Nortel Communication Server 1000
IP Peer Networking Installation and Commissioning

7.0
NN43001-313, 04.04

August 2010

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

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

Preventing toll fraud

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

Avaya fraud intervention

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Contents

New in this Release

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

This chapter describes what is new in IP Peer Networking Installation and Commissioning (NN43001-313) for Nortel Communication Server 1000 Release 7.0.

Feature changes

See the following sections for information about feature changes:

Navigation

Multiple SSG Routes

Release 7.0 provides support for SSG (SIP Signaling Gateway) being able to route the calls to either of two sets of proxies. The CS or SSG decides to route the calls to the appropriate proxies based on the configurations available in the CS or SSG. The New Proxy Server Route 2 is introduced. See section Enabling and configuring the SIP Trunk Gateway on page 193 for more information.

The Prompt **PROU** is introduced in Route List Index (RLI) for the SSG to decide to route the calls between two set of servers. See Table 25: LD 86 Configure the Route List Block for the Virtual Trunk route on page 180 for more information.

H.323 trunks

Communication Server 1000 Release 7.0 provides an increase in the number of H.323 trunks. The maximum number of trunks for H.323 increases from 1200 to 2400.

SIP and SIPL trunks

Communication Server 1000 Release 7.0 provides an increase in the number of SIP and SIP Line trunks. The maximum number of trunks for SIP and SIPL increase from 1800 to 3700.

Tertiary NRS

A tertiary NRS server for a SIP Gateway (SIPGW) provides a third level of redundancy. The tertiary NRS can run on any device on the network and can operate in a one-for-many or in a one-to-one mode. The Tertiary NRS server provides a more flexible alternative and is mutually exclusive to the existing Failsafe operations. The tertiary NRS has a database independent of the primary NRS that is tailored for routing calls during a WAN outage scenario. This is different from the failsafe NRS which has a snapshot of the database on the primary NRS. The third level of redundancy does not apply to the H.323 gateway because if a system has a tertiary NRS defined for the SIPGW, the co-residing H.323 solution has only two levels of redundancy, as the failsafe NRS cannot run on this system. You can configure the Tertiary NRS using the NRS Manager Web User Interface. For more information about configuring the SIP Gateway IP address of the Tertiary NRS server in Element Manager, see section Enabling and configuring the SIP Trunk Gateway on page 193.

Bandwidth management zones

Communication Server 1000 Release 7.0 provides an increase in the number of bandwidth management zones. The range of allowable bandwidth management zone values is increased from 0-–255 to 0–8000

RLI and DMI enhancement

For Communication Server Release 7.0, the range of allowable Route List Index (RLI) and Digit Manipulation Index (DMI) values is increased from 0–999 to 0–1999. For more information about RLI and DMI values, see Configure IP Peer Network on page 129.

IP Peer Interworking with BCM

With Communication Server 1000 Release 7.0 the information for planning, configuration, testing, and troubleshooting of the integration of the Business Communications Manager (BCM) with a Communication Server 1000 system has been moved from *Solution Integration Guide for Communication Server 1000 Release 5.5/Business Communications Manager, NN43001-326* into this document.

Other changes

This release contains no other changes. This section has the following topics:

Revision history on page 11

Revision history

August 2010 Standard 04.04. This document is up-issued to support Communication Server 1000 Release 7.0.

August 2010 Standard 04.03. This document is up-issued to support Communication Server 1000 Release 7.0.

August 2010 Standard 04.02. This document is up-issued to support Communication Server 1000 Release 7.0.

June 2010 Standard 04.01. This document is up-issued to support Communication Server 1000 Release 7.0.

May 2009 Standard 03.02. This document is up-issued to reflect changes in technical content.

May 2009 Standard 03.01. This document is up-issued to support Communication Server 1000 Release 6.0.

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 comprises (1) information on IP Peer Networking that was previously 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 about reconfiguring Call Server alarm notification levels if necessary during Adaptive Network Bandwidth Management configuration. 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 in the following legacy document, now retired: *IP Peer Networking (553-3023-220)*.

Chapter 1: 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 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: http://www130.nortelnetworks.com/go/main.jsp

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: http://www.nortel.com/help/contact/global/index.html

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: http://www.nortel.com/help/contact/erc/index.html

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.

Chapter 2: Introduction

This 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 7.0 software. For more information on legacy products and releases, click the **Technical Documentation** link under Support & Training on the Nortel home page:

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)

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.

Technical documents

The following documents are referenced in this document:

- *Converging the Data Network with VoIP* (NN43001-260)
- *Dialing Plans: Description* (NN43001-283)
- *Branch Office Installation and Commissioning* (NN43001-314)
- *IP Phones Fundamentals* (NN43001-368)
- *Element Manager: System Administration* (NN43001-632)
- *System Management* (NN43001-600)
- *Security Management Fundamentals* (NN43001-604)
- *System Redundancy Fundamentals*
- *Software Input/Output: Administration* (NN43001-611)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Software Input/Output: System Messages* (NN43001-712)
- *Software Input/Output: Maintenance* (NN43001-711)
- *Simple Network Management Protocol: Description and Maintenance* (NN43001-719)
- *SIP Line Fundamentals* (NN43001-508)
- *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)
- *Communication Server 1000E: Installation and Commissioning* (NN43041-310)
- *Communication Server 1000E: Upgrade Procedures* (NN43041-458)
- *Communication Server 1000E: Maintenance* (NN43041-700)
- *Keycode Installation Guide* (NN40010-301)
- *BCM 4.0 Device Configuration Guide* (N0060600)
- *BCM 4.0 Telephony Device Installation Guide* (N0060609)
- *BCM50 Networking Configuration Guide* (NN40020-603)
- *Business Communications Manager 5.0 - Configuration - Telephony , NN40170-502*

Online

To access Nortel documentation online, click the **Technical Documentation** link under Support & Training on the Nortel home page: http://www.avaya.com

CD-ROM

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

Chapter 3: Overview

Contents

This chapter contains information on the following topics:

IP Peer Networking overview

Warning:

Do not contact Red Hat for technical support on your Nortel version of the base operating system. If technical support is required for the Nortel version of the 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 customers 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 on 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 Communication Server 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 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 on page 23 and *Signaling Server IP Line Applications Fundamentals (NN43001-125)*.

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 on page 35 and *Network Routing Service Fundamentals (NN43001-130)*.

A brief overview of the migration procedures is described in *Network Routing Service Fundamentals (NN43001-130)*. 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:
Voice Gateway Media Card is a generic term used to reference a media card running a Voice Gateway application. For more information about Voice Gateway Media Cards, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125) .

Note:
Data calls are not supported on Virtual Trunks.

Both SIP and H.323 Virtual Trunks are supported. Up to 3700 Virtual Trunks can be configured on a Signaling Server.

Table 1: Virtual Trunk limits for each Signaling Server on 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 2400 (see Note 1)
SIP	3700
Combination of both H.323 and SIP	less than or equal to 1800 (see Note 2)

Note:
At least 1024 MB of memory is required on the Signaling Server to obtain 1200 H.323 Virtual Trunks.

Note:
See Table 2: Maximum number of Virtual Trunk on each Signaling Server on page 25.

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

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

For more information, refer to Scalability on page 24 and the Planning and Engineering NTPs.

Figure 1: An example of IP Peer Networking on page 23 illustrates an example of an IP Peer Networking configuration.

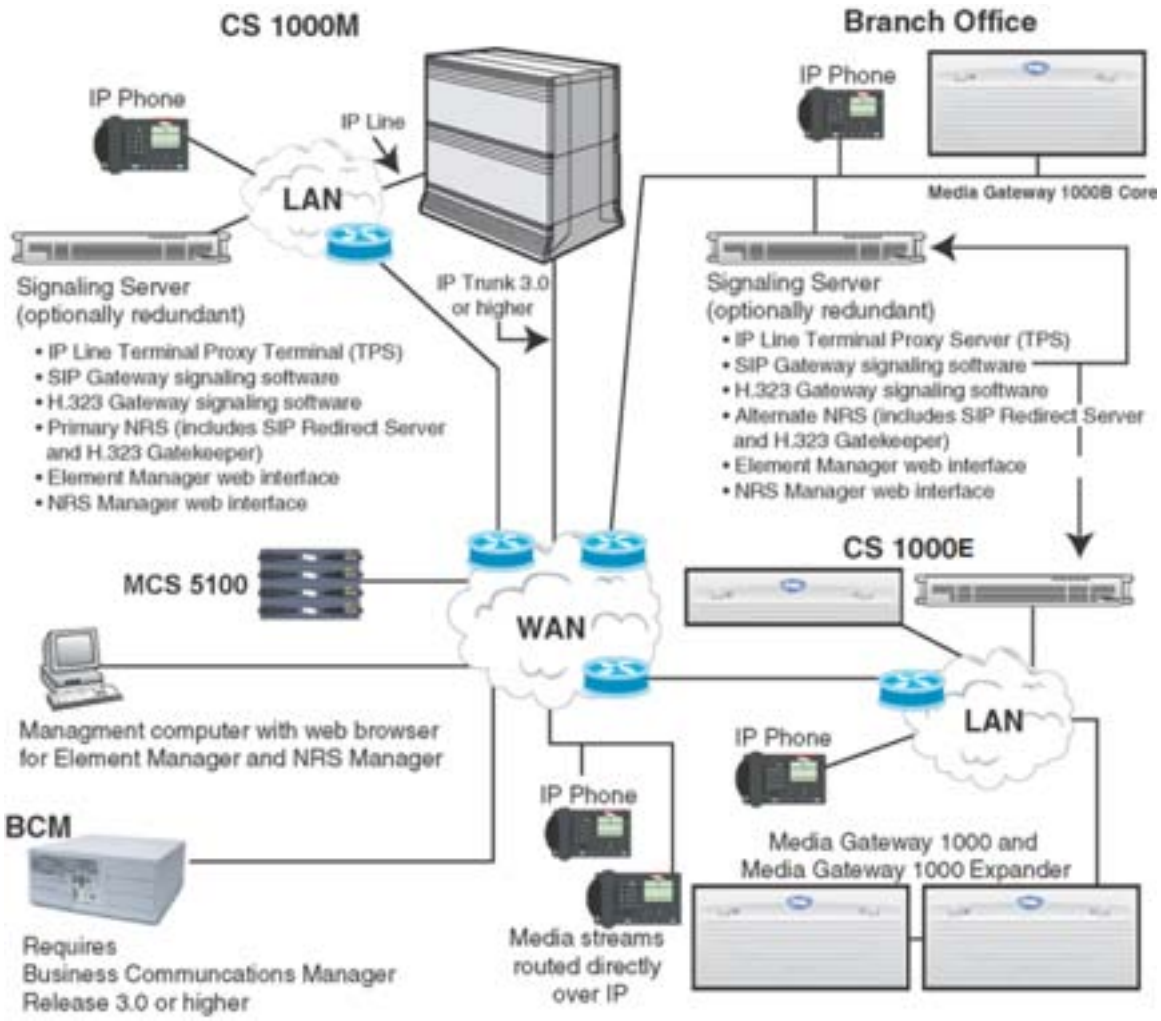

Figure 1: An example of IP Peer Networking

Signaling Server

The Signaling Server provides a central processor to drive SIP and H.323 signaling for IP Phones and IP Peer Networking. The Signaling Server is an industry-standard PC-based server that provides signaling interfaces to the IP network.

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 IP Line Applications Fundamentals (NN43001-125)*.

IP Line 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, Unicode Directory, Callers List and Redial List.

Note:
For detailed information on the IP Line application and the IP Phone Application Server, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

- SIP Gateway signaling software, including IP Peer access and SIP Converged Desktop Service
- H.323 Gateway signaling software for IP Peer access

The software components are described in the sections that follow.

For more information, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Scalability

Both SIP and H.323 Virtual Trunks are supported.

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 4096.

- Each SIP call uses one File Descriptor.
- Each incoming H.323 call uses one File Descriptors.
- Each outgoing H.323 call uses two 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 3700 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 2: Maximum number of Virtual Trunk on each Signaling Server on page 25 gives examples of the maximum number of Virtual Trunks supported for different configurations.

Table 2: Maximum number of Virtual Trunk on each Signaling Server

SIP	H.323 (see Note)			Total Virtual Trunks
	Incoming	Outgoing	Total H.323	
3700	0	0	0	3700
0	1200	1200	2400	2400
0	0	1850	1850	1850
1200	0	1200	1200	2400
1200	600	900	1500	2700

Note:
Assumes H.245 tunneling is enabled.

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

(Num_of_SIP x 1 FD) + (Num_of_Incoming_H323 x 1 FD) + (Num_of_Outgoing_H323 x 2 FD) <= Max_Num_of_SSRCs

where Max_Num_of_FDs = 4096 since maximum SSRC=3700

Impact of H.245 tunneling

By default, H.245 tunneling is enabled. Unless there is a specific reason to disable tunneling, such as for maintenance, it should always be enabled. When tunneling is disabled, the handling capacity of the Signaling Server is reduced to a maximum of 900 H.323 Virtual Trunks. See H.245 tunneling on page 44.

More information

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)*

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.

For a summary of the telephones supported by IP Peer Networking for IP telephony, see *IP Phones Fundamentals* (NN43001-368).

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

SIP Gateway Signaling software

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

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

- acts as a SIP User Agent, which services one or more end users in making/receiving SIP calls
- acts as a signaling gateway for all CS 1000 telephones (IP Phones, analog [500/2500-type] telephones, and digital telephones), which maps ISDN messages to and from SIP messages

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

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

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

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

The direct SIP interface provides the following:

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

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

SIP Converged Desktop Service

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

H.323 Gateway Signaling software

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

Direct IP media paths provide the following benefits:

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

See Interworking protocols on page 39 for further information.

Overlap Signaling

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

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

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

For detailed information, refer to Overlap signaling on page 205.

SIP Line

Inclusion of SIP endpoints into Communication Server 1000 (CS 1000) is based on the Universal Extension (UEXT) line type and SIPL subtype. Virtual TNs are used to represent devices or IP Phones that are external to a CS 1000 system. Configuring SIP IP Phones as CS 1000 UEXTs with SIPL subtype provides a line appearance to the SIP IP Phones.

SIP IP Phones supported by CS 1000 can behave either as a regular UEXT or as a SIP Line. The behavior of a particular IP Phone depends on how it is configured in LD 11. For example, if SIPN is entered at the UXTY prompt, an IP Phone 1120 behaves as a regular UEXT. Only trunk features are provided to such a telephone. However, if SIPL is entered at the UXTY prompt and 1 0 0 0 is entered at the MCCL prompt, then an IP Phone 1120 behaves like a SIP Line telephone. The use of features for a of a particular IP Phone depends on how it is configured.

Each SIP line instance is hosted by a CS 1000 Call Server. Each UEXT represents one SIP user. A SIP Line Gateway (SLG) serves as both a SIP registrar and a SIP Proxy to users, and uses AML or ISDN or SSD messages to communicate internally with the Call Server.

Hardware and software requirements

The SIP Line comprises three major software components:

- CS 1000 Call Server
- SIP Line Gateway
- Short Message Service (SMS)
- Package (346)

Call Server software changes are bundled within the SIPL Package (417). Both SIP Line Gateway and SMS are Signaling Server applications that reside on a commercial off-the-shelf (COTS) or CP PM Signaling Server. The SIP Line Gateway and SMS applications cannot reside on an ISP 1100. You must upgrade CS 1000 Release 7.0 software to enable and configure SIP Line Service.

SIP Line Gateway redundancy

You can implement a leader or follower configuration can be implemented for a SIP Line Gateway node with both servers sharing the same node IP address. However, you can register IP Phones on a redundantly configured SIP Line Gateway node can only on the node master. No load sharing between the two SIP Line Gateways exists.

Codec negotiation and selection

Codec negotiation and selection are the same as for a SIP Gateway. No new codecs are added for SIP Line Gateways.

The following codecs are supported: G.711 u-law/a-law, G.729A/AB, G.723.1, and T.38 for FAX. By default, G.711 needs to be supported at both ends. The default payload sizes for G.711 and G.729 are both 20ms. Any other unrecognized codec (including video) is forwarded to the far-end through the SDP-transparency feature.

Codec selection

A SIP Line Gateway always sends out the offerer codec list in order of preference. The receiver selects one common codec based on its own preference. This means that the receiver of an offer always performs the codec selection, and the receiver selects one common codec based on the best bandwidth or best quality selection mechanism.

For information on codec negotiation and selection, see *Converging the Data Network for VoIP Fundamentals (NN43001-260)*.

Codec payload size considerations

Refer to Table 3: Supported codecs and payload size on page 29 for a list of codec and payload sizes supported by each client.

Table 3: Supported codecs and payload size

Codec	Payload size
G.711 A/mu-law	10 millisecond (ms), 20 ms and 30 ms
G.729 A	10 ms, 20 ms, 30 ms , 40 ms and 50 ms
G.723.1	30 ms, although it can limit the number of DSP channels available. See Limitations on page 127.
T.38 for fax	Supported for fax calls on gateway channels

- If no ptime is included in the SDP, the default payload size shall be used (20 ms for G.711 and G.729, 30 ms for G.723.1). This is the recommended behavior.
- If a specific payload size is configured different from the default payload size, a ptime shall be included in the offer. There can be only one ptime per codec in this version of SDP.

Codec profiles

Codec refers to the voice coding and compression algorithm used by the DSPs on the Virtual Trunk. The G.XXX series of codecs are standards defined by the International Telecommunications Union (ITU). Different codecs have different QoS and compression properties. The specific codecs and the order in which they are to be used for codec negotiation.

The final codec used is determined by the codec negotiation process with the far end during call setup. Parameters can be configured for each codec in an image.

Virtual Trunk supports the following codecs:

- G.711
- G.729AB
- G.729B
- G.723.1

G.711 The G.711 codec delivers "toll quality" audio at 64 kbit/s. This codec is optimal for speech quality, as it has the smallest delay and is resilient to channel errors. However, it uses the largest bandwidth. The G.711 codec is the default codec if the preferred codec of the originating node is not available on the destination Virtual Trunk.

G.729AB The G.729AB codec is the default preferred codec when adding a new Virtual Trunk node. This codec provides near toll-quality voice at a low delay. The G.729AB codec uses compression at 8 kbit/s (8:1 compression rate).

G.729B The G.729B codec uses compression at 8 kbit/s (8:1 compression rate). Optional B Voice Activity Detection/Silence Suppression is configurable

G.723.1 (5.3 kbit/s or 6.3 kbit/s) The G.723.1 codec provides the greatest compression.

Geographic redundancy and Branch Office

Geographic redundancy (GR)/Survivable Branch Office (BO) uses a GR N-Way database replication model that allows the Main Office (MO) and GRMO to use the same database without manual replication. Any BO SIP IP Phone set should be able to register through the BO, the MO or the GRMO, depending on the failover case.

Only GR 1+1 is supported. GR N+1 is not supported.

The GR/BO SIP Line Gateway sends keepalive messages regularly and they are a critical decision maker in case of any incoming registration or calls based on the background keepalive mechanism.

There are two approaches to support GR/BO for SIP Line clients: S1/S2 configuration or DNS configuration. Because not all IP Phones support S1/S2 configuration, both the S1/S2 solution and the DNS solution are offered in GR/BO operation. This option is chosen on a per-SIP Line Gateway basis.

The following behavior is observed for DNS servers:

- Windows Server – multiple IP addresses can be configured without priority control. The default is round robin. Round robin can be configured as static. It is a system wide setting. Response depends on the request subnet. The order is out of control.
- Linux BIND – seems to have order control. The default is cyclic.
- Nortel NetID – based on BIND, multiple IP addresses can be configured without priority control. The default is round robin. It is possible to change to fixed with rules defined.

Branch Office operation

The operation from a BO client point of view in an S1/S2 configuration:

Client configuration

- BO client S1 – pointing to BO SLG
- BO client S2 – pointing to GR SLG

Normal operation

- Client tries registration with BO SLG (S1)
- BO SLG maintains status of both MO and GR
- BO SLG redirects client to MO SLG

BO down

- Client tries registration with GR SLG (S2)
- GR SLG maintains status of MO
- GR SLG redirects BO client to MO SLG

MO down

- Client tries registration with BO SLG (S1)
- BO SLG redirects BO client to GR SLG

MO comes back

- GR SLG stops responding to client “keep alive”
- Client tries registration with BO SLG (S1)
- BO SLG redirects client to MO SLG

Geographic redundancy operation

The operation from a MO client point of view in an S1/S2 configuration:

Client configuration

- MO client S1 – pointing to GR SLG
- MO client S2 – pointing to Main SLG

Normal operation

- Client tries registration with GR SLG (S1)
- GR SLG maintains status of MO
- GR SLG redirects client to MO SLG

MO down

- Client tries registration with GR SLG (S1)
- GR SLG maintains status of MO, client stays at GR

MO comes back

GR SLG redirects client to MO SLG

Signaling Server and system SIP Line capacity

The recommended maximum SIP Line users per-SIP Line Gateway is 1000 on a COTS Signaling Server and 400 on a CP PM Signaling Server. The maximum SIP Line users per CS 1000 system is 10,000. For TN space planning, each SIPL UEXT requires one SIPL VTRK on each call for the duration of the call. SIPL VTRK is not calculated against any ISM checkings. However, it is recommended to have a 1:1 ratio between SIPL UEXT and SIPL VTRK TN.

Line and trunk calculation

All SIP Line users are configured as SIPL UEXT. This line type operates as any other line type, with the exception that one extra SIP Access Point is required per user. Other than this, the Line and Trunk calculation, in terms of TN planning and Traffic planning, applies to the SIP Line feature.

Further information on SIP Line service

For further information on enabling and configuring SIP Line service, see *SIP Line Fundamentals (NN43001-508)*.

Vacant Number Routing

IP networks usually contain only a subset of the numbers that could be used to reach them. Therefore, calls to the IP network need to be able to reroute to an alternate, while maintaining the ability to receive vacant number treatment when the called destination is an unassigned number.

Vacant Number Routing (VNR) and MALT (Meridian ALTernate Routing) functionality are combined for calls routed over an IP network. Vacant Number Routing is a default route used for routing untranslated / invalid /unassigned called numbers (dialed numbers, DN's). MALT is performed at the Call Server to retry the call using an alternate route, if a call over the IP network is disconnected with a cause which matches one of the MALT cause codes, or disconnects with an indication to "use MALT".

If MALT exhausts all the MALT routes, including non-IP routes, in the VNR Route List Index (RLI), then the treatment corresponding to the disconnect cause is provided. If the call clearing message has the cause as 'unassigned number' or 'invalid Number format' in all the accessed entries of the VNR RLI, then vacant number treatment is provided. If any of the accessed

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

MALT on calls routed to the IP domain

With the default MALT handling, there are six causes which perform MALT on a CS 1000 system.

- 3 - No route to destination
- 27 - Destination is out of service
- 34 - No circuit or channel available
- 38 - Network out of service
- 41 - Temporary failure
- 42 - Switching equipment congestion

For VNR over IP, MALT is also performed for cause codes which come with an indication to “use MALT” along with the call clearing message from the Signaling Server. The six default MALT cause codes are the only cause codes supported to trigger any rerouting in PRI and BRI.

Configurable MALT causes for different vendors

An option is provided in Element Manager to configure causes to perform MALT.

The causes which can be configured are

- 01 – Unassigned number or 28 – Invalid number
- 20 – Subscriber absent
- 47 – Resources unavailable
- 51 – Call rejected; blocked by MBG
- 52 – Outgoing call barred
- 53 – Outgoing call barred in closed user group
- 54 – Incoming call barred
- 55 – Incoming call barred in closed user group
- 63 – Service or option not available
- 127 – Interworking unspecified

This is the only provisioning change for CS 1000 Release 6.0. Provisioning for VNR and MALT prior to CS 1000 Release 6.0 remains in effect. There is no change on the Call Server.

If a call is disconnected with one either (1) an H.323 clearing reason or cause code, or (2) a SIP response code that maps to one of the configurable causes and the cause is configured on the Signaling Server to perform MALT, then a new IP IE is built with an indication to “use

MALT” with that cause. The new IE is sent to the Call Server with the ‘Disconnect’ message. The Call Server triggers MALT for that cause.

The configuration on Element Manager to perform MALT is divided into "Nortel vendors" and "Third party vendors". The Nortel vendor option applies to the products in Table 4: NORTEL Systems on page 34. The Third party vendor option applies to the products in Table 5: Third-Party Systems on page 34.

Unassigned Number cause to perform MALT is configured by default in Element Manager for both Nortel and Third Party vendors.

Table 4: NORTEL Systems

Internal constant	ID string	Comments
Early BCM systems	"Nortel Networks Enterprise Edge VoIP Gateway"	H.323 only
Current BCM systems	"Nortel Networks BCM VoIP Gateway"	This ID is used for H.323 and possibly for SIP. BCM supports SIP in the current release.
CS 1000	"Nortel_CSE_1000"	H.323 or SIP
Original ITG Trunk	"Nortel_ITG"	H.323 only. Not compatible with the CS 1000 VTRK except as a minimum function gateway. Cannot provide additional services.
ITG Trunk release 3.0 and 3.01	"Nortel_IPT"	H.323 only. Release 3.0 and 3.01 of ITG-T (Nortel_ITG). Compatible with the CS 1000 gatekeeper
Mediatrix	"H.323 - 4 Ports FXS"	H.323
CS 2000	"Nortel_CS_2000"	H.323 and SIP. This ID is also used by the CS 2100.
CSEMX	"Nortel_IMS"	H.323 and SIP

Table 5: Third-Party Systems

Internal constant	ID string	Comments
ACME	"Acme Packet H.323 Session Border Controller"	H.323
	… all others	H.323 and SIP

Configuration

For the VNR feature to work properly, VNR, MALT and CTVN must be configured.

1. VNR (LD 15)

   VNR has to be set to YES in LD 15; NET_DATA and the RLI that has to be chosen for VNR calls should be given. The prerequisite for configuring VNR is FNP has to be set to YES.

   VNR configuration has not changed. To configure VNR see VNR enhancement on page 182.

2. MALT (LD 86)

   MALT is done based on SBOC configurations done in the RLB for VNR RLI. If SBOC is set to RRA, then rerouting will be done in the current node for all the MALT cause values. If SBOC is set to RRO, then rerouting is done at the originating node. If SBOC is set to NRR, then MALT will not be done. The NALT prompt should be set with the number of the alternate route that is to be tried for the respective RLI.

   Set SBOC on the last entry as any value other than RRA/RRO. That is, make it NRR – no reroute.

   SBOC configuration has not changed.

   To configure causes to perform MALT, follow the steps in Configuring causes to perform MALT on page 168.

3. CTVN (LD 15)

   Follow existing CTVN configuration. For more information on CTVN configuration, see Intercept Treatment in *Features and Services Fundamentals—Book 4 of 6 (I to M) (NN43001-106)*.

Feature impact on upgrade and rollback tasks

There are no specific requirements for upgrade. If a CS 1000 Release 5.5 or 6.0 system has not yet been upgraded to CS 1000 Release 7.0, or if a system is downgraded from CS 1000 Release 7.0, ensure that the lower release systems have the proper patches to build the reason header when interacting with higher releases.

Network Routing Service

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

Note:

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

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

The NRS combines the following:

- SIP Proxy (see SIP Proxy software on page 36) and SIP Registrar (see SIP Registrar on page 36)
- H.323 Gatekeeper (see H.323 Gatekeeper software on page 37)
- Network Connection Service (NCS) (see H.323 Gatekeeper software on page 37)

The SIP Proxy 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 Proxy 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 IP Line Applications running on the Signaling Server on page 24.

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

For more information, see *Network Routing Service Fundamentals (NN43001-130)*.

SIP Proxy software

Building on the H.323 Gatekeeper, the SIP Proxy 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 Proxy translates telephone numbers recognized by Enterprise Business Network (EBN) voice systems to IP addresses in the SIP domain. As a result, the SIP Proxy interfaces with SIP-based products.

The SIP Proxy is used to interconnect with other Nortel communication servers using SIP. Along with the H.323 Gatekeeper application, the SIP Proxy has access to the endpoint/location database. The SIP Proxy 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 Proxy.

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 Fundamentals (NN43001-130)*.

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 Fundamentals (NN43001-130)*.

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.

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

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 Proxy/Redirect Server. NRS Manager is used for populating the location and registration database. For detailed information, refer to *Network Routing Service Fundamentals (NN43001-130)*.

ISSS synchronization

ISSS synchronization provides central configuration from the Nortel Unified Communications Management Common Services (UCM Common Services). ISSS configuration is managed on a network, wide basis. ISSS configuration is written to a file that is securely synchronized on all elements known to UCM Common Services.

For more details on ISSS synchronization, see *Security Management Fundamentals (NN43001-604)*.

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 6: SIP components on page 40 lists and describes the SIP components.

Table 6: 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/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:
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:
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.

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 6.0 NRS is comprised of a SIP Proxy and Redirect Server, NCS, and GK. The SIP Server can operate in Proxy or redirect mode. The 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 (LTPS), IP Peer virtual trunk SIP or H.323 signaling Gateway (VTRK GW), IP Phone Application Server.

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.

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 7: H.323 components on page 43 lists and describes the H.323 components.

Table 7: 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 Virtual Trunk, 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 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 2400 H.323 Virtual Trunks
- up to 3700 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:

3700 - [(1 x H.323 channels) + SIP channels] (where 3700 is the maximum number of Virtual Trunks)

Example 1: 2400 H.323 and 1200 SIP

3700 - [(1 x 2400 H.323 channels) + 1200 SIP channels] = 100 available Virtual Trunks

Example 2: 1800 H.323 and 1800 SIP

3700 - [(1 x 1800 H.323 channels) + 1800 SIP channels] = 100 available Virtual Trunks

Example 3: 0 H.323 and 3700 SIP

3700 - [(1 x 0 H.323 channels) + 3700 SIP channels] = 0 available Virtual Trunks

Example 4: 2400 H.323 and 0 SIP

3700 - [(1 x 2400 H.323 channels) + 0 SIP channels] = 1300 available Virtual Trunks

Note:
The 1300 available trunks must be SIP trunks, as the number of H.323 channels is already at the maximum limit of 2400.

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 1850 H.323 Virtual Trunks
- up to 3700 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:

  3700 - [(2 x H.323 channels) + SIP channels] (where 3700 is the maximum number of Virtual Trunks)

  Example 1: 1850 H.323 and 0 SIP

  3700 - [(2 x 1850 H.323 channels) + 0 SIP channels] 3700 - [(3700 H.323 channels) + 0 SIP channels] = 0 available Virtual Trunks

  Example 2: 1200 H.323 and 1200 SIP

  3700 - [(2 x 1200 H.323 channels) + 1200 SIP channels] 3700 - [(2400 H.323 channels) + 1200 SIP channels] = 100 available Virtual Trunks

  Example 3: 0 H.323 and 3700 SIP

  3700 - [(1 x 0 H.323 channels) + 3700 SIP channels] = 0 available Virtual Trunks

Chapter 4: SIP signaling

Contents

This section contains information on the following topics:

Introduction

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

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

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

For information, see SIP Trunk Gateway software trunk route redundancy on page 111.

Figure 2: CS 1000 SIP Trunk Gateway interworking on page 48 shows the CS 1000 SIP Trunk Gateway interworking.

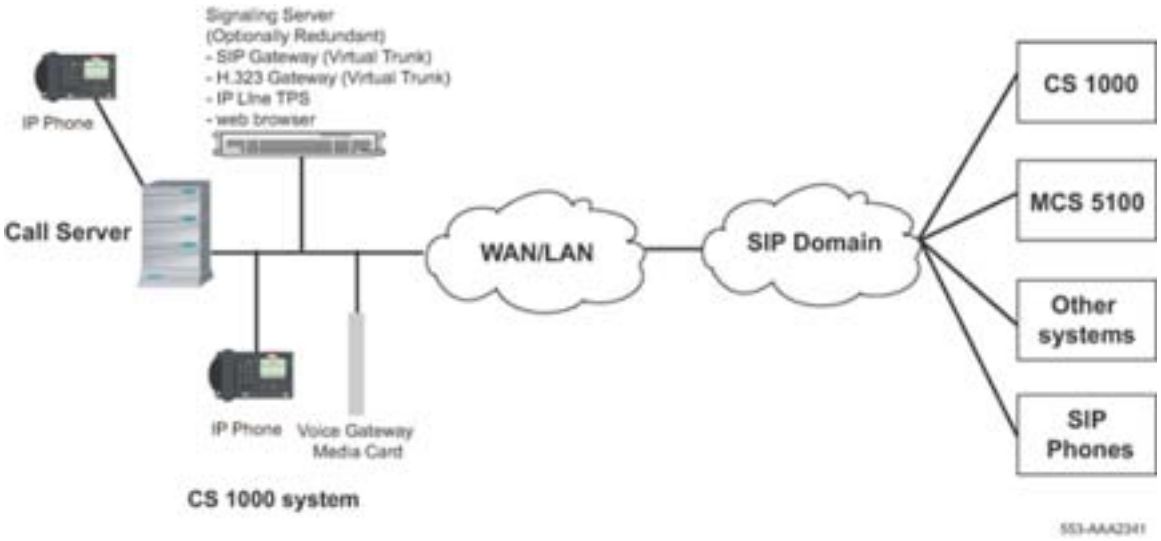

Figure 2: CS 1000 SIP Trunk Gateway interworking

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 8: SIP request methods on page 49 shows the SIP request methods.

Table 8: 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 9: SIP response methods on page 49 shows the SIP response methods.

Table 9: 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:

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:

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 1000MSystems.

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 on page 51 shows a media path routed directly over IP, not using a circuit switch.

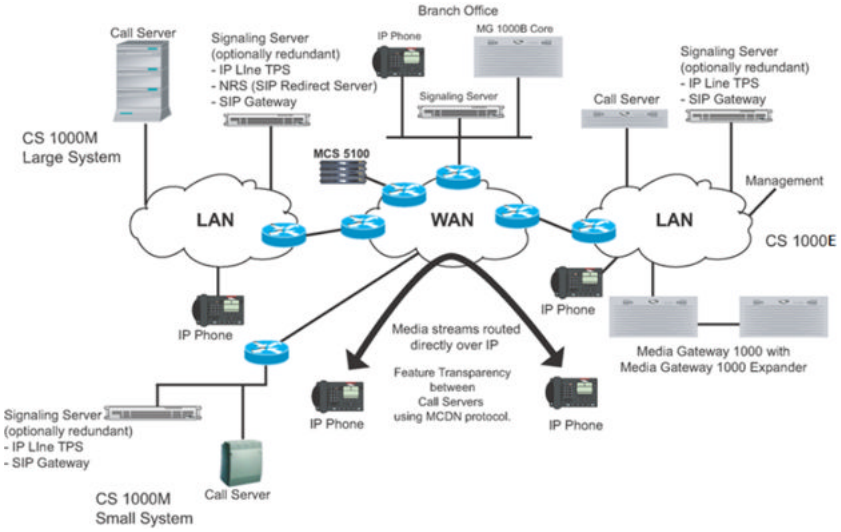

Figure 3: An example of IP Peer Networking using Virtual Trunk and direct media paths

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 on page 53). 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 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 on page 53.

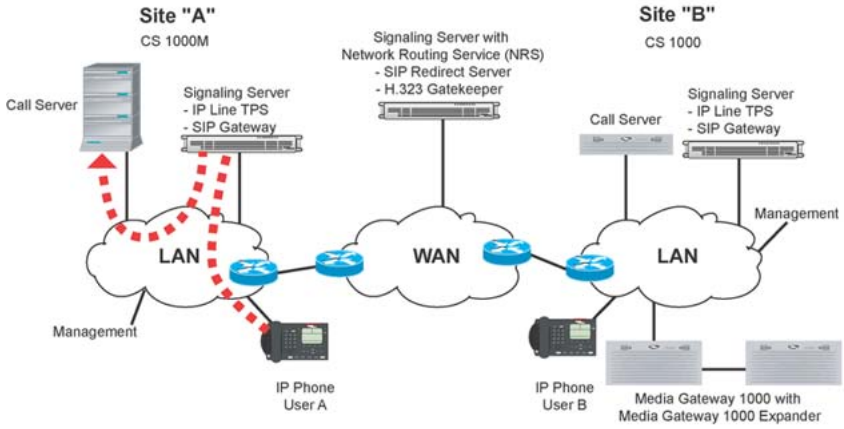

Figure 4: User A dials User B

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 on page 53.

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).

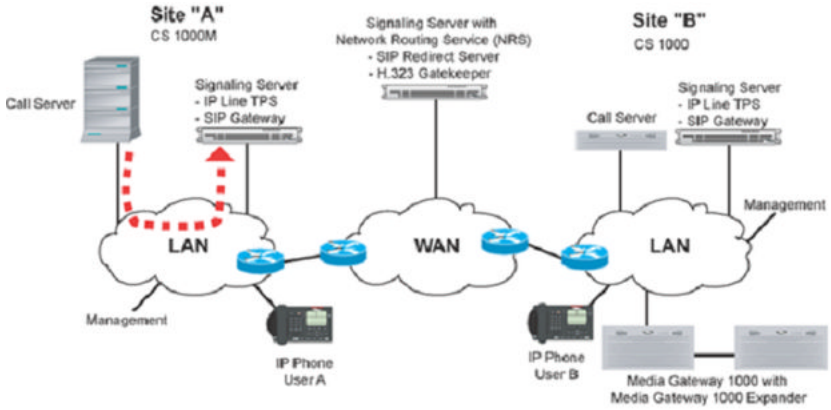

Figure 5: Call Server A routes the call to the IP network

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 on page 54.

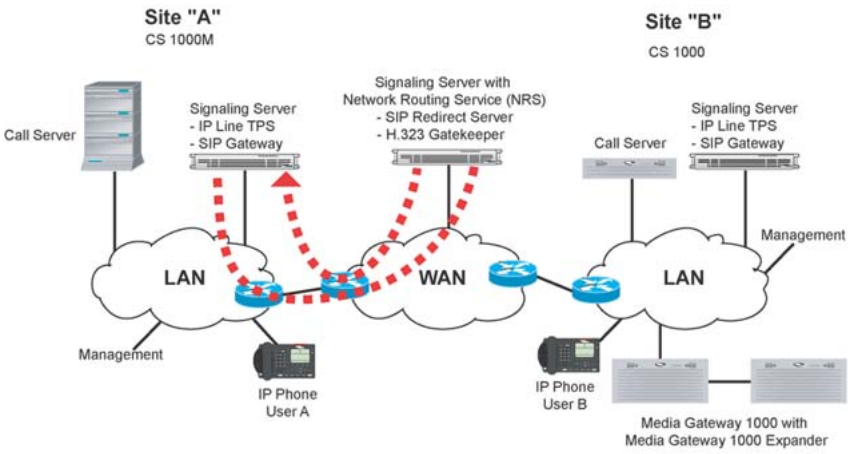

Figure 6: The NRS sends the IP address of SIP Trunk Gateway B to SIP Trunk Gateway A

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 on page 54.

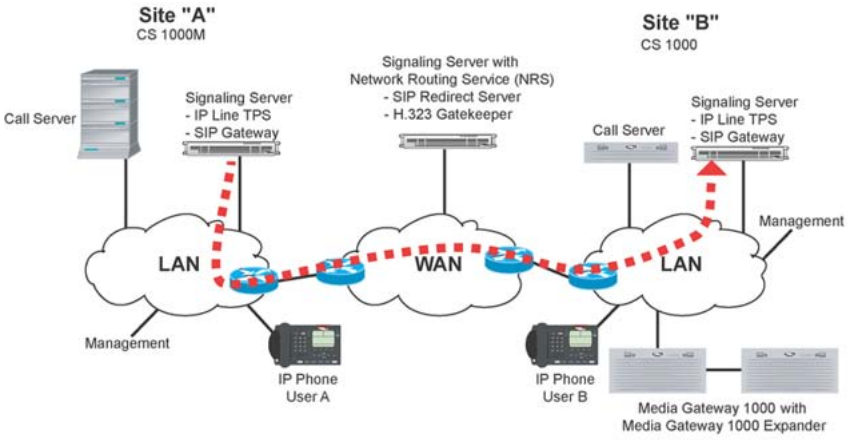

Figure 7: SIP Trunk Gateway A sends an INVITE message to SIP Trunk Gateway B

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 on page 55.

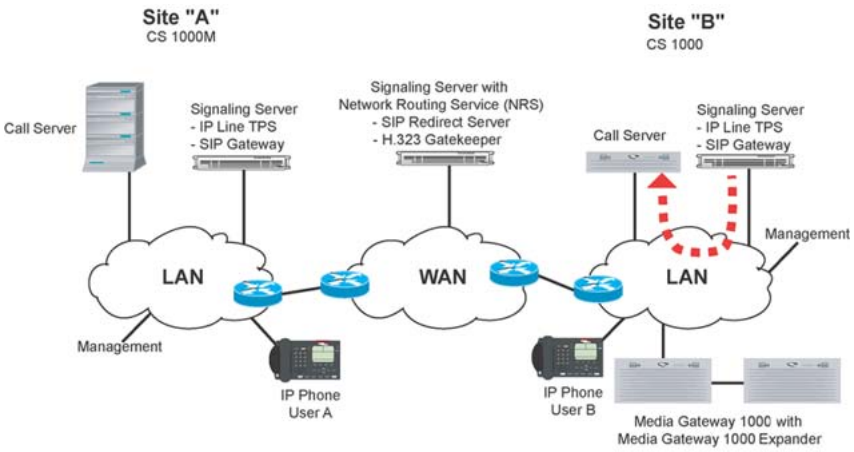

Figure 8: SIP Trunk Gateway B sends the call to Call Server B over a Virtual Trunk

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 on page 55.

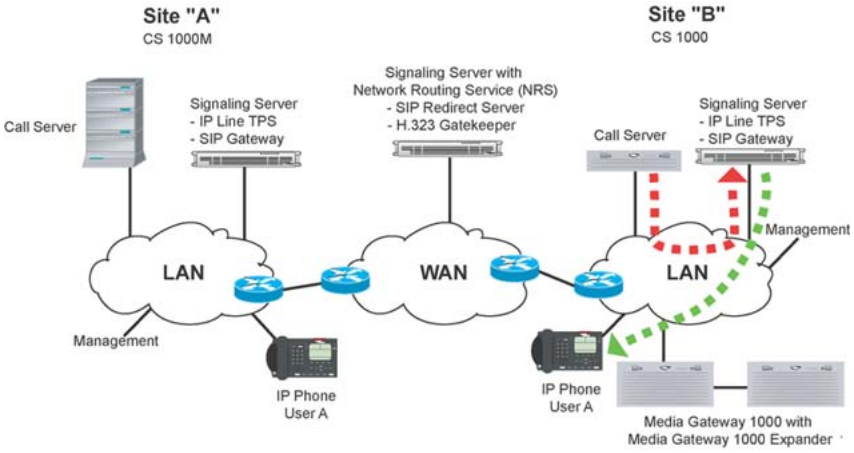

Figure 9: Call Server B sends an Alert message to SIP Trunk Gateway B

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 on page 56.

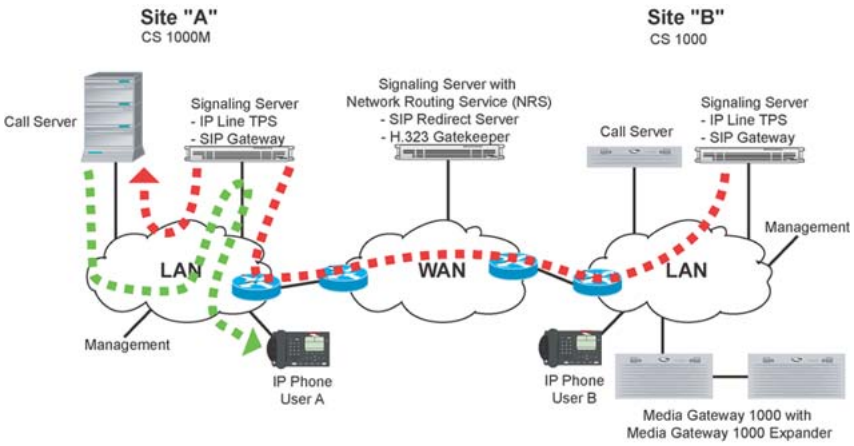

Figure 10: SIP Trunk Gateway B sends an Alert message to Call Server A

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 on page 56.

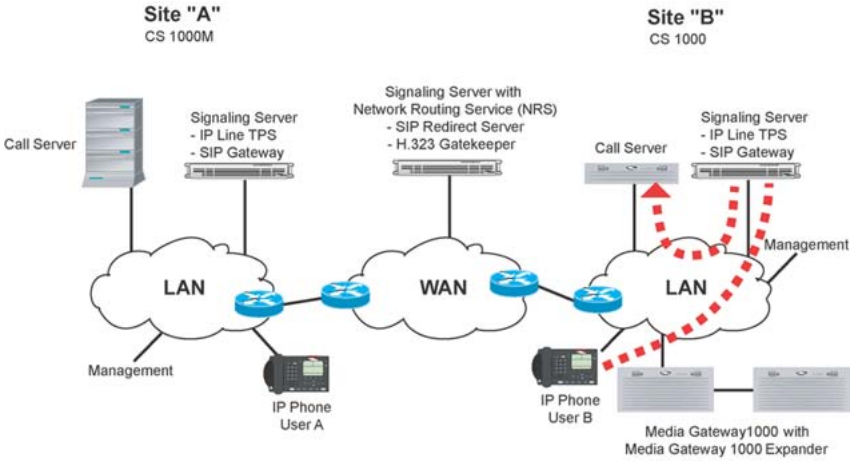

Figure 11: User B answers the call

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 on page 57.

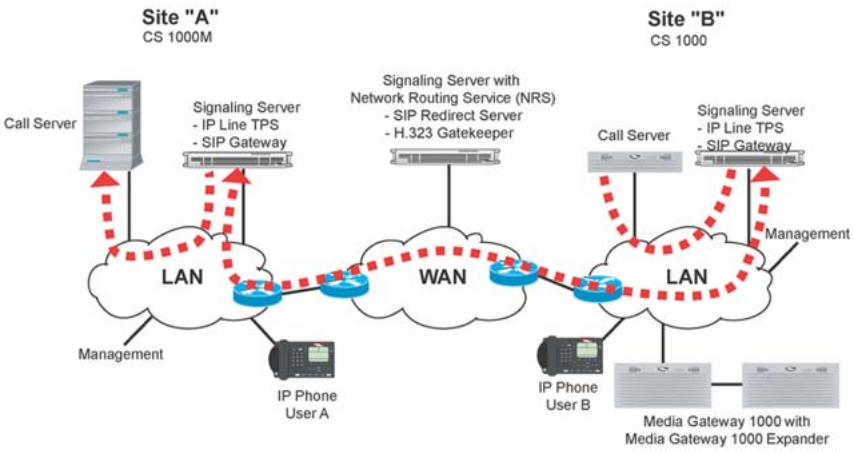

Figure 12: Call Server B sends an ACK message to SIP Trunk Gateway B

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 on page 57.

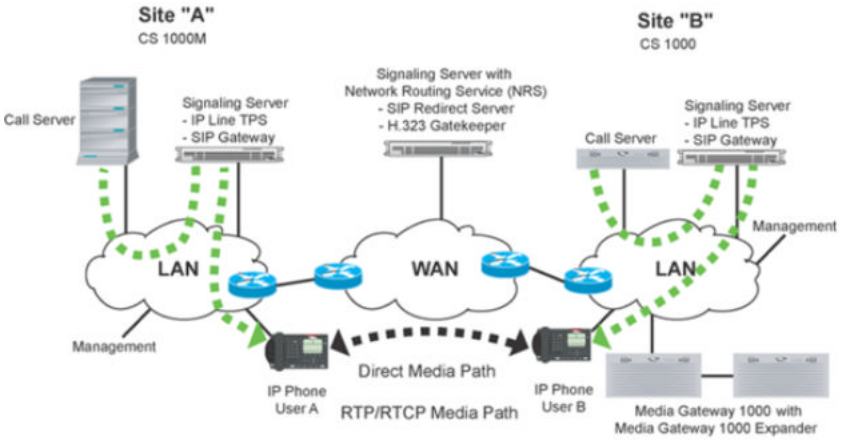

Figure 13: IP Phones start the direct IP media paths

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) on page 52.

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.

Chapter 5: H.323 signaling

Contents

This section contains information on the following topics:

Direct IP Media Paths

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

Note:

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:

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 on page 66 shows a media path routed directly over IP, not using a circuit switch.

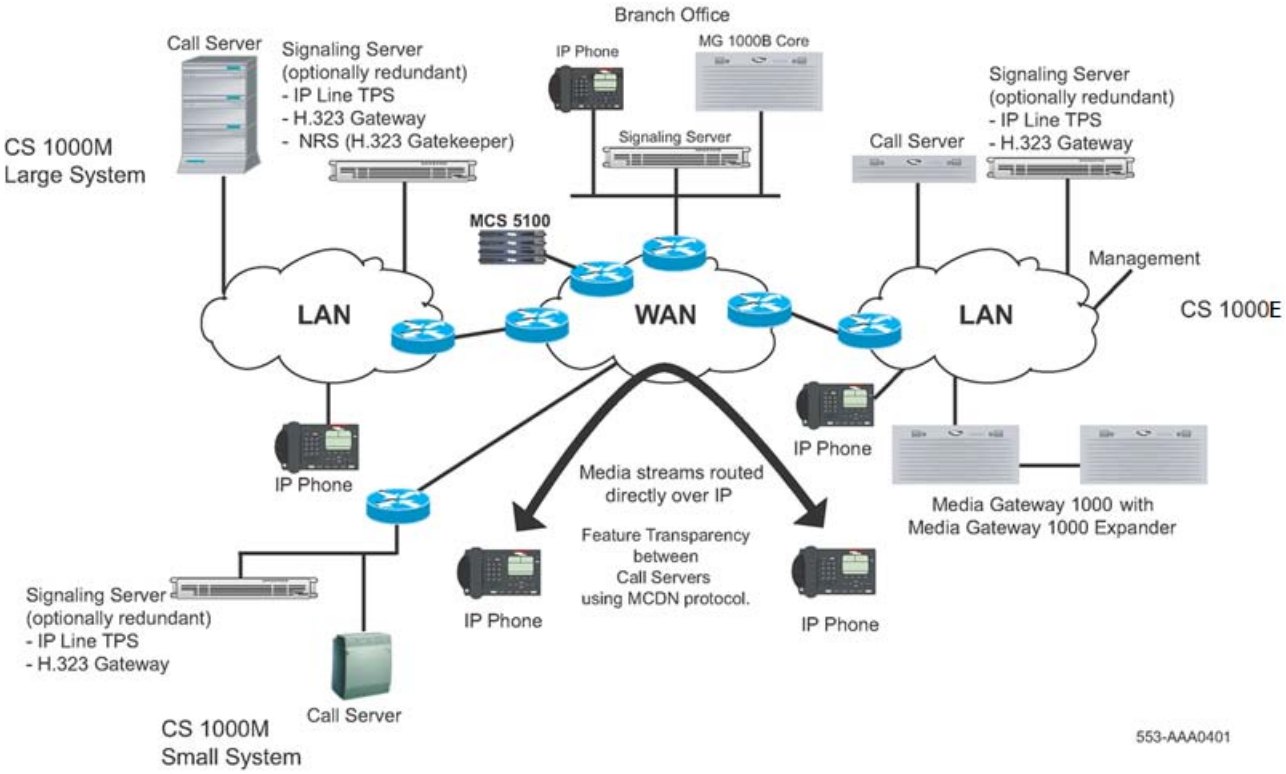

Figure 14: An example of IP Peer Networking using Virtual Trunk and direct media paths

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 on page 68). When the user presses a key on the IP Phone, a signaling message is carried over the IP network.

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

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

originating and terminating Call Servers establish a direct two-way IP media path between the two IP Phones.

Basic network call walk-through

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

By default, H.323 on CS 1000 systems uses en bloc signaling. For overlap signaling, refer to Overlap signaling on page 205.

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:
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 on page 141

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 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 on page 68.

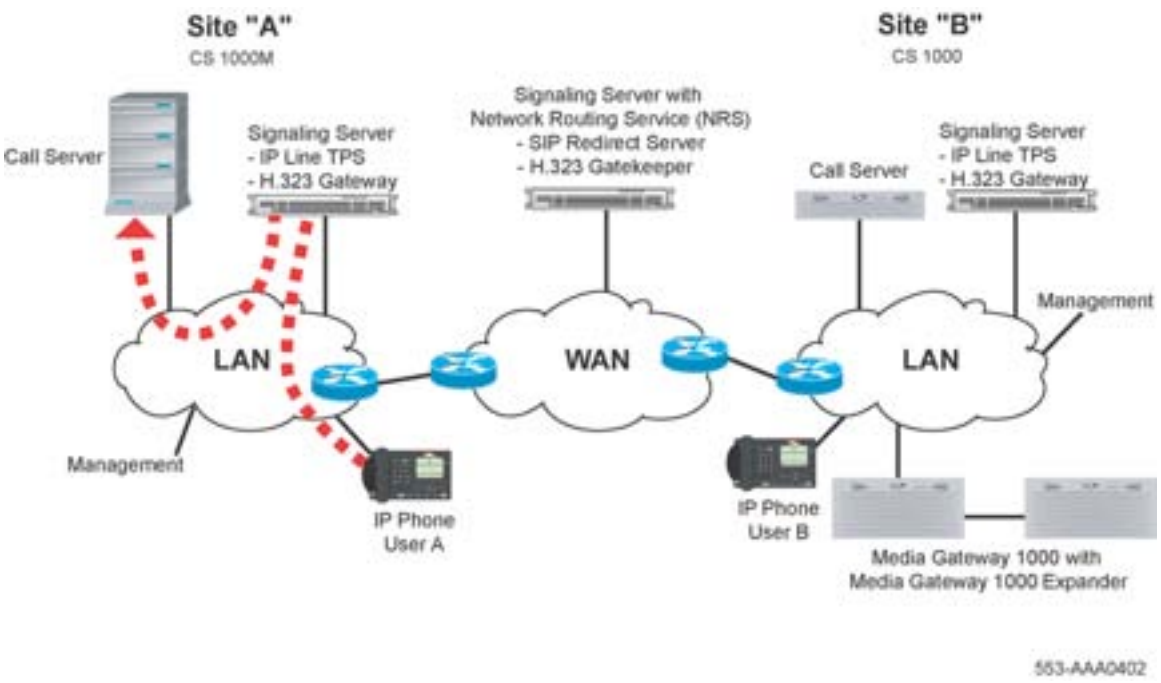

Figure 15: User A dials User B

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 on page 69.

   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).

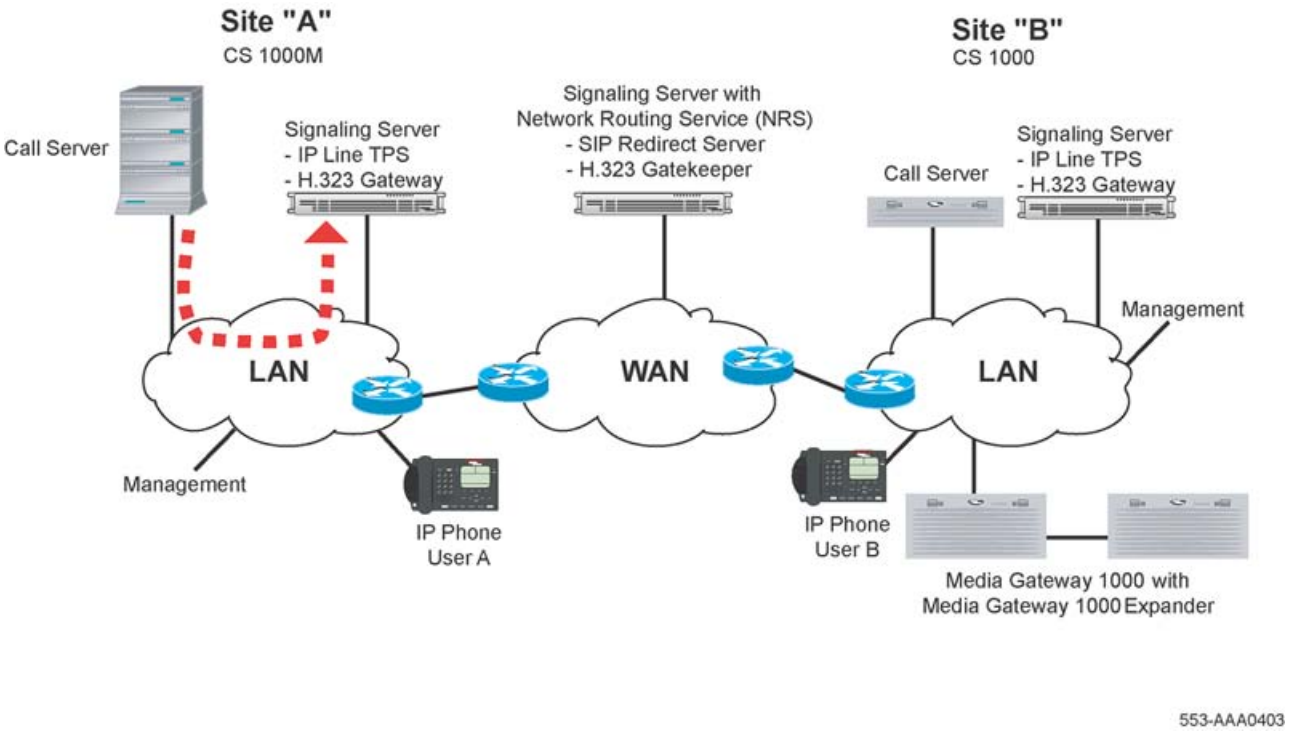

Figure 16: Call Server A routes the call to the IP network

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 on page 70.

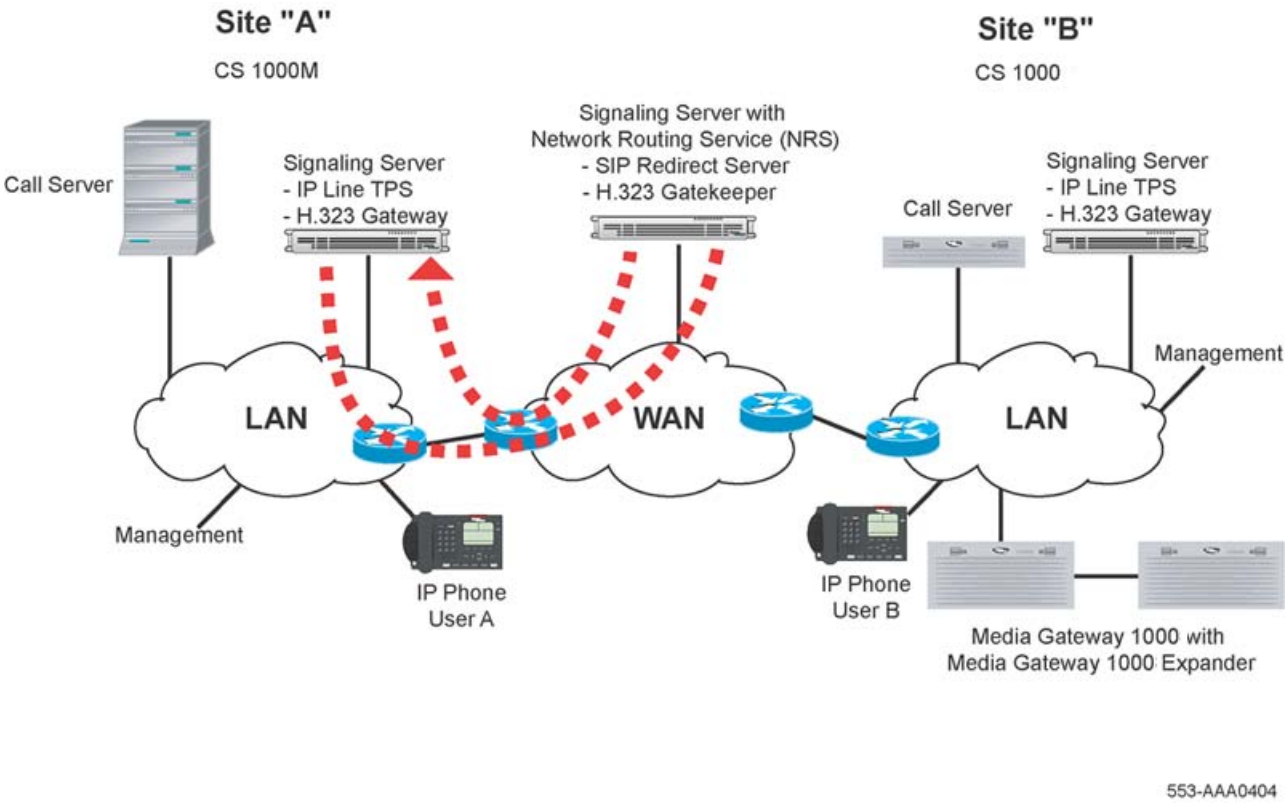

Figure 17: The H.323 Gatekeeper sends the IP address of H.323 Gateway B to H.323 Gateway A

4. H.323 Gateway A sends a SETUP message to H.323 Gateway B, including the DN information. See Figure 18: H.323 Gateway A sends a SETUP message to H.323 Gateway B on page 71.

