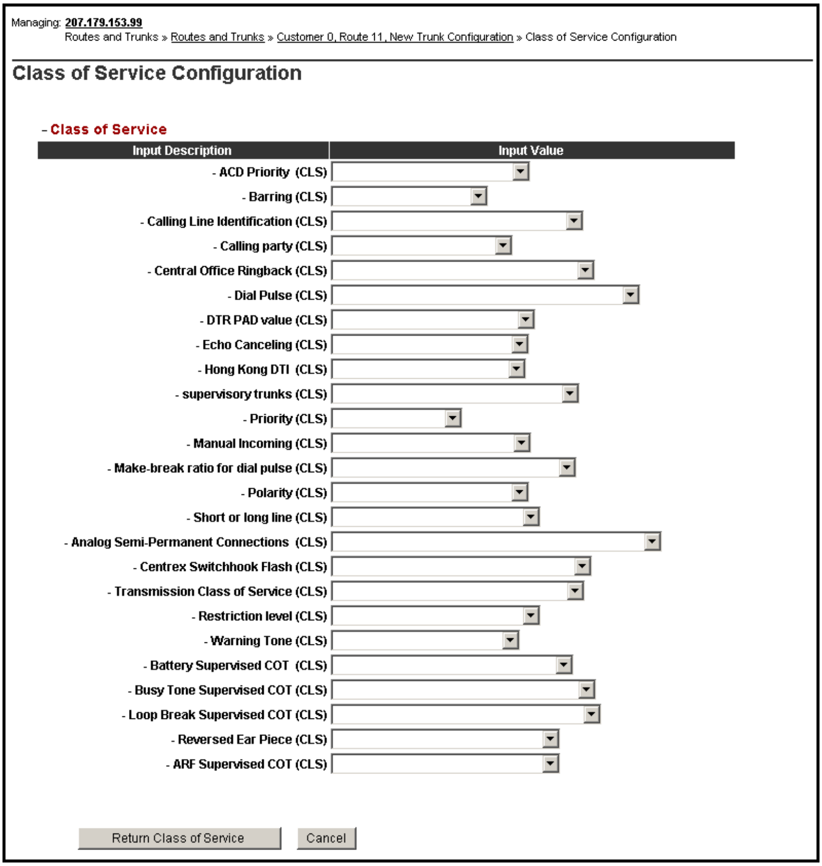
11 Enter a **Channel ID for this trunk (CHID)** = x (where x is in the range of 1-382).

Note: Channel_ID: A numeric input is required. However, there is no requirement for the CHID of Site A to match the CHID of Site B, as required with traditional ISL trunking as the channel is no longer point-to-point.

12 To specify a **Class of Service (CLS)** for the trunk, click **Edit**.

The **Class of Service Configuration** web page opens (see Figure 105). Select a Class of Service.

Figure 105
New Trunk Configuration – Class of Service Configuration web page



Managing: 207.179.153.99
Routes and Trunks » Routes and Trunks » Customer 0, Route 11, New Trunk Configuration » Class of Service Configuration

Class of Service Configuration

- Class of Service

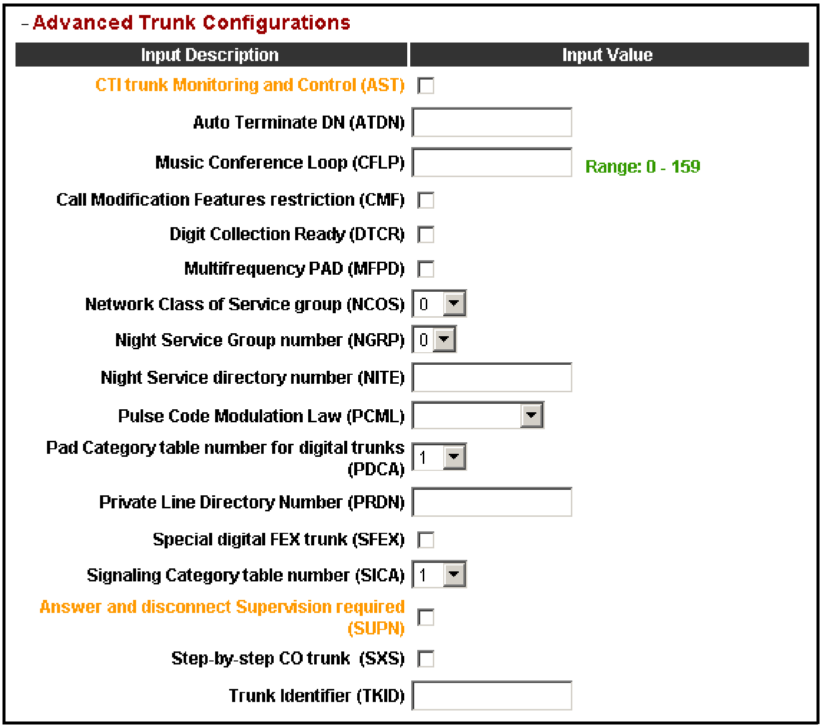
Input Description	Input Value
- ACD Priority (CLS)	
- Barring (CLS)	
- Calling Line Identification (CLS)	
- Calling party (CLS)	
- Central Office Ringback (CLS)	
- Dial Pulse (CLS)	
- DTR PAD value (CLS)	
- Echo Canceling (CLS)	
- Hong Kong DTI (CLS)	
- supervisory trunks (CLS)	
- Priority (CLS)	
- Manual Incoming (CLS)	
- Make-break ratio for dial pulse (CLS)	
- Polarity (CLS)	
- Short or long line (CLS)	
- Analog Semi-Permanent Connections (CLS)	
- Centrex Switchhook Flash (CLS)	
- Transmission Class of Service (CLS)	
- Restriction level (CLS)	
- Warning Tone (CLS)	
- Battery Supervised COT (CLS)	
- Busy Tone Supervised COT (CLS)	
- Loop Break Supervised COT (CLS)	
- Reversed Ear Piece (CLS)	
- ARF Supervised COT (CLS)	

13 Select the Class of Service and then click **Return Class of Service** to return to the **New Trunk Configuration** web page (see Figure 104 on page 307).

14 Select **Advanced Trunk Configurations**.

The **Advanced Trunk Configurations** list expands, as shown in Figure 106.

Figure 106
New Trunk Configuration – Advanced Trunk Configurations



- Advanced Trunk Configurations

Input Description	Input Value
CTI trunk Monitoring and Control (AST)	□
Auto Terminate DN (ATDN)	
Music Conference Loop (CFLP)	Range: 0 - 159
Call Modification Features restriction (CMF)	□
Digit Collection Ready (DTCR)	□
Multifrequency PAD (MFPD)	□
Network Class of Service group (NCOS)	0
Night Service Group number (NGRP)	0
Night Service directory number (NITE)	
Pulse Code Modulation Law (PCML)	
Pad Category table number for digital trunks (PDCA)	1
Private Line Directory Number (PRDN)	
Special digital FEX trunk (SFEX)	□
Signaling Category table number (SICA)	1
Answer and disconnect Supervision required (SUPN)	□
Step-by-step CO trunk (SXS)	□
Trunk Identifier (TKID)	

15 Configure **Network Class of Service group (NCOS)**.

16 Click **Submit** to save the changes.

The **Customer Explorer** web page reopens, showing the new trunk member.

End of Procedure

Configuring networking

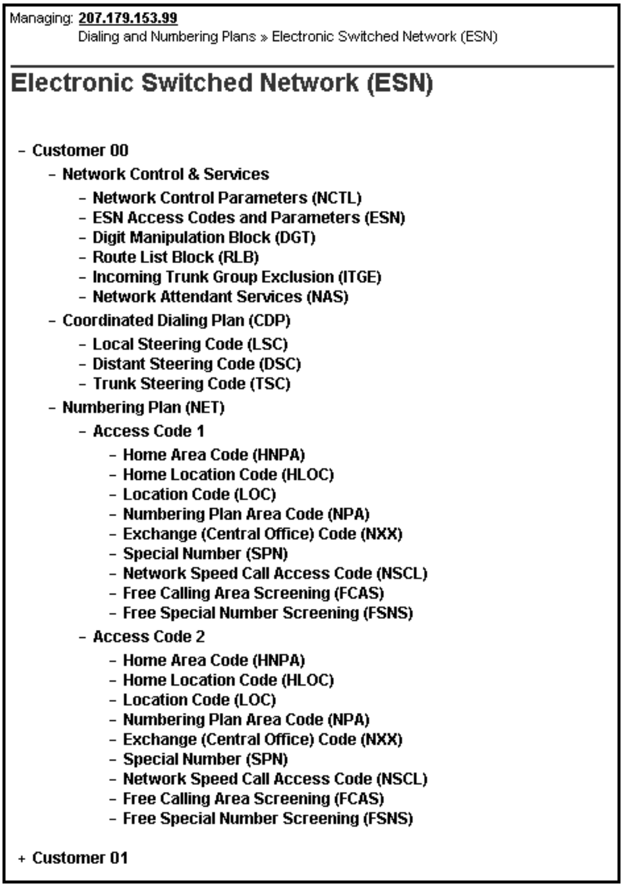
The following procedures indicate a Coordinated Dialing Plan for the configuration of networking.

Procedure 9
Creating an ESN control block

1 Select **Dialing and Numbering Plans > Electronic Switched Network** from the navigator.

The **Electronic Switched Network (ESN)** web page opens, as shown in Figure 107 on page 311.

Figure 107
Electronic Switched Network (ESN) web page



Managing: **207.179.153.99**
Dialing and Numbering Plans » Electronic Switched Network (ESN)

Electronic Switched Network (ESN)

- Customer 00
  - Network Control & Services
    - Network Control Parameters (NCTL)
    - ESN Access Codes and Parameters (ESN)
    - Digit Manipulation Block (DGT)
    - Route List Block (RLB)
    - Incoming Trunk Group Exclusion (ITGE)
    - Network Attendant Services (NAS)
  - Coordinated Dialing Plan (CDP)
    - Local Steering Code (LSC)
    - Distant Steering Code (DSC)
    - Trunk Steering Code (TSC)
  - Numbering Plan (NET)
    - Access Code 1
      - Home Area Code (HNPA)
      - Home Location Code (HLOC)
      - Location Code (LOC)
      - Numbering Plan Area Code (NPA)
      - Exchange (Central Office) Code (NXX)
      - Special Number (SPN)
      - Network Speed Call Access Code (NSCL)
      - Free Calling Area Screening (FCAS)
      - Free Special Number Screening (FSNS)
    - Access Code 2
      - Home Area Code (HNPA)
      - Home Location Code (HLOC)
      - Location Code (LOC)
      - Numbering Plan Area Code (NPA)
      - Exchange (Central Office) Code (NXX)
      - Special Number (SPN)
      - Network Speed Call Access Code (NSCL)
      - Free Calling Area Screening (FCAS)
      - Free Special Number Screening (FSNS)

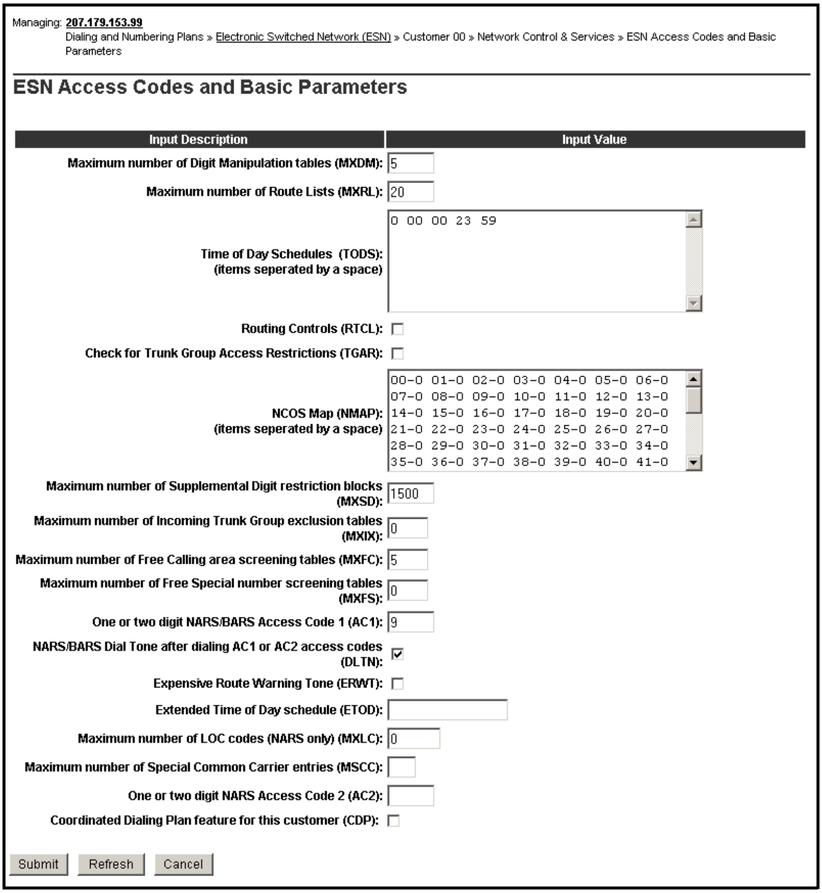
+ Customer 01

2 Under Network Control & Service, click **ESN Access Codes and Parameters (ESN)**.

If no ESN database is configured, a warning dialog box opens. Click **OK** on the warning dialog box.

The **ESN Access Codes and Basic Parameters** web page opens, as shown in Figure 108 on page 312.

Figure 108
ESN Access Codes and Basic Parameters web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » ESN Access Codes and Basic Parameters

ESN Access Codes and Basic Parameters

Input Description	Input Value
Maximum number of Digit Manipulation tables (MXDM):	5
Maximum number of Route Lists (MXRL):	20
Time of Day Schedules (TODS): (items seperated by a space)	0 00 00 23 59
Routing Controls (RTCL):	□
Check for Trunk Group Access Restrictions (TGAR):	□
NCOS Map (NMAP): (items seperated by a space)	00-0 01-0 02-0 03-0 04-0 05-0 06-0 07-0 08-0 09-0 10-0 11-0 12-0 13-0 14-0 15-0 16-0 17-0 18-0 19-0 20-0 21-0 22-0 23-0 24-0 25-0 26-0 27-0 28-0 29-0 30-0 31-0 32-0 33-0 34-0 35-0 36-0 37-0 38-0 39-0 40-0 41-0
Maximum number of Supplemental Digit restriction blocks (MXSD):	1500
Maximum number of Incoming Trunk Group exclusion tables (MXIX):	0
Maximum number of Free Calling area screening tables (MXFC):	5
Maximum number of Free Special number screening tables (MXFS):	0
One or two digit NARS/BARS Access Code 1 (AC1):	9
NARS/BARS Dial Tone after dialing AC1 or AC2 access codes (DLTN):	☑
Expensive Route Warning Tone (ERWT):	□
Extended Time of Day schedule (ETOD):	
Maximum number of LOC codes (NARS only) (MXLC):	0
Maximum number of Special Common Carrier entries (MSCC):	
One or two digit NARS Access Code 2 (AC2):	
Coordinated Dialing Plan feature for this customer (CDP):	□

3 Define the parameters for the network. Include the **Maximum number of Route Lists (MXRL)**.

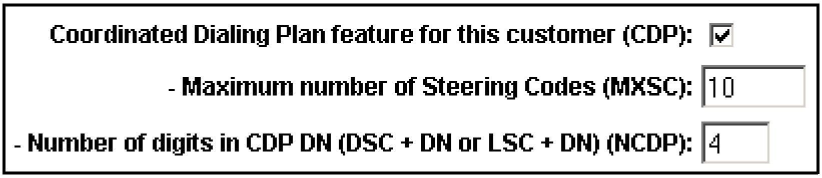
4 Scroll down the page and select the **Coordinated Dialing Plan feature for this customer (CDP)** check box.

The CDP list expands, as shown in Figure 109 on page 313.

a. Configure the number of CDP steering codes (**Maximum number of Steering Codes (MXSC)**).

b. Configure the number of digits of the CDP dialed number (**Number of digits in CDP DN (DSC + DN or LSC + DN) (NCDP)**).

Figure 109
ESN data block configuration – Coordinated Dialing Plan



Coordinated Dialing Plan feature for this customer (CDP): ☑

- Maximum number of Steering Codes (MXSC): 10

- Number of digits in CDP DN (DSC + DN or LSC + DN) (NCDP): 4

5 Click **Submit** to save the changes.

The **Electronic Switched Network (ESN)** web page reopens (Figure 107 on page 311).

End of Procedure

Procedure 10
Configuring network access

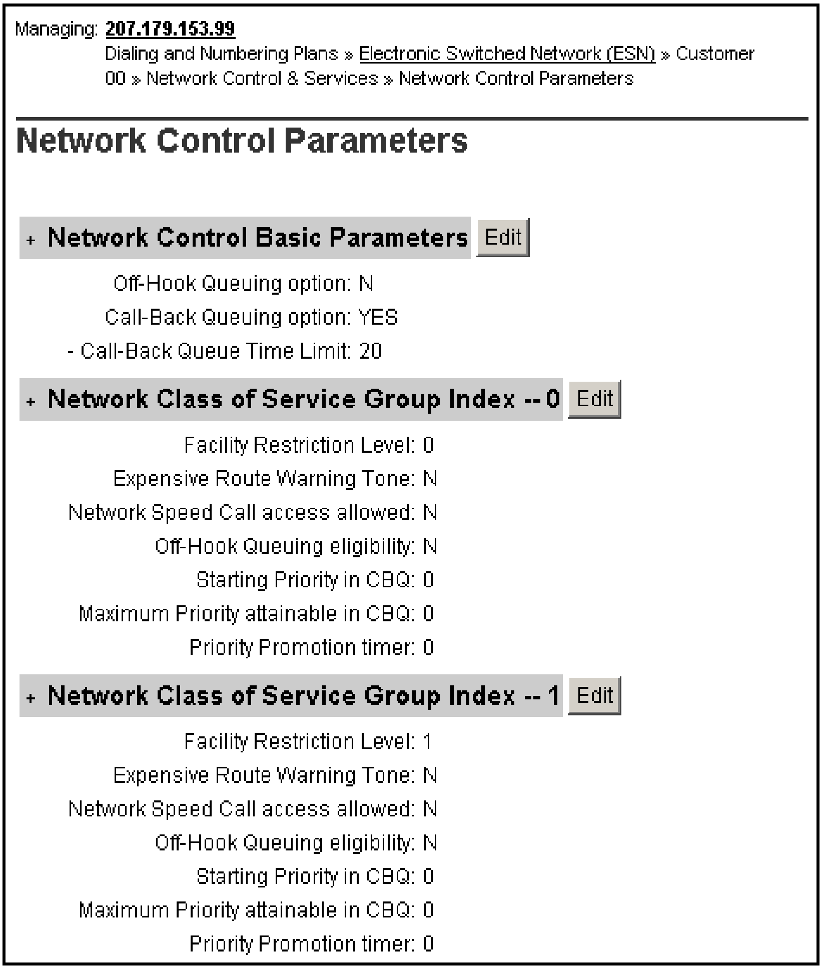
The default parameters for Network Control must be turned on.

1 Select **Dialing and Numbering Plans > Electronic Switched Network** from the navigator.

2 On the **Electronic Switched Network (ESN)** web page shown in Figure 107 on page 311, select **Customer xx > Network Control & Service > Network Control Parameters (NCTL)**.

The **Network Control Parameters** web page opens, as shown in Figure 110 on page 314.

Figure 110
Network Control Parameters web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Network Control Parameters

Network Control Parameters

+ Network Control Basic Parameters

Off-Hook Queuing option: N
Call-Back Queuing option: YES
- Call-Back Queue Time Limit: 20

+ Network Class of Service Group Index -- 0

Facility Restriction Level: 0
Expensive Route Warning Tone: N
Network Speed Call access allowed: N
Off-Hook Queuing eligibility: N
Starting Priority in CBQ: 0
Maximum Priority attainable in CBQ: 0
Priority Promotion timer: 0

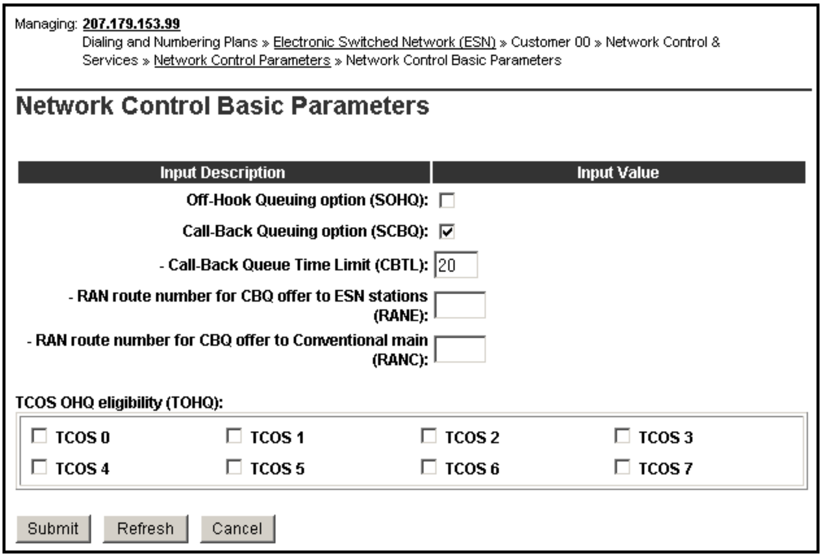
+ Network Class of Service Group Index -- 1

Facility Restriction Level: 1
Expensive Route Warning Tone: N
Network Speed Call access allowed: N
Off-Hook Queuing eligibility: N
Starting Priority in CBQ: 0
Maximum Priority attainable in CBQ: 0
Priority Promotion timer: 0

3 Click **Edit** to the right of **Network Control Basic Parameters**.

The **Network Control Basic Parameters** web page opens, as shown in Figure 111 on page 315.

Figure 111
Network Control Basic Parameters



Managing: **207.179.153.99**
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Network Control Parameters » Network Control Basic Parameters

Network Control Basic Parameters

Input Description	Input Value
Off-Hook Queuing option (SOHQ):	□
Call-Back Queuing option (SCBQ):	☑
- Call-Back Queue Time Limit (CBTL):	20
- RAN route number for CBQ offer to ESN stations (RANE):	
- RAN route number for CBQ offer to Conventional main (RANC):	

TCOS OHQ eligibility (TOHQ):

□ TCOS 0 □ TCOS 1 □ TCOS 2 □ TCOS 3
□ TCOS 4 □ TCOS 5 □ TCOS 6 □ TCOS 7

4 Click **Submit** to accept the default parameters on the **Network Control Basic Parameters** web page.

The **Network Control Parameters** web page reopens.

End of Procedure

Configuring call routing

Procedure 11
Configuring the Route List Block

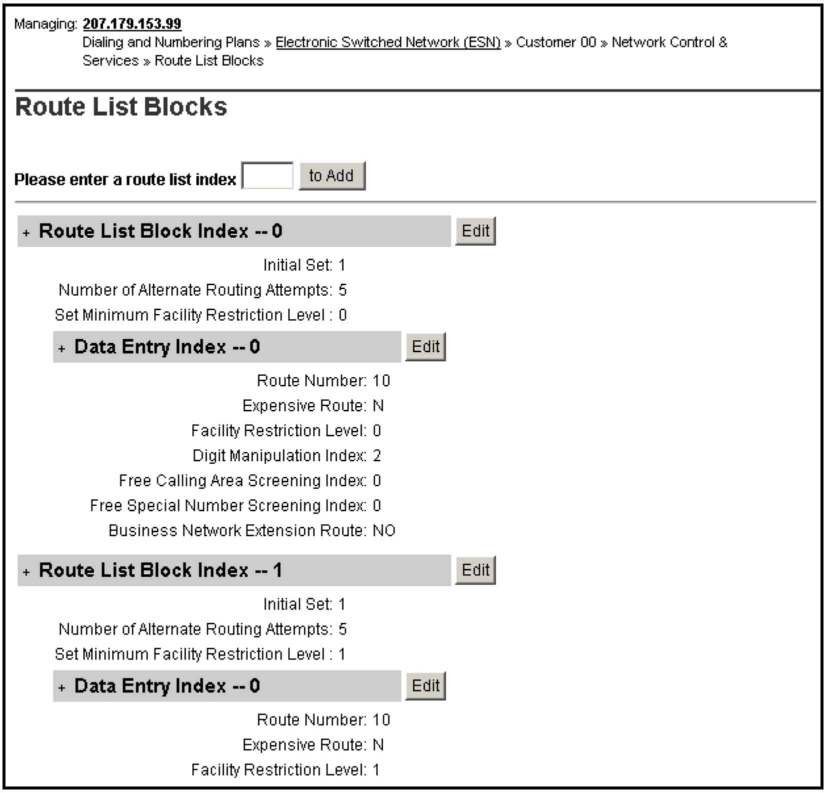
This procedure creates the Route List Block that routes calls over the Virtual Trunk route.

1 Select **Dialing and Numbering Plans > Electronic Switched Network** from the navigator.

2 On the **Electronic Switched Network (ESN)** web page shown in Figure 107 on page 311, select **Customer xx > Network Control & Service > Route List Block (RLB)**.

The **Route List Blocks** web page opens, as shown in Figure 112.

Figure 112
Route List Blocks web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks

Route List Blocks

Please enter a route list index [ ] to Add

+ Route List Block Index -- 0 Edit

Initial Set: 1
Number of Alternate Routing Attempts: 5
Set Minimum Facility Restriction Level : 0

+ Data Entry Index -- 0 Edit

Route Number: 10
Expensive Route: N
Facility Restriction Level: 0
Digit Manipulation Index: 2
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route: NO

+ Route List Block Index -- 1 Edit

Initial Set: 1
Number of Alternate Routing Attempts: 5
Set Minimum Facility Restriction Level : 1

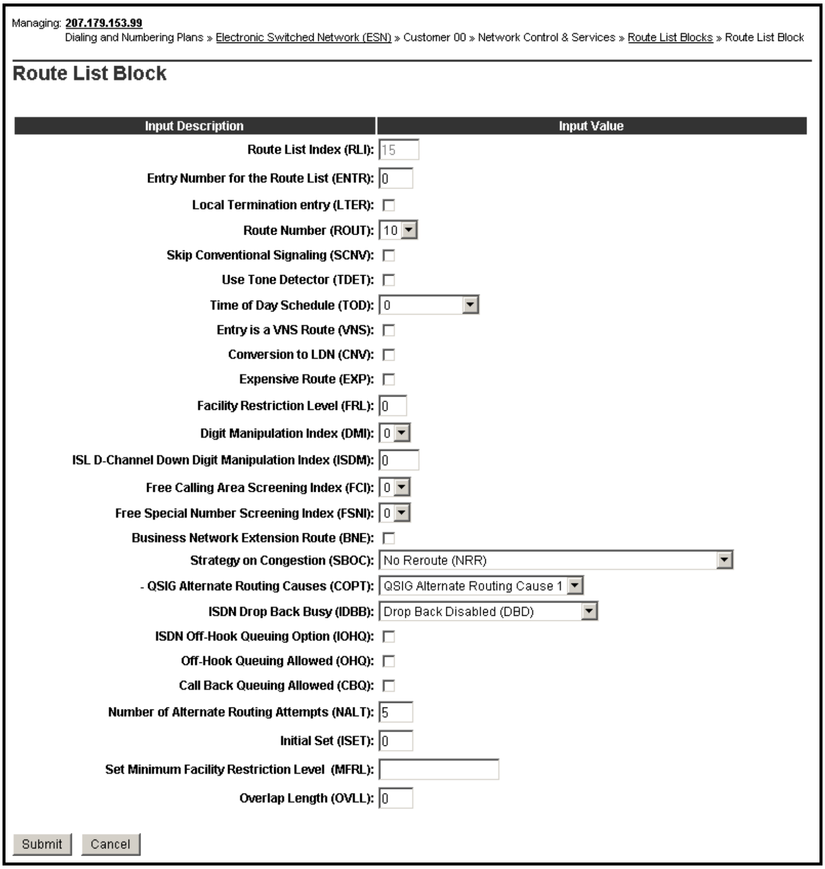
+ Data Entry Index -- 0 Edit

Route Number: 10
Expensive Route: N
Facility Restriction Level: 1

3 Enter the route list index number in the **Please enter a route list index** text box and click **to Add**.

The **Route List Block** web page opens, as shown in Figure 113 on page 317.

Figure 113
Route List Block



Managing: **207.179.153.99**
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks » Route List Block

Route List Block

Input Description	Input Value
Route List Index (RLI):	15
Entry Number for the Route List (ENTR):	0
Local Termination entry (LTER):	□
Route Number (ROUT):	10 ▾
Skip Conventional Signaling (SCNV):	□
Use Tone Detector (TDET):	□
Time of Day Schedule (TOD):	0 ▾
Entry is a VNS Route (VNS):	□
Conversion to LDN (CNV):	□
Expensive Route (EXP):	□
Facility Restriction Level (FRL):	0
Digit Manipulation Index (DMI):	0 ▾
ISL D-Channel Down Digit Manipulation Index (ISDM):	0
Free Calling Area Screening Index (FCI):	0 ▾
Free Special Number Screening Index (FSNI):	0 ▾
Business Network Extension Route (BNE):	□
Strategy on Congestion (SBOC):	No Reroute (NRR) ▾
- QSIG Alternate Routing Causes (COPT):	QSIG Alternate Routing Cause 1 ▾
ISDN Drop Back Busy (IDBB):	Drop Back Disabled (DBD) ▾
ISDN Off-Hook Queuing Option (IOHQ):	□
Off-Hook Queuing Allowed (OHQ):	□
Call Back Queuing Allowed (CBQ):	□
Number of Alternate Routing Attempts (NALT):	5
Initial Set (ISET):	0
Set Minimum Facility Restriction Level (MFRL):	
Overlap Length (OVLL):	0

4 Fill in the appropriate information and click **Submit**.

The new Route List Block is generated, and the initial **Route List Blocks** web page reopens.

End of Procedure

Procedure 12
Configuring Steering Codes

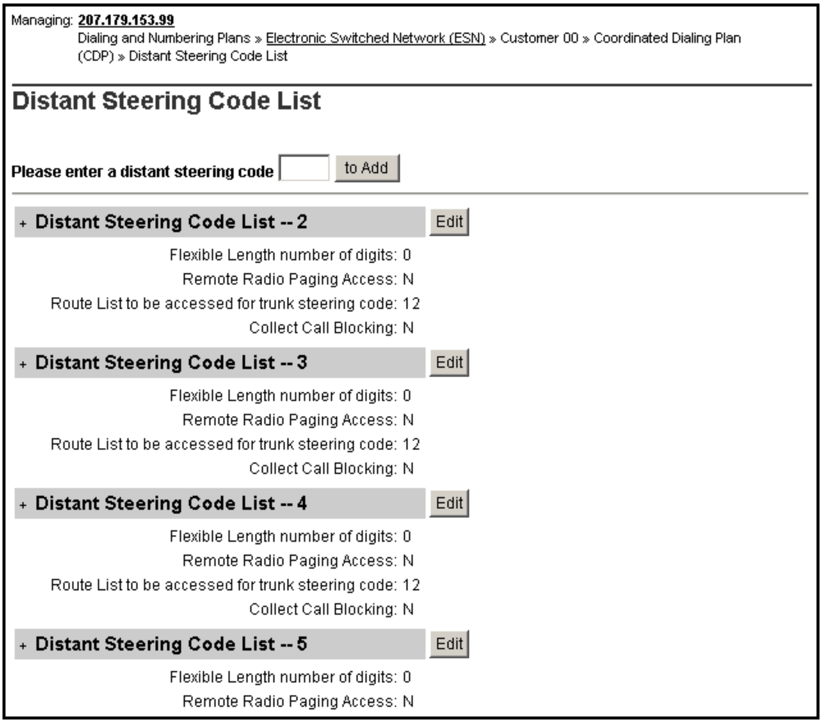
This procedure defines how digits for a call are routed under a Coordinated Dialing Plan.

1 Select **Dialing and Numbering Plans > Electronic Switched Network** from the navigator.

2 On the **Electronic Switched Network (ESN)** web page shown in Figure 107 on page 311, select **Customer xx > Coordinated Dialing Plan (CDP) > Distant Steering Code (DSC)**.

The **Distant Steering Code List** web page opens, as shown in Figure 114.

Figure 114
DIstant Steering Code List web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Coordinated Dialing Plan (CDP) » Distant Steering Code List

Distant Steering Code List

Please enter a distant steering code

+ Distant Steering Code List -- 2

Flexible Length number of digits: 0
Remote Radio Paging Access: N
Route List to be accessed for trunk steering code: 12
Collect Call Blocking: N

+ Distant Steering Code List -- 3

Flexible Length number of digits: 0
Remote Radio Paging Access: N
Route List to be accessed for trunk steering code: 12
Collect Call Blocking: N

+ Distant Steering Code List -- 4

Flexible Length number of digits: 0
Remote Radio Paging Access: N
Route List to be accessed for trunk steering code: 12
Collect Call Blocking: N

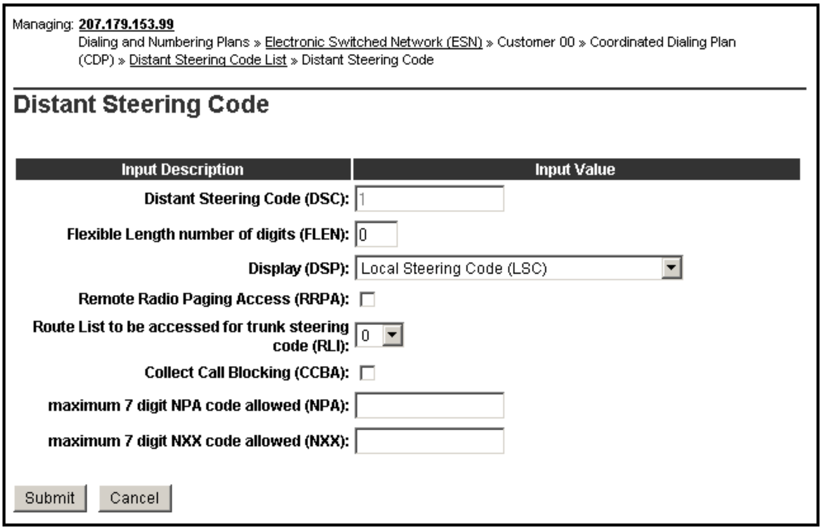
+ Distant Steering Code List -- 5

Flexible Length number of digits: 0
Remote Radio Paging Access: N

3 Enter the steering code in the **Please enter a distant steering code** text box and click **to Add**.

The **Distant Steering Code** web page opens, as shown in Figure 115.

Figure 115
Distant Steering Code web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Coordinated Dialing Plan (CDP) » Distant Steering Code List » Distant Steering Code

Distant Steering Code

Input Description	Input Value
Distant Steering Code (DSC):	1
Flexible Length number of digits (FLEN):	0
Display (DSP):	Local Steering Code (LSC)
Remote Radio Paging Access (RRPA):	□
Route List to be accessed for trunk steering code (RLI):	0
Collect Call Blocking (CCBA):	□
maximum 7 digit NPA code allowed (NPA):	
maximum 7 digit NXX code allowed (NXX):	

4 Fill in the appropriate information and click **Submit**.

The **Distant Steering Code List** web page reopens.

End of Procedure

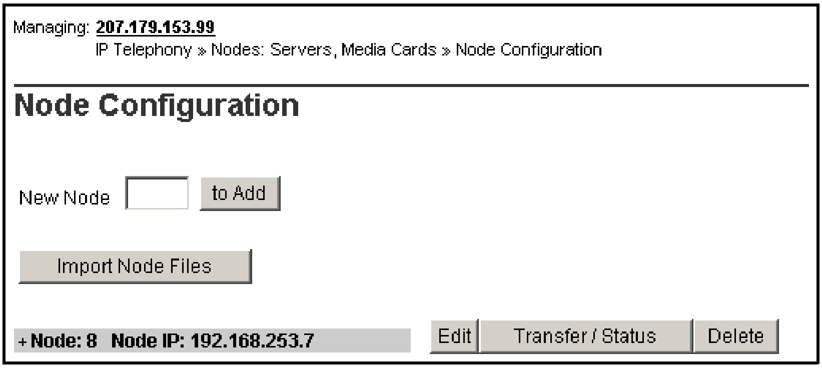
Configuring codecs

Procedure 13
Configuring codecs

1 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the navigator.

The **Node Configuration** web page opens, as shown in Figure 116 on page 320.

Figure 116
Node Configuration web page



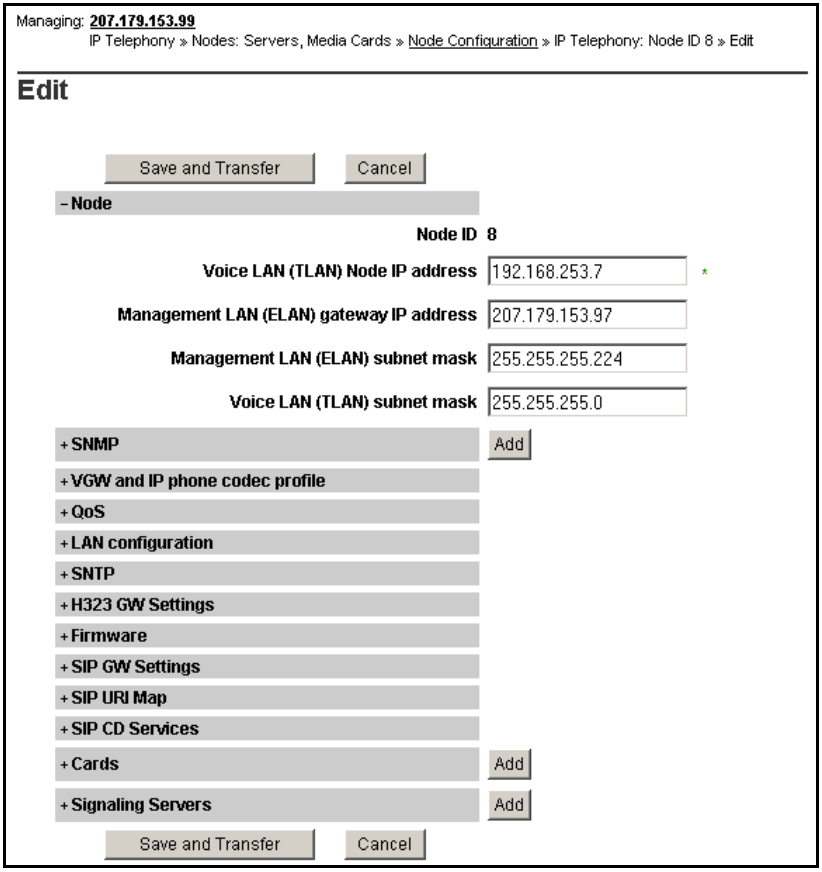
Managing: 207.179.153.99
IP Telephony » Nodes: Servers, Media Cards » Node Configuration

Node Configuration

2 Click **Edit** for the appropriate node.

The **Edit** web page opens, as shown in Figure 117 on page 321.

Figure 117
Edit web page



Managing: **207.179.153.99**
IP Telephony » Nodes: Servers, Media Cards » Node Configuration » IP Telephony: Node ID 8 » Edit

Edit

Node ID 8

Voice LAN (TLAN) Node IP address: 192.168.253.7 *

Management LAN (ELAN) gateway IP address: 207.179.153.97

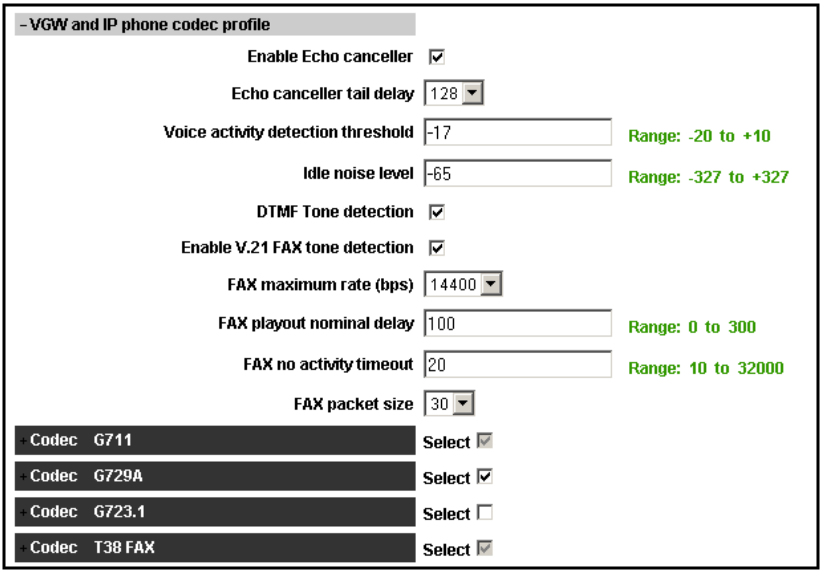
Management LAN (ELAN) subnet mask: 255.255.255.224

Voice LAN (TLAN) subnet mask: 255.255.255.0

3 Click on **VGW and IP phone codec profile** to open the parameter list as shown in Figure 118.

This area also includes a list of codecs.

Figure 118
VGW and IP Phone codec profile



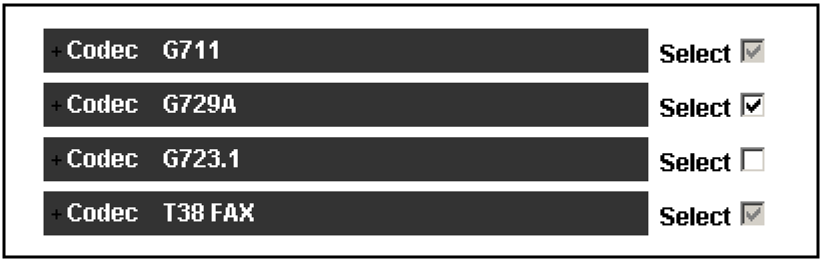
- VGW and IP phone codec profile

Enable Echo canceller	☑	
Echo canceller tail delay	128 ▾	
Voice activity detection threshold	-17	Range: -20 to +10
Idle noise level	-65	Range: -327 to +327
DTMF Tone detection	☑	
Enable V.21 FAX tone detection	☑	
FAX maximum rate (bps)	14400 ▾	
FAX playout nominal delay	100	Range: 0 to 300
FAX no activity timeout	20	Range: 10 to 32000
FAX packet size	30 ▾	
+ Codec G711	Select ☑	
+ Codec G729A	Select ☑	
+ Codec G723.1	Select □	
+ Codec T38 FAX	Select ☑	

4 To configure a codec, select the **Select** check box to the right of the codec name. For example, in Figure 119 on page 323 the G.729A codec has been selected.

Note: The G.711 and T38 FAX codecs are automatically selected.

Figure 119
Example of a selected codec — G.729A



+ Codec G711 Select ☑

+ Codec G729A Select ☑

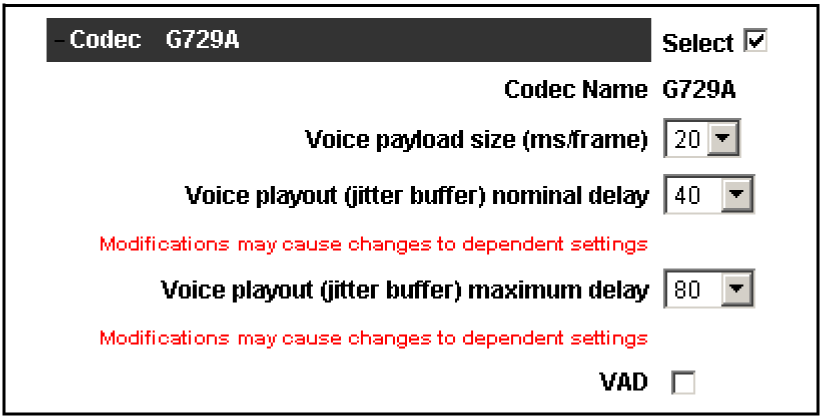
+ Codec G723.1 Select □

+ Codec T38 FAX Select ☑

5 Click on the codec name to modify the **Voice payload size (ms/frame)**, **Voice playout (jitter buffer) nominal delay**, and **Voice playout (jitter buffer) maximum delay** values of a codec.

Use the drop-down lists to choose the values. See the example in Figure 120.

Figure 120
Example of G.729A settings



- Codec G729A Select ☑

Codec Name G729A

Voice payload size (ms/frame) 20

Voice playout (jitter buffer) nominal delay 40

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 80

Modifications may cause changes to dependent settings

VAD □

6 Repeat Step 4 and Step 5 for each codec that requires configuration.

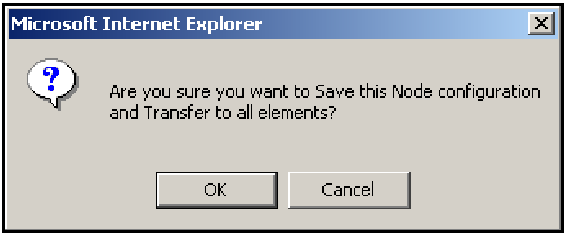
Note: For detailed information about configuring codecs, refer to *Converging the Data Network with VoIP* (553-3001-160) and *IP Line: Description, Installation, and Operation* (553-3001-365).

7 Click **Save and Transfer**.

This saves the changes and transfers the node configuration files to all elements in the node (that is, Signaling Servers, Call Server, and Voice Gateway Media Cards).

A warning dialog box opens asking if you want to save and transfer the configuration changes (see Figure 121).

Figure 121
Save and Transfer dialog box



Microsoft Internet Explorer

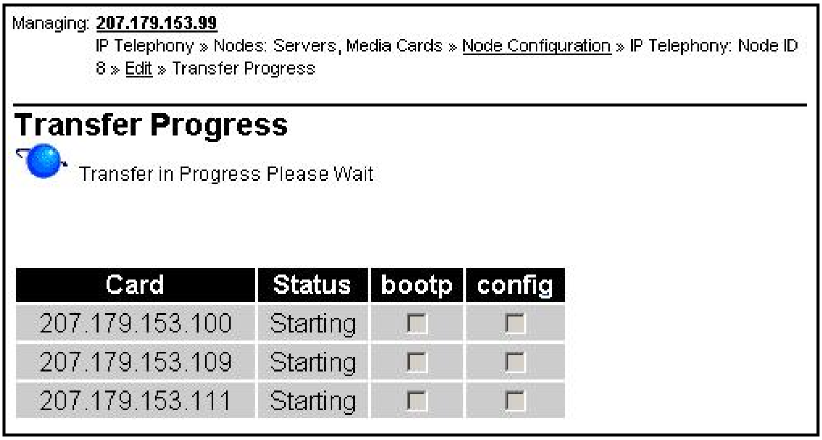
Are you sure you want to Save this Node configuration and Transfer to all elements?

8 Click **OK**.

A series of pages including the following display:

- **Transfer Progress** web page (see Figures 122 and 123 on 325, and Figure 124 on page 326)
- **Transfer Failure Report** web page (if applicable)
- **Transfer / Status** web page (see Figure 125 on page 327)
  This web page shows if the transfer was successful, and allows the node information to be transferred again.

Figure 122
Transfer Progress — Starting



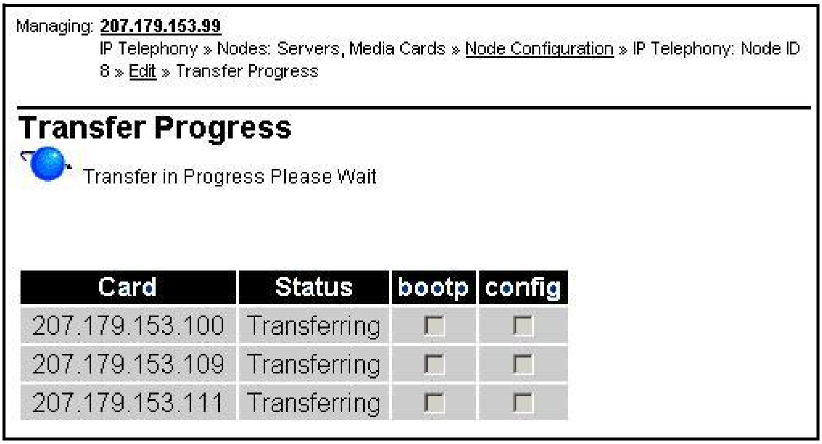
Managing: 207.179.153.99
IP Telephony » Nodes: Servers, Media Cards » Node Configuration » IP Telephony: Node ID 8 » Edit » Transfer Progress

Transfer Progress

Transfer in Progress Please Wait

Card	Status	bootp	config
207.179.153.100	Starting	□	□
207.179.153.109	Starting	□	□
207.179.153.111	Starting	□	□

Figure 123
Transfer Progress — Transferring



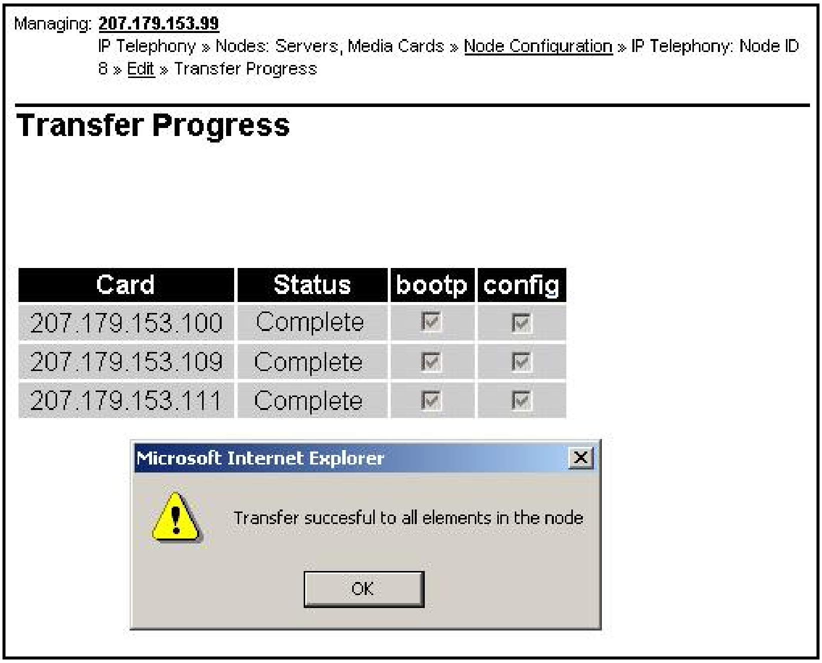
Managing: 207.179.153.99
IP Telephony » Nodes: Servers, Media Cards » Node Configuration » IP Telephony: Node ID 8 » Edit » Transfer Progress

Transfer Progress

Transfer in Progress Please Wait

Card	Status	bootp	config
207.179.153.100	Transferring	□	□
207.179.153.109	Transferring	□	□
207.179.153.111	Transferring	□	□

Figure 124
Transfer Progress — Completed



Managing: 207.179.153.99
IP Telephony » Nodes: Servers, Media Cards » Node Configuration » IP Telephony: Node ID 8 » Edit » Transfer Progress

Transfer Progress

Card	Status	bootp	config
207.179.153.100	Complete	☑	☑
207.179.153.109	Complete	☑	☑
207.179.153.111	Complete	☑	☑

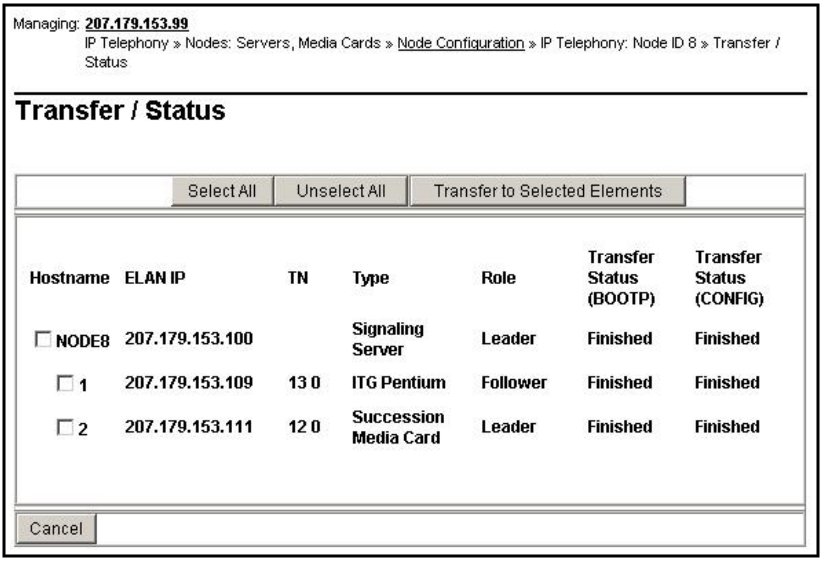
Microsoft Internet Explorer

Transfer succesful to all elements in the node

9 Click **OK**.

The **Transfer / Status** web page opens, as shown in Figure 125 on page 327. This **Transfer / Status** web page allows you to transfer the configuration to selected elements or all elements.

Figure 125
Transfer / Status



Managing: 207.179.153.99
IP Telephony » Nodes: Servers, Media Cards » Node Configuration » IP Telephony: Node ID 8 » Transfer / Status

Transfer / Status

Hostname	ELAN IP	TN	Type	Role	Transfer Status (BOOTP)	Transfer Status (CONFIG)
□ NODE8	207.179.153.100		Signaling Server	Leader	Finished	Finished
□ 1	207.179.153.109	13 0	ITG Pentium	Follower	Finished	Finished
□ 2	207.179.153.111	12 0	Succession Media Card	Leader	Finished	Finished

10 Click **Cancel** to return to the **Node Configuration** web page.

The **Node Configuration** web page (Figure 116 on page 320) reopens if the transfer was successful.

Note: When on the **Node Configuration** web page, clicking **Transfer / Status** opens the **Transfer / Status** web page (see Figure 125). This page is used to send the node configuration files to all IP Telephony components in the node.

- If any element within the Node fails to transfer either BOOTP or CONFIG files, the **Transfer / Status** button is highlighted in red.
- The **Transfer / Status** button is highlighted in yellow if the transfer status of the node elements is unavailable.

End of Procedure

Configuring QoS (DiffServ) values

Quality of Service (QoS) values are configured through Element Manager.

Procedure 14
Configuring QoS (DiffServ) values

1 Select **IP Telephony** > **Nodes: Servers, Media Cards** > **Configuration** from the navigator.

The **Node Configuration** web page opens, as shown in Figure 116 on page 320.

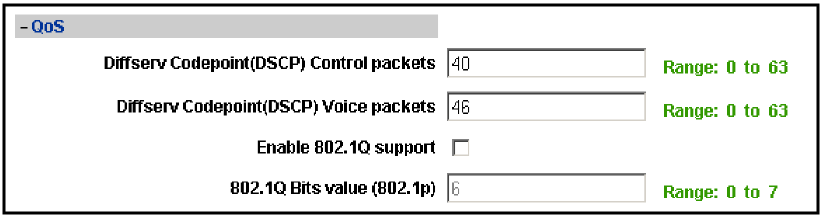
2 Click **Edit** for the appropriate node.

The **Edit** web page opens, as shown in Figure 117 on page 321.

3 Click **QoS**.

The QoS section expands, as shown in Figure 126.

Figure 126
QoS section



- QoS

Diffserv Codepoint(DSCP) Control packets 40 Range: 0 to 63

Diffserv Codepoint(DSCP) Voice packets 46 Range: 0 to 63

Enable 802.1Q support □

802.1Q Bits value (802.1p) 6 Range: 0 to 7

4 Enter the recommended values:

a. **Diffserv Codepoint (DSCP) Control packets =** 40 - Class Selector 5 (CS5). The range is 0 – 63. This configures the priority of the signaling messaging.

b. **Diffserv CodePoint (DSCP) Voice packets =** 46 - Control DSCP - Expedited Forwarding (EF). The range is 0 – 63.

Note: The Differentiated Service (DiffServ) CodePoint (DSCP) determines the priorities of the management and voice packets in the IP Line network. The values are stored in IP telephony CONFIG.INI file. The values used in the IP packets are respectively **160** (40*4) and **184** (46*4).

5 Click **Save and Transfer**.

For more information about Differentiated Service (DiffServ) CodePoint (DSCP), see *Converging the Data Network with VoIP* (553-3001-160) and *IP Line: Description, Installation, and Operation* (553-3001-365).

End of Procedure

Configuring call types

To configure call types and location codes HLOC, HNPA, LOC, NPA, NXX, SPN using Element Manager, follow the steps in Procedure 15.

Procedure 15
Configuring call types

1 Select **Dialing and Numbering Plans > Electronic Switched Network** from the navigator.

The **Electronic Switched Network (ESN)** web page opens.

2 Scroll to the **Numbering Plan (NET)** link (see Figure 127 on page 330).

To configure...	See...
Home Location Code (HLOC)	step 3 on page 331
Home Area Code (HNPA)	step 4 on page 332
Location Code (LOC)	step 5 on page 332
Numbering Plan Area Code (NPA)	step 6 on page 333
Exchange (Central Office) Code (NXX)	step 7 on page 336
Special Number (SPN)	step 8 on page 338

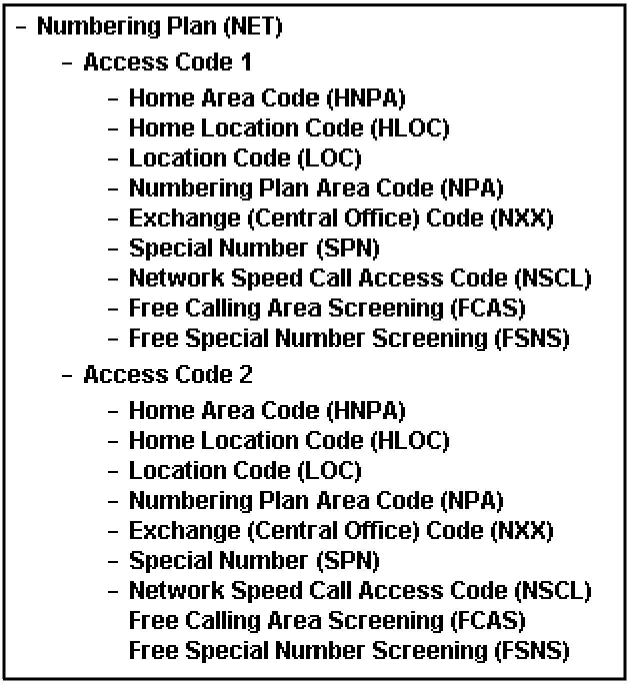
Note 1: Do not provision non-North American numbers as NPA or NXX if you want to configure overlap signaling, as these are still 100% en bloc. For more information about overlap signaling, refer to “Overlap signaling” on page 487.

Note 2: If you use the SPN to provide NPA and NXX equivalents, these can remain associated with the two ESN access codes (that is, AC1 = 6 and AC2 = 9).

- If the destination is accessed by way of another CS 1000 system, then leave the number as an SPN and translate it at the interface to the PSTN.
- If the destination is accessed by way of any other device, then perform call-type conversion as required for that device. Usually, this means changing the call type to national or subscriber (NPA, NXX) in the DMI of the Call Server sending out the number. (Overlap signaling allows this use of NPA and NXX, since the call began as an SPN. This allows national and local number overlap to a third party.)

Note 3: To get an HNPA equivalent with SPN, use local termination (LTER) in the RLI and delete the prefix.

Figure 127
Numbering Plan (NET)

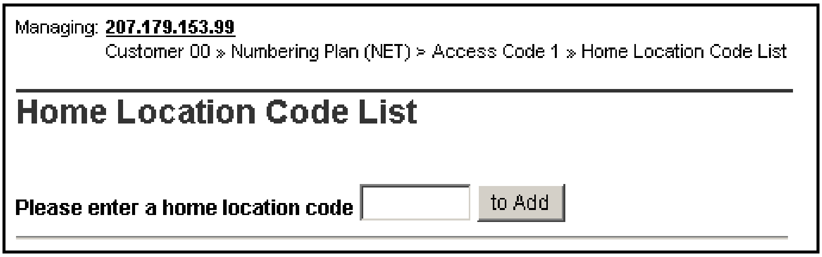

- Numbering Plan (NET)
- Access Code 1
- Home Area Code (HNPA)
- Home Location Code (HLOC)
- Location Code (LOC)
- Numbering Plan Area Code (NPA)
- Exchange (Central Office) Code (NXX)
- Special Number (SPN)
- Network Speed Call Access Code (NSCL)
- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)
- Access Code 2
- Home Area Code (HNPA)
- Home Location Code (HLOC)
- Location Code (LOC)
- Numbering Plan Area Code (NPA)
- Exchange (Central Office) Code (NXX)
- Special Number (SPN)
- Network Speed Call Access Code (NSCL)
Free Calling Area Screening (FCAS)
Free Special Number Screening (FSNS)

3 To configure Home Location Code, perform the following steps:

a. Click **Home Location Code (HLOC)** under **Access Code 1** or **Access Code 2**.

The **Home Location Code List** web page opens, as shown in Figure 128.

Figure 128
Home Location Code List web page



Managing: 207.179.153.99
Customer 00 » Numbering Plan (NET) > Access Code 1 » Home Location Code List

Home Location Code List

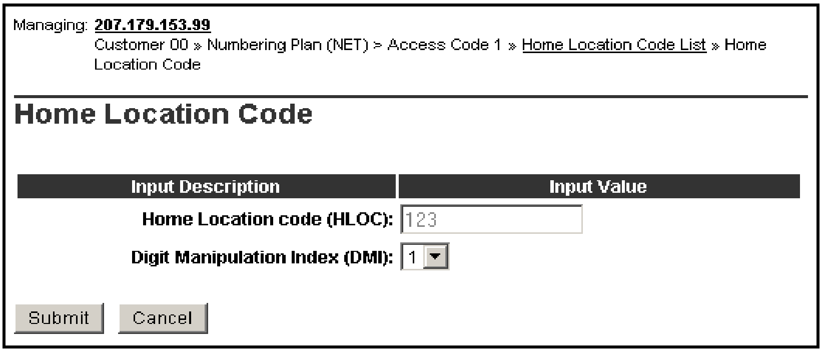
Please enter a home location code

b. Enter a code in the **home location code** text box.

c. Click **to Add**.

The **Home Location Code** web page opens, as shown in Figure 129. The **Home Location code (HLOC)** is auto-filled.

Figure 129
Home Location Code web page



Managing: 207.179.153.99
Customer 00 » Numbering Plan (NET) > Access Code 1 » Home Location Code List » Home Location Code

Home Location Code

Input Description	Input Value
Home Location code (HLOC):	123
Digit Manipulation Index (DMI):	1

d. Select a **Digit Manipulation Index (DMI)**.

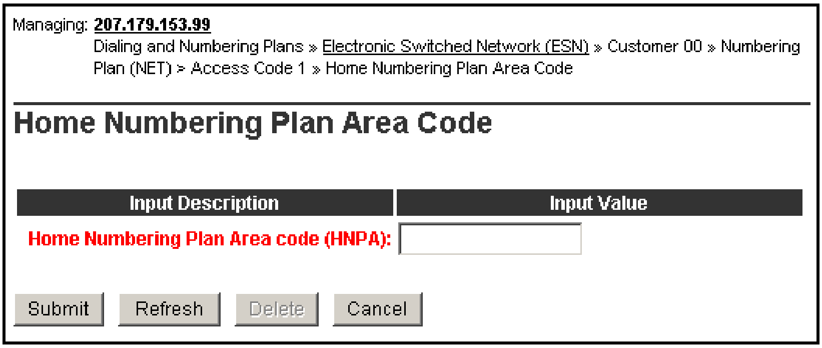
e. Click **Submit**.

4 To configure Home Area Code (HNPA), perform the following steps:

a. Click **Home Area Code (HNPA)** under **Access Code 1** or **Access Code 2**

The **Home Numbering Plan Area Code** web page opens, as shown in Figure 130.

Figure 130
Home Numbering Plan Area Code web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) > Access Code 1 » Home Numbering Plan Area Code

Home Numbering Plan Area Code

Input Description	Input Value
Home Numbering Plan Area code (HNPA):	

b. Enter the **Home Number Plan Area code (HNPA)** in the text box.

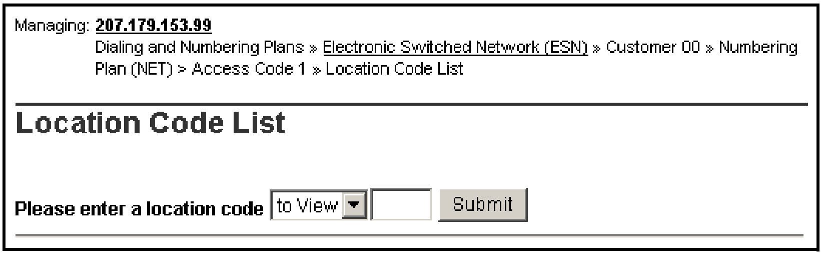
c. Click **Submit**.

5 To configure Location Code (LOC), perform the following steps:

a. Click **Location Code (LOC)** under **Access Code 1** or **Access Code 2**.

The **Location Code List** web page opens, as shown in Figure 131.

