



**NORTEL**

Nortel Communication Server 1000

# IP Peer Networking Installation and Commissioning

Release: 5.5

Document Revision: 02.07

[www.nortel.com](http://www.nortel.com)

---

NN43001-313

Nortel Communication Server 1000  
Release: 5.5  
Publication: NN43001-313  
Document release date: 7 October 2009

Copyright © 2007–2009 Nortel Networks. All Rights Reserved.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

---

# Contents

---

<b>New in this Release</b>	<b>9</b>
Other	9
Revision History	9
<b>How to get help</b>	<b>13</b>
Finding the latest updates on the Nortel Web site	13
Getting help from the Nortel Web site	13
Getting help over the telephone from a Nortel Solutions Center	13
Getting help from a specialist by using an Express Routing Code	14
Getting help through a Nortel distributor or reseller	14
<b>Introduction</b>	<b>15</b>
Subject	15
Note on legacy products and releases	15
Applicable systems	15
Intended audience	16
Conventions	16
Terminology	16
Related information	16
NTPs	16
Online	18
CD-ROM	18
<b>Overview</b>	<b>19</b>
Contents	19
IP Peer Networking overview	20
Assumptions	21
Virtual Trunk	21
Signaling Server	23
Terminal Proxy Server	27
SIP Gateway Signaling software	27
H.323 Gateway Signaling software	28
Overlap Signaling	29
Network Routing Service	29
Element Manager Web interface	32

---

NRS Manager Web interface	33
Interworking protocols	33
Session Initiation Protocol	33
H.323 protocol	36

---

<b>SIP signaling</b>	<b>43</b>
Contents	43
Introduction	43
SIP requests and responses	44
Format of a SIP message	46
Direct IP Media Paths	46
IP Phone to IP Phone (on separate Call Servers)	48
Call scenarios	54

---

<b>H.323 signaling</b>	<b>63</b>
Contents	63
Direct IP Media Paths	63
IP Phone to IP Phone (on separate Call Servers)	64
Call scenarios	75

---

<b>H.323-to-SIP signaling</b>	<b>83</b>
Contents	83
Introduction	83
H.323-to-SIP signaling (coexistence of both H.323 and SIP)	83
Call scenarios summary	85
Call walk-through	85

---

<b>Features</b>	<b>101</b>
Contents	101
Tone handling	101
Progress tones	101
End-to-end DTMF signaling	102
DTMF out-of-band signals from H.323 trunk	105
DTMF out-of-band signals from SIP trunk	105
Fax calls	106
SIP	106
H.323	106
Fax/Modem pass through	107
Modem traffic	108
Reliability and redundancy	109
Alternate Call Server	110
Signaling Server software redundancy	112
H.323 Gateway software trunk route redundancy	113
SIP Trunk Gateway software trunk route redundancy	113
SIP Proxy Trunk Gateway software trunk route redundancy	114
NRS redundancy	115

---

Campus-distributed Media Gateway in survival mode	119
CS 1000M Large System CPU redundancy	120
Least Cost Routing	123
Licenses	123
Limitations	124

---

## **Configure IP Peer Network** **125**

Contents	125
Overview	126
Task summary	127
Launching Element Manager	129
Linux-based Element Manager	129
VxWorks-based Element Manager	133
Using Element Manager for configuration	135
Configuring the Customer Data Block	136
Configuring D-channels	138
Configuring zones	141
Configuring the Virtual routes and trunks	141
Configure virtual superloops for IP Phones (LD 97)	144
Configuring networking	149
Configuring call routing	153
Configuring codecs	157
Configuring QoS (DiffServ) values	157
Configuring call types	157
Configuring digit manipulation tables	167
Feature Implementation of IP Peer Networking	168
Task summary list	168
VTRK Failover Upon Network Failure feature	185
Configuring the Gateways	188
Enabling and configuring the H.323 Gateway	188
Enabling and configuring the SIP Trunk Gateway	191
Restarting the Signaling Server	198
Warm restart	198
Cold restart	198

---

## **Overlap signaling** **199**

Contents	199
Overview	199
Advantages of overlap signaling	201
PSTN-destined calls	202
Feature capabilities	202
Overlap signaling support using the H.323 protocol	202
H.323 Gatekeeper overlap signaling support	202
Overlap sending and receiving configuration support	203
Tandem overlap signaling support	206

Overlap signaling call flow	206
Feature packaging	213
Configuring overlap signaling on the Call Server	213
Task summary list	213
Configuring overlap signaling using Element Manager	220
Overlay changes for overlap signaling	221
Flexible Length number of digits implications	223
System log messages	224

---

## **IP Peer interworking** **225**

Contents	225
Nortel products interworking	225
CS 1000MSystem interworking	225
Multimedia Communication Server 5100 (MCS 5100)	230
CallPilot 2.02	230
Collaboration between a CS 1000 Release 4.0 (or later) NRS and a Succession 3.0 H.323 Gatekeeper or MCS 5100	232

---

## **Maintenance** **233**

Contents	233
Command Line Interface commands	234
Help CLI commands	234
Virtual Trunk CLI commands	234
D-channel CLI command	235
H323GwShow CLI commands	236
SIPGwShow CLI commands	237
Graceful disable CLI commands	239
Trace tools CLI commands	240
NRS database CLI commands	254
Standalone NRS CLI commands	256
ISDN to and from SIP mapping CLI commands	256
Call Server commands	258
Manage Virtual Trunk route members	258
Status commands	258
Signaling Server error logging and SNMP alarms	260
SNMP alarms	260
Error logging	261
Error message format	262

---

## **ISDN/H.323 mapping tables** **265**

---

### **H.323 Gatekeeper overlap signaling support** **269**

Contents	269
Overlap signaling and H.323 Gatekeeper-routed calls	269
Mixed networks of overlap and en bloc H.323 Gatekeepers	270

---

H.323 Gatekeeper recommendations for overlap signaling in mixed overlap and en bloc networks 271

---

**ISDN cause code to SIP status code mapping tables 275**

---

**Passthrough End User License Agreement 279**



---

## New in this Release

---

**WARNING**

Do not contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

Communication Server 1000 Release 5.5 introduces a Fax/Modem pass through. The Fax/Modem pass through feature provides a modem pass through allowed (MPTA) class of service (CLS) for an analog phone TN. MPTA CLS dedicates an analog phone TN to a modem or a Fax machine terminal. A connection that initiates from the dedicated TN, and/or calls that terminate at the dedicated TN through a Digital Signal Processor (DSP), use a G711 NO VAD codec on the Call Server. Modem Pass through is a specific configuration of a G.711 VoIP channel that improves modem performance compared to standard VoIP configuration.

### Other

#### Revision History

**October 2009**

Standard 02.07. This document is up-issued to update the section IP Peer Networking Overview.

**September 2008**

Standard 02.06. This document is up-issued to reflect changes in technical content.

**July 2008**

Standard 02.05. This document is up-issued to reflect changes in technical content.

**July 2008**

Standard 02.04. This document is up-issued to reflect changes in technical content. Sections relating to Bandwidth Management have been moved to *Converging the Data Network with VoIP* ((NN43001-260)).

**June 2008**

Standard 02.03. This document is up-issued to add CS 2000 information to CS 1000M System interworking section and add information on the VTRK Failover Upon Network Failure feature to the *Feature Implementation of IP Peer Networking* section.

**January 2008**

Standard 02.02. This document is up-issued to reflect changes in technical content.

**December 2007**

Standard 02.01. This document is up-issued to support Communication Server 1000 Release 5.5.

**November 2007**

Standard 01.03. This document is up-issued to include changes in technical content for Wireless LAN interworking (802.11 Wireless IP Handsets).

**October 2007**

Standard 01.02. This document is up-issued to include changes in technical content for codec negotiation.

**May 2007**

Standard 01.01. This document is a new NTP for Communication Server 1000 Release 5.0. It was created to support a restructuring of the Documentation Library. This document is comprised of (1) information on IP Peer Networking that was previously contained in the legacy document, now retired: *IP Peer Networking: Installation and Configuration* () (553-3001-213), and (2) a description of the installation and configuration of Communication Server 1000 Release 5.0 IP Peer Networking.

**April 2007**

Standard 10.00. This document is up-issued for: (1) revising the configuration rules for Bandwidth Management. See page 140. (2) Revising the description of loop limitations on a large system. See page 303. (3) Revising the default value of the FOPT (Flexible Orbit Prevention Timer) from 14 to 6 seconds. See page 363. (4) 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 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 specifying that at least 768 MB 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 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 adding a note that Data calls are not supported on Virtual Trunks. See page 28.

**April 2006**

Standard 5.00. This document is up-issued for 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 to add 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)* ().



---

## How to get help

---

This chapter explains how to get help for Nortel products and services.

### Finding the latest updates on the Nortel Web site

The content of this documentation is current at the time the product is released. To check for updates to the latest documentation for Communication Server (CS) 1000, go to [www.nortel.com/documentation](http://www.nortel.com/documentation) and navigate to the Technical Documentation page for CS 1000.

### Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

[www.nortel.com/support](http://www.nortel.com/support)

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

### Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835). Outside North America, go to the following Web site to obtain the telephone number for your region:

[www.nortel.com/callus](http://www.nortel.com/callus)

### **Getting help from a specialist by using an Express Routing Code**

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

[www.nortel.com/erc](http://www.nortel.com/erc)

### **Getting help through a Nortel distributor or reseller**

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

---

# Introduction

---

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 5.0 (or later) 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](http://www.nortel.com)<http://www.nortel.com>

## Applicable systems

This document applies to the following systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 61C
- Meridian 1 PBX 81C

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

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

- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

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

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 61C
- 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* () (NN43001-260)
- *Electronic Switched Network: Signaling and Transmission Guidelines* (NN43001-280)
- *Dialing Plans: Description* () (NN43001-283)
- *Signaling Server Installation and Commissioning* (NN43001-312)
- *Branch Office Installation and Commissioning* ((NN43001-314))
- *System Management* ((NN43001-600))

- *Features and Services* (NN43001-106)
- *System Redundancy Fundamentals* (NN43001-507) (NN43001-507)
- *Software Input/Output: Administration* (NN43001-611)
- *Telephony Manager 3.1: System Administration* ( (NN43050-601))
- *IP Trunk: Description, Installation, and Operation* ((NN43001-563))
- *IP Line: Description, Installation, and Operation* () (NN43100-500)
- *Basic Network Features* (NN43001-579)
- *Software Input/Output: System Messages* (NN43001-712)
- *Software Input/Output: Maintenance* (NN43001-711)
- *Simple Network Management Protocol: Description and Maintenance* ((NN43001-719))
- *Communication Server 1000M and Meridian 1: Small System Planning and Engineering* (NN43011-220)
- *Communication Server 1000M and Meridian 1: Small System Installation and Commissioning* (NN43011-310)
- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (NN43011-459)
- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (NN43021-220)
- *Communication Server 1000M and Meridian 1: Large System Installation and Commissioning* (NN43021-310)
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* ( (NN43011-459))
- *Communication Server 1000E: Planning and Engineering* (NN43041-220) ((NN43041-220))
- *Communication Server 1000E: Installation and Commissioning* ( (NN43041-310))
- *Communication Server 1000E: Upgrade Procedures* ( (NN43041-458))
- *Communication Server 1000E: Maintenance* (NN43041-700)
- *Multimedia Communication Server (MCS) Interworking Fundamentals* ((NN42020-127))
- *CallPilot Planning and Engineering Guide* (NN44200-200) (553-7101-101)
- *CallPilot Installation and Configuration Part 3: T1/SMDI and CallPilot Server Configuration* (NN44200-303) (553-7101-224)
- *CallPilot Administrator's Guide* (44200-601) () (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](http://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” (page 20)
  - “Assumptions” (page 21)
  - “Virtual Trunk” (page 21)
  
- “Signaling Server” (page 23)
- “Terminal Proxy Server” (page 27)
- “SIP Gateway Signaling software” (page 27)
- “SIP Converged Desktop Service” (page 28)
- “H.323 Gateway Signaling software” (page 28)
- “Overlap Signaling” (page 29)
- “Network Routing Service” (page 29)
  - “SIP Redirect Server software” (page 30)
  - “SIP Registrar” (page 31)
  - “H.323 Gatekeeper software” (page 31)
  - “Network Connection Server” (page 32)
- “Element Manager Web interface” (page 32)
- “NRS Manager Web interface” (page 33)
- “Interworking protocols” (page 33)
  - “Session Initiation Protocol” (page 33)
  - “H.323 protocol” (page 36)

## IP Peer Networking overview



### WARNING

Do **not** contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

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 [“Virtual Trunk” \(page 21\)](#).

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 5.0 (or later) 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 can be any of the following: ISP1100 server (1 GB RAM minimum), CPPM-SS server, IBM or HP Commercial-Off-the-Shelf (COTS) server. 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 "[Signaling Server](#)" (page 23) and *Signaling Server Installation and Commissioning* ((NN43001-312)).

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 "[Network Routing Service](#)" (page 29) and *Network Routing Service Installation and Commissioning* (NN43001-564).

A brief overview of the migration procedures is described in *Network Routing Service Installation and Commissioning* (NN43001-564). However, refer to the Upgrade Procedures NTP appropriate to your system for detailed migration procedures.

**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 1:** 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* ((NN43100-500)) .

**Note 2:** 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 "Virtual Trunk limits for each Signaling Server" (page 22) 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)
<p><b>Note 1:</b> At least 1024 MB of memory is required on the Signaling Server to obtain 1200 H.323 Virtual Trunks.</p> <p><b>Note 2:</b> See Table 3 "Maximum number of Virtual Trunk on each Signaling Server" (page 26).</p>	

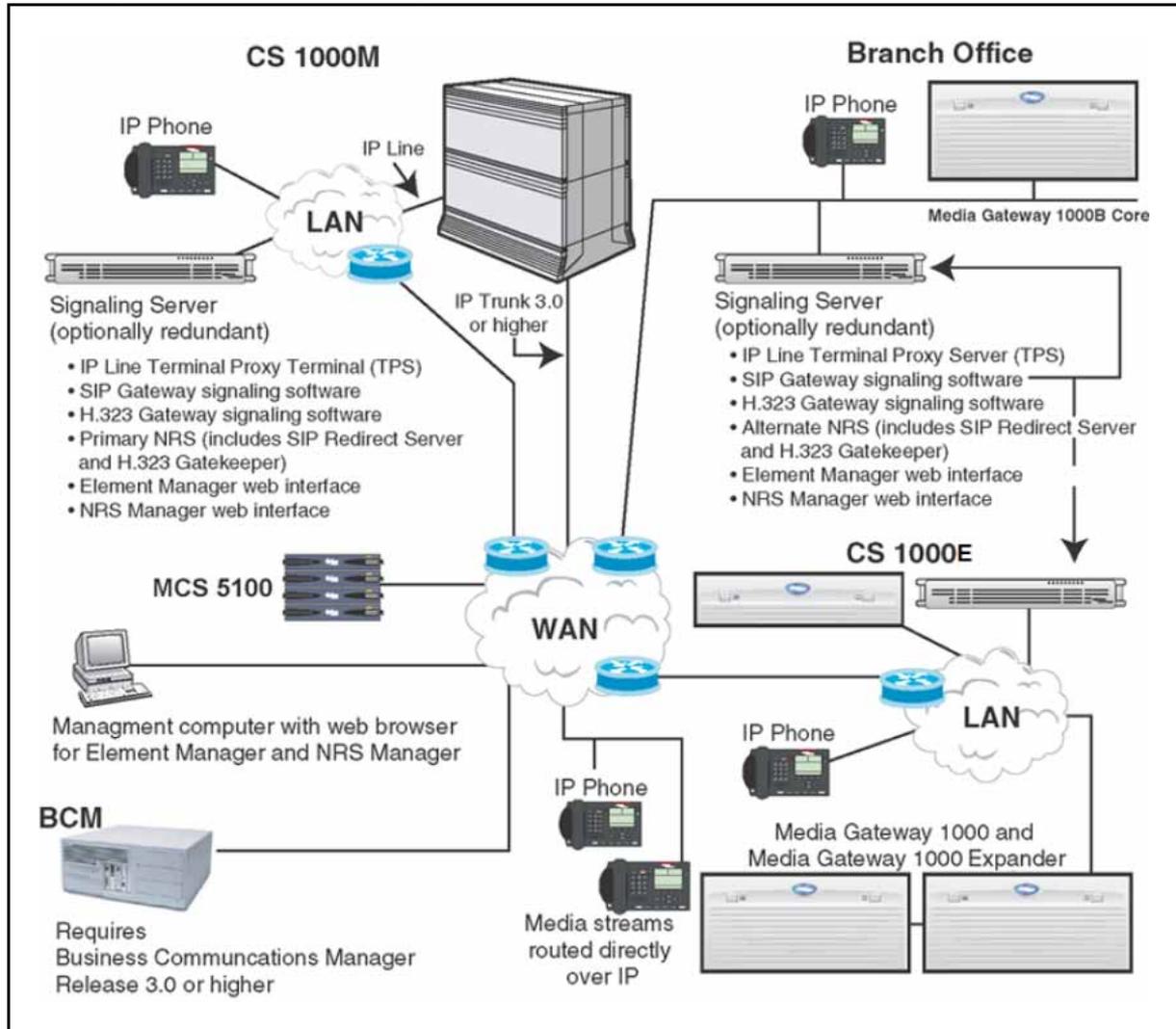
SIP and H.323 Virtual Trunks can reside on the same Signaling Server platform. This is achieved by configuring the Virtual Trunks on separate routes; however, the Virtual Trunks must use the same IP D-channel ID. Each SIP Trunk Gateway occupies one Virtual Trunk route.

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" (page 25) and the Planning and Engineering NTPs.

Figure 1 "An example of IP Peer Networking" (page 23) illustrates an example of an IP Peer Networking configuration.

**Figure 1**  
An example of IP Peer Networking



### Signaling Server

IP Peer Networking uses a Signaling Server. The Signaling Server can be any of the following: ISP1100 server (1 GB RAM minimum), CPPM-SS server, IBM or HP Commercial-Off-the-Shelf (COTS) 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 Commissioning* ((NN43001-312)).

### **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* ((NN43001-500)) .

- 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 "Signaling Server limits" (page 25) 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" (page 26).

**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 ((NN43011-220))*
- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering ((NN43021-220) )*
- *Communication Server 1000E: Planning and Engineering (NN43041-220) ((NN43041-220))*

### 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 "Maximum number of Virtual Trunk on each Signaling Server" \(page 26\)](#) gives examples of the maximum number of Virtual Trunks supported for different configurations.

**Table 3**  
**Maximum number of Virtual Trunk on each Signaling Server**

SIP	H.323 (see Note)			Total Virtual Trunks
	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:

$$(\text{Num\_of\_SIP} \times 1 \text{ FD}) + (\text{Num\_of\_Incoming\_H323} \times 2 \text{ FD}) + (\text{Num\_of\_Outgoing\_H323} \times 1 \text{ FD}) \leq \text{Max\_Num\_of\_FDs}$$

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" \(page 39\)](#).

## 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 1110
- Nortel IP Phone 1120E
- Nortel IP Phone 1140E
- Nortel IP Phone 1150
- 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” \(page 33\)](#) 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” \(page 199\)](#).

## 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:** Communication Server for Enterprise (CSE) 1000 Release 2.0 Gatekeepers do not support nodes running CS 1000 Release 4.0 software or higher. In order to support new features, the NRS must be running the latest software release in the network. In most cases, if the entire network is being upgraded, upgrade the NRS first. It is possible to operate CS 1000 Release 5.5 nodes with CS 1000 Release 5.0 for a short time if the upgrade logistics require this. Some new feature capability may not operate. Note that the NRS must be the same software release as the Alternate NRS in order to synchronize the databases.

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.

**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 VxWorks-based NRS combines the following:

- SIP Redirect Server (see [“SIP Redirect Server software” \(page 30\)](#)) and SIP Registrar (see [“SIP Registrar” \(page 31\)](#))
- H.323 Gatekeeper (see [“H.323 Gatekeeper software” \(page 31\)](#))
- Network Connection Service (NCS) (see [“H.323 Gatekeeper software” \(page 31\)](#))

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:

- Standalone mode — The host Signaling Server does not have an attached Call Server. During installation of a standalone 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” \(page 24\)](#).

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, see *Network Routing Service Installation and Commissioning (NN43001-564)* .

### **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 *Network Routing Service Installation and Commissioning (NN43001-564)*.

### **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, see *Network Routing Service Installation and Commissioning (NN43001-564)*.

### **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 Telephony Manager (TM). The TM 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 *Network Routing Service Installation and Commissioning (NN43001-564)*.

## **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 "SIP components" (page 34) 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
- 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.

CS 1000 Release 5.0 (or later) NRS is offered in two versions: (1) a Vxworks-based NRS comprising a SIP Redirect Server, Network Connect Server (NCS), and H.323 Gatekeeper (GK) ; (2) a Linux-based NRS comprising a SIP Proxy Server and Redirect Server, NCS, and GK.

The VxWorks-based NRS application software can be run on any of the following server platforms: ISP1100 server (1 GB RAM minimum), CP-PM server, IBM or HP Commercial-Off-the-Shelf (COTS) server. On any of those four server platforms the VxWorks-based NRS can be configured to run either standalone or co-resident with other CS 1000 Signaling Server applications, such as UNiStim IP Phone Line Terminal Proxy (LTSP), IP Peer virtual trunk SIP or H.323 signaling Gateway (VTRK GW), IP Phone Application Server. There are no functional changes in the Vxworks-based NRS application in CS 1000 RIs 5.0 (or later), as compared with CS 1000 RIs 4.5. The Linux-based NRS application software can be run on either IBM or HP COTS server. The CS 1000 RIs 5.0 (or later) Signaling Server applications cannot be run on the Nortel Linux-based COTS server, therefore the Linux-based NRS can be configured to run only standalone.

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 multi-site 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 "H.323 components" \(page 38\)](#) 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.

### **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:

$1800 - [(1 \times \text{H.323 channels}) + \text{SIP channels}]$   
(where 1800 is the maximum number of Virtual Trunks)

**Example 1:** 1200 H.323 and 600 SIP

$1800 - [(1 \times 1200 \text{ H.323 channels}) + 600 \text{ SIP channels}]$   
= 0 available Virtual Trunks

**Example 2:** 900 H.323 and 900 SIP

$1800 - [(1 \times 900 \text{ H.323 channels}) + 900 \text{ SIP channels}]$   
= 0 available Virtual Trunks

**Example 3:** 0 H.323 and 1800 SIP

$1800 - [(1 \times 0 \text{ H.323 channels}) + 1800 \text{ SIP channels}]$   
= 0 available Virtual Trunks

**Example 4:** 1200 H.323 and 0 SIP

$1800 - [(1 \times 1200 \text{ H.323 channels}) + 0 \text{ SIP channels}]$   
= 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:

$1800 - [(2 \times \text{H.323 channels}) + \text{SIP channels}]$   
(where 1800 is the maximum number of Virtual Trunks)

**Example 1:** 900 H.323 and 0 SIP

$1800 - [(2 \times 900 \text{ H.323 channels}) + 0 \text{ SIP channels}]$   
 $1800 - [(1800 \text{ H.323 channels}) + 0 \text{ SIP channels}]$   
= 0 available Virtual Trunks

**Example 2:** 600 H.323 and 600 SIP

$1800 - [(2 \times 600 \text{ H.323 channels}) + 600 \text{ SIP channels}]$   
 $1800 - [(1200 \text{ H.323 channels}) + 600 \text{ SIP channels}]$   
= 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” \(page 43\)](#)

[“SIP requests and responses” \(page 44\)](#)

[“Format of a SIP message” \(page 46\)](#)

[“Direct IP Media Paths” \(page 46\)](#)

[“IP Phone to IP Phone \(on separate Call Servers\)” \(page 48\)](#)

[“Call scenarios” \(page 54\)](#)

## 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.

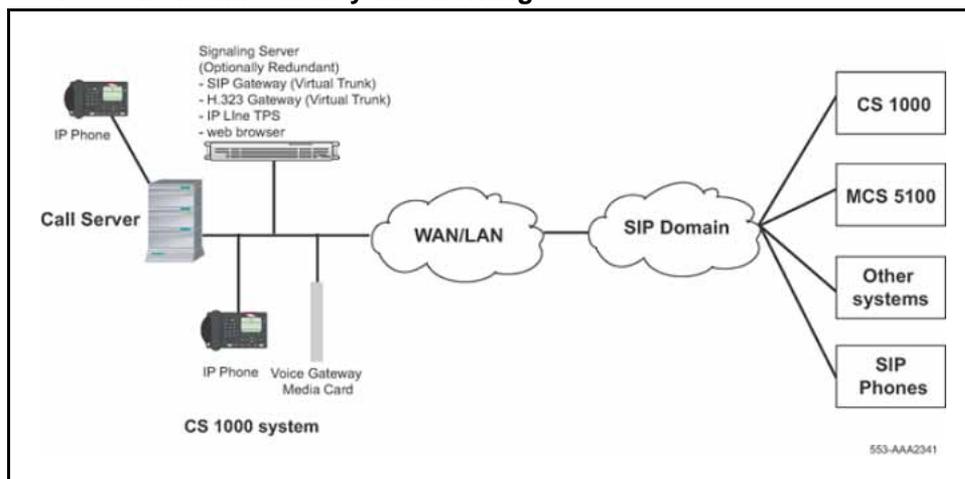
The SIP Trunk Gateway is implemented according to SIP standards. The SIP Trunk Gateway can connect two CS 1000 nodes and can also connect CS 1000 systems to other Nortel or third-party SIP-enabled products. This SIP Trunk Gateway interworks with the MCS 5100 system.

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” \(page 113\)](#).

[Figure 2 “CS 1000 SIP Trunk Gateway interworking” \(page 44\)](#) 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 "SIP request methods" (page 45) shows the SIP request methods.

**Table 6**  
**SIP request methods**

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

Table 7 "SIP response methods" (page 45) 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.

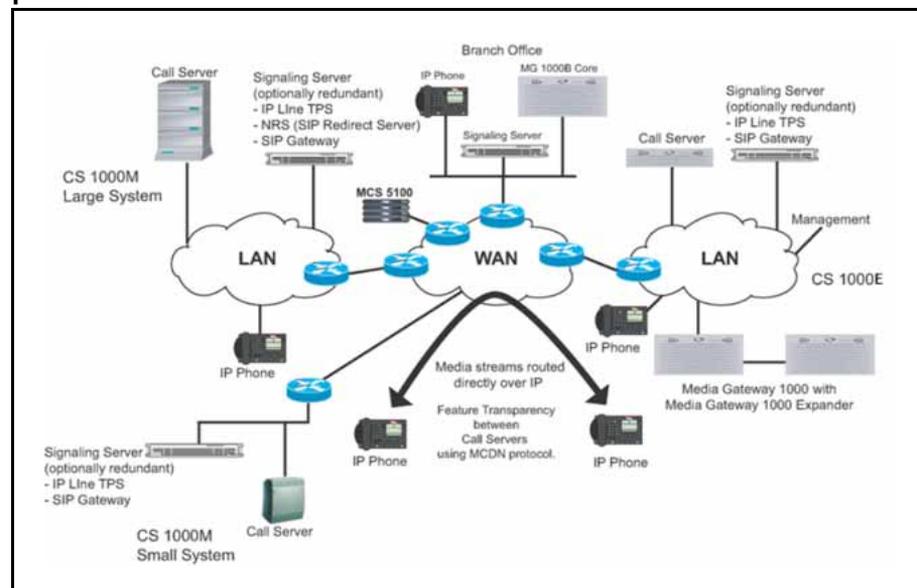
**Note 2:** A Media Gateway is a gateway that uses a protocol similar to the Media Gateway Control Protocol (MGCP). The Media Gateway houses peripheral cards. Media Gateways are controlled directly by the Call Server. Peripheral cards are housed in the Intelligent Peripheral Equipment (IPE) shelf in 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 "An example of IP Peer Networking using Virtual Trunk and direct media paths" (page 47) 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 "User A dials User B" \(page 49\)](#)). 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.

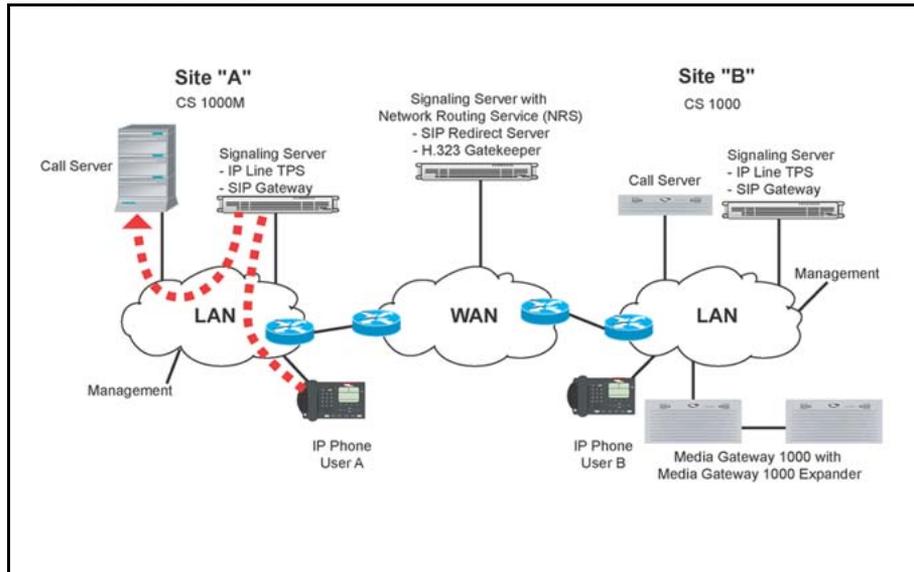
If the user is attempting to reach an internal telephone, the call is terminated on the internal device. When the system determines that the user is attempting to reach a telephone or service using the IP network, the call routes to the SIP Trunk Gateway software. The SIP Trunk Gateway software uses 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 "User A dials User B" \(page 49\)](#).

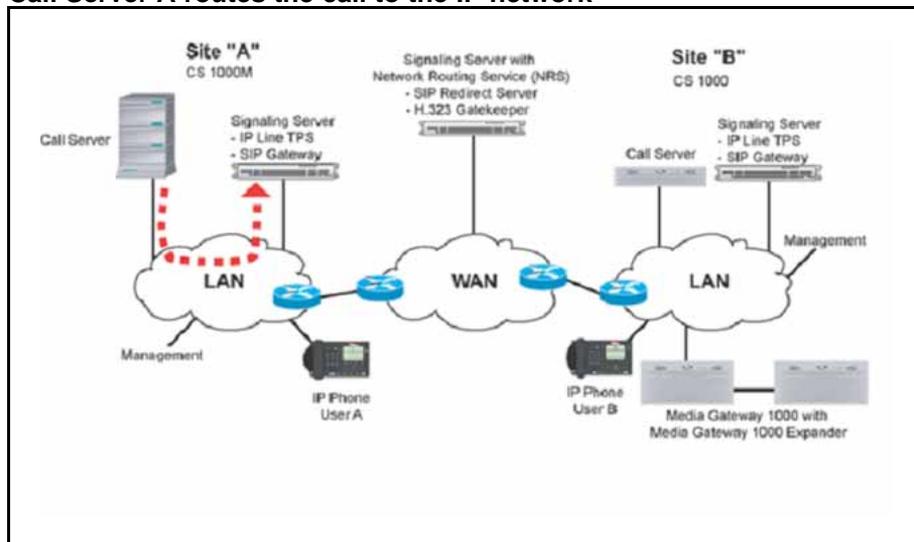
**Figure 4**  
**User A dials User B**



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 "Call Server A routes the call to the IP network"](#) (page 49).

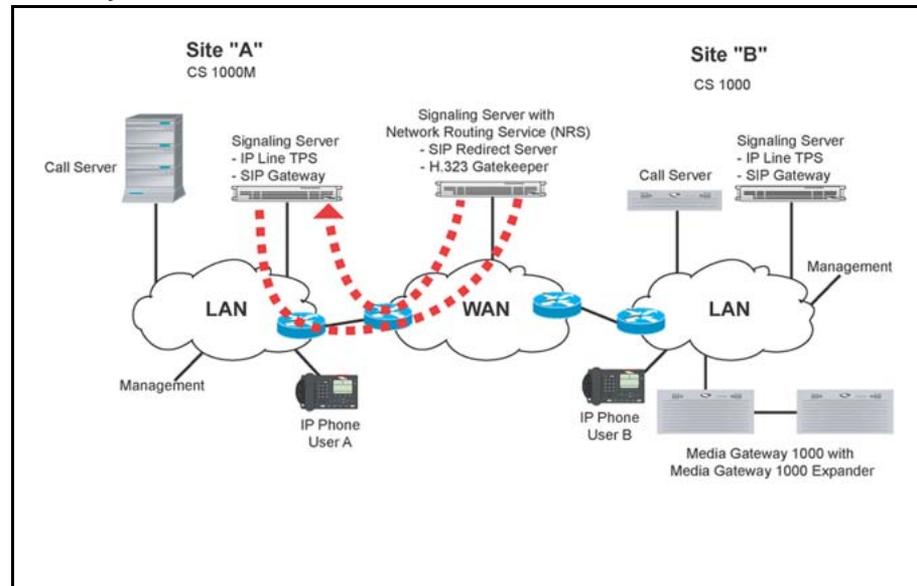
**Note:** To select which Virtual Trunk to use for routing, Call Server A examines the number dialed, and uses various trunk routing and signaling features (for example, ESN and MCDN).

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



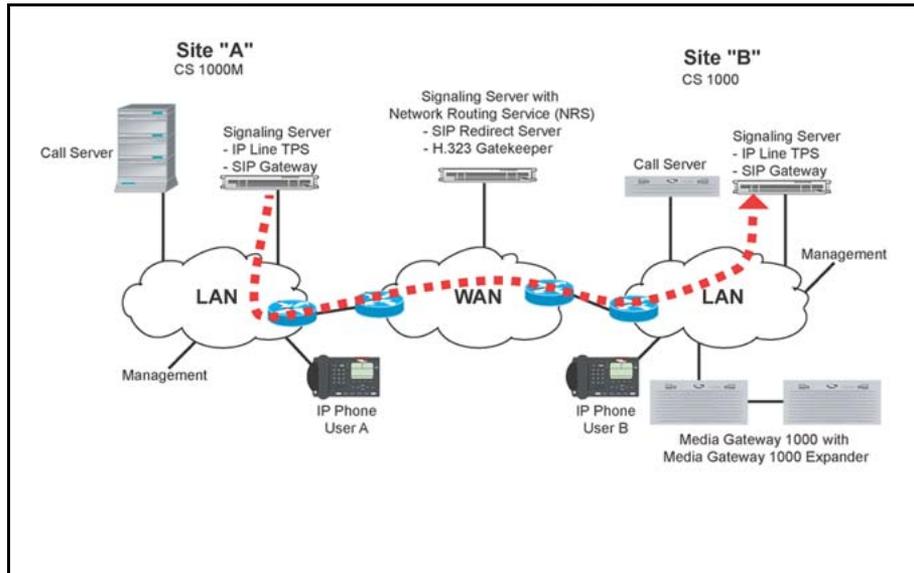
3. SIP Trunk Gateway A asks the NRS to search for the dialed DN in the database (for example, within the appropriate CDP domain). The NRS (SIP Redirect Server) sends the IP address of the SIP Trunk Gateway B to SIP Trunk Gateway A. See [Figure 6 "The NRS sends the IP address of SIP Trunk Gateway B to SIP Trunk Gateway A"](#) (page 50).