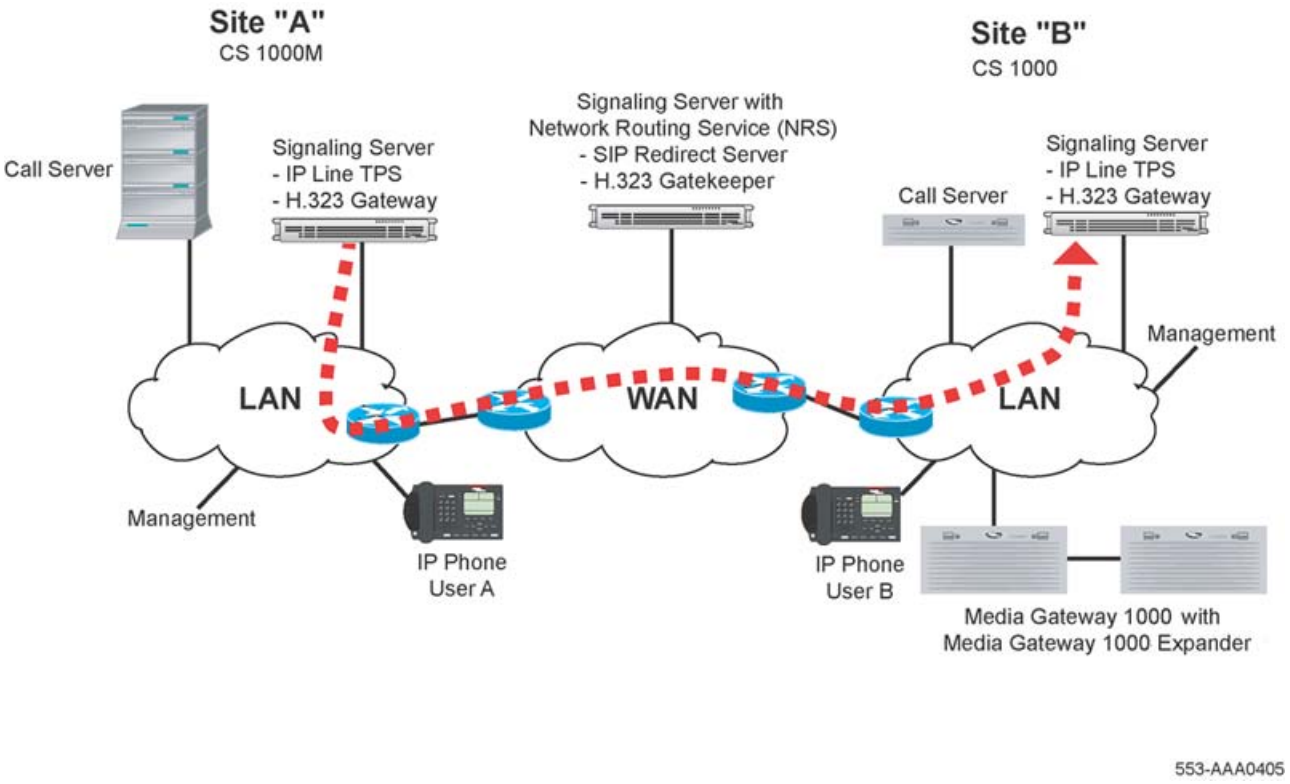

Figure 18: H.323 Gateway A sends a SETUP message to H.323 Gateway B

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 on page 72.

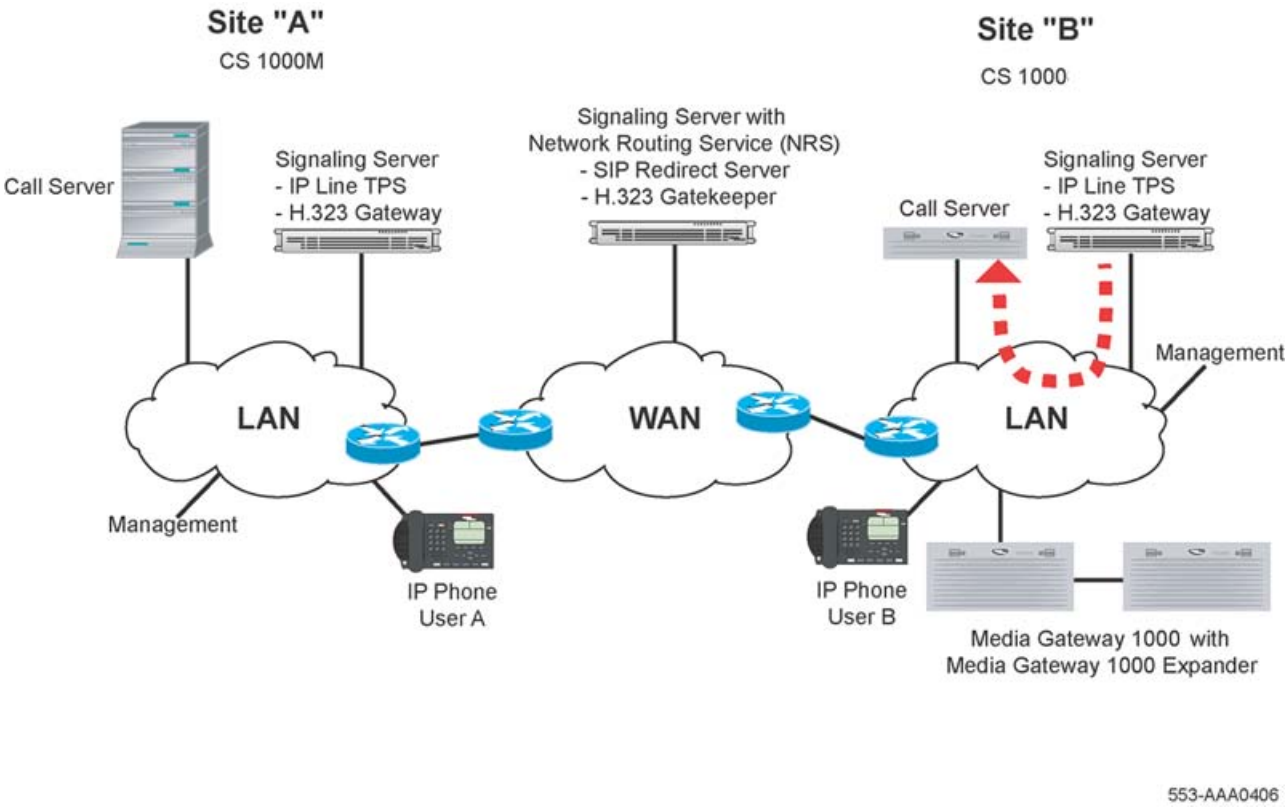

Figure 19: Gateway B sends the call to Call Server B over a Virtual Trunk

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 on page 73.

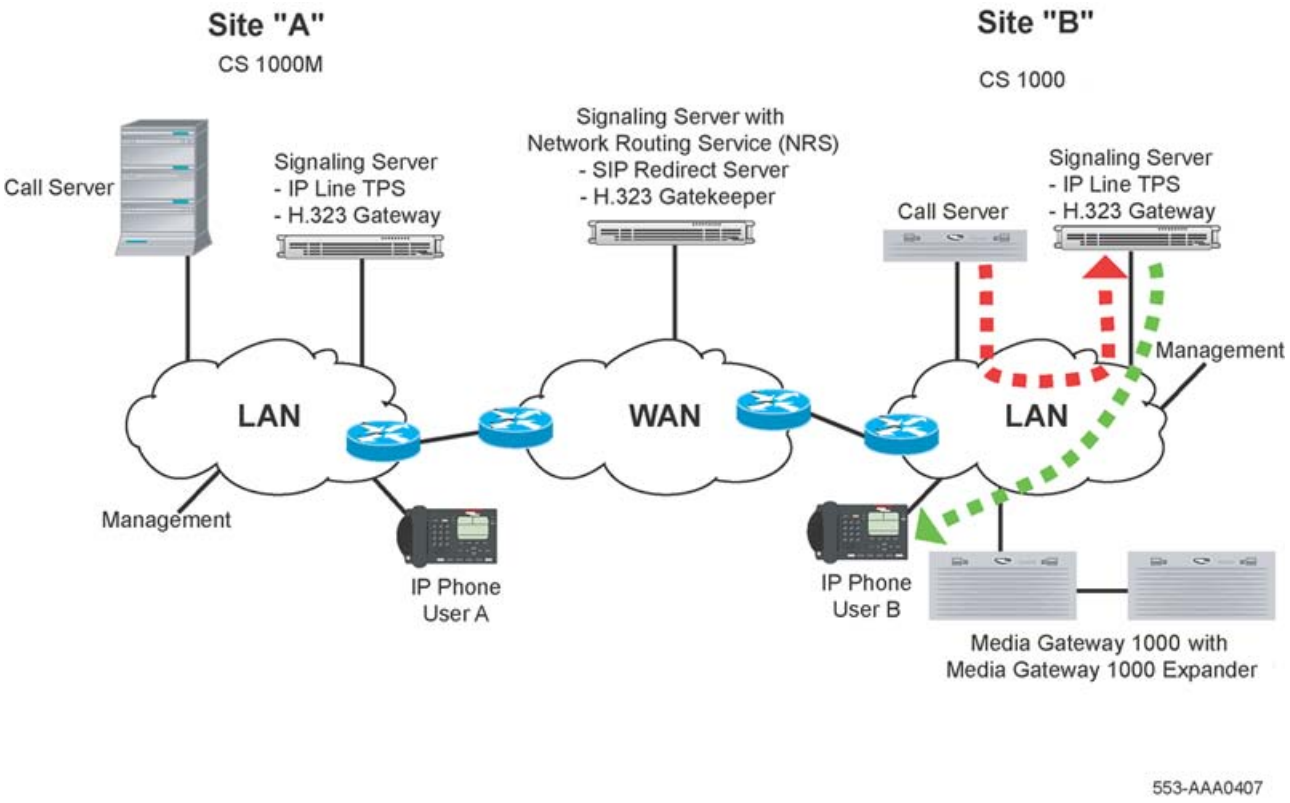

Figure 20: Call Server B sends an alerting message to H.323 Gateway B

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 on page 74.

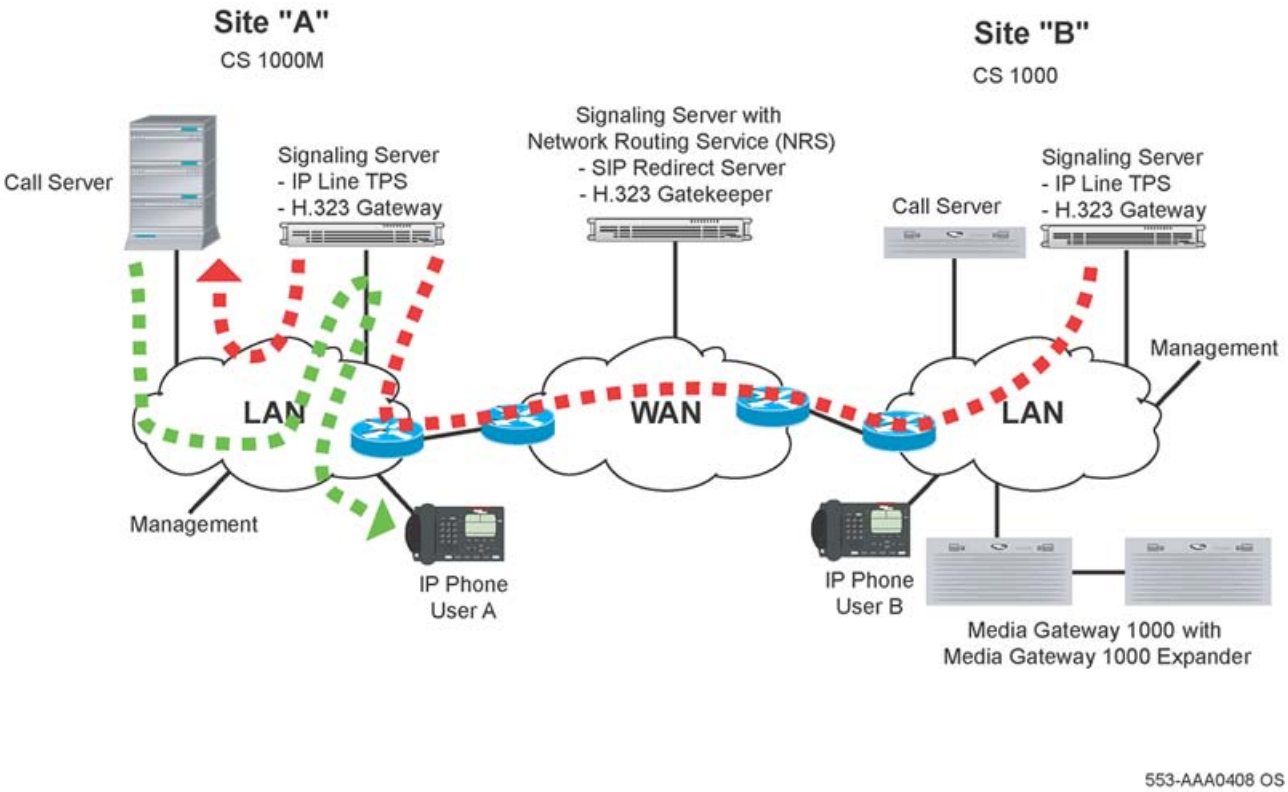

Figure 21: H.323 Gateway B sends an alerting message to Call Server A

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 on page 75.

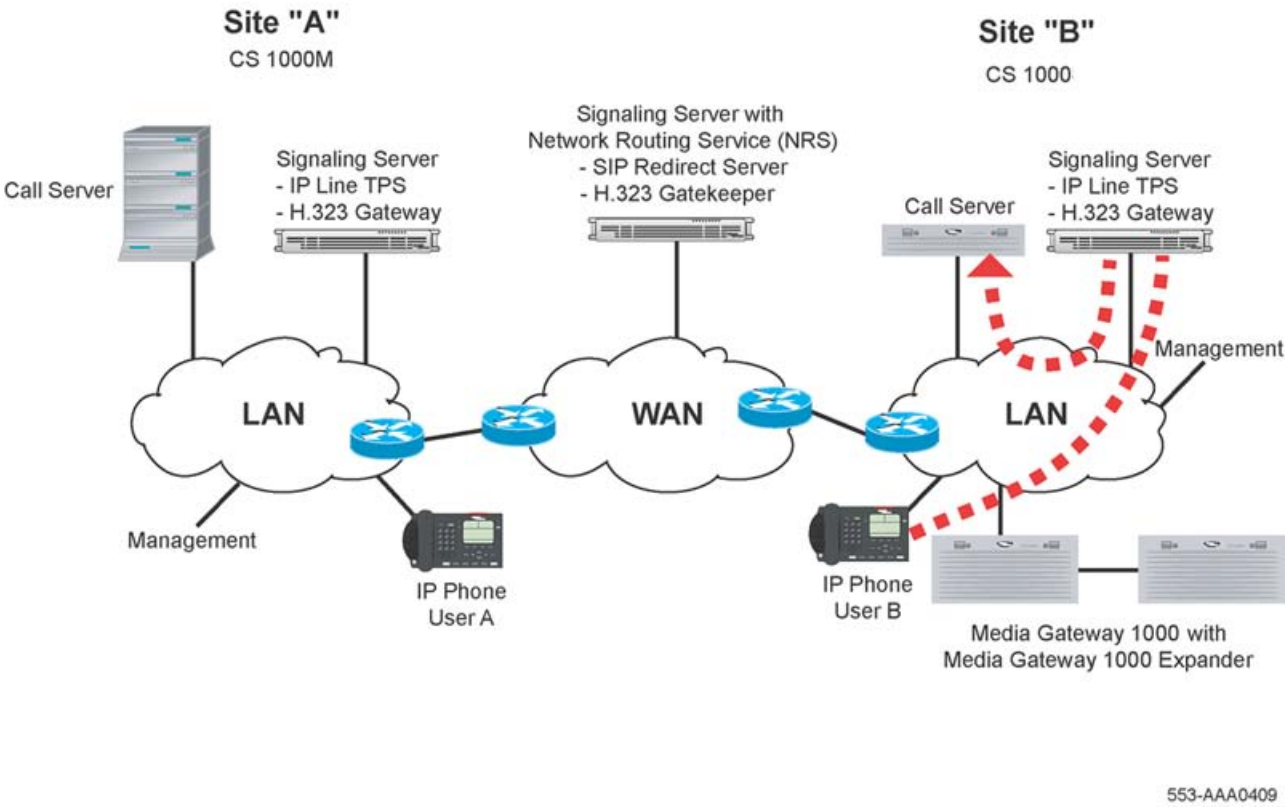

Figure 22: User B answers the call

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 on page 76.

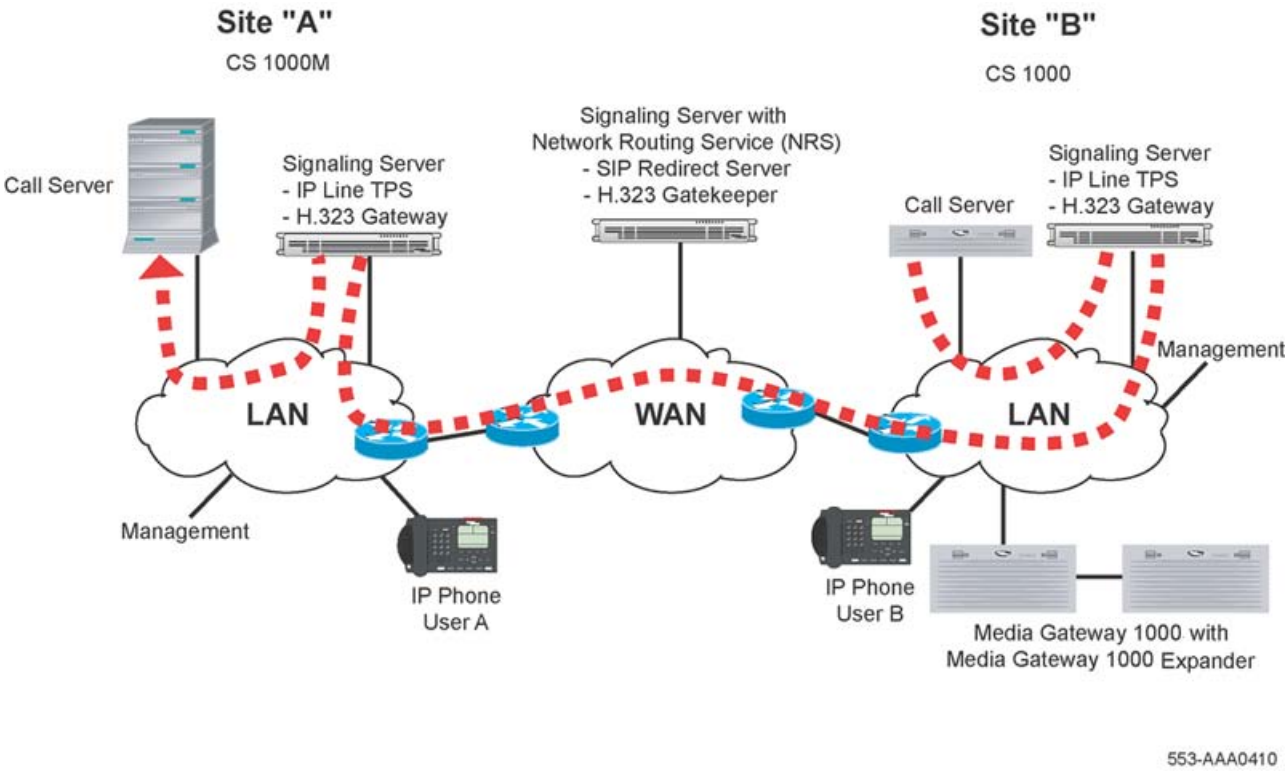

Figure 23: Call Server B sends a CONNECT message to Gateway B

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 on page 77.

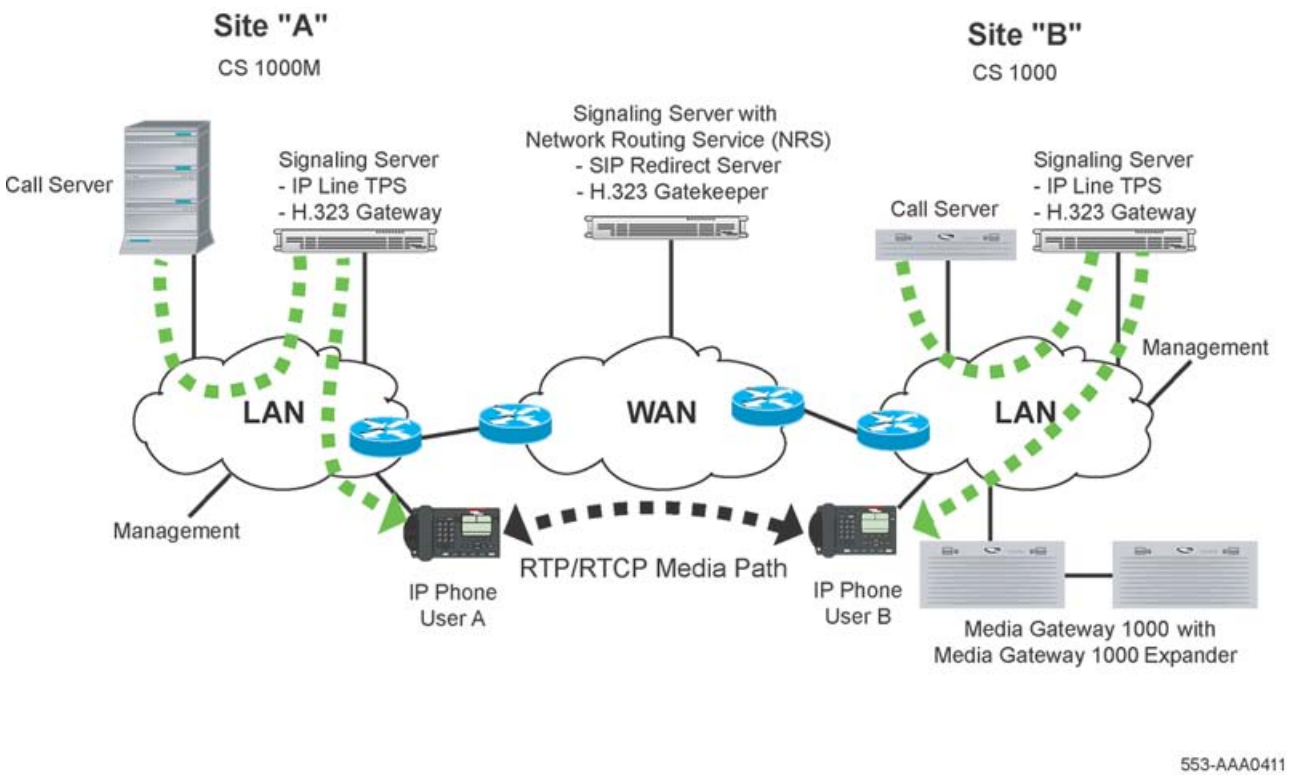

Figure 24: IP Phones start the direct IP media paths

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 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) on page 52.

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.

Chapter 6: H.323-to-SIP signaling

Contents

This section contains information on the following topics:

Introduction

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

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

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

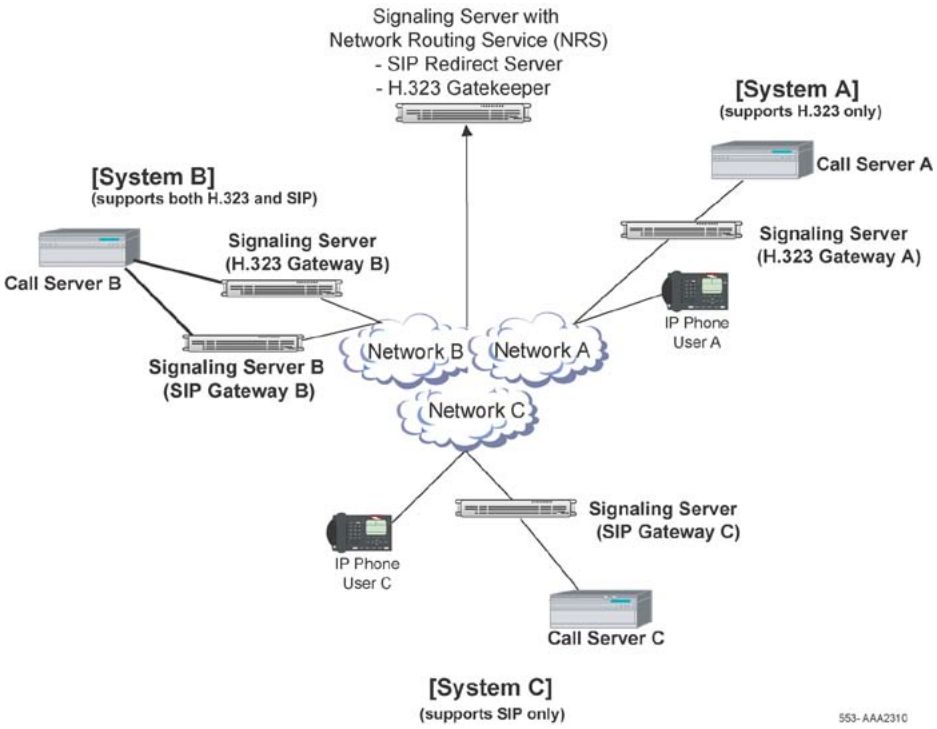

Figure 25: Sample network for H.323-to-SIP call

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 on 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 on page 59 for SIP and Virtual Trunk to Virtual Trunk on page 79 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 on 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 on 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.

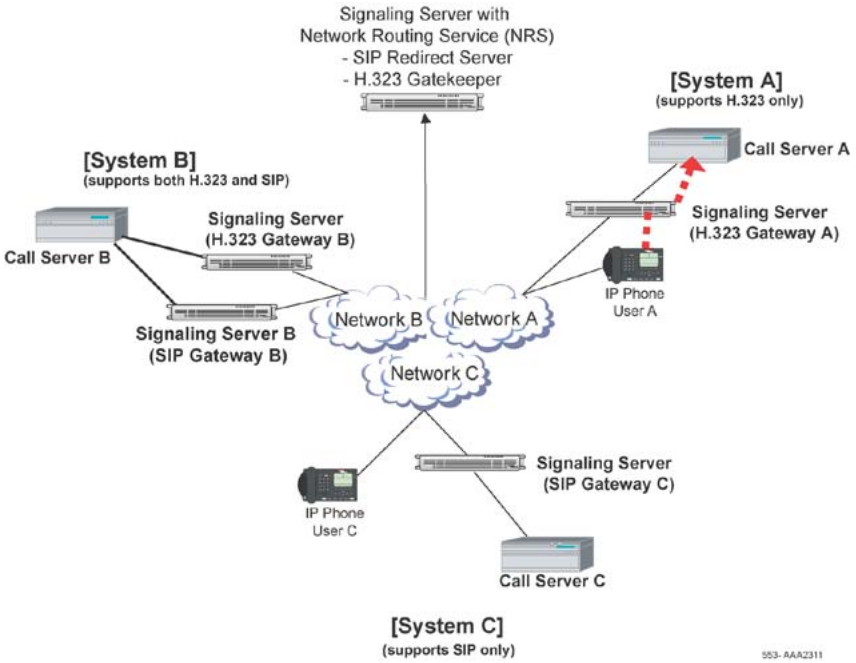

Figure 26: User A dials User C

2. Call Server A determines that the dialed digits are at another site. Call Server A select the codec list, allocates bandwidth, and routes the call to the IP network using a Virtual Trunk and H.323 Gateway A. See Figure 27: Call Server A routes the call to the IP network on page 86.

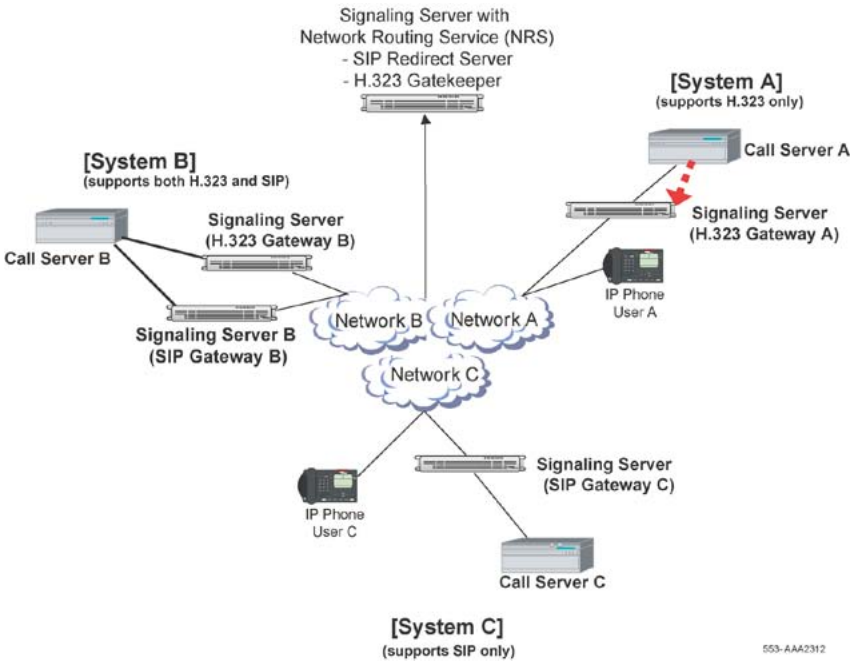

Figure 27: Call Server A routes the call to the IP network

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) on page 87.

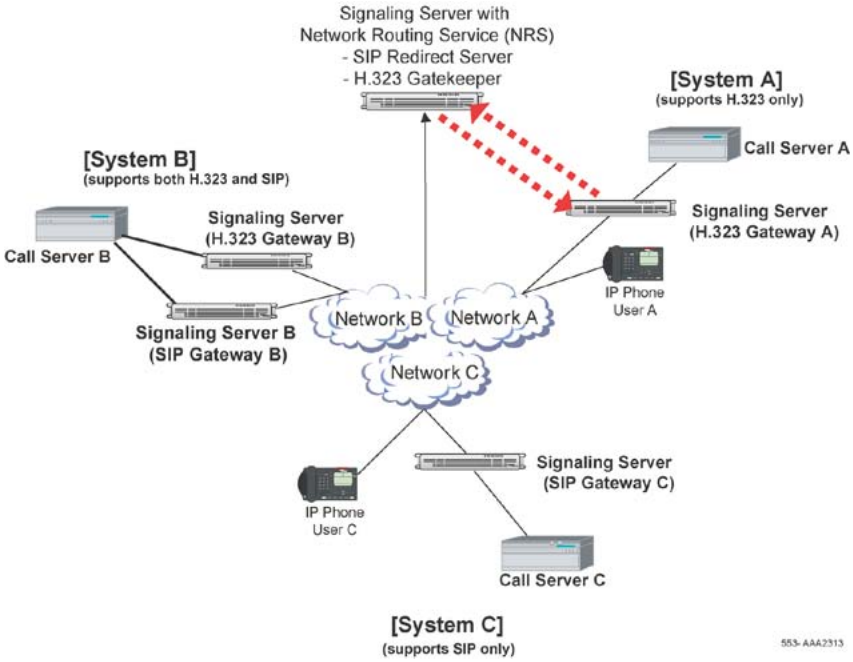

Figure 28: H.323 Gateway A communicates with the NRS (H.323 Gatekeeper)

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 on page 88.

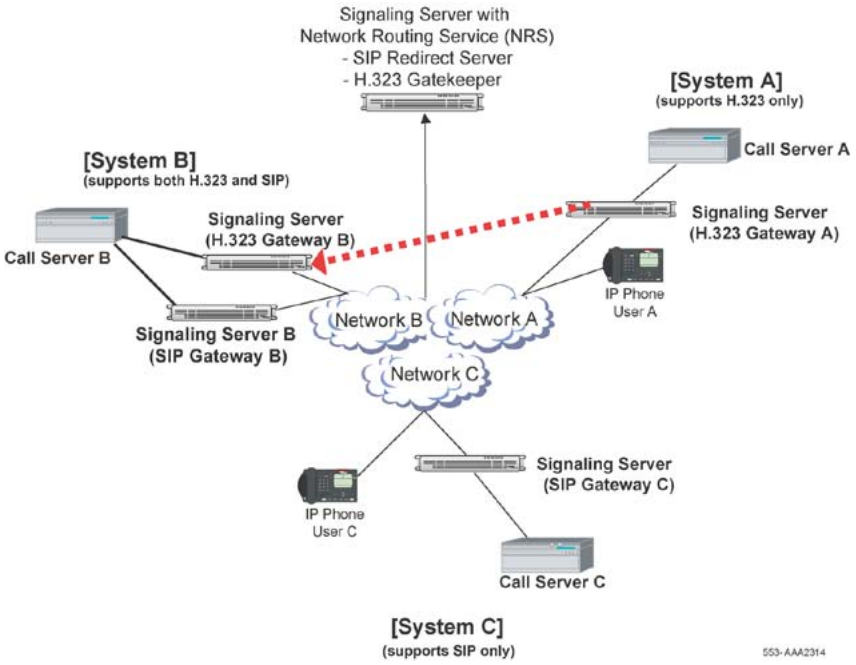

Figure 29: H.323 Gateway A sends information to H.323 Gateway B

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 on page 88.

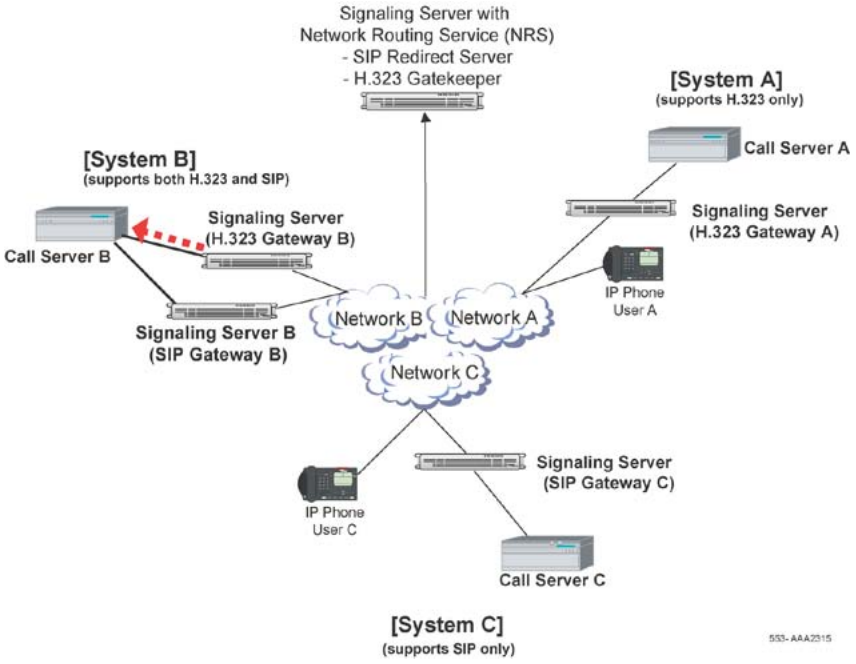

Figure 30: H.323 Gateway B sends calls to Call Server B

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 on page 89.

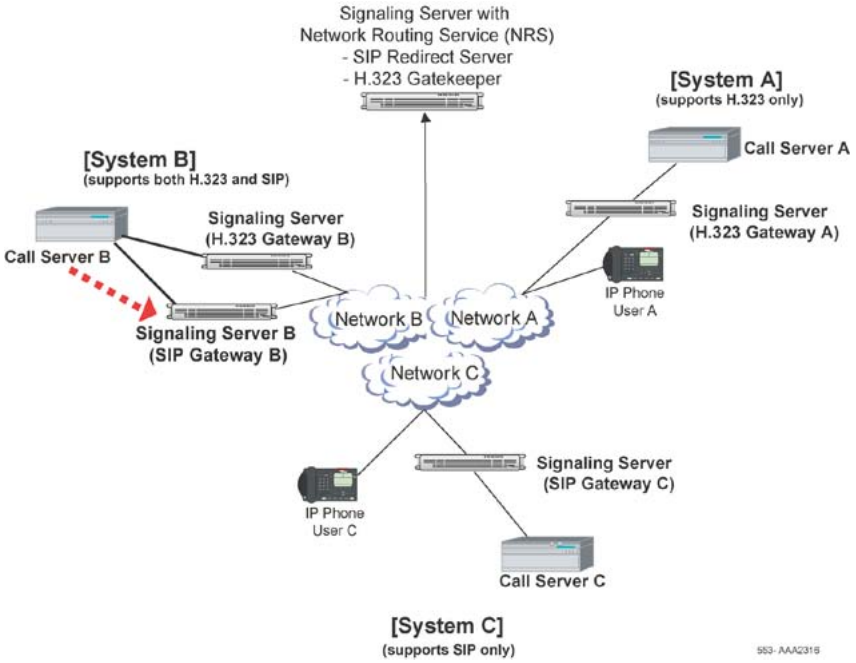

Figure 31: Call Server B sends calls to SIP Trunk Gateway B

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) on page 90.

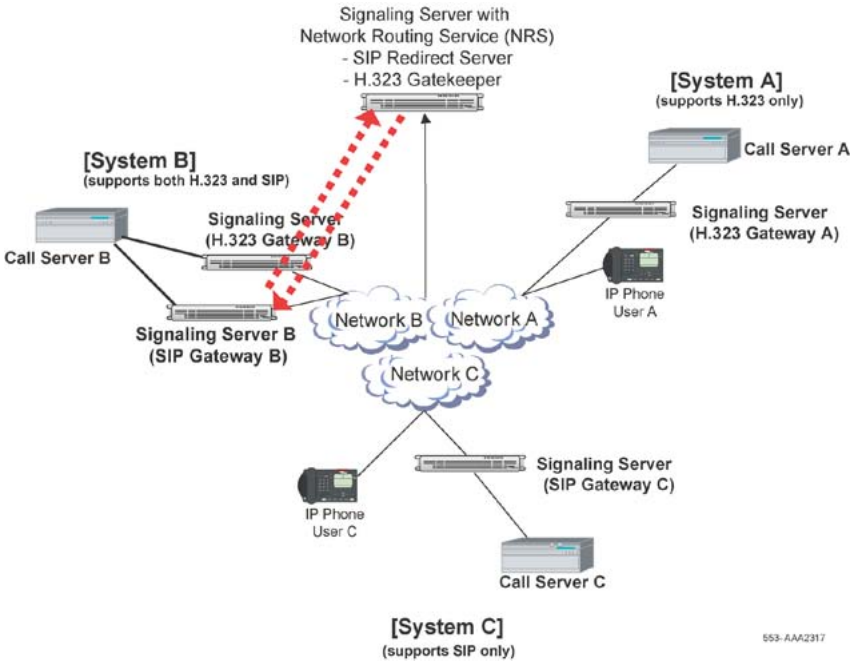

Figure 32: SIP Trunk Gateway B communicates with the NRS (SIP Redirect Server)

8. SIP Trunk Gateway B sends an INVITE message to SIP Trunk Gateway C. See Figure 33: SIP Trunk Gateway B sends INVITE message to SIP Trunk Gateway C on page 90.

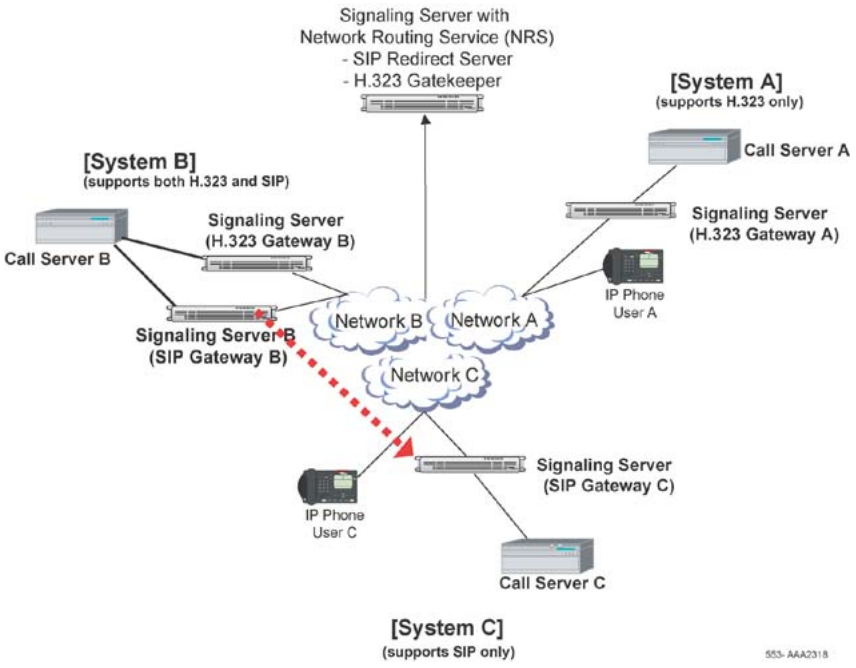

Figure 33: SIP Trunk Gateway B sends INVITE message to SIP Trunk Gateway C

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 on page 91.

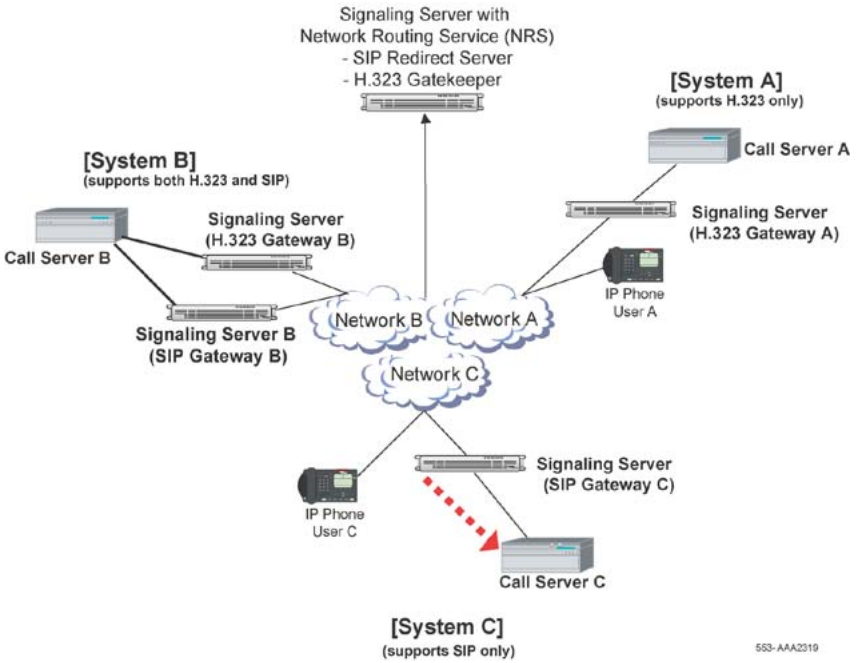

Figure 34: SIP Trunk Gateway C sends call to Call Server C

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 on page 91.

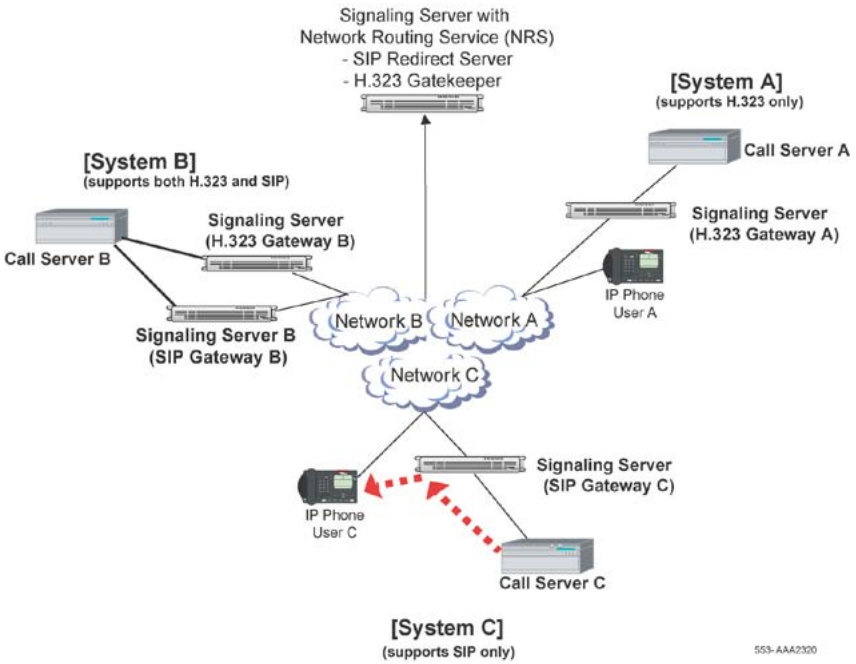

Figure 35: Call Server C sends Alert message to SIP Trunk Gateway C

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 on page 92.

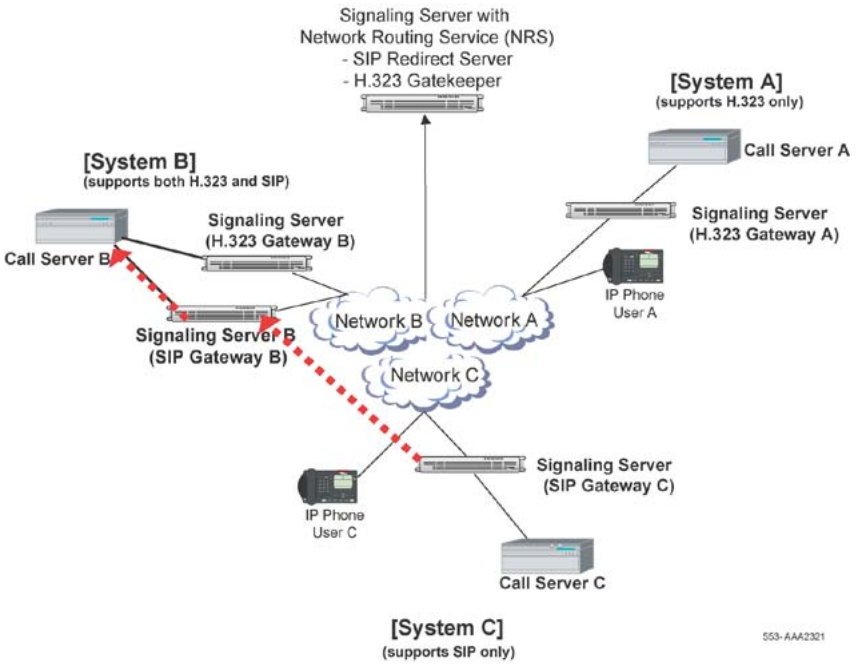

Figure 36: SIP Trunk Gateway B sends ISDN Alert message to Call Server B

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 on page 93.

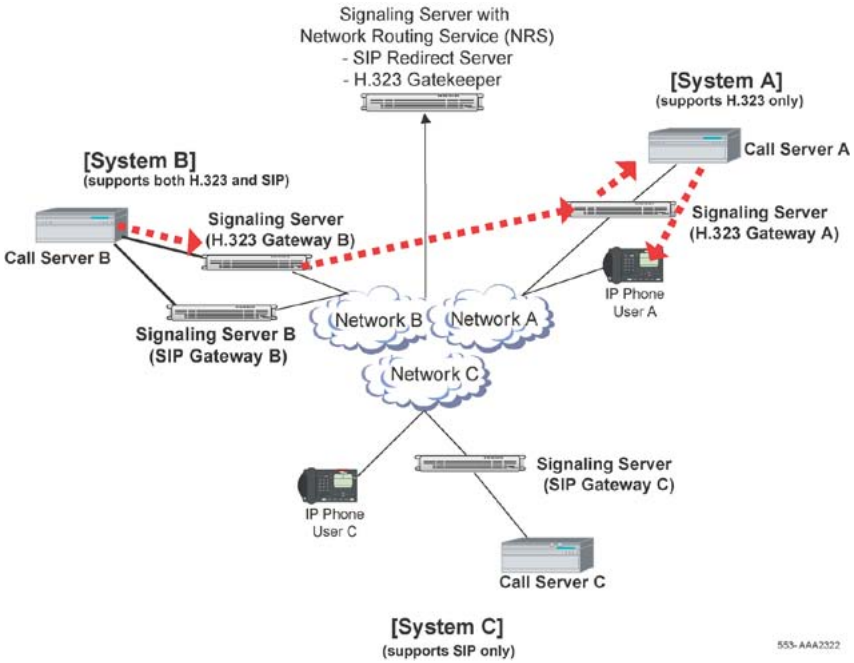

Figure 37: H.323 Gateway B sends Alert message to H.323 Gateway A

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 on page 93.

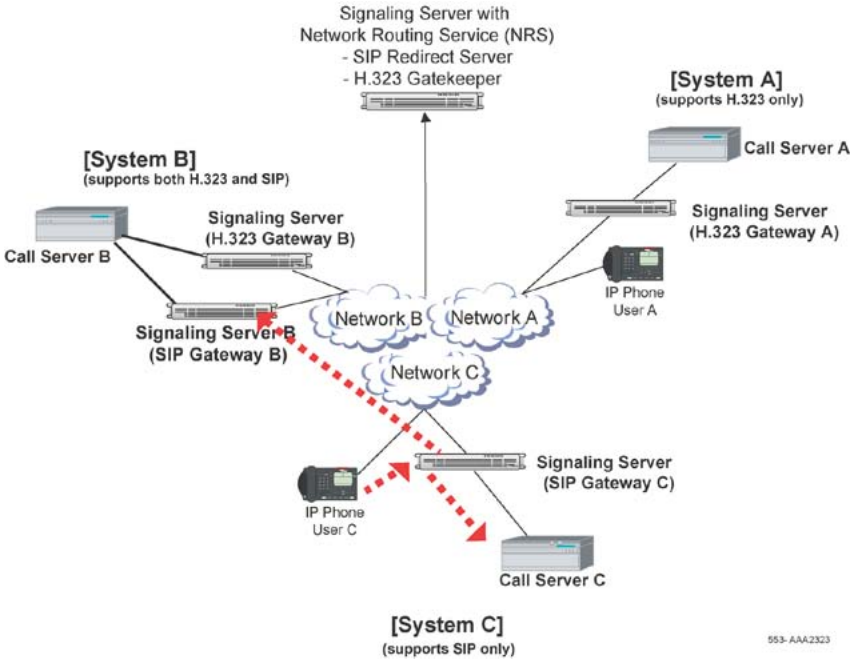

Figure 38: User C answers the call

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 on page 94.

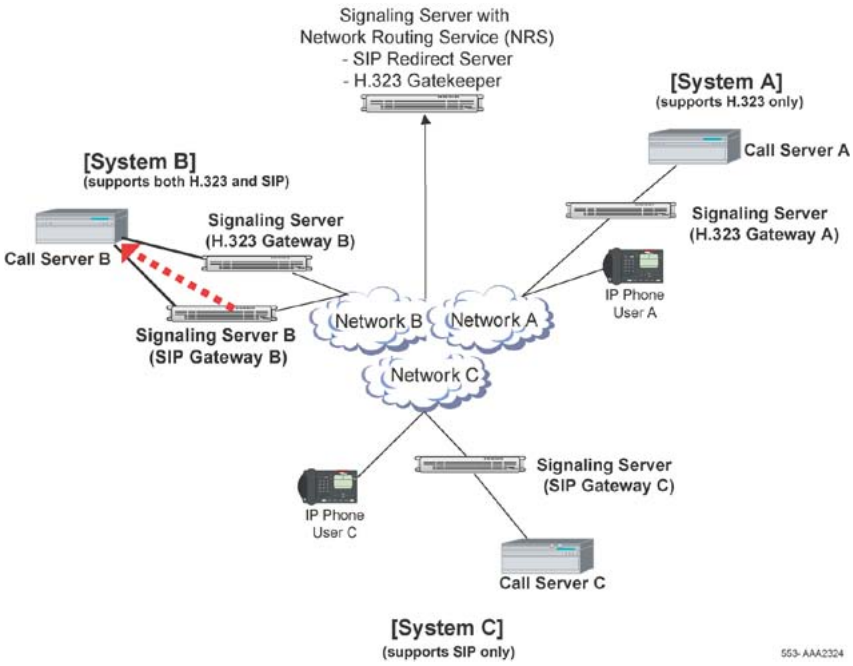

Figure 39: SIP Trunk Gateway B sends message to Call Server B

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 on page 95.

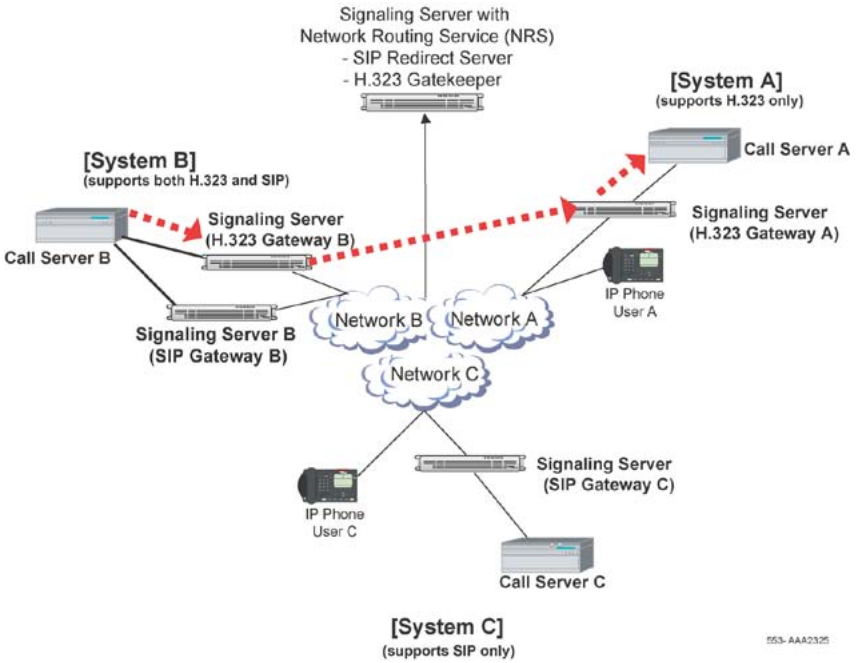

Figure 40: H.323 Gateway B sends message to H.323 Gateway A

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 on page 95.

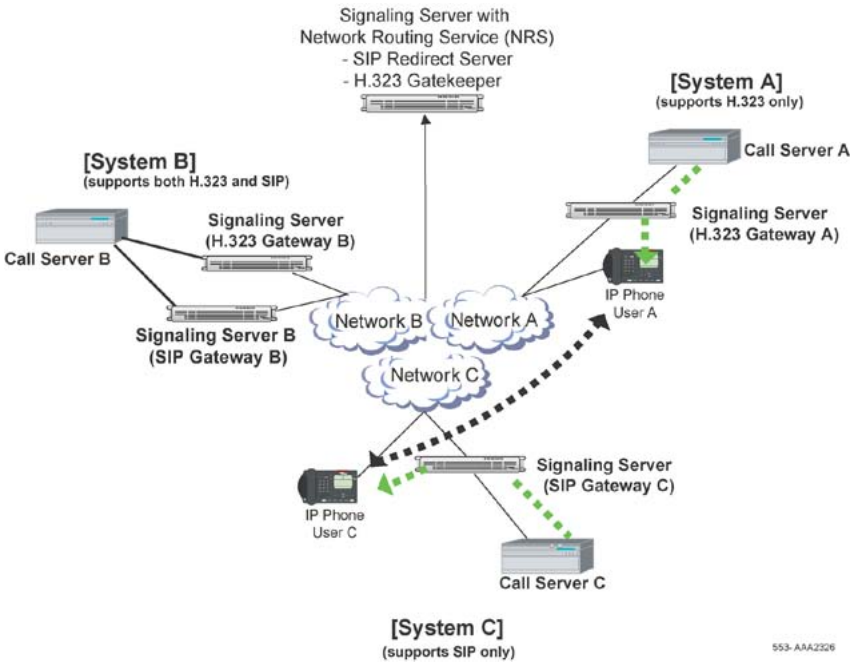

Figure 41: IP Phones start the direct media paths

Chapter 7: Features

Contents

This section contains information on the following topics:

Tone handling

Progress tones

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

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

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

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

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

For call center limitations on tone handling, see the Limitations on page 127.

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.

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 msecs 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 10: Interface commands and responses on page 104.

Table 10: 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 11: Feature packaging requirements on page 104.

Table 11: 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

Package mnemonic	Package number	Package description	Package type (new, existing, or dependency)	Applicable market
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.

Important:
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.

Fax support

The call acts in the same way as a gateway-to-gateway H.323 call. The call is set up using the normal voice call process (that is, the normal voice call codec negotiation process occurs and the corresponding codec payload size and jitter buffer values are used). When the call setup is complete, the two G3 Fax terminals are linked. The DSP detects the fax call setup tones and switches to handle the fax call. For the remainder of the call, the parameters administered for the fax call are used (for example, payload size).

Some implications of the fax call setup process are as follows:

- a voice codec must be configured, even if only fax calls will be made
- both ends of the call must be able to negotiate to a common voice codec for the calls to be successful

Modules supporting facsimile transmission are responsible for the following:

- fax speed detection and adjustment
- protocol conversion from G3 Fax to RTP payload for fax data transfer
- T.30 fax protocol support
- T.38 fax-over-IP protocol
- V.21 channel 2 binary signaling modulation and demodulation
- High-level Data Link Control (HDLC) framing
- V.27 term (2400/4800 bps) high speed data modulation and demodulation
- V.29 (7200/9600 bps) high speed data modulation and demodulation
- V.17 (14390 bps) high speed data modulation
- V.21 channel 2 detection
- Multi-channel operation support

Fax engineering considerations

The fax calculation is based on a 30-byte packet size and a data rate of 64 kbit/s (with no compression) The frame duration (payload) is calculated by using the equation:

30*8/14400=16.6 ms

where 14,400 bit/s is the modem data rate.

Bandwidth output is calculated by the equation:

108*8*1000/16.6=52.0 kbit/sBandwidth output to WAN is:

70*8*1000/16.6=33.7 kbit/s.

Payload and bandwidth output for other packet sizes or modem data rates must be calculated in a similar manner. Fax traffic is always one-way.

Fax pages sent and fax pages received generate data traffic to the TLAN subnet. For WAN calculation, only the larger traffic parcel of the two must be considered.

Trunk Anti-Tromboning (TAT) and Trunk Route Optimization (TRO) considerations

Trunk Anti-Tromboning (TAT) was designed to remove tromboning trunks after a call was answered by a third party. Anti-Tromboning can occur in the following scenarios.

- If a call is re-directed due to call forward or hunt, trunks are torn down after the third party answers.
- Tromboning trunks are removed due to call modification, such as transfer or conference, after the third party answers the call and the call modification is completed.
- For calls entering the private network on CO trunks, the private network trunks being tromboned due to call modification or call redirection are removed.

The removal of trunks in the previous scenarios frees resources that would be otherwise tied up due to tromboning. Therefore, a customer can reduce the call blocking caused by excessive trunk tromboning. This feature works in a PRI, ISL, and VNS network.

TAT validation check that greatly reduces the number of valid anti-tromboning cases for which TAT is blocked. The check works by comparing the H.323 Gateway

Reliability and redundancy

CS 1000 systems provide levels of redundancy to ensure that telephony services can withstand single hardware, software, and network failures. Table 12: Reliability and redundancy features by system type on page 108 shows each reliability and redundancy feature and the systems that support the feature. The reliability and redundancy features include:

- Redundant Call Processor on page 108
- Signaling Server software redundancy on page 110 (including H.323/SIP Trunk Gateway and IP Phone software)
- H.323 Gateway software trunk route redundancy on page 111 (H.323 Gateway interface to Gatekeeper redundancy [Failsafe Gatekeeper])
- SIP Trunk Gateway software trunk route redundancy on page 111
- NRS redundancy on page 112
- Campus-distributed Media Gateway in survival mode on page 116
- CS 1000M Large System CPU redundancy on page 117

Table 12: Reliability and redundancy features by system type on page 108 shows the features and the systems that support the feature.

Table 12: Reliability and redundancy features by system type

Reliability and Redundancy Features		CS 1000M Systems	
	CS 1000E	CS 1000M Single Group	CS 1000M Multi Group
Redundant Call Processor	X	X	X
Signaling Server software redundancy	X	X	X
NRS redundancy	X	X	X
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		

Note:
For CS 1000E redundancy, refer to *Communication Server 1000E: Planning and Engineering* .

Note:
For Geographic Redundancy, refer to *System Redundancy Fundamentals*.

Redundant Call Processor

In a CS 1000E campus environment where Media Gateways are distributed throughout the IP network, all Media Gateways have a full set of call-processing software components and maintain a configuration database that is periodically synchronized with the Call Processor.

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 Processor for feature operation. If the Media Gateway processor loses communication with the Call Processor due to Call Processor or IP network component failure (for example, cabling and L2 switch), one Media Gateway, configured as the Redundant Call Processor, assumes Call Processor responsibilities. The Signaling Server registers with that Redundant Call Processor. Other Media Gateways can access only local Gateway hardware and local non-IP Phones, and are not under the control of the Redundant Call Processor.

The Redundant Call Processor IP address must be in the same ELAN subnet as the Call Processor IP address.