Figure 131
Location Code List web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) > Access Code 1 » Location Code List

Location Code List

Please enter a location code to View

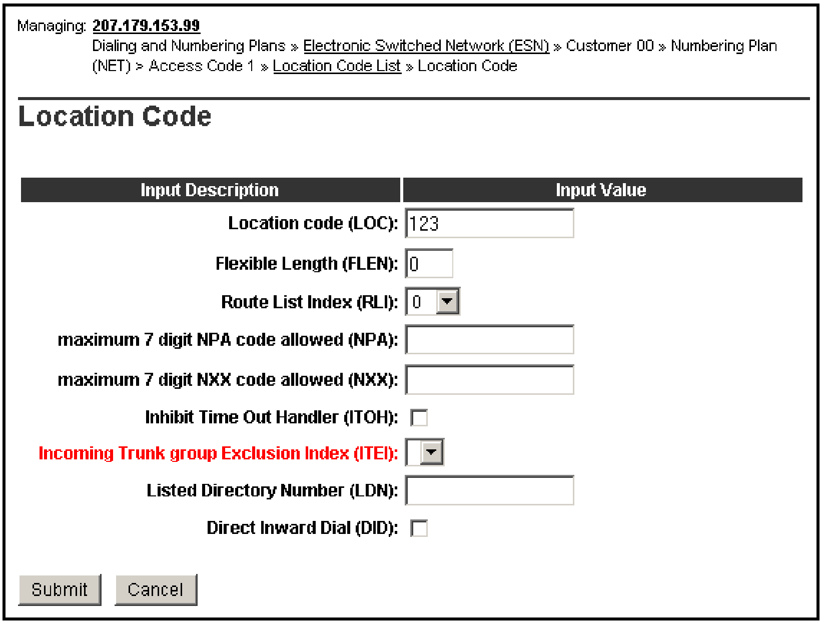
b. Enter a code in the **location code** text box.

c. Select **to Add** from the drop-down list.

d. Click **Submit**.

The **Location Code** web page opens, as shown in Figure 132.

Figure 132
Location Code web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) > Access Code 1 » Location Code List » Location Code

Location Code

Input Description	Input Value
Location code (LOC):	123
Flexible Length (FLEN):	0
Route List Index (RLI):	0
maximum 7 digit NPA code allowed (NPA):	
maximum 7 digit NXX code allowed (NXX):	
Inhibit Time Out Handler (ITOH):	☐
Incoming Trunk group Exclusion Index (ITEI):	
Listed Directory Number (LDN):	
Direct Inward Dial (DID):	☐

e. Enter the appropriate information.

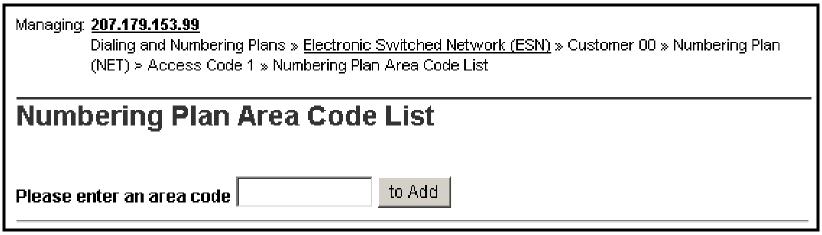
f. Click **Submit**.

6 To configure Number Plan Area Code (NPA), perform the following steps:

a. Click **Numbering Plan Area Code (NPA)** under **Access Code 1** or **Access Code 2**.

The **Numbering Plan Area Code List** web page opens, as shown in Figure 133 on page 334.

Figure 133
Numbering Plan Area Code List web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) > Access Code 1 » Numbering Plan Area Code List

Numbering Plan Area Code List

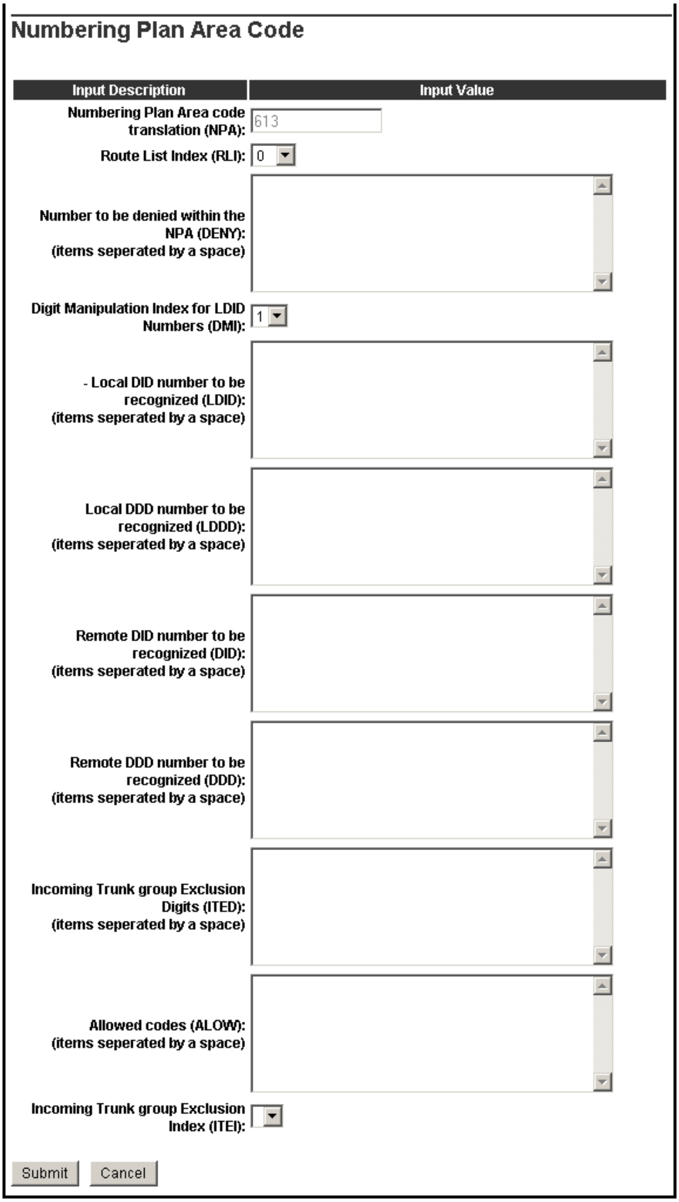
Please enter an area code

b. Enter an area code.

c. Click **to Add**.

The **Numbering Plan Area Code** web page opens, as shown in Figure 134 on page 335.

Figure 134
Numbering Plan Area Code web page



Numbering Plan Area Code

Input Description	Input Value
Numbering Plan Area code translation (NPA):	613
Route List Index (RLI):	0
Number to be denied within the NPA (DENY): (items seperated by a space)	
Digit Manipulation Index for LDID Numbers (DMI):	1
- Local DID number to be recognized (LDID): (items seperated by a space)	
Local DDD number to be recognized (LDDD): (items seperated by a space)	
Remote DID number to be recognized (DID): (items seperated by a space)	
Remote DDD number to be recognized (DDD): (items seperated by a space)	
Incoming Trunk group Exclusion Digits (ITED): (items seperated by a space)	
Allowed codes (ALOW): (items seperated by a space)	
Incoming Trunk group Exclusion Index (ITEI):	

d. Enter the appropriate information.

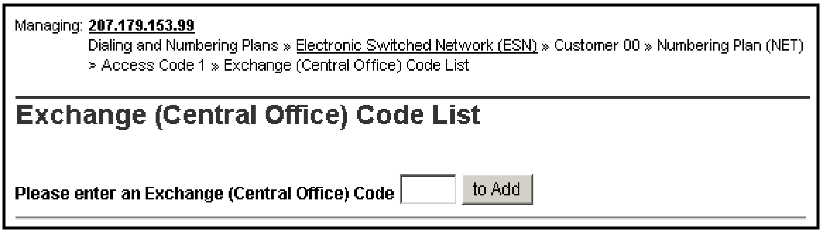
e. Click **Submit**.

7 To configure Exchange (Central Office) Code (NXX), perform the following steps:

a. Click **Exchange (Central Office) Code (NXX)** under **Access Code 1** or **Access Code 2**.

The **Exchange (Central Office) Code List** web page opens, as shown in Figure 135.

Figure 135
Exchange (Central Office) Code List web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 1 » Exchange (Central Office) Code List

Exchange (Central Office) Code List

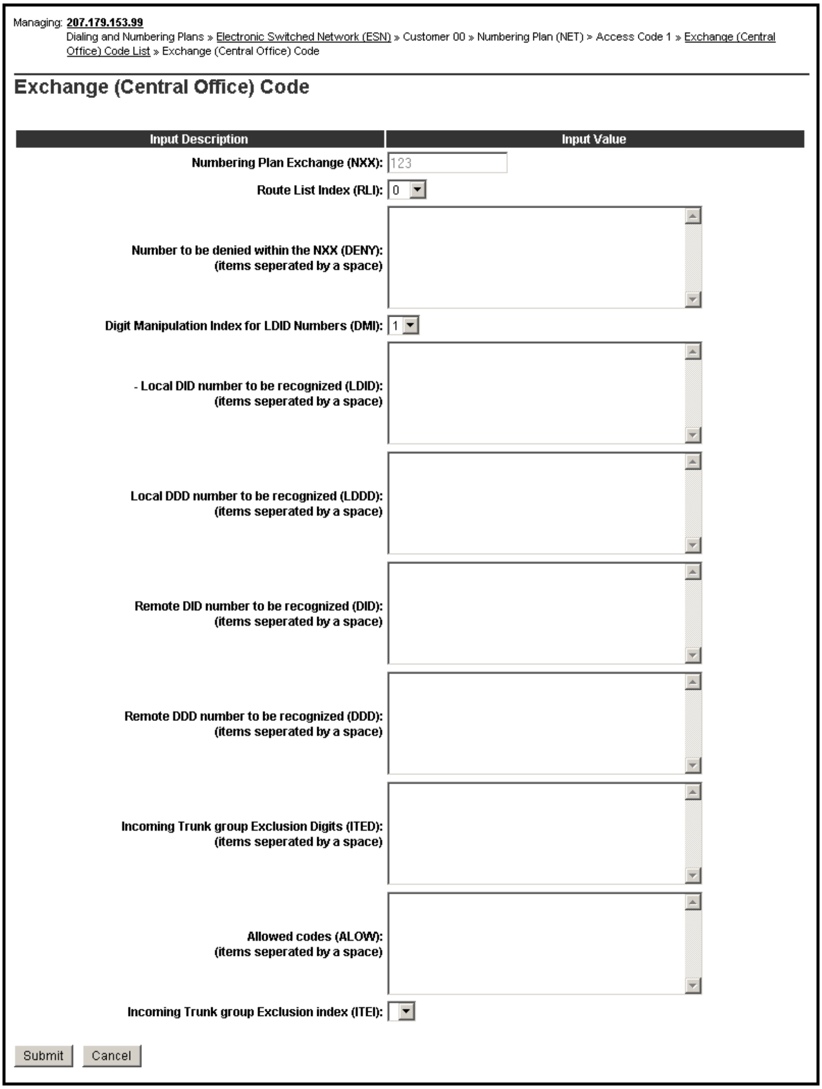
Please enter an Exchange (Central Office) Code

b. Enter the **Exchange (Central Office) Code** in the text box.

c. Click **to Add**.

The **Exchange (Central Office) Code** web page opens, as shown in Figure 136 on page 337.

Figure 136
Exchange (Central Office) Code web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) > Access Code 1 » Exchange (Central Office) Code List » Exchange (Central Office) Code

Exchange (Central Office) Code

Input Description	Input Value
Numbering Plan Exchange (NXX):	123
Route List Index (RLI):	0
Number to be denied within the NXX (DENY): (items seperated by a space)	
Digit Manipulation Index for LDID Numbers (DMI):	1
- Local DID number to be recognized (LDID): (items seperated by a space)	
Local DDD number to be recognized (LDDD): (items seperated by a space)	
Remote DID number to be recognized (DID): (items seperated by a space)	
Remote DDD number to be recognized (DDD): (items seperated by a space)	
Incoming Trunk group Exclusion Digits (ITED): (items seperated by a space)	
Allowed codes (ALOW): (items seperated by a space)	
Incoming Trunk group Exclusion index (ITEI):	

d. Enter the appropriate information.

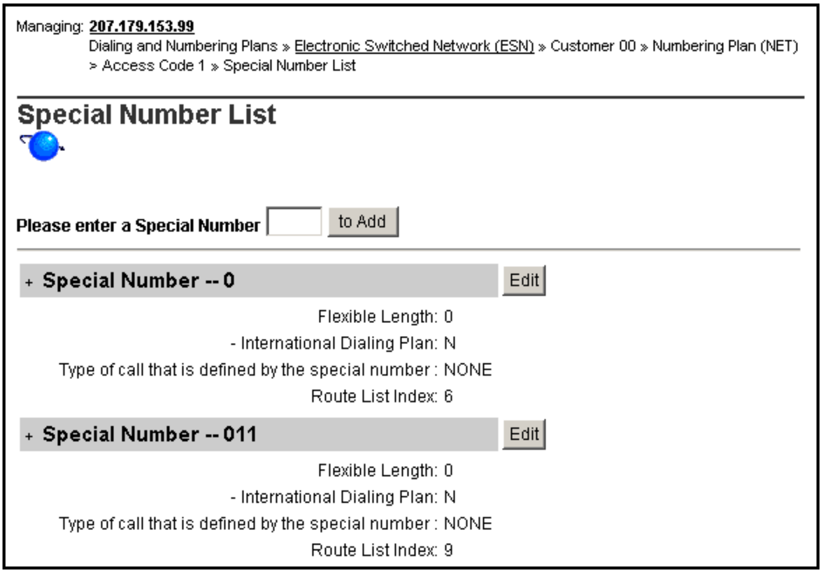
e. Click **Submit**.

8 To configure Special Number (SPN), perform the following steps:

a. Click **Special Number (SPN)** under **Access Code 1** or **Access Code 2**.

The **Special Number List** web page opens, as shown in Figure 137.

Figure 137
Special Number List web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) > Access Code 1 » Special Number List

Special Number List

Please enter a Special Number [ ] to Add

+ Special Number -- 0 Edit

Flexible Length: 0
- International Dialing Plan: N
Type of call that is defined by the special number : NONE
Route List Index: 6

+ Special Number -- 011 Edit

Flexible Length: 0
- International Dialing Plan: N
Type of call that is defined by the special number : NONE
Route List Index: 9

b. Enter the number.

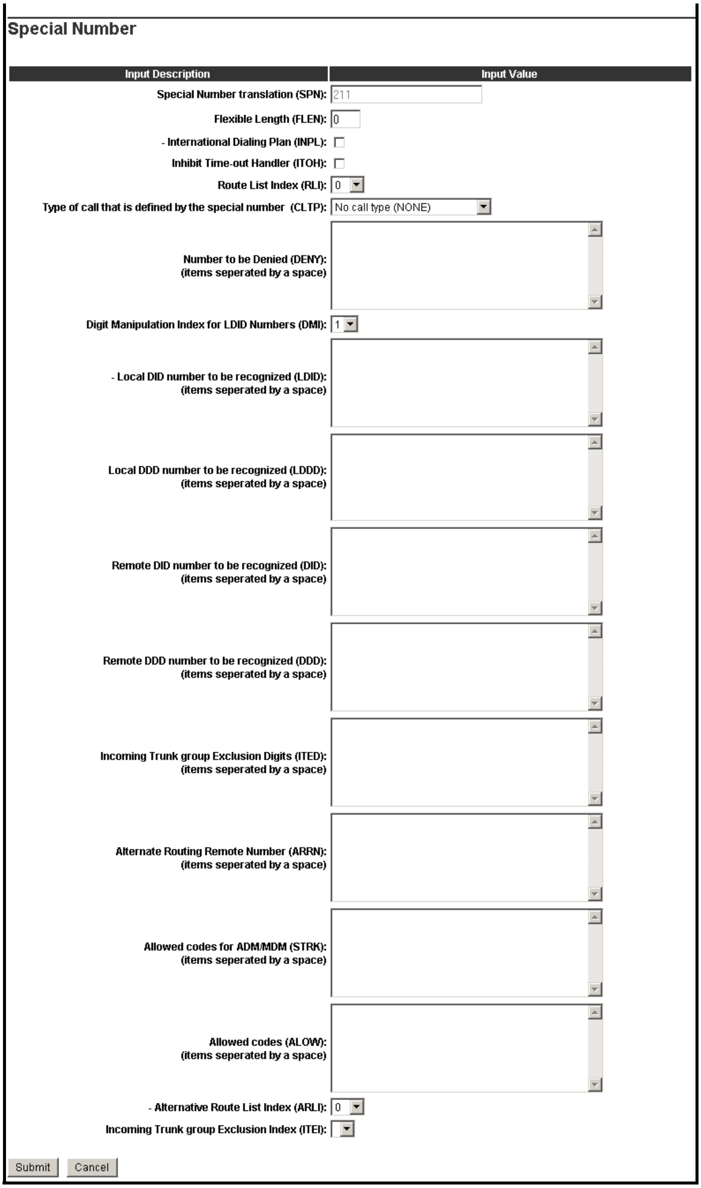
c. Click **to Add**.

The **Special Number** web page opens (see Figure 138 on page 339).

d. Enter the appropriate information.

e. Click **Submit** at the bottom of the web page.

Figure 138
Special Number



Special Number

Input Description	Input Value
Special Number translation (SPN):	211
Flexible Length (FLEN):	0
- International Dialing Plan (INPL):	□
Inhibit Time-out Handler (ITOH):	□
Route List Index (RLI):	0
Type of call that is defined by the special number (CLTP):	No call type (NONE)
Number to be Denied (DENY): (items seperated by a space)	
Digit Manipulation Index for LDID Numbers (DMI):	1
- Local DID number to be recognized (LDID): (items seperated by a space)	
Local DDD number to be recognized (LDDD): (items seperated by a space)	
Remote DID number to be recognized (DID): (items seperated by a space)	
Remote DDD number to be recognized (DDD): (items seperated by a space)	
Incoming Trunk group Exclusion Digits (ITED): (items seperated by a space)	
Alternate Routing Remote Number (ARRN): (items seperated by a space)	
Allowed codes for ADM/MDM (STRK): (items seperated by a space)	
Allowed codes (ALOW): (items seperated by a space)	
- Alternative Route List Index (ARLI):	0
Incoming Trunk group Exclusion Index (ITEI):	

f. Enter the appropriate information.

g. Click **Submit** at the bottom of the web page.

End of Procedure

Configuring digit manipulation tables

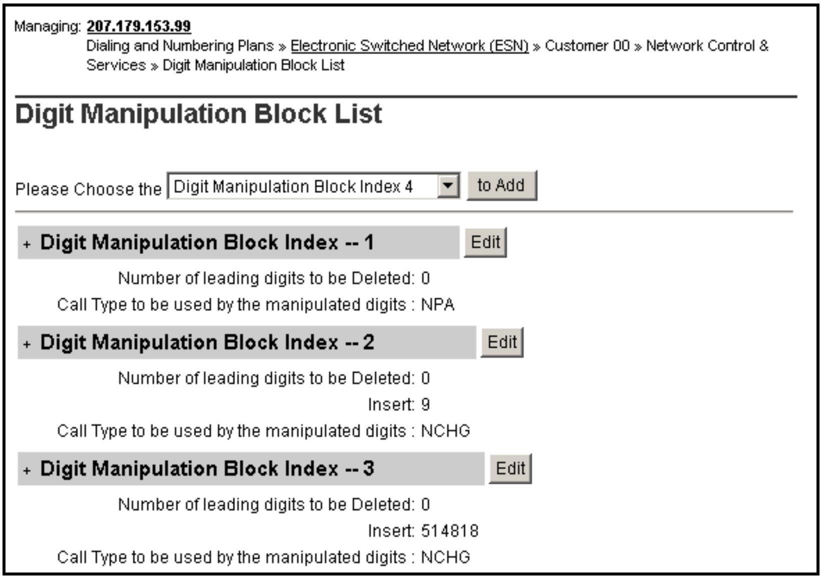
Procedure 16
Configuring digit manipulation tables

1 Select **Dialing and Numbering Plans > Electronic Switched Network** from the navigator.

2 On the **Electronic Switched Network (ESN)** web page shown in Figure 107 on page 311, select **Customer xx > Network Control & Services > Digit Manipulation Block (DGT)**.

The **Digit Manipulation Block List** web page opens, as shown in Figure 139.

Figure 139
Digit Manipulation Block List web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List

Digit Manipulation Block List

Please Choose the Digit Manipulation Block Index 4 to Add

+ Digit Manipulation Block Index -- 1 Edit

Number of leading digits to be Deleted: 0
Call Type to be used by the manipulated digits : NPA

+ Digit Manipulation Block Index -- 2 Edit

Number of leading digits to be Deleted: 0
Insert: 9
Call Type to be used by the manipulated digits : NCHG

+ Digit Manipulation Block Index -- 3 Edit

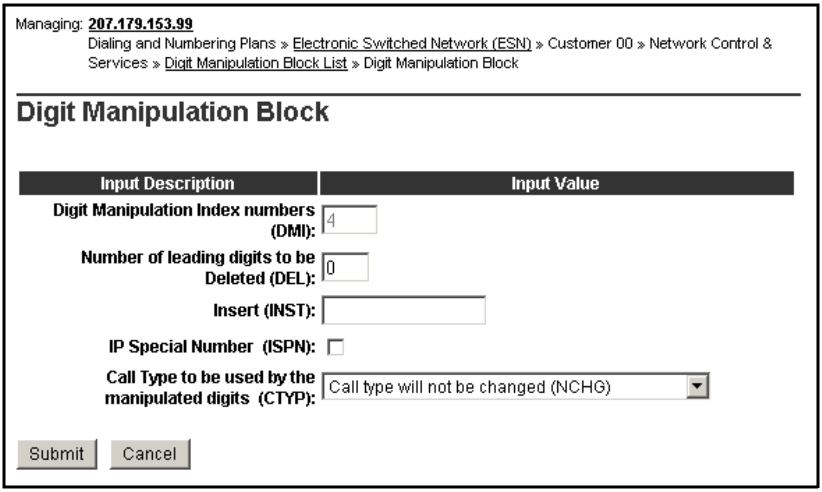
Number of leading digits to be Deleted: 0
Insert: 514818
Call Type to be used by the manipulated digits : NCHG

3 Select a **Digit Manipulation Block Index** number in the drop-down list.

4 Click **to Add**.

The **Data Manipulation Block** web page opens, as shown in Figure 140.

Figure 140
Digit Manipulation Block web page



Managing: **207.179.153.99**
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List » Digit Manipulation Block

Digit Manipulation Block

Input Description	Input Value
Digit Manipulation Index numbers (DMI):	4
Number of leading digits to be Deleted (DEL):	0
Insert (INST):	
IP Special Number (ISPN):	☐
Call Type to be used by the manipulated digits (CTYP):	Call type will not be changed (NCHG)

5 Enter the appropriate information.

6 Click **Submit**.

End of Procedure

Feature Implementation of IP Peer Networking

If you are using the Command Line Interface (CLI), use the following implementation tables to configure the IP Peer Networking feature.

Task summary list

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

1. LD 17 – Configure D-channels.
2. LD 15 – Configure network settings and options.
3. LD 16 – Configure the route. This route can be configured as an H.323 route or a SIP route.
    - To configure a SIP route, see 346.
    - To configure an H.323 route, see 348.
4. LD 97 – Configure the superloop for the Virtual Trunks.
5. LD 14 – Configure Virtual Trunks.
6. LD 86 – Configure dialing plan, networking, and ESN data.
7. LD 87 – Configure network access.
8. LD 86 – Configure the Digit Manipulation Index.
9. LD 86 – Configure the Route List Block for the Virtual Trunk route.
10. LD 87 – Configure CDP steering codes.
11. LD 90 – Configure call types and Location Codes.

LD 17 – Configure D-channels. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	ADAN	Action Device And Number
- ADAN	NEW DCH xx	Action Device And Number, where xx is 0-63.
CAB_TYPE		Cabinet Type
	IP FIBR	IP Expansion Cabinet or Media Gateway Fiber Expansion Cabinet

LD 17 – Configure D-channels. (Part 2 of 2)

Prompt	Response	Description
- CTYP	 DCIP	Card Type D-channel over IP
- DES	x...x	Designator
BANR	YES	Enable security banner printing option
- IFC	SL1	Interface type for D-channel
CO_TYPE	aaa	Central Office switch type, where aaa = (STD) or ATT
- RCVP	YES	Auto-recovery to primary D-channel option.
- - ISLM	(4000)	Integrated Services Signaling Link Maximum The maximum number of ISL trunks controlled by the D-channel. ***Note:*** ISLM prompt is hidden for D-channel on IP and is defaulted to 4000.
- OTBF	1-(32)-127	Output Request Buffers
- RLS	xx	Release ID of the switch at the far end of the D-channel
- RCAP	 ND2	Remote Capabilities Network Name Display method 2
	MWI	Message Waiting Indication support over SIP using a SIP NOTIFY message rather than an MCDN message encapsulated in SIP. ***Note:*** MWI is also used for H.323 if a BCM is in the network.

LD 15 – Configure network settings and options. (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Add new block Change existing data
TYPE:	NET	ISDN and ESN Networking options
CUST		Customer number
	0-99	Range for Large System and CS 1000E system
	0-31	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
...		
OPT	a...a	Options
AC2		Access Code 2
		Enter call types that use Access Code 2 as defined in LD 86, for automatic insertion of UDP access code. Multiple responses are permitted. If a numbering plan is not entered here, it is automatically defaulted to AC1.
	NPA NXX INTL SPN LOC	E.164 National number E.164 Subscriber number International number Special Number Location Code
FNP	(YES)	Enable Flexible Numbering Plan for customer
ISDN	YES	Integrated Services Digital Network
VPNI	1-16283	Virtual Private Network Identifier
- PNI	(0)-32700	Private Network Identifier
- CLID	(NO)	Do not enable Calling Line Identification option

LD 15 – Configure network settings and options. (Part 2 of 2)

Prompt	Response	Description
CNTC	xx	Country code (see Note 1 on 345)
NATC	xx	National access code (see Note 1on 345)
INTC	xxx	International access code (see Note 1on 345)

Note 1: CNTC, NATC and INTC are needed when a public call is tandemed over the Virtual Trunk.

— CNTC is the country code for the country where the switch is located. For example, CNTC = 1 for Canada.

— NATC is the national access code. For example, NATC = 1 for Canada.

— INTC is the international access code. For example, INTC = 011 for Canada.
For example, a caller who wants to reach Austria dials 6-011-61-xxxyyyzzz from endpoint A (for example, in Toronto) over the Virtual Trunk to endpoint B (for example, in the United Kingdom) which serves as a gateway to the PSTN.

The 011 is stripped off at endpoint A because the NRS does not understand it. Endpoint B would receive 61-xxxyyyzzz and compare 61 with its CNTC (= 44) and assumes that this is an international call. So, it inserts the INTC (= 00 for Europe) and sends 00-61-xxxyyyzzz to the PSTN routing to Austria.

Consider another caller from endpoint A making a call to the UK PSTN by dialing 6-011-44-xxxyyyzzz. Endpoint B would receive 44-xxxyyyzzz. It finds that 44 equals to its CNTC and figures that this is a national call. So, it strips off 44 and inserts the NATC (= 0 for UK) and sends 0-xxxyyyzzz to the PSTN.

Note 2: In the Route Data Block, the zone parameter makes the codec selections and calculates the bandwidth usage for calls to the trunk members of a given route.

Configure the routes:

- To configure a SIP route, see "LD 16 – Configure the SIP route." below.
- To configure an H.323 route, see "LD 16 – Configure the H.323 route." on page 348.

LD 16 – Configure the SIP route. (Part 1 of 3)

Prompt	Response	Description
REQ	NEW	Add a new route.
TYPE	RDB	Route Data Block
CUST	xx	Customer number as defined in LD 15.
ROUT		Route number
	0-511	Range for Large System and CS 1000E system
	0-127	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
DES	x...x	Designator The designator field for the trunk groups. This designator can be 0-16 alphanumeric characters.

LD 16 – Configure the SIP route. (Part 2 of 3)

Prompt	Response	Description
TKTP		Trunk Type
	TIE	TIE trunk
VTRK		Virtual Trunk route, where:
	YES	YES = This route is for Virtual Trunk NO = This route is not for Virtual Trunk (default)
ZONE	0-255	Zone for codec selection and bandwidth management
PCID	SIP	Protocol ID for the SIP route. Defines the route as a SIP route.
CRID	(NO) YES	CDR record (for SIP) to include correlation ID. YES = When enabled, the fourth line is included in the new CDR record. NO = The fourth line in not included in the CDR record (default). See *Call Detail Recording: Description and Formats* (553-3001-350) for more information. ***Note:*** This prompt appears only for a SIP Virtual Trunk (that is, if VTRK = YES and PCID = SIP) and CDR is turned on for this route.
NODE	xxxx	Node ID Where the Node ID matches the node of the Signaling Server. The Node ID can have a maximum of four numeric characters.
ISDN	YES	Integrated Services Digital Network option
- MODE	ISLD	Mode of operation
- DCH	0-159	D-channel number

LD 16 – Configure the SIP route. (Part 3 of 3)

Prompt	Response	Description
- IFC	SL1	Interface type for route (IFC responses are listed in *Software Input/Output: Administration* (553-3001-311))
- SRVC	a...a	Service type for AT&T ESS connections (SRVC responses are listed in *Software Input/Output: Administration* (553-3001-311))
- - PNI	(0)-32700	Private Network Identifier
- NCNA	(YES)	Network Calling Name Allowed
- NCRD	YES	Network Call Redirection
- INAC	(NO) YES	Inserts the ESN access code to an incoming private network call. INAC enables an ESN access code to be automatically added to an incoming ESN call from a private network. If INAC = YES, then digit insertion (INST) for NARS or BARS calls is bypassed and Access Code 1 (AC1) is used for all call types. However, calls can be specifically defined to use Access Code 2 (AC2) in LD 15 at the AC2 prompt. INAC is prompted when the route type is either a TIE trunk or an IDA trunk with DPNSS1 signaling.
ICOG		Incoming and Outgoing trunk.
	IAO	Incoming and Outgoing
ACOD	x...x	Access Code for the trunk route.

LD 16 – Configure the H.323 route. (Part 1 of 3)

Prompt	Response	Description
REQ	NEW	Add a new route.

LD 16 – Configure the H.323 route. (Part 2 of 3)

Prompt	Response	Description
TYPE	RDB	Route Data Block
CUST	xx	Customer number as defined in LD 15.
ROUT		Route number
	0-511	Range for Large System and CS 1000E system
	0-127	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
DES	x...x	Designator The designator field for the trunk groups. This designator can be 0-16 alphanumeric characters.
TKTP		Trunk Type
	TIE	TIE trunk
VTRK		Virtual Trunk route, where:
	YES	YES = This route is for Virtual Trunk NO = This route is not for Virtual Trunk (default)
ZONE	0-255	Zone for codec selection and bandwidth management
NODE	xxxx	Node ID Where the Node ID matches the node of the Signaling Server. The Node ID can have a maximum of four numeric characters.
PCID	H323	Protocol ID for the H.323 route.
ISDN	YES	Integrated Services Digital Network option
- MODE	ISLD	Mode of operation
- DCH	0-159	D-channel number

LD 16 – Configure the H.323 route. (Part 3 of 3)

Prompt	Response	Description
- IFC	SL1	Interface type for route (IFC responses are listed in *Software Input/Output: Administration* (553-3001-311))
- SRVC	a...a	Service type for AT&T ESS connections (SRVC responses are listed in *Software Input/Output: Administration* (553-3001-311))
- - PNI	(0)-32700	Private Network Identifier
- NCNA	(YES)	Network Calling Name Allowed
- NCRD	YES	Network Call Redirection
- INAC	(NO) YES	Inserts the ESN access code to an incoming private network call. INAC enables an ESN access code to be automatically added to an incoming ESN call from a private network. If INAC = YES, then digit insertion (INST) for NARS or BARS calls is bypassed and Access Code 1 (AC1) is used for all call types. However, calls can be specifically defined to use Access Code 2 (AC2) in LD 15 at the AC2 prompt. INAC is prompted when the route type is either a TIE trunk or an IDA trunk with DPNSS1 signaling.

LD 97 – Configure the superloop for the Virtual Trunks. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change existing data.

LD 97 – Configure the superloop for the Virtual Trunks. (Part 2 of 2)

Prompt	Response	Description
TYPE	SUPL	Superloop
SUPL	 0-159 0-255	Superloop number 0-159: Superloop number in multiples of 4 0-255: Systems with Fiber Network Fabric

LD 14 – Configure Virtual Trunks. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW NEW x	Create a trunk Create x trunks, where x = 1-255 (to create that number of consecutive trunks)
TYPE	IPTI	IP TIE trunk data block
TN		Terminal Number
	l s c u	Format for Large System and CS 1000E system, where l = loop, s = shelf, c = card, u = unit
	c u	Format for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T, where c = card and u = unit
DES	a....a	Virtual Trunk descriptor Designator field for trunk groups where a...a = 0-16 alphanumeric characters (DES is an optional entry)
XTRK	 VTRK	Extended Trunk Virtual Trunk type ***Note:*** If you entered a virtual TN at the TN prompt, then the XTRK prompt only accepts the VTRK option.
CUST	xx	Customer number as defined in LD 15.

LD 14 – Configure Virtual Trunks. (Part 2 of 2)

Prompt	Response	Description
...		
RTMB		Route number and Member Number
	0-511 1-4000	Range for Large System and CS 1000E system
	0-127 1-4000	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
CHID	1-4300	Channel ID for this trunk, dependent on the ISLM parameter (LD 17)
STRI		Start arrangement Incoming
	IMM	Immediate
STRO		Start arrangement Outgoing
	IMM	Immediate
SUPN	YES	Answer and disconnect Supervision required
		SUPN must equal YES for a COT with Virtual Network Service
...		
TKID	nnnnnnn	Trunk Identifier

LD 86 – Configure dialing plan, networking, and ESN data. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
FEAT	ESN	Electronic Switched Network

LD 86 – Configure dialing plan, networking, and ESN data. (Part 2 of 2)

Prompt	Response	Description
MXLC	0-999 0-16000	Maximum number of Location Codes (NARS only) Maximum number of Location Codes (NARS only) (with the ESN Location Code Expansion feature and the FNP feature enabled). Refer to ESN Location Code Expansion feature in *ISDN Primary Rate Interface: Features* (553-3001-369).
...		
CDP	YES	Coordinated Dialing Plan feature for this customer
- MXSC	x	Maximum number of Steering Codes Where x = • 0-8000 = Maximum number of Steering Codes for Small Systems and CS 1000S Systems • 0-10000 = Maximum number of Steering Codes in North America • 0-32000 = Maximum number of Steering Codes outside North America
- NCDP	x	Number of digits to be included as part of the CDP DN (DSC + DN or LSC + DN) where x = 3-7.
AC1	x	One- or two-digit NARS/BARS Access Code 1
AC2	x	One- or two-digit NARS Access Code 2
DLTN	(YES)	NARS/BARS Dial Tone after dialing AC1 or AC2 access codes
ERWT	(YES)	Expensive Route Warning Tone
...		
TGAR	(NO)	Check for Trunk Group Access Restriction.

LD 87 – Configure network access.

Prompt	Response	Description
REQ	NEW	Add new data.
FEAT	NCTL	Network Control Block
SOHQ	(NO)	Off-Hook Queuing option
SCBQ	(NO)	Call-Back Queuing option
NCOS	(0)	Network Class of Service group number
TOHQ	(0)	TCOS OHQ eligibility

LD 86 – Configure the Digit Manipulation Index. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data.
CUST	xx	Customer number as defined in LD 15.
FEAT	DGT	Digit manipulation data block
DMI	xxxx	Digit Manipulation Index numbers Digit Manipulation Index with Flexible Numbering Plan (FNP) package 160 DMI is only prompted when the Directory Number Expansion (DNXP) package 150 is equipped and SDRR = LDID.
DEL	xx	Delete Number of leading digits to be deleted
INST	<cr>	Insert Up to 31 leading digits can be inserted

LD 86 – Configure the Digit Manipulation Index. (Part 2 of 2)

Prompt	Response	Description
CTYP	<cr>	Call Type to be used by the manipulated digits. This call type must be recognized by the far-end switch.
...		

Nortel recommends that all routes in a Route List Block (RLI) be configured as either overlap or en bloc. That is, an en bloc route should not have alternate routes that are configured as overlap, and vice versa. Erratic behavior can occur when overlap and en bloc routes are configured as alternate routes. Normal behavior occurs on alternate routes as long as the alternate route has the same overlap capabilities as the main route.

LD 86 – Configure the Route List Block for the Virtual Trunk route. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
FEAT	RLB	Route list block
...		
RLI	 0-127 0-255 0-999	Route List Index to be accessed CDP and BARS NARS FNP
ENTR	xxx	Entry number for NARS/BARS Route list Where xxx = • 0-63 Entry number for NARS/BARS Route List • 0-6 Route list entry number for CDP • X Precede with x to remove
LTER	(NO)	Local Termination entry

LD 86 – Configure the Route List Block for the Virtual Trunk route. (Part 2 of 2)

Prompt	Response	Description
ROUT		Route number
	0-511	Range for Large System and CS 1000E system
	0-127	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
DMI		Digit Manipulation Index
	0	No digit manipulation required
	1-31	CDP
	0-255	NARS and BARS
	0-999	FNP
...		

LD 87 – Configure the CDP steering codes. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
FEAT	CDP	Coordinated Dialing Plan
TYPE		Type of steering code
	DSC	Distant Steering Code
DSC	x..x	Distant Steering Code Up to 4 digits; up to 7 digits with Directory Number Expansion (DNXP) package 150.
- FLEN	(0)	Flexible Length number of digits
- DSP	(LSC)	Display (Local Steering Code)
- RRPA	(NO)	Remote Radio Paging Access

LD 87 – Configure the CDP steering codes. (Part 2 of 2)

Prompt	Response	Description
- RLI		Route List Index to be accessed for Distant Steering Code. Cannot use non-zero entries or DMI.
	0-31	CDP
	0-127	BARS
	0-255	NARS
	0-999	Flexible Numbering Plan (FNP)
- CCBA	(NO)	Collect Call Blocking (CCB) Denied
- NPA	<cr>	North American Numbering Plan Routing code: maximum 7-digit National code enabled
- NXX	<cr>	North American Numbering Plan Routing code: maximum 7-digit subscriber code allowed

LD 90 – Configure call types and Location Codes. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
	CHG	Change existing data block
CUST	xx	Customer number as defined in LD 15.
FEAT	NET	Network Translator (Network translation tables)
TRAN		Translator
	AC1	Access Code 1 (NARS/BARS)
	AC2	Access Code 2 (NARS)
TYPE	LOC	Location Code
LOC	x...x	Location Code

LD 90 – Configure call types and Location Codes. (Part 2 of 2)

Prompt	Response	Description
- FLEN	(0)-10	Flexible Length Enter the maximum number of digits expected. When this number of digits is dialed, dialing is considered to be complete and end-of-dial processing begins. Default is zero (0) digits.
- RLI	0-999	Route List Index Enter Route List Index for this LOC.
…		

VNR enhancement

To configure the VNR enhancement, configure AC2, PFX1, VNR, RLI, CDPL, UDPL, CNTC, CATC, and INTC in LD 15.

LD 15 – Configure the VNR enhancement. (Part 1 of 7)

Prompt	Response	Description
REQ:	NEW	Add new data block to the system.
TYPE:	NET	ISDN and ESN networking options
CUST		Customer number
	0-99	Range for Large System and CS 1000E system
	0-31	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
OPT		Options
	RTD	Coordinated Dialing Plan routing feature Denied
AC2	SPN LOC	Special Number; Location Code
FNP	(YES)	Enable Flexible Numbering Plan for customer.

LD 15 – Configure the VNR enhancement. (Part 2 of 7)

Prompt	Response	Description
ISDN	YES	Integrated Services Digital Network allowed for customer. ***Note:*** Prompted when ISDN signaling package 145 is equipped and either the Integrated Service Digital Network BRI Trunk Access (BRIT) package 233 is equipped or at least one PRA link is configured.
- VPNI	1-16283	Virtual Private Network Identifier
- CLID	YES	Allow Calling Line Identification option Calling Line Identification does not require ISDN.
- - ENTRY	xx	CLID entry to be configured. CLID entries must be between 0 and the value entered at the SIZE prompt - 1. Precede entry or entries with X to delete. ENTRY is repeated until a <cr> is entered.
- - - HLOC	100-9999999	Home Location Code (ESN) as defined in LD 90 1 to 7 digits with extended code. Prompted when ISDN=YES, or with Digital Private Network Signaling System 1 (DPNSS) package 123.
- - - LSC	0 .. x..x	Local Steering Code 1 to 7 digits. LSCs are required if the CDP DNs are longer than the local PDNs. The CLID sent for a CDP call is composed of the LSC defined in LD 15 plus the PDN of the calling set. Various ISDN network features depend on the CLID as the return address for sending feature control messages. Multiple LSCs may be defined in LD 87 for CDP but only one LSC can be defined here for the CLID. The LSC prompt appears only if the user has a five or six digit dialing plan, or if the DPNSS software package is equipped. LSC is prompted here if ISDN = NO, otherwise LSC is a subprompt of ISDN.

LD 15 – Configure the VNR enhancement. (Part 3 of 7)

Prompt	Response	Description
- PFX1	xxxx	Prefix 1. Prefix or area code for International PRA. First element of Calling Party Number. PFX1 + PFX2 + DN cannot exceed 8 numbers for AXE-10. Prompted with International Primary Rate Access (IPRA) package 202.
- PRX2	xxxx	Prefix 2. Central Office Prefix for International PRA. Second element of Calling Part Number. PFX1 + PFX2 + DN cannot exceed 8 numbers for AXE-10. Prompted with International Primary Rate Access (IPRA) package 202.
- RCNT	0-(5)	Redirection Count for ISDN calls Maximum number of inter-node hops allowed in a network redirection call, only enforced when ISDN = YES. This field must be set to greater than 0 for a network redirection to take place.
- PSTN	(NO)	Public Service Telephone Networks Limit the number of PSTNs allowed in a network connection to one PSTN. The default (NO) puts no limit on the number of PSTN connections.
- - TNDM	0-(15)-31	Tandem Threshold/Loop Avoidance Limit This is the value permitted in a network connection. If the value entered is greater than 25, then 25 will be used for DPNSS calls. Prompted when Integrated Services Digital Network (ISDN) package 245 and ISDN Supplementary Features (ISDN INTL SUP) package 161, or Digital Private Signaling System Network Services (DNWK) package 231 is equipped.

LD 15 – Configure the VNR enhancement. (Part 4 of 7)

Prompt	Response	Description
- - PCMC	0-(15)-31	Pulse Code Modulation Conversions permitted in a network connection, μ-Law to A- Law or A- Law to μ-Law, in a network connection
- SATD	0-(1)-5	Satellite Delays. Number of satellite delays allowed in a network connection
OCLI	NO	NO manipulation is done on outgoing CLID for calls forwarded to EuroISDN link.
TIDM	(NO)	Trunk Identity Meaningful
DASC	xxxx	Display Access Code Enter the access code which is to be placed on displays before Originating Line Identities (OLI) and Terminating Line Identities (TLI) are received from the ISDN. The default is no code, when creating a new data block. Prompted with Multi Language Wake Up (MLWU) package 206 and Integrated Digital Access (IDA) package 122.
ROPT	(NRO)	No Route Optimization This option may be used to suppress Route Optimization on switches which already have high traffic.
DITI	(NO)	DID to TIE connections allowed
TRNX	(NO)	Prevent transfer on ringing of supervised external trunks across a private network
EXTT	(NO)	Prevent connection of supervised external trunks via either call transfer or conference

LD 15 – Configure the VNR enhancement. (Part 5 of 7)

Prompt	Response	Description
FTOP	(FRES)	Flexible Trunk to Trunk Options. Flexible Trunk to Trunk Connections Restricted. FTT feature is inactive.
APAD	x y (0) (0)	Alternative Pad. Where: x = trunk pad selection and y = conference pad selection Valid inputs for x are: (0) = default North America 1 = Australia 2 = New Zealand 3 = Italy 4 = China EPE or EPE/IPE systems 5 = China pure IPE system 6-7 = future usage currently set to default Valid inputs for y are: (0) = default North America 1 = Alternative Conference pads selected The default = 0 when REQ = NEW. The default is the existing value when REQ = CHG.Alternative Conference pads are only provided on specific Conference cards.
DMWM	(NO)	Enable the output of DPNSSI Message Waiting Indication Non Specified Information error messages
MWNS	(NO)	Message Waiting Indication DPNSSI Non Specified Information string to recognize.
VNR	(YES)	Vacant Number Routing
- RLI	0-999	Route List Index as defined in LD 86

LD 15 – Configure the VNR enhancement. (Part 6 of 7)

Prompt	Response	Description
- CDPL	1-(10)	Flexible length of Vacant Number Routing (VNR) Coordinated Dialing Plan (CDP)
- UDPL	1-(19)	Uniform Plan Public Flexible length of Vacant Number Routing (VNR) Uniform Dialing Plan digits (UDP). Enter the maximum number of UDP digits expected by VNR.
NIT	2-(8)	Network Alternate Route Selection (NARS) Interdigit Timer
NAS_ATCL	(YES)	Network Attendant Service Attendant Control allowed
NAS_ACTV	NO	Network Attendant Service routing Activated
FOPT	0-(6)-30	Flexible Orbiting Prevention Timer The number of seconds in two second intervals that CFW should be suspended on a set that has just forwarded a call off-node. Odd entries are rounded up to the next valid entry. A response of 0 disables FOPT.
CNDN	0 .. x..x	Customer Calling Number Identification DN on outgoing Multifrequency Compelled Signaling (MFC) calls
- CNIP	(YES)	Calling Number Identification Presentation Send Customer Calling Number Identification (CNDN) + Trunk ID (TKID) if Calling Line ID (CLID) = NO in LD 17
CNAT	0 .. x..x	CNI Attendant DN on outgoing Multifrequency Compelled Signaling (MFC) calls.
CNTC	x	Country Code (see Note 1 on 345)
NATC	x	National Access Code (see Note 1 on 345)

LD 15 – Configure the VNR enhancement. (Part 7 of 7)

Prompt	Response	Description
INTC	xxx	International Access Code (see Note 1 on 345)

LD 21 prints which dialing plan is used with AC1. This helps identify which dialing plans use AC1 and which other dialing plans use AC2.

LD 21 - Print the dialing plan.

Prompt	Response	Description
REQ	PRT	Print data block for the TYPE specified
TYPE	NET	ISDN and ESN networking options
CUST	xx	Customer number as defined in LD 15.

Configuring the Gateways

Both H.323 Gateways and SIP Trunk Gateways (that is, the Virtual Trunk applications) are supported.

The four possible configurations are:

- no Gateways (no Virtual Trunk)
- H.323 Gateway only (H.323 Virtual Trunk only)
- SIP Trunk Gateway only (SIP Virtual Trunk only)
- Both H.323 and SIP Trunk Gateways (both H.323 and SIP Virtual Trunks)

Enabling and configuring the H.323 Gateway

The H.323 Gateway runs only on the Signaling Server. However, configuration of the H.323 Gateway requires configuration on both the Call Server and the Signaling Server. You must use Element Manager to configure the H.323 Gateway on the Signaling Server.

- For Call Server configuration, follow “Feature Implementation of IP Peer Networking” on page 341. In LD 16, configure the route as an H.323 route (see 348).
- For Signaling Server configuration, perform the following procedures using Element Manager:
  - — Procedure 17: “Enabling the H.323 Gateway (H.323 Virtual Trunk application)” on page 365”
  - — Procedure 18: “Configuring the H.323 Gateway settings” on page 367”

Procedure 17
Enabling the H.323 Gateway (H.323 Virtual Trunk application)

1 Log in to Element Manager.

2 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the navigator.

The **Node Configuration** web page opens, as shown in Figure 116 on page 320.

3 Click **Edit**.

The **Edit** web page opens, as shown in Figure 117 on page 321.

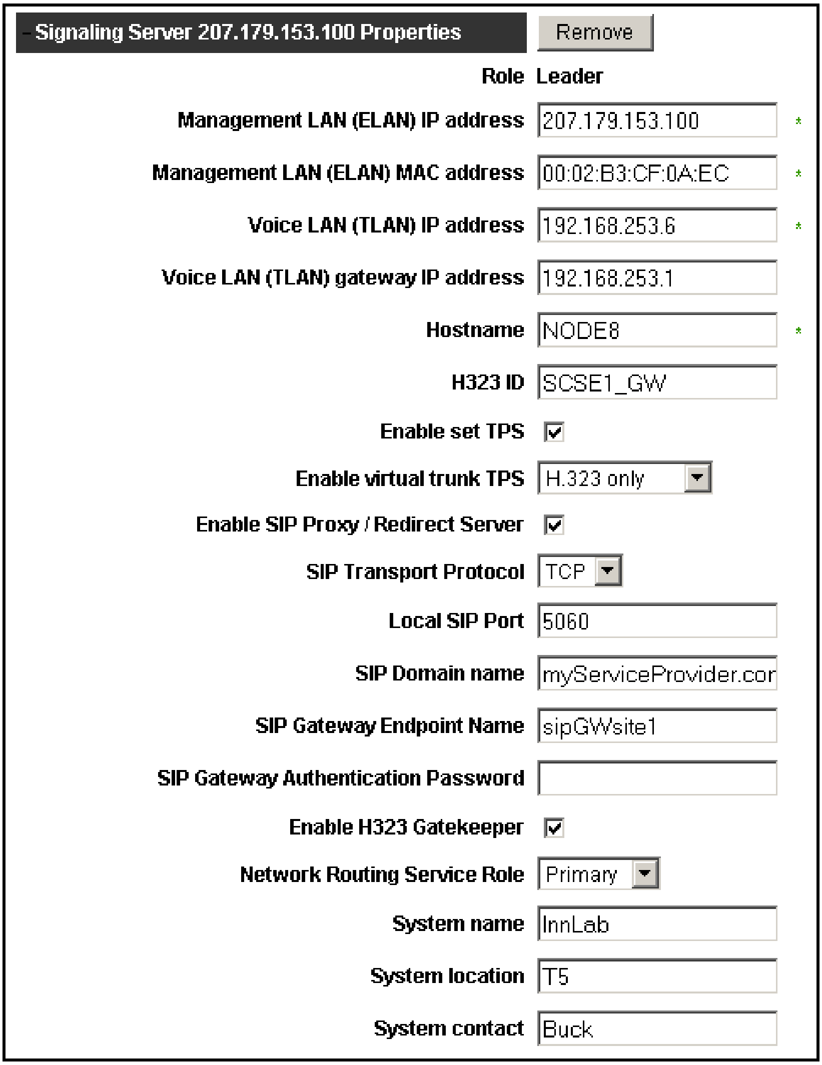
4 Click **Signaling Servers** to expand the section.

A list of Signaling Servers opens.

5 Select the appropriate **Signaling Server xxx.xxx.xxx.xxx Properties**.

The properties for that Signaling Server display, as shown Figure 143 on page 370.

Figure 141
Signaling Server xxx.xxx.xxx.xxx properties



Role	Leader
Management LAN (ELAN) IP address	207.179.153.100 *
Management LAN (ELAN) MAC address	00:02:B3:CF:0A:EC *
Voice LAN (TLAN) IP address	192.168.253.6 *
Voice LAN (TLAN) gateway IP address	192.168.253.1
Hostname	NODE8 *
H323 ID	SCSE1_GW
Enable set TPS	☑
Enable virtual trunk TPS	H.323 only
Enable SIP Proxy / Redirect Server	☑
SIP Transport Protocol	TCP
Local SIP Port	5060
SIP Domain name	myServiceProvider.cor
SIP Gateway Endpoint Name	sipGWsite1
SIP Gateway Authentication Password	
Enable H323 Gatekeeper	☑
Network Routing Service Role	Primary
System name	InnLab
System location	T5
System contact	Buck

6 Select an **H.323 option** from the **Enable virtual trunk TPS** drop-down list. This field is used to enable H.323 Gateway.

Note: The four supported modes are: None, H.323 only, SIP only, and H.323 and SIP.

7 Verify the **H323 ID**. Each H.323 Gatekeeper is configured with an H.323 Gatekeeper alias name, which is an H323-ID. Enter any text string to describe the H.323 Virtual Trunk source in the **H323 ID** text box.

8 Click **Save and Transfer**.

End of Procedure

Procedure 18
Configuring the H.323 Gateway settings

1 Log in to Element Manager.

2 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the navigator.

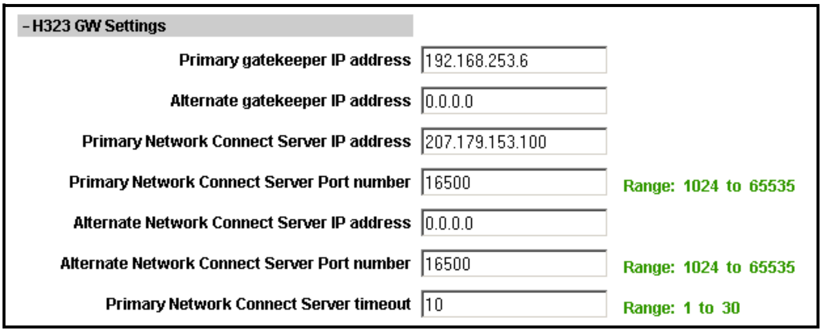
The **Node Configuration** web page opens, as shown in Figure 116 on page 320.

3 Click **Edit**.

The **Edit** web page opens, as shown in Figure 117 on page 321.

4 Select **H323 GW Settings** to expand the section, as shown in Figure 142.

Figure 142
H323 GW Settings



- H323 GW Settings

Primary gatekeeper IP address	192.168.253.6	
Alternate gatekeeper IP address	0.0.0.0	
Primary Network Connect Server IP address	207.179.153.100	
Primary Network Connect Server Port number	16500	Range: 1024 to 65535
Alternate Network Connect Server IP address	0.0.0.0	
Alternate Network Connect Server Port number	16500	Range: 1024 to 65535
Primary Network Connect Server timeout	10	Range: 1 to 30

5 Configure the following fields:

a. **Primary gatekeeper IP address:** Enter the TLAN network interface IP address (not the Node IP address) of the Leader Signaling Server running the H.323 Gatekeeper.

b. **Alternate gatekeeper IP address:** Enter the IP address if an Alternate Gatekeeper exists.

c. **Primary Network Connect Server IP address:** Enter or verify that the NCS IP address matches the Primary gatekeeper IP address (NRS). The NCS is used for IP Line Virtual Office, Branch Office (including the SRG), and Geographic Redundancy features. The NCS allows the Line TPS (LTPS) to query the NRS using the UNIStim protocol.

d. **Primary Network Connect Server Port number:** Enter a port number for the Primary NCS. The port number must be numeric and up to 5 numbers in length. The range is 1024 to 65535. The default value is 16500.

e. **Alternate Network Connect Server IP address:** Enter the IP address of the alternate NCS IP address.

f. **Alternate Network Connect Server Port number:** Enter a port number for the Alternate NCS. The port number must be numeric and up to 5 numbers in length. The range is 1024 to 65535. The default value is 16500.

g. **Primary Network Connect Server timeout:** Enter a timeout value for the Primary NCS. The range is 1 to 30 seconds. The default value is 10 seconds.

6 Click **Save and Transfer**.

End of Procedure

Enabling and configuring the SIP Trunk Gateway

The SIP Trunk Gateway runs only on the Signaling Server. Configuration of the SIP Trunk Gateway requires configuration on both the Call Server and the Signaling Server. You must use Element Manager to configure the SIP Trunk Gateway on the Signaling Server.

- For Call Server configuration, follow "Feature Implementation of IP Peer Networking" on page 341. In LD 16, configure the route as a SIP route.
- For Signaling Server configuration, perform the following procedures using Element Manager:
  - Procedure 19: "Enabling the SIP Trunk Gateway (SIP Virtual Trunk application)"
  - Procedure 20: "Configuring the SIP Trunk Gateway settings" on page 372.
  - Procedure 21: "Configuring the SIP URI to NPI/TON mapping" on page 374

Procedure 19
Enabling the SIP Trunk Gateway (SIP Virtual Trunk application)

1 Log in to Element Manager.

2 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the navigator.

The **Node Configuration** web page opens, as shown in Figure 116 on page 320.

3 Click **Edit**.

The **Edit** web page opens, as shown in Figure 117 on page 321.

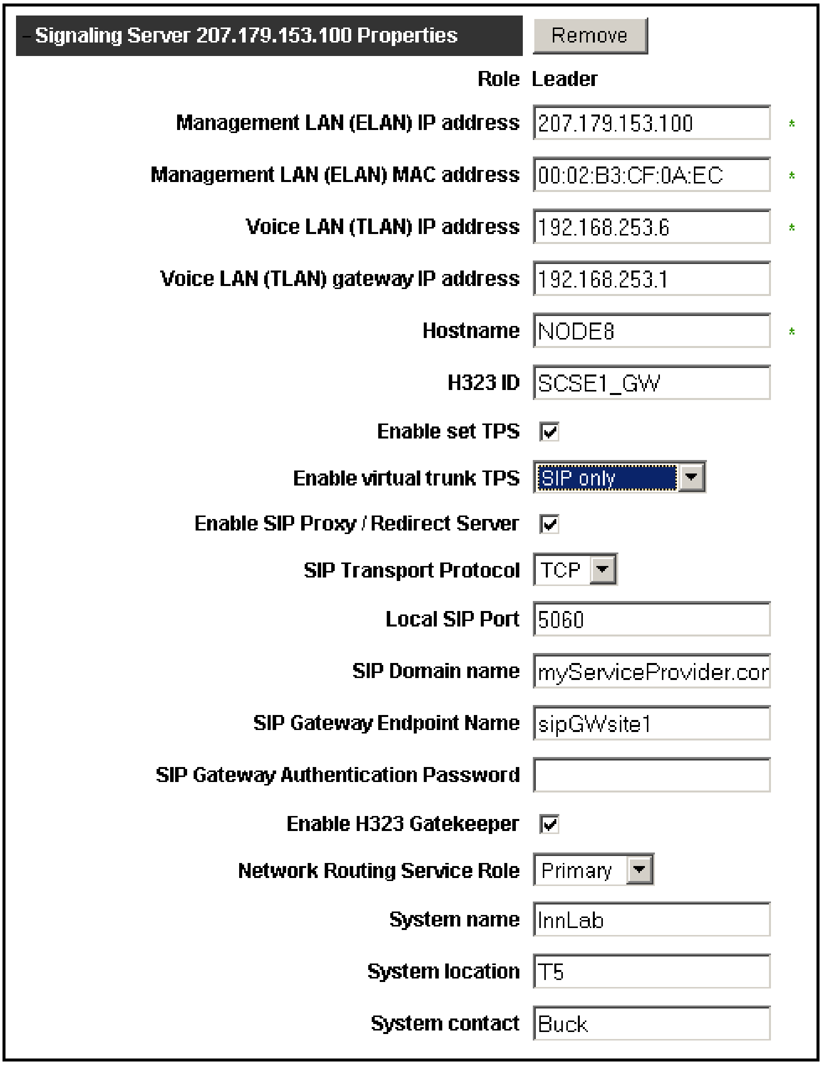
4 Select **Signaling Servers** to expand the section.

A list of Signaling Servers opens.

5 Select the appropriate **Signaling Server xxx.xxx.xxx.xxx Properties**.

The properties for that Signaling Server display, as shown in Figure 143 on page 370.

Figure 143
Signaling Server xxx.xxx.xxx.xxx properties



Signaling Server 207.179.153.100 Properties

Role	Leader	
Management LAN (ELAN) IP address	207.179.153.100	*
Management LAN (ELAN) MAC address	00:02:B3:CF:0A:EC	*
Voice LAN (TLAN) IP address	192.168.253.6	*
Voice LAN (TLAN) gateway IP address	192.168.253.1	
Hostname	NODE8	*
H323 ID	SCSE1_GW	
Enable set TPS	☑	
Enable virtual trunk TPS	SIP only	
Enable SIP Proxy / Redirect Server	☑	
SIP Transport Protocol	TCP	
Local SIP Port	5060	
SIP Domain name	myServiceProvider.cor	
SIP Gateway Endpoint Name	sipGWsite1	
SIP Gateway Authentication Password		
Enable H323 Gatekeeper	☑	
Network Routing Service Role	Primary	
System name	InnLab	
System location	T5	
System contact	Buck	

6 Select a **SIP option** from the **Enable virtual trunk TPS** drop-down list. This field is used to enable SIP Trunk Gateway and Services.

Note: The four supported modes are: None, H.323 only, SIP only, and H.323 and SIP.

7 Select the **SIP Transport Protocol**. This is the transport protocol used for SIP message exchange between the Gateway and Redirect/Proxy Server. The two options are TCP and UDP. TCP is the default option.

Note: Nortel recommends that you use the default option (TCP) for SIP traffic.

8 Verify the **Local SIP Port**. This is the port to which the gateway listens. The default is 5060.

9 Enter the **SIP Domain Name**. This string identifies the SIP Service Domain. The SIP Domain Name configured in the Signaling Server properties must match the Service Domain name configured in the NRS (see “Adding a Service Domain” on page 413). This string is used in building all SIP messages and appears in the phone context. The string must be less than 128 characters in length. The valid characters are a-z, 0-9, period (.), hyphen (-), comma (,), and underscore (_). This field must be specified if the SIP Trunk Gateway application is enabled.

10 If authentication is turned on in the NRS (SIP Redirect Server) or on the MCS 5100 Proxy Server, then the **SIP Gateway Endpoint Name** and **SIP Gateway Authentication Password** must be entered and must match the Gateway Endpoint name and Gateway Endpoint authentication password used by the SIP Redirect Server (see “Adding a Gateway Endpoint” on page 424). The name and authentication password are used in authenticating the Gateway Endpoint with the SIP Redirect Server.

a. **SIP Gateway Endpoint Name**: Enter the endpoint name. This is the username that is used when authenticating this gateway with the NRS (SIP Redirect Server) or the MCS 5100 Proxy Server. This field must be specified if authentication is enabled for the Gateway Endpoint in the NRS or Proxy Server.

b. **SIP Gateway Authentication Password**: Enter the password. This is the password that is used when authenticating this gateway with the NRS (SIP Redirect Server) or the MCS 5100 Proxy Server. This field must be specified if authentication is enabled for the Gateway Endpoint in the NRS or Proxy Server.

11 Click **Save and Transfer**.

End of Procedure

Procedure 20
Configuring the SIP Trunk Gateway settings

1 Log in to Element Manager.

2 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the navigator.

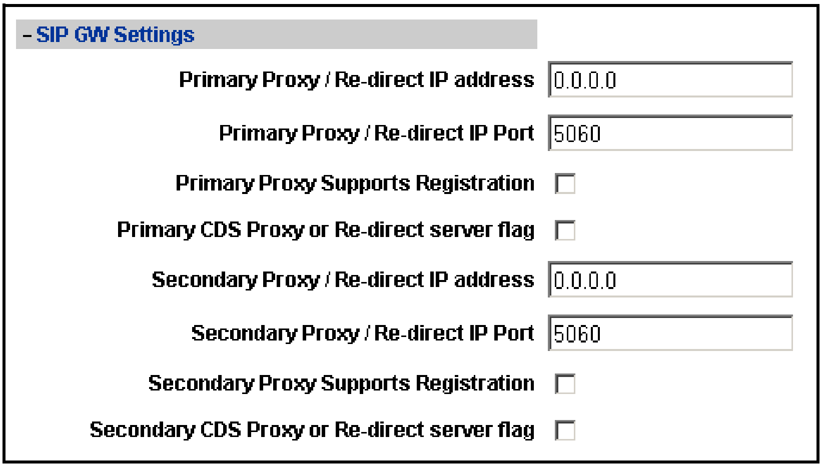
The **Node Configuration** web page opens, as shown in Figure 116 on page 320.

3 Click **Edit**.

The **Edit** web page opens, as shown in Figure 117 on page 321.

4 Select **SIP GW Settings** to expand the section (see Figure 144 on page 372).

Figure 144
SIP GW Settings



- SIP GW Settings

Primary Proxy / Re-direct IP address: 0.0.0.0

Primary Proxy / Re-direct IP Port: 5060

Primary Proxy Supports Registration □

Primary CDS Proxy or Re-direct server flag □

Secondary Proxy / Re-direct IP address: 0.0.0.0

Secondary Proxy / Re-direct IP Port: 5060

Secondary Proxy Supports Registration □

Secondary CDS Proxy or Re-direct server flag □

5 Complete the following for the Primary server:

a. **Primary Proxy / Re-direct IP address**: Enter the TLAN network interface IP address of the Primary SIP Redirect Server or the MCS 5100 Proxy Server.

b. **Primary Proxy / Re-direct IP Port**: Leave the default port value as 5060 for the Primary SIP Redirect Server or the MCS 5100 Proxy Server.

c. **Primary Proxy Supports Registration**: This check box tells the SIP Trunk Gateway whether the primary NRS (SIP Redirect Server) supports registration. If the check box is selected, then the SIP Trunk Gateway must register with the primary NRS. If the check box is not selected, then the SIP Trunk Gateway will not register with the primary NRS.

d. The **Primary CDS Proxy or Re-direct server flag** is not used in this release.

e. **Secondary Proxy / Re-direct IP address**: Enter the TLAN network interface IP address of the Secondary SIP Redirect Server or the MCS 5100 Proxy Server (if configured).

f. **Secondary Proxy / Re-direct IP Port**: Leave the default port value as 5060 for the Secondary SIP Redirect Server or the MCS 5100 Proxy Server (if configured).

g. **Secondary Proxy Supports Registration**: This check box tells the SIP Trunk Gateway whether the secondary NRS (SIP Redirect Server) supports registration. If the check box is selected, then the SIP Trunk Gateway must register with the secondary NRS. If the check box is not selected, then the SIP Trunk Gateway will not register with the secondary NRS.

h. The **Secondary CDS Proxy or Re-direct server flag** is not used in this release.