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



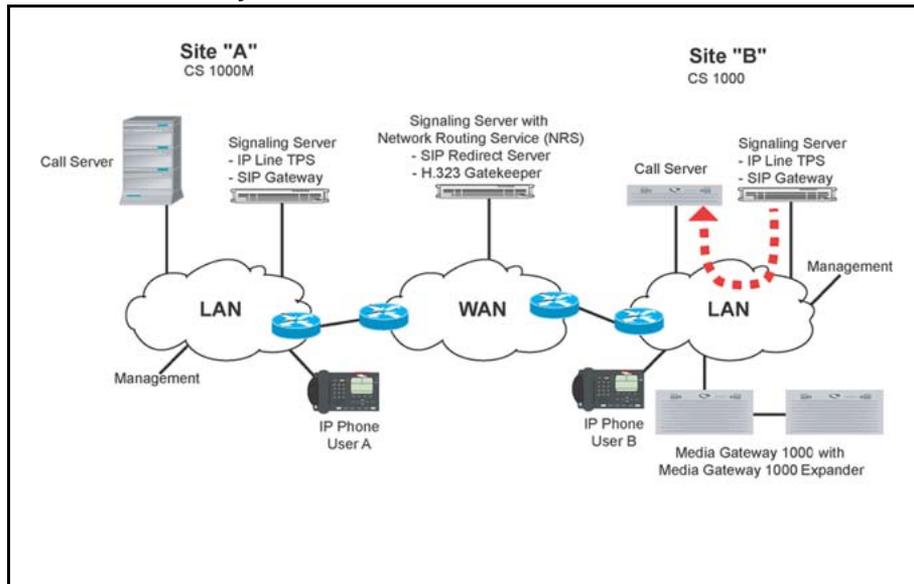
4. SIP Trunk Gateway A sends an INVITE message to SIP Trunk Gateway B, including the DN information. See [Figure 7 "SIP Trunk Gateway A sends an INVITE message to SIP Trunk Gateway B"](#) (page 51).

**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 "SIP Trunk Gateway B sends the call to Call Server B over a Virtual Trunk"](#) (page 51).

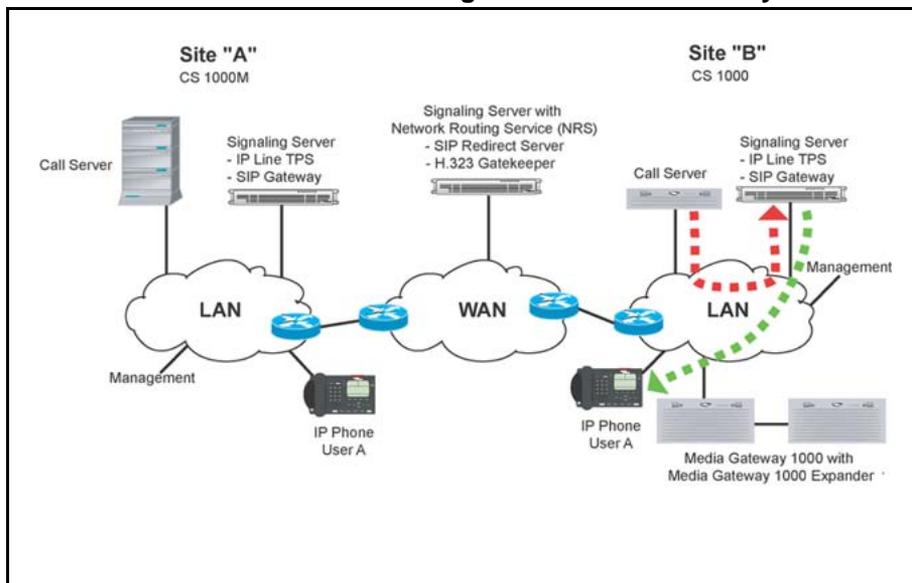
**Figure 8**  
**SIP Trunk Gateway B sends the call to Call Server B over a Virtual Trunk**



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

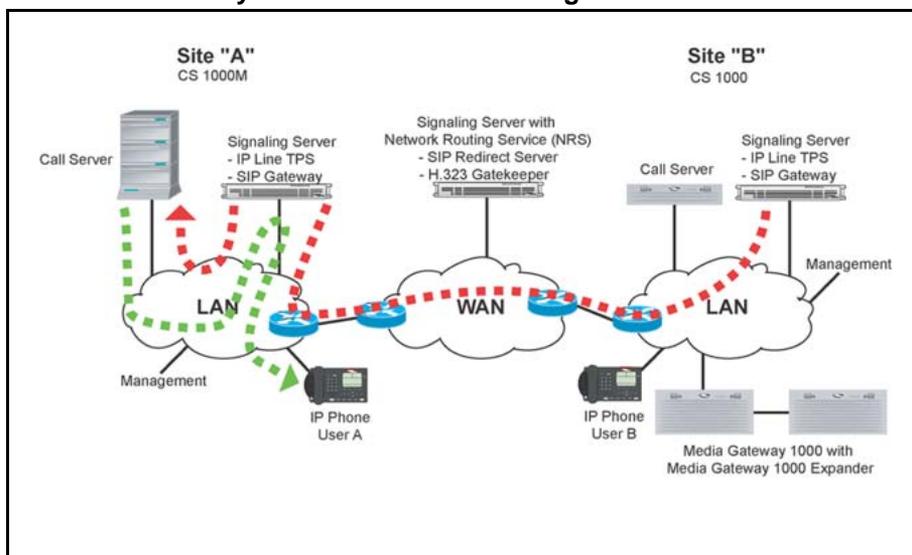
B over the Virtual Trunk. See [Figure 9 "Call Server B sends an Alert message to SIP Trunk Gateway B"](#) (page 52).

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



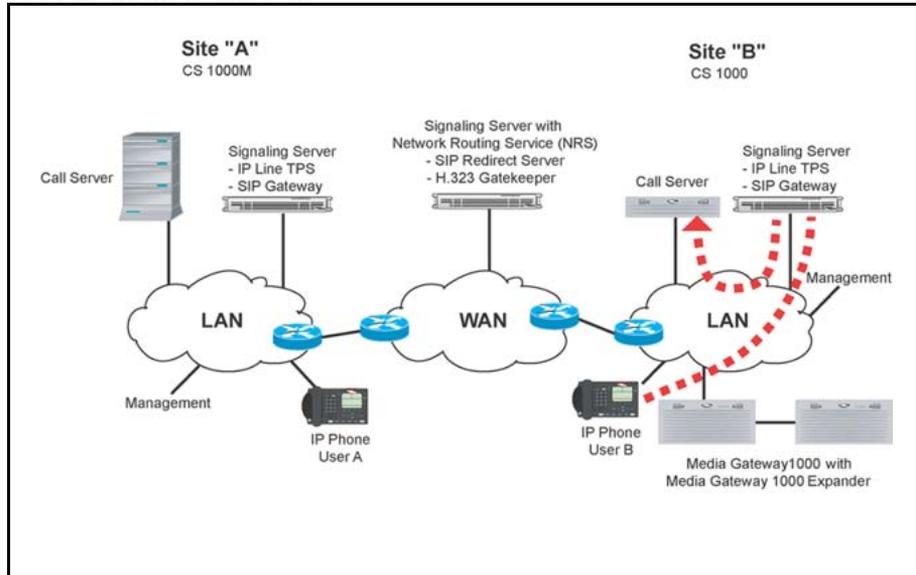
7. SIP Trunk Gateway B converts the ISDN Alert message to a SIP 180 response message. SIP Trunk Gateway B sends the SIP message to SIP Trunk Gateway A. SIP Trunk Gateway A converts the SIP 180 message back to the ISDN Alert message. SIP Trunk Gateway A then sends the message to Call Server A. Call Server A requests that the IP Phone play ringback tone. See [Figure 10 "SIP Trunk Gateway B sends an Alert message to Call Server A"](#) (page 52).

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



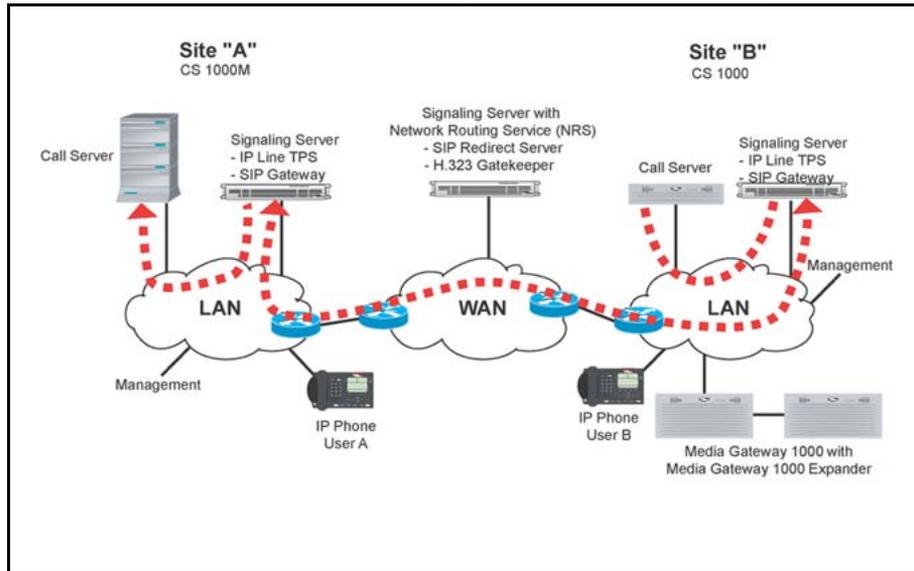
8. User B answers the call. A message is sent to Call Server B through the TPS on Signaling Server B. See [Figure 11 "User B answers the call"](#) (page 53).

**Figure 11**  
**User B answers the call**



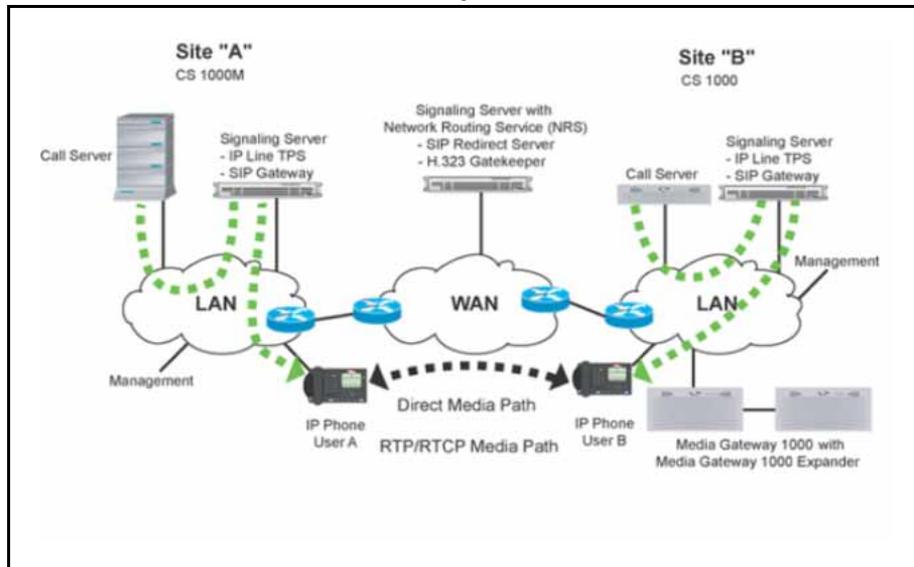
9. Call Server B sends an ISDN CONNECT message to SIP Trunk Gateway B. SIP Trunk Gateway B converts the CONNECT message to the SIP 200 OK message. SIP Trunk Gateway B sends the SIP 200 OK message to SIP Trunk Gateway A. SIP Trunk Gateway A sends an ACK message back to SIP Trunk Gateway B to acknowledge 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 "Call Server B sends an ACK message to SIP Trunk Gateway B"](#) (page 54).

**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 "IP Phones start the direct IP media paths"](#) (page 54).

**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 *SIP Phone-to-SIP Phone communication*)
- SIP Gateway and SIP Phone (see *SIP Trunk Gateway-to-SIP Phone communication*)

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.

**TRO versus TAT on transferred call** The TRO feature will optimize a redirected call initiated on the transfer key. Station A calls Station B on Node 1. Station B puts the call on hold and initiates a call transfer over a SIP trunk to Station C on Node 2, which call forwards no answer to Station D on Node 1. While Station D is ringing (Station B hasn't completed the call transfer), optimization will be done by the TRO feature. If Station B completes the call transfer while Station C is ringing, and then the call is forwarded no answer to Station D, the TRO feature will optimize the redirected call and release the two SIP trunks connecting Node 1 and Node 2 before Station D answers the call.

**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 \(on separate Call Servers\)"](#) (page 48).

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” \(page 63\)](#)

[“IP Phone to IP Phone \(on separate Call Servers\)” \(page 64\)](#)

[“Call scenarios” \(page 75\)](#)

## 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.

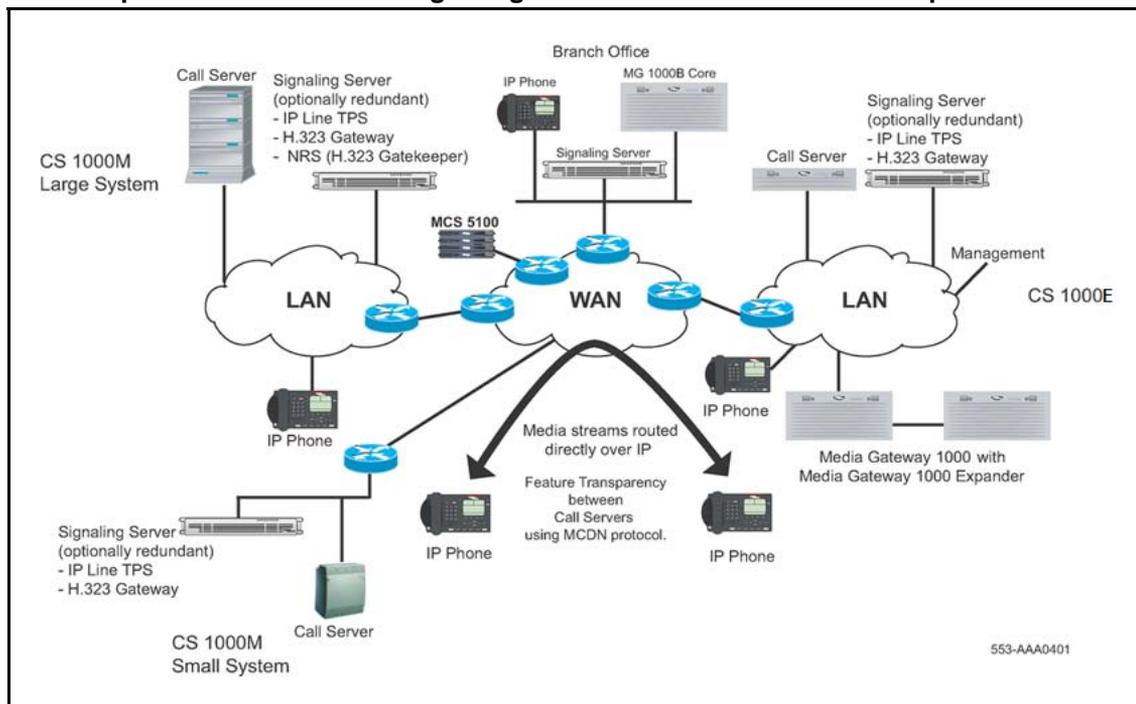
**Note 2:** A Media Gateway is a gateway that uses a protocol similar to the Media Gateway Control Protocol (MGCP). The Media Gateway houses peripheral cards. Media Gateways are controlled directly by the Call Server.

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 "An example of IP Peer Networking using Virtual Trunk and direct media paths" (page 64) 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 "User A dials User B" \(page 66\)](#)). 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” \(page 199\)](#).

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.

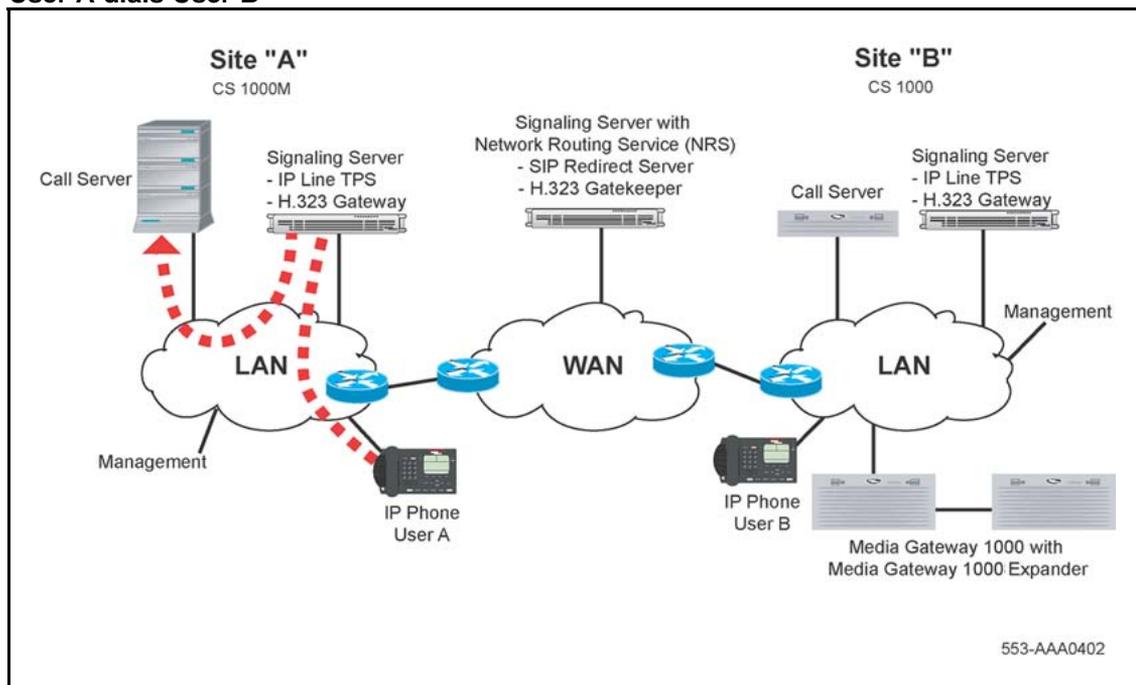
**Note 1:** Configure Virtual Trunk routes as circuit-switched routes. Use CS 1000 Element Manager or LD 14 and LD 16 in the Command Line Interface (CLI). [“Configuring the Virtual routes and trunks” \(page 141\)](#)

**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 “User A dials User B” \(page 66\)](#).

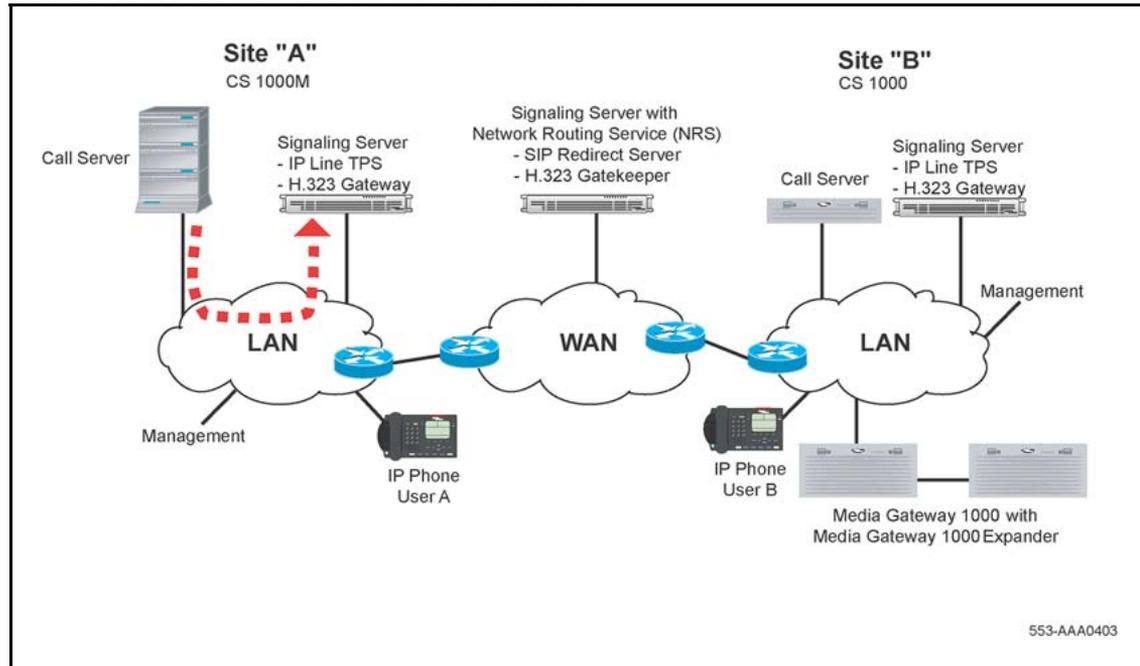
**Figure 15**  
**User A dials User B**



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 "Call Server A routes the call to the IP network"](#) (page 67).

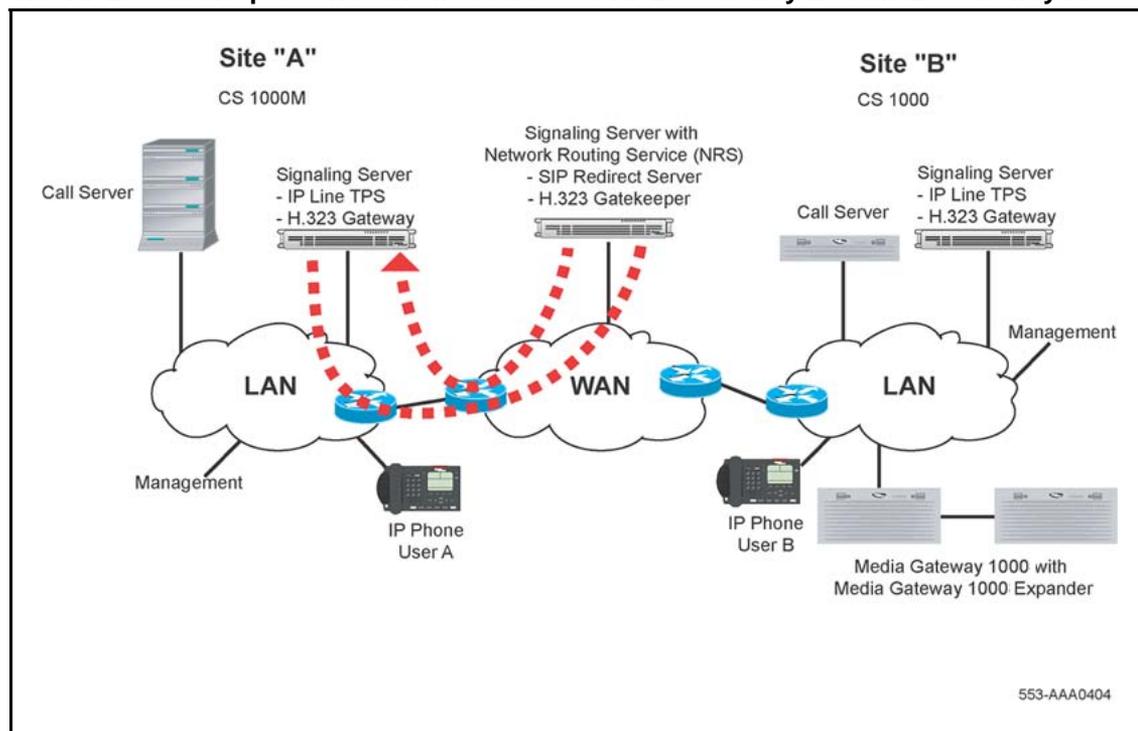
**Note:** To select which Virtual Trunk to use for routing, Call Server A examines the number dialed and uses various trunk routing and signaling features (for example, ESN and MCDN).

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



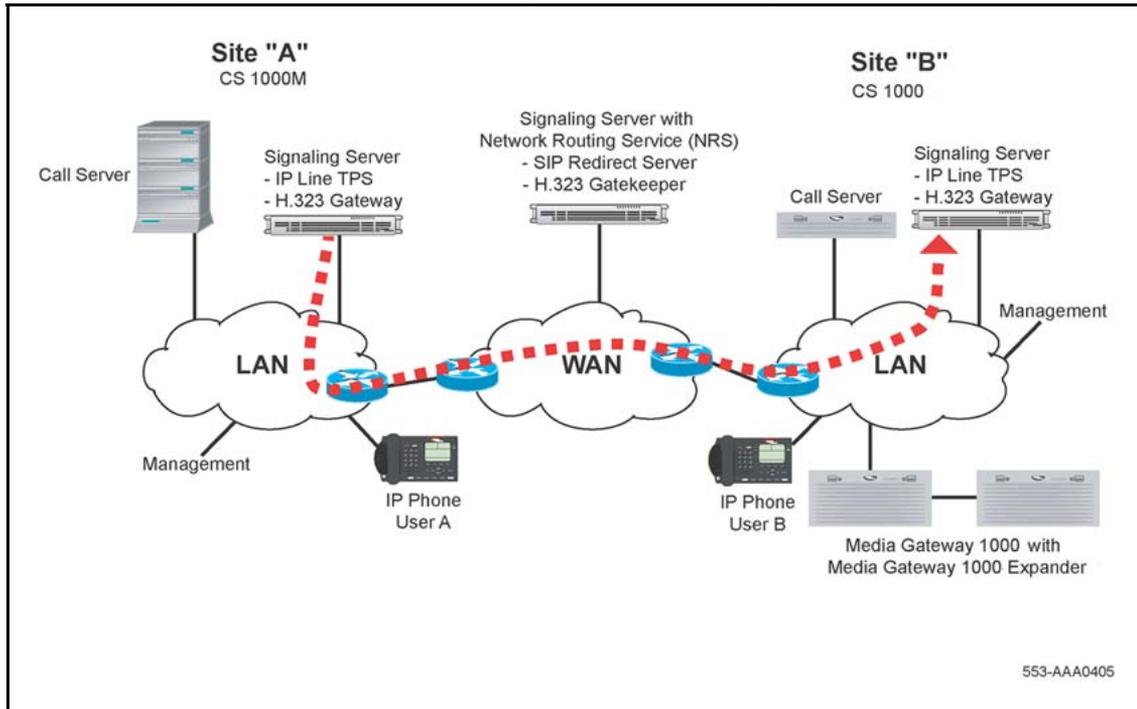
3. H.323 Gateway A asks the NRS (specifically the H.323 Gatekeeper) to search for the dialed DN in the database (for example, within the appropriate CDP domain). The NRS (H.323 Gatekeeper) sends the IP address of H.323 Gateway B to H.323 Gateway A. See [Figure 17 "The H.323 Gatekeeper sends the IP address of H.323 Gateway B to H.323 Gateway A"](#) (page 68).

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



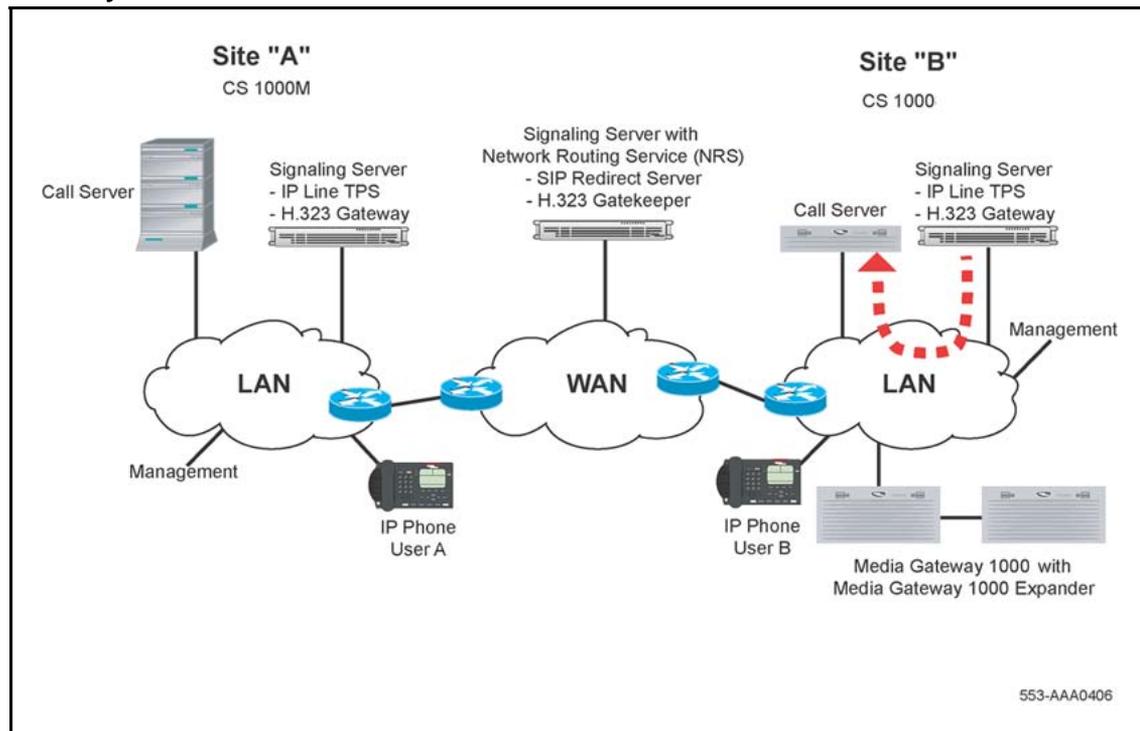
- H.323 Gateway A sends a SETUP message to H.323 Gateway B, including the DN information. See [Figure 18 "H.323 Gateway A sends a SETUP message to H.323 Gateway B"](#) (page 69).

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



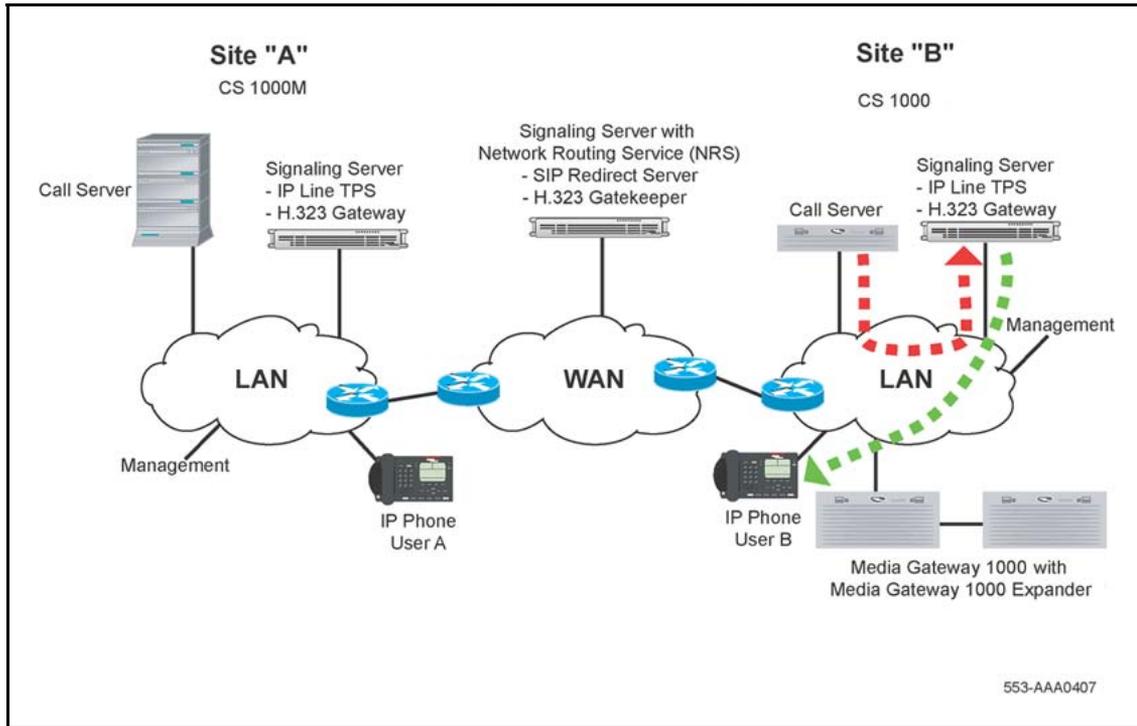
5. H.323 Gateway B treats the call as an incoming call from a Virtual Trunk. H.323 Gateway B sends the call to Call Server B over a Virtual Trunk. Call Server B also treats the call as an incoming call from a Virtual Trunk. See [Figure 19 "Gateway B sends the call to Call Server B over a Virtual Trunk"](#) (page 70).