As an example,Figure 42: Example Normal mode of operation for a CS 1000Esystem on page 109 shows the normal mode of operation for a CS 1000E system.

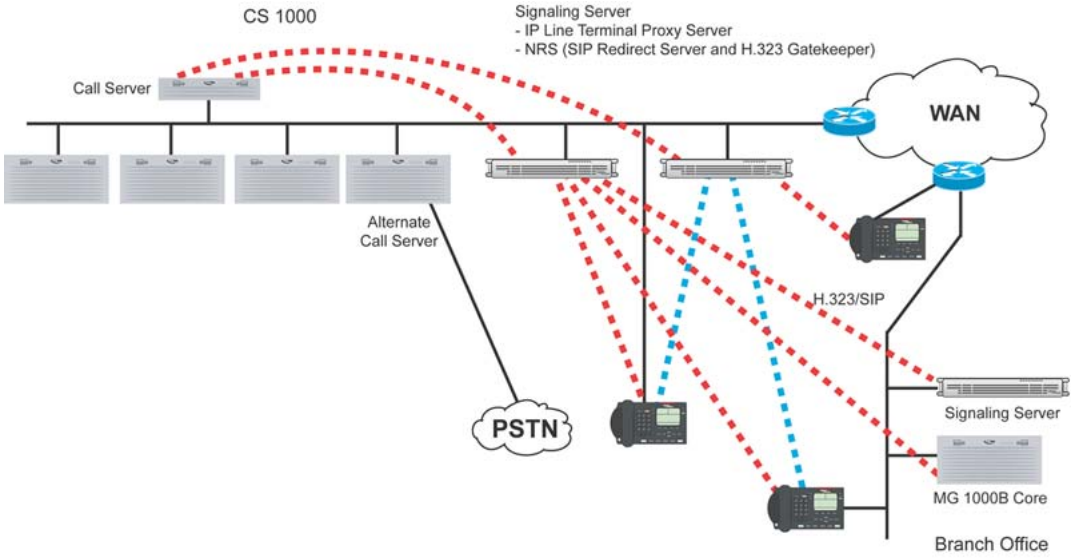

Figure 42: Example Normal mode of operation for a CS 1000Esystem

Figure 43: Call Server failure and redundancy in a CS 1000Esystem on page 110 illustrates what occurs when the Call Processor in a CS 1000E system fails:

1. The Call Processor database periodically synchronizes at the Redundant Call Processor.
2. The Call Processor fails.
3. The Redundant Call Processor assumes the role of Call Processor for IP Phones.
4. The Signaling Server registers at the Redundant Call Processor.
5. Operation resumes with all Media Gateways, but the Signaling Server registers only with the Redundant Call Processor.

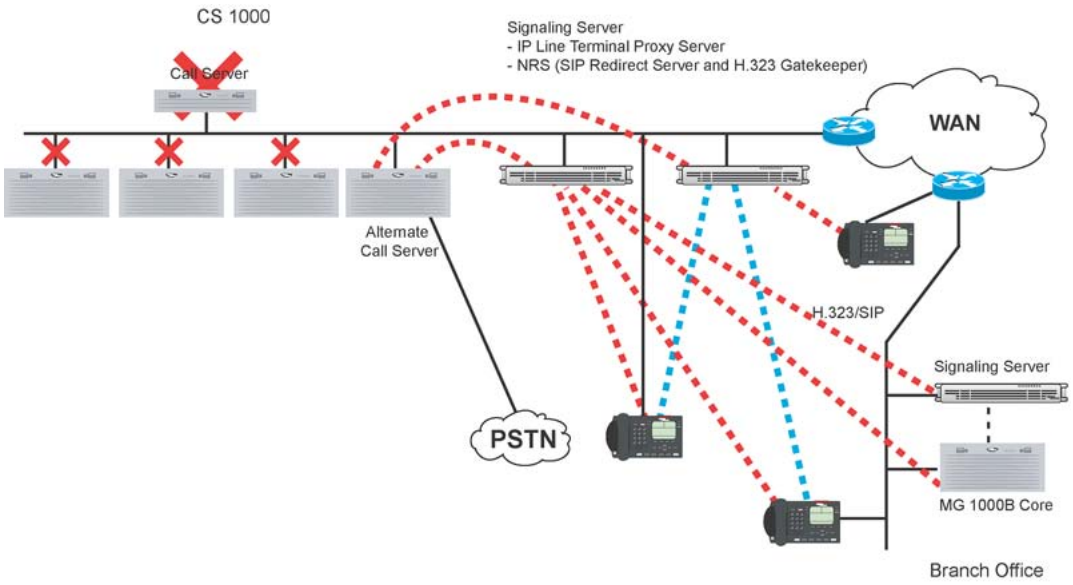

Figure 43: Call Server failure and redundancy in a CS 1000Esystem

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, Secondary, 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 1000E system on page 111 shows Signaling Server redundancy in a CS 1000E system. In the example, the following occurs:

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

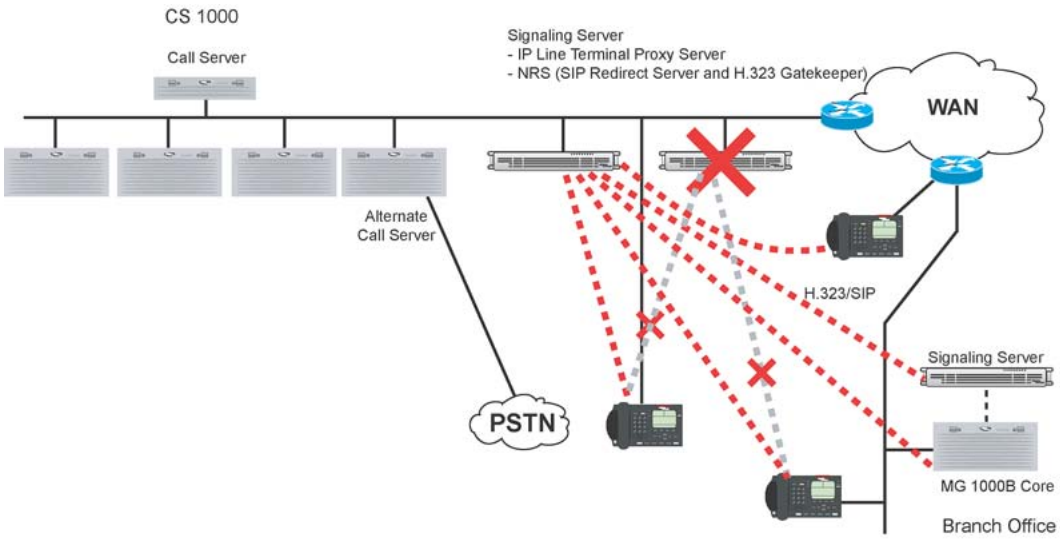

Figure 44: Signaling Server redundancy in a CS 1000E system

H.323 Gateway software trunk route redundancy

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

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

SIP Trunk Gateway software trunk route redundancy

Each Call Processor 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 Secondary 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 Secondary NRS periodically synchronizes its database with the Primary NRS.

Primary, Secondary, 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:

- Secondary NRS
- Failsafe NRS

The Secondary 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 on page 115.

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 on page 114 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.

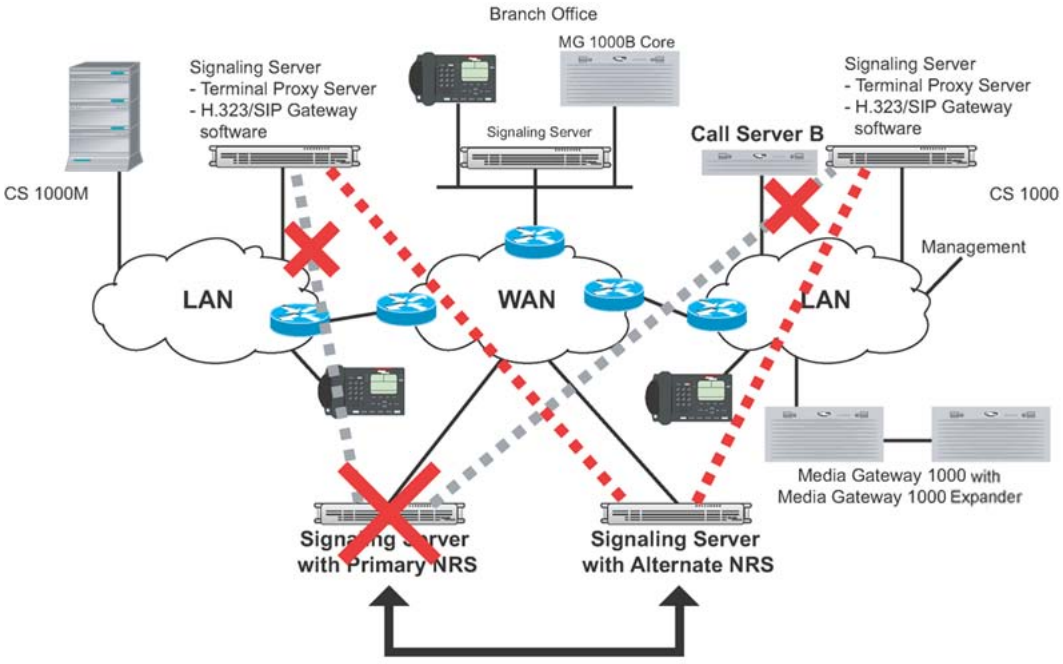

Figure 45: Primary NRS failure and redundancy

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 Redundant Call Processor, 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 on page 117 illustrates how such an outage is handled.

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

1. The Call Processor database periodically synchronizes at the campus-distributed Media Gateway.
2. The Primary Call Processor fails.
3. The campus-distributed Media Gateway assumes the role of the Primary Call Processor for IP Phones.
4. The Signaling Server registers at the campus-distributed Media Gateway.
5. Operation resumes with the single Media Gateway.

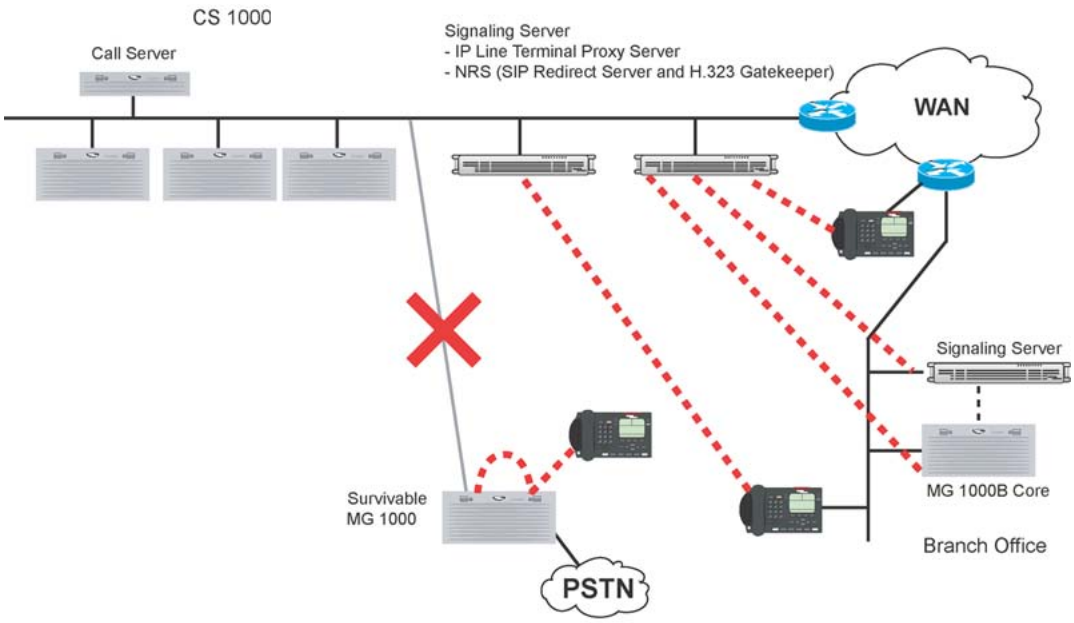

Figure 46: Network failure with Survivable Media Gateways

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 Processor. IP Peer Networking supports the following Large System redundancy features:

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

Health Monitoring

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

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

Table 13: Health count on page 118 shows the health count scheme.

Table 13: 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 on page 118 illustrates health monitoring under normal operation.

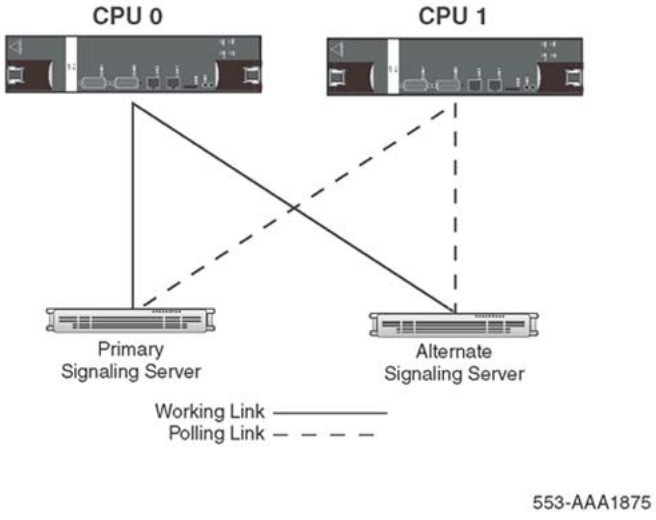

Figure 47: Health Monitoring

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.

When multiple gateway route entries are available for a given number, the gateway route with least cost value is preferred over other gateways. To ensure that gateways are not overloaded with calls, proper planning and engineering must be considered when assigning cost values and routing calls to gateways.

Multi-node configuration

The following example explains a possible configuration between two Meridian 1/CS 1000M switches to achieve both resiliency into the IP network and load balancing.

Meridian 1/CS 1000M switch A has two Virtual Trunk nodes, A1 and A2, for the destination NPA 613. A Route List Block (RLB) is created, in order to have two route entries (one for each). If the trunks of node A1 are all in use or node A1 is down, call traffic is routed to node A2. This provides resiliency by preventing failure of a single Virtual Trunk (for example, DCH failure or Leader subnet fails) from completely eliminating VoIP service.

It is desirable to distribute calls to multiple nodes at a remote destination. The configuration of multiple dialing plan entries at the local Virtual Trunk node allows routing based on the dialed digits.

For example, switch B node B1 has two entries for NPA 408 and 4085, which point to nodes A1 and A2 of switch A, respectively. Calls from B1 with dialed digits 408-5xx-xxxx are routed to the Virtual Trunk node A1 while all other 408-xxx-xxxx calls are routed to Virtual Trunk node A2.

Flexible Numbering Plan

A Flexible Numbering Plan (FNP) allows the length of Location Codes (LOCs) to vary from node to node. As well, the total number of digits dialed to reach a station can vary from station to station. It also allows flexibility for the length of the location codes from node to node.

An FNP can be used to support country-specific dialing plans. FNP also allows users to dial numbers of varying lengths to terminate at a destination. Flexibility of the number of digits which can be dialed is achieved using Special Numbers (SPNs).

Electronic Switched Network (ESN5) network signaling

Virtual Trunk 2.x support a mixed network of remote nodes with ESN5 and standard (that is, non-network) signaling. ESN5 is an extension of MCDN signaling which can be used by Virtual Trunk 2.x and IP Peer (CS 1000M).

ESN5 inserts the Network Class of Service (NCOS) prefix ahead of the dialed numbers. Make sure that, if ESN5 is to be used, it is provisioned on both the Virtual Trunk and the Route Data Block (RDB) for that node. If ESN5 is provisioned, all remote Virtual Trunk 2.x must have that node provisioned as "SL1ESN5" in the dialing plan. If this is not done, a default NCOS is inserted by the ESN5 node receiving the call from the non-ESN5 VoIP gateway.

Quality of Service

Quality of Service (QoS) is the gauge of quality of the IP network between two nodes. As QoS degrades, existing calls suffer from poor voice and fax quality. New calls will not be initiated if transmissions degrade below an acceptable level.

Behavioral characteristics of the IP network depend on the following:

- Round Trip Time (RTT)
- latency
- queuing delay in the intermediate nodes
- packet loss
- available bandwidth

The Type of Service (ToS) bits in the IP packet header can affect how efficiently data is routed through the network.

Packet jitter related to latency affects the quality of real-time IP transmissions. For good voice quality, the Virtual Trunk reassembles the voice packets in an ordered continuous speech stream and plays them out at regular intervals despite varying packet arrival times.

QoS is measured for each remote gateway. For example, if a given Leader has three remote leaders in its dialing plan table, it performs three QoS measurements and calculations (one per remote gateway).

Since IP trunks use the same port for both voice and fax, the same QoS thresholds apply for both voice and fax calls. Network requirements for fax are more stringent than for voice. Fax protocols, such as T.30, are more sensitive to transmission errors than the human ear.

Quality of Service parameters

Quality of Service for both voice and fax depends on end-to-end network performance and available bandwidth. A number of parameters determine the Virtual Trunk voice QoS over the data network.

Packet loss

Packet loss is the percentage of packets sent that do not arrive at their destination. Packet loss is caused by transmission equipment problems and congestion. Packet loss can also occur when packet delays exceed configured limits and the packets are discarded. In a voice

conversation, packet loss is heard as gaps in the conversation. Some packet loss, less than five percent, can be acceptable without too much degradation in voice quality. Sporadic loss of small packets can be more acceptable than infrequent loss of large packets.

Packet delay

Packet delay is the time between when a packet is sent and when it is received. The total packet delay time consists of fixed and variable delay. Variable delay is more manageable than fixed delay, is dependent on network technology. Variable delay is caused by the network routing of packets. The Virtual Trunk node must be as close as possible to the network backbone (WAN) with a minimum number of hops, in order to minimize packet delay and increase voice quality. Virtual Trunk provides echo cancellation, so that a one-way delay up to 200 milliseconds is acceptable.

Delay variation (jitter)

The amount of variation in packet delay is referred to as delay variation or jitter. Jitter affects the ability of the receiving Virtual Trunk to assemble voice packets into a continuous stream when the packets are received at irregular intervals.

Latency

Latency is the amount of time it takes for a discrete event to occur.

Bandwidth

Bandwidth is a measure of information carrying capacity available for a transmission medium. The greater the bandwidth the more information that can be sent in a given amount of time. Bandwidth is expressed in bits per second (bps).

Network performance utilities

Two common network performance utilities, Packet InterNet Groper (PING) and Traceroute, are described in this section. Other utilities can be used to gather information about Virtual Trunk network performance.

Network conditions can vary over time, collect performance data over a period of at least four hours. Use performance utilities to measure network performance from each Virtual Trunk node in the network.

Packet InterNet Groper (PING)

Packet InterNet Groper (PING) sends an Internet Control Message Protocol (ICMP) echo request message to a host, expecting an ICMP echo reply. This allows the measurement of the round-trip time to a selected host. By sending repeated ICMP echo request messages, the percentage of packet loss for a route can be measured.

Traceroute

Traceroute uses the IP Time-To-Live (TTL) field to forward router hops to a specific IP address. A router must not forward an IP packet with a TTL field of 0 or 1. It must, instead, discard the packet and return an ICMP "time exceeded" message to the originating IP address. Traceroute uses this mechanism by sending an IP datagram with a TTL of 1 to the specified destination host. The first router to handle the datagram returns a "time exceeded" message. This identifies the first router on the route. Traceroute sends out a datagram with a TTL of 2. This causes the second router on the route to return a "time exceeded" message, and so on, until all hops have been identified. The Traceroute IP datagram has a port number unlikely to be in use at the destination (usually >30,000). This causes the destination to return a "port unreachable" ICMP packet which identifies the destination host. Traceroute can be used to measure round-trip times to all hops along a route, identifying bottlenecks in the network.

E-Model

E-Model, a method similar to the ITU-T Recommendation G.107, to determine voice quality. This model evaluates the end-to-end network transmission performance and outputs a scalar rating, R, for the network transmission quality. Virtual Trunk uses a simplified version of the model to correlate the network QoS to the subjective Mean Opinion Score (MOS).

MOS is a numerical scale used to rate voice quality. When MOS is equal to 5.0, voice quality is good. When MOS is equal to 0.0, voice quality is bad.

For packet loss over 16%, the MOS value is set to 0, and the remote node is considered to be in fallback mode.

End-to-end latency

Virtual Trunk network end-to-end latency consists of several components: routing delay on the Virtual Trunk network, frame duration delay and jitter buffer delay on the codec, and delay on the circuit-switched network. The determination of end-to-end delay depends on the dynamics of the Virtual Trunk network and the detailed service specification.

MOS values are calculated based on the routing delay and frame duration and jitter buffer delay on the codec. These latencies must be taken into consideration during the engineering of the total network’s latency. If the end-to-end latency of the network is specified and the latency of the PSTN circuit-switched components is removed, the remainder is the latency

available for the IP trunks. This latency value plays a large role when configuring Virtual Trunk node QoS values.

For instance, assume the end-to-end network latency is 300 milliseconds (ms) and the part of that latency which the IP network contributes is 180 ms. Furthermore, assume the network has low packet loss. Using the G.711 codec, this means the configured QoS can be a minimum of 4.3. If the latency in the IP network increases, the configured QoS is not met and fallback to alternate facilities occurs.

Equipment Impairment factor

Equipment Impairment factors are important parameters used for transmission planning purposes. They are applicable for the E-Model.

Set QoS expectations

Figure 48: QoS levels with G.729A/AB codec on page 125, Figure 49: QoS level with G.711 codec on page 125, and Figure 50: QoS level with G.723 codec on page 126 show the operating regions in terms of one-way delay and packet loss for each codec and required QoS level as determined by Virtual Trunk. Note that among the codecs, G.711(A-law)/G.711(u-law) delivers the best quality for a given intranet QoS, followed by G.729AB and then G.723.1 (6.4 kbp/s) and lastly G.723.1 (5.3 kbp/s). These figures determine the delay and error budget for the underlying intranet in order for it to deliver a required quality of voice service.

Fax is more susceptible to packet loss than the human ear is; quality starts to degrade when packet loss exceeds 4%. Nortel recommends that fax services be supported with Virtual Trunk operating in either the Excellent or Good QoS level. Avoid offering fax services between two sites that can guarantee no better than a Fair or Poor QoS level.

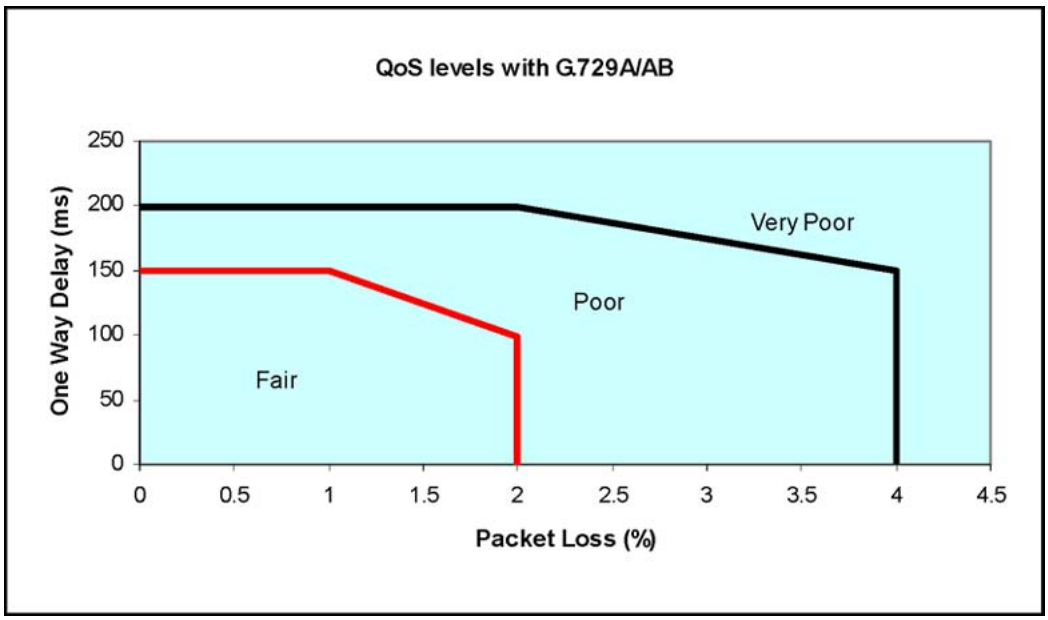

Figure 48: QoS levels with G.729A/AB codec

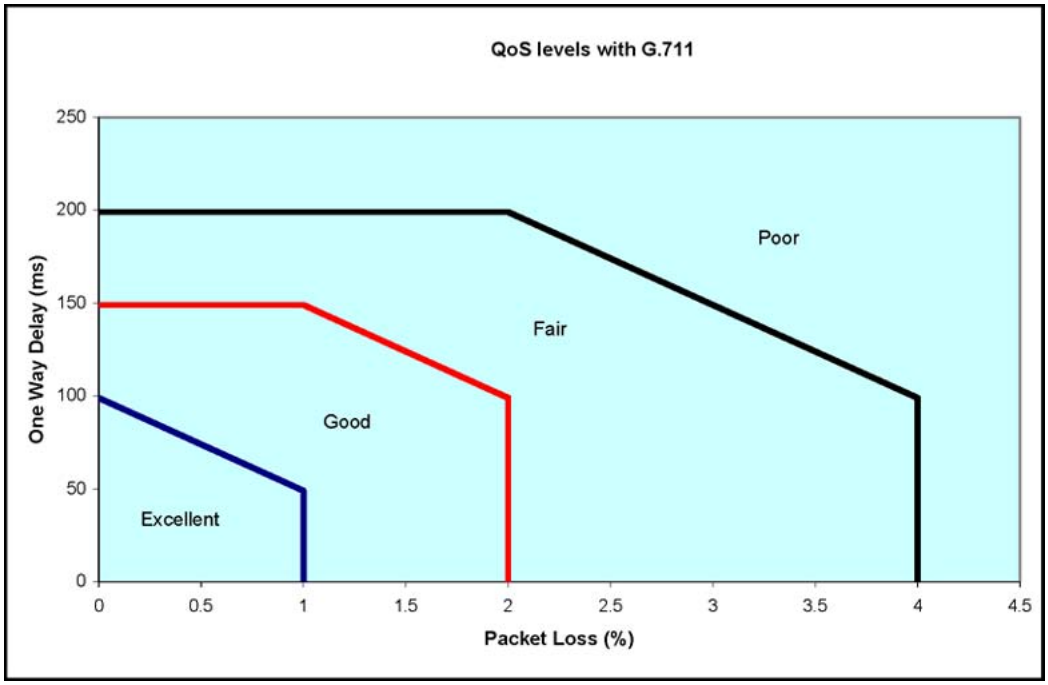

Figure 49: QoS level with G.711 codec

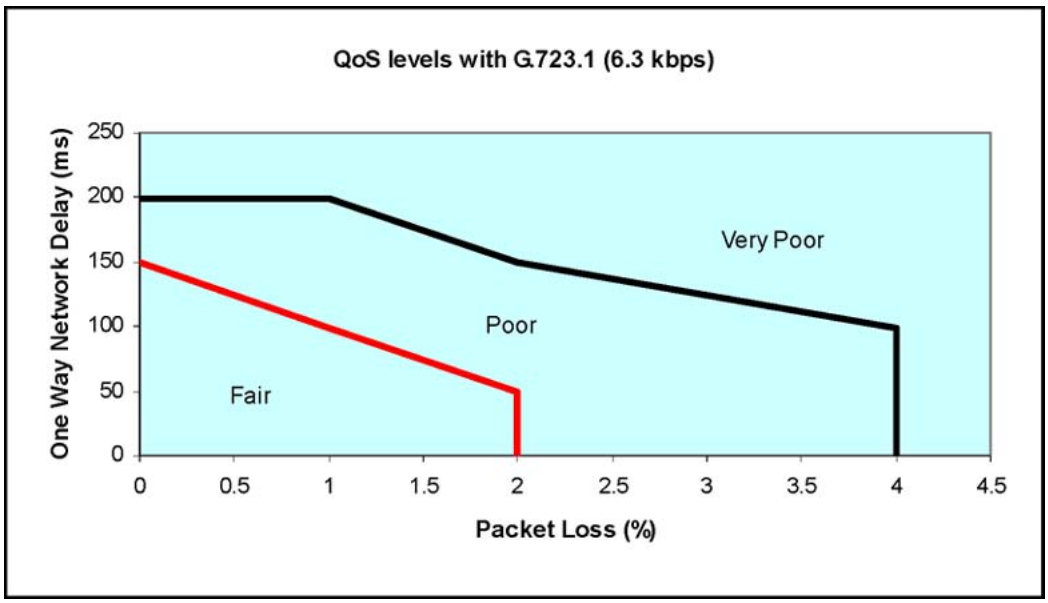

Figure 50: QoS level with G.723 codec

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, Secondary, 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 use of the bandwidth intensive G.723 codec can limit the number of DSP channels available. The use of codec G.729A/AB and G.723 impacts the voice quality, including music provided to the user.

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

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

Chapter 8: Configure IP Peer Network

Contents

This section contains information on the following topics:

Overview

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

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

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 Fundamentals (NN43001-130)*.

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:
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.

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 IP Line Applications Fundamentals (NN43001-125)*
3. Configure the Primary, Secondary, and Failsafe NRS at installation and initial setup of the Signaling Server. See *Signaling Server IP Line Applications Fundamentals (NN43001-125)* .

    Note:
    The NRS requires IP telephony node configuration files. These files are installed and configured during the Signaling Server software installation (basic configuration step).
4. Configure the Customer Data Block with any desired networking settings and options, including ISDN. Use Element Manager or the Command Line Interface (LD 15). See Configuring the Customer Data Block on page 135 and Feature Implementation of IP Peer Networking on page 171.
5. Configure the D-channel using Element Manager or the Command Line Interface (LD 17). See Configuring D-channels on page 138 and Feature Implementation of IP Peer Networking on page 171.
6. Configure the zones.
7. Configure the SIP and/or H.323 Virtual Trunk routes using Element Manager or the Command Line Interface (LD 16). Configure the Route Data Blocks and associate the Virtual Trunk routes with the IP network by configuring the following parameters:

a. route information
b. network management information (for example, Access Restrictions)
c. bandwidth zone
d. protocol identifier
e. associated Node ID

For the Element Manager procedure, see Configuring the Virtual routes and trunks on page 141. For the CLI procedure, see Feature Implementation of IP Peer Networking on page 171.

8. Configure the Virtual Trunks using Element Manager (see Configuring the Virtual routes and trunks on page 141) or the Command Line Interface (LD 14) and Feature Implementation of IP Peer Networking on page 171.
9. Use Element Manager or the Command Line Interface (CLI) to configure networking (Configuring networking on page 148) and numbering plan features (Configuring call routing on 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.
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)* .
12. Configure the gateways. See Configuring the Gateways on page 189.
    • See Enabling and configuring the H.323 Gateway on page 189
    • Enabling and configuring the SIP Trunk Gateway on page 193
13. Configure the NRS.

Launching Element Manager

Element Manager (EM) for Communication Server 1000 Release 7.0 is a component of the Nortel Unified Communications Management Common Services (UCM Common Services). The UCM Common Services provides security and navigation infrastructure services for the web-based management applications: Element Manager (EM), NRS Manager and Subscriber

Manager. Refer to *Unified Communications Management (NN43001-116)* for detailed information on UCM Common Services.

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

Log in to UCM Common Services and Access Element Manager

To log in to EM follow the steps in Logging in to UCM Common Services and Accessing Element Manager on page 133.

Logging in to UCM Common Services and Accessing Element Manager

1. In the browser's address field, enter the Fully Qualified Domain Name (FQDN) of an UCM Common Services server that is a member of the Security Domain that the EM server is a member of.

   Note:
   The FQDN of the ECM server can be bookmarked in the Internet Explorer Favorites list.

   The Security Alert Web page opens, as shown in Figure 51: Security Alert Web page on page 133.

Figure 51: Security Alert Web page

2. Click the **Yes** button. The UCM log in Web page opens, as shown in Figure 52: UCM log in Web page on page 134.

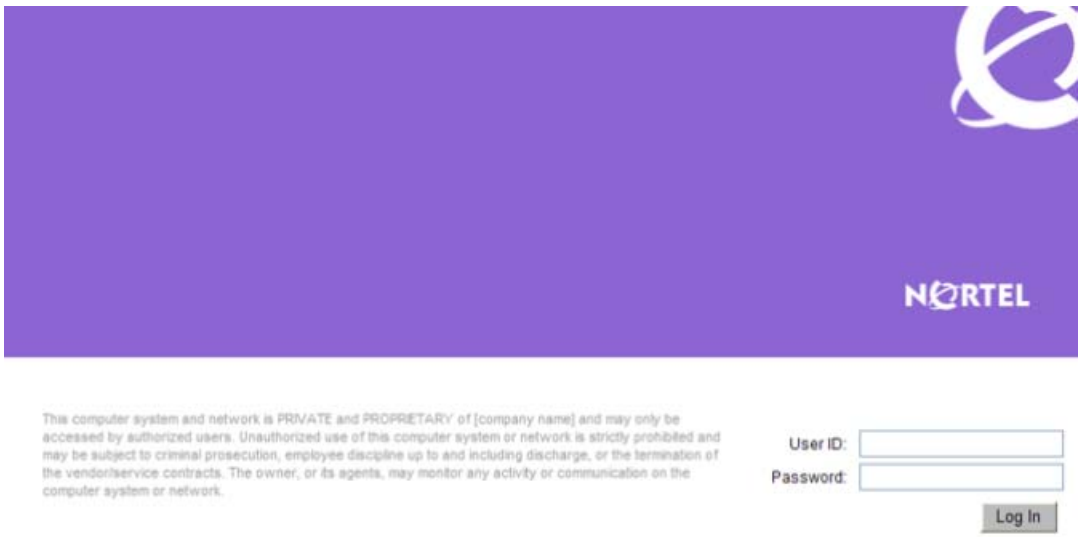

Figure 52: UCM log in Web page

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

   The UCM Elements Web page opens, as shown in Figure 53: UCM Elements Web page on page 134.

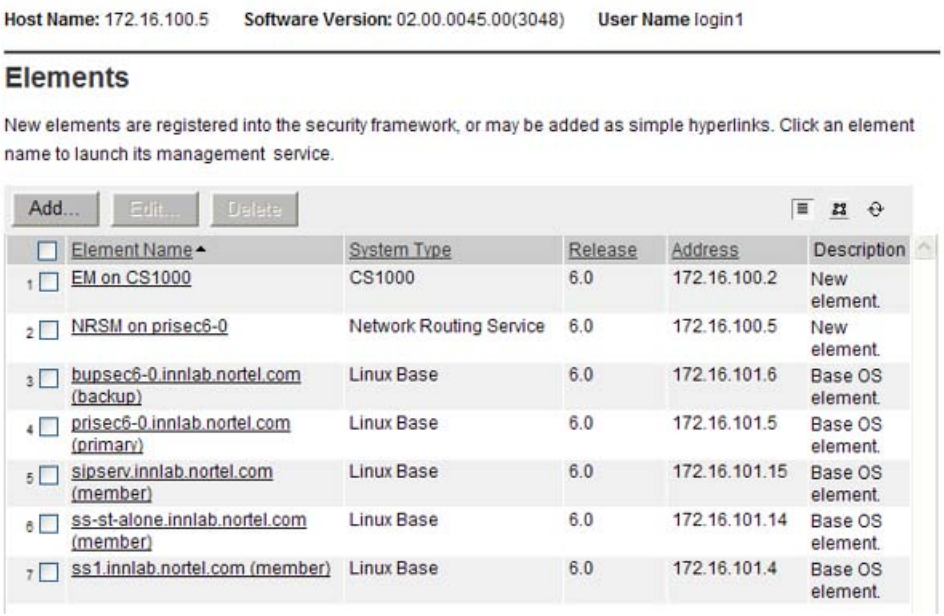

Figure 53: UCM Elements Web page

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 54: Element Manager System Overview Web page on page 135.

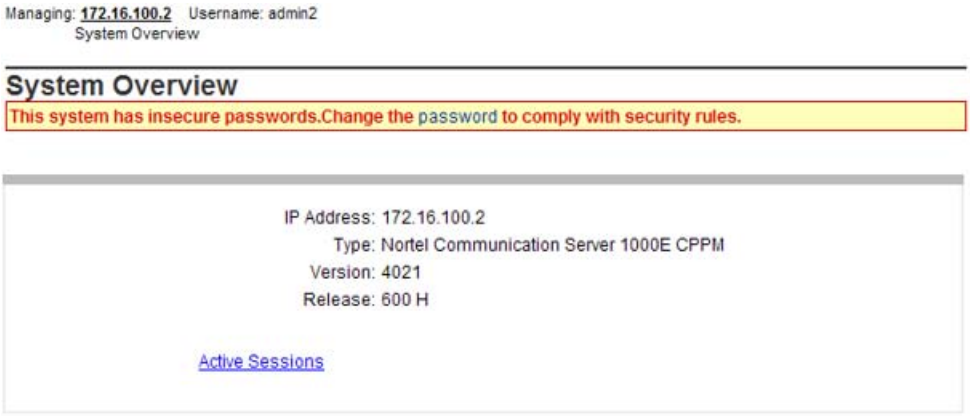

Figure 54: Element Manager System Overview Web page

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 Configuring the Customer Data Block and enabling ISDN on page 135.

Configuring the Customer Data Block and enabling ISDN

To configure the Customer Data Block with network settings and options, you can use Element Manager or LD 15 of the Command Line Interface.

1. Click **Customers** in the EM Navigator.

   The Customers Web page opens, as shown in Figure 55: Customers Web page on page 136.

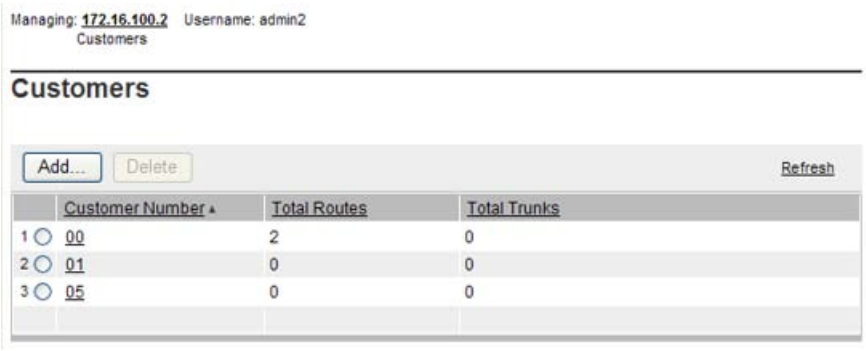

Figure 55: Customers Web page

2. Click a link in the **Customer Number** column. The Edit Web page for Customer number xx opens, as shown in Figure 56: Customer xx Edit Web page on page 136.

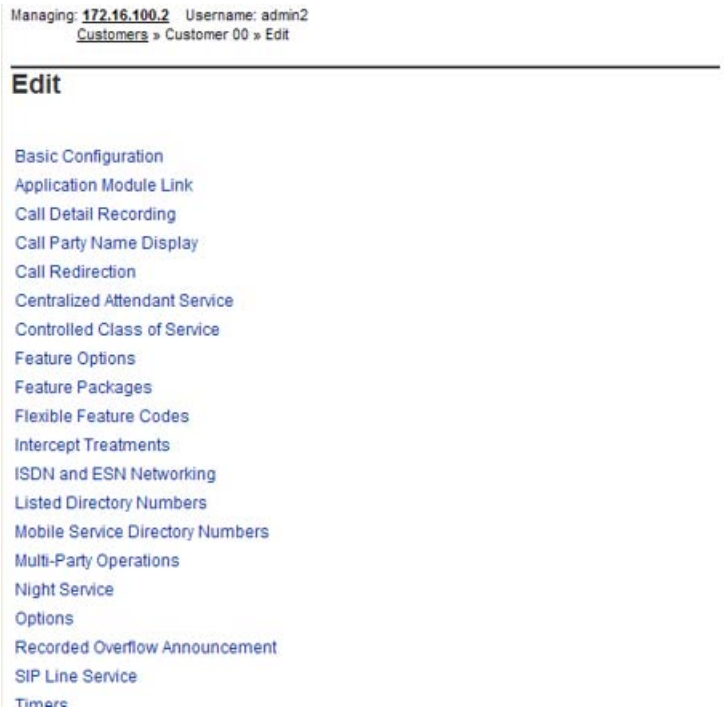

Figure 56: Customer xx Edit Web page

3. Click **Feature Packages**. The Feature Packages Web page opens, as shown in Figure 57: Feature Packages Web page on page 137.

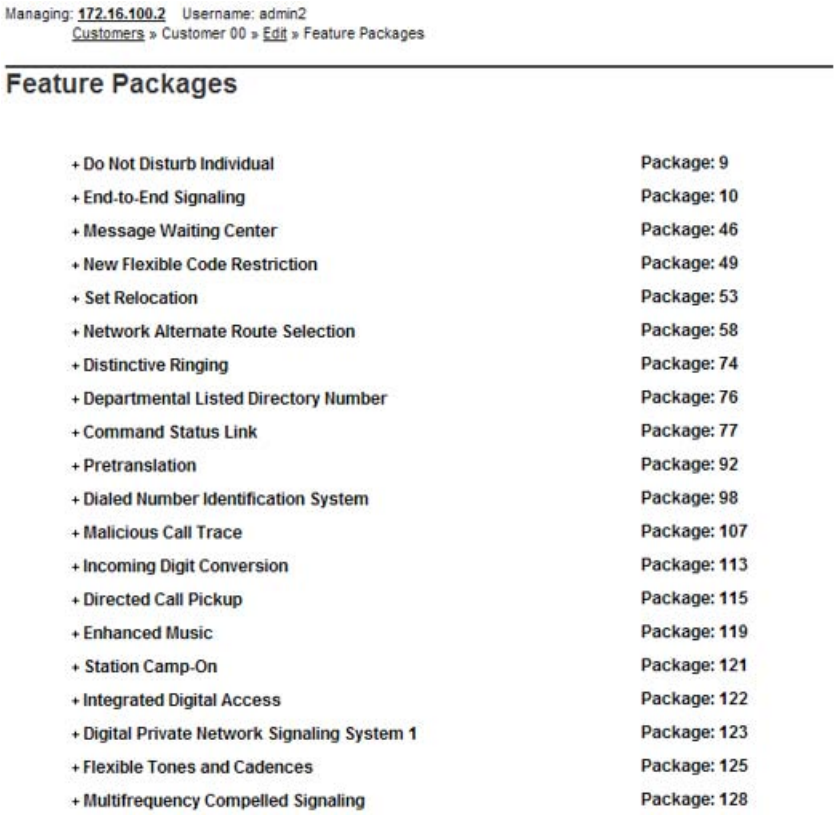

Figure 57: Feature Packages Web page

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:** package options.

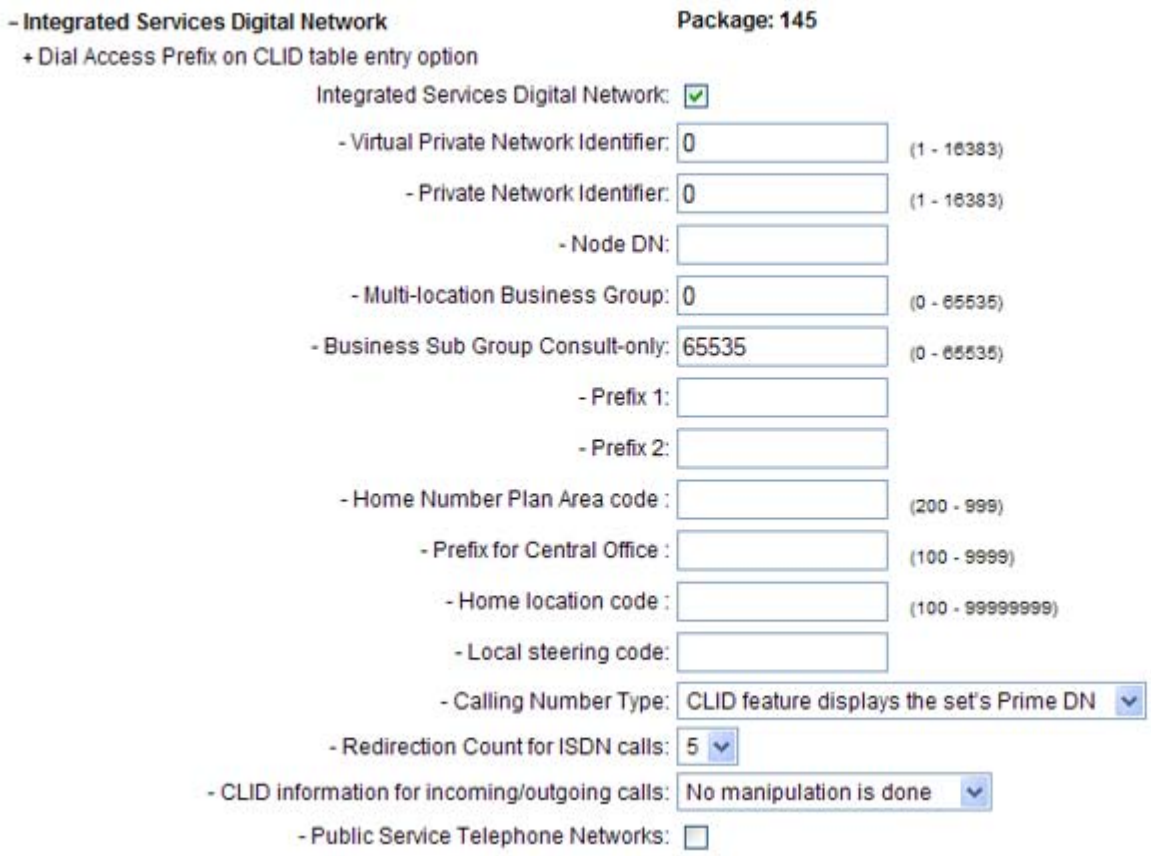

Figure 58: Integrated Services Digital Network Package: 145 Expanded

5. Scroll to the bottom of the page and click **Save**.

Configuring D-channels

Configuring D-channels

To configure D-channels, use Element Manager or LD 17 of the Command Line Interface. Figure 59: D-Channels Web page on page 139 and Figure 60: D-channels xx Property Configuration Web page on page 139 show the D-Channel Configuration Web pages in Element Manager. Use these Web pages to configure D-channels.

1. Select **Routes and Trunks > D-Channels** from the 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 59: D-Channels Web page on page 139. This window also contains links to D-Channel maintenance and diagnostic pages.

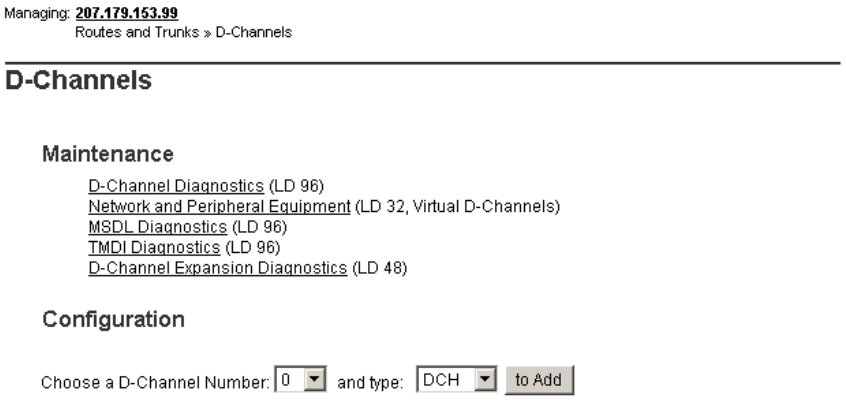

Figure 59: D-Channels Web page

2. In the **Configuration** section, input the D-channel number and type. Click **to Add**.

   The D-Channels xx Property Configuration Web page opens, as shown in Figure 60: D-channels xx Property Configuration Web page on page 139. The D-channel number is denoted by xx. Required fields are indicated with a green asterisk.

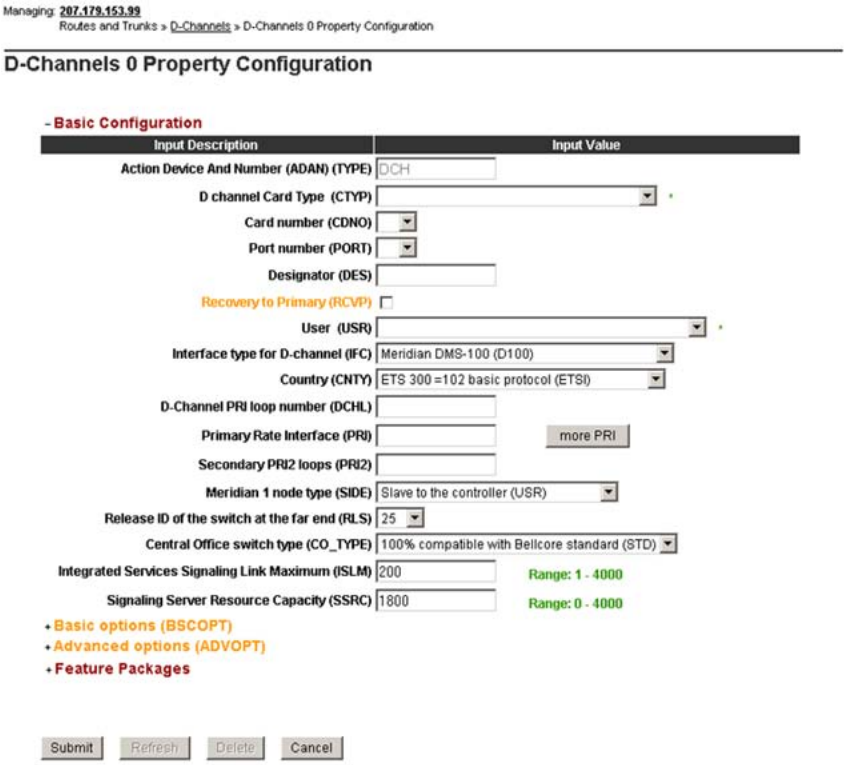

Figure 60: D-channels xx Property Configuration Web page

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 61: D-channel Basic options on page 140.

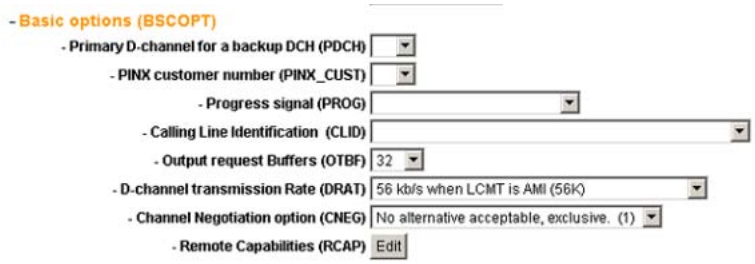

Figure 61: D-channel Basic options

   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 62: D-channel configuration results on page 140) with the changes.

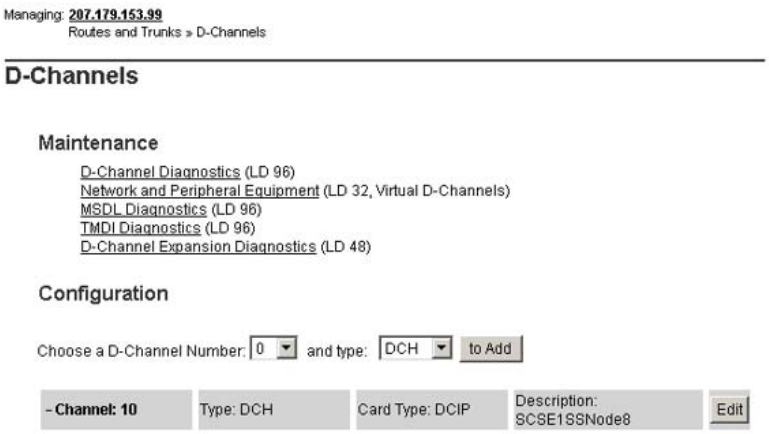

Figure 62: D-channel configuration results

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 64: New Route Configuration Web page on 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.

Configuring Virtual Trunk routes

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

   The Routes and Trunks Web page opens, as shown in Figure 63: Routes and Trunks Web page on page 141.

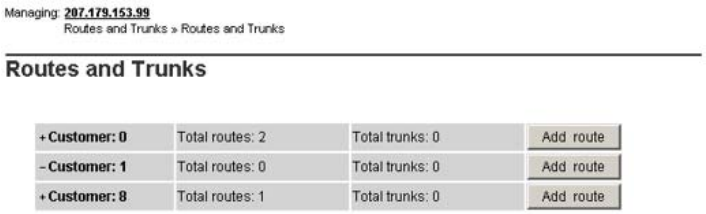

Figure 63: Routes and Trunks Web page

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 64: New Route Configuration Web page on page 142.

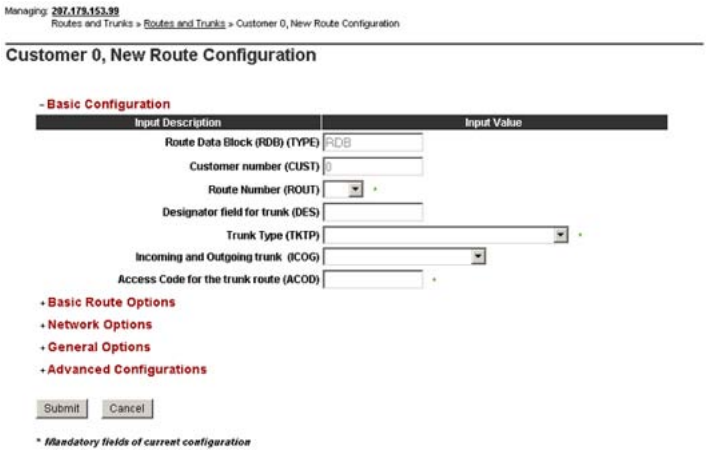

Figure 64: New Route Configuration Web page

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 65: Options available when TIE is selected on page 142):

    - **The route is for a virtual trunk route (VTRK)** (see step 4 on page 142)
    - **Digital Trunk Route (DTRK)**
    - **Integrated Services Digital Network option (ISDN)** (see step 5 on page 143)

    c. Enter the **Access Code for the trunk route (ACOD)**.

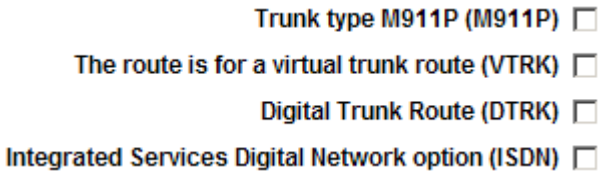

Figure 65: Options available when TIE is selected

4. Select **The route is for a virtual trunk route (VTRK)** check box.

    Three fields display as shown in Figure 66: Virtual trunk route on page 143.

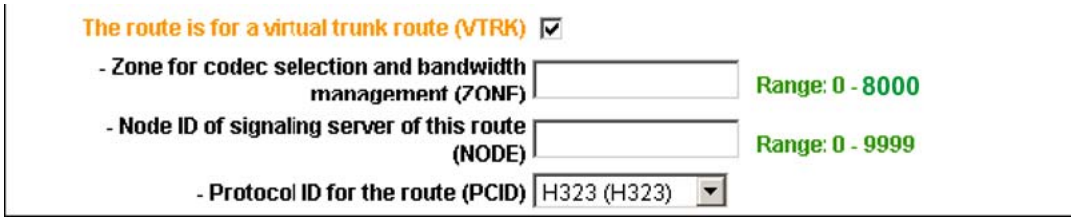

Figure 66: Virtual trunk route

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 67: ISDN option on page 143.

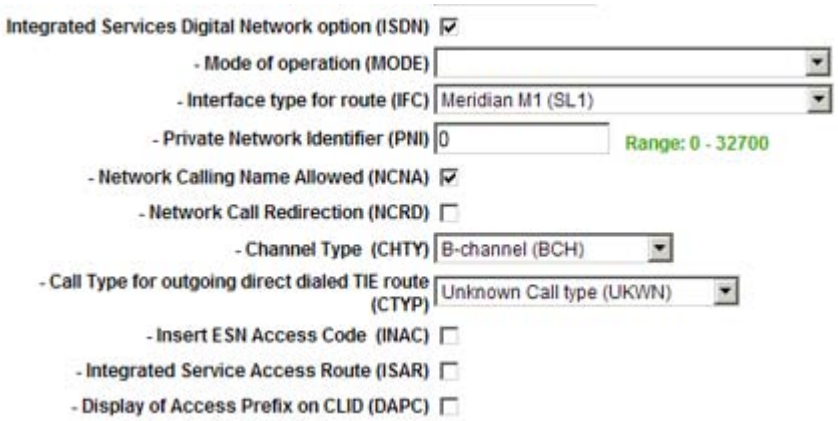

Figure 67: ISDN option

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 68: NCRD on page 143).

Figure 68: NCRD

7. Click General Options.

   The General Options list expands, as shown in Figure 69: General Options on page 144.

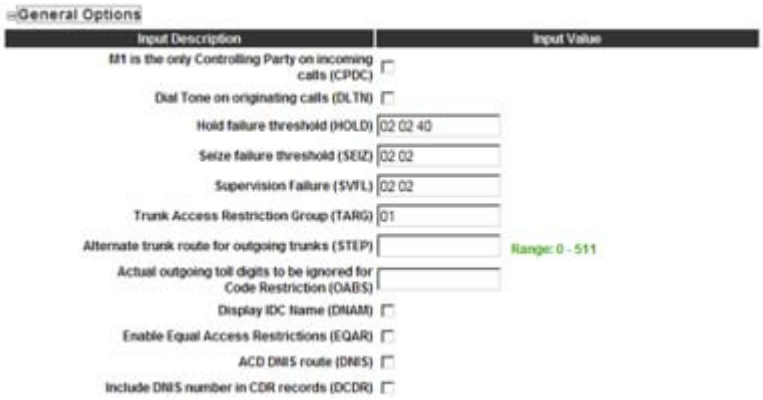

Figure 69: General Options

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.

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 CS 1000M single group machine can have physical loops 0-31 and virtual loops up to 159.

A CS 1000M multi-group system can have physical and virtual loops 0-159. A CS 1000M multi-group system 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 14: 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 System without Fiber Network Package (FIBN) package 365 xxx = 0 – 252 in multiples of four for a System with Fiber Network Package (FIBN) package 365 xxx = 0 – 252 in multiples of four for a CS 1000E system

CS 1000Esystems

Table 15: Virtual superloop/virtual card mapping for CS 1000ESystems on page 145 lists the virtual superloop and virtual card mapping for the CS 1000Esystem.

Table 15: 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.

Configuring Virtual Trunks

To configure Virtual Trunks in Element Manager, use the "New Member Property" pages. Figure 71: New Trunk Configuration Web page on page 146 to Figure 73: New Trunk Configuration Advanced Trunk Configurations on page 148 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 63: Routes and Trunks Web page on 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 70: Customer routes on page 146.

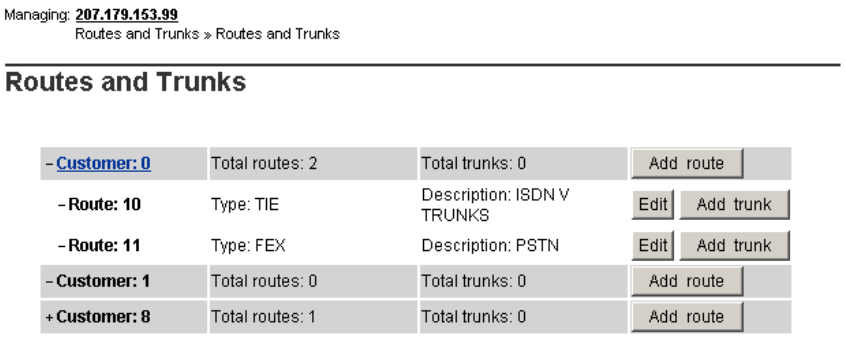

Figure 70: Customer routes

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 71: New Trunk Configuration Web page on page 146.

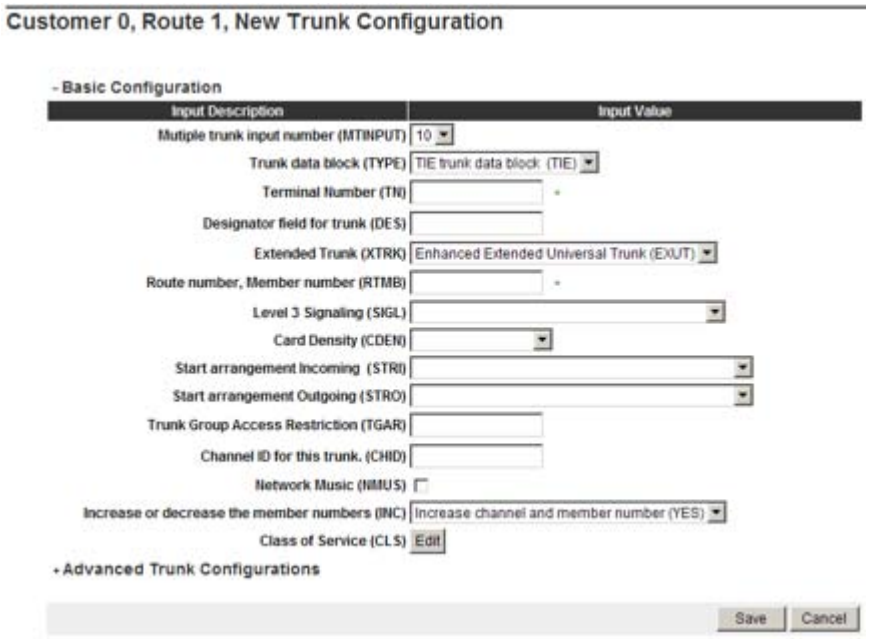

Figure 71: New Trunk Configuration Web page

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 72: New Trunk Configuration Class of Service Configuration Web page on page 147). Select a Class of Service.