6 Click **Save and Transfer**.

End of Procedure

Configuring the SIP URI to NPI/TON mapping using Element Manager

The SIP URI to NPI/TON mapping is used as a translation of a signaling request between the SIP Trunk Gateway and the NRS.

The SIP Trunk Gateway sends a request to the NRS to find the SIP address resolution. To configure the SIP Trunk Gateway to communicate with the NRS (SIP Redirect Server), the SIP URI to NPI/TON mapping must be done.

Once the NRS server is properly configured properly and the NRS numbering plan database had been provisioned (see “Configuring and managing the Network Routing Service” on page 379), you must build the SIP URI to NPI/TON mapping using Element Manager.

Procedure 21 provides the steps to create this SIP URI to NPI/TON mapping using an NRS example and an example for the MCS 5100.

Procedure 21
Configuring the SIP URI to NPI/TON mapping

1 Log in to Element Manager.

2 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the navigator.

The **Node Configuration** web page opens, as shown in Figure 116 on page 320.

3 Click **Edit**.

The **Edit** web page opens, as shown in Figure 117 on page 321.

4 Select **SIP URI Map** to expand the section.

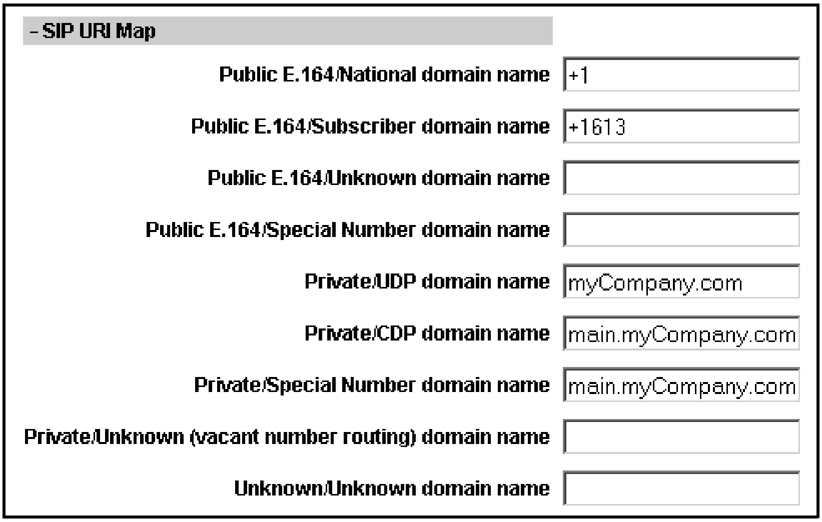
Note: The fields require a character string that is less than 128 characters in length. The valid characters include: a-z, 0-9, ., -, _, and +. These fields must be completed if the SIP Trunk Gateway application is enabled.

The values in this SIP URI Map section are based on the example provided in the chapter “Network Routing Service overview” on page 201, specifically the examples provided in Table 13: “Numbering plan mapping” on page 217.

To complete the NRS example, refer to Figure 145 on page 375 and go to step 5 on page 375.

To complete the MCS 5100 example, refer to Figure 146 on page 376 and go to step 6 on page 376.

Figure 145
SIP URI Map for the NRS example



- SIP URI Map

Public E.164/National domain name	+1
Public E.164/Subscriber domain name	+1613
Public E.164/Unknown domain name	
Public E.164/Special Number domain name	
Private/UDP domain name	myCompany.com
Private/CDP domain name	main.myCompany.com
Private/Special Number domain name	main.myCompany.com
Private/Unknown (vacant number routing) domain name	
Unknown/Unknown domain name	

5 Fill in the following fields for the NRS example (see Figure 145):

a. Type **+1** in the **Public E.164/National domain name** text box.

b. Type **+1613** in the **Public E.164/Subscriber domain name** text box.

c. Leave the **Public E.164/Unknown domain name** text box blank.

d. Leave the **Public E.164/Special Number domain name** text box blank

e. Type **myCompany.com** in the **Private/UDP domain name** text box.

f. Type **myCdpDomain.myCompany.com** in the **Private/CDP domain name** text box.

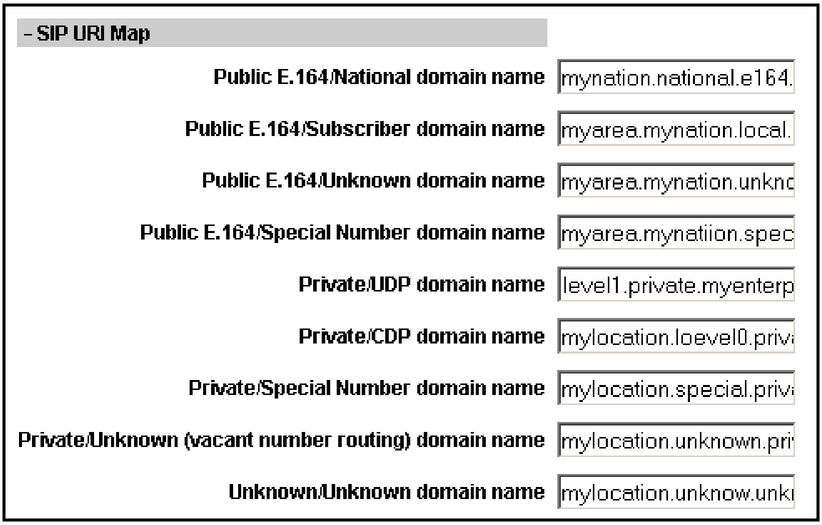
g. Type **special.myCdpDomain.myCompany.com** in the **Private/Special Number domain name** text box.

h. Leave the **Private/Unknown (vacant number routing) domain name** text box blank.

i. Leave the **Unknown/Unknown domain name** text box blank.

j. Click **Save and Transfer**.

Figure 146
SIP URI Map for the MCS 5100 example



- SIP URI Map

Public E.164/National domain name	mynation.national.e164.
Public E.164/Subscriber domain name	myarea.mynation.local.
Public E.164/Unknown domain name	myarea.mynation.unknc
Public E.164/Special Number domain name	myarea.mynatiion.spec
Private/UDP domain name	level1.private.myenterp
Private/CDP domain name	mylocation.loevel0.priv
Private/Special Number domain name	mylocation.special.priv
Private/Unknown (vacant number routing) domain name	mylocation.unknown.pri
Unknown/Unknown domain name	mylocation.unknow.unk

6 Fill in the following fields for the MCS 5100 example (see Figure 146):

a. Type **mynation.national.e164.myrootdomain** in the Public E.164/ National domain name text box.

b. Type **myarea.mynation.local.e164.myrootdomain** in the Public E.164/Subscriber domain name text box.

c. Type **myarea.mynation.unknown.e164.myrootdomain** in the Public E.164/Unknown domain name text box.

d. Type **myarea.mynation.special.e164.myrootdomain** in the Public E.164/Special Number domain name text box.

e. Type **level1.private.myenterprise** in the Private/UDP domain name text box.

f. Type **mylocation.level0.private.myenterprise** in the Private/CDP domain name text box.

g. Type **mylocation.special.private.myenterprise** in the Private/ Special Number domain name text box.

h. Type **mylocation.unknown.private.myenterprise** in the Private/ Unknown (vacant number routing) domain name text box.

i. Type **mylocation.unknown.unknown.myrootdomain** in the Unknown/Unknown domain name text box.

j. Click **Save and Transfer**.

End of Procedure

Restarting the Signaling Server

Some fields in Element Manager can be changed at run-time: SIP domain name, CDS proxy (yes or no), Gateway username and password, dialing plans, and all "SIP Service" related fields except ACD DN. The rest of the fields require a restart of the Signaling Server.

Warm restart

To warm restart the Signaling Server, following the steps in Procedure 22.

Procedure 22
Warm restarting the Signaling Server

1 Select **IP Telephony > Nodes: Servers, Media Cards > Maintenance and Reports** from the navigator in Element Manager.

2 Select the node containing the Signaling Server to be restarted.

3 Click **Reset** for the Signaling Server.

End of Procedure

Cold restart

Press the **RST** button on the front panel to cold restart the Signaling Server.

Configuring and managing the Network Routing Service

Contents

This section contains information on the following topics:

Introduction

The Network Routing Service (NRS) can be configured and maintained through a web interface called NRS Manager.

> ***Note:*** NRS Manager replaces the Succession 3.0 H.323 Gatekeeper web pages in CS 1000 Element Manager in CS 1000 Release 4.0 and later.

NRS Manager is a multi-customer user interface. The NRS includes a Service Domain level that is used to support multiple customers.

The NRS can also be accessed directly from the Command Line Interface of the Signaling Server. This does not provide access to NRS Manager, but does allow users to run NRS-specific CLI commands listed in "Command Line Interface commands" on page 568.

Browser configuration

Your web browser must be properly configured before using NRS Manager.

Supported browser

NRS Manager is supported only on Microsoft Internet Explorer version 6.0 (or later).

IMPORTANT!

Nortel discourages use of the Back, Forward, and Refresh buttons of the browser.

Use of the Back button is not recommended while the NRS Manager application is launched, because NRS Manager pages contain dynamic data content. NRS Manager provides a path for navigation purposes on top of every NRS Manager page.

Nortel recommends that the user click the navigation path to go back to the previous page (instead of using the Back button).

Configuring the browser and display settings

Before you can use NRS Manager, the following tasks must be completed:

- Enable popups in the browsers search utility (mandatory).
- Configure the Internet Explorer browser settings (mandatory).
- Configure the Windows Display settings (highly recommended).

Note: The interface for the Internet Explorer browser settings and Windows Display settings may vary by browser version and by operating system.

Enabling popups

If you are using a browser search utility (such as the Google™ search engine or the Yahoo!™ search engine), ensure that pop-ups are enabled. Enabling pop-up windows is usually done at the search utility's toolbar.

IMPORTANT!

Do not block pop-up windows if you are using a search utility (such as Google or Yahoo! search engines) in your browser.

Configuring the browser settings

Use Procedure 23 to configure the following Internet Explorer browser settings:

- Configure the browser retrieve page information.
- Configure the empty session information.
- Deselect the AutoComplete options.

Procedure 23
Configure the Internet Explorer browser settings

1 Select **View > Text Size > Medium** to configure text size in the browser.

2 Select **Tools > Internet Options** In the Internet Explorer browser window.

The **Internet Options** window opens.

3 Configure the browser retrieve page information:

a. On the **General** tab under the **Temporary Internet files** section, click **Settings**.

The **Settings** window opens.

b. Under the **Check for newer versions of stored pages** section, select the **Every visit to the page** option.

c. Click **OK**.

4 Configure the empty session information:

a. Select the **Advanced** tab.

b. Under **Security**, select **Empty Temporary Internet Files folder when browser is closed**.

5 Deselect the AutoComplete options.

a. Select the **Content** tab.

b. Under **Personal Information**, click **AutoComplete**.

The **AutoComplete Settings** window opens.

c. Under the **Use AutoComplete for** section, deselect **Forms** and **User names and passwords on forms**.

End of Procedure

Configuring the Windows Display settings

Use Procedure 24 to configure the Windows display settings.

Procedure 24
Configuring the Windows Display settings

1 Select **Start > Settings > Control Panel > Display**.

The **Display Settings** window opens.

2 Select the **Settings** tab.

3 Select **True Color (32 bit)** from the **Colors** drop-down list.

4 Under **Screen area**, select **1280 by 1024 pixels**.

5 Click **OK**.

End of Procedure

Enabling and configuring the NRS server

The NRS server must be enabled and properly configured before any NRS data can be provisioned using NRS Manager.

IMPORTANT!

The Network Routing Service can be redundantly installed across a cluster of Network Routing Servers sharing a distributed database.

In CS 1000 Release 4.5 the cluster is comprised of a Primary Network Routing Server and an Alternate Network Routing Server. Optionally, a Failsafe Network Routing Server can be co-resident with an IP Peer Gateway (H.323 or SIP) on a Signaling Server in an IP telephony node.

The Primary, Alternate and (optional) Failsafe Network Routing Servers must host the same major software release. For example, all servers must host release 4.00.xx or 4.50.xx. Network Routing Servers hosting different major software releases cannot synchronize the NRS databases.

Refer to *Signaling Server: Installation and Configuration* (553-3001-212) for detailed information on the Network Routing Server installation procedures

The NRS server can be configured in two modes:

- Stand-alone mode — The host Signaling Server is not registered to a Call Server. During installation of the Signaling Server, ensure that the Call Server IP address is configured as 0.0.0.0.

  Note: During installation of the Signaling Server in stand-alone mode (using the Signaling Server Software Install Tool), the administrator is not prompted to enter the Call Server IP address. Instead, the Call Server IP address defaults to 0.0.0.0. During the installation, the parameter confirmation screen displays the IP address as 0.0.0.0.

- Co-resident mode — The NRS is co-resident on a Signaling Server that is registered to a Call Server. The Signaling Server can also run other applications, such as the IP Line TPS and the Virtual Trunk applications.

Stand-alone mode

Procedure 25
Enabling and configuring the NRS server in stand-alone mode

1 Enable the NRS and configure the NRS server settings using the Signaling Server Software Install Tool.

Refer to *Signaling Server: Installation and Configuration* (553-3001-212) for detailed information on the Signaling Server Software Install Tool and for detailed installation procedures for configuring a stand-alone Signaling Server.

The following is a summary of the tasks required for the installation of a stand-alone Signaling Server; however, follow the detailed procedures presented in *Signaling Server: Installation and Configuration* (553-3001-212) for complete instructions.

a. Perform the introductory steps for the Signaling Server installation.

b. Configure the Signaling Server as a Leader, when prompted.

c. Configure stand-alone mode (NRS only — no Call Server) for the Signaling Server.

d. Select whether the NRS supports the SIP Redirect Server, the H.323 Gatekeeper, or both.

e. Select the type of NRS — Primary or Alternate.

f. Enter the following:

i. Enter the hostname.

ii. Enter the ELAN network interface IP address, subnet mask, and gateway IP address.

iii. Enter the TLAN network interface IP address, subnet mask, and gateway IP address.

g. The Call Server IP address defaults to 0.0.0.0. for a stand-alone Signaling Server.

h. Enter the IP address of the NRS (Primary or Alternate NRS IP address).

2 Restart the Signaling Server after proper configuration of the Signaling Server.

If the Signaling Server restarts successfully, the NRS is configured with the default settings.

3 Log in to the NRS Manger using the default user ID and password. See Procedure 28 on page 394.

4 Configure the NRS Server Settings in NRS Manager. See Procedure 32 on page 405.

5 Log out of the NRS. See Procedure 29 on page 401.

6 Restart the Signaling Server.

If the Signaling Server boots successfully, then the NRS server is properly configured.

End of Procedure

Co-resident mode

Procedure 26
Enabling and configuring the NRS server in co-resident mode

Note: If the Signaling Server has been configured as co-resident mode, proceed directly to step 3 on page 387.

1 Enable the NRS and configure the NRS server settings using the Signaling Server Software Install Tool.

Refer to *Signaling Server: Installation and Configuration* (553-3001-212) for detailed information on the Signaling Server Software Install Tool and for detailed installation procedures for configuring a co-resident Signaling Server.

The following is a summary of the tasks required for the installation of a co-resident Signaling Server; however, follow the detailed procedures presented in *Signaling Server: Installation and Configuration* (553-3001-212) for complete instructions.

a. Perform the introductory steps for the Signaling Server installation.

b. Configure the Signaling Server as a Leader, when prompted.

c. Select co-resident mode (LTPS + VTRK + NRS) for the Signaling Server.

d. Select whether the NRS supports the SIP Redirect Server, the H.323 Gatekeeper, or both. (The option to configure no NRS is also available.)

e. Select the type of NRS — Primary, Alternate or Failsafe.

f. Enter the following:

i. Enter the hostname.

ii. Enter the ELAN network interface IP address, subnet mask, and gateway IP address.

iii. Enter the TLAN network interface IP address, subnet mask, and gateway IP address.

g. Enter the IP address of the NRS (Primary and/or Alternate NRS IP address).

2 Restart the Signaling Server after proper configuration of the Signaling Server. See Procedure 22 on page 377.

3 Log in to Element Manager. See Procedure 3 on page 286.

4 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the navigator.

The **Node Configuration** web page opens, as shown in Figure 116 on page 320.

5 Click **Edit**.

The **Edit** web page opens, as shown in Figure 117 on page 321.

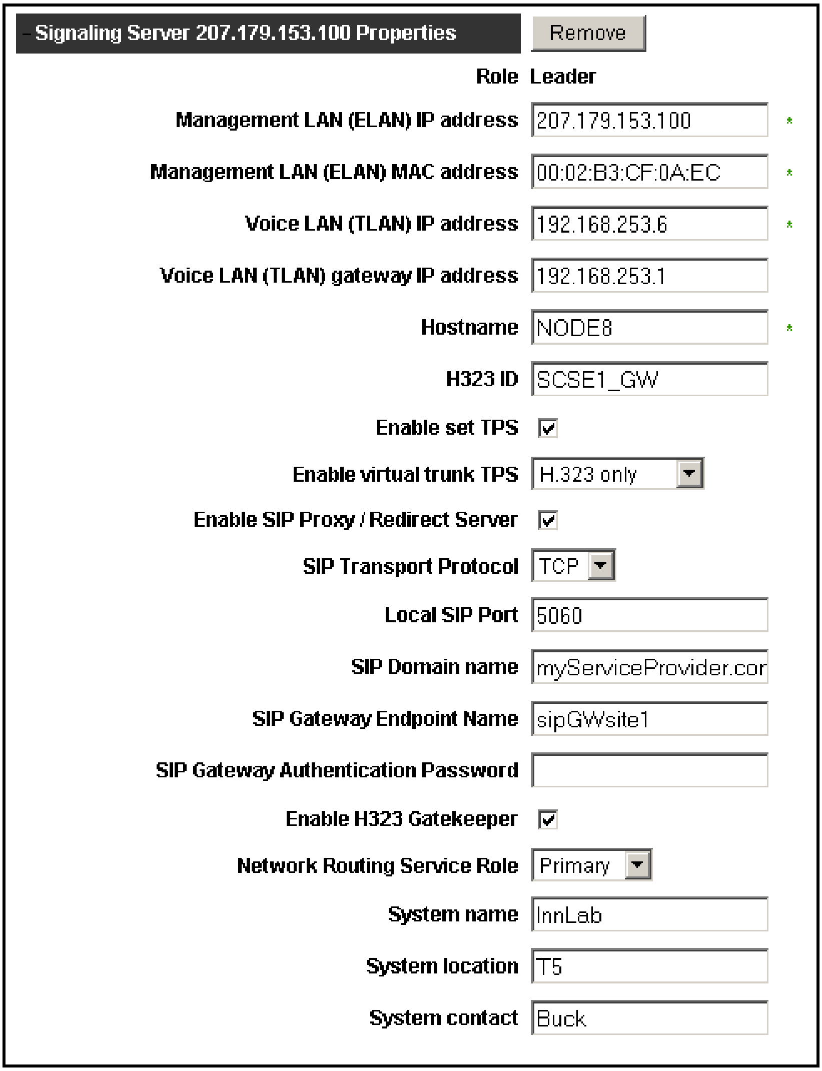
6 Click **Signaling Servers** to expand the section.

A list of Signaling Servers opens.

7 Select the appropriate **Signaling Server xxx.xxx.xxx.xxx Properties**.

The properties for that Signaling Server display, as shown in Figure 147 on page 388.

Figure 147
Signaling Server xxx.xxx.xxx.xxx properties



- Signaling Server 207.179.153.100 Properties

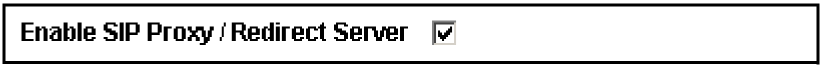
Role	Leader	
Management LAN (ELAN) IP address	207.179.153.100	*
Management LAN (ELAN) MAC address	00:02:B3:CF:0A:EC	*
Voice LAN (TLAN) IP address	192.168.253.6	*
Voice LAN (TLAN) gateway IP address	192.168.253.1	
Hostname	NODE8	*
H323 ID	SCSE1_GW	
Enable set TPS	☑	
Enable virtual trunk TPS	H.323 only	
Enable SIP Proxy / Redirect Server	☑	
SIP Transport Protocol	TCP	
Local SIP Port	5060	
SIP Domain name	myServiceProvider.cor	
SIP Gateway Endpoint Name	sipGWsite1	
SIP Gateway Authentication Password		
Enable H323 Gatekeeper	☑	
Network Routing Service Role	Primary	
System name	InnLab	
System location	T5	
System contact	Buck	

8 To enable the NRS, do the following:

a. Enable the SIP Proxy/Redirect Server and/or the H.323 Gatekeeper, as appropriate:

- Select the **Enable SIP Proxy / Redirect Server** check box to enable the SIP Redirect Server (see Figure 148).

Figure 148
Enabling the SIP Redirect Server



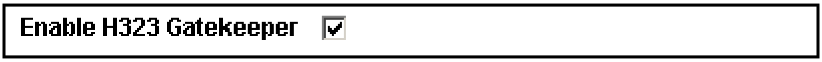
Enable SIP Proxy / Redirect Server ☑

Note 1: CS 1000 does not support the SIP Proxy Server.

Note 2: The SIP Trunk Gateway must also be configured, see "Enabling and configuring the SIP Trunk Gateway" on page 369.

- Select the **Enable H.323 Gatekeeper** check box to enable the H.323 Gatekeeper (see Figure 149).

Figure 149
Enabling the H.323 Gatekeeper



Enable H323 Gatekeeper ☑

Note: The H.323 Gateway must also be configured, see "Enabling and configuring the H.323 Gateway" on page 364.

b. Select the role of the NRS from the **Network Routing Service Role** drop-down list.

The three options are Primary, Alternate, and Failsafe.

9 Configure the other required Signaling Server properties.

10 Click **Save and Transfer** to save the changes and transfer the properties to all nodes.

11 Click **Logout** at the bottom of the navigator to log out of Element Manager.

12 Restart the Signaling Server. See Procedure 22 on page 377.

13 After a successful restart of the Signaling Server, log in to NRS Manager using the default user ID and password. See Procedure 28 on page 394.

14 Configure the NRS Server Settings in NRS Manager. See Procedure 32 on page 405.

15 Log out of the NRS. See Procedure 29 on page 401.

16 Restart the Signaling Server.

If the Signaling Server boots successfully, then the NRS server is properly configured.

End of Procedure

Changing a co-resident NRS server to a stand-alone NRS server

Use the Signaling Server Software Install Tool to change a co-resident NRS server to a stand-alone NRS.

Task summary

This section is intended as a summary of how to navigate and use NRS Manager. The section also provides instructions for configuring and managing the NRS database. The NRS database provides a central database of addresses that are required to route calls across the network.

> ***Note:*** This section also includes procedures for doing other tasks in the NRS such as enabling/disabling the NRS server, viewing reports, and testing routes.

1 Log in to NRS Manager (see "Accessing NRS Manager" on page 393).

You can log in two ways:

— See "Logging in to NRS Manager from Element Manager" on page 393.

— See "Logging in to NRS Manager using the browser address field" on page 394.

2 Configure NRS elements. Verify that the NRS is the Primary NRS and is active. See "Verifying that the NRS is the Primary NRS and is active" on page 401.

3 Configure the System Wide Settings. See "Configuring system-wide settings" on page 403.

4 Configure the NRS Server Settings. See “Configuring NRS Server Settings” on page 405.

5 Build the structure of the NRS database.

Note: The following steps must be performed in the order given.

a Create the Service Domain, Level 1 Domains (UDP), Level 1 Domains (CDP), which hold the endpoint numbering plans on the NRS. This is complementary to the CDP configuration on the Call Server.

i. See “Adding a Service Domain” on page 413.

ii. See “Adding a Level 1 Domain (UDP)” on page 415.

iii. See “Adding a Level 0 Domain (CDP)” on page 419.

b Add the endpoints and add the endpoint prefixes.

i. See “Adding a Gateway Endpoint” on page 424.

ii. See “Adding a User Endpoint” on page 543.

c Add the numbering plan entries for each endpoint, including the Cost Factor for each entry.

i. See “Adding a Routing Entry” on page 432.

ii. See “Adding a Default Route” on page 438.

d Add collaborative servers.

i. See “Viewing the Collaborative Servers” on page 447.

ii. See “Adding a Collaborative Server” on page 442.

Note: You do not have to configure Gateway Endpoint, User Endpoints, or Routing Entries before you configure the Collaborative Servers.

e Verify the numbering plan configuration. See “Verifying the numbering plan and saving the NRS configuration” on page 447.

f Perform database actions. See “Performing NRS database actions” on page 454. To save the NRS configuration, refer to the procedures in this section.

6 Test the numbering plans (see“H.323 and SIP Routing Tests” on page 448).

- See “Performing an H.323 Routing Test” on page 448.
- See “Performing a SIP Routing Test” on page 449.

7 Perform server actions (see“Enabling and disabling the NRS Server” on page 451).

- See “Disabling the NRS server” on page 452.
- See “Enabling the NRS server” on page 453.

8 Perform database actions (see “Performing NRS database actions” on page 454).

- See “Cutting over the database” on page 455.
- See “Reverting the database changes” on page 456.
- See “Rolling back changes to the database” on page 458.
- See “Committing the database” on page 459.
- See “Cutting over and committing changes to the database” on page 460.

9 Back up the NRS database. See “Backing up the database” on page 461.

- See “Automatically backing up the database” on page 461.
- See “Manually backing up the database” on page 462.

The NRS database can also be restored, if required. See “Restoring the database” on page 465.

- See “Restoring from the connected Signaling Server” on page 466.
- See “Restoring from an FTP site” on page 467.
- See “Restoring from a client machine” on page 469.

10 If necessary, convert the Succession 3.0 Gatekeeper database to a CS 1000 Release 4.0 (or later) NRS database. See “GK/NRS Data Upgrade” on page 471 and refer to the Upgrades NTPs for detailed information.

11 View the SIP Phone Context. See “SIP Phone Context” on page 474.

12 View reports on the status of the database. See “Viewing the database reports” on page 476.

13 Administer users of the NRS (see “Configuring and administering users” on page 479).

— See “Creating new users” on page 480.

— See “Viewing configured users” on page 481.

— See “Editing or deleting configured users” on page 482.

14 Log out of NRS Manager. See “Logging out of NRS Manager” on page 401.

Accessing NRS Manager

Access NRS Manager in one of the following two ways:

- Select the **Network Routing Service** link in the navigator within Element Manager. See “Logging in to NRS Manager from Element Manager” on page 393.
- Enter the IP address of NRS Manager in the browser’s address field. See “Logging in to NRS Manager using the browser address field” on page 394.

Note: To access the NRS directly from the Signaling Server, see “Accessing the NRS directly from the Signaling Server” on page 484.

To log in to the NRS from Element Manager, follow the steps in Procedure 27.

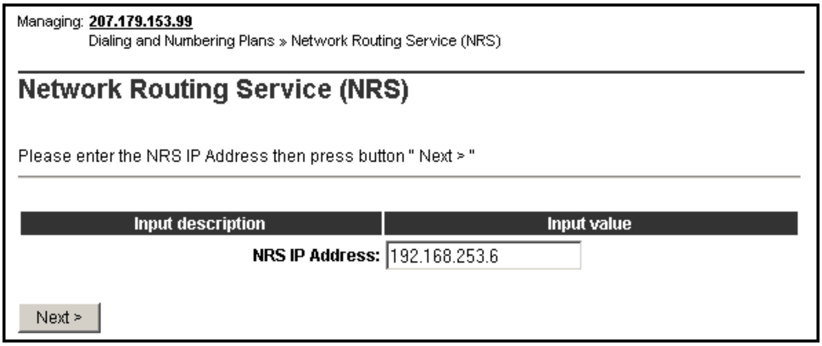
Procedure 27
Logging in to NRS Manager from Element Manager

1 Log in to Element Manager using Procedure 3 on page 286.

2 Select **Dialing and Numbering Plans > Network Routing Service** from the navigator.

The **Network Routing Service (NRS) configuration** web page opens (see Figure 150 on page 394).

Figure 150
Network Routing Service (NRS) configuration web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Network Routing Service (NRS)

Network Routing Service (NRS)

Please enter the NRS IP Address then press button " Next > "

Input description	Input value
NRS IP Address:	192.168.253.6

3 Enter the IP address of the NRS in the **NRS IP Address** text box.

Note: The IP address that automatically appears may not be the IP address of the NRS; the displayed address is the address defined in Element Manager for the H.323 Gatekeeper or SIP Redirect Server.

4 Click **Next>**.

The **Network Routing Service** login window opens (see Figure 151 on page 395)

5 Go to step 4 on page 396 of Procedure 28.

End of Procedure

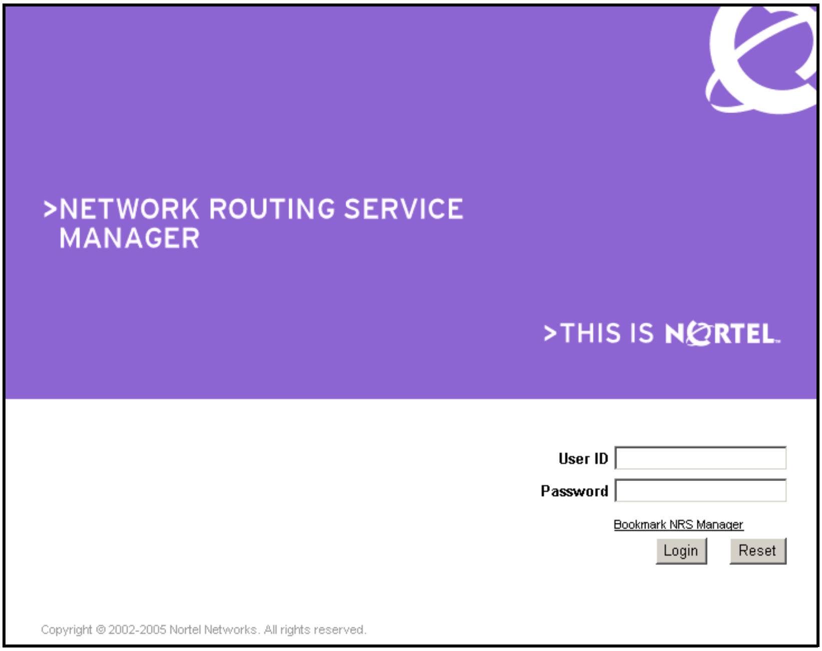
Procedure 28
Logging in to NRS Manager using the browser address field

1 Open the Microsoft Internet Explorer 6.0 (or later) browser.

2 Type the URL for NRS Manager into the address field of the browser. The URL has the following format:
http://[Signaling_Server_ELAN_network_interface_IP_address]/nrs/

3 The NRS Manager Login web page displays (see Figure 151 on page 395).

Figure 151
NRS Manager login web page


>NETWORK ROUTING SERVICE MANAGER
>THIS IS NORTEL
User ID
Password
Bookmark NRS Manager
Login
Reset
Copyright © 2002-2005 Nortel Networks. All rights reserved.

Note: The H.323 Gatekeeper or SIP Redirect Server must be enabled before you can log into NRS Manager. If the H.323 Gatekeeper or the SIP Redirect Server are not enabled, the web page turns white, and the following error message is displayed:

```
Error code is WC0030:

Error: Network Routing Service (NRS) Manager is not
accessible when neither Gatekeeper nor SIP Proxy/Redirect
applications are enabled.

Please close the IE window. Enable the application(s).
Reboot the Signaling Server, then access NRS Manager again.
```

To enable the H.323 Gatekeeper or SIP Redirect Server, refer to “Enabling and configuring the NRS server in stand-alone mode” on page 385 or “Enabling and configuring the NRS server in co-resident mode” on page 386.

4 Enter the **User ID** and **Password** to log in.

A username and password must be provided to prevent unauthorized access.

IMPORTANT!

Nortel recommends that you log in to NRS Manager using the default User ID and Password when configuring the NRS server. When the NRS server configuration is complete, change the User ID and Password for increased system security.

The default values are:

- User ID — **`admin`**
- password — **`admin`**

Note: NRS Manager is not available directly from the Signaling Server. To log on to the NRS from the Signaling Server, see "Accessing the NRS directly from the Signaling Server" on page 484.

Security is implemented through authentication and database access privileges. A username and password is required to access the NRS database. The username and password are stored (in encrypted format) in the same database as the SIP Redirect Server or Proxy Server data. The authentication parameters are configurable in the Element Manager but the NRS does the authentication.

Two types of access privileges are supported:

- Administrative privileges — Administrative users have full read/write privileges. An administrator can view and modify NRS data.
- Monitor privileges — Observers have read-only privileges. An observer can only view the NRS data.

Note 1: Once you are logged in as an administrator, new users can be created using Procedure 70 on page 480.

Note 2: An administrator must create each monitor (observer) user individually. There is no default User ID and password for a monitor.

Note 3: After 60 minutes of inactivity, your NRS session times out, and you are logged out of NRS Manager. The default session timeout is 60 minutes; however, this is configurable using the CLI.

5 Click **Login**.

If the login is successful, then the User ID and Password are securely transferred from the web client to the NRS web server. The web server verifies the User ID and Password and if the login is valid, then the **NRS Overview** web page opens (see Figure 152).

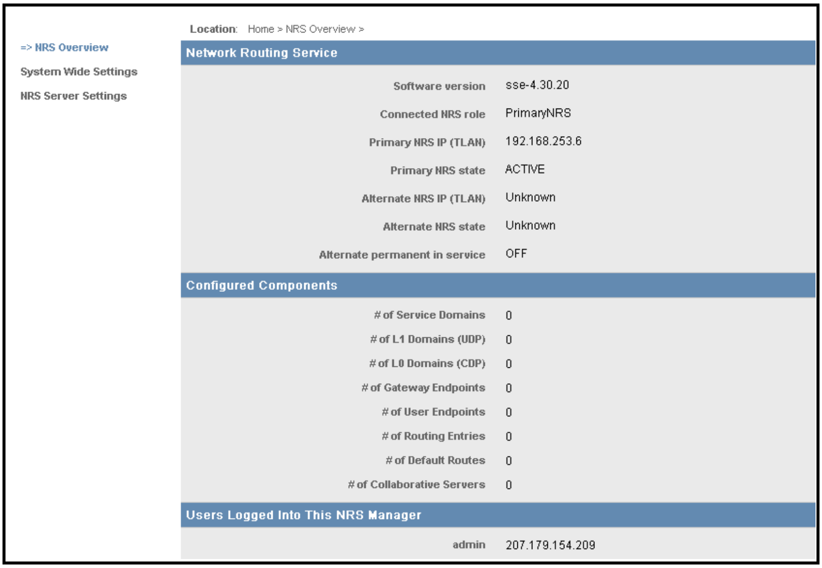
NRS Manager allows you to navigate to specific components of the NRS, and allows you to configure and maintain these components.

If the login is not successful, then you may have entered an incorrect User ID or Password.

Note 1: The **Reset** button clears the User ID and Passwords text boxes.

Note 2: To add a bookmark to your Internet Explorer Favorites list, click the **Bookmark NRS Manager** link on the login page.

Figure 152
NRS Overview web page



Location: Home > NRS Overview >

Network Routing Service

Software version	sse-4.30.20
Connected NRS role	PrimaryNRS
Primary NRS IP (TLAN)	192.168.253.6
Primary NRS state	ACTIVE
Alternate NRS IP (TLAN)	Unknown
Alternate NRS state	Unknown
Alternate permanent in service	OFF

Configured Components

# of Service Domains	0
# of L1 Domains (UDP)	0
# of L0 Domains (CDP)	0
# of Gateway Endpoints	0
# of User Endpoints	0
# of Routing Entries	0
# of Default Routes	0
# of Collaborative Servers	0

Users Logged Into This NRS Manager

admin	207.179.154.209

The **NRS Overview** is displayed in the main area of the web page:

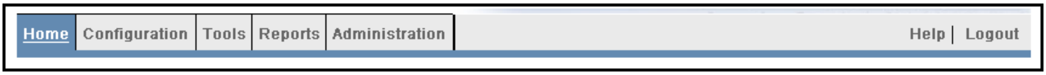
- The upper part of the window, **Network Routing Service**, provides the following information about the NRS:
  - — The software version
  - — The role of the connected NRS
  - — The IP address of the Primary NRS
  - — The status of the Primary NRS
  - — The IP address of the Alternate NRS
  - — The status of the Alternate NRS
  - — Whether the Alternate NRS is permanently in service
- The middle part of the web page, **Configured Components**, provides the number of configured components of the NRS, as follows:
  - — Number of Service Providers
  - — Number of Level 1 Domains (this maps to UDP)
  - — Number of Level 0 Domains (this maps to CDP)
  - — Number of Gateway Endpoints
  - — Number of User Endpoints
  - — Number or Routing Entries
  - — Number of Default Endpoints
  - — Number of Collaborative Servers
- The lower part of the web page, Users Logged into this NRS Manager, provides of list of logged-in users and their IP Addresses.

End of Procedure

The NRS Manager interface

The NRS has a set of five tabs for configuring and maintaining the NRS. Help and Logout links are also provided in the header area of the NRS Manager window. See Figure 153.

Figure 153
NRS Manager toolbar



NRS tabs

NRS Manager has five tabs, as shown in Figure 153.

Home tab (see page 401)

The Home tab provides summary information about the NRS. The Home tab shows an overview of the NRS and a view of any components that are configured. This tab is also used to configure the system-wide settings and the NRS server settings.

Configuration tab (see page 411)

The Configuration tab is used to structure how data is stored in the NRS database. The following are configured on the Configuration tab:

- Service Domains
- L1 Domains (UDP)
- L0 Domains (CDP)
- Gateway Endpoints
- User Endpoints
- Routing Entries
- Default Routes
- Collaborative Servers

Tools tab (see page 448)

The Tools tab provides a group of tools for performing the following:

- H.323 and SIP routing tests against the active and standby databases
- server actions such as enabling and disabling the database

- database-related actions such as cutover, commit, revert, rollback, and single-step cutover and commit
- database backups and restores
- database conversion/upgrade (such as converting the Succession 3.0 H.323 Gatekeeper database to the CS 1000 Release 4.0 (or later) NRS database)
- SIP Phone context

Reports tab (see page 476)

The Reports tab provides database synchronization reports for the Alternate and Failsafe NRS (if configured) and also provides information for the current state of the database.

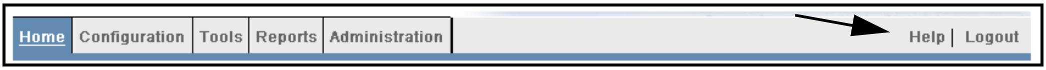
Administration tab (see page 479)

The Administration tab is use to administer, configure, and view users. Users can be added and user privileges can be modified.

Help and Logout links

The Help and Logout links are located on the upper right side of the NRS Manager web page (see Figure 154).

Figure 154
Help and Logout links



Help link

The Help link provides access to the NRS Manager Help.

NRS Manager provides contact-sensitive help. That is, the help page displayed depends on the page from which you navigate. However, once in the NRS Manager Help Files, you can navigate to any other area of the help files.

Logout link

The Logout link allows a user to terminate the current session. See “Logging out of NRS Manager” on page 401.

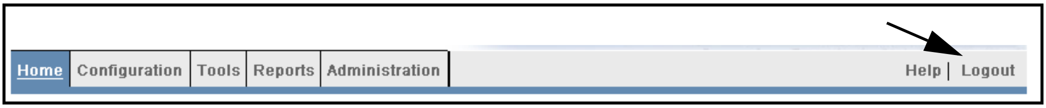
Logging out of NRS Manager

Follow the steps in Procedure 29 to log out of NRS Manager. Logging out of NRS Manager terminates the current session.

Procedure 29
Logging out of NRS Manager

1 Click **Logout** (see Figure 155).

Figure 155
Logout link



The **Network Routing Service Manager** logout web page opens.

2 Close the browser window.

End of Procedure

Home tab

Verifying that the NRS is the Primary NRS and is active

To verify that the NRS you are configuring is the Primary NRS and that it is active, follow the steps in Procedure 30.

Procedure 30
Verifying that the NRS is the Primary NRS and is active

1 Select **Home** tab from the navigator.

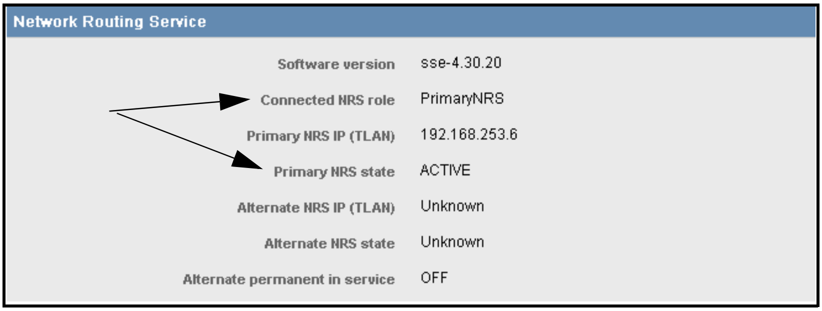
The **NRS Overview** web page opens, as shown in Figure 152 on page 397.

2 In the **Network Routing Service** section (the top section of the **NRS Overview** web page), shown in Figure 156:

a. Ensure that **Connected NRS Role** = PrimaryNRS.

b. Ensure that **Primary NRS State** = Active.

Figure 156
Network Routing Service section



Network Routing Service

Software version	sse-4.30.20
Connected NRS role	PrimaryNRS
Primary NRS IP (TLAN)	192.168.253.6
Primary NRS state	ACTIVE
Alternate NRS IP (TLAN)	Unknown
Alternate NRS state	Unknown
Alternate permanent in service	OFF

End of Procedure

Configuring system-wide settings

System-wide settings are used to configure system-wide parameters and are used to schedule backup jobs. System-wide settings include the following:

- Database synchronization interval for the Alternate and Failsafe NRS databases.
- SIP registration and H.323 Gatekeeper registration Time-to-Live timer settings.
- H.323 Gatekeeper alias name.
- Whether the Alternate NRS server is in permanent server.
- Automatic backup time setting.
- Whether automatic backup to an FTP site is enabled. If enabled, the IP address, path, and username for the FTP site must be provided.

Follow the steps in Procedure 31 to configure system-wide settings.

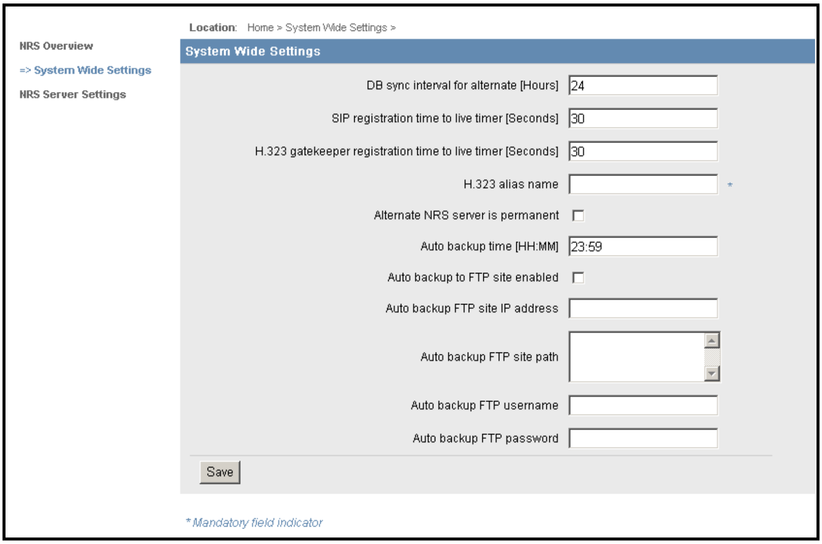
Procedure 31
Configuring system-wide settings

1 Select the **Home** tab.

2 Click **System Wide Settings** from the navigator.

The **Setting Wide Settings** web page opens (see Figure 157 on page 403).

Figure 157
System Wide Settings



Location: Home > System Wide Settings >

NRS Overview
=> System Wide Settings
NRS Server Settings

System Wide Settings

DB sync interval for alternate [Hours]	24
SIP registration time to live timer [Seconds]	30
H.323 gatekeeper registration time to live timer [Seconds]	30
H.323 alias name	*
Alternate NRS server is permanent	□
Auto backup time [HH:MM]	23:59
Auto backup to FTP site enabled	□
Auto backup FTP site IP address	
Auto backup FTP site path	
Auto backup FTP username	
Auto backup FTP password	

Save

** Mandatory field indicator*

3 Enter a value in the **DB sync interval for alternate [Hours]** text box. This is the time interval between database synchronization with the Primary NRS and the Alternate NRS. The range is 1 to 24 hours.

4 Enter the value for the Time-to-Live timers.

a. Enter a value in the **SIP registration time to live timer [Seconds]** text box. Nortel recommends that the timer be set to 30 seconds. The range is 30 to 3600 seconds.

b. Enter a value in the **H.323 gatekeeper registration time to live timer [Seconds]** text box. Nortel recommends that the timer be set to 30 seconds. The range is 30 to 3600 seconds.

5 Enter the alias name of the H.323 Gatekeeper in the **H.323 alias name** text box. This is a mandatory field. The alias name must be alphanumeric, can be up to 30 characters in length, and cannot have spaces.

In order for the H.323 Gatekeeper to send out Location Requests (LRQ), the Gatekeeper must have an H.323 Gatekeeper alias name that is an H323-ID. The default value assigned to this parameter is the same as the "HostName" value configured in the Signaling Server's config.ini file.

6 Select the **Alternate NRS server is permanent** check box if you want the Alternate NRS Server to be permanently in service.

Select the check box if the Alternate NRS Server is to remain in service after a switchover, even if the Primary NRS recovers. Clear the check box if the Alternate NRS will switchover functions to the Primary NRS Server after the Primary NRS Server recovers.

7 Enter the time when the database backup will automatically occur in the **Auto backup time [HH:MM]** text box.

8 If you want to automatically back up the NRS database to an FTP site, then complete the following steps:

a. Select the **Auto backup to FTP site enabled** check box.

b. Enter the IP address of the FTP site in the **Auto backup FTP site IP address** text box.

c. Enter the path to the FTP site in the **Auto backup FTP site path** text box. The FTP site path must be alphanumeric and can be up to120 characters in length.

d. Enter the username used to access the FTP site in the **Auto backup FTP username** text box. The FTP username must be alphanumeric and can be up to30 characters in length.

e. Enter the password used to access the FTP site in **Auto backup FTP password** text box. The FTP password must be alphanumeric and can be up to30 characters in length but cannot include the single quote (') symbol. The FTP username must be alphanumeric and can be up to30 characters in length.

9 Click **Save**.

End of Procedure

Configuring NRS Server Settings

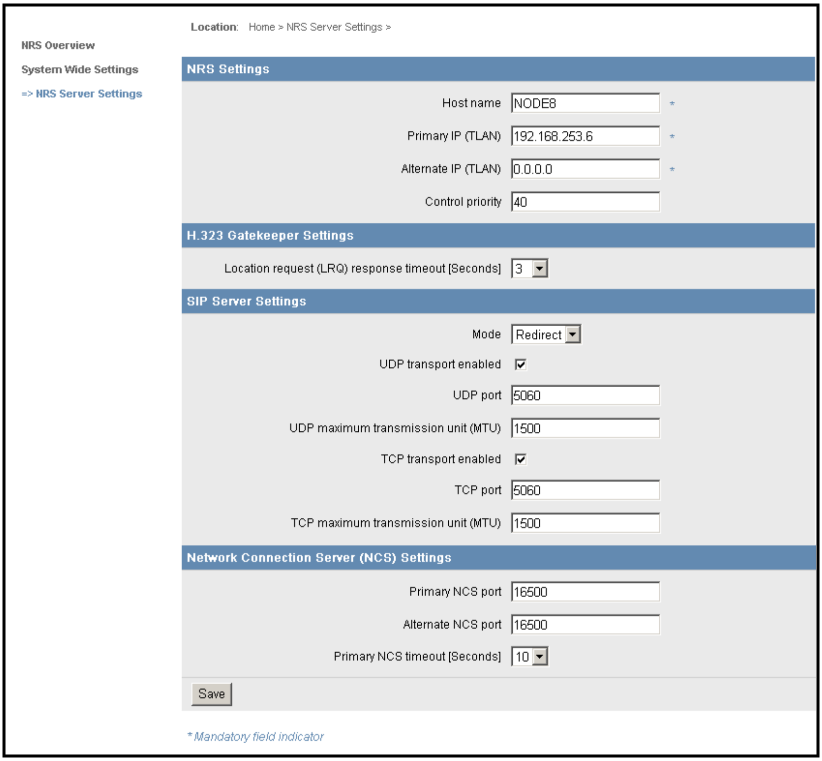
Procedure 32
Configuring NRS Server Settings

1 Select the **Home** tab.

2 Click **NRS Server Settings** from the navigator.

The **NRS Server Settings** web page opens (see Figure 158).

Figure 158
NRS Server Settings



NRS Settings

Host name: NODE8 *

Primary IP (TLAN): 192.168.253.6 *

Alternate IP (TLAN): 0.0.0.0 *

Control priority: 40

H.323 Gatekeeper Settings

Location request (LRQ) response timeout [Seconds]: 3

SIP Server Settings

Mode: Redirect

UDP transport enabled ☑

UDP port: 5060

UDP maximum transmission unit (MTU): 1500

TCP transport enabled ☑

TCP port: 5060

TCP maximum transmission unit (MTU): 1500

Network Connection Server (NCS) Settings

Primary NCS port: 16500

Alternate NCS port: 16500

Primary NCS timeout [Seconds]: 10

** Mandatory field indicator*

The NRS Server Settings are composed of the following:

- NRS Settings — These are generic settings applicable to H.323, SIP, and NCS.
- H.323 Gatekeeper Settings
- SIP Server Settings
- Network Connection Server (NCS) Settings
- SNMP Settings — These settings are available only when the connected NRS is in stand-alone mode. If the connected NRS is in co-residence mode, the SNMP Settings section is not displayed in NRS Manager. Instead, the SNMP parameters are configured using Element Manager. For more information, refer to *Simple Network Management Protocol: Description and Maintenance* (553-3001-519).

3 For **NRS Settings** (see Figure 159), configure the following:

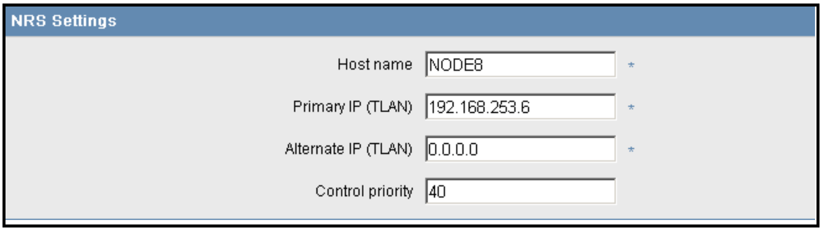
a. **Host name:** Enter the name of the connected/host Signaling Server. The host name must be alphanumeric and can be up to20 characters in length.

b. **Primary IP (TLAN):** Enter the IP address of the Primary NRS (that is, the TLAN network interface IP address). The default is 0.0.0.0.

c. **Alternate IP (TLAN):** Enter the IP address of the Alternate NRS (that is, the TLAN network interface IP address), if the Alternate NRS is configured. The default is 0.0.0.0.

d. **Control priority:** Enter a value for the control priority. This is a priority bit setting inside the protocol that determines the signaling routing priority. The range is 0 to 63. The default value is 40. The control priority must be a numeric value.

Figure 159
NRS Settings section

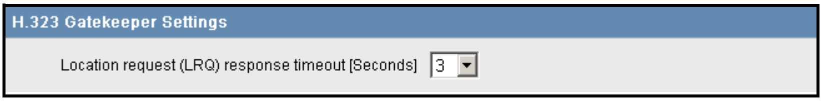


NRS Settings

Host name	NODE8	*
Primary IP (TLAN)	192.168.253.6	*
Alternate IP (TLAN)	0.0.0.0	*
Control priority	40	

4 For **H.323 Gatekeeper Settings** (see Figure 160), configure the LRQ response timeout by selecting a value from the **Location request (LRQ) response timeout [Seconds]** drop-down list. The default is 3 seconds, the minimum value is 1 second, and the maximum value is 10 seconds.

Figure 160
H.323 Gatekeeper Settings section



H.323 Gatekeeper Settings

Location request (LRQ) response timeout [Seconds] 3

5 For **SIP Server Settings** (see Figure 161 on page 408), configure the following:

a. Select **Redirect** from the **Mode** drop-down list. This is the mode of the SIP Server. A redirect server receives requests, but rather than passing the request onto the next server, it sends a response to the caller indicating the address for the called user. This provides the address for the caller to contact the called party at the next server directly.

b. Select the transport protocol type.

The following two options are available when selecting the transport protocol:

— UDP is selected only, or

— UDP and TCP are both selected. TCP cannot be selected alone.

To enable UDP, do the following:

i. Select the **UDP transport enabled** check box.

ii. Enter the **UDP port**. The default port number is 5060. The UDP port must be numeric and can be up to five digits in length.

iii. Enter the **UDP maximum transmission unit (MTU)**. MTU is the maximum size of packet going out on the IP network (specifically, an Ethernet Layer 2 packet). In this case, MTU is the maximum size of a SIP packet that is sent out on the UDP interface. The default value is 1500 bytes. The maximum value for MTU is 64K; however, when configuring this value, remember that there is a trade-off between packet size and the increase in the number of packets that have to be transmitted over the network.

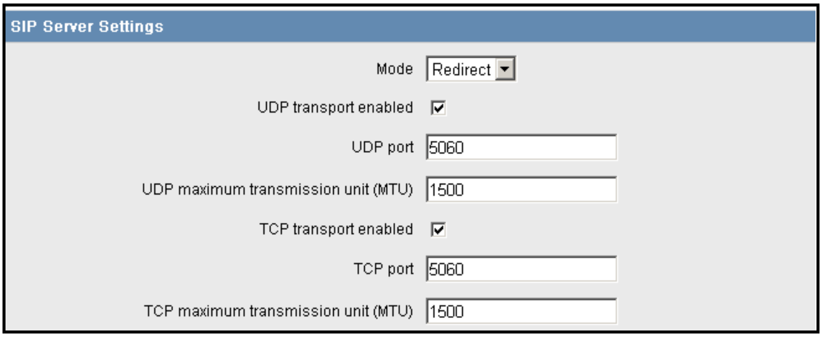
To enable TCP, perform the following steps. UDP must also be selected in order to enable TCP.

i. Select the **TCP transmission enabled** check box.

ii. Enter the **TCP port**. The default port number is 5060. The TCP must be numeric and can be up to five digits in length.

iii. Enter the **TCP maximum transmission unit (MTU)**. MTU is the maximum size of packet going out on the IP network (specifically, an Ethernet Layer 2 packet). In this case, MTU is the maximum size of a SIP packet that is sent out on the TCP interface. The default value is 1500 bytes. The maximum value for MTU is 64K; however, when configuring this value, remember that there is a trade-off between packet size and the increase in the number of packets that have to be transmitted over the network.

Figure 161
SIP Server Settings section



SIP Server Settings

Mode: Redirect
UDP transport enabled: ☑
UDP port: 5060
UDP maximum transmission unit (MTU): 1500
TCP transport enabled: ☑
TCP port: 5060
TCP maximum transmission unit (MTU): 1500

6 For **Network Connection Server (NCS) Settings** (see Figure 162 on page 409), configure the following:

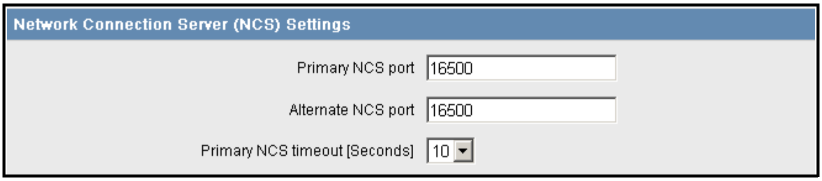
a. **Primary NCS port:** Enter a port number for the Primary NCS. The port number must be numeric and up to five digits in length. The range is 1024 to 65535. The default value is 16500.

b. **Alternate NCS port:** Enter a port number for the Alternate NCS. The port number must be numeric and up to five digits in length. The range is 1024 to 65535. The default value is 16500.

c. **Primary NCS timeout [Seconds]:** Select a timeout value for the Primary NCS. The default value is 10 seconds.

Note: The NCS Settings are used for the Branch Office (including the SRG), Virtual Office, and Geographic Redundancy features.

Figure 162
Network Connection Server (NCS) Settings



Network Connection Server (NCS) Settings

Primary NCS port: 16500

Alternate NCS port: 16500

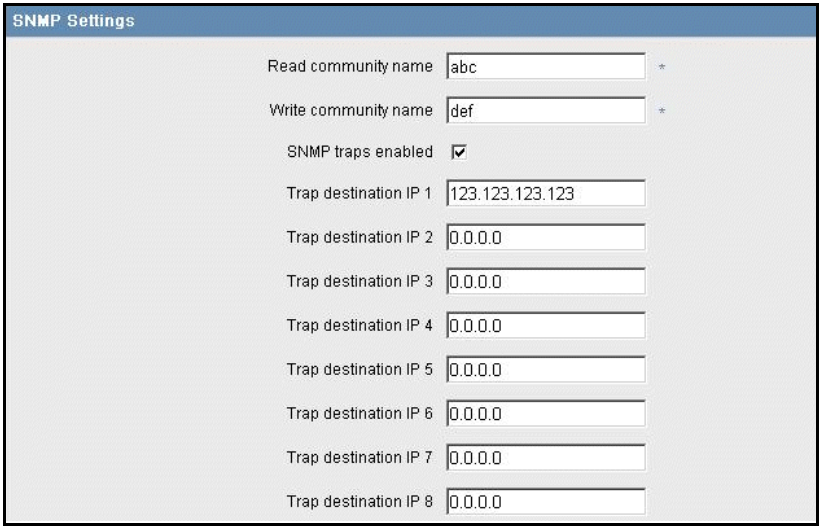
Primary NCS timeout [Seconds]: 10

7 If the NRS is in stand-alone mode (see page 385), go to step 8 and configure the SNMP Settings. The SNMP trap settings are available only when the NRS is in stand-alone mode, that is, not connected to the Call Server.

If the NRS is in co-resident mode (see page 385) the SNMP Settings section is not displayed in NRS Manager. Go to step 9 on page 411.

8 For **SNMP Settings** (see Figure 163 on page 410), configure the following if the NRS is in stand-alone mode:

Figure 163
SNMP Settings



SNMP Settings

Read community name	abc *
Write community name	def *
SNMP traps enabled	☑
Trap destination IP 1	123.123.123.123
Trap destination IP 2	0.0.0.0
Trap destination IP 3	0.0.0.0
Trap destination IP 4	0.0.0.0
Trap destination IP 5	0.0.0.0
Trap destination IP 6	0.0.0.0
Trap destination IP 7	0.0.0.0
Trap destination IP 8	0.0.0.0

a. **Read community name:** Enter the read community name. The name must be alphanumeric and can be up to 32 characters in length.

b. **Write community name:** Enter the read/write community name. The name must be alphanumeric and can be up to 32 characters in length.

Note: The read community name and the write community name control access to the Management Information Base (MIB). For detailed information, refer to *Simple Network Management Protocol: Description and Maintenance* (553-3001-519).

c. **SNMP traps enabled:** Select the check box to enable SNMP traps if configuring one or more SNMP management IP addresses to receive SNMP traps from cards in the IP Telephony node.

d. **Trap destination IP 1** to **Trap destination IP 8**: If SNMP traps are enabled, the SNMP traps are sent to the IP address entered in the text boxes. Up to eight SNMP trap servers can be defined. The default IP address is 0.0.0.0

9 Click **Save**.

End of Procedure

Configuration tab

The configuration tab is used to configure the NRS database. Configuration controls how data is stored in the database. The data is used by both the SIP Redirect Server and the H.323 Gatekeeper.

Configuring the NRS database

Use the procedures in this section to configure the NRS database.

Task summary list

To complete these tasks, perform the following procedures:

- Procedure 33: “Switching between the active and standby databases” on page 412
- Procedure 34: “Adding a Service Domain” on page 413
- Procedure 36: “Adding an L1 Domain (UDP)” on page 416
- Procedure 38: “Adding an L0 Domain (CDP)” on page 420
- Procedure 40: “Adding a Gateway Endpoint” on page 424
- Procedure 42: “Adding a Routing Entry” on page 432
- Procedure 46: “Adding a Collaborative Server” on page 442
- Procedure 57: “Cutting over and committing changes to the database” on page 460

Note 1: To add a SIP Phone refer to Procedure 76: “Adding a User Endpoint” on page 543. This procedure is located in the chapter that discusses “SIP Phone support” on page 523.

Note 2: Changes to the database do not affect call processing immediately. The database must first be cut over to the main active database. See Procedure 57 on page 460. Changes can be saved individually or in batches, depending on user preference.

Switching between the active and standby databases

The database has two schemas, active and standby.

- The active database is used for runtime queries.
- The standby database is used for administrator modifications.

  Note: By default, the database is in active database view when it is first started. In order to make changes on the configuration tab, the database must be in standby database view and you must have administrative authority.

To the right of the tabs is an area for switching between the active and standby databases (see Figure 165 on page 413).

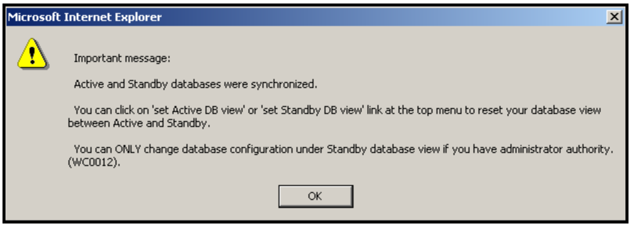
Use Procedure 33 to switch between the active and standby database.

Procedure 33
Switching between the active and standby databases

1 Click the **Configuration** tab.

A dialog box displays indicating the status of the active and standby database (see Figure 164).

Figure 164
Configuration tab message



Important message:

Active and Standby databases were synchronized.

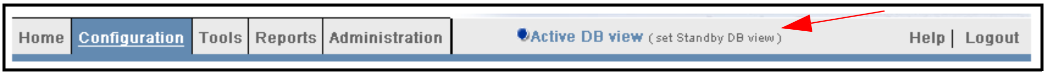
You can click on 'set Active DB view' or 'set Standby DB view' link at the top menu to reset your database view between Active and Standby.

You can ONLY change database configuration under Standby database view if you have administrator authority. (WC0012).

2 Click **OK**.

3 Click **set Standby DB view** to switch to the standby database (see Figure 165). The standby database is used for database modification.

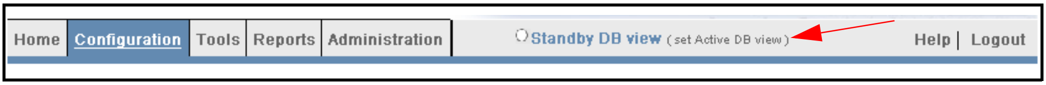
Figure 165
Active DB view selected



When the database is in standby database view, **Standby DB view** is bold (see Figure 166).

4 Click **set Active DB view** to switch to the active database (see Figure 166). The active database is used for database queries.

Figure 166
Switching between active and standby database view



End of Procedure

Note: Procedures 34 to 42 use the example hierarchy (myServiceProvider.com, myCompany.com, and so on) provided in the "Network Routing Service overview" on page 201.

Adding a Service Domain

The Service Domain is a building block of the routable SIP URI. It represents the service domain name field in the URI (see "SIP Uniform Resource Identifiers" on page 215).

Procedure 34
Adding a Service Domain

1 Select the **Configuration** tab.

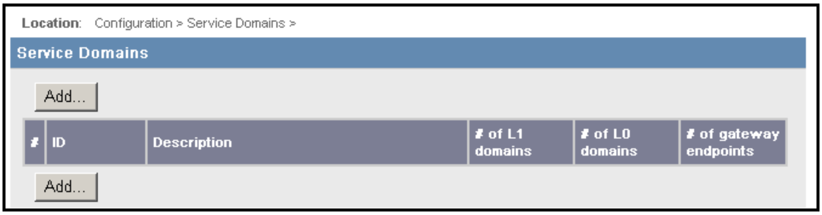
A dialog box displays indicating the status of the active and standby database (see Figure 164 on page 412). Click **OK**.

2 Switch to the **Standby DB view** (see Procedure 33 on page 412).

3 Click **Service Domains** in the navigator.

The **Service Domains** web page opens, as shown in Figure 167.

