Enterprise: Common

Solution Integration Guide for Communication Server 1000 Release 5.5/Business Communications Manager

NN43001-326

Document status: Standard
Document version: 02.01
Document date: 3 April 2009

Sourced in Canada

Contents

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 of product release. To check for updates to the latest documentation and software, go to the Nortel Technical Support Web site:

www.nortel.com/support

Getting help from the Nortel Web site

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

www.nortel.com/support

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 phone 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 phone 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 phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

About this document

This document describes the planning, configuration, and troubleshooting of the integration of the Business Communications Manager (BCM) with a Communication Server 1000 system. 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 guide:

- Communication Server 1000 (CS 1000) Release 5.5
- 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 50 (BCM50) Release 3.0

This document is intended to be a stand-alone guide, covering the prerequisites to and implementation of a successful CS 1000/BCM integration. A minimum skill set and level of understanding are assumed. References to other NTPs, engineering guides, or troubleshooting guides are made for informational purposes.

Audience

The intended audience for this document includes installation, planning, and maintenance personnel.

Related information

The following NTPs are referenced in this guide:

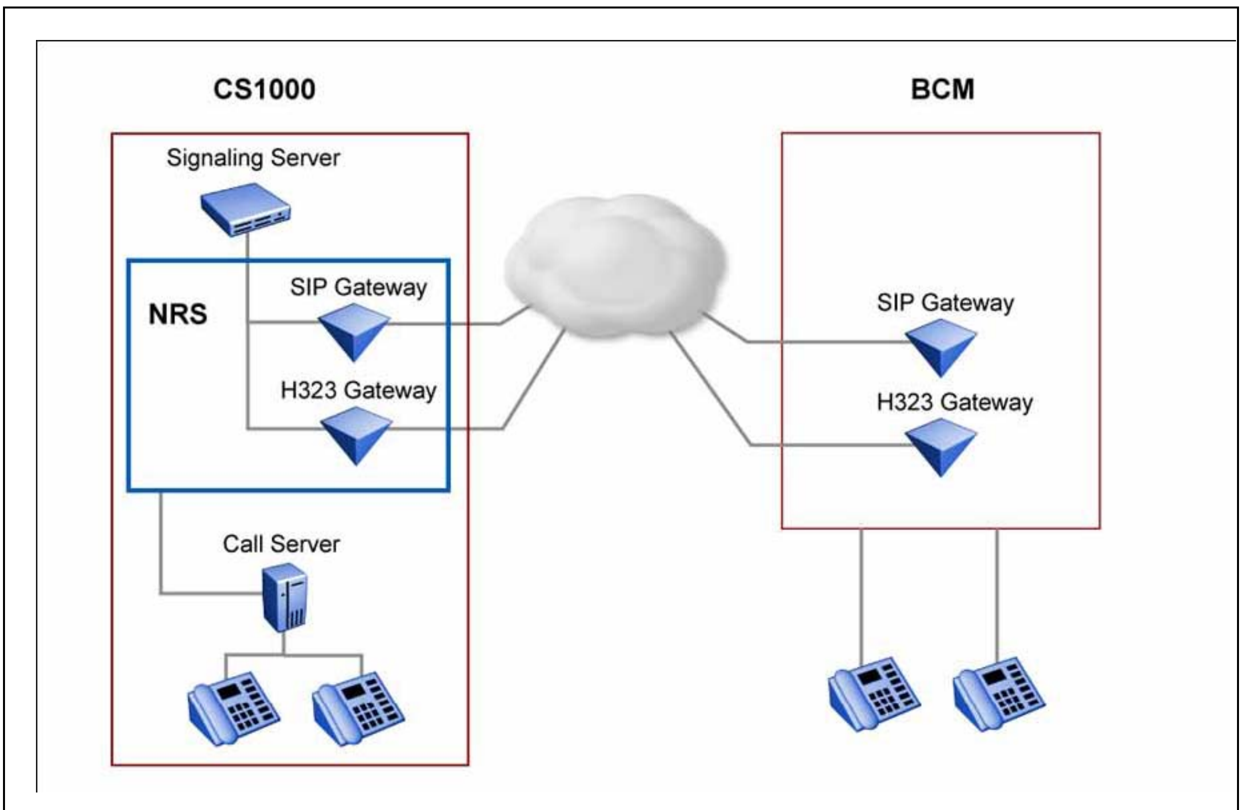
- *BCM 4.0 Device Configuration Guide* (N0060600)
- *BCM 4.0 Telephony Device Installation Guide* (N0060609)
- *BCM50 Networking Configuration Guide* (NN40020-603)
- *Communication Server 1000E: Installation and Configuration* (553-3041-210)

- *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)
- *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210)
- *Communication Server 1000S: Installation and Configuration* (553-3031-210)
- *Dialing Plans: Description* (553-3001-183)
- *IP Line Description, Installation, and Maintenance* (553-3001-365)
- *IP Peer Networking Installation and Configuration Guide* (553-3001-213)
- *Keycode Installation Guide* (NN40010-301)
- *Signaling Server: Installation and Configuration* (553-3001-212)

Overview

An example of a Communication Server 1000/Business Communications Manager (BCM) systems integration is shown in Figure 1 "CS 1000/BCM architecture" (page 11).

Figure 1
CS 1000/BCM architecture

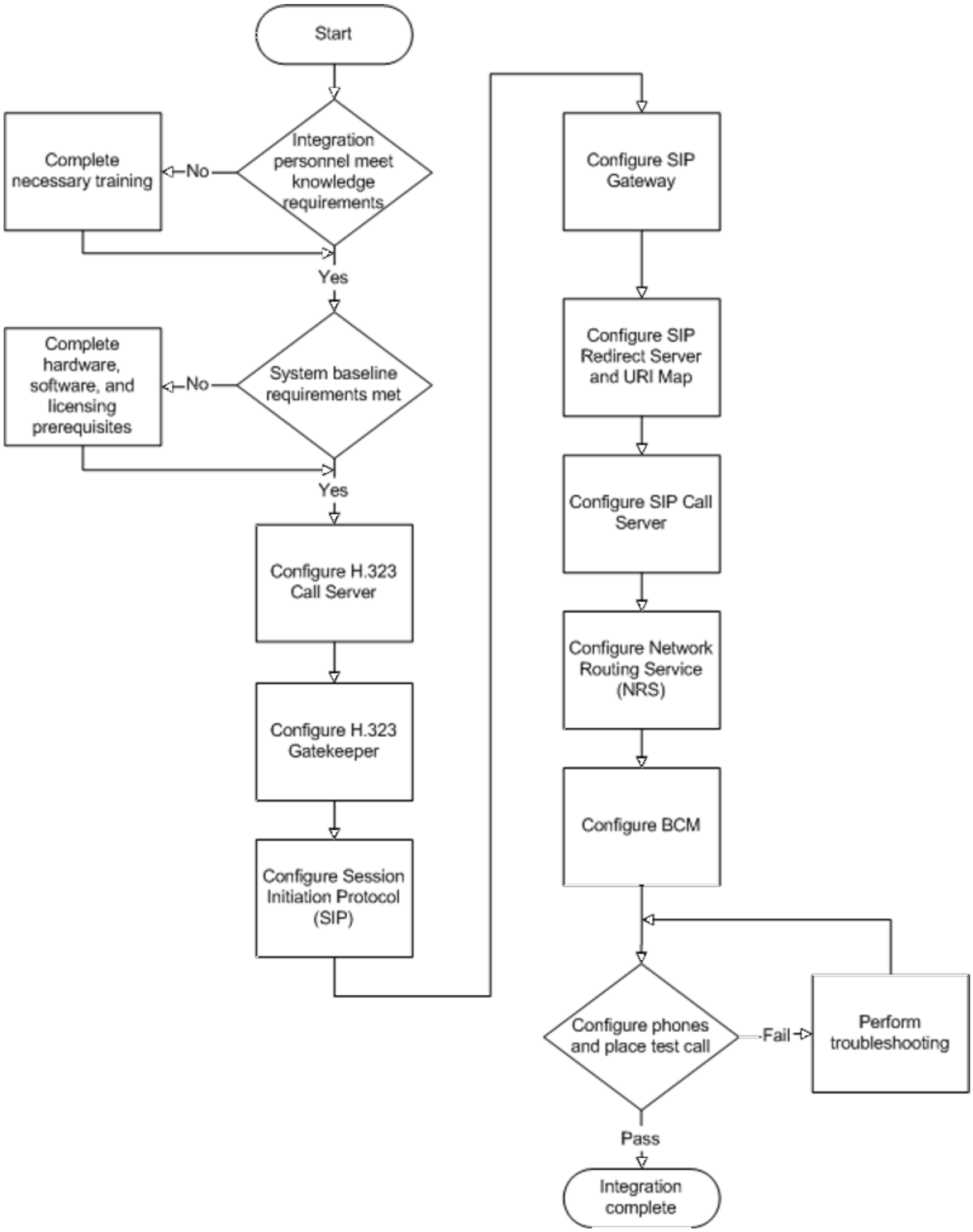


CS1000 Gateway IP address	10.10.11.1	
CS1000 Endpoint IP address	10.12.12.3	
BCM 400 Endpoint IP address	10.20.12.8	BCM Gateway Alias name BCM40
Signaling Server T-LAN IP Address	10.12.13.1	

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 2 "CS 1000/BCM integration process" (page 13) shows the sequence of procedures you perform to integrate the CS 1000 and BCM systems.

Figure 2
CS 1000/BCM integration process



The tasks in the CS 1000/BCM systems integration process are listed in Table 1 "Task Completion Checklist" (page 14). Use this checklist to implement the integration.

Table 1
Task Completion Checklist

	Task	Reference
	Configure the H.323 Call Server	1. "Defining the customer to support ISDN" (page 27) 2. "Creating the virtual D-channel" (page 28) 3. "Configuring zones (LD 117)" (page 31) 4. "Creating the virtual route (LD 16)" (page 32) 5. "Creating the virtual trunks (LD 14)" (page 34) 6. "Creating the ESN data block for CDP" (page 36) 7. "Creating the Network Control Block (NCTL) for network access (LD 87)" (page 38) 8. "Creating the RLB for the virtual trunk route (LD 86)" (page 40) 9. "Creating the CDP steering codes (LD 87)" (page 41) 10. "Checking CODEC and QoS settings" (page 43)
	Configure the H.323 Gatekeeper	"Configuring Element Manager" (page 46)
	Configure the SIP protocol	"Enabling the SIP Virtual Trunk application" (page 48)
	Configure the SIP Gateway	"Configuring the SIP Gateway" (page 50)
	Configure the SIP Redirect Server and URI Map	"Configuring the SIP Redirect Server and URI map" (page 52)
	Configure the SIP Call Server	1. "Defining the customer to support ISDN" (page 54) 2. "Creating the virtual D-channel" (page 56) 3. "Configuring zones (LD 117)" (page 59) 4. "Creating the virtual route (LD 16)" (page 60) 5. "Creating the virtual trunks (LD 14)" (page 62) 6. "Creating the ESN data block for CDP" (page 64) 7. "Creating the Network Control Block (NCTL) for network access (LD 87)" (page 66) 8. "Creating the RLB for the virtual trunk route (LD 86)" (page 68) 9. "Creating the CDP steering codes (LD 87)" (page 69) 10. "Checking CODEC and QoS settings" (page 71)

	Task	Reference
	Configure NRS	1. "Launching NRS Manager" (page 75) 2. "Verifying and adjusting system-wide settings" (page 76) 3. "Configuring the NRS server settings (H.323 Gatekeeper or SIP)" (page 78) 4. "Configuring the service domain" (page 80) 5. "Configuring the L1 domain (UDP)" (page 81) 6. "Configuring the L0 domain (CDP)" (page 83) 7. "Configuring Gateway endpoints" (page 86) 8. "Configuring routing entries" (page 90) 9. "Configuring collaborative servers" (page 92) 10. "Updating the database" (page 94) 11. "Checking the status of registered endpoints" (page 95) 12. "Checking the status of virtual D-channels" (page 96) 13. "Checking the status of virtual trunks" (page 97)
	Configure BCM	BCM 200/400 1. "Configuring incoming VoIP trunks" (page 99) 2. "Verifying system license and keycodes" (page 100) 3. "Configuring VoIP trunk media parameters" (page 101) 4. "Configuring local Gateway parameters" (page 104) 5. "Configuring target lines" (page 109) 6. "Configuring VoIP lines" (page 112) BCM50 1. "Configuring incoming VoIP trunks" (page 119) 2. "Verifying system license and keycodes" (page 120) 3. "Configuring VoIP trunk media parameters" (page 121) 4. "Configuring local Gateway parameters" (page 125) 5. "Configuring VoIP lines" (page 130) 6. "Configuring target lines" (page 134)

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" (page 17)
- "Capturing integration parameters" (page 18)
- "Establishing the system baseline" (page 19)

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 www.nortel.com

Capturing integration parameters

Table 2 "Integration parameters" (page 18) provides a list of parameters required to successfully complete the integration. Record these parameters during the initial planning phase of the integration.

Table 2
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)	
T-LAN IP address of the Signaling Server	
T-LAN 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	
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	

Parameter	Value
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 3 "Pre-integration checklist" (page 19) to complete system baselines prior to integration.

Table 3
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* (553- 3001-183)	Are you using a Uniform Dialing Plan (UDP) or a 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 5.5.		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.

	Task	Reference	Comments
			3 The software release is referred to as Release.
	Signaling Server software is Release 5.5.		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: Small System Installation and Configuration* (553-3011-210) *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210) *Communication Server 1000S: Installation and Configuration* (553-3031-210) *Communication Server 1000E: Installation and Configuration* (553-3041-210) *Signaling Server: Installation and Configuration* (553-3001-212)	

	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: Installation and Configuration* (553-3001-212)	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* (553-3001-213)	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* (553-3001-213)	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.	*IP Line Description, Installation, and Maintenance* (553- 3001-365)	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**.

	Task	Reference	Comments
			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 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.		

	Task	Reference	Comments
	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.
	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.		To check the software version: **1** Log on to Element Manager. **2** Select the **Configuration** tab. **3** Expand the **System** folder. **4** Select **Identification**.

	Task	Reference	Comments
	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* (NN40010-30	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* (NN40010-30	To check Feature Licenses: **1** Log on to Element Manager. **2** Select the **Configuration** tab. **3** Expand the **System** folder. **4** Select **Keycodes**.

CS 1000 setup and IP Peer Networking configuration

Although you can configure the Communication Server 1000 and IP Peer Networking through overlays, the use of Element Manager and Network Routing Services (NRS) Manager are recommended. The Element Manager Web server resides on the Signaling Server and you can access it directly through a Web browser or by using Optivity Telephony Manager (OTM). You must configure NRS through Network Routing Service Manager (NRS Manager), which you can access only through the Element Manager.

Configure the Call Server through Element Manager in the following order:

- H.323 Call Server
- H.323 Gate Keeper
- Session Initiation Protocol (SIP)
  - SIP Protocol
  - SIP Gateway
  - SIP Redirect Server and URI Map
  - SIP Call Server
  - Network Routing Service in the NRS Manager
  - SIP addressing
  - SIP virtual trunking

CS 1000/IP Peer Networking configuration procedures

The sequence of CS 1000/IP Peer Networking configuration procedures is as follows:

- "Configuration of H.323 Trunks in the Call Server" (page 26)
  - "Defining the customer to support ISDN" (page 27)
  - "Creating the virtual D-channel" (page 28)
  - "Configuring zones (LD 117)" (page 31)

Configuration of H.323 Trunks in the Call Server

The procedures in this section are as follows:

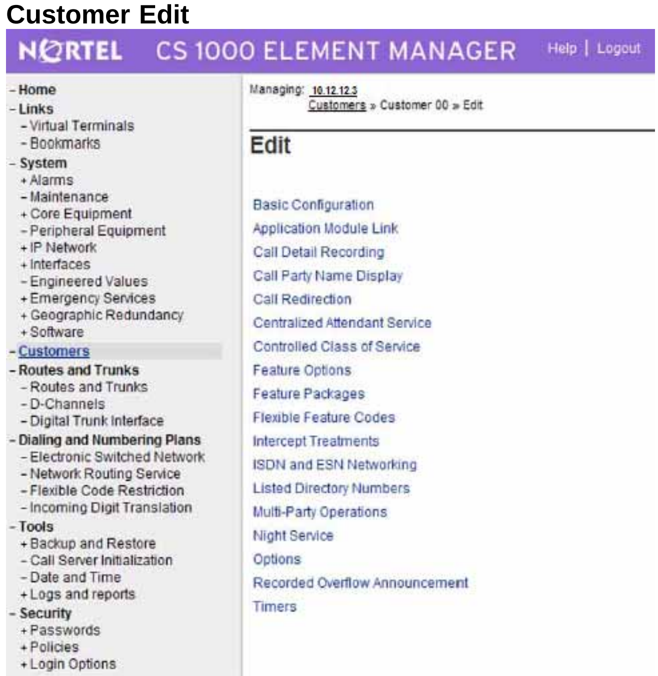
- "Creating the ESN data block for CDP" (page 36)
- "Configuring the L0 domain (CDP)" (page 83)
- "Creating the RLB for the virtual trunk route (LD 86)" (page 40)
- "Creating the CDP steering codes (LD 87)" (page 41)
- "Checking CODEC and QoS settings" (page 43)

Defining the customer to support ISDN

Complete the following procedure to define the customer to support ISDN.

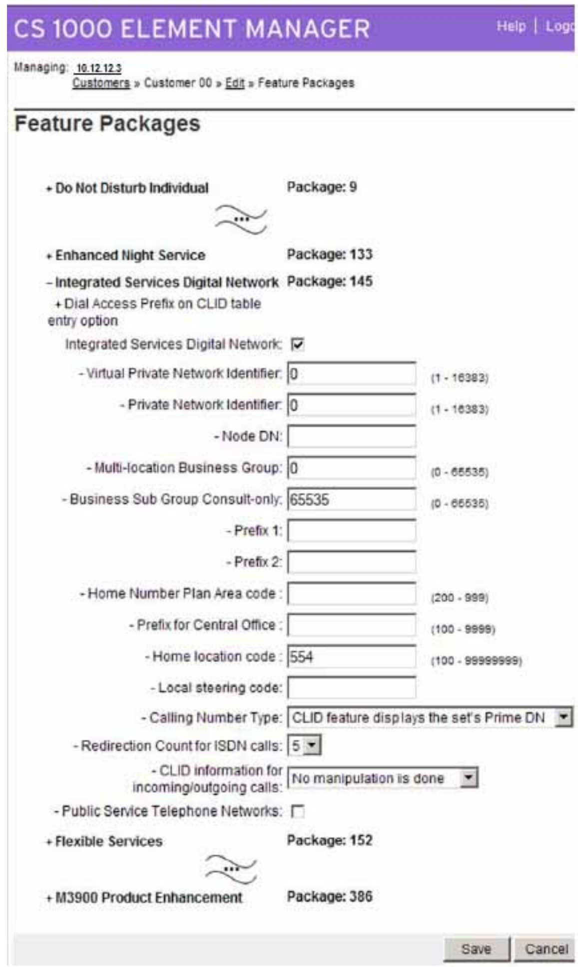
Step	Action
1	Log on to Element Manager.
2	Select **Customers**.
3	Select the **Customer Number** you wish to edit. The Customer Edit page appears. See Figure 3 "Customer Edit" (page 27).

Figure 3
Customer Edit



4	Select the **Feature Packages** heading. The Feature Packages page appears. See Figure 4 "Feature Packages" (page 28).

Figure 4
Feature Packages



5 Expand the **Integrated Services Digital Network Package 145** heading.

6 Ensure that the **Integrated Services Digital Network** check box is selected.

7 Click **Save**.

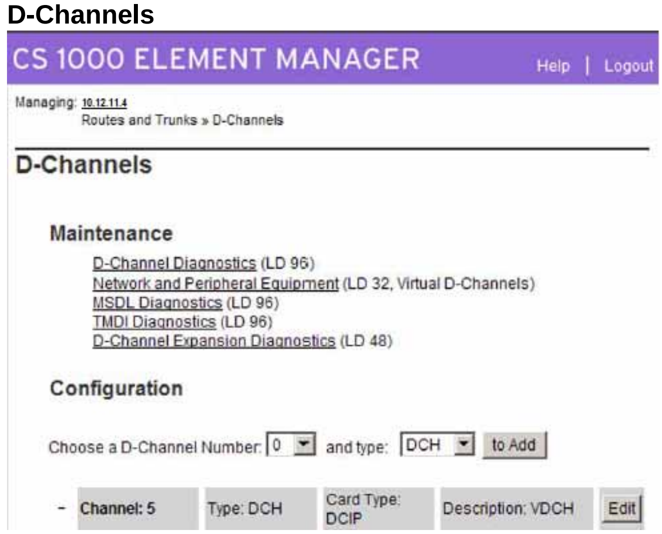
—End—

Creating the virtual D-channel

Perform the following procedure to create the virtual D-channel.

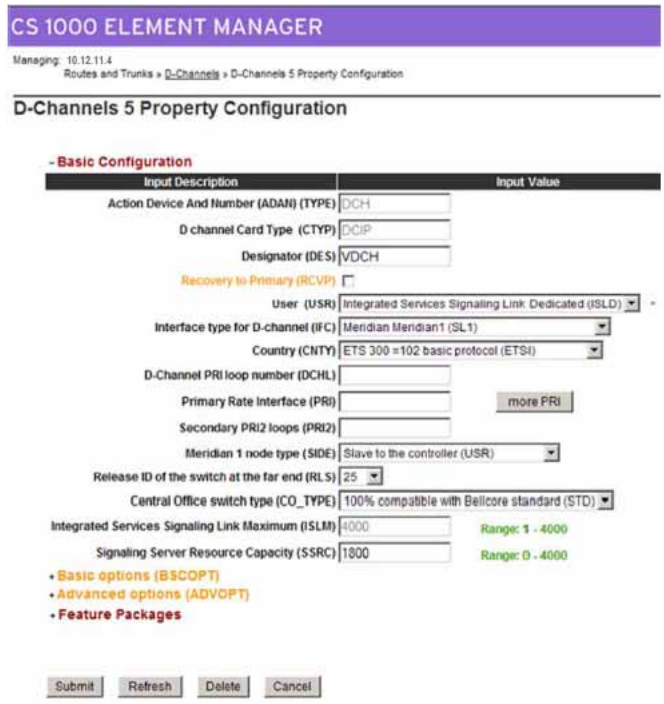
Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > D-Channels**. A message appears if a D-channel is not configured. Click **OK**. The D-Channels page appears. See Figure 5 "D-Channels" (page 29).

Figure 5
D-Channels



Step	Action
3	From the **Choose a D-Channel Number** menu, select the D-Channel number. D-channels 0,1, and 2 are usually used or shared with other applications. It is recommended that you begin configuring virtual D-channels on channel 3.
4	From the **Type** menu, select the D-Channel type.
5	Click **to Add**. The D-Channels Property Configuration page appears. See Figure 6 "D-Channels Property Configuration" (page 30).

Figure 6
D-Channels Property Configuration



6 For the **D channel Card Type (CTYP)**, select **D-Channel is over IP (DCIP)**.

7 For the **Designator (DES)**, type a meaningful name.
The Designator must not contain spaces; use underscores instead.
Make a note of the Designator in your records for future reference.

8 For **User (USR)**, select **Integrated Services Signaling Link Dedicated (ISLD)**.

9 For **Interface type for D-channel (IFC)**, select **Meridian Meridian1 (SL1)**.

10 Leave all other parameters as is and click **Submit**.
The new channel appears.

—End—

Configuring zones (LD 117)

Before you can configure the virtual routes and trunks, the following zones must be configured, in any order:

- Zone 1 = IP Phones zone (ZBRN = MO)
- Zone 2 = Voice Gateway Channels zone, which should be different from the IP Phones zone (ZBRN = VTRK)

Ensure that enough bandwidth is allocated for the zones with the heaviest traffic.

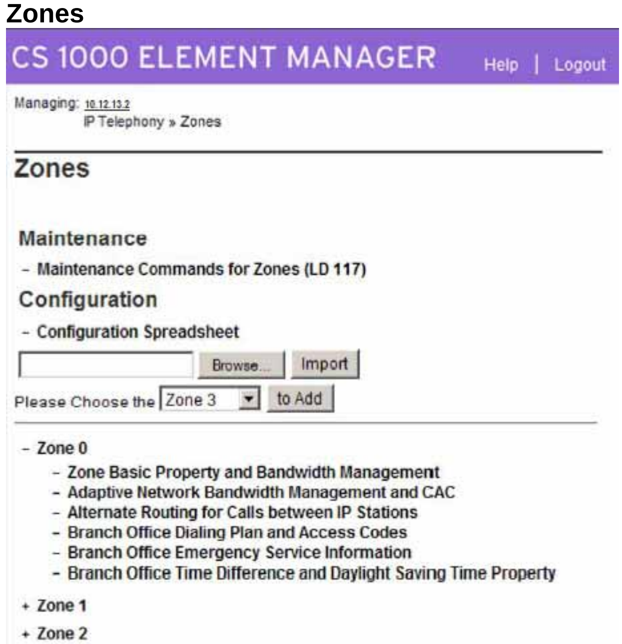
Never use or configure zone 0.