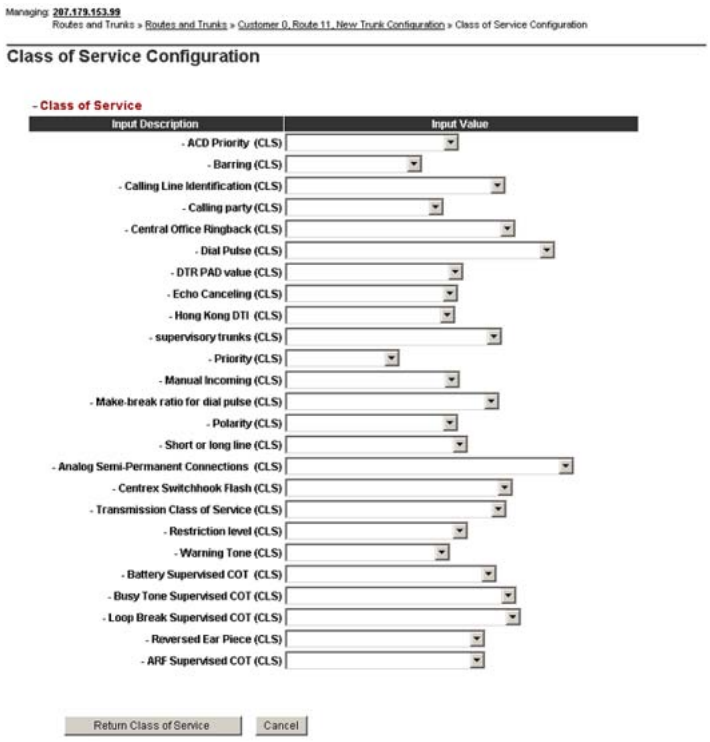

Figure 72: New Trunk Configuration Class of Service Configuration Web page

13. Select the Class of Service and then click **Return Class of Service** to return to the New Trunk Configuration Web page (see Figure 71: New Trunk Configuration Web page on page 146).
14. Select Advanced Trunk Configurations.

The Advanced Trunk Configurations list expands, as shown in Figure 73: New Trunk Configuration Advanced Trunk Configurations on page 148.

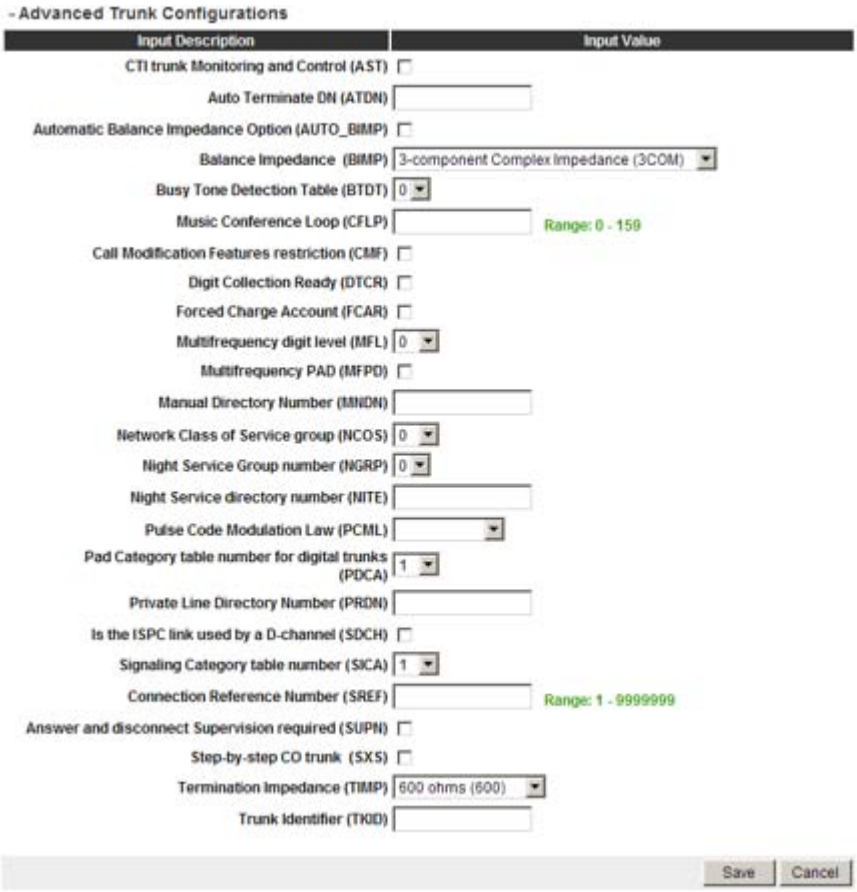

Figure 73: New Trunk Configuration Advanced Trunk Configurations

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.

Configuring networking

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

Creating an ESN control block

1. Select **Dialing and Numbering Plans > Electronic Switched Network** from the EM Navigator.

   The Electronic Switched Network (ESN) Web page opens, as shown in Figure 74: Electronic Switched Network (ESN) Web page on page 149.

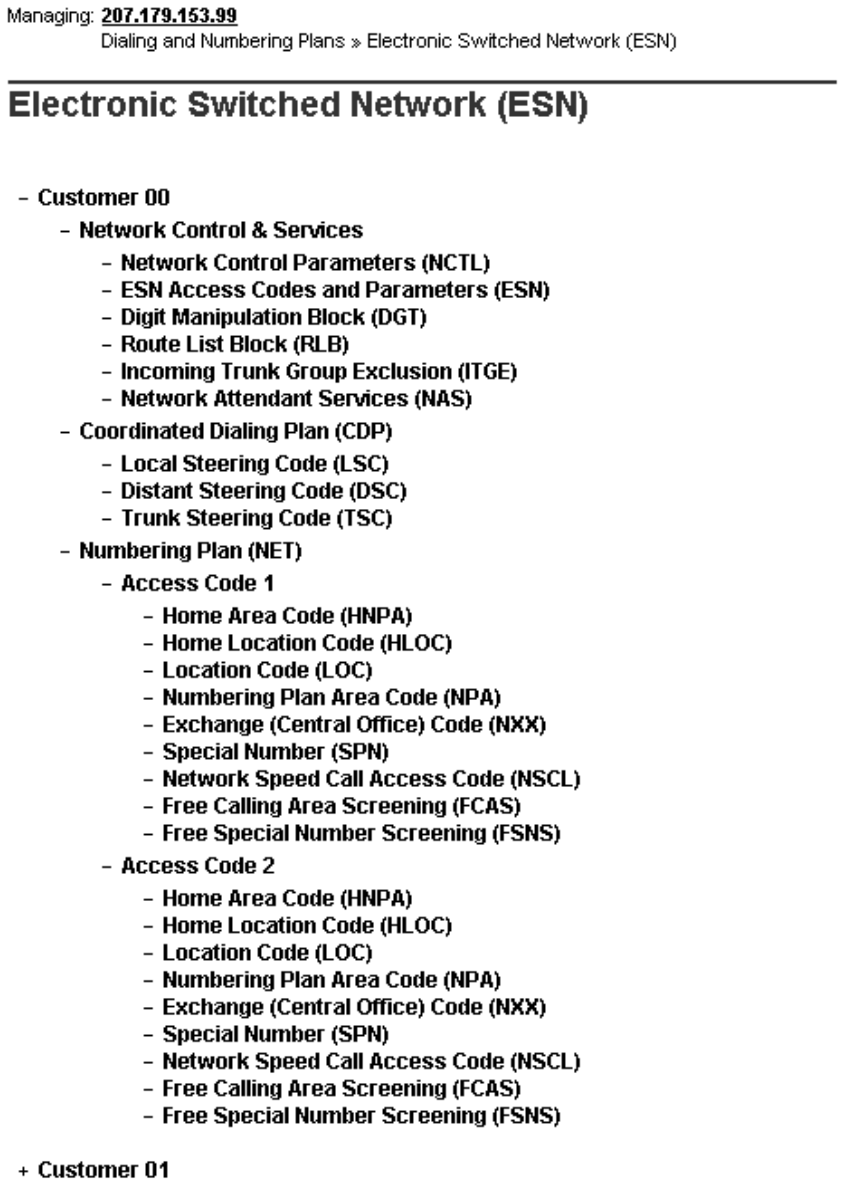

Figure 74: Electronic Switched Network (ESN) Web page

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 75: ESN Access Codes and Basic Parameters Web page on page 150.

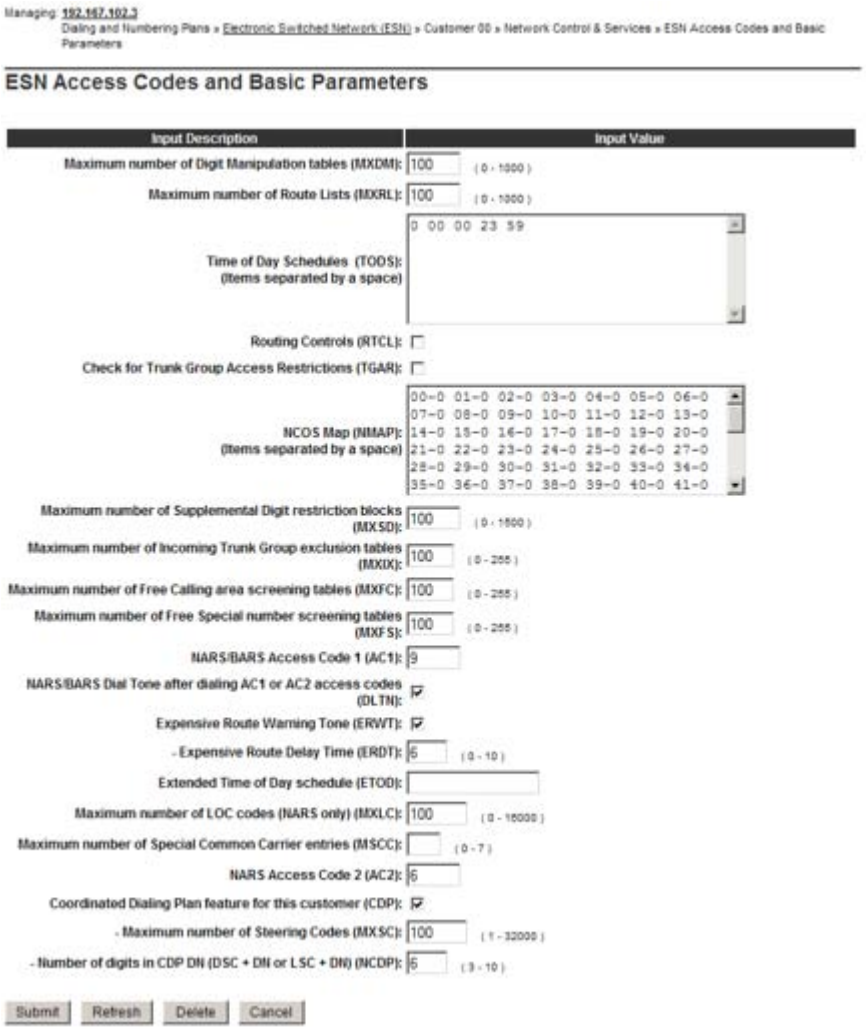

Figure 75: ESN Access Codes and Basic Parameters Web page

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 76: ESN data block configuration Coordinated Dialing Plan on 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)**).

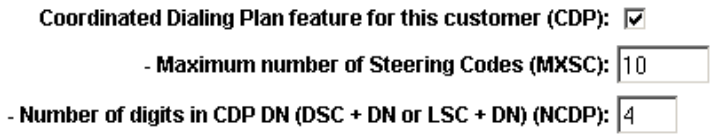

Figure 76: ESN data block configuration Coordinated Dialing Plan

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

   The Electronic Switched Network (ESN) Web page reopens (Figure 74: Electronic Switched Network (ESN) Web page on page 149).

Configuring network access

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 74: Electronic Switched Network (ESN) Web page on page 149, select **Customer xx > Network Control & Service > Network Control Parameters (NCTL)**.

   The Network Control Parameters Web page opens, as shown in Figure 77: Network Control Parameters Web page on page 152.

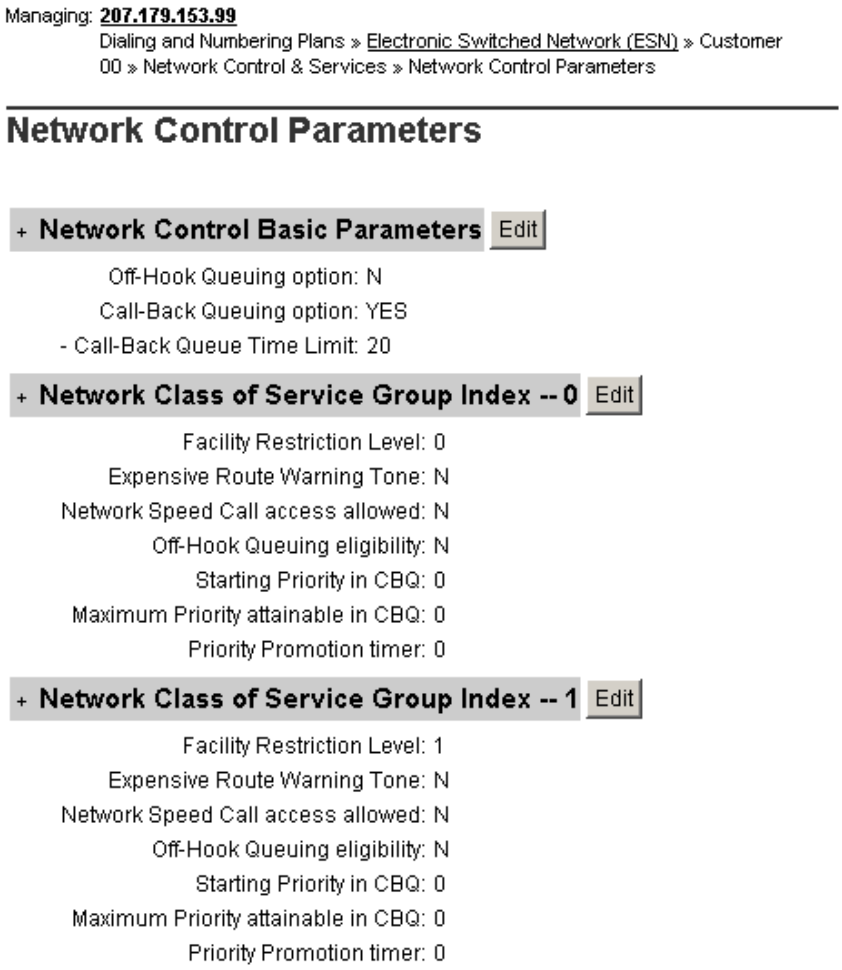

Figure 77: Network Control Parameters Web page

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

   The Network Control Basic Parameters Web page opens, as shown in Figure 78: Network Control Basic Parameters on page 153.

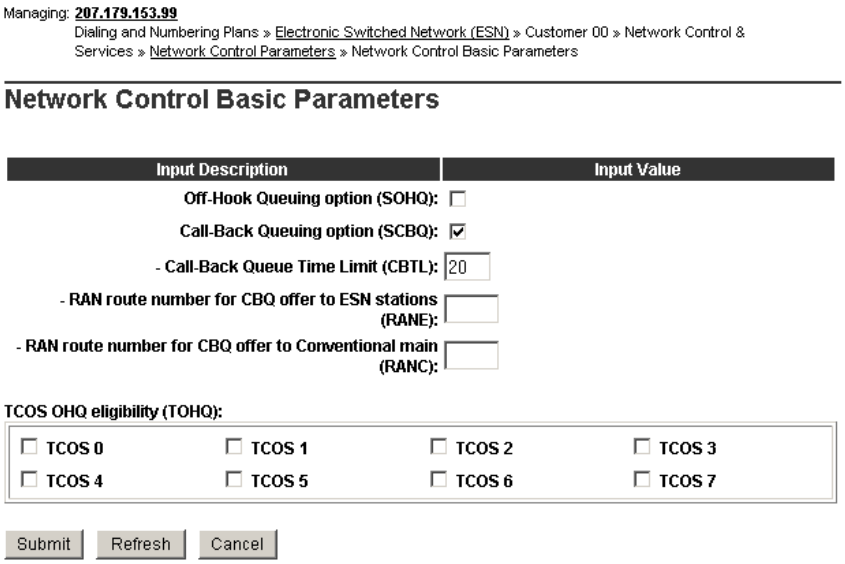

Figure 78: Network Control Basic Parameters

4. Click **Submit** to accept the default parameters on the Network Control Basic Parameters Web page.

   The Network Control Parameters Web page reopens.

Configuring call routing

Configuring digit manipulation tables on page 167 must be performed before Configuring the Route List Block.

Configuring the Route List Block

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

1. Select **Dialing and Numbering Plans > Electronic Switched Network** from the EM Navigator.
2. On the Electronic Switched Network (ESN) Web page shown in Figure 74: Electronic Switched Network (ESN) Web page on page 149, select **Customer xx > Network Control & Service > Route List Block (RLB)**.

   The Route List Blocks Web page opens, as shown in Figure 79: Route List Blocks Web page on page 154.

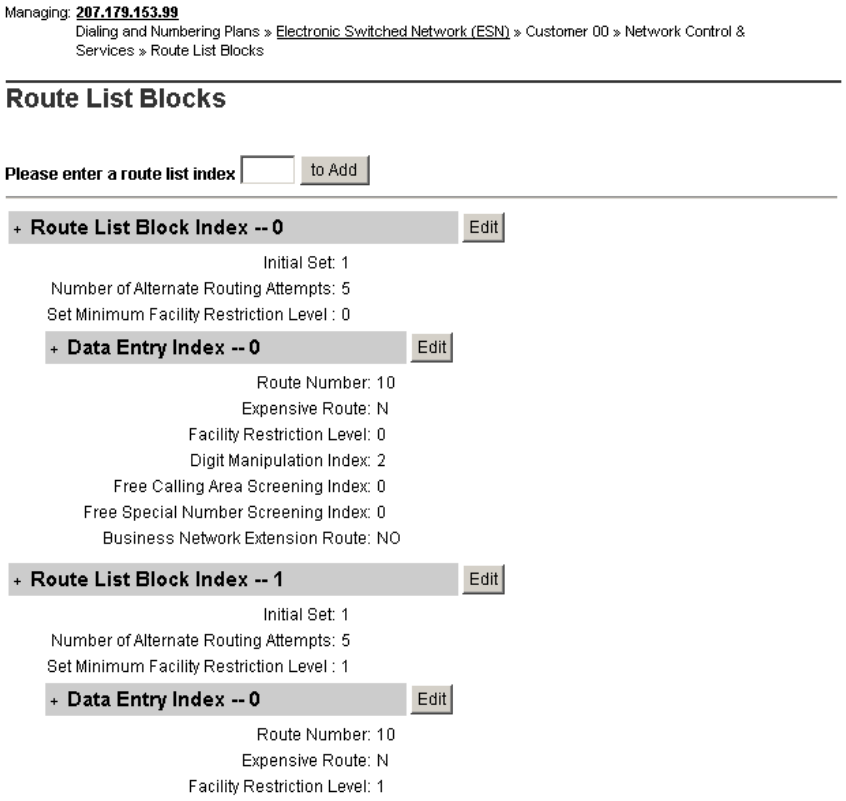

Figure 79: Route List Blocks Web page

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 80: Route List Block on page 155.

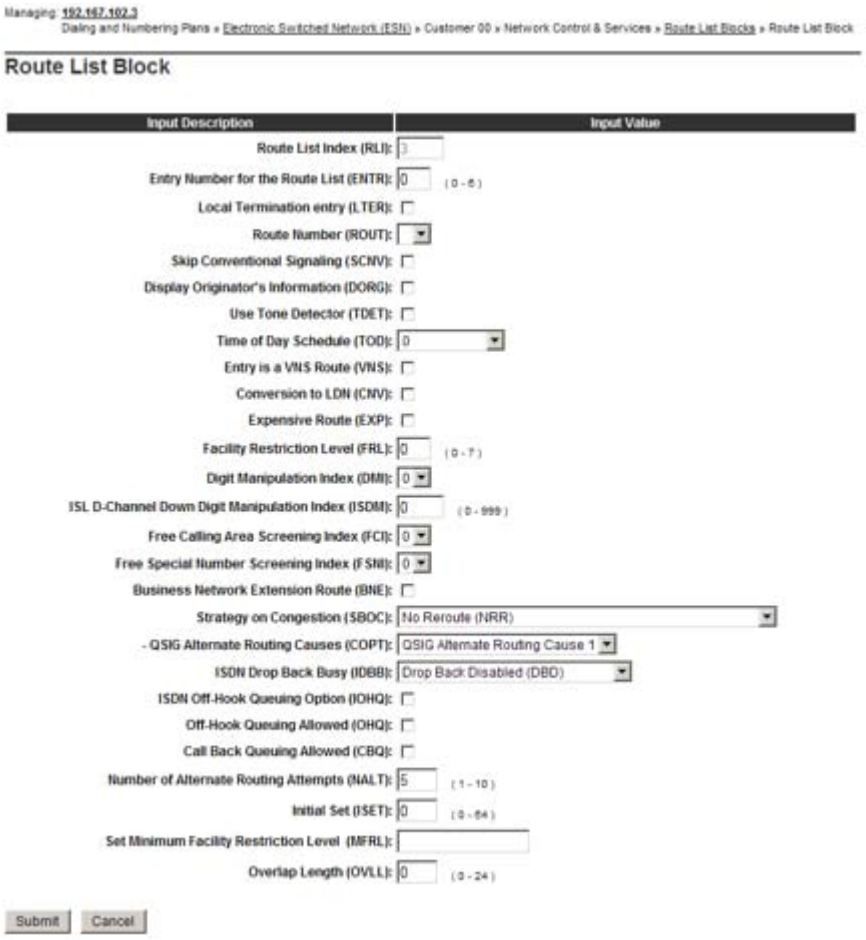

Figure 80: Route List Block

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.

Configuring Steering Codes

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

1. Select **Dialing and Numbering Plans > Electronic Switched Network** from the EM Navigator.
2. On the Electronic Switched Network (ESN) Web page shown in Figure 74: Electronic Switched Network (ESN) Web page on page 149, select **Customer xx > Coordinated Dialing Plan (CDP) > Distant Steering Code (DSC)**.

   The Distant Steering Code List Web page opens, as shown in Figure 81: EM Distant Steering Code List Web page on page 156.

Figure 81: 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 82: EM Distant Steering Code List Web page refreshed on page 156.

Figure 82: 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 83: Distant Steering Code Web page on page 156.

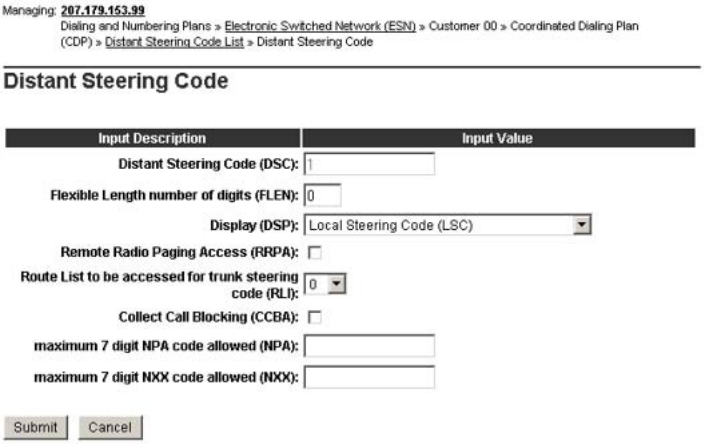

Figure 83: Distant Steering Code Web page

4. Fill in the appropriate information and click **Submit**.

   The Distant Steering Code List Web page reopens.

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 Configuring call types on page 157.

Configuring call types

1. Select **Dialing and Numbering Plans > Electronic Switched Network** from the EM Navigator.

   The Electronic Switched Network (ESN) Web page opens.

2. Scroll to the **Numbering Plan (NET)** link (see Figure 84: Numbering Plan (NET) on page 158).

To configure...	See...
Home Location Code (HLOC)	step 3 on page 158
Home Area Code (HNPA)	step 4 on page 159
Location Code (LOC)	step 5 on page 160
Numbering Plan Area Code (NPA)	step 6 on page 160
Exchange (Central Office) Code (NXX)	step 7 on page 162
Special Number (SPN)	step 8 on page 164

Note:
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, see Overlap signaling on page 205.

Note:

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:

To get an HNPA equivalent with SPN, use local termination (LTER) in the RLI and delete the prefix.

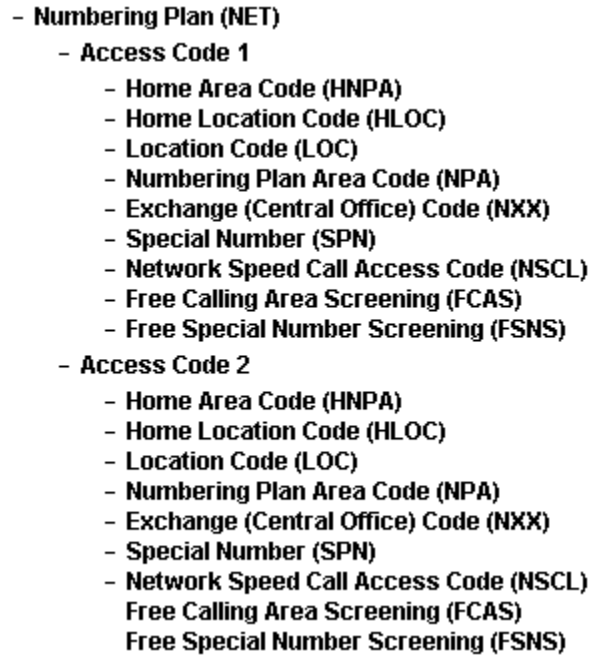

Figure 84: Numbering Plan (NET)

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 85: Home Location Code List Web page on page 159.

Figure 85: 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 86: Home Location Code Web page on page 159. The **Home Location code (HLOC)** is auto-filled.

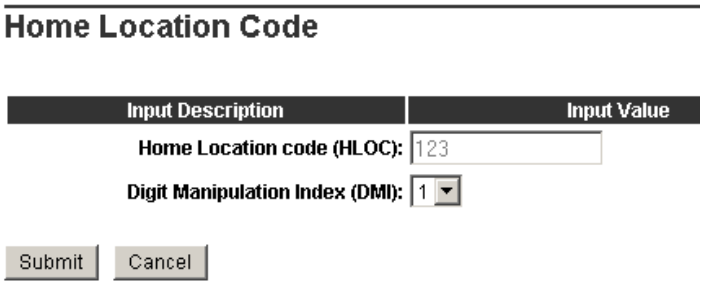

Figure 86: Home Location Code Web page

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 87: Home Numbering Plan Area Code Web page on page 159.

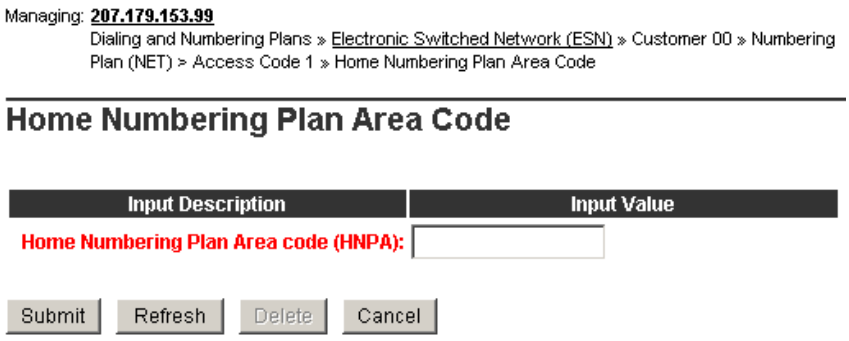

Figure 87: Home Numbering Plan Area Code Web page

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 88: Location Code List Web page on page 160.

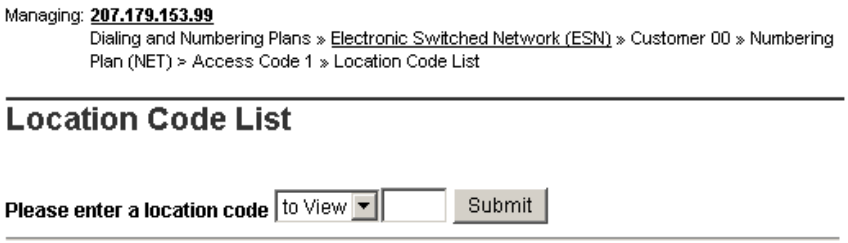

Figure 88: Location Code List Web page

    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 89: Location Code Web page on page 160.

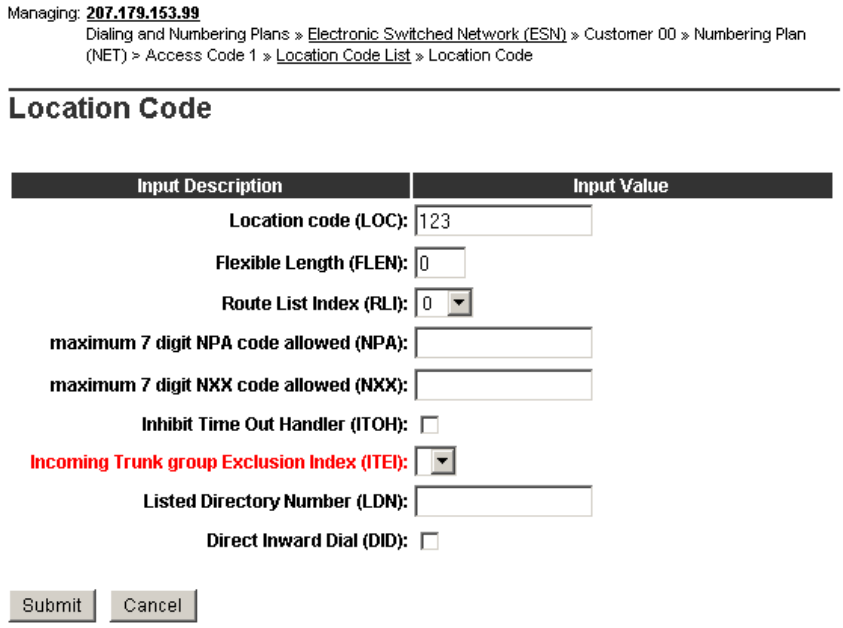

Figure 89: Location Code Web page

    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 90: Numbering Plan Area Code List Web page on page 161.

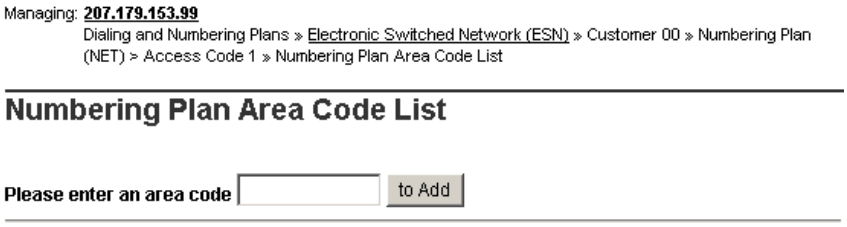

Figure 90: Numbering Plan Area Code List Web page

b. Enter an area code.

c. Click **to Add**.

   The Numbering Plan Area Code Web page opens, as shown in Figure 91: Numbering Plan Area Code Web page on page 162.

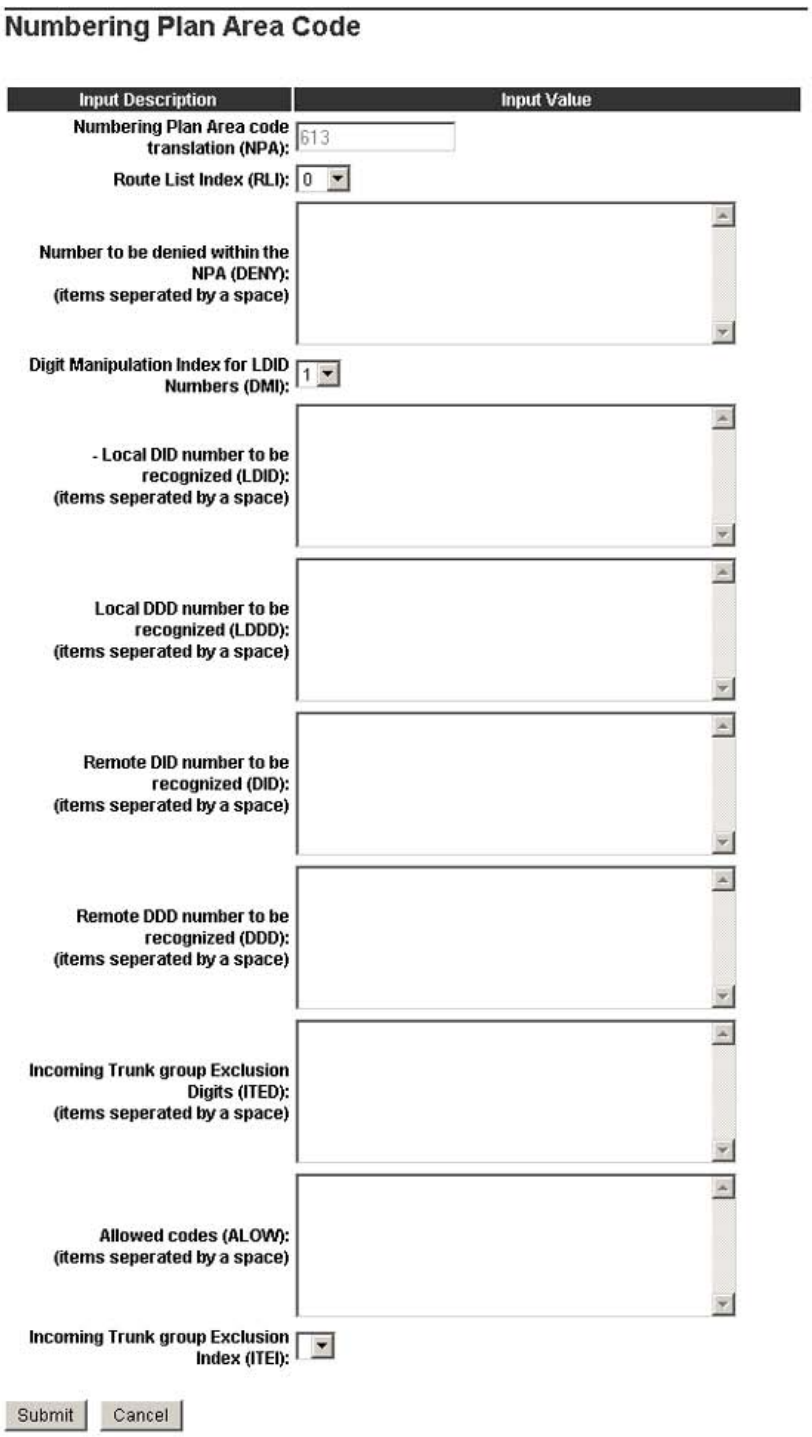

Figure 91: Numbering Plan Area Code Web page

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 92: Exchange (Central Office) Code List Web page on page 163.

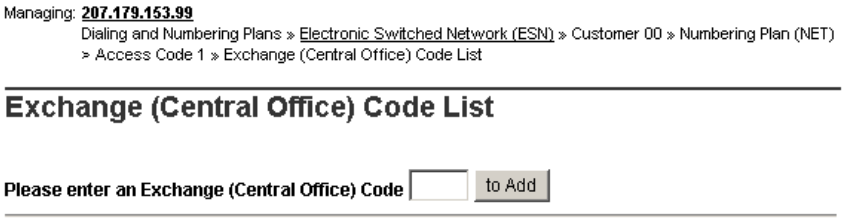

Figure 92: Exchange (Central Office) Code List Web page

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 93: Exchange (Central Office) Code Web page on page 164.

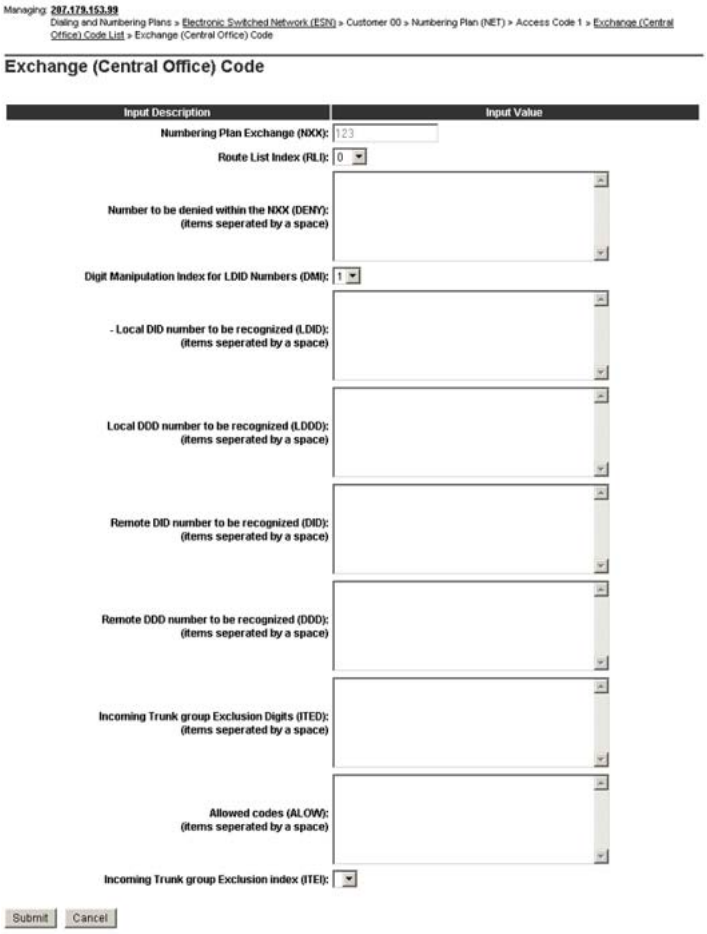

Figure 93: Exchange (Central Office) Code Web page

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 94: Special Number List Web page on page 165.

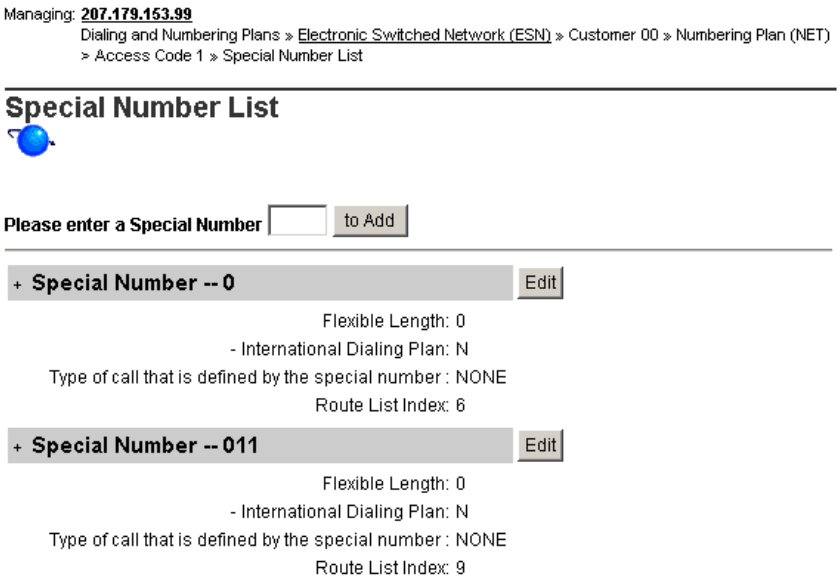

Figure 94: Special Number List Web page

b. Enter the number.

c. Click **to Add**.

   The Special Number Web page opens (see Figure 95: Special Number on page 166).

d. Enter the appropriate information.

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

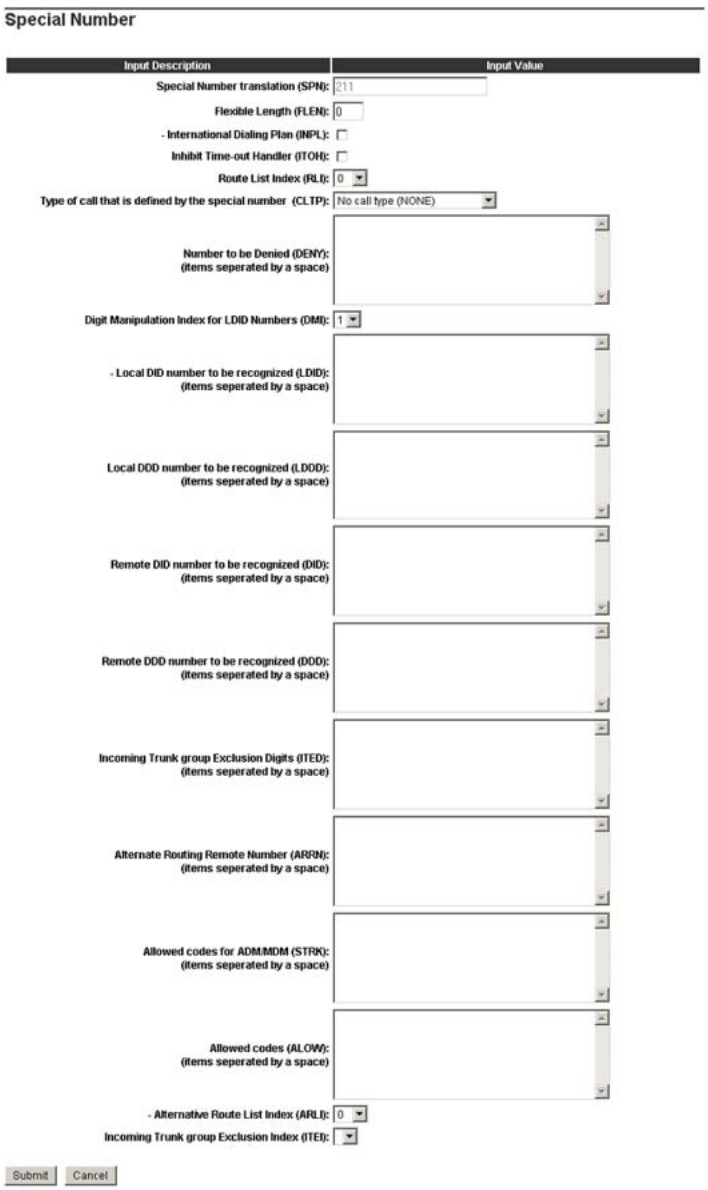

Figure 95: Special Number

f. Enter the appropriate information.

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

Configuring digit manipulation tables

Configuring digit manipulation tables

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 74: Electronic Switched Network (ESN) Web page on page 149, select **Customer xx > Network Control & Services > Digit Manipulation Block (DGT)**.

   The Digit Manipulation Block List Web page opens, as shown in Figure 96: Digit Manipulation Block List Web page on page 167.

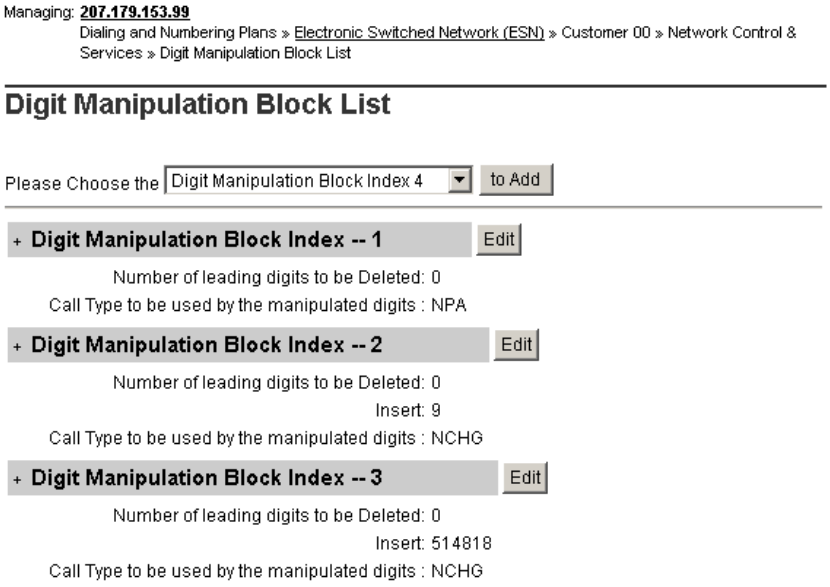

Figure 96: Digit Manipulation Block List Web page

3. Select a **Digit Manipulation Block Index** number in the drop-down list.
4. Click **to Add**.

   The Digit Manipulation Block Web page opens, as shown in Figure 97: Digit Manipulation Block Web page on page 168.

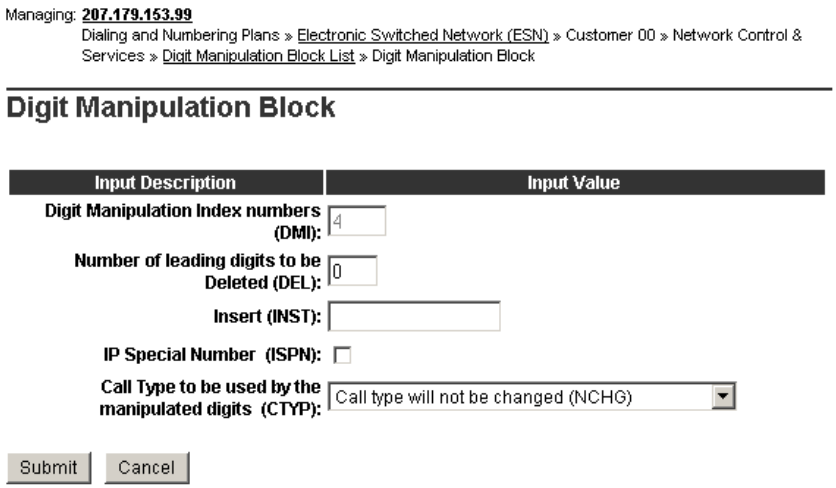

Figure 97: Digit Manipulation Block Web page

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

Configure causes to perform MALT

To configure causes to perform MALT, follow the steps in Configuring causes to perform MALT on page 168.

Configuring causes to perform MALT

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

   The IP Telephony Nodes Web page opens, as shown in Figure 98: IP Telephony Nodes Web page on page 168.

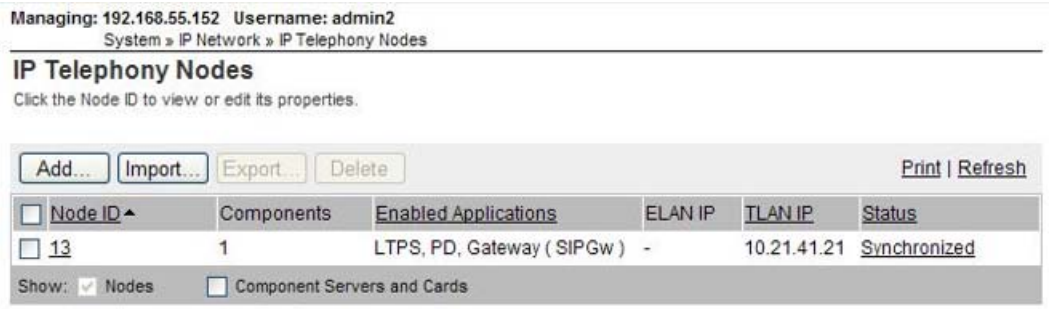

Figure 98: IP Telephony Nodes Web page

2. Click on a hyperlink in the Node ID column.

   The IP Telephony Nodes Web page refreshes with the Node Details for the selected node, as shown in Figure 99: Node Details Web page on page 169.

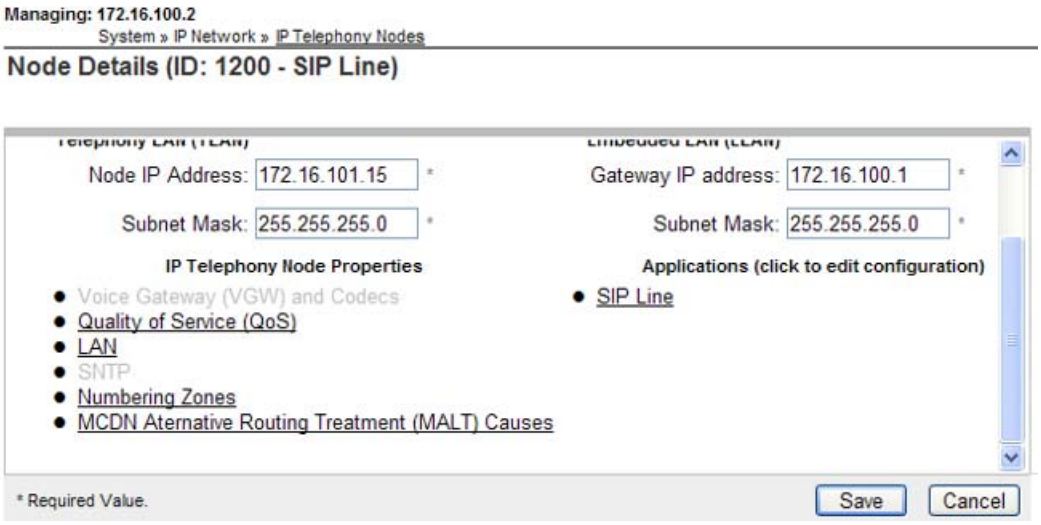

Figure 99: Node Details Web page

3. Scroll down and click on the MCDN Alternative Routing Treatment (MALT) Causes hyperlink.

   The IP Telephony Nodes Web page refreshes with a list of configurable MCDN Alternative Routing Treatment (MALT) Causes for the selected node, as shown in Figure 100: Configurable MALT Causes on page 169.

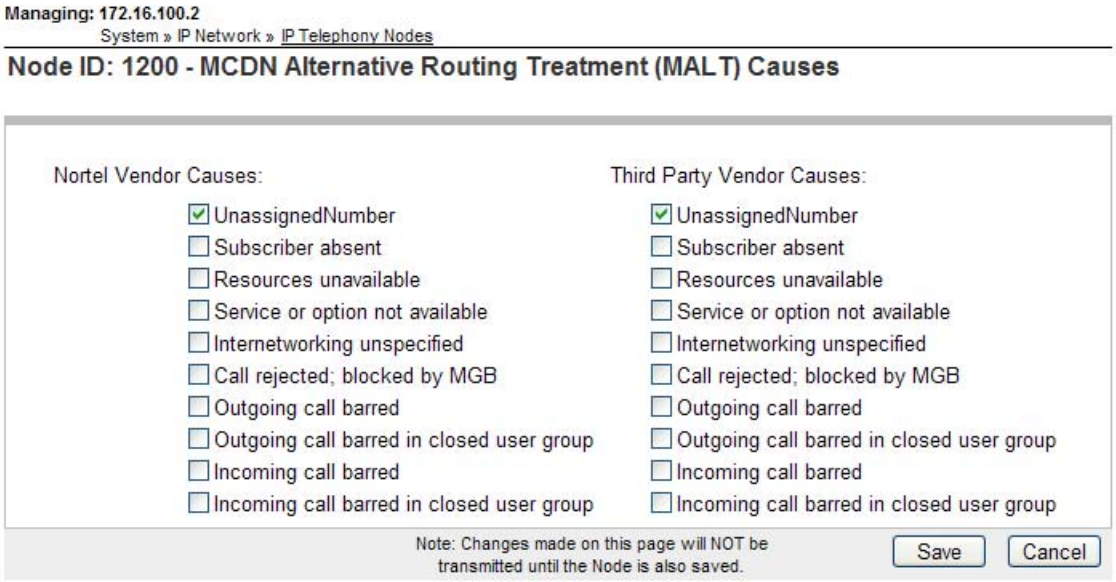

Figure 100: Configurable MALT Causes

4. Place a check mark in the box next to the configurable causes. UnassignedNumber is configured by default.
5. Click the Save button.

   The Figure 99: Node Details Web page on page 169 opens.
6. Click the Save button on the Figure 99: Node Details Web page on page 169.

The IP Telephony Nodes Web page refreshes with the Node Saved summary for the selected node, as shown in Figure 101: Node Saved summary on page 170.

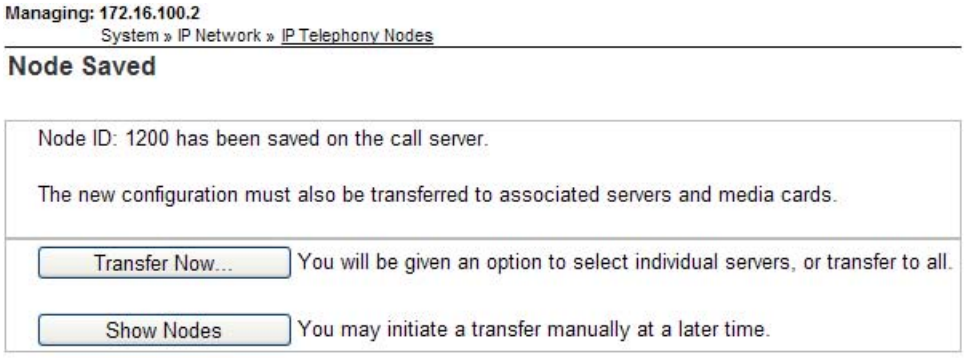

Figure 101: Node Saved summary

You can transfer the new configuration to the associated servers and media cards, or initiate a transfer manually at a later time.

1. Click the Transfer Now button to transfer the new configuration to the associated servers and media cards.

   The IP Telephony Nodes Web page opens, as shown in Figure 102: Synchronize Configuration Files on page 170.

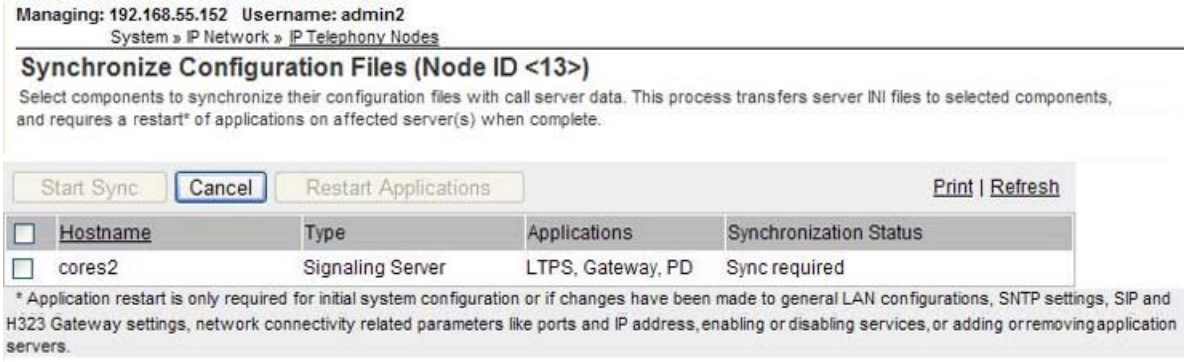

Figure 102: Synchronize Configuration Files

2. Place a check mark in the box next to the server or media card in the Hostname column.
3. Click the Start Sync button.

   The IP Telephony Nodes Web page refreshes, as shown in Figure 103: Refreshed Synchronize Configuration Files on page 171.

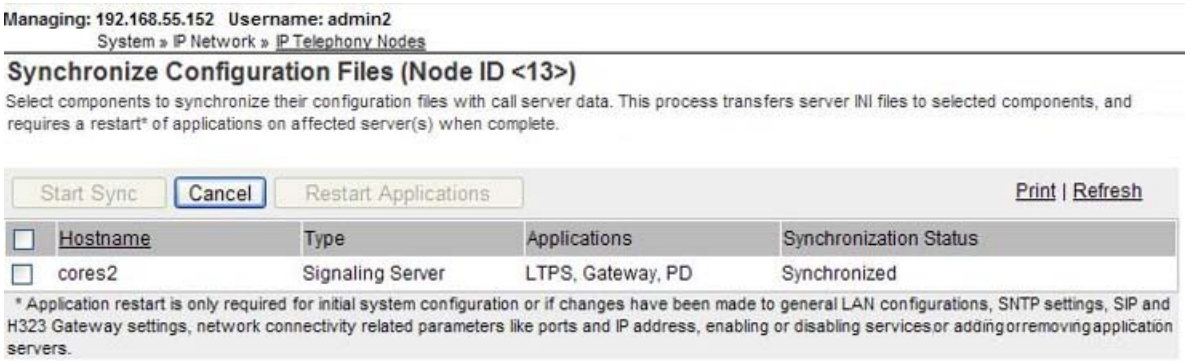

Figure 103: Refreshed Synchronize Configuration Files

Or

4. Click the Show Nodes button to transfer the new configuration manually at a later time.

   The IP Telephony Nodes Web page opens, as shown in Figure 104: IP Telephony Nodes Web page - Status Changed on page 171 .

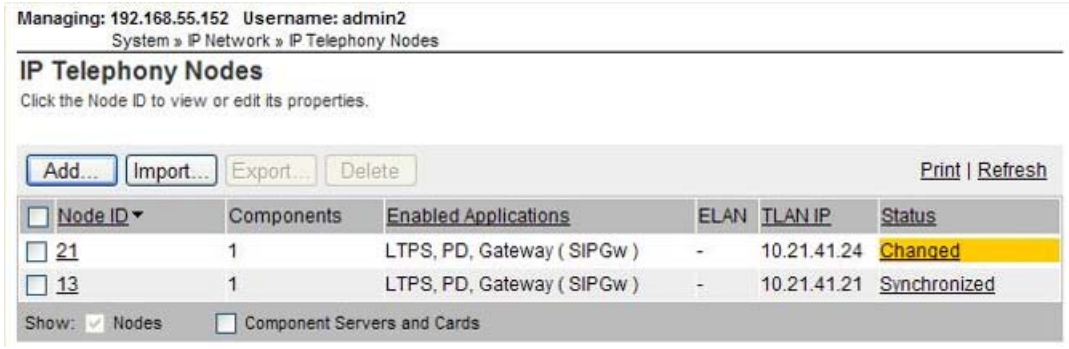

Figure 104: IP Telephony Nodes Web page - Status Changed

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.

Note:
D-channels must be unique for different nodes and routes.

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 18: LD 16 Configure the SIP route. on page 175.
   - To configure an H.323 route, see Table 19: LD 16 Configure the H.323 route. on page 176.
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 16: 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. **Note:** DCH must be unique for different nodes and routes.
CAB_TYPE		Cabinet Type
	IP FIBR	IP Expansion Cabinet or Media Gateway Fiber Expansion Cabinet
- CTYP	DCIP	Card Type D-channel over IP
- DES	x...x	Designator
BANR	YES	Enable security banner printing option
- IFC	SL1	Interface type for D-channel
CO_TYPE	aaa	Central Office switch type, where aaa = (STD) or ATT

Prompt	Response	Description
- RCVP	YES	Auto-recovery to primary D-channel option.
- - ISLM	(4000)	Integrated Services Signaling Link Maximum The maximum number of ISL trunks controlled by the D-channel. **Note:** ISLM prompt is hidden for D-channel on IP and is defaulted to 4000.
- OTBF	1-(32)-127	Output Request Buffers
- RLS	xx	Release ID of the switch at the far end of the D-channel
- RCAP	ND1, ND2 , ND3	Remote Capabilities All nodes must use same RCAP 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. **Note:** MWI is also used for H.323 if a BCM is in the network.

Table 17: LD 15 Configure network settings and options.

Prompt	Response	Description
REQ:	NEW CHG	Add new block Change existing data
TYPE:	NET	ISDN and ESN Networking options
CUST		Customer number
	0-99	Range for Large System and CS 1000E system
	0-31	Range for Small System, CS 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.

Prompt	Response	Description
	NPA NXX INTL SPN LOC	E.164 National number E.164 Subscriber number International number Special Number Location Code
FNP	(YES)	Enable Flexible Numbering Plan for customer
ISDN	YES	Integrated Services Digital Network
VPNI	1-16283	Virtual Private Network Identifier
- PNI	(0)-32700	Private Network Identifier
- CLID	(NO)	Do not enable Calling Line Identification option
CNTC	xx	Country code[1] [1]
NATC	xx	National access code[1]
INTC	xxx	International access code[1]

Note:

— CNTC is the country code for the country where the switch is located. For example, CNTC = 1 for Canada.

— NATC is the national access code. For example, NATC = 1 for Canada.

— INTC is the international access code. For example, INTC = 011 for Canada. For example, a caller who wants to reach Austria dials 6-011-61-xxxyyyzzz from endpoint A (for example, in Toronto) over the Virtual Trunk to endpoint B (for example, in the United Kingdom) which serves as a gateway to the PSTN.

The 011 is stripped off at endpoint A because the NRS does not understand it. Endpoint B would receive 61-xxxyyyzzz and compare 61 with its CNTC (= 44) and assumes that this is an international call. So, it inserts the INTC (= 00 for Europe) and sends 00-61-xxxyyyzzz to the PSTN routing to Austria.