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



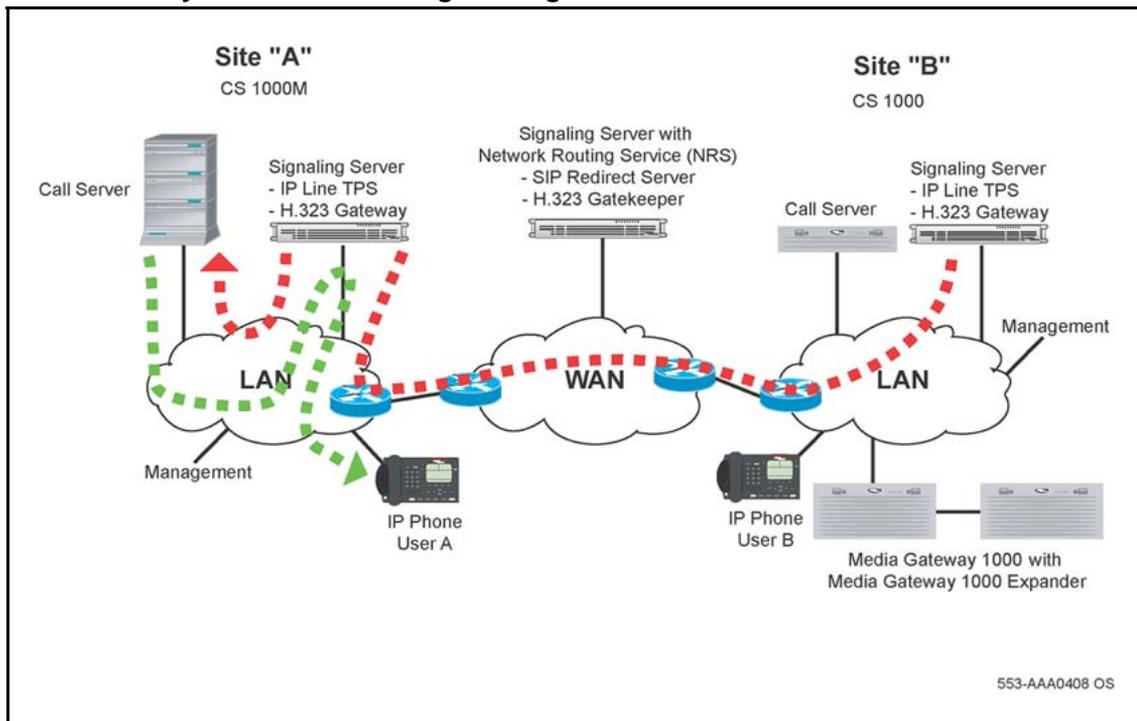
6. Call Server B selects the codec, allocates bandwidth, rings the telephone, and sends an alerting message to H.323 Gateway B. See [Figure 20 "Call Server B sends an alerting message to H.323 Gateway B"](#) (page 71).

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



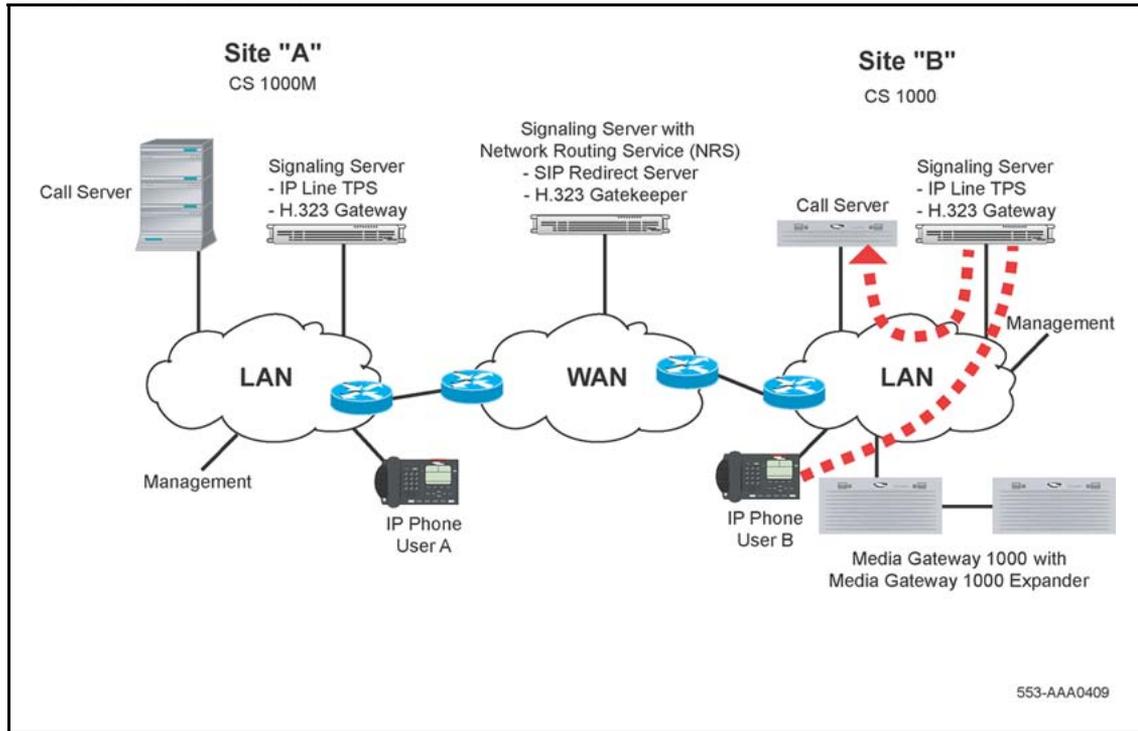
7. H.323 Gateway B sends an alerting message to Call Server A. Call Server A requests that the IP Phone play ringback tone. See [Figure 21 "H.323 Gateway B sends an alerting message to Call Server A"](#) (page 72).

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



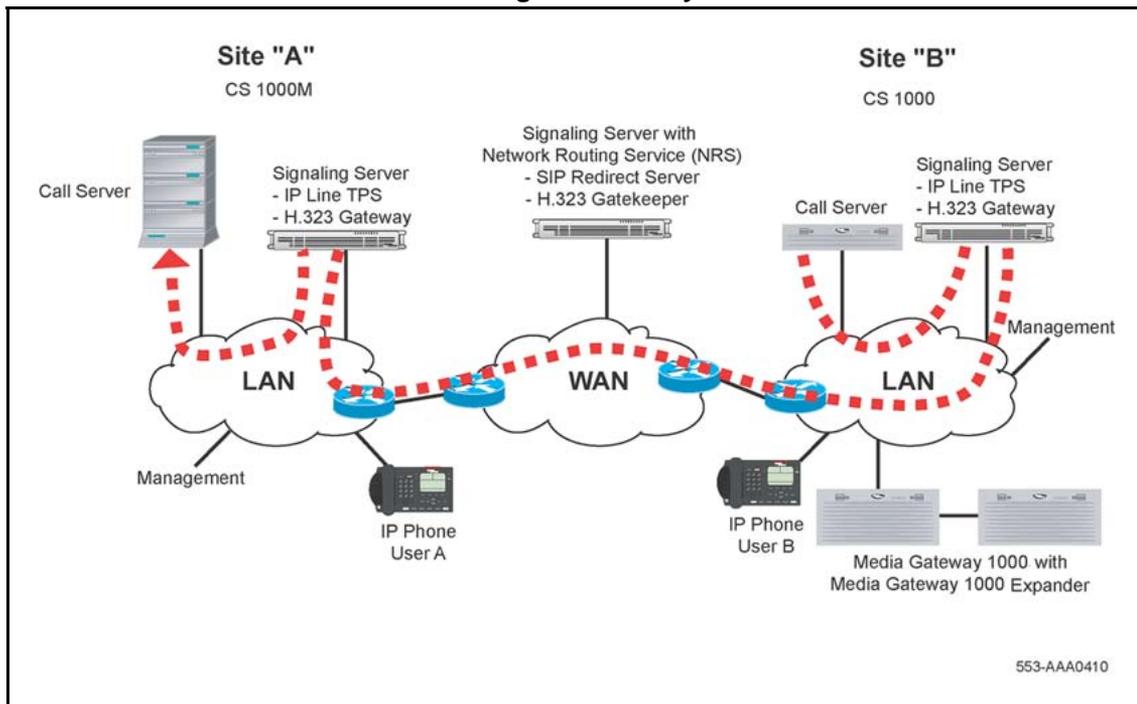
8. User B answers the call. A message is sent to Call Server B through the TPS on the Signaling Server. See [Figure 22 "User B answers the call"](#) (page 73).

**Figure 22**  
**User B answers the call**



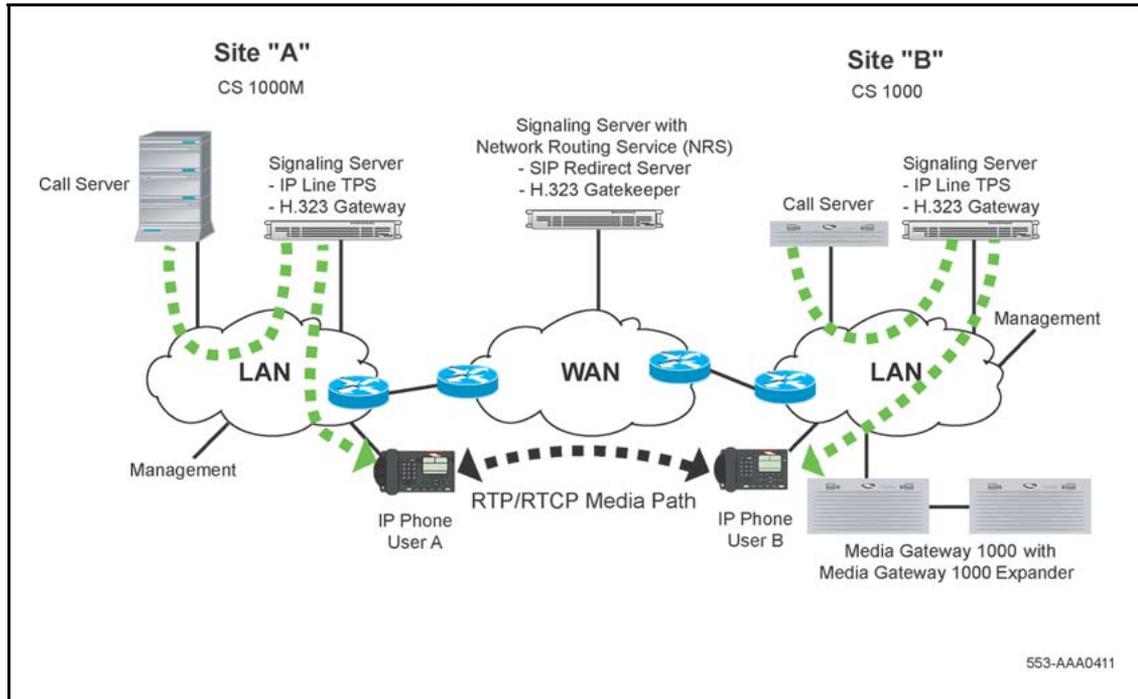
9. Call Server B sends a CONNECT message to H.323 Gateway B. H.323 Gateway B sends an H.323 CONNECT message to H.323 Gateway A and Call Server A. See [Figure 23 "Call Server B sends a CONNECT message to Gateway B"](#) (page 74).

**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 "IP Phones start the direct IP media paths"](#) (page 75).

**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.

**TRO versus TAT on transferred call** The TRO feature will optimize a redirected call initiated on the transfer key. Station A calls Station B on Node 1. Station B puts the call on hold and initiates a call transfer over an H.323 trunk to Station C on Node 2, which call forwards no answer

to Station D on Node 1. While Station D is ringing (Station B hasn't completed the call transfer), optimization will be done by the TRO feature. If Station B completes the call transfer while Station C is ringing, and then the call is forwarded no answer to Station D, the TRO feature will optimize the redirected call and release the two H.323 trunks connecting Node 1 and Node 2 before Station D answers the call.

**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 \(on separate Call Servers\)"](#) (page 48).

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" \(page 83\)](#)

["H.323-to-SIP signaling \(coexistence of both H.323 and SIP\)" \(page 83\)](#)

["Call scenarios summary" \(page 85\)](#)

["Call walk-through" \(page 85\)](#)

## Introduction

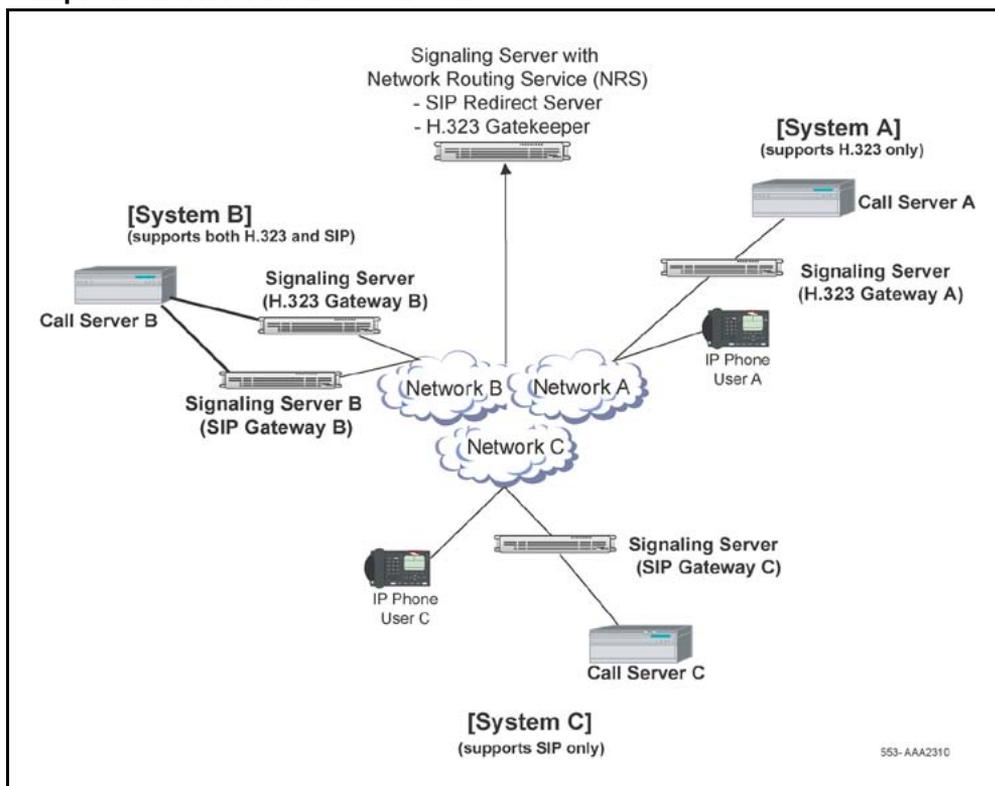
H.323 is used to set up and tear down H.323 calls, while SIP is used to set up and tear down SIP calls. If a network uses both the SIP and H.323 protocols, then an H.323-to-SIP "bridge" must exist between the H.323 domain and the SIP domain.

## 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 "Sample network for H.323-to-SIP call" \(page 84\)](#).

**Note:** In CS 1000 Release 5.0 (or later), RFC2833 provides digit handling for DTMF signaling. With RFC2833, CS 1000 systems can inter-operate with SIP-based devices that do not support out-of-band DTMF digit signaling. RFC2833 can be used for SIP calls only. H.323 and local calls are not supported.

**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 "Sample network for H.323-to-SIP call" \(page 84\)](#) 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](#)” (page 56) for SIP and “[Virtual Trunk to Virtual Trunk](#)” (page 77) 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 "Sample network for H.323-to-SIP call"](#) (page 84), 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).

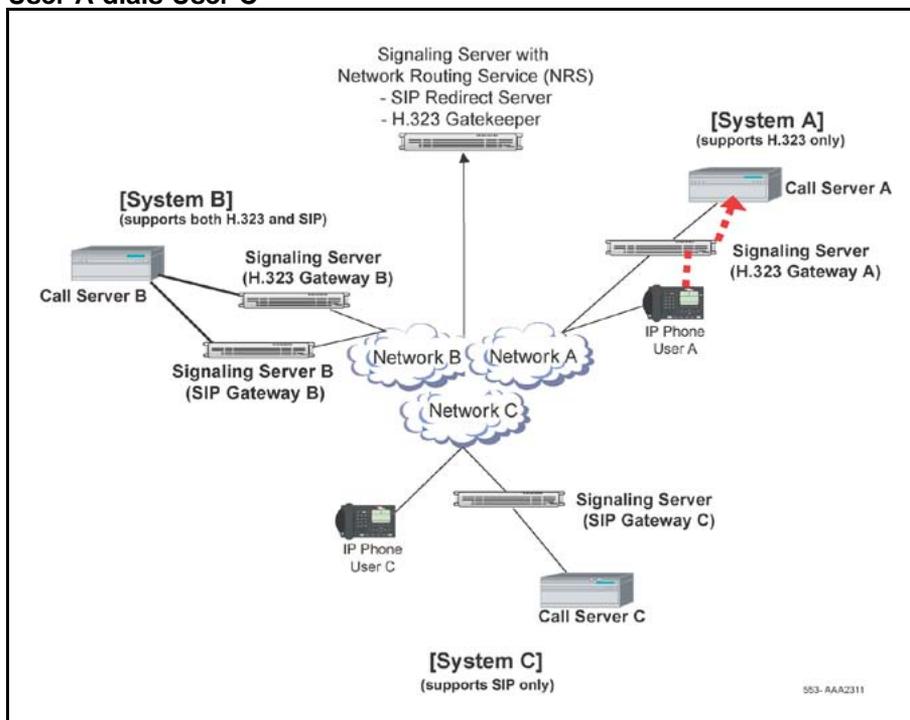
The following scenario describes the Direct IP Media Path functionality for a basic network call.

**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 "User A dials User C"](#) (page 86).

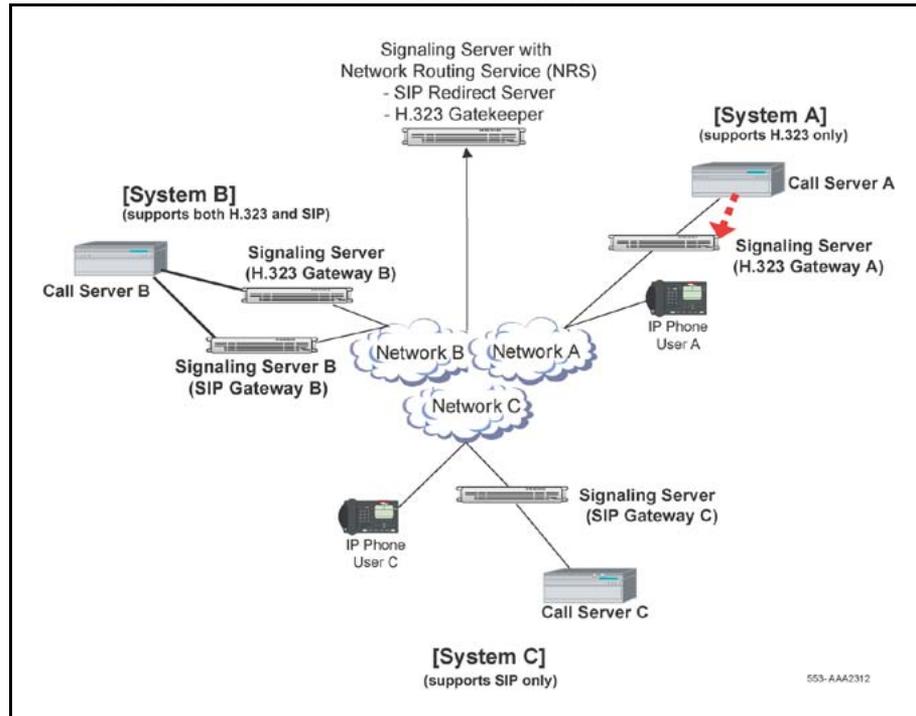
**Note:** The following call walk-through assumes that System A is using an H.323 Gateway only, System C is using a SIP Trunk Gateway only, and System B has both an H.323 Gateway and a SIP Trunk Gateway.

**Figure 26**  
**User A dials User C**



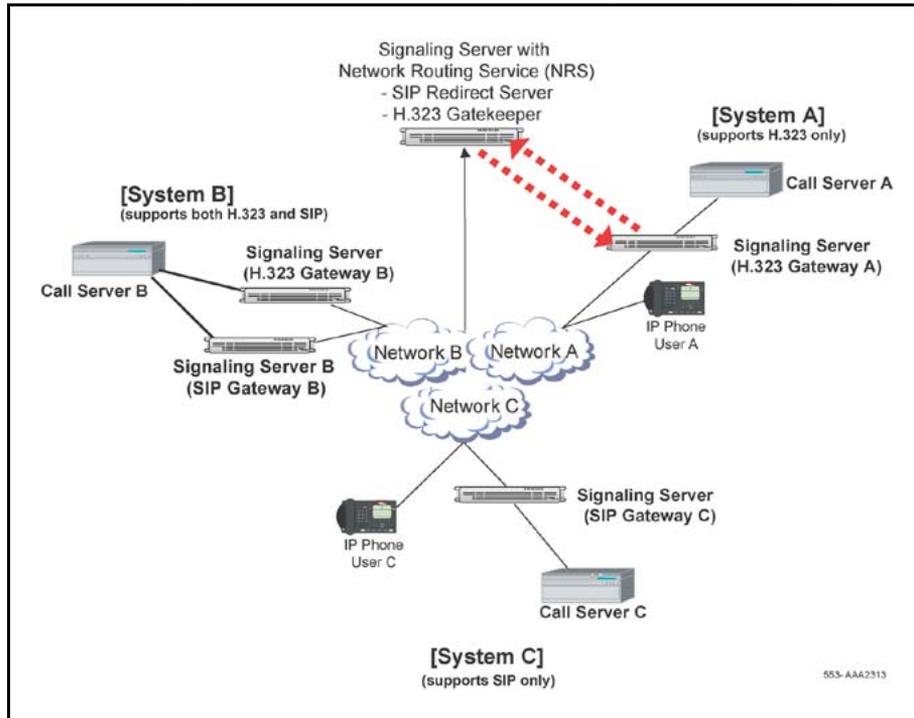
2. Call Server A determines that the dialed digits are at another site. Call Server A selects the codec list, allocates bandwidth, and routes the call to the IP network using a Virtual Trunk and H.323 Gateway A. See [Figure 27 "Call Server A routes the call to the IP network"](#) (page 87).

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



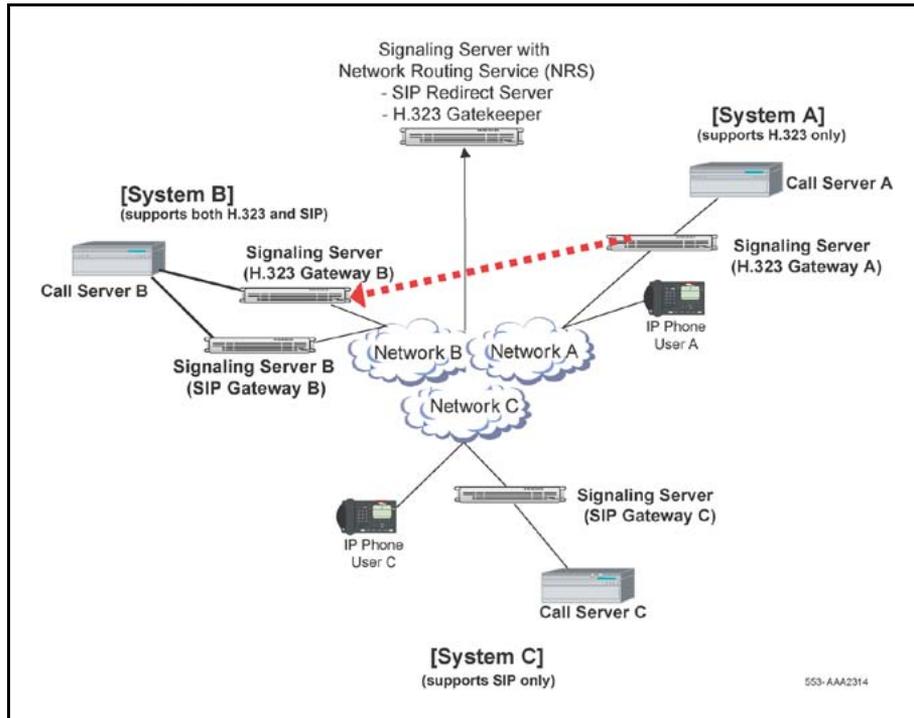
3. H.323 Gateway A asks the NRS (H.323 Gatekeeper) to search for the dialed DN in its database, as System A cannot go directly to System C because System A is using H.323 only and System C is using SIP. The NRS (H.323 Gatekeeper) responds back to H.323 Gateway A with the IP address of the H.323 Gateway B in System B. See [Figure 28 "H.323 Gateway A communicates with the NRS \(H.323 Gatekeeper\)"](#) (page 88).

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



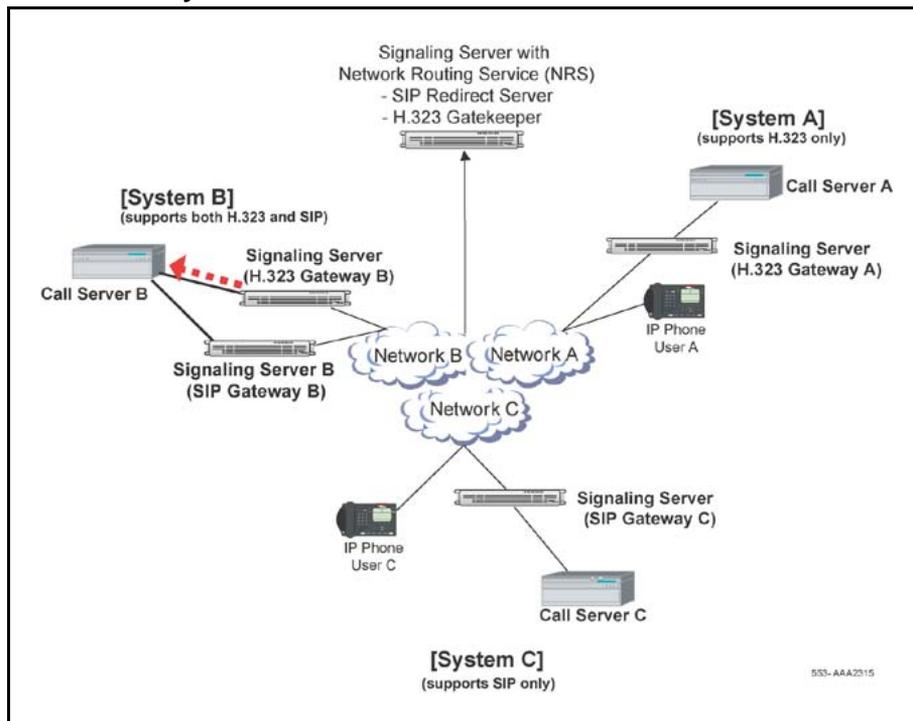
4. H.323 Gateway A sends an H.323 SETUP message to H.323 Gateway B including the DN information and IP Phone information (IP address and port number) for User A. See [Figure 29 "H.323 Gateway A sends information to H.323 Gateway B"](#) (page 89).

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



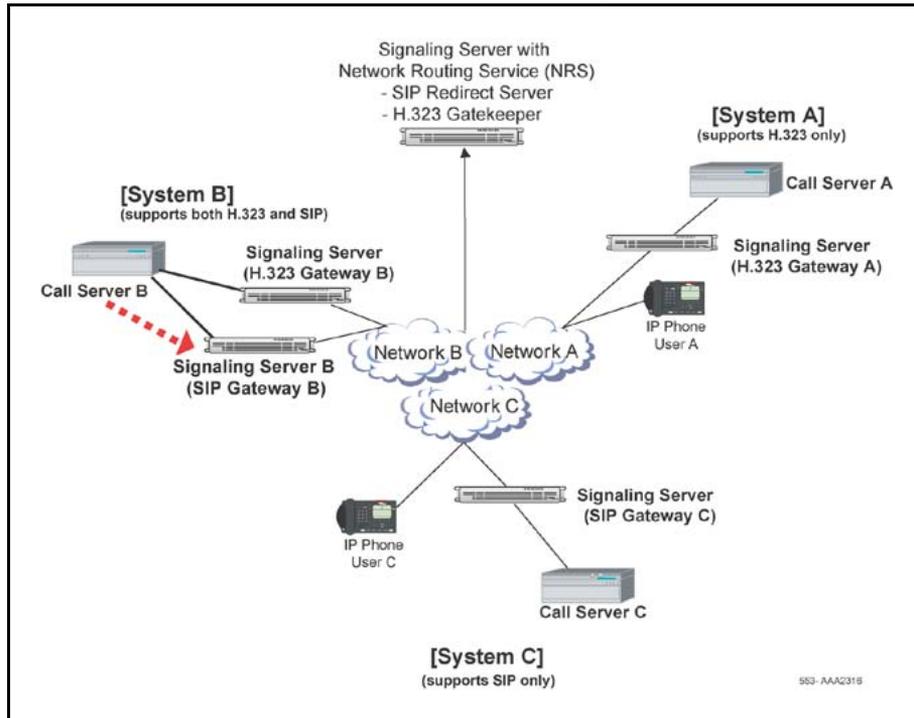
5. H.323 Gateway B receives the message from H.323 Gateway A and sends the call to Call Server B over a Virtual Trunk. Call Server B also treats the call as an incoming call from a Virtual Trunk. See [Figure 30 "H.323 Gateway B sends calls to Call Server B"](#) (page 90).

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



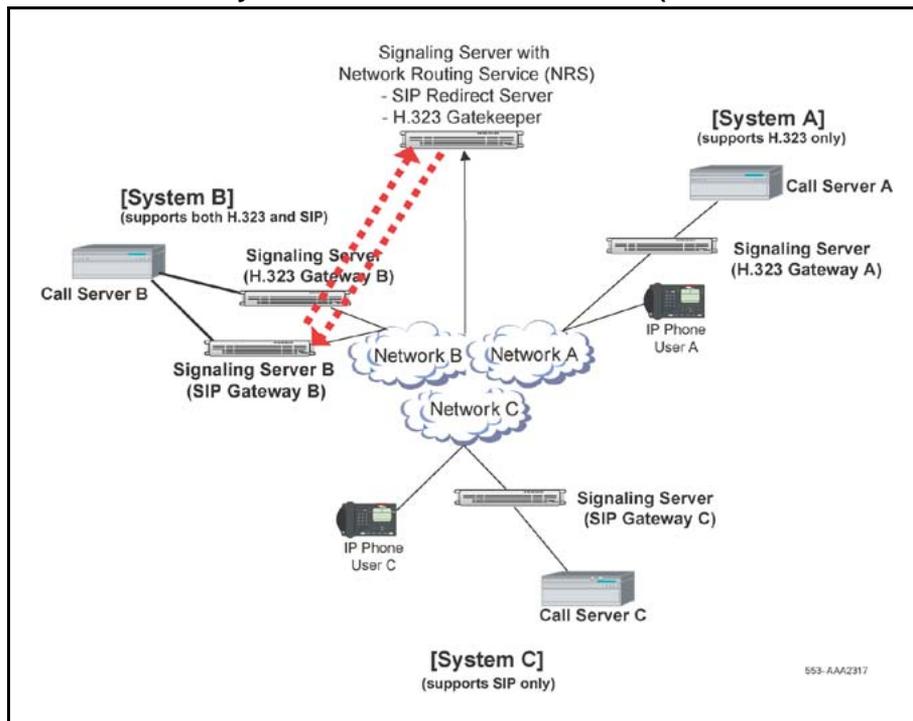
6. Call Server B processes the incoming message and determines that the call should go to System C through SIP Trunk Gateway B. Call Server B routes the call to SIP Trunk Gateway B. See [Figure 31 "Call Server B sends calls to SIP Trunk Gateway B"](#) (page 91).

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



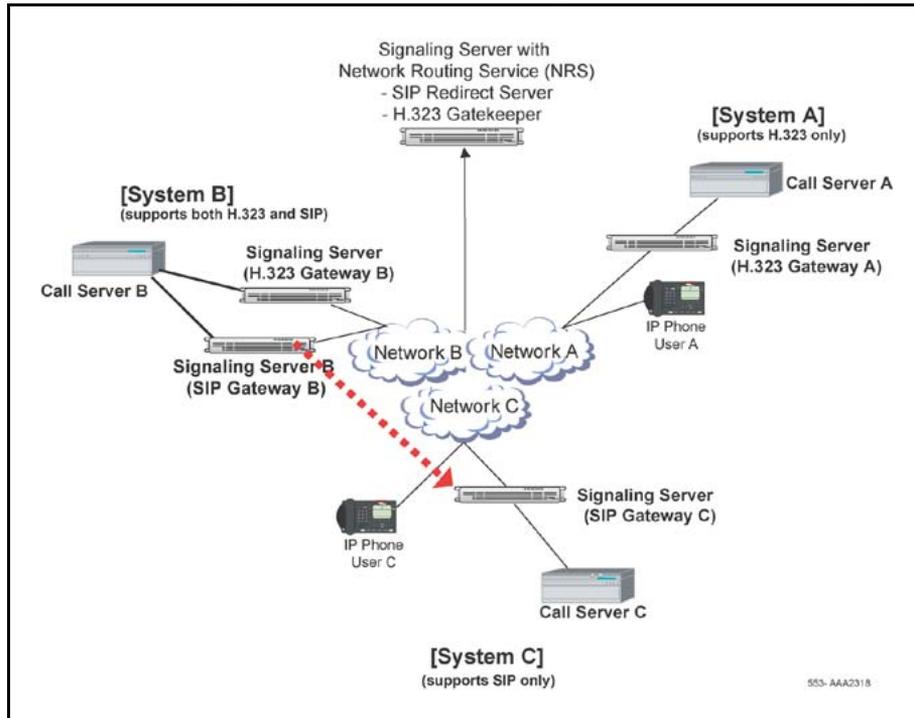
7. SIP Trunk Gateway B asks the NRS (SIP Redirect Server) to do a search for the DN of User C. The NRS (SIP Redirect Server) sends the IP address of SIP Trunk Gateway C to SIP Trunk Gateway B. See [Figure 32 "SIP Trunk Gateway B communicates with the NRS \(SIP Redirect Server\)"](#) (page 92).

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



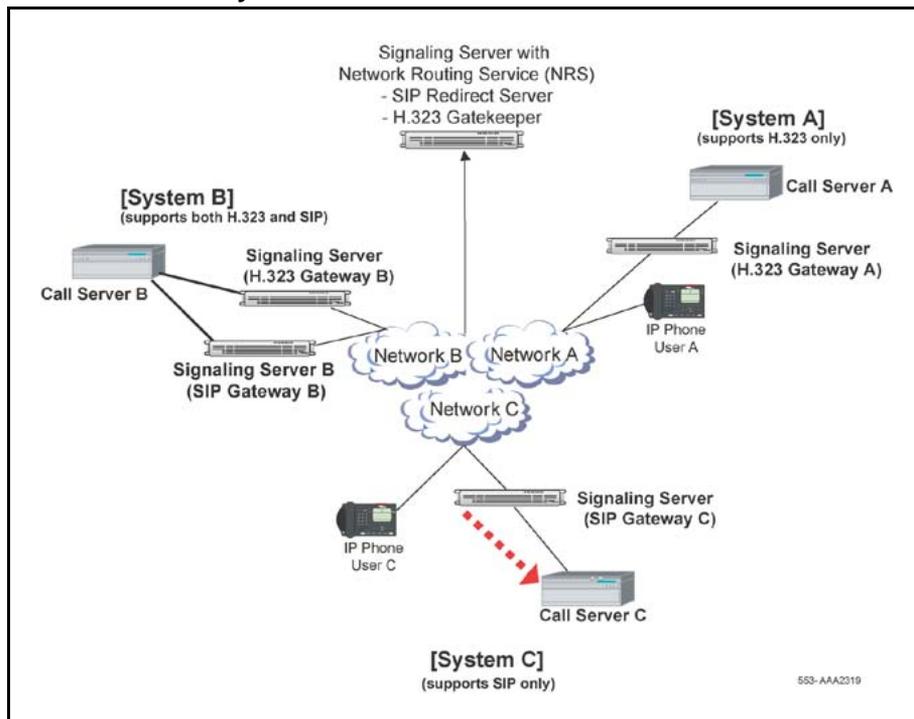
- SIP Trunk Gateway B sends an INVITE message to SIP Trunk Gateway C. See [Figure 33 "SIP Trunk Gateway B sends INVITE message to SIP Trunk Gateway C"](#) (page 93).