Step **Action**

1 Log on to Element Manager.

2 Select **System > IP Network > Zones**.
See Figure 7 "Zones" (page 31).

Figure 7
Zones



3 Select the **Zone** you wish to configure.
Configured zones appear in the list at the bottom of the page.

4 Click **to Add**.

5 After you click **to Add**, a message may appear prompting you to use the Zone Basic Property and Bandwidth Management Spreadsheet. Click **OK**.

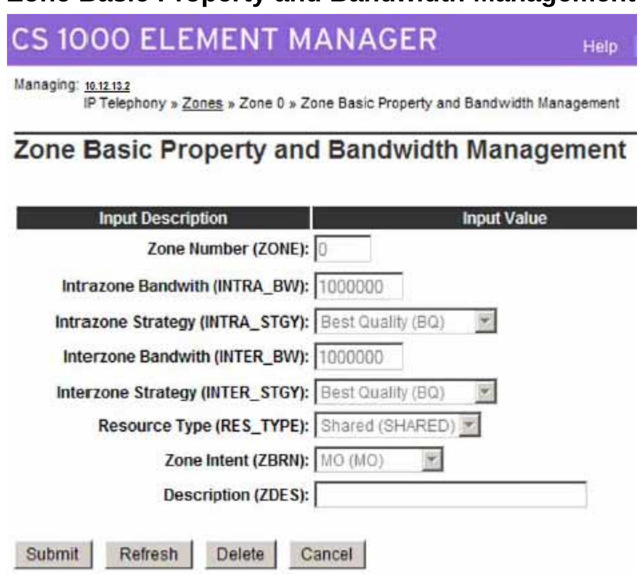
6 Leave the default values for bandwidth and resource type as is.

7 Set the **Zone Intent (ZBRN)** as follows:

- Zone 1 is for the IP Phones at the Main Office. Set Zone Intent (ZBRN) for Zone 1 to **MO (MO)**.
- Zone 2 is for the Voice Gateway Channels. Set Zone Intent (ZBRN) for Zone 2 to **VTRK (VTRK)**.

See Figure 8 "Zone Basic Property and Bandwidth Management" (page 32).

Figure 8
Zone Basic Property and Bandwidth Management



8 For **Description (ZDES)**, type a meaningful description.

9 Click **Submit**.

10 Repeat this procedure for all additional zones you wish to create.

—End—

Creating the virtual route (LD 16)

Perform the following procedure to create the virtual route.

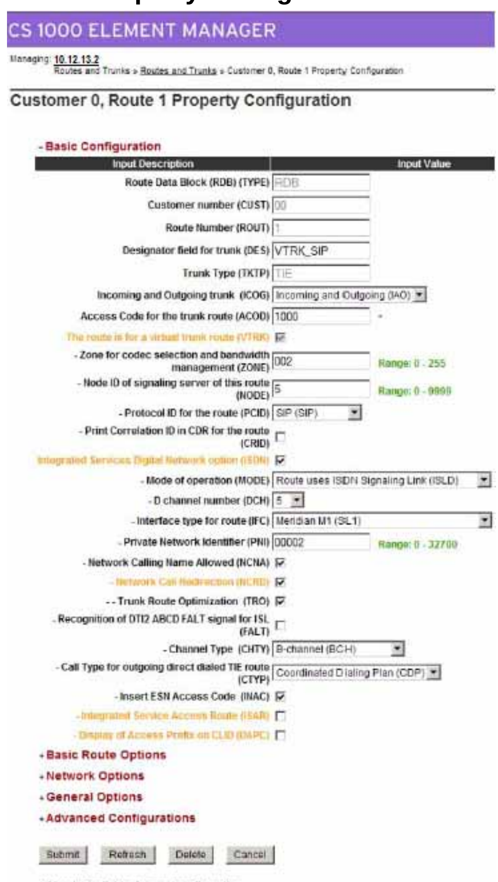
Step	Action

1 Log on to Element Manager.

2 Select **Routes and Trunks > Routes and Trunks**.

3 Click the **Add route** button.
The Route Property Configuration page appears. The trunk type (TKTP) you choose determines the parameters available on this page. SeeFigure 9 "Route Property Configuration" (page 33) for one possible view of the Route Property Configuration page.

Figure 9
Route Property Configuration



4 Select the **Route Number (ROUT)**.

5 For **Designator field for trunk (DES)**, type a meaningful name.

6 For **Trunk Type (TKTP)**, select **TIE trunk data block (TIE)**.

7 For **Incoming and Outgoing trunk (ICOG)**, select **Incoming and Outgoing (IAO)**.

8 Set the **Access Code for the trunk route (ACOD)**.

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

10 Type the **Zone** number of the zone with the ZBRN set to Vtrk for the new route.
This value must match the values you configure in the Signaling Server.

11 Type the **Node ID of signaling server of this route (NODE)**.
This value must match the values you configure in the Signaling Server.

12 For **Protocol ID for the route (PCID)**, select **SIP (SIP)**.

13 Select the **Integrated Services Digital Network option (ISDN)** check box.

14 For **Mode of operation (MODE)**, select **Route uses ISDN Signaling Link (ISLD)**.

15 Select the virtual **D channel number (DCH)**.

16 For **Interface type for route (IFC)**, select **Meridian M1 (SL1)**.

17 Leave the **Call Type for outgoing direct dialed TIE route (CTYP)** at the default value.
It is best to let NARS/BARS entries determine the NPI/TON for a number so that the route can be used for multiple call types.

18 Select the **Insert ESN Access Code (INAC)** check box.

19 Leave the other default values as is and click **Submit**.
The Routes and Trunks page appears showing the created routes.

—End—

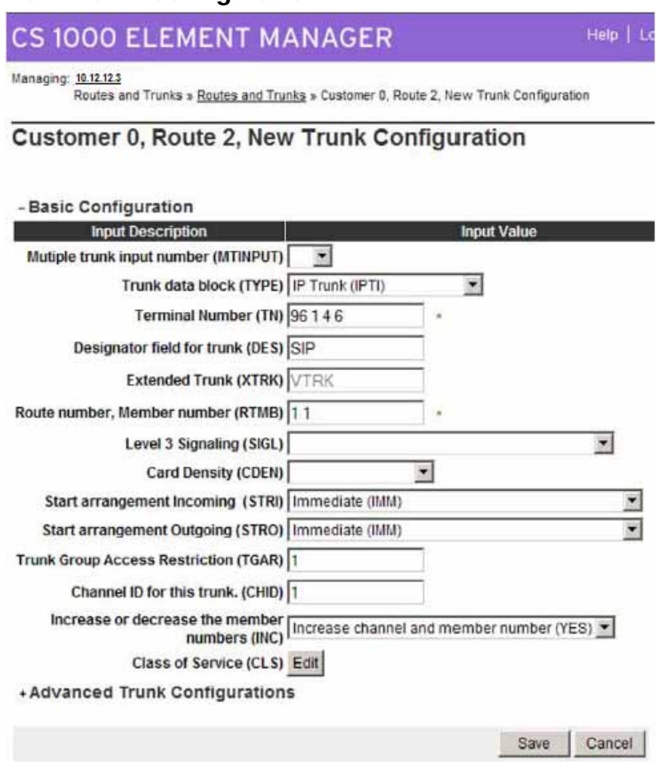
Creating the virtual trunks (LD 14)

The Virtual Trunk TNs that you configure in this procedure cannot overlap with the ones that you configure for IP Phones.

Create separate virtual routes for SIP and H.323. The SIP route is configured in the procedure "Configuring IP networking for SIP" (page 54).

Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > Routes and Trunks**.
3	Expand the **Customer** heading.
4	Click **Add trunk** next to the route to which you wish to add the trunk. The New Trunk Configuration page appears. See Figure 10 "New Trunk Configuration" (page 35). Your configuration determines the parameters available on this page.

Figure 10
New Trunk Configuration



Step	Action
5	If you are configuring several trunks the same way, select the **Multiple trunk input number (MTINPUT)** (optional).
6	For **Trunk data block (TYPE)**, select **IP Trunk (IPTI)**.
7	Type the **Terminal Number (TN)** for the trunk.
8	For **Designator field for trunk (DES)**, type a meaningful value.
9	Type the **Route number, Member number (RTMB)** for the trunk.

10 Set the values of **Start arrangement Incoming (STRI)** and **Start arrangement Outgoing (STRO)**.
Immediate (IMM) is recommended for both fields.

11 Type the **Channel ID for this trunk (CHID)**.

12 You can add a Class of Service (CLS) for all features that you wish. In a basic configuration, you can leave the CLS as is.

13 Select **Advanced Trunk Configurations** to display a list of advanced features.

14 Edit the necessary fields or accept the default values.

15 Click **Submit**.

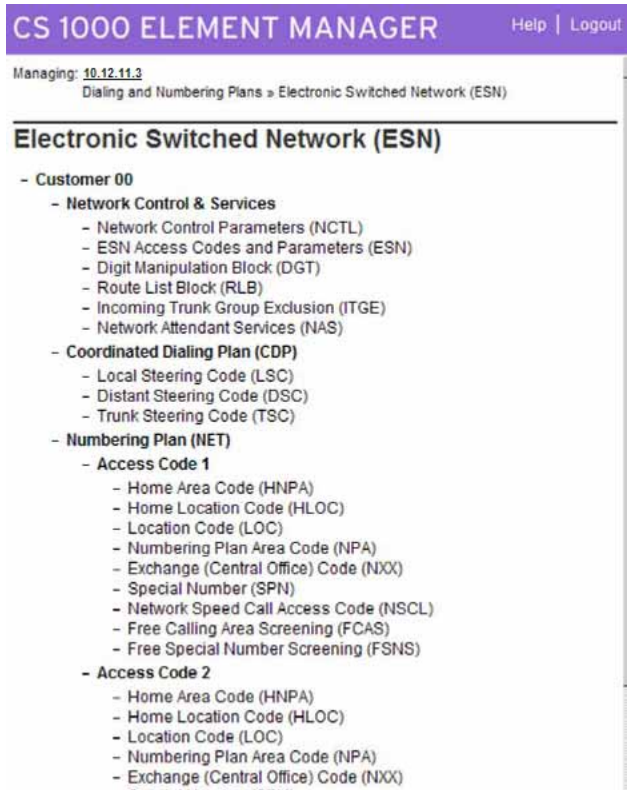
—End—

Creating the ESN data block for CDP

Perform the following procedure to create the ESN data block for CDP.

Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans > Electronic Switched Network**. The Electronic Switched Network page appears. See Figure 11 "Electronic Switched Network" (page 37).

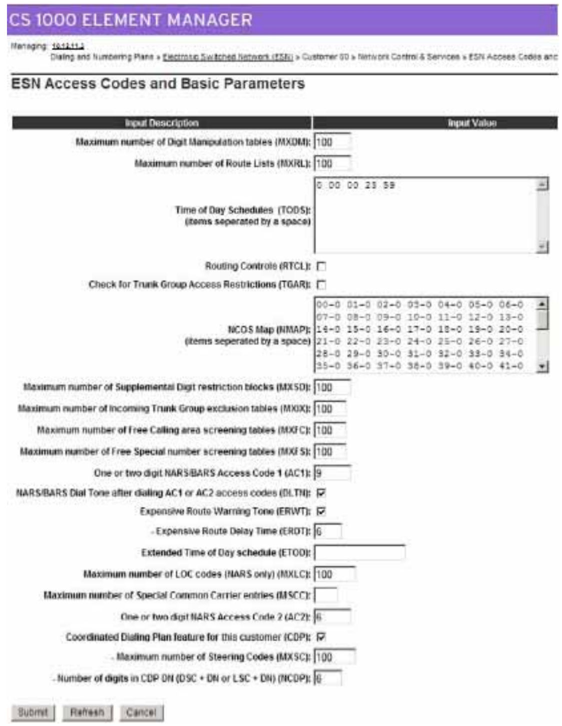
Figure 11
Electronic Switched Network



3 Select **Customer > Network Control & Services > ESN Access Codes and Parameters (ESN)**.

4 A message appears if ESN data is not configured. Click **OK**.
The ESN Access Codes and Basic Parameters page appears. See Figure 12 "ESN Access Codes and Basic Parameters" (page 38).
If ESN data is configured on your switch, the fields on this page appear populated.

Figure 12
ESN Access Codes and Basic Parameters



5 Edit the main parameters (**MXDM**, **MXRL**, **MXSD**, **MXIX**, **MXFC**, **MXFS** and **MXLC**) if required, or leave the default values as is.

6 Select the **Coordinated Dialing Plan feature for this customer (CDP)** check box.

7 Set the value of the **Maximum number of Steering Codes (MXSC)**.

8 Set the value of the **Number of digits in CDP DN (DSC+DN or LSC+DN) (NCDP)**.

9 Click **Submit**.

—End—

Creating the Network Control Block (NCTL) for network access (LD 87)

Perform the following procedure to create the Network Control Block.

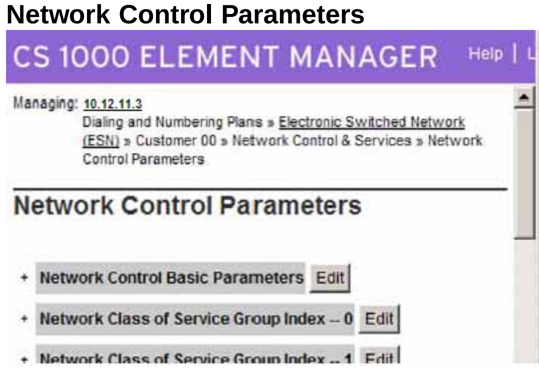
Step	Action
1	Log onto Element Manager.

2 Select **Dialing and Numbering Plans > Electronic Switched Network**.

3 Select **Customer > Network Control & Services > Network Control Parameters (NCTL)**.
See Figure 11 "Electronic Switched Network" (page 37).

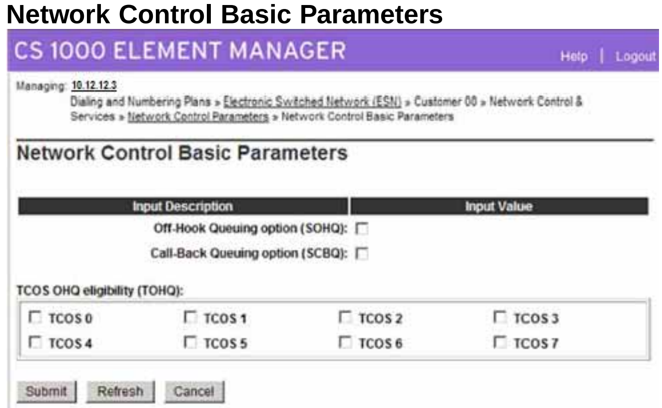
4 A message appears if no network control data is configured. Click **OK** to configure new data.
The Network Control Parameters page appears. See Figure 13 "Network Control Parameters" (page 39).

Figure 13
Network Control Parameters



5 Click the **Edit** button next to Network Control Basic Parameters.
The Network Control Basic Parameters page appears. See Figure 14 "Network Control Basic Parameters" (page 39).

Figure 14
Network Control Basic Parameters



6 Choose the basic control parameters for your network.

7 Click **Submit**.

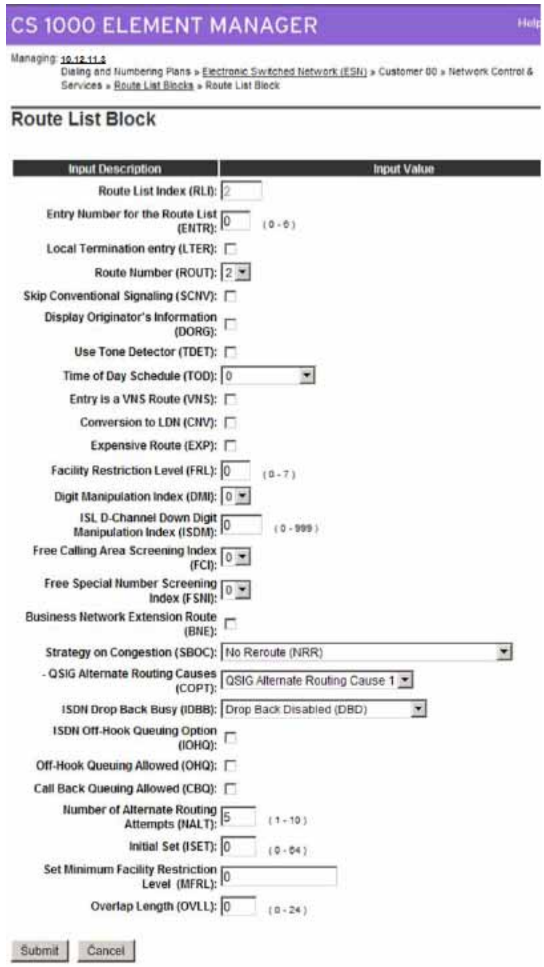
—End—

Creating the RLB for the virtual trunk route (LD 86)

Perform the following procedure to create the RLB for the virtual trunk route.

Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans > Electronic Switched Network**.
3	Select **Customer > Network Control & Services > Route List Block (RLB)**. If route list blocks are not configured, the error message “Route List does not exist” appears. Click **OK**.
4	Type the **Route List Index number**.
5	Click **to Add**. The Route List Block Configuration page appears. See Figure 15 "Route List Block" (page 41).

Figure 15
Route List Block



6 Select the **Route Number (ROUT)** you previously defined.

7 For **Strategy on Congestion (SBOC)**, select **Reroute All (RRA)**.

8 Accept the other defaults and click **Submit**.
The new Route List Block is generated. You can check the configuration by selecting Route List Block Index and Data Entry Index.

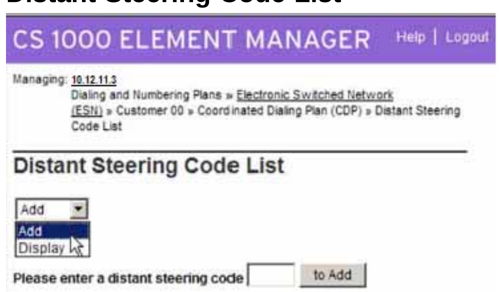
—End—

Creating the CDP steering codes (LD 87)

Perform the following procedure to create the CDP steering codes.

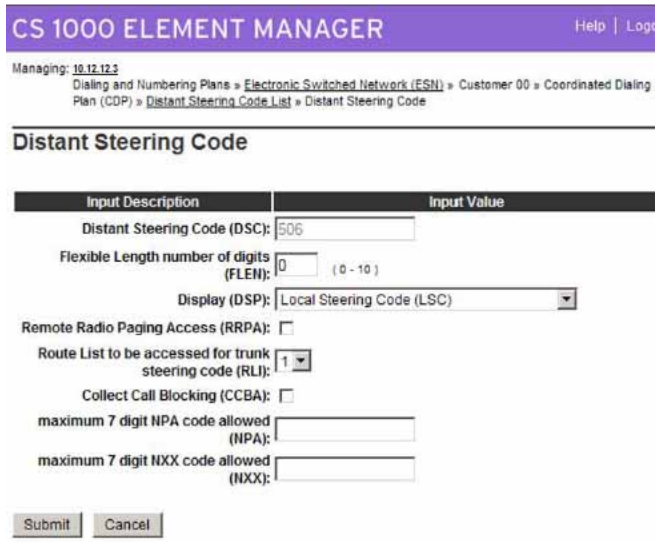
Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans > Electronic Switched Network**. The Electronic Switched Network page appears. See Figure 11 "Electronic Switched Network" (page 37).
3	Select **Customer > Coordinated Dialing Plan (CDP) > Distant Steering Code (DSC)**. The Distant Steering Code List page appears. See Figure 16 "Distant Steering Code List" (page 42).

Figure 16
Distant Steering Code List



Step	Action
4	Select **Add** to add a new Distant Steering Code.
5	Enter a **Distant Steering Code (DSC)**. The Distant Steering Code is a unique identifier for remote switches or locations. Add a Distant Steering Code for all remote locations.
6	Click **to Add**. The Distant Steering Code page appears. See Figure 17 "Distant Steering Code" (page 43).

Figure 17
Distant Steering Code



7 Check that the parameters are configured appropriately for your system.

8 Select a **Route list to be accessed for trunk steering code (RLI)**.

9 Click **Submit**.

10 Repeat this procedure for all other DSCs on your network.

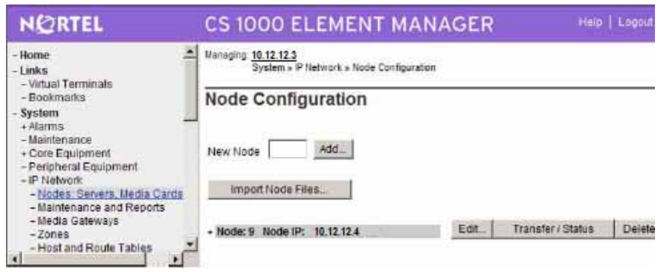
—End—

Checking CODEC and QoS settings

At this point, the Call Server configuration is complete. It is recommended that you check the CODEC and QoS settings.

Step	Action
1	Log on to Element Manager.
2	Select **System > IP Network > Nodes: Servers, Media Cards**. See Figure 18 "Node Configuration" (page 44).

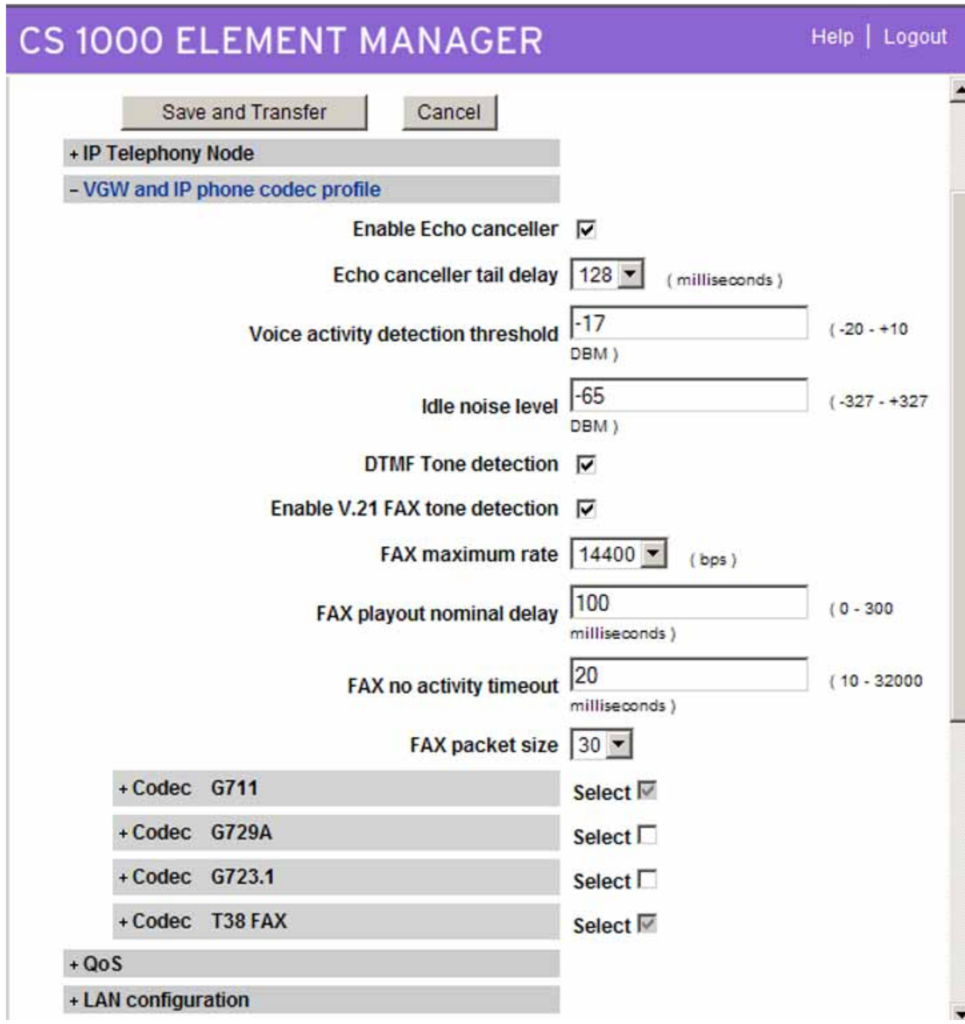
Figure 18
Node Configuration



3 Click **Edit**.

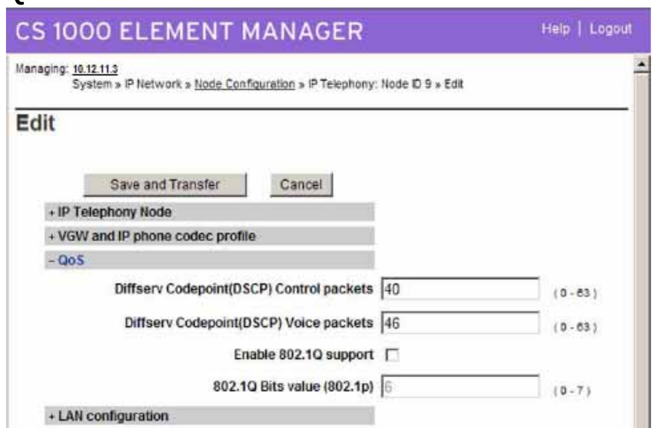
4 Expand the **VGW and IP phone codec profile** heading and edit the fields as necessary.
See Figure 19 "VGW and IP phone codec profile" (page 45).