Consider another caller from endpoint A making a call to the UK PSTN by dialing 6-011-44-xxxyyyzzz. Endpoint B would receive 44-xxxyyyzzz. It finds that 44 equals to its CNTC and figures that this is a national call. So, it strips off 44 and inserts the NATC (= 0 for UK) and sends 0-xxxyyyzzz to the PSTN.

Note:

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 18: LD 16 Configure the SIP route. on page 175 below.
- To configure an H.323 route, see Table 19: LD 16 Configure the H.323 route. on page 176.

[1] CNTC, NATC and INTC are needed when a public call is tandemed over the Virtual Trunk.

Table 18: 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	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
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	0-2550–8000	Zone for codec selection and bandwidth management
PCID	SIP	Protocol ID for the SIP route. Defines the route as a SIP route.
CRID	(NO) YES	CDR record (for SIP) to include correlation ID. YES = When enabled, the fourth line is included in the new CDR record. NO = The fourth line in not included in the CDR record (default). See *Call Detail Recording: Description and Formats (NN43001-550)* for more information. **Note:** This prompt appears only for a SIP Virtual Trunk (that is, if VTRK = YES and PCID = SIP) and CDR is turned on for this route.
NODE	xxxx	Node ID Where the Node ID matches the node of the Signaling Server. The Node ID can have a maximum of four numeric characters.
ISDN	YES	Integrated Services Digital Network option
- MODE	ISLD	Mode of operation
- DCH	0-159	D-channel number
- IFC	SL1	Interface type for route (IFC responses are listed in *Software Input/Output: Administration (NN43001-611)*

Prompt	Response	Description
- SRVC	a...a	Service type for AT&T ESS connections (SRVC responses are listed in *Software Input/Output: Administration (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.
ICOG	IAO	Incoming and Outgoing trunk. Incoming and Outgoing
ACOD	x...x	Access Code for the trunk route.

Table 19: 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	 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
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	0-2550–8000	Zone for codec selection and bandwidth management
NODE	xxxx	Node ID

Prompt	Response	Description
		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 *Software Input/Output: Administration (NN43001-611)*
- SRVC	a...a	Service type for AT&T ESS connections (SRVC responses are listed in *Software Input/Output: Administration (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 20: 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 21: 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
DES	a....a	Virtual Trunk descriptor Designator field for trunk groups where a...a = 0-16 alphanumeric characters (DES is an optional entry)
XTRK	VTRK	Extended Trunk Virtual Trunk type **Note:** If you entered a virtual TN at the TN prompt, then the XTRK prompt only accepts the VTRK option.
CUST	xx	Customer number as defined in LD 15.
...		
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 **Note:** Immediate (IMM) is recommended for both fields, unless the trunk is intended for SIP DECT or Converged Office applications; in that case, use WNK/WNK.
SUPN	YES	Answer and disconnect Supervision required SUPN must equal YES for a COT with Virtual Network Service
...		
TKID	nnnnnnn	Trunk Identifier

Table 22: 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 *ISDN Primary Rate Interface: Features* (NN43001-569-B1).
...		
CDP	YES	Coordinated Dialing Plan feature for this customer
- MXSC	x	Maximum number of Steering Codes Where x = • 0-10000 = Maximum number of Steering Codes in North America • 0-32000 = Maximum number of Steering Codes outside North America
- NCDP	x	Number of digits to be included as part of the CDP DN (DSC + DN or LSC + DN) where x = 3-7.
AC1	x	One- or two-digit NARS/BARS Access Code 1
AC2	x	One- or two-digit NARS Access Code 2
DLTN	(YES)	NARS/BARS Dial Tone after dialing AC1 or AC2 access codes
ERWT	(YES)	Expensive Route Warning Tone
...		
TGAR	(NO)	Check for Trunk Group Access Restriction.

Table 23: LD 87 Configure network access.

Prompt	Response	Description
REQ	NEW	Add new data.
FEAT	NCTL	Network Control Block
SOHQ	(NO)	Off-Hook Queuing option
SCBQ	(NO)	Call-Back Queuing option
NCOS	(0)	Network Class of Service group number
TOHQ	(0)	TCOS OHQ eligibility

Table 24: 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 25: 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
...		
RLI	0-127 0-255 0-1999	Route List Index to be accessed CDP and BARS NARS FNP
PROU	(1) 2	Preferred Routing. 1 -> Takes Proxy Server Route 1 (Primary/Secondary/tertiary) 2 - >Takes Proxy Server Route 2 (Primary) Default value is 1.
ENTR	xxx	Entry number for NARS/BARS Route list Where xxx = • 0-63 Entry number for NARS/BARS Route List • 0-6 Route list entry number for CDP • X Precede with x to remove

Prompt	Response	Description
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 0-1999	Digit Manipulation Index No digit manipulation required CDP NARS and BARS FNP
...		

Table 26: LD 87 Configure the CDP steering codes.

Prompt	Response	Description
REQ	NEW	Create new data block
FEAT	CDP	Coordinated Dialing Plan
TYPE	DSC	Type of steering code 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
- RLI	0-31 0-127 0-255 0-1999	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 27: 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	AC1 AC2	Translator Access Code 1 (NARS/BARS) Access Code 2 (NARS)

Prompt	Response	Description
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	0-1999	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 28: 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 Coordinated Dialing Plan routing feature
	RTD	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. **Note:** Prompted when ISDN signaling package 145 is equipped and either the Integrated Service Digital Network BRI Trunk Access (BRIT) package 233 is equipped or at least one PRA link is configured.
- VPNI	1-16283	Virtual Private Network Identifier

Prompt	Response	Description
- CLID	YES	Allow Calling Line Identification option Calling Line Identification does not require ISDN.
- - ENTRY	xx	CLID entry to be configured. CLID entries must be between 0 and the value entered at the SIZE prompt - 1. Precede entry or entries with X to delete. ENTRY is repeated until a <cr> is entered.
- - - HLOC	100-9999999	Home Location Code (ESN) as defined in LD 90 1 to 7 digits with extended code. Prompted when ISDN=YES, or with Digital Private Network Signaling System 1 (DPNSS) package 123.
- - - LSC	0 .. x..x	Local Steering Code 1 to 7 digits. LSCs are required if the CDP DNs are longer than the local PDNs. The CLID sent for a CDP call is composed of the LSC defined in LD 15 plus the PDN of the calling set. Various ISDN network features depend on the CLID as the return address for sending feature control messages. Multiple LSCs may be defined in LD 87 for CDP but only one LSC can be defined here for the CLID. The LSC prompt appears only if the user has a five or six digit dialing plan, or if the DPNSS software package is equipped. LSC is prompted here if ISDN = NO, otherwise LSC is a sub-prompt of ISDN.
- PFX1	xxxx	Prefix 1. Prefix or area code for International PRA. First element of Calling Party Number. PFX1 + PFX2 + DN cannot exceed 8 numbers for AXE-10. Prompted with International Primary Rate Access (IPRA) package 202.
- PRX2	xxxx	Prefix 2. Central Office Prefix for International PRA. Second element of Calling Part Number. PFX1 + PFX2 + DN cannot exceed 8 numbers for AXE-10. Prompted with International Primary Rate Access (IPRA) package 202.
- RCNT	0-(5)	Redirection Count for ISDN calls Maximum number of inter-node hops allowed in a network redirection call, only enforced when ISDN = YES. This field must be set to greater than 0 for a network redirection to take place.
- PSTN	(NO)	Public Service Telephone Networks Limit the number of PSTNs allowed in a network connection to one PSTN. The default (NO) puts no limit on the number of PSTN connections.
- - TNDM	0-(15)-31	Tandem Threshold/Loop Avoidance Limit This is the value permitted in a network connection.

Prompt	Response	Description
		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, µ-Law to A- Law or A- Law to µ-Law, in a network connection
- SATD	0-(1)-5	Satellite Delays. Number of satellite delays allowed in a network connection
OCLI	NO	NO manipulation is done on outgoing CLID for calls forwarded to EuroISDN link.
TIDM	(NO)	Trunk Identity Meaningful
DASC	xxxx	Display Access Code Enter the access code which is to be placed on displays before Originating Line Identities (OLI) and Terminating Line Identities (TLI) are received from the ISDN. The default is no code, when creating a new data block. Prompted with Multi Language Wake Up (MLWU) package 206 and Integrated Digital Access (IDA) package 122.
ROPT	(NRO)	No Route Optimization This option may be used to suppress Route Optimization on switches which already have high traffic.
DITI	(NO)	DID to TIE connections allowed
TRNX	(NO)	Prevent transfer on ringing of supervised external trunks across a private network
EXTT	(NO)	Prevent connection of supervised external trunks through either call transfer or conference
FTOP	(FRES)	Flexible Trunk to Trunk Options. Flexible Trunk to Trunk Connections Restricted. FTT feature is inactive.
APAD	x y (0) (0)	Alternative Pad. Where: x = trunk pad selection and y = conference pad selection Valid inputs for x are: (0) = default North America 1 = Australia 2 = New Zealand 3 = Italy 4 = China EPE or EPE/IPE systems 5

Prompt	Response	Description
		= 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	0-1999	Route List Index as defined in LD 86
- CDPL	1-(10)	Flexible length of Vacant Number Routing (VNR) Coordinated Dialing Plan (CDP)
- UDPL	1-(19)	Uniform Plan Public Flexible length of Vacant Number Routing (VNR) Uniform Dialing Plan digits (UDP). Enter the maximum number of UDP digits expected by VNR.
NIT	2-(8)	Network Alternate Route Selection (NARS) Interdigit Timer
NAS_ATCL	(YES)	Network Attendant Service Attendant Control allowed
NAS_ACTV	NO	Network Attendant Service routing Activated
FOPT	0-(6)-30	Flexible Orbiting Prevention Timer The number of seconds in two second intervals that CFW should be suspended on a set that has just forwarded a call off-node. Odd entries are rounded up to the next valid entry. A response of 0 disables FOPT.
CNDN	0 .. x..x	Customer Calling Number Identification DN on outgoing Multifrequency Compelled Signaling (MFC) calls
- CNIP	(YES)	Calling Number Identification Presentation Send Customer Calling Number Identification (CNDN) + Trunk ID (TKID) if Calling Line ID (CLID) = NO in LD 17
CNAT	0 .. x..x	CNI Attendant DN on outgoing Multifrequency Compelled Signaling (MFC) calls.

Prompt	Response	Description
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 29: 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 for Features and Services Fundamentals - Book 6 of 6 (NN43001-106-B6).

Note:
This feature is enabled by default.

Use Element Manager to configure the following 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 System > IP Network > Nodes: Servers, Media Cards to open the Node Configuration window to begin configuration.

Adding an IP address to VTRK Network Health Monitor

1. Click on a link in the **Node ID** column.

The Node Details Web page opens.

2. Click the Gateway (H323GW) Applications link.

   The Virtual Trunk Gateway Configuration Details Web page opens.

3. Select the Monitor IP Addresses (listed below) check box in the Virtual Trunk Network Health Monitor section.
4. Enter the IP address into the Monitor IP field and click the Add button beside the Monitor IP field to add the IP address.

   When the maximum of 8 IP address fields is reached, the Add button is disabled.

5. Click Save to save the configuration.

   The Node Details Web page opens.

6. Click Save in the Node Details Web page to save the Node.

   The Node Saved Web page opens.

7. Click Transfer Now... to launch the Synchronize Configuration Files Web page.
8. Select the Servers from the Hostname column and click Start Sync.

Viewing new CLI commands in Element Manager

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

Deleting a monitored IP address in VTRK Network Health Monitor

1. Click on a link in the **Node ID** column.

   The Node Details Web page opens.

2. Click the Gateway (H323GW) Applications link.

   The Virtual Trunk Gateway Configuration Details Web page opens.

3. Select the Monitor IP Addresses (listed below) check box in the Virtual Trunk Network Health Monitor section.
4. Select a configured IP address from the list in the Monitor addresses box and click the Remove button beside the Monitor addresses box.
5. Click Save to save the configuration.

   The Node Details Web page opens.

6. Click Save in the Node Details Web page to save the Node.

   The Node Saved Web page opens.

7. Click Transfer Now... to launch the Synchronize Configuration Files Web page.
8. Select the Servers from the Hostname column and click Start Sync.

Table 30: 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	IPv4 32 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: ENABLE = 1 IP = 47.11.221.22 IP = 47.11.221.23
	IPv6 128 bit IPv4 address in the format: 2001:0DB8:0000:0000:0000:0008:200C:3457 compressed as: 2001:DB8::8:200C:3457	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: ENABLE = 1 IP = 2001:DB8:0:0:0:8:1428:57AB IP = 2001:DB8:0:0:0:8:1428:57AB
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 if 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	Click the Remove button beside the Monitored IP address to delete the IP address. If the Monitor check

Action	Response	Comment
	reflect the current row number.	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

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.

Configuring the Gateways

Both H.323 Gateways and SIP Trunk Gateways (that is, the Virtual Trunk applications) are supported.

The three possible configurations are:

- H.323 Gateway only (H.323 Virtual Trunk only)
- SIP Trunk Gateway only (SIP Virtual Trunk only)
- Both H.323 and SIP Trunk Gateways (both H.323 and SIP Virtual Trunks)

Enabling and configuring the H.323 Gateway

The H.323 Gateway runs only on the Signaling Server. However, configuration of the H.323 Gateway requires configuration on both the Call Server and the Signaling Server. You must use Element Manager to configure the H.323 Gateway on the Signaling Server.

- For Call Server configuration, follow Feature Implementation of IP Peer Networking on page 171. In LD 16, configure the route as an H.323 route (see Table 19: LD 16 Configure the H.323 route. on page 176).
- For Signaling Server configuration, perform the following procedures using Element Manager:
  - Enabling the H.323 Gateway (H.323 Virtual Trunk application) on page 190

- Configuring the H.323 Gateway settings on page 192

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

1. Log in to Element Manager.
2. Select **System > IP Network > Nodes: Servers, Media Cards** from the EM Navigator.

   The IP Telephony Nodes Web page opens, as shown in Figure 98: IP Telephony Nodes Web page on page 168.
3. Click on a link in the **Node ID** column to Edit the Node properties.

   The Node Details Web page opens.

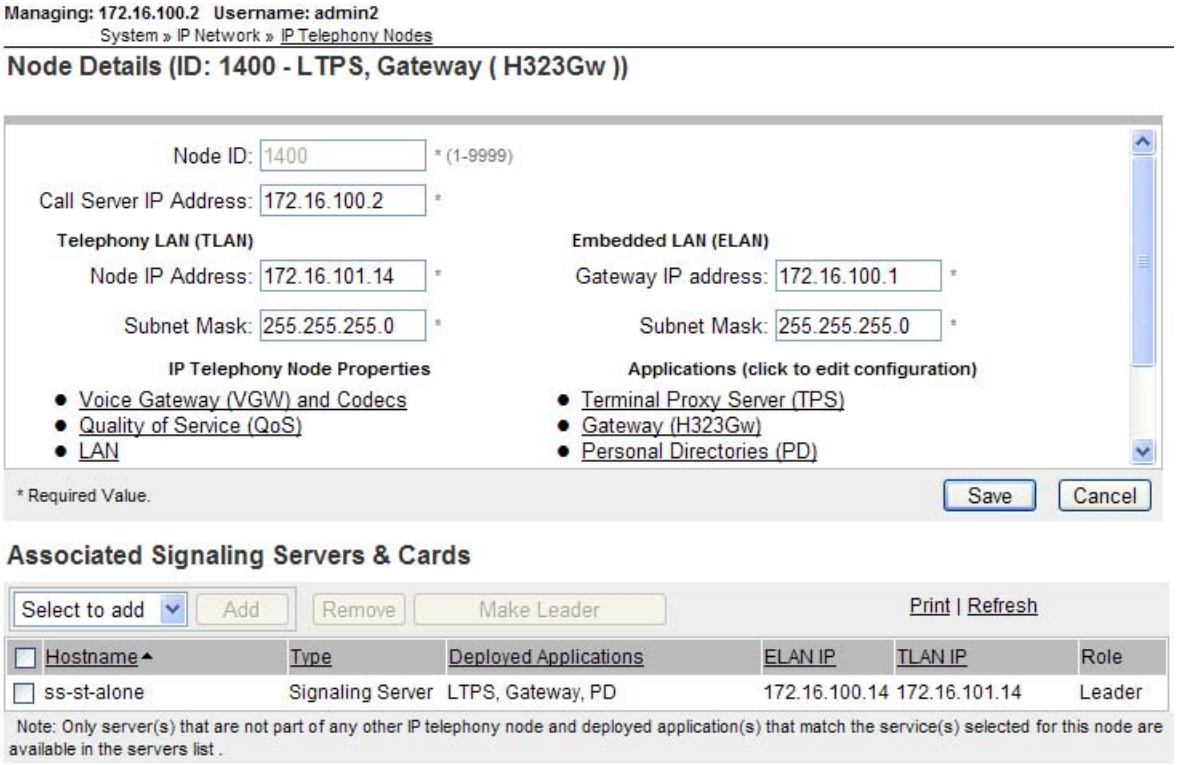

Figure 105: Node Details Web page

4. Click **Gateway (H323GW)** Applications link.

   The Virtual Trunk Gateway Configuration Details Web page opens.

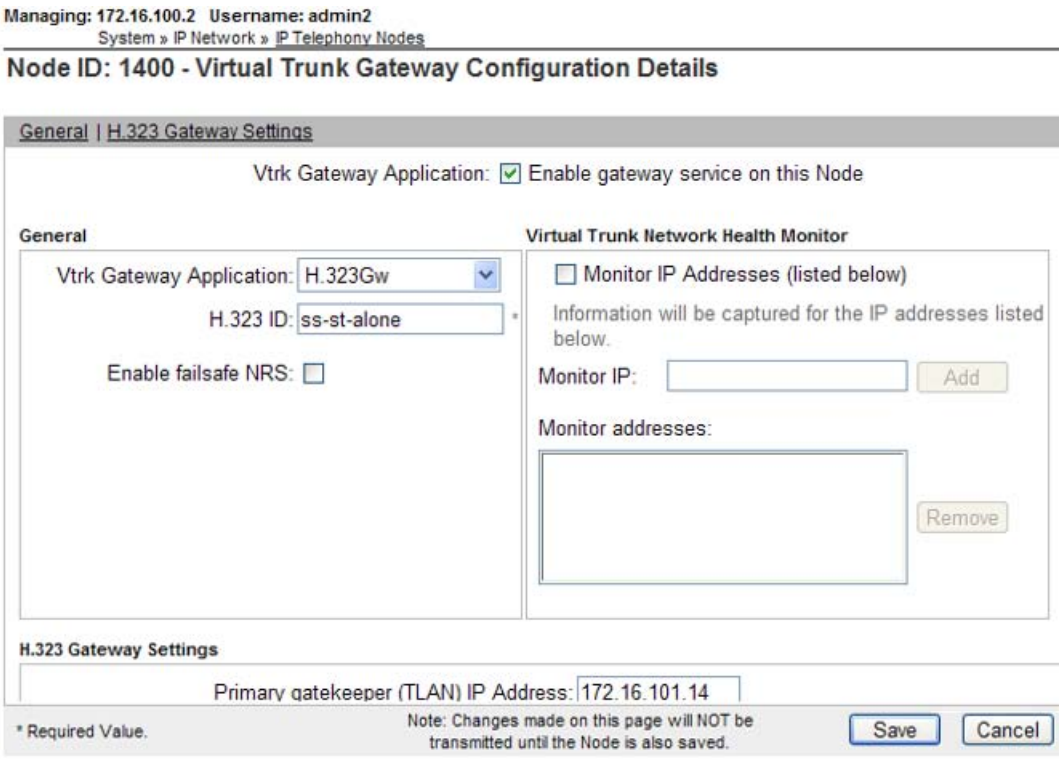

Figure 106: Virtual Trunk Gateway Configuration Details Web page

5. Check the Enable gateway service on this Node box.
6. Select an **H.323GW option** from the Vtrk Gateway Application: drop-down list.

   This field is used to enable H.323 Gateway.

   Note:

   The three supported modes are: SIP Gateway (SIPGw), H.323Gw, and SIPGw and H.323Gw.

   The Virtual Trunk Gateway Configuration Details Web page refreshes.
7. Verify the H.323 ID. Each H.323 Gatekeeper is configured with an H.323 Gatekeeper alias name, which is an H.323-ID. Enter a text string to describe the H. 323 Virtual Trunk source in the H.323 ID: text box.
8. Click Save to save the configuration.

   The Node Details Web page opens.
9. Click Save in the Node Details Web page to save the Node.

   The Node Saved Web page opens.
10. Click Transfer Now... to launch the Synchronize Configuration Files Web page.
11. Select the Servers from the Hostname column and click Start Sync.

Configuring the H.323 Gateway settings

1. Log on to Element Manager.
2. Select **System > IP Network > Nodes: Servers, Media Cards** from the EM Navigator.

   The IP Telephony Nodes Web page opens, as shown in Figure 98: IP Telephony Nodes Web page on page 168.
3. Click on a link in the **Node ID** column to Edit the Node properties.

   The Node Details Web page opens, as shown in Figure 105: Node Details Web page on page 190.
4. Click **Gateway (H323GW)** applications link.

   The Virtual Trunk Gateway Configuration Details Web page opens, as shown in Figure 106: Virtual Trunk Gateway Configuration Details Web page on page 191.
5. Click the H.323 Gateway Settings link or scroll down to the H.323 Gateway Settings pane.

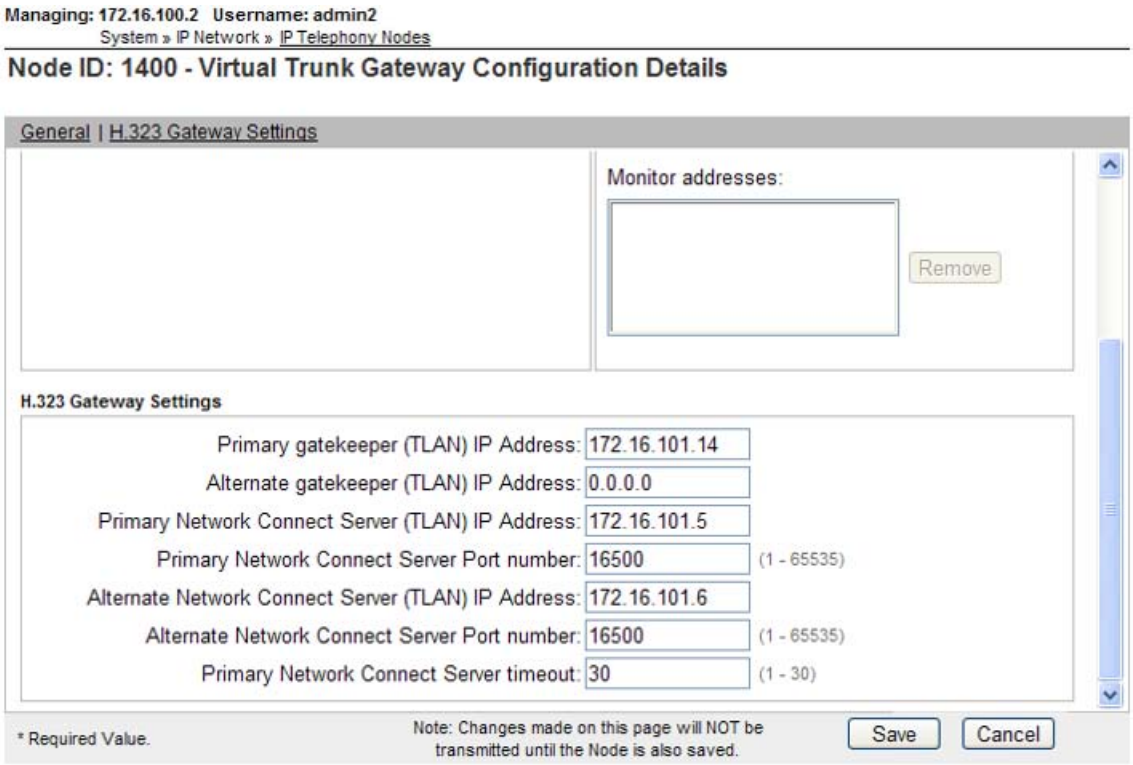

Figure 107: H323 GW Settings

6. Configure the following fields:

   a. Primary gatekeeper (TLAN) IP address: Enter the TLAN network interface IP address (not the Node IP address) of the Leader Signaling Server running the H.323 Gatekeeper.

b. Alternate gatekeeper (TLAN) IP address: Enter the IP address if an Alternate Gatekeeper exists.

c. Primary Network Connect Server (TLAN) IP address: Enter or verify that the NCS IP address matches the Primary gatekeeper IP address (NRS). The NCS is used for IP Line Virtual Office, Branch Office (including the SRG), and Geographic Redundancy features. The NCS allows the Line TPS (LTPS) to query the NRS using the UNIStim protocol.

d. Primary Network Connect Server Port number: Enter a port number for the Primary NCS. The port number must be numeric and up to 5 numbers in length. The range is 1024 to 65535. The default value is 16500.

e. Alternate Network Connect Server (TLAN) 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.

7. Click Save to save the configuration.

   The Node Details Web page opens.

8. Click Save in the Node Details Web page to save the Node.

   The Node Saved Web page opens.

9. Click Transfer Now... to start the Synchronize Configuration Files Web page.

10. Select the Servers from the Hostname column and click Start Sync.

Enabling and configuring the SIP Trunk Gateway

The SIP Trunk Gateway runs only on the Signaling Server. Configuration of the SIP Trunk Gateway requires configuration on both the Call Server and the Signaling Server. You must use Element Manager to configure the SIP Trunk Gateway on the Signaling Server.

- For Call Server configuration, follow Feature Implementation of IP Peer Networking on page 171. In LD 16, configure the route as a SIP route.
- For Signaling Server configuration, perform the following procedures using Element Manager:
  - Enabling the SIP Trunk Gateway (SIP Virtual Trunk application) on page 194
  - Configuring the SIP URI to NPI/TON mapping on page 200

Enabling the SIP Trunk Gateway (SIP Virtual Trunk application)

1. Log in to Element Manager.
2. Select **System > IP Network > Nodes: Servers, Media Cards** from the EM Navigator.

   The IP Telephony Nodes Web page opens, as shown in Figure 98: IP Telephony Nodes Web page on page 168.
3. Click on a link in the **Node ID** column to Edit the Node properties.

   The Node Details Web page opens, as shown in Figure 105: Node Details Web page on page 190.
4. Click the Gateway Applications Link. Depending on your configuration, you see: **(H323Gw), (SIPGw),** or **(SIPGw and H323Gw)**

   The Virtual Trunk Gateway Configuration Details Web page opens, as shown in Figure 106: Virtual Trunk Gateway Configuration Details Web page on page 191.
5. In the **General** pane, select a **SIPGw option** from the **Vtrk Gateway Application:** drop-down list.

   This field is used to enable SIP Trunk Gateway and Services.

   Note:
   The three supported modes are: SIP Gateway (SIPGw), H.323Gw, and SIPGw and H.323Gw.

   The Virtual Trunk Gateway Configuration Details Web page refreshes.

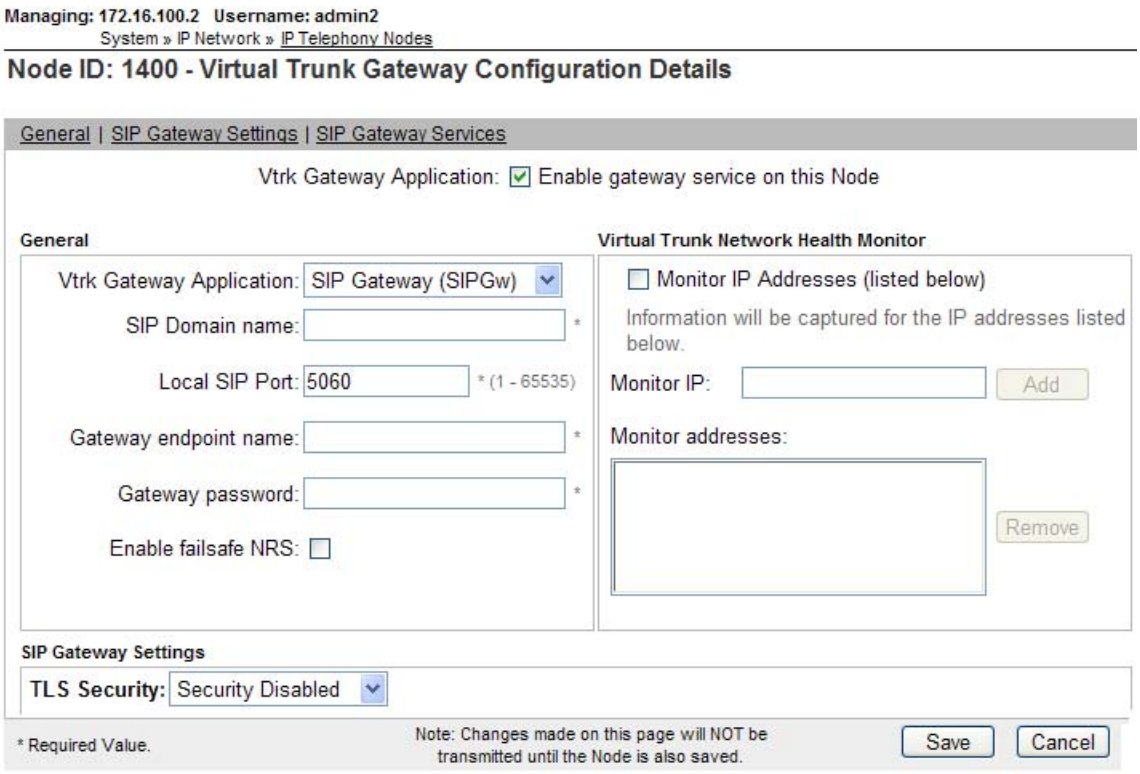

Figure 108: Virtual Trunk Gateway Configuration Details General pane

6. 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 *Network Routing Service Fundamentals (NN43001-130)*. 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.
7. Verify the **Local SIP Port**. This is the port to which the gateway listens. The default is 5060.
8. The **Gateway Endpoint Name** and **Gateway Password** must be entered and must match the Gateway Endpoint name and Gateway Endpoint authentication password used by the SIP Proxy/Redirect Server. The name and authentication password are used in authenticating the Gateway Endpoint with the SIP Proxy/ Redirect Server.
    a. **Gateway Endpoint Name:** Enter the endpoint name. This is the username that is used when authenticating this gateway with the NRS (SIP Proxy/ Redirect Server) or the MCS 5100 Proxy Server.
    b. **Gateway Password:** Enter the password. This is the password that is used when authenticating this gateway with the NRS (SIP Proxy/ Redirect Server) or the MCS 5100 Proxy Server.
9. The **VTRK Registration ID** used by the Call Server to register the Virtual trunk must be updated if the associated Node ID configured in the Route Data Block of the Call

Server is different from the Trunk Gateway Node ID. By default, the **VTRK Registration ID** is configured equal to the Node ID of the Trunk Gateway.

10. Click **Save** to save the configuration.

    The **Node Details** Web page opens.

11. Click **Save** in the Node Details Web page to save the Node.

    The Node Saved Web page opens.

12. Click **Transfer Now...** to launch the **Synchronize Configuration Files** Web page.
13. Select the Servers from the **Hostname** column and click **Start Sync.**

Configuring the SIP Trunk Gateway settings

1. Log on to Element Manager.
2. Select **System > IP Network > Nodes: Servers, Media Cards** from the EM navigation pane.

   The IP Telephony Nodes Web page opens, as shown in Figure 98: IP Telephony Nodes Web page on page 168.

3. Click on a link in the **Node ID** column to Edit the Node properties.

   The Node Details Web page opens, as shown in Figure 105: Node Details Web page on page 190.

4. Click the **Gateway** (H323Gw or SIPGw) Applications link.

   The Virtual Trunk Gateway Configuration details Web page opens, as shown in Figure 106: Virtual Trunk Gateway Configuration Details Web page on page 191.

5. Click the **SIP Gateway Settings** link or scroll down to the SIP Gateway Settings section.

Figure 109: SIP Gateway Settings

6. In the **TLS Security** section, select **Security Policy** from the list and configure the following:

   - **Port**
   - **Number of Byte Re-negotiation**

- **Options**
  - **Client Authentication**
  - **X.509 Certificate Authentication**

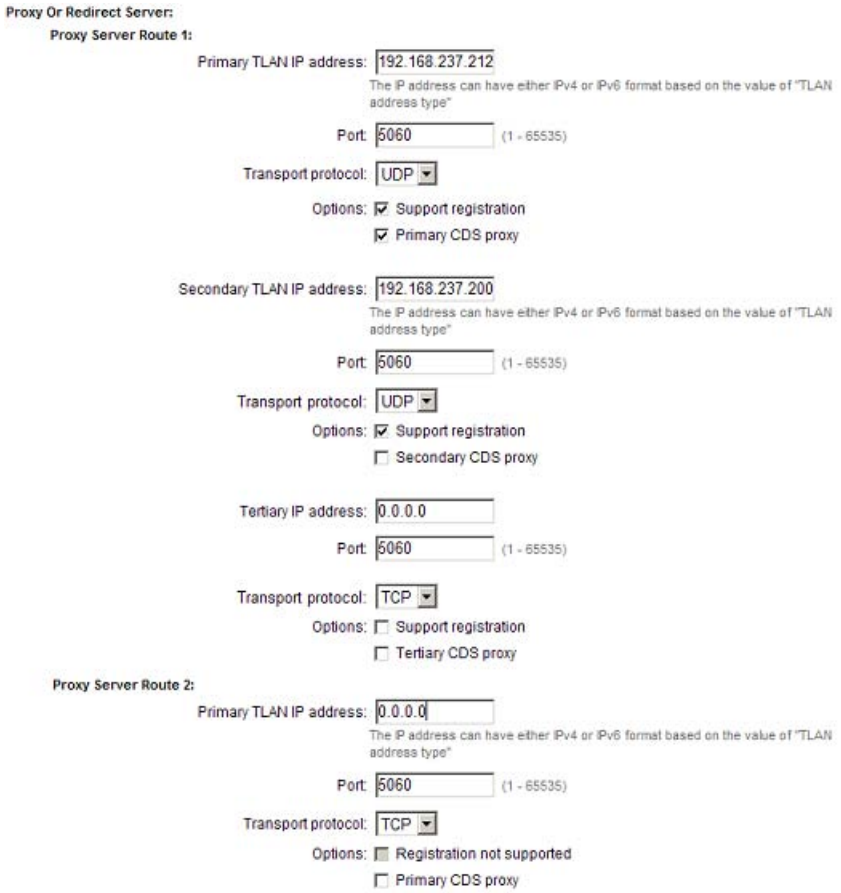

Figure 110: SIP Gateway Settings (Contd)

7. In the **Proxy or Redirect Server** section for **Proxy Server Route 1:**, configure the following fields:

   a. **Primary TLAN IP address** Type the TLAN network interface IP address of the Primary SIP Proxy/Redirect Server or the MCS 5100 Proxy Server.

   b. **Port** Leave the default port value as 5060 for the Primary SIP Proxy/ Redirect Server or the MCS 5100 Proxy Server.

   c. Select the **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.

d. **Options:**

- **Supports Registration** Select the check box to tell the SIP Trunk Gateway whether the primary NRS (SIP Proxy/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.
- Do not select the check box **Primary CDS Proxy**. This option is not used in this release.

e. **Secondary TLAN IP address** Type the TLAN network interface IP address of the Secondary SIP Proxy/Redirect Server or the MCS 5100 Proxy Server (if configured).

f. **Port** Leave the default port value as 5060 for the Secondary SIP Proxy/Redirect Server or the MCS 5100 Proxy Server (if configured).

g. **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.

h. **Options**:

- **Support Registration** Select the check box to tell the SIP Trunk Gateway whether the secondary NRS (SIP Proxy/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.
- Do not select the check box **Secondary CDS Proxy**. This option is not used in this release.

i. **Tertiary IP Address** Type the TLAN network interface IP address of the tertiary SIP Proxy/Redirect Server or the MCS 5100 Proxy Server.

j. **Port** Leave the default port value as 5060 for the Tertiary SIP Proxy/Redirect Server or the MCS 5100 Proxy Server (if configured).

k. **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.

l. **Options:**

- **Support registration** Select the check box to inform the SIP Trunk Gateway that the tertiary NRS (SIP proxy/Redirect Server) supports registration. If the check box is selected, then the SIP Trunk Gateway must register with the tertiary NRS. If the check box is not

selected, the SIP Trunk Gateway will not register with the tertiary NRS.

- Do not select the check box **Tertiary CDS Proxy**. This option is not used in this release.

8. In the **Proxy or Redirect Server** section for **Proxy Server Route 2:**, configure the following fields:
    a. **Primary TLAN IP address**. Type the TLAN network interface IP address of the Primary SIP Proxy/Redirect Server or the MCS 5100 Proxy Server.
    b. **Port**. Leave the default port value as 5060 for the Primary SIP Proxy/ Redirect Server or the MCS 5100 Proxy Server.
    c. **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.
    d. **Options:**
        - **Registration not supported**. Registration for proxy server route 2 is not supported.
        - **Primary CDS Proxy**. This option is not used in this release.
9. Click **Save**.

    The Node Details Web page opens.
10. Click **Save** in the Node Details Web page to save the Node.

    The Node Saved Web page opens.
11. Click **Transfer Now..**. to launch the Synchronize Configuration Files Web page.
12. Select the Servers from the **Hostname** column and click **Start Sync.**

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 Proxy/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 has been provisioned (see *Network Routing Service Fundamentals (NN43001-130)*, you must build the SIP URI to NPI/TON mapping using Element Manager.

Configuring the SIP URI to NPI/TON mapping on page 200 provides the steps to create this SIP URI to NPI/TON mapping using an NRS example and an example for the MCS 5100.

Configuring the SIP URI to NPI/TON mapping

1. Log in to Element Manager.
2. Select **System > IP Network > Nodes: Servers, Media Cards** from the EM Navigator.

   The IP Telephony Nodes Web page opens, as shown in Figure 98: IP Telephony Nodes Web page on page 168.
3. Click on a link in the **Node ID** column to Edit the Node properties.

   The Node Details Web page opens, as shown in Figure 105: Node Details Web page on page 190.
4. Click **Gateway (H323GW)** Applications link.

   The Virtual Trunk Gateway Configuration Details Web page opens, as shown in Figure 106: Virtual Trunk Gateway Configuration Details Web page on page 191.
5. Scroll down to the **SIP URI Map** section of the SIP Gateway Settings pane.

   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 Fundamentals (NN43001-130)*, specifically the examples provided in Numbering plan mapping.

   To complete the NRS example, refer to Figure 111: SIP URI Map for the NRS example on page 201 and go to step 6.

   To complete the MCS 5100 example, refer to Figure 112: SIP URI Map for the MCS 5100 example on page 202 and go to step 7.

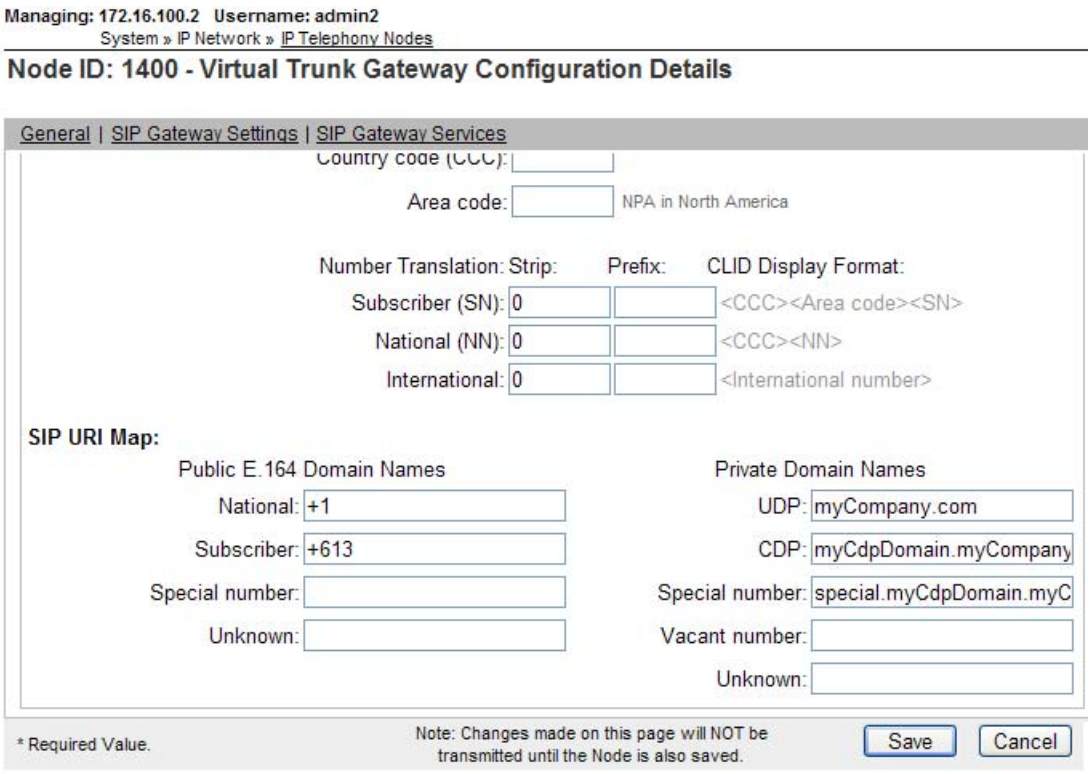

Figure 111: SIP URI Map for the NRS example

6. Fill in the following fields for the NRS example (see Figure 111: SIP URI Map for the NRS example on page 201):

   For the Public E.164 Domain Names

   a. Type +1 in the National: text box.
   b. Type +613 in the Subscriber: text box.
   c. Leave the Special Number: text box blank
   d. Leave the Unknown: text box blank.

   For the Private Domain Names

   e. Type myCompany.com in the UDP: text box.
   f. Type myCdpDomain.myCompany.com in the CDP: text box.
   g. Type special.myCdpDomain.myCompany.com in the Special number: text box.
   h. Leave the Vacant number: text box blank.
   i. Leave the Unknown text box blank.
   j. Click Save to save the configuration.

      The Node Details Web page opens.

   k. Click Save in the Node Details Web page to save the Node.

The Node Saved Web page opens.

l. Click Transfer Now... to launch the Synchronize Configuration Files Web page.

m. Select the Servers from the Hostname column and click Start Sync.

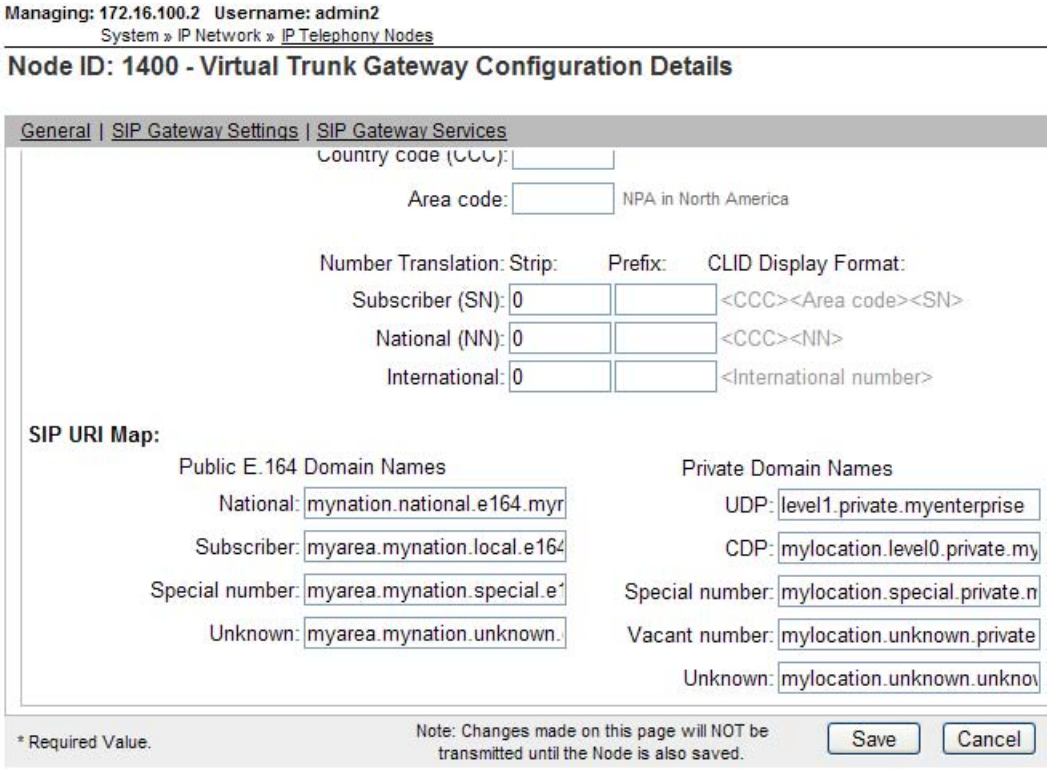

Figure 112: SIP URI Map for the MCS 5100 example

7. Fill in the following fields for the MCS 5100 example (see Figure 112: SIP URI Map for the MCS 5100 example on page 202):

   For the Public E.164 Domain Names

   a. Type mynation.national.e164.myrootdomain in the National: text box.

   b. Type myarea.mynation.local.e164.myrootdomain in the Subscriber: text box.

   c. Type myarea.mynation.special.e164.myrootdomain in the Special number: text box.

   d. Type myarea.mynation.unknown.e164.myrootdomain in the Unknown: text box.

   For the Private Domain Names

   e. Type level1.private.myenterprise in the UDP: text box.

   f. Type mylocation.level0.private.myenterprise in the CDP: text box.

   g. Type mylocation.special.private.myenterprise in the Special number: text box.

h. Type mylocation.unknown.private.myenterprise in the Vacant number: text box.

i. Type mylocation.unknown.unknown.myrootdomain in the Unknown: text box.

j. Click Save to save the configuration.

   The Node Details Web page opens.

k. Click Save in the Node Details Web page to save the Node.

   The Node Saved Web page opens.

l. Click Transfer Now... to launch the Synchronize Configuration Files Web page.

m. Select the Servers from the Hostname column and click Start Sync.

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 Warm restarting the Signaling Server on page 203.

Warm restarting the Signaling Server

1. Select **System > IP Network > Maintenance and Reports** from the EM Navigator.
2. Select the node containing the Signaling Server to be restarted.
3. Click **Reset** for the Signaling Server.

Cold restart

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

Chapter 9: Overlap signaling

Contents

This section contains information on the following topics:

Overview

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

Note:

Overlap signaling is not supported using the Session Initiation Protocol (SIP).

Both overlap signaling and en bloc signaling is supported. The difference between overlap and en bloc signaling is as follows:

- In en bloc signaling, the switch waits for all digits of the called-party number from the user and then sends all the digits in a single SETUP message.
- In overlap signaling, the called-party digits are sent out as they are dialed from the user, instead of waiting for an interdigit timer to expire.

Note:

The interdigit timer starts when the user presses a digit key. The timer is restarted when the user presses the next digit key. Expiration of the timer indicates the end-of-dial (EOD).

In the H.323 network, dialed digits can be sent out or received in either en bloc (normal dialing) or overlap modes.

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

Using the H.323 protocol and IP Peer Networking, overlap signaling is supported over IP between:

- two or more CS 1000 systems running CS 1000 Release 4.0 (or later) on both nodes
- CS 1000 IP Peer systems running CS 1000 Release 4.0 (or later) and another gateway (either a Nortel or third-party gateway) supporting overlap signaling (provided the capability is enabled on the gateway)

Figure 113: Network diagram on page 207 shows a network diagram with overlap signaling.

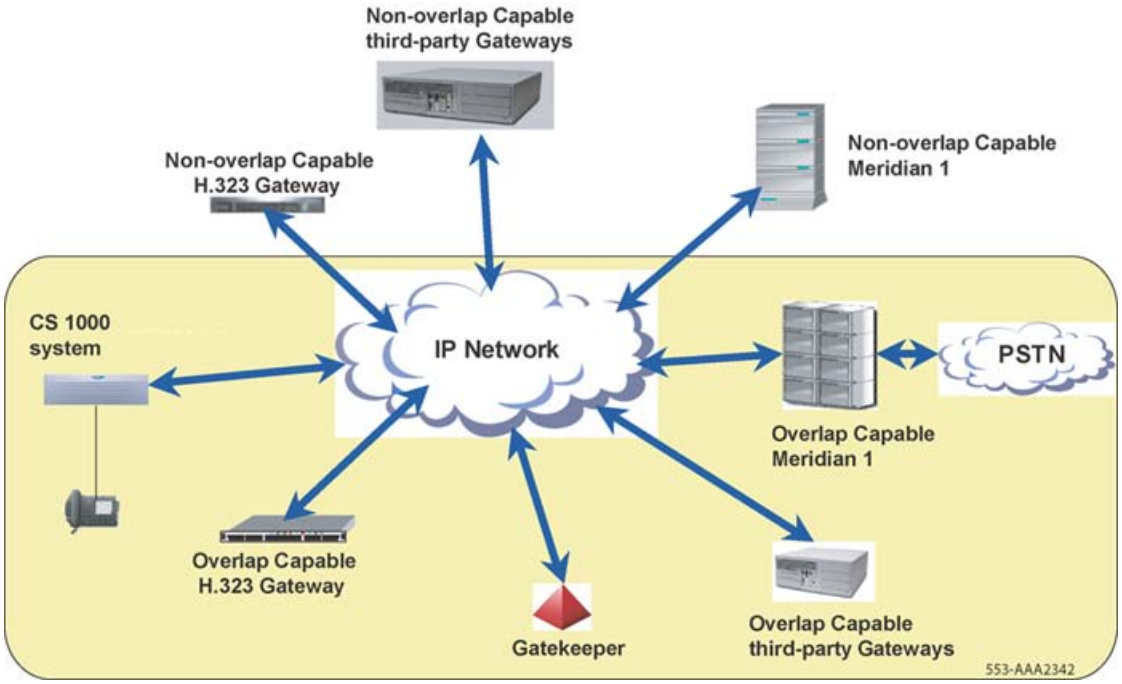

Figure 113: Network diagram

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 on page 317.

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 114: Changing an overlap-capable endpoint to an en bloc endpoint on page 211 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.'

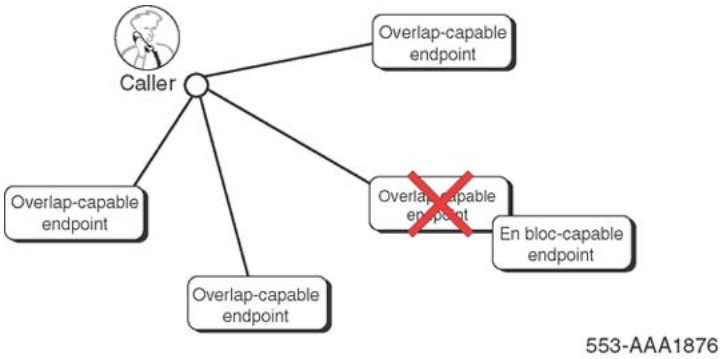

Figure 114: Changing an overlap-capable endpoint to an en bloc endpoint

For efficiency, configure another RLI as en bloc in LD 86 to change that endpoint from overlap signaling-capable to en bloc:

1. In LD 86, define a new RLI.
2. Configure the Overlap Length (OVLL) prompt to 0.

   Note:

   The OVLL prompt determines the number of digits required before the SETUP message is sent. If OVLL = 0, then all the dialed digits are sent in the SETUP message and the call is an en bloc call (even if LD 17 is configured for overlap signaling).
3. Change the entries pointing to the destination (that just changed to en bloc) to use the new RLI. After all ESN and CDP code entries have been changed, you can then remove the overlap RLI.

Example: Assume that Location Code (LOC) 425 currently uses the overlap-capable RLI 21 to call an overlap node. If that node changes to en bloc, then the following changes must be made:

- In LD 86, define a new RLI (such as RLI 22) with OVLL configured to 0. (All other prompts in the RLI can be identical to the original RLI 21.)
- In LD 90, change the LOC 425 to use the new RLI 22.

Tandem overlap signaling support

In addition to supporting originating and terminating overlap calls, IP Peer Overlap Signaling also supports the following tandem scenarios:

- ISDN (en bloc/overlap) to IP Peer (H.323-overlap/en bloc)
- Non-ISDN (en bloc/overlap) to IP Peer (H.323-overlap/en bloc)
- IP Peer (H.323-overlap) to IP Peer (H.323-overlap/en bloc)
- IP Peer (H.323-overlap) to IP Peer (SIP)

Overlap signaling call flow

Any messaging after the Alerting message is identical to the en bloc call flow and is not repeated in this section.

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

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

1. User A on Call Server A dials the DN of User B on Call Server B. Call Server A collects the routing-prefix digits through the Terminal Proxy Server (TPS) on Signaling Server A. See Figure 115: User A dials User B on page 213.

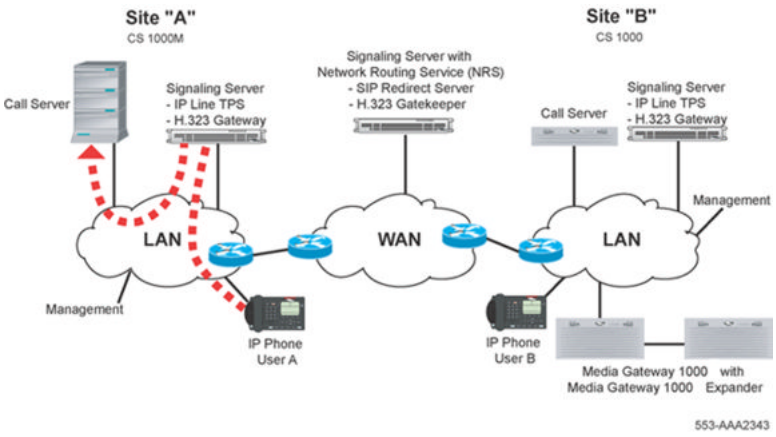

Figure 115: User A dials User B

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 116: Call Server A routes the call to the IP network on page 213.

   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).

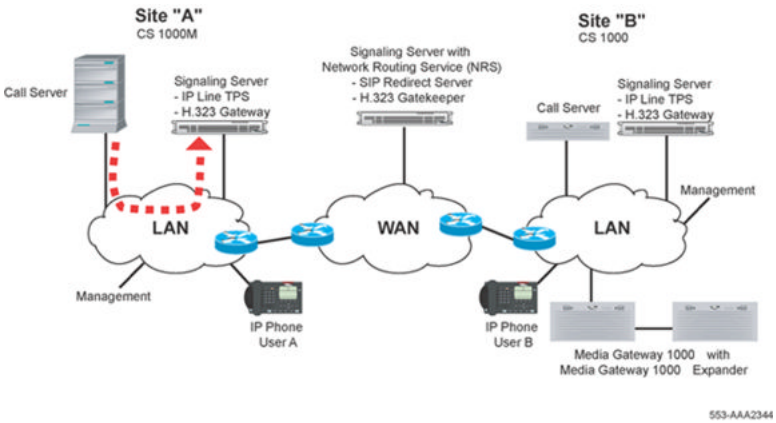

Figure 116: Call Server A routes the call to the IP network

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 117: The H.323 Gatekeeper sends the IP address of H.323 Gateway B to H.323 Gateway A on page 214.

   Otherwise, the NRS requests more digits.

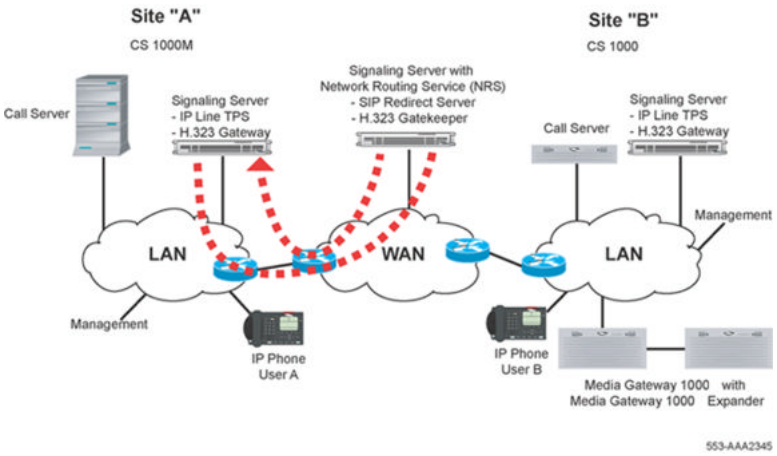

Figure 117: The H.323 Gatekeeper sends the IP address of H.323 Gateway B to H.323 Gateway A

4. User A dials an additional digit. The TPS forwards it to Call Server A. See Figure 115: User A dials User B on page 213.
5. Call Server A forwards the digits to H.323 Gateway A on the Signaling Server. See Figure 116: Call Server A routes the call to the IP network on page 213.
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 117: The H.323 Gatekeeper sends the IP address of H.323 Gateway B to H.323 Gateway A on page 214.

   Otherwise, the NRS requests more digits.

   Note:

   Until the call succeeds, step 4 on page 214, step 5 on page 214, and step 6 on page 214 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 118: H.323 Gateway A sends a SETUP message to H.323 Gateway B on page 215.

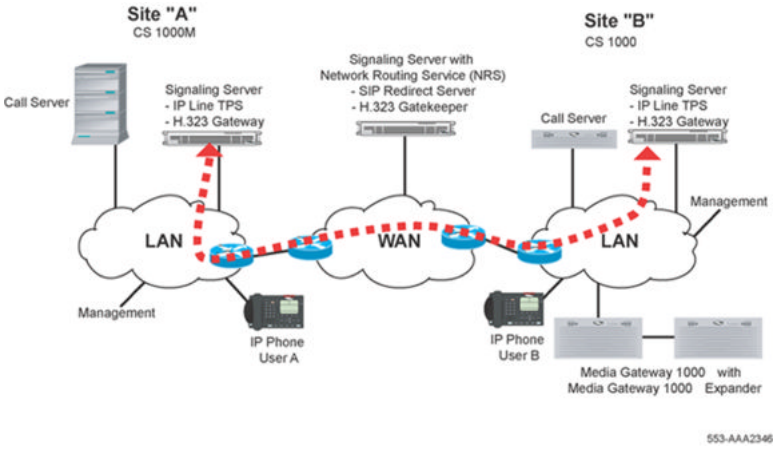

Figure 118: H.323 Gateway A sends a SETUP message to H.323 Gateway B

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 119: Gateway B sends the call to Call Server B over a Virtual Trunk on page 215.

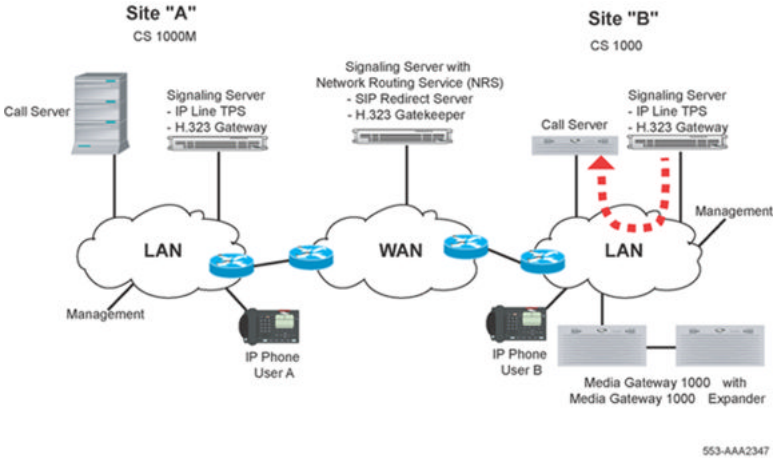

Figure 119: Gateway B sends the call to Call Server B over a Virtual Trunk

9. User A on Call Server A dials additional digits. See Figure 115: User A dials User B on page 213.
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 120: Call Server A sends digits to Call Server B on page 216.

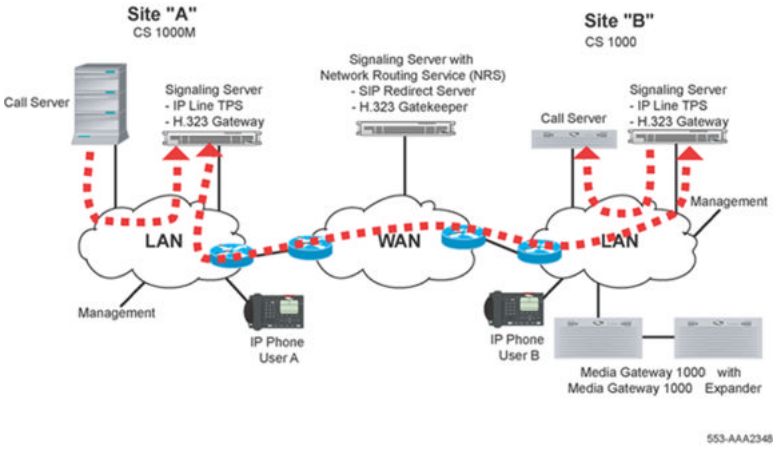

Figure 120: Call Server A sends digits to Call Server B

11. Call Server B selects the codec, allocates bandwidth, rings the telephone, and sends an alerting message to H.323 Gateway B. See Figure 121: Call Server B sends an alerting message to H.323 Gateway B on page 216.