**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](#) "SIP Trunk Gateway C sends call to Call Server C" (page 93).

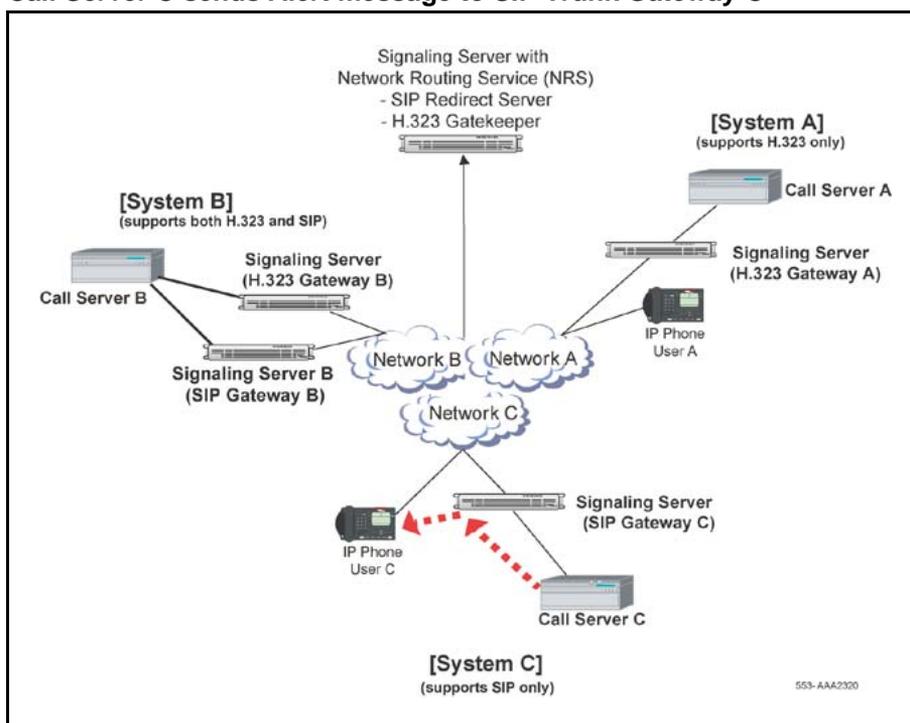
**Figure 34**  
**SIP Trunk Gateway C sends call to Call Server C**



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 "Call Server C sends Alert message to SIP Trunk Gateway C"](#) (page 94).

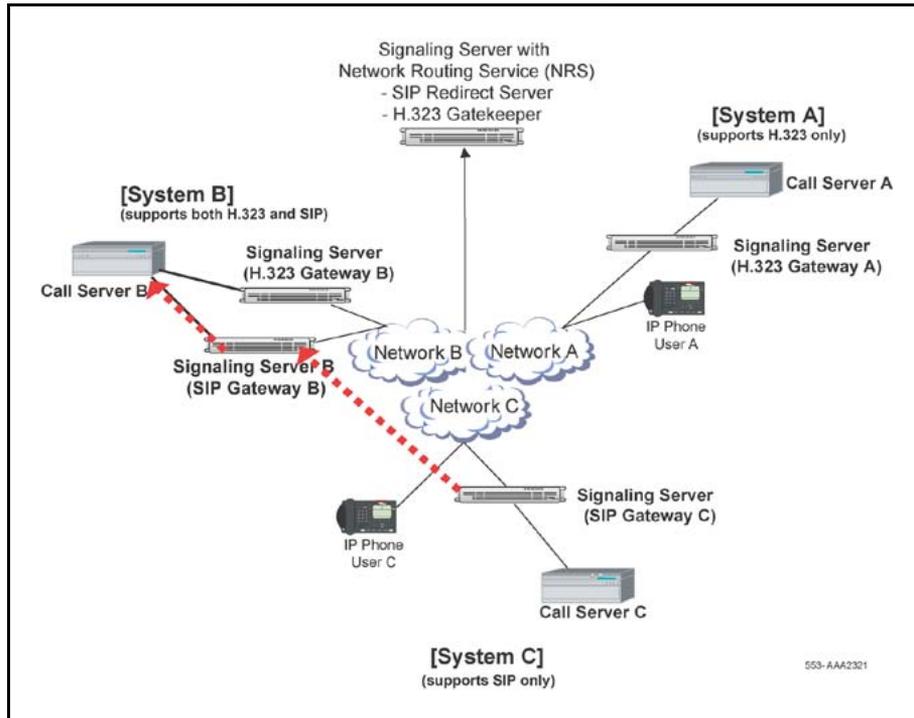
**Figure 35**

**Call Server C sends Alert message to SIP Trunk Gateway C**



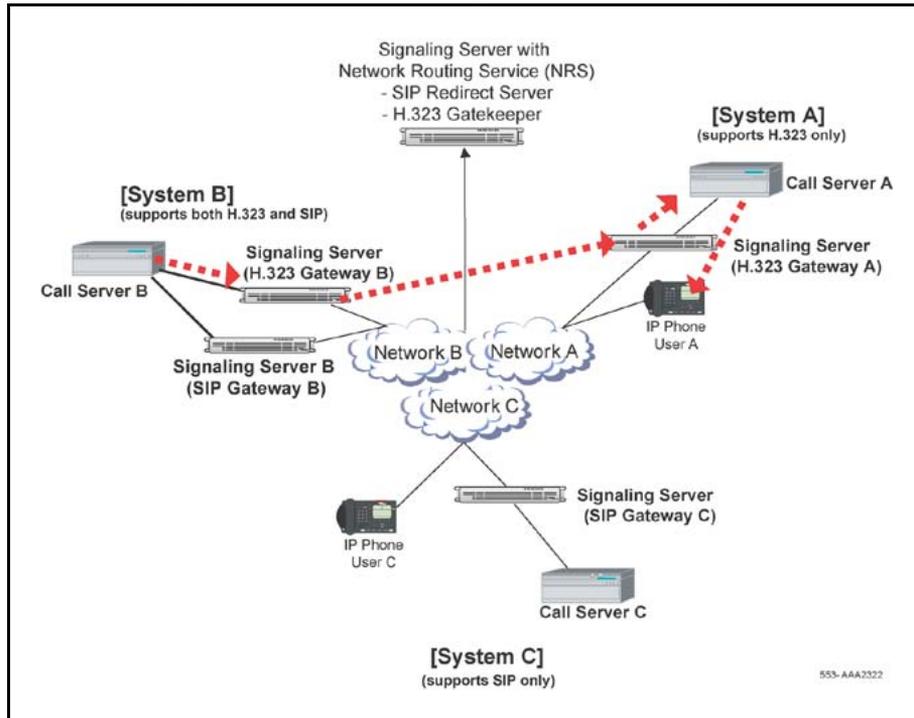
11. SIP Trunk Gateway C converts the ISDN Alert message to a SIP 180 response message. SIP Trunk Gateway C sends the SIP message to SIP Trunk Gateway B. SIP Trunk Gateway B converts the incoming SIP 180 response message back to the ISDN Alert message. SIP Trunk Gateway B then sends the message to Call Server B. See [Figure 36 "SIP Trunk Gateway B sends ISDN Alert message to Call Server B"](#) (page 95).

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



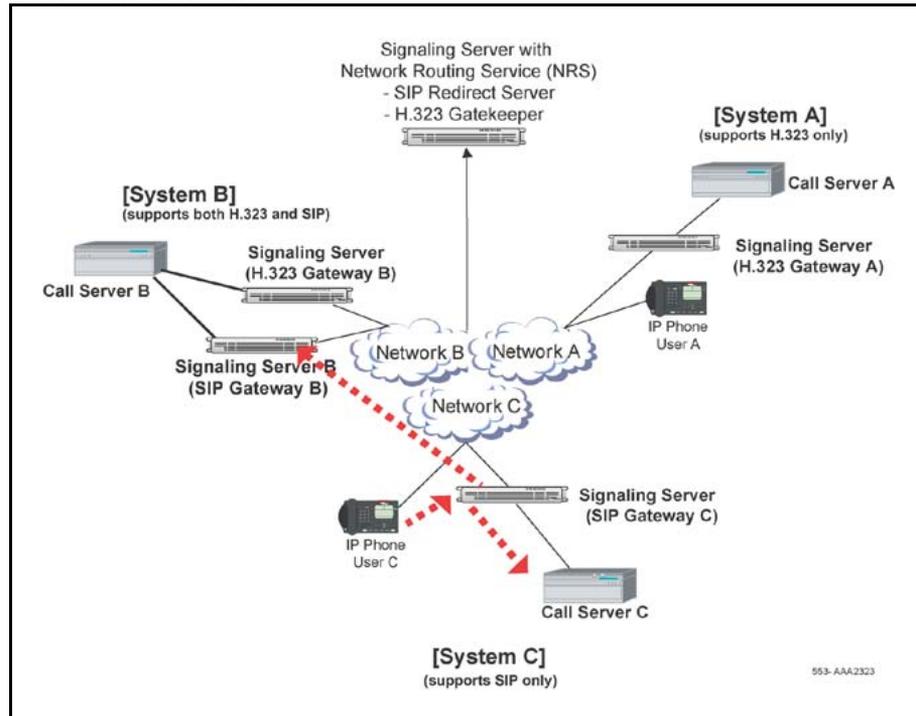
12. Call Server B forwards the ISDN Alert message to H.323 Gateway B. H.323 Gateway B sends the message to H.323 Gateway A. H.323 Gateway A sends the message to Call Server A. Call Server A requests that IP Phone User A play ringback tone. See [Figure 37 "H.323 Gateway B sends Alert message to H.323 Gateway A"](#) (page 96).

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



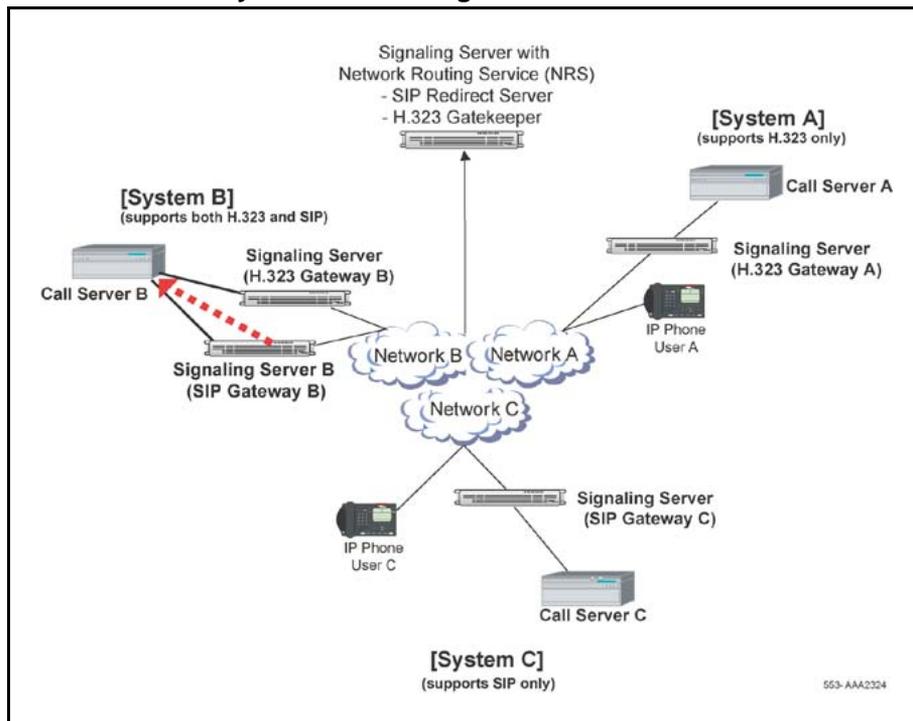
13. IP Phone User C answers the call. A message is sent to Call Server C on SIP Trunk Gateway C. SIP Trunk Gateway C sends a SIP 200 OK message along with the IP Phone information (IP address, port numbers, and codec) to SIP Trunk Gateway B. See [Figure 38 "User C answers the call"](#) (page 97).

**Figure 38**  
**User C answers the call**



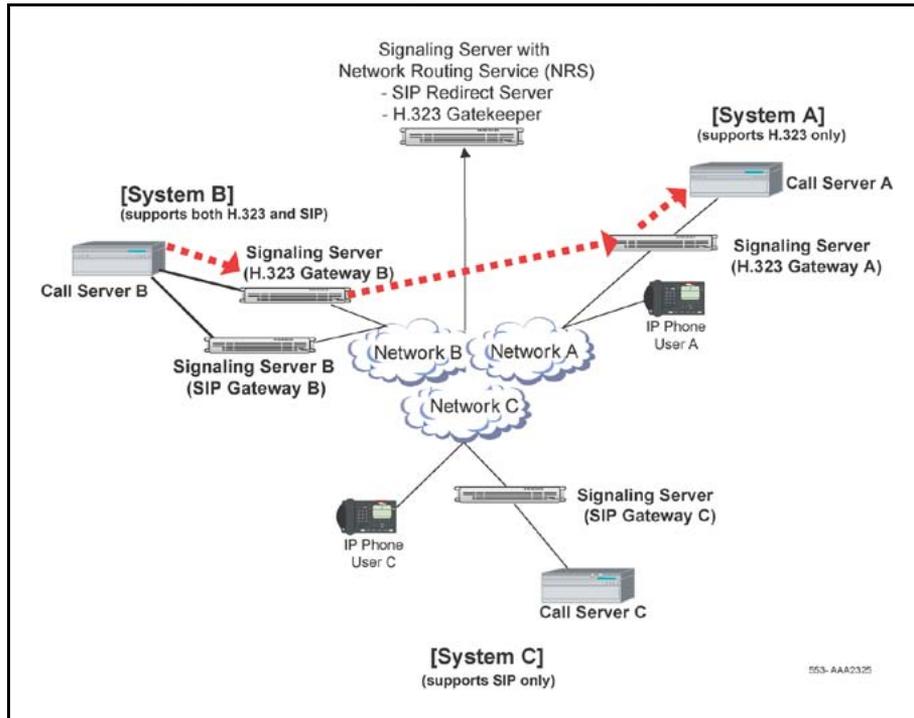
14. SIP Trunk Gateway B converts the SIP 200 OK message to an ISDN CONNECT message and sends the message to Call Server B. See [Figure 39 "SIP Trunk Gateway B sends message to Call Server B"](#) (page 98).

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



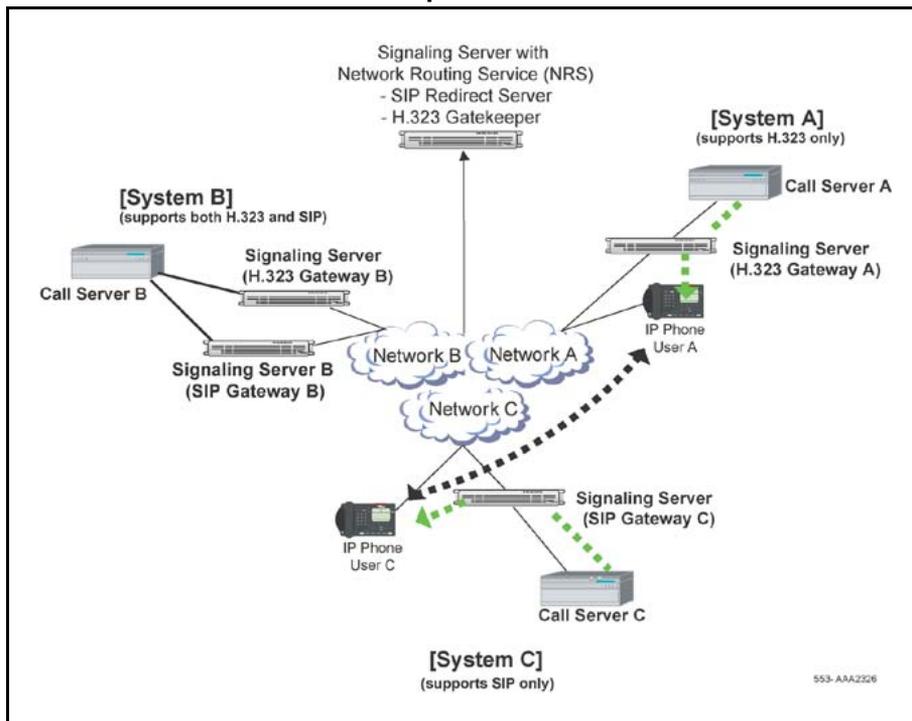
15. Call Server B forwards the ISDN CONNECT message to H.323 Gateway B. H.323 Gateway B then sends a message to H.323 Gateway A. H.323 Gateway A sends the message to Call Server A. See [Figure 40 "H.323 Gateway B sends message to H.323 Gateway A"](#) (page 99).

**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 "IP Phones start the direct media paths"](#) (page 100).

**Figure 41**  
**IP Phones start the direct media paths**



---

# Features

---

## Contents

This section contains information on the following topics:

- “Tone handling” (page 101)
  - “Progress tones” (page 101)
  - “End-to-end DTMF signaling” (page 102)
  - “DTMF out-of-band signals from H.323 trunk” (page 105)
  - “DTMF out-of-band signals from SIP trunk” (page 105)
- “Fax calls” (page 106)
  - “SIP” (page 106)
- “H.323” (page 106)
- “Reliability and redundancy” (page 109)
  - “Alternate Call Server” (page 110)
  - “Signaling Server software redundancy” (page 112)
  - “H.323 Gateway software trunk route redundancy” (page 113)
  - “SIP Trunk Gateway software trunk route redundancy” (page 113)
  - “NRS redundancy” (page 115)
  - “Campus-distributed Media Gateway in survival mode” (page 119)
  - “CS 1000M Large System CPU redundancy” (page 120)
- “Least Cost Routing” (page 123)
- “Licenses” (page 123)
- “Limitations” (page 124)

## 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”](#) (page 124).

### **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, See 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.

**Note:** RFC2833 allows interoperability with other SIP products that do not support out-of-band DTMF tones.

## **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 support and limitations, see *IP Trunk: Description, Installation, and Operation* ((NN43001-563)) .

## Fax/Modem pass through

The Fax/Modem pass through feature provides a modem pass through allowed (MPTA) class of service (CLS) for an analog phone TN. MPTA CLS dedicates an analog phone TN to a modem or a Fax machine terminal. A connection that initiates from the dedicated TN, and/or calls that terminate at the dedicated TN through a Digital Signal Processor (DSP), use a G711 NO VAD codec on the Call Server.

Modem Pass through is a specific configuration of a G.711 VoIP channel that improves modem performance compared to standard VoIP configuration. Auto switch to Voice Band Data (VBD) is a feature of the DSP; the DSP monitors the data stream to distinguish between voice and data calls. The DSP reconfigures to modem pass through mode when it determines the call is a modem call.

For modem calls between CS 1000 systems connected by analog and digital trunks, you must configure MPTA CLS on the Call Server of each CS 1000 system for analog units connected to modems. MPTA CLS configuration is necessary because the call setup negotiation is not done end to end as it is for virtual trunks. If the analog unit on one Call Server uses MPTA CLS and the analog unit on the other Call Server uses modem pass through denied (MPTD) CLS, the modem call fails.

MPT CLS is supported by the G.711 codec only; MPT CLS includes no other codecs. The packet interval for G.711 codec is set to 20 msec in MPT.

The maximum speed supported for modem and fax is 33.6 Kbp/s. This limit is imposed by the analog line card.

MPT allows CS 1000 to support the following:

- modem pass through
- Super G3 (SG3) fax at V.34 (33.6 Kbp/s)
- V.34 rate (33.6 Kbp/s) modems
- Fax machines that support V.17, V.27, V.29, and V.34 protocols

For interface commands, responses, and definitions for MPT see [Table 8 "Interface commands and responses"](#) (page 108).

**Table 8**  
Interface commands and responses

Command prompt	User response	Description
CLS	MPTA	Turn on the MPT feature.
CLS	MPTD	Turn off the MPT feature.

**Note:** CLS MPTA and MPTD is included in LD10 (analogue devices) .

For information about feature packaging requirements, see [Table 9](#) "Feature packaging requirements" (page 108).

**Table 9**  
Feature packaging requirements

Package mnemonic	Package number	Package description	Package type (new, existing, or dependency)	Applicable market
Softswitch	402	Identifies a softswitch system.	Existing	All
IPMG	403	Identifies a system that is equipped with IPMGs.	Existing	All

### Modem traffic

CS 1000E supports modem traffic in a campus-distributed network with the following characteristics:

- Media card configuration:
  - G.711 codec
  - 20 msec packet size
- one-way delay less than 5 msec
- low packet loss
- V.34 rate (33.6 Kbp/s)

**Note:** Performance degrades significantly with packet loss.

**ATTENTION**

Nortel has conducted extensive but not exhaustive tests of modem-to-modem calls, data transfers, and file transfers between a CS 1000E and MG 1000E, using Virtual Trunks and PRI tandem trunks. While all tests have been successful, Nortel cannot guarantee that all modem brands will operate properly over all G.711 Voice over IP (VoIP) networks. Before deploying modems, test the modem brand within the network to verify reliable operation. Contact your system supplier or your Nortel representative for more information.

**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 "Reliability and redundancy features by system type" \(page 109\)](#) shows each reliability and redundancy feature and the systems that support the feature. The reliability and redundancy features include:

- ["Alternate Call Server" \(page 110\)](#)
- ["Signaling Server software redundancy" \(page 112\)](#) (including H.323/SIP Trunk Gateway and IP Phone software)
- ["H.323 Gateway software trunk route redundancy" \(page 113\)](#) (H.323 Gateway interface to Gatekeeper redundancy [Failsafe Gatekeeper])
- ["SIP Trunk Gateway software trunk route redundancy" \(page 113\)](#)
- ["NRS redundancy" \(page 115\)](#)
- ["Campus-distributed Media Gateway in survival mode" \(page 119\)](#)
- ["CS 1000M Large System CPU redundancy" \(page 120\)](#)

[Table 10 "Reliability and redundancy features by system type" \(page 109\)](#) 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 Large Systems		
	CS 1000E	CS 1000M Single Group	CS 1000M Multi Group
Alternate Call Server	X		
Signaling Server software redundancy	X	X	X
NRS redundancy	X	X	X
<b>Note 1:</b> For CS 1000E redundancy, refer to <i>Communication Server 1000E: Planning and Engineering (NN43041-220)</i> .			
<b>Note 2:</b> For Geographic Redundancy, refer to <i>System Redundancy Fundamentals (NN43001-507)</i> .			

**Table 10**  
**Reliability and redundancy features by system type (cont'd.)**

Reliability and Redundancy Features	CS 1000M Large Systems		
	CS 1000E	CS 1000M Single Group	CS 1000M Multi Group
SIP Trunk Gateway	X	X	X
H.323 Gateway	X	X	X
Campus distributed Media Gateway in survival mode	X		
CPU redundancy		X	X
Survivable IP Expansion (SIPE)	X		
<p><b>Note 1:</b> For CS 1000E redundancy, refer to <i>Communication Server 1000E: Planning and Engineering (NN43041-220)</i>.</p> <p><b>Note 2:</b> For Geographic Redundancy, refer to <i>System Redundancy Fundamentals (NN43001-507)</i>.</p>			

### 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.

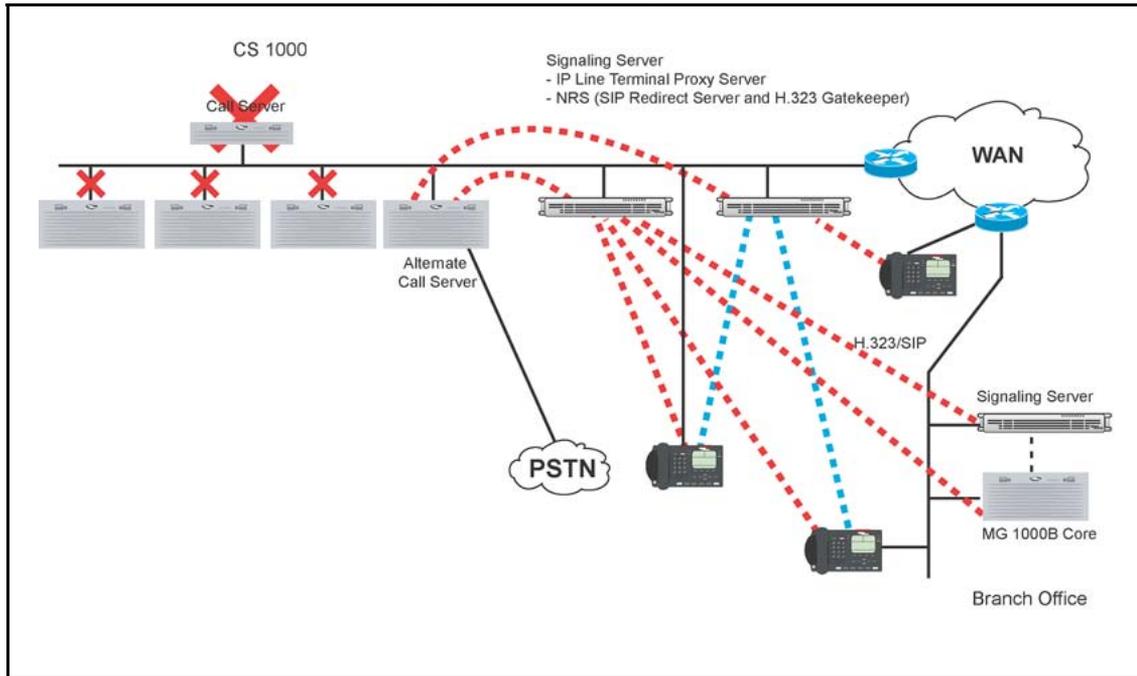
The Alternate Call Server IP address must be in the same ELAN subnet as the Primary Call Server IP address.

The Alternate Call Server is applicable only to the CS 1000Esystem and CS 1000MSmall Systems.

As an example, [Figure 42 "Example Normal mode of operation for a CS 1000Esystem" \(page 111\)](#) shows the normal mode of operation for a CS 1000Esystem.



**Figure 43**  
**Call Server failure and redundancy in a CS 1000Esystem**



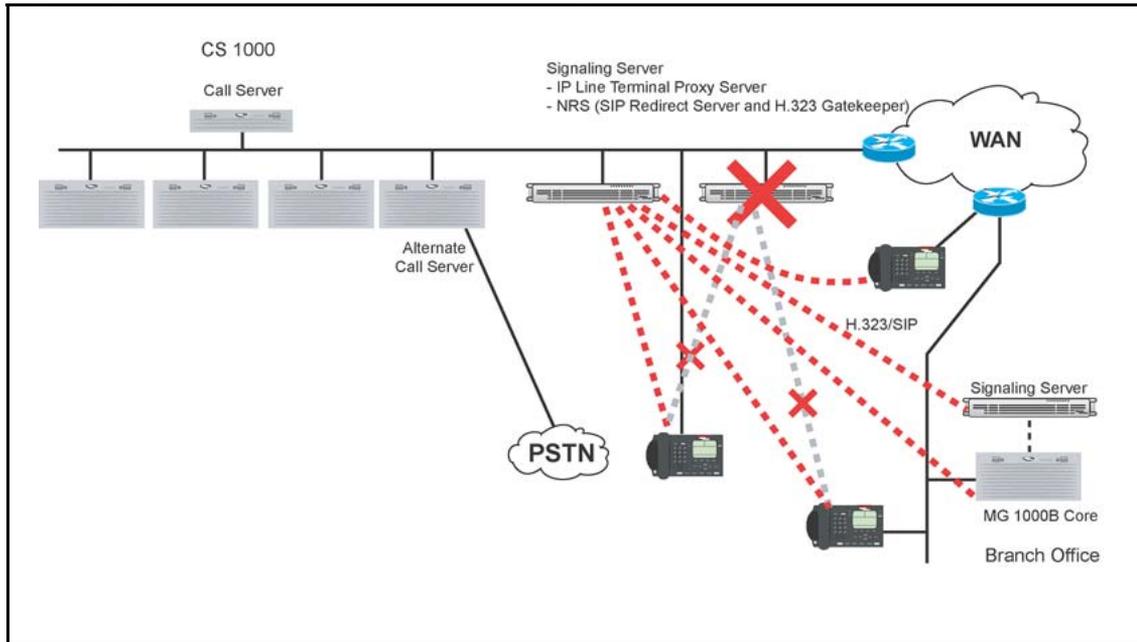
### Signaling Server software redundancy

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 44 "Signaling Server redundancy in a CS 1000Esystem" \(page 113\)](#) shows Signaling Server redundancy in a CS 1000Esystem. 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 44**  
**Signaling Server redundancy in a CS 1000Esystem**



### 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.

### **SIP Proxy Trunk Gateway software trunk route redundancy**

The following scenario applies to the SIP Proxy Trunk gateway.

When active calls are switched from a follower Signaling Server to a leader Signaling Server and vice versa:

1. Since this is not a hot standby redundancy and non-loadsharing implementation, there will be a complete loss of service for virtual trunking for 2 to 30 seconds when switching from the leader to follower Signaling Server. (The loss of service will be about 10 seconds if the leader goes down or if the TLAN goes down and 2 minutes if the ELAN goes down).
2. When a VTRK switch over occurs, all of the idle VTRKs will register to the new master and active VTRKs will be kept on the old master.
3. When a call over a Signaling Server is released from the far end, the follower is not the master anymore and the near end VTRK is not released until the near end hangs up. If for some reason the near end fails to hang up the VTRK stays busy.
4. When a call over a Signaling Server is released from the near end, the follower is not the master anymore and the far end VTRK is not released until the far end hangs up. If for some reason the far end fails to hang up the VTRK stays busy.

## 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.

By optimizing timeout and threshold parameters used in retries of the heartbeat mechanism, ungraceful switchover trigger time is reduced to less than 15 seconds with CS Release 5.0 (or later). The optimization in the timing leads to a change in the INI policy. When the active core warm starts, the inactive core also reboots, so no swapping of the cores takes place.

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

For NRS/SIP Redirect Server redundancy, see [“NRS SIP Redirect Server redundancy” \(page 118\)](#).

### 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.

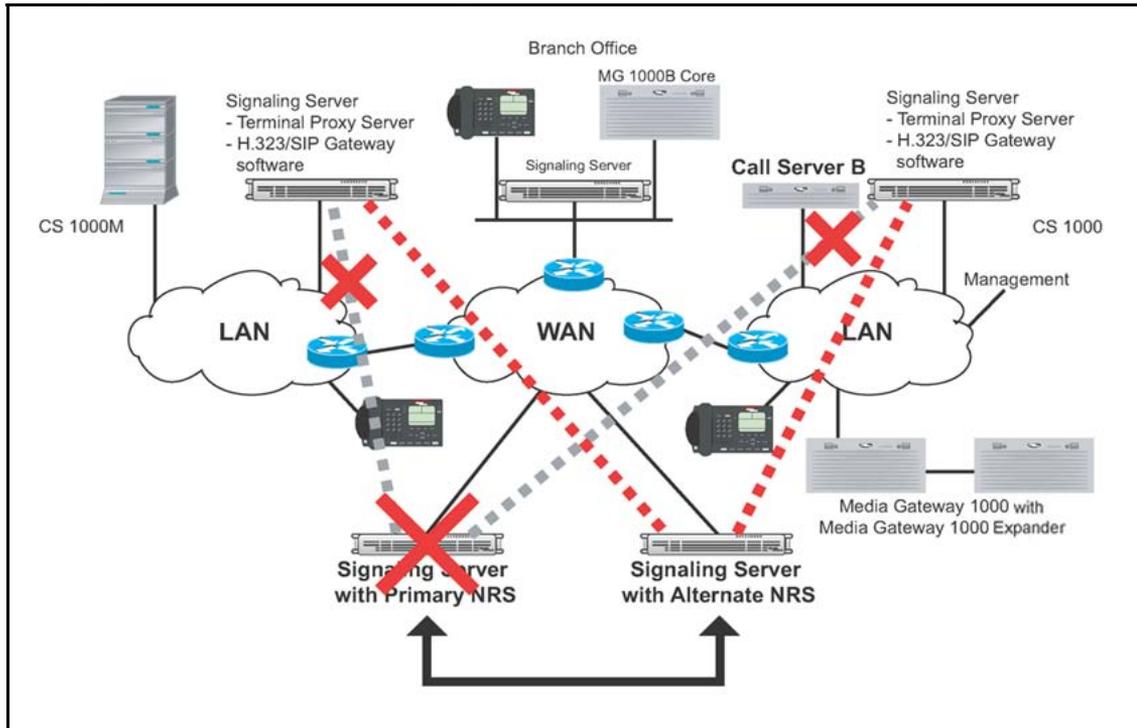
**Polling and switchover** A Time-to-Live timer is provided to ensure that if a Gatekeeper stops responding for a specified amount of time, the H.323 Gateway software registers at the Alternate Gatekeeper to resume operation. This ensures Gatekeeper redundancy across the network.

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*). 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 45 "Primary NRS failure and redundancy" \(page 117\)](#) 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 45**  
**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. When a failsafe GW registers to itself it always sends the registration message over UDP.