Figure 19
VGW and IP phone codec profile



5 Expand the **QoS** heading and edit the fields as necessary. See Figure 20 "QoS" (page 46).

Figure 20
QoS



6 If you make configuration changes, click **Save and Transfer**. When the successful transfer notification message appears, click **OK**.
If you do not make configuration changes, click **Cancel**.

—End—

H.323 Gatekeeper configuration

Configure the H.323 Gatekeeper in both Element Manager and the NRS. Configure the Element Manager before the NRS.

The sequence of H.323 Gatekeeper configuration procedures is as follows:

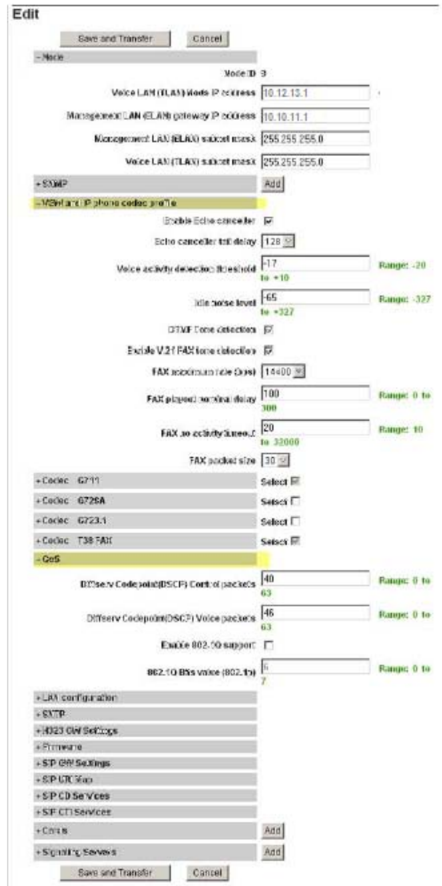
- "Configuring Element Manager" (page 46)

Configuring Element Manager

Set the Primary and Alternate Gatekeeper IP addresses. This IP address is configured at each H.323 Gateway (Signaling Server).

Step	Action
1	Log on to Element Manager.
2	Select **System > IP Network > Nodes:Servers, Media Cards**. See Figure 18 "Node Configuration" (page 44).
3	Click **Edit** next to the node you are configuring.
4	Expand the **H.323 GW Settings** heading. See Figure 21 "H323 Gateway and Signaling Server" (page 47).

Figure 21
H323 Gateway and Signaling Server



5 Enter the **Primary Gatekeeper (TLAN) IP address**.
This is the T-LAN IP address of the Signaling Server that runs the Gatekeeper application. This is not the same as the Node IP.

6 Enter the **Alternate Gatekeeper (TLAN) IP address** if you have an alternate on your system (optional).

7 Expand the **Signaling Servers** heading.

8 Expand the **Signaling Server Properties** heading at the bottom of the page.

9 Enter the **H323 ID**.
This should be the same as the Signaling Server that hosts the Primary H.323 Gatekeeper. Make a note of the H323 ID for the NRS configuration.
The host name does not need to be the same as the H323 ID, but it is recommended that both names are the same.

10 Select the **Enable Gatekeeper** check box.

11 If you make configuration changes, click **Save and Transfer**. When the successful transfer notification message appears, click **OK**.
If you do not make configuration changes, click **Cancel**.

—End—

SIP protocol configuration

The procedures in this section are as follows:

Configuration for the SIP protocol is very similar to that of the Call Server.

If you select YES at the CRID prompt, a new line (SIP message) is added to the end of the Call Detail Record. This message shows the SIP addressing scheme.

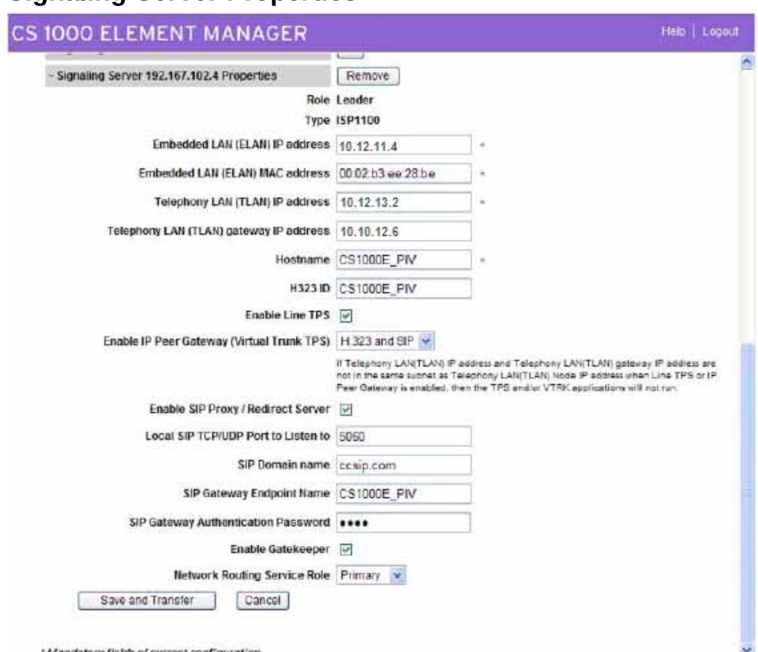
The SIP Gateway also supports H.323 Gateway functionality so that both Gateways can interoperate. Also, you can point the virtual trunks, whether they are H.323 or SIP, to the same node ID on the signaling server. Then, the signaling server can perform the signaling for both protocols.

Enabling the SIP Virtual Trunk application

Perform the following procedure to enable SIP functionality in Element Manager. You must reboot the system during this procedure.

Step	Action
1	Log on to Element Manager.
2	Select **System > IP Network > Nodes: Servers, Media Cards**. See Figure 18 "Node Configuration" (page 44).
3	Click **Edit** next to the node you are editing.
4	Expand the **Signaling Servers** heading.
5	Expand the **Signaling Server Properties** heading. See Figure 22 "Signaling Server Properties" (page 49).

Figure 22
Signaling Server Properties



Step	Action
6	For **Enable IP Peer Gateway (Virtual Trunk TPS)**, select a SIP option (**SIP only** or **H.323 and SIP**).
7	Select the **Enable SIP Proxy/Redirect Server** check box.
8	Check that **Local SIP TCP/UDP Port to Listen to** is set appropriately. The default is 5060.
9	Enter the **SIP Domain name**.

The SIP Domain Name must be less than 128 characters in length. Valid characters are a-z, 0-9, period, hyphen, comma, and underscore.
This string builds all SIP messages and appears in the URI phone context. If you enable the SIP Gateway application, specify this field. This name must match the Service Domain name configured in NRS.

10 Enter the **SIP Gateway Endpoint Name** and **SIP Gateway Authentication Password**.
These values must match the data in NRS. The SIP Gateway Endpoint Name becomes the Gateway's user ID.

11 If you make configuration changes, click **Save and Transfer**. When the successful transfer notification message appears, click **OK**.
If you do not make configuration changes, click **Cancel**.

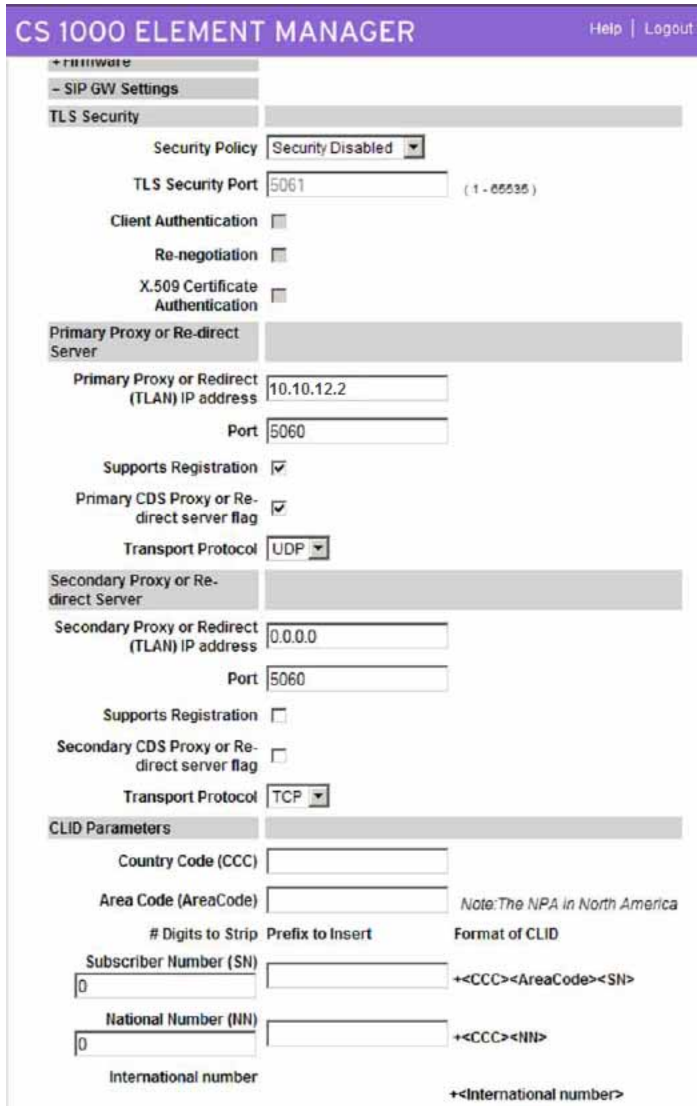
—End—

Configuring the SIP Gateway

Before you configure the SIP Gateway, check which route is configured as a SIP route in LD 16. You must configure this route later.

Step	Action
1	Log on to Element Manager.
2	Select **System > IP Network > Nodes: Servers, Media Cards**. See Figure 18 "Node Configuration" (page 44).
3	Click the **Edit** button next to the node you are configuring.
4	Expand the **SIP GW Settings** heading. See Figure 23 "SIP GW settings" (page 51).

Figure 23
SIP GW settings



5 In the Primary Proxy or Redirect Server section, type the **Primary Proxy or Re-direct (TLAN) IP address**.

6 In the Primary Proxy or Redirect Server section, type the **Port** number. The default port value is 5060.

7 Select the **Supports Registration** check box.

8 Select the **Transport Protocol**.

9 If you plan to configure a secondary or redundant proxy server, repeat steps 6 through 9 for the Secondary Proxy or Re-direct Server section.

10 If you make configuration changes, click **Save and Transfer**. When the successful transfer notification message appears, click **OK**.
If you do not make configuration changes, click **Cancel**.

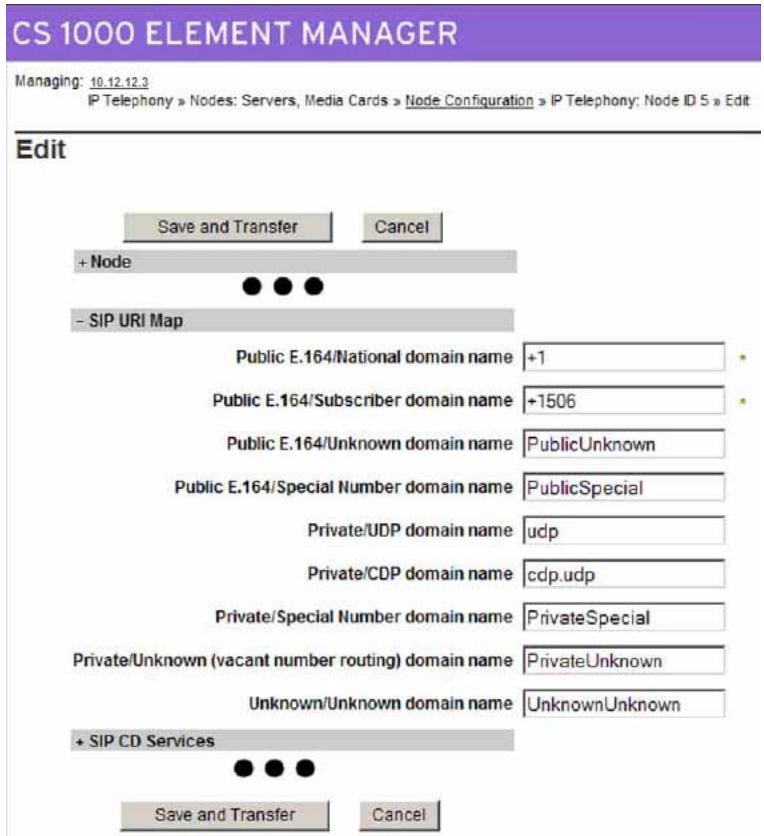
—End—

Configuring the SIP Redirect Server and URI map

Use this procedure to configure your SIP numbering plan mapping. You can use this mapping to interpret TON/NPI numbers and map them to the associated context (to or from SIP). The TON/NPI field explicitly maps to the SIP phone-context attribute in the URI address.

Step	Action
1	Log on to Element Manager.
2	Select **System > IP Network > Nodes:Servers, Media Cards**.
3	Click the **Edit** button beside the node to be edited.
4	Expand the **SIP URI Map** heading. See Figure 24 "Edit SIP URI Map" (page 53).

Figure 24
Edit SIP URI Map



5 For **Private/UDP domain name**, type the L1 domain.

6 For **Private/CDP domain name**, type the L0 and L1 domains in the format <L0 domain.L1 domain>.

7 Enter the values for your SIP numbering plan in the appropriate fields.

8 Click **Save and Transfer**.

9 Click **OK** when the system is done transferring data and the successful transfer message appears.

—End—

Configuring IP networking for SIP

The IP Peer Networking configuration for SIP in the Call Server is similar to the H.323 configuration. For each Call Server in the IP Peer Network, perform the following tasks:

1. Define the customer to support ISDN (LD 15).
2. Create the virtual D-channel (LD 17).
3. Configure the zones (LD 117).
4. Create the virtual route (LD 16).
   Enter **SIP** in the VTRK page.
5. Create the virtual trunk.
6. Create the ESN data block for CDP (LD 86).
7. Create the Network Control (NCTL) block for network access (LD 87).
8. Create the RLB that uses the virtual trunk route (LD 86).
9. Create the CDP steering codes (LD 87).

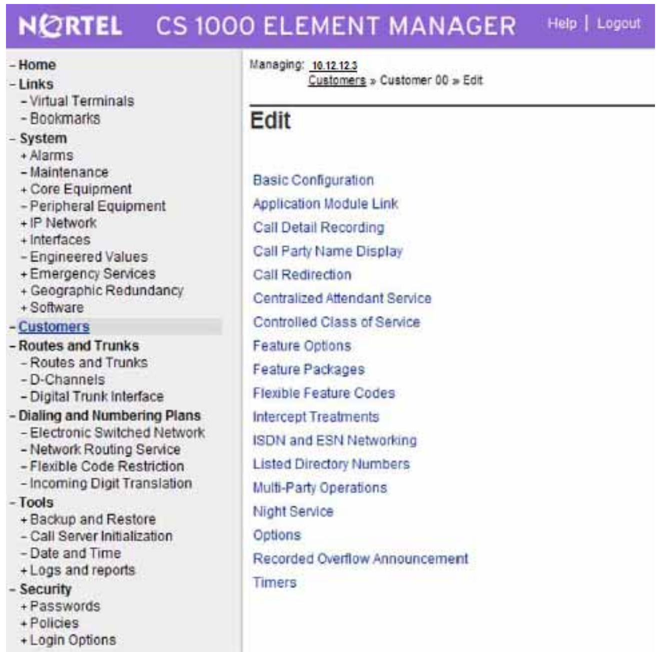
If the system is already configured for H.323, you do not need to perform steps 1, 2, 3, 6, and 7 again.

Defining the customer to support ISDN

Complete the following procedure to define the customer to support ISDN.

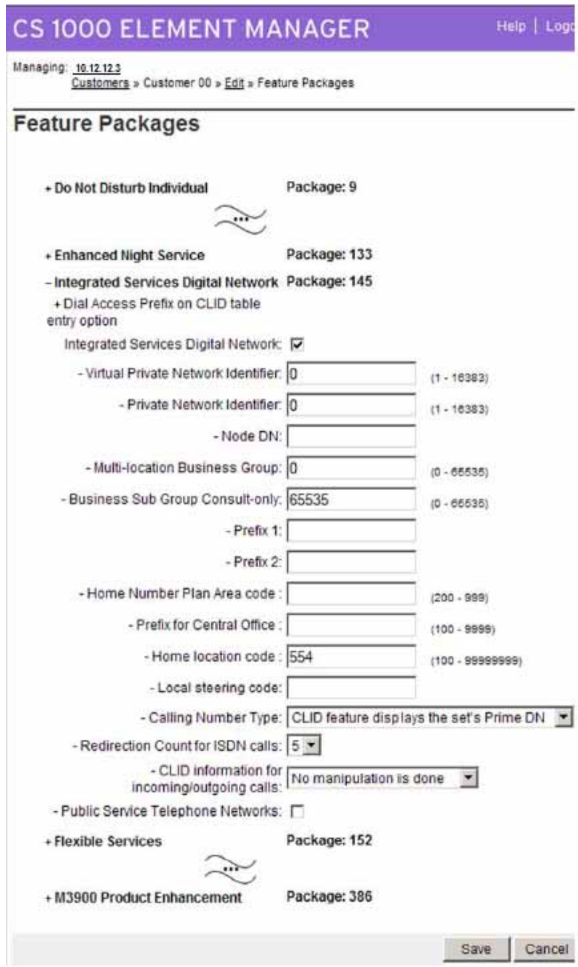
Step	Action
1	Log on to Element Manager.
2	Select **Customers**.
3	Select the **Customer Number** you wish to edit. The Customer Edit page appears. See Figure 25 "Customer Edit" (page 55).

Figure 25
Customer Edit



4 Select the **Feature Packages** heading.
The Feature Packages page appears. See Figure 26 "Feature Packages" (page 56).

Figure 26
Feature Packages



5 Expand the **Integrated Services Digital Network Package 145** heading.

6 Ensure that the **Integrated Services Digital Network** check box is selected.

7 Click **Save**.

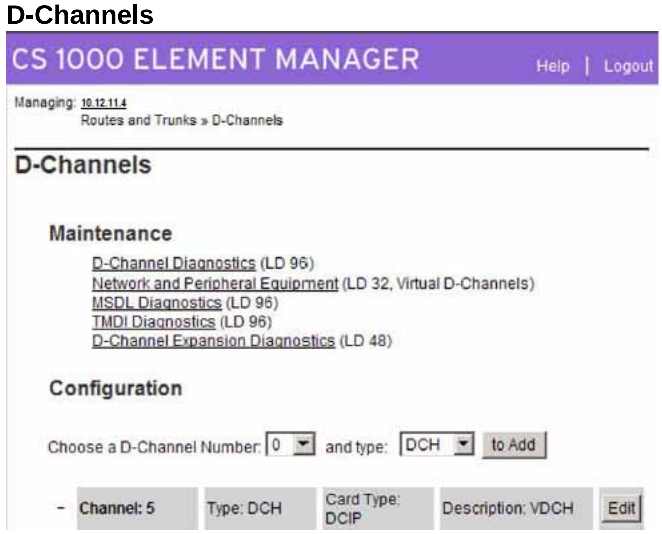
—End—

Creating the virtual D-channel

Perform the following procedure to create the virtual D-channel.

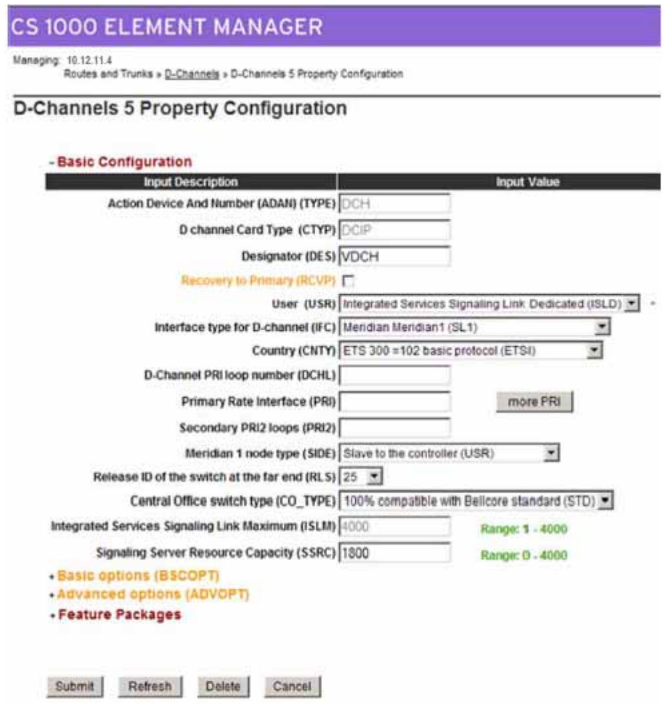
Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > D-Channels**. The D-Channels page appears. See Figure 27 "D-Channels" (page 57). A message appears if a D-channel is not configured. Click **OK**.

Figure 27
D-Channels



Step	Action
3	From the **Choose a D-Channel Number** menu, select the D-Channel number. D-channels 0,1, and 2 are usually used or shared with other applications. It is recommended that you begin configuring virtual D-channels on channel 3.
4	From the **Type** menu, select the D-Channel type.
5	Click **to Add**. The D-Channels Property Configuration page appears. See Figure 28 "D-Channels Property Configuration" (page 58).

Figure 28
D-Channels Property Configuration



6 For the **D channel Card Type (CTYP)**, select **D-channel is over IP (DCIP)**.

7 For the **Designator (DES)**, type a meaningful name.
The Designator must not contain spaces; use underscores instead.
Make a note of the Designator in your records for future reference.

8 For **User (USR)**, select **Integrated Services Signaling Link Dedicated (ISLD)**.

9 For **Interface type for D-channel (IFC)**, select **Meridian Meridian1 (SL1)**.

10 Leave all other parameters as is and click **Submit**.
The new channel appears.

—End—

Configuring zones (LD 117)

Before you can configure the virtual routes and trunks, the following zones must be configured, in any order:

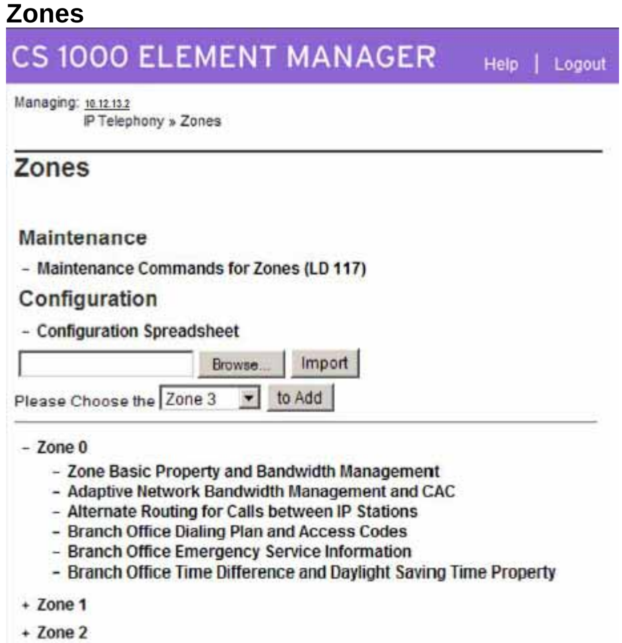
- Zone 1 = IP Phones zone (ZBRN = MO)
- Zone 2 = Voice Gateway Channels zone, which should be different from the IP Phones zone (ZBRN = VTRK)

Ensure that enough bandwidth is allocated for the zones with the heaviest traffic.