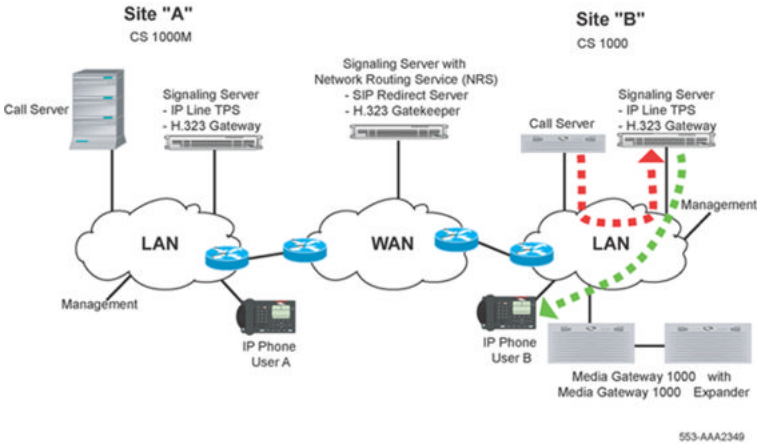

Figure 121: Call Server B sends an alerting message to H.323 Gateway B

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 122: H.323 Gateway B sends an alerting message to Call Server A on page 217.

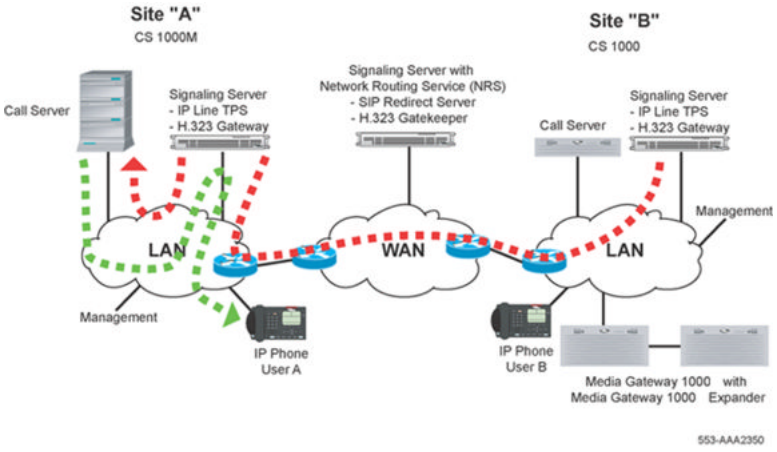

Figure 122: H.323 Gateway B sends an alerting message to Call Server A

13. User B answers the call. A message is sent to Call Server B through the TPS on the Signaling Server. See Figure 123: User B answers the call on page 217.

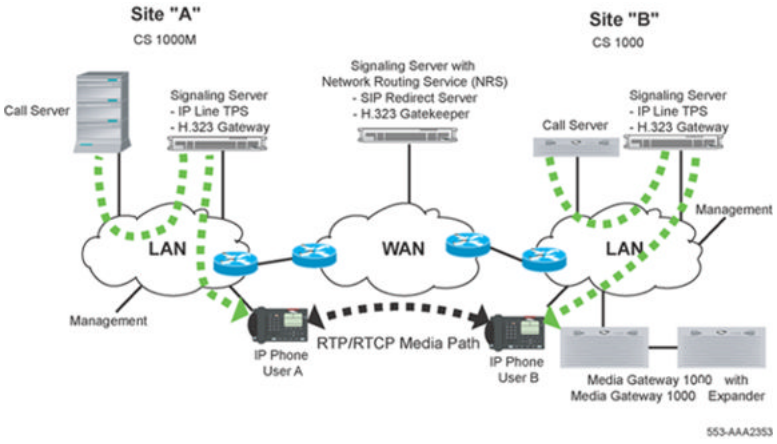

Figure 123: User B answers the call

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 124: Call Server B sends a CONNECT message to Gateway B and onto Call Server A on page 218.

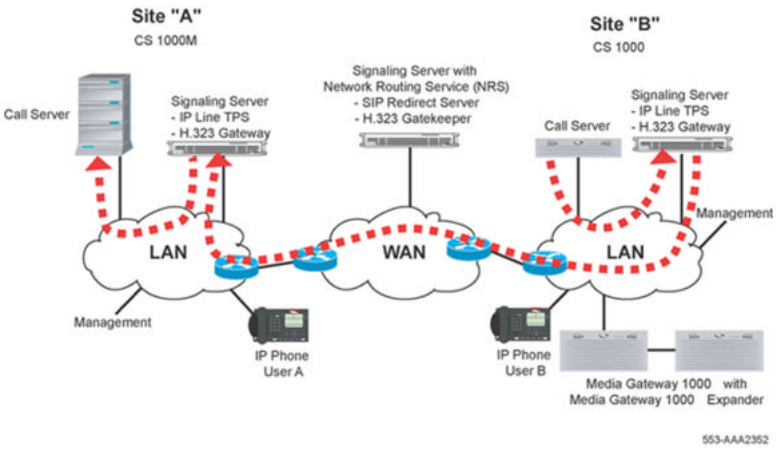

Figure 124: Call Server B sends a CONNECT message to Gateway B and onto Call Server A

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 125: IP Phones start the direct media paths on page 218.

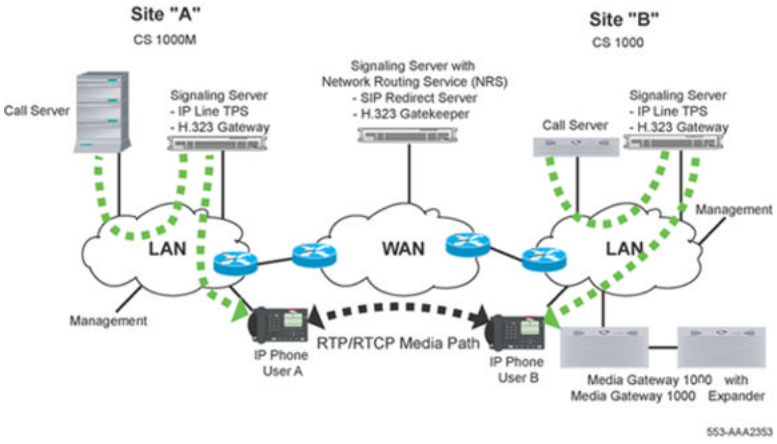

Figure 125: IP Phones start the direct media paths

Feature packaging

IP Peer Overlap Signaling requires the following packages:

- Overlap Signaling (OVLP) package 184
- H.323 Virtual Trunk (H323_VTRK) package 399

Note:
The packaging for H.323 includes the Overlap Signaling package.

Configuring overlap signaling on the Call Server

The following task summary list includes all the tasks required to configure IP Peer with overlap signaling. In particular, overlap signaling is configured using LD 17 and LD 86 as follows:

- Use LD 17 to configure the D-channel to support overlap signaling.
- Use LD 86 to configure the number of digits to be included in the SETUP message.

When configuring overlap signaling, the network must be optimized using a combination of the Overlap Length (OVLL) prompt in LD 86 and the Overlap Timer (OVLT) prompt in LD 17. Nortel recommends that:

- OVLL be configured to a reasonable length such that the Gatekeeper can resolve the called-party number with a minimum number of transactions
- OVLT be configured to 1 second

Warning:

When using SPNs to provide local, national, and international number handling, the incoming local, national, and international numbers are treated as en bloc. If the number was sent using overlap signaling, the call will always be incomplete.

If the Call Server receives an unknown type (CDP, LOC, or SPN) on an overlap capable D-channel, the Call Server processes the call as overlap. If it receives E.164 numbers, the Call Server treats them as North American formatted (and therefore, en bloc).

Task summary list

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

1. LD 17 – Configure D-channels to support overlap signaling.
2. LD 16 – Configure the H.323 route.
3. LD 86 – Configure the Route List Block for the Virtual Trunk route and configure the minimum number of digits included in the overlap signaling SETUP message.
4. LD 87 – Configure the CDP steering codes.
5. LD 90 – Configure E.164 plan call types and private plan Location Codes.
6. LD 90 – Configure Special Numbers.

Note:

Only the Overlays directly affected by the overlap signaling feature are included here.

Table 31: 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	dcip	Card Type 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 **Note:** OVLT applies only to Overlap Sending (OVLS = YES).

In the Route Data Block, the zone parameter makes the codec selections and calculates the bandwidth usage for calls to the trunk members of a given route.

Table 32: 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

Prompt	Response	Description
VTRK	yes	Virtual Trunk route, where: YES = This route is for Virtual Trunk NO = This route is not for Virtual Trunk (default)
ZONE	0-2550–8000	Zone for codec selection and bandwidth management
PCID	H323	Protocol ID for the H.323 route Defines the route as an H.323 route.
NODE	xxxx	Node ID Where the Node ID matches the node of the Signaling Server. The Node ID can have a maximum of four numeric characters.
ISDN	yes	Integrated Services Digital Network option
MODE		Mode of operation
	ISLD	Route uses ISDN Signaling Link (ISL) ISLD is allowed only if ISDN = YES, and the Integrated Services Digital Network Signaling Link (ISL) package 147 is equipped. ISLD is allowed only on ISA and TIE trunks.
DCH	0-159	D-channel number
IFC	sl1	Interface type for route (IFC responses are listed in *Software Input/Output: Administration (NN43001-611)*
SRVC	a...a	Service type for AT&T ESS connections (SRVC responses are listed in *Software Input/Output: Administration (NN43001-611*
PNI	(0)-32700	Private Network Identifier
NCNA	(YES)	Network Calling Name Allowed
NCRD	YES	Network Call Redirection
INAC	(NO) YES	Insert ESN Access Code Inserts the ESN access code in an incoming private network call. INAC enables an ESN access code to be automatically added to an incoming ESN call from a private network. If INAC = YES, then digit insertion (INST) for NARS or BARS calls is bypassed and Access Code 1 (AC1) is used for all call types. However, calls can be specifically defined to use Access Code 2 (AC2) in LD 15 at the AC2 prompt. INAC is prompted when the route type is either a TIE trunk or an IDA trunk with DPNSS1 signaling.
ICOG	IAO	Incoming and Outgoing trunk. Incoming and Outgoing
ACOD	x...x	Access Code for the trunk route.

Nortel recommends that all routes in a Route List Block (RLI) be configured as either overlap or en bloc. That is, an en bloc route should not have alternate routes that are configured as overlap, and vice versa. Erratic behavior can occur when overlap and en bloc routes are configured as alternate routes. Normal behavior occurs on alternate routes as long as the alternate route has the same overlap capabilities as the main route.

A warning message is displayed if alternate routes are configured as a different type from the main route.

Table 33: 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 0-255 0-1999	CDP and BARS NARS FNP
ENTR	xxx	Entry number for NARS/BARS Route list Where xxx = • 0-63 Entry number for NARS/BARS Route List • 0-6 Route list entry number for CDP • X Precede with x to remove
ROUT		Route number
	0-511	Range for Large System and CS 1000E system
	0-127	Range for Small System, Media Gateway 1000B, and Media Gateway 1000T **Note:** The route must be overlap capable.
...		
ENTR	<cr>	Entry number for NARS/BARS Route list
ISET	(0)-8	Initial Set Number of entries in Initial Set for route list block.
...		
OVLL	(0)-24	Overlap Length Number of digits required before the SETUP message is sent.

Prompt	Response	Description
		If OVLL = 0 then all the dialed digits are sent in a single SETUP message and the call is an en bloc call (even if LD 17 suggests overlap signaling). A value of x, where x is a 1 to 24, that x digits are required before sending the SETUP message. **Note:** Setting the OVLL to the expected digit string length (for example, OVLL = 7 when using seven-digit UDP) effectively forces en bloc. The SETUP message must have all seven digits before the message is sent. Therefore, the whole number is sent in the first message.

Table 34: 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	DSC TSC	Type of steering code Distant Steering Code 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 **Note:** See Flexible Length number of digits implications on page 227 for more information about FLEN.
TSC	x..x	Trunk Steering Code Up to 4 digits, up to 7 digits with Directory Number Expansion (DNXP) package 150.
- FLEN	(0)-24	Flexible Length number of digits **Note:** See Flexible Length number of digits implications on page 227 for more information about FLEN.

Table 35: LD 90 Configure E.164 plan call types and private plan Location Codes.

Prompt	Response	Description
REQ	NEW CHG	Create new data block Change existing data block
CUST	xx	Customer number as defined in LD 15.
FEAT	NET	Network Translator (Network translation tables)

Prompt	Response	Description
TRAN	AC1 AC2	Translator Access Code 1 (NARS/BARS) Access Code 2 (NARS)
TYPE	LOC	Type Location Code
LOC	xxx y..y	Location code, where xxx = home location code and y..y = extended code of 1-4 digits. The extended code is optional.
- FLEN	(0)-10	Flexible Length number of digits Enter the maximum number of digits expected. When this number of digits is dialed, dialing is considered to be complete and end-of-dial processing begins. Default is zero (0) digits. **Note:** See Flexible Length number of digits implications on page 227 for more information about FLEN.

Table 36: LD 90 Configure Special Numbers.

Prompt	Response	Description
REQ	NEW CHG	Create new data block Change existing data block
CUST	xx	Customer number as defined in LD 15.
FEAT	NET	Network Translator (Network translation tables)
TRAN	AC1 AC2	Translator Access Code 1 (NARS/BARS) Access Code 2 (NARS)
TYPE	SPN	Type Special Number Translation
SPN	xxx	Special Number translation 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. The maximum number of groups allowed is 5.
- FLEN	(0)-24	Flexible Length number of digits Enter the maximum number of digits expected. When this number of digits is dialed, dialing is considered to be complete and end-of-dial processing begins. Default is zero (0) digits. **Note:** See Flexible Length number of digits implications on page 227 for more information about FLEN.

Configuring overlap signaling using Element Manager

To configure a D-channel to support overlap signaling, follow the steps in Configuring D-channels to support overlap signaling on page 225.

Configuring D-channels to support overlap signaling

1. Log in to CS 1000 Element Manager.
2. Select **Routes and Trunks > D-Channels** from the EM Navigator.

   The D-Channel Web page opens.
3. Click the **Edit** button associated with the D-channel.

   The D-Channel xx Property Configuration Web page opens where xx is the D-channel number.
4. Choose **Advance Options (ADVOPT)**.
5. Choose **H.323 Overlap Signaling Settings (H323)** (see Figure 126: H.323 Overlap Signaling on page 225).
   a. Select the **Overlap Receiving (OVLR)** check box.
   b. Select the **Overlap Sending (OVLS)** check box.
   c. Select a timer value (in seconds) from the **Overlap Timer (OVLT)** drop-down list.

Figure 126: H.323 Overlap Signaling

6. Click **Submit**.

To configure the number of digits required before the SETUP message is sent, follow the steps in Configuring the minimum number of digits included in the SETUP message on page 225.

Configuring the minimum number of digits included in the SETUP message

1. Refer to Configuring the Route List Block on page 153.
2. Enter a value for **Overlap Length (OVLL)**.

   If OVLL = 0 (the default), then all the dialed digits are sent in a single SETUP message and the call is an en bloc call (even if Configuring D-channels to support overlap signaling on page 225/LD 17 suggests overlap signaling). A value of x, where x is 1-24, indicates that x digits are required before sending the SETUP message.

Note:

Setting the OVLL to the expected digit string length (for example, OVLL = 7 when using seven-digit UDP) effectively forces en bloc. The SETUP message must have all seven digits before the message is sent. Therefore, the whole number is sent in the first message.

Overlay changes for overlap signaling

LD 17 displays the H323 prompt is displayed for a D-channel over IP (type DCIP). The H323 prompt has three key prompts, OVLR, OVLS, and OVLT, that are provided for an H.323 D-channel.

Note:

This prompt sequence is displayed only for a D-channel of type DCIP if the H.323 Virtual Trunk (H323_VTRK) package 399 and Overlap Signaling (OVLP) package 184 are enabled. Otherwise, the OVLR, DIDD, OVLS, and OVLT prompt sequence is displayed.

The user must configure OVLS, OVLR, and OVLT in LD 17 in order for overlap signaling to work.

Note:

The D-channel must be disabled before modifying the OVLR and OVLS prompts. The OVLR and OVLS data must be transmitted to the Signaling Server. This occurs only when the D-channel is enabled.

- If the Call Server is to send overlap calls over IP, then Overlap Sending (OVLS) must be configured as YES. This setting turns on overlap sending from the Call Server to the IP domain.
- If the Call Server is to receive overlap calls over IP, then Overlap Receiving (OVLR) must be configured as YES. This setting turns on overlap signaling from the IP domain to the Call Server.
- The Overlap Timer (OVLT) prompt only has meaning for Overlap Sending (OVLS = YES). The OVLT value indicates the time the system waits to accumulate digits to send in an INFORMATION message after the SETUP message is sent. The valid values for OVLT are 0-8 where:
  - A value of 0 results in the generation of an INFORMATION message for every digit dialed after the minimum overlap called number length (as provisioned in LD 86 for the RLI).
  - A value of 1 is the default value for a D-channel over IP.

In LD 86, a warning is issued if a mixture of IP capable overlap routes and en bloc capable routes exist in an RLI. The warning is also issued if an en bloc IP route coexists with overlap capable routes. The warning is displayed only at the Call Server login window. It is not transmitted to Element Manager.

The use of the Flexible Length number of digits (FLEN) prompt has changed (in LD 87 and LD 90) for overlap signaling but has not changed for en bloc.

With IP Peer overlap signaling calls, the usage of the FLEN prompt is changed as follows:

- If FLEN = 0, then (in general) overlap handling has not changed. The SETUP message is sent once the OVLL digits are received and the dialing plan entry can be determined. However, the end-of-dial timer starts, and on expiration, the Call Server sends an INFORMATION message with Sending Complete to indicate end-of-dial.
- If FLEN is greater than 0 and also greater than both of the following:

  - the length of the digit string provisioned in LD 87 or LD 90, and

  - the OVLL value,

  then overlap signaling meets the two requirements for the SETUP message. After that, further digits are sent in the INFORMATION messages. In addition, for IP overlap signaling, when the value configured for FLEN is reached, the INFORMATION message carrying the digits also carries the Sending Complete Information Element (IE).

Note:

An IE is a unit of information in Q.931 and H.323 messaging.

If FLEN is less than OVLL, then the SETUP message is sent immediately. To ensure that the Signaling Server does not wait for more digits, the SETUP message also includes the Sending Complete IE.

With en bloc calls, the usage of the FLEN prompt is as follows:

- If FLEN is a non-zero value, then the Call Server collects digits until the total count of collected digits equals FLEN. The Call Server then sends a SETUP message.
- If FLEN = 0, then the Call Server uses an end-of-dial timer to determine when it has a completed number. The Call Server collects digits, restarting the end-of-dial timer after each digit, and waits for the timer to expire to send the SETUP message.

Flexible Length number of digits implications

A non-zero FLEN value indicates the number of digits the system should expect for the current number type and plan entry. When the digits collected reach the expected length, the system sends an end-of-dial indication to the remote switch. A value of 0 means the length is unknown and FLEN = 0 has a specific impact on the system.

En bloc dialing handles an unknown length by using an end-of-dial timer. It uses the end-of-dial timer to decide how many digits it must collect. When the timer expires, all received digits are sent in the SETUP message.

When PRI uses overlap signaling and FLEN = 0, the network relies on the remote switch to determine the correct length. The originating switch can use overlap signaling to send the digits once the OVLL and dialing plan entry requirements are met.

For IP, however, the remote switch may be one of many devices (for example, a CS 1000 system, an H.323 gateway, or a Business Communications Manager (BCM) node). The remote

switch may also be overlap- or en bloc-capable. An overlap call to an overlap destination is not an issue. However, an en bloc destination requires overlap-to-en bloc conversion, which in turn requires knowledge of when a digit string is completed. Therefore, for overlap signaling on IP Peer to perform overlap-to-en bloc conversion with a FLEN of 0, the system must know when the digit string ended. As a result, unlike the PRI overlap-signaling case, when the end-of-dial timer expires (for an IP overlap signaling call) the Call Server sends a Sending Complete IE in the INFORMATION message to indicate end-of-dial.

Nortel recommends that all numbers with a known length set FLEN equal to the length of the digit string. For example, if all Location Codes (LOC) are eight digits in length, then use FLEN = 8 for all LOC codes. However, when the destination is unknown, use FLEN = 0. This process provides full overlap capability to an overlap-enabled destination, while providing the end-of-dial indication to allow interworking with an en bloc destination.

Note:
Dialing the octothorpe (#) forces an immediate end-of-dial, so the Call Server immediately provides end-of-dial treatment.

System log messages

The Signaling Server has a log file. A system log message is issued to this log file when the Signaling Server detects an incoming H.323 overlap signaling call that must revert to en bloc.

This system log message is output no more than once every hour. The message indicates the number of occurrences of overlap-to-en bloc conversion since the last system log message. No output is generated during a period in which no overlap-to-en bloc conversion occurred.

Chapter 10: IP Peer Interworking with Multimedia Communication Server 5100 (MCS 5100)

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)* .

Chapter 11: IP Peer Interworking with CallPilot 2.02

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)*

Chapter 12: IP Peer Interworking with BCM

This chapter describes the planning, configuration, testing, and troubleshooting of the integration of the Business Communications Manager (BCM) with a Communication Server 1000 system. Only integrate the CS 1000 and BCM systems when both systems have been installed and a baseline of operation has been achieved and tested.

The following systems and software releases are covered in this chapter:

- Communication Server 1000 (CS 1000) Release 6.0 or later
- Business Communications Manager 200 (BCM 200) Release 4.0
- Business Communications Manager 400 (BCM 400) Release 4.0
- Business Communications Manager 450 (BCM 450) Release 1.0
- Business Communications Manager 450 (BCM 450) Release 5.0
- Business Communications Manager 50 (BCM 50) Release 3.0
- Business Communications Manager 50 (BCM 50) Release 5.0

Overview

An example of a Communication Server 1000/Business Communications Manager (BCM) systems integration is shown in Figure 127: CS 1000/BCM architecture on page 234.

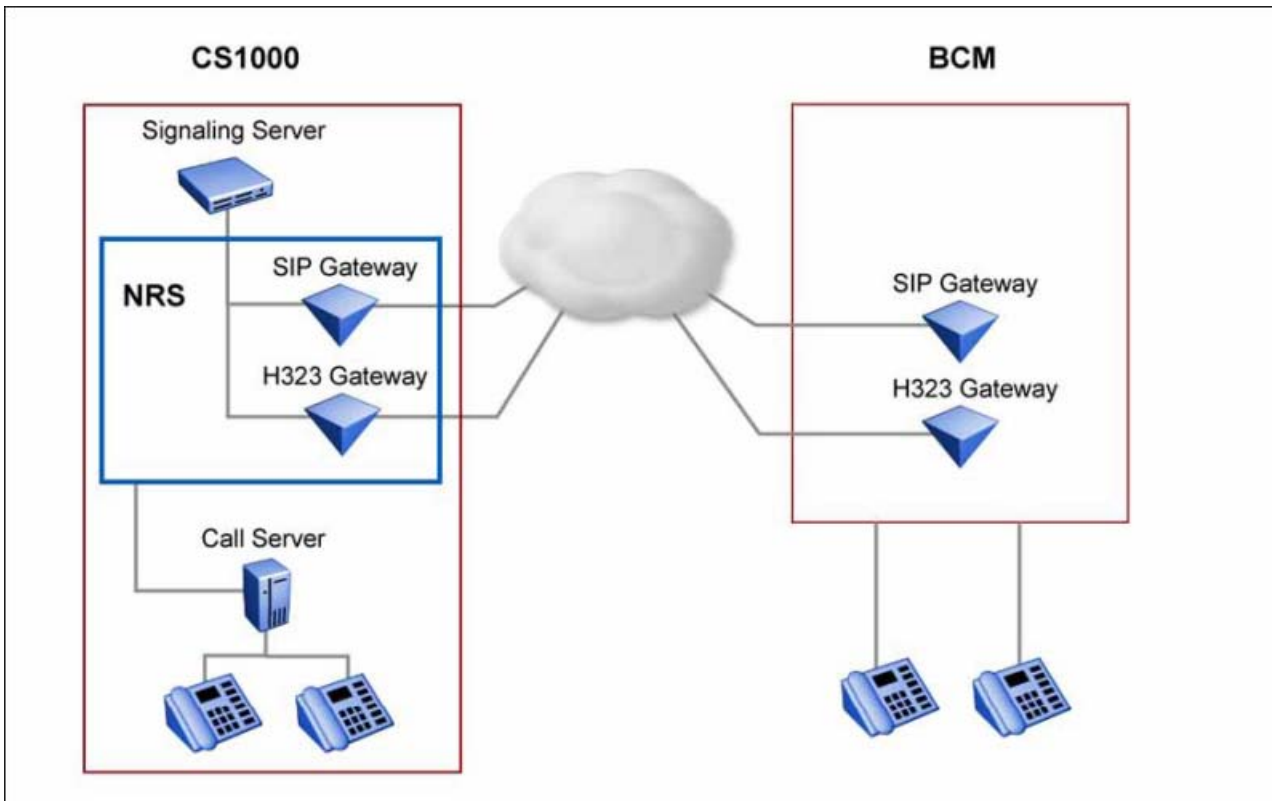

Figure 127: CS 1000/BCM architecture

CS1000 Gateway IP address	10.10.11.1	
CS1000 Endpoint IP address	10.12.12.3	
BCM 400 Endpoint IP address	10.20.12.8	BCM Gateway Alias name BCM40
Signaling Server T-LAN IP Address	10.12.13.1	
Signaling Server E-LAN IP Address	10.12.13.2	
Call Server E-LAN IP Address	10.12.12.3	
NRS IP Address	10.10.12.2	NRS Host name CS1000E_PIV
NCS IP Address	10.10.12.3	
BCM IP Address	10.26.12.9	

Figure 128: CS 1000/BCM integration process on page 235 shows the sequence of procedures you perform to integrate the CS 1000 and BCM systems.

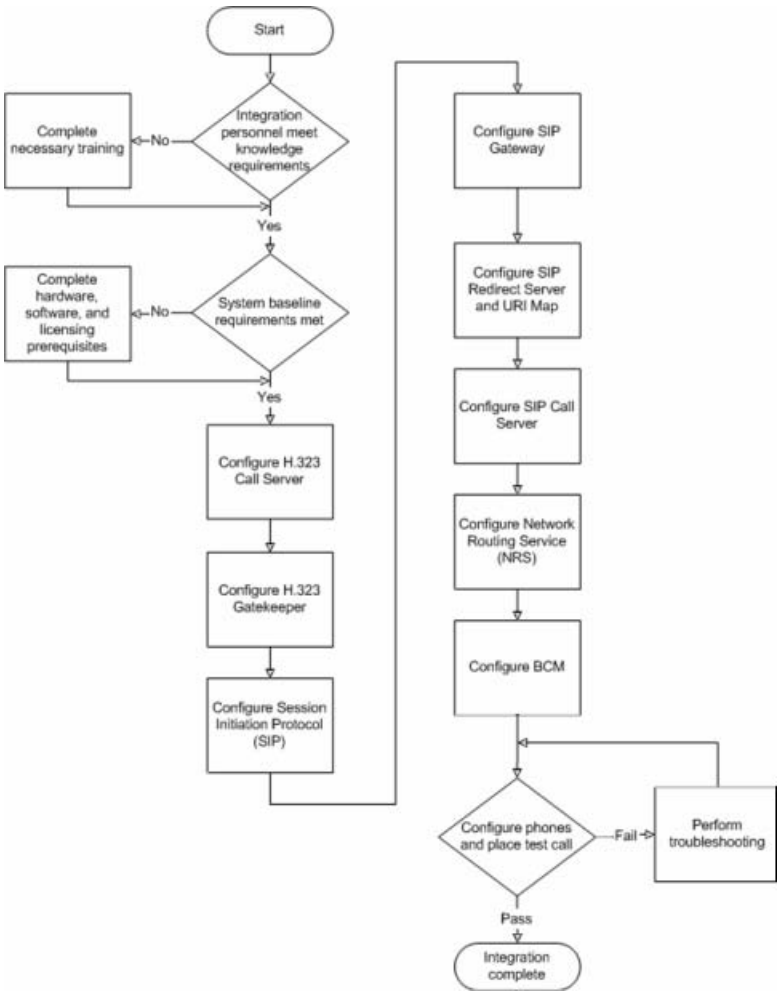

Figure 128: CS 1000/BCM integration process

The tasks in the CS 1000/BCM systems integration process are listed in Table 37: Task Completion Checklist on page 235. Use this checklist to implement the integration.

Table 37: Task Completion Checklist

Task	Reference
Configure the H.323 Call Server See Configure IP Peer Network on page 129	
Configure the H.323 Gatekeeper See Configure IP Peer Network on page 129	
Configure the SIP protocol See Configure IP Peer Network on page 129	
Configure the SIP Gateway	

Task	Reference
See Configure IP Peer Network on page 129	
Configure the SIP Redirect Server and URI Map See Configure IP Peer Network on page 129	
Configure the SIP Call Server See Configure IP Peer Network on page 129	
Configure NRS **Note:** For information about configuring NRS, see *Network Routing Service Fundamentals, NN43001-130*.	
Configure BCM	

Prerequisites

Before you begin to integrate the Communication Server 1000 (CS 1000) and Business Communications Manager (BCM) systems, ensure that you complete the following prerequisites:

- Knowledge requirements
- Capturing integration parameters
- Establishing the system baseline

Knowledge requirements

The following knowledge and skills are required to implement a CS 1000/BCM systems integration:

- basic programming and provisioning skills for the CS 1000 system
- basic programming and provisioning skills for Network Routing Service (NRS)
- basic programming and provisioning skills for BCM systems
- working knowledge of various operating systems, including VxWorks, Unix, Linux, and Windows
- principles of Voice over IP (VoIP) protocols

- networking principles
- knowledge of core data components

Training

Nortel recommends that you complete product-specific training before you begin integrating the CS 1000 and BCM systems. Training includes course 6034C, “CS 1000 BCM Multi-site Integration”, which deals specifically with the CS 1000/BCM integration and multi-site BCM integration processes. A complete list of courses is available at http://www.avaya.com

Capturing integration parameters

Table 38: Integration parameters on page 237 provides a list of parameters required to successfully complete the integration. Record these parameters during the initial planning phase of the integration.

Table 38: Integration parameters

Parameter	Value
User IDs and passwords	
SIP Gateway endpoint authentication password (must match the NRS password)	
IP addresses and URLs	
Gatekeeper IP address	
Alternate Gatekeeper IP address (optional)	
TLAN IP address of the Signaling Server	
TLAN IP address of the alternate Signaling Server	
Primary SIP proxy address	
Alternate SIP proxy address	
Primary NCS IP address	
Alternate NCS IP address)	
Static endpoint IP address (same as the Node IP address)	
Collaborative server IP address	
Names	

Parameter	Value
Service domain name in NRS	
SIP domain name (must be the same as the service domain name)	
SIP Gateway endpoint name (must match the NRS user ID)	
L0 domain name	
L1 domain name	
H.323 ID (preferable if it is the same as the one in the Primary Signaling Server)	
H.323 Gatekeeper alias name (default is the H.323 ID)	
Endpoint alias for BCM	
Read and write community names	
Miscellaneous	
Coordinated Dialing Plan steering codes	
SIP access port to use (port 5060 is recommended)	

Establishing the system baseline

To successfully integrate voice services, you must first establish the system baseline for the Call Server, Signaling Server, and Business Communications Manager (BCM) so that the systems are configured and working in a stand-alone environment.

Use Table 39: Pre-integration checklist on page 238 to complete system baselines prior to integration.

Table 39: Pre-integration checklist

Task	Reference	Comments
The Enterprise software package is purchased and installed, with appropriate licenses for virtual trunks, lines, and IP Phones as required.		
The Network Numbering Plan is implemented.	*Dialing Plans: Description* (NN43001-283)	Are you using a Uniform Dialing Plan (UDP) or a

Task	Reference	Comments
		Coordinated Dialing Plan (CDP), or both? Are you also using a Group Dialing Plan (GDP), a North American Numbering Plan (NANP), or a Flexible Numbering Plan (FNP)?
CS 1000 software is Release 6.0 or later.		To check the CS 1000 software release: Log on, enter LD 22, and type PRT ISS. OR 1 Log on to Element Manager. 2 On the left navigation pane, select Home. The System Overview page appears. 3 The software release is referred to as Release.
Signaling Server software		The Signaling Server software should be the most recent GA release compatible with your Call Server software version. To check the software release of the Signaling Server: 1 Log on to Element Manager. 2 On the left navigation pane, select Home. The System Overview page appears. 3 Refer to the Signaling Server Details section for the Software Version.
Basic installation, setup, and configuration of the Call Server components and the Signaling Server are complete.	*Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (NN43021-310) *Communication Server 1000E: Installation and Configuration* (NN43041-310) *Signaling Server IP Line Applications Fundamentals* (NN43001-125)	

Task	Reference	Comments
Primary, alternate, and fail-safe Network Routing Service (NRS) are configured at installation and initial setup of the Signaling Server.	*Signaling Server IP Line Applications Fundamentals* (NN43001-125)	The NRS requires IP telephony node configuration files. These files are installed and configured during the Signaling Server software installation as a basic configuration step.
Digital Data Block configuration is complete in LD 73.	*IP Peer Networking Installation and Configuration Guide* (NN43001-313)	To configure a Digital Data Block: 1 Connect to the Call Server. 2 Enter LD 73. 3 Enter NEW. 4 Enter DDB. 5 Press Enter to accept all defaults. 6 Perform a data dump.
PTI or DTI trunks (DLOP) configuration is complete in LD 17.	*IP Peer Networking Installation and Configuration Guide* (NN43001-313)	To check PTI or DTI trunks: 1 Log on to Element Manager. 2 Select Routes and Trunks > Digital Trunk Interface. 3 Select Digital Trunk Interface Data Block (DDB). 4 Check that the configuration is complete.
A basic node is configured in Element Manager.	*Signaling Server IP Line Applications Fundamentals* (NN43001-125)	This node information is updated through the integration process.
Voice Gateway Media Card configuration is complete if IP to PSTN translation is required.		To check that Media Gateway Cards are installed: 1 Log on to Element Manager. 2 On the left side navigation pane, expand the System tab. 3 Expand the Software tab. 4 Select Voice Gateway Media Card. The Voice Gateway Media Card (VGMC) Loadware Upgrade page appears. 5 Select Open all nodes. Attention: The servers and Media Cards installed and configured are listed under each node. Any installed

Task	Reference	Comments
		Voice Gateway Media Card is listed under Type.
H.323 Virtual Trunk package 399 is installed.		To check that the package is loaded: 1 Connect to the Call Server. 2 Log on to the Signaling Server. 3 Enter LD 22. 4 Enter PRT. 5 Enter PKG 399. 6 The package is loaded if you do not receive a “package is restricted” message.
IPT is Release 3.0 or newer if you are using IP Trunk cards.		To check that IPT Trunk cards are installed: 1 Log on to Element Manager. 2 On the left navigation pane, expand the IP Network tab. 3 Select Nodes: Servers, Media Cards. 4 Expand the appropriate Node. Attention: The servers and Media Cards installed and configured are listed under each node. Any installed IPT Trunk cards are listed under Type.
BCM configuration is complete and passing data traffic.		
BCM networking hardware is installed for integration.		To check the installed hardware: 1 Log on to Element Manager. 2 Select the Administration tab. 3 Expand the General folder. 4 Select Hardware Inventory. 5 Select the PCI cards tab. The cards installed in BCM are listed.

Task	Reference	Comments
PEC III Media Service Cards (MSC) are later.		PECIII MSCs are required for T.38 Fax and IP telephony. To check the PEC hardware: 1 Log on to Element Manager. 2 Select the Administration tab. 3 Expand the General folder. 4 Select Hardware Inventory. 5 Select the PCI cards tab. 6 Select the MSC PCI card and scroll down to the Details for Card section.
BCM 200/400 is Release 4.0. BCM50 is Release 2.0, 3.0, or 5.0. BCM450 is Release 1.0 or 5.0.		To check the software version: 1 Log on to Element Manager. 2 Select the Configuration tab. 3 Expand the System folder. 4 Select Identification.
VoIP Gateway Trunk licensing is purchased and loaded on BCM.	*Keycode Installation Guide* (NN40010-301)	To check Feature Licenses: 1 Log on to Element Manager. 2 Select the Configuration tab. 3 Expand the System folder. 4 Select Keycodes.
IP Client licensing is purchased and loaded on BCM.	*Keycode Installation Guide* (NN40010-301)	To check Feature Licenses: 1 Log on to Element Manager. 2 Select the Configuration tab. 3 Expand the System folder. 4 Select Keycodes.
MCDN feature licensing is purchased and loaded on BCM.	*Keycode Installation Guide* (NN40010-301)	To check Feature Licenses: 1 Log on to Element Manager. 2 Select the Configuration tab. 3 Expand the System folder. 4 Select Keycodes.

BCM configuration to integrate with a CS 1000 system prior to Release 5.0

The following details the steps to integrate a Business Communications Manager (BCM) prior to Release 5.0 with a Communication Server 1000 system.

- BCM 200/400 configuration on page 243
- BCM 50/450 configuration prior to Release 5.0 on page 264

BCM 200/400 configuration

This section describes configuration procedures for the Business Communications Manager (BCM) 200 and 400 systems.

Note:
The Element Manager referred to in this section is the BCM Element Manager.

BCM Element Manager as viewed on your system may differ slightly from the screens shown in this chapter because you can customize the column display in BCM Element Manager.

BCM 200/400 configuration procedures

The sequence of BCM 200/400 configuration procedures is as follows:

- BCM 200/400 configuration procedures
- Verifying system license and keycodes on page 244
- Configuring VoIP trunk media parameters on page 245
- Configuring local Gateway parameters on page 249
- Configuring target lines on page 255
- Configuring VoIP lines on page 259

Configuring incoming VoIP trunks

Perform the following procedure to configure incoming VoIP trunks.

Configuring incoming VoIP trunks

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select System > Keycodes.
4. Select System > Keycodes. See Figure 129: Keycodes on page 244.

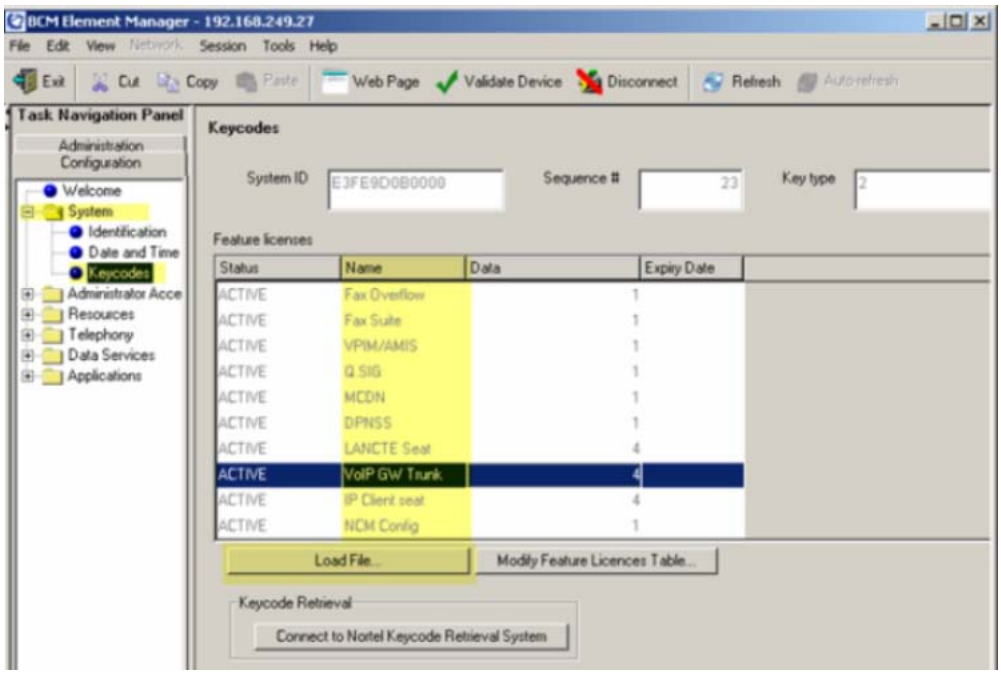

Figure 129: Keycodes

5. Load new Keycodes by loading a new keycode file or connecting to Nortel's Keycode Retrieval System (KRS). For more information about keycodes and keycode retrieval, see *Keycode Installation Guide* (NN40010-301).

Verifying system license and keycodes

Perform the following procedure to verify system license and keycodes.

Verifying system license and keycodes

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select System > Keycodes. See Figure 129: Keycodes on page 244 .
4. In the Name column, scroll down to VoIP GW Trunk. The number of license keys you have are listed in the Data column.

Configuring VoIP trunk media parameters

Perform the following procedure to configure VoIP trunk media parameters.

Configuring VoIP trunk media parameters

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select Resources > Telephony Resources. See Figure 130: Telephony Resources on page 245.

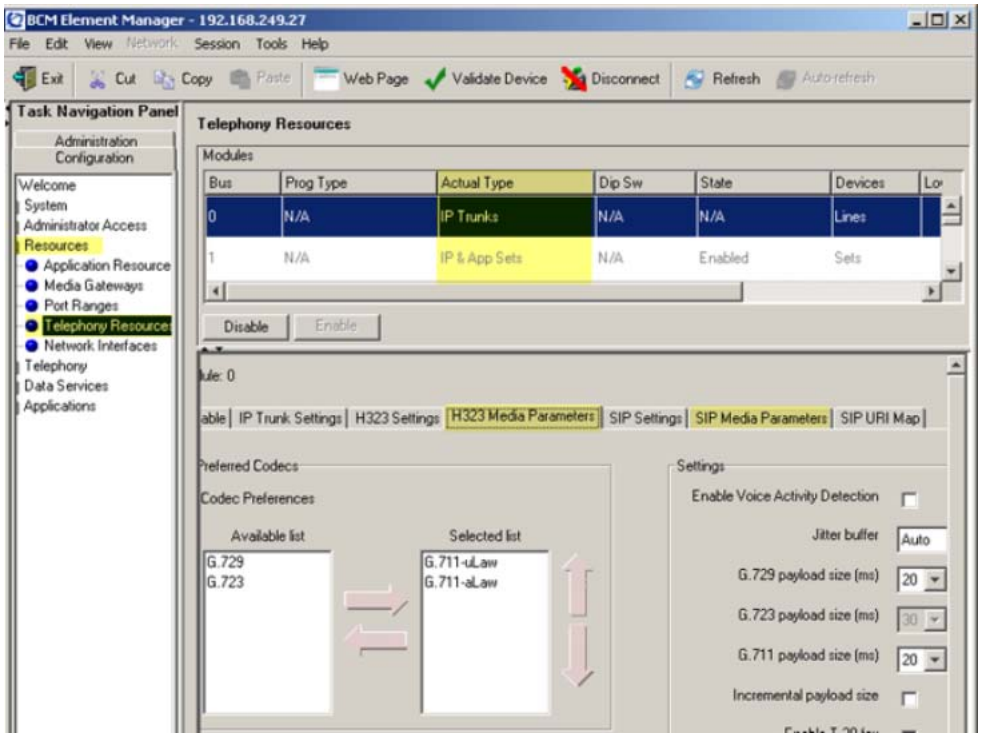

Figure 130: Telephony Resources

4. In the Modules panel, select the line where the Module Type column is set to IP Trunks.
5. Select the H.323 Media Parameters or SIP Media Parameters tab.
6. Enter the information that supports your system. Ensure that these settings are consistent with the other systems on your network. Refer to Table 40: H.323 Media Parameters fields on page 246 and Table 41: SIP Media Parameters fields on page 247 for a description of the parameters.

The following table describes the H.323 Media Parameters fields.

Table 40: H.323 Media Parameters fields

Field	Value	Description
Preferred Codecs	G.711 -muLaw G.711 -aLaw G.729 G.723	Add codecs to the Selected list and order them in the order in which you want the system to attempt to use them. The system attempts to use the codecs in top-to-bottom sequence. Performance note: Codecs on all networked BCMs must be consistent to ensure the proper functionality of interacting features such as Transfer and Conference. Systems running BCM Release 3.5 or later allow codec negotiation and renegotiation to accommodate inconsistencies in codec settings over VoIP trunks.
Enable Voice Activity Detection	<check box>	Voice Activity Detection (VAD), also known as silence suppression, identifies periods of silence in a conversation and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. If VAD is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support VAD. G. 711 does not support VAD. Performance note: VAD on all networked BCMs and IPT systems must be consistent to ensure functionality of features such as Transfer and Conference. The Payload size on the IPT must be set to 30ms.
Jitter Buffer	Auto None Small Medium Large	Select the size of jitter buffer for your system. Note: Slower networks require larger Jitter Buffers to decrease voice break up, but increase end-to-end delay.
G.729 payload size (ms) G.723 payload size (ms) G.711 payload size (ms)	10,20,30,40,50,60 30 10,20,30,40,50,60	Set the maximum required payload size, per codec, for the VoIP calls sent over SIP trunks. Note: Payload size can also be set for Nortel IP telephones. See *BCM50 Networking Configuration Guide* (NN40020-603).
Incremental payload size	<check box>	When enabled, the system advertises a variable payload size (40, 30, 20, 10 ms).
Enable T.38 fax	<check box>	When enabled, the system supports T.38 fax over IP. Caution: Fax tones broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. To minimize the possibility of your VoIP calls being dropped due to fax tone interference:

Field	Value	Description
		• place the fax machine away from other telephones • turn the fax machine's speaker volume to the lowest level, or off, if available
Force G.711 for 3.1k Audio	<check box>	When enabled, the system forces the VoIP trunk to use the G.711 codec for 3.1k audio signals, such as modem or TTY machines. Note: You also can use this setting for fax machines if T.38 fax is not enabled on the trunk.

The following table describes the SIP Media Parameters fields.

Table 41: SIP Media Parameters fields

Field	Value	Description
Preferred Codecs	G.711 -muLaw G.711 -aLaw G.729 G.723	Add codecs to the Selected list and order them in the order in which you want the system to attempt to use them. The system attempts to use the codecs in a top-to-bottom sequence. Performance note: Codecs on all networked BCMs must be consistent to ensure the proper functionality of interacting features such as Transfer and Conference. Systems running BCM Release 3.5 or later allow codec negotiation and renegotiation to accommodate inconsistencies in codec settings over VoIP trunks.
Enable Voice Activity Detection	<check box>	Voice Activity Detection (VAD), also known as silence suppression, identifies periods of silence in a conversation and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is

Field	Value	Description
		listening. If VAD is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support VAD. G.711 does not support VAD. Performance note: VAD on all networked BCMs and IPT systems must be consistent to ensure functionality of features such as Transfer and Conference. The Payload size on the IPT must be set to 30ms.
Jitter Buffer	Auto None Small Medium Large	Select the size of jitter buffer for your system. Note: Slower networks require larger Jitter buffers to decrease voice break up, but increase end-to-end delay.
G.729 payload size (ms) G.723 payload size (ms) G.711 payload size (ms)	10,20,30,40,50,60 30 10,20,30,40,50,60	Set the maximum required payload size, per codec, for the VoIP calls sent over SIP trunks. Note: Payload size can also be set for Nortel IP telephones. See *BCM50 Networking Configuration Guide* (NN40020-603).
Enable T.38 fax	<check box>	When enabled, the system supports T.38 fax over IP. Caution: Fax tones broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. To minimize the possibility of your VoIP calls being dropped due to fax tone interference: • place the fax machine away from other telephones • turn the fax machine's speaker volume to the

Field	Value	Description
		lowest level, or off, if available

Configuring local Gateway parameters

Perform the following procedure to configure local Gateway parameters.

Configuring local Gateway parameters

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select Resources > Telephony Resources.
4. In the Modules panel, select the line in which the Module Type column is set to IP Trunks. See Figure 130: Telephony Resources on page 245.
5. Select the IP Trunk Settings tab and enter the information that supports your system. See Figure 131: IP Trunk Settings on page 249. Refer to Table 42: IP Trunk Settings fields on page 249 for information about the IP Trunk Settings fields.

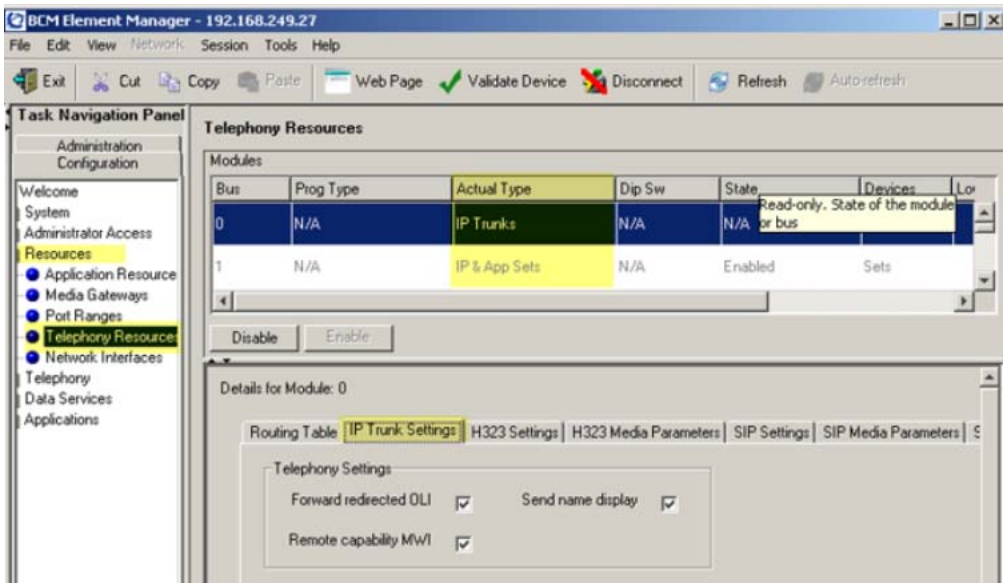

Figure 131: IP Trunk Settings

Table 42: IP Trunk Settings fields

Field	Value	Description
Forward redirected OLI	<check box>	If enabled, the OLI of an internal telephone is forwarded over the VoIP

Field	Value	Description
		trunk when a call is transferred to an external number over the private VoIP network. If disabled, only the CLID of the transferred call is forwarded.
Send name display	<check box>	If enabled, the telephone name is sent with outgoing calls to the network.
Remote capability MWI	<check box>	This setting must coordinate with the functionality of the remote system hosting remote voice mail.

6. For H.323 VoIP trunks, select the H.323 Settings tab. See Figure 132: H.323 Settings on page 251.

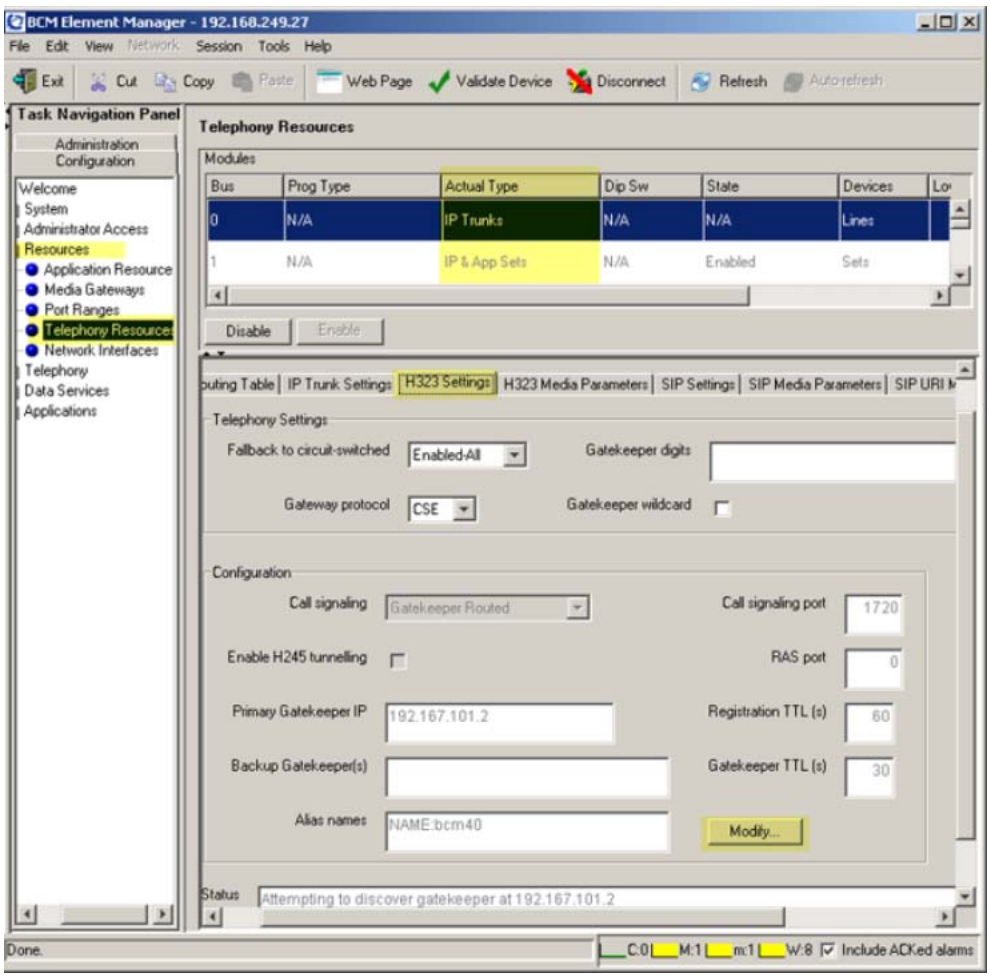

Figure 132: H.323 Settings

7. When implementing your dialing plan, in the H.323 Settings tab, select a value for Fall back to circuit-switched. This determines how the system handles calls if the IP network cannot be used.
8. For Gateway protocol, select CSE.
9. Scroll down to Alias names and click Modify. The Modify Call Signaling Settings page appears.
10. Enter the information that supports your system. Applying the changes made to the Call Signaling Settings causes all H.323 calls to be dropped. It is recommended that you make changes to the Call Signaling Settings during off-peak hours or a scheduled maintenance window. Refer to Table 43: H.323 Call Signaling Settings fields on page 251.

Table 43: H.323 Call Signaling Settings fields

Field	Value	Description
Call Signaling	Direct	Call signaling information is passed directly

Field	Value	Description
		between H.323 endpoints. You must set up remote Gateways.
	Gatekeeper Resolved	All call signaling occurs directly between H.323 endpoints. This means that the Gatekeeper resolves the phone numbers into IP addresses, but the Gatekeeper is not involved in call signaling.
	Gatekeeper Routed	Gatekeeper Routed uses a Gatekeeper for call setup and control. In this method, call signaling is directed through the Gatekeeper.
	Gatekeeper Routed no RAS	Use this setting for a NetCentrex Gatekeeper. With this setting, the system routes all calls through the Gatekeeper but does not use any of the Gatekeeper Registration and Admission Services (RAS). Choose this option if RAS is not enabled on the NRS.
Call Signaling Port	<port value>	If VoIP applications are installed that require nonstandard call signaling ports, enter the port number here. Port number 0 means that the system uses the first available port. The default port for call signaling is 1720.
RAS Port	<port value>	If the VoIP application requires a nonstandard RAS port, enter the port number here. Port number 0 means that the

Field	Value	Description
		system uses the first available port. This specifies the source port that the BCM uses for sending out RAS requests. They will always be sent to port 1719.
Enable H245 tunneling	<check box>	Select this field to allow H.245 messages within H.225.
Primary Gatekeeper IP	<IP address>	Fill in this field only if the network is controlled by a Gatekeeper. This is the IP address of the primary Gatekeeper (TLAN IP address).
Backup Gatekeeper(s)	<IP address>	NetCentrex Gatekeeper does not support RAS. Any backup Gatekeepers must be entered in this field. Gatekeepers that use RAS can provide a list of backup Gatekeepers for the endpoint to use in the event of a primary Gatekeeper failure.
Alias names	NAME:<alias name>	Enter the alias names of the BCM required to direct call signals to your system. Note: The Alias name is case sensitive. It must match the name configured in NRS.
Registration TTL(s)	<numeric value>	Specifies the keep-alive interval.

11. For SIP trunks, select the SIP Settings tab. See Figure 133: SIP Settings on page 254.

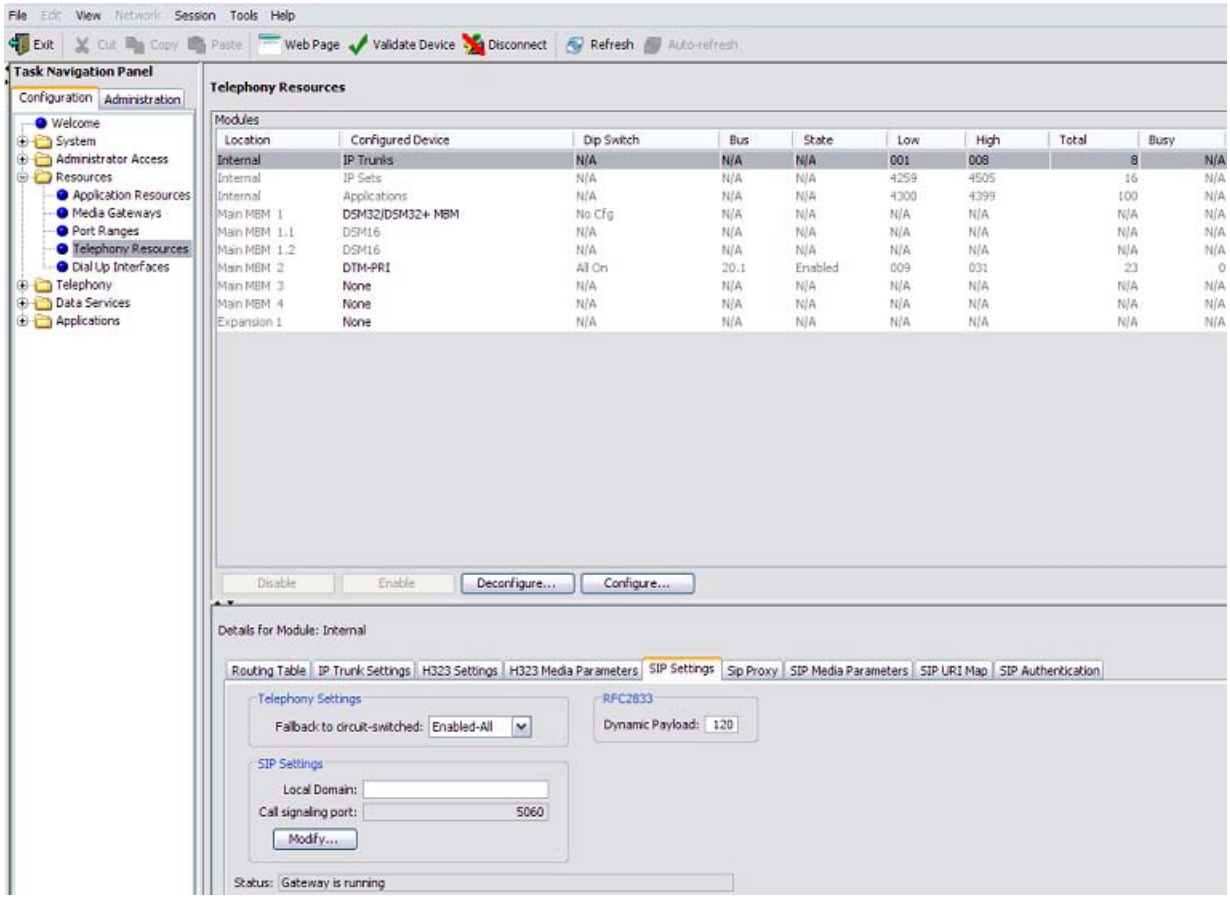

Figure 133: SIP Settings

12. Enter the information that supports your system. Refer to Table 44: SIP Settings fields on page 254 for more information.

Table 44: SIP Settings fields

Field	Value	Description
Fallback to Circuit-Switched	Disabled	Defines how you want the system to handle calls that the system fails to send over the VoIP trunk. Enabled-TDM enables fallback for calls originating on digital telephones. This is useful if your IP telephones are connected remotely, on the public side of the BCM network, because PSTN fallback is unlikely to result in better quality of service.
	Enabled-TDM	
	Enabled-All	

Field	Value	Description
Domain Name		Type the domain name of the SIP network.
Call Signaling Port	<port value>	If VoIP applications are installed that require nonstandard call signaling ports, enter the port number here. Port number 0 means that the system uses the first available port.
Outgoing Transport	UDP	
	TCP	
Proxy		If entered, all SIP calls originate to this address.
Status	Read Only	This field displays the current status of the Gatekeeper.

Configuring target lines

Target lines are virtual communication paths between trunks and telephones on the BCM system. They are incoming lines only and cannot be selected for outgoing calls or networking applications.

Configuring target lines

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab
3. elect Telephony > Lines > Target Lines.
4. Highlight the individual line you wish to configure.
5. Select the Parameters tab and enter the appropriate information for your network. See Figure 134: Parameters on page 256. Refer to Table 45: Parameters fields on page 256 for configuration information.