### **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:

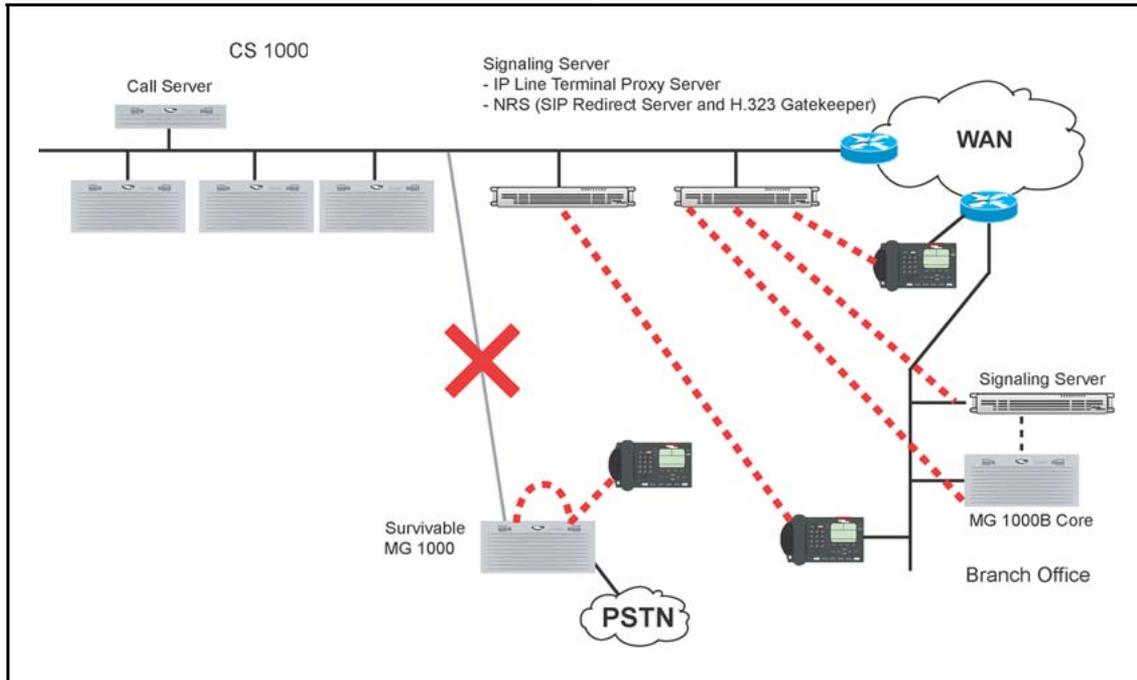
- CS 1000ESystem
- CS 1000MSystem

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 46 "Network failure with Survivable Media Gateways" \(page 120\)](#) illustrates how such an outage is handled.

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

<b>Step</b>	<b>Action</b>
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.
--End--	

**Figure 46**  
**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 Signaling 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 "Health count" \(page 121\)](#) shows the health count scheme.

**Table 11**  
**Health count**

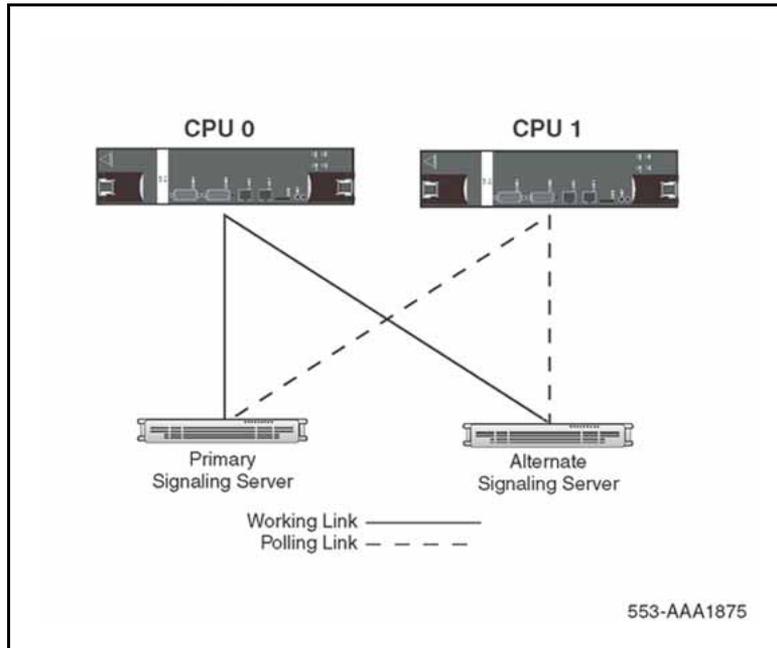
Number of cards	Health count
2 or 3 cards	1 health count
4 or 5 cards	2 health counts
6 or 7 cards	3 health counts
8 or 9 cards	4 health counts
...	...

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 47 "Health Monitoring" \(page 122\)](#) illustrates health monitoring under normal operation.

**Figure 47**  
**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.

**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* ((NN43001-579)) .

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*.

**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 Commissioning ((NN43011-310))*
- *Communication Server 1000M and Meridian 1: Large System Installation and Commissioning ((NN43021-310))*
- *Communication Server 1000E: Installation and Commissioning ((NN43041-310))*

## 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 UNISlim 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.

---

# Configure IP Peer Network

---

## Contents

This section contains information on the following topics:

- “Overview” (page 126)
- “Task summary” (page 127)
- “Launching Element Manager” (page 129)
  
- “Using Element Manager for configuration” (page 135)
  - “Configuring the Customer Data Block” (page 136)
  - “Configuring D-channels” (page 138)
  - “Configuring the Virtual routes and trunks” (page 141)
  - “Configuring networking” (page 149)
  - “Configuring call routing” (page 153)
  - “Configuring call types” (page 157)
  - “Configuring digit manipulation tables” (page 167)
- “Feature Implementation of IP Peer Networking” (page 168)
  - “Task summary list” (page 168)
  - “VNR enhancement” (page 179)
- “Configuring the Gateways” (page 188)
  - “Enabling and configuring the H.323 Gateway” (page 188)
  - “Enabling and configuring the SIP Trunk Gateway” (page 191)
- “Restarting the Signaling Server” (page 198)
  - “Warm restart” (page 198)
  - “Cold restart” (page 198)

## Overview

You use the following interfaces for configuring various components of IP Peer Networking:

- CS 1000 Element Manager
- Command Line Interface (CLI)
- NRS Manager
- Telephony Manager (TM)

**Note:** You can use TM to launch Element Manager. Refer to *Telephony Manager 3.1: System Administration* ( NN43050-601)) for detailed information on TM.

This chapter provides instructions on how to implement IP Peer Networking in your IP Peer network using overlays and Element Manager. Once you implement the IP Peer network, you must configure data in the NRS. For information about configuring data in the NRS, see *Network Routing Service Installation and Commissioning* (NN43001-564) .

For information about how to install system components and how to perform basic configuration, see the following NTPs:

- *Communication Server 1000M and Meridian 1: Small System Installation and Commissioning* ((NN43011-310))
- *Communication Server 1000M and Meridian 1: Large System Installation and Commissioning* ((NN43021-310))
- *Communication Server 1000E: Installation and Commissioning* ((NN43041-310))

For a description of system management, refer to *System Management* ((NN43600)). For a detailed description of Element Manager, refer to *Element Manager: System Administration* ((NN43001-632)).

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 TM to access the Web server running on the Signaling Server.

## Task summary

You must configure the following data when setting up an IP network:

1. Plan your Network Numbering Plan. Refer to *Dialing Plans: Description* ((NN43001-283)) .
  - 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 Commissioning* ((NN43011-310))
  - *Communication Server 1000M and Meridian 1: Large System Installation and Commissioning* ((NN43021-310))
  - *Communication Server 1000E: Installation and Commissioning* ((NN43041-310))
  - *Signaling Server Installation and Commissioning* ((NN43001-312))
3. Configure the Primary, Alternate, and Failsafe NRS at installation and initial setup of the Signaling Server. See *Signaling Server Installation and Commissioning* ((NN43001-312)) .

**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”](#) (page 136) and [“Feature Implementation of IP Peer Networking”](#) (page 168).

5. Configure the D-channel using Element Manager or the Command Line Interface (LD 17). See [“Configuring D-channels” \(page 138\)](#) and [“Feature Implementation of IP Peer Networking” \(page 168\)](#).
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” \(page 141\)](#). For the CLI procedure, see [“Feature Implementation of IP Peer Networking” \(page 168\)](#).

8. Configure the Virtual Trunks using Element Manager (see [“Configuring the Virtual routes and trunks” \(page 141\)](#)) or the Command Line Interface (LD 14) and [“Feature Implementation of IP Peer Networking” \(page 168\)](#).
9. Use Element Manager or the Command Line Interface (CLI) to configure networking ([“Configuring networking” \(page 149\)](#)) and numbering plan features ([“Configuring call routing” \(page 153\)](#)) 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](#)).
11. Configure dialing plan information for calls that must be routed to circuit-switched trunks (for example, PSTN interfaces). See *Dialing Plans: Description* ((NN43001-283) ) and *IP Trunk: Description, Installation, and Operation* ((NN43001-563)) .
12. Configure the gateways. See [“Configuring the Gateways” \(page 188\)](#).

- See “Enabling and configuring the H.323 Gateway” (page 188)
- “Enabling and configuring the SIP Trunk Gateway” (page 191)

13. Configure the NRS.

## Launching Element Manager

Element Manager (EM) for CS 1000 Release 5.0 (or later) software is offered in two versions: a Linux-based EM and a VxWorks-based EM.

The Linux-based EM is a component of the Nortel Enterprise Common Manager (ECM). The ECM provides security and navigation infrastructure services for the Web-based management applications: Element Manager and NRS Manager. Refer to *Enterprise Common Manager Fundamentals (NN43001-116)* for detailed information on ECM.

Element Manager is supported only on Microsoft® Internet Explorer 6.0 (or later) for the Windows® operating systems.

### Linux-based Element Manager

#### Log in to ECM and Access Element Manager

Access the Linux-based EM through the ECM. To log in to Linux-based EM follow the steps in [Procedure 1 “Logging in to ECM and Accessing Linux-based Element Manager” \(page 129\)](#).

#### Procedure 1

#### Logging in to ECM and Accessing Linux-based Element Manager

Step	Action
1	<p>Enter the Fully Qualified Domain Name (FQDN), in the browser’s address field, of an ECM server.</p> <p><b>Note:</b> The FQDN of the ECM server can be bookmarked in the Internet Explorer Favorites list.</p> <p>The Security Alert Web page opens. See <a href="#">Figure 48 “Security Alert Web page” (page 130)</a>.</p>

**Figure 48**  
**Security Alert Web page**



- 2 Click the **Yes** button. The ECM log in Web page opens. See [Figure 49 "ECM log in Web page" \(page 130\)](#).

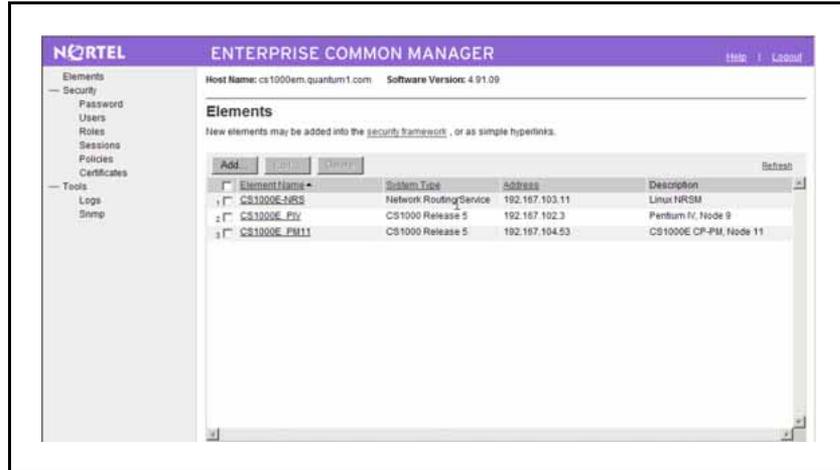
**Figure 49**  
**ECM log in Web page**



- 3 Enter **User Name** and **Password** in the text boxes. Click the **Log in** button.

The ECM Elements Web page opens. See [Figure 50 "ECM Elements Web page" \(page 131\)](#).

**Figure 50**  
ECM Elements Web page



4 Click the link to the Element Manager in the **Element Name** column.

The Element Manager System Overview Web page opens, as shown in [Figure 51 "Element Manager System Overview Web page"](#) (page 131).

**Figure 51**  
Element Manager System Overview Web page



--End--

### Element Manager interface

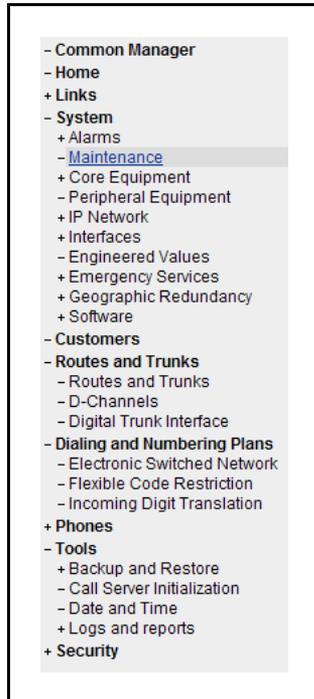
The **EM Navigator**, located on the left side of the Element Manager Web pages, contains links to other Web pages. **Common Manager**, the root of the EM Navigator, is a link to the ECM Web page. The IP Peer Network is configured from Web pages accessed through the following branches in the EM Navigator:

- Systems
- Customers
- Routes and Trunks

- Dialing and Numbering Plans
- Tools

In [Figure 52 "EM Navigator" \(page 132\)](#), the EM Navigator is displayed with those branches expanded.

**Figure 52**  
**EM Navigator**



The **Help** and **Logout** links are located on the right side of the EM Web page header. See [Figure 53 "Help and Logout Links" \(page 132\)](#).

**Figure 53**  
**Help and Logout Links**



**Help Link** Select the **Help** link to access the **EM Help files** .

EM provides context-sensitive help. That is, the help page displayed depends on the EM Web page from which it is opened. Once a help page is opened, click the **Show** link in the upper left corner of the page to display the **Contents** and an **Index** of the **EM Help Files**.

**Logout Link** Select the **Logout** link to terminate the current Enterprise Common Manager session. See [Procedure 2 “Logging out of ECM” \(page 133\)](#).

**Common Manager link** Select the **Common Manager** link on the **EM Navigator** to return to the ECM Web page without terminating the current ECM session. See [“Element Manager interface” \(page 131\)](#).

**Log out of ECM**

See [Procedure 2 “Logging out of ECM” \(page 133\)](#) to log out of the ECM. Logging out of the ECM terminates the current session.

**Procedure 2  
Logging out of ECM**

Step	Action
1	<p>Click the <b>Logout</b> link on the right side of the EM Web page header.</p> <p>The <b>Enterprise Common Manager Logout successful</b> Web page opens.</p> <p><b>Figure 54</b> <b>Enterprise Common Manager Logout successful Web page</b></p> <div style="border: 1px solid black; padding: 10px; text-align: center;"> <p>Logout successful. Your secure session has ended.  <a href="#">Login Again</a></p> </div>
2	<p>Close the browser window.</p>

---

--End--

---

**VxWorks-based Element Manager**

To log in to VxWorks-based EM, follow the steps in [Procedure 3 “Launching VxWorks-based Element Manager” \(page 133\)](#) [Procedure 3 “Launching VxWorks-based Element Manager” \(page 133\)](#).

**Procedure 3  
Launching VxWorks-based Element Manager**

Step	Action
1	<p>Open the Web browser.</p>

- 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 55 "Element Manager Login Web page" \(page 134\)](#)).

- 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 55**  
**Element Manager Login Web page**



- 4 The **System Overview** Web page opens (see [Figure 56 "Element Manager System Overview" \(page 135\)](#)).

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 56**  
**Element Manager System Overview**



**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 56 "Element Manager System Overview"](#) (page 135)). The **Login** Web page (see [Figure 55 "Element Manager Login Web page"](#) (page 134)) is displayed again. If you need to log back in to Element Manager, repeat [step 3](#).

**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 [Edit Web page](#)). 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 Commissioning** (NN43001-312))
- **Element Manager: System Administration** (NN43001-632))

---

--End--

---

## Using Element Manager for configuration

Read the following sections and follow the procedures in the order given.

## Configuring the Customer Data Block

To configure the Customer Data Block EM, follow the steps in [Procedure 4](#) "Configuring the Customer Data Block and enabling ISDN" (page 136).

### Procedure 4 Configuring the Customer Data Block and enabling ISDN

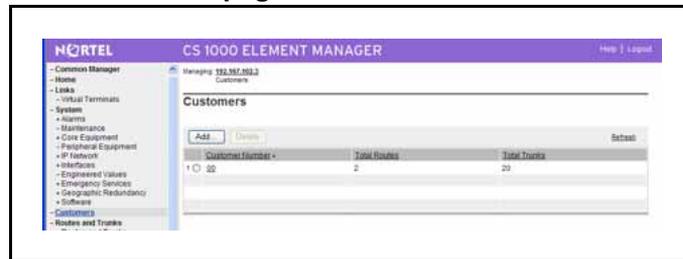
Step	Action
------	--------

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 EM Navigator.

The **Customers** Web page opens, as shown in [Figure 57](#) "Customers Web page" (page 136).

**Figure 57**  
Customers Web page



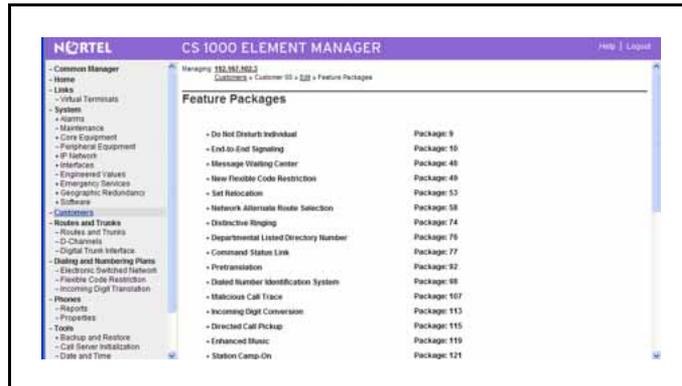
- 2 Click a link in the **Customer Number** column. The **Edit** Web page for Customer number xx opens, as shown in [Figure 58](#) "Customer xx Edit Web page" (page 136).

**Figure 58**  
Customer xx Edit Web page



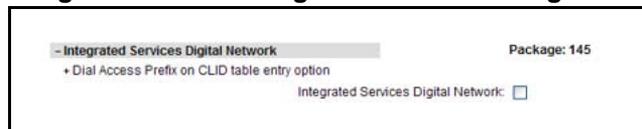
- 3 Click **Feature Packages**. The **Feature Packages** Web page opens, as shown in [Figure 59](#) "Feature Packages Web page" (page 137).

**Figure 59**  
**Feature Packages Web page**



- 4 Scroll down the page and select **Integrated Services Digital Network Package: 145**. The **Feature packages** Web page expands to display the **Integrated Services Digital Network**: check box.

**Figure 60**  
**Integrated Services Digital Network Package: 145 Expanded**



- 5 Click the **Integrated Services Digital Network**: check box. The ISDN list expands to show the ISDN package options, as shown in [Figure 61 "ISDN package options"](#) (page 137).

**Figure 61**  
**ISDN package options**

- 6 Scroll to the bottom of the page and click **Save**.

---

--End--

---

## Configuring D-channels

### Procedure 5 Configuring D-channels

Step	Action
------	--------

*To configure D-channels, use Element Manager or LD 17 of the Command Line Interface. Figure 62 "D-Channels Web page" (page 138) and Figure 63 "D-channels xx Property Configuration Web page" (page 139) show the **D-Channel Configuration** Web pages in Element Manager. Use these Web pages to configure D-channels.*

- |   |  |
|---|--|
| 1 | Select <b>Routes and Trunks &gt; D-Channels</b> from the EM 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 62 "D-Channels Web page" \(page 138\)](#). This window also contains links to D-Channel maintenance and diagnostic pages.

**Figure 62**  
**D-Channels Web page**

- |   |  |
|---|--|
| 2 | In the <b>Configuration</b> section, input the D-channel number and type. Click <b>Add</b> . |
|---|--|

The **D-Channels xx Property Configuration** Web page opens, as shown in [Figure 63 "D-channels xx Property Configuration Web page" \(page 139\)](#). The D-channel number is denoted by xx. Required fields are indicated with a green asterisk.

**Figure 63**  
**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)	[dropdown]
Card number (CDNO)	[dropdown]
Port number (PORT)	[dropdown]
Designator (DES)	[text]
Recovery to Primary (RCVP)	<input type="checkbox"/>
User (USR)	[dropdown]
Interface type for D-channel (IFC)	Meridian DMS-100 (D100)
Country (CNTY)	ETS 300 =102 basic protocol (ETS)
D-Channel PRI loop number (DCHL)	[text]
Primary Rate Interface (PRI)	[text] more PRI
Secondary PRI2 loops (PRI2)	[text]
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

Submit Refresh Delete Cancel

- 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 64 "D-channel Basic options"](#) (page 140).

**Figure 64**  
**D-channel Basic options**

- 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-Channels** Web page reopens ([Figure 65 "D-channel configuration results"](#) (page 140)) with the changes.

**Figure 65**  
**D-channel configuration results**

--End--

## Configuring zones

For information about configuring zones, see *Converging the Data Network for VoIP Fundamentals* ( (NN43001-260)).

## Configuring the Virtual routes and trunks

To configure Virtual Trunk routes, you can use Element Manager or LD 16 of the Command Line Interface.

Figure 67 "New Route Configuration Web page" (page 142) 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.

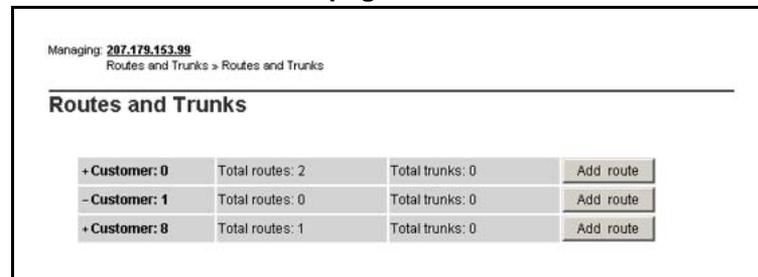
### Procedure 6 Configuring Virtual Trunk routes

Step	Action
------	--------

- 1 Select **Routes and Trunks > Routes and Trunks** from the EM Navigator.

The **Routes and Trunks** Web page opens, as shown in Figure 66 "Routes and Trunks Web page" (page 141).

**Figure 66**  
**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 67 "New Route Configuration Web page" (page 142).

**Figure 67**  
**New Route Configuration Web page**

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 68 "Options available when TIE is selected"](#) (page 142)):

- **The route is for a virtual trunk route (VTRK)** (see [step 4](#))
  - **Digital Trunk Route (DTRK)**
  - **Integrated Services Digital Network option (ISDN)** (see [step 5](#))
- c Enter the **Access Code for the trunk route (ACOD)**.

**Figure 68**  
**Options available when TIE is selected**

4 Select **The route is for a virtual trunk route (VTRK)** check box. Three fields display as shown in [Figure 69 "Virtual trunk route"](#) (page 143).

**Figure 69**  
**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)

- 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 70 "ISDN option" \(page 143\)](#).

**Figure 70**  
**ISDN option**

Integrated Services Digital Network option (ISDN)

- Mode of operation (MODE)

- Interface type for route (IFC)

- Private Network Identifier (PNI)  Range: 0 - 32700

- Network Calling Name Allowed (NCNA)

- Network Call Redirection (NCRD)

- Channel Type (CHTY)

- Call Type for outgoing direct dialed TIE route (CTYP)

- 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 71 "NCRD" \(page 144\)](#)).

**Figure 71**  
**NCRD**

- Network Call Redirection (NCRD)	<input checked="" type="checkbox"/>
-- Trunk Route Optimization (TRO)	<input type="checkbox"/>

7 Click **General Options**.

The General Options list expands, as shown in [Figure 72 "General Options"](#) (page 144).

**Figure 72**  
**General Options**

Input Description	Input Value
SR is the only Controlling Party on incoming calls (CPDC)	<input type="checkbox"/>
Dial Tone on originating calls (DLTND)	<input type="checkbox"/>
Hold failure threshold (HOLD)	02 02 40
Seize failure threshold (SEIZ)	02 02
Supervision Failure (SVFL)	02 02
Trunk Access Restriction Group (TARG)	01
Alternate trunk route for outgoing trunks (STEP)	<input type="text"/> Range: 0 - 511
Actual outgoing toll digits to be ignored for Code Restriction (DABS)	<input type="text"/>
Display IDC Name (DIAM)	<input type="checkbox"/>
Enable Equal Access Restrictions (EQAR)	<input type="checkbox"/>
ACD DNS route (DNS)	<input type="checkbox"/>
Include DNS number in CDR records (DCDR)	<input type="checkbox"/>

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--

## 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 single 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.

**Table 12**  
**LD 97 Configure virtual superloop for Large Systems.**

Prompt	Response	Description
REQ	CHG	Change
TYPE	SUPL	Superloop
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

### CS 1000Esystems

Table 13 "Virtual superloop/virtual card mapping for CS 1000Esystems" (page 145) lists the virtual superloop and virtual card mapping for the CS 1000Esystem.

**Table 13**  
**Virtual superloop/virtual card mapping for CS 1000Esystems**

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 7  
Configuring Virtual Trunks**

Step	Action
------	--------

*To configure Virtual Trunks in Element Manager, use the "New Member Property" pages. [Figure 74 "New Trunk Configuration Web page"](#) (page 147) to [Figure 76 "New Trunk Configuration Advanced Trunk Configurations"](#) (page 149) 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 EM Navigator.

The **Routes and Trunks** Web pages opens (see [Figure 66 "Routes and Trunks Web page"](#) (page 141)).

- 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 73 "Customer routes"](#) (page 146).

**Figure 73  
Customer routes**

Managing: <a href="#">207.179.153.99</a> Routes and Trunks > Routes and Trunks			
<b>Routes and Trunks</b>			
- <a href="#">Customer: 0</a>	Total routes: 2	Total trunks: 0	<input type="button" value="Add route"/>
- <b>Route: 10</b>	Type: TIE	Description: ISDN V TRUNKS	<input type="button" value="Edit"/> <input type="button" value="Add trunk"/>
- <b>Route: 11</b>	Type: FEX	Description: PSTN	<input type="button" value="Edit"/> <input type="button" value="Add trunk"/>
- <b>Customer: 1</b>	Total routes: 0	Total trunks: 0	<input type="button" value="Add route"/>
+ <b>Customer: 8</b>	Total routes: 1	Total trunks: 0	<input type="button" value="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 74 "New Trunk Configuration Web page"](#) (page 147).

**Figure 74**  
**New Trunk Configuration Web page**

- 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)** option.
- 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 75 "New Trunk Configuration Class of Service Configuration Web page"](#) (page 148)). Select a Class of Service.

**Figure 75**  
**New Trunk Configuration Class of Service Configuration Web page**

Managing 287.178.153.99  
 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)	

Return Class of Service Cancel

13 Select the Class of Service and then click **Return Class of Service** to return to the **New Trunk Configuration** Web page (see [Figure 74 "New Trunk Configuration Web page"](#) (page 147)).

14 Select **Advanced Trunk Configurations**.

The **Advanced Trunk Configurations** list expands, as shown in [Figure 76 "New Trunk Configuration Advanced Trunk Configurations"](#) (page 149).

**Figure 76**  
**New Trunk Configuration Advanced Trunk Configurations**

15 Configure **Network Class of Service group (NCOS)**.

16 Click **Save** to save the changes.

The **Customer Explorer** Web page reopens, showing the new trunk member.

--End--

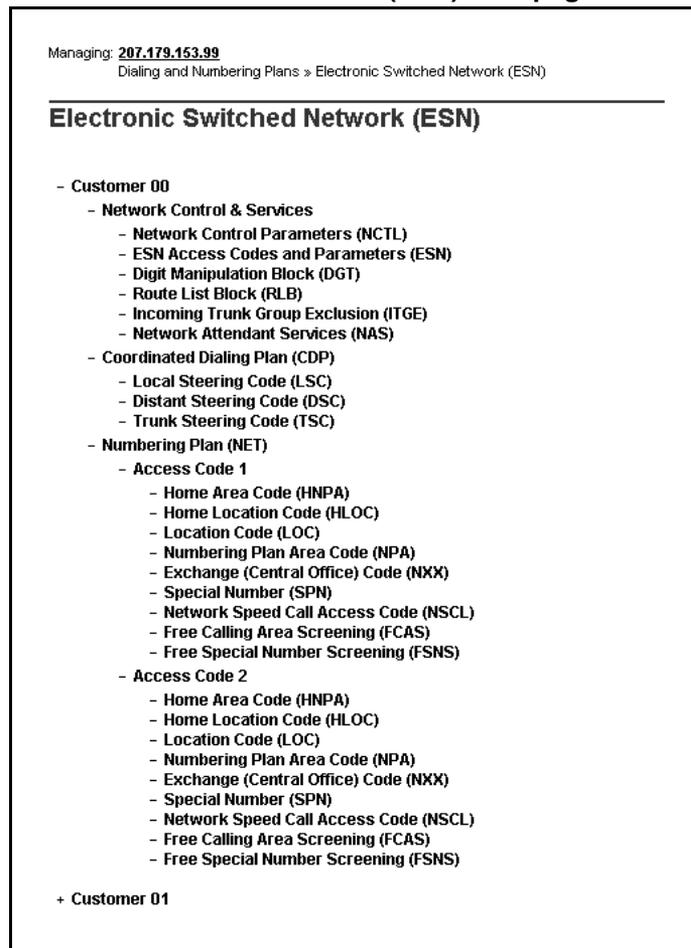
## Configuring networking

The following procedures indicate a Coordinated Dialing Plan for the configuration of networking.

### Procedure 8 Creating an ESN control block

Step	Action
1	Select <b>Dialing and Numbering Plans &gt; Electronic Switched Network</b> from the EM Navigator.  The <b>Electronic Switched Network (ESN)</b> Web page opens, as shown in <a href="#">Figure 77 "Electronic Switched Network (ESN) Web page"</a> (page 150).

**Figure 77**  
**Electronic Switched Network (ESN) Web page**



- 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 78 "ESN Access Codes and Basic Parameters Web page"](#) (page 151).

**Figure 78**  
**ESN Access Codes and Basic Parameters Web page**

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 79 "ESN data block configuration Coordinated Dialing Plan"](#) (page 151).

- 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 79**  
**ESN data block configuration Coordinated Dialing Plan**

5 Click **Submit** to save the changes.

The **Electronic Switched Network (ESN)** Web page reopens (Figure 77 "Electronic Switched Network (ESN) Web page" (page 150)).

--End--

### Procedure 9 Configuring network access

Step	Action
------	--------

- The default parameters for Network Control must be turned on.*
- 1 Select **Dialing and Numbering Plans > Electronic Switched Network** from the EM Navigator.
  - 2 On the **Electronic Switched Network (ESN)** Web page shown in Figure 77 "Electronic Switched Network (ESN) Web page" (page 150), select **Customer xx > Network Control & Service > Network Control Parameters (NCTL)**.

The **Network Control Parameters** Web page opens, as shown in Figure 80 "Network Control Parameters Web page" (page 152).

**Figure 80**  
**Network Control Parameters Web page**

- 3 Click **Edit** to the right of **Network Control Basic Parameters**.

The **Network Control Basic Parameters** Web page opens, as shown in [Figure 81 "Network Control Basic Parameters"](#) (page 153).

**Figure 81**

**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):	<input type="checkbox"/>
Call-Back Queuing option (SCBQ):	<input checked="" type="checkbox"/>
- Call-Back Queue Time Limit (CBTL):	<input type="text" value="20"/>
- RAN route number for CBQ offer to ESN stations (RANE):	<input type="text"/>
- RAN route number for CBQ offer to Conventional main (RANC):	<input type="text"/>

TCOS OHQ eligibility (TOHQ):

<input type="checkbox"/> TCOS 0	<input type="checkbox"/> TCOS 1	<input type="checkbox"/> TCOS 2	<input type="checkbox"/> TCOS 3
<input type="checkbox"/> TCOS 4	<input type="checkbox"/> TCOS 5	<input type="checkbox"/> TCOS 6	<input type="checkbox"/> 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--

## Configuring call routing

[Procedure 13 "Configuring digit manipulation tables"](#) (page 167) must be performed before Configuring the Route List Block.

### Procedure 10 Configuring the Route List Block

Step	Action
------	--------

*This procedure creates the Route List Block that routes calls over the Virtual Trunk route.*

- |          |   |
|----------|---|
| <b>1</b> | Select <b>Dialing and Numbering Plans &gt; Electronic Switched Network</b> from the EM Navigator.   |
| <b>2</b> | On the <b>Electronic Switched Network (ESN)</b> Web page shown in <a href="#">Figure 77 "Electronic Switched Network (ESN) Web page"</a> (page 150), select <b>Customer xx &gt; Network Control &amp; Service &gt; Route List Block (RLB)</b> . |

The **Route List Blocks** Web page opens, as shown in [Figure 82 "Route List Blocks Web page"](#) (page 154).

**Figure 82**  
**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 83 "Route List Block"](#) (page 155).

**Figure 83**  
**Route List Block**

Input Description	Input Value
Route List Index (RLI):	0
Entry Number for the Route List (ENTR):	0 (0-9)
Local Termination entry (L.TER):	<input type="checkbox"/>
Route Number (ROUT):	0
Skip Conventional Signaling (SCNV):	<input type="checkbox"/>
Display Originator's Information (DORG):	<input type="checkbox"/>
Use Tone Detector (TDET):	<input type="checkbox"/>
Time of Day Schedule (TOD):	0
Entry is a VHS Route (VHS):	<input type="checkbox"/>
Conversion to LDN (CNV):	<input type="checkbox"/>
Expansive Route (EXP):	<input type="checkbox"/>
Facility Restriction Level (FRL):	0 (0-7)
Digit Manipulation Index (DMI):	0
ISL D-Channel Down Digit Manipulation Index (ISDM):	0 (0-999)
Free Calling Area Screening Index (FCI):	0
Free Special Number Screening Index (FSNI):	0
Business Network Extension Route (BNE):	<input type="checkbox"/>
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 (IDHQ):	<input type="checkbox"/>
Off-Hook Queuing Allowed (OHQ):	<input type="checkbox"/>
Call Back Queuing Allowed (CBQ):	<input type="checkbox"/>
Number of Alternate Routing Attempts (NAL):	5 (1-10)
Initial Set (ISET):	0 (0-94)
Set Minimum Facility Restriction Level (MFR):	0
Overlap Length (OVLL):	0 (0-24)

- 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--

## Procedure 11 Configuring Steering Codes

Step	Action
------	--------

*This procedure defines how digits for a call are routed under a Coordinated Dialing Plan.*

- |   |  |
|---|--|
| 1 | Select <b>Dialing and Numbering Plans &gt; Electronic Switched Network</b> from the EM Navigator.  |
| 2 | On the <b>Electronic Switched Network (ESN)</b> Web page shown in <a href="#">Figure 77 "Electronic Switched Network (ESN) Web page" (page 150)</a> , select <b>Customer xx &gt; Coordinated Dialing Plan (CDP) &gt; Distant Steering Code (DSC)</b> . |

The **Distant Steering Code List** Web page opens, as shown in [Figure 84 "EM Distant Steering Code List Web page" \(page 156\)](#).