Figure 167
Service Domains web page



Location: Configuration > Service Domains >

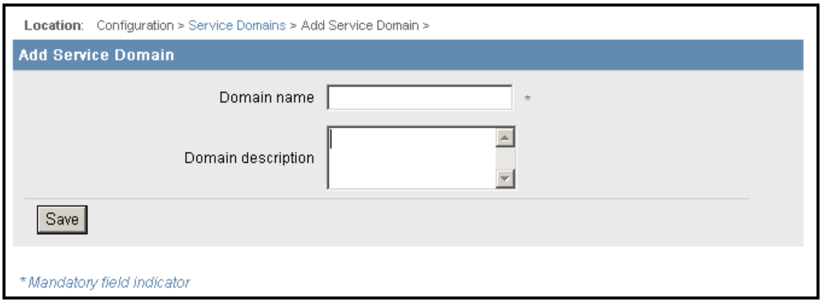
Service Domains

#	ID	Description	# of L1 domains	# of L0 domains	# of gateway endpoints

4 Click **Add...**.

The **Add Service Domain** web page opens, as shown in Figure 168.

Figure 168
Add Service Domain web page



Location: Configuration > Service Domains > Add Service Domain >

Add Service Domain

Domain name *

Domain description

*Mandatory field indicator

5 Enter a **Domain name** for the Service Domain.

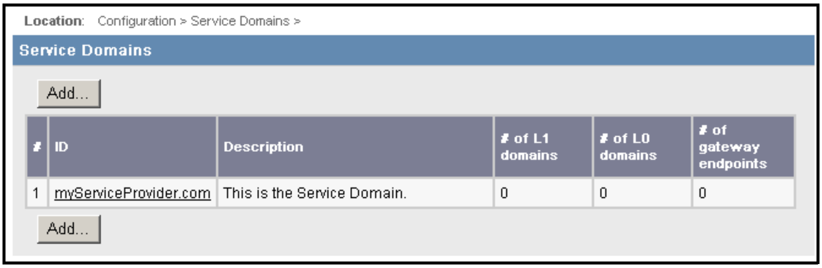
For example, enter myServiceProvider.com.

6 Enter a **Domain description** for the Service Domain.

7 Click **Save**.

The **Service Domains** web page opens, showing the newly added Service Domain. See Figure 169 on page 415.

Figure 169
Added Service Domain



Location: Configuration > Service Domains >

Service Domains

#	ID	Description	# of L1 domains	# of L0 domains	# of gateway endpoints
1	myServiceProvider.com	This is the Service Domain.	0	0	0

End of Procedure

Procedure 35
Viewing the Service Domains

1. Select the **Configuration** tab.

   A dialog box displays indicating the status of the active and standby database (see Figure 164 on page 412). Click **OK**.

2. Ensure the **Active DB view** is selected.

3. Click **Service Domains** from the navigator.

   The **Service Domains** web page opens and displays a list of any configured Service Domains.

End of Procedure

Adding a Level 1 Domain (UDP)

The Level 1 (L1) Domain is a building block of the phone context for private addresses. It represents the phone context root. For more information on phone context, refer to “SIP Uniform Resource Identifiers” on page 215.

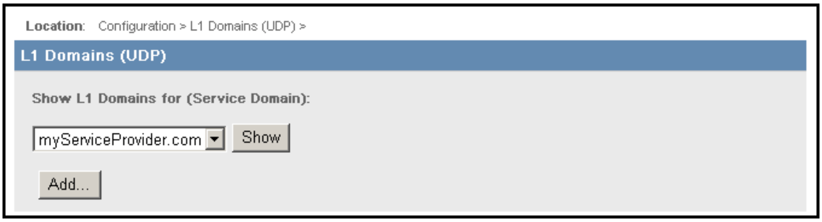
Procedure 36
Adding an L1 Domain (UDP)

1 Ensure the **Standby DB view** is selected.

2 Click **L1 Domains (UDP)** from the navigator.

The **L1 Domains (UDP)** web page opens, as shown in Figure 170. The drop-down list contains any available Service Domains.

Figure 170
L1 Domains (UDP) web page



Location: Configuration > L1 Domains (UDP) >

L1 Domains (UDP)

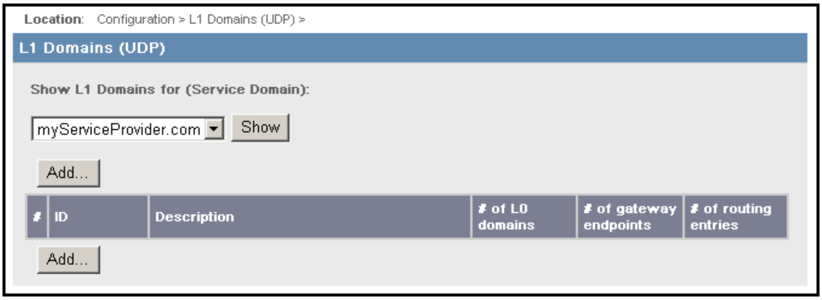
Show L1 Domains for (Service Domain): myServiceProvider.com

3 Select the **Service Domain** from the drop-down list.

This is the Service Domain where the new L1 subdomain will be added.

4 (Optional) Click **Show** to display a list of configured L1 Domains associated with the selected Service Domain. See Figure 171.

Figure 171
L1 Domains (UDP) web page for selected Service Domain



Location: Configuration > L1 Domains (UDP) >

L1 Domains (UDP)

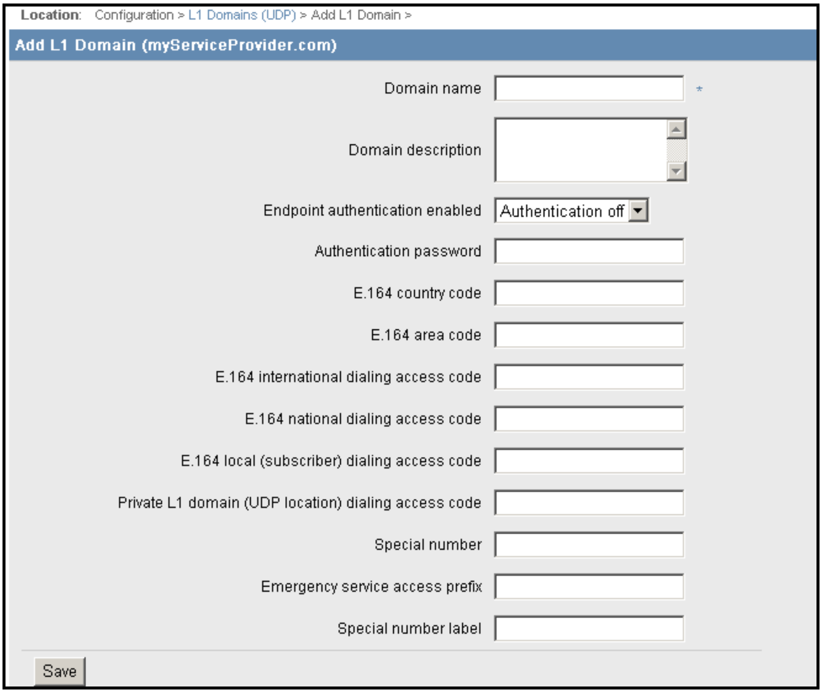
Show L1 Domains for (Service Domain): myServiceProvider.com

#	ID	Description	# of L0 domains	# of gateway endpoints	# of routing entries

5 Click **Add...**.

The **Add L1 Domain** web page opens, as shown in Figure 172 on page 417.

Figure 172
Add L1 Domain web page



Location: Configuration > L1 Domains (UDP) > Add L1 Domain >

Add L1 Domain (myServiceProvider.com)

Domain name *

Domain description

Endpoint authentication enabled: Authentication off

Authentication password

E.164 country code

E.164 area code

E.164 international dialing access code

E.164 national dialing access code

E.164 local (subscriber) dialing access code

Private L1 domain (UDP location) dialing access code

Special number

Emergency service access prefix

Special number label

6 Enter the **Domain name** of the L1 Domain. The name must be alphanumeric and can be up to30 characters in length.

For example, enter myCompany.com.

7 Enter the **Domain description**. The description can include any character except single quotes and can be up to 120 characters in length.

8 Select whether authentication is on or off from the **Endpoint authentication enabled** drop-down list.

If **Authentication on** is selected, then all endpoints require authentication.

9 Enter the **Authentication password**, if **Authentication on** was selected in step 8. The password must be alphanumeric and up to 30 characters in length.

10 Enter the **E.164 country code**. The code must be numeric and can be up to seven characters in length.

11 Enter the **E.164 area code**. The code must be numeric and can be up to seven characters in length.

12 Enter the **E.164 international dialing access code**. The code must be numeric and can be up to seven characters in length.

13 Enter the **E.164 national dialing access code**. The code must be numeric and can be up to seven characters in length.

14 Enter the **E.164 local (subscriber) dialing access code**. The code must be numeric and can be up to seven characters in length.

15 Enter the **Private L1 domain (UDP location) dialing access code**. The code must be numeric and can be up to seven characters in length.

16 Enter the **Special number**. The number must be numeric and can be up to 30 characters in length.

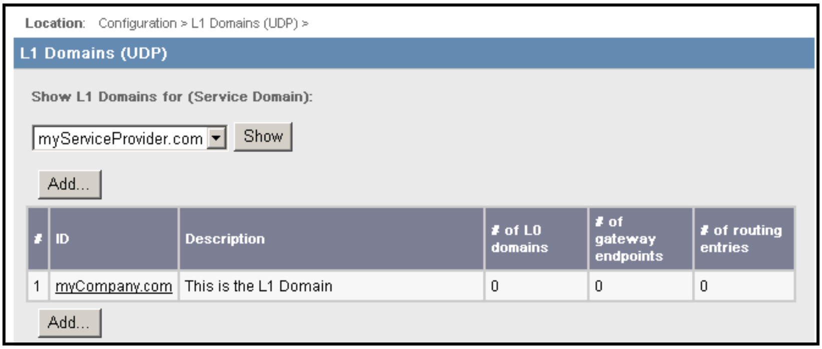
17 Enter the **Emergency service access prefix**. The number must be numeric and can be up to 30 characters in length.

18 Enter the **Special number label**. The label must be alphanumeric and can be up to 30 characters in length. The first character in the label must be alphabetic.

19 Click **Save**.

The **L1 Domains (UDP)** web page opens, showing the newly added myCompany.com L1 domain in the myServiceProvider.com Service Domain. See Figure 173 on page 419.

Figure 173
Added L1 Domain



Location: Configuration > L1 Domains (UDP) >

L1 Domains (UDP)

Show L1 Domains for (Service Domain):

myServiceProvider.com

#	ID	Description	# of L0 domains	# of gateway endpoints	# of routing entries
1	myCompany.com	This is the L1 Domain	0	0	0

End of Procedure

Procedure 37
Viewing the L1 Domains (UDP)

1 Select the **Configuration** tab.

A dialog box displays indicating the status of the active and standby database (see Figure 164 on page 412). Click **OK**.

2 Ensure the **Active DB view** is selected.

3 Click **L1 Domains (UDP)** from the navigator.

The **L1 Domains (UDP)** web page opens and displays a drop-down list of any configured Service Domains.

4 Select a Service Domain from the drop-down list.

5 Click **Show**.

The web page expands to display a list of any configured L1 Domains.

End of Procedure

Adding a Level 0 Domain (CDP)

The Level 0 (L0) Domain is a building block of the phone context for private addresses. For more information on phone context, refer to “SIP Uniform Resource Identifiers” on page 215.

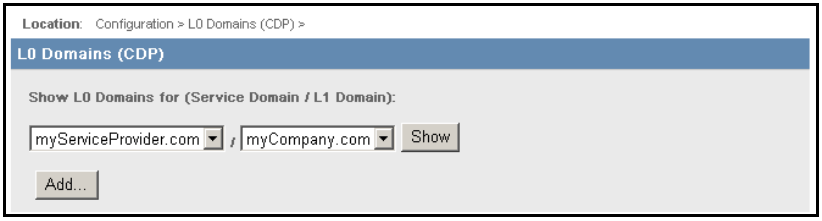
Procedure 38
Adding an L0 Domain (CDP)

1 Ensure the **Standby DB view** is selected.

2 Click **L0 Domains (CDP)** from the navigator.

The **L0 Domains (CDP)** web page opens, as shown in Figure 174. The two drop-down lists contains any available Service Domains and L1 Domains.

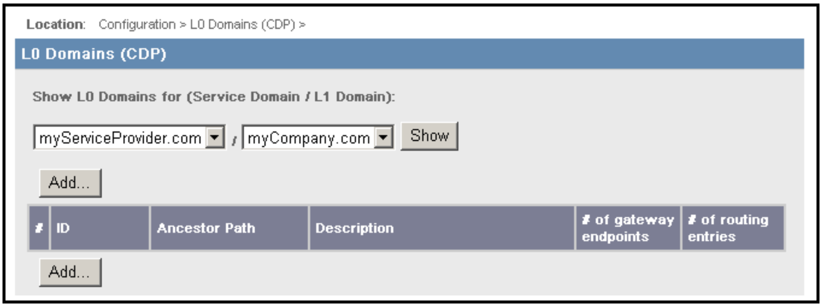
Figure 174
L0 Domain (CDP) web page


Location: Configuration > L0 Domains (CDP) >
L0 Domains (CDP)
Show L0 Domains for (Service Domain / L1 Domain):
myServiceProvider.com / myCompany.com
Show
Add...

3 Select the Service Domain and the L1 Domain from the respective drop-down lists.

4 (Optional) Click **Show** to display a list of configured L0 Domains associated with the selected Service Domain and L1 Domain. See Figure 175.

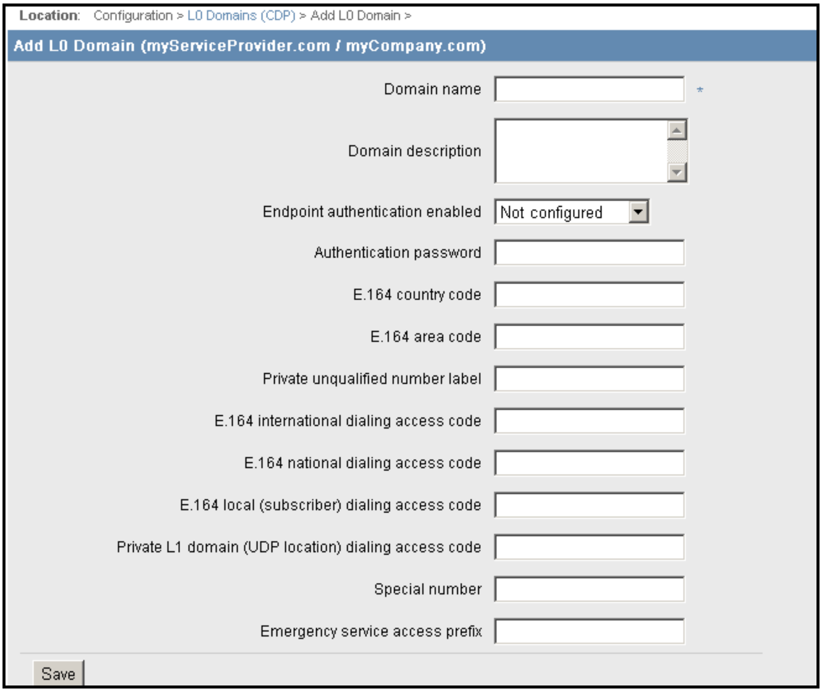
Figure 175
L0 Domains (CDP) web page for selected Service Domain / L1 Domain


Location: Configuration > L0 Domains (CDP) >
L0 Domains (CDP)
Show L0 Domains for (Service Domain / L1 Domain):
myServiceProvider.com / myCompany.com
Show
Add...
#
ID
Ancestor Path
Description
# of gateway endpoints
# of routing entries
Add...

5 Click **Add...**.

The **Add L0 Domain** web page opens, as shown in Figure 176 on page 421.

Figure 176
Add L0 Domain web page



Location: Configuration > L0 Domains (CDP) > Add L0 Domain >

Add L0 Domain (myServiceProvider.com / myCompany.com)

Domain name	*
Domain description	
Endpoint authentication enabled	Not configured
Authentication password	
E.164 country code	
E.164 area code	
Private unqualified number label	
E.164 international dialing access code	
E.164 national dialing access code	
E.164 local (subscriber) dialing access code	
Private L1 domain (UDP location) dialing access code	
Special number	
Emergency service access prefix	

6 Enter the **Domain name** of the L0 Domain. The name must be alphanumeric and up to 30 characters in length.

For example, enter myCdpDomain.

7 Enter the **Domain description**. The description can include any character except single quotes and can be up to 120 characters in length.

8 Select whether authentication is not configured, on, or off from the **Endpoint authentication enabled** drop-down list.

If **Authentication on** is selected, then all endpoints require authentication.

9 Enter the **Authentication password**, if **Authentication on** was selected in step 8 on page 421. The password must be alphanumeric and up to 30 characters in length.

10 Enter the **E.164 country code**. The code must be numeric and can be up to seven characters in length.

11 Enter the **E.164 area code**. The code must be numeric and can be up to seven characters in length.

12 Enter the **Private unqualified number label**. The label must be alphanumeric and can be up to 30 characters in length. The first character in the label must be alphabetic.

13 Enter the **E.164 international dialing access code**. The code must be numeric and can be up to seven characters in length.

14 Enter the **E.164 national dialing access code**. The code must be numeric and can be up to seven characters in length.

15 Enter the **E.164 local (subscriber) dialing access code**. The code must be numeric and can be up to seven characters in length.

16 Enter the **Private L1 domain (UDP location) dialing access code**. The code must be numeric and can be up to seven characters in length.

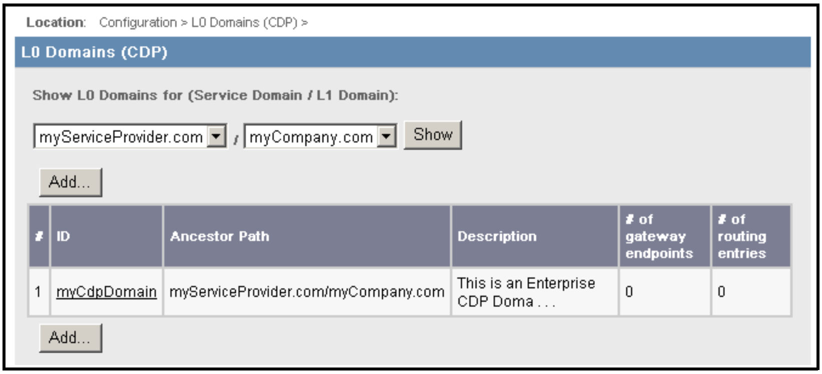
17 Enter the **Special number**. The number must be numeric and can be up to 30 characters in length.

18 Enter the **Emergency services access prefix**. The number must be numeric and can be up to 30 characters in length.

19 Click **Save**.

The **L0 Domains (CDP)** web page opens, showing the newly added myCdpDomain L0 domain. See Figure 177 on page 423.

Figure 177
Added L0 Domain



Location: Configuration > L0 Domains (CDP) >

L0 Domains (CDP)

Show L0 Domains for (Service Domain / L1 Domain):

myServiceProvider.com / myCompany.com

#	ID	Ancestor Path	Description	# of gateway endpoints	# of routing entries
1	myCdpDomain	myServiceProvider.com/myCompany.com	This is an Enterprise CDP Doma . . .	0	0

End of Procedure

Procedure 39
Viewing the L0 Domains (CDP)

1 Select the **Configuration** tab.

A dialog box displays indicating the status of the active and standby database (see Figure 164 on page 412). Click **OK**.

2 Ensure the **Active DB view** is selected.

3 Click **L0 Domains (CDP)** from the navigator.

The **Lo Domains (CDP)** web page opens and displays two drop-down lists of Service Domains and any configured L1 Domains.

4 Select a Service Domain and L1 Domain from the drop-down lists.

5 Click **Show**.

The web page expands to display a list of any configured LO Domains.

End of Procedure

Adding a Gateway Endpoint

Use Procedure 40 to add a gateway endpoint.

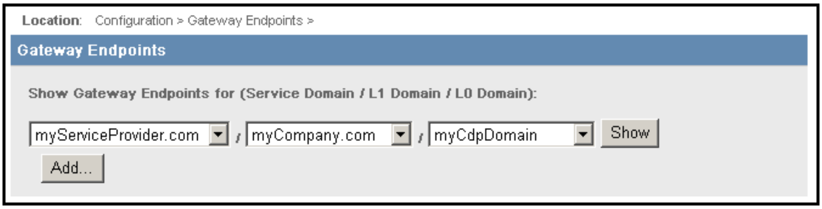
Procedure 40
Adding a Gateway Endpoint

1 Ensure the **Standby DB view** is selected.

2 Click **Gateway Endpoints** from the navigator.

The **Gateway Endpoints** web page opens, as shown in Figure 178. The three drop-down lists contain any available Service Domains, L1 Domains, and L0 Domains.

Figure 178
Gateway Endpoints web page



Location: Configuration > Gateway Endpoints >

Gateway Endpoints

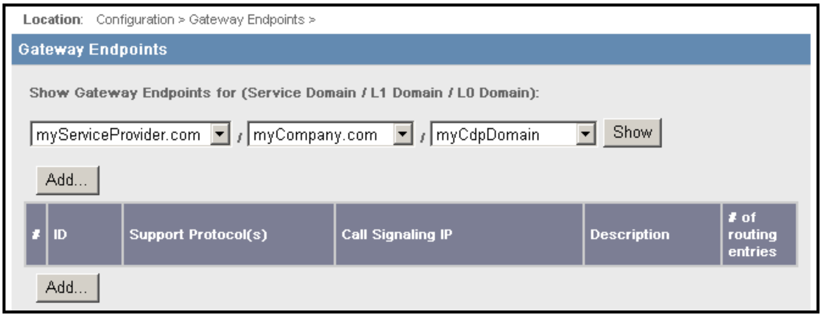
Show Gateway Endpoints for (Service Domain / L1 Domain / L0 Domain):

myServiceProvider.com / myCompany.com / myCdpDomain

3 Select the Service Domain, the L1 Domain, and L0 Domain from the respective drop-down lists.

4 (Optional) Click **Show** to display a list of configured L0 Domains associated with the selected Service Domain, L1 Domain, and L0 Domain. See Figure 175 on page 420.

Figure 179
Gateway Endpoints web page for selected Service Domain / L1 Domain / L0 Domain



Location: Configuration > Gateway Endpoints >

Gateway Endpoints

Show Gateway Endpoints for (Service Domain / L1 Domain / L0 Domain):

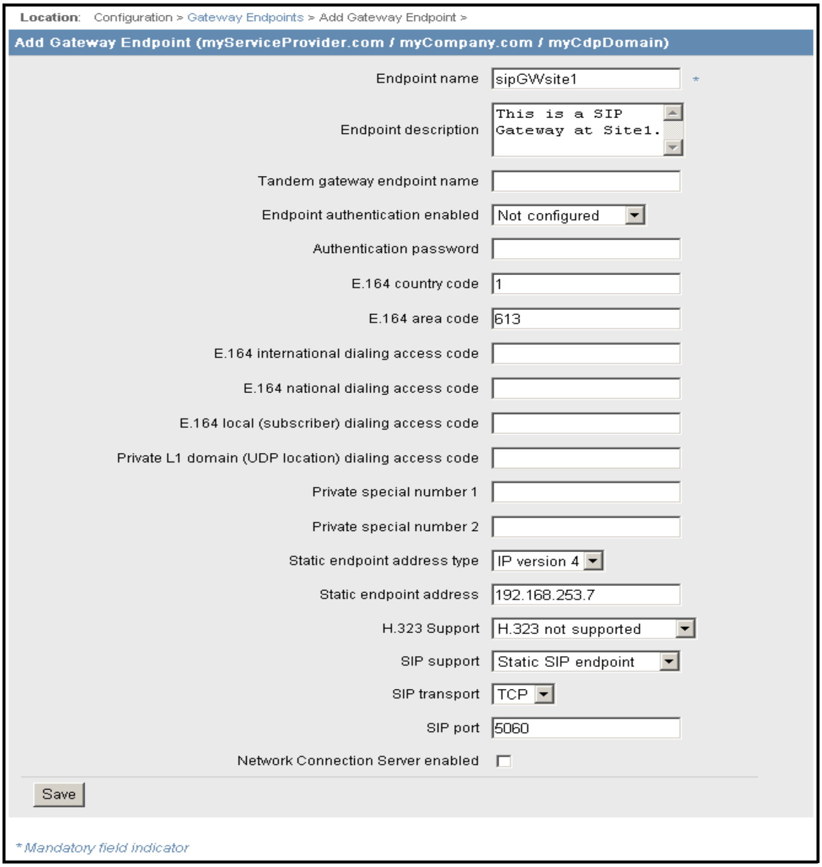
myServiceProvider.com / myCompany.com / myCdpDomain

#	ID	Support Protocol(s)	Call Signaling IP	Description	# of routing entries

5 Click **Add...**.

The **Add Gateway Endpoint** web page opens, as shown in Figure 180 on page 426.

Figure 180
Add Gateway Endpoint web page



Location: Configuration > Gateway Endpoints > Add Gateway Endpoint >

Add Gateway Endpoint (myServiceProvider.com / myCompany.com / myCdpDomain)

Endpoint name	sipGWsite1 *
Endpoint description	This is a SIP Gateway at Site1.
Tandem gateway endpoint name	
Endpoint authentication enabled	Not configured
Authentication password	
E.164 country code	1
E.164 area code	613
E.164 international dialing access code	
E.164 national dialing access code	
E.164 local (subscriber) dialing access code	
Private L1 domain (UDP location) dialing access code	
Private special number 1	
Private special number 2	
Static endpoint address type	IP version 4
Static endpoint address	192.168.253.7
H.323 Support	H.323 not supported
SIP support	Static SIP endpoint
SIP transport	TCP
SIP port	5060
Network Connection Server enabled	□

** Mandatory field indicator*

6 Enter the **Endpoint name** of the gateway. The name must be alphanumeric and can be up to 30 characters in length.

For example, enter sipGWSite1.

7 Enter a description of the endpoint in the **Endpoint description** text box. The description must be alphanumeric and can be up to 120 characters in length.

8 Enter the **Tandem gateway endpoint name**, if required. This indicates whether the endpoint is used to tandem calls from outside the network. The name must be alphanumeric and can be up to 30 characters in length.

Note: Use the **Look-up** link to find configured Gateway endpoints.

9 Select whether authentication is used from the **Endpoint authentication enabled** drop-down list.

The three options are:

- **Not configured**: If this option is selected, then the gateway endpoint uses the L1 or L0 Authentication (if L1 or L0 authentication is enabled).
- **Authentication off**: If this option is selected, then authentication is off for this gateway endpoint even if L1 or L0 authentication is enabled.
- **Authentication on**: If this option is selected, then authentication is on for this gateway endpoint and the authentication overrides the L1 or L0 authentication (if it is enabled).

10 Enter the **Authentication password**, if **Authentication on** was selected in step 9. The password must be alphanumeric and can be up to 30 characters in length.

11 Enter the **E.164 country code**. The code must be numeric and can be up to seven characters in length.

12 Enter the **E.164 area code**. The code must be numeric and can be up to seven characters in length.

13 Enter the **E.164 international dialing access code**. The code must be numeric and can be up to seven characters in length.

14 Enter the **E.164 national dialing access code**. The code must be numeric and can be up to seven characters in length.

15 Enter the **E.164 local (subscriber) dialing access code**. The code must be numeric and can be up to seven characters in length.

16 Enter the **Private L1 domain (UDP location) dialing access code**. The code must be numeric and can be up to seven characters in length.

17 Enter the **Private special number 1**. The number must be numeric and can be up to 30 characters in length.

18 Enter the **Private special number 2**. The number must be numeric and can be up to 30 characters in length

19 Select **IP Version 4** from the **Static endpoint address type** drop-down list.

20 Enter the **Static endpoint address**.

This is the Node IP address of the Signaling Server. If a third-party gateway is being used, then it is the IP address of the gateway.

21 Select whether H.323 support is enabled from the **H.323 Support type** drop-down list.

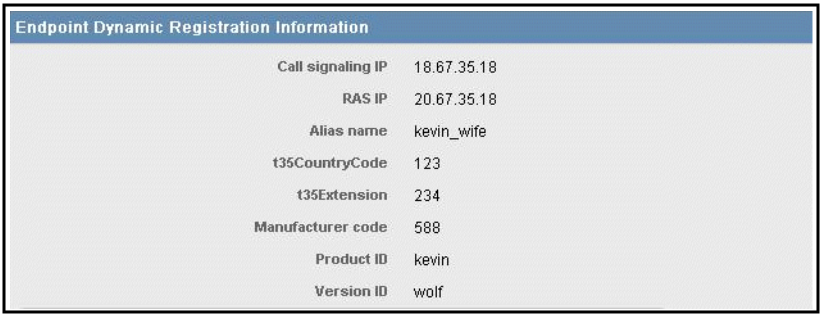
The three options are: H.323 not supported, RAS H.323 endpoint, and Not RAS H.323 endpoint.

Note: If an H.323 Gateway Endpoint is configured with an H.323 Support type of RAS H.323 endpoint, then NRS Manager displays Endpoint Dynamic Registration information after the H.323 Gateway registers with the NRS.

Endpoint Dynamic Registration information includes the following: Call Signaling IP, RAS IP, Alias name, t35Country code, t35Extension, Manufacturer code, Product ID, and Version ID.

The H.323 **Endpoint Dynamic Registration Information** web page (see Figure 181) is displayed only when NRS Manager is in **Active DB view**. The detailed dynamic registration information also is displayed only inside the Gateway Endpoint web page.

Figure 181
H.323 Endpoint Dynamic Registration Information web page



Endpoint Dynamic Registration Information

Call signaling IP	18.67.35.18
RAS IP	20.67.35.18
Alias name	kevin_wife
t35CountryCode	123
t35Extension	234
Manufacturer code	588
Product ID	kevin
Version ID	wolf

22 Select whether SIP support is enabled.

a. Select an option from the **SIP Support type** drop-down list. The three options are: SIP not supported, Static SIP endpoint, and Dynamic SIP endpoint.

b. Select the transport protocol from the **SIP transport** drop-down list. The two options are: TCP and UDP. TCP is selected by default.

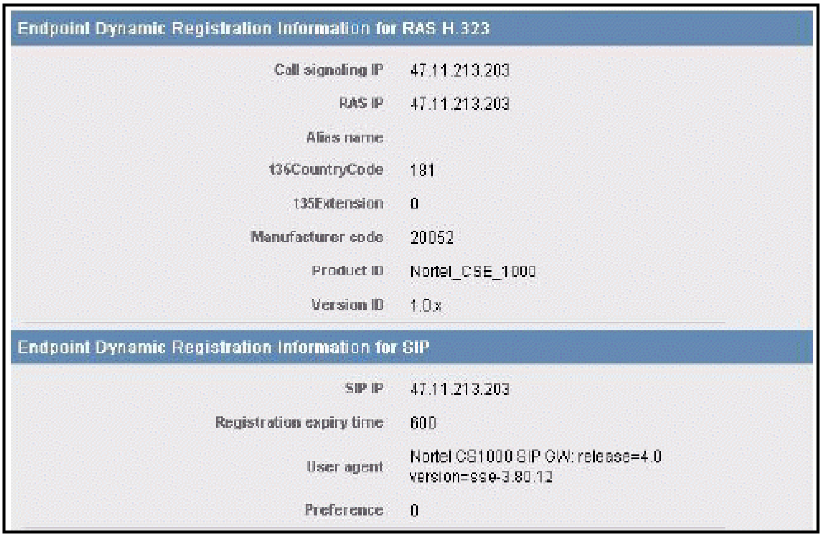
c. Verify that the port number is **5060** for the **SIP port**. If the SIP Port is changed the value must be numeric and can be up to 5 numbers in length. The range is 0 to 65535 and the default is 5060.

Note: If a SIP Trunk Gateway Endpoint is configured with a SIP Support type of Dynamic SIP endpoint, then NRS Manager displays Endpoint Dynamic Registration Information for SIP after the SIP Trunk Gateway registers with the NRS.

Endpoint Dynamic Registration Information includes the following: SIP IP, Registration expiry time, User agent, and Preference.

The SIP **Endpoint Dynamic Registration Information** web page (see Figure 182 on page 430) is displayed only when NRS Manager is in **Active DB view**. The detailed dynamic registration information also is displayed only inside the Gateway Endpoint web page.

Figure 182
SIP Endpoint Dynamic Registration Information web page



Endpoint Dynamic Registration Information for RAS H.323

Call signaling IP	47.11.213.203
RAS IP	47.11.213.203
Alias name	
t36CountryCode	181
t35Extension	0
Manufacturer code	20052
Product ID	Nortel_CSE_1000
Version ID	1.0.x

Endpoint Dynamic Registration Information for SIP

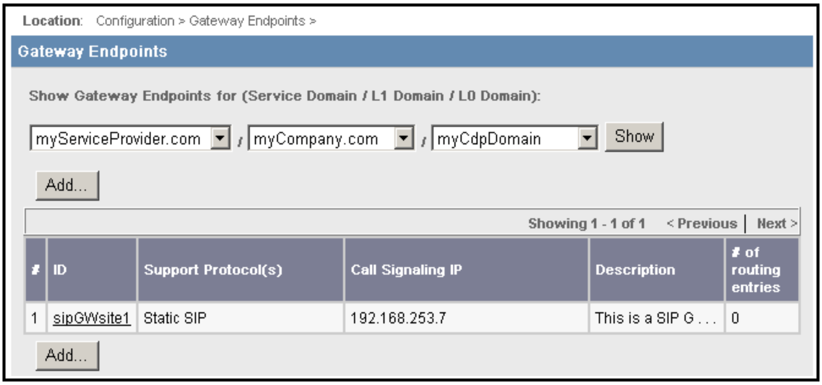
SIP IP	47.11.213.203
Registration expiry time	600
User agent	Nortel CS1000 SIP GW: release=4.0 version=sse-3.80.12
Preference	0

23 Select the **Network Connection Server is enabled** check box if this Gateway Endpoint supports the NCS for branch office or SRG user redirection to the main office, Virtual Office, or Geographic Redundancy.

24 Click **Save**.

The **Gateway Endpoints** web page opens, showing the newly added sipGWSite1 endpoint. See Figure 183 on page 431.

Figure 183
Added Gateway Endpoints



Location: Configuration > Gateway Endpoints >

Gateway Endpoints

Show Gateway Endpoints for (Service Domain / L1 Domain / L0 Domain):

myServiceProvider.com / myCompany.com / myCdpDomain

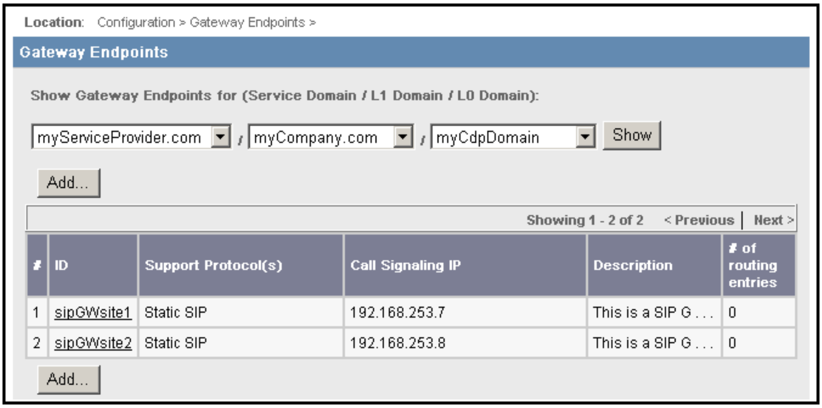
Showing 1 - 1 of 1 < Previous | Next >

#	ID	Support Protocol(s)	Call Signaling IP	Description	# of routing entries
1	sipGWsite1	Static SIP	192.168.253.7	This is a SIP G . . .	0

25 If required, click **Add...** to add additional gateway endpoints. Repeat step 6 to step 24.

Any new endpoints are displayed in the **Gateway Endpoints** web page (see Figure 184).

Figure 184
Gateway Endpoints



Location: Configuration > Gateway Endpoints >

Gateway Endpoints

Show Gateway Endpoints for (Service Domain / L1 Domain / L0 Domain):

myServiceProvider.com / myCompany.com / myCdpDomain

Showing 1 - 2 of 2 < Previous | Next >

#	ID	Support Protocol(s)	Call Signaling IP	Description	# of routing entries
1	sipGWsite1	Static SIP	192.168.253.7	This is a SIP G . . .	0
2	sipGWsite2	Static SIP	192.168.253.8	This is a SIP G . . .	0

End of Procedure

Procedure 41
Viewing the Gateway Endpoints

1 Select the **Configuration** tab.

A dialog box displays indicating the status of the active and standby database (see Figure 164 on page 412). Click **OK**.

2 Ensure the **Active DB view** is selected.

3 Click **Gateway Endpoints** from the navigator.

The **Gateway Endpoints** web page opens and displays three drop-down lists: Service Domains, L1 Domains, and any configured L0 Domains.

4 Select a Service Domain, L1 Domain, and L0 Domain from the drop-down lists.

5 Click **Show**.

The web page expands to display a list of any configured Gateway Endpoints.

End of Procedure

Adding a User Endpoint

To add a User Endpoint (that is, a SIP Phone), refer to “SIP Phone support” on page 523 and Procedure 76: “Adding a User Endpoint” on page 543.

Adding a Routing Entry

Procedure 42
Adding a Routing Entry

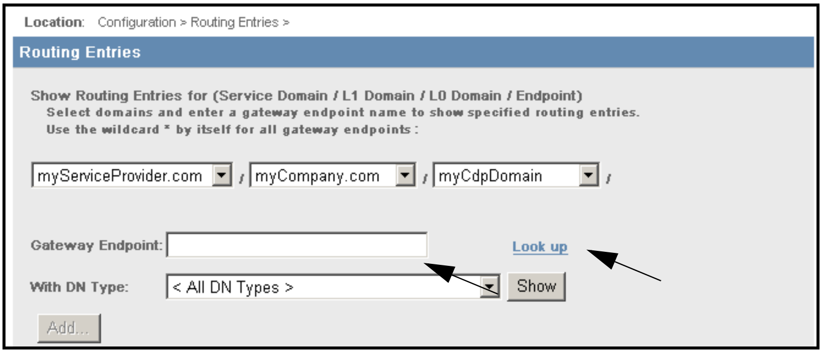
1 Ensure the **Standby DB view** is selected.

2 Click **Routing Entries** from the navigator.

The **Routing Entries** web page opens, as shown in Figure 185 on page 433.

Note: The **Gateway Endpoint** field is empty.

Figure 185
Routing Entries web page



Location: Configuration > Routing Entries >

Routing Entries

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified routing entries.
Use the wildcard * by itself for all gateway endpoints :

mySeriviceProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint:

With DN Type: < All DN Types >

3 Fill the **Gateway Endpoint** text box using one of the following two methods:

- Enter * to display all Gateway Endpoints; or
- Click **Look up** to find a Gateway Endpoint name and to accurately fill the Endpoint text box.

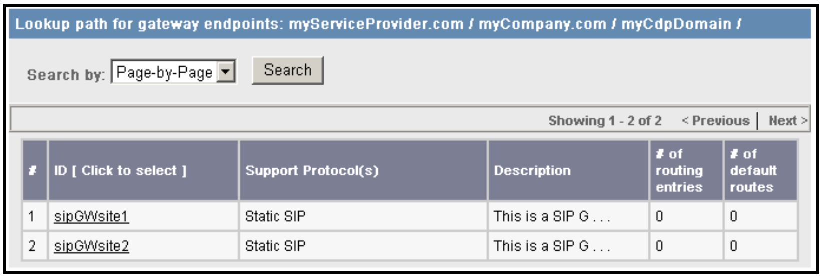
  The **Look up path for gateway endpoints** web page opens, as shown in Figure 186 on page 434. This **Look up** search utility allows you to search for Gateway Endpoint in two ways: Page-by-Page and Name prefix.

  — The **Page-by-Page** search is the default search method, and the results are displayed in the **Look up path for gateway endpoints** web page, as shown in Figure 186 on page 434.

  — To perform a Name prefix search, select **Name prefix** from the drop-down list. In the text box, enter the name of a Gateway Endpoint for which to search, as shown in Figure 187 on page 434. Click **Search**, and the Gateway Endpoints are displayed, as shown in Figure 188 on page 434.

  Click an Endpoint ID to select the Gateway Endpoint. The ID of the selected Gateway Endpoint is entered in the **Gateway Endpoint** text box, as shown in Figure 189 on page 435.

Figure 186
Lookup path for gateway endpoints web page — Page-by-Page search



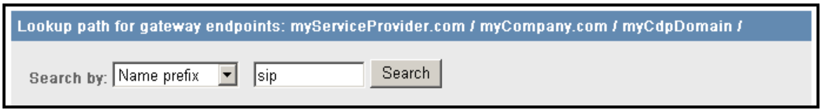
Lookup path for gateway endpoints: myServiceProvider.com / myCompany.com / myCdpDomain /

Search by: Page-by-Page Search

Showing 1 - 2 of 2 < Previous | Next >

#	ID [Click to select]	Support Protocol(s)	Description	# of routing entries	# of default routes
1	sipGWsite1	Static SIP	This is a SIP G . . .	0	0
2	sipGWsite2	Static SIP	This is a SIP G . . .	0	0

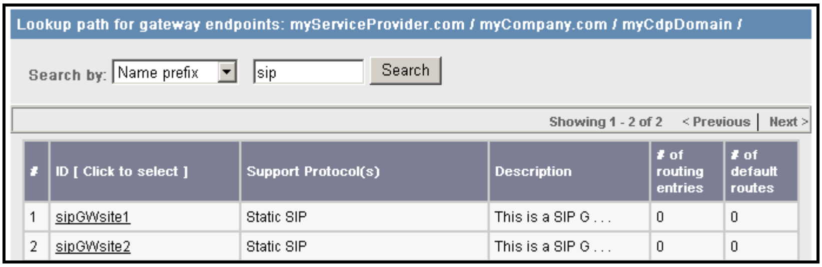
Figure 187
Name prefix search entry



Lookup path for gateway endpoints: myServiceProvider.com / myCompany.com / myCdpDomain /

Search by: Name prefix sip Search

Figure 188
Results of Name prefix search



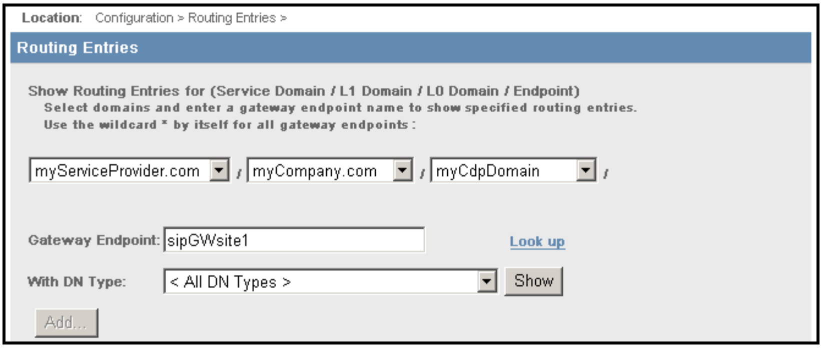
Lookup path for gateway endpoints: myServiceProvider.com / myCompany.com / myCdpDomain /

Search by: Name prefix sip Search

Showing 1 - 2 of 2 < Previous | Next >

#	ID [Click to select]	Support Protocol(s)	Description	# of routing entries	# of default routes
1	sipGWsite1	Static SIP	This is a SIP G . . .	0	0
2	sipGWsite2	Static SIP	This is a SIP G . . .	0	0

Figure 189
Results of Gateway Endpoint look up



Location: Configuration > Routing Entries >

Routing Entries

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified routing entries.
Use the wildcard * by itself for all gateway endpoints :

myServiceProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint: sipGWsite1

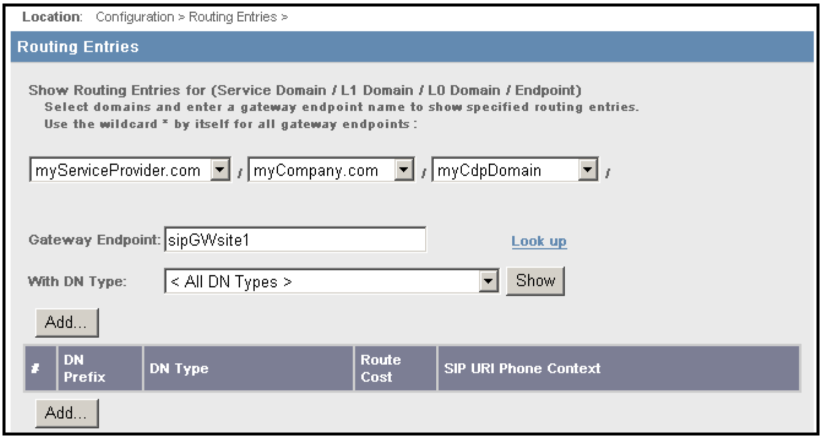
With DN Type: < All DN Types >

4 Select the DN type(s) from the **With DN Type** drop-down list. The seven choices are <All DN Types>, E.164 international, E.164 national, E.164 local (subscriber), Private level 1 regional (UDP location code), Private level 0 regional (CDP steering code), and Private special.

5 Click **Show**.

The window expands to display a list of any DNs of the type selected in step 4, and associated with this Gateway Endpoint(s). See Figure 190.

Figure 190
DNs of selected type associated with selected Endpoint(s)



Location: Configuration > Routing Entries >

Routing Entries

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified routing entries.
Use the wildcard * by itself for all gateway endpoints :

myServiceProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint: sipGWsite1

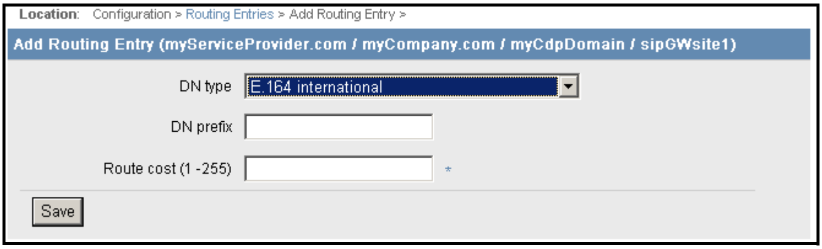
With DN Type: < All DN Types >

#	DN Prefix	DN Type	Route Cost	SIP URI Phone Context

6 Click **Add...**.

The **Add Routing Entry** web page opens, as shown in Figure 191.

Figure 191
Add Routing Entry



Location: Configuration > Routing Entries > Add Routing Entry >

Add Routing Entry (myServiceProvider.com / myCompany.com / myCdpDomain / sipGWsite1)

DN type: E.164 international

DN prefix:

Route cost (1 -255): *

7 Select the **DN type**.

The six options are E.164 international, E.164 national, E.164 local (subscriber), Private level 1 regional (UDP location code), Private level 0 regional (CDP steering code), and Private special.

This attribute determines how to build the phone context value (out of the possible building block configured against the routing entry parents) that is used to qualify the DN prefix.

8 Enter the **DN prefix**. The DN prefix can include 0-9, #, -, ?. The prefix can be up to 30 characters in length; however, the first character must be numeric.

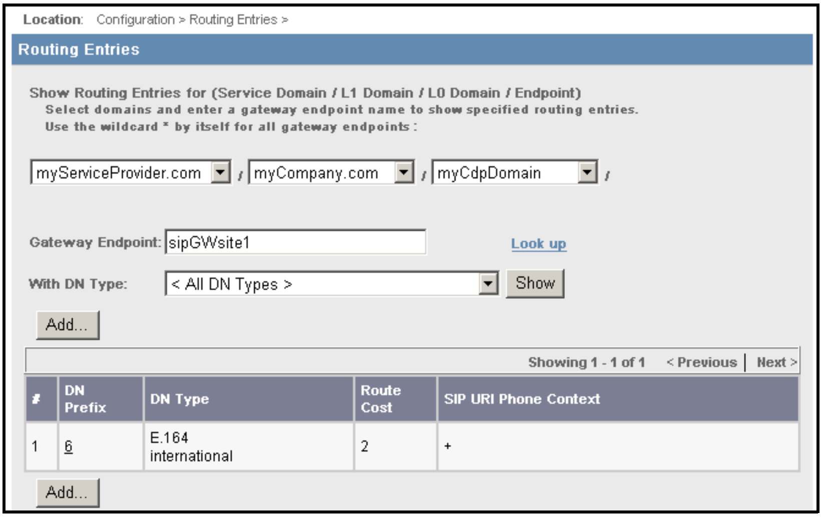
9 Enter the **Route cost**. The range is 1-255. The cost must be numeric and can be up to three characters in length.

This number is used to define least-cost routing. Higher numbers indicate higher costs.

10 Click **Save**.

The **Routing Entries** web page opens, showing the newly added routing entry, as shown in Figure 192 on page 437.

Figure 192
Added Routing Entry



Location: Configuration > Routing Entries >

Routing Entries

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified routing entries.
Use the wildcard * by itself for all gateway endpoints :

myServiceProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint: sipGWsite1

With DN Type: < All DN Types >

#	DN Prefix	DN Type	Route Cost	SIP URI Phone Context
1	6	E.164 international	2	+

End of Procedure

Procedure 43
Viewing the Routing Entries

1 Select the **Configuration** tab.

A dialog box displays indicating the status of the active and standby database (see Figure 164 on page 412). Click **OK**.

2 Ensure the **Active DB view** is selected.

3 Click **Routing Entries** from the navigator.

The **Routing Entries** web page opens.

4 Select a Service Domain, L1 Domain, and L0 Domain from the three drop-down lists, respectively.

5 Fill the **Gateway Endpoint** text using either of the methods described in Procedure 42, step 3 on page 438.

6 Select the DN type from the **With DN Type** drop-down list.

7 Click **Show**.

The web page expands to display a list of configured Routing Entries.

End of Procedure

Adding Default Routes

If the routing entry DN prefix in an incoming H.323/SIP signaling request does not match any corresponding DN prefix Gateway Endpoint routing entry recorded in the NRS, then the default route is returned to the gateway.

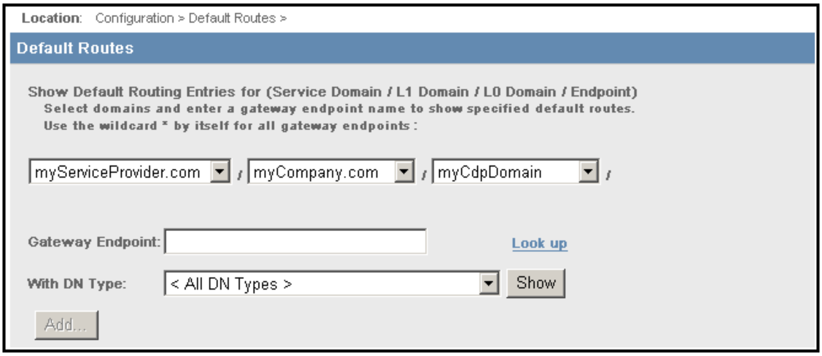
Procedure 44
Adding a Default Route

1 Ensure the **Standby DB view** is selected.

2 Click **Default Routes** from the navigator.

The **Default Routes** web page opens, as shown in Figure 193.

Figure 193
Default Routes web page



Location: Configuration > Default Routes >

Default Routes

Show Default Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified default routes.
Use the wildcard * by itself for all gateway endpoints :

mySericeProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint:

With DN Type: < All DN Types >

3 Fill the **Gateway Endpoint** text using either of the methods described in Procedure 42, step 3 on page 438.

4 Select the DN type from the **With DN Type** drop-down list.

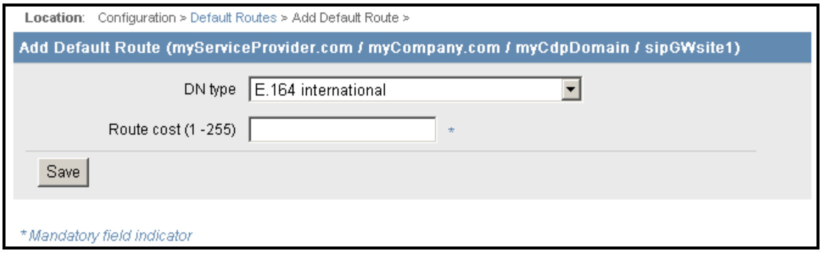
5 Click **Show**.

The window expands to show any DNs associated with the selected Endpoint(s).

6 Click **Add...**.

The **Add Default Route** web page opens, as shown in Figure 194 on page 439.

Figure 194
Add Default Route web page



Location: Configuration > Default Routes > Add Default Route >

Add Default Route (myServiceProvider.com / myCompany.com / myCdpDomain / sipGWsite1)

DN type: E.164 international

Route cost (1 -255): *

* Mandatory field indicator

7 Select the **DN type**.

The six options are E.164 international, E.164 national, E.164 local (subscriber), Private level 1 regional (UDP location code), Private level 0 regional (CDP steering code), and Private special.

This attribute determines how to build the phone context value (out of the possible building blocks configured against the routing entry parents) that is used to qualify the DN prefix.

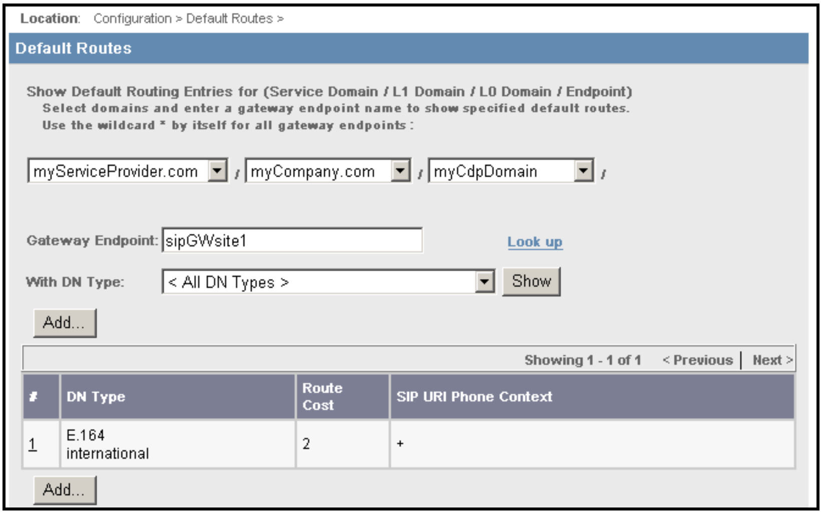
Note: Each DN type has only one default route.

8 Enter the **Route cost**. The range is 1-255. The cost must be numeric and can be up to three characters in length.

9 Click **Save**.

The **Default Routes** web page opens showing the new default route. See Figure 195 on page 440.

Figure 195
Added Default Route



Location: Configuration > Default Routes >

Default Routes

Show Default Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified default routes.
Use the wildcard * by itself for all gateway endpoints :

myServiceProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint: sipGWsite1

With DN Type: < All DN Types >

#	DN Type	Route Cost	SIP URI Phone Context
1	E.164 international	2	+

End of Procedure

Procedure 45
Viewing Default Routes

1 Ensure the **Standby DB view** is selected.

2 Click **Default Routes** from the navigator.

The **Default Routes** web page opens.

3 Select a Service Domain, L1 Domain, and L0 Domain from the three drop-down lists, respectively.

4 Fill the **Gateway Endpoint** text using either of the methods described in Procedure 42, step 3 on page 438.

5 Select the DN type from the **With DN Type** drop-down list.

6 Click **Show**.

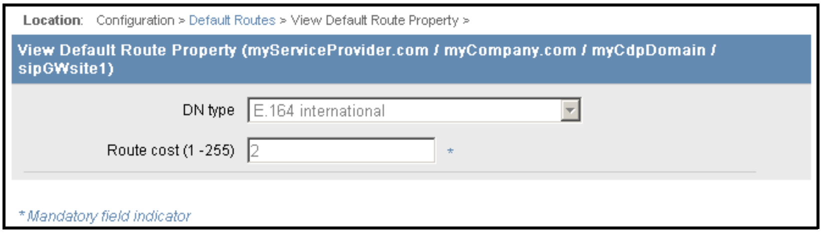
The web page expands to display a list of any configured Routing Entries.

7 Click the listed route number for the Default Route.

8 The **View Default Route Property** web page opens, as shown in Figure 196.

You can edit the properties of this Default Route on this page, or delete the Default Route altogether.

Figure 196
View Default Route Property web page



Location: Configuration > Default Routes > View Default Route Property >

View Default Route Property (myServiceProvider.com / myCompany.com / myCdpDomain / sipGWsite1)

DN type: E.164 international

Route cost (1 -255): 2 *

Mandatory field indicator

End of Procedure

Adding a Collaborative Server

A Collaborative Server is a server in another network zone that can be used to resolve requests when the NRS cannot find a match in its numbering plan database.

NRS Manager provides a utility for adding and viewing Collaborative Servers either system-wide or in different network domains.

A Collaborative Server can be configured as “system-wide”, across all domains. This configuration allows IP addresses to be shared by users across multiple domains. This also allows domains to be spread geographically.

NRS Collaborative Servers in different network domains can also be specified in the NRS.

If a request comes in from a gateway and the NRS cannot find a match in its database for the request, then the NRS provides the IP address of another Collaborative Server to the gateway. The gateway can then send its request to the provided Collaborative Server.

> *Note:* Calls can only be made in the same domain, even though calls go through the Collaborative Server to find a match.

For more information about the Collaborative Server, refer to "Collaboration between a CS 1000 Release 4.0 (or later) NRS and a Succession 3.0 H.323 Gatekeeper or MCS 5100" on page 559.

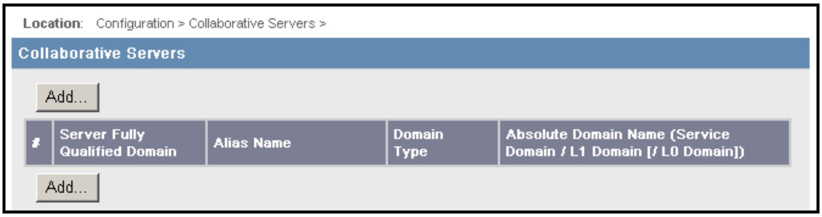
Procedure 46
Adding a Collaborative Server

1 Ensure the **Standby DB view** is selected.

2 Click **Collaborative Server** from the navigator.

The **Collaborative Servers** web page opens, as shown in Figure 197.

Figure 197
Collaborative Servers web page



Location: Configuration > Collaborative Servers >

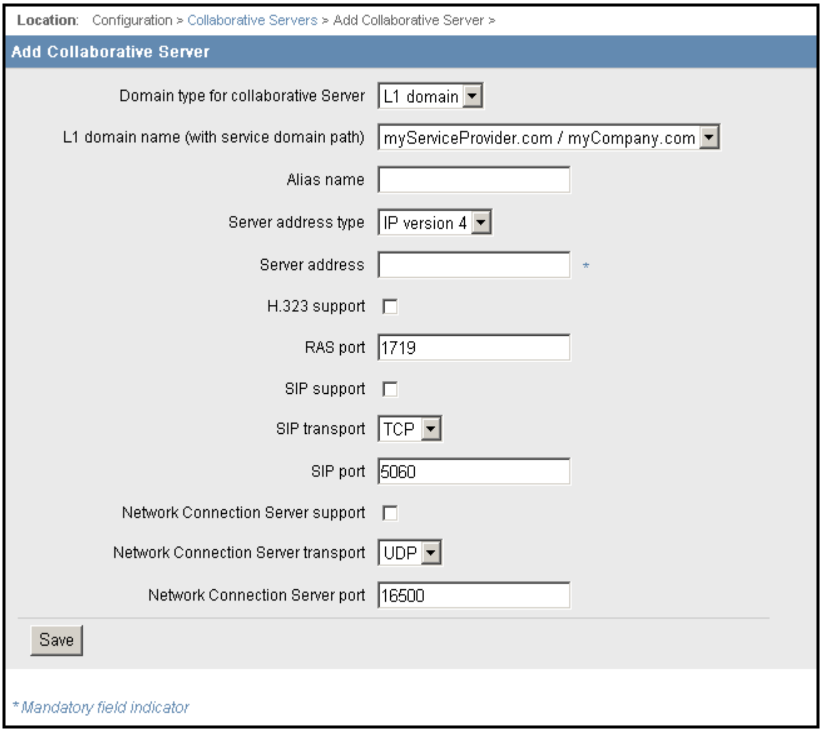
Collaborative Servers

#	Server Fully Qualified Domain	Alias Name	Domain Type	Absolute Domain Name (Service Domain / L1 Domain [/ L0 Domain])

3 Click **Add...**.

The **Add Collaborative Server** web page opens, as shown in Figure 198 on page 443.

Figure 198
Add Collaborative Server (with L1 Domain)



Location: Configuration > Collaborative Servers > Add Collaborative Server >

Add Collaborative Server

Domain type for collaborative Server	L1 domain ▾
L1 domain name (with service domain path)	myServiceProvider.com / myCompany.com ▾
Alias name	
Server address type	IP version 4 ▾
Server address	*
H.323 support	□
RAS port	1719
SIP support	□
SIP transport	TCP ▾
SIP port	5060
Network Connection Server support	□
Network Connection Server transport	UDP ▾
Network Connection Server port	16500

** Mandatory field indicator*

4 Select the **Domain type for Collaborative Server** from the drop-down list.

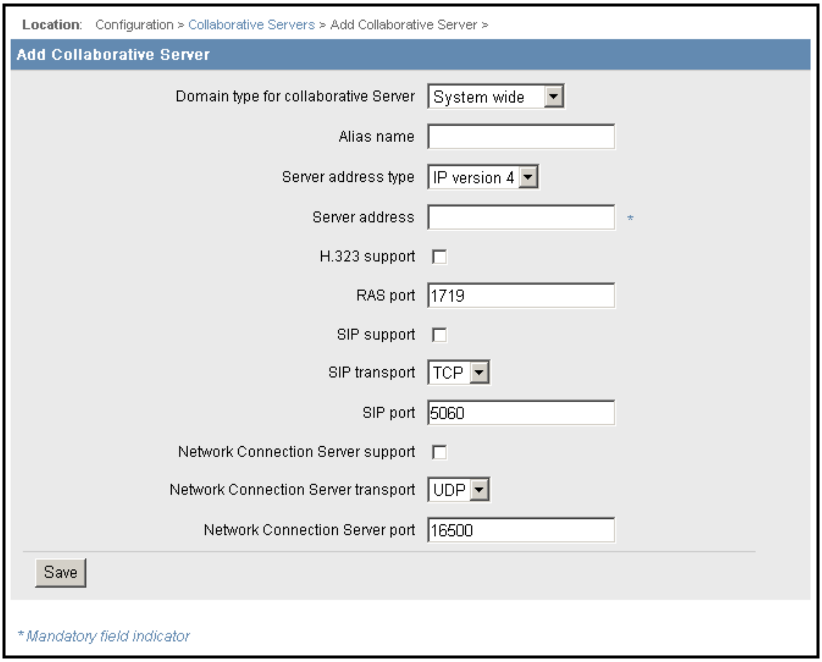
- Select **System wide** if the Collaborative Server is to be a system-wide server. See Figure 199 on page 444.
- Select **Service domain** is the Collaborative Server is to be a Service Domain server.
- Select **L1 domain** if the Collaborative Server is to be an L1 Domain server.
- Select **L0 domain** if the Collaborative Server is to be an L0 Domain server.

An additional field **L0 Domain** is displayed, prompting for the name of the L0 domain. See Figure 200 on page 445. Select the name of the L0 Domain from the drop-down list.

Note 1: Ensure that the Succession Release 3.0 Gatekeeper is provisioned in the same Service Domain and Level 1 Domain (UDP) as the originating endpoint.

Note 2: Provision the Succession Release 3.0 Gatekeeper as a Level 1 Domain Gatekeeper to allow support for CDP interzone dialing for multiple zones. That is, if the Succession Release 3.0 Gatekeeper supports CDP Domain A and Domain B, then provisioning the Gatekeeper as a Level 1 Zone Collaborative Server allows the CS 1000 Release 4.5 NRS to send its calls from both zones A and B (depending on the CDP domain of the call originator on the CS 1000 Release 4.5 NRS zone).