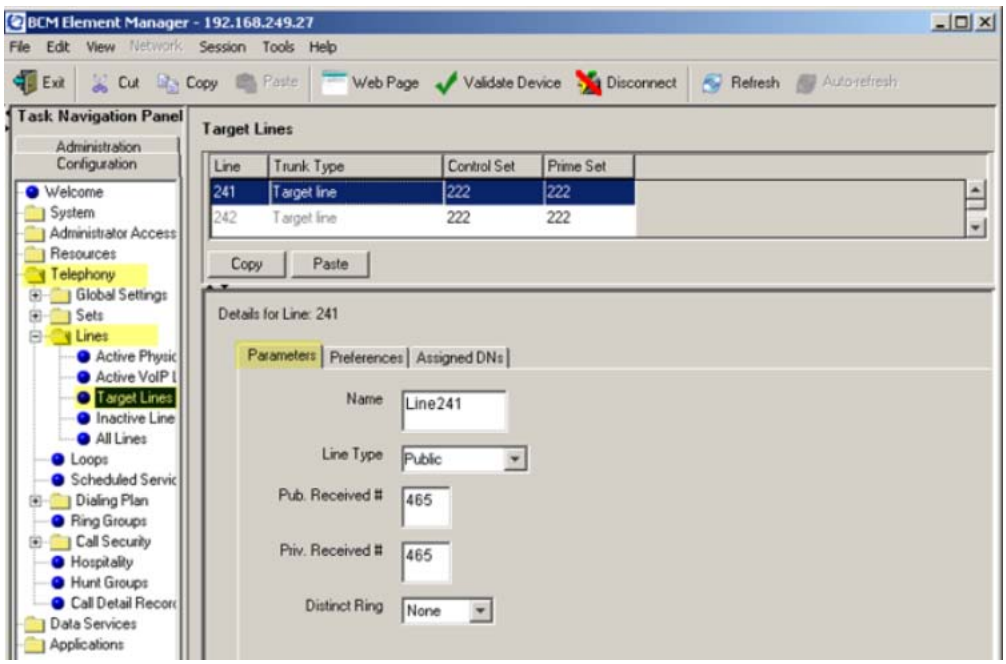

Figure 134: Parameters

Table 45: Parameters fields

Field	Value	Description
Line Type	Public DN:*	If the line is to be shared among telephones, select Public. If the line is only assigned to one telephone, select DN:*:.
Pub. Received #		Confirm the existing number or enter a public received number (PSTN DID or PRI trunks) that the system uses to identify calls from the public network to the target line. The public received number cannot be the same as the beginning digits of a line pool access code or destination code.
Priv. Received #		If private network trunks (PRI or VoIP trunks) are configured, enter a private received number.

Field	Value	Description
		The private received number specifies the digits the system uses to identify calls from the private network to a target line. This number is usually the same as the DN.
Distinct Ring	2, 3, 4, or None	If you want this line to have a special ring, select a ring pattern.

6. Select the Preferences tab and enter the appropriate information for your network. See Figure 135: Preferences on page 257. Refer to Table 46: Preferences fields on page 257 for configuration information.

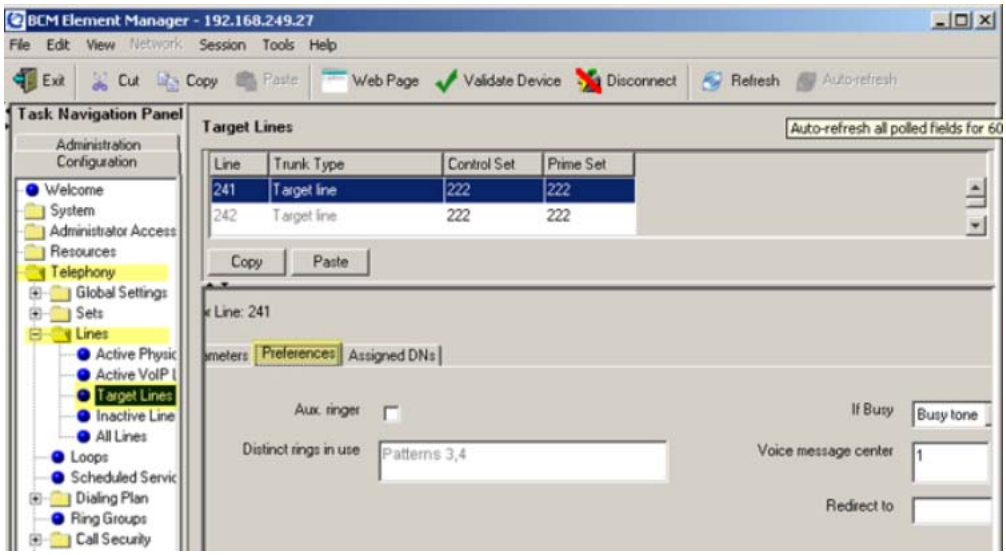

Figure 135: Preferences

Table 46: Preferences fields

Field	Value	Description
Aux. ringer	<check box>	If your system is equipped with an external ringer, you can enable this setting so that this line rings at the external ringer.
If Busy	Busy tone	To automatically direct calls to the prime telephone, select To

Field	Value	Description
	To Prime	prime. Otherwise, select Busy tone.
Distinct rings in use	Read only	Indicates which ring patterns are already configured on this system.
Voice message center		If the system is using a remote voice mail, select the center configured with the contact number.
Redirect to		To automatically direct calls out of the system to a specific telephone, such as a head office answer attendant, enter that remote number here. Ensure that you include the proper routing information.

7. Select the Assigned DNs tab. See Figure 136: Assigned DNs on page 258.

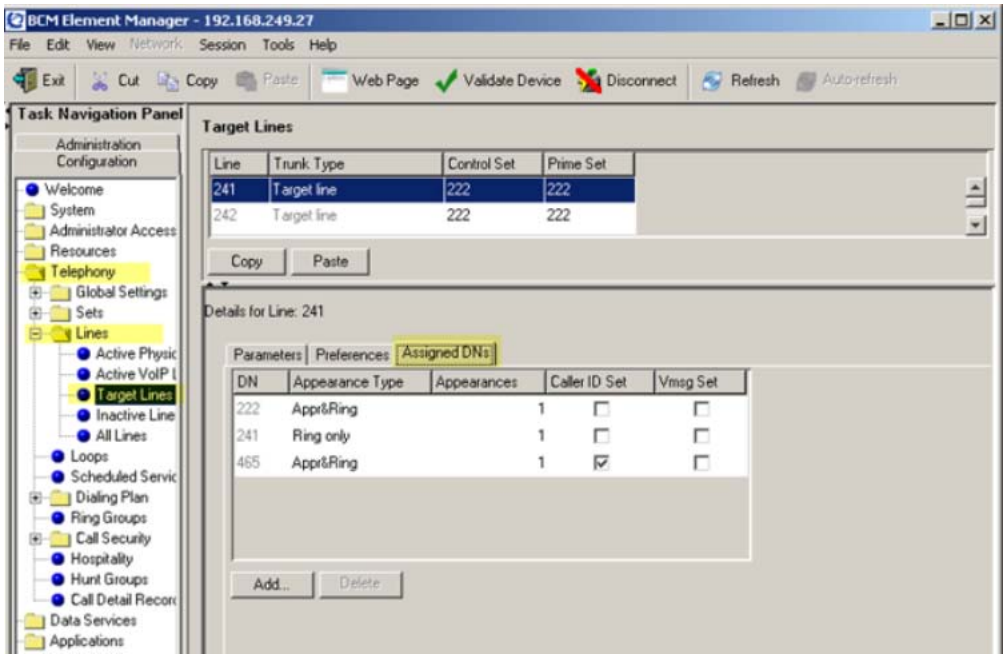

Figure 136: Assigned DNs

8. Edit the listed DNs, or click Add to add a DN as required.
9. Enter the appropriate information for your network. Refer to Table 50: Assigned DNs fields on page 264 for configuration information.

Configuring VoIP lines

Voice over IP (VoIP) lines simulate traditional Central Office (CO) lines. VoIP lines transmit data over an IP network rather than over physical lines.

Configuring VoIP lines

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select Telephony > Lines > All Lines.
4. Highlight the individual line you wish to configure.
5. Select the Parameters tab. See Figure 137: VoIP lines on page 259.

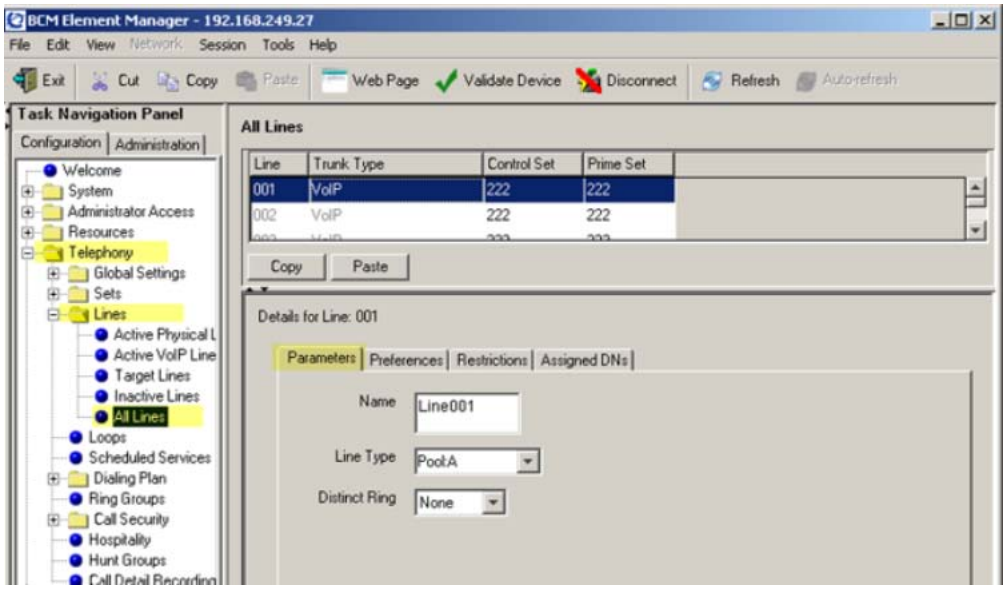

Figure 137: VoIP lines

6. Configure the Parameters tab appropriately for your network. Refer to Table 47: VoIP line descriptions on page 259 for configuration information.

Table 47: VoIP line descriptions

Field	Value	Description
Line	001-060	Unique line number.
Trunk Type	VoIP	Ensure that the trunk type is set to VoIP when configuring VoIP lines.
Control Set		Identify a DN if you are using this line with scheduling. To change

Field	Value	Description
		the DN, double-click the Control Set DN. For VoIP trunks, it is recommended that the Control Set be set to None because these are virtual trunks. Ensure that the VoIP trunk is assigned to a line pool.
Prime Set		Use the Prime Set if you want the line to be answered at another telephone when the line is not answered at the target telephone. To change the Prime set, double-click the Prime set DN. For VoIP trunks, it is recommended that the Prime Set be set to None because these are virtual trunks. Ensure that the VoIP trunk is assigned to a line pool.
Name		Identify the line in a meaningful way.
Line Type		Defines how the line is used in relation to other lines in the system.
	Public	If the line is to be shared among telephones, set to Public.
	DN:*	If the line is assigned to only one telephone, set to DN:*.
	Pool [A to O]	If you are using routing, put the line into line pool (A to F). If you are using line pools, configure the target lines. If your system uses both H.323 and SIP trunks, assign H.323 trunks to one pool and SIP trunks to another.

Field	Value	Description
Distinct Ring	2, 3, 4, or None	For trunks assigned to line pools, set the Distinct Ring pattern to None.

7. Select the Preferences tab. See Figure 138: Preferences on page 261.

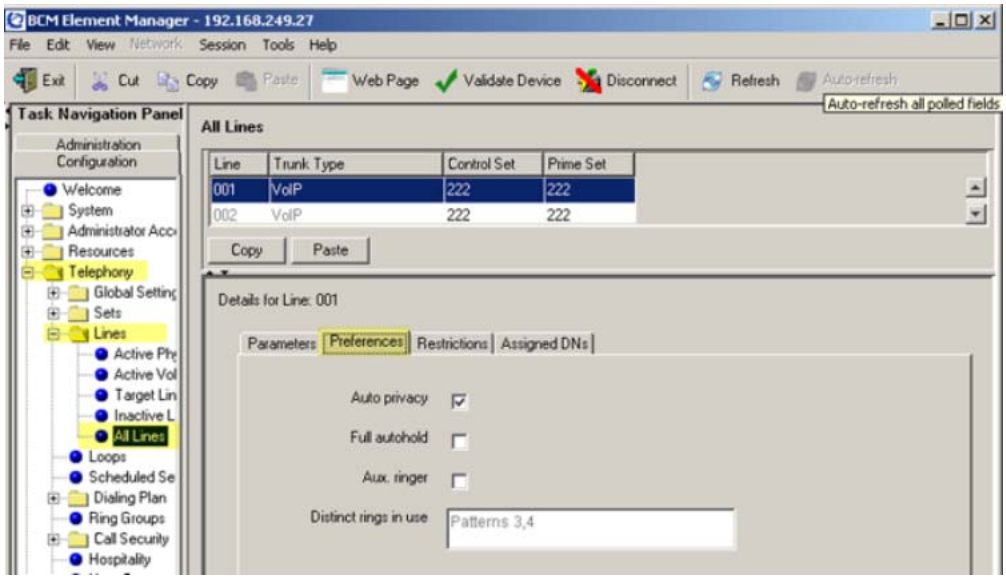

Figure 138: Preferences

8. Configure the Preferences tab appropriately for your network. Refer to Table 48: Preferences fields on page 261 for configuration information.

Table 48: Preferences fields

Field	Value	Description
Auto privacy	<check box>	Defines whether one BCM user can select a line in use at another telephone to join an existing call. For more information, see *BCM 4.0 Device Configuration Guide* (N0060600).
Full autohold	<check box>	Enables or disables Full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if the caller selects another line. Change the default setting only if Full

Field	Value	Description
		autohold is required for a specific application.
Aux. ringer	<check box>	If your system is equipped with an external ringer, you can enable this setting so that this line rings at the external ringer.
Distinct rings in use	Read only	Indicates whether a special ring is assigned.

9. Select the Restrictions tab. See Figure 139: Restrictions on page 262.

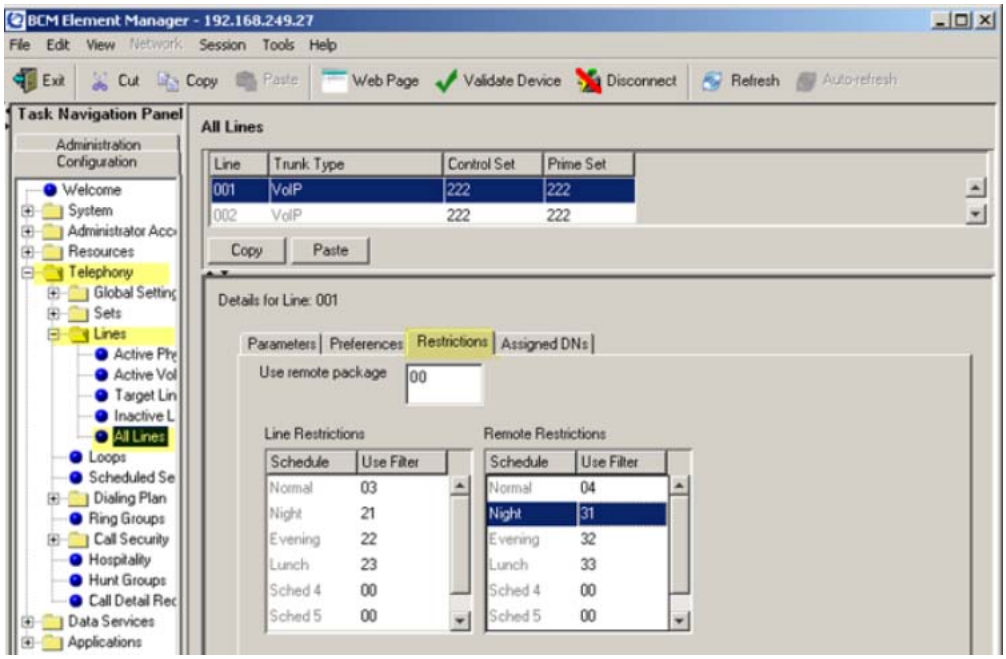

Figure 139: Restrictions

10. Configure the Restrictions tab appropriately for your network. Refer to Table 49: Restrictions fields on page 262 for configuration information.

Table 49: Restrictions fields

Field	Value	Description
Use remote package	< package #>	If the line is used to receive external calls or calls from other nodes on the private network, ensure that you indicate a remote package that provides only the

Field	Value	Description
		availability that you want for external callers. This attribute is typically used for tandeming calls.
Schedule	Default: Normal, Night, Evening, Lunch, Sched 4, Sched 5, Sched 6	
Line Restrictions - Use Filter	<00-99>	Enter the restriction filter number that applies to each schedule. These settings control outgoing calls.
Remote Restrictions - Use Filter	<00-99>	Enter the restriction filter that applies to each schedule. These settings provide call controls for incoming calls over a private network or from a remote user dialing in over PSTN.

11. Select the Assigned DNs tab. See Figure 140: Assigned DNs on page 263.

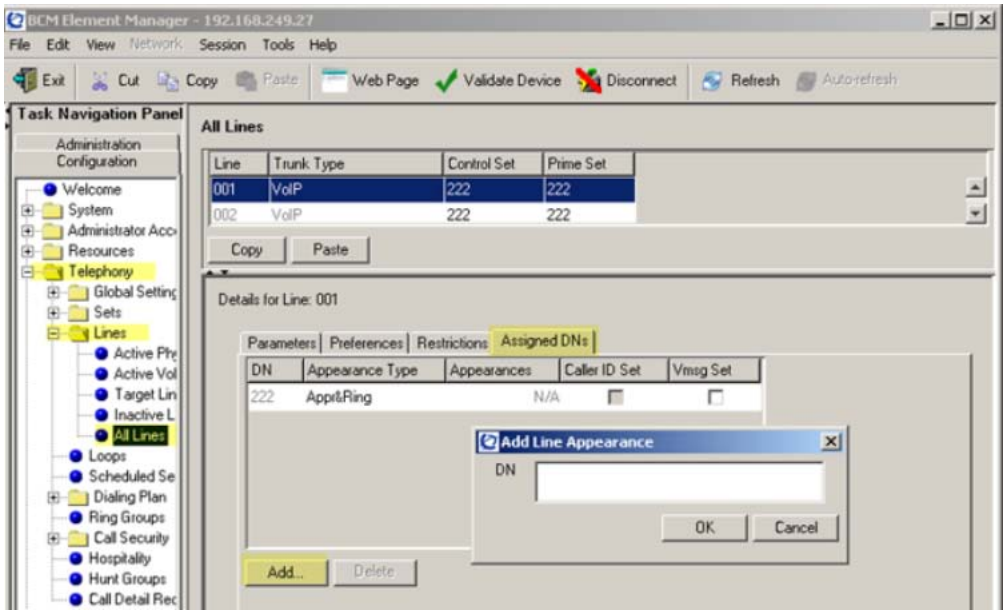

Figure 140: Assigned DNs

12. Click Add to add the Target Line DN.
13. Enter the appropriate information for your network. Refer to Table 50: Assigned DNs fields on page 264for configuration information.

Table 50: Assigned DNs fields

Field	Value	Description
DN		Unique number
Appearance Type	Ring only Appr&Ring Appr only	Select Appr Only or Appr&Ring if the telephone has an available button. Otherwise select Ring Only.
Appearances		Target lines can have more than one appearance to accommodate multiple calls. For telephones that have these lines set to Ring Only, set to None.
Caller ID Set	<check box>	When enabled, displays caller ID for calls coming in over the target line.
Vmsg Set	<check box>	When enabled, an indicator appears on the telephone when a message is waiting from a remote voice mail system. Check with your system administrator for the system voice mail setup before changing this parameter.

BCM 50/450 configuration prior to Release 5.0

This section describes configuration procedures for the Business Communications Manager (BCM) 50 and 450 systems prior to Release 5.0.

Note:

The Element Manager referred to in this section is the BCM Element Manager.

BCM Element Manager as viewed on your system may differ slightly from the screens shown in this chapter because you can customize the column display in BCM Element Manager.

BCM 50/450 configuration procedures

The sequence of BCM 50/450 configuration procedures is as follows:

Configuring incoming VoIP trunks

Perform the following procedure to configure incoming VoIP trunks.

Configuring incoming VoIP trunks

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select System > Keycodes. See Figure 141: Keycodes on page 266.

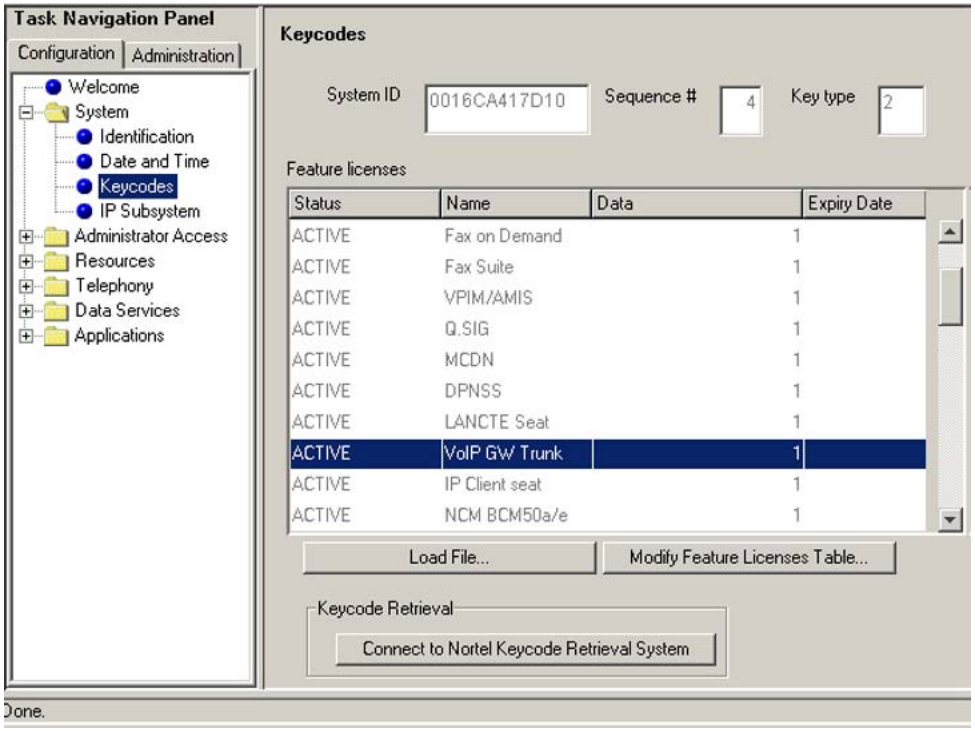

Figure 141: Keycodes

4. Load new Keycodes by loading a new keycode file or connecting to Nortel's Keycode Retrieval System (KRS). For more information about keycodes and keycode retrieval, see*Keycode Installation Guide* (NN40010-301).

Verifying system license and keycodes

Perform the following procedure to verify system license and keycodes.

Verifying system license and keycodes

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select System > Keycodes. See Figure 141: Keycodes on page 266.
4. In the Name column, scroll down to VoIP GW Trunk. The number of license keys you have are listed in the Data column.

Configuring VoIP trunk media parameters

Perform the following procedure to configure VoIP trunk media parameters.

Configuring VoIP trunk media parameters

1. Log on to BCM Element Manager.
2. n the Task Navigation Panel, select the Configuration tab.
3. Select Resources > Telephony Resources. See Figure 142: Telephony Resources on page 267.

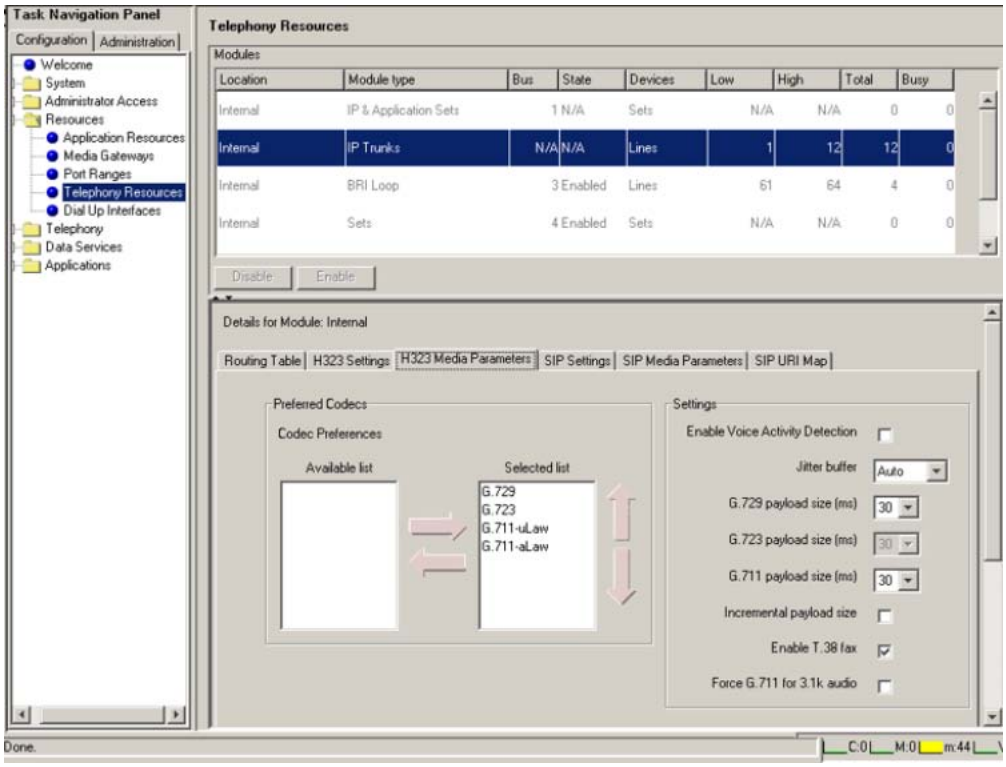

Figure 142: Telephony Resources

4. In the Modules panel, select the line where the Module Type column is set to IP Trunks.
5. Select the H.323 Media Parameters or SIP Media Parameters tab.
6. Enter the information that supports your system. Ensure that these settings are consistent with the other systems on your network. Refer to Table 51: H.323 Media Parameters fields on page 267 and Table 52: SIP Media Parameters fields on page 270 for a description of the parameters.

The following table describes the H.323 Media Parameters fields.

Table 51: H.323 Media Parameters fields

Field	Value	Description
Preferred Codecs	G.711 -muLaw G.711 -aLaw G.729 G.723	Add codecs to the Selected list and order them in the order in which you want the system to attempt to use

Field	Value	Description
		them. The system attempts to use the codecs in top-to-bottom sequence. Performance note: Codecs on all networked BCMs must be consistent to ensure the proper functionality of interacting features such as Transfer and Conference. Systems running BCM Release 3.5 or later allow codec negotiation and renegotiation to accommodate inconsistencies in codec settings over VoIP trunks.
Enable Voice Activity Detection	<check box>	Voice Activity Detection (VAD), also known as silence suppression, identifies periods of silence in a conversation and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. If VAD is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support VAD. G.711 does not support VAD. Performance note: VAD on all networked BCMs and IPT systems must be consistent to ensure functionality of features such as Transfer and Conference. The Payload size on the IPT must be set to 30ms.
Jitter Buffer	Auto None Small Medium Large	Select the size of jitter buffer for your system. Note: Slower networks require larger Jitter Buffers to

Field	Value	Description
		decrease voice break up, but increase end-to-end delay.
G.729 payload size (ms) G.723 payload size (ms) G.711 payload size (ms)	10,20,30,40,50,60 30 10,20,30,40,50,60	Set the maximum required payload size, per codec, for the VoIP calls sent over SIP trunks. Note: Payload size can also be set for Nortel IP telephones. See *BCM 4.0 Telephony Device Installation Guide* (N0060609).
Incremental payload size	<check box>	When enabled, the system advertises a variable payload size (40, 30, 20, 10 ms).
Enable T.38 fax	<check box>	When enabled, the system supports T.38 fax over IP. Caution: Fax tones broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. To minimize the possibility of your VoIP calls being dropped due to fax tone interference: • place the fax machine away from other telephones • turn the fax machine's speaker volume to the lowest level, or off, if available
Force G.711 for 3.1k Audio	<check box>	When enabled, the system forces the VoIP trunk to use the G.711 codec for 3.1k audio signals, such as modem or TTY machines. Note: You also can use this setting for fax machines if T. 38 fax is not enabled on the trunk.

The following table describes the SIP Media Parameters fields.

Table 52: SIP Media Parameters fields

Field	Value	Description
Preferred Codecs	G.711 -muLaw G.711 -aLaw G.729 G.723	Add codecs to the Selected list and order them in the order in which you want the system to attempt to use them. The system attempts to use the codecs in a top-to-bottom sequence. Performance note: Codecs on all networked BCMs must be consistent to ensure the proper functionality of interacting features such as Transfer and Conference. Systems running BCM Release 3.5 or later allow codec negotiation and renegotiation to accommodate inconsistencies in codec settings over VoIP trunks.
Enable Voice Activity Detection	<check box>	Voice Activity Detection (VAD), also known as silence suppression, identifies periods of silence in a conversation and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. If VAD is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support VAD. G.711 does not support VAD. Performance note: VAD on all networked BCMs and IPT systems must be consistent to ensure functionality of features such as Transfer and Conference. The

Field	Value	Description
		Payload size on the IPT must be set to 30ms.
Jitter Buffer	Auto None Small Medium Large	Select the size of jitter buffer for your system. Note: Slower networks require larger Jitter buffers to decrease voice break up, but increase end-to-end delay.
G.729 payload size (ms) G.723 payload size (ms) G.711 payload size (ms)	10,20,30,40,50,60 30 10,20,30,40,50,60	Set the maximum required payload size, per codec, for the VoIP calls sent over SIP trunks. Note: Payload size can also be set for Nortel IP telephones. See *BCM 4.0 Telephony Device Installation Guide* (N0060609).
Fax Transport	T.38 (default) G.711	T.38: T.38 is the preferred method of fax transport. G.711: G.711 is the preferred method of fax transport. Caution: Fax tones broadcast through a telephone speaker can disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. To minimize the possibility of your VoIP calls being dropped due to fax tone interference: • place the fax machine away from other telephones • turn the fax machine's speaker volume to the lowest level, or off, if available

Configuring local Gateway parameters

Perform the following procedure to configure local Gateway parameters.

Configuring local Gateway parameters

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select Resources > Telephony Resources.
4. In the Modules panel, select the line in which the Module Type column is set to IP Trunks. See Figure 142: Telephony Resources on page 267.
5. For H.323 VoIP trunks, select the H.323 Settings tab. See Figure 143: H.323 Settings on page 272.

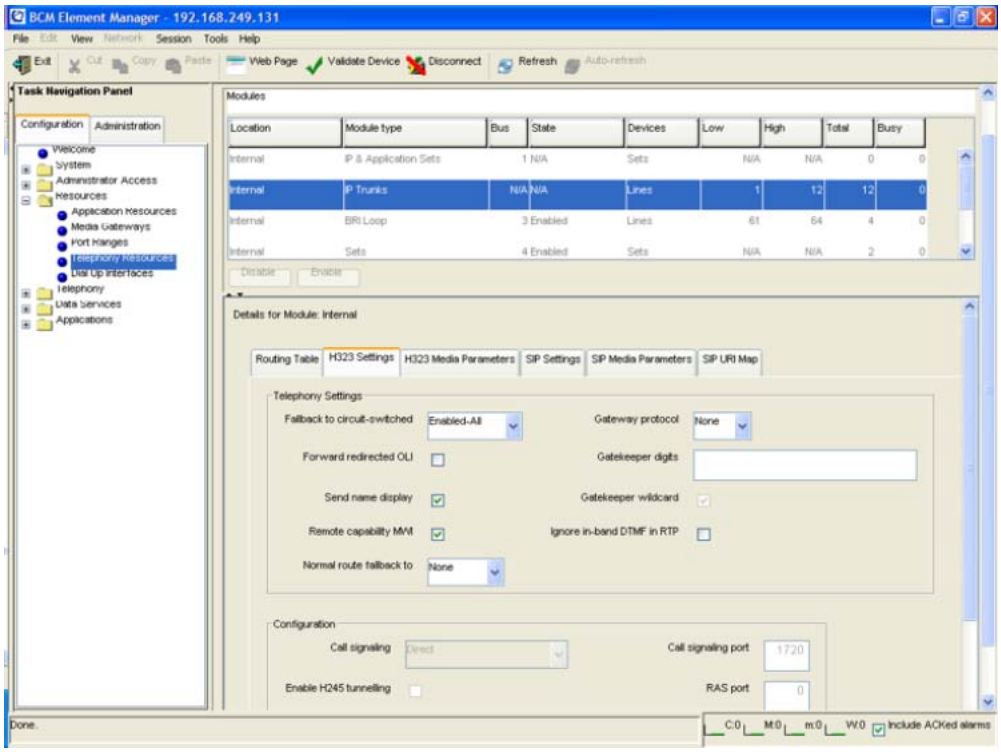

Figure 143: H.323 Settings

6. When implementing your dialing plan, in the H323 Settings tab, select a value for Fall back to circuit-switched. This determines how the system handles calls if the IP network cannot be used.
7. For Gateway protocol, select CSE.
8. Scroll down to Alias names and click Modify. The Modify Call Signaling Settings page appears.
9. Enter the information that supports your system. Applying the changes made to the Call Signaling Settings causes all H.323 calls to be dropped. It is recommended that you make changes to the Call Signaling Settings during off-peak hours or a scheduled maintenance window. Refer to Table 53: H.323 Call Signaling Settings fields on page 273.

Table 53: H.323 Call Signaling Settings fields

Field	Value	Description
Call signaling	Direct	Call signaling information is passed directly between H.323 endpoints. You must set up remote Gateways.
	Gatekeeper Resolved	All call signaling occurs directly between H.323 endpoints. This means that the Gatekeeper resolves the phone numbers into IP addresses, but the Gatekeeper is not involved in call signaling.
	Gatekeeper Routed	Gatekeeper Routed uses a Gatekeeper for call setup and control. In this method, call signaling is directed through the Gatekeeper.
	Gatekeeper Routed no RAS	Use this setting for a NetCentrex Gatekeeper. With this setting, the system routes all calls through the Gatekeeper but does not use any of the Gatekeeper Registration and Admission Services (RAS). Choose this option if RAS is not enabled on the NRS.
Call signaling port	<port value>	If VoIP applications are installed that require nonstandard call signaling ports, enter the port number here. Port number 0 means that the system uses the first available port. The default port for call signaling is 1720.

Field	Value	Description
RAS port	<port value>	If the VoIP application requires a nonstandard RAS port, enter the port number here. Port number 0 means that the system uses the first available port. This specifies the source port that the BCM uses for sending out RAS requests. They will always be sent to port 1719.
Enable H245 tunneling	<check box>	Select this field to allow H.245 messages within H.225.
Primary Gatekeeper IP	<IP address>	Fill in this field only if the network is controlled by a Gatekeeper. This is the IP address of the primary Gatekeeper (TLAN IP address).
Backup Gatekeeper(s)	<IP address>	NetCentrex Gatekeeper does not support RAS. Any backup Gatekeepers must be entered in this field. Gatekeepers that use RAS can provide a list of backup Gatekeepers for the endpoint to use in the event of a primary Gatekeeper failure.
Alias names	NAME:<alias name>	Enter the alias names of the BCM required to direct call signals to your system. Note: The Alias name is case sensitive. It must match the name configured in NRS.
Registration TTL(s)	<numeric value>	Specifies the keep-alive interval.

10. For SIP trunks, select the SIP Settings tab. See Figure 144: SIP Settings on page 275.

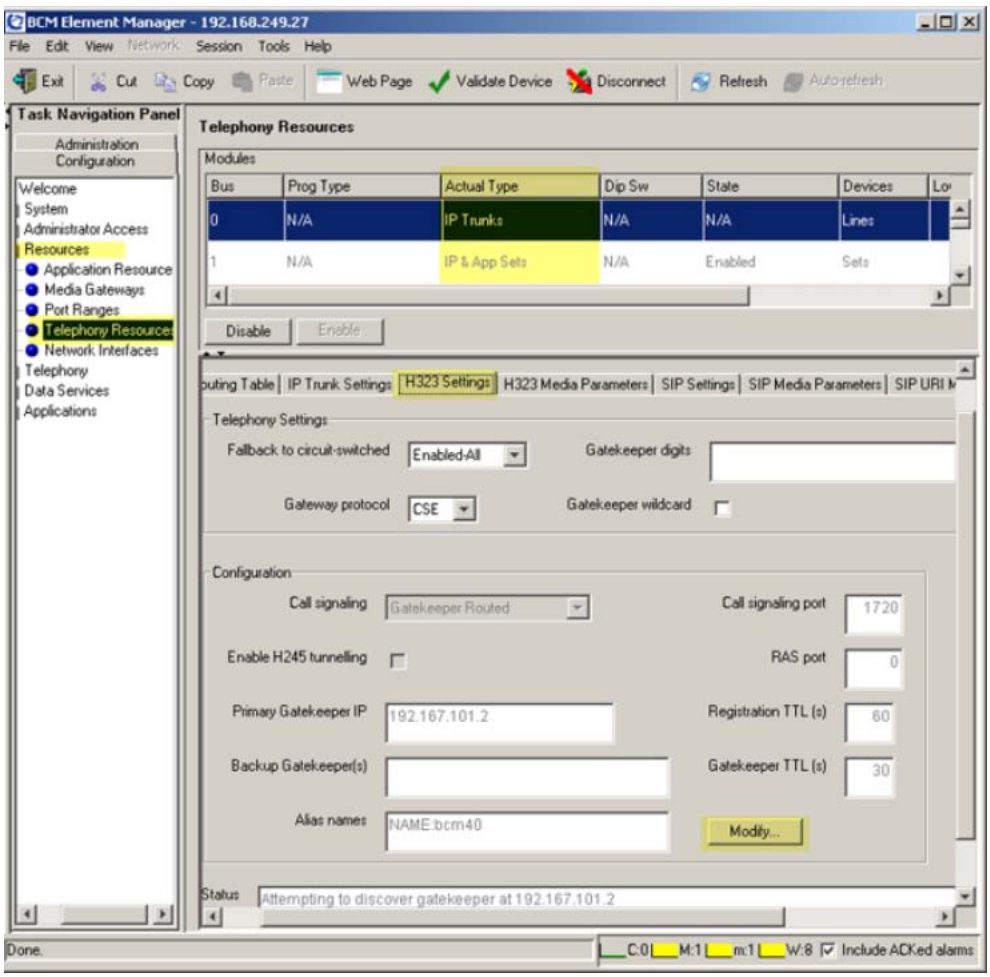

Figure 144: SIP Settings

11. Enter the information that supports your system. Refer to Table 54: SIP Settings fields on page 275 for more information.

Table 54: SIP Settings fields

Field	Value	Description
Fallback to circuit-switched	Disabled	Defines how you want the system to handle calls that the system fails to send over the VoIP trunk. Enabled-TDM enables fallback for calls originating on digital telephones. This is useful if your IP telephones are connected remotely, on the public side of the BCM network, because
	Enabled-TDM	
	Enabled-All	

Field	Value	Description
		PSTN fallback is unlikely to result in better quality of service.
Local Domain		Type the domain name of the SIP network.
Call signaling port	<port value>	If VoIP applications are installed that require nonstandard call signaling ports, enter the port number here. Port number 0 means that the system uses the first available port.
Status	Read Only	This field displays the current status of the IP Trunk Gateway.

12. To configure SIP Proxy click the SIP Proxy Tab. Refer to Table 55: SIP Proxy Tab on page 276 for more information.

Table 55: SIP Proxy Tab

Field	Value	Description
Domain	<IP address>	SIP domain serviced by proxy.
Route all calls using Proxy	<check box>	Ignore the SIP entries in the Routing Table - this does not override the H.323 entries, or the H.323 Gatekeeper settings.
MCDN Protocol	None CSE	Choose CSE for CS1000 interoperability.
Optional IP address for legacy routing		Enter the IP address of the BCM if proxy is a CS1000 4.0 system.
Outbound Proxy Table	Name	If there is no IP address given, then this name must be DNS resolvable.
	<IP address>	If known and fixed - name becomes only an identifier in the table.
	<port value>	Non-zero if non-standard.
	Load Balancing	If non-zero, then outgoing calls are distributed by weight among the alive entries. There

Field	Value	Description
		is only one zero weight entry that will be used (the first in the table) if the non-zero proxies are deemed to be all unavailable.
	Keep Alive	If 'none' then the server will always be considered to be alive. If OPTIONS then a SIP OPTIONS ping is used to determine responsiveness.

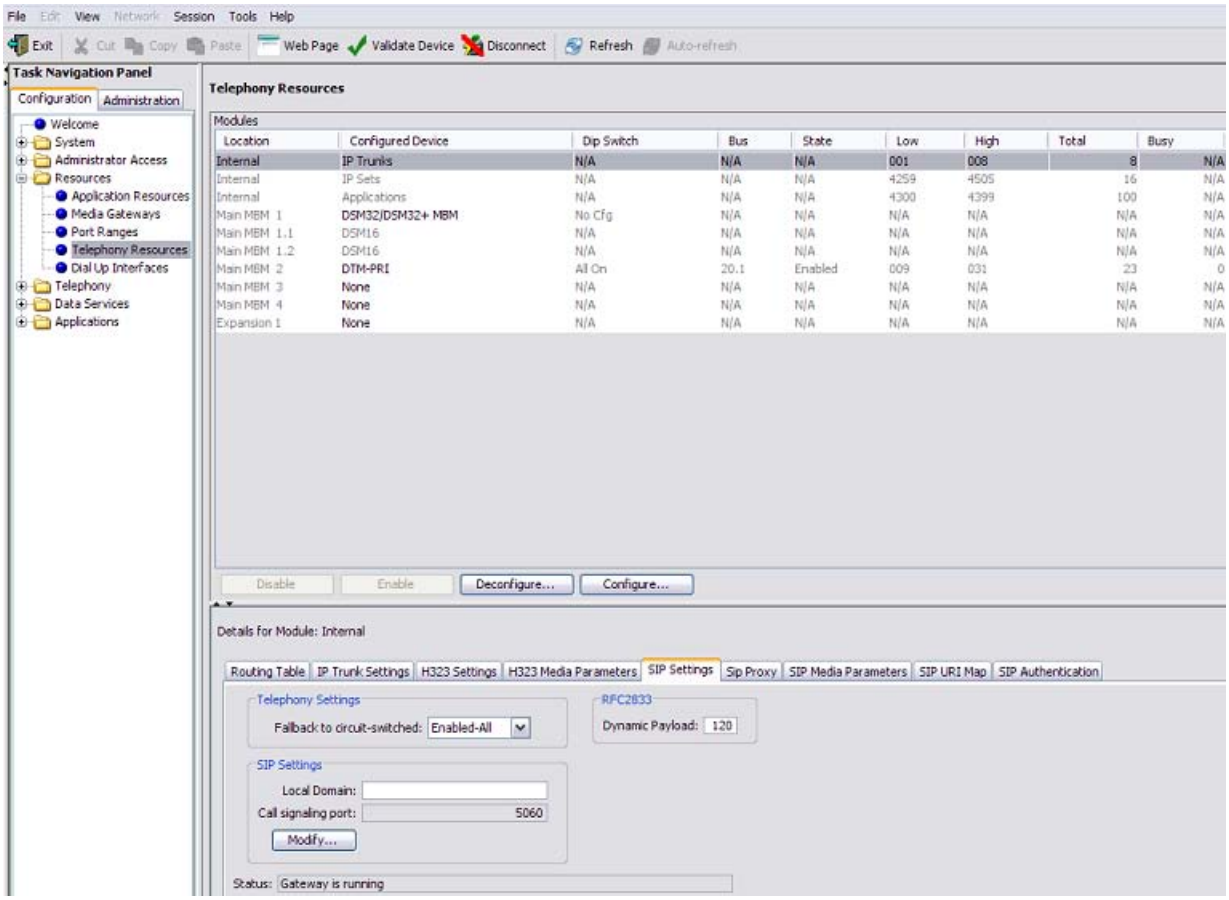

Figure 145: SIP Proxy Tab

Configuring VoIP lines

Voice over IP (VoIP) lines simulate traditional Central Office (CO) lines. VoIP lines transmit data over an IP network rather than over physical lines.

Configuring VoIP lines

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select Telephony > Lines > All Lines.
4. Highlight the individual line you wish to configure.
5. Select the Preferences tab. See Figure 146: Preferences on page 278.

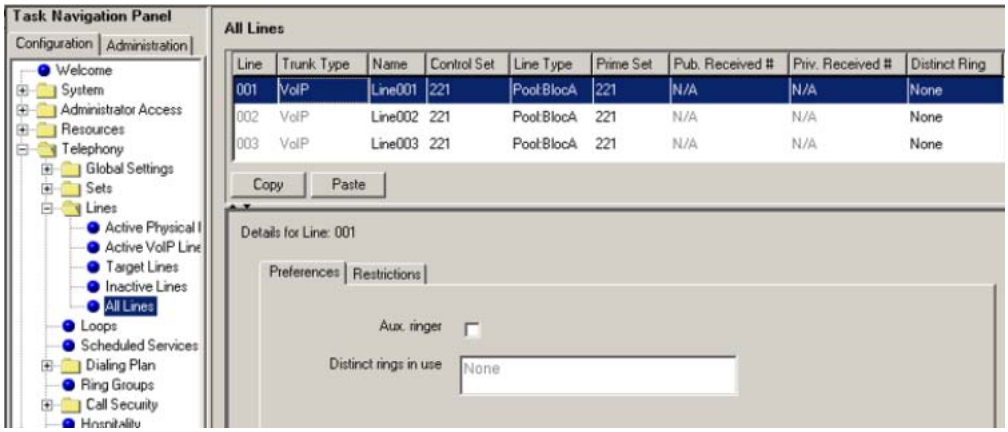

Figure 146: Preferences

6. Configure the Preferences tab appropriately for your network. Refer to Table 56: Preferences fields on page 278 for configuration information.

Table 56: Preferences fields

Field	Value	Description
Aux. ringer	<check box>	If your system is equipped with an external ringer, you can enable this setting so that this line rings at the external ringer.
Distinct rings in use	Read only	Indicates which ring patterns are already configured on this system.

7. Select the Restrictions tab. See Figure 147: Restrictions on page 279.

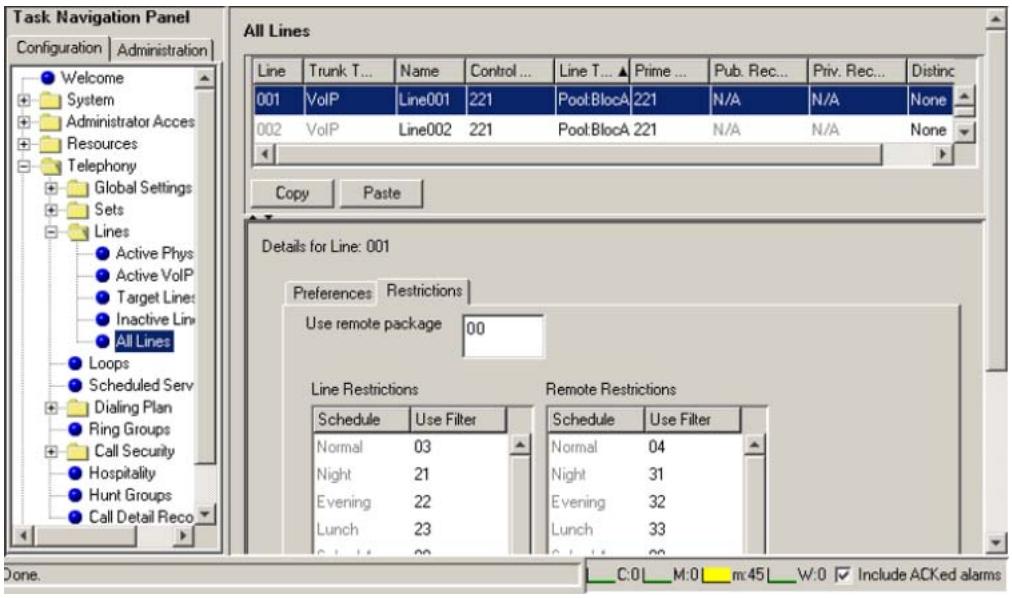

Figure 147: Restrictions

8. Configure the Restrictions tab appropriately for your network. Refer to Table 57: Restrictions fields on page 279 for configuration information.

Table 57: Restrictions fields

Field	Value	Description
Use remote package	< package #>	If the line is used to receive external calls or calls from other nodes on the private network, ensure that you indicate a remote package that provides only the availability that you want for external callers. This attribute is typically used for tandeming calls.
Schedule	Default: Normal, Night, Evening, Lunch, Sched 4, Sched 5, Sched 6	
Line Restrictions - Use Filter	<00-99>	Enter the restriction filter number that applies to each schedule. These settings control outgoing calls.
Remote Restrictions - Use Filter	<00-99>	Enter the restriction filter that applies to each schedule. These settings

Field	Value	Description
		provide call controls for incoming calls over a private network or from a remote user dialing in over PSTN.

9. In the Task Navigation Panel, in the Configuration tab, select Telephony > Sets > All DNs.
10. Highlight the individual line you wish to configure.
11. Select the Line Assignment tab. See Figure 148: Line Assignment on page 280.

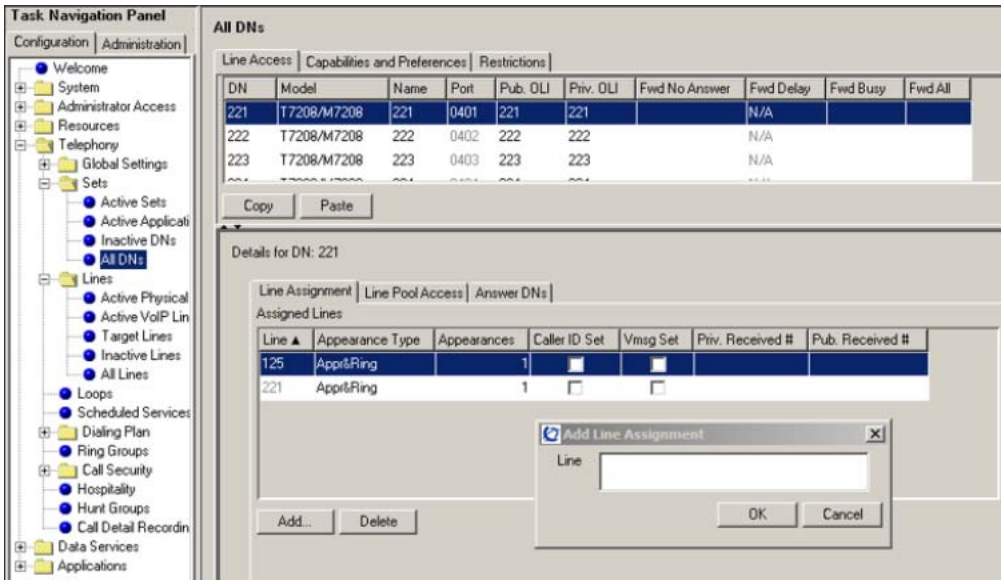

Figure 148: Line Assignment

12. Edit the listed DNs, or click Add to add a DN as required.
13. Enter the appropriate information for your network. Refer to Table 58: Assigned DNs fields on page 280 for configuration information.

Table 58: Assigned DNs fields

Field	Value	Description
DN		Unique number
Appearance Type	Ring Only Appr&Ring Appr Only	Select Appr Only or Appr&Ring if the telephone has an available button. Otherwise select Ring Only.
Appearances		Target lines can have more than one

Field	Value	Description
		appearance to accommodate multiple calls. For telephones that have these lines set to Ring Only, set to None.
Caller ID Set	<check box>	When enabled, displays caller ID for calls coming in over the target line.
Vmsg Set	<check box>	When enabled, an indicator appears on the telephone when a message is waiting from a remote voice mail system. Check with your system administrator for the system voice mail setup before changing this parameter.

Configuring target lines

Target lines are virtual communication paths between trunks and telephones on the BCM system. They are incoming lines only and cannot be selected for outgoing calls or networking applications.

Configuring target lines

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select Telephony > Lines > Target Lines.
4. Highlight the individual line you wish to configure.
5. Select the Preferences tab and enter the appropriate information for your network. See Figure 149: Preferences on page 282. Refer to Table 59: Preferences fields on page 282 for configuration information.

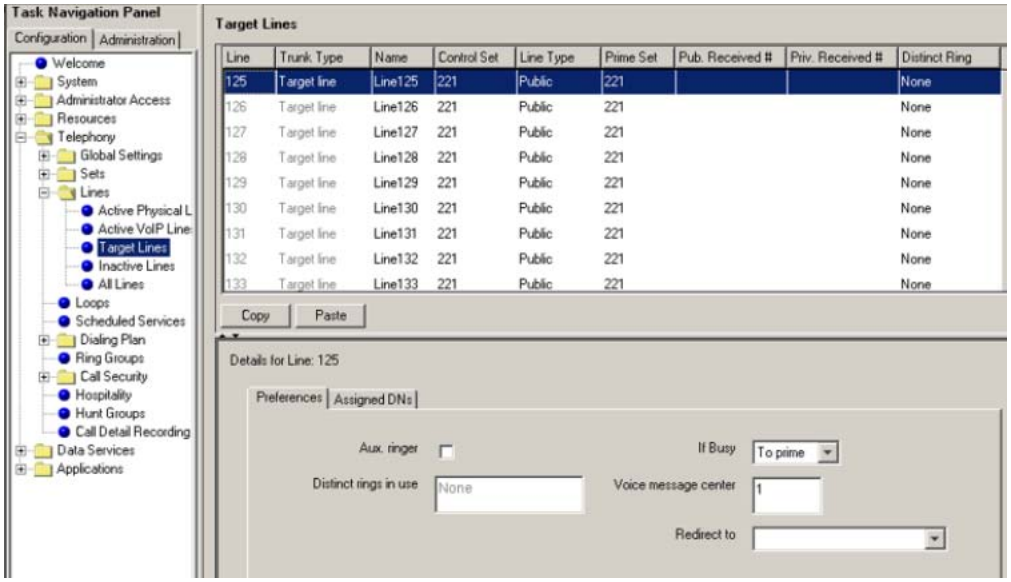

Figure 149: Preferences

Table 59: Preferences fields

Field	Value	Description
Aux. ringer	<check box>	If your system is equipped with an external ringer, you can enable this setting so that this line rings at the external ringer.
If Busy	Busy tone To Prime	To automatically direct calls to the prime telephone, select To prime. Otherwise, select Busy tone.
Distinct rings in use	Read only	
Voice message center		If the system is using a remote voice mail, select the center configured with the contact number.
Redirect to		To automatically direct calls out of the system to a specific telephone, such as a head office answer attendant, enter that remote number here. Ensure that you include

Field	Value	Description
		the proper routing information.

6. Select the Assigned DNs tab. See Figure 150: Assigned DNs on page 283.

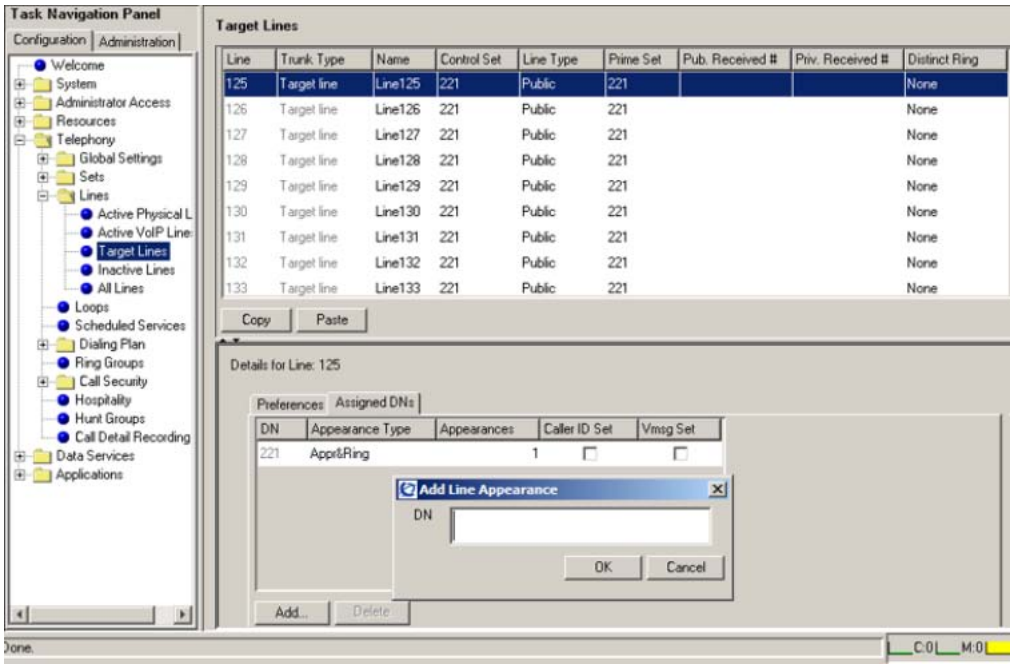

Figure 150: Assigned DNs

7. Edit the listed DNs, or click Add to add a DN as required.
8. Enter the appropriate information for your network. Refer Table 58: Assigned DNs fields on page 280 for configuration information.

BCM Release 5.0 configuration to integrate with a Communication Server 1000 system

The following details the steps to integrate a Business Communications Manager (BCM) Release 5.0 with a Communication Server 1000 system.

BCM 50/450 Release 5.0 configuration on page 284

BCM 50/450 Release 5.0 configuration

This section describes configuration procedures for the Business Communications Manager (BCM) 50 and 450 systems for Release 5.0.

Note:
The Element Manager referred to in this section is the BCM Element Manager.

BCM Element Manager as viewed on your system may differ slightly from the screens shown in this chapter because you can customize the column display in BCM Element Manager.

BCM 50/450 configuration procedures

The sequence of BCM 50/450 configuration procedures is as follows:

- Configuring incoming VoIP trunks on page 284
- Verifying system license and keycodes on page 285
- Configuring VoIP trunk media parameters on page 285
- Configuring local Gateway parameters on page 291
- Configuring VoIP lines on page 297
- Configuring target lines on page 301

Configuring incoming VoIP trunks

Perform the following procedure to configure incoming VoIP trunks.

Configuring incoming VoIP trunks

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.

3. Select System > Keycodes. See Figure 151: Keycodes on page 285.

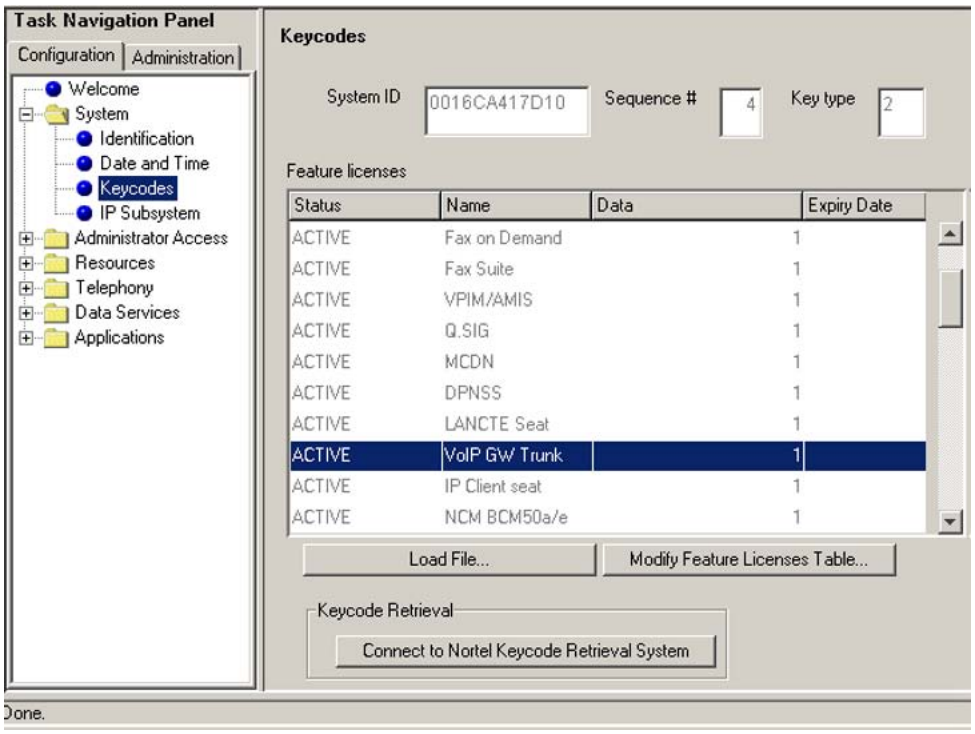

Figure 151: Keycodes

4. Load new Keycodes by loading a new keycode file or connecting to Nortel's Keycode Retrieval System (KRS). For more information about keycodes and keycode retrieval, see*Keycode Installation Guide* (NN40010-301).