Never use or configure zone 0.

Step	Action
1	Log on to Element Manager.
2	Select **System > IP Network > Zones**. See Figure 29 "Zones" (page 59).

Figure 29
Zones



Step	Action
3	Select the **Zone** you wish to configure. Configured zones appear in the list at the bottom of the page.
4	Click **to Add**.

5 After you click **to Add**, a message may appear prompting you to use the Zone Basic Property and Bandwidth Management Spreadsheet. Click **OK**.

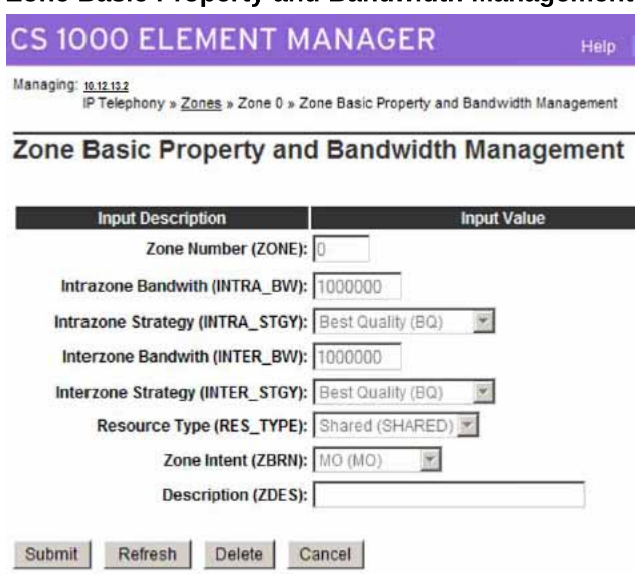
6 Leave the default values for bandwidth and resource type as is.

7 Set the **Zone Intent (ZBRN)** as follows:

- Zone 1 is for the IP Phones at the Main Office. Set Zone Intent (ZBRN) for Zone 1 to **MO (MO)**.
- Zone 2 is for the Voice Gateway Channels. Set Zone Intent (ZBRN) for Zone 2 to **VTRK (VTRK)**.

See Figure 30 "Zone Basic Property and Bandwidth Management" (page 60).

Figure 30
Zone Basic Property and Bandwidth Management



8 For **Description (ZDES)**, type a meaningful description.

9 Click **Submit**.

10 Repeat this procedure for all additional zones you wish to create.

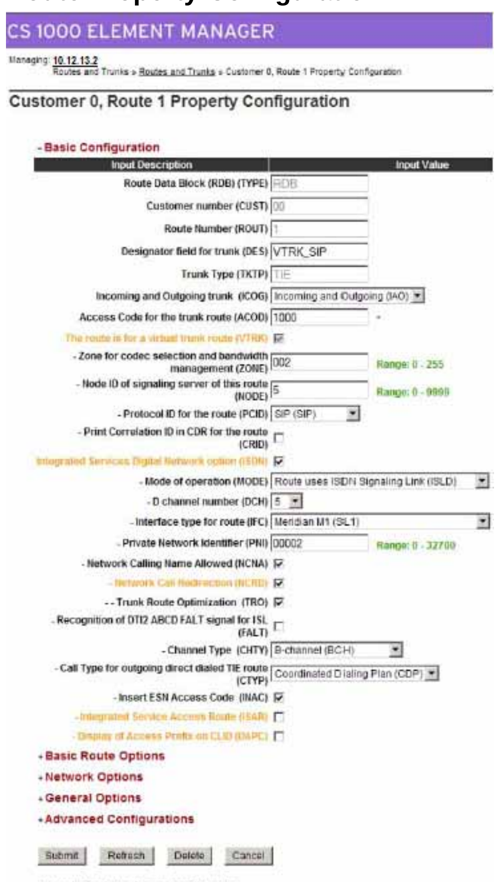
—End—

Creating the virtual route (LD 16)

Perform the following procedure to create the virtual route.

Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > Routes and Trunks**.
3	Click the **Add route** button. The Route Property Configuration page appears. The trunk type (TKTP) you choose determines the parameters available on this page. See Figure 31 "Route Property Configuration" (page 61) for one possible view of the Route Property Configuration page.

Figure 31
Route Property Configuration



Step	Action
4	Select the **Route Number (ROUT)**.
5	For **Designator field for trunk (DES)**, type a meaningful name.
6	For **Trunk Type (TKTP)**, select **TIE trunk data block (TIE)**.

7 For **Incoming and Outgoing trunk (ICOG)**, select **Incoming and Outgoing (IAO)**.

8 Set the **Access Code for the trunk route (ACOD)**.

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

10 Type the **Zone** number of the zone with the ZBRN set to Vtrk for the new route.
This value must match the values you configure in the Signaling Server.

11 Type the **Node ID of signaling server of this route (NODE)**.
This value must match the values you configure in the Signaling Server.

12 For **Protocol ID for the route (PCID)**, select **SIP (SIP)**.

13 Select the **Integrated Services Digital Network option (ISDN)** check box.

14 For **Mode of operation (MODE)**, select **Route uses ISDN Signaling Link (ISLD)**.

15 Select the virtual **D channel number (DCH)**.

16 For **Interface type for route (IFC)**, select **Meridian M1 (SL1)**.

17 Leave the **Call Type for outgoing direct dialed TIE route (CTYP)** at the default value.
It is best to let NARS/BARS entries determine the NPI/TON for a number so that the route can be used for multiple call types.

18 Select the **Insert ESN Access Code (INAC)** check box.

19 Leave the other default values as is and click **Submit**.
The Routes and Trunks page appears showing the created routes.

—End—

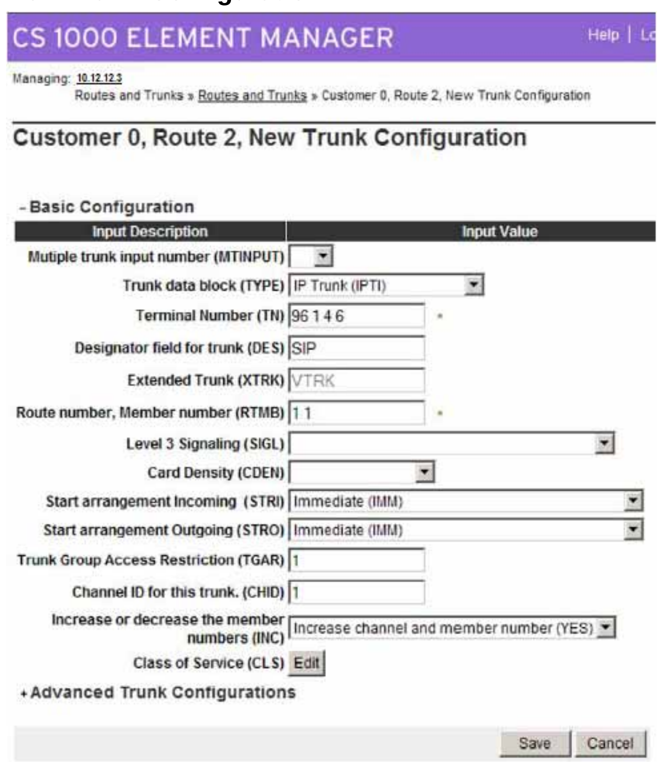
Creating the virtual trunks (LD 14)

The Virtual Trunk TNs that you configure in this procedure cannot overlap with the ones that you configure for IP Phones.

Create separate virtual routes for SIP and H.323. The SIP route is configured in the procedure "Configuring IP networking for SIP" (page 54).

Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > Routes and Trunks**.
3	Expand the **Customer** heading.
4	Click **Add trunk** next to the route to which you wish to add the trunk. The New Trunk Configuration page appears. See Figure 32 "New Trunk Configuration" (page 63). Your configuration determines the parameters available on this page.

Figure 32
New Trunk Configuration



Step	Action
5	If you are configuring several trunks the same way, select the **Multiple trunk input number (MTINPUT)** (optional).
6	For **Trunk data block (TYPE)**, select **IP Trunk (IPTI)**.
7	Type the **Terminal Number (TN)** for the trunk.
8	For **Designator field for trunk (DES)**, type a meaningful value.
9	Type the **Route number, Member number (RTMB)** for the trunk.

10 Set the values of **Start arrangement Incoming (STRI)** and **Start arrangement Outgoing (STRO)**.
Immediate (IMM) is recommended for both fields.

11 Type the **Channel ID for this trunk (CHID)**.

12 You can add a Class of Service (CLS) for all features that you wish. In a basic configuration, you can leave the CLS as is.

13 Select **Advanced Trunk Configurations** to display a list of advanced features.

14 Edit the necessary fields or accept the default values.

15 Click **Submit**.

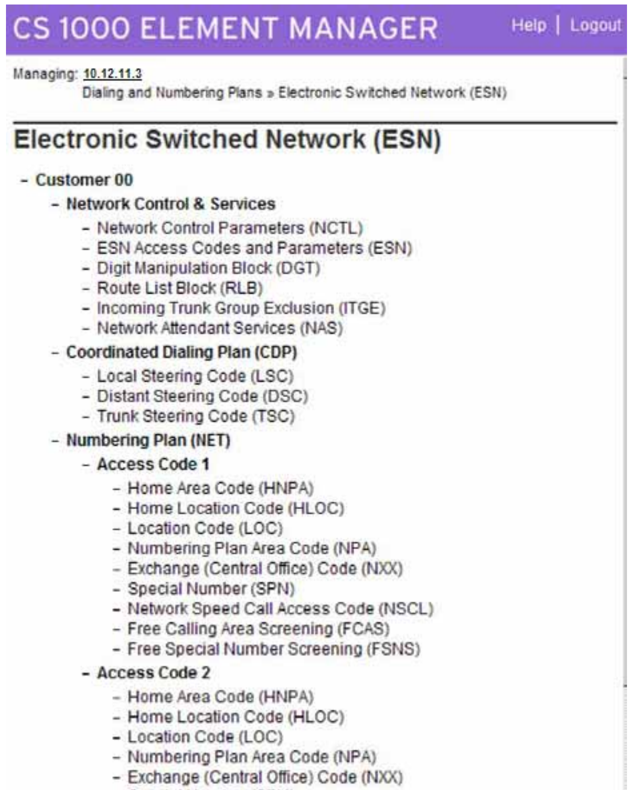
—End—

Creating the ESN data block for CDP

Perform the following procedure to create the ESN data block for CDP.

Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans > Electronic Switched Network**. The Electronic Switched Network page appears. See Figure 33 "Electronic Switched Network" (page 65).

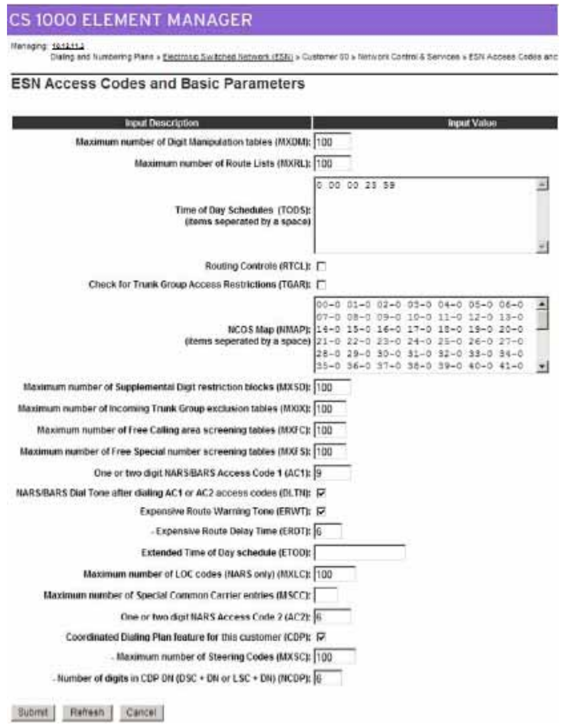
Figure 33
Electronic Switched Network



3 Select **Customer > Network Control & Services > ESN Access Codes and Parameters (ESN)**.

4 A message appears if ESN data is not configured. Click **OK**.
The ESN Access Codes and Basic Parameters page appears. See Figure 34 "ESN Access Codes and Basic Parameters" (page 66).
If ESN data is configured on your switch, the fields on this page appear populated.

Figure 34
ESN Access Codes and Basic Parameters



5 Edit the main parameters (**MXDM**, **MXRL**, **MXSD**, **MXIX**, **MXFC**, **MXFS** and **MXLC**) if required, or leave the default values as is.

6 Select the **Coordinated Dialing Plan feature for this customer (CDP)** check box.

7 Set the value of the **Maximum number of Steering Codes (MXSC)**.

8 Set the value of the **Number of digits in CDP DN (DSC+DN or LSC+DN) (NCDP)**.

9 Click **Submit**.

—End—

Creating the Network Control Block (NCTL) for network access (LD 87)

Perform the following procedure to create the Network Control Block.

Step **Action**

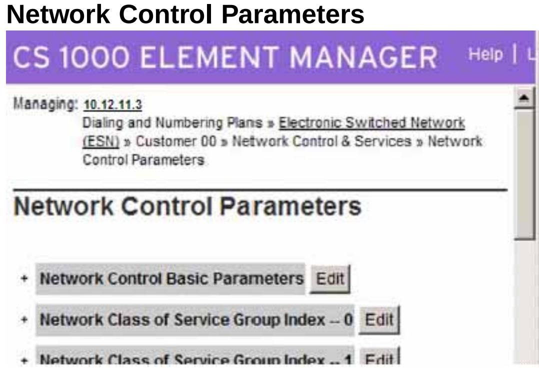
1 Log onto Element Manager.

2 Select **Dialing and Numbering Plans > Electronic Switched Network**.

3 Select **Customer > Network Control & Services > Network Control Parameters (NCTL)**.
See Figure 33 "Electronic Switched Network" (page 65).

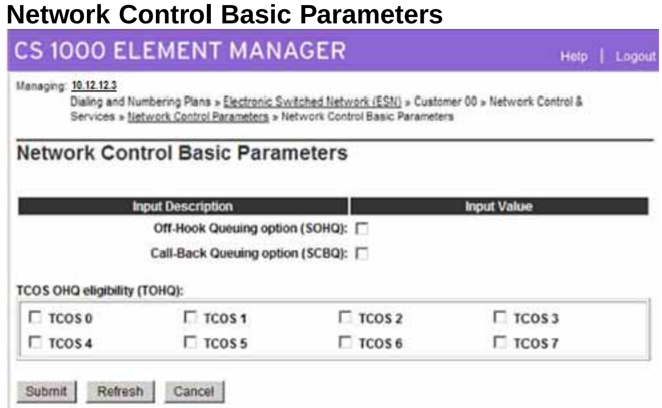
4 A message appears if no network control data is configured. Click **OK** to configure new data.
The Network Control Parameters page appears. See Figure 35 "Network Control Parameters" (page 67).

Figure 35
Network Control Parameters



5 Click the **Edit** button next to Network Control Basic Parameters.
The Network Control Basic Parameters page appears. See Figure 36 "Network Control Basic Parameters" (page 67).

Figure 36
Network Control Basic Parameters



6 Choose the basic control parameters for your network.

7 Click **Submit**.

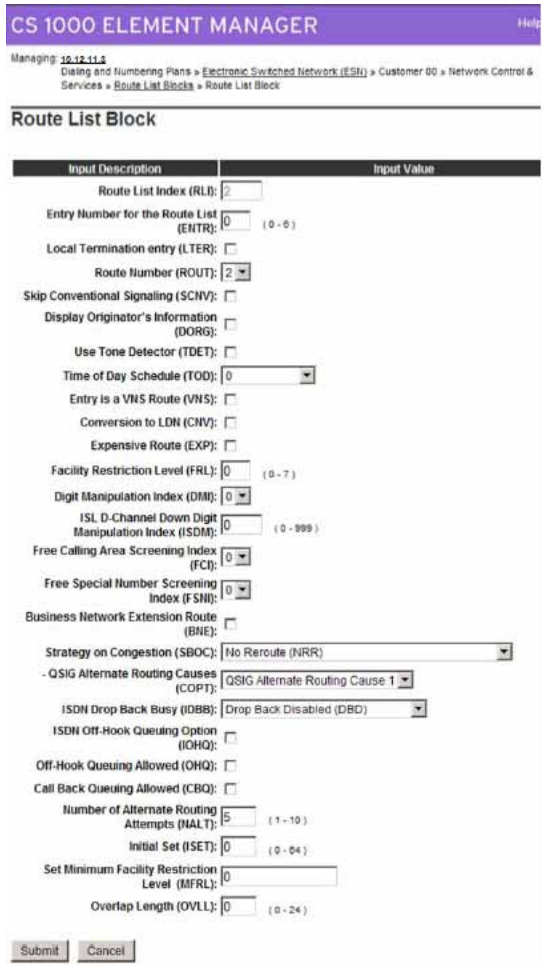
—End—

Creating the RLB for the virtual trunk route (LD 86)

Perform the following procedure to create the RLB for the virtual trunk route.

Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans > Electronic Switched Network**.
3	Select **Customer > Network Control & Services > Route List Block (RLB)**. If route list blocks are not configured, the error message “Route List does not exist” appears. Click **OK**.
4	Type the **Route List Index number**.
5	Click **to Add**. The Route List Block Configuration page appears. See Figure 37 "Route List Block" (page 69).

Figure 37
Route List Block



6 Select the **Route Number (ROUT)** you previously defined.

7 For **Strategy on Congestion (SBOC)**, select **Reroute All (RRA)**.

8 Accept the other defaults and click **Submit**.
The new Route List Block is generated. You can check the configuration by selecting Route List Block Index and Data Entry Index.

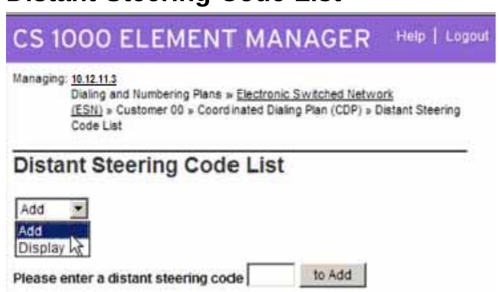
—End—

Creating the CDP steering codes (LD 87)

Perform the following procedure to create the CDP steering codes.

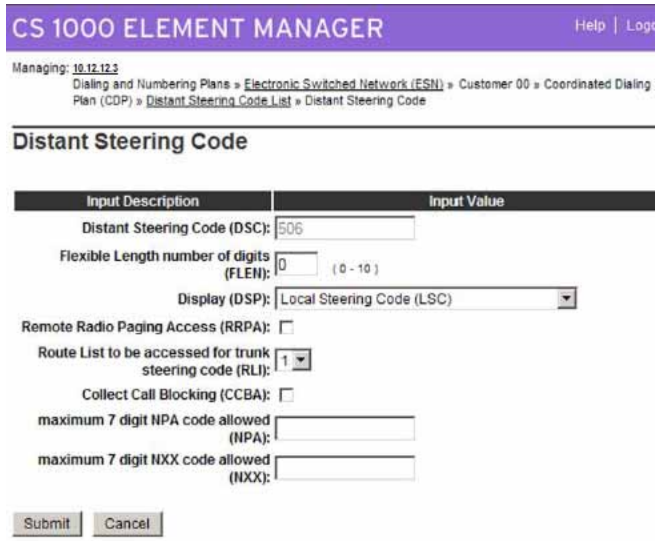
Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans > Electronic Switched Network**. The Electronic Switched Network page appears. See Figure 33 "Electronic Switched Network" (page 65).
3	Select **Customer > Coordinated Dialing Plan (CDP) > Distant Steering Code (DSC)**. The Distant Steering Code List page appears. See Figure 38 "Distant Steering Code List" (page 70).

Figure 38
Distant Steering Code List



Step	Action
4	Select **Add** to add a new Distant Steering Code.
5	Enter a **Distant Steering Code (DSC)**. The Distant Steering Code is a unique identifier for remote switches or locations. Add a Distant Steering Code for all remote locations.
6	Click **to Add**. The Distant Steering Code page appears. See Figure 39 "Distant Steering Code" (page 71).

Figure 39
Distant Steering Code



7 Check that the parameters are configured appropriately for your system.

8 Select a **Route List to be accessed for trunk steering code (RLI)**.

9 Click **Submit**.

10 Repeat this procedure for all other DSCs on your network.

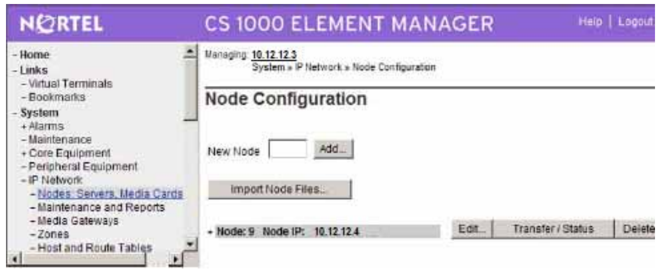
—End—

Checking CODEC and QoS settings

At this point, the Call Server configuration is complete. It is recommended that you check the CODEC and QoS settings.

Step	Action
1	Log on to Element Manager.
2	Select **System > IP Network > Nodes: Servers, Media Cards**. See Figure 40 "Node Configuration" (page 72).

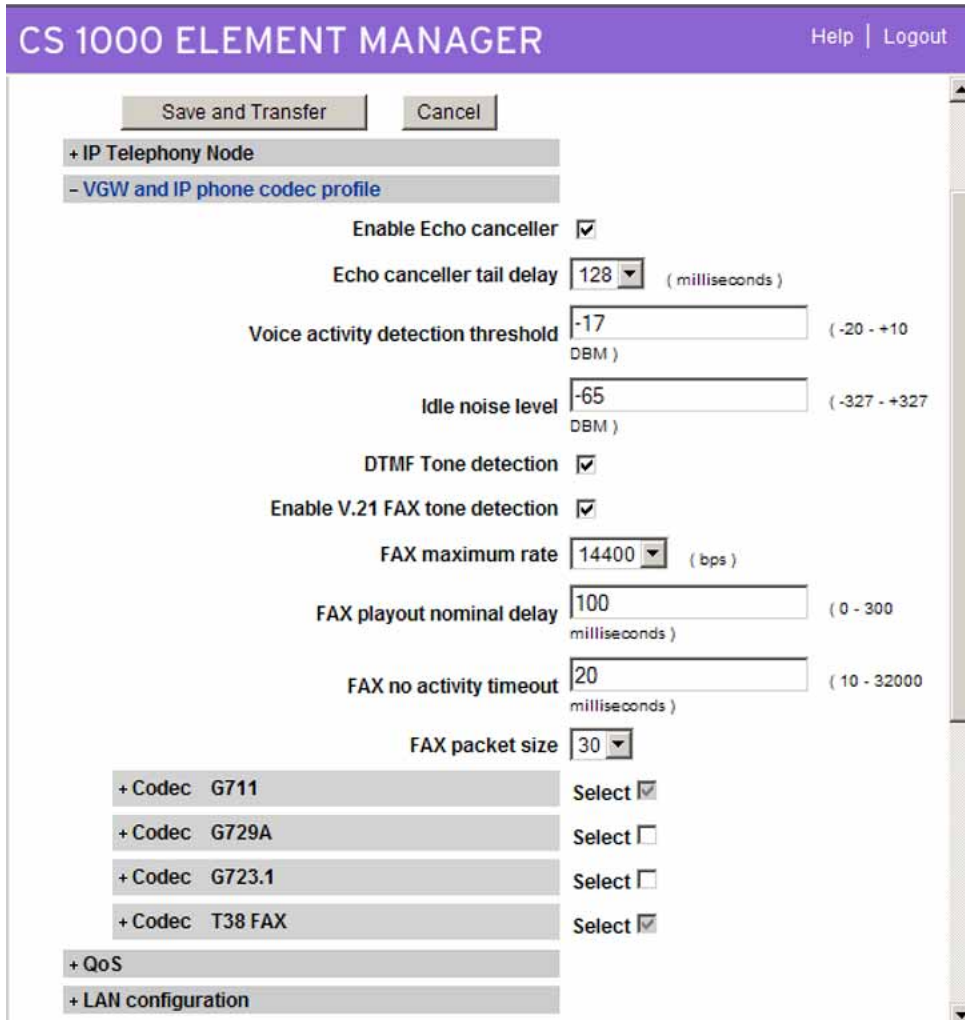
Figure 40
Node Configuration



3 Click **Edit**.

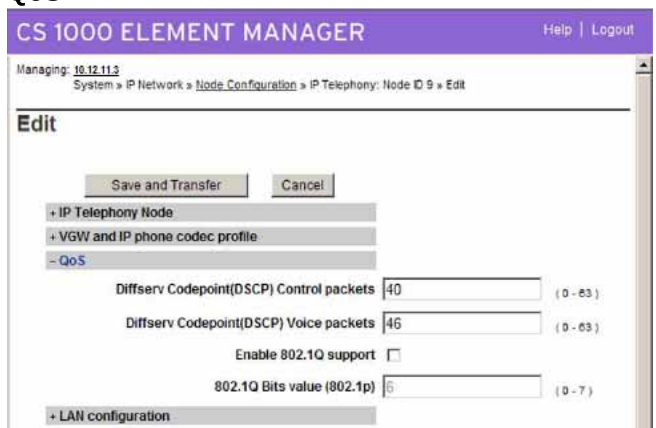
4 Expand the **VGW and IP phone codec profile** heading and edit the fields as necessary.
See Figure 41 "VGW and IP phone codec profile" (page 73).