Figure 199
Add Collaborative Server (system-wide)



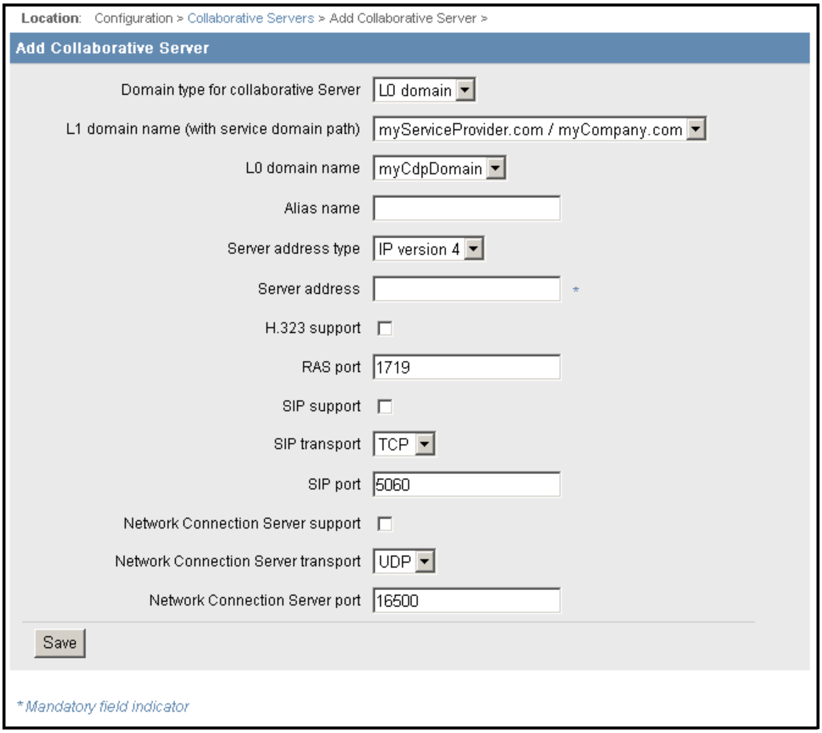
Location: Configuration > Collaborative Servers > Add Collaborative Server >

Add Collaborative Server

Domain type for collaborative Server	System wide ▾
Alias name	
Server address type	IP version 4 ▾
Server address	*
H.323 support	□
RAS port	1719
SIP support	□
SIP transport	TCP ▾
SIP port	5060
Network Connection Server support	□
Network Connection Server transport	UDP ▾
Network Connection Server port	16500

* Mandatory field indicator

Figure 200
Add Collaborative Server (with L0 Domain)



Location: Configuration > Collaborative Servers > Add Collaborative Server >

Add Collaborative Server

Domain type for collaborative Server	L0 domain ▾
L1 domain name (with service domain path)	myServiceProvider.com / myCompany.com ▾
L0 domain name	myCdpDomain ▾
Alias name	
Server address type	IP version 4 ▾
Server address	*
H.323 support	□
RAS port	1719
SIP support	□
SIP transport	TCP ▾
SIP port	5060
Network Connection Server support	□
Network Connection Server transport	UDP ▾
Network Connection Server port	16500

** Mandatory field indicator*

5 Enter the **Alias name** of the collaborative server. The alias name must be alphanumeric and can be up to 30 characters in length. The name cannot include spaces.

6 Select **IP version 4** from the **Server address type** drop-down list.

7 Enter the TLAN IP address of the server in the **Server address** text box.

8 Select the protocol(s) supported by the server.

- If H.323 is supported, then perform the following steps:

  i. Select the **H.323 support** check box.

  ii. Enter the **RAS port** number. The port number must be numeric and can be up to five characters in length.

- If SIP is supported, then perform the following steps:

  i. Select the **SIP support** check box.

  ii. Select the transport protocol from the **SIP transport** drop-down list. TCP is the default.

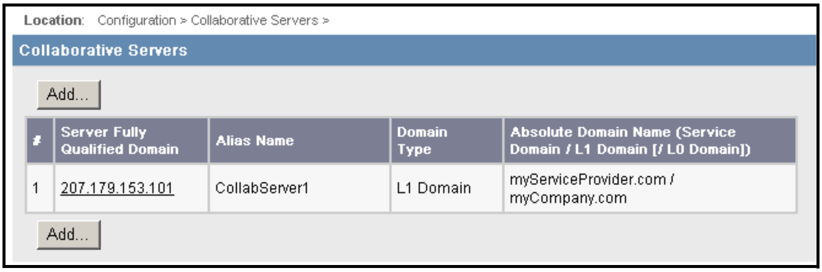
  iii. Enter the **SIP port** number. The port number must be numeric and can be up to five characters in length.

9 Ensure that the **Network Connection Server support** check box is not selected. The Collaborative Server does not support the Network Connection Service (NCS).

10 Click **Save**.

The **Collaborative Servers** web page opens with the newly added collaborative server, as shown in Figure 201.

Figure 201
Added Collaborative Server



Location: Configuration > Collaborative Servers >

Collaborative Servers

#	Server Fully Qualified Domain	Alias Name	Domain Type	Absolute Domain Name (Service Domain / L1 Domain [/ L0 Domain])
1	207.179.153.101	CollabServer1	L1 Domain	myServiceProvider.com / myCompany.com

End of Procedure

Procedure 47
Viewing the Collaborative Servers

1 Select the **Configuration** tab.

A dialog box displays indicating the status of the active and standby database (see Figure 164 on page 412). Click **OK**.

2 Ensure the **Active DB view** is selected.

3 Click **Collaborative Server** in the navigator.

The **Collaborative Server** web page opens and displays a list of any configured Collaborative Servers in different network zones.

End of Procedure

Verifying the numbering plan and saving the NRS configuration

Once the numbering plan is configured in the NRS, you should verify your numbering plan.

Procedure 48
Verifying the numbering plan

1 Perform a database cutover. Cutting over places the database on the real network. See "Cutting over the database" on page 455.

2 Perform the routing tests.

- See "Performing an H.323 Routing Test" on page 448.
- See "Performing a SIP Routing Test" on page 449.

3 If the routing tests succeed, perform a database commit. See "Committing the database" on page 459.

4 If there are problems with the real network testing when using the database cutover command, then use the database revert command to undo the cutover.

If you want to undo the latest provisioning changes, then use a database rollback command to resynchronize the Standby database with the previous Active database.

End of Procedure

Tools tab

H.323 and SIP Routing Tests

To check a numbering plan entry to see if it exists in the active or standby database:

- Use Procedure 49 to perform an H.323 Routing Test.
- Use Procedure 50 on page 449 to perform a SIP Routing Test.

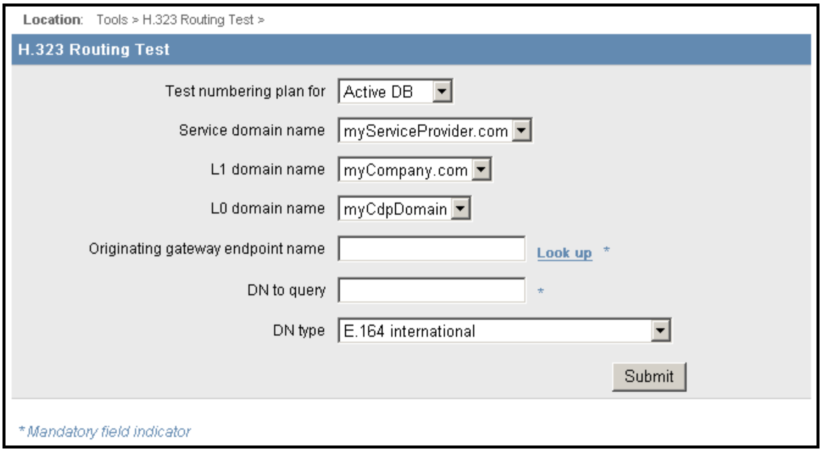
Procedure 49
Performing an H.323 Routing Test

1 Select the **Tools** tab.

2 Click **H.323 Routing Test** in the navigator.

The **H.323 Routing Test** web page opens, as shown in Figure 202.

Figure 202
H.323 Routing Test



Location: Tools > H.323 Routing Test >

H.323 Routing Test

Test numbering plan for: Active DB

Service domain name: myServiceProvider.com

L1 domain name: myCompany.com

L0 domain name: myCdpDomain

Originating gateway endpoint name: Look up *

DN to query: *

DN type: E.164 international

Submit

*Mandatory field indicator

3 Select **Active DB** or **Standby DB** from the **Test numbering plan for** drop-down list.

4 Select the **Service domain name** from the drop-down list.

5 Select the **L1 domain name** from the drop-down list.

6 Select the **L0 domain name** from the drop-down list.

7 Enter the **Originating gateway endpoint name** using the **Lookup** link.

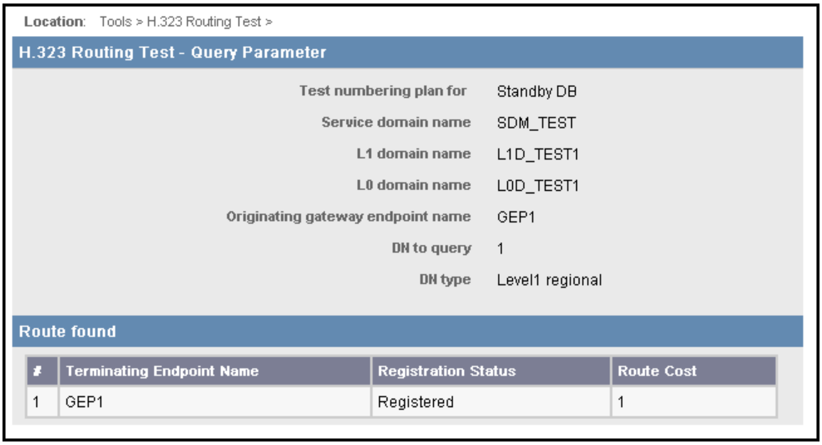
8 Enter a numbering plan entry you want to check in the **DN to query** text box.

9 Select a number type from the **DN type** drop-down list.

10 Click **Submit**.

The results of the H.323 Routing Test are displayed, as shown in Figure 203.

Figure 203
H.323 Routing Test — results



Location: Tools > H.323 Routing Test >

H.323 Routing Test - Query Parameter

Test numbering plan for	Standby DB
Service domain name	SDM_TEST
L1 domain name	L1D_TEST1
L0 domain name	L0D_TEST1
Originating gateway endpoint name	GEP1
DN to query	1
DN type	Level1 regional

Route found

#	Terminating Endpoint Name	Registration Status	Route Cost
1	GEP1	Registered	1

End of Procedure

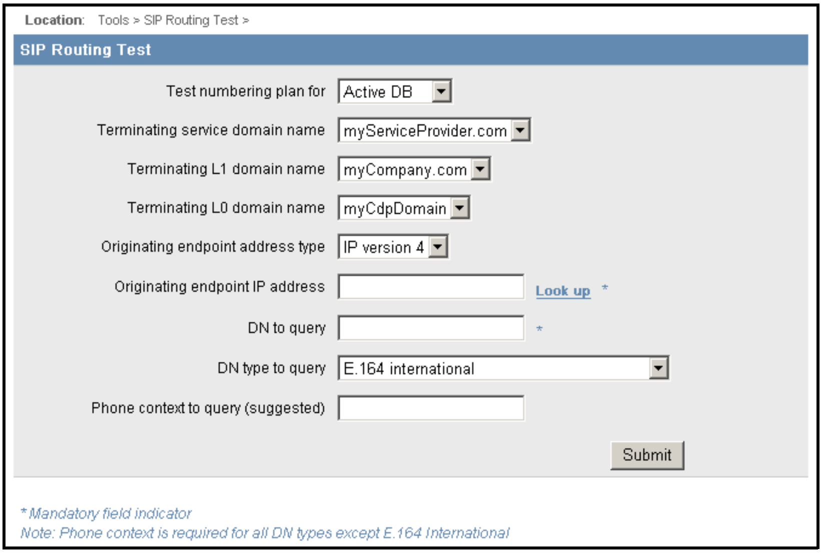
Procedure 50
Performing a SIP Routing Test

1 Select the **Tools** tab.

2 Click **SIP Routing Test** in the navigator.

The **SIP Routing Test** web page opens, as shown in Figure 204 on page 450.

Figure 204
SIP Routing Test



Location: Tools > SIP Routing Test >

SIP Routing Test

Test numbering plan for: Active DB

Terminating service domain name: myServiceProvider.com

Terminating L1 domain name: myCompany.com

Terminating L0 domain name: myCdpDomain

Originating endpoint address type: IP version 4

Originating endpoint IP address: Look up *

DN to query: *

DN type to query: E.164 international

Phone context to query (suggested):

** Mandatory field indicator*
Note: Phone context is required for all DN types except E.164 International

3 Select **Active DB** or **Standby DB** from the **Test numbering plan for** drop-down list.

4 Select the Service Domain from the **Terminating service domain name** drop-down list.

5 Select the L1 Domain name from the **Terminating L1 domain name** drop-down list.

6 Select the L0 Domain name from the **Terminating L0 domain name** drop-down list.

7 Ensure IP version 4 is selected from the **Originating endpoint address type** drop-down list.

8 Enter the **Originating endpoint IP address** using the **Lookup** link.

9 Enter a numbering plan entry you want to check in the **DN to query** text box.

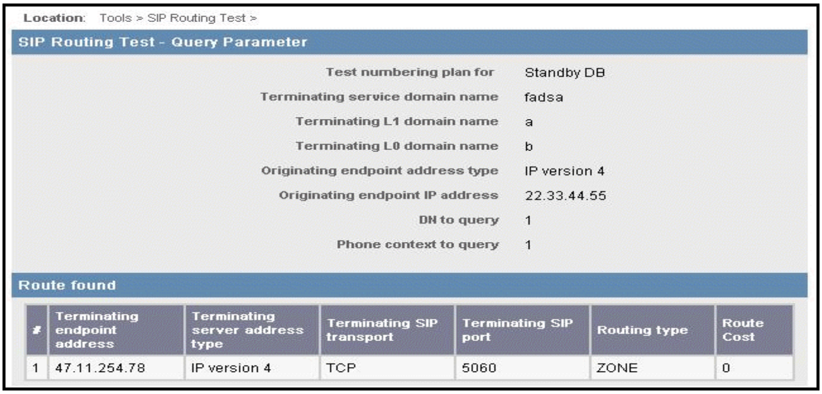
10 Select the DN type you want to check from the **DN type to query** drop-down list.

11 Enter the **Phone context to query**.

12 Click **Submit**.

The results of the SIP Routing Test are displayed (see Figure 205 on page 451).

Figure 205
SIP Routing Test — results



Location: Tools > SIP Routing Test >

SIP Routing Test - Query Parameter

Test numbering plan for	Standby DB
Terminating service domain name	fadsa
Terminating L1 domain name	a
Terminating L0 domain name	b
Originating endpoint address type	IP version 4
Originating endpoint IP address	22.33.44.55
DN to query	1
Phone context to query	1

Route found

#	Terminating endpoint address	Terminating server address type	Terminating SIP transport	Terminating SIP port	Routing type	Route Cost
1	47.11.254.78	IP version 4	TCP	5060	ZONE	0

End of Procedure

Enabling and disabling the NRS Server

The following server actions can be performed using NRS Manager or the Command Line Interface (CLI):

- Forcefully disable the NRS server (nrsForceDisableServer)
- Gracefully disable the NRS server (nrsDisableServer)
  This command should not interrupt the existing calls.
- Enable the NRS server (nrsEnableServer)

The NRS can be taken out-of-service to perform maintenance or to place an Alternate NRS into service.

> ***Note:*** Only users with administrator access level can execute the NRS server action commands.

To take the NRS out-of-service (disabling the NRS server), follow the steps in Procedure 51. To bring the NRS back in to service, follow the steps in Procedure 52 on page 453.

Procedure 51
Disabling the NRS server

1 Select the **Tools** tab.

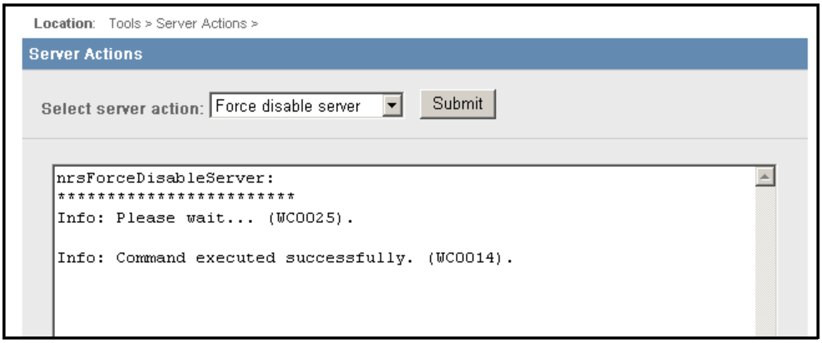
2 Click **Server Actions** from the navigator.

3 Select **Graceful disable server** or **Forceful disable server** from the **Select server action** drop-down list.

4 Click **Submit**.

The nrsDisableServer or nrsForceDisableServer command is issued. The results are shown in the text area, as shown in Figure 206.

Figure 206
Disabling the server



Select server action: Force disable server

```
nrsForceDisableServer:
************************
Info: Please wait... (WC0025).

Info: Command executed successfully. (WC0014).
```

End of Procedure

Procedure 52
Enabling the NRS server

1 Select the **Tools** tab.

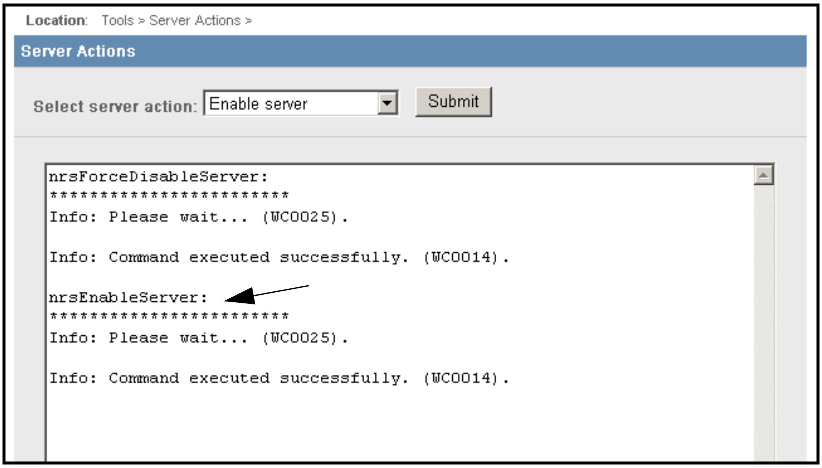
2 Click **Server Actions** from the navigator.

3 Select **Enable server** from the **Select server action** drop-down list.

4 Click **Submit**.

The nrsEnableServer command is issued. The results are shown in the text area, as shown in Figure 207.

Figure 207
Enabling the server



Select server action: Enable server

```
nrsForceDisableServer:
************************
Info: Please wait... (WC0025).

Info: Command executed successfully. (WC0014).

nrsEnableServer:
************************
Info: Please wait... (WC0025).

Info: Command executed successfully. (WC0014).
```

End of Procedure

Performing NRS database actions

The following database action commands can be performed using NRS Manager:

- Cut over — Switches the active and standby database access pointer. This swaps the primary and standby databases, so configuration changes take effect.
- Commit — Mirrors data from active schema to standby schema. Synchronizes the primary and standby databases. Overwrites the previous configuration data with the new configuration.
- Revert — After Cut over, this command switches the active and standby access pointer back.
- Roll back — Undoes/rolls back changes to the database. Swaps the primary and standby databases to revert to the previous configuration. This operation is available after you perform a Cut over and before you perform a Commit.
- Cut over and Commit — Swaps the primary and standby databases and synchronize both the databases with the new configuration in a single step. You cannot Roll back to a previous configuration.

  Note: Only users with administrator access level can execute the database action commands.

For more information, refer to "Database synchronization/operation component" on page 219.

The status of the database is displayed in the title of the **DB Actions** web page. The title indicates the current database status. Depending on the database status, some database actions may be not in the **Select database action** drop-down list.

For example:

- If the database is in Switched Over mode, the available commands in the **Select database action** drop-down list are Revert, Roll back, and Commit.

- If the database is in Changed mode, the available commands in the **Select database action** drop-down list are Cut over, Roll back, and Cut over & Commit.
- If the database is in Committed mode, no commands are available.

For information about these database action commands, refer to "Database synchronization/operation component" on page 219.

To perform the following database actions:

- database cut over, see Procedure 53
- database revert, see Procedure 54 on page 456
- database commit, see Procedure 56 on page 459
- database cut over and commit, see Procedure 57 on page 460
- database roll back, see Procedure 55 on page 458

Performing a database cutover

Cutting over a database switches the active and standby database access pointer. This swaps the primary and standby databases, so configuration changes take effect.

To perform a database cut over, follow the steps in Procedure 53.

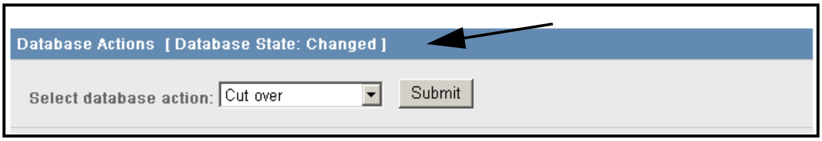
Procedure 53
Cutting over the database

1 Click the **Tools** tab.

2 Select **Database Actions** from the navigator.

The status of the database is displayed, as shown in Figure 208.

Figure 208
Database State: Changed



Database Actions [Database State: Changed]

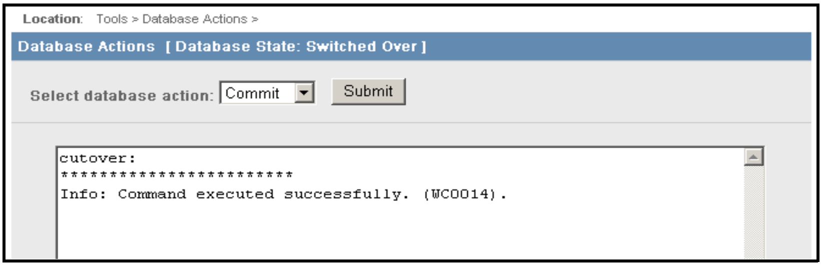
Select database action: Cut over

3 Select **Cut over** from the **Select database action** drop-down list.

4 Click **Submit**.

Text appears in the text area indicating that the Cut over command executed successfully (see Figure 209).

Figure 209
Database Actions – Cut over


Location: Tools > Database Actions >
Database Actions [Database State: Switched Over]
Select database action: Commit
Submit

```
cutover:
************************
Info: Command executed successfully. (WC0014).
```

5 To save the changes after the cut over, perform a Commit (see Procedure 56 on page 459). If you do not want to save the changes to the database, perform a Revert (see Procedure 54 on page 456) or Roll back (see Procedure 55 on page 458).

End of Procedure

Reverting the database changes

After a database cut over, the Revert command switches the active and standby database access pointer back.

To revert the changes to the database, follow the steps in Procedure 54 on page 456.

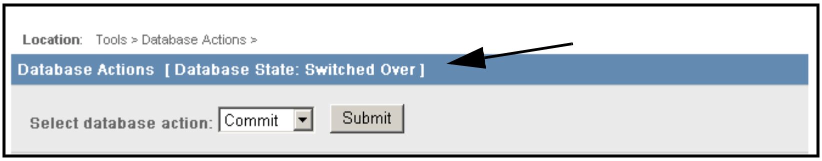
Procedure 54
Reverting the database changes

1 Click the **Tools** tab.

2 Select **Database Actions** from the navigator.

The database is in Switched Over mode, as shown in Figure 210 on page 457.

Figure 210
Database State: Switched Over



Location: Tools > Database Actions >

Database Actions [Database State: Switched Over]

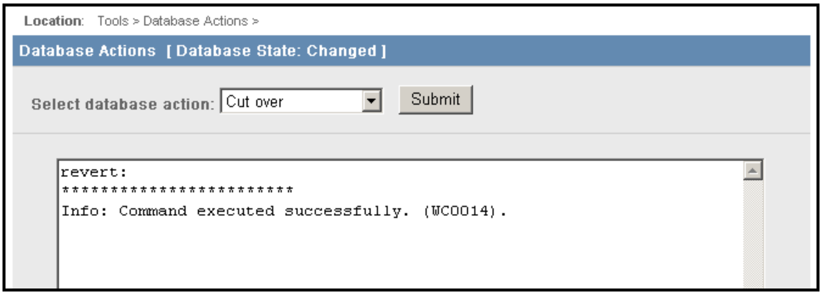
Select database action: Commit

3 Select **Revert** from the **Select database action** drop-down list.

4 Click **Submit**.

Text appears in the text area indicating that the Revert command executed successfully. The database is placed back into a changed state (see Figure 211).

Figure 211
Database Actions – revert



Location: Tools > Database Actions >

Database Actions [Database State: Changed]

Select database action: Cut over

```
revert:
************************
Info: Command executed successfully. (WC0014).
```

End of Procedure

Performing database rollback

The Roll back command copies the previous active database to the standby database. As a result, any changes the user made during the latest provisioning are erased. This operation is available if the database is in Changed or Switched Over modes.

To roll back changes made on the database, perform Procedure 55 on page 458.

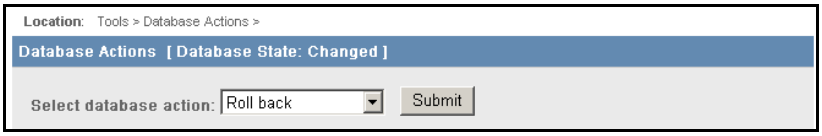
Procedure 55
Rolling back changes to the database

1 Click the **Tools** tab.

2 Select **Database Actions** from the navigator.

3 Select **Roll back** from the **Select database action** drop-down list, as shown in Figure 212.

Figure 212
Database Actions – Roll back



Location: Tools > Database Actions >

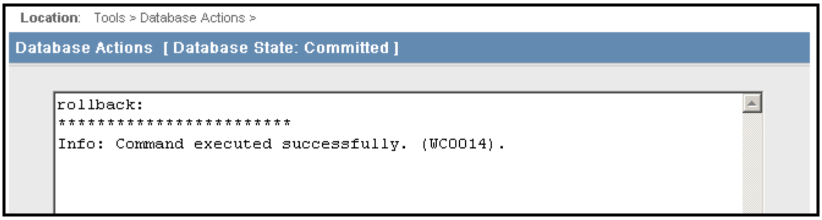
Database Actions [Database State: Changed]

Select database action: Roll back

4 Click **Submit**.

Text appears in the text area indicating that the Roll back command executed successfully (see Figure 213). The **Select database action** drop-down list is also removed from the web page.

Figure 213
Database Actions – Roll back (successful)



Location: Tools > Database Actions >

Database Actions [Database State: Committed]

```
rollback:
************************
Info: Command executed successfully. (WC0014).
```

End of Procedure

Committing the database changes

After Cut over, the Commit command synchronizes the primary and standby databases. The previous configuration data is overwritten with the new configuration data.

To perform a database commit, follow the steps in Procedure 56 on page 459.

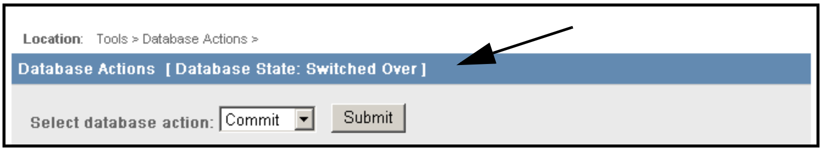
Procedure 56
Committing the database

1 Click the **Tools** tab.

2 Select **Database Actions** from the navigator.

The database is in Switched Over mode, as shown in Figure 214.

Figure 214
Database State: Switched Over



Location: Tools > Database Actions >

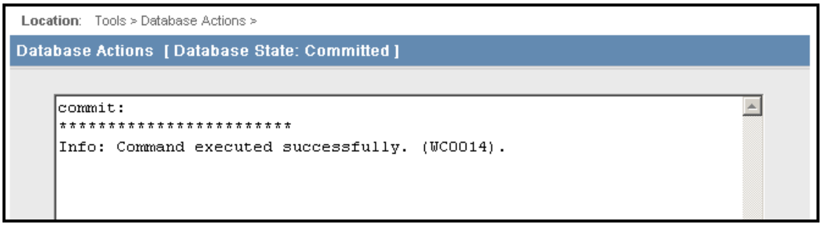
Database Actions [Database State: Switched Over]

3 Select **Commit** from the **Select database action** drop-down list.

4 Click **Submit**.

Text appears in the text area indicating that the Commit command executed successfully. The database is placed back into a committed state (see Figure 215).

Figure 215
Database Actions – Commit



Location: Tools > Database Actions >

Database Actions [Database State: Committed]

```
commit:
************************
Info: Command executed successfully. (WC0014).
```

End of Procedure

Saving changes to the database with a single-step cutover and commit

Once the service domain, L1 domains, L0 domains, gateway endpoints, and routing entries are configured, the changes must be saved to the database. The changes can be saved in a single step using the Cut over & Commit command.

To perform a single-step cut over and commit, follow the steps in Procedure 57.

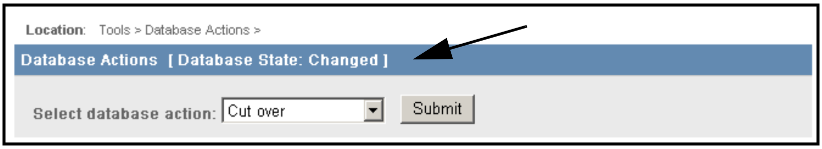
Procedure 57
Cutting over and committing changes to the database

1 Click the **Tools** tab.

2 Select **Database Actions** from the navigator.

The status of the database is displayed as changed, as shown in Figure 216.

Figure 216
Database State: Changed



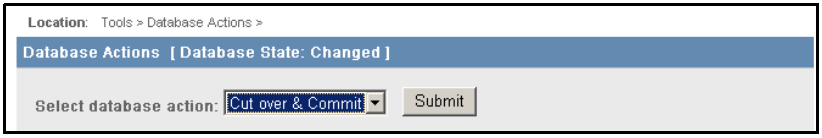
Location: Tools > Database Actions >

Database Actions [Database State: Changed]

Select database action: Cut over

3 Select **Cut over & Commit** from the **Select database action** drop-down list, as shown in Figure 217.

Figure 217
Database Actions – Cut over & Commit



Location: Tools > Database Actions >

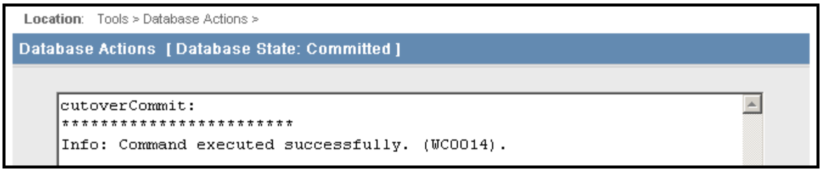
Database Actions [Database State: Changed]

Select database action: Cut over & Commit

4 Click **Submit**.

Text appears in the text area indicating that the Cutover & Commit command executed successfully. The **Select database action** drop-down list is also removed from the web page. See Figure 218.

Figure 218
Database Actions – Cut over & Commit (successful)



Location: Tools > Database Actions >

Database Actions [Database State: Committed]

```
cutoverCommit:
************************
Info: Command executed successfully. (WC0014).
```

End of Procedure

Backing up the database

NRS Manager provides a facility for backing up the NRS database.

The database can be automatically backed up or manually backed up.

- The automatic backup option allows you to configure the backup time and location (using system-wide settings; see Procedure 31 on page 403).
- The manual backup option allows you to immediately back up the database.

Note: Only users with administrator access level can execute the database backup commands.

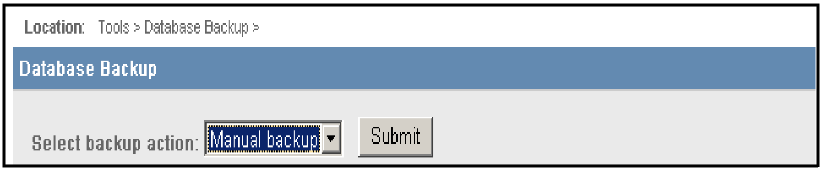
Procedure 58
Automatically backing up the database

1 Click the **Tools** tab.

2 Select **Database Backup** from the navigator.

This **Database Backup** web page opens, as shown in Figure 219 on page 462.

Figure 219
Database Backup web page



Location: Tools > Database Backup >

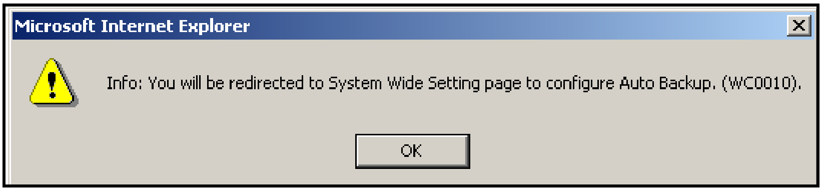
Database Backup

Select backup action: Manual backup

3 Select **Auto backup** from the **Select backup action** drop-down list.

A dialog box opens indicating that you will be redirected to the System Wide Settings web page (see Figure 220).

Figure 220
Automatically back up the database — redirection to System Wide Settings



Microsoft Internet Explorer

Info: You will be redirected to System Wide Setting page to configure Auto Backup. (WC0010).

4 Click **OK**.

The **System Wide Settings** web page opens (see Figure 157 on page 403).

5 Perform the following steps from Procedure 31 on page 403:

- step 7 on page 404
- step 8 on page 404
- step 9 on page 404

End of Procedure

Procedure 59
Manually backing up the database

1 Click the **Tools** tab.

2 Select **Database Backup** from the navigator.

The Database Backup web page opens, as shown in Figure 219 on page 462. **Manual backup** is automatically selected in the **Select backup action** drop-down list.

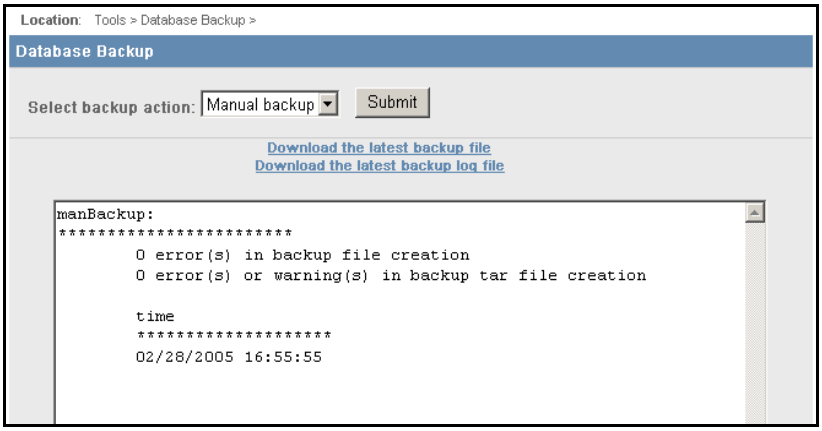
3 Click **Submit**.

A message is displayed in the text area showing backup summary information (see Figure 221).

Two links appear on the screen:

- **Download the latest backup file**
(To download the latest backup file, see Procedure 60 on page 463.)
- **Download the latest backup log file**
(To download the latest backup log file, see Procedure 61 on page 464.)

Figure 221
Manual back up.


Location: Tools > Database Backup >
Database Backup
Select backup action: Manual backup
Submit
Download the latest backup file
Download the latest backup log file

```
manBackup:
************************
        0 error(s) in backup file creation
        0 error(s) or warning(s) in backup tar file creation

        time
        ********************
        02/28/2005 16:55:55
```

End of Procedure

Procedure 60
Downloading the latest backup file

1 Click **Download the latest backup file** (see Figure 221).

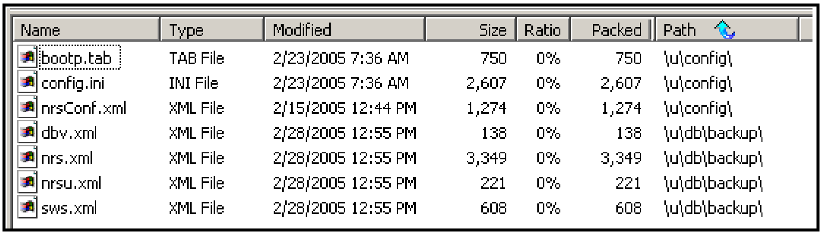
The **File Download** dialog box opens.

The **File Download** dialog box provides the option to view the latest backup file or download and save the latest backup file to the user's local client (PC).

2 Click **Open** to view the latest backup file or click **Save** to save the file to a local client.

The file is a compressed file that contains multiple backup files. The name of the compressed file is nrsback.tar (see Figure 222).

Figure 222
NRS backup files



Name	Type	Modified	Size	Ratio	Packed	Path
bootp.tab	TAB File	2/23/2005 7:36 AM	750	0%	750	\u\config\
config.ini	INI File	2/23/2005 7:36 AM	2,607	0%	2,607	\u\config\
nrsConf.xml	XML File	2/15/2005 12:44 PM	1,274	0%	1,274	\u\config\
dbv.xml	XML File	2/28/2005 12:55 PM	138	0%	138	\u\db\backup\
nrs.xml	XML File	2/28/2005 12:55 PM	3,349	0%	3,349	\u\db\backup\
nrsu.xml	XML File	2/28/2005 12:55 PM	221	0%	221	\u\db\backup\
sws.xml	XML File	2/28/2005 12:55 PM	608	0%	608	\u\db\backup\

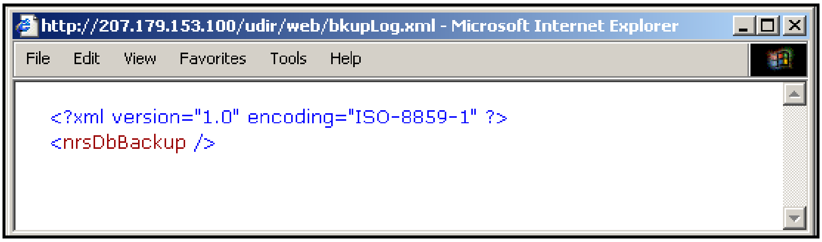
End of Procedure

Procedure 61
Downloading the latest backup log file

1 Click **Download the latest backup log file**.

A window opens containing the latest backup log file. The name of the log file is bkLog.xml (see Figure 223 on page 464). The bkLog.xml file contains information about the backup (for example, if there were errors during the back up process).

Figure 223
Backup log file



http://207.179.153.100/udir/web/bkupLog.xml - Microsoft Internet Explorer
File Edit View Favorites Tools Help

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<nrsDbBackup />
```

2 The backup log file can be saved using the **File > Save As...** menu option.

End of Procedure

Restoring the database

NRS Manager provides the option to select a restore source to complete the database restore action. Restore sources include the following:

- From the connected Signaling Server
- From an FTP site
- From the client machine

Note: Only users with administrator access level can execute the database restore commands.

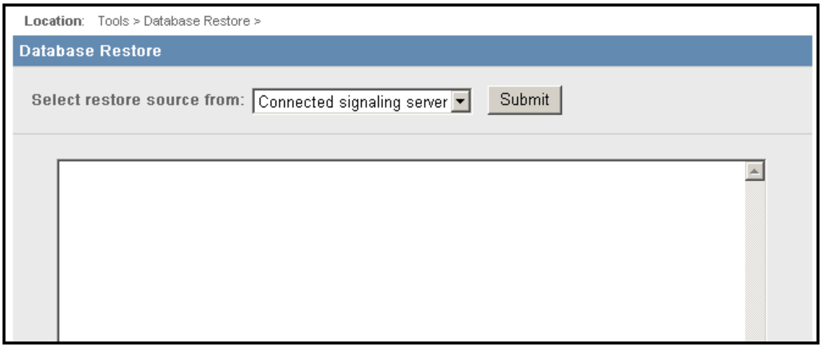
Procedure 62
Restoring the database

1 Click the **Tools** tab.

2 Select **Database Restore** from the navigator.

This **Database Restore** web page opens, as shown in Figure 224 on page 465.

Figure 224
Database Restore web page



Location: Tools > Database Restore >

Database Restore

Select restore source from: Connected signaling server

The database can be restored from three source locations:

- From the **Connected Signaling Server**
  (Use Procedure 63.)
- From an **FTP site**
  (Use Procedure 64 on page 467.)
- From the **Client machine**
  (Use Procedure 65 on page 469.)

End of Procedure

Procedure 63
Restoring from the connected Signaling Server

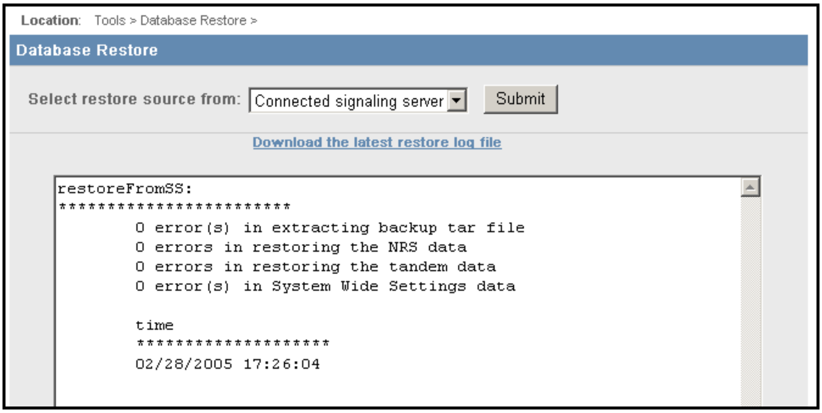
1 Select **Connected Signaling Server** from the **Select restore source from** drop-down list (see Figure 224 on page 465).

2 Click **Submit**.

A message displays in the text area showing the summary of the database restore from the Signaling Server (see Figure 225 on page 467).

The **Download the latest restore log file** link also appears on the web page. See Procedure 66 on page 470 for downloading the restore log file.

Figure 225
Database Restore — from connected Signaling Server


Location: Tools > Database Restore >
Database Restore
Select restore source from: Connected signaling server
Submit
Download the latest restore log file

```
restoreFromSS:
************************
        0 error(s) in extracting backup tar file
        0 errors in restoring the NRS data
        0 errors in restoring the tandem data
        0 error(s) in System Wide Settings data

        time
        ********************
        02/28/2005 17:26:04
```

End of Procedure

Procedure 64
Restoring from an FTP site

1 Select **FTP site** from the **Select restore source from** drop-down list (see Figure 224 on page 465).

The **DB Restore from FTP Site** web page opens (see Figure 226 on page 468).

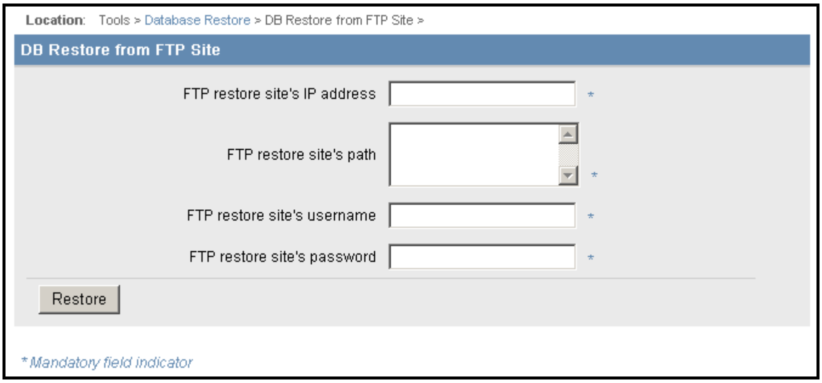
a. Enter the **FTP restore site’s IP address**.

b. Enter the **FTP restore site’s path**.

c. Enter the **FTP restore site’s username**.

d. Enter the **FTP restore site’s password**.

Figure 226
Database Restore — from FTP site



Location: Tools > Database Restore > DB Restore from FTP Site >

DB Restore from FTP Site

FTP restore site's IP address *

FTP restore site's path *

FTP restore site's username *

FTP restore site's password *

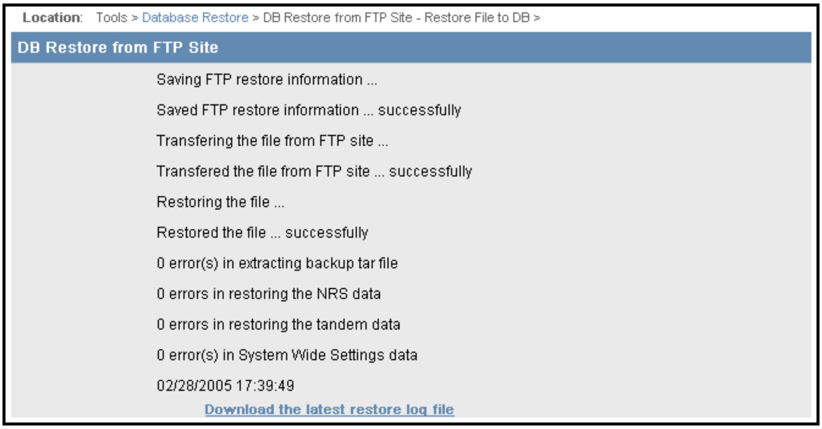
* Mandatory field indicator

2 Click **Restore**.

A message is display in the text area showing summary information about the database restore from the FTP site (see Figure 227).

The **Download the latest restore log file** link also appears on the web page. See Procedure 66 on page 470 for downloading the restore log file.

Figure 227
Database Restore — from FTP site - results



Location: Tools > Database Restore > DB Restore from FTP Site - Restore File to DB >

DB Restore from FTP Site

```
Saving FTP restore information ...
Saved FTP restore information ... successfully
Transfering the file from FTP site ...
Transfered the file from FTP site ... successfully
Restoring the file ...
Restored the file ... successfully
0 error(s) in extracting backup tar file
0 errors in restoring the NRS data
0 errors in restoring the tandem data
0 error(s) in System Wide Settings data
02/28/2005 17:39:49
```

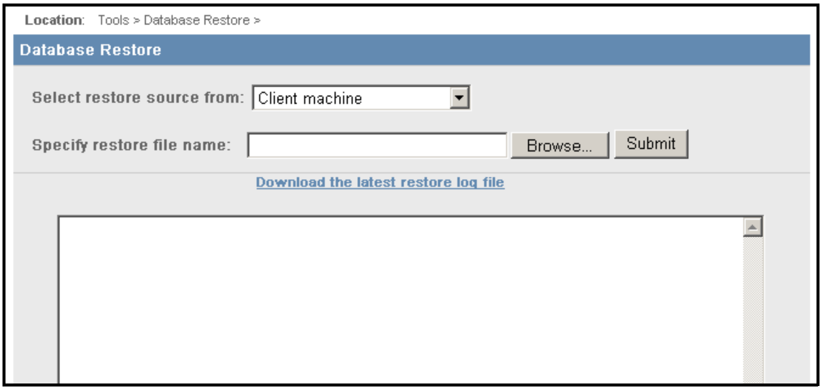
End of Procedure

Procedure 65
Restoring from a client machine

1 Select **Client machine** from the **Select restore source from** drop-down list (see Figure 224 on page 465).

The **Database Restore** web page opens, as shown in Figure 228. The the **Specify restore file name** text box and **Browse** button have been added to the web page.

Figure 228
Database Restore — from client machine


Location: Tools > Database Restore >

Database Restore

Select restore source from: Client machine

Specify restore file name:

2 Click **Browse** to navigate to the folder containing the backup file.

The **Choose file** dialog window opens.

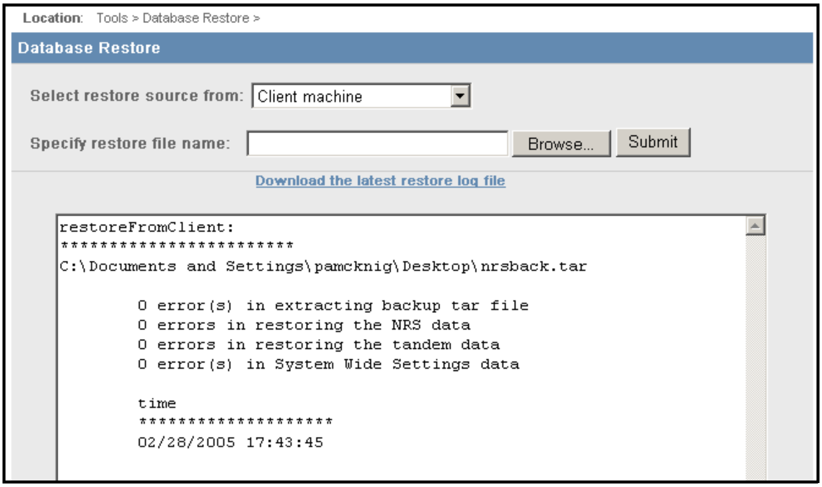
3 Select the backup file, and click **OK**.

The path and filename for the backup file is entered in the **Specify restore file name** text box.

4 Click **Submit**.

A message is displayed in the text area showing summary information about the database restore from the client machine (see Figure 229 on page 470).

Figure 229
Database Restore — client machine — results


Location: Tools > Database Restore >
Database Restore
Select restore source from:
Client machine
Specify restore file name:
Browse...
Submit
Download the latest restore log file

```
restoreFromClient:
************************
C:\Documents and Settings\pamcknig\Desktop\nrsback.tar

        0 error(s) in extracting backup tar file
        0 errors in restoring the NRS data
        0 errors in restoring the tandem data
        0 error(s) in System Wide Settings data

        time
        ********************
        02/28/2005 17:43:45
```

The **Download the latest restore log file** link also appears on the web page. See Procedure 66 for downloading the restore log file.

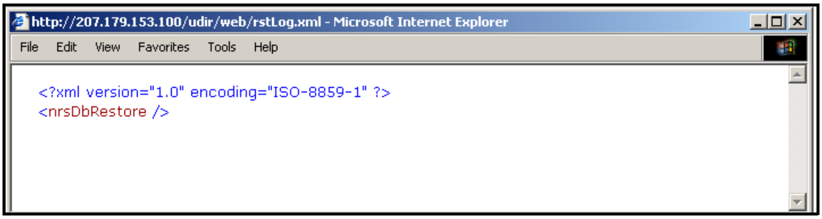
End of Procedure

Procedure 66
Downloading the latest restore log file

1 Click the **Download the latest restore log file** link to view the Restore log file.

A window opens containing the latest restore log file. The name of the log file is rstLog.xml (see Figure 230 on page 471). The rstLog.xml file contains information about the database restore.

Figure 230
Restore log file


http://207.179.153.100/udir/web/rstLog.xml - Microsoft Internet Explorer
File Edit View Favorites Tools Help

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<nrsDbRestore />
```

2 The restore log file can be saved, using the **File > Save As...** menu option.

End of Procedure

GK/NRS Data Upgrade

The **GK/NRS Data Upgrade** link on the Tools web page is used to upgrade a Succession 3.0 H.323 Gatekeeper to a CS 1000 Release 4.0 (or later) NRS. If required, this procedure must be completed as part of your upgrade procedures.

For detailed procedures, refer to *Signaling Server: Installation and Configuration* (553-3001-212).

Migration overview

To migrate your system, you must convert the Succession 3.0 H.323 Gatekeeper database into a CS 1000 Release 4.0 (or later) NRS database. This involves the following tasks:

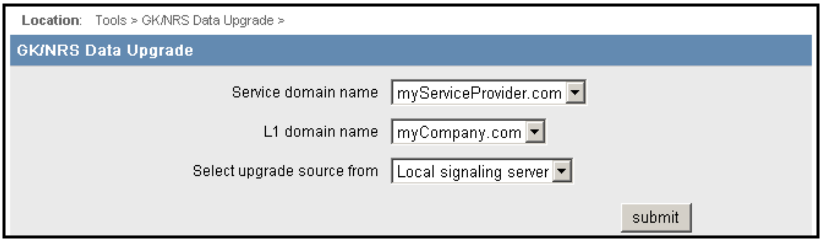
- backing up the Succession 3.0 H.323 Gatekeeper database using Element Manager
- verifying that the backup files (.tar file) exist
- upgrading the Signaling Server software from Succession 3.0 to CS 1000 Release 4.0 (or later)
- reconfiguring the Signaling Server
- creating a Service Domain and Level 1 domain using NRS Manager (These two domains do not exist in the Succession 3.0 Gatekeeper.)

- converting the H.323 Gatekeeper database to the CS 1000 Release 4.0 (or later) NRS database using NRS Manager
- performing a database cutover and commit
  (The data is only converted to standby database in NRS. The database must be cutover and committed before the data be properly used by NRS.)

  Note: Only users with administrator access level can execute Gatekeeper/NRS (GK/NRS) data conversion.

Figure 231 below and Figure 232 on page 473 are only for illustration purposes, to show the user interface for the Gatekeeper to NRS Upgrade area in NRS Manager.

Figure 231
GK/NRS Data Upgrade web page



Location: Tools > GK/NRS Data Upgrade >

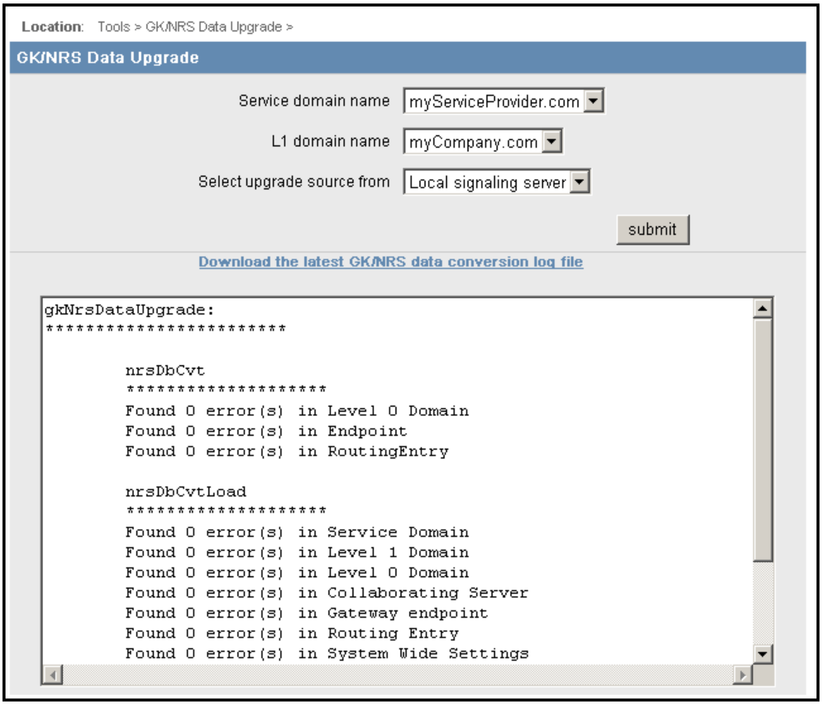
GK/NRS Data Upgrade

Service domain name: myServiceProvider.com

L1 domain name: myCompany.com

Select upgrade source from: Local signaling server

Figure 232
GK/NRS Data Upgrade — results



Location: Tools > GK/NRS Data Upgrade >

GK/NRS Data Upgrade

Service domain name: myServiceProvider.com

L1 domain name: myCompany.com

Select upgrade source from: Local signaling server

Download the latest GK/NRS data conversion log file

```
gkNrsDataUpgrade:
************************


        nrsDbCvt
        ********************
        Found 0 error(s) in Level 0 Domain
        Found 0 error(s) in Endpoint
        Found 0 error(s) in RoutingEntry

        nrsDbCvtLoad
        ********************
        Found 0 error(s) in Service Domain
        Found 0 error(s) in Level 1 Domain
        Found 0 error(s) in Level 0 Domain
        Found 0 error(s) in Collaborating Server
        Found 0 error(s) in Gateway endpoint
        Found 0 error(s) in Routing Entry
        Found 0 error(s) in System Wide Settings
```

SIP Phone Context

The SIP Phone Context provides the ability to view possible SIP phone-context constructions under a configured Level 0 Domain or Gateway Endpoint.

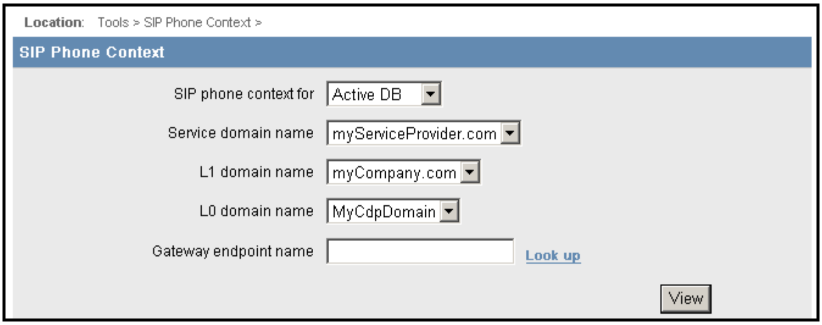
Procedure 67
SIP Phone Context

1 Click the **Tools** tab.

2 Select **SIP Phone Context** from the navigator.

The **SIP Phone Context** web page opens, as shown in Figure 233.

Figure 233
SIP Phone Context web page



Location: Tools > SIP Phone Context >

SIP Phone Context

SIP phone context for: Active DB
Service domain name: myServiceProvider.com
L1 domain name: myCompany.com
L0 domain name: MyCdpDomain
Gateway endpoint name:

3 Select **Standby DB** or **Active DB** from the **SIP phone context for** drop-down list.

4 Select the **Service domain name**.

5 Select the **L1 domain name**.

6 Select the **L0 domain name**.

If the selected **L0 domain name** has configured Gateway Endpoints, the **Look up** link appears beside the **Gateway endpoint name** field. This link is used to navigate to and select a configured Gateway Endpoint. Clicking the **Look up** link opens the Look up path for Gateway Endpoints web page (see step • on page 433).

7 The Gateway endpoint name field is optional, as follows:

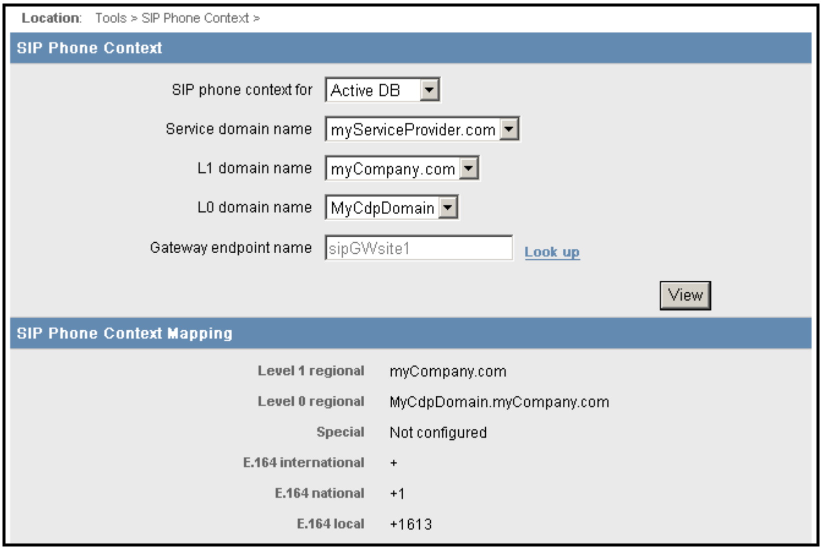
- If you do not select a Gateway Endpoint name and click **View**, then the SIP Phone Context Mapping information is displayed based on L0 domain configuration (which also applies to the User Endpoint configuration).
- If you select a Gateway Endpoint name and click **View**, then the SIP Phone Context Mapping information is displayed based on Gateway Endpoint configuration.

  To select a Gateway Endpoint name, click **Look up** and use the **Look up** facility to select a Gateway Endpoint using a Page-by-Page or Name Prefix search method. Click on the ID of the Gateway Endpoint to select the endpoint name. You cannot enter an endpoint name directly in the **Gateway endpoint name** field.

8 Click **View**.

The **SIP Phone Context Mapping** appears, as shown in Figure 234. In this case, a Gateway Endpoint is selected.

Figure 234
SIP Phone Context Mapping



Location: Tools > SIP Phone Context >

SIP Phone Context

SIP phone context for: Active DB

Service domain name: myServiceProvider.com

L1 domain name: myCompany.com

L0 domain name: MyCdpDomain

Gateway endpoint name: sipGWsite1 Look up

View

SIP Phone Context Mapping

Level 1 regional	myCompany.com
Level 0 regional	MyCdpDomain.myCompany.com
Special	Not configured
E.164 international	+
E.164 national	+1
E.164 local	+1613

End of Procedure

SSL/TLS Configuration

The SSL/TLS Configuration utility in NRS Manager configures the SSL/TLS certificate to enforce system security. Refer to *Element Manager: System Administration* (553-3001-332) for information on this function.

Reports tab

Viewing the database reports

NRS Manager provides three database reports. The report types are:

- Last database synchronization for the Alternate NRS
- Last database synchronization for the Failsafe NRS
- Current database status

Note: Alternate and Failsafe NRS servers must exist for Procedure 68 and Procedure 69 on page 478.

Last database synchronization

Use Procedure 68 to view the last database synchronization.

Procedure 68
Viewing the last database synchronization for the Alternate or Failsafe NRS

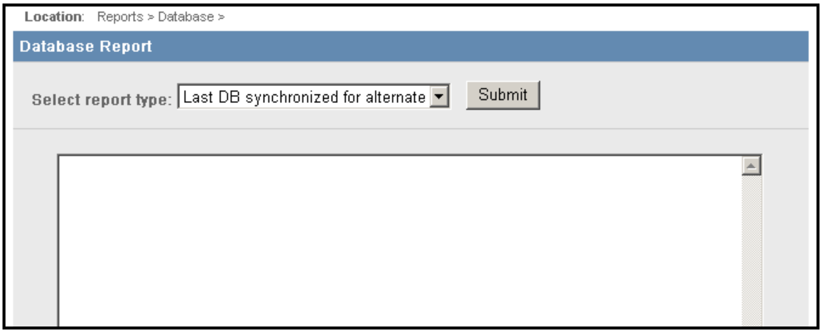
1 Select the **Reports** tab.

2 Click **Database** in the navigator.

The **Database Report** web page opens.

3 Select **Last DB synchronized for alternate** or **Last DB synchronized for failsafe** from the **Select report type** drop-down list. See Figure 235 on page 477.

Figure 235
Last DB synchronized


Location: Reports > Database >

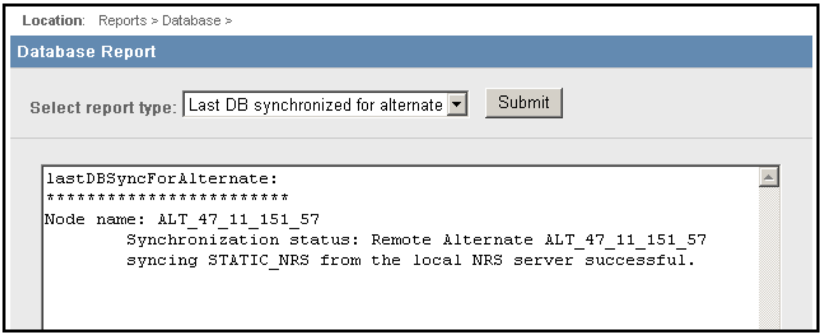
Database Report

Select report type: Last DB synchronized for alternate

4 Click **Submit**.

Figure 236 shows the results of the last database synchronization for the Alternate NRS.

Figure 236
Last DB synchronized for Alternate — results


Location: Reports > Database >

Database Report

Select report type: Last DB synchronized for alternate

```
lastDBSyncForAlternate:
*************************
Node name: ALT_47_11_151_57
        Synchronization status: Remote Alternate ALT_47_11_151_57
        syncing STATIC_NRS from the local NRS server successful.
```

End of Procedure

Current database status

Use Procedure 69 on page 478 to view the current database status.

Procedure 69
Viewing the current database status

1 Select the **Reports** tab.

2 Click **Database** in the navigator.

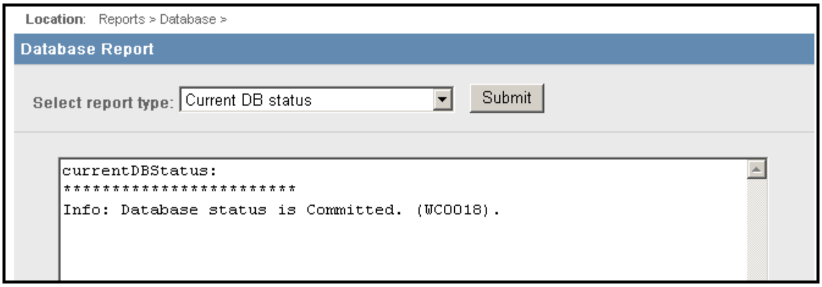
The **Database Report** web page opens.

3 Select **Current DB status** from the **Select report type** drop-down list.

4 Click **Submit**.

The **Database Report** web page opens, as shown in Figure 237 on page 478.

Figure 237
Viewing the current database status



Select report type: Current DB status

```
currentDBStatus:
************************
Info: Database status is Committed. (WC0018).
```

There are three database states:

- Changed — The current standby database has changed. The active and standby databases are not the same.
- Switched Over — The standby database has switched to the active database and the active database has switched to the standby database. The two databases are not the same.
- Committed — The switched standby database (that is, the current active database) has finally been committed as the active database and its contents copied to the current standby database. The two databases are now identical.

End of Procedure

Administration tab

Configuring and administering users

The usernames and passwords used to access NRS Manager can be changed under the Administration tab.

The two user access levels are administrator and monitor.

- administrator level — A user with administrator-level access can view and modify the NRS. An administrator has the power to manage the entire NRS. This is the highest authority level.
- monitor level — A user with monitor-level access can view only existing NRS configuration data.

The administrator has the ability to view, create, and modify the login names and passwords which are used for configuration and maintenance. The NRS Manager blocks certain navigation operations for monitor-access level users. If a user has monitor-level access, then NRS Manager does not allow the user to change NRS provisioning operations.

If the currently logged-in user has administrator-level access, the user:

- can only change their own properties
- cannot delete themselves
- cannot change their user access level

Another administrator account must be used to modify an administrator account.

> ***Note:*** Administrator-level users for an NRS running on a stand-alone Signaling Server can also be configured and managed using the CLI commands given in “Stand-alone NRS CLI commands” on page 598.

Creating new users

Follow the steps in Procedure 70 to create new users.

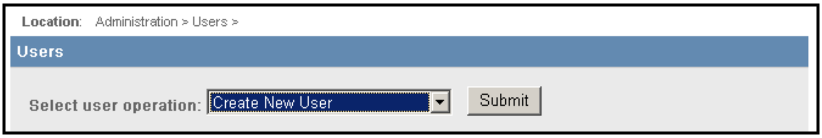
Procedure 70
Creating new users

1 Click the **Administration** tab.

The **Users** web page opens.