**Figure 84**  
EM Distant Steering Code List Web page

Select **Add** from the drop-down list. The **Distant Steering Code List** Web page refreshes, as shown in [Figure 85 "EM Distant Steering Code List Web page refreshed"](#) (page 156).

**Figure 85**  
EM Distant Steering Code List Web page refreshed

- 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 86 "Distant Steering Code Web page"](#) (page 156).

**Figure 86**  
Distant Steering Code Web page

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):	<input type="checkbox"/>
Route List to be accessed for trunk steering code (RL):	0
Collect Call Blocking (CCBA):	<input type="checkbox"/>
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--

## Configuring codecs

For information about configuring codecs, see *Converging the Data Network for VoIP Fundamentals* ((NN43001-260)) .

## Configuring QoS (DiffServ) values

For information about configuring Quality of Service (QoS) values, see *Converging the Data Network for VoIP Fundamentals* ((NN43001-260)) .

## Configuring call types

To configure call types and location codes HLOC, HNPA, LOC, NPA, NXX, SPN using Element Manager, follow the steps in [Procedure 12 "Configuring call types" \(page 157\)](#).

### Procedure 12 Configuring call types

Step	Action
1	Select <b>Dialing and Numbering Plans &gt; Electronic Switched Network</b> from the EM Navigator.  The <b>Electronic Switched Network (ESN)</b> Web page opens.
2	Scroll to the <b>Numbering Plan (NET)</b> link (see <a href="#">Figure 87 "Numbering Plan (NET)" (page 158)</a> ).

To configure...	See...
Home Location Code (HLOC)	<a href="#">step 3</a>
Home Area Code (HNPA)	<a href="#">step 4</a>
Location Code (LOC)	<a href="#">step 5</a>
Numbering Plan Area Code (NPA)	<a href="#">step 6</a>
Exchange (Central Office) Code (NXX)	<a href="#">step 7</a>
Special Number (SPN)	<a href="#">step 8</a>

**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" \(page 199\)](#).

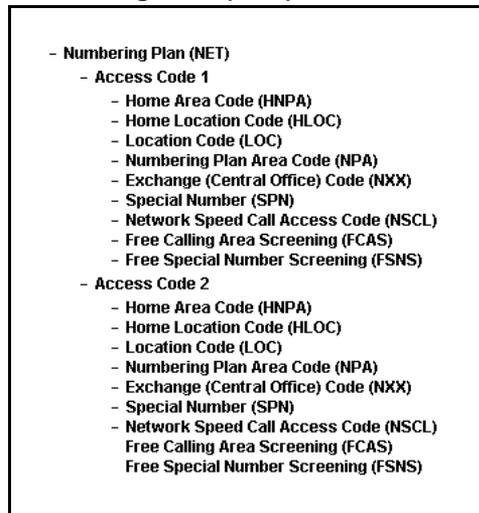
**Note 2:** If you use the SPN to provide NPA and NXX equivalents, these can remain associated with the two ESN access codes (that is, AC1 = 6 and AC2 = 9).

- **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 87**  
**Numbering Plan (NET)**



**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 88 "Home Location Code List Web page"](#) (page 158).

**Figure 88**  
**Home Location Code List Web page**



- 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 89 "Home Location Code Web page"](#) (page 159). The **Home Location code (HLOC)** is auto-filled.

**Figure 89**  
Home Location Code Web page

Input Description	Input Value
Home Location code (HLOC):	123
Digit Manipulation Index (DMI):	1

Submit Cancel

- 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 90 "Home Numbering Plan Area Code Web page"](#) (page 159).

**Figure 90**  
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):	

Submit Refresh Delete Cancel

- 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 91 "Location Code List Web page"](#) (page 160).

**Figure 91**  
**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 Select to **Add** from the drop-down list.
- c Enter a code in the **location code** text box.
- d Click **Submit**.

The **Location Code** Web page opens, as shown in [Figure 92 "Location Code Web page"](#) (page 160).

**Figure 92**  
**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):	<input type="text" value="123"/>
Flexible Length (FLEN):	<input type="text" value="0"/>
Route List Index (RLI):	<input type="text" value="0"/>
maximum 7 digit NPA code allowed (NPA):	<input type="text"/>
maximum 7 digit NXX code allowed (NXX):	<input type="text"/>
Inhibit Time Out Handler (ITOH):	<input type="checkbox"/>
Incoming Trunk group Exclusion Index (ITEI):	<input type="text"/>
Listed Directory Number (LDN):	<input type="text"/>
Direct Inward Dial (DID):	<input type="checkbox"/>

- 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 93 "Numbering Plan Area Code List Web page"](#) (page 161).

**Figure 93**  
**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 94 "Numbering Plan Area Code Web page"](#) (page 162).

**Figure 94**  
**Numbering Plan Area Code Web page**

Input Description	Input Value
Numbering Plan Area code translation (NPA):	<input type="text" value="613"/>
Route List Index (RLI):	<input type="text" value="0"/>
Number to be denied within the NPA (DENY): (items seperated by a space)	<input type="text"/>
Digit Manipulation Index for LDID Numbers (DMI):	<input type="text" value="1"/>
- Local DID number to be recognized (LDID): (items seperated by a space)	<input type="text"/>
Local DDD number to be recognized (LDDD): (items seperated by a space)	<input type="text"/>
Remote DID number to be recognized (DID): (items seperated by a space)	<input type="text"/>
Remote DDD number to be recognized (DDD): (items seperated by a space)	<input type="text"/>
Incoming Trunk group Exclusion Digits (ITED): (items seperated by a space)	<input type="text"/>
Allowed codes (ALLOW): (items seperated by a space)	<input type="text"/>
Incoming Trunk group Exclusion Index (ITEI):	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

**d** Enter the appropriate information.

**e** Click **Submit**.

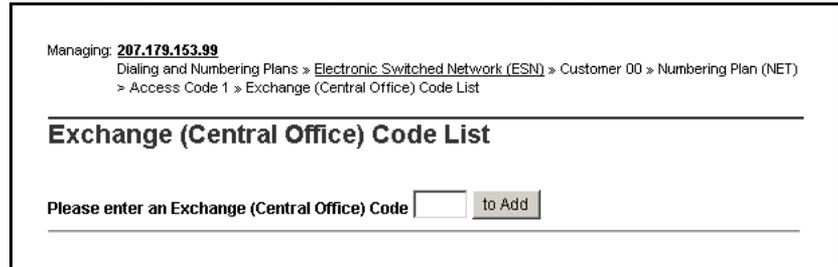
- 7** To configure Exchange (Central Office) Code (NXX), perform the following steps:

- 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 95 "Exchange \(Central Office\) Code List Web page"](#) (page 163).

**Figure 95**

**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 96 "Exchange \(Central Office\) Code Web page"](#) (page 164).

**Figure 96**  
**Exchange (Central Office) Code Web page**

Managing: 287.178.153.88  
 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 (NOX):	123
Route List Index (RLI):	0
Number to be denied within the NOX (DENY): (items seperated by a space)	
Digit Manipulation Index for LDD Numbers (DMI):	1
- Local DID number to be recognized (LDD): (items seperated by a space)	
Local DDD number to be recognized (LDD): (items seperated by a space)	
Remote DID number to be recognized (RDD): (items seperated by a space)	
Remote DDD number to be recognized (RDD): (items seperated by a space)	
Incoming Trunk group Exclusion Digits (ITED): (items seperated by a space)	
Allowed codes (ALLOW): (items seperated by a space)	
Incoming Trunk group Exclusion index (ITEI):	

Submit Cancel

- 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 97 "Special Number List Web page"](#) (page 165).

**Figure 97**  
**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

---

<b>+ Special Number -- 0</b>	<input type="button" value="Edit"/>
Flexible Length: 0	
- International Dialing Plan: N	
Type of call that is defined by the special number : NONE	
Route List Index: 6	

---

<b>+ Special Number -- 011</b>	<input type="button" value="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 98 "Special Number" \(page 166\)](#)).

**d** Enter the appropriate information.

**e** Click **Submit** at the bottom of the Web page.

**Figure 98**  
**Special Number**

Input Description	Input Value
Special Number translation (SPN):	211
Flexible Length (FLEN):	0
- International Dialing Plan (INPL):	<input type="checkbox"/>
Inhibit Time-out Handler (ITOH):	<input type="checkbox"/>
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 (LDD): (items seperated by a space)	
Remote DID number to be recognized (RID): (items seperated by a space)	
Remote DDD number to be recognized (RDD): (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 ADMMDM (STRK): (items seperated by a space)	
Allowed codes (ALLOW): (items seperated by a space)	
- Alternative Route List Index (ARLI):	0
Incoming Trunk group Exclusion Index (ITEI):	

Submit Cancel

- f Enter the appropriate information.
- g Click **Submit** at the bottom of the Web page.

--End--

## Configuring digit manipulation tables

### Procedure 13

#### Configuring digit manipulation tables

Step	Action
1	Select <b>Dialing and Numbering Plans &gt; Electronic Switched Network</b> from the EM Navigator.
2	On the <b>Electronic Switched Network (ESN)</b> Web page shown in <a href="#">Figure 77 "Electronic Switched Network (ESN) Web page" (page 150)</a> , select <b>Customer xx &gt; Network Control &amp; Services &gt; Digit Manipulation Block (DGT)</b> .

The **Digit Manipulation Block List** Web page opens, as shown in [Figure 99 "Digit Manipulation Block List Web page" \(page 167\)](#).

**Figure 99**

#### 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 -- 1**

Number of leading digits to be Deleted: 0  
 Call Type to be used by the manipulated digits : NPA

**+ Digit Manipulation Block Index -- 2**

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**

Number of leading digits to be Deleted: 0  
 Insert: 514818  
 Call Type to be used by the manipulated digits : NCHG

- |   |  |
|---|--|
| 3 | Select a <b>Digit Manipulation Block Index</b> number in the drop-down list. |
| 4 | Click <b>to Add</b> .  |

The **Digit Manipulation Block** Web page opens, as shown in [Figure 100 "Digit Manipulation Block Web page" \(page 168\)](#).

**Figure 100**  
**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):	<input style="width: 50px;" type="text" value="4"/>
Number of leading digits to be Deleted (DEL):	<input style="width: 50px;" type="text" value="0"/>
Insert (INST):	<input style="width: 100px;" type="text"/>
IP Special Number (ISPN):	<input type="checkbox"/>
Call Type to be used by the manipulated digits (CTYP):	<input type="text" value="Call type will not be changed (NCHG)"/>

- 5 Enter the appropriate information.
- 6 Click **Submit**.

--End--

## 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 [Table 16 "LD 16 Configure the SIP route." \(page 171\)](#).
  - To configure an H.323 route, see [Table 17 "LD 16 Configure the H.323 route." \(page 173\)](#).
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.

**Table 14**  
**LD 17 Configure D-channels.**

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	IP Expansion Cabinet or Media Gateway
	FIBR	Fiber Expansion Cabinet
- CTYP		Card Type
	DCIP	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.
		<b>Note:</b> 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		Remote Capabilities
		All nodes must use same RCAP
	ND1, ND2 , ND3	ND3 ensures same level of service between MCDN and QSIG Name Display Supplementary Service
	MWI	Message Waiting Indication support over SIP using a SIP NOTIFY message rather than an MCDN message encapsulated in SIP.
		<b>Note:</b> MWI is also used for H.323 if a BCM is in the network.

**Table 15**  
**LD 15 Configure network settings and options.**

Prompt	Response	Description
REQ:	NEW	Add new block
	CHG	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 1000Esystem, 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	E.164 National number
	NXX	E.164 Subscriber number
	INTL	International number
	SPN	Special Number
	LOC	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
CNTC	xx	Country code (see "Note 1" (page 170) )
NATC	xx	National access code (see "Note 1" (page 170) )
INTC	xxx	International access code (see "Note 1" (page 170) )

**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-xxxxxyzzz 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-xxxxyyzzz 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-xxxxyyzzz to the PSTN routing to Austria. Consider another caller from endpoint A making a call to the UK PSTN by dialing 6-011-44-xxxxyyzzz. Endpoint B would receive 44-xxxxyyzzz. It finds that 44 equals 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-xxxxyyzzz 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 [Table 16 "LD 16 Configure the SIP route." \(page 171\)](#) below.
- To configure an H.323 route, see [Table 17 "LD 16 Configure the H.323 route." \(page 173\)](#).

**Table 16**  
**LD 16 Configure the SIP route.**

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, 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	TIE	Trunk Type TIE trunk
VTRK	YES	Virtual Trunk route, where: 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

**Table 16**  
**LD 16 Configure the SIP route. (cont'd.)**

Prompt	Response	Description
PCID	SIP	Protocol ID for the SIP route.
CRID	(NO) YES	<p>Defines the route as a SIP route.</p> <p>CDR record (for SIP) to include correlation ID.</p> <p>YES = When enabled, the fourth line is included in the new CDR record.            NO = The fourth line is not included in the CDR record (default).</p> <p>See <i>Call Detail Recording: Description and Formats</i> ((NN43001-550)) for more information.</p> <p><b>Note:</b> 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.</p>
NODE	xxxx	<p>Node ID</p> <p>Where the Node ID matches the node of the Signaling Server. The Node ID can have a maximum of four numeric characters.</p>
ISDN	YES	Integrated Services Digital Network option
- MODE	ISLD	Mode of operation
- DCH	0-159	D-channel number
- IFC	SL1	Interface type for route (IFC responses are listed in <i>Software Input/Output: Administration</i> () [NN43001-611])
- SRVC	a...a	Service type for AT&T ESS connections (SRVC responses are listed in <i>Software Input/Output: Administration</i> () [NN43001-611])
- - PNI	(0)-32700	Private Network Identifier
- NCNA	(YES)	Network Calling Name Allowed
- NCRD	YES	Network Call Redirection

**Table 16**  
**LD 16 Configure the SIP route. (cont'd.)**

Prompt	Response	Description
- 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.
ICOG	IAO	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. Incoming and Outgoing trunk.
ACOD	x...x	Incoming and Outgoing Access Code for the trunk route.

**Table 17**  
**LD 16 Configure the H.323 route.**

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, 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	TIE	Trunk Type TIE trunk
VTRK	YES	Virtual Trunk route, where: 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

**Table 17**  
**LD 16 Configure the H.323 route. (cont'd.)**

Prompt	Response	Description
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
- IFC	SL1	Interface type for route (IFC responses are listed in <i>Software Input/Output: Administration ()</i> [NN43001-611])
- SRVC	a...a	Service type for AT&T ESS connections (SRVC responses are listed in <i>Software Input/Output: Administration ()</i> [NN43001-611])
- - 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.

**Table 18**  
**LD 97 Configure the superloop for the Virtual Trunks.**

Prompt	Response	Description
REQ	CHG	Change existing data.
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

**Table 19**  
**LD 14 Configure Virtual Trunks.**

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, 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  <b>Note:</b> 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.
...		
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, Media Gateway 1000B, and Media Gateway 1000T
CHID	1-4300	Channel ID for this trunk, dependent on the ISLM parameter (LD 17)
STRI	IMM	Start arrangement Incoming Immediate
STRO	IMM	Start arrangement Outgoing Immediate
SUPN	YES	Answer and disconnect Supervision required  SUPN must equal YES for a COT with Virtual Network Service
...		
TKID	nnnnnnn	Trunk Identifier

**Table 20**  
**LD 86 Configure dialing plan, networking, and ESN data.**

Prompt	Response	Description
REQ	NEW	Create new data block
FEAT	ESN	Electronic Switched Network
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 <i>ISDN Primary Rate Interface: Features</i> (NN43001-569-B1) .
...		
CDP	YES	Coordinated Dialing Plan feature for this customer
- MXSC	x	Maximum number of Steering Codes  Where x = <ul style="list-style-type: none"> <li>• 0-8000 = Maximum number of Steering Codes for Small Systems</li> <li>• 0-10000 = Maximum number of Steering Codes in North America</li> <li>• 0-32000 = Maximum number of Steering Codes outside North America</li> </ul>
- 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.

**Table 21**  
**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

**Table 21**  
**LD 87 Configure network access. (cont'd.)**

Prompt	Response	Description
NCOS	(0)	Network Class of Service group number
TOHQ	(0)	TCOS OHQ eligibility

**Table 22**  
**LD 86 Configure the Digit Manipulation Index.**

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
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.

**Table 23**  
**LD 86 Configure the Route List Block for the Virtual Trunk route.**

Prompt	Response	Description
REQ	NEW	Create new data block
FEAT	RLB	Route list block
...		

**Table 23**  
**LD 86 Configure the Route List Block for the Virtual Trunk route. (cont'd.)**

Prompt	Response	Description
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 = <ul style="list-style-type: none"> <li>• 0-63 Entry number for NARS/BARS Route List</li> <li>• 0-6 Route list entry number for CDP</li> <li>• X Precede with x to remove</li> </ul>
LTER	(NO)	Local Termination entry
ROUT		Route number
	0-511	Range for Large System and CS 1000E system
	0-127	Range for Small System, Media Gateway 1000B, and Media Gateway 1000T
DMI	0 1-31 0-255 0-999	Digit Manipulation Index No digit manipulation required CDP NARS and BARS FNP
...		

**Table 24**  
**LD 87 Configure the CDP steering codes.**

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

**Table 24**  
**LD 87 Configure the CDP steering codes. (cont'd.)**

Prompt	Response	Description
- RLI	0-31 0-127 0-255 0-999	Route List Index to be accessed for Distant Steering Code. Cannot use non-zero entries or DMI. CDP BARS NARS 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

**Table 25**  
**LD 90 Configure call types and 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 AC2	Access Code 1 (NARS/BARS) Access Code 2 (NARS)
TYPE	LOC	Location Code
LOC	x...x	Location Code
- 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.

**Table 26**  
**LD 15 Configure the VNR enhancement.**

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, 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.
ISDN	YES	Integrated Services Digital Network allowed for customer.
		<b>Note:</b> 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.

**Table 26**  
**LD 15 Configure the VNR enhancement. (cont'd.)**

Prompt	Response	Description
- - - LSC	0 .. x..x	<p>Local Steering Code</p> <p>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.</p> <p>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.</p> <p>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 sub-prompt of ISDN.</p>
- PFX1	xxxx	<p>Prefix 1. Prefix or area code for International PRA.</p> <p>First element of Calling Party Number.</p> <p>PFX1 + PFX2 + DN cannot exceed 8 numbers for AXE-10. Prompted with International Primary Rate Access (IPRA) package 202.</p>
- PRX2	xxxx	<p>Prefix 2. Central Office Prefix for International PRA.</p> <p>Second element of Calling Part Number.</p> <p>PFX1 + PFX2 + DN cannot exceed 8 numbers for AXE-10. Prompted with International Primary Rate Access (IPRA) package 202.</p>
- RCNT	0-(5)	<p>Redirection Count for ISDN calls</p> <p>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.</p>
- PSTN	(NO)	<p>Public Service Telephone Networks</p> <p>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.</p>

**Table 26**  
**LD 15 Configure the VNR enhancement. (cont'd.)**

Prompt	Response	Description
- - 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.
- - PCMC	0-(15)-31	Pulse Code Modulation Conversions permitted in a network connection, $\mu$ -Law to A- Law or A- Law to $\mu$ -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

**Table 26**  
**LD 15 Configure the VNR enhancement. (cont'd.)**

Prompt	Response	Description
FTOP	(FRES)	Flexible Trunk to Trunk Options.
APAD	x y  (0) (0)	Flexible Trunk to Trunk Connections Restricted. FTT feature is inactive. 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
- CDPL	1-(10)	Flexible length of Vacant Number Routing (VNR) Coordinated Dialing Plan (CDP)

**Table 26**  
**LD 15 Configure the VNR enhancement. (cont'd.)**

Prompt	Response	Description
- 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
NATC	x	National Access Code
INTC	xxx	International Access Code

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.

**Table 27**  
**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.

## VTRK Failover Upon Network Failure feature

The VTRK Failover Upon Network Failure feature implements the VTRK Network Health Monitor to monitor the health of the network, which is configured using Element Manager.

The VTRK Network Health Monitor task starts when the Signaling Server boots. The VTRK Network Health Monitor task receives a request from the Signaling Server applications to monitor the connectivity status of a given IP address. The Virtual Trunk uses this monitor task to send ping messages to the list of preconfigured IP addresses.

For more information on this feature, see *New in this Release (NN43001-115)* for CS 1000 5.0 and *Features and Services Fundamentals - Book 6 of 6 (NN43001-106-B6)* for CS 1000 5.5.

**Note:** This feature is enabled by default.

Use Element Manager to configure the following new functions:

- VTRK Network Health Monitor configuration for an IP Telephony node
- VTRK Network Health Monitor CLI commands support for an IP Telephony node

## VTRK Network Health Monitor configuration for an IP Telephony node

Login to Element Manager. Navigate to **IP Network > Nodes: Servers, Media Cards** to open the Node Configuration window to begin configuration.

### Adding an IP address to VTRK Network Health Monitor

Step	Action
1	Enter a node number in the New Node field or expand a configured node.
2	Expand the VTRK Network Monitor configuration window.
3	Click <b>Add</b> .
4	Expand the Virtual Trunk Network Health Monitor configuration window.  The Monitor check box is selected by default.
5	Click <b>Add</b> beside Monitored IP address to add a new IP address field.  Once the maximum of 8 IP address fields is reached, the Add button is disabled.

- 6 Enter a valid IP address.
- 7 Click **Save and Transfer**.

---

--End--

---

#### Editing a monitored IP address in VTRK Network Health Monitor

Step	Action
1	In the Node Configuration window, click the <b>Edit</b> button of a node.
2	Expand the VTRK Network Monitor configuration window.
3	Edit the configured monitored IP address.
4	Select or clear the Monitor check box.  If the Monitor check box is cleared, the Add button beside Monitored IP address and the Add button beside each monitored IP address rows are disabled.
5	Click <b>Save and Transfer</b> .

---

--End--

---

#### Viewing new CLI commands in Element Manager

Step	Action
1	Login to Element Manager. Navigate to <b>IP Network &gt; Maintenance and Reports</b> .
2	Expand a configured node.
3	Click <b>GEN CMD</b> against a Signaling Server element.
4	Select <b>Vtrk</b> from the Group drop down list.
5	Select <b>vtrkNetMonShow</b> from the Command drop down list.
6	Click <b>Run</b> .

---

--End--

---

#### Deleting a monitored IP address in VTRK Network Health Monitor

Step	Action
1	In the Node Configuration window, expand the Node.
2	Expand the VTRK Network Monitor configuration window.
3	Click the <b>Remove</b> button beside a configured monitored IP address to delete it.

---

**4** Click **Save and Transfer**.
 

---

--End--

---

**Table 28**  
**VTRK Network Monitor button description in Element Manager**

Action	Response	Comment
Monitor	Check box	Selected by default. If selected, ENABLE = 1 If deselected, ENABLE = 0.
IP address	128 bit IPv4 address in the format: xxx.xxx.xxx.xxx	Each row caption is suffixed with the number of rows. Up to 8 IP addresses are configured. Config.ini stores these values in the following format: [VTRK NETMON] ENABLE = 1 IP = 47.11.221.22 IP = 47.11.221.23
Click the Check box	If the check box is selected, the Add and Remove buttons are enabled. If the check box is cleared, the Add and Remove buttons are disabled.	When the Monitored check box is cleared, all configured IP addresses, and the Add and Remove buttons are disabled.
Click the Add button	A new row appears to enter a Monitored IP address.	The Add button is enabled if the number of IP address rows are less than 8. The Add button is disabled after 8 rows of IP addresses are displayed and when the Monitor check box is deselected.
Click the Remove button	The Monitored IP address row is deleted and the next row caption changes to reflect the current row number.	Click the Remove button beside the Monitored IP address to delete the IP address. If the Monitor check box is cleared, the Remove button is disabled.

### VTRK Network Health Monitor Configuration CLI commands

Login to Element Manager. Navigate to **IP Network > Maintenance and Reports**.

#### Running the vtrkNetMonShow command

---

Step	Action
------	--------

---

1	Expand a configured node.
---	---------------------------

---

- 2 Click the **GEN CMD** button against a Signaling Server element.
- 3 Select **vtrk** from the Group drop down list.
- 4 Select **vtrkNetMonShow**.
- 5 Click **Run**.

---

--End--

---

## 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” \(page 168\)](#). In LD 16, configure the route as an H.323 route (see [Table 17 “LD 16 Configure the H.323 route.” \(page 173\)](#)).
- For Signaling Server configuration, perform the following procedures using Element Manager:
  - [Procedure 14 “Enabling the H.323 Gateway \(H.323 Virtual Trunk application\)” \(page 188\)](#)
  - [Procedure 15 “Configuring the H.323 Gateway settings” \(page 190\)](#)

#### Procedure 14

#### Enabling the H.323 Gateway (H.323 Virtual Trunk application)

---

Step	Action
------	--------

---

- |   |                            |
|---|----------------------------|
| 1 | Log in to Element Manager. |
|---|----------------------------|

- 2 Select **System > IP Network > Nodes: Servers, Media Cards** from the EM Navigator.

The **Node Configuration** Web page opens, as shown in Node Configuration Web page.

- 3 Click **Edit**.

The **Edit** Web page opens, as shown in Edit Web page.

- 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 101 "Signaling Server xxx.xxx.xxx.xxx properties"](#) (page 189)[Figure 101 "Signaling Server xxx.xxx.xxx.xxx properties"](#) (page 189).

**Figure 101**  
**Signaling Server xxx.xxx.xxx.xxx properties**

The screenshot shows the configuration page for a Signaling Server. The title is "Signaling Server 192.167.102.4 Properties". The page contains several fields and checkboxes:

- Role: Leader
- Type: SIP1100
- Embedded LAN (ELAN) IP address: 192.167.102.4
- Embedded LAN (ELAN) MAC address: 00:02:b3:ae:20:0e
- Telephony LAN (TLAN) IP address: 192.167.102.2
- Telephony LAN (TLAN) gateway IP address: 192.167.102.1
- Hostname: CS1000E\_PIV
- H323 ID: CS1000E\_PIV
- Enable Line TPS:
- Enable IP Peer Gateway (Virtual Trunk TPS):  H.323 and SIP
- Enable SIP Proxy / Redirect Server:
- Local SIP TCP/UDP Port to Listen to: 5060
- SIP Domain name: csip.com
- SIP Gateway Endpoint Name: CS1000E\_PIV
- SIP Gateway Authentication Password: \*\*\*\*
- Enable Gatekeeper:
- Network Routing Service Role: Primary

- 6 Select an **H.323 option** from the **Enable IP Peer Gateway (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--

### Procedure 15 Configuring the H.323 Gateway settings

Step	Action
1	Log in to Element Manager.
2	Select <b>System &gt; IP Network &gt; Nodes: Servers, Media Cards</b> from the EM Navigator.  The <b>Node Configuration</b> Web page opens, as shown in Node Configuration Web page.
3	Click <b>Edit</b> .  The <b>Edit</b> Web page opens, as shown in Edit Web page.
4	Select <b>H323 GW Settings</b> to expand the section, as shown in <a href="#">Figure 102 "H323 GW Settings" (page 190)</a> .

**Figure 102**  
**H323 GW Settings**

- H323 GW Settings	
Primary gatekeeper (TLAN) IP address	192.167.103.2
Alternate gatekeeper (TLAN) IP address	0.0.0.0
Primary Network Connect Server (TLAN) IP address	192.167.103.2
Primary Network Connect Server Port number	16500 (1024 - 65535)
Alternate Network Connect Server (TLAN) IP address	0.0.0.0
Alternate Network Connect Server Port number	16500 (1024 - 65535)
Primary Network Connect Server timeout	10 (1 - 30)

- 5 Configure the following fields:
- 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.
  - Alternate gatekeeper IP address:** Enter the IP address if an Alternate Gatekeeper exists.
  - 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 UNISlim protocol.
  - 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.
  - 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--

---

## 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” \(page 168\)](#). In LD 16, configure the route as a SIP route.
- For Signaling Server configuration, perform the following procedures using Element Manager:
  - [Procedure 16 “Enabling the SIP Trunk Gateway \(SIP Virtual Trunk application\)” \(page 191\)](#)
  - [Procedure 17 “Configuring the SIP Trunk Gateway settings” \(page 193\)](#)
  - [Procedure 18 “Configuring the SIP URI to NPI/TON mapping” \(page 195\)](#)

### Procedure 16 Enabling the SIP Trunk Gateway (SIP Virtual Trunk application)

Step	Action
1	Log in to Element Manager.
2	Select <b>System &gt; IP Network &gt; Nodes: Servers, Media Cards</b> from the EM Navigator.  The <b>Node Configuration</b> Web page opens, as shown in Node Configuration Web page.
3	Click <b>Edit</b> .  The <b>Edit</b> Web page opens, as shown in Edit Web page.
4	Select <b>Signaling Servers</b> 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 103 "Signaling Server xxx.xxx.xxx.xxx properties"](#) (page 192).

**Figure 103**  
**Signaling Server xxx.xxx.xxx.xxx properties**

- 6 Select a **SIP** option from the **Enable IP Peer Gateway (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*). 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*). 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--

---

**Procedure 17**  
**Configuring the SIP Trunk Gateway settings**

Step	Action
1	Log in to Element Manager.
2	Select <b>System IP Network &gt; Nodes: Servers, Media Cards</b> from the EM Navigator.  The <b>Node Configuration</b> Web page opens, as shown in Node Configuration Web page.
3	Click <b>Edit</b> .  The <b>Edit</b> Web page opens, as shown in Edit Web page.
4	Select <b>SIP GW Settings</b> to expand the section (see <a href="#">Figure 104 "SIP GW Settings" (page 194)</a> ).

**Figure 104**  
**SIP GW Settings**

- 5 Complete the following for the Primary server:
- a **TLS Security:** Select the **Security Policy** from the drop-down list.
  - b **TLS Security Port:** Enter a value for the port in the text box.
  - c **Client Authentication:**
  - d **Re-negotiation:**
  - e **X.500 Certificate Authentication:**
  - f **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.
  - g **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.
  - h **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.
  - i The **Primary CDS Proxy or Re-direct server flag** is not used in this release.

- j **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).
  - k **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).
  - l **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.
  - m The **Secondary CDS Proxy or Re-direct server flag** is not used in this release.
- 6 Click **Save and Transfer**.

---

--End--

---

### 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 *Network Routing Service Installation and Commissioning (NN43001-564)* ), you must build the SIP URI to NPI/TON mapping using Element Manager.

[Procedure 18 “Configuring the SIP URI to NPI/TON mapping” \(page 195\)](#) provides the steps to create this SIP URI to NPI/TON mapping using an NRS example and an example for the MCS 5100.

#### Procedure 18 Configuring the SIP URI to NPI/TON mapping

Step	Action
1	Log in to Element Manager.
2	Select <b>System IP Network &gt; Nodes: Servers, Media Cards</b> from the EM Navigator.

The **Node Configuration** Web page opens, as shown in Node Configuration Web page.

- 3 Click **Edit**.

The **Edit** Web page opens, as shown in Edit Web page.

- 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 *Network Routing Service overview* chapter of *Network Routing Service Installation and Commissioning (NN43001-564)* (), specifically the examples provided in *Numbering plan mapping*.

To complete the NRS example, refer to [Figure 105 "SIP URI Map for the NRS example"](#) (page 196) and go to [Step 5](#).

To complete the MCS 5100 example, refer to [Figure 106 "SIP URI Map for the MCS 5100 example"](#) (page 197) and go to [Step 6](#).

**Figure 105**  
**SIP URI Map for the NRS example**

- SIP URI Map	
Public E.164/National domain name	<input type="text" value="+1"/>
Public E.164/Subscriber domain name	<input type="text" value="+1613"/>
Public E.164/Unknown domain name	<input type="text"/>
Public E.164/Special Number domain name	<input type="text"/>
Private/UDP domain name	<input type="text" value="myCompany.com"/>
Private/CDP domain name	<input type="text" value="main.myCompany.com"/>
Private/Special Number domain name	<input type="text" value="main.myCompany.com"/>
Private/Unknown (vacant number routing) domain name	<input type="text"/>
Unknown/Unknown domain name	<input type="text"/>

- 5 Fill in the following fields for the NRS example (see ["Configuring call routing"](#) (page 153)):

- 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 106**  
SIP URI Map for the MCS 5100 example

- SIP URI Map	
Public E.164/National domain name	<input type="text" value="mynation.national.e164."/>
Public E.164/Subscriber domain name	<input type="text" value="myarea.mynation.local."/>
Public E.164/Unknown domain name	<input type="text" value="myarea.mynation.unknown."/>
Public E.164/Special Number domain name	<input type="text" value="myarea.mynation.special."/>
Private/UDP domain name	<input type="text" value="level1.private.myenterprise."/>
Private/CDP domain name	<input type="text" value="mylocation.level0.private."/>
Private/Special Number domain name	<input type="text" value="mylocation.special.private."/>
Private/Unknown (vacant number routing) domain name	<input type="text" value="mylocation.unknown.private."/>
Unknown/Unknown domain name	<input type="text" value="mylocation.unknown.private."/>

- 6 Fill in the following fields for the MCS 5100 example (see [Figure 106 "SIP URI Map for the MCS 5100 example"](#) (page 197)):
- 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--

---

## 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 19 "Warm restarting the Signaling Server" \(page 198\)](#).

#### Procedure 19 Warm restarting the Signaling Server

Step	Action
1	Select <b>System &gt; IP Network &gt; Maintenance and Reports</b> from the EM Navigator.
2	Select the node containing the Signaling Server to be restarted.
3	Click <b>Reset</b> for the Signaling Server.

---

--End--

---

### Cold restart

Press the **RST** button on the front panel to cold restart the Signaling Server.