Figure 41
VGW and IP phone codec profile



5 Expand the **QoS** heading and edit the fields as necessary. See Figure 42 "QoS" (page 74).

Figure 42
QoS



6 If you make configuration changes, click **Save and Transfer**. When the successful transfer notification message appears, click **OK**.
If you do not make configuration changes, click **Cancel**.

—End—

NRS configuration

The Network Routing Service (NRS) uses a basic SIP structure for its configuration, which is applicable for SIP, H.323, and Network Connection Server (NCS) call completion. This structure is the basis of the single network dialing/numbering plan.

Before you begin configuration of the NRS, gather the names of all domains and subdomains.

NRS configuration procedures

The sequence of NRS configuration procedures is as follows:

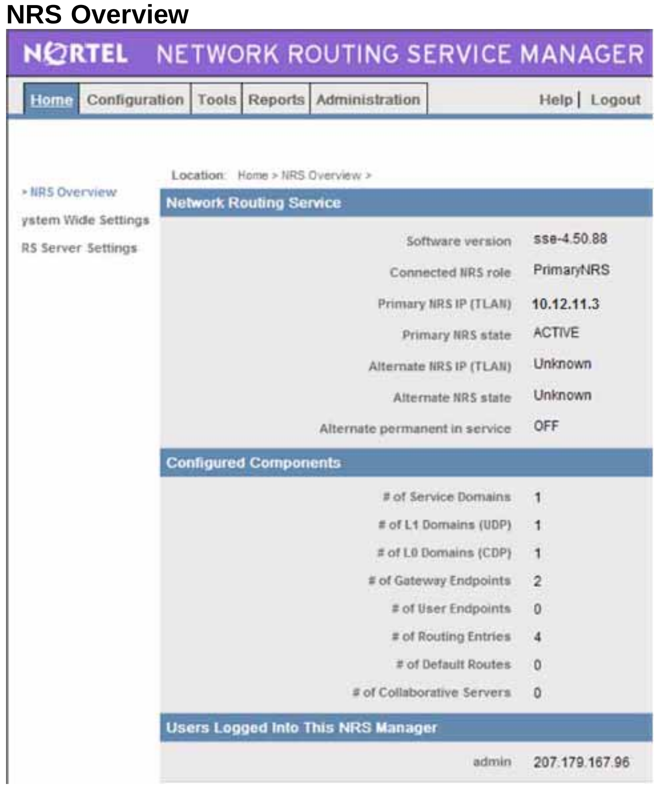
- "Launching NRS Manager" (page 75)
- "Verifying and adjusting system-wide settings" (page 76)
- "Configuring the NRS server settings (H.323 Gatekeeper or SIP)" (page 78)
- "Configuring the service domain" (page 80)
- "Configuring the L1 domain (UDP)" (page 81)
- "Configuring the L0 domain (CDP)" (page 83)
- "Configuring Gateway endpoints" (page 86)
- "Configuring routing entries" (page 90)
- "Configuring collaborative servers" (page 92)
- "Updating the database" (page 94)
- "Checking the status of registered endpoints" (page 95)
- "Checking the status of virtual D-channels" (page 96)
- "Checking the status of virtual trunks" (page 97)

Launching NRS Manager

Perform the following procedure to launch NRS Manager.

Step	Action
1	Log on to Element Manager.
2	Select **Dialing and Numbering Plans > Network Routing Service**.
3	Click **Next**. The NRS logon page appears.
4	Click **Login**.
5	Enter the user ID and password. The NRS Overview page appears. See Figure 43 "NRS Overview" (page 76).

Figure 43
NRS Overview



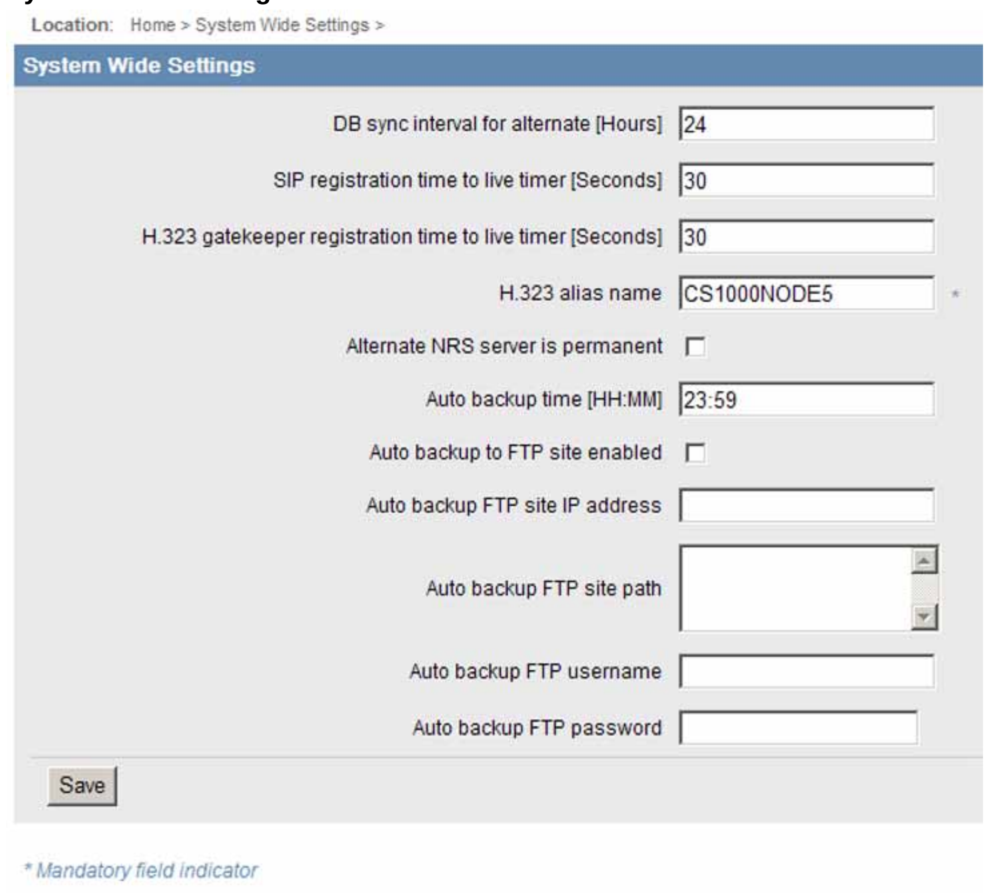
—End—

Verifying and adjusting system-wide settings

You can check system-wide settings and make changes from NRS Manager.

Step	Action
1	Log on to NRS Manager.
2	Select **System Wide Settings**. The System Wide Settings page appears. See Figure 44 "System Wide Settings" (page 77).

Figure 44
System Wide Settings



Step	Action
3	Configure the information in the System Wide Settings page. Refer to Table 4 "System Wide Settings fields" (page 77).

Table 4
System Wide Settings fields

Field	Description
DB synch interval for alternate [Hours]	24 is the default.

Field	Description
SIP registration time to live timer [Seconds]	30 seconds is recommended.
H.323 Gatekeeper registration time to live timer [Seconds]	30 seconds is recommended.
H.323 alias name	This is a mandatory field. The H.323 Alias Name must be alphanumeric and contain no spaces. The default value is the same as the H.323 ID and HostName value configured in the PRIMARY Signaling Server's config.ini file.
Alternate NRS server is permanent	Select this check box if the Alternate NRS Server is to remain in service after a switch-over, even if the Primary NRS recovers. Clear the check box if the Alternate NRS switches over functions to the Primary NRS Server after the Primary NRS Server recovers.
Auto backup time [HH:MM]	Enter the time when the database backup automatically occurs.
Auto backup to FTP site enabled	Select this check box to enable automatic backup of the NRS database to an FTP site.
Auto backup FTP site IP address **Auto backup FTP site path** **Auto backup FTP username** **Auto backup FTP password**	Enter values for Autobackup FTP if you enabled automatic backup of the NRS database to an FTP site.

4 Click **Save**.

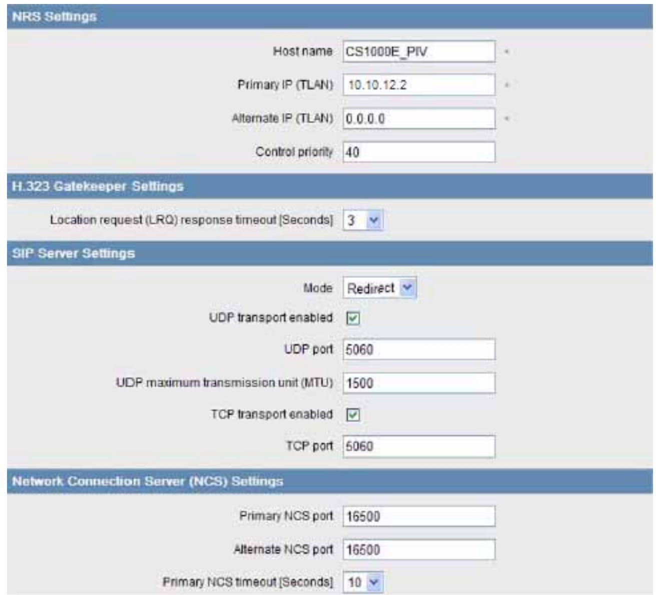
—End—

Configuring the NRS server settings (H.323 Gatekeeper or SIP)

Perform the following procedure to configure NRS server settings.

Step	Action
1	Log on to NRS Manager.
2	Select **NRS Server Settings**. The NRS Settings page appears. See Figure 45 "NRS Settings" (page 79).

Figure 45
NRS Settings



3 Under **NRS Settings**, set the following values:

- **Host name**
- **Primary IP (TLAN)**
- **Alternate IP (TLAN)**
- **Control priority**

4 Under **H.323 Gatekeeper Settings**, select the **Location request (LRQ) response timeout [Seconds]**.

5 Under **SIP Server Settings**, set the following values:

- **Mode**
- **UDP transport enabled/disabled**
- **UDP port**
- **UDP maximum transmission unit (MTU)**
- **TCP transport enabled/disabled**
- **TCP port**
- **TCP maximum transmission unit (MTU)**

Make the values under SIP Server Settings the same as those you configure for the SIP Proxy in Element Manager.

6 Under **Network Connection Server (NCS) Settings**, set the following values:

- **Primary NCS port**
- **Alternate NCS port**
- **Primary NCS timeout [Seconds]**

7 Click **Save**.

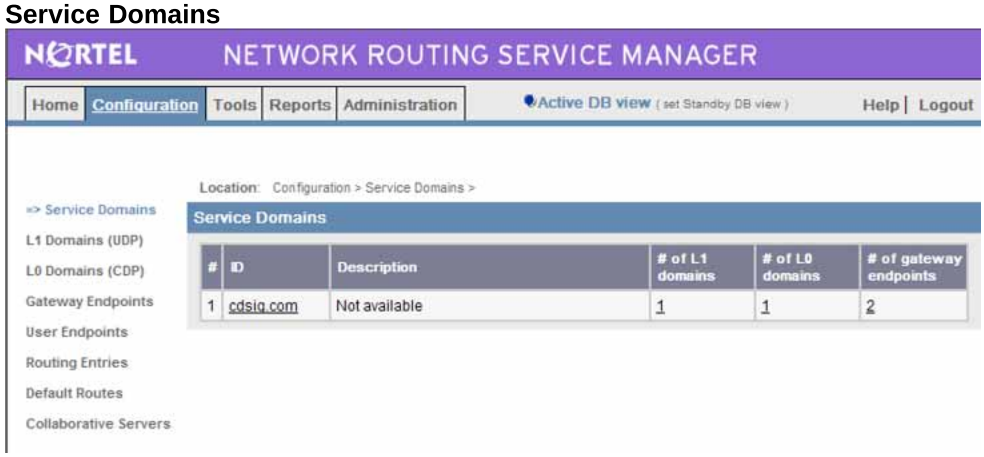
—End—

Configuring the service domain

The NRS database information configured in this procedure is required by both the SIP Redirect Server and the H.323 Gatekeeper.

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab.
3	A message may appear if the active and Standby databases are not synchronized. Click **OK**.
4	Click **set Standby DB view** to switch from active to standby database view. The active database view is the default view. Use the active database for runtime queries, and the standby database for administrator modifications. You must use standby view to make changes to the database. See Figure 46 "Service Domains" (page 80).

Figure 46
Service Domains



5 Select **Service Domains**.

6 Click **Add**.

7 Enter your **Domain name** and a **Domain description**.
These values must match that set for the Signaling Server.

8 Click **Save**.
The Service Domains page appears again with the new domain added.
When no description is entered, the service domain is shown with the message “Not available”. This means that the description is not entered, but the service domain is still active. This applies to all description fields in NRS Manager.

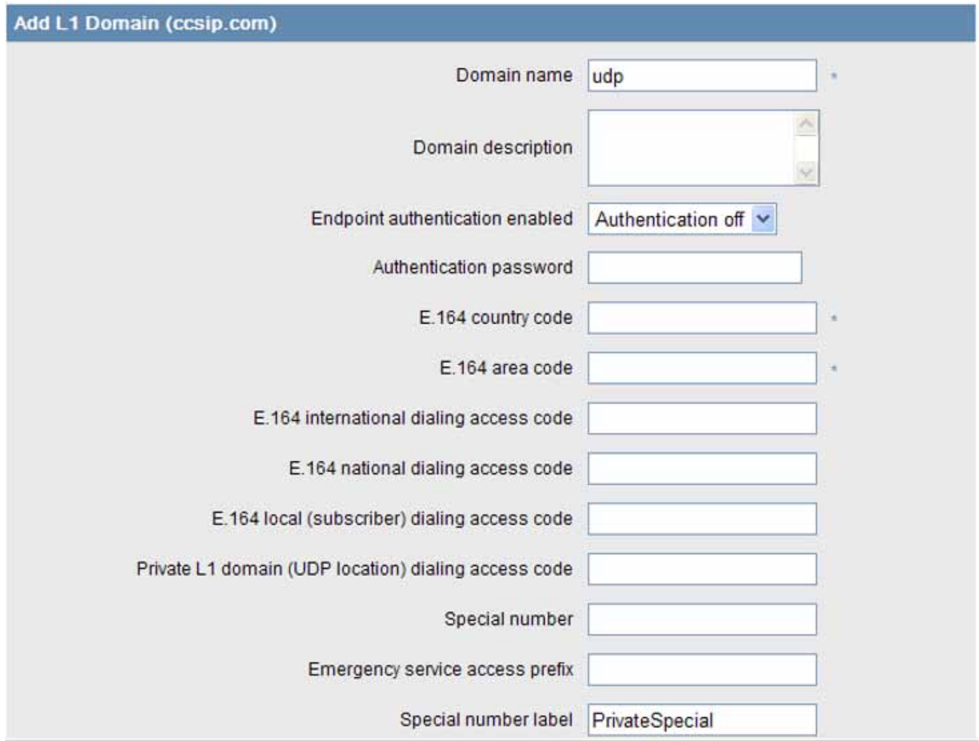
—End—

Configuring the L1 domain (UDP)

You can configure the L1 domain after you configure the service domain. The L1 domain is a service domain associated with UDP.

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab.
3	Click **set Standby DB view** to switch from active to standby database view.
4	Select **L1 Domains (UDP)**.
5	Click **Add**. The Add L1 Domain page appears. See Figure 47 "Add L1 Domain" (page 82).

Figure 47
Add L1 Domain



6 Configure the L1 domain.
Refer to Table 5 "L1 domain fields" (page 82) for configuration information.

Table 5
L1 domain fields

Field	Value	Description
Domain name	<alphanumeric string>	Mandatory. The name must be alphanumeric and can be up to 30 characters in length.
Domain description	<character string>	Optional. The description can include any character except single quotes and be up to 120 characters in length.
Endpoint authentication enabled	Authentication off Authentication on Not configured	If Authentication on is selected, all endpoints require authentication.
Authentication password	<alphanumeric string>	If Authentication on is selected, enter an authentication password. The password must be alphanumeric and up to 30 characters in length.

Field	Value	Description
E.164 country code	<numeric string>	Mandatory. The code must be numeric and up to 7 characters in length.
E.164 area code	<numeric string>	Mandatory. The code must be numeric and up to 7 characters in length.
E.164 international dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 national dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 local (subscriber) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Private L1 domain (UDP) location) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Special number	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.
Emergency service access prefix	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.
Special number label	<alphanumeric string>	Optional. The label must be alphanumeric and up to 30 characters in length. The first character in the label must be alphabetic.

7 Click **Save**.
The L1 Domains page appears again with the new L1 domain added.

8 To view the configured data for the L1 domain, click the **ID** in the **L1 Domains (UDP)** menu.
The View L1 Domain Property page appears, displaying your configured data.

—End—

Configuring the L0 domain (CDP)

The L0 domain is a service domain associated with CDP, representing the private addresses field in the SIP URI. This address is composed of the service, L1, and L0 domains.

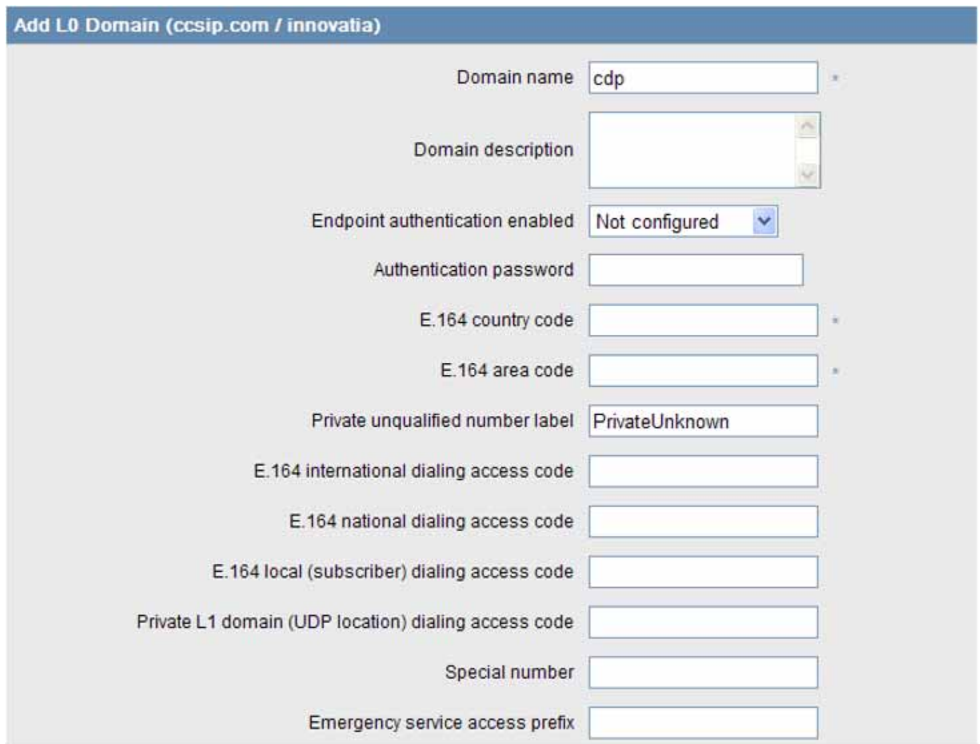
Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab.

3 Click **set Standby DB view** to switch from active to standby database view.

4 Select **L0 Domains (CDP)**.

5 Click **Add**.
The Add L0 Domain page appears. See Figure 48 "Add L0 Domain" (page 84).

Figure 48
Add L0 Domain



6 Enter the appropriate values for your network.
Refer to Table 6 "Add L0 Domain fields" (page 84)for configuration information.
The country codes, area codes, public prefixes, and private prefixes must match those of your L1 domain.

Table 6
Add L0 Domain fields

Field	Value	Description
Domain name	<alphanumeric string>	Mandatory. The name must be alphanumeric and can be up to 30 characters in length.

Field	Value	Description
Domain description	<character string>	Optional. The description can include any character except single quotes and can be up to 120 characters in length.
Endpoint authentication enabled	Authentication off Authentication on Not configured	If Authentication on is selected, then all endpoints require authentication.
Authentication password	<alphanumeric string>	if Authentication on is selected, enter a password. The password must be alphanumeric and up to 30 characters in length.
E.164 country code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 area code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Private unqualified number label	<alphanumeric string>	The label must be alphanumeric and up to 30 characters in length. The first character in the label must be alphabetic.
E.164 international dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 national dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 local (subscriber) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Private L1 domain (UDP location) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Special number	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.
Emergency service access prefix	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.

7 Click **Save**.
The L0 Domains page appears again, showing the added domain.

8 To view the configured data, in the L0 domain page, select the service domain and L1 domain and click **Show**.
A list of configured L0 domains appears.

9 Select the L0 domain to view its configuration information.

The View L0 Domain Property page appears. See Figure 48 "Add L0 Domain" (page 84).

—End—

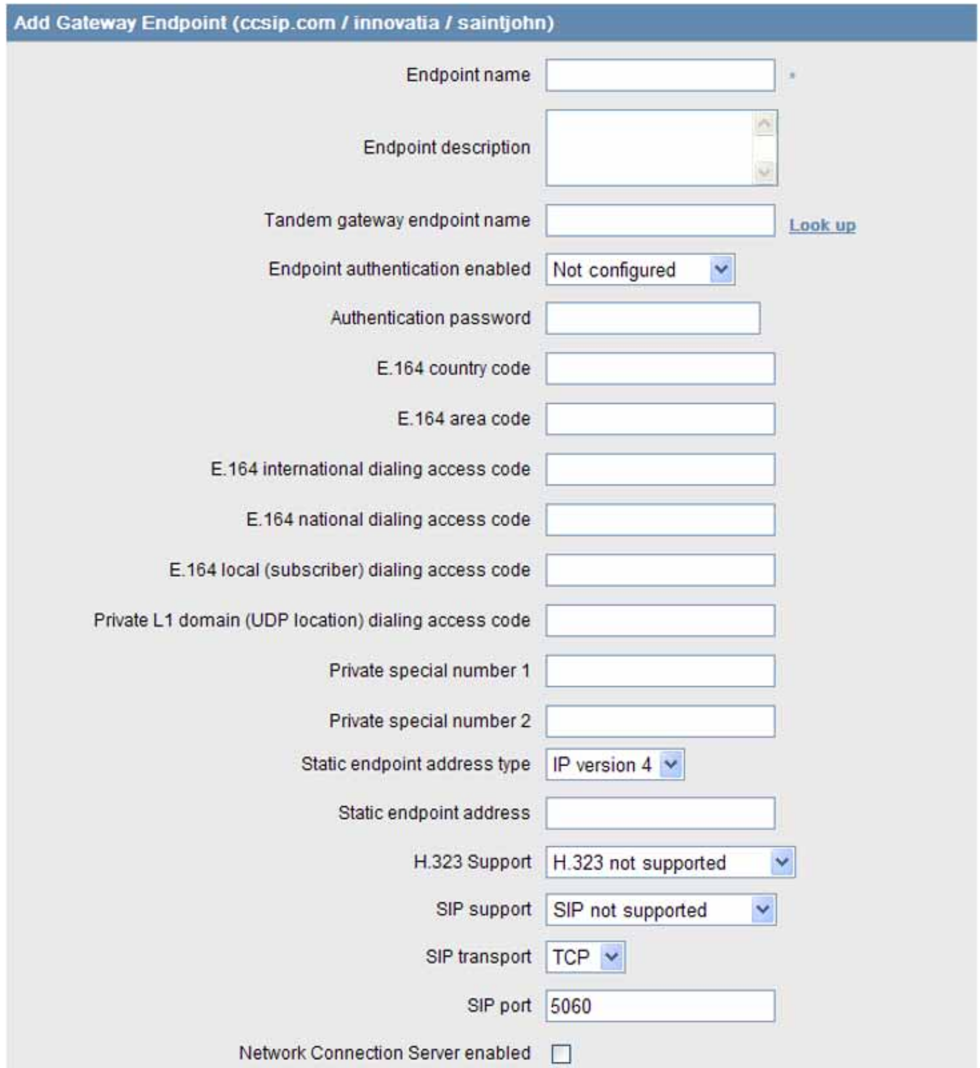
Configuring Gateway endpoints

Add an endpoint for both the Communication Server 1000 (CS 1000) and Business Communications Manager (BCM) systems.

These are Gateway endpoints, which can be served by several users. You can add multiple endpoints, some SIP-only, some H.323-only, and Unistim. You can also configure a user endpoint, which can be only one of these three protocols.

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab
3	Click **set Standby DB view** to switch from active to standby database view.
4	Click **Gateway Endpoints**.
5	Click **Add**. The Add Gateway Endpoint page appears. See Figure 49 "Add Gateway Endpoint" (page 87).

Figure 49
Add Gateway Endpoint



6 Enter the appropriate values for your network.
Refer to Table 7 "Add Gateway Endpoint fields" (page 87) for configuration information.

Table 7
Add Gateway Endpoint fields

Field	Value	Description
Endpoint name	<alphanumeric string>	The name must be alphanumeric and up to 30 characters in length.

Field	Value	Description
Endpoint description	<alphanumeric string>	The description must be alphanumeric and up to 120 characters in length.
Tandem gateway endpoint name	<alphanumeric string>	The tandem Gateway is optional. This indicates whether the endpoint is used to tandem calls from outside the network. The name must be alphanumeric and up to 30 characters in length. **Note**: Use the Look-up link to find configured Gateway endpoints.
Endpoint authentication enabled	Not configured Authentication off Authentication on	If this option is selected, the Gateway endpoint uses the L1 or L0 authentication (if enabled). If this option is selected, authentication is off for this Gateway endpoint even if L1 or L0 authentication is enabled. If this option is selected, authentication is on for this Gateway endpoint, and the authentication overrides the L1 or L0 authentication (if enabled).
Authentication password	<alphanumeric string>	If Authentication on is selected, choose a password. The password must be alphanumeric and up to 30 characters in length.
E.164 country code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 area code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 international dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 national dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
E.164 local (subscriber) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Private L1 domain (UDP location) dialing access code	<numeric string>	Optional. The code must be numeric and up to 7 characters in length.
Private special number 1	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.
Private special number 2	<numeric string>	Optional. The number must be numeric and up to 30 characters in length.
Static endpoint address type	IP version 4	Select IP version 4 from the drop-down list.

Field	Value	Description
Static endpoint address	<Node IP address>	This is the address of the BCM application server. If a third-party Gateway is used, it is the IP address of the Gateway.
H.323 support	H.323 not supported RAS H.323 endpoint Not RAS H.323 endpoint	RAS H.323 Endpoint is recommended. If an H.323 Gateway Endpoint is configured with an H.323 Support type of RAS H.323 endpoint, NRS Manager displays Endpoint Dynamic Registration information after the H.323 Gateway registers with the NRS. Endpoint Dynamic Registration information includes Call Signaling IP, RAS IP, Alias name, t35Country code, t35Extension, Manufacturer code, Product ID, and Version ID.
SIP support	SIP not supported Static SIP endpoint Dynamic SIP endpoint	Dynamic SIP Endpoint is recommended. If a SIP Trunk Gateway Endpoint is configured with a SIP Support type of Dynamic SIP endpoint, NRS Manager displays Endpoint Dynamic Registration Information for SIP after the SIP Trunk Gateway registers with the NRS. Endpoint Dynamic Registration Information includes SIP IP, Registration expiry time, User agent, and Preference.
SIP transport	TCP UDP TLS	TCP is selected by default. Select UDP or TLS if security is enabled, as the BCM system does not support TCP. Ensure that the far end matches this setting.
SIP port	<port value>	Default SIP port value is 5060. If the SIP Port is changed, the value must be numeric and up to 5 numbers in length. The range is 0 to 65535.
Network Connection Server enabled	<check box>	Select the Network Connection Server is enabled check box if this Gateway Endpoint supports the NCS for branch office or SRG user redirection to the main office, Virtual Office, or Geographic Redundancy.

7 Click **Save**.
The Gateway Endpoints window appears again with the new endpoints added.

8 From the Gateway Endpoint page, select the **Service Domain**, **L1 domain**, and **L0 domain** to view the configured data of an endpoint.

9 Click **Show**.
A list of configured Gateways appears.

10 Click the **Gateway ID** you wish to view.
The Add Gateway Endpoint page appears. See Figure 49 "Add Gateway Endpoint" (page 87).

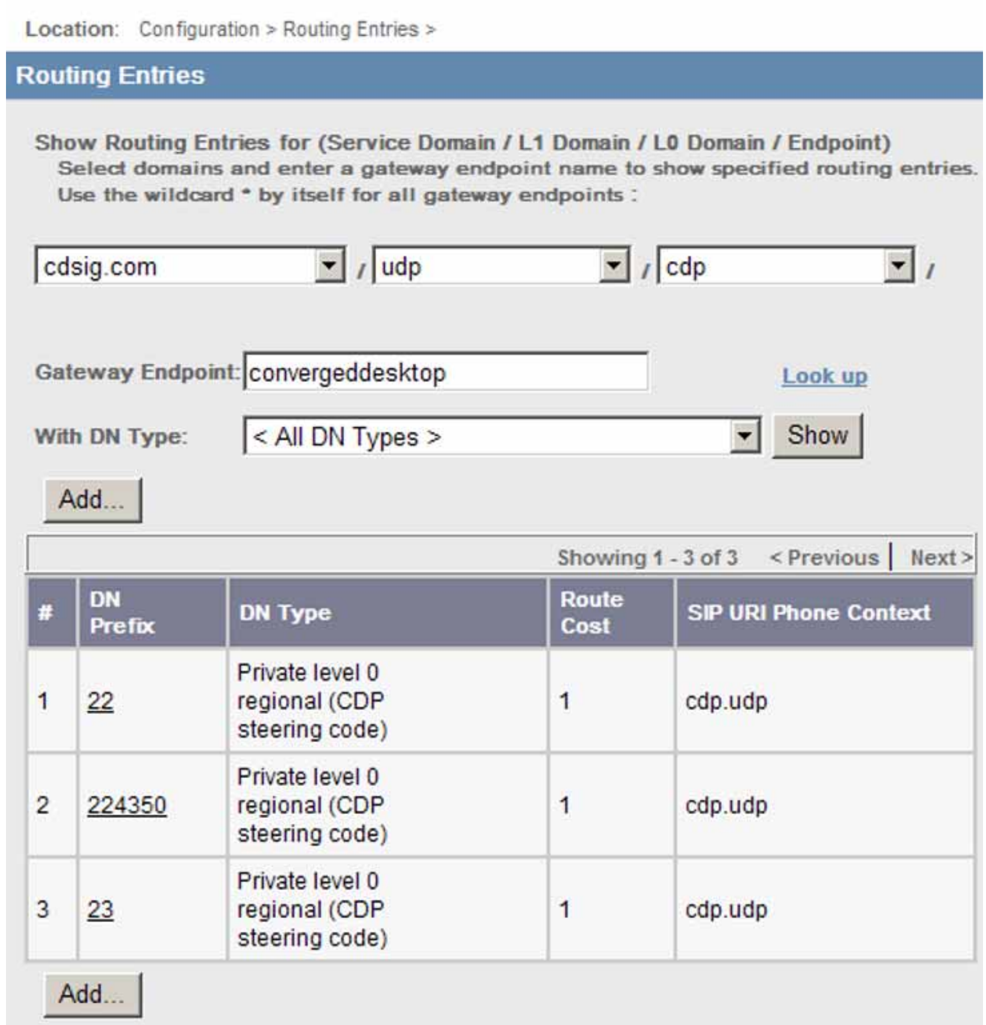
—End—

Configuring routing entries

Perform the following procedure to configure routing entries.

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab
3	Click **set Standby DB view** to switch from active to standby database view.
4	Click **Routing Entries**.
5	Type the relevant **Gateway Endpoint** OR Click the **Look up** link and perform a search. All configured endpoints appear.
6	Click the endpoint to configure as a Routing Entry.
7	Select a **DN** type. For **UDP**, select **Private level 1 regional (UDP location code)**.
8	For **CDP**, select **Private level 0 regional (CDP steering code)**.
9	Click **Show**. The Routing Entries page appears. See Figure 50 "Routing Entries" (page 91).

Figure 50
Routing Entries



10 Click **Add** to add a new Routing Entry.
The Add Routing Entry page appears. See Figure 51 "Add Routing Entry" (page 92).

Figure 51
Add Routing Entry

11 Enter the **DN prefix**.
This is the CDP DSC steering code.

12 Enter the **Route cost**.
The higher the number, the higher the cost. This is equivalent to Least Cost Routing.

13 Click **Save**.

—End—

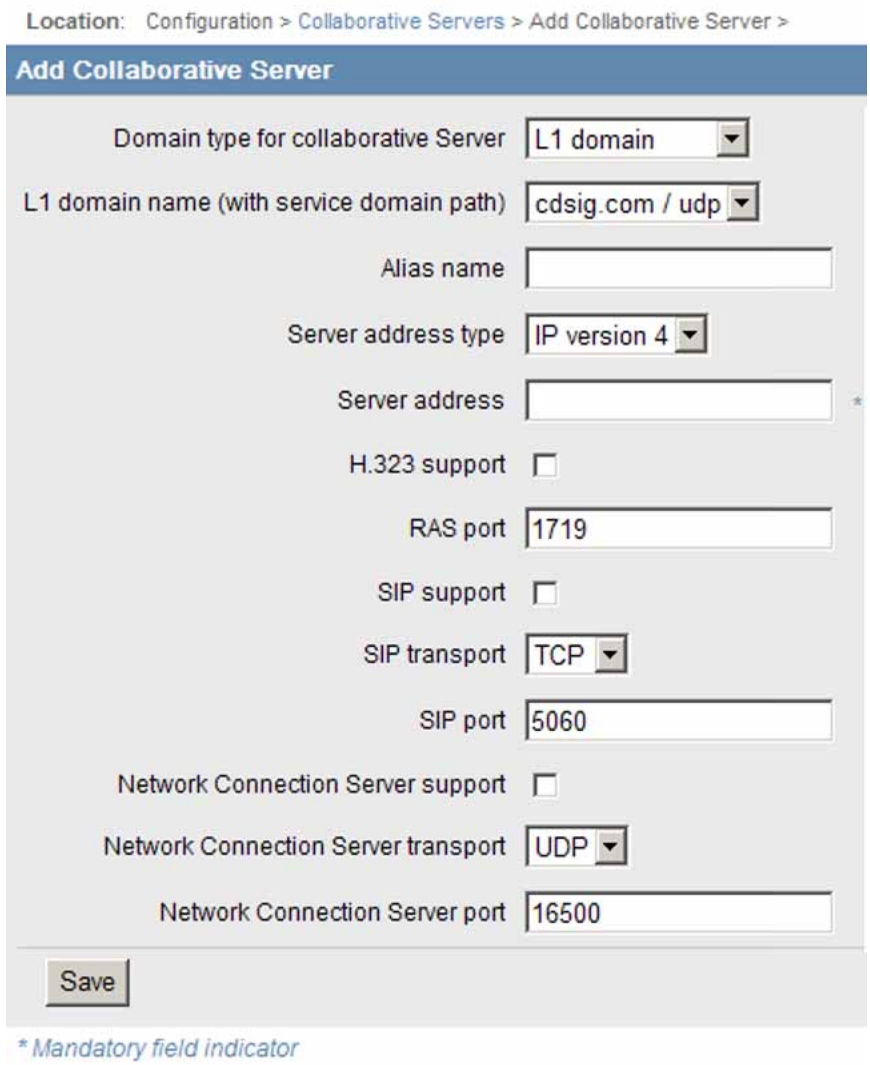
Configuring collaborative servers

A Collaborative Server is a server in another network zone that can resolve requests when your NRS cannot find a match in its numbering plan database.

You can specify a list of Networking Routing Servers in different network zones in your NRS. The NRS Manager provides a utility for adding and viewing a list of NRSs (Collaborative Servers) in different network zones.

Step	Action
1	Log on to NRS Manager.
2	Select the **Configuration** tab
3	Click **set Standby DB view** to switch from active to standby database view.
4	Click **Collaborative Servers**.
5	Click **Add**. The Add Collaborative Server page appears. See Figure 52 "Add Collaborative Server" (page 93). This page may differ from the view shown here depending on the value you choose for the Domain type for collaborative server.

Figure 52
Add Collaborative Server



6 For **Domain type for collaborative Server**, select either **L0 domain** or **L1 domain**.

7 For the **L1** or **L0 domain name**, select the L1 or L0 domain name.

8 Enter the **Alias name** of the collaborative server.
The alias name must be alphanumeric and contain no spaces.

9 For **Server address type**, select **IP version 4**.

10 For **Server address**, type the server IP address.

11 If the H.323 protocol is supported by the server, populate the following fields:

- **H.323 support** check box
- **RAS port**

12 If the SIP protocol is supported by the server, populate the following fields:

- **SIP support** check box
- **SIP transport** protocol
- **SIP port**

13 If Network Connection Service is supported by the server, populate the following fields:

- **Network Connection Server support** check box
- **Network Connection Server transport**
- **Network Connection Server port**

14 Click **Save**.
The Collaborative Servers page appears with the new server.

15 For redundancy purposes, perform this procedure again for the alternate NRS in the other network zone.

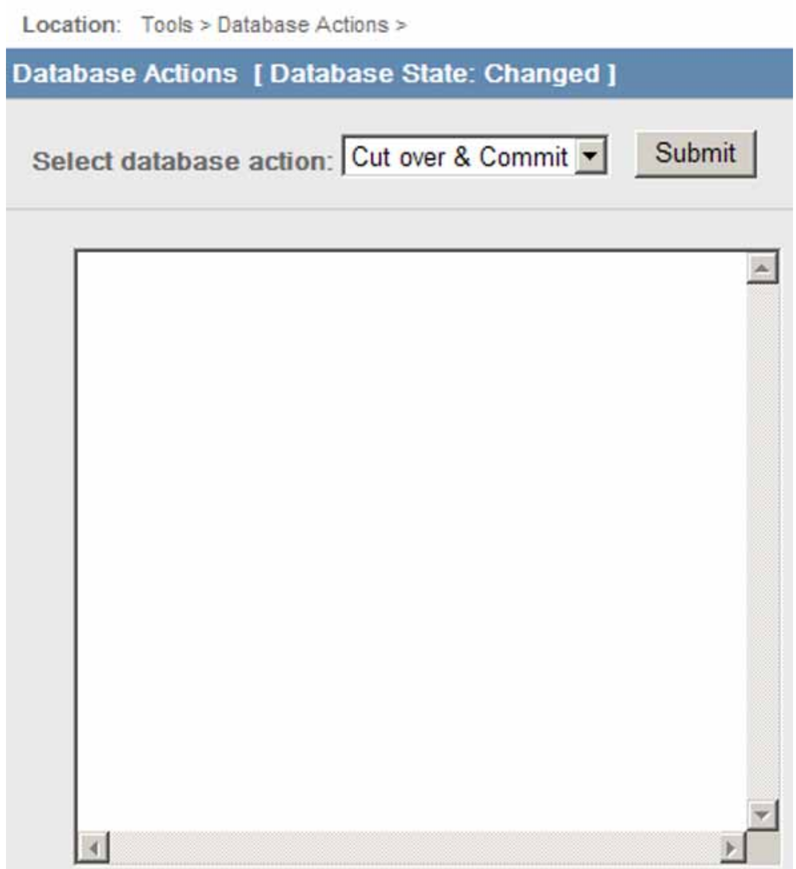
—End—

Updating the database

To save your entries, you must update the database.

Step	Action
1	Log on to NRS Manager.
2	Click the **Tools** tab.
3	Click the **Database Actions** tab. The Database Actions page appears, showing the Database State as Changed. See Figure 53 "Database Actions" (page 95).

Figure 53
Database Actions



4 From the **Select database action** menu, select **Cut over & Commit**.

5 Click **Submit**.

—End—

Checking the status of registered endpoints

Perform the following procedure to check the status of registered endpoints.

Step	Action
1	Log on to NRS Manager.
2	Click the **Configuration** tab.
3	Select **Service Domains**. See Figure 46 "Service Domains" (page 80).

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 54 "Gateway Endpoints" (page 96).

Figure 54
Gateway Endpoints

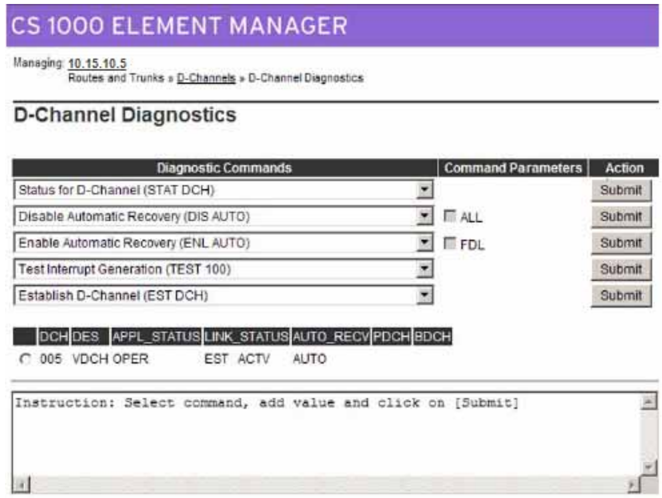
—End—

Checking the status of virtual D-channels

Perform the following procedure to check the status of virtual D-channels.

Step	Action
1	Log on to Element Manager.
2	Select **Routes and Trunks > D-Channels**.
3	Select **D-Channel Diagnostics (LD 96)**. The D-Channel Diagnostics page appears. See Figure 55 "D-Channel Diagnostics" (page 97).

Figure 55
D-Channel Diagnostics



4 Under **Diagnostic Commands**, select **Status for D-Channel (STAT DCH)**.

5 Click **Submit**.

6 Check that the D-Channel is operational, established, and active.

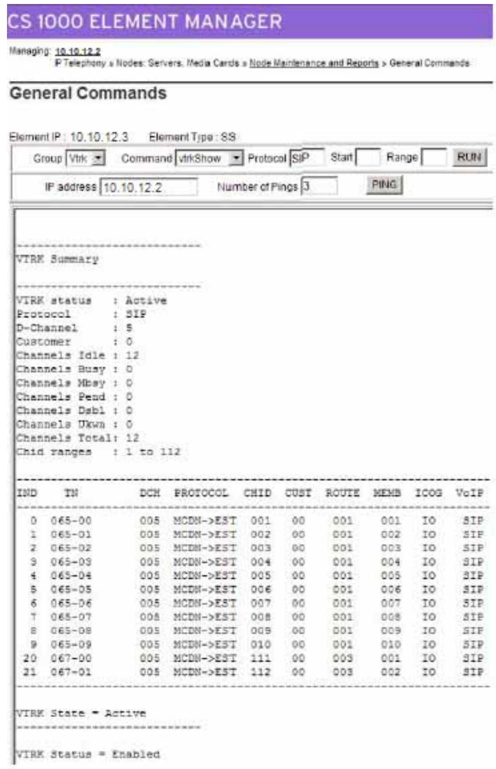
—End—

Checking the status of virtual trunks

Perform the following procedure to check the status of virtual trunks.

Step	**Action**
1	Log on to Element Manager.
2	Select **System > IP Network > Maintenance and Reports**.
3	Expand the **Node ID** heading.
4	Click **GEN CMD** for the switch. The General Commands page appears. See Figure 56 "General Commands" (page 98).

Figure 56
General Commands



5 For **Group**, select **Vtrk**.

6 For **Command**, select **vtrkShow**.

7 For **Protocol**, type **H323**.

8 Click **Run**.
The Virtual Trunk status appears.

9 Check each IP Phone manually (that is, not through Element Manager). At the **DEF GW** option, verify that the IP address is the same as the T-LAN Gateway of that system.
If the phones ring and have dial tone but there is no speech path, the Default Gateway is 0.0.0.0 and is not operational.

—End—

BCM 200/400 configuration

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

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 Element Manager.

BCM 200/400 configuration procedures

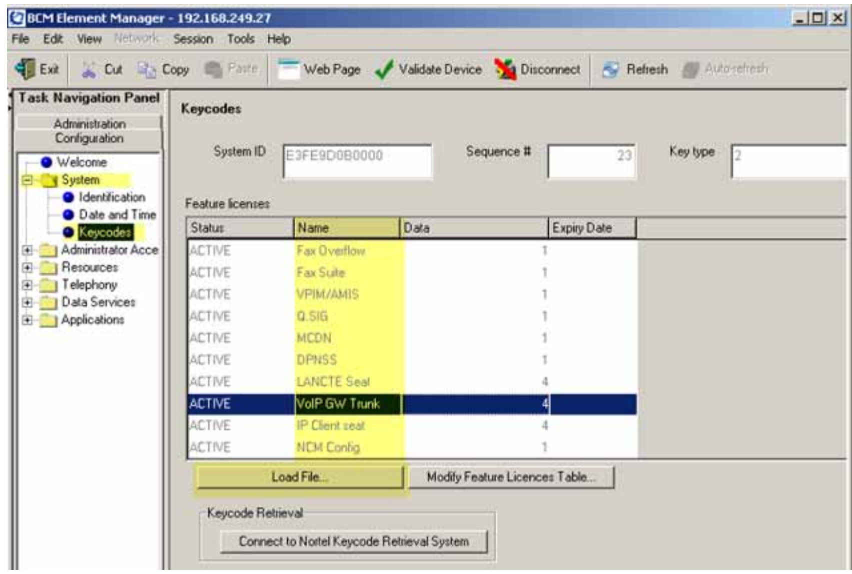
The sequence of BCM 200/400 configuration procedures is as follows:

Configuring incoming VoIP trunks

Perform the following procedure to configure incoming VoIP trunks.

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **System > Keycodes**. See Figure 57 "Keycodes" (page 100).

Figure 57
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).

—End—

Verifying system license and keycodes

Perform the following procedure to verify system license and keycodes.

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **System > Keycodes**. See Figure 57 "Keycodes" (page 100).
4	In the **Name** column, scroll down to **VoIP GW Trunk**. The number of license keys you have are listed in the Data column.

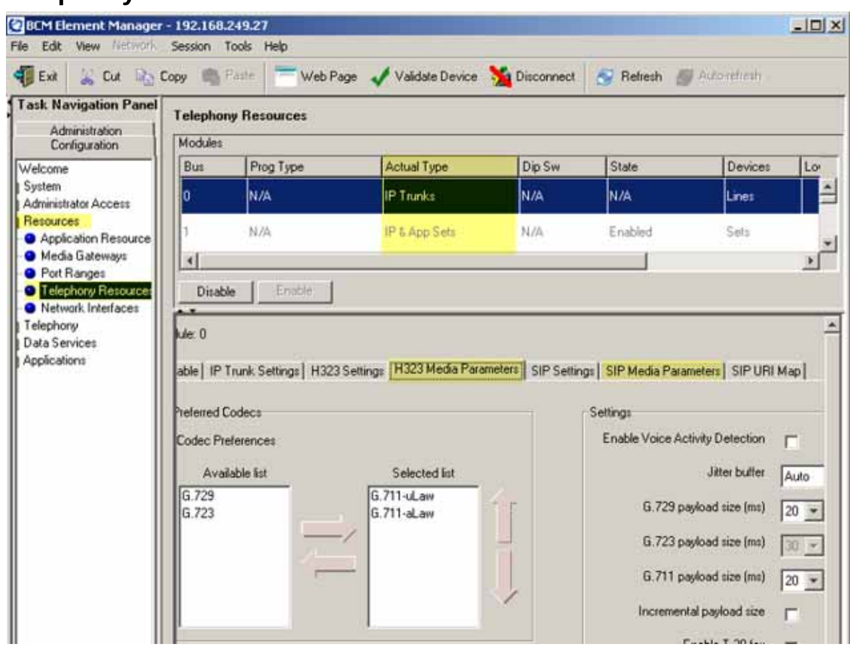
—End—

Configuring VoIP trunk media parameters

Perform the following procedure to configure VoIP trunk media parameters.

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **Resources > Telephony Resources**. See Figure 58 "Telephony Resources" (page 101).

Figure 58
Telephony Resources



Step	Action
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 8 "H.323 Media Parameters fields" (page 102) and Table 9 "SIP Media Parameters fields" (page 103) for a description of the parameters.

—End—

Table 8
H.323 Media Parameters fields

Field	Value	Description
Preferred Codecs	G.711 -uLaw 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).

Field	Value	Description
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.

Table 9
SIP Media Parameters fields

Field	Value	Description
Preferred Codecs	G.711 -uLaw 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.

Field	Value	Description
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).
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

Configuring local Gateway parameters

Perform the following procedure to configure local Gateway parameters.

Step	Action
1	Log on to 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 58 "Telephony Resources" (page 101).
5	Select the **IP Trunk Settings** tab and enter the information that supports your system. See Figure 59 "IP Trunk Settings" (page 105). Refer to Table 10 "IP Trunk Settings fields" (page 105) for information about the IP Trunk Settings fields.

Figure 59
IP Trunk Settings

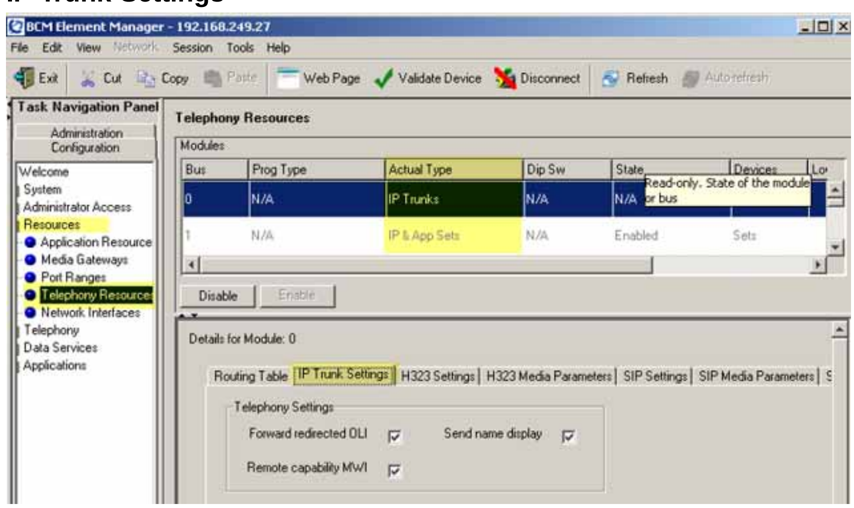


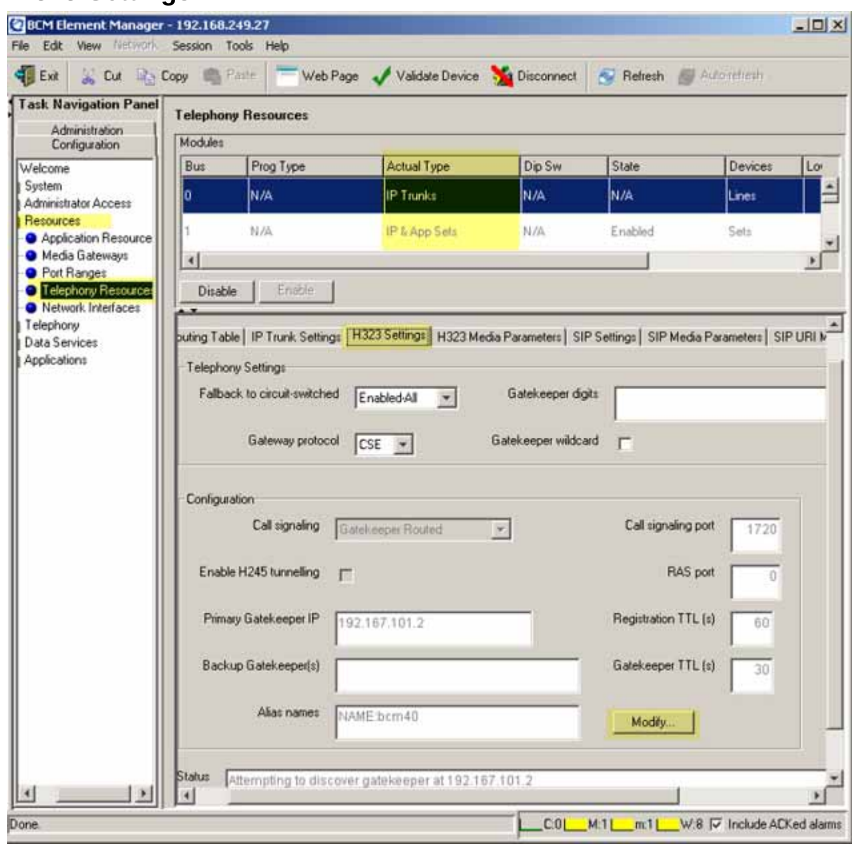
Table 10
IP Trunk Settings fields

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

Field	Value	Description
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 60 "H.323 Settings" (page 106).

Figure 60
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 11 "H.323 Call Signaling Settings fields" (page 107).

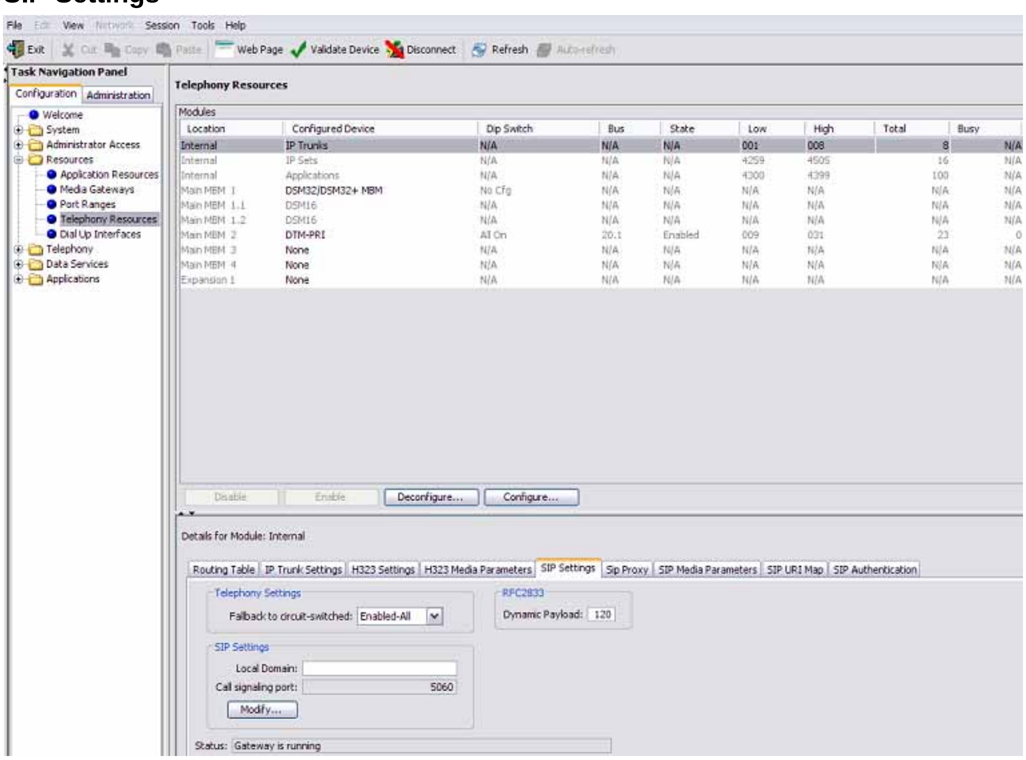
Table 11
H.323 Call Signaling Settings fields

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.
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).

Field	Value	Description
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 61 "SIP Settings" (page 108).

Figure 61
SIP Settings



12 Enter the information that supports your system.
Refer to Table 12 "SIP Settings fields" (page 109) for more information.

Table 12
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-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-All	
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.

—End—

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.

Step	Action
1	Log on to 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 **Parameters** tab and enter the appropriate information for your network. See Figure 62 "Parameters" (page 110). Refer to Table 13 "Parameters fields" (page 110) for configuration information.

Figure 62
Parameters

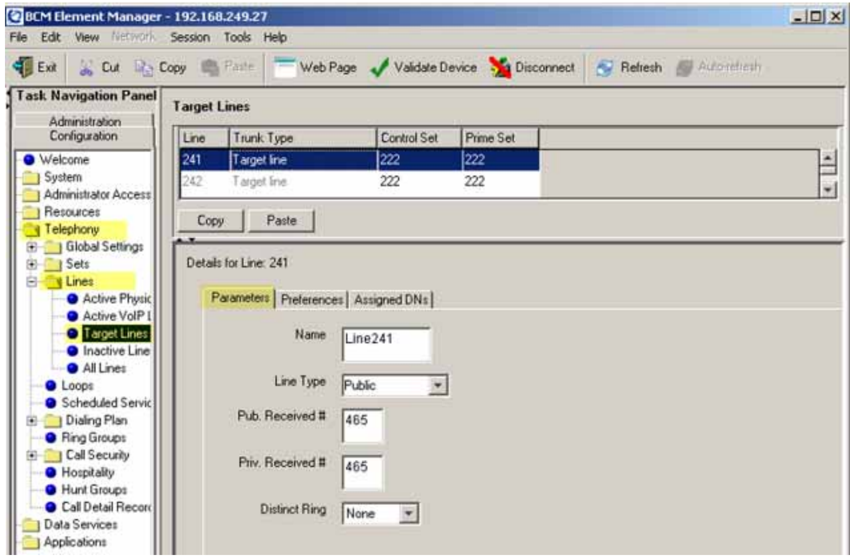


Table 13
Parameters fields

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. 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 63 "Preferences" (page 111). Refer toTable 14 "Preferences fields" (page 111) for configuration information.

Figure 63
Preferences

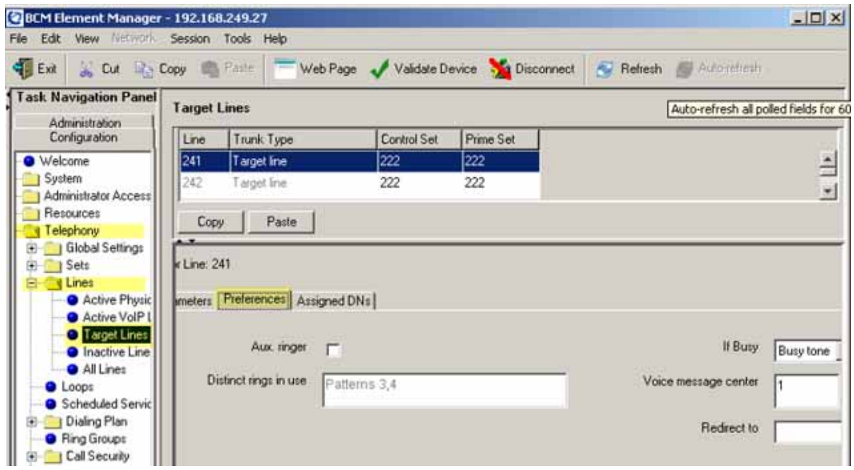
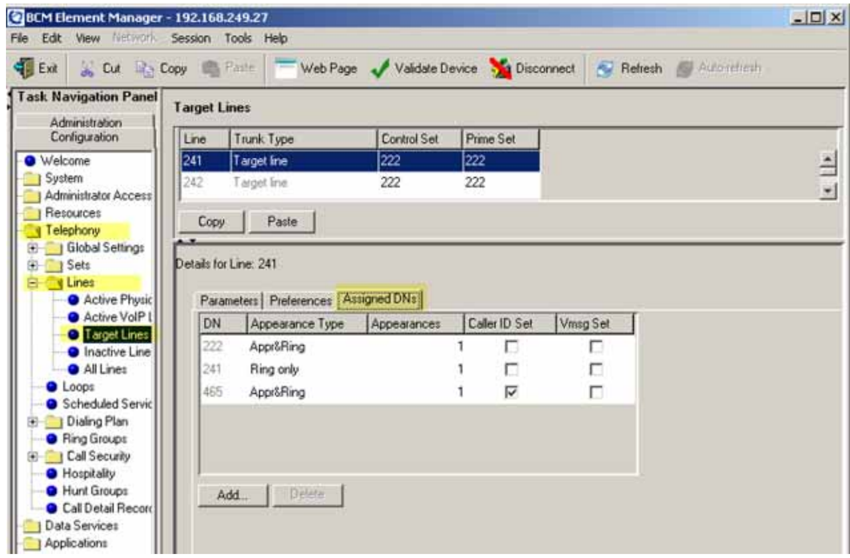


Table 14
Preferences fields

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	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 64 "Assigned DNs" (page 112).

Figure 64
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 18 "Assigned DNs fields" (page 117) for configuration information.

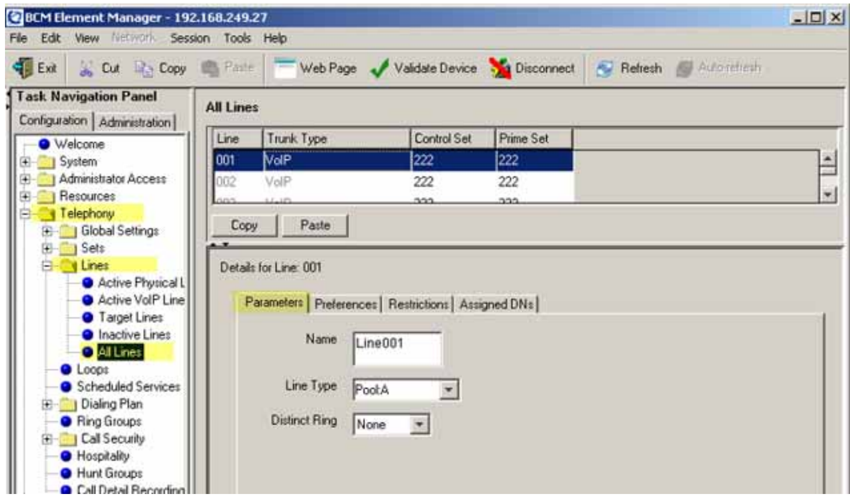
—End—

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.

Step	Action
1	Log on to 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 65 "VoIP lines" (page 113).

Figure 65
VoIP lines



6 Configure the Parameters tab appropriately for your network. Refer to Table 15 "VoIP line descriptions" (page 113) for configuration information.

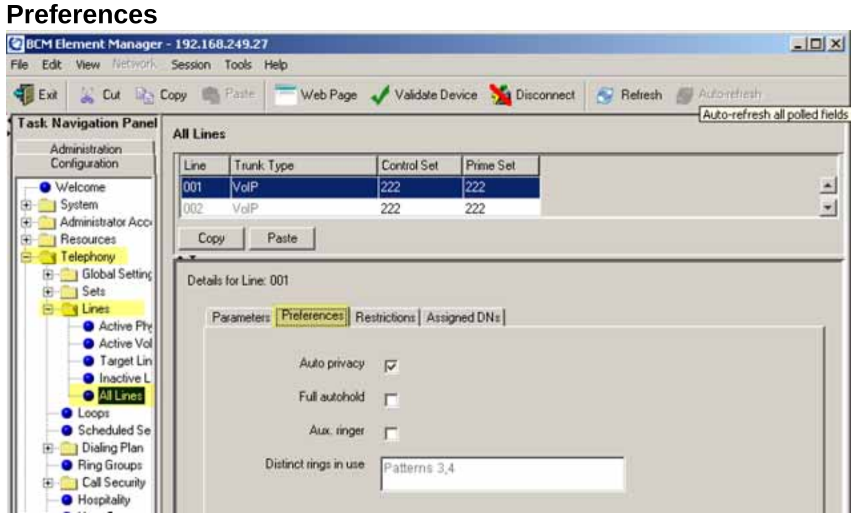
Table 15
VoIP line descriptions

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 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.

Field	Value	Description
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.
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 66 "Preferences" (page 114).

Figure 66
Preferences



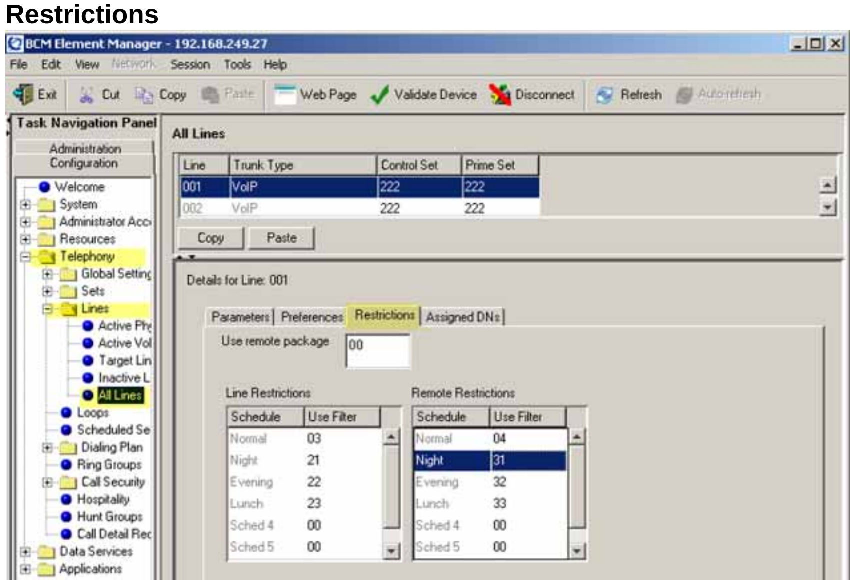
8 Configure the Preferences tab appropriately for your network.
Refer to Figure 66 "Preferences" (page 114) for configuration information.

Table 16
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 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 67 "Restrictions" (page 115).

Figure 67
Restrictions



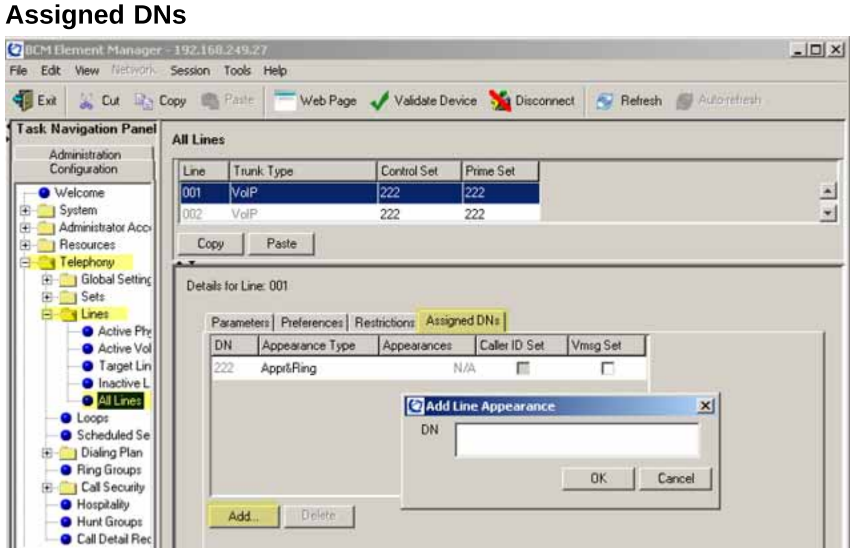
10 Configure the Restrictions tab appropriately for your network.
Refer to Table 17 "Restrictions fields" (page 116) for configuration information.

Table 17
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 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 68 "Assigned DNs" (page 116).

Figure 68
Assigned DNs



12 Click **Add** to add the Target Line DN.

13 Enter the appropriate information for your network.

Refer to Table 18 "Assigned DNs fields" (page 117) for configuration information.

Table 18
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.

—End—

BCM 50/450 configuration

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

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 Element Manager.

BCM 50/450 configuration procedures

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

- "Configuring incoming VoIP trunks" (page 119)
- "Verifying system license and keycodes" (page 120)
- "Configuring VoIP trunk media parameters" (page 121)
- "Configuring local Gateway parameters" (page 125)
- "Configuring VoIP lines" (page 130)
- "Configuring target lines" (page 134)

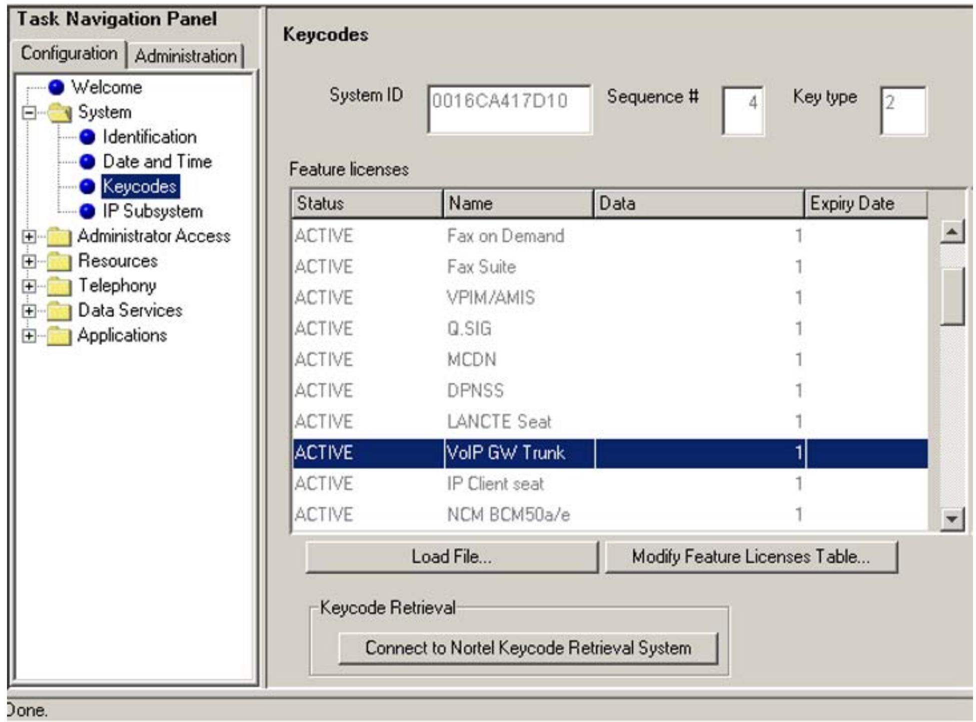
Configuring incoming VoIP trunks

Perform the following procedure to configure incoming VoIP trunks.

Configuring incoming VoIP trunks

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **System > Keycodes**. See Figure 69 "Keycodes" (page 120).

Figure 69
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).

—End—

Verifying system license and keycodes

Perform the following procedure to verify system license and keycodes.

Verifying system license and keycodes

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **System > Keycodes**. See Figure 69 "Keycodes" (page 120).

4 In the **Name** column, scroll down to **VoIP GW Trunk**. The number of license keys you have are listed in the Data column.

—End—

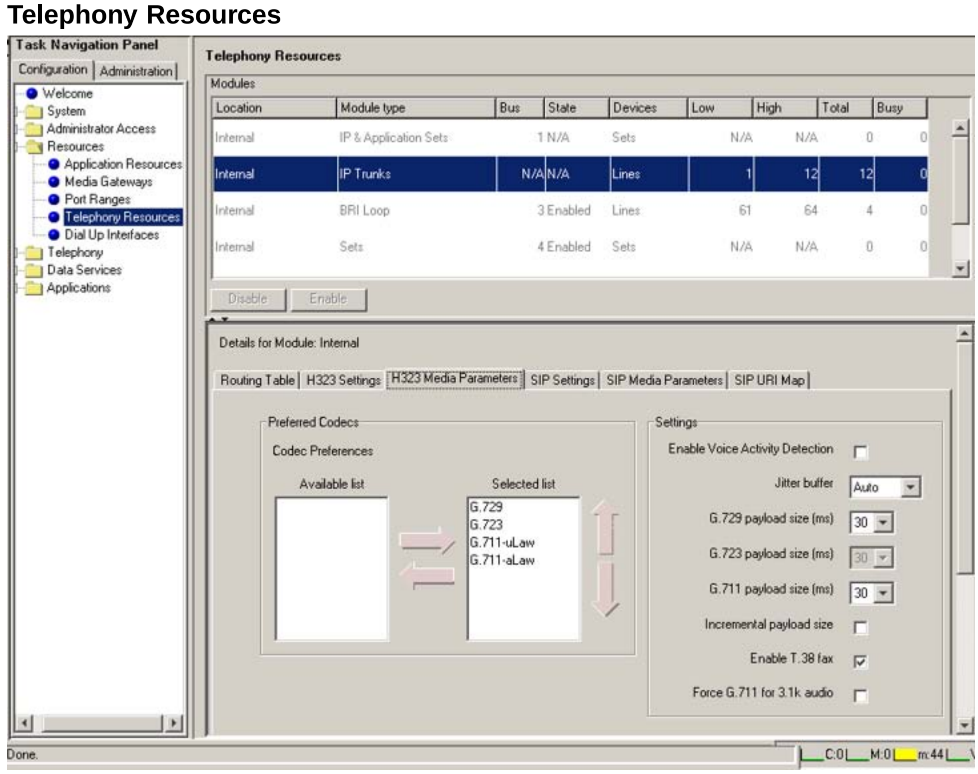
Configuring VoIP trunk media parameters

Perform the following procedure to configure VoIP trunk media parameters.

Configuring VoIP trunk media parameters

Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.
3	Select **Resources > Telephony Resources**. See Figure 70 "Telephony Resources" (page 121).

Figure 70
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 19 "H.323 Media Parameters fields" (page 122) and Table 20 "SIP Media Parameters fields" (page 123) for a description of the parameters.

—End—

Table 19
H.323 Media Parameters fields

Field	Value	Description
Preferred Codecs	G.711 -uLaw 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.

Field	Value	Description
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).
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.

Table 20
SIP Media Parameters fields

Field	Value	Description
Preferred Codecs	G.711 -uLaw G.711 -aLaw G.729	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.

Field	Value	Description
	G.723	**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 *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 may disrupt calls at other telephones using VoIP trunks in the vicinity of

Field	Value	Description
		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

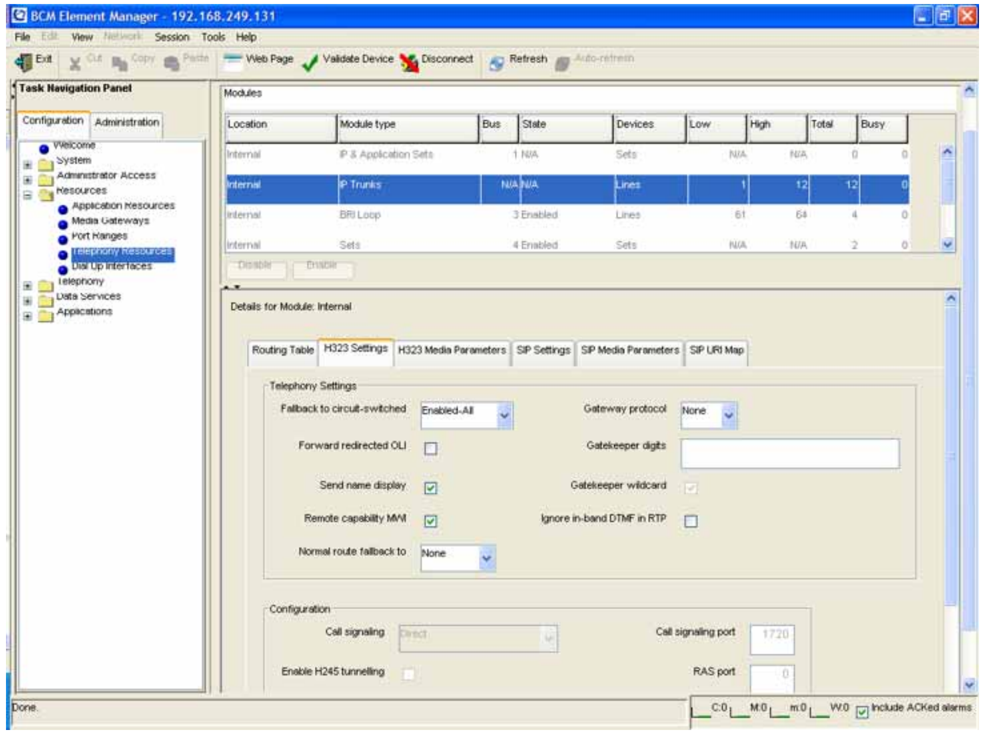
Configuring local Gateway parameters

Perform the following procedure to configure local Gateway parameters.

Configuring local Gateway parameters

Step	Action
1	Log on to 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 70 "Telephony Resources" (page 121).
5	For H.323 VoIP trunks, select the **H.323 Settings** tab. See Figure 71 "H.323 Settings" (page 126).

Figure 71
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 21 "H.323 Call Signaling Settings fields" (page 127).

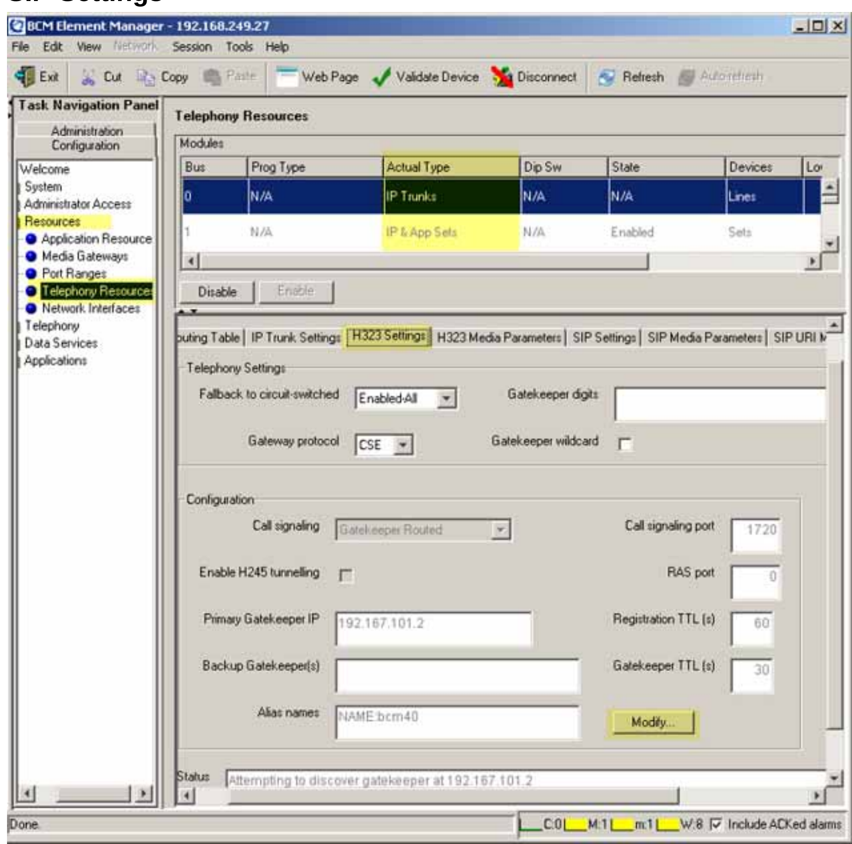
Table 21
H.323 Call Signaling Settings fields

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.
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.

Field	Value	Description
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 72 "SIP Settings" (page 128).

Figure 72
SIP Settings



11 Enter the information that supports your system.
Refer to Table 22 "SIP Settings fields" (page 129) for more information.

Table 22
SIP Settings fields

Field	Value	Description
Fallback to circuit-switched	Disabled Enabled-TDM Enabled-All	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.
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.

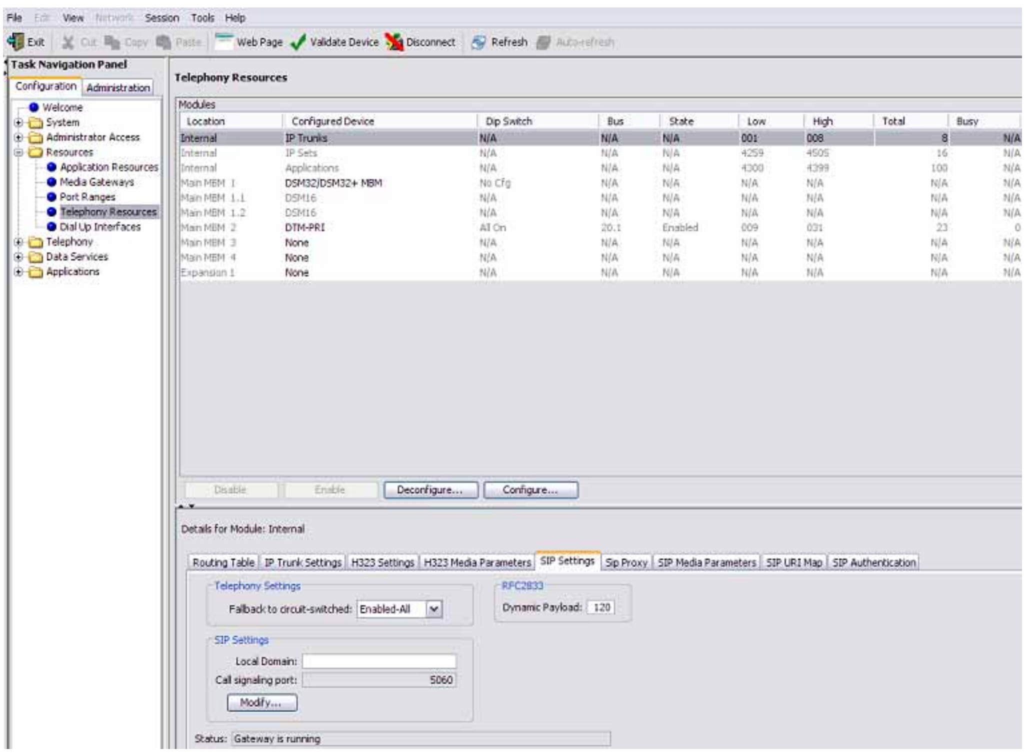
12 To configure SIP Proxy click the SIP Proxy Tab.
Refer to Table 23 "SIP Proxy Tab" (page 129)for more information.

Table 23
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 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.

Field	Value	Description
	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 73
SIP Proxy Tab



—End—

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

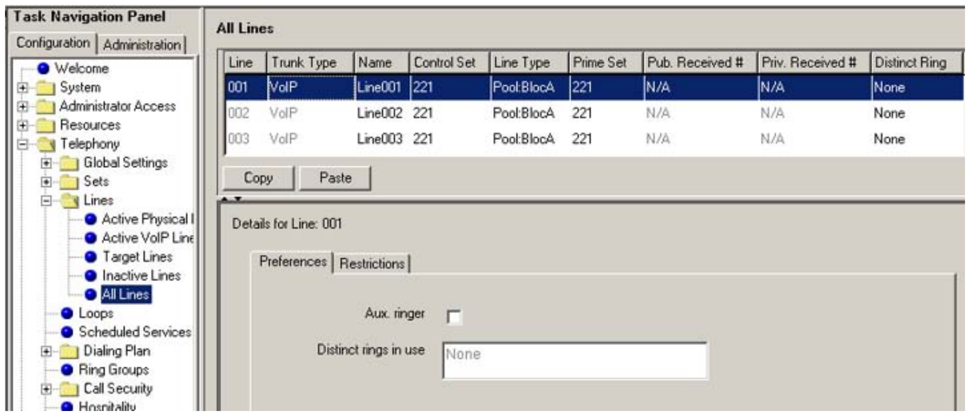
Step	Action
1	Log on to Element Manager.
2	In the **Task Navigation Panel**, select the **Configuration** tab.

3 Select **Telephony > Lines > All Lines**.

4 Highlight the individual line you wish to configure.

5 Select the **Preferences** tab.
See Figure 74 "Preferences" (page 131).

Figure 74
Preferences



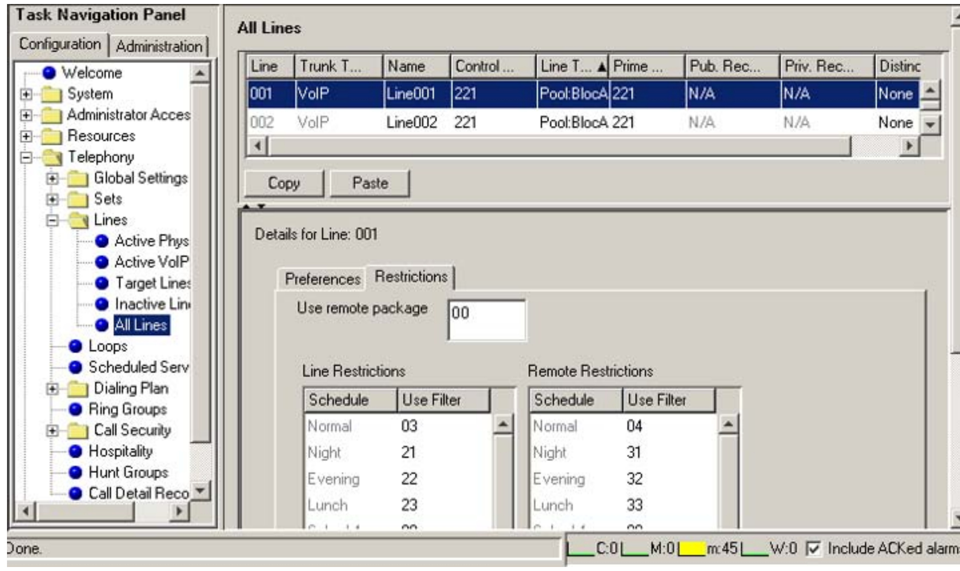
6 Configure the Preferences tab appropriately for your network.
Refer to Table 24 "Preferences fields" (page 131) for configuration information.

Table 24
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 75 "Restrictions" (page 132).

Figure 75
Restrictions



8 Configure the Restrictions tab appropriately for your network. Refer to Table 25 "Restrictions fields" (page 132) for configuration information.

Table 25
Restrictions fields

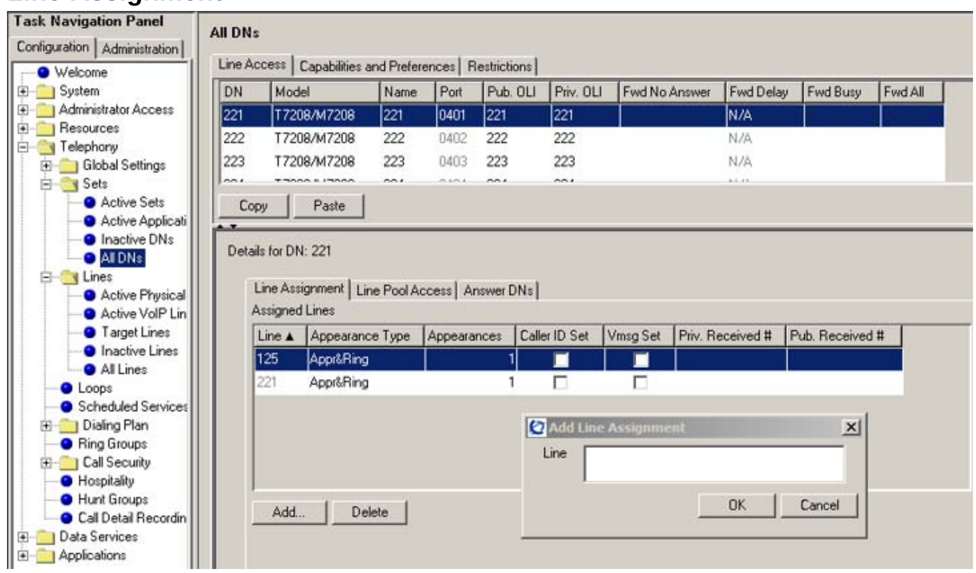
Field	Value	Description
Use remote package	< package #>	If the line is used to receive external calls or calls from other nodes on the private network, ensure that you indicate a remote package that provides only the availability that you want for external callers. This attribute is typically used for 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 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 76 "Line Assignment" (page 133).

Figure 76
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 26 "Assigned DNs fields" (page 133) for configuration information.

Table 26
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.

Field	Value	Description
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.

—End—

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

Step	Action
1	Log on to 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 77 "Preferences" (page 135). Refer toTable 27 "Preferences fields" (page 135) for configuration information.

Figure 77
Preferences

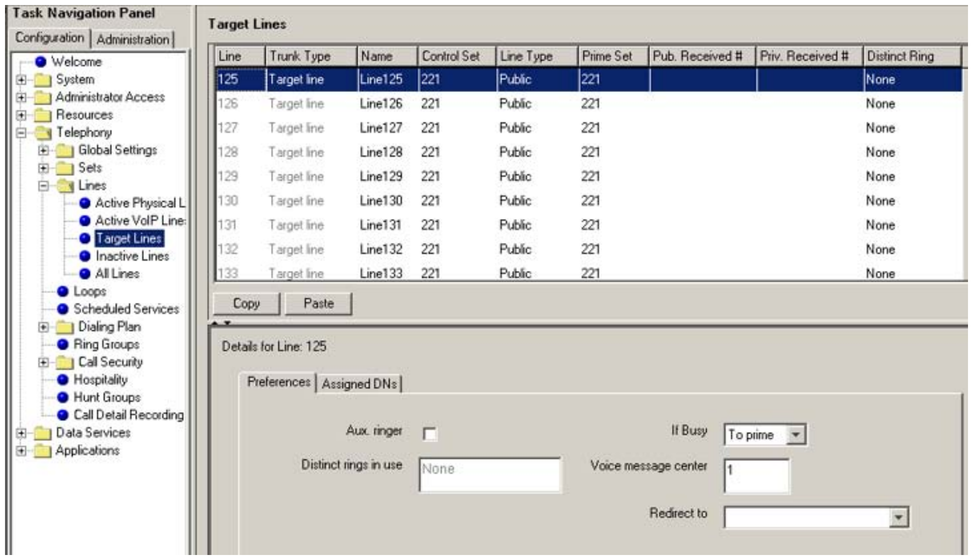
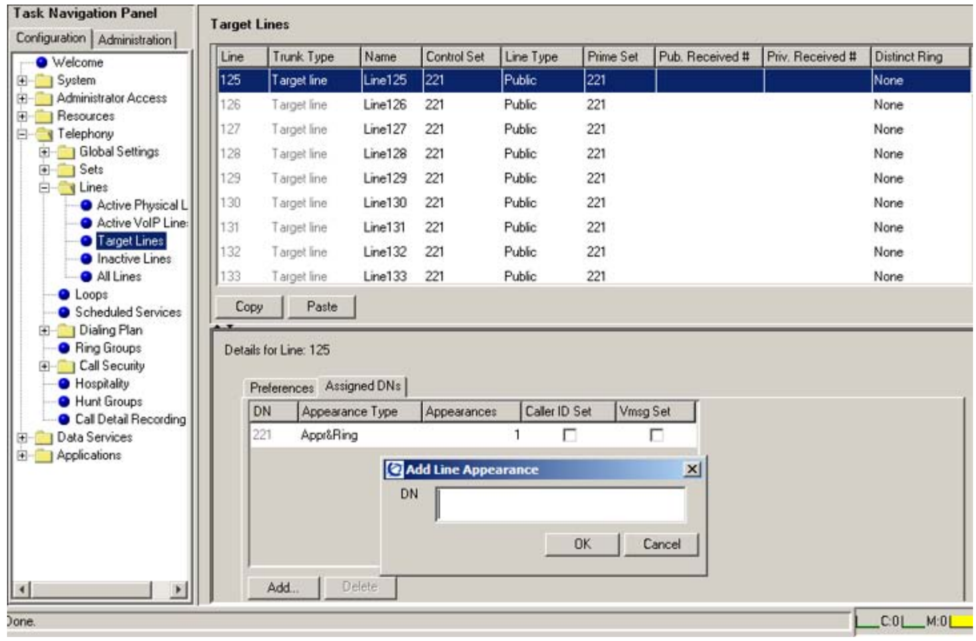


Table 27
Preferences fields

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 the proper routing information.

6 Select the **Assigned DNs** tab.
See Figure 78 "Assigned DNs" (page 136).

Figure 78
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 to Table 18 "Assigned DNs fields" (page 117) for configuration information.

—End—

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

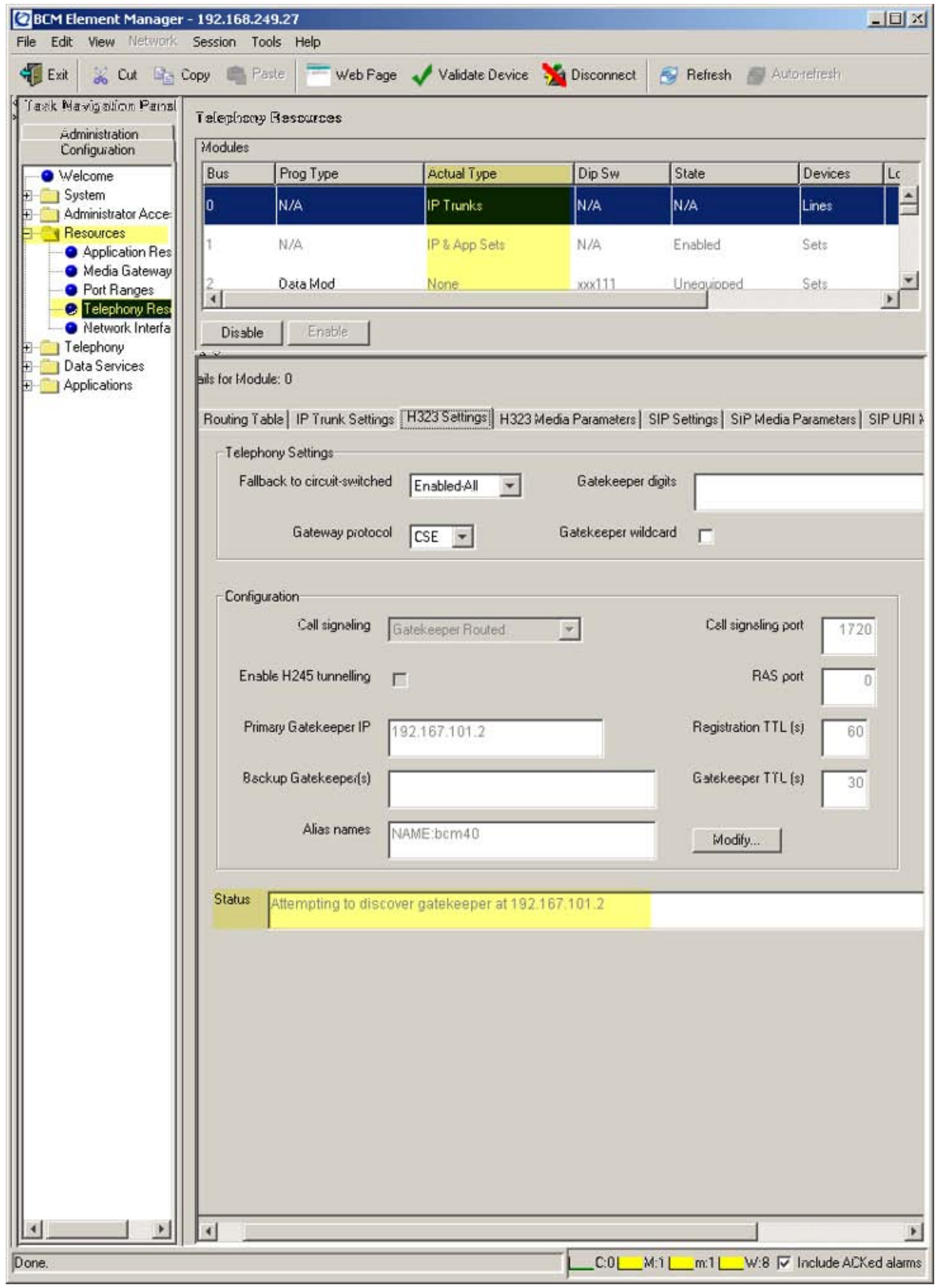
The CS 1000/BCM integration is considered successful if BCM and Network Routing Service (NRS) are able to register to each other. You can determine this from either the CS 1000 side or the BCM side.

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* (553-3001-183).

Testing the integration from the BCM system

Step	Action
1	Log on to Element Manager on the BCM system.
2	Select **Resources > Telephony Resources**. See Figure 79 "Status" (page 139).

Figure 79
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 two systems are successfully registered.

—End—

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. Refer to the procedure "Checking the status of registered endpoints" (page 95).

Troubleshooting

Refer to these troubleshooting procedures to resolve common integration issues.

BCM is unable to contact the gatekeeper at IP address

Step	Action
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.

—End—

Unable to complete any calls

Step	Action
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* (553-3001-183).

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* (553-3001-183).

—End—

Cannot make calls between the CS 1000 and BCM

Symptoms:

- calls between the CS 1000 and BCM fail
- CDP calls fail
- no channel/circuit is available

Step	Action
1	Verify your dialing plan and call routing.
2	On the BCM, log on to 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.

—End—

BCM fails to register to NRS

Symptoms:

- BCM fails to register to the NRS
- calls fail between the CS 1000 and BCM in both directions

Step	Action
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.

—End—

H.323 Gateway service is down

Symptoms:

- VoIP H.323 Gateway service is down
- VoIP Gateway cannot be started manually
- VoIP Gateway does not start after a reboot or power cycle

Step	Action
1	On the BCM, log on to 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" (page 138).

—End—

Enterprise: Common

Solution Integration Guide for Communication Server 1000 Release 5.5/Business Communications Manager

Publication: NN43001-326
Document status: Standard
Document version: 02.01
Document date: 3 April 2009

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

Sourced in Canada

NORTEL