2 Select **Create New User** from the **Select user operation** drop-down list (see Figure 238).

Figure 238
Users web page



Location: Administration > Users >

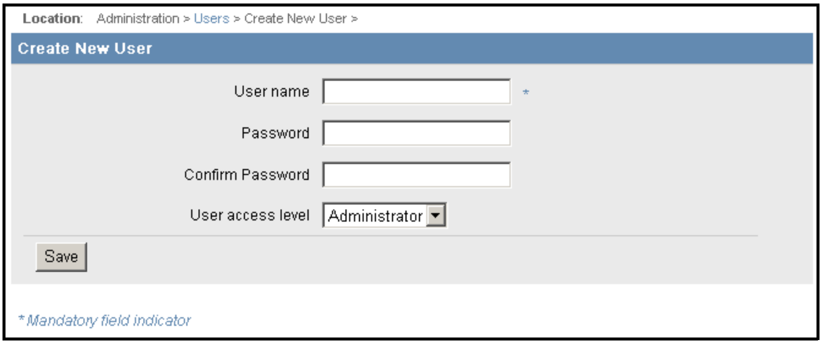
Users

Select user operation: Create New User

3 Click **Submit**.

The **Create New User** web pages opens, as shown in Figure 239.

Figure 239
Create New User web page



Location: Administration > Users > Create New User >

Create New User

User name *

Password

Confirm Password

User access level Administrator

* Mandatory field indicator

4 Enter a **User name**. The username is alphanumeric and can be up to 30 characters in length. The username cannot have spaces and the first character must be a letter.

5 Enter a **Password**. The password is alphanumeric and can be up to 24 characters in length.

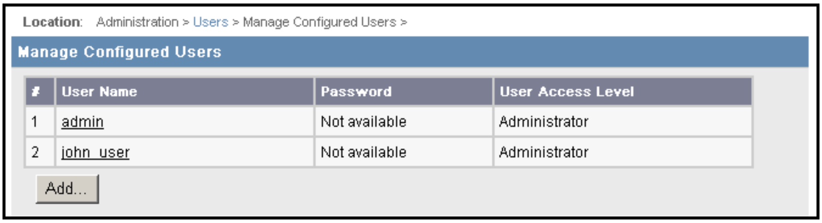
6 Re-enter the password in the **Confirm Password** text box.

7 Select the access level of Administrator or Monitor from the **User access level** drop-down list.

8 Click **Save**.

The **Manage Configured Users** web page opens, as shown in Figure 240 on page 481.

Figure 240
Manage Configured Users web page



Location: Administration > Users > Manage Configured Users >

Manage Configured Users

#	User Name	Password	User Access Level
1	admin	Not available	Administrator
2	john_user	Not available	Administrator

End of Procedure

Viewing configured users

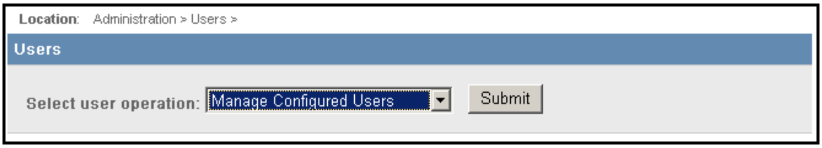
Follow the steps in Procedure 71 to view configured users.

Procedure 71
Viewing configured users

1 Click the **Administration** tab.

2 Select **Manage Configured Users** from the **Select user operation** drop-down list (see Figure 241).

Figure 241
Users web page



Location: Administration > Users >

Users

Select user operation: Manage Configured Users

3 Click **Submit**.

The **Manage Configured Users** web pages opens. A list of configured users is displayed, as shown in Figure 240.

Note: You can create new users from the View Configured Users web pages by clicking **Add...**. Follow the steps in Procedure 70 on page 480 to configure the new user.

End of Procedure

Editing or deleting configured users

Use Procedure 72 to edit a user's username, password, or access level. Procedure 72 can also be used to delete users.

Procedure 72
Editing or deleting configured users

1 Click the **Administration** tab.

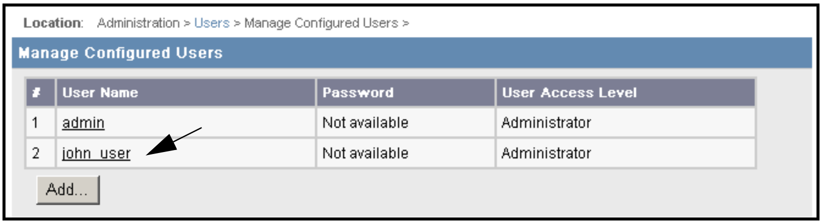
2 Select **Manage Configured Users** from the **Select user operation** drop-down list (see Figure 241 on page 482).

3 Click **Submit**.

The **Manage Configured Users** web page opens, as shown in Figure 242. A list of configured users is displayed.

4 Select the link for the user to be edited or deleted.

Figure 242
Manage Configured Users web page



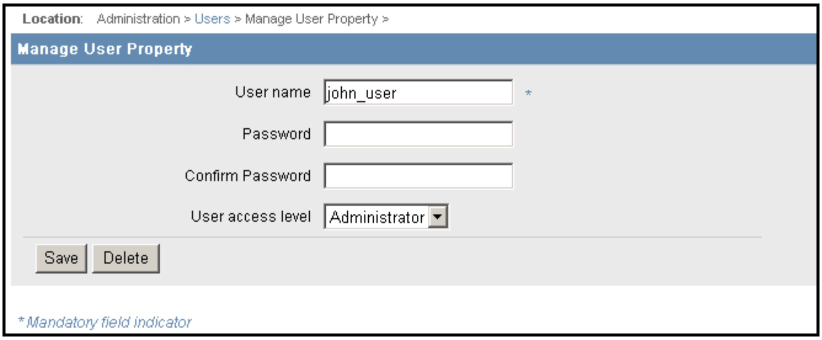
Location: Administration > Users > Manage Configured Users >

Manage Configured Users

#	User Name	Password	User Access Level
1	admin	Not available	Administrator
2	john_user	Not available	Administrator

The **View User Property** web page opens, as shown in Figure 243 on page 483. The web page includes two buttons: **Save** and **Delete**.

Figure 243
Manage User Property web page



Location: Administration > Users > Manage User Property >

Manage User Property

User name john_user *

Password

Confirm Password

User access level Administrator

* Mandatory field indicator

5 Edit the user’s password or access level as required.

Note: The username cannot be changed. If you want to change a user’s username, simply delete the user and then recreate the user with the new username.

6 Click **Save.**

The **Manage Configured User** web page re-opens.

7 To delete a user, click **Delete**.

The **Manage Configured Users** web page re-opens and the user is no longer displayed in list of configured users.

End of Procedure

Changing your password

Use Procedure 73 to change your password.

Procedure 73
Changing your password

1. Click the **Administration** tab.
2. Select **Manage Current User Property** from the **Select user operation** drop-down list.
3. Click **Submit**.

   The **Manage User Property** web page opens, as shown in Figure 242 on page 483.
4. Edit your new password in the **Password** field.
5. Re-enter your new password in the **Confirm Password** field.
6. Click **Save.**

   The **User** web page re-opens.

End of Procedure

Accessing the NRS directly from the Signaling Server

The NRS can be accessed directly from the Signaling Server using a maintenance terminal. Follow the login procedure given in *Signaling Server: Installation and Configuration* (553-3001-212).

Use the following login credentials:

- User ID: **`admin`**
- Password: **`cseadmin`** or `<current>`

  If you use the default password, you are prompted to change your password. If this is not your first login from the Signaling Server, and you have already changed your password, enter your new password (`<current>` above).

  Note: You cannot access NRS Manager from the Signaling Server using this access method.

After you have logged in, you can use the Signaling Server CLI commands listed in “Command Line Interface commands” on page 568. These commands include NRS-specific commands listed in “NRS database CLI commands” on page 596 and “Stand-alone NRS CLI commands” on page 598.

Overlap signaling

Contents

This section contains information on the following topics:

Overview

Overlap signaling over IP is supported using the H.323 protocol.

> ***Note:*** Overlap signaling is not supported using the Session Initiation Protocol (SIP).

Both overlap signaling and en bloc signaling is supported. The difference between overlap and en bloc signaling is as follows:

- In en bloc signaling, the switch waits for all digits of the called-party number from the user and then sends all the digits in a single SETUP message.
- In overlap signaling, the called-party digits are sent out as they are dialed from the user, instead of waiting for an interdigit timer to expire.

  Note: The interdigit timer starts when the user presses a digit key. The timer is restarted when the user presses the next digit key. Expiration of the timer indicates the end-of-dial (EOD).

In the H.323 network, dialed digits can be sent out or received in either en bloc (normal dialing) or overlap modes.

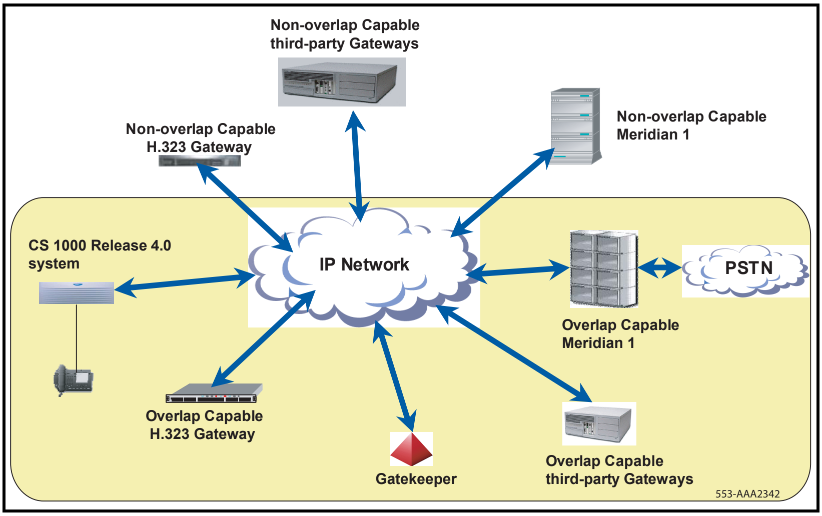
Overlap signaling consists of sending some digits of the called-party number in the first signaling message (SETUP messages) followed by further digits in subsequent signaling messages (INFORMATION messages).

Using the H.323 protocol and IP Peer Networking, overlap signaling is supported over IP between:

- two or more CS 1000 systems running CS 1000 Release 4.0 (or later) on both nodes
- CS 1000 IP Peer systems running CS 1000 Release 4.0 (or later) and another gateway (either a Nortel or third-party gateway) supporting overlap signaling (provided the capability is enabled on the gateway)

Figure 244 on page 489 shows a network diagram with overlap signaling.

Figure 244
Network diagram



Advantages of overlap signaling

Overlap signaling allows the system to initiate a call from the originating node (towards the terminating node) while the originator is still dialing digits. As a result, overlap signaling improves the call setup time. Overlap signaling accelerates the transmittal of dialed digits which allows the terminating node to determine if the complete directory number (DN) is dialed. It also reduces the post-dial delay in networks where variable-length dialing plans are used.

Overlap signaling is useful when a system cannot determine the completion of all the digits, unless the caller terminates dialing with an octothorpe (#). For example, when a caller dials international numbers or when a caller dials private numbers where sub-DN digits may not be fully known across the whole network.

> ***Note:*** If overlap signaling is enabled on the Virtual Trunk D-channel for H.323, and the call is tandemed to DTI/Analog/DTI2, configure the Overlap Length parameter OVLL in the Route List Block for the DTI/Analog/DTI2 as 0.

Overlap signaling is in use in several countries with variable-length dialing plans (for example, Germany, Belgium, and Italy, and some other countries in Europe and Asia).

Overlap signaling also can improve interoperability with third-party gateways.

PSTN-destined calls

Overlap signaling support mainly impacts outgoing calls destined for PSTN terminations. Both line-originating calls and tandem trunk calls require overlap support.

This feature is applicable to PSTN calls with CS 1000 systems, because such calls can tandem through an IP Peer H.323 Gateway.

Feature capabilities

IP Peer Overlap Signaling includes the following capabilities:

- IP Peer overlap signaling support using the H.323 protocol
- Gatekeeper overlap signaling support
- Overlap sending/receiving configuration support
- Overlap signaling to en bloc conversion
- Tandem overlap signaling support

Overlap signaling support using the H.323 protocol

Overlap signaling is supported over IP Peer using version 4-compliant H.323 protocol signaling, as specified by the ITU-T H.323 and companion H.225 and H.245 standards.

IP Peer overlap signaling using H.323 is modeled on and parallels the Primary Rate Interface (PRI) overlap signaling. For more information on overlap signaling, refer to *ISDN Primary Rate Interface: Features* (553-3001-369).

H.323 Gatekeeper overlap signaling support

The H.323 Gatekeeper provides support for overlap signaling.

When a CS 1000 H.323 Gatekeeper receives an ARQ message from the gateway, the message can include enough digits to resolve the address, or it can be incomplete (because overlap signaling has started but not completed). If it is incomplete (that is, the number is an incomplete prefix of one or more entries in the dialing plan), then the Gatekeeper supports overlap signaling by replying to the gateway with an "incomplete address" rejection reason.

The H.323 Gatekeeper also replies when the following occur:

- The number is invalid (that is, there are no possible matches in the dialing plan).
- There are at least two H.323 Gatekeepers in the network (one H.323 Gatekeeper that received the ARQ and could not resolve it, and a second H.323 Gatekeeper to receive the LRQ), and one of the following events occur:
    - — at least one H.323 Gatekeeper failed to respond
    - — the local H.323 Gatekeeper is provisioned with a default IP destination

The local Gatekeeper replies with an Admission Confirm (ACF) message. The ACF message includes the default IP destination and additional information. This additional information tells the gateway that the call handling has two options:

- The gateway can use the provided information and immediately continue with the call.
- The Gateway can carry out overlap to en bloc conversion and retry the ARQ.

For more information, refer to Appendix B: “H.323 Gatekeeper overlap signaling support” on page 613.

Overlap sending and receiving configuration support

Overlap sending and receiving are configurable for H.323 endpoints over IP Peer.

The user has the option to turn overlap sending and receiving on or off for the H.323 signaling gateway. In addition, the user can turn off overlap sending on specific destinations on an IP route (using the same signaling gateway) which is overlap enabled.

> ***Note:*** The IP Peer Overlap Signaling feature provides the ability to terminate overlap calls at an en bloc destination; however, this approach may not be efficient. If the nodes in the network are capable of supporting overlap signaling, then Nortel recommends that all nodes in the network be configured to use overlap signaling for optimal efficiency.

If a network must be configured such that some calls are en bloc and all other calls are overlap, then there are two ways to configure the network to avoid overlap to en bloc conversion. The two methods are:

- Configure separate Route List Index (RLI) instances to create different Route List Blocks (RLB). This is the preferred method.
- Configure separate Signaling Servers for en bloc and overlap traffic.

Separate Route List Index (RLI) instances

Nortel recommends that separate Route List Index (RLI) instances be configured to create different Route List Blocks (RLB) for en bloc and overlap traffic to the same CS 1000 Signaling Server. Using different RLBs for overlap and en bloc calls saves provisioning and hardware resources, because only one D-channel on the Call Server and one Signaling Server are used.

> ***Note:*** RLBs provide an option to configure the Overlap Length (OVLL) for different RLIs. If OVLL is defined as 0, then (for any route on that particular RLI) all the calls made over that route are en bloc.

Separate Signaling Servers

As an alternate approach, separate CS 1000 Signaling Servers can be used for en bloc and overlap traffic.

Two CS 1000 Signaling Servers can be configured, where:

- one Signaling Server carries overlap signaling traffic
- one Signaling Server carries en bloc traffic

This configuration requires two D-channels on the Call Server. One D-channel can be configured as en bloc and the other as overlap.

Overlap to en bloc conversion

Nortel recommends that all nodes in the network that are capable of overlap signaling have overlap receiving enabled as a minimum, and, if possible, have both overlap receiving and overlap sending enabled.

However, a network can have nodes that are not capable of supporting overlap signaling. If an H.323 overlap call encounters such a destination, then the originating node can complete the call by reverting to en bloc mode. This is known as overlap to en bloc conversion.

The following two events can occur when an H.323 SETUP message (for an overlap-capable call) reaches an en bloc destination:

- In response to the SETUP message, an H.323 CALL PROCEEDING message is sent indicating the end-of-dial. This message is followed by a call clear, which indicates an incomplete number may occur.
- The call can clear immediately, indicating an incomplete number.

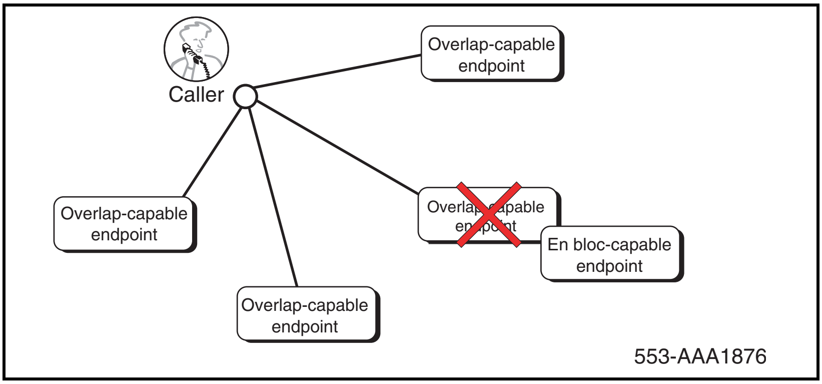
In both cases, overlap to en bloc conversion begins. The interdigit timer starts and digits are collected until an end-of-dial indication. That is, the interdigit timer expires on the Call Server, triggering the end-of-dial indication or the Call Server sends an end-of-dial indication for some other reason; this mechanism exists within the Call Server messages. The reasons can include reaching the provisioned maximum length, user input, or a tandem transmission of the end-of-dial indication. At that time, the gateway sends a new H.323 SETUP message with all received digits, and an end-of-dial indication. All further call processing occurs using en bloc signaling.

Changing the provisioning from using overlap signaling (to reach a destination) to using en bloc signaling

Figure 245 shows a network of overlap-capable endpoints where one of the endpoints must be changed to en bloc-capable.

> ***Note:*** "Overlap-capable endpoint" implies that signaling to this destination uses overlap dialing, while "En bloc-capable endpoint" implies that overlap signaling is not used to reach this destination. The true capabilities of the destinations are not known at the originator.'

Figure 245
Changing an overlap-capable endpoint to an en bloc endpoint



For efficiency, configure another RLI as en bloc in LD 86 to change that endpoint from overlap signaling-capable to en bloc:

1. In LD 86, define a new RLI.
2. Configure the Overlap Length (OVLL) prompt to 0.

   Note: The OVLL prompt determines the number of digits required before the SETUP message is sent. If OVLL = 0, then all the dialed digits are sent in the SETUP message and the call is an en bloc call (even if LD 17 is configured for overlap signaling).

3. Change the entries pointing to the destination (that just changed to en bloc) to use the new RLI. After all ESN and CDP code entries have been changed, you can then remove the overlap RLI.

Example: Assume that Location Code (LOC) 425 currently uses the overlap-capable RLI 21 to call an overlap node. If that node changes to en bloc, then the following changes must be made:

- In LD 86, define a new RLI (such as RLI 22) with OVLL configured to 0. (All other prompts in the RLI can be identical to the original RLI 21.)
- In LD 90, change the LOC 425 to use the new RLI 22.

Tandem overlap signaling support

In addition to supporting originating and terminating overlap calls, IP Peer Overlap Signaling also supports the following tandem scenarios:

- ISDN (en bloc/overlap) to IP Peer (H.323-overlap/en bloc)
- Non-ISDN (en bloc/overlap) to IP Peer (H.323-overlap/en bloc)
- IP Peer (H.323-overlap) to IP Peer (H.323-overlap/en bloc)
- IP Peer (H.323-overlap) to IP Peer (SIP)

Overlap signaling call flow

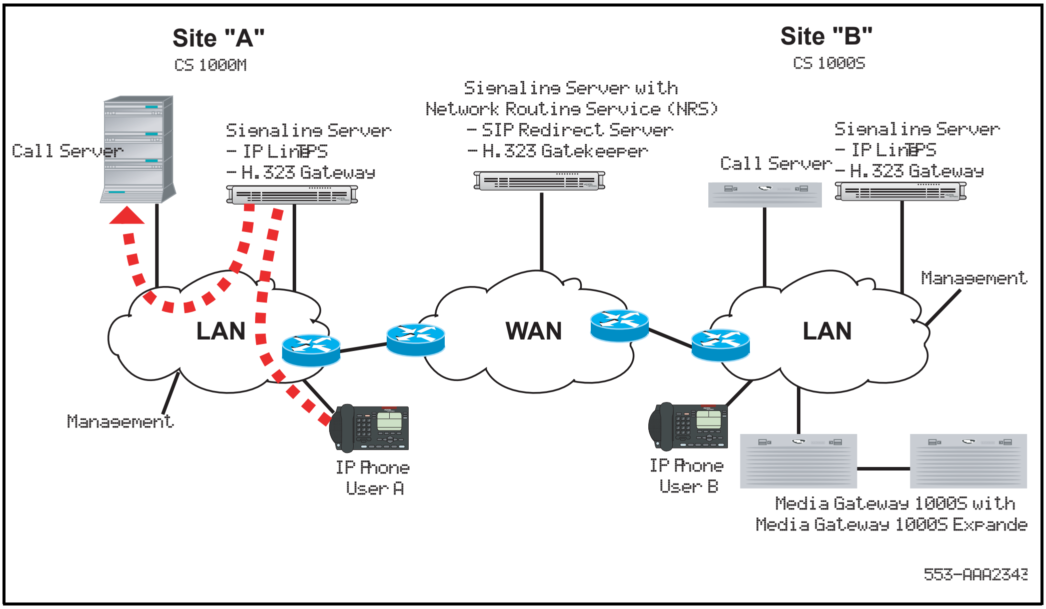
Any messaging after the Alerting message is identical to the en bloc call flow and is not repeated in this section.

> ***Note:*** Only the primary messages are illustrated in the following call flows.

The following scenario describes the Direct IP Media Path functionality for a basic network call using overlap signaling:

1 User A on Call Server A dials the DN of User B on Call Server B. Call Server A collects the routing-prefix digits through the Terminal Proxy Server (TPS) on Signaling Server A. See Figure 246.

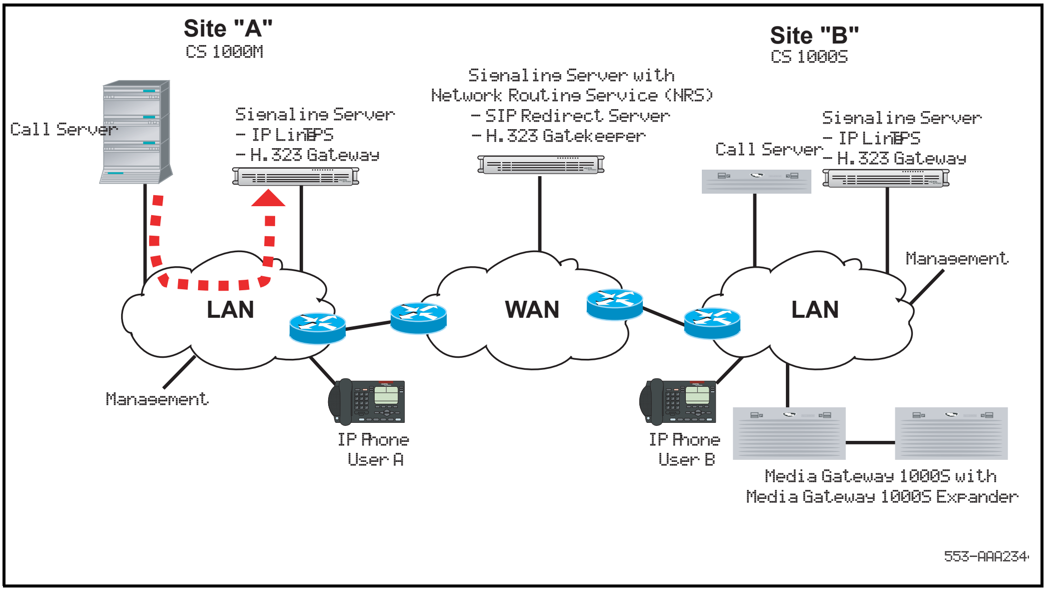
Figure 246
User A dials User B



2 Call Server A determines that the dialed DN is at another site reachable using overlap signaling. Call Server A selects the codec list, allocates bandwidth, and routes the call to the IP network using a Virtual Trunk and an H.323 Gateway. See Figure 247.

Note: To select which Virtual Trunk to use for routing, Call Server A examines the number dialed and uses various trunk routing and signaling features (for example, ESN and MCDN).

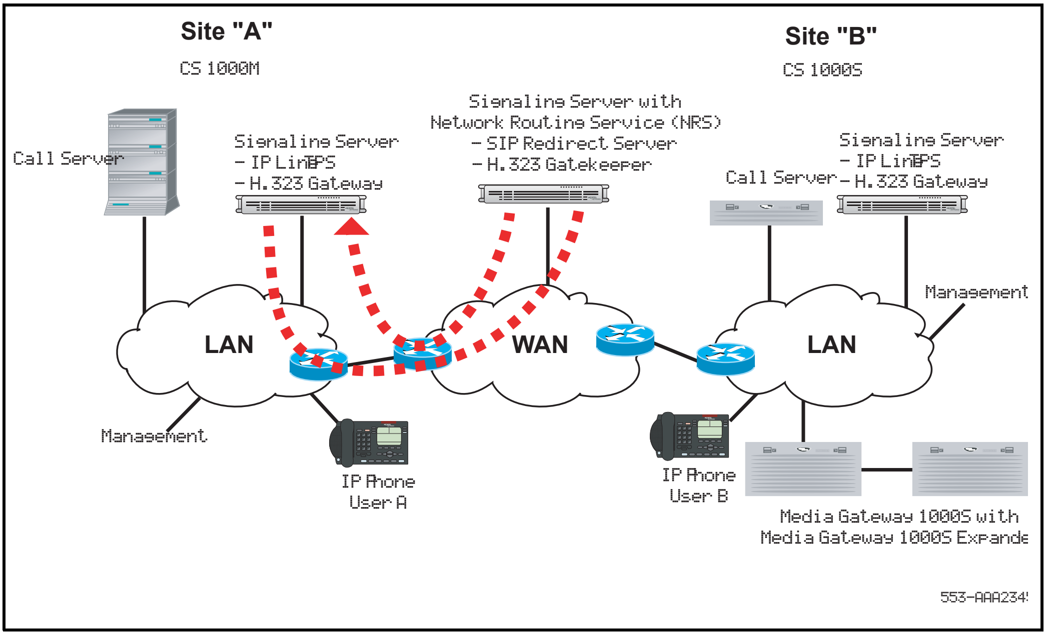
Figure 247
Call Server A routes the call to the IP network



3 H.323 Gateway A asks the NRS (specifically the H.323 Gatekeeper) to search for the dialed DN in the database (for example, within the appropriate CDP domain). If the NRS (H.323 Gatekeeper) can unambiguously resolve the destination digits, it sends the IP address of H.323 Gateway B to H.323 Gateway A. See Figure 248.

Otherwise, the NRS requests more digits.

Figure 248
The H.323 Gatekeeper sends the IP address of H.323 Gateway B to H.323 Gateway A



4 User A dials an additional digit. The TPS forwards it to Call Server A. See Figure 246 on page 496.

5 Call Server A forwards the digits to H.323 Gateway A on the Signaling Server. See Figure 247 on page 497.

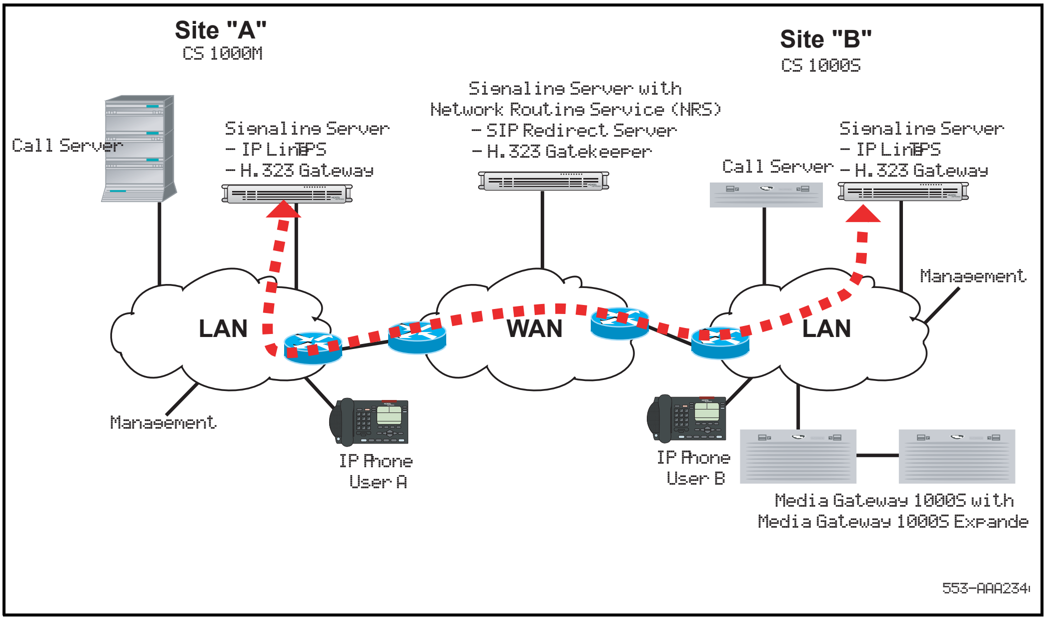
6 H.323 Gateway A asks the NRS (specifically the H.323 Gatekeeper) to search for the dialed DN in the database (for example, within the appropriate CDP domain). If the NRS (H.323 Gatekeeper) can unambiguously resolve the destination digits, it sends the IP address of H.323 Gateway B to H.323 Gateway A. See Figure 248 on page 498.

Otherwise, the NRS requests more digits.

Note: Until the call succeeds, Step 4, Step 5, and Step 6 are repeated for each new dialed digit.

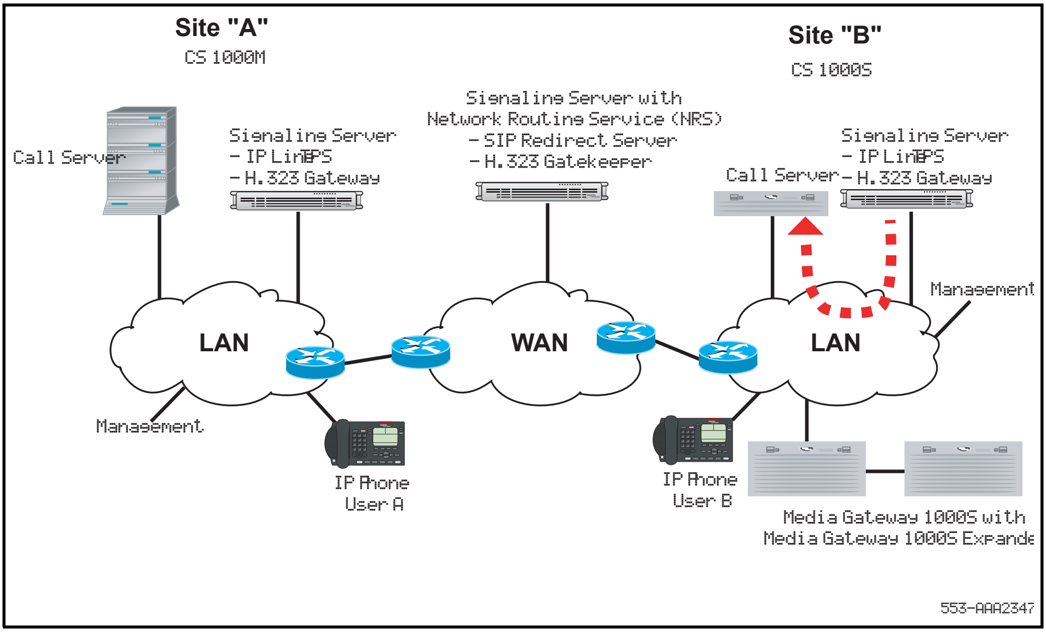
7 H.323 Gateway A sends a SETUP message to H.323 Gateway B, including the DN information and an indication that H.323 Gateway A is overlap capable. H.323 Gateway B replies with a SETUP ACK indicating that it is also overlap capable. See Figure 249.

Figure 249
H.323 Gateway A sends a SETUP message to H.323 Gateway B



8 H.323 Gateway B treats the call as an incoming overlap signaling call from a Virtual Trunk. H.323 Gateway B sends the call to Call Server B over a Virtual Trunk. Call Server B also treats the call as an incoming call from a Virtual Trunk. See Figure 250.

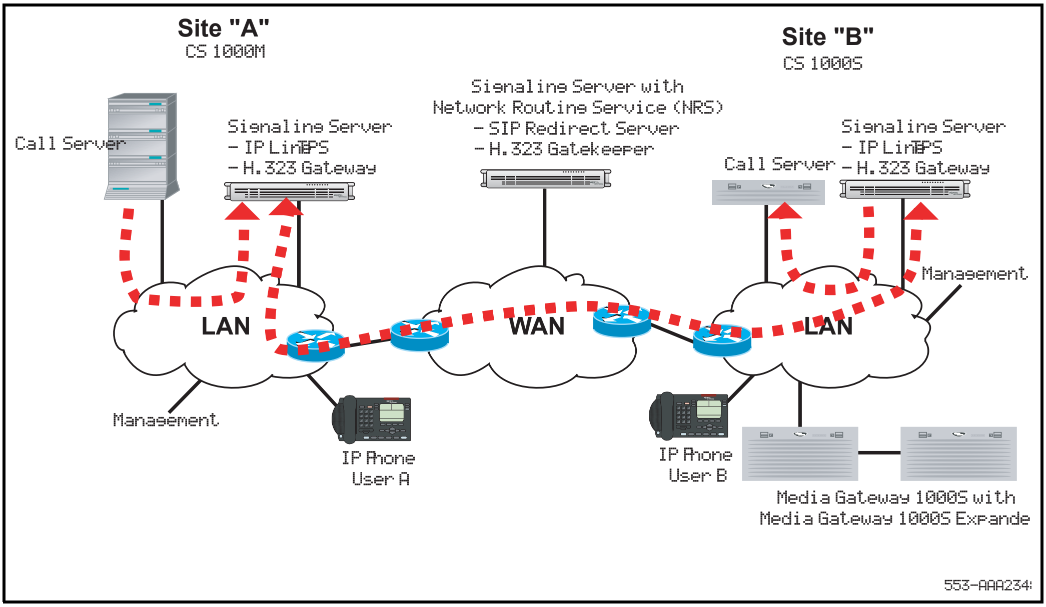
Figure 250
Gateway B sends the call to Call Server B over a Virtual Trunk



9 User A on Call Server A dials additional digits. See Figure 246 on page 496.

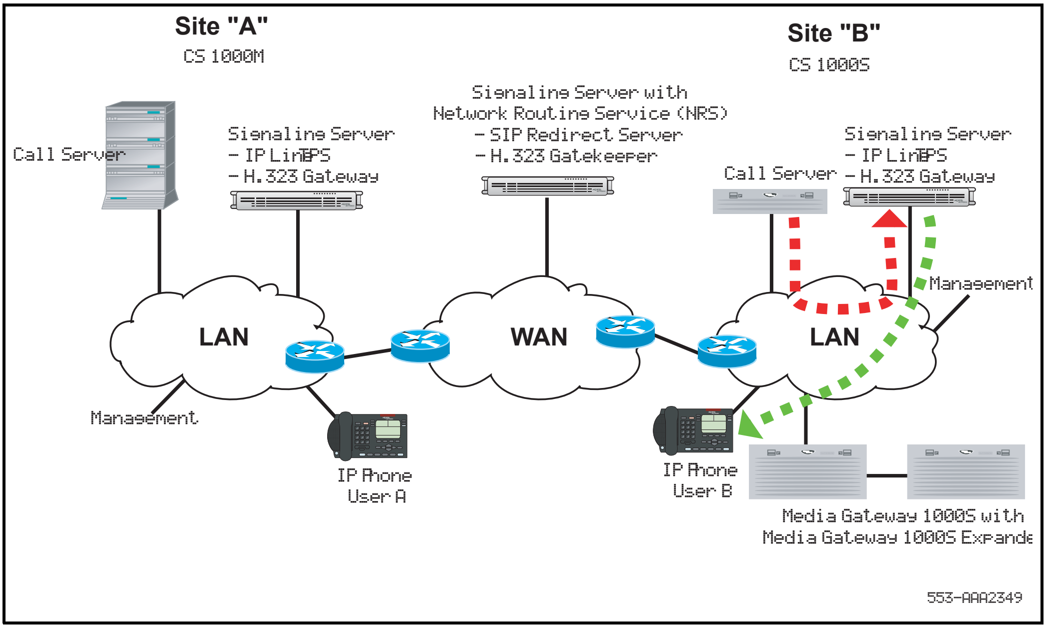
10 Call Server A sends the new digits to Call Server B through the two gateways. This repeats until Call Server B receives all the digits. At that time, Call Server B sends an end-of-dial indication to Call Server A. See Figure 251.

Figure 251
Call Server A sends digits to Call Server B



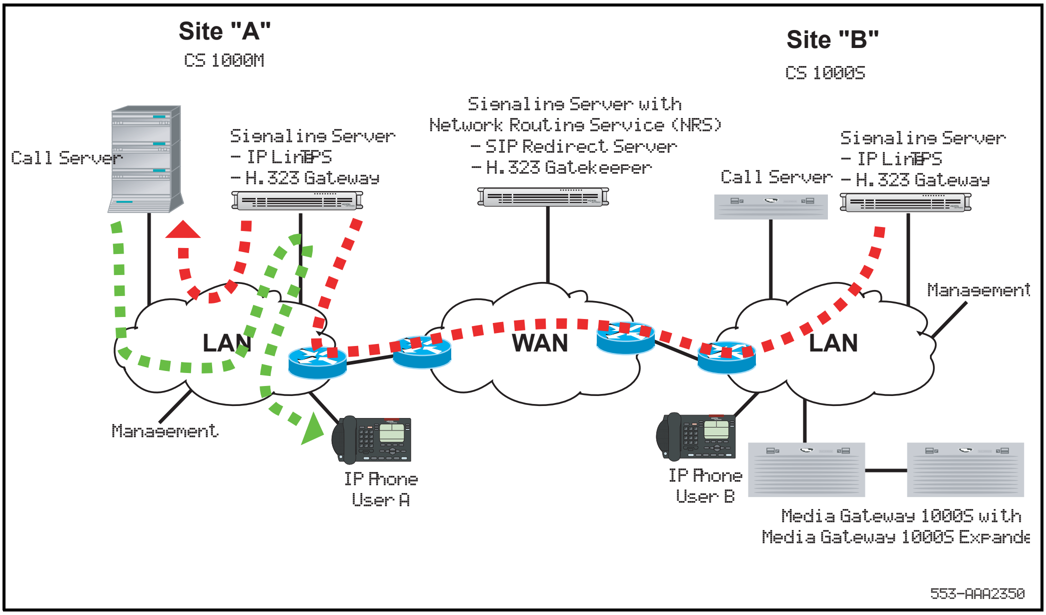
11 Call Server B selects the codec, allocates bandwidth, rings the telephone, and sends an alerting message to H.323 Gateway B. See Figure 252.

Figure 252
Call Server B sends an alerting message to H.323 Gateway B



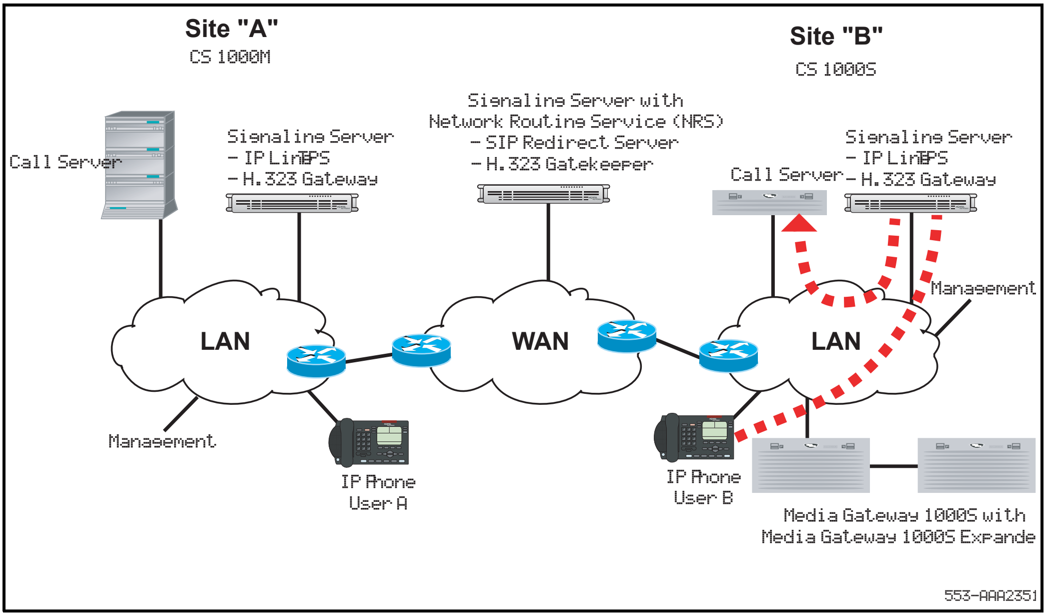
12 H.323 Gateway B sends an alerting message to Call Server A. Call Server A requests that the IP Phone play ringback tone. See Figure 253.

Figure 253
H.323 Gateway B sends an alerting message to Call Server A



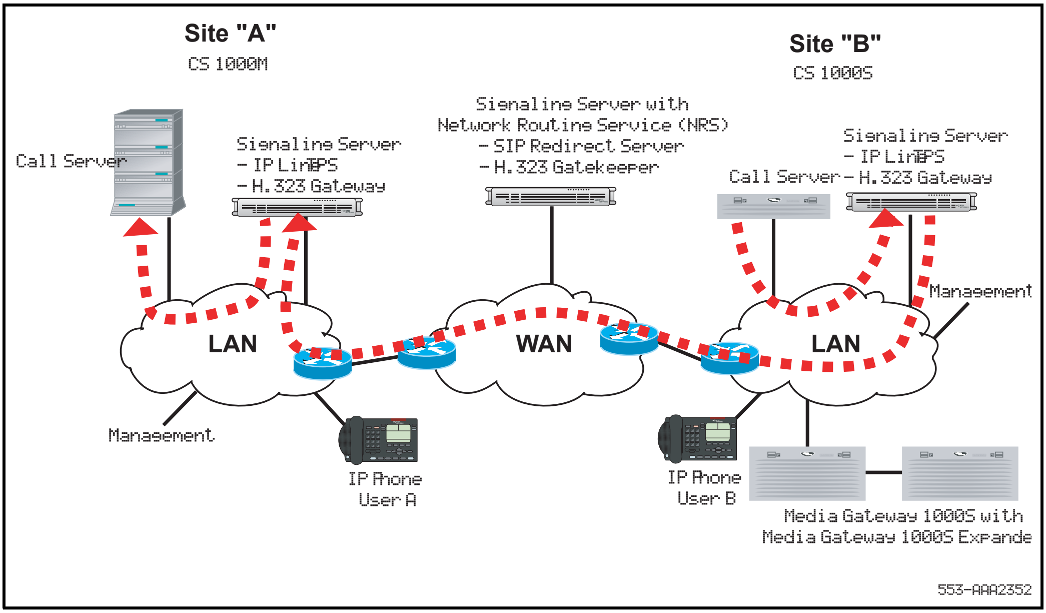
13 User B answers the call. A message is sent to Call Server B through the TPS on the Signaling Server. See Figure 254.

Figure 254
User B answers the call



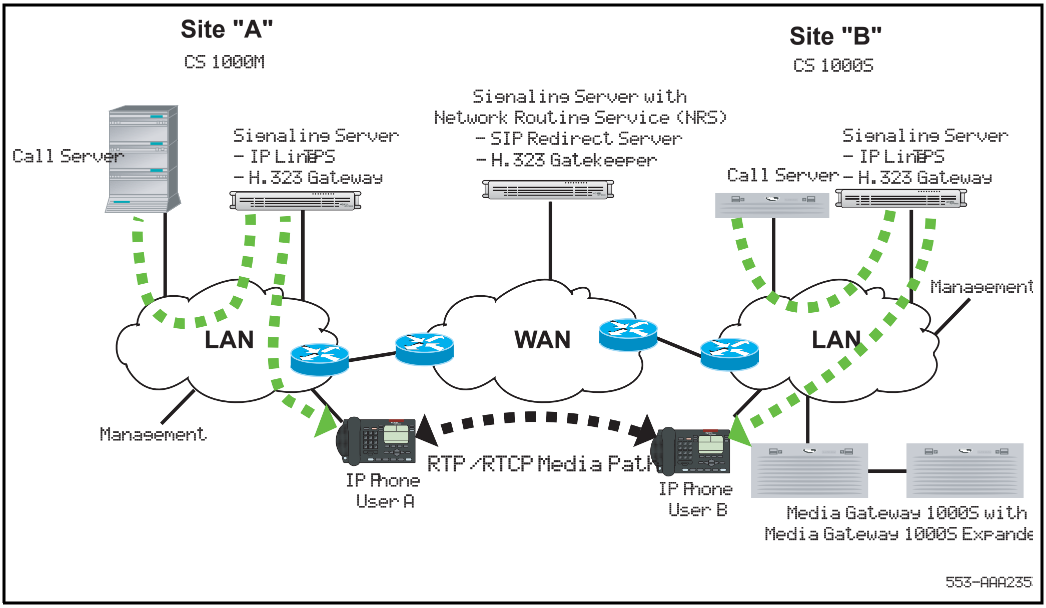
14 Call Server B sends a CONNECT message to H.323 Gateway B. H.323 Gateway B sends an H.323 CONNECT message to H.323 Gateway A. H.323 Gateway A forwards the message to Call Server A. See Figure 255.

Figure 255
Call Server B sends a CONNECT message to Gateway B and onto Call Server A



15 The Call Servers tell the IP Phones to start the direct IP media paths. The IP Phones then begin to transmit and receive voice over the IP network. See Figure 256.

Figure 256
IP Phones start the direct media paths



Feature packaging

IP Peer Overlap Signaling requires the following packages:

- Overlap Signaling (OVLP) package 184
- H.323 Virtual Trunk (H323_VTRK) package 399

Note: The packaging for H.323 includes the Overlap Signaling package.

Configuring overlap signaling on the Call Server

The following task summary list includes all the tasks required to configure IP Peer with overlap signaling. In particular, overlap signaling is configured using LD 17 and LD 86 as follows:

- Use LD 17 to configure the D-channel to support overlap signaling.
- Use LD 86 to configure the number of digits to be included in the SETUP message.

When configuring overlap signaling, the network must be optimized using a combination of the Overlap Length (OVLL) prompt in LD 86 and the Overlap Timer (OVLT) prompt in LD 17. Nortel recommends that:

- OVLL be configured to a reasonable length such that the Gatekeeper can resolve the called-party number with a minimum number of transactions
- OVLT be configured to 1 second

WARNING

When using SPNs to provide local, national, and international number handling, the incoming local, national, and international numbers are treated as en bloc. If the number was sent using overlap signaling, the call will always be incomplete.

If the Call Server receives an unknown type (CDP, LOC, or SPN) on an overlap capable D-channel, the Call Server processes the call as overlap. If it receives E.164 numbers, the Call Server treats them as North American formatted (and therefore, en bloc).

Task summary list

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

1. LD 17 – Configure D-channels to support overlap signaling.
2. LD 16 – Configure the H.323 route.
3. LD 86 – Configure the Route List Block for the Virtual Trunk route and configure the minimum number of digits included in the overlap signaling SETUP message.
4. LD 87 – Configure the CDP steering codes.
5. LD 90 – Configure E.164 plan call types and private plan Location Codes.
6. LD 90 – Configure Special Numbers.

Note: Only the Overlays directly affected by the overlap signaling feature are included here.

LD 17 – Configure D-channels to support overlap signaling. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	ADAN	Action Device And Number
- ADAN	NEW DCH xx	Action Device And Number, where xx is 0-63.
- CTYP		Card Type
	DCIP	D-channel over IP
BANR	YES	Enable security banner printing option
- IFC	SL1	Interface type for D-channel
H323		Indicates overlap signaling prompts for H.323
- OVLR	YES	Overlap Receiving

LD 17 – Configure D-channels to support overlap signaling. (Part 2 of 2)

Prompt	Response	Description
- OVLS	YES	Overlap Sending
OVLT	0-(1)-8	Overlap Timer (in seconds) The timer controls the interval between the sending of INFORMATION messages. Defaults to 1 for D-channel over IP ***Note:*** OVLT applies only to Overlap Sending (OVLS = YES).

In the Route Data Block, the zone parameter makes the codec selections and calculates the bandwidth usage for calls to the trunk members of a given route.

LD 16 – Configure the H.323 route. (Part 1 of 3)

Prompt	Response	Description
REQ	NEW	Add a new route.
TYPE	RDB	Route Data Block
CUST	xx	Customer number as defined in LD 15.
ROUT		Route number
	0-511	Range for Large System and CS 1000E system
	0-127	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T
DES	x...x	Designator The designator field for the trunk groups. This designator can be 0-16 alphanumeric characters.
TKTP		Trunk Type
	TIE	TIE trunk

LD 16 – Configure the H.323 route. (Part 2 of 3)

Prompt	Response	Description
VTRK		Virtual Trunk route, where:
	YES	YES = This route is for Virtual Trunk NO = This route is not for Virtual Trunk (default)
ZONE	0-255	Zone for codec selection and bandwidth management
PCID	H323	Protocol ID for the H.323 route Defines the route as an H.323 route.
NODE	xxxx	Node ID Where the Node ID matches the node of the Signaling Server. The Node ID can have a maximum of four numeric characters.
ISDN	YES	Integrated Services Digital Network option
- MODE		Mode of operation
	ISLD	Route uses ISDN Signaling Link (ISL) ISLD is allowed only if ISDN = YES, and the Integrated Services Digital Network Signaling Link (ISL) package 147 is equipped. ISLD is allowed only on ISA and TIE trunks.
- DCH	0-159	D-channel number
- IFC	SL1	Interface type for route (IFC responses are listed in *Software Input/Output: Administration* (553-3001-311))
- SRVC	a...a	Service type for AT&T ESS connections (SRVC responses are listed in *Software Input/Output: Administration* (553-3001-311))
- - PNI	(0)-32700	Private Network Identifier
- NCNA	(YES)	Network Calling Name Allowed

LD 16 – Configure the H.323 route. (Part 3 of 3)

Prompt	Response	Description
- NCRD	YES	Network Call Redirection
- INAC	(NO) YES	Insert ESN Access Code Inserts the ESN access code in an incoming private network call. INAC enables an ESN access code to be automatically added to an incoming ESN call from a private network. If INAC = YES, then digit insertion (INST) for NARS or BARS calls is bypassed and Access Code 1 (AC1) is used for all call types. However, calls can be specifically defined to use Access Code 2 (AC2) in LD 15 at the AC2 prompt. INAC is prompted when the route type is either a TIE trunk or an IDA trunk with DPNSS1 signaling.
ICOG		Incoming and Outgoing trunk.
	IAO	Incoming and Outgoing
ACOD	x...x	Access Code for the trunk route.

Nortel recommends that all routes in a Route List Block (RLI) be configured as either overlap or en bloc. That is, an en bloc route should not have alternate routes that are configured as overlap, and vice versa. Erratic behavior can occur when overlap and en bloc routes are configured as alternate routes. Normal behavior occurs on alternate routes as long as the alternate route has the same overlap capabilities as the main route.

A warning message is displayed if alternate routes are configured as a different type from the main route.

LD 86 – Configure the Route List Block for the Virtual Trunk route and configure the minimum number of digits included in the SETUP message. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number as defined in LD 15.
FEAT	RLB	Route list block
...		
RLI		Route List Index to be accessed
	0-127 0-255 0-999	CDP and BARS NARS FNP
ENTR	xxx	Entry number for NARS/BARS Route list Where xxx = • 0-63 Entry number for NARS/BARS Route List • 0-6 Route list entry number for CDP • X Precede with x to remove
ROUT		Route number
	0-511	Range for Large System and CS 1000E system
	0-127	Range for Small System, CS 1000S system, Media Gateway 1000B, and Media Gateway 1000T ***Note:*** The route must be overlap capable.
...		
ENTR	<cr>	Entry number for NARS/BARS Route list
ISET	(0)-8	Initial Set Number of entries in Initial Set for route list block.

LD 86 – Configure the Route List Block for the Virtual Trunk route and configure the minimum number of digits included in the SETUP message. (Part 2 of 2)

Prompt	Response	Description
...		
OVLL	(0)-24	Overlap Length Number of digits required before the SETUP message is sent. If OVLL = 0 then all the dialed digits are sent in a single SETUP message and the call is an en bloc call (even if LD 17 suggests overlap signaling). A value of x, where x is a 1 to 24, that x digits are required before sending the SETUP message. ***Note:*** Setting the OVLL to the expected digit string length (for example, OVLL = 7 when using seven-digit UDP) effectively forces en bloc. The SETUP message must have all seven digits before the message is sent. Therefore, the whole number is sent in the first message.

LD 87 – Configure the CDP steering codes. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in LD 15.
FEAT	CDP	Coordinated Dialing Plan
TYPE		Type of steering code
	DSC	Distant Steering Code
	TSC	Trunk Steering Code
DSC	x..x	Distant Steering Code Up to 4 digits; up to 7 digits with Directory Number Expansion (DNXP) package 150.

LD 87 – Configure the CDP steering codes. (Part 2 of 2)

Prompt	Response	Description
- FLEN	(0)-10	Flexible Length number of digits ***Note:*** See page 520 for more information about FLEN.
TSC	x..x	Trunk Steering Code Up to 4 digits, up to 7 digits with Directory Number Expansion (DNXP) package 150.
- FLEN	(0)-24	Flexible Length number of digits ***Note:*** See page 520 for more information about FLEN.

LD 90 – Configure E.164 plan call types and private plan Location Codes.

Prompt	Response	Description
REQ	NEW CHG	Create new data block Change existing data block
CUST	xx	Customer number as defined in LD 15.
FEAT	NET	Network Translator (Network translation tables)
TRAN		Translator
	AC1	Access Code 1 (NARS/BARS)
	AC2	Access Code 2 (NARS)
TYPE		Type
	LOC	Location Code
LOC	xxx y..y	Location code, where xxx = home location code and y..y = extended code of 1-4 digits. The extended code is optional.

LD 90 – Configure E.164 plan call types and private plan Location Codes.

Prompt	Response	Description
- FLEN	(0)-10	Flexible Length number of digits Enter the maximum number of digits expected. When this number of digits is dialed, dialing is considered to be complete and end-of-dial processing begins. Default is zero (0) digits. ***Note:*** See page 520 for more information about FLEN.

LD 90 – Configure Special Numbers.

Prompt	Response	Description
REQ	NEW CHG	Create new data block Change existing data block
CUST	xx	Customer number as defined in LD 15.
FEAT	NET	Network Translator (Network translation tables)
TRAN		Translator
	AC1 AC2	Access Code 1 (NARS/BARS) Access Code 2 (NARS)
TYPE		Type
	SPN	Special Number Translation
SPN	xxx	Special Number translation Enter the SPN digits in groups of 3 or 4 digits, separated by a space (e.g., xxxx xxx xxxx). The SPN can be up to 19 digits long. The maximum length no longer depends on whether or not the first digit of the SPN is a “1”. That restriction has been removed. The maximum number of groups allowed is 5.

LD 90 – Configure Special Numbers.

Prompt	Response	Description
- FLEN	(0)-24	Flexible Length number of digits Enter the maximum number of digits expected. When this number of digits is dialed, dialing is considered to be complete and end-of-dial processing begins. Default is zero (0) digits. ***Note:*** See page 520 for more information about FLEN.

Configuring overlap signaling using Element Manager

To configure a D-channel to support overlap signaling, follow the steps in Procedure 74.

Procedure 74
Configuring D-channels to support overlap signaling

1. Log in to CS 1000 Element Manager.
2. Select **Routes and Trunks** > **D-Channels** from the navigator.

   The **D-Channel** web page opens.
3. Click the **Edit** button associated with the D-channel.

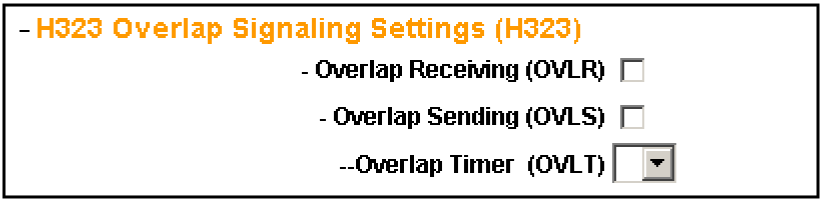
   The **D-Channel xx Property Configuration** web page opens where xx is the D-channel number.
4. Choose **Advance Options (ADVOPT)**.
5. Choose **H.323 Overlap Signaling Settings (H323)** (see Figure 257 on page 518).

   a. Select the **Overlap Receiving (OVLR)** check box.

   b. Select the **Overlap Sending (OVLS)** check box.

   c. Select a timer value (in seconds) from the **Overlap Timer (OVLT)** drop-down list.

Figure 257
H.323 Overlap Signaling



- H323 Overlap Signaling Settings (H323)

- Overlap Receiving (OVLR) □

- Overlap Sending (OVLS) □

--Overlap Timer (OVLT) ▾

6 Click **Submit**.

End of Procedure

To configure the number of digits required before the SETUP message is sent, follow the steps in Procedure 75.

Procedure 75
Configuring the minimum number of digits included in the SETUP message

1 Refer to Procedure 11: "Configuring the Route List Block" on page 315.

2 Enter a value for **Overlap Length (OVLL)**.

If OVLL = 0 (the default), then all the dialed digits are sent in a single SETUP message and the call is an en bloc call (even if Procedure 74/ LD 17 suggests overlap signaling). A value of x, where x is 1-24, indicates that x digits are required before sending the SETUP message.

Note: Setting the OVLL to the expected digit string length (for example, OVLL = 7 when using seven-digit UDP) effectively forces en bloc. The SETUP message must have all seven digits before the message is sent. Therefore, the whole number is sent in the first message.

End of Procedure

Overlay changes for overlap signaling

LD 17 displays the H323 prompt is displayed for a D-channel over IP (type DCIP). The H323 prompt has three key prompts, OVLR, OVLS, and OVLT, that are provided for an H.323 D-channel.

> ***Note:*** This prompt sequence is displayed only for a D-channel of type DCIP if the H.323 Virtual Trunk (H323_VTRK) package 399 and Overlap Signaling (OVLP) package 184 are enabled. Otherwise, the OVLR, DIDD, OVLS, and OVLT prompt sequence is displayed.

The user must configure OVLS, OVLR, and OVLT in LD 17 in order for overlap signaling to work.

> ***Note:*** The D-channel must be disabled before modifying the OVLR and OVLS prompts. The OVLR and OVLS data must be transmitted to the Signaling Server. This occurs only when the D-channel is enabled.

- If the Call Server is to send overlap calls over IP, then Overlap Sending (OVLS) must be configured as YES. This setting turns on overlap sending from the Call Server to the IP domain.
- If the Call Server is to receive overlap calls over IP, then Overlap Receiving (OVLR) must be configured as YES. This setting turns on overlap signaling from the IP domain to the Call Server.
- The Overlap Timer (OVLT) prompt only has meaning for Overlap Sending (OVLS = YES). The OVLT value indicates the time the system waits to accumulate digits to send in an INFORMATION message after the SETUP message is sent. The valid values for OVLT are 0-8 where:
  - A value of 0 results in the generation of an INFORMATION message for every digit dialed after the minimum overlap called number length (as provisioned in LD 86 for the RLI).
  - A value of 1 is the default value for a D-channel over IP.

In LD 86, a warning is issued if a mixture of IP capable overlap routes and en bloc capable routes exist in an RLI. The warning is also issued if an en bloc IP route coexists with overlap capable routes. The warning is displayed only at the Call Server login window. It is not transmitted to Element Manager.

The use of the Flexible Length number of digits (FLEN) prompt has changed (in LD 87 and LD 90) for overlap signaling but has not changed for en bloc.

With IP Peer overlap signaling calls, the usage of the FLEN prompt is changed as follows:

- If FLEN = 0, then (in general) overlap handling has not changed. The SETUP message is sent once the OVLL digits are received and the dialing plan entry can be determined. However, the end-of-dial timer starts, and on expiration, the Call Server sends an INFORMATION message with Sending Complete to indicate end-of-dial.
- If FLEN is greater than 0 and also greater than both of the following:
  - the length of the digit string provisioned in LD 87 or LD 90, and
  - the OVLL value,

  then overlap signaling meets the two requirements for the SETUP message. After that, further digits are sent in the INFORMATION messages. In addition, for IP overlap signaling, when the value configured for FLEN is reached, the INFORMATION message carrying the digits also carries the Sending Complete Information Element (IE).

  Note: An IE is a unit of information in Q.931 and H.323 messaging.
- If FLEN is less than OVLL, then the SETUP message is sent immediately. To ensure that the Signaling Server does not wait for more digits, the SETUP message also includes the Sending Complete IE.

With en bloc calls, the usage of the FLEN prompt is as follows:

- If FLEN is a non-zero value, then the Call Server collects digits until the total count of collected digits equals FLEN. The Call Server then sends a SETUP message.
- If FLEN = 0, then the Call Server uses an end-of-dial timer to determine when it has a completed number. The Call Server collects digits, restarting the end-of-dial timer after each digit, and waits for the timer to expire to send the SETUP message.

Flexible Length number of digits implications

A non-zero FLEN value indicates the number of digits the system should expect for the current number type and plan entry. When the digits collected reach the expected length, the system sends an end-of-dial indication to the remote switch. A value of 0 means the length is unknown and FLEN = 0 has a specific impact on the system.

En bloc dialing handles an unknown length by using an end-of-dial timer. It uses the end-of-dial timer to decide how many digits it must collect. When the timer expires, all received digits are sent in the SETUP message.

When PRI uses overlap signaling and FLEN = 0, the network relies on the remote switch to determine the correct length. The originating switch can use overlap signaling to send the digits once the OVLL and dialing plan entry requirements are met.

For IP, however, the remote switch may be one of many devices (for example, a CS 1000 system, an H.323 gateway, or a Business Communications Manager (BCM) node). The remote switch may also be overlap- or en bloc-capable. An overlap call to an overlap destination is not an issue. However, an en bloc destination requires overlap-to-en bloc conversion, which in turn requires knowledge of when a digit string is completed. Therefore, for overlap signaling on IP Peer to perform overlap-to-en bloc conversion with a FLEN of 0, the system must know when the digit string ended. As a result, unlike the PRI overlap-signaling case, when the end-of-dial timer expires (for an IP overlap signaling call) the Call Server sends a Sending Complete IE in the INFORMATION message to indicate end-of-dial.

Nortel recommends that all numbers with a known length set FLEN equal to the length of the digit string. For example, if all Location Codes (LOC) are eight digits in length, then use FLEN = 8 for all LOC codes. However, when the destination is unknown, use FLEN = 0. This process provides full overlap capability to an overlap-enabled destination, while providing the end-of-dial indication to allow interworking with an en bloc destination.

> ***Note:*** Dialing the octothorpe (#) forces an immediate end-of-dial, so the Call Server immediately provides end-of-dial treatment.

System log messages

The Signaling Server has a log file. A system log message is issued to this log file when the Signaling Server detects an incoming H.323 overlap signaling call that must revert to en bloc.

This system log message is output no more than once every hour. The message indicates the number of occurrences of overlap-to-en bloc conversion since the last system log message. No output is generated during a period in which no overlap-to-en bloc conversion occurred.

SIP Phone support

Contents

This section contains information on the following topics:

Introduction

Certified compatible third-party industry-standard SIP Phones are supported.

SIP Phones are configured on, and register to the NRS (specifically, the SIP Redirect Server), where they are configured as SIP user endpoints. As such, they communicate directly with the SIP Redirect Server, SIP Trunk Gateways, and other SIP Phones on the system. In contrast, IP Phones are configured on, and are controlled by, the Call Server.

IP Phones use the Unified Networks IP Stimulus Protocol (UNIStim) and are stimulus-based telephones. The features on an IP Phone are delivered by the Communication Server. SIP Phones use the Session Initiation Protocol which is an open industry standard-based signaling protocol. Some of the telephony features of the SIP Phones are delivered by the Communication Server. However, SIP Phones can have additional features that are available on the telephone itself. These features vary based on manufacturer and the model of the telephone.

A SIP Phone is a standards-based SIP device.

> ***Note:*** CS 1000 does not support Call Forward across NRS Collaborative Servers by third-party SIP Phones.

SIP Phone interaction

Table 34 on page 525 shows the interaction between SIP Phones and components in the CS 1000 network.