---

# Overlap signaling

---

## Contents

This section contains information on the following topics:

- “Overview” (page 199)
- “Advantages of overlap signaling” (page 201)
- “PSTN-destined calls” (page 202)
- “Feature capabilities” (page 202)
  - “Overlap signaling support using the H.323 protocol” (page 202)
  - “H.323 Gatekeeper overlap signaling support” (page 202)
  - “Overlap sending and receiving configuration support” (page 203)
  - “Overlap to en bloc conversion” (page 204)
  - “Tandem overlap signaling support” (page 206)
- “Overlap signaling call flow” (page 206)
- “Feature packaging” (page 213)
- “Configuring overlap signaling on the Call Server” (page 213)
  - “Task summary list” (page 213)
  - “Configuring overlap signaling using Element Manager” (page 220)
- “Overlay changes for overlap signaling” (page 221)
  - “Flexible Length number of digits implications” (page 223)
- “System log messages” (page 224)

## 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.

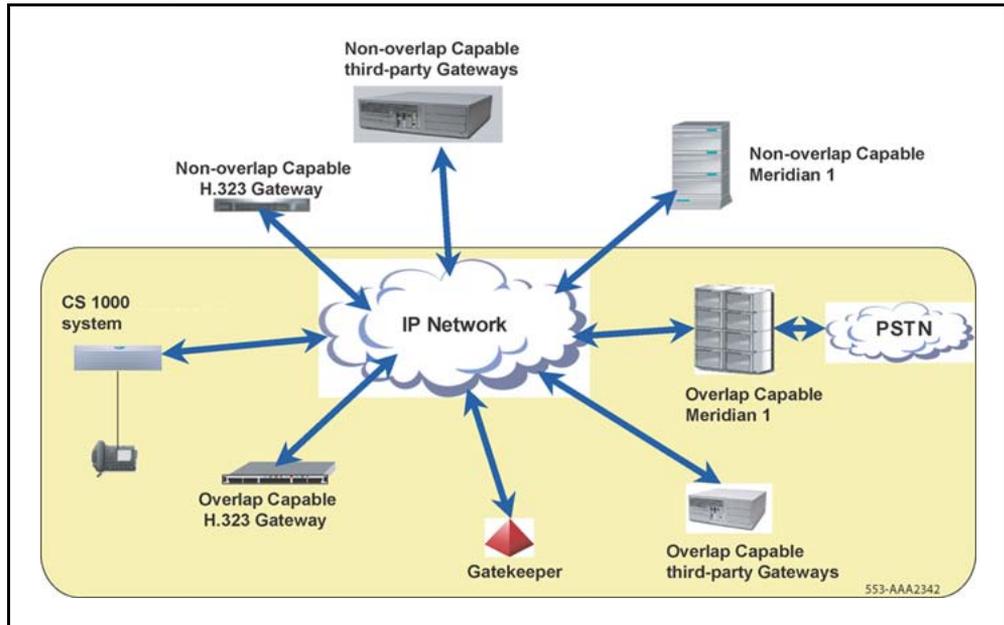
Overlap signaling consists of sending some digits of the called-party number in the first signaling message (SETUP messages) followed by further digits in subsequent signaling messages (INFORMATION messages).

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 107 "Network diagram" \(page 201\)](#) shows a network diagram with overlap signaling.

**Figure 107**  
**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 ((NN43001-569-B1))* .

## 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 [“H.323 Gatekeeper overlap signaling support” \(page 269\)](#).

### **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.

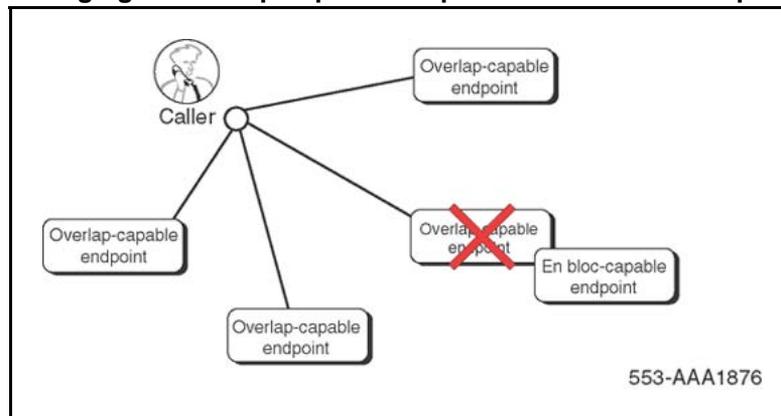
In both cases, overlap to en bloc conversion begins. The interdigit timer starts and digits are collected until an end-of-dial indication. That is, the interdigit timer expires on the Call Server, triggering the end-of-dial indication or the Call Server sends an end-of-dial indication for some other 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 108 "Changing an overlap-capable endpoint to an en bloc endpoint" (page 205) 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 108**  
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:

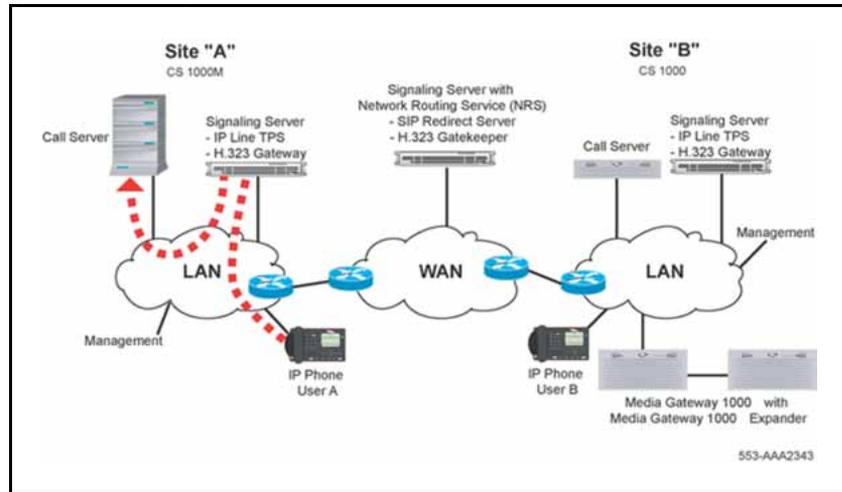
---

Step	Action
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 109 "User A dials User B"](#) (page 207).

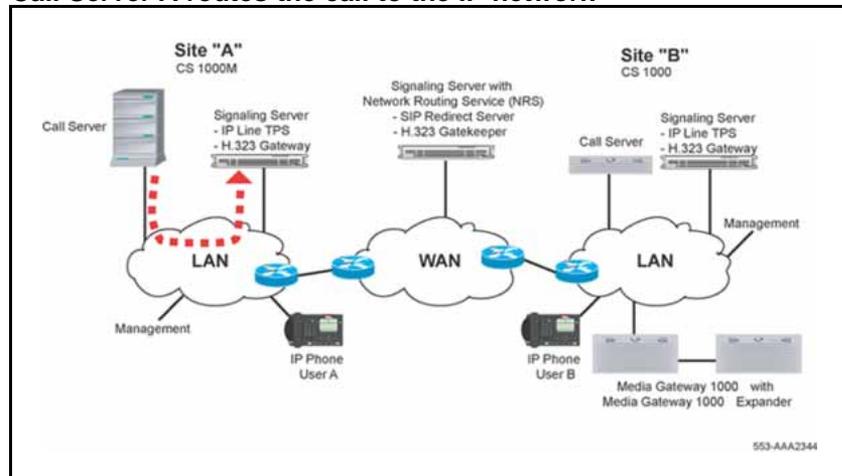
**Figure 109**  
User A dials User B



- 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 110 "Call Server A routes the call to the IP network"](#) (page 207).

**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 110**  
Call Server A routes the call to the IP network



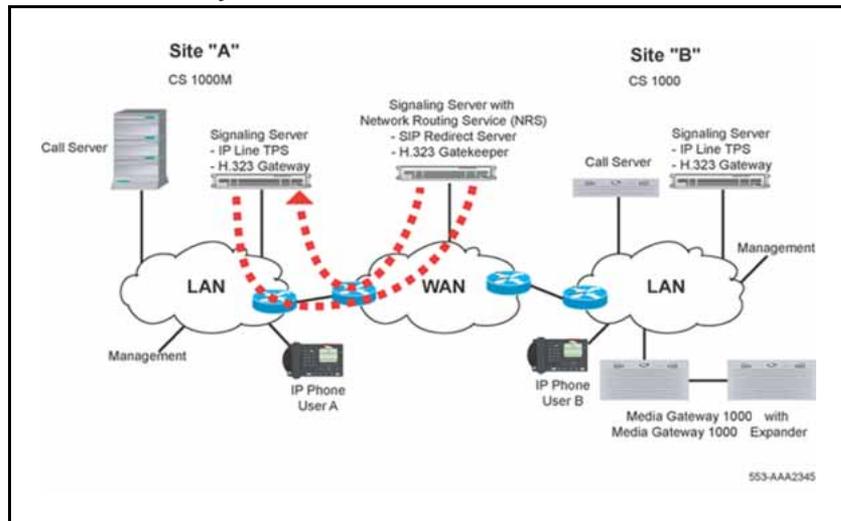
- 3 H.323 Gateway A asks the NRS (specifically the H.323 Gatekeeper) to search for the dialed DN in the database (for example, within the appropriate CDP domain). If the NRS (H.323

Gatekeeper) can unambiguously resolve the destination digits, it sends the IP address of H.323 Gateway B to H.323 Gateway A. See [Figure 111 "The H.323 Gatekeeper sends the IP address of H.323 Gateway B to H.323 Gateway A" \(page 208\)](#).

Otherwise, the NRS requests more digits.

**Figure 111**

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



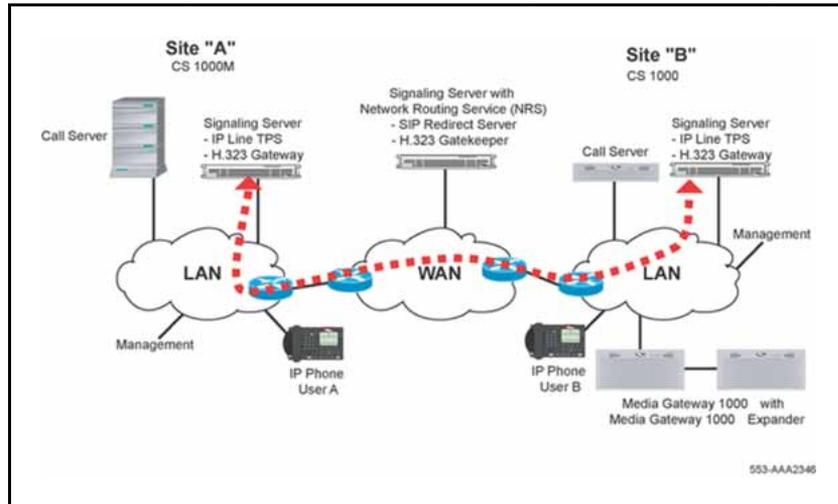
- 4 User A dials an additional digit. The TPS forwards it to Call Server A. See [Figure 109 "User A dials User B" \(page 207\)](#).
- 5 Call Server A forwards the digits to H.323 Gateway A on the Signaling Server. See [Figure 110 "Call Server A routes the call to the IP network" \(page 207\)](#).
- 6 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 111 "The H.323 Gatekeeper sends the IP address of H.323 Gateway B to H.323 Gateway A" \(page 208\)](#).

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.

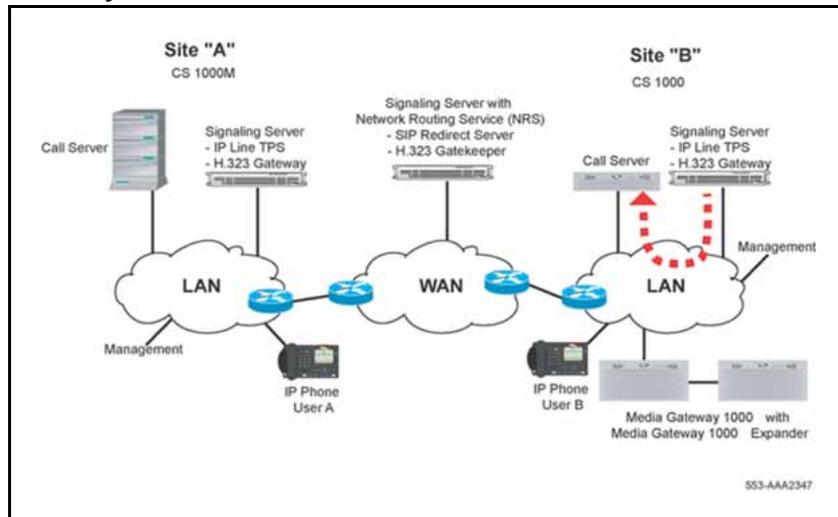
- 7 H.323 Gateway A sends a SETUP message to H.323 Gateway B, including the DN information and an indication that H.323 Gateway A is overlap capable. H.323 Gateway B replies with a SETUP ACK indicating that it is also overlap capable. See [Figure 112 "H.323 Gateway A sends a SETUP message to H.323 Gateway B" \(page 209\)](#).

**Figure 112**  
**H.323 Gateway A sends a SETUP message to H.323 Gateway B**



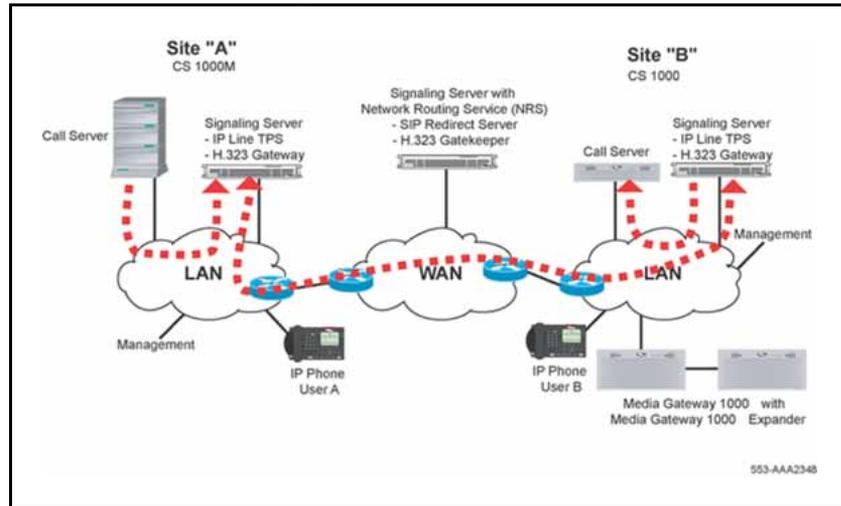
- 8 H.323 Gateway B treats the call as an incoming overlap signaling call from a Virtual Trunk. H.323 Gateway B sends the call to Call Server B over a Virtual Trunk. Call Server B also treats the call as an incoming call from a Virtual Trunk. See [Figure 113 "Gateway B sends the call to Call Server B over a Virtual Trunk"](#) (page 209).

**Figure 113**  
**Gateway B sends the call to Call Server B over a Virtual Trunk**



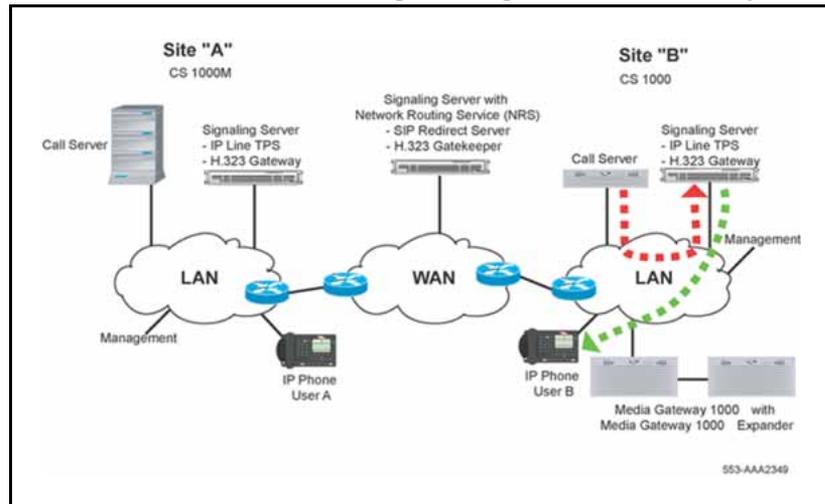
- 9 User A on Call Server A dials additional digits. See [Figure 109 "User A dials User B"](#) (page 207).
- 10 Call Server A sends the new digits to Call Server B through the two gateways. This repeats until Call Server B receives all the digits. At that time, Call Server B sends an end-of-dial indication to Call Server A. See [Figure 114 "Call Server A sends digits to Call Server B"](#) (page 210).

**Figure 114**  
**Call Server A sends digits to Call Server B**



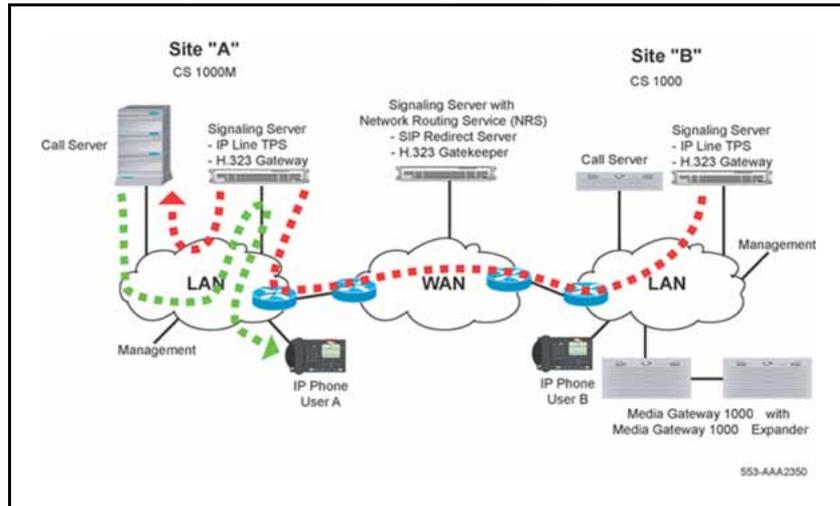
- 11 Call Server B selects the codec, allocates bandwidth, rings the telephone, and sends an alerting message to H.323 Gateway B. See [Figure 115 "Call Server B sends an alerting message to H.323 Gateway B"](#) (page 210).

**Figure 115**  
**Call Server B sends an alerting message to H.323 Gateway B**



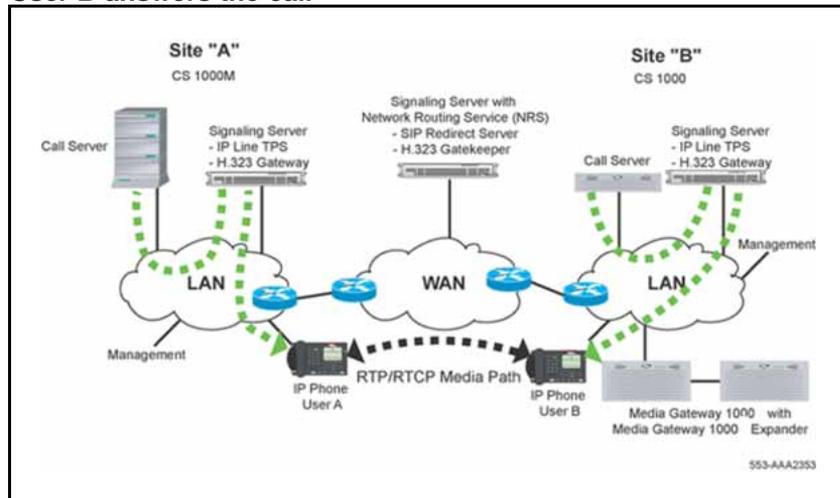
- 12 H.323 Gateway B sends an alerting message to Call Server A. Call Server A requests that the IP Phone play ringback tone. See [Figure 116 "H.323 Gateway B sends an alerting message to Call Server A"](#) (page 211).

**Figure 116**  
**H.323 Gateway B sends an alerting message to Call Server A**



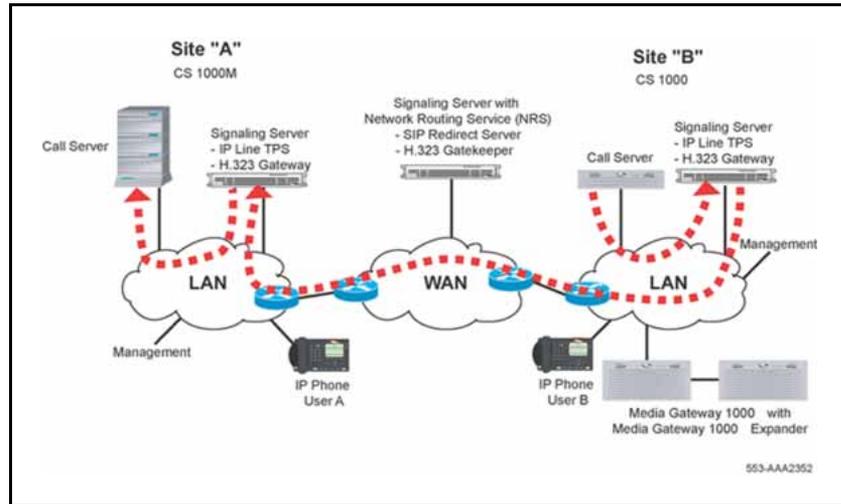
- 13 User B answers the call. A message is sent to Call Server B through the TPS on the Signaling Server. See [Figure 117 "User B answers the call"](#) (page 211).

**Figure 117**  
**User B answers the call**



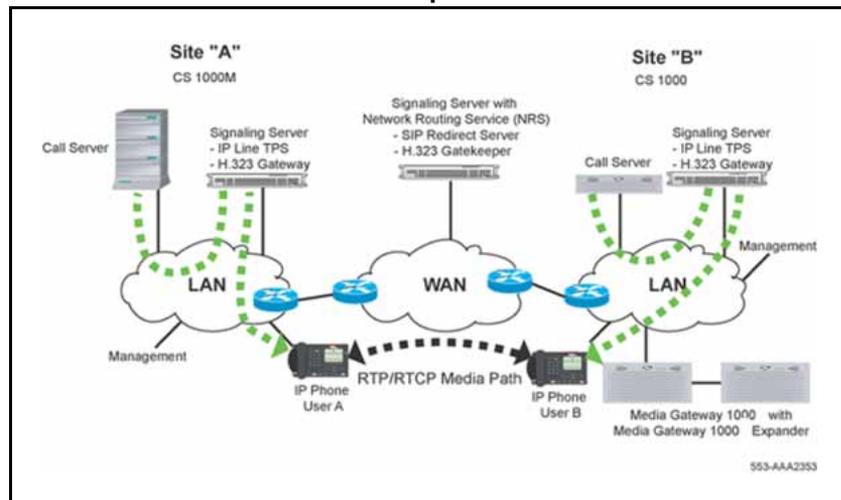
- 14 Call Server B sends a CONNECT message to H.323 Gateway B. H.323 Gateway B sends an H.323 CONNECT message to H.323 Gateway A. H.323 Gateway A forwards the message to Call Server A. See [Figure 118 "Call Server B sends a CONNECT message to Gateway B and onto Call Server A"](#) (page 212).

**Figure 118**  
**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 119 "IP Phones start the direct media paths"](#) (page 212).

**Figure 119**  
**IP Phones start the direct media paths**



--End--

## 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.

**Table 29**  
**LD 17 Configure D-channels to support overlap signaling.**

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
H.323		Indicates overlap signaling prompts for H.323
OVLR	yes	Overlap Receiving
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
		<b>Note:</b> 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.

**Table 30**  
**LD 16 Configure the H.323 route.**

Prompt	Response	Description
REQ	new	Add a new route.
TYPE	rdb	Route Data Block
CUST	xx	Customer number as defined in LD 15.

**Table 30**  
**LD 16 Configure the H.323 route. (cont'd.)**

Prompt	Response	Description
ROUT		Route number
	0-511	Range for Large System and CS 1000E system
	0-127	Range for Small 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	tie	Trunk Type TIE trunk
VTRK	yes	Virtual Trunk route, where: 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 <i>Software Input/Output: Administration ()</i> [NN43001-611])
SRVC	a...a	Service type for AT&T ESS connections (SRVC responses are listed in <i>Software Input/Output: Administration ()</i> [NN43001-611])
PNI	(0)-32700	Private Network Identifier
NCNA	(YES)	Network Calling Name Allowed
NCRD	YES	Network Call Redirection

**Table 30**  
**LD 16 Configure the H.323 route. (cont'd.)**

Prompt	Response	Description
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	IAO	Incoming and Outgoing trunk.
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.

**Table 31**  
**LD 86 Configure the Route List Block for the Virtual Trunk route and configure the minimum number of digits included in the SETUP message.**

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	CDP and BARS
	0-255	NARS
	0-999	FNP

**Table 31**  
**LD 86 Configure the Route List Block for the Virtual Trunk route and configure the minimum number of digits included in the SETUP message. (cont'd.)**

Prompt	Response	Description
ENTR	xxx	Entry number for NARS/BARS Route list  Where xxx = <ul style="list-style-type: none"> <li>• 0-63 Entry number for NARS/BARS Route List</li> <li>• 0-6 Route list entry number for CDP</li> <li>• X Precede with x to remove</li> </ul>
ROUT	0-511 0-127	Route number Range for Large System and CS 1000E system Range for Small System, Media Gateway 1000B, and Media Gateway 1000T  <b>Note:</b> The route must be overlap capable.
...		
ENTR	<cr>	Entry number for NARS/BARS Route list
ISSET	(0)-8	Initial Set  Number of entries in Initial Set for route list block.
...		
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.  <b>Note:</b> 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.

**Table 32**  
**LD 87 Configure the CDP steering codes.**

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.
- FLEN	(0)-10	Flexible Length number of digits  <b>Note:</b> See “Flexible Length number of digits implications” (page 223) 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  <b>Note:</b> See “Flexible Length number of digits implications” (page 223) for more information about FLEN.

**Table 33**  
**LD 90 Configure E.164 plan call types and private plan Location Codes.**

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		Type
	LOC	Location Code

**Table 33**  
**LD 90 Configure E.164 plan call types and private plan Location Codes. (cont'd.)**

Prompt	Response	Description
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.
- FLEN	(0)-10	<p>Flexible Length number of digits</p> <p>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.</p> <p>Default is zero (0) digits.</p> <p><b>Note:</b> See “Flexible Length number of digits implications” (page 223) for more information about FLEN.</p>

**Table 34**  
**LD 90 Configure Special Numbers.**

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		Type
	SPN	Special Number Translation
SPN	xxx	<p>Special Number translation</p> <p>Enter the SPN digits in groups of 3 or 4 digits, separated by a space (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.</p> <p>The maximum number of groups allowed is 5.</p>
- FLEN	(0)-24	<p>Flexible Length number of digits</p> <p>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.</p> <p>Default is zero (0) digits.</p>

**Table 34**  
**LD 90 Configure Special Numbers. (cont'd.)**

Prompt	Response	Description
		<b>Note:</b> See “Flexible Length number of digits implications” (page 223) 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 20 “Configuring D-channels to support overlap signaling”](#) (page 220).

#### Procedure 20 Configuring D-channels to support overlap signaling

Step	Action
1	Log in to CS 1000 Element Manager.
2	Select <b>Routes and Trunks &gt; D-Channels</b> from the EM Navigator.  The <b>D-Channel Web</b> page opens.
3	Click the <b>Edit</b> button associated with the D-channel.  The <b>D-Channel xx Property Configuration</b> Web page opens where xx is the D-channel number.
4	Choose <b>Advance Options (ADVOPT)</b> .
5	Choose <b>H.323 Overlap Signaling Settings (H323)</b> (see <a href="#">Figure 120 “H.323 Overlap Signaling”</a> (page 220)).  <ul style="list-style-type: none"> <li>a Select the <b>Overlap Receiving (OVL R)</b> check box.</li> <li>b Select the <b>Overlap Sending (OVL S)</b> check box.</li> <li>c Select a timer value (in seconds) from the <b>Overlap Timer (OVL T)</b> drop-down list.</li> </ul>
6	Click <b>Submit</b> .

**Figure 120**  
**H.323 Overlap Signaling**

- H323 Overlap Signaling Settings (H323)

- Overlap Receiving (OVL R)

- Overlap Sending (OVL S)

- Overlap Timer (OVL T)

--End--

To configure the number of digits required before the SETUP message is sent, follow the steps in [Procedure 21 “Configuring the minimum number of digits included in the SETUP message”](#) (page 221).

#### Procedure 21

#### Configuring the minimum number of digits included in the SETUP message

Step	Action
1	Refer to <a href="#">Procedure 10 “Configuring the Route List Block”</a> (page 153).
2	<p>Enter a value for <b>Overlap Length (OVLL)</b>.</p> <p>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 <a href="#">Procedure 20 “Configuring D-channels to support overlap signaling”</a> (page 220)/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.</p>

**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--

## 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 (OVL R) 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.

---

# IP Peer interworking

---

## Contents

This section contains information on the following topics:

“Nortel products interworking” (page 225)

“CS 1000MSystem interworking” (page 225)

“Meridian 1 IE (IP Trunk Release 3.0 or later)/Succession 3.0” (page 226)

“Business Communications Manager Release 3.01 (or later)” (page 229)

“Multimedia Communication Server 5100 (MCS 5100)” (page 230)

“CallPilot 2.02” (page 230)

## Nortel products interworking

### CS 1000MSystem interworking

A CS 1000MSystem internetworks with other Nortel products. This chapter discusses interworking between CS 1000Msystems 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)
- CS 2000–SIP Authentication Password Management

**Note:** If your system is interworking with a CS 2000, when you change the SIP Gateway Authentication Password on the Signaling Server for the CS 2000 endpoint, you must match the change on the CS 2000 in the provisioning client under the domain ISN Data in the SSL Platform.

### **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**

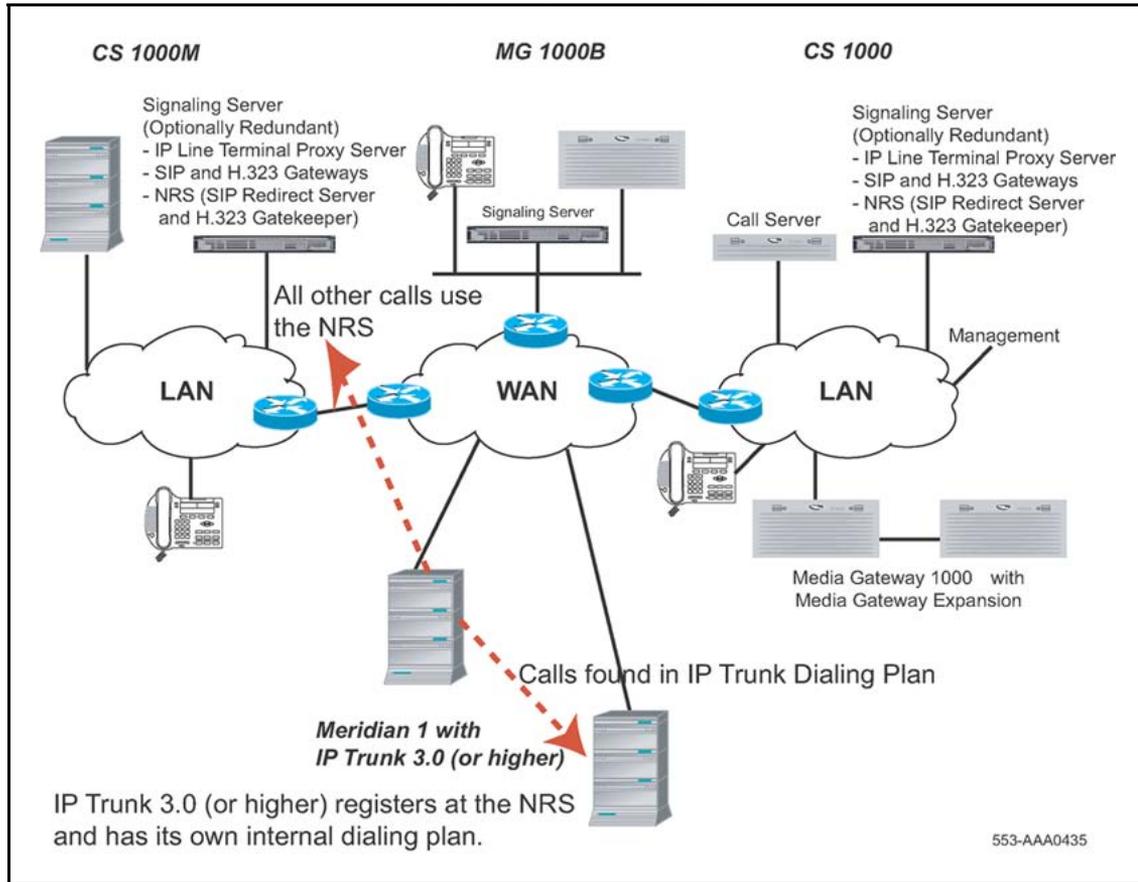
CS 1000 Release 4.0 and later networks with Meridian 1 Release 25.xx (or later) and Succession 3.0. Nortel Meridian Customer Defined Network (MCDN) protocol over PRI trunks provides the rich feature set currently available to networks of Meridian 1 Systems.

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 121 "IP Peer to Meridian 1 IP Trunk 3.0 \(or later\) Interworking"](#) (page 227).

**Figure 121**  
**IP Peer to Meridian 1 IP Trunk 3.0 (or later) Interworking**



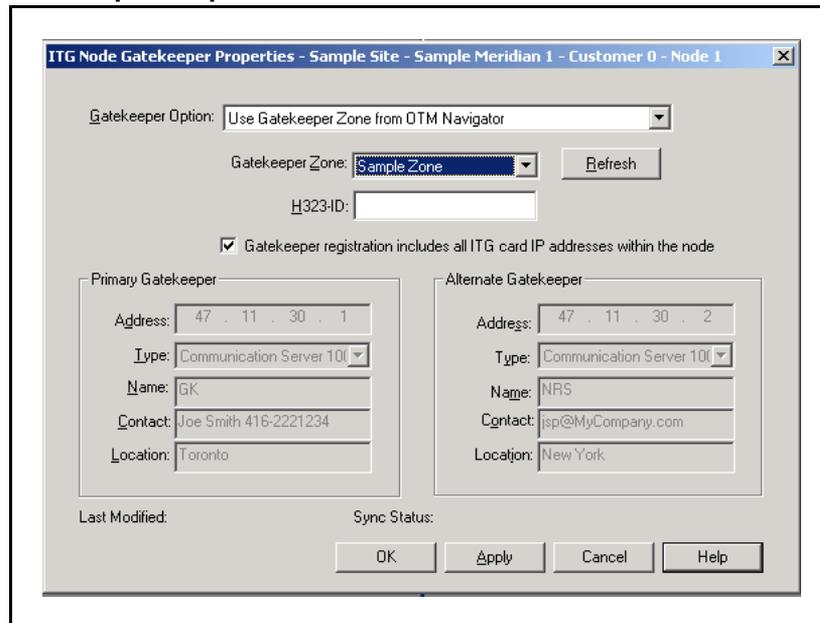
For a CS 1000M System to interwork with a Meridian 1 IE system, the following requirements must be met:

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 TM 2.2 to perform the upgrade. Refer to *Telephony Manager 3.1: System Administration* ((NN43050-601)) for information on installing, upgrading, and configuring IP Trunk 3.0 (or later) parameters.
2. Configure the IP Trunk 3.0 (or later) node LAN register with the CS 1000M NRS, using the TM 2.2 ITG Node Gatekeeper Properties window shown in [Figure 122 "Gatekeeper Properties window"](#) (page 228). 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 123 "Options in the Gatekeeper Option drop-down list"](#) (page 228) shows the options in the **Gatekeeper Option** drop-down list. [Figure 124 "Options in](#)

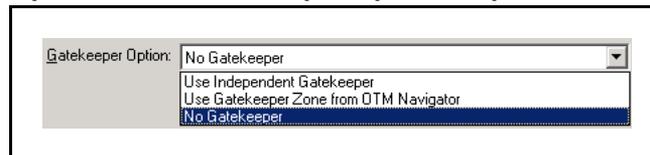
the Primary Gatekeeper Type drop down list" (page 228) shows the options in the **Primary Gatekeeper Type** drop-down list.