Verifying system license and keycodes

Perform the following procedure to verify system license and keycodes.

Verifying system license and keycodes

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select System > Keycodes. See Figure 151: Keycodes on page 285.
4. In the Name column, scroll down to VoIP GW Trunk. The number of license keys you have are listed in the Data column.

Configuring VoIP trunk media parameters

Perform the following procedure to configure VoIP trunk media parameters.

Configuring VoIP trunk media parameters

1. Log on to BCM Element Manager.
2. n the Task Navigation Panel, select the Configuration tab.
3. Select Resources > Telephony Resources. See Figure 152: Telephony Resources on page 286.

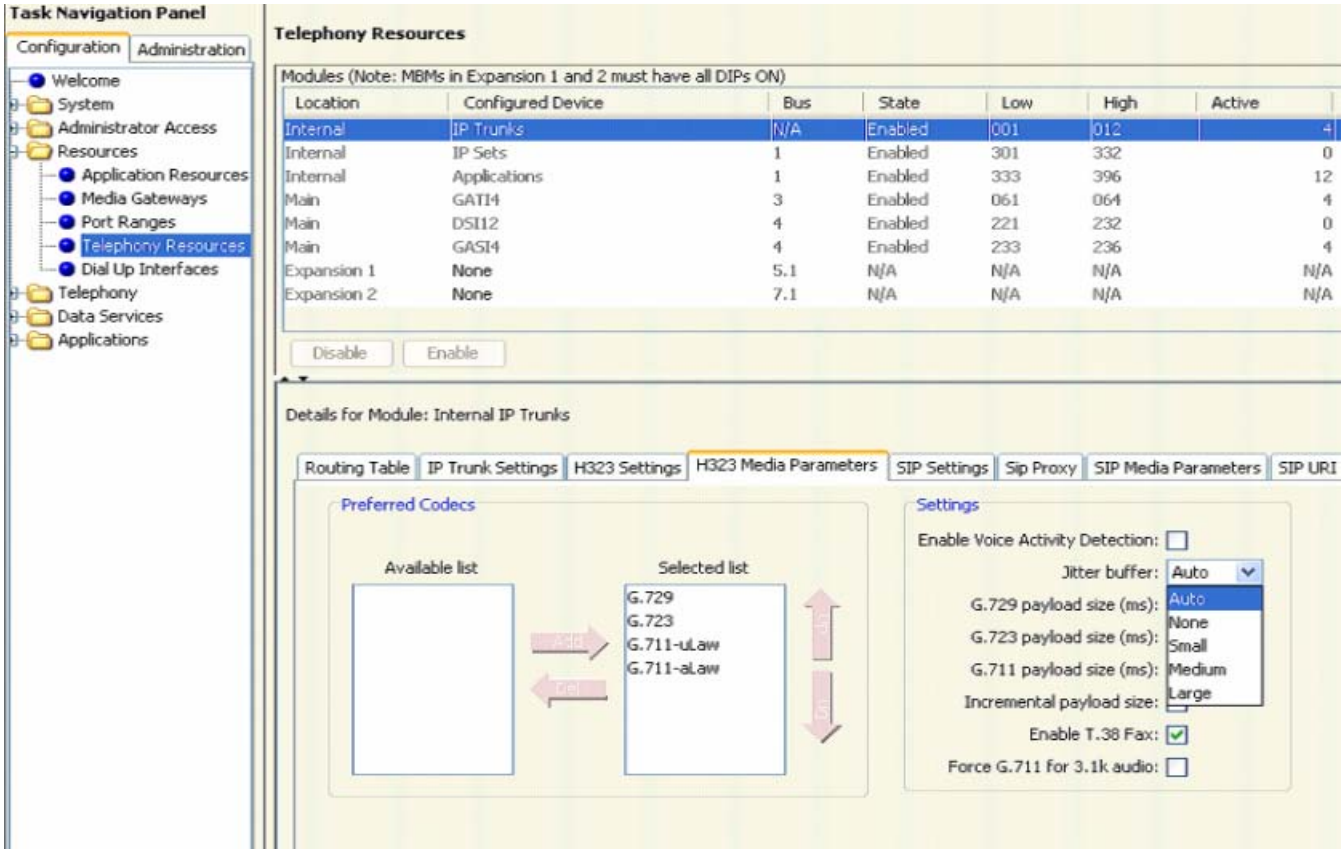

Figure 152: Telephony Resources

4. In the Modules panel, select the line where the Module Type column is set to IP Trunks.
5. Select the H.323 Media Parameters or SIP Media Parameters tab.
6. Enter the information that supports your system. Ensure that these settings are consistent with the other systems on your network. Refer to Table 60: H.323 Media Parameters fields on page 287 and Table 61: SIP Media Parameters fields on page 289 for a description of the parameters.

The following table describes the H.323 Media Parameters fields.

Table 60: H.323 Media Parameters fields

Field	Value	Description
Preferred Codecs	G.711 -muLaw G.711 -aLaw G.729 G.723	Add codecs to the Selected list and order them in the order in which you want the system to attempt to use them. The system attempts to use the codecs in top-to-bottom sequence. Performance note: Codecs on all networked BCMs must be consistent to ensure the proper functionality of interacting features such as Transfer and Conference. Systems running BCM Release 3.5 or later allow codec negotiation and renegotiation to accommodate inconsistencies in codec settings over VoIP trunks.
Enable Voice Activity Detection	<check box>	Voice Activity Detection (VAD), also known as silence suppression, identifies periods of silence in a conversation and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. If VAD is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support VAD. G.711 does not support VAD. Performance note: VAD on all networked BCMs and IPT systems must be consistent to ensure functionality of features such as Transfer and Conference. The

Field	Value	Description
		Payload size on the IPT must be set to 30ms.
Jitter Buffer	Auto None Small Medium Large	Select the size of jitter buffer for your system. Note: Slower networks require larger Jitter Buffers to decrease voice break up, but increase end-to-end delay.
G.729 payload size (ms) G.723 payload size (ms) G.711 payload size (ms)	10,20,30,40,50,60 30 10,20,30,40,50,60	Set the maximum required payload size, per codec, for the VoIP calls sent over SIP trunks. Note: Payload size can also be set for Nortel IP telephones. See *Business Communications Manager 5.0 - Configuration - Telephony , NN40170-502*.
Incremental payload size	<check box>	When enabled, the system advertises a variable payload size (40, 30, 20, 10 ms).
Enable T.38 fax	<check box>	When enabled, the system supports T.38 fax over IP. Caution: Fax tones broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. To minimize the possibility of your VoIP calls being dropped due to fax tone interference: • place the fax machine away from other telephones • turn the fax machine's speaker volume to the lowest level, or off, if available
Force G.711 for 3.1k Audio	<check box>	When enabled, the system forces the VoIP trunk to use the G.711 codec for 3.1k audio signals, such as modem or TTY machines.

Field	Value	Description
		Note: You also can use this setting for fax machines if T.38 fax is not enabled on the trunk.

The following table describes the SIP Media Parameters fields.

Table 61: SIP Media Parameters fields

Field	Value	Description
Preferred Codecs	G.711 -muLaw G.711 -aLaw G.729 G.723	Add codecs to the Selected list and order them in the order in which you want the system to attempt to use them. The system attempts to use the codecs in a top-to-bottom sequence. Performance note: Codecs on all networked BCMs must be consistent to ensure the proper functionality of interacting features such as Transfer and Conference. Systems running BCM Release 3.5 or later allow codec negotiation and renegotiation to accommodate inconsistencies in codec settings over VoIP trunks.
Enable Voice Activity Detection	<check box>	Voice Activity Detection (VAD), also known as silence suppression, identifies periods of silence in a conversation and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. If VAD is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and

Field	Value	Description
		G.729 support VAD. G.711 does not support VAD. Performance note: VAD on all networked BCMs and IPT systems must be consistent to ensure functionality of features such as Transfer and Conference. The Payload size on the IPT must be set to 30ms.
Jitter Buffer	Auto None Small Medium Large	Select the size of jitter buffer for your system. Note: Slower networks require larger Jitter buffers to decrease voice break up, but increase end-to-end delay.
G.729 payload size (ms) G.723 payload size (ms) G.711 payload size (ms)	10,20,30,40,50,60 30 10,20,30,40,50,60	Set the maximum required payload size, per codec, for the VoIP calls sent over SIP trunks. Note: Payload size can also be set for Nortel IP telephones. See *Business Communications Manager 5.0 - Configuration - Telephony , NN40170-502*
Fax Transport	T.38 (default) G.711	T.38: T.38 is the preferred method of fax transport. G.711: G.711 is the preferred method of fax transport. Caution: Fax tones broadcast through a telephone speaker can disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. To minimize the possibility of your VoIP calls being dropped due to fax tone interference: • place the fax machine away from other telephones • turn the fax machine's speaker volume to the

Field	Value	Description
		lowest level, or off, if available

Configuring local Gateway parameters

Perform the following procedure to configure local Gateway parameters.

Configuring local Gateway parameters

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select Resources > Telephony Resources.
4. In the Modules panel, select the line in which the Module Type column is set to IP Trunks. See Figure 152: Telephony Resources on page 286.
5. For H.323 VoIP trunks, select the H.323 Settings tab. See Figure 153: H.323 Settings on page 291.

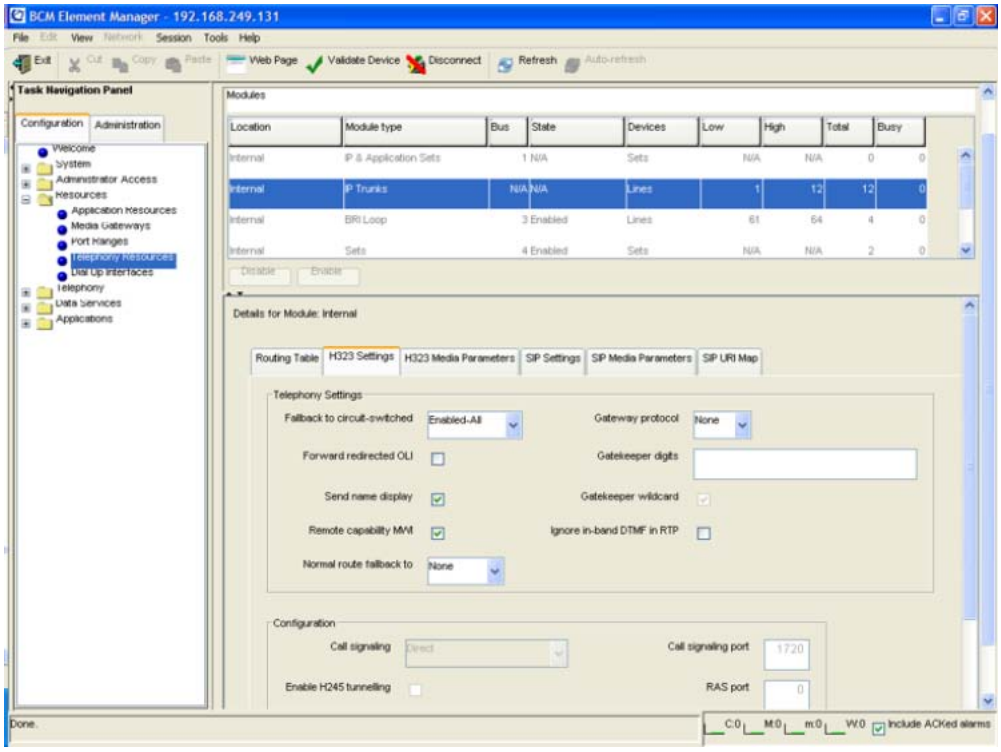

Figure 153: H.323 Settings

6. When implementing your dialing plan, in the H323 Settings tab, select a value for Fall back to circuit-switched. This determines how the system handles calls if the IP network cannot be used.

7. For MCDN protocol, select CSE.
8. Scroll down to Alias names and click Modify. The Modify Call Signaling Settings page appears.
9. Enter the information that supports your system. Applying the changes made to the Call Signaling Settings causes all H.323 calls to be dropped. It is recommended that you make changes to the Call Signaling Settings during off-peak hours or a scheduled maintenance window. Refer to Table 62: H.323 Call Signaling Settings fields on page 292.

Table 62: H.323 Call Signaling Settings fields

Field	Value	Description
Call signaling	Direct	Call signaling information is passed directly between H.323 endpoints. You must set up remote Gateways.
	Gatekeeper Resolved	All call signaling occurs directly between H.323 endpoints. This means that the Gatekeeper resolves the phone numbers into IP addresses, but the Gatekeeper is not involved in call signaling.
	Gatekeeper Routed	Gatekeeper Routed uses a Gatekeeper for call setup and control. In this method, call signaling is directed through the Gatekeeper.
	Gatekeeper Routed no RAS	Use this setting for a NetCentrex Gatekeeper. With this setting, the system routes all calls through the Gatekeeper but does not use any of the Gatekeeper Registration and Admission Services (RAS). Choose this option if RAS is not enabled on the NRS.
Call signaling port	<port value>	If VoIP applications are installed that require

Field	Value	Description
		nonstandard call signaling ports, enter the port number here. Port number 0 means that the system uses the first available port. The default port for call signaling is 1720.
RAS port	<port value>	If the VoIP application requires a nonstandard RAS port, enter the port number here. Port number 0 means that the system uses the first available port. This specifies the source port that the BCM uses for sending out RAS requests. They will always be sent to port 1719.
Enable H245 tunneling	<check box>	Select this field to allow H.245 messages within H.225.
Primary Gatekeeper IP	<IP address>	Fill in this field only if the network is controlled by a Gatekeeper. This is the IP address of the primary Gatekeeper (TLAN IP address).
Backup Gatekeeper(s)	<IP address>	NetCentrex Gatekeeper does not support RAS. Any backup Gatekeepers must be entered in this field. Gatekeepers that use RAS can provide a list of backup Gatekeepers for the endpoint to use in the event of a primary Gatekeeper failure.
Alias names	NAME:<alias name>	Enter the alias names of the BCM required to direct call signals to your system.

Field	Value	Description
		Note: The Alias name is case sensitive. It must match the name configured in NRS.
Registration TTL(s)	<numeric value>	Specifies the keep-alive interval.

10. For SIP trunks, select the SIP Settings tab. See Figure 154: SIP Settings on page 294.

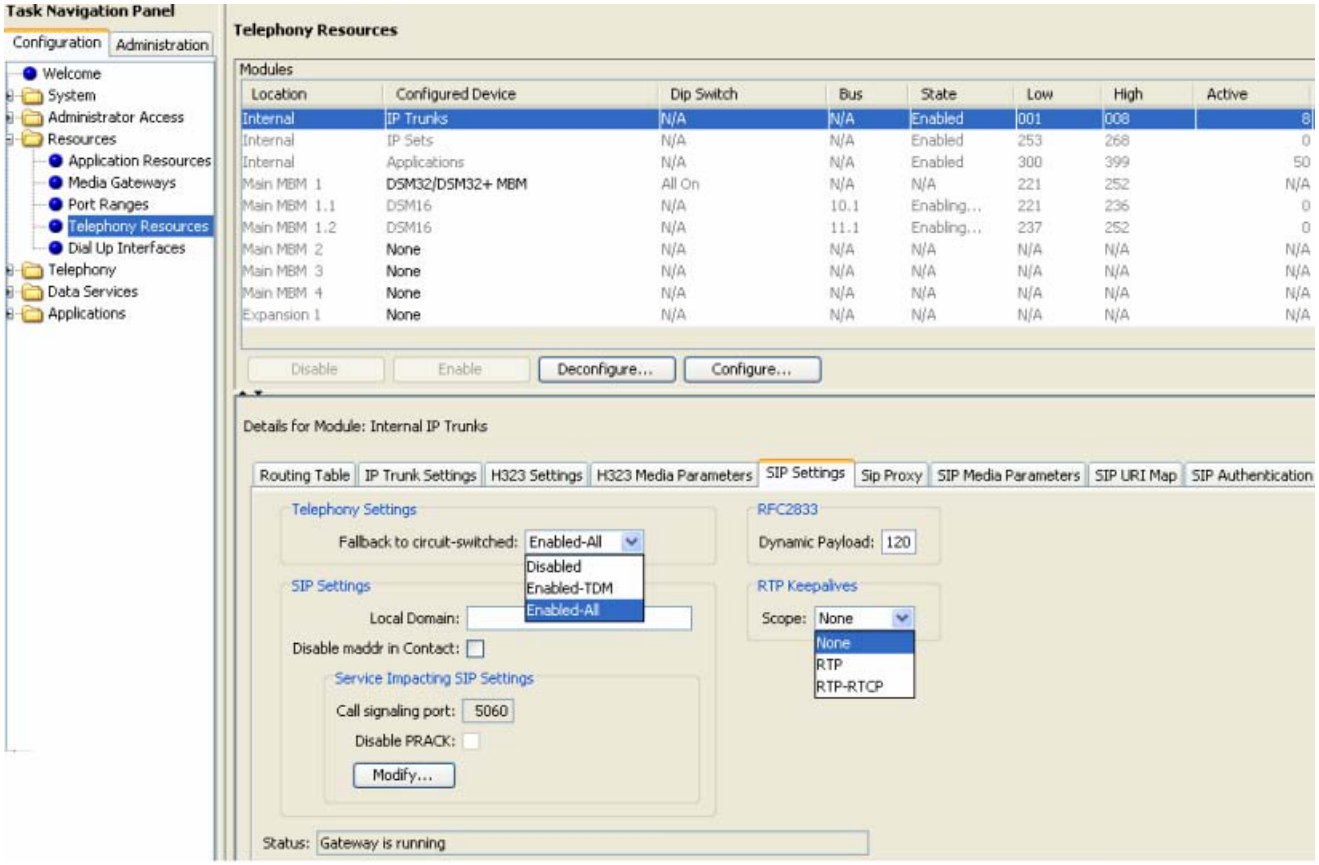

Figure 154: SIP Settings

11. Enter the information that supports your system. Refer to Table 63: SIP Settings fields on page 294 for more information.

Table 63: SIP Settings fields

Field	Value	Description
Fallback to circuit-switched	Disabled	Defines how you want the system to handle calls that the system fails to send over the VoIP trunk.
	Enabled-TDM	
	Enabled-All	

Field	Value	Description
		Enabled-TDM enables fallback for calls originating on digital telephones. This is useful if your IP telephones are connected remotely, on the public side of the BCM network, because PSTN fallback is unlikely to result in better quality of service.
Local Domain		Type the domain name of the SIP network.
Call signaling port	<port value>	If VoIP applications are installed that require nonstandard call signaling ports, enter the port number here. Port number 0 means that the system uses the first available port.
Disable PRACK	Click box to disable PRACK	Provides reliable provisional response messages.
RTP Keepalives	None RTP RTP-RTCP	Real-time Transport Protocol (RTP) and Real-time Control Protocol (RTCP)
Status	Read Only	This field displays the current status of the IP Trunk Gateway.

12. To configure SIP Proxy click the SIP Proxy Tab. Refer to Table 64: SIP Proxy Tab on page 295 for more information.

Table 64: SIP Proxy Tab

Field	Value	Description
Domain	<IP address>	SIP domain serviced by proxy.
Route all calls using Proxy	<check box>	Ignore the SIP entries in the Routing Table - this does not override the H.323 entries, or the H.323 Gatekeeper settings.
MCDN Protocol	None CSE	Choose CSE for CS1000 interoperability.

Field	Value	Description
Optional IP address for legacy routing		Enter the IP address of the BCM if proxy is a CS1000 4.0 system.
Outbound Proxy Table	Name	If there is no IP address given, then this name must be DNS resolvable.
	<IP address>	If known and fixed - name becomes only an identifier in the table.
	<port value>	Non-zero if non-standard.
	Load Balancing	If non-zero, then outgoing calls are distributed by weight among the alive entries. There is only one zero weight entry that will be used (the first in the table) if the non-zero proxies are deemed to be all unavailable.
	Keep Alive	If 'none' then the server will always be considered to be alive. If OPTIONS then a SIP OPTIONS ping is used to determine responsiveness.

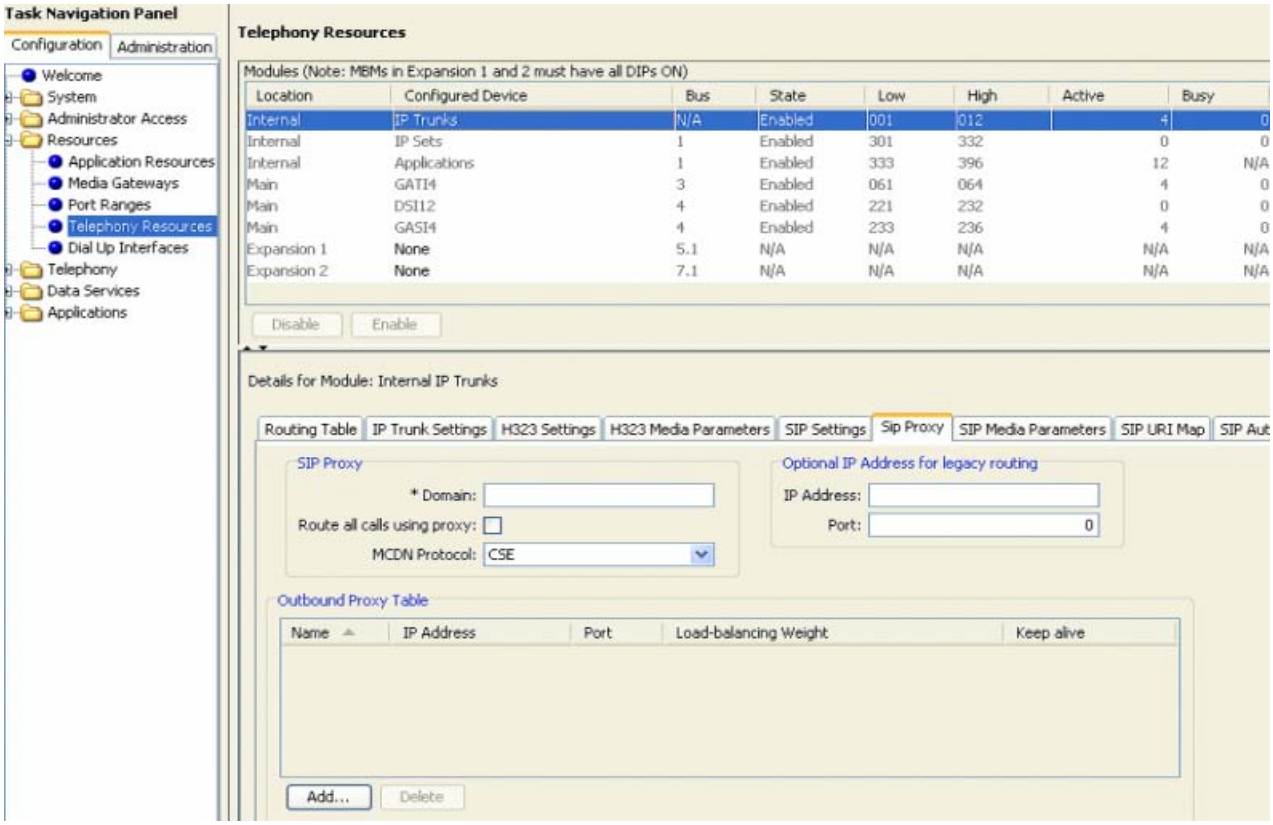

Figure 155: SIP Proxy Tab

Configuring VoIP lines

Voice over IP (VoIP) lines simulate traditional Central Office (CO) lines. VoIP lines transmit data over an IP network rather than over physical lines.

Configuring VoIP lines

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select Telephony > Lines > All Lines.
4. Highlight the individual line you wish to configure.
5. Select the Preferences tab. See Figure 156: Preferences on page 298.

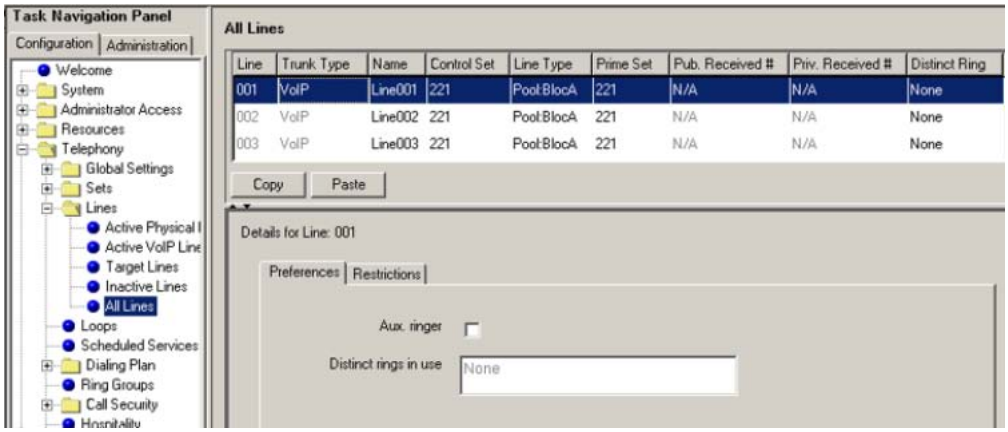

Figure 156: Preferences

6. Configure the Preferences tab appropriately for your network. Refer to Table 65: Preferences fields on page 298 for configuration information.

   Table 65: Preferences fields

Field	Value	Description
Aux. ringer	<check box>	If your system is equipped with an external ringer, you can enable this setting so that this line rings at the external ringer.
Distinct rings in use	Read only	Indicates which ring patterns are already configured on this system.

7. Select the Restrictions tab. See Figure 157: Restrictions on page 299.

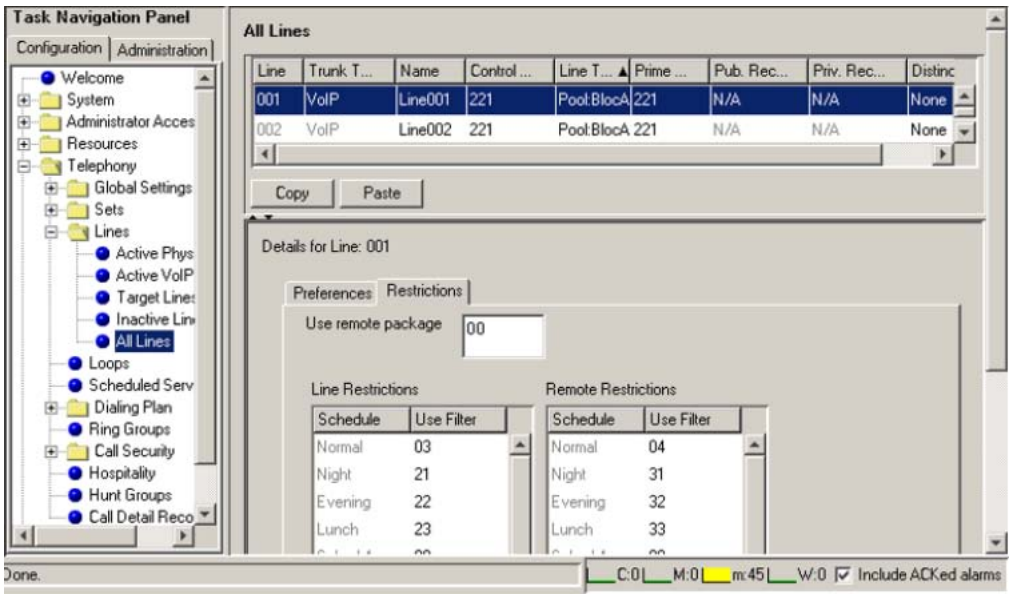

Figure 157: Restrictions

8. Configure the Restrictions tab appropriately for your network. Refer to Table 66: Restrictions fields on page 299 for configuration information.

Table 66: Restrictions fields

Field	Value	Description
Use remote package	< package #>	If the line is used to receive external calls or calls from other nodes on the private network, ensure that you indicate a remote package that provides only the availability that you want for external callers. This attribute is typically used for tandeming calls.
Schedule	Default: Normal, Night, Evening, Lunch, Sched 4, Sched 5, Sched 6	
Line Restrictions - Use Filter	<00-99>	Enter the restriction filter number that applies to each schedule. These settings control outgoing calls.
Remote Restrictions - Use Filter	<00-99>	Enter the restriction filter that applies to each schedule. These settings

Field	Value	Description
		provide call controls for incoming calls over a private network or from a remote user dialing in over PSTN.

9. In the Task Navigation Panel, in the Configuration tab, select Telephony > Sets > All DNs.
10. Highlight the individual line you wish to configure.
11. Select the Line Assignment tab. See Figure 158: Line Assignment on page 300.

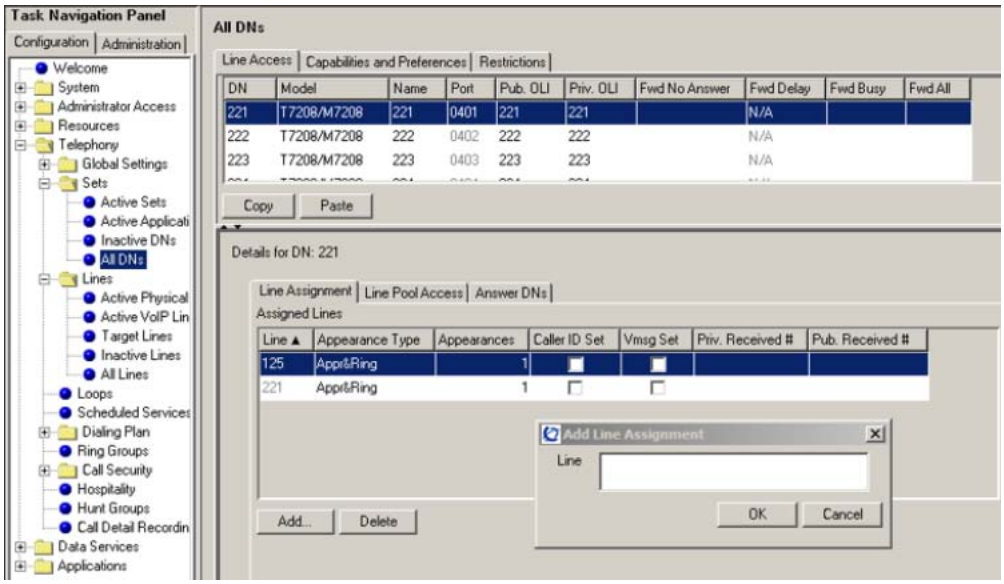

Figure 158: Line Assignment

12. Edit the listed DNs, or click Add to add a DN as required.
13. Enter the appropriate information for your network. Refer to Table 67: Assigned DNs fields on page 300 for configuration information.

Table 67: Assigned DNs fields

Field	Value	Description
DN		Unique number
Appearance Type	Ring Only Appr&Ring Appr Only	Select Appr Only or Appr&Ring if the telephone has an available button. Otherwise select Ring Only.
Appearances		Target lines can have more than one

Field	Value	Description
		appearance to accommodate multiple calls. For telephones that have these lines set to Ring Only, set to None.
Caller ID Set	<check box>	When enabled, displays caller ID for calls coming in over the target line.
Vmsg Set	<check box>	When enabled, an indicator appears on the telephone when a message is waiting from a remote voice mail system. Check with your system administrator for the system voice mail setup before changing this parameter.

Configuring target lines

Target lines are virtual communication paths between trunks and telephones on the BCM system. They are incoming lines only and cannot be selected for outgoing calls or networking applications.

Configuring target lines

1. Log on to BCM Element Manager.
2. In the Task Navigation Panel, select the Configuration tab.
3. Select Telephony > Lines > Target Lines.
4. Highlight the individual line you wish to configure.
5. Select the Preferences tab and enter the appropriate information for your network. See Figure 159: Preferences on page 302. Refer to Table 68: Preferences fields on page 302 for configuration information.

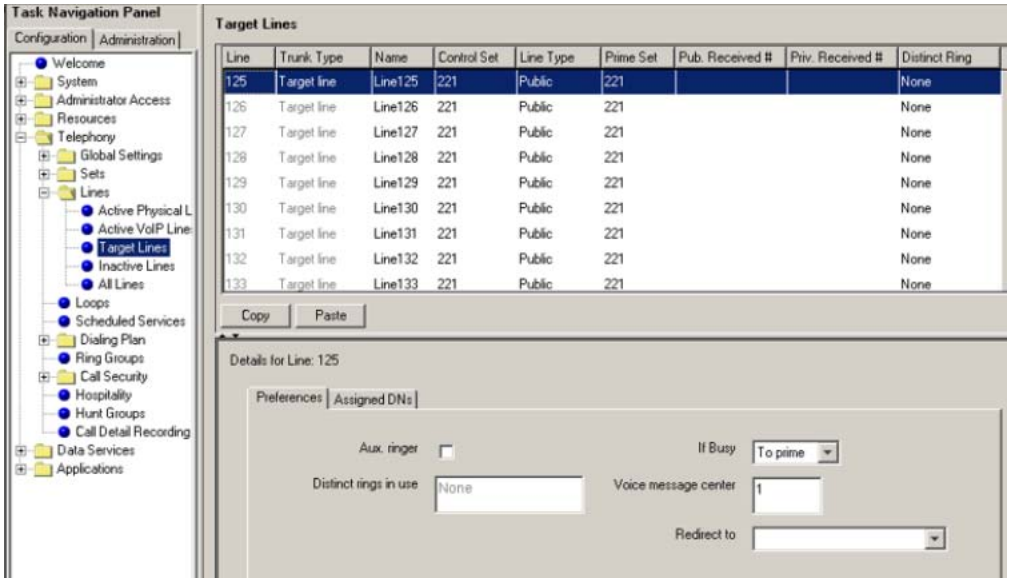

Figure 159: Preferences

Table 68: Preferences fields

Field	Value	Description
Aux. ringer	<check box>	If your system is equipped with an external ringer, you can enable this setting so that this line rings at the external ringer.
If Busy	Busy tone To Prime	To automatically direct calls to the prime telephone, select To prime. Otherwise, select Busy tone.
Distinct rings in use	Read only	
Voice message center		If the system is using a remote voice mail, select the center configured with the contact number.
Redirect to		To automatically direct calls out of the system to a specific telephone, such as a head office answer attendant, enter that remote number here. Ensure that you include

Field	Value	Description
		the proper routing information.

6. Select the Assigned DNs tab. See Figure 160: Assigned DNs on page 303.

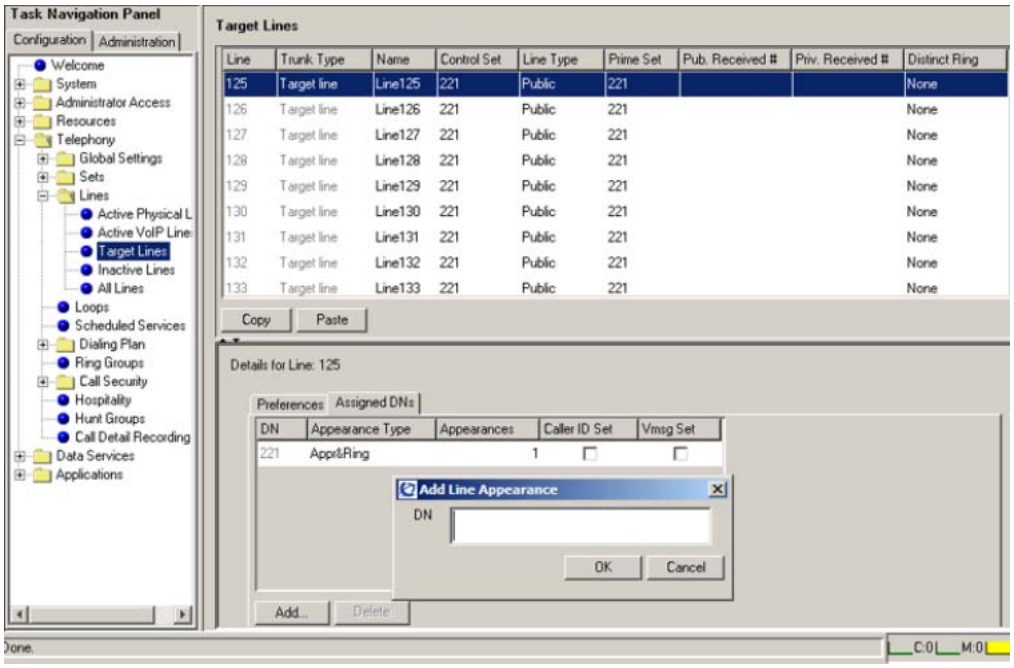

Figure 160: Assigned DNs

7. Edit the listed DNs, or click Add to add a DN as required.
8. Enter the appropriate information for your network. Refer Table 67: Assigned DNs fields on page 300 for configuration information.

Testing and troubleshooting

This chapter contains procedures to test and troubleshoot your Communication Server 1000/ Business Communications Manager (BCM) integration.

Testing and troubleshooting procedures

The sequence of testing and troubleshooting procedures is as follows:

Testing

The CS 1000/BCM integration is considered successful if BCM and Network Routing Service (NRS) are able to register to each other. You can determine this from either the CS 1000 side or the BCM side.

Successful call completion is not a criterion of integration success because call completion is dependent on the dialing plan and how it is implemented. For information about dialing plans, see*Dialing Plans: Description* (NN43001-283).

Testing the integration from the BCM system

To test the integration from the BCM system, complete the following procedure.

Testing the integration from the BCM system

1. Log on to Element Manager on the BCM system.
2. Select Resources > Telephony Resources. See Figure 161: Status on page 305 .

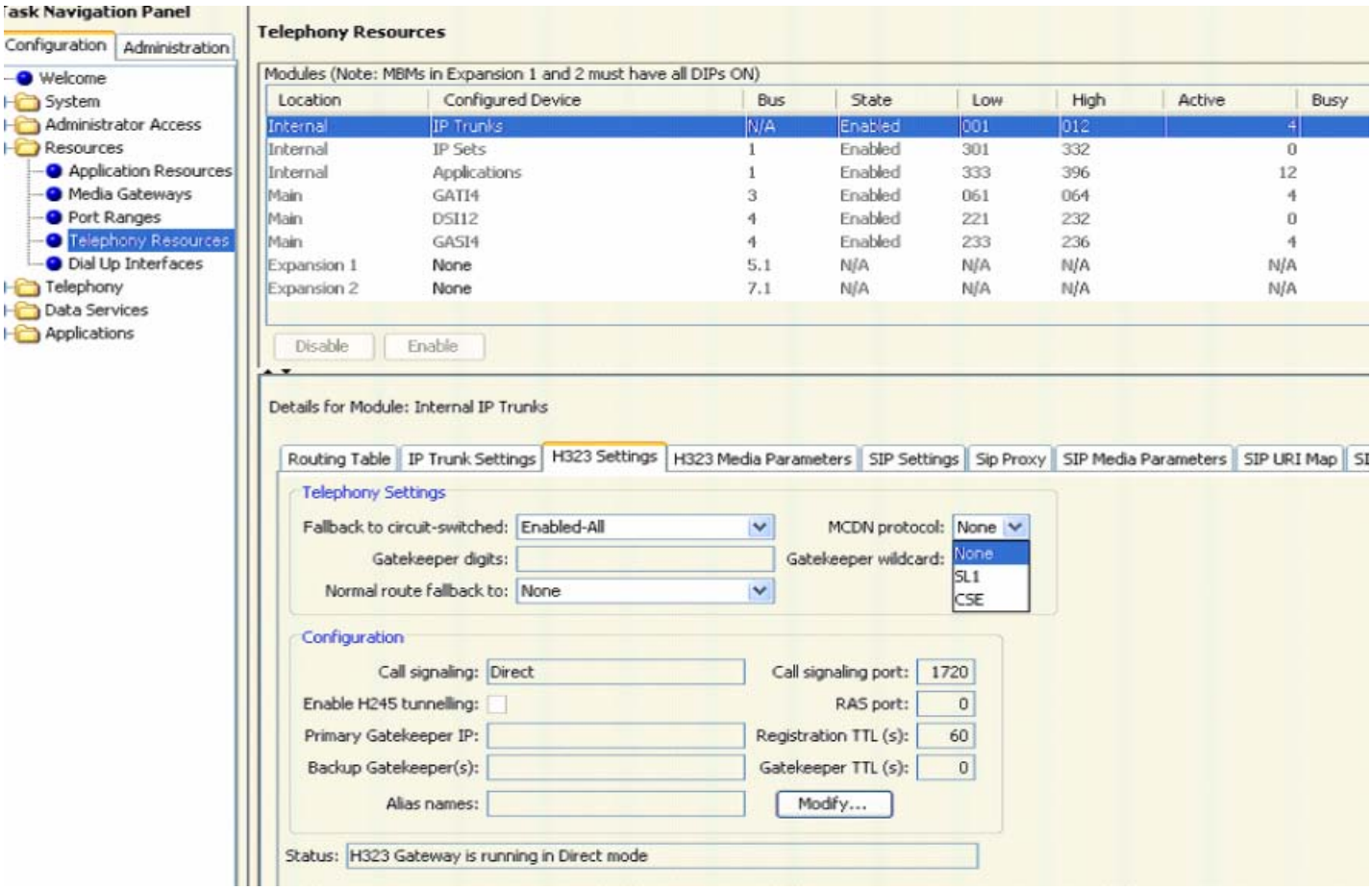

Figure 161: Status

3. In the Actual Type column, highlight IP Trunks.
4. In the bottom half of the page, select the H323 Settings tab.
5. Scroll down to the Status bar to determine if the systems is successfully registered.

Testing the integration from the CS 1000 system

To determine if the two systems are registered from the CS 1000 side, check the status of the endpoints. To check the status of registered endpoints complete the following procedure.

Checking the status of registered endpoints

1. Log on to NRS Manager.
2. Click the Configuration tab.
3. Select Service Domains.
4. Ensure that Active DB View is selected.

5. Click the number in the # of gateway endpoints column.
6. Click Show. The Gateway Endpoints page appears. See Figure 162: Gateway Endpoints on page 306.

Figure 162: Gateway Endpoints

Troubleshooting

Refer to these troubleshooting procedures to resolve common integration issues.

BCM is unable to contact the gatekeeper at IP address

If the BCM is unable to contact the gatekeeper at the IP address, complete the following procedure.

1. Check whether you are able to ping the Gatekeeper across the network. If not, a routing issue can exist in your network. Contact your network administrator to resolve any routing issues.
2. Check that the correct Gateway endpoint IP address is configured in BCM. You may need to reset the feps service under the Service Manager.
3. Check that the correct Gateway endpoint IP address is configured in the CS 1000.
4. Check that the Alias name is properly configured in BCM. The alias name is case sensitive and must match exactly what is configured in the CS 1000.
5. Check that the Gateway protocol is set to CSE.

Unable to complete any calls

If the system is unable to complete any calls, complete the following procedure.

1. Check whether the BCM and Gatekeeper have established connectivity. If not, ensure that the BCM and NRS can communicate with each other.
2. Check that the line is configured for outgoing calls. DNs need to have lines configured for both incoming and outgoing calls. Check your networks dialing plan or see *Dialing Plans: Description* (NN43001-283).
3. Verify that the dialing plan has been properly implemented on both the CS 1000 and BCM. For more information about dialing plans, see *Dialing Plans: Description* (NN43001-283).

Cannot make calls between the CS 1000 and BCM

The following are possible symptoms when calls cannot be made between the CS 1000 system and BCM:

- calls between the CS 1000 and BCM fail
- CDP calls fail
- no channel/circuit is available

If calls cannot be made between the CS 1000 system and BCM, complete the following procedure.

1. Verify your dialing plan and call routing.
2. Log on to BCM Element Manager and select Telephony > Dialing Plan > Private Network.
3. Verify that Private Network Type is set to CDP.
4. Ensure that packets are not blocked by your network firewall.

BCM fails to register to NRS

The following are possible symptoms when the BCM fails to register to NRS:

- BCM fails to register to the NRS
- calls fail between the CS 1000 and BCM in both directions

If calls cannot be made between the CS 1000 system and BCM, complete the following procedure.

1. Check whether you can ping the BCM from the NRS command line. If unsuccessful, check your network settings. Note that the NRS does not respond to pings.
2. In the H323 Settings tab for IP trunks under Resources > Telephony Resources, verify that the BCM includes its alias name as “NAME:aliasname”.
3. Verify that the Alias names match on the NRS and BCM.
4. In the H323 Settings tab for IP trunks under Resources > Telephony Resources, make sure the Gateway protocol is set to CSE.
5. Verify that the NRS has the proper routing entries.

H.323 Gateway service is down

The following are possible symptoms when the H.323 Gateway service is down:

- VoIP H.323 Gateway service is down
- VoIP Gateway cannot be started manually
- VoIP Gateway does not start after a reboot or power cycle

If the H.323 Gateway service is down, complete the following procedure.

1. Log on to BCM Element Manager.
2. Select Resources > Telephony Resources.
3. In the Actual Type column, highlight IP Trunks.
4. Select the H.323 Settings tab and verify that the Call signaling port is set to 1720.
5. Refer to the procedure Testing the integration from the BCM system on page 304.

Chapter 13: Signaling Server error logging and SNMP alarms

Contents

This section contains information on the following topics:

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.

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.

Viewing the error log file

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 163: Node Maintenance and Reports Web page on page 310.

Figure 163: 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 164: MGC Report Logs Web page on page 310. For more information about this page, refer to *Element Manager: System Administration (NN43001-632)*.

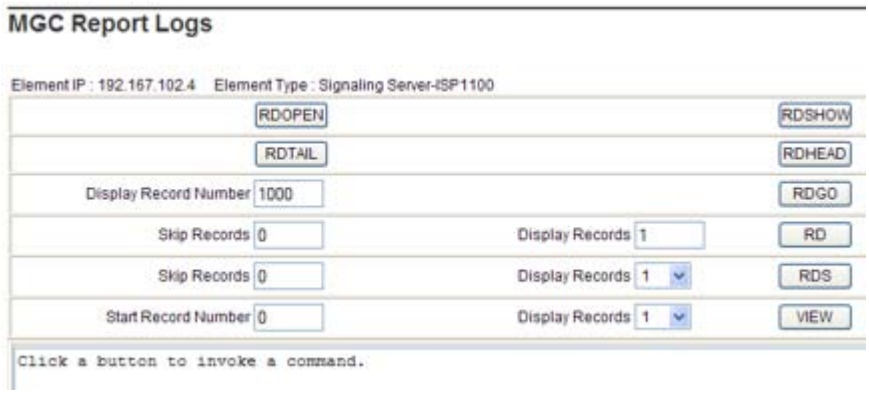

Figure 164: MGC Report Logs Web page

3. Click a button to invoke a command.

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 1000Eand CS 1000Mcomponents. 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 1000Eand CS

1000Mcomponents. 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 A: ISDN/H.323 mapping tables

Nortel proprietary Private UDP numbers (ESN LOC) are encoded as Private Level 1 Regional numbers in H.323. CDP numbers are encoded as Private Level 0 Regional numbers in H.323. In H.225.0 (Q.931) messages, public numbers (E.164) are encoded in the Information Element (IE). Private numbers are encoded in the User to User Information Element (UUIE). On reception, both the IE and UUIE are accepted. If both are included, preference is given to the proper format (that is, the IE for public numbers and the UUIE for private numbers). The numbers in the Signaling Server are encoded using the Universal ISDN Protocol Engine (UIPE) format (which is different from Q.931/MCDN/H.323). Table 69: Mapping from UIPE to H.225.0 for NPI on page 313 to Table 78: Mapping from H.225.0 UUIE to UIPE for Unqualified Number on page 315 describe the mapping.

Table 69: 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 70: Mapping from UIPE to H.225.0 for TON (NPI = E.164/E.163)

TON (NPI=E.164/E.163)	UIPE TON	H.225.0 IE TON	H.225.0 UUIE TON
Unknown	000 (0)	000 (0)	unknown
International number	001 (1)	001 (1)	internationalNumber
National number	010 (2)	010 (2)	nationalNumber
Special number	011 (3)	011 (3)	networkSpecificNumber
Subscriber number	100 (4)	100 (4)	subscriberNumber

Table 71: Mapping from UIPE to H.225.0 for TON (NPI = Private)

TON (NPI = Private)	UIPE TON	H.225.0 IE TON	H.225.0 UUIE TON
Unknown	000 (0)	000 (0)	unknown
ESN LOC (UDP)	101 (5)	000 (0)	level1RegionalNumber
ESN CDP	110 (6)	000 (0)	localNumber
ESN Special Number	011 (3)	000 (0)	pISNSpecificNumber

Note:
When NPI = Private, the number digits are encoded in the privateNumber of PartyNumber, which includes the Type of Number (TON). The TON in the H.225.0 IE are ignored on receipt and coded as Unknown (that is, 0000.) In H.323 version 4.0, publicNumber is renamed e164Number

Table 72: 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 73: Mapping from H.225.0 Information Element to UIPE for TON (NPI = E.164/E.163)

TON (NPI = E.164/E.163)	H.225.0 IE TON	UIPE TON
International number	001 (1)	001 (1)
National number	010 (2)	010 (2)
Network specific number	011 (3)	011 (3)
Subscriber number	100 (4)	100 (4)
Unknown	all others	000 (0)

Table 74: 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)

TON (NPI = Private)	H.225.0 IE TON	UIPE TON
PISN Specific Number	011 (3)	011 (3)
Unknown	all others	000 (0)

Note:
When NPI = Private, precedence is given to any number in the H.225.0 UUIE. The H.225.0 IE is only used if the H.225.0 UUIE is not present. The Presentation Indicator and Screening Indicator are always in the information H.225.0 IE. The H.225.0 UUIE is only used if the H.225.0 IE is not present. In H.323 version 4.0, publicNumber is renamed e164Number.

Table 75: Mapping from H.225.0 UUIE to UIPE for NPI

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

Table 76: Mapping from H.225.0 UUIE to UIPE for TON (NPI = E.164/E.163)

TON (NPI = E.164/E.163)	H.225.0 UUIE TON	UIPE TON
International number	internationalNumber	001 (1)
National number	nationalNumber	010 (2)
Network specific number	networkSpecificNumber	011 (3)
Subscriber number	subscriberNumber	100 (4)
Unknown	all others	000 (0)

Table 77: Mapping from H.225.0 UUIE to UIPE for TON (NPI = Private)

TON (NPI = Private)	H.225.0 UUIE TON	UIPE TON
Level 1 Regional Number	level1 RegionalNumber	101 (5)
Local Number/ Level 0 Regional	localNumber	110 (6)
PISN Specific Number	pISNSpecificNumber	011 (3)
Unknown	all others	000 (0)

Table 78: Mapping from H.225.0 UUIE to UIPE for Unqualified Number

Unqualified Number	H.225.0 UUIE	UIPE NPI	UIPE TON
Dialed Digits	e164	0000 (0)	0000 (0)

Unqualified Number	H.225.0 UUIE	UIPE NPI	UIPE TON
Note: In H.323 version 4.0, e164 is renamed dialedDigits. In H.323 version 4.0, publicNumber is renamed e164Number.			

Appendix B: H.323 Gatekeeper overlap signaling support

Contents

This section contains information on the following topics:

Overlap signaling and H.323 Gatekeeper-routed calls

With H.323 Gatekeeper-routed signaling, admission messages are exchanged between the endpoints and the H.323 Gatekeeper on RAS channels. The H.323 Gatekeeper receives the call-signaling messages on the call-signaling channel from one endpoint and routes them to the other endpoint on the call-signaling channel of the other endpoint.

With direct-routed signaling in the admission confirmation, the H.323 Gatekeeper indicates that the endpoints can exchange call-signaling messages directly. The endpoints exchange the call signaling on the call-signaling channel.

If the H.323 Gatekeeper uses H.323 Gatekeeper routing, it may or may not also use "pre-granted admission". That is, it may not (and usually does not) need the Admission Request message. As a result, the SETUP message is sent to the H.323 Gatekeeper by the Gateway, and all further processing is done by the H.32 gatekeeper.

For processing to succeed, the H.323 Gatekeeper must be fully compliant with H.323 overlap signaling. That is, the H.323 Gatekeeper must be able to receive multiple messages with digits — the SETUP and subsequent INFORMATION messages.

When the calls are H.323 Gatekeeper-routed, the H.323 Gatekeeper must have the ability to do the following:

- decode digits from SETUP and INFORMATION messages
- perform the address resolution

It must then originate overlap calls (or overlap to en bloc, if necessary) to the destination.

Mixed networks of overlap and en bloc H.323 Gatekeepers

Overlap-capable H.323 Gatekeepers can co-reside with H.323 Gatekeepers that cannot do all the necessary overlap functions. As a result, the H.323 Gatekeepers and the H.323 Gateways must be able to accommodate this occurrence.

The simplest example is in the Location Request (LRQ) handling.

- H.323 versions prior to H.323 Release 4.0 do not support the "incomplete address" reason code in the Location Reject (LRJ). As a result, if an overlap H.323 Gatekeeper is registered to a local overlap-capable H.323 Gatekeeper, then the H.323 Gatekeeper sends a digit string in the ARQ that the H.323 Gatekeeper cannot resolve, and that H. 323 Gatekeeper queries its peers.
- However, if the remote H.323 Gatekeeper supports H.323 Release 3 or earlier (or does not support overlap signaling even though the H.323 Gatekeeper conforms to Release 4), no "incomplete" message can be returned.

Any LRQ sent to the remote H.323 Gatekeeper is either rejected with a cause indicating failure, or is ignored. The local H.323 Gatekeeper can determine its own capabilities; however, it cannot determine the capabilities of the remote H.323 Gatekeeper. The local H.323 Gatekeeper also cannot "guess" the returned reasons. For example, a "request denied" may have been triggered by a messaging error or by the sender not having any way to indicate an incomplete number.

To resolve this issue, when a local H.323 Gatekeeper determines from the local provisioning and received responses that no completion can occur, it returns either the Default Route as the destination in the ACF or an ARJ indicating failure to the gateway. However, because differentiation between a "normal ACF" and a "default route ACF" cannot be made, the non-standard data is enhanced to indicate this to the gateway. This indication is done in the non-standard data because the element includes vendor information and, as a result, non-Nortel gateways can read the manufacturer information and ignore the data.

As part of the protocol, all endpoints supporting the protocol must have a predefined way to handle the indication. That is, if the H.323 Gatekeeper indicates that a default route was selected (or would have been selected if the entry had been provisioned) by sending the Default Route Indicator (DRI), then any gateway supporting the protocol must have a predetermined general handling procedure to handle the indication.

The rationale for the general handling procedure is simple. The protocol is designed to be fully forward-compatible. If any recommendation (DRI Recommendation [DRIR]) sent to a gateway

by the H.323 Gatekeeper cannot be found in the list of DRIR values understood by the gateway, then the gateway must have a defined procedure for handling this event. That is, the following algorithm applies:

- If the gateway recognizes the recommendation and it is completely valid, the gateway uses the recommendation.
- If the gateway recognizes the recommendation but there is a reason that it cannot apply (for example, if a recommendation such as "wait for more digits" existed but the call was from an en bloc gateway and there are no more digits), the gateway uses either the general handling procedure or some other selected procedure.
- If the gateway does not recognize the recommendation, it uses the general handling procedure. This includes recommendations that have not yet been defined, so the protocol covers forward compatibility.

The importance of this capability within a mixed network is simple. If LRQs are broadcast to the peer H.323 Gatekeepers and no positive responses return, then this may be because no positive responses are possible; the number may be completely undefined. On the other hand, the H.323 Gatekeeper "may just not have responded" but the number may be valid.

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

There are two key concepts behind the recommendations:

- First, calls placed using overlap signaling to an en bloc gateway use processing resources that they do not need to use. The SETUP and subsequent INFORMATION messages can trigger multiple Admission Requests to the H.323 Gatekeeper, which in turn can trigger Location Requests throughout a significant part of the IP telephony network. If the average count of ARQs for each call doubles, then the maximum through-put of the H.323 Gatekeeper in calls per hour is halved. For an en bloc call, there is only a single ARQ, which either succeeds or fails the first time.
- Second, calls placed to an en bloc gateway can terminate prematurely to a terminal to handle failed calls. That is, misdialed numbers can route to a specified answering position such as an Attendant, the Security Desk, or some other site. If the destination gateway is provisioned with this sort of capability, then the calls that should have been rejected and sent back to the originator for overlap-to-en bloc conversion. However, the calls receive manual overlap-to-en bloc conversion, as the caller tells the party (answering the intercepted call) the destination that the caller really wanted.

A third item acting as a base for the recommendations is call control traffic on the Signaling Server. Although the call control traffic is not heavy enough to make optimization necessary, it does provide additional justification. Overlap signaling adds some overhead, but much less on the H.323 signaling gateway than on the H.323 Gatekeeper.

With this background information, the following recommendations apply:

1. Even though a gateway may support overlap signaling, if the H.323 Gatekeeper that the gateway uses does not support overlap signaling, then do not provision the gateway as overlap.

   Note:
   All further recommendations assume that the H.323 Gatekeeper supports overlap signaling.

2. Assume that an en bloc destination is registered with the local H.323 Gatekeeper. If this destination is known to be en bloc only, but returns the "unassigned number" or "invalid number format" cause codes, then the administrator can provision the originating Call Server to leave this call as an overlap call. The returned cause code in the RELEASE COMPLETE message triggers overlap-to-en bloc conversion. However, the Overlap Length (OVLL) prompt (in LD 86) must be configured to a value that gives a reasonable probability that the H.323 Gatekeeper can resolve the call on the first attempt. This is to avoid excessive querying of the H.323 Gatekeeper.
3. Assume that an en bloc destination is registered with the local H.323 Gatekeeper. If this destination is known to be en bloc only, but either will not return the desired cause code or will intercept the call, then provision the entry on the originating Call Server with an en bloc Route List Index (RLI). That is, even though the D-channel can accept overlap signaling, define the RLI used for this call with an OVLL of 0. This forces the call into en bloc handling.
4. Assume that an en bloc destination is registered with a remote H.323 Gatekeeper. En bloc destinations, that must be reached using Location Request (LRQ) messages to their H.323 Gatekeeper, are subject to the limitations of that H.323 Gatekeeper. The en bloc destination is also subject to their own limitations regarding handling incomplete numbers. If possible, these destinations should be provisioned as en bloc using OVLL 0, since the remote H.323 Gatekeeper may not be able to handle an overlap call LRQ with an incomplete called-party digit string.
5. Assume that an en bloc destination is registered with a remote H.323 Gatekeeper and OVLL on the originating Call Server is not configured as 0. H.323 Gatekeepers that cannot support overlap signaling may not be able to respond to an LRQ message with an LRJ message to reject the call. If this occurs, the Signaling Server attempts overlap-to-en bloc conversion (unless a prior reply indicated either a successful termination at another destination or that the number was incomplete on another H.323 Gatekeeper). If the local H.323 Gatekeeper fails to receive any response to its LRQ from one or more H.323 Gatekeepers while all others indicate failure, and it has a default route defined, this is provided to the gateway. In addition, the H,323 Gatekeeper provides an indication that the call was terminated to the default route. This allows the gateway to either route the call to the default route destination, or to try overlap-to-en bloc conversion. Therefore, Nortel recommends that the administrator provision any CS 1000 Release 4.0 (or later) H.323 Gatekeepers (with the NRS) with a default route.

6. Assume that a destination is known to be en bloc and OVLL is configured to 0. For all these en bloc destination numbers, if the length of the number is known, then ensure that the Flexible Length (FLEN) prompt is provisioned for that number. Provisioning the FLEN of an eight-digit number as 8 triggers an immediate SETUP on dialing the eighth digit. If the FLEN is longer (or configured to 0), then the Call Server runs an end-of-dial timer to determine whether the number is complete. Failing to configure the FLEN correctly adds several seconds to the post-dial delay (the time between the last digit being dialed and hearing 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 RLIs.
10. If a call is a remote E.164 plan (International, National, or Local/Subscriber) type of number, then this call must traverse the IP network as a Special Number (SPN). Otherwise, all overlap capability is lost. At the node where the call tandems to the PSTN, the type of number is changed to International, National, or Local (as applicable). However, if the PSTN supports these as overlap calls, then it is guaranteed that the node must be able to receive them as overlap as well. Therefore, provision the originating Call Server with this call as an SPN, and prefix any local numbers with the national code. Then, if it is required that local calls not have national prefixes at the destination, then when the call to the PSTN breaks out to the PSTN, remove any national prefixes from calls going to the local area.

Appendix C: ISDN cause code to SIP status code mapping tables

When an ISDN: Release message is received before receiving a SIP final response, a 4xx/5xx message is sent to the far end indicating a corresponding error situation. Table 79: ISDN cause code to SIP status code mapping on page 323 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 79: ISDN cause code to SIP status code mapping on page 323 is received, the default SIP response 500 Server internal erroris 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 79: ISDN cause code to SIP status code mapping on page 323 shows the ISDN cause code to SIP status code mapping, and Table 80: ISDN cause code to SIP status code mapping on page 325 shows the SIP error response to ISDN cause code mapping.

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

Table 79: ISDN cause code to SIP status code mapping on page 323 shows the ISDN cause code to SIP status code mapping.

Table 79: 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

ISDN cause code	SIP response
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
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 80: ISDN cause code to SIP status code mapping on page 325 shows the SIP error response to ISDN cause code mapping.

Table 80: 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
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

SIP response	ISDN cause code
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 D: 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 authorizations(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.