Table 34
SIP Phone and CS 1000 component interaction

Component	Description
SIP Phone	SIP Phones are intelligent telephones which deliver many common business telephony features (for example, CLID, Conference, Transfer, MWI, and Name Display). See “SIP Phone features” on page 526 for more details. SIP Phones can also have other manufacturer-dependant features.
SIP Redirect Server	The NRS, specifically the SIP Redirect Server, provides the following: • a web-based interface (NRS Manager) for provisioning SIP Phones • registration and authentication for SIP Phones • routing definitions for all SIP traffic (including SIP Phones)
SIP Trunk Gateway	The SIP Trunk Gateway provides the following: • a signaling gateway for all SIP calls originating from and terminating to the CS 1000 system • standard SIP support for CLID, MWI, Name Display, and Call Redirection
CS 1000 Call Server	The Call Server provides call processing software which enables the following: • CDR using the tandem CDR feature • Trunk Access Restrictions using Class of Service (CLS) and Trunk Group Access Restrictions (TGAR) • SIP Access Port Licenses
TDM telephones and IP Phones, IP Trunk, and CallPilot	SIP Phones can interwork with the full suite of CS 1000 TDM and IP endpoints. CallPilot provides Unified Messaging for SIP Phones, including MWI.

SIP Phone features

The following is a list of features delivered through the CS 1000 system:

- Calling Line Identification (CLID)
- Network Call Party Name display
- Network Call Redirection
- Message Waiting Indication
- Network Class of Service Access controls
- Network Alternate Route Selection (NARS, UDP, CDP)
- Call Detail Recording (CDR) — using Tandem CDR features

The following is a a list of intelligent SIP Phone-based features supported by the CS 1000 system. The features are dependant on the SIP Phone.

- Conference calling
- Call hold
- Call waiting
- Call forwarding
- Call transfer
- Caller ID
- Call waiting caller ID

The following features are available through the user interface in a web server-based configuration:

- Speed dial from phone book
- Call logs

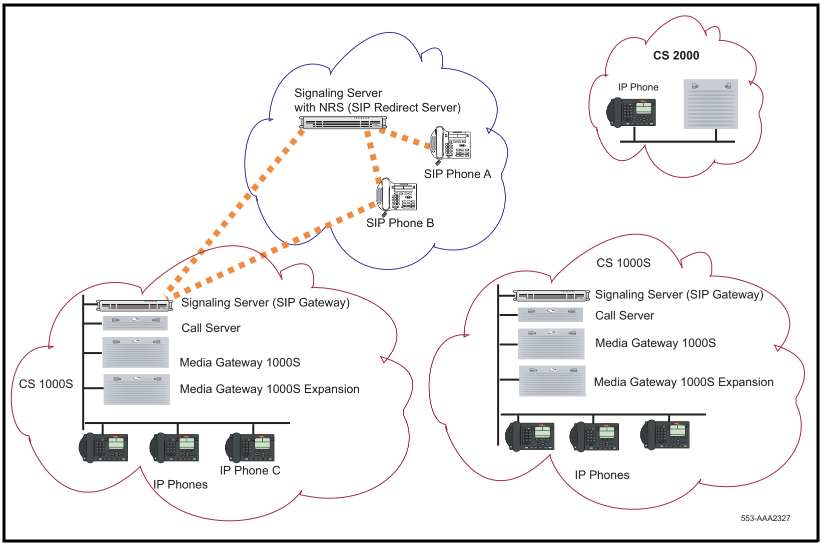
SIP-compliant telephones can interoperate with voice, data, video, and Internet applications and services that are SIP-enabled or provide full SIP support.

SIP Phones are configured on the Signaling Server using NRS Manager. See "Configuring a SIP Phone" on page 542.

SIP Phone calls

Figure 258 shows SIP Phone-to-SIP Phone connectivity and SIP Phone-to-SIP Trunk Gateway connectivity.

Figure 258
SIP Phones and SIP Trunk Gateways in the network



When two SIP Phones (SIP Phones A and B) want to communicate with each other, the originating SIP Phone must communicate directly with the SIP Redirect Server for authentication and address resolution. Then communication is established between the two SIP Phones. Refer to “SIP Phone-to-SIP Phone communication” for the call flow between two SIP Phones in the same network.

When a SIP Phone (A) wants to communicate with another non-SIP telephone (for example, IP Phone C), then the SIP Trunk Gateway is involved. Refer to “SIP Trunk Gateway-to-SIP Phone communication” on page 533 for the call flow between a SIP Phone and another telephone using the SIP Trunk Gateway.

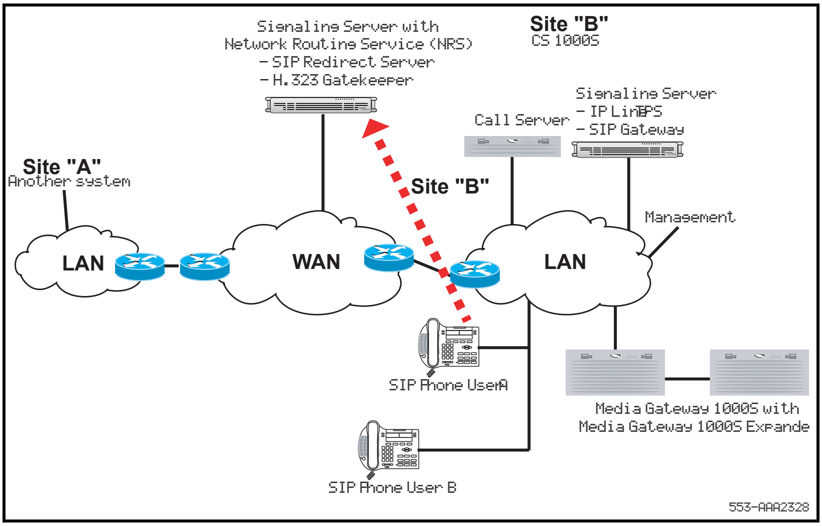
Note: The following call flows are not exhaustive descriptions of the protocol, and exclude some of the components in the CS 1000 system. They are examples for illustrative purposes only.

SIP Phone-to-SIP Phone communication

When SIP Phone User A wants to call SIP Phone User B, the following occurs:

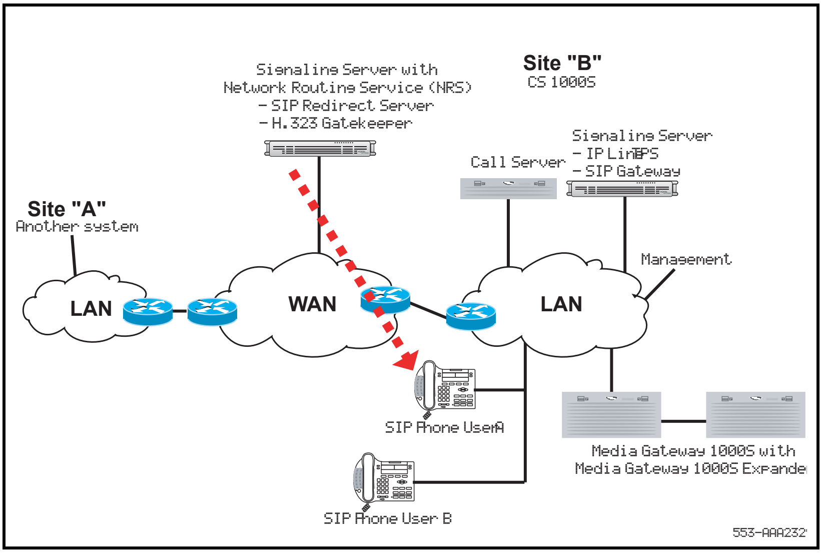
1 SIP Phone A sends an INVITE message to the NRS (specifically the SIP Redirect Server). See Figure 259.

Figure 259
SIP Phone A sends INVITE message to SIP Redirect Server



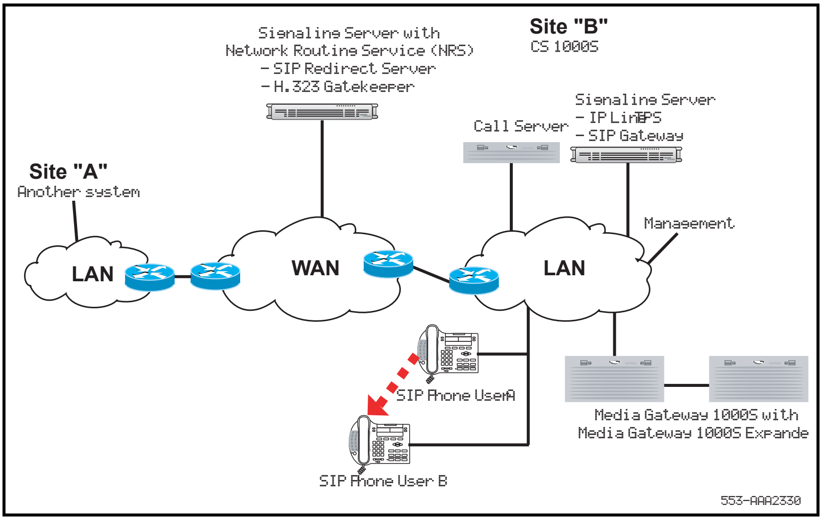
2 The SIP Redirect Server responds with a REDIRECT message and informs SIP Phone User A to directly contact SIP Phone User B. See Figure 260.

Figure 260
SIP Redirect Server responds to SIP Phone A



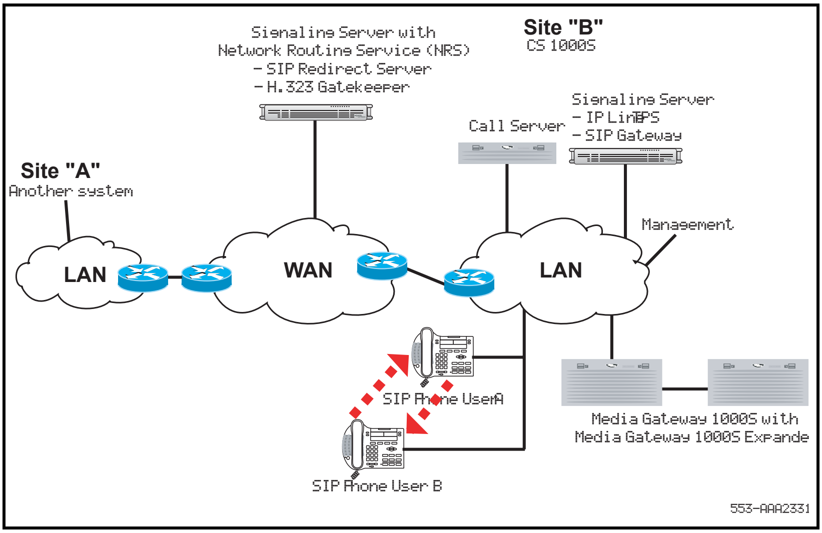
3 SIP Phone A sends an INVITE message directly to SIP Phone B. SIP Phone B rings. See Figure 261.

Figure 261
SIP Phone A sends INVITE message to SIP Phone B



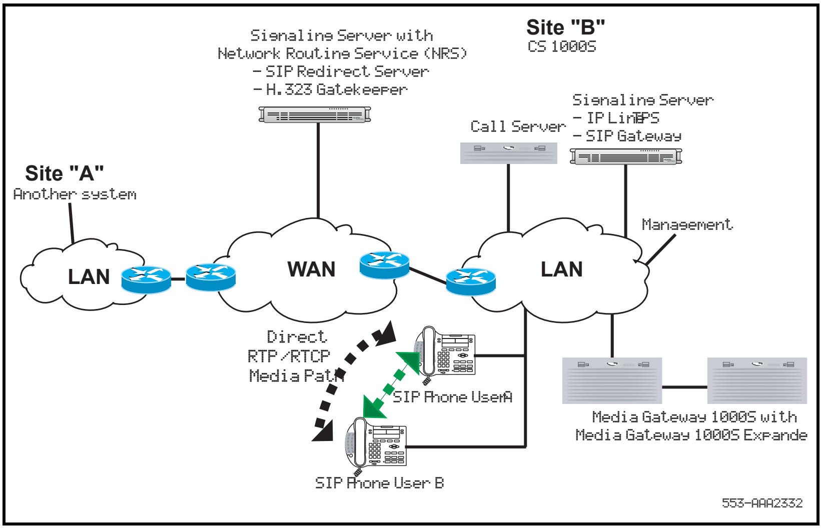
4 SIP Phone User B sends a SIP 200 OK message to SIP Phone User A. SIP Phone A replies by sending a 200 ACK message to SIP Phone B. See Figure 262.

Figure 262
SIP Phone B sends 200 OK message to SIP Phone A



5 The call is set up between the two SIP Phones, and two-way RTP messages are exchanged between SIP Phone A and SIP Phone B. See Figure 263.

Figure 263
SIP Phones start the direct IP media paths

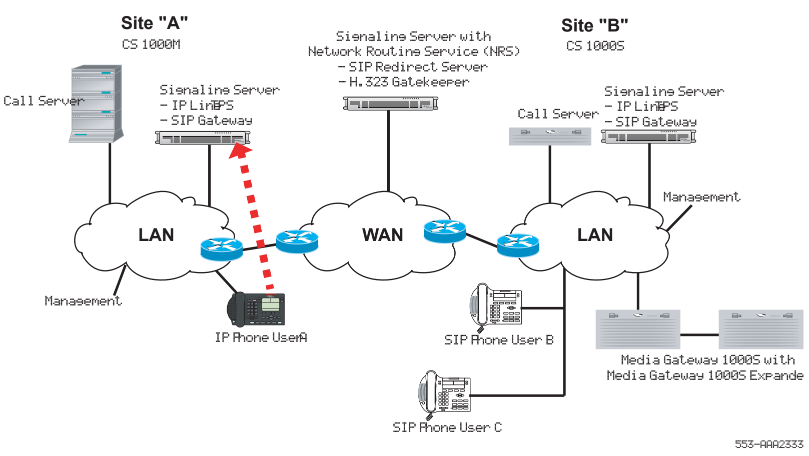


SIP Trunk Gateway-to-SIP Phone communication

When IP Phone User A wants to call SIP Phone User B, the following occurs:

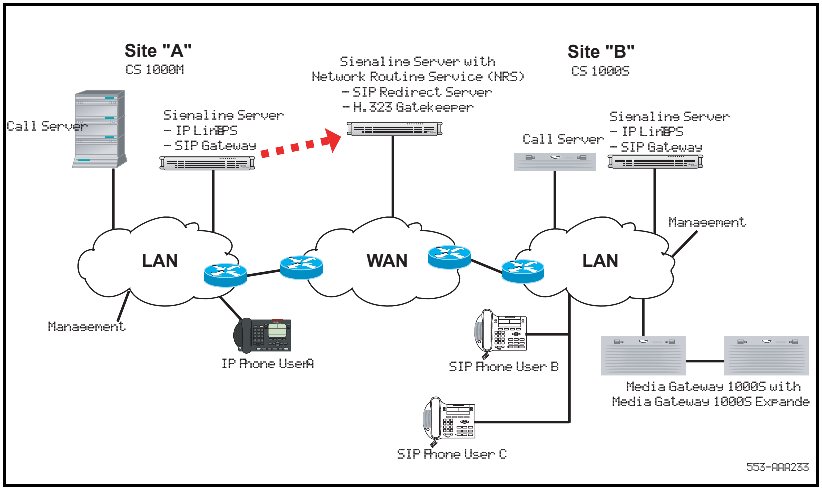
1 IP Phone A makes a call that is routed through Call Server A. See Figure 264.

Figure 264
IP Phone A sends message to SIP Trunk Gateway A



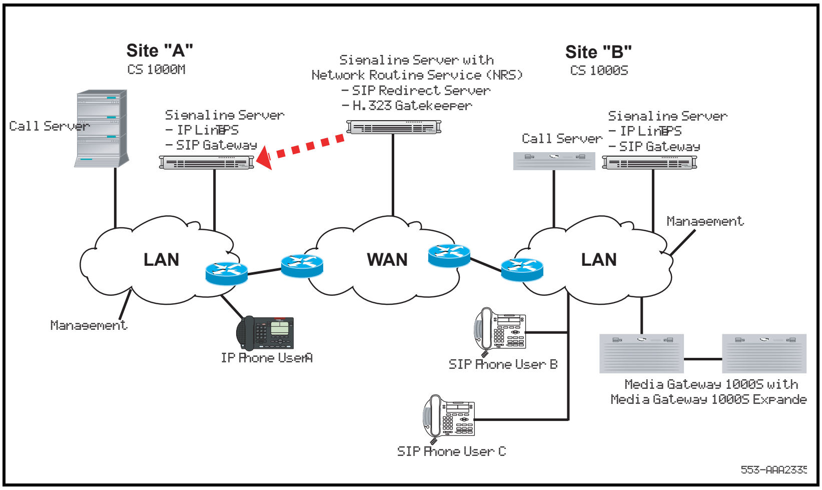
2 SIP Trunk Gateway A sends an INVITE message to the NRS (SIP Redirect Server). See Figure 265.

Figure 265
SIP Trunk Gateway A sends INVITE message to SIP Redirect Server



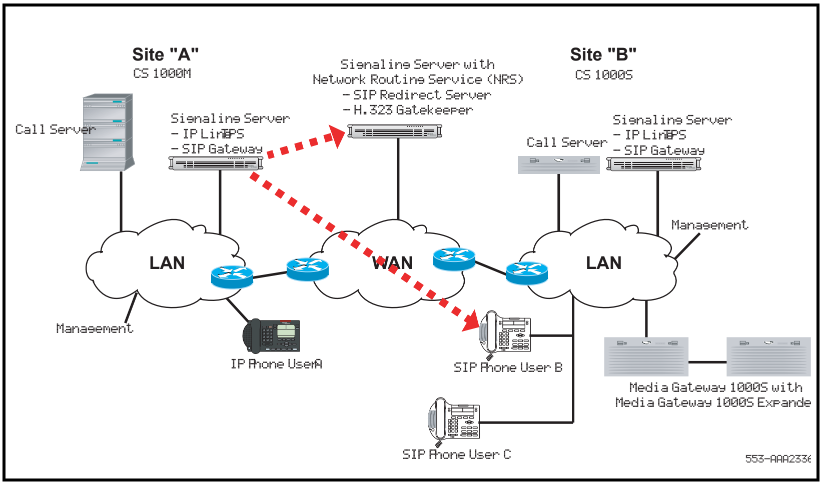
3 The SIP Redirect Server replies back to SIP Trunk Gateway A with a REDIRECT message. The SIP Redirect Server informs SIP Trunk Gateway A of the location of SIP Phone B. See Figure 266.

Figure 266
SIP Redirect Server replies to SIP Trunk Gateway A



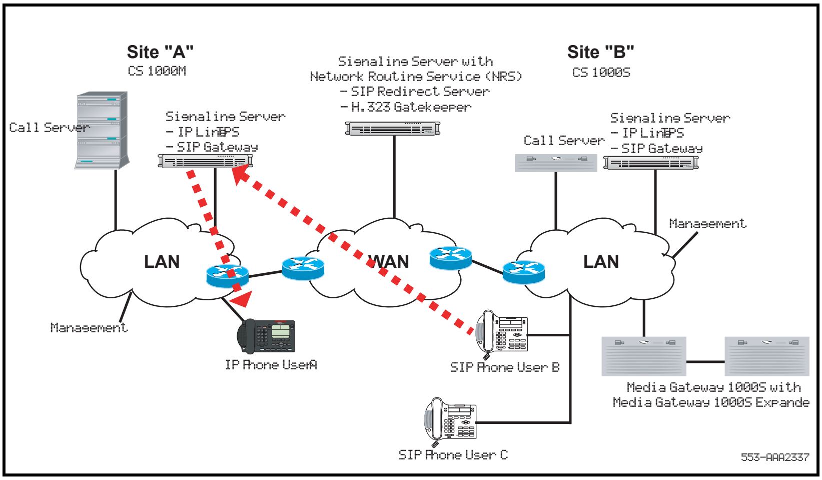
4 SIP Trunk Gateway A acknowledges the message from the SIP Redirect Server with an ACK message. SIP Trunk Gateway A then sends an INVITE message directly to SIP Phone B. See Figure 267.

Figure 267
SIP Trunk Gateway A sends INVITE message to SIP Phone B



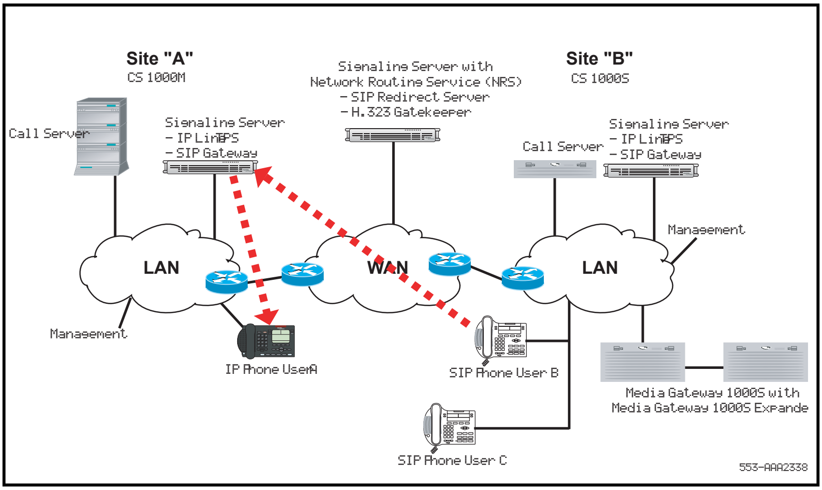
5 SIP Phone B sends a TRYING message and a Ringing message to the SIP Trunk Gateway A. SIP Trunk Gateway A then sends an Alerting message to IP Phone A. See Figure 268.

Figure 268
SIP Phone B communicates with SIP Trunk Gateway A and SIP Trunk Gateway A communicates with IP Phone A



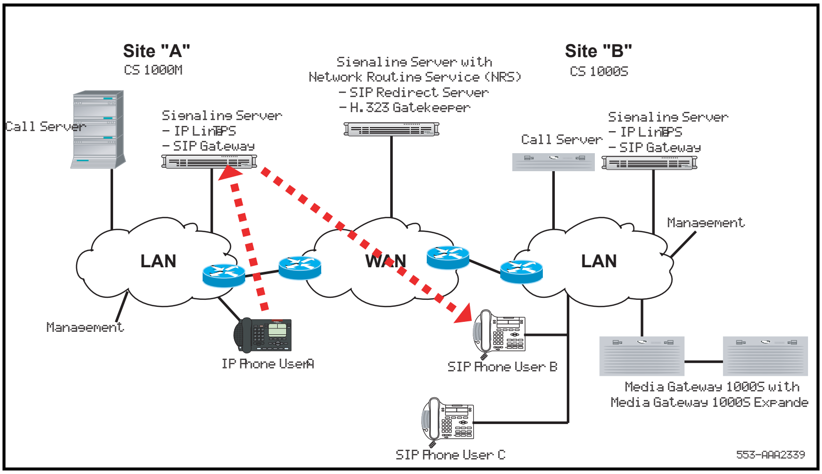
6 SIP Phone B sends a SIP 200 OK message to the SIP Trunk Gateway A. SIP Trunk Gateway A sends a Connect message to IP Phone A. See Figure 269.

Figure 269
SIP Trunk Gateway A communicates with SIP Phone B and IP Phone A



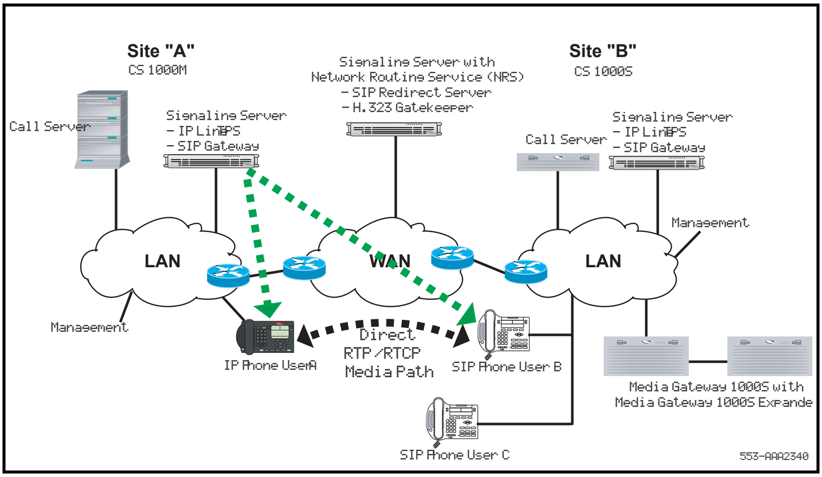
7 IP Phone User A responds to SIP Trunk Gateway A with a Connect ACK message. SIP Trunk Gateway A sends a SIP 200 ACK message to SIP Phone B. See Figure 270.

Figure 270
IP Phone A acknowledges SIP Trunk Gateway A and SIP Trunk Gateway A sends SIP 200 ACK message to SIP Phone B



8 The call is set up between IP Phone A and SIP Phone B. Two-way RTP messages are exchanged between IP Phone A and SIP Phone B. See Figure 271.

Figure 271
Direct media path is set up between IP Phone A and SIP Phone B



SIP Phone dynamic registration

SIP Phone dynamic registration facilitates the creation of a contact list for the authorized SIP Phones. A SIP Phone client registers as an endpoint with the SIP Redirect Server (in the NRS). A phone number and a username are mandatory routing entries for the endpoint and are provided during provisioning in the NRS (see Procedure 76 on page 543).

At registration, only one IP address of the SIP Phone is registered in the endpoint contact list. That is, if a SIP Phone provides more than one IP address in the registration message, then only one IP address (the first one) is stored on the NRS. Usually only one IP address is provided in the registration message; however, the number of provided IP addresses depends on the SIP Phone.

The SIP Redirect Server provides the phone context for SIP Phones when calling users behind the SIP Trunk Gateway.

Note: SIP Phones typically do not qualify DN-based URIs with the phone context. Basic support for dealing with raw numbers (as they are dialed by the user) is provided by the SIP Redirect Server. The SIP Redirect Server provides support of unqualified DN-based URIs by performing a pretranslation in order to find the appropriate phone-context.

Assumptions

SIP Phones must support the following for the dynamic registration and establishment of the SIP Phone calls:

- REGISTER message
- 302 message
- Re-INVITE message
- REFER message
- SUBSCRIBE message
- NOTIFY message
- INFO message for end-to-end DTMF
- phone-context transfer from 302 message to INVITE message
- vendor information
- username and password
- static or DHCP assigned IP address
- Expires and Expires Refresh Time based on a 423 (Interval Too Brief) message

Log files

SIP Phones generate log files. SIP Phone user registration and deregistration generate informational report log entries. However, SIP Trunk Gateways generate both log files and SNMP alarms. SIP Trunk Gateway endpoint registration and deregistrations generate SNMP alarms, as well as report log entries.

Installing a SIP Phone

Follow the manufacturer's installation and configuration instructions to set up your SIP Phone.

Configuring a SIP Phone

A SIP Phone is configured on the Signaling Server using NRS Manager. A SIP Phone registers and communicates as an endpoint in the NRS.

Routing of unqualified numbers

To support routing of unqualified numbers dialed by SIP Phones, the NRS provides several types of dialing prefixes at the Level 1 regional domain, Level 0 regional domain, and for endpoints. The dialing prefixes include the following:

- E.164 International dialing access code (for example, 6011)
- E.164 National dialing access code (for example, 61)
- E.164 Local dialing access code (for example, 9)
- Level 1 Regional dialing access code (for example, 6)
- Level 0 Regional dialing access code (the default, if none of above match)

Up to two special numbers can be specified at L1 and/or L0.

Task summary

Before a SIP Phone can be added as a User Endpoint in the NRS, the Service Domain, Level 1 Regional Domain, and Level 0 Regional Domain must be configured. To complete these tasks, perform the following procedures:

- Procedure 34: “Adding a Service Domain” on page 413
- Procedure 36: “Adding an L1 Domain (UDP)” on page 416
- Procedure 38: “Adding an L0 Domain (CDP)” on page 420

Then configure the SIP Phone in the NRS. To configure the SIP Phones, perform the steps in Procedure 76: "Adding a User Endpoint" on page 543.

Adding a User Endpoint (SIP Phone)

To configure SIP Phones, use the **User Endpoints** link in the NRS **Configuration** tab. The NRS User Endpoints support only SIP Phone user configuration.

User Endpoints configuration is at the same level configuration as Gateway Endpoints. That is, both the User Endpoints and Gateway Endpoints are under the Level 0 Regional Domain.

Use Procedure 76 to add a user endpoint (SIP Phone).

Procedure 76
Adding a User Endpoint

1 Log in to the NRS. See "Accessing NRS Manager" on page 393.

2 Click the **Configuration** tab.

A dialog box displays indicating the status of the active and standby database (see Figure 164 on page 412). Click **OK**.

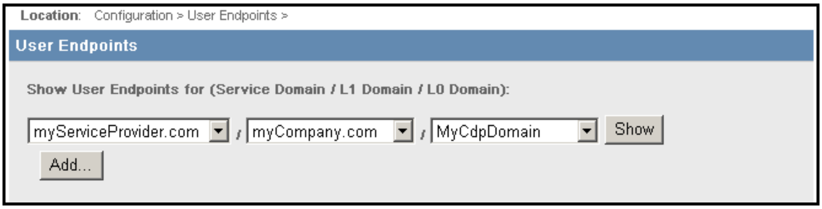
3 Ensure the **Standby DB view** is selected.

4 Click **User Endpoints** from the navigator.

Note: User Endpoint configuration is currently supported only for SIP.

The **User Endpoints** web page opens, as shown in Figure 273.

Figure 272
User Endpoints web page



Location: Configuration > User Endpoints >

User Endpoints

Show User Endpoints for (Service Domain / L1 Domain / L0 Domain):

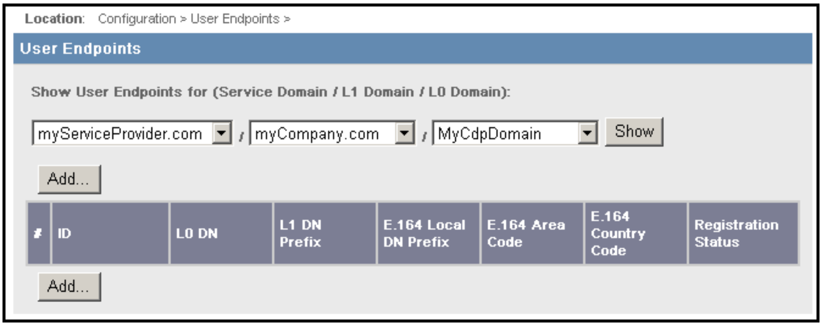
mySeviceProvider.com / myCompany.com / MyCdpDomain

5 Select a Service Domain, LI Domain, and L0 Domain from the respective drop-down lists.

6 (Optional) Click **Show**.

The web page expands to display a list of configured User Endpoints for the selected Service Domain, L1 Domain, and L0 Domain. See Figure 273.

Figure 273
Configured User Endpoints



Location: Configuration > User Endpoints >

User Endpoints

Show User Endpoints for (Service Domain / L1 Domain / L0 Domain):

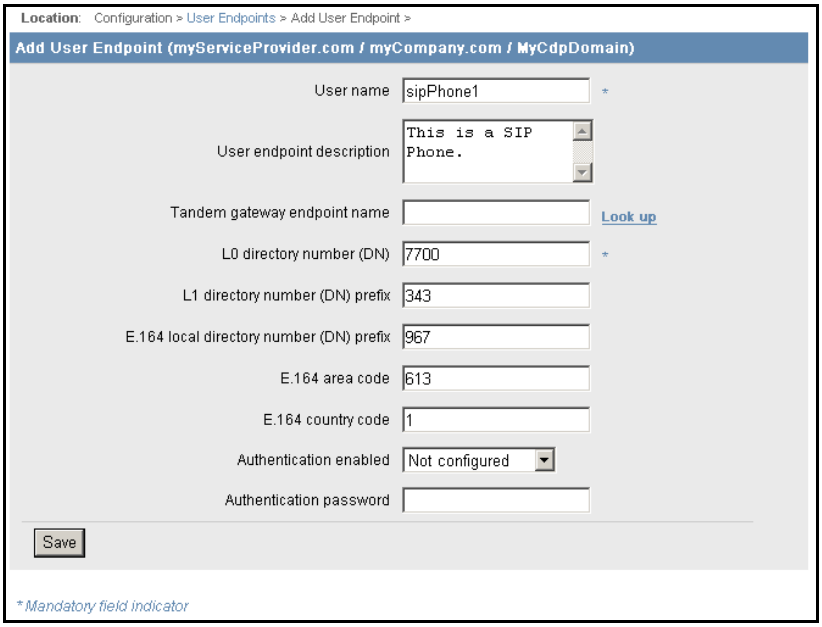
myServiceProvider.com / myCompany.com / MyCdpDomain

#	ID	L0 DN	L1 DN Prefix	E.164 Local DN Prefix	E.164 Area Code	E.164 Country Code	Registration Status

7 Click **Add...**.

The **Add User Endpoint** web page opens, as shown in Figure 274 on page 545.

Figure 274
Add User Endpoint web page



Location: Configuration > User Endpoints > Add User Endpoint >

Add User Endpoint (myServiceProvider.com / myCompany.com / MyCdpDomain)

User name	sipPhone1	*
User endpoint description	This is a SIP Phone.	
Tandem gateway endpoint name		Look up
L0 directory number (DN)	7700	*
L1 directory number (DN) prefix	343	
E.164 local directory number (DN) prefix	967	
E.164 area code	613	
E.164 country code	1	
Authentication enabled	Not configured	
Authentication password		

** Mandatory field indicator*

8 Enter a **User name** for the SIP Phone. The endpoint's username must be alphanumeric and can be up to 30 characters in length.

The username, together with the Service Domain names, becomes a string that is used to build the user's SIP URI:

[username]@[service_domain_name]

This SIP URI is used during SIP Phone registration. The username is used by the SIP authentication procedures.

9 Enter the **User endpoint description**. The endpoint's description must be alphanumeric (except single quotes) and can be up to 120 characters in length.

10 (Optional) Enter the **Tandem gateway endpoint name**.

A tandem gateway endpoint must be an existing endpoint on the network. It is usually a Gateway Endpoint. The tandem gateway endpoint name is used to tandem all calls originating from this User Endpoint. That is, all calls originating from this User Endpoint are forwarded to the tandem gateway endpoint, which then routes all the call to the appropriate destinations. This is useful for generating Call Records for originating User Endpoint calls.

Note 1: The tandem gateway endpoint name field is also present on the Gateway Endpoint web page.

Note 2: A tandem gateway endpoint must ONLY be configured if the customer wants all the outgoing calls from the SIP User Endpoint to tandem through a SIP Trunk Gateway Endpoint, in that case the SIP Trunk Gateway Endpoint name should be specified in the tandem endpoint box.

Note 3: To accurately add the SIP Trunk Gateway Endpoint name, a **Look up** link is provided to the right of the **Tandem gateway endpoint name** text box. Clicking the **Look up** link opens the **Look up path for Gateway Endpoints** web page (see the second bullet in step 3 on page 433).

11 Enter the **LO directory number (DN)** of the SIP Phone. The DN must be numeric and can be up to 30 numbers in length.

An example is 5000. The DN is the user’s DN. That is, the CDP number.

12 Enter the **L1 directory number (DN) prefix**. The DN prefix must be numeric and can be up to seven characters in length.

An example is 343. The L1 DN prefix together with the L0 DN creates the user’s DN which is unique within the parent L1 Regional Domain. That is, the UDP number. For example, 3435000.

L1 domain prefix + L0 DN = User’s DN
343 + 5000 = 3435000

13 Enter the **E.164 local directory number (DN) prefix**. The DN prefix must be numeric and can be up to seven characters in length.

An example is 967. The E.164 local DN prefix is the location code. The E.164 local prefix, together with the L0 DN, creates the user’s E.164 Local (subscriber) DN. For example, 9675000.

E.164 local prefix + L0 DN = User’s E.164 Local (subscriber) DN
967 + 5000 = 9675000

14 Enter the **E.164 area code**. The code must be numeric and can be up to 7 characters in length.

An example is 613. The E.164 area code together with both the E.164 local prefix and L0 DN creates the user's national E.164 National DN. For example, 6139675000.

E.164 area code + E.164 local prefix + L0 DN = User's E.164 National DN
613 + 967 + 5000 = 6139675000

15 Enter the **E.164 country code**. The code must be numeric and can be up to 7 characters in length.

An example is 1 (for North America). The E.164 country code, together with the E.164 area code, E.164 local prefix, and L0 DN, creates the user's E.164 International DN. For example, 16139675000.

E.164 country code + E.164 area code + E.164 local prefix + L0 DN
= User's E.164 International DN
1 + 613 + 967 + 5000 = 16139675000

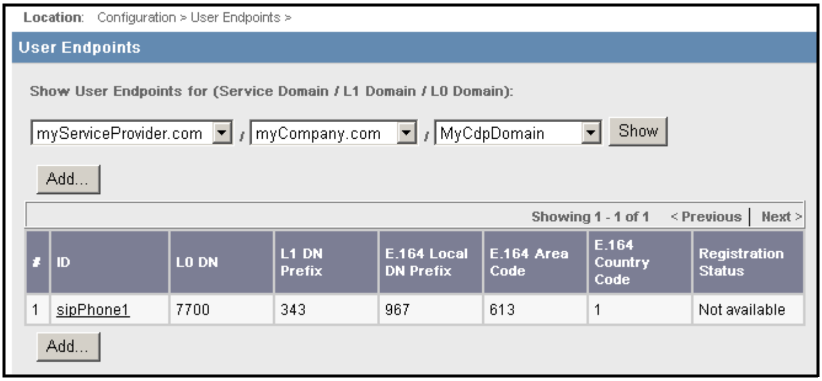
16 Select **Authentication on** from the **Authentication enabled** drop-down list, if you want to enable authentication for this endpoint.

17 If authentication is enabled in step 16, then enter the **Authentication password**. The password must be alphanumeric and can be up to 30 characters in length.

18 Click **Save**.

The **User Endpoints** web page opens, showing the newly added SIP Phone user endpoint. See Figure 275 on page 548.

Figure 275
Added User Endpoints



Location: Configuration > User Endpoints >

User Endpoints

Show User Endpoints for (Service Domain / L1 Domain / L0 Domain):

mySeviceProvider.com / myCompany.com / MyCdpDomain

#	ID	L0 DN	L1 DN Prefix	E.164 Local DN Prefix	E.164 Area Code	E.164 Country Code	Registration Status
1	sipPhone1	7700	343	967	613	1	Not available

19 If required, click **Add...** to add additional SIP Phone user endpoints. Repeat step 7 to step 18.

Any new endpoints are displayed in the **User Endpoints** web page.

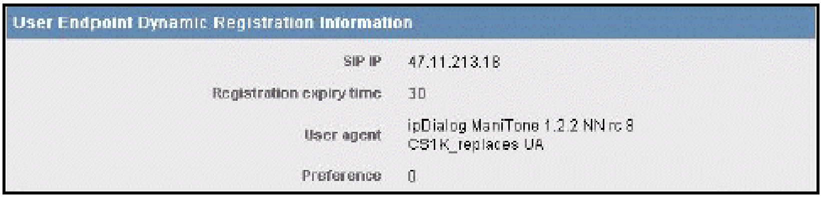
Note 1: A maximum of 50 user endpoints can be displayed on the **User Endpoints** web page.

Note 2: If a User Endpoint is configured, then the supported protocol type is dynamic SIP. NRS Manager displays User Endpoint Dynamic Registration Information after the User Endpoint registers with the NRS (see Figure 276 on page 549).

User Endpoint Dynamic Registration information includes the following: SIP IP, Registration expiry time, User agent, and Preference.

The **User Endpoint Dynamic Registration Information** web page is displayed only when NRS Manager is in Active database mode. Detailed dynamic registration information is displayed inside the **User Endpoints** web page.

Figure 276
User Endpoint Dynamic Registration Information



User Endpoint Dynamic Registration Information

SIP IP	47.11.213.18
Registration expiry time	30
User agent	ipDialog ManiTone 1.2.2 NN rc 8 CS1K_replaces UA
Preference	0

End of Procedure

IP Peer internetworking

Contents

This section contains information on the following topics:

Nortel products internetworking

CS 1000M System interworking

A CS 1000M System internetworks with other Nortel products. This chapter discusses internetworking between CS 1000M systems and the following products:

- Meridian 1 IE (IP Trunk Release 3.0 or later)
- Succession Release 3.0
- Business Communications Manager (BCM) Release 3.01 (or later)

Business Communications Manager

Business Communications Manager (BCM) can be part of an overall CS 1000 network. BCM can interwork with the H.323 Gatekeeper, supporting the basic network numbering plan and providing MCDN non-call associated signaling (such as Message Waiting Indication for network voice mail service).

> ***Note:*** IP Peer Networking with CS 1000 requires BCM Release 3.0 or higher.

Meridian 1 IE (IP Trunk Release 3.0 or later) / Succession 3.0

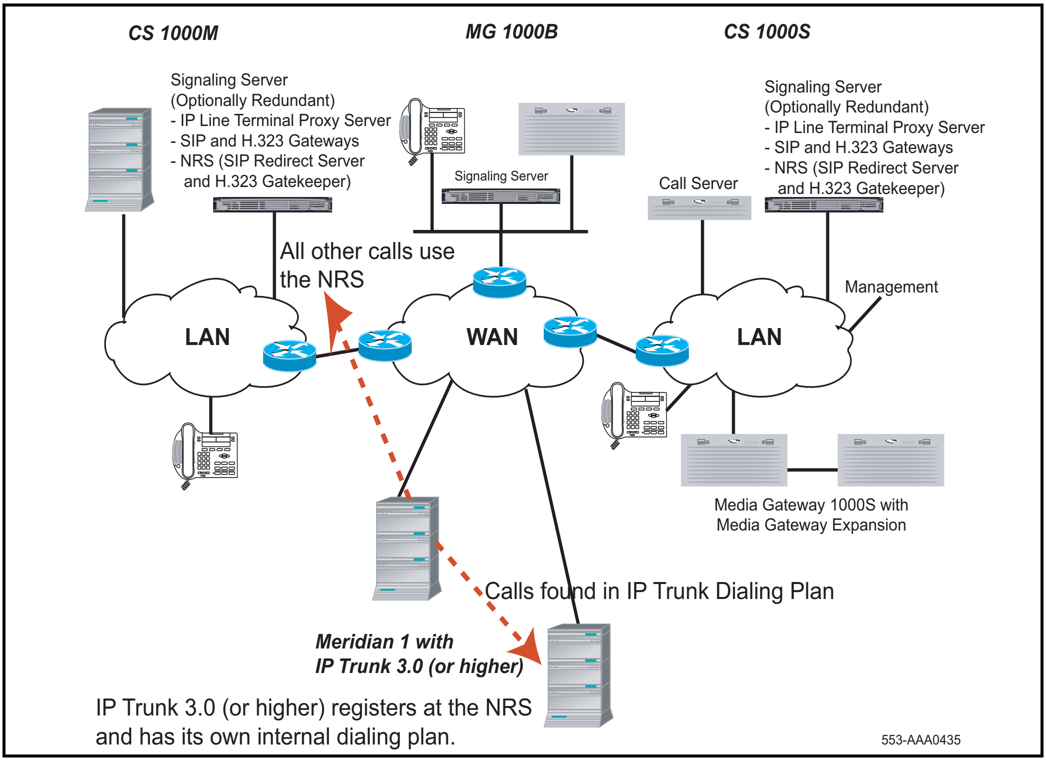
CS 1000 Release 4.0 and later networks with Meridian 1 Release 25.xx (or later) and Succession 3.0. Nortel Meridian Customer Defined Network (MCDN) protocol over PRI trunks provides the rich feature set currently available to networks of Meridian 1 Systems.

Any existing IP Trunks in the system must be upgraded to IP Trunk 3.0 (or later) in order to interwork with an IP Peer Networking node.

IP Peer Networking interworks with IP Trunk 3.0 (or later). It also supports all the MCDN features that IP Trunk 3.0 (or later) supports including Trunk Route Optimization.

With IP Trunk, the numbering plan is configured for each site. With IP Peer Networking, the NRS maintains the numbering plan for all sites. IP Trunk 3.0 (or later) maintains a point-to-point configuration. If a call is routed using IP Trunk 3.0 (or later) and the path is found, then the session is established. If the route path is not found, the lookup process is handed off to the NRS to resolve the route path. See Figure 277 on page 553.

Figure 277
IP Peer to Meridian 1 IP Trunk 3.0 (or later) Interworking



For a CS 1000M System to interwork with a Meridian 1 IE system, the following requirements must be met:

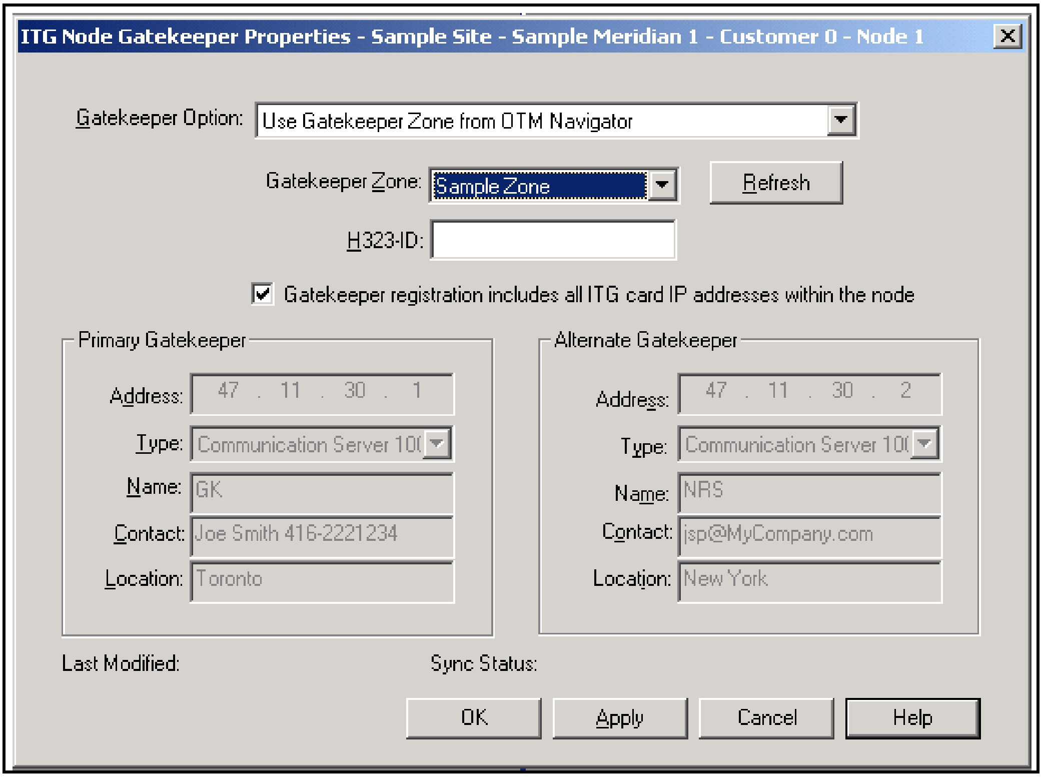
1 The ITG-P 24-port and Media Card 32-port trunk cards must be upgraded to IP Trunk 3.0 (or later) software. This upgrade supports MCDN features and NRS registration. Use OTM 2.2 to perform the upgrade. Refer to *Optivity Telephony Manager: System Administration* (553-3001-330) for information on installing, upgrading, and configuring IP Trunk 3.0 (or later) parameters.

2 Configure the IP Trunk 3.0 (or later) node to register with the CS 1000M NRS, using the OTM 2.2 ITG Node Gatekeeper Properties window shown in Figure 278 on page 554. This window enables the administrator to link an IP Trunk 3.0 (or later) endpoint to an NRS

(Gatekeeper) zone (automatically providing Primary and Alternate NRSs). This window is also used to manually provision an NRS (Gatekeeper) for the node. Figure 279 on page 555 shows the options in the **Gatekeeper Option** drop-down list. Figure 280 on page 555 shows the options in the **Primary Gatekeeper Type** drop-down list.

Refer to *Optivity Telephony Manager: System Administration* (553-3001-330) for information on how to configure the IP Trunk 3.0 (or later) options.

Figure 278
Gatekeeper Properties window



ITG Node Gatekeeper Properties - Sample Site - Sample Meridian 1 - Customer 0 - Node 1

Gatekeeper Option: Use Gatekeeper Zone from OTM Navigator

Gatekeeper Zone: Sample Zone

H323-ID:

☑ Gatekeeper registration includes all ITG card IP addresses within the node

Primary Gatekeeper

Address: 47 . 11 . 30 . 1

Type: Communication Server 10(

Name: GK

Contact: Joe Smith 416-2221234

Location: Toronto

Alternate Gatekeeper

Address: 47 . 11 . 30 . 2

Type: Communication Server 10(

Name: NRS

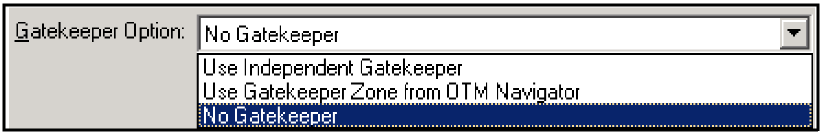
Contact: jsp@MyCompany.com

Location: New York

Last Modified:

Sync Status:

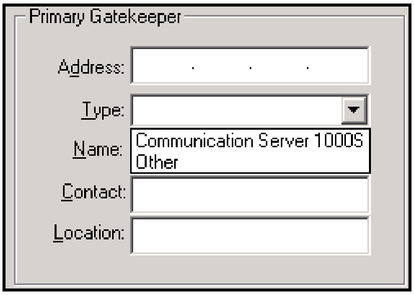
Figure 279
Options in the Gatekeeper Option drop-down list



Gatekeeper Option: No Gatekeeper

Use Independent Gatekeeper
Use Gatekeeper Zone from OTM Navigator
No Gatekeeper

Figure 280
Options in the Primary Gatekeeper's Type drop-down list



If configured appropriately, the IP Trunk 3.0 (or later) node uses Registration, Admission, and Status signaling (RAS) messaging to register with the NRS. The IP Trunk 3.0 (or later) node then processes calls by scanning its DN information and routing unresolved calls to the NRS, using the Address Translation Protocol Module (ATPM).

The IP Trunk 3.0 (or later) node is subordinate to the NRS for all calls requiring the NRS. The IP Trunk 3.0 (or later) node:

1. registers with the NRS (H.323 Gatekeeper), according to H.323 protocol
2. requests admission
3. accepts the reply, according to H.323 protocol
4. proceeds to handle the call as required, based on the returned message

Note: IP Trunk 3.0 (or later) supports the Media Card 32-port trunk card and/or the ITG-P 24-port trunk card.

Refer to *IP Trunk: Description, Installation, and Operation* (553-3001-363) for information on how to install, configure, and operate IP Trunk 3.0 (or later) functions, as well as information on IP Trunk signaling support (for example, MCDN, non-call associated signaling, and ESN5).

Business Communications Manager Release 3.01 (or later)

IP Peer Networking Phase 2 interoperates with BCM Release 3.01 (or later). BCM has been enhanced with many additional MCDN features, including the following:

- Network Call Transfer
- Network Call Redirection Information
- Message Waiting Indication
- ISDN Call Connection Limitation
- Trunk Route Optimization
- Trunk Anti-Tromboning
- Camp-On
- Break-In

For interworking between BCM and a system running CS 1000 Release 4.0 (or later), upgrade the BCM to version 3.01 (or later) software.

A BCM endpoint is configured on the Gatekeeper in the same way that a CS 1000 endpoint is configured. Configure the following on the BCM so that the BCM system can interwork with the CS 1000 Release 4.0 (or later) system:

- Configure **Unified Manager: Services > IP telephony > IP Trunks > H.323 Trunks > Call Signaling** as **GatekeeperRouted** or **GatekeeperResolved**
- Configure **Unified Manager: Services > IP telephony > IP Trunks > H.323 Trunks > Gatekeeper IP** as the IP address of the NRS
- Configure **Unified Manager: Services > IP telephony > IP Trunks > H.323 Trunks > Alias Names** as the Alias name that was used when the H.323 Endpoint for the BCM was created on the NRS

> ***Note:*** When working with a BCM 50 system, the Unified Manager is called the BCM Element Manager.

In order to make a BCM 3.01 (or later)-to-CS 1000 call, ensure that the BCM routes and dialing plan (used to reach the CS 1000 systems) match the numbering plan entry assigned to the CS 1000 systems through NRS Manager.

Similarly, to make a CS 1000 system-to-BCM 3.01 call, ensure that the numbering plan entry assigned to the BCM (through NRS Manager) matches the dialing plan information configured on the CS 1000 systems.

Multimedia Communication Server 5100 (MCS 5100)

The SIP Trunk Gateway connects the CS 1000 systems to other Nortel or third-party SIP-enabled products. This direct SIP interface is used to interwork with products such as the MCS 5100. The MCS 5100 brings multimedia features to the CS 1000 system.

For detailed information about MCS 5100 and CS 1000 interworking, refer to *Multimedia Portfolio Communication (MCP) Interworking Basics NTP (NN10372-111)*.

Also refer to “Configuring the MCS 5100 system as a Collaborative Server” on page 564.

CallPilot 2.02

CallPilot integrates voicemail, e-mail, and fax messages into a single mailbox. These messages are accessible by telephone, e-mail client, or by any browser-enabled PC.

The SIP Converged Desktop Service (CDS) is a feature convergence of the MCS 5100 and CS 1000 systems. SIP CDS allows users to have simultaneous access to both multimedia features on MCS 5100 and voice features on CS 1000. The CS 1000 system can communicate with the MCS 5100 system by hosting a CallPilot 2.02 mailbox on the CS 1000 system. With SIP, a centralized CallPilot can provide services to a network of CS 1000 and MCS 5100 systems.

CallPilot behind CS 1000

Currently, the unified messaging support for stand-alone MCS 5100 users is provided by a dedicated CallPilot system connected directly to the MCS 5100 system, using a T1/SMDI over IP interface. It is also possible to send Message Waiting Indication (MWI) and call-redirection information to and from a CallPilot behind the CS 1000 system to stand-alone MCS 5100 users, through the SIP interface on the CS 1000 system.

With CallPilot behind CS 1000, all CS 1000 users receive CallPilot service through the existing interface. All MCS 5100 users receive unified messaging services through the SIP Trunk Gateway. For a Converged Desktop user, however, the MWI is sent only to the CS 1000 desktop and is not extended to the SIP client. At this time, the SIP client can get MWI using CallPilot Desktop Manager or My CallPilot (web messaging).

Message Waiting Indication handling

The SIP Trunk Gateway on the CS 1000 system provides MWI service for MCS 5100 remote users served by CallPilot. MCS 5100 users are provisioned on CallPilot, and they are not required to explicitly subscribe MWI service from the CS 1000 SIP Trunk Gateway. When a new message is left for an MCS 5100 user, the CS 1000 system sends an MCDN Facility message with MWI indication to the SIP Trunk Gateway. The message is translated into an unsolicited SIP NOTIFY message with a proper alias address and is sent to the MCS 5100 proxy for further processing. Only the MWI on/off indication is carried in the SIP NOTIFY message.

Subscription for MWI notification is implicit and persistent. The out-of-dialog NOTIFY is used to send MWI notification (that is, the NOTIFY creates its own dialog). The message-summary event package draft defines the structure of the NOTIFY (including its body content). The SIP Trunk Gateway translates the MCDN Facility message to an unsolicited SIP NOTIFY only if the RCAP on D-channel configuration has the MWI settings; otherwise, the SIP Trunk Gateway tunnels the MCDN message into a SIP INVITE message.

Call redirection

MCS 5100 users redirect the call to CallPilot using facilities between the CS 1000 and MCS 5100 systems. The redirecting number is required for the mailbox, and the redirection reason is required for the greeting. The implementation is based on SIP extension headers. In particular, the History header is used to convey the redirection reason (for example, no answer or busy) so that the proper greeting can be played by CallPilot.

CallPilot configuration

Note the following about the CallPilot configuration:

- MCS 5100 users are configured as users on a remote Network Management System (NMS)-node.
- Mailboxes are configured according to the selected numbering plan (UDP or CDP).

For detailed CallPilot configuration information, refer to the following CallPilot NTPs.

- *CallPilot Planning and Engineering Guide (553-7101-101)*
- *CallPilot Installation and Configuration Part 3: T1/SMDI and CallPilot Server Configuration (553-7101-224)*
- *CallPilot Administrator's Guide (553-7101-301)*

Collaboration between a CS 1000 Release 4.0 (or later) NRS and a Succession 3.0 H.323 Gatekeeper or MCS 5100

A CS 1000 Release 4.0 (or later) NRS is capable of interworking with a Succession 3.0 H.323 Gatekeeper to set up Gatekeeper zones. The Location Request message that is sent between the CS 1000 Release 4.0 (or later) NRS and the Succession 3.0 H.323 Gatekeeper is fully compatible between the two software releases.

> ***Note:*** Collaboration for CDP calls can only be achieved in the same Level 0 Domain (CDP).

As in Succession Release 3.0, there is no need to configure the terminating endpoint on the originating CS 1000 Release 4.0 (or later) NRS (this was only needed for Release 2.0 Gatekeepers).

The following sections provide details for configuring zones between a CS 1000 Release 4.0 (or later) NRS and a Succession Release 3.0 Gatekeeper:

- “Configuring the CS 1000 Release 4.0 (or later) NRS” on page 560
- “Configuring the Succession Release 3.0 Gatekeeper” on page 563
- “Configuring the MCS 5100 system as a Collaborative Server” on page 564

Configuring the CS 1000 Release 4.0 (or later) NRS

Procedure 77
Configuring the CS 1000 Release 4.0 (or later) NRS for collaboration with a Succession Release 3.0 Gatekeeper

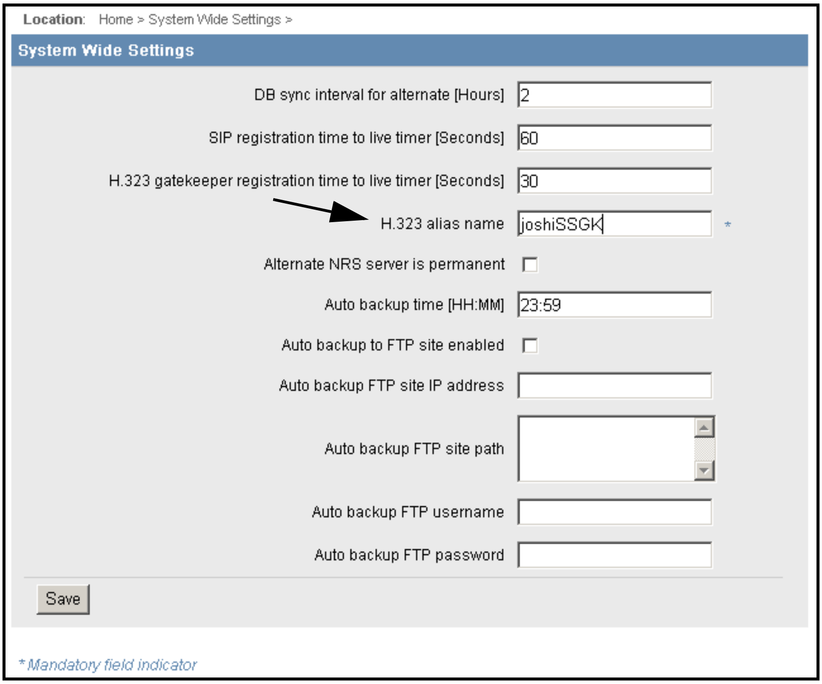
1 Log in to NRS Manager. See Procedure 28: “Logging in to NRS Manager using the browser address field” on page 394.

2 Select the **Home** tab.

3 Select **System Wide Settings**. For more information, refer to Procedure 31: “Configuring system-wide settings” on page 403.

4 Ensure that the **H.323 alias name** has been entered for the CS 1000 Release 4.0 (or later) NRS (see Figure 281 on page 561).

Figure 281
NRS System Wide Settings web page



Location: Home > System Wide Settings >

System Wide Settings

DB sync interval for alternate [Hours] 2

SIP registration time to live timer [Seconds] 60

H.323 gatekeeper registration time to live timer [Seconds] 30

H.323 alias name joshiSSGK *

Alternate NRS server is permanent □

Auto backup time [HH:MM] 23:59

Auto backup to FTP site enabled □

Auto backup FTP site IP address

Auto backup FTP site path

Auto backup FTP username

Auto backup FTP password

* Mandatory field indicator

5 Select the **Configuration** tab. Click **OK**.

A dialog box displays indicating the status of the active and standby database (see Figure 164 on page 412). Click **OK**.

6 Switch to **Standby DB view**.

7 Select **Collaborative Servers**.

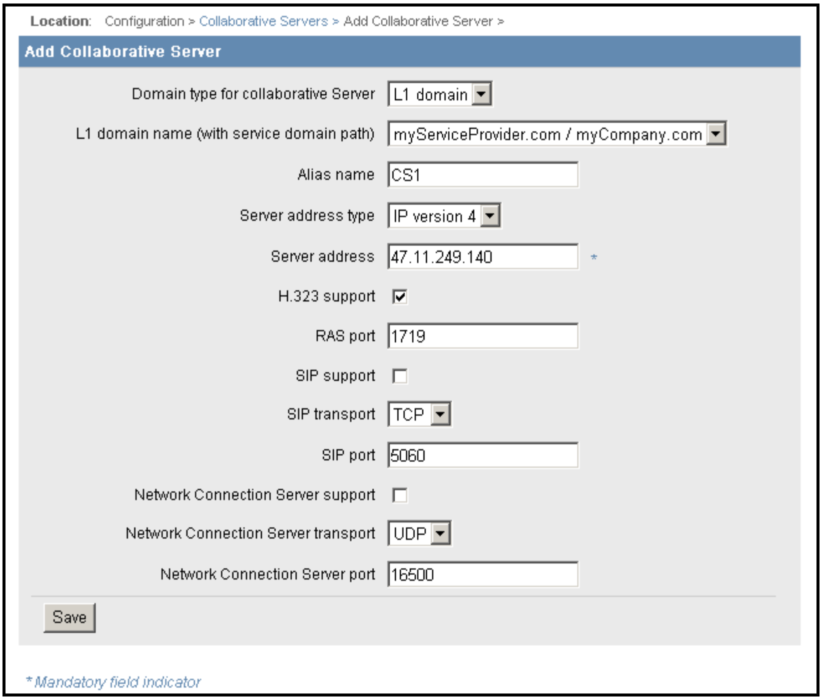
8 Click **Add**. See Figure 282 on page 562.

9 Configure the Succession Release 3.0 Gatekeeper as a collaborative Server. For more information, refer to Procedure 46: “Adding a Collaborative Server” on page 442.

Note 1: Ensure that the Succession Release 3.0 Gatekeeper is provisioned in the same Service Domain and Level 1 Domain (UDP) as the originating endpoint.

Note 2: Provision the Succession Release 3.0 Gatekeeper as a Level 1 Domain Gatekeeper to allow support for CDP interzone dialing for multiple zones. That is, if the Succession Release 3.0 Gatekeeper supports CDP Domain A and Domain B, then provisioning the Gatekeeper as a Level 1 Zone Collaborative Server allows the CS 1000 Release 4.0 (or later) NRS to send it calls from both zones A and B (depending on the CDP domain of the call originator on the CS 1000 Release 4.0 [or later] NRS zone).

Figure 282
Add Collaborative Servers web page



Location: Configuration > Collaborative Servers > Add Collaborative Server >

Add Collaborative Server

Domain type for collaborative Server	L1 domain
L1 domain name (with service domain path)	myServiceProvider.com / myCompany.com
Alias name	CS1
Server address type	IP version 4
Server address	47.11.249.140 *
H.323 support	☑
RAS port	1719
SIP support	□
SIP transport	TCP
SIP port	5060
Network Connection Server support	□
Network Connection Server transport	UDP
Network Connection Server port	16500

* Mandatory field indicator

10 Select the **Tools** tab.

11 Select **Database Actions**.

12 Use the **Commit** command if you are sure the configuration is correct. Otherwise, first use the **Cutover** command to test the configuration changes.