Refer to *Telephony Manager 3.1: System Administration* ((NN43050-601)) for information on how to configure the IP Trunk 3.0 (or later) options.

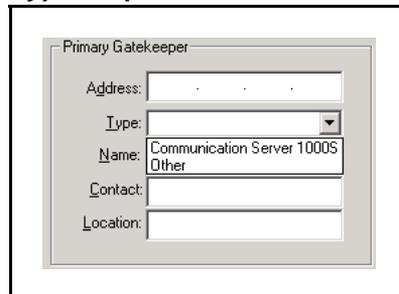
**Figure 122**  
**Gatekeeper Properties window**



**Figure 123**  
**Options in the Gatekeeper Option drop-down list**



**Figure 124**  
**Options in the Primary Gatekeeper 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* ((NN43001-563)) 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 Communication Server (MCS) Interworking Fundamentals* ((NN42020-127)) .

Also refer to Configuring the MCS 5100 system as a Collaborative Server.

### **CallPilot 2.02**

CallPilot integrates voice mail, 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 standalone 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 standalone 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 (NN44200-200)*
- *CallPilot Installation and Configuration Part 3: T1/SMDI and CallPilot Server Configuration (NN44200-303)*
- *CallPilot Administrator's Guide (44200-601)*

### **Collaboration between a CS 1000 Release 4.0 (or later) NRS and a Succession 3.0 H.323 Gatekeeper or MCS 5100**

For information about collaboration between a CS 1000 Release 4.0 (or later) NRS and a Succession 3.0 H.323 Gatekeeper or MCS 5100, see *Converging the Data Network for VoIP Fundamentals ((NN43001-260))* .

---

# Maintenance

---

## Contents

This section contains information on the following topics:

- “Command Line Interface commands” (page 234)
  - “Help CLI commands” (page 234)
  - Table 36 "Virtual Trunk CLI commands" (page 235)
  - “D-channel CLI command” (page 235)
  - “H323GwShow CLI commands” (page 236)
  - “SIPGwShow CLI commands” (page 237)
  - “Graceful disable CLI commands” (page 239)
  
- “Trace tools CLI commands” (page 240)
  - “General trace tool commands” (page 241)
  - “Gatekeeper protocol trace tool commands” (page 241)
  - “SIPCallTrace trace tool commands” (page 245)
  - “H.323CallTrace trace tool commands” (page 250)
  - “Network Connection Service trace tool commands” (page 253)
- “NRS database CLI commands” (page 254)
- Table 48 "Standalone NRS CLI commands" (page 256)
- “ISDN to and from SIP mapping CLI commands” (page 256)
- “Call Server commands” (page 258)
  - “Manage Virtual Trunk route members” (page 258)
  - “Status commands” (page 258)
- “Signaling Server error logging and SNMP alarms” (page 260)
  - “SNMP alarms” (page 260)
  - “Error logging” (page 261)
  - “Error message format” (page 262)

## 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 VxWorks CLI commands available at that interface that are applicable to IP Peer Networking.

Signaling Server VxWorks 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<sup>Ta</sup> 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 VxWorks CLI commands. Refer to *Signaling Server Installation and Commissioning* ((NN43001-312)) for this procedure.

### Help CLI commands

Table 35 "Help CLI commands" (page 234) 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 "Virtual Trunk CLI commands" (page 235) 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.  <b>Note:</b> 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: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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#.</li> </ul>

### D-channel CLI command

[Table 37 "D-channel CLI commands" \(page 235\)](#) 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:

CLI Command	Description
	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 "H323GwShow trace tool CLI commands" (page 236) 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**

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 (cont'd.)**

CLI Command	Description
H323GwShow num <calling/called number> <NPI> <TON>	<p>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.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>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.</li> <li>NPI specifies the numbering plan identifier for the calls. The calls using this numbering plan are to be traced. The values are: <ul style="list-style-type: none"> <li>0 - ALL</li> <li>1 - Unknown</li> <li>2 - ISDN/telephony numbering plan (E.164)</li> <li>4 - E.163</li> <li>5 - Telex numbering plan (F.69)</li> <li>6 - Data numbering plan</li> <li>7 - National standard numbering plan</li> </ul> </li> <li>TON specifies the type of number to use as a filter for tracing. Only calls using this TON setting are traced. The values are: <ul style="list-style-type: none"> <li>0 - ALL</li> <li>1 - Unknown Number</li> <li>2 - International Number</li> <li>3 - National Number</li> <li>4 - Network Specific Number</li> <li>5 - Subscriber Number</li> <li>6 - Level 1 Regional</li> <li>7 - Level 0 Interface</li> </ul> </li> </ul>
help H323GwShow	Displays the usage of the H323GwShow commands.

### SIPGwShow CLI commands

Table 38 "H323GwShow trace tool CLI commands" (page 236) 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**

CLI Command	Description
SIPGwShow	Shows the general SIP Virtual Trunk settings.

**Table 39**  
**SIPGwShow trace tool CLI commands (cont'd.)**

CLI Command	Description
SIPGwShow ch <channel #>	<p>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).</p> <p>The channel # indicates the channel number to trace. The values range from 0 - maximum channel number.</p>
SIPGwShow num <calling/called number>	<p>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.</p> <p>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.</p>
SIPGwShow num <calling/called number> <NPI> <TON>	<p>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.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• NPI specifies the numbering plan identifier for the calls to be traced. The values are: <ul style="list-style-type: none"> <li>0 - ALL</li> <li>1 - Unknown</li> <li>2 - ISDN/telephony numbering plan (E.164)</li> <li>4 - E.163</li> <li>5 - Telex numbering plan (F.69)</li> <li>6 - Data numbering plan</li> <li>7 - National standard numbering plan</li> </ul> </li> <li>• TON specifies the type of number to use as a filter for tracing. Only calls using this TON setting are traced. The values are: <ul style="list-style-type: none"> <li>0 - ALL</li> <li>1 - Unknown Number</li> <li>2 - International Number</li> <li>3 - National Number</li> <li>4 - Network Specific Number</li> <li>5 - Subscriber Number</li> </ul> </li> </ul>

**Table 39**  
**SIPGwShow trace tool CLI commands (cont'd.)**

CLI Command	Description
	6 - Level 1 Regional 7 - Level 0 Interface
help SIPGwShow	Displays the usage of the SIPGwShow commands.

### Graceful disable CLI commands

Table 40 "Graceful Disable commands" (page 239) includes graceful disable CLI commands applicable to the Signaling Server. They are issued from the OAM shell.

**Table 40**  
**Graceful Disable commands**

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. On the Signaling Server the TPS disable command affects only the LTPS. It does not affect the virtual trunks or gatekeeper components, which means the node mastership is not moved to another LTPS. TPS disable command is only intended to disable phone registration on current device. It is not intended to call election, unless no VTRK is configured on this device.
disVTRK	Causes the Virtual Trunk to gracefully switch the registered Virtual Trunks to other Signaling Servers located in the same node.  <b>Note:</b> 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.

**Table 40**  
**Graceful Disable commands (cont'd.)**

CLI Command	Description
forcedisTPS	Forces all registered line LTPS to unregister from the local server. On the Signaling Server the TPS disable command affects only the LTPS. It does not affect the virtual trunks or gatekeeper components, which means the node mastership is not moved to another LTPS. TPS disable command is only intended to disable phone registration on current device. It is not intended to call election, unless no VTRK is configured on this device.
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.
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 "General trace tool CLI commands" \(page 241\)](#) shows the general trace tool commands.
- [Table 42 "Gatekeeper protocol trace tool CLI commands" \(page 242\)](#) shows the Gatekeeper protocol trace tool commands.
- [Table 43 "SIPCallTrace trace tool CLI commands" \(page 245\)](#) shows the SIP trace tool commands.
- [Table 44 "H.323CallTrace trace tool CLI commands" \(page 251\)](#) shows the H.323 trace tool commands.
- [Table 45 "NCS CLI commands" \(page 253\)](#) shows the Network Connection Service (NCS) trace tool commands

**Note:** A warm boot of the system causes all tracing to cease. Traces must be entered again after the system has restarted.

### General trace tool commands

Table 41 "General trace tool CLI commands" (page 241) 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 entered again 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 "Gatekeeper protocol trace tool CLI commands" (page 242) 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**

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: <ul style="list-style-type: none"> <li>• Alias Name is the H.323 ID string.</li> <li>• IP address is the endpoint's IP address.</li> <li>• ALL causes a trace on all endpoints.</li> </ul>
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: <ul style="list-style-type: none"> <li>• Alias Name is the H.323 ID string.</li> <li>• IP address is the endpoint's IP address.</li> <li>• ALL causes a trace on all endpoints.</li> </ul>
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: <ul style="list-style-type: none"> <li>• Alias Name is the H.323 ID string.</li> <li>• IP address specifies the endpoint's IP address.</li> <li>• 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.</li> <li>• NPI - Specifies the numbering plan identifier for which calls using this numbering plan are to be traced. The values are:               <ul style="list-style-type: none"> <li>0 - ALL</li> <li>1 - Unknown</li> <li>2 - ISDN/telephony numbering plan (E.164)</li> <li>4 - E.163</li> <li>5 - Telex numbering plan (F.69)</li> <li>6 - Data numbering plan</li> <li>7 - National standard numbering plan</li> </ul> </li> <li>• TON - specifies the type of number to use as a filter for tracing. Only calls using this TON setting are traced. The values are:</li> </ul>

**Table 42**  
**Gatekeeper protocol trace tool CLI commands (cont'd.)**

CLI Command	Description
	<p>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</p> <ul style="list-style-type: none"> <li>• ALL - Causes a trace on all endpoints</li> </ul> <p><b>Note:</b> A maximum of ten number traces are allowed.</p>
<p>gkProtocolTrace</p> <p>ID &lt;"Alias Name"&gt;            &lt;"protocol"&gt;</p> <p>IP &lt;"IP address"&gt;            &lt;"protocol"&gt;</p> <p>NUM &lt;calling/called            Number&gt; &lt;"protocol"&gt;</p> <p>NUM &lt;calling/called            Number&gt; &lt;NPI&gt; &lt;TON&gt;            &lt;"protocol"&gt;</p> <p>ALL &lt;protocol&gt;</p>	<p>Traces messages for the specified endpoint.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• Alias Name is the H.323 ID string.</li> <li>• IP address specifies the endpoint's IP address.</li> <li>• 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.</li> <li>• 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</li> </ul>
	<ul style="list-style-type: none"> <li>• 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</li> <li>• ALL causes a trace on all endpoints</li> <li>• protocol - specifies which protocols to trace.            (1) Valid protocol types for IP and ALL tracing</li> </ul>

**Table 42**  
**Gatekeeper protocol trace tool CLI commands (cont'd.)**

CLI Command	Description
	<ul style="list-style-type: none"> <li>— 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.</li> <li>— 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</li> </ul> <p>(2) Valid protocols for NUM tracing</p> <ul style="list-style-type: none"> <li>— Individually: ALL, ARQ, ACF, ARJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, LRQ, LCF, LRJ</li> <li>— by category: AXX – ARQ, ACF, ARJ BXX – BRQ, BCF, BRJ DXX – DRQ, DCF, DRJ LXX – LRQ, LCF, LRJ</li> </ul> <p>(3) Protocols that cannot be traced by any endpoint:</p> <ul style="list-style-type: none"> <li>— IACK, INAC, IRQ, IRR, RAI, RAC, SCI, SCR, XRS To trace multiple protocols, separate the input with a space (for example, ARQ ACF ARJ).</li> </ul> <p style="text-align: center;"><b>Note:</b> A maximum of ten number traces are allowed.</p>
<p>gkTraceOff</p> <p>IP &lt;"IP address"&gt;</p> <p>ALL</p>	<p>Turns off the trace for the specified endpoint.</p>
<p>gkTraceOutput</p> <p>&lt;Output_Destination&gt;</p> <p>&lt;"File Pathname"&gt;</p>	<p>Sets the output for all gk protocol traces.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• Output_Destination specifies where all the trace messages for the gkTrace are to be directed. Values are: 1 = TTY 2 = RPTLOG</li> </ul>

**Table 42**  
**Gatekeeper protocol trace tool CLI commands (cont'd.)**

CLI Command	Description
	3 = File 4 = File and TTY <ul style="list-style-type: none"> <li>"File Pathname" is a string encapsulated in quotes. It specifies the file to output to if option 3 or 4 was selected</li> </ul>
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: <ul style="list-style-type: none"> <li>refining the NUM trace filter to be more exact</li> <li>reducing the number of NUM trace filters</li> <li>running the trace during lower traffic periods</li> </ul>
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 entered again after the system restarts.

### SIPCallTrace trace tool commands

Table 43 "SIPCallTrace trace tool CLI commands" (page 245) 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**

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.

**Table 43**  
**SIPCallTrace trace tool CLI commands (cont'd.)**

CLI Command	Description
SIPTraceLevel <Output Option>	<p>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.</p> <p>Output Option specifies the level of the SIP Message Trace. The values are:</p> <p style="padding-left: 40px;">0 = SIP Message Trace – Summary (default)</p> <p style="padding-left: 40px;">1 = SIP Message Trace – Detailed</p> <p>See <a href="#">Figure 125 "SIPCallTrace output example (INVITE message only) Summary format" (page 249)</a> for an example of SIPCallTrace in Summary format. See <a href="#">Figure 126 "SIPCallTrace output example (INVITE message only) Detailed format" (page 250)</a> for an example of SIPCallTrace in Detailed format.</p>
help SIPTraceLevel	Displays the usage for the SIPTraceLevel CLI command.
SIPCallTrace <MsgRecv> <MsgSend>	<p>Allows tracing of all SIP channels in the receiving and/or sending directions.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF.</li> <li>• MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.</li> </ul>
SIPCallTrace ch <channel #> <MsgRecv> <MsgSend>	<p>Allows tracing of a specified SIP channel in the receiving and/or sending directions.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• channel # indicates the channel number to trace. The values range from 0 - maximum channel number.</li> <li>• MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF.</li> <li>• MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.</li> </ul>

**Table 43**  
**SIPCallTrace trace tool CLI commands (cont'd.)**

CLI Command	Description
SIPCallTrace num <calling/called number> <MsgRecv> <MsgSend>	<p>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.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF.</li> <li>• MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.</li> </ul>
SIPCallTrace ch <beginning channel #> <ending channel #> <MsgRecv> <MsgSend>	<p>Allows the tracing of a range of SIP Virtual Trunk channels in the receiving and/or sending directions.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• beginning channel # indicates the channel number to trace. The values range from 0 - maximum channel number.</li> <li>• ending channel # indicates the channel number to trace. The values range from 0 - maximum channel number, but must be greater than the beginning channel #.</li> <li>• MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF.</li> <li>• MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.</li> </ul>
SIPCallTrace num <calling/called number> <NPI> <TON> <MsgRecv > <MsgSend>	<p>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.</p> <p>Where:</p>

**Table 43**  
**SIPCallTrace trace tool CLI commands (cont'd.)**

CLI Command	Description
	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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</li> <li>• 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</li> <li>• MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF.</li> <li>• MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.</li> </ul>
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">	<p>Specifies where the output for the trace tool is to be directed.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• Output_Destination specifies where all the trace messages for the SIPCallTrace are to be directed. The values are:  1 = TTY  2 = RPTLOG</li> </ul>

**Table 43**  
**SIPCallTrace trace tool CLI commands (cont'd.)**

CLI Command	Description
	3 = File 4 = File+TTY <ul style="list-style-type: none"> <li>"File Pathname" is a string encapsulated in quotes. The file pathname must be specified if option 3 (File) was selected as the output destination.</li> </ul>
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 125 "SIPCallTrace output example (INVITE message only) Summary format" (page 249) shows an example of SIPCallTrace results in Summary format. Figure 126 "SIPCallTrace output example (INVITE message only) Detailed format" (page 250) shows an example of SIPCallTrace results in Detailed format.

**Figure 125**  
**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 126**  
**SIPCallTrace output example (INVITE message only) Detailed format**

```
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=-

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 "H.323CallTrace trace tool CLI commands" (page 251) 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**

CLI Command	Description
H323CallTrace ch <channel #> <MsgRecv> <MsgSend>	<p>Traces a specified channel.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>channel # indicates the channel number to trace. Values range from 0 - maximum channel number.</li> <li>MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF.</li> <li>MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.</li> </ul> <p><b>Note:</b> Replaces the H323CallTrace &lt;channel #&gt; &lt;MsgRecv &gt; &lt;MsgSend&gt; command.</p>
H323CallTrace num <calling/called number> <MsgRecv> <MsgSend>	<p>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.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>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.</li> <li>MsgRecv specifies if the messages sent to the specified channel should be traced. The values are ON or OFF.</li> <li>MsgSend specifies if the messages sent from the specified channel should be traced. The values are ON or OFF.</li> </ul>
H323CallTrace ch <beginning channel #> <ending channel #> <MsgRecv> <MsgSend>	<p>Traces a range of Virtual Trunk channels.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>beginning channel # indicates the channel number to trace. The values range from 0 - maximum channel number.</li> <li>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.</li> <li>MsgRecv specifies if the messages sent to the designated channel should be traced. The values are ON or OFF.</li> <li>MsgSend specifies if the messages sent from the designated channel should be traced. The values are ON or OFF.</li> </ul>

**Table 44**  
**H.323CallTrace trace tool CLI commands (cont'd.)**

CLI Command	Description
	<p><b>Note:</b> Replaces the H323CallTrace &lt;beginning channel #&gt; &lt;ending channel #&gt; &lt;MsgRecv&gt; &lt;MsgSend&gt; command.</p>
<p>H323CallTrace num            &lt;calling/called number&gt;            &lt;NPI&gt; &lt;TON&gt;            &lt;MsgRecv&gt; &lt;MsgSend&gt;</p>	<p>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.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• calling/called number indicates the telephone number to trace on. The value can be a number from 1 to 32 digits.</li> <li>• NPI specifies the numbering plan identifier for which calls using this numbering plan are to be traced. The values are:               <ul style="list-style-type: none"> <li>0 - ALL</li> <li>1 - Unknown</li> <li>2 - ISDN/telephony numbering plan (E.164)</li> <li>4 - E.163 5 - Telex numbering plan (F.69)</li> <li>6 - Data numbering plan</li> <li>7 - National standard numbering plan</li> </ul> </li> <li>• TON specifies the type of number to use as a filter for tracing. Only calls using this TON setting are traced. Values are:               <ul style="list-style-type: none"> <li>0 - ALL</li> <li>1 - Unknown Number</li> <li>2 - International Number</li> <li>3 - National Number</li> <li>4 - Network Specific Number</li> <li>5 - Subscriber Number</li> <li>6 - Level 1 Regional</li> <li>7 - Level 0 Interface</li> </ul> </li> <li>• MsgRecv specifies if the messages sent to the designated channel should be traced. The values are ON or OFF.</li> <li>• MsgSend specifies if the messages sent from the designated channel should be traced. The values are ON or OFF.</li> </ul>
<p>help H323CallTrace</p>	<p>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).</p>

**Table 44**  
**H.323CallTrace trace tool CLI commands (cont'd.)**

CLI Command	Description
H323Output <Output_Destination> <File Pathname>	<p>Specifies where the output for the trace tool is to be directed.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• Output_Destination specifies where all the trace messages for H323CallTrace are to be directed. The values are: <ul style="list-style-type: none"> <li>1 = TTY</li> <li>2 = RPTLOG</li> <li>3 = File</li> <li>4 = File and TTY</li> </ul> </li> <li>• File Pathname specifies the file to output to if option 3 or 4 is selected.</li> </ul>
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 "NCS CLI commands" (page 253) 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**

CLI command	Description
tpsARTrace IP <IP address> ID <user ID> ALL	<p>Allows tracing of the tpsAR protocol, which is used to determine where an IP Phone should register.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• IP address - a string containing the IP Phone's IP address</li> <li>• 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</li> <li>• ALL - all IP Phones are to be monitored</li> </ul>

**Table 45**  
**NCS CLI commands (cont'd.)**

CLI command	Description
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.
tpsAROutput <Output_Destination> <"File Pathname">	<p>Sets the output for all tpsAR protocol traces.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>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: <ul style="list-style-type: none"> <li>1 = TTY</li> <li>2 = RPTLOG</li> <li>3 = File</li> <li>4 = TTY + File</li> </ul> <p>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:</p> <p>TTY RPTLOG FILE TTY+FILE</p> </li> <li>"File Pathname" is a string encapsulated in quotes. It specifies the file to output to if option 3 or 4 was selected.</li> </ul>
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 "NRS database CLI commands OAM shell" (page 255) 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 "NRS database CLI commands PDT shell" (page 255) 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.  <b>Note:</b> This command should not interrupt the existing calls.

**Table 47**  
**NRS database CLI commands PDT shell (cont'd.)**

CLI command	Description
forcedisNRS	Forces the NRS server out-of-service.
enINRS	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.

### Standalone NRS CLI commands

Table 46 "NRS database CLI commands OAM shell" (page 255) lists CLI commands for an NRS running on a standalone Signaling Server. They are issued from the PDT shell.

**Table 48**  
**Standalone NRS CLI commands**

CLI command	Description
adminUserPasswordChange [userID]	Changes the administrator-level user password for an NRS running on a standalone Signaling Server, where: <ul style="list-style-type: none"> <li>• userID = userID of administrator-level user</li> </ul>
adminUserCreate [userID]	Creates an administrator-level user of an NRS running on a standalone Signaling Server, where: <ul style="list-style-type: none"> <li>• userID = userID of new administrator-level user</li> </ul>
adminUserDelete [userID]	Deletes an administrator-level user of an NRS running on a standalone Signaling Server, where: <ul style="list-style-type: none"> <li>• userID = userID of administrator-level user to be deleted</li> </ul>
adminAccountShow	Displays the userID and access privileges for all users of an NRS running on a standalone Signaling Server.

### ISDN to and from SIP mapping CLI commands

Table 49 "ISDN-to-SIP commands" (page 257) shows the commands for mapping from ISDN to SIP, and Table 50 "SIP-to-ISDN commands" (page 257) 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: <ul style="list-style-type: none"> <li>• num1 is the ISDN cause code</li> <li>• num2 is the SIP status code</li> </ul>
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: <ul style="list-style-type: none"> <li>• num1 is the SIP status code</li> <li>• num2 is the ISDN cause code</li> </ul>
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.

**Table 51**

**LD 32 Manage Virtual Route members.**

Command	Description
DIS VTRM <cust #> <route #>	<p>Disables all route members in a customer's route.</p> <p>This command:</p> <ul style="list-style-type: none"> <li>• disconnects all active calls associated with the trunks</li> <li>• disables all route members on the Call Server</li> <li>• unregisters all trunks</li> <li>• removes them from the RLM table</li> </ul> <p>On the Signaling Server, all trunks are removed from the Signaling Server list.</p>
ENL VTRM <cust #> <route #>	<p>Enables all the route members (Virtual Trunks)</p> <p>This command:</p> <ul style="list-style-type: none"> <li>• enables all route members in a customer's route</li> <li>• enables all route members</li> <li>• register the member</li> <li>• puts the members into the RLM table</li> </ul> <p>On the Signaling Server, all trunks are put on the Signaling Server list.</p>
STAT VTRM <cust#> <rou#> start_mb# end_mb#	<p>Displays the Virtual Trunk status specified by customer number, route number, and starting and ending member number.</p> <p><b>Note:</b> Also see <a href="#">Table 53 "LD 32 STAT VTRM commands"</a> (page 259) for additional usage of the STAT VTRM command.</p>

### 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.

**Table 52**  
**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: <ul style="list-style-type: none"> <li>• LTPS (Line TPS)</li> <li>• VTRK (Virtual Trunk)</li> <li>• GK (Gatekeeper)</li> </ul>
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.

**Table 53**  
**LD 32 STAT VTRM commands**

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.

**Table 53**  
**LD 32 STAT VTRM commands (cont'd.)**

<b>STAT command</b>	<b>Description</b>
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.
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, the Signaling Server sends an alarm trap to any configured trap destinations. TM receives SNMP traps from the CS 1000 Systems and stores the traps in a circular log file on the TM Server. The TM Alarm Notification application monitors incoming traps

and notifies the appropriate users of important events and alarms. For more information about TM alarm management, refer to *Communication Server 1000E: Maintenance* ( (NN43041-700)).

HPOpenView is an example of an SNMP manager.

For detailed information, refer to *Simple Network Management Protocol: Description and Maintenance* ((NN43001-719)) .

### 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 following procedure to view the error log in EM Navigator.

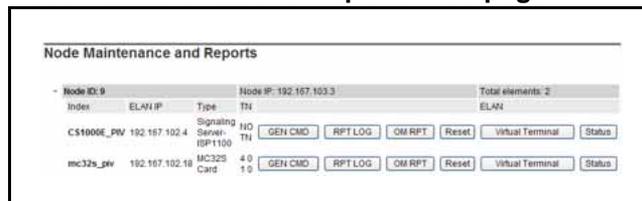
#### Procedure 22 Viewing the error log file

Step	Action
------	--------

- 1 Select **Tools > Logs and Reports > IP Telephony Nodes** from the EM Navigator.

The **Node Maintenance and Reports** Web age opens, as shown in [Figure 127 "Node Maintenance and Reports Web page" \(page 261\)](#).

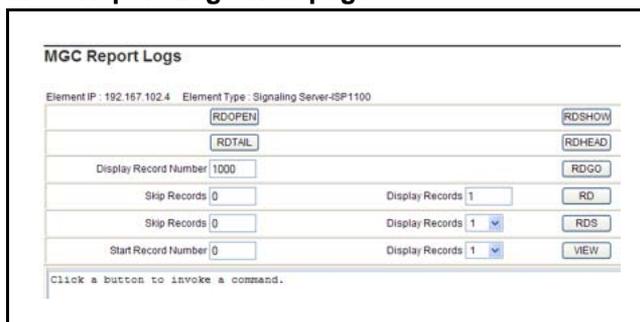
**Figure 127  
Node Maintenance and Reports Web page**



- 2 Click **RPT LOG** for the **Index** entry containing the associated Signaling Server.

The **MGC Report Logs** Web age opens, as shown in [Figure 128 "MGC Report Logs Web page" \(page 262\)](#). For more information about this page, refer to *Element Manager: System Administration* ( (NN43001-632)).

**Figure 128**  
**MGC Report Logs Web page**



3 Click a button to invoke a command.

--End--

The **Node Maintenance and Reports** Web page provides status information about the system and access to diagnostic tools. These tools enable users to issue commands to maintain CS 1000E and CS 1000M components. Use features on the **Node Maintenance and Reports** Web page to perform maintenance tasks, troubleshooting, and problem resolution.

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 1000E 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 ((NN43001-712))* .



## Appendix

# 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). [Table 54 "Mapping from UIPE to H.225.0 for NPI"](#) (page 265) to [Table 63 "Mapping from H.225.0 UUIE to UIPE for Unqualified Number"](#) (page 268) describe the mapping.

**Table 54**  
**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 55**  
**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 UIIE 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 56**  
**Mapping from UIPE to H.225.0 for TON (NPI = Private)**

TON (NPI = Private)	UIPE TON	H.225.0 IE TON	H.225.0 UIIE 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)	plSNSpecificNumber

**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 57**  
**Mapping from H.225.0 Information Element to UIPE for NPI**

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)
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 58**  
**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)

**Table 58**

**Mapping from H.225.0 Information Element to UIPE for TON (NPI = E.164/E.163) (cont'd.)**

TON (NPI = E.164/E.163)	H.225.0 IE TON	UIPE TON
Subscriber number	100 (4)	100 (4)
Unknown	all others	000 (0)

**Table 59**

**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 UIPE. The H.225.0 IE is only used if the H.225.0 UIPE is not present. The Presentation Indicator and Screening Indicator are always in the information H.225.0 IE. The H.225.0 UIPE is only used if the H.225.0 IE is not present. In H.323 version 4.0, *publicNumber* is renamed *e164Number*.

**Table 60**

**Mapping from H.225.0 UIPE to UIPE for NPI**

NPI	H.225.0 UIPE NPI	UIPE NPI
ISDN/Telephony (E.164)	publicNumber	0001 (1)
Private	privateNumber	0010 (2)

**Table 61**

**Mapping from H.225.0 UIPE to UIPE for TON (NPI = E.164/E.163)**

TON (NPI = E.164/E.163)	H.225.0 UIPE 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 62**

**Mapping from H.225.0 UIPE to UIPE for TON (NPI = Private)**

TON (NPI = Private)	H.225.0 UIPE 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 63**  
**Mapping from H.225.0 UIIE to UIPE for Unqualified Number**

Unqualified Number	H.225.0 UIIE	UIPE NPI	UIPE TON
Dialed Digits	e164	0000 (0)	0000 (0)
<b>Note:</b> In H.323 version 4.0, <i>e164</i> is renamed <i>dialedDigits</i> . In H.323 version 4.0, <i>publicNumber</i> is renamed <i>e164Number</i> .			

---

# Appendix

## H.323 Gatekeeper overlap signaling support

---

### Contents

This section contains information on the following topics:

[“Mixed networks of overlap and en bloc H.323 Gatekeepers” \(page 270\)](#)

[“H.323 Gatekeeper recommendations for overlap signaling in mixed overlap and en bloc networks” \(page 271\)](#)

### 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 ringback) 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 RLI.
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

# 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 64 "ISDN cause code to SIP status code mapping" \(page 276\)](#) 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 64 "ISDN cause code to SIP status code mapping" \(page 276\)](#) 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 64 "ISDN cause code to SIP status code mapping" \(page 276\)](#) shows the ISDN cause code to SIP status code mapping, and [Table 65 "ISDN cause code to SIP status code mapping" \(page 277\)](#) shows the SIP error response to ISDN cause code mapping.

**Note:** If desired, a user can change those default mappings through CLI commands.

Table 64 "ISDN cause code to SIP status code mapping" (page 276) shows the ISDN cause code to SIP status code mapping.

**Table 64**  
**ISDN cause code to SIP status code mapping**

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
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

**Table 64**  
**ISDN cause code to SIP status code mapping (cont'd.)**

ISDN cause code	SIP response
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 65 "ISDN cause code to SIP status code mapping" (page 277) shows the SIP error response to ISDN cause code mapping.

**Table 65**  
**ISDN cause code to SIP status code mapping**

SIP response	ISDN cause code
400 Bad Request	41 Temporary Failure
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

**Table 65**  
**ISDN cause code to SIP status code mapping (cont'd.)**

<b>SIP response</b>	<b>ISDN cause code</b>
485 Ambiguous	1 Unallocated number
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

---

## Appendix

# Passthrough End User License Agreement

---

**WARNING**

Do *not* contact Red Hat for technical support on your Nortel version of the Linux base operating system. If technical support is required for the Nortel version of the Linux base operating system, contact Nortel technical support through your regular channels.

This section governs the use of the Red Hat Software and any updates to the Red Hat Software, regardless of the delivery mechanism and is governed by the laws of the state of New York in the U.S.A. The Red Hat Software is a collective work under U.S. Copyright Law. Subject to the following terms, Red Hat, Inc. (“Red Hat”) grants to the user (“Customer”) a license to this collective work pursuant to the GNU General Public License. Red Hat Enterprise Linux (the “Red Hat Software”) is a modular operating system consisting of hundreds of software components. The end user license agreement for each component is located in the component’s source code. With the exception of certain image files identified below, the license terms for the components permit Customer to copy, modify, and redistribute the component, in both source code and binary code forms. This agreement does not limit Customer’s rights under, or grant Customer rights that supersede, the license terms of any particular component. The Red Hat Software and each of its components, including the source code, documentation, appearance, structure and organization are owned by Red Hat and others and are protected under copyright and other laws. Title to the Red Hat Software and any component, or to any copy, modification, or merged portion shall remain with the aforementioned, subject to the applicable license. The “Red Hat” trademark and the “Shadowman” logo are registered trademarks of Red Hat in the U.S. and other countries. This agreement does not permit Customer to distribute the Red Hat Software using Red Hat’s trademarks. If Customer makes a commercial redistribution of the Red Hat Software, unless a separate agreement with Red Hat is executed or other permission granted, then Customer must modify any files identified as “REDHAT-LOGOS” and

“anaconda-images” to remove all images containing the “Red Hat” trademark or the “Shadowman” logo. As required by U.S. law, Customer represents and warrants that it: (a) understands that the Software is subject to export controls under the U.S. Commerce Department’s Export Administration Regulations (“EAR”); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria); (c) will not export, re-export, or transfer the Software to any prohibited destination, entity, or individual without the necessary export license(s) or authorization(s) from the U.S. Government; (d) will not use or transfer the Red Hat Software for use in any sensitive nuclear, chemical or biological weapons, or missile technology end-uses unless authorized by the U.S. Government by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Software to eligible end users, it will, as required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department’s Bureau of Industry & Security (BIS), which include the name and address (including country) of each transferee; and (f) understands that countries other than the United States may restrict the import, use, or export of encryption products and that it shall be solely responsible for compliance with any such import, use, or export restrictions. Red Hat may distribute third party software programs with the Red Hat Software that are not part of the Red Hat Software. These third party programs are subject to their own license terms. The license terms either accompany the programs or can be viewed at <http://www.redhat.com/licenses/>. If Customer does not agree to abide by the applicable license terms for such programs, then Customer may not install them. If Customer wishes to install the programs on more than one system or transfer the programs to another party, then Customer must contact the licensor of the programs. If any provision of this agreement is held to be unenforceable, that shall not affect the enforceability of the remaining provisions. Copyright © 2003 Red Hat, Inc. All rights reserved. "Red Hat" and the Red Hat "Shadowman" logo are registered trademarks of Red Hat, Inc. "Linux" is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners.



Nortel Communication Server 1000

## IP Peer Networking Installation and Commissioning

Release: 5.5

Publication: NN43001-313

Document revision: 02.07

Document release date: 7 October 2009

Copyright © 2007–2009 Nortel Networks. All Rights Reserved.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

To provide feedback or to report a problem in this document, go to [www.nortel.com/documentfeedback](http://www.nortel.com/documentfeedback).

[www.nortel.com](http://www.nortel.com)