End of Procedure

Configuring the Succession Release 3.0 Gatekeeper

Procedure 78
Configuring the Succession Release 3.0 Gatekeeper

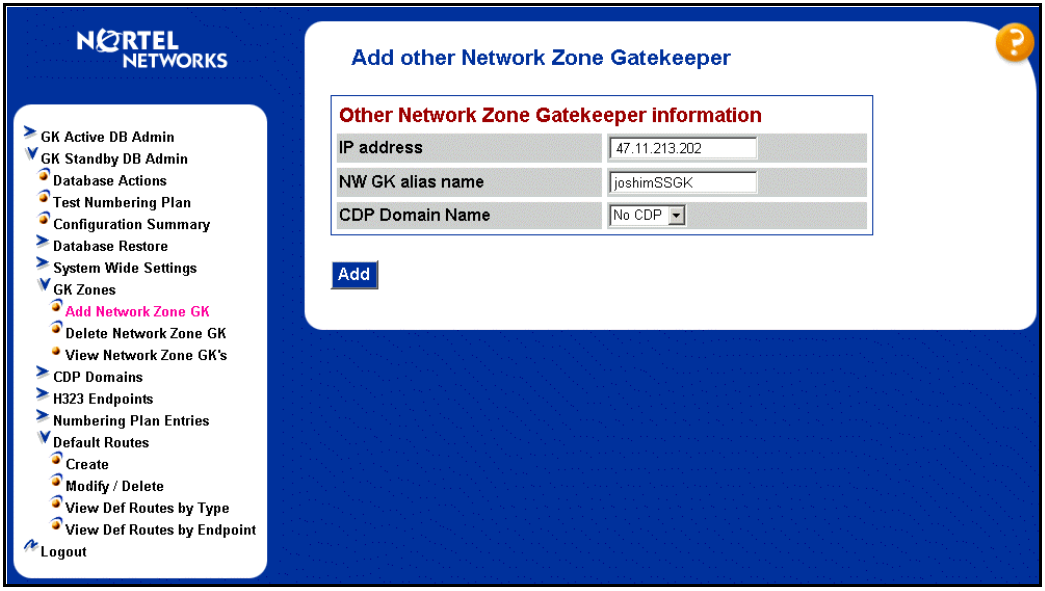
1 Log in to the **Gatekeeper** web pages in Element Manager (for Succession Release 3.0).

2 Select the **GK Standby DB Admin > GK Zones > Add Network Zone GK** link (see Figure 283).

3 Add the CS 1000 Release 4.0 (or later) NRS as a Network Zone Gatekeeper using the same Gatekeeper H.323 alias name as configured in step 4 on page 560.

Note: A Succession Release 3.0 Network Zone Gatekeeper is similar to a CS 1000 Release 4.0 (or later) Collaborative Server.

Figure 283
Add other Network Zone Gatekeeper



Add other Network Zone Gatekeeper

Other Network Zone Gatekeeper information

IP address	47.11.213.202
NW GK alias name	joshimSSGK
CDP Domain Name	No CDP

4 Select the **GK Standby Database Admin > Database Actions** link.

5 Click the **SingleStepCutoverCommit** command once you are sure that the configuration is correct. Otherwise, first use the **Cutover** command to test the configuration.

End of Procedure

Configuring the MCS 5100 system as a Collaborative Server

The MCS 5100 can be configured as a collaborative server which supports H.323 and SIP.

The configuration for H.323 is the same as configuring another Succession Release 3.0 Gatekeeper with the limitation that MCS 5100 can only be configured as a Level 0 Domain Collaborative Server. The MCS 5100 cannot parse the H.323 LRQ messages which specify a Level 0 Domain on a per-call basis. So it always routes the call to a fixed Level 0 Domain. So in this case, it is only the MCS 5100 H.323 alias name (which is configured as the Collaborative Server Gatekeeper alias name) and IP address that is relevant.

For SIP calls, the MCS 5100 can be configured as a Level 1 or Level 0 Domain Collaborative Server. The Service Domain on the NRS should match the Service Domain on the MCS 5100. A Level 1 Domain is preferred, so the MCS 5100 can be used for calls originating from multiple Level 0 Domains without restriction.

Maintenance

Contents

This section contains information on the following topics:

Command Line Interface commands

The Signaling Server provides a Command Line Interface (CLI) through a serial port or a Telnet session. This section contains the CLI commands available at that interface that are applicable to IP Peer Networking.

Signaling Server CLI commands are available at three levels:

- Level One — Operations, Administration, and Maintenance (OAM) shell for basic technician support and general status system checking (**`oam>prompt`**)
- Level Two — Problem Determination Tool (PDT) shell for expert support; also includes all Level One (OAM) commands (**`pdt>prompt`**)
- Level Three — Nortel proprietary vxWorks™ shell for advanced debugging and design support (**`prompt`**)

  Note: This section describes the Level One (OAM) and Level Two (PDT) CLI commands. Level Three commands are considered expert support and design level commands, and are not documented here.

You must log in to the Signaling Server to use the CLI commands. Refer to *Signaling Server: Installation and Configuration* (553-3001-212) for this procedure.

Help CLI commands

Table 35 includes the general help CLI commands. These commands are available only at the OAM and PDT shells.

Table 35
Help CLI commands

CLI Command	Description
help	Lists all command groups available at current shell level.
help <command>	Provides Help text on a particular command.

Virtual Trunk CLI commands

Table 36 includes the CLI commands used when working with Virtual Trunks.

Table 36
Virtual Trunk CLI commands

CLI Command	Description
help vtrk	Lists all Virtual Trunk-related commands (for example, vtrkShow). This help command is available at the OAM and PDT shells. ***Note:*** The Virtual Trunk group includes both H.323 and SIP Virtual Trunk commands.
vtrkShow <protocol>, <start#>, <howMany>	Provides a summary of the Virtual Trunk configuration of a particular protocol. Where: • protocol is either SIP or H.323. If the protocol parameter is omitted, then the command prints a summary of both the H.323 and SIP trunks. Otherwise, the command prints the specified protocol. • start# specifies that the printing starts from specified channel ID. If the start# parameter is omitted, then the command starts from the first channel of specific protocol. • howMany specifies the number of channels to be printed. If the howMany parameter is omitted, then the command prints all channels for specified protocol starting from the start#.

D-channel CLI command

Table 37 includes D-channel CLI commands.

Table 37
D-channel CLI commands

CLI Command	Description
DCHmenu	Displays a menu to perform various information retrieval operations for the D-channel. The output for DCHmenu: oam->DCHmenu Please select one of the DCHmenu options: 0 - Print menu (default) 1 - Print current DCH state 2 - Print current DCH configuration 3 - Print application error log 4 - Print link error log 5 - Print protocol error log 6 - Print message log 7 - Enable printing all messages processed by UIPC 8 - Enable error printing 9 - Enable info printing 10 - Enter manual message mode 11 - Print b channel control blocks 99 - Exit menu Please enter your DCHmenu choice (0 to print the menu): 1

H323GwShow CLI commands

Table 38 includes the H323GwShow trace tool CLI commands applicable to the Signaling Server. The commands are issued from the OAM shell.

Table 38
H323GwShow trace tool CLI commands (Part 1 of 2)

CLI Command	Description
H323GwShow	Provides a general summary of the H.323 Virtual Trunk settings.
H323GwShow ch <channel #>	Provides a snapshot summary of the state of the H.323 Virtual Trunk setting and a snapshot of the active call on the specified channel (if the call exists). Where channel # indicates the channel number to trace. The values range from 0 - maximum channel number.
H323GwShow num <calling/called number>	Provides a snapshot summary of the state of the H.323 Virtual Trunk settings and a snapshot of the active calls using the calling/ called number or partial number specified. Where calling/called number indicates the telephone number to trace. The value can be a number from 1 to 32 digits and can be a partial calling/called number.

Table 38
H323GwShow trace tool CLI commands (Part 2 of 2)

CLI Command	Description
H323GwShow num <calling/called number> <NPI> <TON>	Provides a snapshot summary of the state of the H.323 Virtual Trunk settings. It also provides a snapshot of the active calls using the calling/called number or partial number with the specified NPI and TON values. Where: • calling/called number indicates the telephone number to trace. The value can be a number from 1 to 32 digits and can be a partial calling/called number. • NPI specifies the numbering plan identifier for the calls. The calls using this numbering plan are to be traced. The values are: 0 - ALL 1 - Unknown 2 - ISDN/telephony numbering plan (E.164) 4 - E.163 5 - Telex numbering plan (F.69) 6 - Data numbering plan 7 - National standard numbering plan • TON specifies the type of number to use as a filter for tracing. Only calls using this TON setting are traced. The values are: 0 - ALL 1 - Unknown Number 2 - International Number 3 - National Number 4 - Network Specific Number 5 - Subscriber Number 6 - Level 1 Regional 7 - Level 0 Interface
help H323GwShow	Displays the usage of the H323GwShow commands.

SIPGwShow CLI commands

Table 38 includes the SIPGwShow trace tool CLI commands applicable to the Signaling Server. The commands are issued from the OAM shell.

Table 39
SIPGwShow trace tool CLI commands (Part 1 of 2)

CLI Command	Description
SIPGwShow	Shows the general SIP Virtual Trunk settings.
SIPGwShow ch <channel #>	Provides a snapshot summary of the SIP Virtual Trunk configuration for the specific channel ID. The command also provides a snapshot of the active call on the specified channel (if the call exists). The channel # indicates the channel number to trace. The values range from 0 - maximum channel number.
SIPGwShow num <calling/called number>	Provides a snapshot summary of the SIP Virtual Trunk configuration for the specific calling-party or called-party number. The command also provides a snapshot of the active calls using the calling-party/called-party number or partial number specified. The calling/called number indicates the telephone number to trace. The value can be a number from 1 to 32 digits and can be a partial calling/called number.

Table 39
SIPGwShow trace tool CLI commands (Part 2 of 2)

CLI Command	Description
SIPGwShow num <calling/called number> <NPI> <TON>	Provides a snapshot summary of the SIP Virtual Trunk configuration. The command also provides a snapshot of the active calls using the calling/called number or partial number with the specified NPI and TON values. Where: • calling/called number indicates the telephone number to trace. The value can be a number from 1 to 32 digits and can be a partial calling/called number. • NPI specifies the numbering plan identifier for the calls to be traced. The values are: 0 - ALL 1 - Unknown 2 - ISDN/telephony numbering plan (E.164) 4 - E.163 5 - Telex numbering plan (F.69) 6 - Data numbering plan 7 - National standard numbering plan • TON specifies the type of number to use as a filter for tracing. Only calls using this TON setting are traced. The values are: 0 - ALL 1 - Unknown Number 2 - International Number 3 - National Number 4 - Network Specific Number 5 - Subscriber Number 6 - Level 1 Regional 7 - Level 0 Interface
help SIPGwShow	Displays the usage of the SIPGwShow commands.

Graceful disable CLI commands

Table 40 includes graceful disable CLI commands applicable to the Signaling Server. They are issued from the OAM shell.

Table 40
Graceful Disable commands (Part 1 of 2)

CLI Command	Description
disServices	Causes the server to gracefully switch all registered resources (including telephone, Virtual Trunk, and Voice Gateways) to the other services (Signaling Server or Voice Gateway Media Card) in the same node. This command should not interrupt existing calls.
disTPS	Causes the line TPS to gracefully switch the registered telephones to the other cards located in the same node.
disVTRK	Causes the Virtual Trunk to gracefully switch the registered Virtual Trunks to other Signaling Servers located in the same node. ***Note:*** LTPS and VTRK functions must be enabled on a Signaling Server located in the same node to accept VTRK registrations. The number of VTRK resources available must be equal to or greater than the number of VTRK resources being switched over.
forcedisServices	Forces the server to switch all registered resources to another Signaling Server or Voice Gateway Media Card in the same node. This command causes any existing calls to be dropped.
forcedisTPS	Forces all registered line LTPS to unregister from the local server.
forcedisVTRK	Forces all registered Virtual Trunks to unregister from the local server.
enlServices	Causes all the services to accept registration of resources.
enlTPS	Causes line TPS application to be enabled and to accept set registrations.

Table 40
Graceful Disable commands (Part 2 of 2)

CLI Command	Description
enlVTRK	Causes the Virtual Trunk application to be enabled and to accept Virtual Trunk registrations.
loadBalance	Causes the service to attempt to balance the registration load of sets between this service and the rest of the node services.
servicesStatusShow	Shows the status of services (tps/iset/vtrk/gk)
soHelpMenu	Displays all the commands that can be used for Services Switch-Over.

Trace tools CLI commands

The following section outlines the CLI commands for the message trace tools.

- Table 41 on page 577 shows the general trace tool commands.
- Table 42 on page 578 shows the Gatekeeper protocol trace tool commands.
- Table 43 on page 584 shows the SIP trace tool commands.
- Table 44 on page 590 shows the H.323 trace tool commands.
- Table 45 on page 594 shows the Network Connection Service (NCS) trace tool commands

Note: A warm boot of the system causes all tracing to cease. Traces must be re-entered after the system has restarted.

General trace tool commands

Table 41 on page 577 includes the general trace tool CLI commands applicable to the Signaling Server and the Voice Gateway Media Cards. The commands are issued from the OAM shell of the Signaling Server and the LTPS prompt of the Voice Gateway Media Cards.

Table 41
General trace tool CLI commands

CLI Command	Description
traceShow	Displays the names of active traces in the system.
traceAllOff	Causes all traces that use the monitorLib server to stop their output.
tracePrintOff	Blocks all logging of information received by the monitorLib service to the TTY output. This does not include traces directed through the monitorLib service to the RPT.LOG or SYSLOG.n services.
traceFileOff	Causes the monitorLib server to stop logging to the log files any and all trace information received by the service. The log files include syslog.n for the Voice Gateway Media Card and rpt.log for the Signaling Server.
traceAllOn	Clears the blocking of all trace information imposed on the monitorLib service by the traceAllOff command, the tracePrintOff command, and the traceFileOff command. By default, all tracing is on.
tracePrintOn	Clears only the TTY output blocking that was imposed by the traceAllOff and tracePrintOff commands.
traceFileOn	Clears only the blocking of logging to files that was imposed by the traceAllOff and traceFileOff commands.

Note 1: A warm boot of the system causes all tracing to cease. Traces must be re-entered after the system has restarted.

Note 2: If no directory path is supplied with the filename specified, then the file is written to the C:/U/trace directory on the Voice Gateway Media Cards and to the /u/trace directory on the Signaling Server.

Note 3: If no filename is given, then no trace file is generated and output is directed to the TTY. If the filename does not meet the DOS 8.3 restriction, then the filename is rejected and no file is generated. If the file is deleted, cannot be found, or has a write error, then the output is directed to the TTY.

Note 4: If the output for the trace cannot be determined, then the output is directed to the TTY.

Gatekeeper protocol trace tool commands

Table 42 includes the protocol trace tool CLI commands for the Gatekeeper. These commands are issued from the OAM shell.

Table 42
Gatekeeper protocol trace tool CLI commands (Part 1 of 6)

CLI Command	Description
gkDiscoveryTrace ID <"Alias Name"> IP <"IP address"> ALL	The trace outputs the GRQ, GCF, and GRJ messages for the specified endpoint. Where: • Alias Name is the H.323 ID string. • IP address is the endpoint's IP address. • ALL causes a trace on all endpoints.
gkRegTrace ID <"Alias Name"> IP <"IP address"> ALL	The trace outputs the RRQ, RCF, RRJ, URQ, UCF, and URJ messages for the specified endpoint. Where: • Alias Name is the H.323 ID string. • IP address is the endpoint's IP address. • ALL causes a trace on all endpoints.

Table 42
Gatekeeper protocol trace tool CLI commands (Part 2 of 6)

CLI Command	Description
gkCallTrace ID <“Alias Name”> IP <“IP address”> NUM <calling/called Number> NUM <calling/called Number> <NPI> <TON> ALL	The trace outputs the ARQ, ACF, ARJ, LRQ, LCF, LRJ, BRQ, BCF, BRJ, DRQ, DCF, and DRJ messages for the specified endpoint. Where: • Alias Name is the H.323 ID string. • IP address specifies the endpoint’s IP address. • calling/called number indicates the telephone number to trace. The value can be a number from 1 to 32 digits and can be a partial calling/called number. • NPI - Specifies the numbering plan identifier for which calls using this numbering plan are to be traced. The values are: 0 - ALL 1 - Unknown 2 - ISDN/telephony numbering plan (E.164) 4 - E.163 5 - Telex numbering plan (F.69) 6 - Data numbering plan 7 - National standard numbering plan • TON - specifies the type of number to use as a filter for tracing. Only calls using this TON setting are traced. The values are: 0 - ALL 1 - Unknown Number 2 - International Number 3 - National Number 4 - Network Specific Number 5 - Subscriber Number 6 - Level 1 Regional 7 - Level 0 Interface • ALL - Causes a trace on all endpoints ***Note:*** A maximum of ten number traces are allowed.

Table 42
Gatekeeper protocol trace tool CLI commands (Part 3 of 6)

CLI Command	Description
gkProtocolTrace ID <“Alias Name”> <“protocol”> IP <“IP address”> <“protocol”> NUM <calling/called Number> <“protocol”> NUM <calling/called Number> <NPI> <TON> <“protocol”> ALL <protocol>	Traces messages for the specified endpoint. Where: • Alias Name is the H.323 ID string. • IP address specifies the endpoint’s IP address. • calling/called number indicates the telephone number to trace. The value can be a number from 1 to 32 digits and can be a partial calling/called number. • NPI specifies the numbering plan identifier for which calls using this numbering plan are to be traced. The values are: 0 - ALL 1 - Unknown 2 - ISDN/telephony numbering plan (E.164) 4 - E.163 5 - Telex numbering plan (F.69) 6 - Data numbering plan 7 - National standard numbering plan

Table 42
Gatekeeper protocol trace tool CLI commands (Part 4 of 6)

CLI Command	Description
	• TON - specifies the type of number to use as a filter for tracing. Only calls using this TON setting are traced. The values are: 0 - ALL 1 - Unknown Number 2 - International Number 3 - National Number 4 - Network Specific Number 5 - Subscriber Number 6 - Level 1 Regional 7 - Level 0 Interface • ALL causes a trace on all endpoints • protocol - specifies which protocols to trace. (1) Valid protocol types for IP and ALL tracing — individually: ALL, ARQ, ACF, ARJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, GRQ, GCF, GRJ, LRQ, LCF, LRJ, NSM, RRQ, RCF, RRJ, RIP, URQ, UCF, AND URJ are acceptable inputs. — by category: AXX – ARQ, ACF, ARJ BXX – BRQ, BCF, BRJ DXX – DRQ, DCF, DRJ GXX – GRQ, GCF, GRJ LXX – LRQ, LCF, LRJ RXX – RRQ, RCF, RRJ UXX – URQ, UCF, URJ

Table 42
Gatekeeper protocol trace tool CLI commands (Part 5 of 6)

CLI Command	Description
	(2) Valid protocols for NUM tracing — Individually: ALL, ARQ, ACF, ARJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ,LRQ, LCF, LRJ — by category: AXX – ARQ, ACF, ARJ BXX – BRQ, BCF, BRJ DXX – DRQ, DCF, DRJ LXX – LRQ, LCF, LRJ (3) Protocols that cannot be traced by any endpoint: — IACK, INAC, IRQ, IRR, RAI, RAC, SCI, SCR, XRS To trace multiple protocols, separate the input with a space (for example, “ARQ ACF ARJ”). ***Note:*** A maximum of ten number traces are allowed.
gkTraceOff IP <“IP address”> ALL	Turns off the trace for the specified endpoint.

Table 42
Gatekeeper protocol trace tool CLI commands (Part 6 of 6)

CLI Command	Description
gkTraceOutput <Output_Destination> <"File Pathname">	Sets the output for all gk protocol traces. Where: • Output_Destination specifies where all the trace messages for the gkTrace are to be directed. Values are: 1 = TTY 2 = RPTLOG 3 = File 4 = File and TTY • "File Pathname" is a string encapsulated in quotes. It specifies the file to output to if option 3 or 4 was selected
gkTraceSettings	Displays all endpoints that are being traced. The command also displays the location where the output is sent (TTY, RPT.LOG, or a file and the file's location).
gkTraceTblClear	Clears the calling/called number table associated with the NUM trace filter(s). A maximum of 200 tables entries are allowed. If there are more than 200 table entries, the system displays the following error: gkTrace callIdentifier table is full Clearing the table is a temporary solution. Better options may include: • refining the NUM trace filter to be more exact • reducing the number of NUM trace filters • running the trace during lower traffic periods
gkTraceTblShow	Displays the calling/called number table associated with the NUM trace filter(s). Some entries may be shown twice, since intrazone calls generate two ARQ messages. Interzone calls generate only one ARQ message.

Note: A warm boot of the system causes all tracing to cease. Traces must be re-entered after the system restarts.

SIPCallTrace trace tool commands

Table 43 includes the SIPCallTrace trace tool CLI commands applicable to the Signaling Server. They are issued from the OAM shell.

Table 43
SIPCallTrace trace tool CLI commands (Part 1 of 5)

CLI Command	Description
SIPCallTrace on	Turns on SIP Virtual Trunk tracing for all channels.
SIPCallTrace off	Turns off SIP Virtual Trunk tracing for all channels.
SIPTraceLevel <Output Option>	Sets the SIPCallTrace output to Summary or Detailed format. The Summary format provides only information normally displayed by the SIPCallTrace command. The Detailed format provides a more detailed output of the SIP signaling messages associated with the traces that are set using the SIPCallTrace utility. Output Option specifies the level of the SIP Message Trace. The values are: 0 = SIP Message Trace – Summary (default) 1 = SIP Message Trace – Detailed See Figure 284 on page 589 for an example of SIPCallTrace in Summary format. See Figure 285 on page 589 for an example of SIPCallTrace in Detailed format.
help SIPTraceLevel	Displays the usage for the SIPTraceLevel CLI command.
SIPCallTrace <MsgRecv> <MsgSend>	Allows tracing of all SIP channels in the receiving and/or sending directions. Where: • MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF. • MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.

Table 43
SIPCallTrace trace tool CLI commands (Part 2 of 5)

CLI Command	Description
SIPCallTrace ch <channel #> <MsgRecv> <MsgSend>	Allows tracing of a specified SIP channel in the receiving and/or sending directions. Where: • channel # indicates the channel number to trace. The values range from 0 - maximum channel number. • MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF. • MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.
SIPCallTrace num <calling/called number> <MsgRecv> <MsgSend>	Allows the tracing of SIP messages using the called and calling numbers in the receiving and/or sending directions. If the called or calling number of a SIP Virtual Trunk session matches the number specified, then the messages to and from the Virtual Trunk are traced. Where: • calling/called number indicates the telephone number to trace on. The number can be from 1 to 32 numeric digits and can be a partial calling/called number. • MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF. • MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.

Table 43
SIPCallTrace trace tool CLI commands (Part 3 of 5)

CLI Command	Description
SIPCallTrace ch <beginning channel #> <ending channel #> <MsgRecv> <MsgSend>	Allows the tracing of a range of SIP Virtual Trunk channels in the receiving and/or sending directions. Where: • beginning channel # indicates the channel number to trace. The values range from 0 - maximum channel number. • ending channel # indicates the channel number to trace. The values range from 0 - maximum channel number, but must be greater than the beginning channel #. • MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF. • MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.

Table 43
SIPCallTrace trace tool CLI commands (Part 4 of 5)

CLI Command	Description
SIPCallTrace num <calling/called number> <NPI> <TON> <MsgRecv > <MsgSend>	Allows a user to trace SIP messages using the called and calling numbers in the receiving and/or sending directions. If the called or calling number of a SIP Virtual Trunk session matches the number specified and the specified NPI and TON values match the call type, then the messages to and from the SIP Virtual Trunk are traced. Where: • calling/called number indicates the telephone number to trace on. The number can be from 1 to 32 numeric digits and can be a partial calling/called number. • NPI specifies the numbering plan identifier for which calls using this numbering plan are to be traced. The values are: 0 - ALL 1 - Unknown 2 - ISDN/telephony numbering plan (E.164) 4 - E.163 5 - Telex numbering plan (F.69) 6 - Data numbering plan 7 - National standard numbering plan • TON - specifies the type of number to use as a filter for tracing. Only calls using this TON setting are traced. The values are: 0 - ALL 1 - Unknown Number 2 - International Number 3 - National Number 4 - Network Specific Number 5 - Subscriber Number 6 - Level 1 Regional 7 - Level 0 Interface

Table 43
SIPCallTrace trace tool CLI commands (Part 5 of 5)

CLI Command	Description
	• MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF. • MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.
help SIPCallTrace	Provides a description of the SIPCallTrace commands. It also supplies parameters and possible parameter values for each command. The command also supplies a list of associated CLIs (that is, SIPTraceShow and SIPOutput).
SIPOutput <Output_Destination> <“File Pathname”>	Specifies where the output for the trace tool is to be directed. Where: • Output_Destination specifies where all the trace messages for the SIPCallTrace are to be directed. The values are: 1 = TTY 2 = RPTLOG 3 = File 4 = File+TTY • “File Pathname” is a string encapsulated in quotes. The file pathname must be specified if option 3 (File) was selected as the output destination.
help SIPOutput	Displays the usage for the SIPOutput CLI command.
SIPTraceShow	Displays the SIP trace settings, including the output format, output destination and filename, as well as all active traces for the SIPCallTrace trace tool.
help SIPTraceShow	Displays the usage for the SIPTraceShow CLI command.

Figure 284 on page 589 shows an example of SIPCallTrace results in Summary format. Figure 285 on page 589 shows an example of SIPCallTrace results in Detailed format.

Figure 284
SIPCallTrace output example (INVITE message only) — Summary format

```
03/03/05 09:40:02 LOG0006 SIPNPM: SIPCallTrace: 3/3/5 9:40:2 Send chid:128
ip:47.17.153.212:5060 SIP method INVITE(0)
```

Figure 285
SIPCallTrace output example (INVITE message only) — Detailed format (Part 1 of 2)

```
03/03/05 09:44:04 LOG0006 SIPNPM: -> INVITE
sip:7405;phone-context=cdp_3S.udp_BL60Lab@NPI.com;transport=udp;user=phone SIP/2.0

03/03/05 09:44:04 LOG0006 SIPNPM: -> From:
<sip:5200;phone-context=cdp_3S.udp_BL60Lab@NPI.com;user=phone>;tag=f29911

03/03/05 09:44:04 LOG0006 SIPNPM: ->> 2d08-5ee8

03/03/05 09:44:04 LOG0006 SIPNPM: -> To:
<sip:7405;phone-context=cdp_3S.udp_BL60Lab@NPI.com;user=phone>

03/03/05 09:44:04 LOG0006 SIPNPM: -> Call-ID:
104ed414-f299112f-13c4-4226dc64-6d572d08-13da@NPI.com

03/03/05 09:44:04 LOG0006 SIPNPM: -> CSeq: 1 INVITE

03/03/05 09:44:04 LOG0006 SIPNPM: -> Via: SIP/2.0/UDP 47.17.153.
212:5060;branch=z9hG4bK-4226dc64-6d572d08-4901

03/03/05 09:44:04 LOG0006 SIPNPM: -> Max-Forwards: 70

03/03/05 09:44:04 LOG0006 SIPNPM: -> User-Agent: Nortel CS1000 SIP GW: release=4.0
version=sse-4.00.31

03/03/05 09:44:04 LOG0006 SIPNPM: -> P-Asserted-Identity:
<sip:5200;phone-context=cdp_3S.udp_BL60Lab@NPI.com;user=phone>

…

03/03/05 09:44:04 LOG0006 SIPNPM: -> --unique-boundary-1

03/03/05 09:44:04 LOG0006 SIPNPM: -> Content-Type: application/SDP

03/03/05 09:44:04 LOG0006 SIPNPM: -> o=- 48 1 IN IP4 47.17.153. 212

03/03/05 09:44:04 LOG0006 SIPNPM: -> s=-
```

Figure 285
SIPCallTrace output example (INVITE message only) — Detailed format (Part 2 of 2)

```
03/03/05 09:44:04 LOG0006 SIPNPM: -> t=0 0

03/03/05 09:44:04 LOG0006 SIPNPM: -> m=audio 5200 RTP/AVP 0 8 18
```

H.323CallTrace trace tool commands

Table 44 includes the H.323 trace tool CLI commands applicable to the Signaling Server. They are issued from the OAM shell.

Table 44
H.323CallTrace trace tool CLI commands (Part 1 of 4)

CLI Command	Description
H323CallTrace ch <channel #> <MsgRecv> <MsgSend>	Traces a specified channel. Where: • channel # indicates the channel number to trace. Values range from 0 - maximum channel number. • MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF. • MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF. ***Note:*** Replaces the H323CallTrace <channel #> <MsgRecv > <MsgSend> command.

Table 44
H.323CallTrace trace tool CLI commands (Part 2 of 4)

CLI Command	Description
H323CallTrace num <calling/called number> <MsgRecv> <MsgSend>	Traces H.323 messages using the called and calling numbers. If the calling/called number of a Virtual Trunk session matches the number specified, then the messages to and from the Virtual Trunk are traced. Where: • calling/called number indicates the telephone number to trace on. The value can be a number from 1 to 32 digits and can be a partial calling/called number. • MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF. • MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.
H323CallTrace ch <beginning channel #> <ending channel #> <MsgRecv> <MsgSend>	Traces a range of Virtual Trunk channels. Where: • beginning channel # indicates the channel number to trace. The values range from 0 - maximum channel number. • ending channel # indicates the channel number to trace. The values range from 0 - maximum channel number, but must be greater than the beginning channel number. • MsgRecv specifies if the messages sent to the designated channel should be traced. The values are ON or OFF. • MsgSend specifies if the messages sent from the designated channel should be traced. The values are ON or OFF. ***Note:*** Replaces the H323CallTrace <beginning channel #> <ending channel #> <MsgRecv> <MsgSend> command.

Table 44
H.323CallTrace trace tool CLI commands (Part 3 of 4)

CLI Command	Description
H323CallTrace num <calling/called number> <NPI> <TON> <MsgRecv> <MsgSend>	Traces H.323 messages using the calling or called number. If the calling/called number of a Virtual Trunk session matches the number specified, and the specified NPI and TON values match the call type, then the messages to and from the Virtual Trunk are traced. Where: • calling/called number indicates the telephone number to trace on. The value can be a number from 1 to 32 digits. • NPI specifies the numbering plan identifier for which calls using this numbering plan are to be traced. The values are: 0 - ALL 1 - Unknown 2 - ISDN/telephony numbering plan (E.164) 4 - E.163 5 - Telex numbering plan (F.69) 6 - Data numbering plan 7 - National standard numbering plan • TON specifies the type of number to use as a filter for tracing. Only calls using this TON setting are traced. Values are: 0 - ALL 1 - Unknown Number 2 - International Number 3 - National Number 4 - Network Specific Number 5 - Subscriber Number 6 - Level 1 Regional 7 - Level 0 Interface

Table 44
H.323CallTrace trace tool CLI commands (Part 4 of 4)

CLI Command	Description
	• MsgRecv specifies if the messages sent to the designated channel should be traced. The values are ON or OFF. • MsgSend specifies if the messages sent from the designated channel should be traced. The values are ON or OFF.
help H323CallTrace	Describes the H323CallTrace commands. It supplies each command's parameters and possible parameter values. The command also supplies a list of associated CLIs (that is, H323TraceShow and H3232Output).
H323Output <Output_Destination> <File Pathname>	Specifies where the output for the trace tool is to be directed. Where: • Output_Destination specifies where all the trace messages for H323CallTrace are to be directed.The values are: 1 = TTY 2 = RPTLOG 3 = File 4 = File and TTY • File Pathname specifies the file to output to if option 3 or 4 is selected.
H323TraceShow	Displays the trace settings, including the output destination and filename, as well as all active traces for the H323CallTrace trace tool.

Network Connection Service trace tool commands

Table 45 includes the protocol trace tool CLI commands for the Network Connection Service (NCS) applicable to the Signaling Server and the Voice Gateway Media Cards. They are issued from the OAM shell.

Table 45
NCS CLI commands (Part 1 of 2)

CLI command	Description
tpsARTrace IP <IP address> ID <user ID> ALL	Allows tracing of the tpsAR protocol, which is used to determine where an IP Phone should register. Where: • IP address - a string containing the IP Phone's IP address • user UID - the ID of the IP Phone to be traced (the DN used to log in) or the H323_Alias of where the IP Phone is trying to register • ALL - all IP Phones are to be monitored
tpsARTraceOff IP <IP address> ID <user ID> ALL	Removes the specified endpoint from the list of endpoints to be traced.
tpsARTraceAllOff	Turns off the trace for all tpsAR trace identifiers.

Table 45
NCS CLI commands (Part 2 of 2)

CLI command	**Description**
tpsAROutput <Output_Destination> <“File Pathname”	Sets the output for all tpsAR protocol traces. Where: • Output_Destination specifies where all the trace messages for the tpsARTraceSet are to be directed and whether the command is run from the Voice Gateway Media Card or the vxWorks shell prompt. The values are: 1 = TTY 2 = RPTLOG 3 = File 4 =TTY + File If the command is run from the OAM prompt or PDT prompt on the Signaling Server, then the values are the actual word, not a number: TTY RPTLOG FILE TTY+FILE • “File Pathname” is a string encapsulated in quotes. It specifies the file to output to if option 3 or 4 was selected.
tpsARTraceSettings	Displays the trace tool settings, which endpoints are being traced, and where the trace output is being directed.
tpsARTraceHelp	Displays a list of all CLIs used for tracing tpsAR protocol messages, including usage and parameters.

NRS database CLI commands

Table 46 includes the NRS CLI commands applicable to the Signaling Server. They are issued from the OAM shell.

Table 46
NRS database CLI commands — OAM shell

CLI command	Description
nrsGWEndpointShow	Lists all the NRS endpoints with corresponding IP addresses.
nrsUserEPShow	Lists all the NRS users with corresponding IP addresses.
nrsCollaboratingServerShow	Lists all the Collaborating Servers in the database.
nrsL0DomainShow	Lists all the Level 0 regional domains.
nrsL1DomainShow	Lists all the Level 1 regional domains.
nrsRoutingEntryShow	Lists all the Routing Entries in the database.
nrsServiceDomainsShow	Lists all the service provider domains.
nrsGWEndpointQuery	Queries an NRS endpoint with IP and protocol information.
nrsUserEPQuery	Queries an NRS endpoint with IP and protocol information.
nrsL0DomainQuery	Queries a Level 0 regional domain with E164 information.
nrsL1DomainQuery	Queries a Level 1 regional domain.
nrsServiceDomainQuery	Queries a service provider domain.
nrsCollaboratingServerQuery	Queries one Collaborating Server from the database.
nrsDefaultRouteQuery	Queries an NRS default route.
nrsDBShow	DIsplays the state of the Primary and Alternate NRS database and the local NRS database.
NrsOmmShow	Shows the SIP and H.323 NRS statistics for the current hour.
NrsOmmAvShow	Shows the SIP and H.323 NRS total statistics and average statistics for the last seven days.

Table 47 includes the NRS CLI commands applicable to the Signaling Server. These commands are applicable to the database. They are issued from the PDT shell.

Table 47
NRS database CLI commands — PDT shell

CLI command	Description
nrsDbCutover	Switches the active and standby database access pointer.
nrsDbCommit	Mirrors data from active schema to standby schema.
nrsDbCommitNow	Performs cutover and commit in one command.
nrsDbRollback	Undoes the changes.
nrsDbRevert	After the cutover, this command switches the active and standby database access pointer back.
disNRS	Gracefully disables the NRS server service. ***Note:*** This command should not interrupt the existing calls.
forcedisNRS	Forces the NRS server out-of-service.
enlNRS	Enables the SIP Redirect Server service.
nrsSIPTestQuery	Queries a SIP Routing Entry with DN and cost information.
nrsGKTestQuery	Queries an H.323 Routing Entry with DN and cost information.

Stand-alone NRS CLI commands

Table 46 lists CLI commands for an NRS running on a stand-alone Signaling Server. They are issued from the PDT shell.

Table 48
Stand-alone NRS CLI commands

CLI command	Description
adminUserPasswordChange [userID]	Changes the administrator-level user password for an NRS running on a stand-alone Signaling Server, where: • userID = userID of administrator-level user
adminUserCreate [userID]	Creates an administrator-level user of an NRS running on a stand-alone Signaling Server, where: • userID = userID of new administrator-level user
adminUserDelete [userID]	Deletes an administrator-level user of an NRS running on a stand-alone Signaling Server, where: • userID = userID of administrator-level user to be deleted
adminAccountShow	Displays the userID and access privileges for all users of an NRS running on a stand-alone Signaling Server.

ISDN to and from SIP mapping CLI commands

Table 49 shows the commands for mapping from ISDN to SIP, and Table 50 on page 600 shows the commands for mapping from SIP to ISDN. These commands are issued from the PDT prompt.

Table 49
ISDN-to-SIP commands

Command	**Description**
isdn2SipSet num1, num2	Changes the ISDN cause code to the SIP status code mapping. Where: • num1 is the ISDN cause code • num2 is the SIP status code
isdn2SipReset num	Resets a single ISDN cause code to the default SIP status code mapping. Where num is the ISDN cause code.
isdn2SipResetAll	Resets all the ISDN cause codes to the default SIP status code mappings.
isdn2SipShow num	Shows one specific ISDN cause code to SIP status code mapping.
isdn2SipShowAll	Shows all mappings from ISDN cause codes to SIP status codes.

Table 50
SIP-to-ISDN commands

Command	Description
sip2IsdnSet num1, num2	Changes the SIP status code to the ISDN cause code mapping. Where: • num1 is the SIP status code • num2 is the ISDN cause code
sip2IsdnReset num	Resets a single SIP status code to the default ISDN cause code mapping. Where num is the SIP status code.
sip2IsdnResetAll	Resets all SIP status codes to the default ISDN cause code mappings.
sip2IsdnShow num	Shows one specific SIP status code to ISDN cause code mapping. Where num is the ISDN cause code.
sip2IsdnShowAll	Shows all mappings from SIP status code to ISDN cause code.

Call Server commands

Manage Virtual Trunk route members

Use the commands in LD 32 to enable or disable Virtual Trunk route members, or to display information about route members.

LD 32 – Manage Virtual Route members.

Command	Description
DIS VTRM <cust #> <route #>	Disables all route members in a customer’s route. This command: • disconnects all active calls associated with the trunks • disables all route members on the Call Server • unregisters all trunks • removes them from the RLM table On the Signaling Server, all trunks are removed from the Signaling Server list.
ENL VTRM <cust #> <route #>	Enables all the route members (Virtual Trunks) This command: • enables all route members in a customer’s route • enables all route members • register the member • puts the members into the RLM table On the Signaling Server, all trunks are put on the Signaling Server list.
STAT VTRM <cust#> <rout#> start_mb# end_mb#	Displays the Virtual Trunk status specified by customer number, route number, and starting and ending member number. ***Note:*** Also see LD 32 — STAT VTRM commands on page 603 for additional usage of the STAT VTRM command.

Status commands

Use the STAT LINK and STAT SERV commands in LD 117 and the STAT VTRM command in LD 32 to display link information of connected services.

LD 117 — STAT LINK and STAT SERV commands

Command	Description
stat link ip <IP address>	Displays the link information and link status of the server with the specified IP address or contained specified subnet.
stat link srv ss	Displays the link information and link status of the Signaling Servers.
stat link name <hostname>	Displays the link information and link status of the server with the specified hostname.
stat link node <node ID>	Displays the link information and link status of the server with the specified node ID.
stat serv ip <IP address>	Displays the information of the server with the specified IP address or contained specified subnet.
stat serv app <applicationType>	Displays the information of the server running the specified application. Where application type can be: • LTPS (Line TPS) • VTRK (Virtual Trunk) • GK (Gatekeeper)
stat serv node <node ID>	Displays the information of the server with the specified node ID.
stip tn <tn>	Displays the IP information and status of the specified TN.
stip type ipti	Displays the IP information and status of all TNs that are of IPTI (Virtual Trunk and ITG Trunk) type.

LD 32 — STAT VTRM commands (Part 1 of 2)

STAT command	Description
STAT VTRM	Displays a status summary for all IP Peer Virtual Trunk routes associated with all customer numbers.
STAT VTRM <Cust>	Displays a status summary for all IP Peer Virtual Trunk routes associated with the customer number.
STAT VTRM <Cust> <Rout>	Displays a status summary for the specified IP Peer Virtual Trunk route.
STAT VTRM <Cust> <Rout> <Starting Member> <number of trunks>	Displays a status summary for the specified IP Peer Virtual Trunk route followed by a listing of Virtual Trunk TNs in the specified range.
STAT VTRM <Cust> SIP / H323	Displays a status summary for all IP Peer Virtual Trunk routes of the specified VoIP signaling protocol associated with the customer number.
STAT VTRM <Cust> <Rout> ALL	Displays a status summary for the specified IP Peer Virtual Trunk route followed by a listing of all Virtual Trunk TNs in the specified route.
STAT VTRM <Cust> <Rout> REG	Displays a status summary for the specified IP Peer Virtual Trunk route followed by a listing of registered Virtual Trunk TNs in the specified route.
STAT VTRM <Cust> <Rout> UNR	Displays a status summary for the specified IP Peer Virtual Trunk route followed by a listing of unregistered Virtual Trunk TNs in the specified route.
STAT VTRM <Cust> <Rout> BUSY	Displays a status summary for the specified IP Peer Virtual Trunk route followed by a listing of busy Virtual Trunk TNs in the specified route.
STAT VTRM <Cust> <Rout> IDLE	Displays a status summary for the specified IP Peer Virtual Trunk route followed by a listing of idle Virtual Trunk TNs in the specified route.

LD 32 — STAT VTRM commands (Part 2 of 2)

STAT command	Description
STAT VTRM <Cust> <Rout> MBSY	Displays a status summary for the specified IP Peer Virtual Trunk route followed by a listing of maintenance busy Virtual Trunk TNs in the specified route.
STAT VTRM <Cust> <Rout> DSBL	Displays a status summary for the specified IP Peer Virtual Trunk route followed by a listing of disabled Virtual Trunk TNs in the specified route.
STAT VTRM <Cust> <Rout> LCKO	Displays a status summary for the specified IP Peer Virtual Trunk route followed by a listing of locked out Virtual Trunk TNs in the specified route.
ENL VTRM <Cust> <Rout>	Enables all IP Peer Virtual Trunk TNs in the specified route associated with the specified customer.
DIS VTRM <Cust> <Rout>	Disables all IP Peer Virtual Trunk TNs in the specified route associated with the specified customer.

Signaling Server error logging and SNMP alarms

SNMP alarms

When the IP Peer Gateway and NRS applications generate alarms, these alarms are output from the Signaling Server. For example, an SNMP alarm is generated if the Signaling Server loses the link to the Call Server.

When an error or specific event occurs, SNMP sends an alarm trap to OTM or any SNMP manager that is configured in the SNMP section of the Node Properties in CS 1000 Element Manager. OTM receives SNMP traps from the CS 1000 Systems and stores the traps in a circular log file on the OTM Server. The OTM Alarm Notification application monitors incoming traps and notifies the appropriate users of important events and alarms. For more information about OTM alarm management, refer to *Communication Server 1000S: Maintenance* (553-3031-500).

HPOpenView or Optivity NMS are examples of SNMP managers.

For detailed information, refer to *Simple Network Management Protocol: Description and Maintenance* (553-3001-519).

Error logging

An SNMP alarm places a system error message into the Signaling Server's error log file. The error log file can be viewed using Element Manager. The file can also be viewed in any text browser once the file is uploaded to an FTP host using the LogFilePut command.

Use Procedure 79 to view the error log in Element Manager.

Procedure 79
Viewing the error log file in Element Manager

1 Select **System Status** from the navigator.

2 Select **IP Telephony**. The **IP Telephony Information** web page opens.

3 Expand the node containing the associated Signaling Server.

4 Click **RPT LOG**.

The RPT LOG button launches the **Report Utility** web page for Signaling Servers. For more information about this page, refer to *Element Manager: System Administration* (553-3001-332).

End of Procedure

The System Status web page provides status information about the system and access to diagnostic tools. These tools enable users to issue commands to maintain CS 1000S components and CS 1000M components. Use features on the System Status web page to perform maintenance tasks, troubleshooting, and problem resolution.

Error message format

ITG messages are generated from the Voice Gateway Media Cards and the Signaling Server. ITS messages are generated from the IP Phone and are reported through the Signaling Server.

The format of the ITG and ITS error messages is ITGsxxx or ITSsxxx, where sxxx is a four digit number. For example, ITG0351.

The first digit of the four digit number in the error message represents the severity category of the message. The severity categories are:

1 = Critical
2 = Major
3 = Minor
4 = Warning
5 = Cleared (Info)
6 = Indeterminate (Info)

Note: Message numbers beginning with 0 do not follow this format.

For a detailed list of the ITG and ITS error messages, refer to *Software Input/ Output: System Messages* (553-3001-411).

Appendix A: ISDN/H.323 mapping tables

Nortel proprietary Private UDP numbers (ESN LOC) are encoded as Private Level 1 Regional numbers in H.323. CDP numbers are encoded as Private Level 0 Regional numbers in H.323. In H.225.0 (Q.931) messages, public numbers (E.164) are encoded in the Information Element (IE). Private numbers are encoded in the User to User Information Element (UUIE). On reception, both the IE and UUIE are accepted. If both are included, preference is given to the proper format (that is, the IE for public numbers and the UUIE for private numbers). The numbers in the Signaling Server are encoded using the Universal ISDN Protocol Engine (UIPE) format (which is different from Q.931/MCDN/H.323). Tables 51 to 60 describe the mapping.

Table 51
Mapping from UIPE to H.225.0 for NPI

Numbering Plan Indicator (NPI)	UIPE	H.225.0 IE NPI	H.225.0 UUIE NPI
Unknown	0000 (0)	1001 (9)	privateNumber
ISDN/Telephony (E.164)	0001 (1)	0001 (1)	publicNumber
Private	0010 (2)	1001 (9)	privateNumber
Telephony (E.163)	0011 (3)	0001 (1)	publicNumber
Telex (F.69)	0100 (4)	0100 (4)	N/A
Data (X.121)	0101 (5)	0011 (3)	N/A
National Standard	0110 (6)	1000 (8)	N/A

Table 52
Mapping from UIPE to H.225.0 for TON (NPI = E.164/E.163)

TON (NPI=E.164/E.163)	UIPE TON	H.225.0 IE TON	H.225.0 UUIE TON
Unknown	000 (0)	000 (0)	unknown
International number	001 (1)	001 (1)	internationalNumber
National number	010 (2)	010 (2)	nationalNumber
Special number	011 (3)	011 (3)	networkSpecificNumber
Subscriber number	100 (4)	100 (4)	subscriberNumber

Table 53
Mapping from UIPE to H.225.0 for TON (NPI = Private)

TON (NPI = Private)	UIPE TON	H.225.0 IE TON	H.225.0 UUIE TON
Unknown	000 (0)	000 (0)	unknown
ESN LOC (UDP)	101 (5)	000 (0)	level1RegionalNumber
ESN CDP	110 (6)	000 (0)	localNumber
ESN Special Number	011 (3)	000 (0)	pISNSpecificNumber
Note: When NPI = Private, the number digits are encoded in the privateNumber of PartyNumber, which includes the Type of Number (TON). The TON in the H.225.0 IE are ignored on receipt and coded as Unknown (that is, 0000.) In H.323 version 4.0, “publicNumber” is renamed “e164Number”.			

Table 54
Mapping from H.225.0 Information Element to UIPE for NPI (Part 1 of 2)

NPI	H.225.0 IE NPI	UIPE NPI
ISDN/Telephony (E.164)	0001 (1)	0001(1)
Private	1001 (9)	0010 (2)
Telephony (E.163)	0010 (2)	0011 (3)

Table 54
Mapping from H.225.0 Information Element to UIPE for NPI (Part 2 of 2)

NPI	H.225.0 IE NPI	UIPE NPI
Telex (F.69)	0100 (4)	0100 (4)
Data (X.121)	0011 (3)	0101 (5)
National Standard	1000 (8)	0110 (6)
Unknown	all others	0000 (0)

Table 55
Mapping from H.225.0 Information Element to UIPE for TON (NPI = E.164/E.163)

TON (NPI = E.164/E.163)	H.225.0 IE TON	UIPE TON
International number	001 (1)	001 (1)
National number	010 (2)	010 (2)
Network specific number	011 (3)	011 (3)
Subscriber number	100 (4)	100 (4)
Unknown	all others	000 (0)

Table 56
Mapping from H.225.0 Information Element to UIPE for TON (NPI = Private)

TON (NPI = Private)	H.225.0 IE TON	UIPE TON
Level 1 Regional Number	010 (2)	101 (5)
Local Number/ Level 0 Regional	100 (4)	110 (6)
PISN Specific Number	011 (3)	011 (3)
Unknown	all others	000 (0)
Note: When NPI = Private, precedence is given to any number in the H.225.0 UUIE. The H.225.0 IE is only used if the H.225.0 UUIE is not present. The Presentation Indicator and Screening Indicator are always in the information H.225.0 IE. The H.225.0 UUIE is only used if the H.225.0 IE is not present. In H.323 version 4.0, “publicNumber” is renamed “e164Number”.		

Table 57
Mapping from H.225.0 UUIE to UIPE for NPI

NPI	H.225.0 UUIE NPI	UIPE NPI
ISDN/Telephony (E.164)	publicNumber	0001 (1)
Private	privateNumber	0010 (2)

Table 58
Mapping from H.225.0 UUIE to UIPE for TON (NPI = E.164/E.163)

TON (NPI = E.164/E.163)	H.225.0 UUIE TON	UIPE TON
International number	internationalNumber	001 (1)
National number	nationalNumber	010 (2)
Network specific number	networkSpecificNumber	011 (3)
Subscriber number	subscriberNumber	100 (4)
Unknown	all others	000 (0)

Table 59
Mapping from H.225.0 UUIE to UIPE for TON (NPI = Private)

TON (NPI = Private)	H.225.0 UUIE TON	UIPE TON
Level 1 Regional Number	level1 RegionalNumber	101 (5)
Local Number/ Level 0 Regional	localNumber	110 (6)
PISN Specific Number	pISNSpecificNumber	011 (3)
Unknown	all others	000 (0)

Table 60
Mapping from H.225.0 UUIE to UIPE for Unqualified Number

Unqualified Number	H.225.0 UUIE	UIPE NPI	UIPE TON
Dialed Digits	e164	0000 (0)	0000 (0)
Note: In H.323 version 4.0, “e164” is renamed “dialedDigits”. In H.323 version 4.0, “publicNumber” is renamed “e164Number”.			

Appendix B: H.323 Gatekeeper overlap signaling support

Contents

This section contains information on the following topics:

Overlap signaling and H.323 Gatekeeper-routed calls

With H.323 Gatekeeper-routed signaling, admission messages are exchanged between the endpoints and the H.323 Gatekeeper on RAS channels. The H.323 Gatekeeper receives the call-signaling messages on the call-signaling channel from one endpoint and routes them to the other endpoint on the call-signaling channel of the other endpoint.

With direct-routed signaling in the admission confirmation, the H.323 Gatekeeper indicates that the endpoints can exchange call-signaling messages directly. The endpoints exchange the call signaling on the call-signaling channel.

If the H.323 Gatekeeper uses H.323 Gatekeeper routing, it may or may not also use “pre-granted admission”. That is, it may not (and usually does not) need the Admission Request message. As a result, the SETUP message is sent to the H.323 Gatekeeper by the Gateway, and all further processing is done by the H.32 gatekeeper.

For processing to succeed, the H.323 Gatekeeper must be fully compliant with H.323 overlap signaling. That is, the H.323 Gatekeeper must be able to receive multiple messages with digits — the SETUP and subsequent INFORMATION messages.

When the calls are H.323 Gatekeeper-routed, the H.323 Gatekeeper must have the ability to do the following:

- decode digits from SETUP and INFORMATION messages
- perform the address resolution

It must then originate overlap calls (or overlap to en bloc, if necessary) to the destination.

Mixed networks of overlap and en bloc H.323 Gatekeepers

Overlap-capable H.323 Gatekeepers can co-reside with H.323 Gatekeepers that cannot do all the necessary overlap functions. As a result, the H.323 Gatekeepers and the H.323 Gateways must be able to accommodate this occurrence.

The simplest example is in the Location Request (LRQ) handling.

- H.323 versions prior to H.323 Release 4.0 do not support the “incomplete address” reason code in the Location Reject (LRJ). As a result, if an overlap H.323 Gatekeeper is registered to a local overlap-capable H.323 Gatekeeper, then the H.323 Gatekeeper sends a digit string in the ARQ that the H.323 Gatekeeper cannot resolve, and that H.323 Gatekeeper queries its peers.
- However, if the remote H.323 Gatekeeper supports H.323 Release 3 or earlier (or does not support overlap signaling even though the H.323 Gatekeeper conforms to Release 4), no “incomplete” message can be returned.

Any LRQ sent to the remote H.323 Gatekeeper is either rejected with a cause indicating failure, or is ignored. The local H.323 Gatekeeper can determine its own capabilities; however, it cannot determine the capabilities of the remote H.323 Gatekeeper. The local H.323 Gatekeeper also cannot “guess” the returned reasons. For example, a “request denied” may have been triggered by a messaging error or by the sender not having any way to indicate an incomplete number.

To resolve this issue, when a local H.323 Gatekeeper determines from the local provisioning and received responses that no completion can occur, it returns either the Default Route as the destination in the ACF or an ARJ indicating failure to the gateway. However, because differentiation between a "normal ACF" and a "default route ACF" cannot be made, the non-standard data is enhanced to indicate this to the gateway. This indication is done in the non-standard data because the element includes vendor information and, as a result, non-Nortel gateways can read the manufacturer information and ignore the data.

As part of the protocol, all endpoints supporting the protocol must have a predefined way to handle the indication. That is, if the H.323 Gatekeeper indicates that a default route was selected (or would have been selected if the entry had been provisioned) by sending the Default Route Indicator (DRI), then any gateway supporting the protocol must have a predetermined general handling procedure to handle the indication.

The rationale for the general handling procedure is simple. The protocol is designed to be fully forward-compatible. If any recommendation (DRI Recommendation [DRIR]) sent to a gateway by the H.323 Gatekeeper cannot be found in the list of DRIR values understood by the gateway, then the gateway must have a defined procedure for handling this event. That is, the following algorithm applies:

- If the gateway recognizes the recommendation and it is completely valid, the gateway uses the recommendation.
- If the gateway recognizes the recommendation but there is a reason that it cannot apply (for example, if a recommendation such as "wait for more digits" existed but the call was from an en bloc gateway and there are no more digits), the gateway uses either the general handling procedure or some other selected procedure.
- If the gateway does not recognize the recommendation, it uses the general handling procedure. This includes recommendations that have not yet been defined, so the protocol covers forward compatibility.

The importance of this capability within a mixed network is simple. If LRQs are broadcast to the peer H.323 Gatekeepers and no positive responses return, then this may be because no positive responses are possible; the number may be completely undefined. On the other hand, the H.323 Gatekeeper “may just not have responded” but the number may be valid.

H.323 Gatekeeper recommendations for overlap signaling in mixed overlap and en bloc networks

There are two key concepts behind the recommendations:

- First, calls placed using overlap signaling to an en bloc gateway use processing resources that they do not need to use. The SETUP and subsequent INFORMATION messages can trigger multiple Admission Requests to the H.323 Gatekeeper, which in turn can trigger Location Requests throughout a significant part of the IP telephony network. If the average count of ARQs for each call doubles, then the maximum through-put of the H.323 Gatekeeper in calls per hour is halved. For an en bloc call, there is only a single ARQ, which either succeeds or fails the first time.
- Second, calls placed to an en bloc gateway can terminate prematurely to a terminal to handle failed calls. That is, misdialed numbers can route to a specified answering position such as an Attendant, the Security Desk, or some other site. If the destination gateway is provisioned with this sort of capability, then the calls that should have been rejected and sent back to the originator for overlap-to-en bloc conversion. However, the calls receive manual overlap-to-en bloc conversion, as the caller tells the party (answering the intercepted call) the destination that the caller really wanted.

A third item acting as a base for the recommendations is call control traffic on the Signaling Server. Although the call control traffic is not heavy enough to make optimization necessary, it does provide additional justification. Overlap signaling adds some overhead, but much less on the H.323 signaling gateway than on the H.323 Gatekeeper.

With this background information, the following recommendations apply:

1. Even though a gateway may support overlap signaling, if the H.323 Gatekeeper that the gateway uses does not support overlap signaling, then do not provision the gateway as overlap.

Note: All further recommendations assume that the H.323 Gatekeeper supports overlap signaling.

2 Assume that an en bloc destination is registered with the local H.323 Gatekeeper. If this destination is known to be en bloc only, but returns the "unassigned number" or "invalid number format" cause codes, then the administrator can provision the originating Call Server to leave this call as an overlap call. The returned cause code in the RELEASE COMPLETE message triggers overlap-to-en bloc conversion. However, the Overlap Length (OVLL) prompt (in LD 86) must be configured to a value that gives a reasonable probability that the H.323 Gatekeeper can resolve the call on the first attempt. This is to avoid excessive querying of the H.323 Gatekeeper.

3 Assume that an en bloc destination is registered with the local H.323 Gatekeeper. If this destination is known to be en bloc only, but either will not return the desired cause code or will intercept the call, then provision the entry on the originating Call Server with an en bloc Route List Index (RLI). That is, even though the D-channel can accept overlap signaling, define the RLI used for this call with an OVLL of 0. This forces the call into en bloc handling.

4 Assume that an en bloc destination is registered with a remote H.323 Gatekeeper. En bloc destinations, that must be reached using Location Request (LRQ) messages to their H.323 Gatekeeper, are subject to the limitations of that H.323 Gatekeeper. The en bloc destination is also subject to their own limitations regarding handling incomplete numbers. If possible, these destinations should be provisioned as en bloc using OVLL 0, since the remote H.323 Gatekeeper may not be able to handle an overlap call LRQ with an incomplete called-party digit string.

5 Assume that an en bloc destination is registered with a remote H.323 Gatekeeper and OVLL on the originating Call Server is not configured as 0. H.323 Gatekeepers that cannot support overlap signaling may not be able to respond to an LRQ message with an LRJ message to reject the call. If this occurs, the Signaling Server attempts overlap-to-en bloc conversion (unless a prior reply indicated either a successful termination at another destination or that the number was incomplete on another H.323 Gatekeeper). If the local H.323 Gatekeeper fails to receive any response to its LRQ from one or more H.323 Gatekeepers while all others indicate failure, and it has a default route defined, this is provided to the gateway. In addition, the H,323 Gatekeeper provides an indication that the call was terminated to the default route. This allows the gateway to either route the call to the default route destination, or to try overlap-to-en bloc conversion. Therefore, Nortel recommends that the administrator provision any CS 1000 Release 4.0 (or later) H.323 Gatekeepers (with the NRS) with a default route.

6 Assume that a destination is known to be en bloc and OVLL is configured to 0. For all these en bloc destination numbers, if the length of the number is known, then ensure that the Flexible Length (FLEN) prompt is provisioned for that number. Provisioning the FLEN of an eight-digit number as 8 triggers an immediate SETUP on dialing the eighth digit. If the FLEN is longer (or configured to 0), then the Call Server runs an end-of-dial timer to determine whether the number is complete. Failing to configure the FLEN correctly adds several seconds to the post-dial delay (the time between the last digit being dialed and hearing ring-back) for the call.

7 If a destination is known to be overlap-capable, the best performance is possible by using overlap dialing. This allows the H.323 Gatekeepers to minimize their database size. A ‘smaller’ database speeds up responses to queries and allows calls to reach the destination faster. Also, when a call tandems to an overlap-capable PSTN, this gives the best end-to-end performance. So, for destinations in overlap-capable countries, it is a good rule of thumb to always provision any overlap-capable destination to use overlap signaling.

8 If a network is located in an en bloc-only jurisdiction, then there is no harm in provisioning the gateways that can do overlap dialing to receive overlap calls. In this manner, if a new domain from an overlap-compatible area is added later, then all calls that are received as overlap (from the new domain) can be processed more efficiently.

9 If the call terminates on an en bloc-only PSTN, do not use overlap for this call. As an example, the North American dialing plan uses an NPA-NXX-XXXX format. North America also uses en bloc to the PSTN. Therefore, for calls provisioned on the originating Call Server as NPA and NXX calls, do not use overlap. These calls must use OVLL 0 RLIs.

10 If a call is a remote E.164 plan (International, National, or Local/Subscriber) type of number, then this call must traverse the IP

network as a Special Number (SPN). Otherwise, all overlap capability is lost. At the node where the call tandems to the PSTN, the type of number is changed to International, National, or Local (as applicable). However, if the PSTN supports these as overlap calls, then it is guaranteed that the node must be able to receive them as overlap as well. Therefore, provision the originating Call Server with this call as an SPN, and prefix any local numbers with the national code. Then, if it is required that local calls not have national prefixes at the destination, then when the call to the PSTN breaks out to the PSTN, remove any national prefixes from calls going to the local area.

Appendix C: ISDN cause code to SIP status code mapping tables

When an "ISDN: Release" message is received before receiving a SIP final response, a 4xx/5xx message is sent to the far end indicating a corresponding error situation. Table 61 on page 622 maps the cause code in the "ISDN: Release" message to SIP status code according to RFC 3398. If an ISDN cause value other than those listed in Table 61 is received, the default SIP response "500 Server internal error" is used. If a SIP status code other than those listed is received, the default ISDN cause code is "21 call rejected".

Note that the SIP code to ISDN cause code is not one-to-one mapping. Several cause codes can map to one single SIP response. For example, ISDN reason 1, 2, and 3 map to SIP "404" message, but the SIP "404" message only maps to ISDN reason 1. This implies that, when mapping a 4xx/5xx message to ISDN cause value, some information may be lost and further investigation should be done on an individual call basis.

The SIP warning phrase is modified to include the ISDN cause code. For example, "503 Service unavailable ISDN: 34". With MCDN tunneling, the ISDN cause code is presented in tunneled MCDN message as well as the SIP message. The receiver of such a message uses the cause code in MCDN message instead of the SIP warning phrase.

Table 61 on page 622 shows the ISDN cause code to SIP status code mapping, and Table 62 on page 623 shows the SIP error response to ISDN cause code mapping.

> ***Note:*** If desired, a user can change those default mappings through CLI commands.

Table 61 shows the ISDN cause code to SIP status code mapping.

Table 61
ISDN cause code to SIP status code mapping (Part 1 of 2)

ISDN cause code	SIP response
1 unallocated number	404 Not Found
2 no route to network	404 Not Found
3 no route to destination	404 Not found
16 normal call clearing	BYE or Cancel
17 user busy	486 Busy here
18 no user responding	408 Request Timeout
19 no answer from the user	480 Temporarily unavailable
20 subscriber absent	480 Temporarily unavailable
21 call rejected	403 Forbidden (If the cause location is 'user', then code 603 could be given rather than the 403 code)
22 number changed (w/o diagnostic)	410 Gone
22 number changed (w/ diagnostic)	301 Moved Permanently
23 redirection to new destination	410 Gone
26 non-selected user clearing	404 Not Found
27 destination out of order	502 Bad Gateway
28 address incomplete	484 Address incomplete
29 facility rejected	501 Not implemented
31 normal unspecified	480 Temporarily unavailable
34 no circuit available	503 Service unavailable
38 network out of order	503 Service unavailable

Table 61
ISDN cause code to SIP status code mapping (Part 2 of 2)

ISDN cause code	SIP response
41 temporary failure	503 Service unavailable
42 switching equipment congestion	503 Service unavailable
47 resource unavailable	503 Service unavailable
55 incoming calls barred within CUG	403 Forbidden
57 bearer capability not authorized	403 Forbidden
58 bearer capability not presently available	503 Service unavailable
65 bearer capability not implemented	488 Not Acceptable Here
70 only restricted digital avail	488 Not Acceptable Here
79 service or option not implemented	501 Not implemented
87 user not member of CUG	403 Forbidden
88 incompatible destination	503 Service unavailable
102 recovery of timer expiry	504 Gateway timeout
111 protocol error	500 Server internal error
127 interworking unspecified	500 Server internal error

Table 62 shows the SIP error response to ISDN cause code mapping.

Table 62
ISDN cause code to SIP status code mapping (Part 1 of 3)

SIP response	ISDN cause code
400 Bad Request	41 Temporary Failure

Table 62
ISDN cause code to SIP status code mapping (Part 2 of 3)

SIP response	ISDN cause code
401 Unauthorized	21 Call rejected
402 Payment required	21 Call rejected
403 Forbidden	21 Call rejected
404 Not found	1 Unallocated number
405 Method not allowed	63 Service or option unavailable
406 Not acceptable	79 Service/option not implemented
407 Proxy authentication required	21 Call rejected
408 Request timeout	102 Recovery on timer expiry
410 Gone	22 Number changed (without diagnostic)
413 Request Entity too long	127 Interworking
414 Request-URI too long	127 Interworking
415 Unsupported media type	79 Service/option not implemented
416 Unsupported URI Scheme	127 Interworking
420 Bad extension	127 Interworking
421 Extension Required	127 Interworking
423 Interval Too Brief	127 Interworking
480 Temporarily unavailable	18 No user responding
481 Call/Transaction Does not Exist	41 Temporary Failure
482 Loop Detected	25 Exchange - routing error
483 Too many hops	25 Exchange - routing error
484 Address incomplete	28 Invalid Number Format
485 Ambiguous	1 Unallocated number

Table 62
ISDN cause code to SIP status code mapping (Part 3 of 3)

SIP response	ISDN cause code
486 Busy here	17 User busy
487 Request Terminated	no mapping
488 Not Acceptable here	by Warning header
500 Server internal error	41 Temporary failure
501 Not implemented	79 Not implemented, unspecified
502 Bad gateway 3	8 Network out of order
503 Service unavailable	41 Temporary failure
504 Server time-out	02 Recovery on timer expiry
505 Version Not Supported	127 Interworking
513 Message Too Large	127 Interworking
600 Busy everywhere	17 User busy
603 Decline	21 Call rejected
604 Does not exist anywhere	1 Unallocated number
606 Not acceptable	by Warning header

Nortel Communication Server 1000

IP Peer Networking

Installation and Configuration

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Publication number: 553-3001-213
Document release: Standard 11.00
Date: May 2007
Produced in Canada

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback