Succession 1000
Succession 1000M
Succession 3.0 Software

IP Peer Networking

Document Number: 553-3001-213
Document Release: Standard 1.00
Date: October 2003

Produced in Canada

Revision history

October 2003

Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: IP Peer Networking (553-3023-220).

Contents

About this document

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

Subject

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

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Succession 3.0 Software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support** on the Nortel Networks home page:

http://www.nortelnetworks.com/

Applicable systems

This document applies to the following systems:

- Succession 1000
- Succession 1000M Chassis
- Succession 1000M Cabinet
- Succession 1000M Half Group
- Succession 1000M Single Group
- Succession 1000M Multi Group

System migration

When particular Meridian 1 systems are upgraded to run Succession 3.0 Software and configured to include a Succession Signaling Server, they become Succession 1000M systems. Table 1 lists each Meridian 1 system that supports an upgrade path to a Succession 1000M system.

Table 1
Meridian 1 systems to Succession 1000M systems

This Meridian 1 system...	Maps to this Succession 1000M system
Meridian 1 Option 11C Chassis	Succession 1000M Chassis
Meridian 1 Option 11C Cabinet	Succession 1000M Cabinet
Meridian 1 Option 51C	Succession 1000M Half Group
Meridian 1 Option 61	Succession 1000M Single Group
Meridian 1 Option 61C	Succession 1000M Single Group
Meridian 1 Option 61C CP PII	Succession 1000M Single Group
Meridian 1 Option 81	Succession 1000M Multi Group
Meridian 1 Option 81C	Succession 1000M Multi Group
Meridian 1 Option 81C CP PII	Succession 1000M Multi Group

Note the following:

- When an Option 11C Mini system is upgraded to run Succession 3.0 Software, that system becomes a Meridian 1 Option 11C Chassis.
- When an Option 11C system is upgraded to run Succession 3.0 Software, that system becomes a Meridian 1 Option 11C Cabinet.

For more information, see one or more of the following NTPs:

- *Small System: Upgrade Procedures* (553-3011-258)
- *Large System: Upgrade Procedures* (553-3021-258)
- *Succession 1000 System: Upgrade Procedures* (553-3031-258)

Intended audience

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

Conventions

Terminology

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

- Succession 1000
- Succession 1000M

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

- Succession 1000M Chassis
- Succession 1000M Cabinet

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

- Succession 1000M Half Group
- Succession 1000M Single Group
- Succession 1000M Multi Group

The call processor in Succession 1000 and Succession 1000M systems is referred to as the "Succession Call Server".

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Data Networking for Voice over IP* (553-3001-160)
- *Electronic Switched Network: Signaling and Transmission Guidelines* (553-3001-180)
- *Dialing Plans: Description* (553-3001-183)
- *Signaling Server: Installation and Configuration* (553-3001-212)
- *Branch Office* (553-3001-214)
- *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232)
- *System Management* (553-3001-300)
- *Optivity Telephony Manager: System Administration* (553-3001-330)
- *IP Trunk: Description, Installation, and Operation* (553-3001-363)
- *Basic Network Features* (553-3001-379)
- *Software Input/Output: System Messages* (553-3001-411)
- *Small System: Planning and Engineering* (553-3011-120)
- *Small System: Installation and Configuration* (553-3011-210)
- *Small System: Upgrade Procedures* (553-3011-258)
- *Large System: Planning and Engineering* (553-3021-120)
- *Large System: Installation and Configuration* (553-3021-210)
- *Large System: Upgrade Procedures* (553-3021-258)
- *Succession 1000 System: Overview* (553-3031-010)
- *Succession 1000 System: Planning and Engineering* (553-3031-120)
- *Succession 1000 System: Installation and Configuration* (553-3031-210)

- *Succession 1000 System: Upgrade Procedures* (553-3031-258)
- *Succession 1000 System: Maintenance* (553-3031-500)

Online

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

http://www.nortelnetworks.com/

CD-ROM

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

Overview

Contents

This section contains information on the following topics:

IP Peer Networking overview

Succession 3.0 Software supports IP Peer Networking Phase 2. This enables the customer to distribute the functionality of the Succession 1000 and Succession 1000M systems over a Wide Area Network (WAN), using either standard H.323 Gateways or Nortel Networks IP Gateways (Nortel Networks Succession Signaling Server).

IP Peer Networking Phase 2 brings the same features to the Succession 1000M System as IP Peer Networking brings to the Succession 1000 System, plus enhancements. See "IP Peer Networking enhancements" on page 56.

Key advantages of IP Peer Networking are as follows:

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

  IP Peer Networking uses direct IP media paths for connections that involve two IP devices. Media streams route directly between the Internet Telephones and Gateways over the IP network, using Virtual Trunks. This minimizes voice quality issues caused by delay and transcoding between circuit-switched voice and IP packets. For more information on Virtual Trunks, see page 17).

IP Peer Networking uses an H.323 Gatekeeper to simplify the configuration of IP component addressing. The H.323 Gatekeeper (optionally redundant) manages a centralized numbering plan for the network.

A existing system must be upgraded with the Succession 3.0 Software for IP Peer Networking and a Succession Signaling Server must also be installed and configured to provide the H.323 signaling for Virtual Trunks. Refer to page 19 for more information about the Succession Signaling Server.

The Succession Signaling Server is an industry-standard, PC-based server that provides a central processor to drive H.323 signaling for Internet Telephones and IP Peer Networking. For more information about the Succession Signaling Server, see *Signaling Server: Installation and Configuration* (553-3001-212).

Virtual Trunk

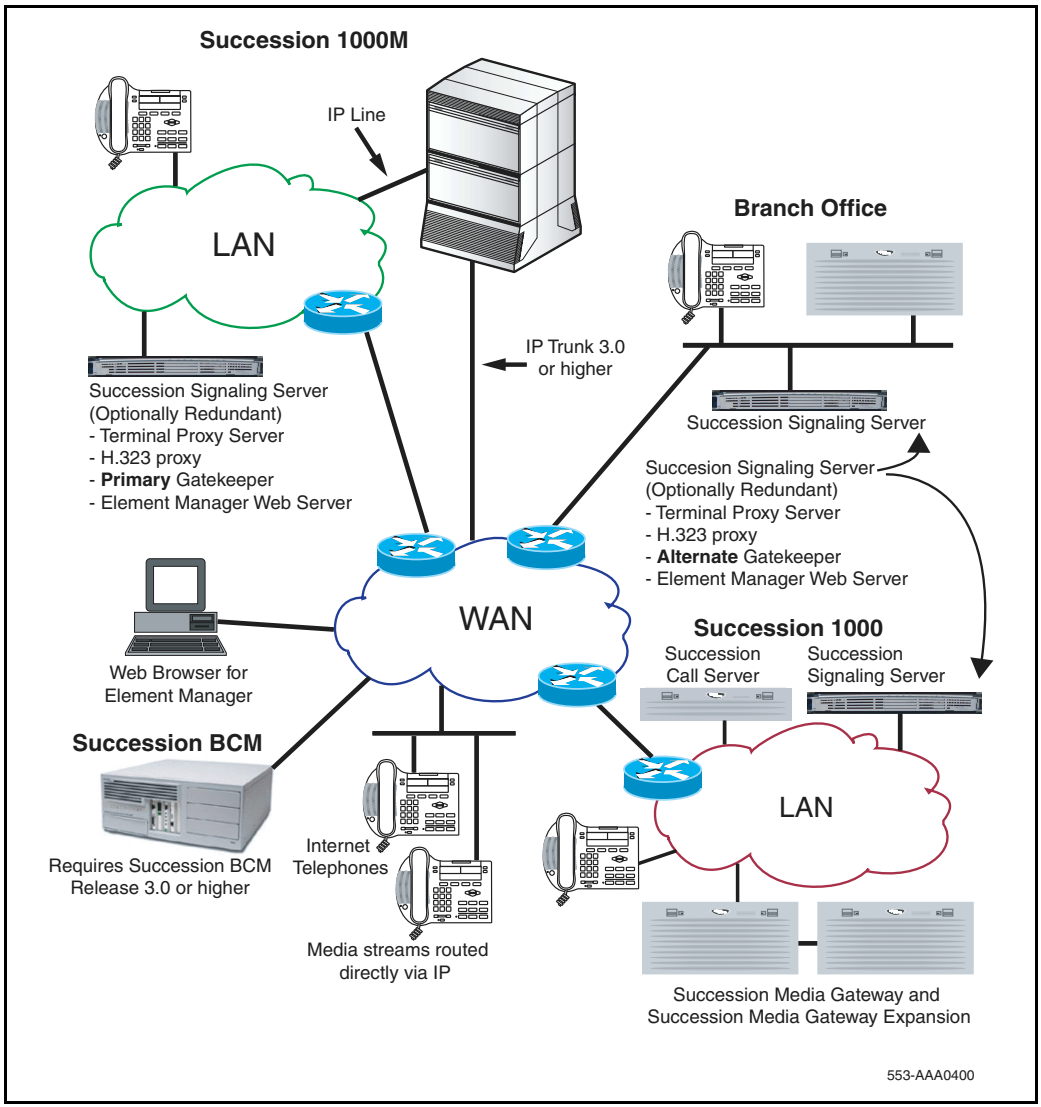
Virtual Trunks are software components configured on virtual loops, similar to Internet Telephones. A Virtual Trunk acts as the bridge between existing call processing features and the IP network. It enables access to all trunk routing and access features that are part of the MCDN networking feature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

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

The number of Virtual Trunks supported by each Succession Signaling Server increases from 200 to 382 with the Succession 3.0 Software.

Figure 1 on page 18 illustrates an IP Peer Networking configuration.

Figure 1
IP Peer Networking



Succession Signaling Server

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

The Succession Signaling Server can be installed in a load-sharing redundant configuration for higher scalability and reliability.

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

The following software components can operate on the Succession Signaling Server:

- Terminal Proxy Server (TPS)
- H.323 Gateway Signaling software
- H.323 Gatekeeper software (optionally redundant)
- Element Manager web server

> ***Note:*** Element Manager has a set of dedicated webpages for managing the Gatekeeper.

The software components are described in the sections that follow.

Terminal Proxy Server

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

IP Peer Networking supports the i2002 and i2004 Internet Telephones, and the i2050 Software Phone (soft client) for IP telephony. Each Internet Telephone can be configured through the Dynamic Host Configuration Protocol (DHCP) to register with a Call Server for feature control.

H.323 Gateway Signaling software

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

Direct IP media paths provide the following benefits:

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

See “Interworking protocols” on page 52 for further information.

H.323 Gatekeeper software

The IP Peer Networking feature provides a Gatekeeper where all Succession 1000 and Succession 1000M Large and Small Systems in the network are registered. This eliminates the need for manual configuration of IP addresses and numbering plan information at every site.

The Gatekeeper manages a centralized numbering plan for the network. This enables simplified management of the Succession 1000 and Succession 1000M network. The H.323 Gatekeeper software identifies the IP addresses of H.323 Gateways, based on the network-wide numbering plan. This includes the Succession 1000 System, Succession 1000M Large and Small Systems, and third-party systems.

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

The Gatekeeper can operate in stand-alone mode without being connected to a Succession Call Server.

For Succession 1000 and Succession 1000M Systems, the Gatekeeper can be a co-resident Gatekeeper in the same Succession Signaling Server or a stand-alone Gatekeeper in a different Succession Signaling Server.

For more information about stand-alone Gatekeepers, see “Stand-alone Gatekeeper support for Meridian 1 and BCM nodes” on page 112.

Element Manager has a set of webpages for managing the Gatekeeper.

See “Gatekeeper functionality” on page 89 and “Managing the Gatekeeper” on page 239 for further information.

Element Manager web server

The Element Manager web server functions on the Succession Signaling Server platform. Use the web browser interfaces, in conjunction with Optivity Telephony Manager (OTM) and the Command Line Interface (CLI) overlays, to configure and maintain the elements in the Succession 1000 and Succession 1000M Large and Small Systems.

Direct IP Media Paths

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

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

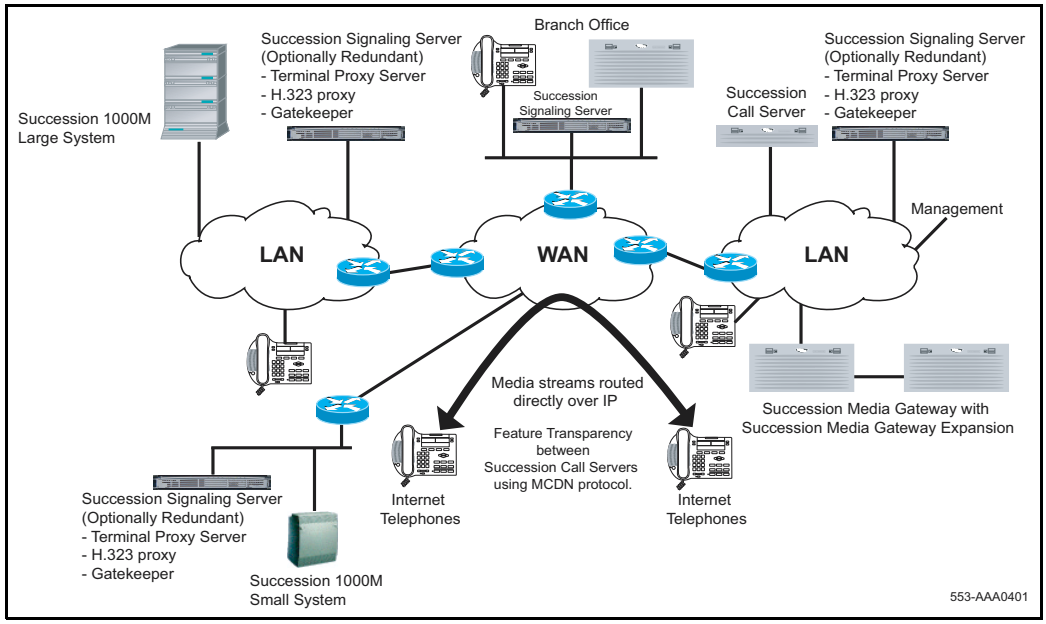
Note 2: A Media Gateway is a gateway that uses a protocol similar to the Media Gateway Control Protocol (MGCP). The Succession Media Gateway was introduced in Succession Communication Server for Enterprise 1000 Release 1.0 and houses peripheral cards. Succession Media Gateways are controlled directly by the Succession Call Server. Peripheral cards are housed in the IPE Shelf in Succession 1000M Systems.

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

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

Figure 2 on page 23 shows a media path routed directly over IP, not using a circuit switch.

Figure 2
An example of IP Peer Networking using Virtual Trunk and direct media paths



Internet Telephone to Internet Telephone (on separate Succession Call Servers)

An Internet Telephone at Site A calls an Internet Telephone at Site B (see Figure 3 on page 25). When the user presses a key on the Internet Telephone, a signaling message is carried over the IP network.

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

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

Basic network call walk-through

When a user makes a call on a Succession 1000 or a Succession 1000M Large or Small System, the dialed digits are translated to determine if the user is attempting to reach an internal or external telephone.

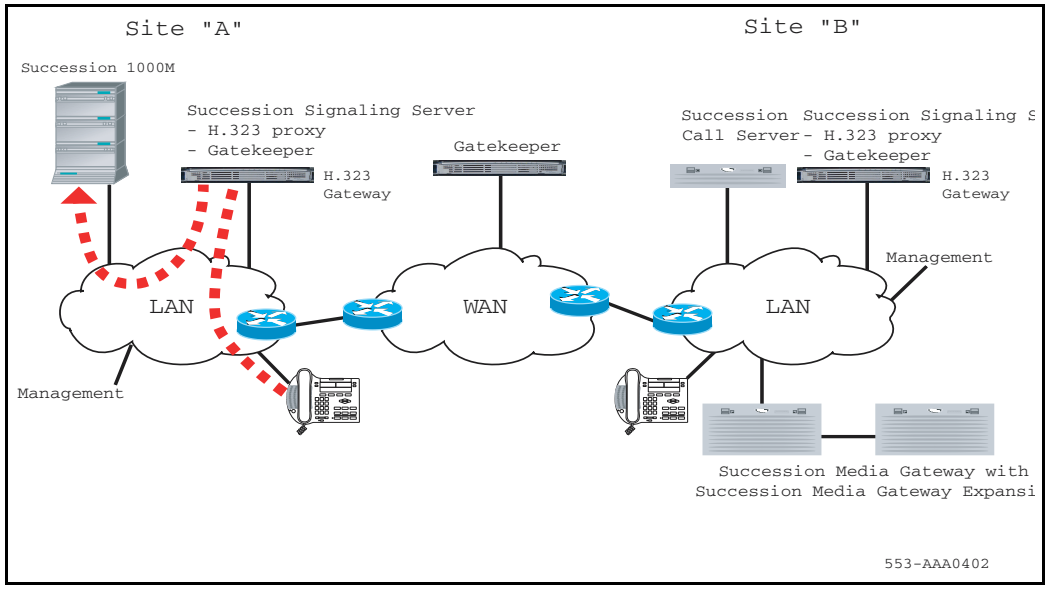
If the user is attempting to reach an internal telephone, the call is terminated on the internal device. When the system determines that the user is attempting to reach a telephone or service using the IP network, the call routes to the H.323 Gateway software. The H.323 Gateway software uses the Gatekeeper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

Note: Configure Virtual Trunk routes as circuit-switched routes. Use Element Manager or LD 14 and LD 16 in the Command Line Interface (CLI). See “Configuring the Virtual routes and trunks” on page 167.

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

1 User A on Succession Call Server A dials the DN of User B on Succession Call Server B. Succession Call Server A collects the digits through the TPS on the Succession Signaling Server. See Figure 3.

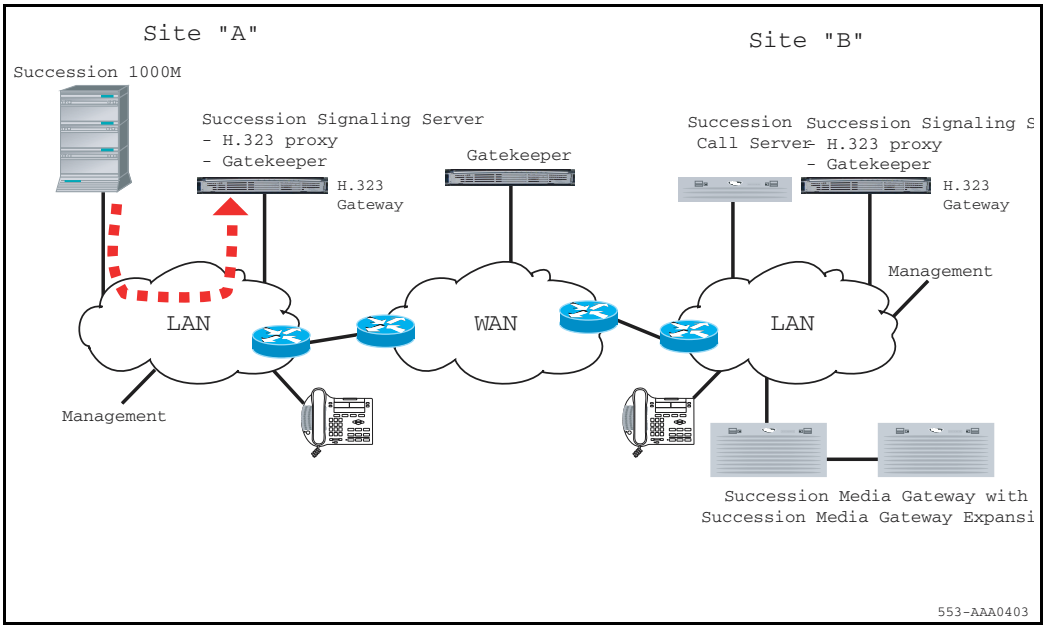
Figure 3
User A dials User B



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

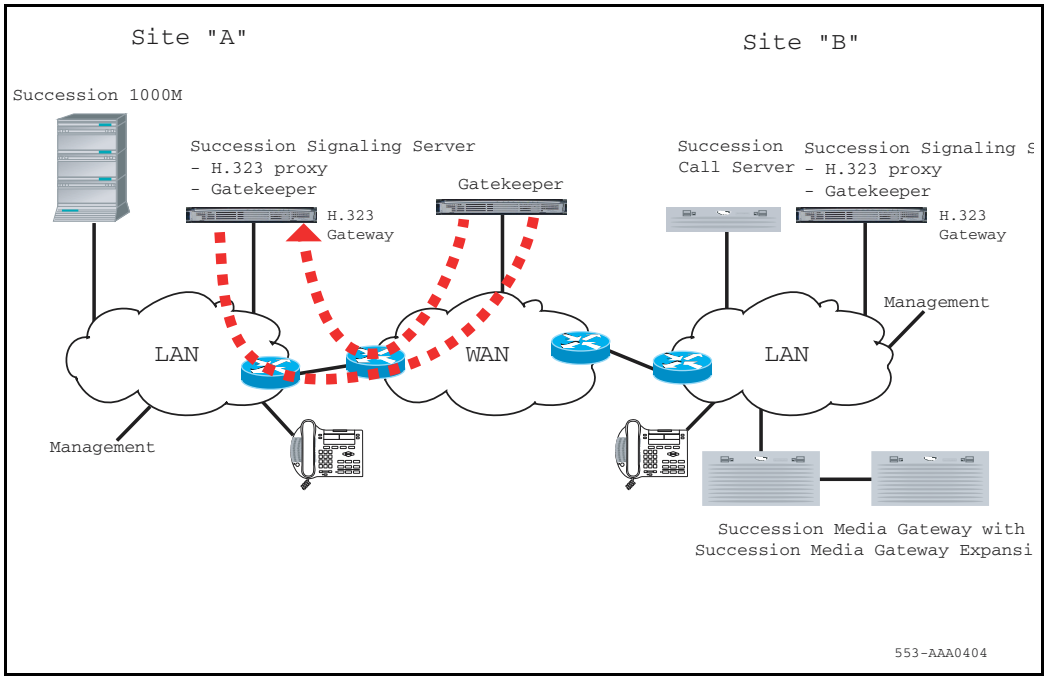
Note: To select which Virtual Trunk to use for routing, Succession Call Server A examines the number dialed and uses various trunk routing and signaling features (for example, ESN and MCDN).

Figure 4
Succession Call Server A routes the call to the IP network



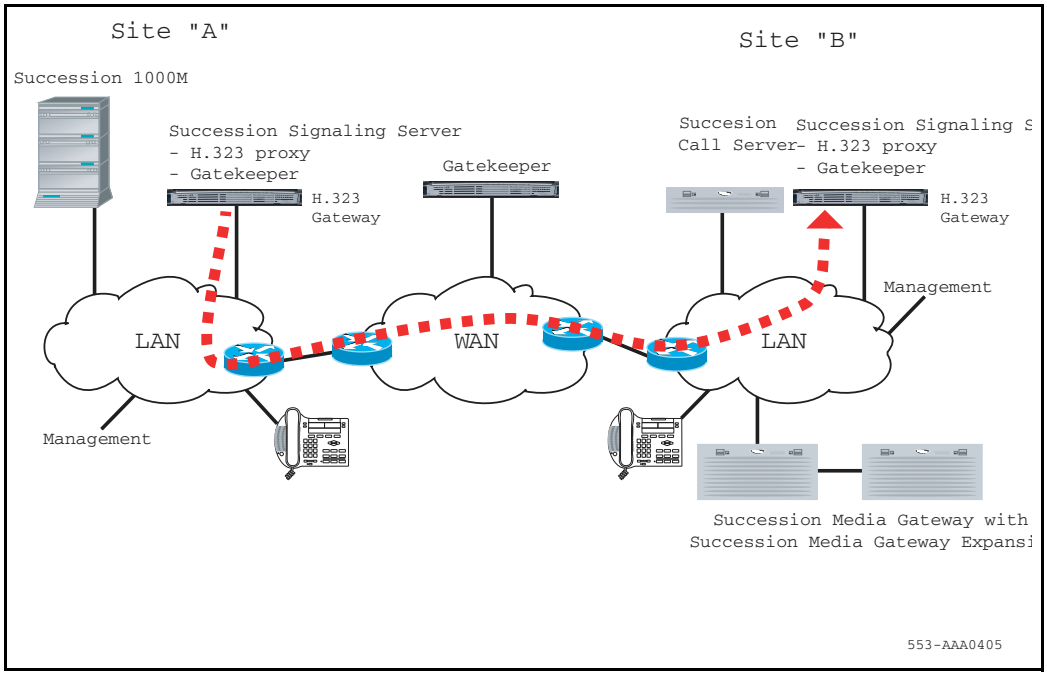
3 H.323 Gateway A asks the Gatekeeper to search for the dialed DN in the database (for example, within the appropriate CDP domain).
The Gatekeeper sends the IP address of the H.323 Gateway B to H.323 Gateway A. See Figure 5.

Figure 5
The Gatekeeper sends the IP address of H.323 Gateway B to H.323 Gateway A



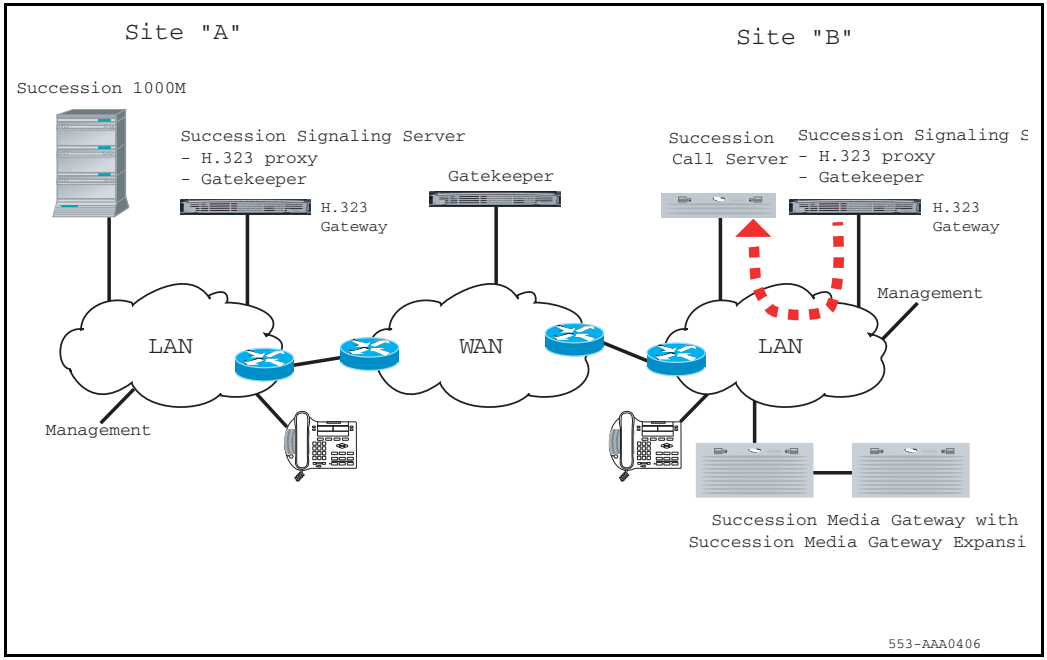
4 H.323 Gateway A sends a Setup message to H.323 Gateway B, including the DN information. See Figure 6.

Figure 6
H.323 Gateway A sends a Setup message to H.323 Gateway B



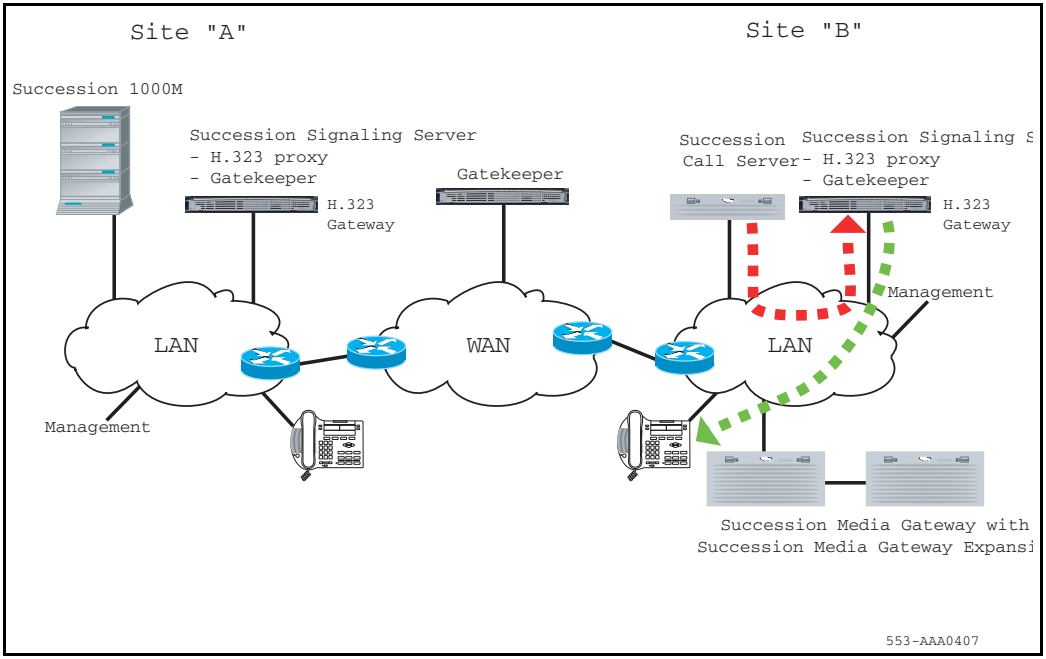
5 H.323 Gateway B treats the call as an incoming call from a Virtual Trunk. H.323 Gateway B sends the call to Succession Call Server B over a Virtual Trunk. Succession Call Server B also treats the call as an incoming call from a Virtual Trunk. See Figure 7.

Figure 7
Gateway B sends the call to Succession Call Server B over a Virtual Trunk



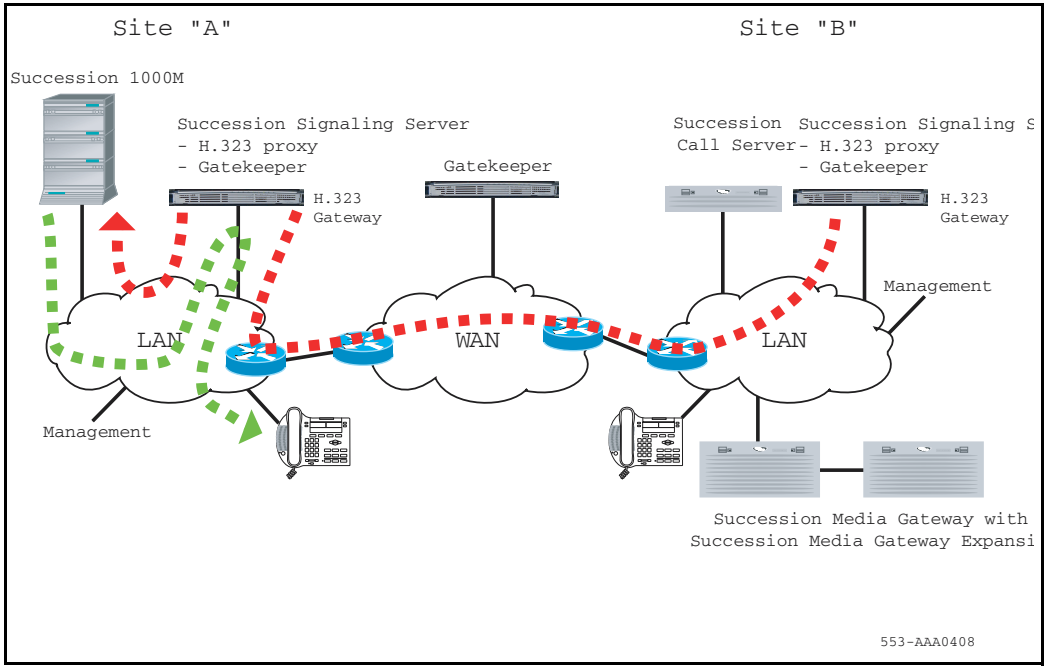
6 Succession Call Server B selects the codec, allocates bandwidth, rings the telephone, and sends an alerting message to H.323 Gateway B. See Figure 8.

Figure 8
Call Server B sends an alerting message to H.323 Gateway B



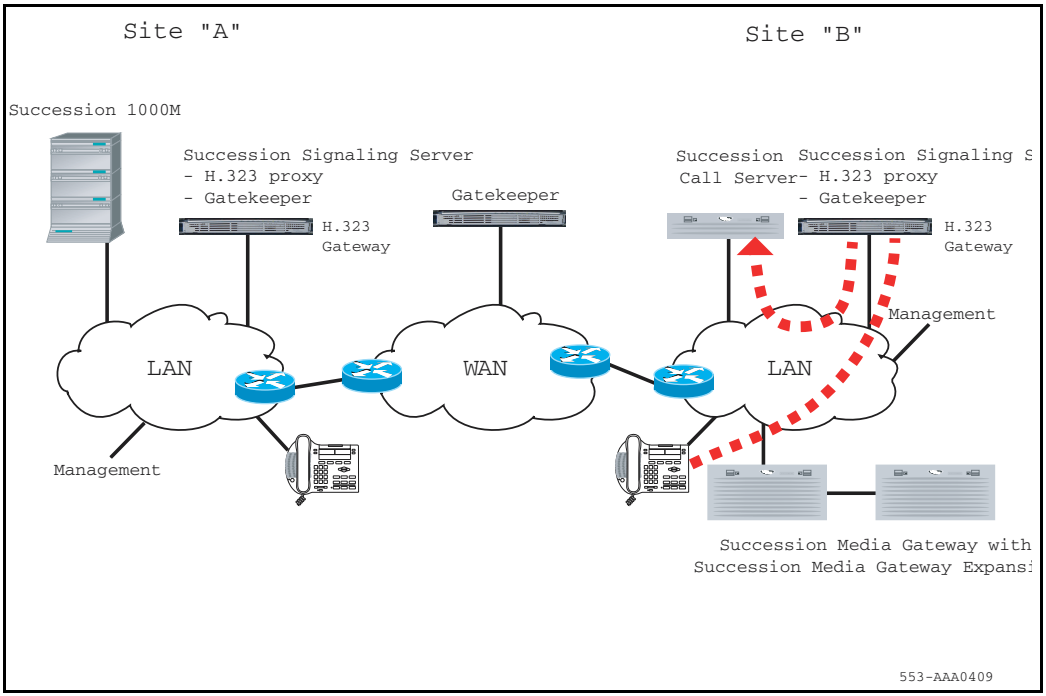
7 H.323 Gateway B sends an alerting message to Succession Call Server A. Succession Call Server A requests that the Internet Telephone play ringback tone. See Figure 9.

Figure 9
H.323 Gateway B sends an alerting message to Succession Call Server A



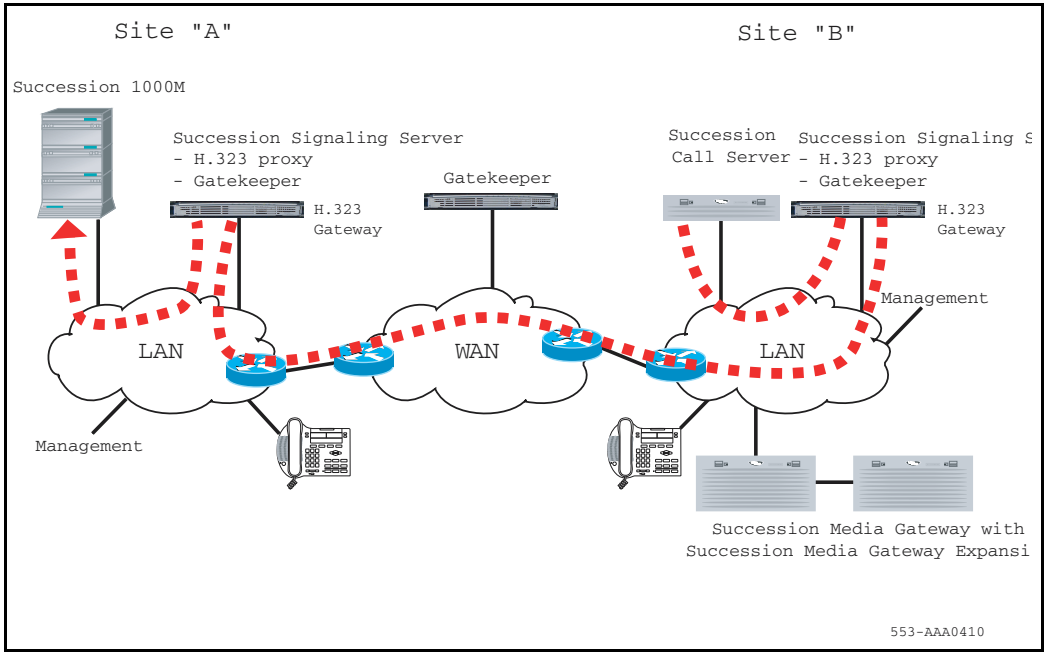
8 User B answers the call. A message is sent to Succession Call Server B through the TPS on the Succession Signaling Server. See Figure 10.

Figure 10
User B answers the call



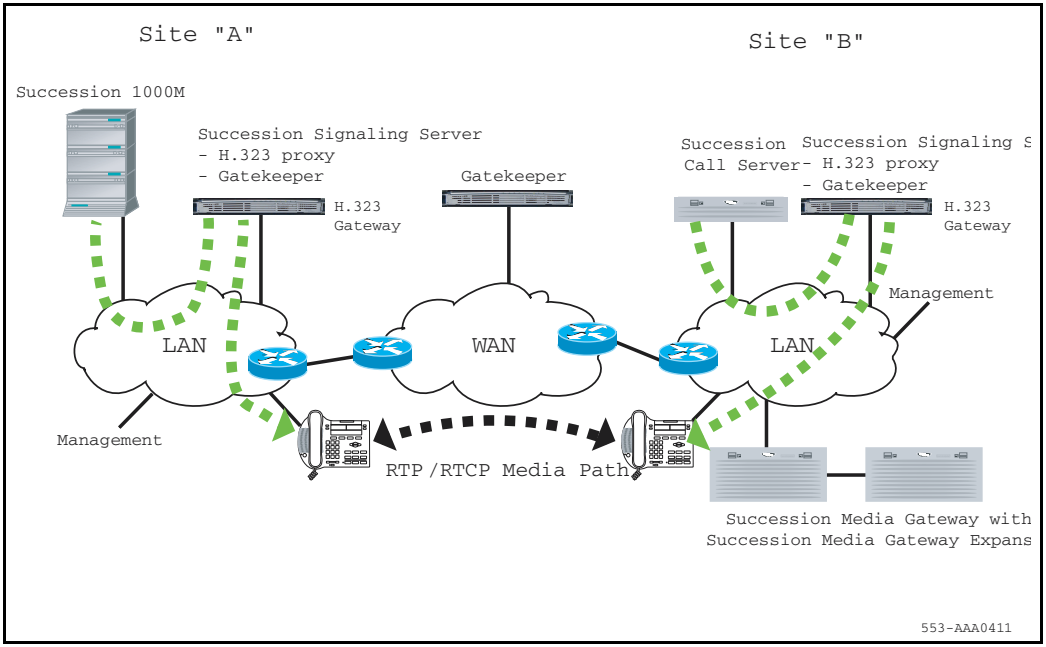
9 Succession Call Server B sends a Connect message to H.323 Gateway B. Gateway B sends an H.323 Connect message to H.323 Gateway A and Succession Call Server A. See Figure 11.

Figure 11
Succession Call Server B sends a Connect message to Gateway B



10 The Succession Call Servers tell the Internet Telephones to start the direct IP media paths. The Internet Telephones then begin to transmit and receive voice over the IP network. See Figure 12.

Figure 12
Internet Telephones start the direct



Call scenarios

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

- Internet Telephone and Internet Telephone
- Internet Telephone and circuit-switched gateway
- circuit-switched gateway and circuit-switched gateway

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

Internet Telephone to circuit-switched telephone (on separate Succession Call Servers)

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

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

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

When the terminating circuit-switched party answers the call, the terminating node returns a Q.931 CONNECT message, and the Succession Signaling Servers complete the exchange of IP media information required to establish the IP media path. The originating and terminating Succession Call Servers

and Media Gateway Controllers establish a direct two-way IP media path between the Internet Telephone and the DSP. The terminating node also establishes a circuit-switched speechpath between the DSP and the circuit-switched telephone.

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

Internet Telephone to Recorded Announcement or Music

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

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

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

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

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

Virtual Trunk to Virtual Trunk

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

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

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

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

Tandem operations

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

Direct tandem calls

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

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

Tandem feature calls

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

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

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

TRO is used when a call from Node A to Node B forwards to Node C. Node B sends a TRO facility message to Node A. The message contains the digits of the “forwarded-to” party. Node A resolves these digits to a route and determines whether it has a direct route configured to Node C. In Node A’s routing configuration, all remote locations are reached using the same Virtual Trunk (the Gatekeeper subsequently translates the digits to separate IP nodes). When TRO is attempted at Node A, the call processing treats the call as though it does not have a direct route to Node C. The tandem call routing is maintained through Node B.

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

Circuit-switched tandem calls

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

Virtual Trunk calls in conference

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

Virtual Trunk to circuit-switched party transferred to an Internet Telephone

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

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

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

Virtual Trunk to a circuit-switched party “transferred before answer” to an Internet Telephone

A call is established between a party on a remote node and a circuit-switched party on the local node over a Virtual Trunk. A direct IP media path exists between the remote party (for example, an Internet Telephone or circuit-switched gateway) and a circuit-switched gateway on the local node.

The local circuit-switched party initiates a transfer to an Internet Telephone on the local node. While the Internet Telephone is ringing, the transferring party completes the transfer by disconnecting or pressing the Transfer key. The originating party receives ringback tone.

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

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

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

Internet Telephone to local Internet Telephone transferred to a Virtual Trunk

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

When the Internet Telephone party initiates the transfer, call processing on the local node places the other party on hold. The media path between the two Internet Telephones is torn down. A call is set up between the transferring Internet Telephone and the remote party (this could be an Internet Telephone or circuit-switched telephone). See "Internet Telephone to Internet Telephone (on separate Succession Call Servers)" on page 24.

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

Fallback to PSTN

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

- the IP network is down
- the destination IP Peer endpoint is not responding
- the destination IP Peer endpoint responds that there are no available IP Peer trunk resources
- the destination IP Peer endpoint is not registered with the Gatekeeper
- there are address translation errors
- all Virtual Trunks are busy at the originating sites
- all bandwidth configured for a bandwidth zone has been allocated

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

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

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

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

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

Fallback to PSTN based upon QoS measurements is not provided in the current release of software.

Best IP network engineering practices for IP Telephony

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

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

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

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

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

- QoS Fallback to PSTN only works between symmetrically-configured pairs of IP Trunk nodes. QoS Fallback to PSTN does not work between an IP Trunk node and an IP Peer node. Each IP Trunk node in a symmetrically-configured pair must have QoS Fallback to PSTN enabled for the opposite destination node.
- A pair of symmetrically-configured IP Trunk nodes must each have a local Dialing Plan entry in the IP Trunk node that points to these opposite IP Trunk nodes. The Succession Gatekeeper cannot be used for any IP Trunk destinations that are symmetrically-configured to enable QoS Fallback to PSTN.
- An IP Trunk node configured in a Succession 1000 System or Succession 1000M Large or Small System with an IP Peer node does not support the Direct Media Path feature of IP Peer Networking. Therefore all IP Trunk calls originating or terminating at the network location that require QoS Fallback to PSTN must have a tandem media path connection through the Succession 1000 or Succession 1000M IP Peer node. The tandem media path can occasionally cause voice quality degradation due to multiple transcoding and higher end-to-end latency of the voice conversation.

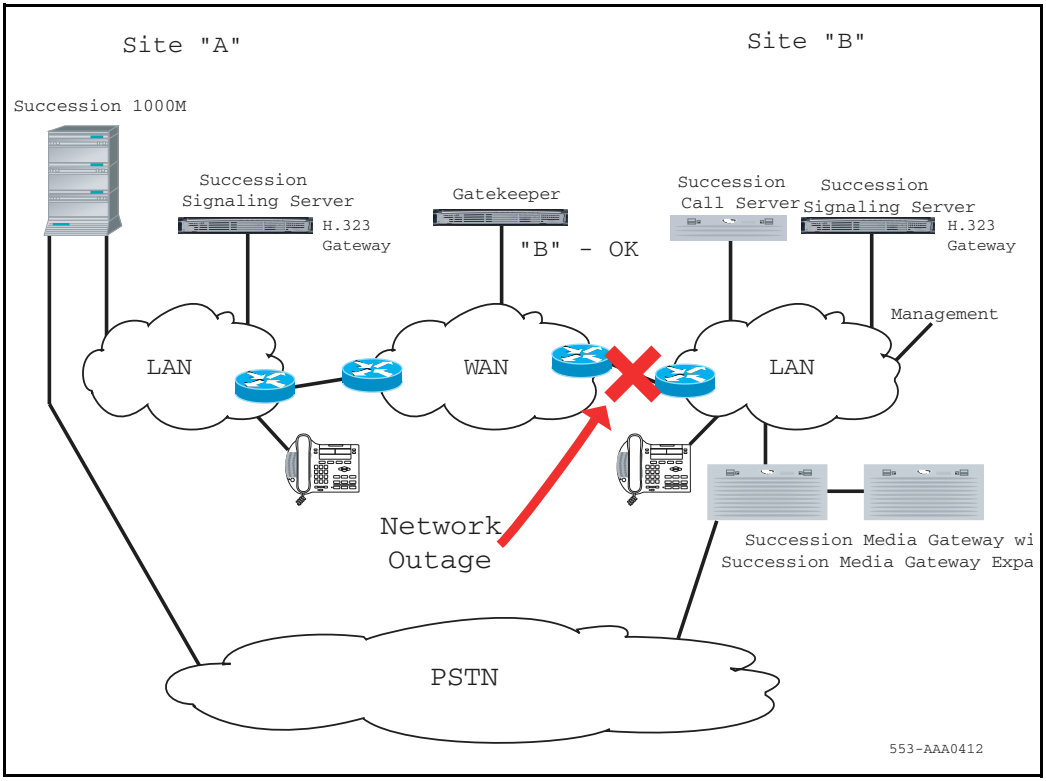
For more information, refer to *Basic Network Features* (553-3001-379).

Alternate circuit-switched routing

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

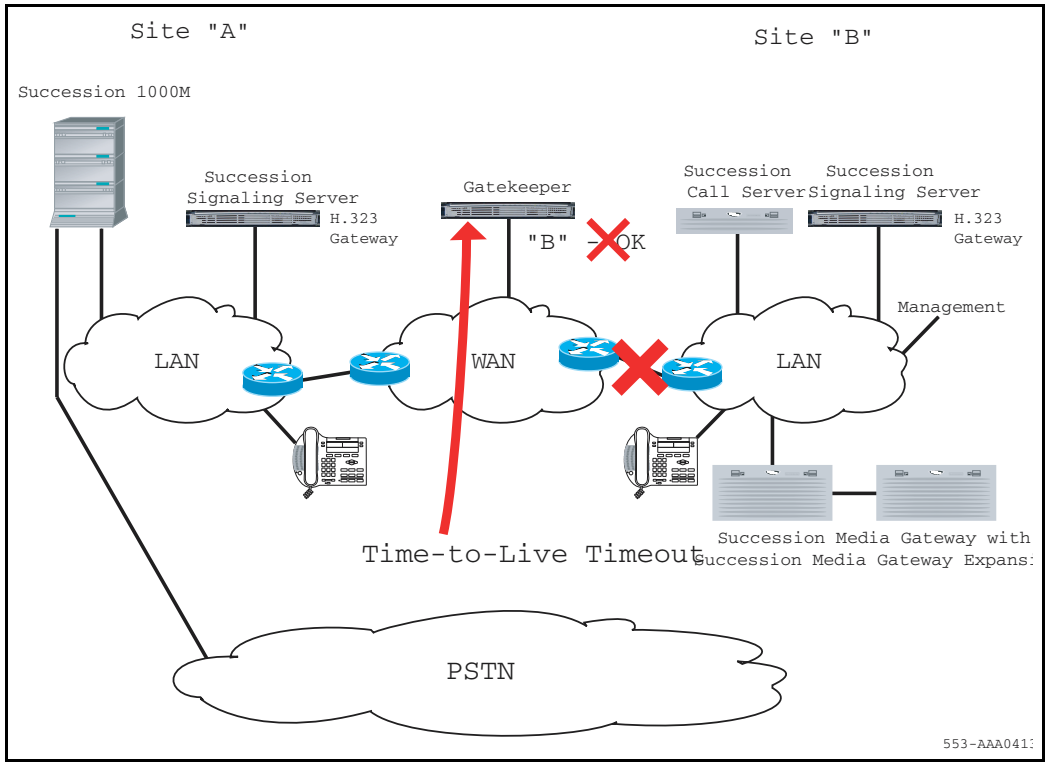
1 An IP network outage occurs at Site B. See Figure 13.

Figure 13
IP network outage at Site B



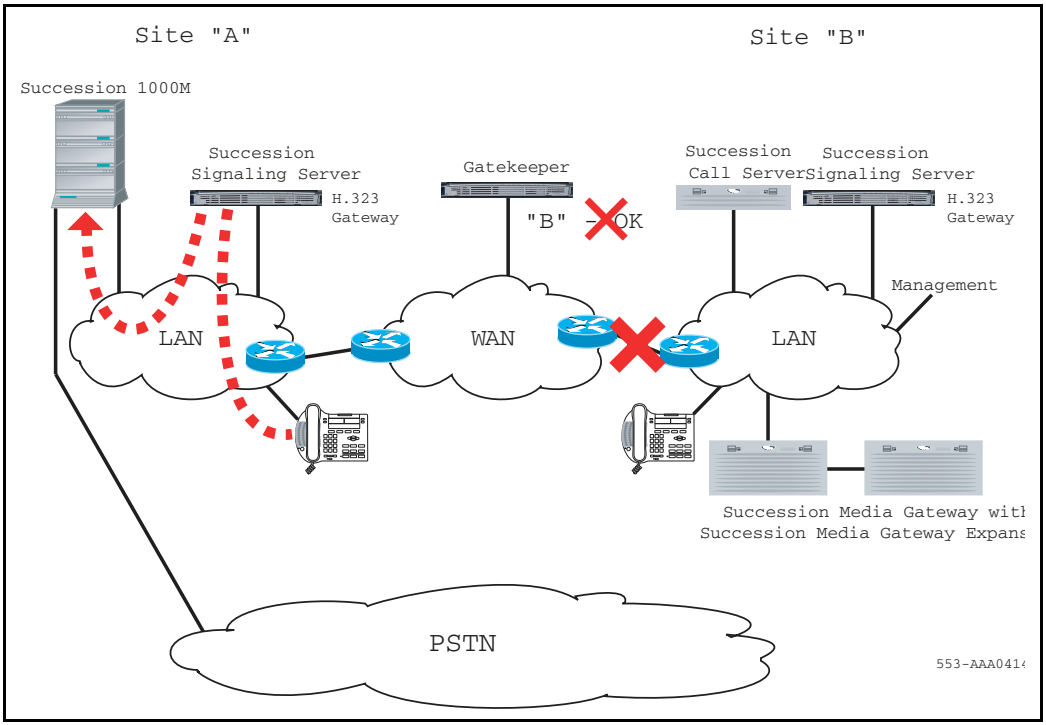
2 The registration of Site B times out at the Gatekeeper; the status updates. See Figure 14.

Figure 14
Registration at Site B times out



3 User A on Succession Call Server A dials the DN of User B on Succession Call Server B. Succession Call Server A collects the dialed digits through the TPS on the Succession Signaling Server. See Figure 15.

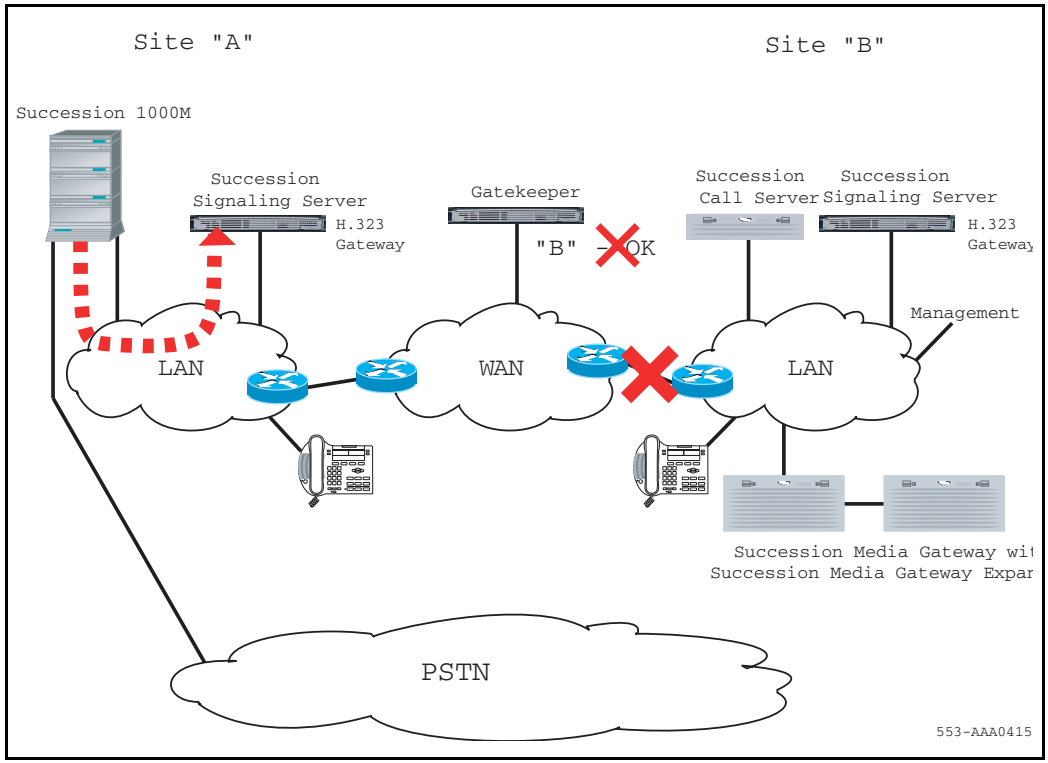
Figure 15
User A dials User B



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

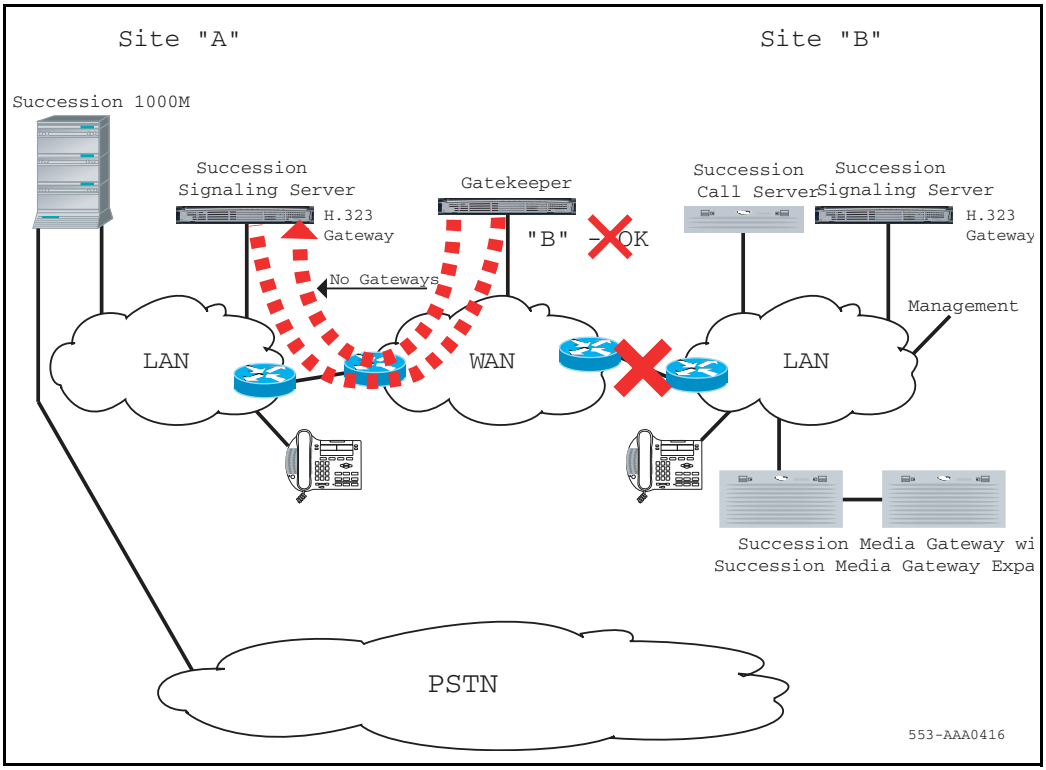
Note: To select which Virtual Trunk to use for routing, Succession Call Server A examines the number dialed and uses various trunk routing and signaling features (for example, ESN and MCDN).

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



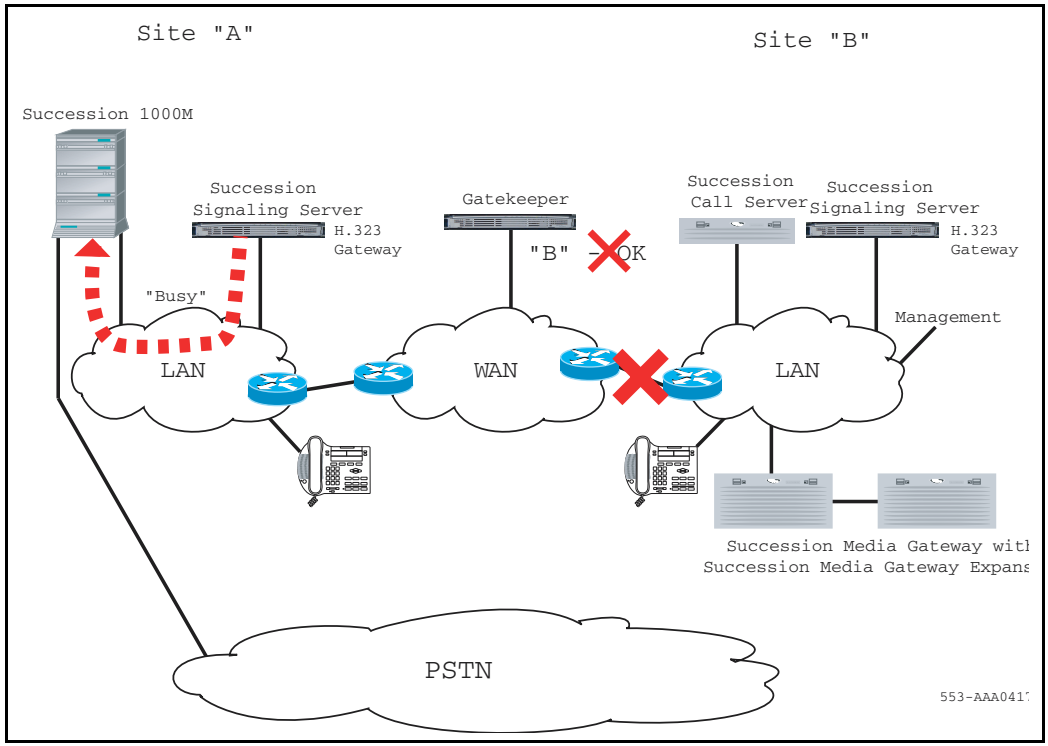
5 H.323 Gateway A asks the Gatekeeper to search for dialed DN in the database (for example, within the appropriate CDP domain).
The Gatekeeper replies that there are no H.323 Gateways available for the dialed number. See Figure 17.

Figure 17
No H.323 Gateways are available for the dialed DN



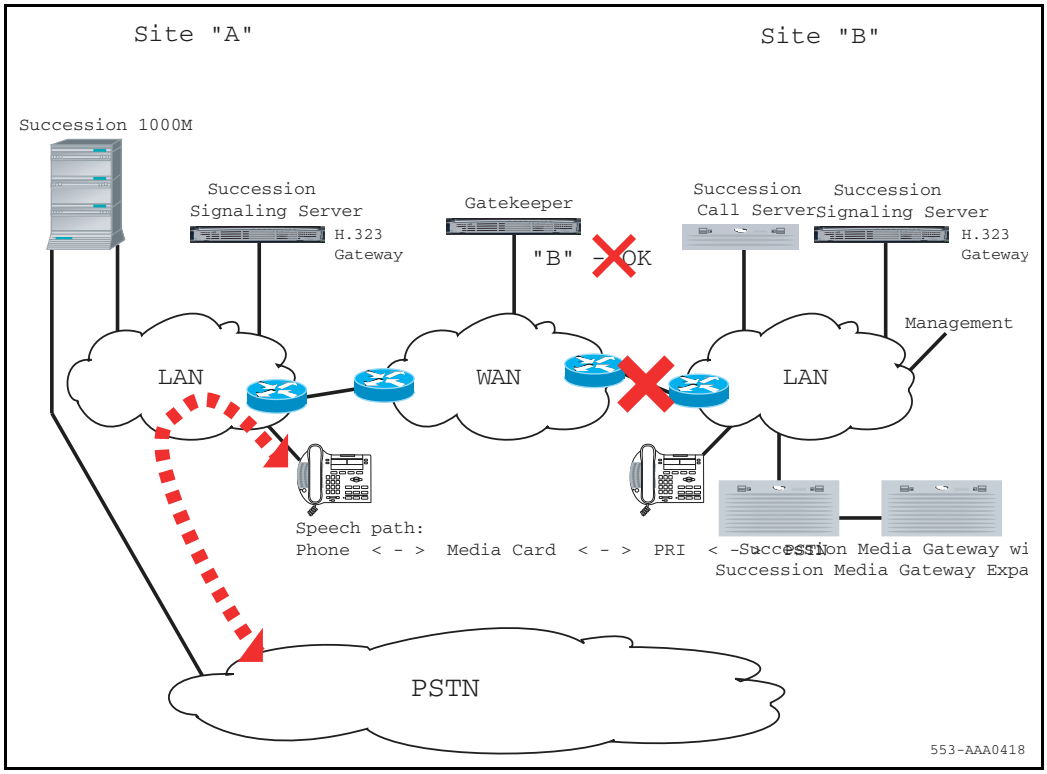
6 H.323 Gateway A replies to Succession Call Server A with a message that says that all IP trunks are busy for the dialed DN. See Figure 18.

Figure 18
H.323 Gateway A replies to Succession Call Server A



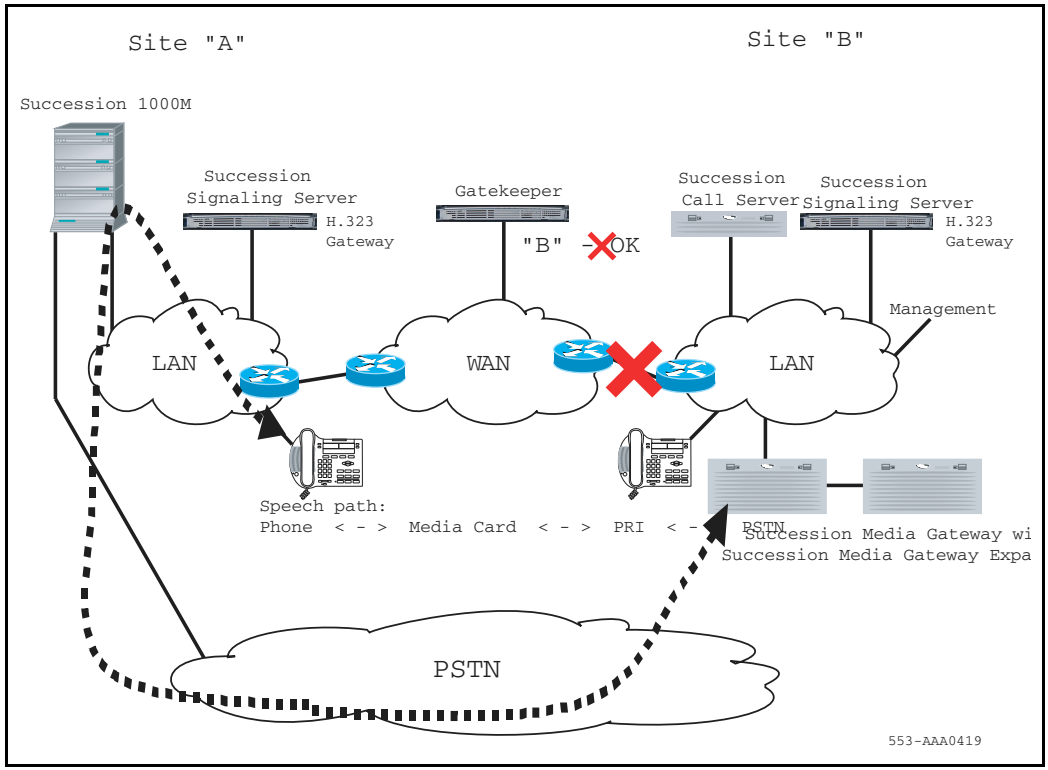
7 Succession Call Server A chooses the next route in the Route List Data Block. The next route is a local PSTN trunk route. Call Server A allocates a Voice Gateway Media Card and PRI channel. Digit manipulation is applied to the route using the local PSTN. A successful call is made. See Figure 19.

Figure 19
Succession Call Server A chooses the next route in the Route List Data Block



8 The call is routed across PSTN and enables the users to talk to each other. The call is terminated over PSTN to Site B. See Figure 20.

Figure 20
Call is terminated over PSTN



Interworking protocols

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

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

The Succession 3.0 Software only supports H.323 protocol and MCDN tunnelling.

H.323 protocol

The Succession 1000 System and Succession 1000M Large and Small Systems support H.323 version 3.

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

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

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

By definition, H.323 focuses on IP packet-based networks that do not provide any guaranteed service quality; for example, packets can be lost and there is no prioritization of the real-time (voice and video) traffic over non-real-time, and therefore delay-insensitive, data traffic.

Recent development in IP networking technology introduced Quality of Service (QoS) mechanisms that led to improved voice/video quality. However, with the majority of IP networks today still not having QoS capabilities, the mechanisms of H.323 help provide reliable communication.

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

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

Recent implementation proved that H.323 could be also used beyond LANs, in multiside configurations over Wide Area Networks based on T1, Frame Relay, and ATM technology.

H.323 is often characterized as an "umbrella specification," because it refers to various other ITU standards. Not only the topology, but also its parts as well as the protocols and standards are specified in H.323.

Table 2 lists and describes the H.323 components.

Table 2
H.323 components

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

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

- Audio (digitized and coded) voice
- Video (digitized and coded full-motion image communication)
- Data (files such as text documents or images)
- Communication control (such as exchange of supported functions and controlling logical channels)
- Controlling connections (such as connection setup and connection release)

H.323/MCDN

Succession 3.0 requires tunnelling of MCDN in H.323. This is achieved using the proprietary UIPE format.

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

Wireless LAN interworking (802.11 Wireless IP Handsets)

802.11 Wireless IP Handsets use H.323 as a protocol to access a Succession Call Server as opposed to H.323 to access an H.323 network. For the 802.11 Wireless IP Handset, the H.323 network consists of the 802.11 Wireless IP Gateway to which it terminates, not the whole H.323 network. The Succession Call Server sees the 802.11 Wireless IP Handsets as ordinary telephones.

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

Call independent signaling connection and connectionless transport

With IP Peer Networking, there is no way to signal directly from endpoint to endpoint without first determining the signaling IP address of the remote endpoint, using standard Gatekeeper procedures.

The connectionless MCDN Non-Call Associated Signaling (NCAS) is transported using the H.323 call independent call signaling connection. Since this is essentially an H.323 call with no media, standard Gatekeeper procedures apply.

MCDN connectionless transport services cannot be transported using H.323 connectionless transport since such a thing does not exist. These services are transported using the H.323 call independent procedures.

IP Peer Networking enhancements

Succession 3.0 introduces many new enhancements that affect IP Peer Networking.

Scalability

The Succession 3.0 Software increases IP scalability. Table 3 on page 56 shows the limits for each Succession Signaling Server.

Table 3
Succession Signaling Server limits

Succession Signaling Server component	Limit
Gatekeeper	2000 H.323 endpoints 10,000 numbering plan entries 60,000 calls per hour
Terminal Proxy Server (TPS)	5000 lines
Virtual Trunks	382 trunks

The Gatekeeper on each Succession Signaling Server has increased limits:

- Increased number of supported H.323 endpoints to 2000

  Note: Performance degradation occurs if the number of endpoints supported by a Gatekeeper exceeds 2000. Degradation, in this case, refers to the increased time that is required to complete actions such as the following:

  — Synchronization between the Primary Gatekeeper and the Alternate Gatekeeper, and synchronization between the Active Gatekeeper and the Failsafe Gatekeeper

— Database actions (such as Commit, Rollback, Automatic Backup, and Restore)

— Boot-up

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

- 10 000 numbering plan entries (Prior to IP Peer Networking Phase 2, each Gatekeeper could hold 512 entries per type of number for each endpoint (where a range is considered as one entry). The new limit is 10 000 numbering plan entries.)

  Note: Increased time is required for the following actions if there are more than 10 000 entries in the Gatekeeper:

  — Database actions (such as Commit, Rollback, and Restore)

  — Boot-up

  However, the ability of the Gatekeeper to resolve Admission Requests (ARQ) is not affected by an increased number of numbering plan entries.

- Each Gatekeeper can now handle 60 000 calls per hour.

The TPS on each Succession Signaling Server can support up to 5000 lines.

The number of Virtual Trunks supported by each Succession Signaling Server increases from 200 to 382. This increase reduces the number of Succession Signaling Servers that a large endpoint requires.

Talk-slot expansion allows non-blocking operation for virtual TNs. The number of supported Internet Telephones and Virtual Trunks are increased as a result of the talk-slot expansion. The increase in the number of talk-slots guarantees a talk-slot for speech path connection for every virtual TN that is used by an Internet Telephone or a Virtual Trunk.

The number of supported users in a system equals the maximum number of TNs supported in the system. The number of supported users increases to 10 000 per Call Server node, while the maximum number of users per network increases to 100 000. For more information about scalability and capacity engineering, refer to the Planning and Engineering NTPs.

Serviceability

This feature improves the serviceability of the IP Telephony equipment, resulting in the following benefits:

- Modified overlays provide operational consistency over IP Telephony Management equipment versus existing line equipment.
- Improved statistic gathering capabilities on the IP Telephony equipment through overlays.
- CLI commands for filtering and simplifying equipment tracing tools.
- Improved operational measurements threshold alarms and configuration CLIs for VGW and LTPS TRP packet loss, latency, and jitter.
- Hand-off CLI that gracefully switches resources from a targeted system to the connected resource, load-sharing system.

Reduction of provisioning effort

Vacant Number Routing (VNR) is improved to direct calls to the Gatekeeper that controls routing. This reduces the provisioning effort required for Branch Offices. For more information, see “Vacant Number Routing” on page 121 and “VNR enhancement” on page 232.

Features

Contents

This section contains information on the following topics:

Codec negotiation

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

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

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

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

IP Peer Networking performs codec negotiation by providing a list of codecs that the devices can support. Use Element Manager to configure the list of codec capabilities. See Procedure 11 “Configuring codecs” on page 193.

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

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

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

The G.723.1 codec provides the greatest compression.

Note 1: Payload default values need to be changed if the customer wants to communicate with a third party gateway that does not support the above default payload sizes. Otherwise, IP Peer calls to or from the third party gateway are not successful.

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

G.711 A-law and u-law interworking

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

Zone bandwidth management

Zone bandwidth management is a mechanism that defines which codecs are used intrazone and interzone.

Zone bandwidth management enables administrators to define codec preferences for Internet Telephone to Internet Telephone calls controlled by the same Succession 1000 or Succession 1000M Large or Small System. This is different than the codec preferences for calls between an Internet Telephone on the Succession 1000 and Succession 1000M Large or Small System to a Virtual Trunk (potentially an Internet Telephone on another Succession 1000, Succession 1000M Large or Small System).

For example, you may prefer high quality (G.711) over low bandwidth (G.729 A/AB or G.723.1) within one system, and low bandwidth over high quality to a Virtual Trunk. Such a mechanism can be useful when a system is on the same LAN as the Internet Telephones it controls, but the other systems are on a different LAN (connected through a WAN).

Zone bandwidth management is based on static configuration. It does account for data network topology, and, therefore, does not always fulfill its QoS

goals. Because of this, the Virtual Trunks' usage of bandwidth zones is different than Internet Telephone bandwidth usage. For Virtual Trunks, a zone number is configured in the Route Data Block (LD 16). The zone number determines codec selection for interzone and intrazone calls (that is, Best Bandwidth or Best Quality). See "Configuring IP Peer Networking" on page 143 for information on configuring the RDB zone.

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

Connections between two Virtual Trunks (that is, tandem IP calls) do not accumulate bandwidth usage or blocking due to bandwidth requirements.

Codec selection

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

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

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

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

Once the above conditions are met, a codec selection algorithm selects the codec to be used. Two different codec selection algorithms are discussed in "H.323 Master/Slave algorithm" on page 63 and "'Best Bandwidth' codec selection algorithm" on page 64.

H.323 Master/Slave algorithm

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

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

Algorithm details

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

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

Issues caused by the H.323 Master/Slave algorithm

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

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

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

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

'Best Bandwidth' codec selection algorithm

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

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

Algorithm details

The selected codec is the type considered as the best bandwidth codec type. To know whether one codec type has better bandwidth than another, see the rule as summarized in Table 4.

Table 4
"Best Bandwidth" codec type

	G.711 aLaw	**G.711 uLaw**	**G.729 A**	**G. 729 AB**	**G. 723.1**
G.711 aLaw	G.711 aLaw	G.711 uLaw	G.729 A	G. 729 AB	G. 723.1
G.711 uLaw	G.711 uLaw	G.711 uLaw	G.729 A	G. 729 AB	G. 723.1
G.729 A	G.729 A	G.729 A	G.729 A	G. 729 AB	G.729 A
G. 729 AB	G. 729 AB	G. 729 AB	G. 729 AB	G. 729 AB	G. 729 AB
G. 723.1	G. 723.1	G. 723.1	G.729 A	G. 729 AB	G. 723.1

Tone handling

Progress tones

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

Dial tone is always the responsibility of the originating side. The call is not setup with the far end as long as the digits are gathered for en-bloc transmission. Other tones are provided by the originating side when the call cannot proceed to the far end.

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

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

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

For call center limitations on tone handling, see the "Limitations" on page 88.

End-to-end DTMF signaling

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

DTMF signaling can be received from the following:

- analog (500/2500-type) telephones
- digital telephones
- Internet Telephones
- H.323 trunks
- analog trunks
- PRI trunks

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

Note: IP Peer Networking does not support long DTMF tones over Virtual Trunks.

Tone handling methods

DTMF tones must be transmitted using out-of-band signaling, because sources of delay and distortion caused by IP media streams can cause invalid tone detection when transmitted in-band. The out-of-band method uses H.245 channel signaling messages to represent the DTMF tones.

Out-of-band signaling

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

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

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

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

In-band signaling

The Succession 1000 and Succession 1000M systems do not support in-band signaling.

For more information on in-band signaling, refer to RFC2833 at the following website: http://www.ietf.org/rfc/rfc2833.txt

Internet Telephone End-to-End Signaling (EES)

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

Internet Telephones EES to H.323 trunks

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

Circuit-switched device DTMF and EES

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

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

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

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

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

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

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

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

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

Tandem H.323 trunks to H.323 trunks

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

Fax calls

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

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

The Succession 1000 System and the Succession 1000M Large and Small Systems comply with H.323 version 3 with the version 4 extensions necessary for voice-to-fax switchover. This version standardizes the procedures in switching from voice mode to fax mode. Some third-party H.323 gateways can use different implementations of protocols to switch from voice to fax. Using a third-party gateway requires fax interoperability testing of the system. The end result can be that fax is not supported, due to

the complexity of the H.323 protocol and other factors. Check with your Nortel Networks sales representative for approved third-party gateways.

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

Reliability and redundancy

The systems can provide levels of redundancy to ensure that telephony services can withstand single hardware, software, and network failures. Table 5 on page 71 shows each reliability and redundancy feature and the systems that support the feature. The reliability and redundancy features include:

- Alternate Succession Call Server (see page 72)
- Succession Signaling Server software redundancy, including H.323 Gateway and Internet Telephone software (see page 75)
- H.323 Gatekeeper redundancy (see page 76)
- H.323 Gateway interface to Gatekeeper redundancy (Failsafe Gatekeeper) (see page 77)
- Campus distributed Succession Media Gateway in survival mode (see page 80)
- Succession 1000M Large System CPU redundancy (see page 82)
- Survivable IP Expansion (SIPE) (see page 85)

Table 5 shows the feature and the systems that support the feature.

Table 5
Reliability and redundancy features by system type

Reliability and Redundancy Features		Succession 1000M Small Systems		Succession 1000M Large Systems	
	Succession 1000	Succession 1000M Cabinet	Succession 1000M Chassis	Succession 1000M Single Group	Succession 1000M Multi Group
Alternate Succession Call Server	X	X	X		
Succession Signaling Server software redundancy	X	X	X	X	X
H.323 Gatekeeper redundancy	X	X	X	X	X
H.323 Gateway interface to Gatekeeper redundancy (Failsafe Gatekeeper)	X	X	X	X	X
Campus distributed Succession Media Gateway in survival mode	X	X	X		
CPU redundancy				X	X
Survivable IP Expansion (SIPE)		X	X		

Alternate Succession Call Server

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

During normal operation, the processor in the Succession Media Gateway handles low-level control of the interface cards in the gateway slots and communicates with the Succession Call Server for feature operation. If the Succession Media Gateway processor loses communication with the Succession Call Server due to Call Server or IP network component failure (for example, cabling and L2 switch), the Succession Media Gateways assume Succession Call Server responsibilities for all accessible Gateway hardware and all telephones and Virtual Trunks. The Succession Signaling Server registers with the Alternate Succession Call Server.

The Alternate Succession Call Server is only applicable to the Succession 1000 System and the Succession 1000M Small Systems.

As an example, Figure 21 on page 73 shows the normal mode of operation for a Succession 1000 System.

Figure 21
Normal mode of operation for a Succession 1000 System

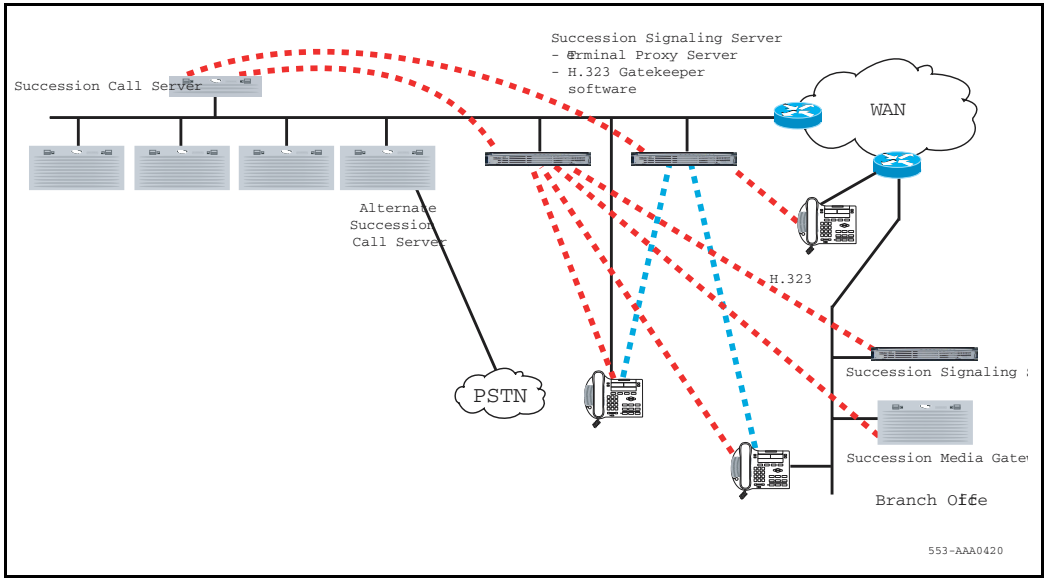
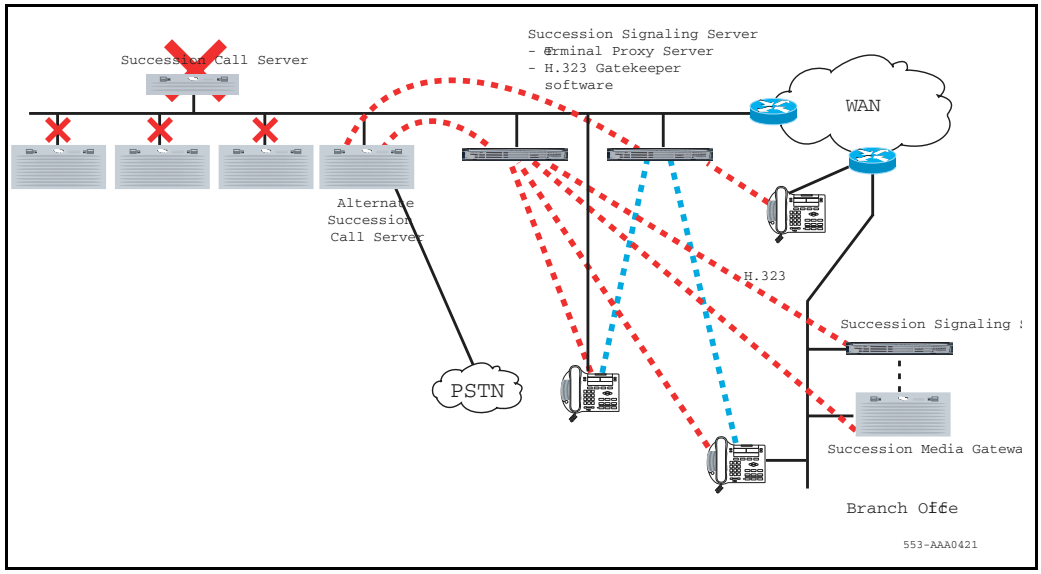


Figure 22 illustrates what occurs when the Succession Call Server fails in a Succession 1000 System:

1. The Succession Call Server database periodically synchronizes at the Alternate Succession Call Server.
2. The Primary Succession Call Server fails.
3. The Alternate Succession Call Server assumes the role of the Primary Succession Call Server for Internet Telephones.
4. The Succession Signaling Server registers at the Alternate Succession Call Server.
5. Operation resumes with the single Succession Media Gateway.

Figure 22
Succession Call Server failure and redundancy in a Succession 1000 System



Succession Signaling Server redundancy

Succession Signaling Server redundancy is provided on a load-sharing basis for the TPS. The Alternate Succession Signaling Server is the IP route for the H.323 Gateway software. The Gatekeeper (Primary, Alternate, or Failsafe) cannot reside on an Alternate Succession Signaling Server. It has to be on a Primary (Leader) Succession Signaling Server. As an example, Figure 23 on page 76 shows Succession Signaling Server redundancy of a Succession 1000 System. In Figure 23, the following occurs:

1 The Internet Telephones are distributed between the two Succession Signaling Servers. The H.323 Gateway software runs on the Primary Succession Signaling Server.

2 The Primary Succession Signaling Server fails.

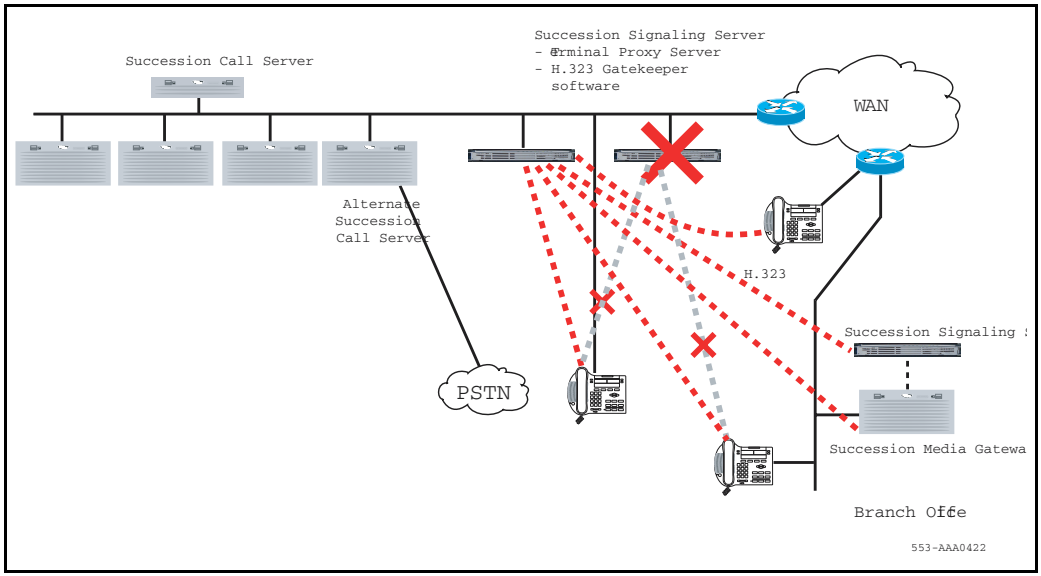
3 The Alternate Succession Signaling Server assumes the Connection Server IP address, if necessary.

4 The Internet Telephones Time-to-Live time-out triggers the reset of the Internet Telephones and registration to the Alternate Succession Signaling Server.

5 The Alternate Succession Signaling Server assumes responsibility for the H.323 Gateway software.

6 Operation resumes.

Figure 23
Succession Signaling Server redundancy in a Succession 1000 System



H.323 Gatekeeper redundancy

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

Succession 1000 and Succession 1000M networks have at least one H.323 Gatekeeper to provide network numbering plan management for private and public numbers. An optionally redundant Gatekeeper can be installed in the network. The Alternate Gatekeeper periodically synchronizes its database with the Primary Gatekeeper.

A Gatekeeper can provide alternate endpoint information in the Admission Confirm (ACF) message. If call setup fails, the endpoint that originated the Admission Request (ARQ) message sequentially attempts call setup with the

alternate endpoints until it succeeds. After all the endpoints are tried and if none was successful, the call is rejected.

Note: If the call is rejected, standard alternate route selections can apply.

H.323 gateway software — trunk route redundancy

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

Existing calls are kept when the Primary Succession Signaling Server fails. This applies to Internet Telephones that are not registered with the Primary Succession Signaling Server, and for all circuit-switched telephones. Internet Telephones that are registered with the Primary Succession Signaling Server reboots after the Time-to-Live time-out, hence active calls on those sets are lost.

H.323 gateway software — Gatekeeper redundancy

The H.323 gateway software attempts to recover system functionality if there is a failure at the Gatekeeper. There are two types of Gatekeeper redundancy: Alternate Gatekeeper and Failsafe Gatekeeper.

Alternate Gatekeeper

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

To enable Alternate Gatekeepers to provide Gatekeeper redundancy, the Succession 1000 and Succession 1000M Systems can accept a prioritized list of Alternate Gatekeepers in the Gatekeeper Confirmation (GCF) and Registration Confirmation (RCF) messages returning from the Primary Gatekeeper at the Gatekeeper Discovery and Gatekeeper Registration times respectively.

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

Polling and switchover

A Time-to-Live timer is provided to ensure that if a Gatekeeper stops responding for a specified amount of time, the H.323 Gateway software registers at the Alternate Gatekeeper to resume operation. This ensures Gatekeeper redundancy across the network. For more information about endpoint registration and Time-to-Live, refer to "Time-to-Live" on page 99.

The Alternate Gatekeeper is inactive and in standby mode by default. It constantly polls the Primary Gatekeeper by sending Information Response Request (IRR) messages to the Primary Gatekeeper. The default for the poll interval is set to approximately 30 seconds and can be configured through the Gatekeeper Element Manager (see Procedure 21 "Setting the Database and Registration Synchronization Poll Interval" on page 251). The endpointType.gatekeeper field of the IRR message is set to indicate that the IRR is coming from a Gatekeeper and not an endpoint. If the Primary Gatekeeper is currently in service and accepting registrations, then it returns an Information Request Negative Acknowledgement (INAK) message with nakReason set to notRegistered.

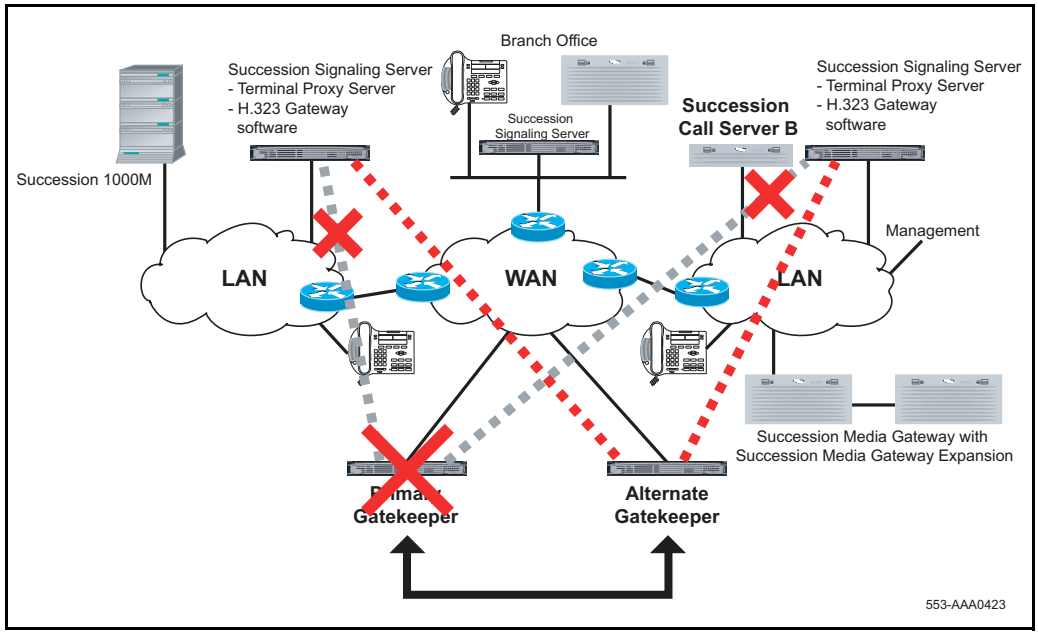
Figure 24 on page 79 shows the handling of the Gateway interface and the Alternate Gatekeeper in the event of Primary Gatekeeper failure:

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

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

5 The network calls resume.

Figure 24
Primary Gatekeeper failure and redundancy



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

Failsafe Gatekeeper

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

When configuring the Gatekeeper, the administrator must configure whether the Gatekeeper is the Primary Gatekeeper (GKP) or the Alternate Gatekeeper (GKA). If the Gatekeeper is the Primary Gatekeeper, the administrator can

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

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

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

Campus-distributed Media Gateway in survival mode

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

The Media Gateway survival modes applies to the following systems:

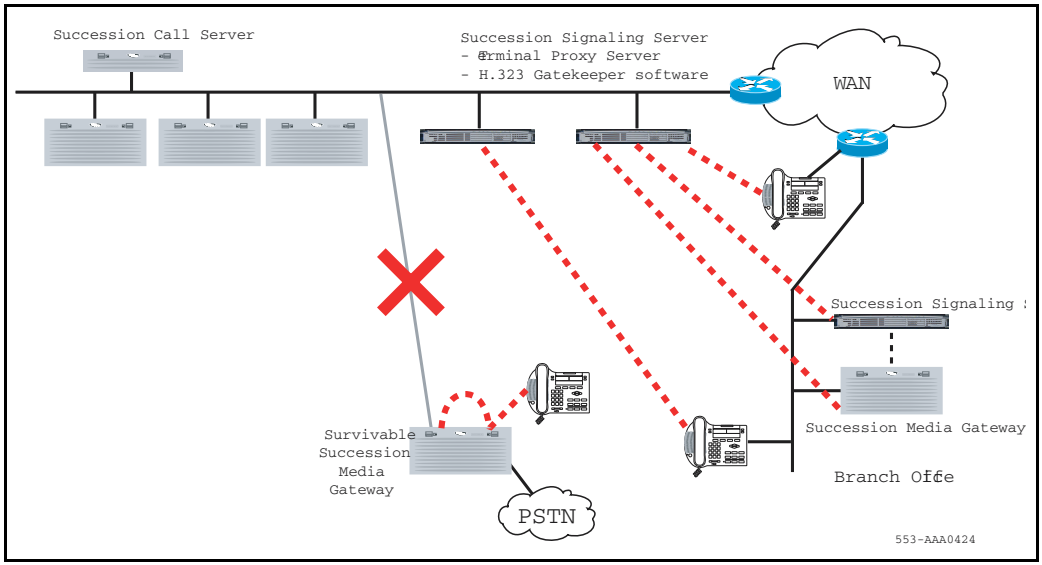
- Succession 1000 System
- Succession 1000M Small System

Media Gateways can be configured as survivable when distributed throughout a campus environment. In this case, basic telephony services are provided in the event of a network outage. Figure 25 on page 81 illustrates how such an outage is handled.

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

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

Figure 25
Network failure with Survivable Media Gateways



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

Succession 1000M Large System CPU redundancy

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

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

Health Monitoring

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

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

Table 6 on page 82 shows the health count scheme.

Table 6
Health count

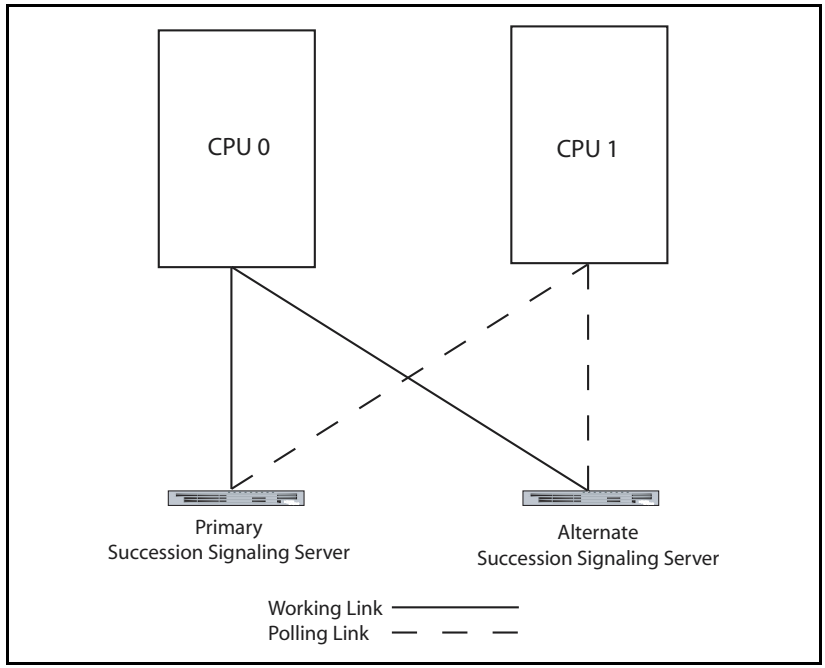
Number of cards	Health count
2 or 3 cards	1 health count
4 or 5 cards	2 health counts
6 or 7 cards	3 health counts
8 or 9 cards	4 health counts
...	...

Under normal operation, the following occurs:

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

Figure 26 on page 83 illustrates health monitoring under normal operation.

Figure 26
Health Monitoring



When all the links are up and running there is no CPU switch-over. However, if the Ethernet port in the active CPU (CPU 0) stops working both Succession Signaling Servers cannot communicate with the active CPU and the health count on the active CPU is decreased. The health count of the standby CPU

remains the same because both Succession Signaling Servers can communicate with it.

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

Virtual Trunk redundancy

If the Ethernet port on the Primary Succession Signaling Server fails or the server itself fails, there is no CPU switch-over since both the active and the standby CPU lose contact with the Primary Succession Signaling Server. As a result, they have the same health count.

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

Graceful switch-over

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

Ungraceful switch-over

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

Survivable IP Expansion (SIPE)

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

- Succession 1000M Cabinet
- Succession 1000M Chassis

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

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

Least Cost Routing

IP Peer Networking supports the traditional methods of managing costs in a circuit-switched environment (for example, through BARS/NARS). IP Peer Networking also supports a method to manage costs at the Gatekeeper. This is done in an IP environment using Least Cost Routing. With Least Cost Routing, you can assign a cost factor to the routes using Gatekeeper Element Manager. You can also use Least Cost Routing to identify the preferred H.323 Gateways for specific numbering plan entries. See “Managing the Gatekeeper” on page 239.

Quality of Service

For optimum performance, Internet Telephones must be deployed on an IP Telephony-grade network. To create an IP Telephony-grade network, a minimum Quality of Service (QoS) level must be met. QoS is the gauge of quality between two nodes in an IP network. As QoS degrades, existing calls suffer poor voice and data quality.

Several QoS parameters can be measured and monitored to determine if desired service levels are provisioned. See *Data Networking for Voice over IP* (553-3001-160) for detailed information on the QoS parameters.

Lost data packets can contribute to poor QoS. Lost data packets can occur before reaching a Layer 3 switch or router, due to congestion at the Layer 2 switch. Data packets can also be lost at a Layer 3 switch or higher when routing decisions are made.

Prior to reaching a Layer 3 routing device, a voice packet can pass through one or more Layer 2 switches. The “uplinks” between these switches can encounter congestion. The 802.1Q/802.1p protocols provide a mechanism to treat voice media and voice signaling with a higher priority, dropping other traffic (for example, http) instead of voice.

Layer 2 packet marking (802.1Q/802.1p protocols)

Layer 2 packet marking prioritizes traffic at the Link level, using the 802.1Q/802.1p standard. This is important when going through Layer 2 switches because these switches are typically the first thing an endpoint encounters when accessing the network. In addition, under 802.1Q protocol, VLANs can be used to manage priority.

The 802.1Q/802.1p protocols apply to Internet Telephones, which support Automatic Negotiation. Automatic Negotiation or encoding of 802.1Q/ 802.1p protocol settings is not provided on Voice Gateway Media Cards or on the 100BaseT interface of the Succession Media Gateways. Support of 802.1Q/802.1p protocols and higher must be provided by fixed configuration of a Layer 2/3 switch that supports these features. The priority and VLAN settings are set on a physical port basis.

Layer 3 packet marking (Differentiated Services)

Layer 3 packet marking prioritizes traffic at the IP level using Differentiated Services (DiffServ). The Succession 1000 and Succession 1000M systems support configurable DiffServ markings for voice packets from Internet Telephones and Voice Gateway Media Cards. The configuration of DiffServ is done through the Element Manager interface. See Procedure 12 on page 200.

Layer 4 port numbers

Many routers support the management of QoS using Layer 4 port numbers. You can select Layer 4 port numbers for Internet Telephones and Voice Gateway Media Cards through Element Manager. This enables customers to manage QoS in their network by selecting User Data Protocol (UDP) and TCP ports as high priority.

Loss and Level Plan

Loss and Level Plan configuration is discussed in the following NTPs:

- *Transmission Parameters* (553-3001-182)
- *Succession 1000 System: Planning and Engineering* (553-3031-120)

Incremental Software Management

For each Virtual Trunk configuration, you must purchase ITG ISDN trunks through Incremental Software Management. The number of trunks must match those that are enabled with the installation keycode.

The following package and ISM parameter are needed for IP Peer Networking:

- H323 Virtual Trunk (H323_VTRK) package 399
- IP PEER H.323 TRUNK parameter

For more information, refer to the following NTPs.

- *Small System: Installation and Configuration* (553-3011-210)
- *Large System: Installation and Configuration* (553-3021-210)
- *Succession 1000 System: Installation and Configuration* (553-3031-210)

Limitations

The Gatekeeper (Primary, Alternate, or Failsafe) cannot reside on an Alternate Succession Signalling Server. It has to be on a Primary (Leader) Succession Signalling Server.

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

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

The use of G.723 codec can limit the number of DSP channels available on the 32-port Succession Media Card to 24. For ITG-P Line cards, all 24 ports can be used. The use of codec G729A/AB and G723 impacts the voice quality, including music provided to the user.

H.323 does not support NAT. If address translation is required, it needs H.323-aware NAT or VPN facilities. Internet Telephones (which use the proprietary UniSTIM protocol) have a limited implementation of NAT.

While the Succession 1000 and Succession 1000M systems supports MCDN, it does not support H.450 supplementary services, which is the industry-standard version of MCDN.

Gatekeeper functionality

Contents

This section contains information on the following topics:

Gatekeeper overview

All systems in the IP Peer network must register with the Gatekeeper.

The primary function of the H.323 Gatekeeper is to provide the following services:

- endpoint and Gateway registration
- call admission control
- address translation and telephone number to IP lookup
- centralized numbering plan administration

Note: The Gatekeeper (Primary and Alternate) can operate in stand-alone mode, without being connected to the Succession Call Server.

The Gatekeeper is H.323 compliant and can provide Gatekeeper features to other H.323-compliant Nortel Networks endpoints (for example, Succession 1000 and IP Trunk 3.0 (or later) endpoints). A static IP address must be configured for these endpoints, as well as the telephone numbers that the endpoints can terminate.

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

Refer to "Configuring endpoints" on page 259.

Gatekeeper components

The Gatekeeper consists of the following major components:

- Gatekeeper Network Protocol Module (GKNPM)
- Database Module (DBM)
  - primary and standby databases
- web server
- vxWorks shell

Gatekeeper Network Protocol Module

The Gatekeeper Network Protocol Module (GKNPM) interfaces with the H.323 stack and is responsible for sending and receiving all H.323 RAS messaging.

When a RAS request message arrives over the network, the H.323 stack informs the GKNPM of the incoming request. The GKNPM uses H.323 Application Programming Interfaces (APIs) to retrieve the relevant data. For example, if the incoming request is an ARQ, the GKNPM extracts the originator's endpointIdentifier and the desired terminator's destinationInfo fields from the ARQ message.

After all relevant information has been extracted from the incoming RAS request, the GKNPM passes the request to the DBM for resolution. The DBM consults its numbering plan configuration and informs the GKNPM of the result. The GKNPM then sends the relevant RAS response to the RAS request originator.

Database Module

The Database Module (DBM) is responsible for the following:

- configuring the numbering plan
- reading and updating the primary and standby databases on disk
- resolving all registration and admission requests which the GKNPM passes to the DBM

The Gatekeeper numbering plan configuration is stored in XML format in two databases on disk. The primary database is used for call processing and the standby database is used for configuration changes.

The DBM interfaces with the primary and standby databases on disk. All call processing requests that the GKNPM passes to the DBM are resolved using the primary database. The DBM uses the information that the GKNPM extracted from the RAS request (for example, ARQdestinationInfo) to search its database. In the case of an ARQ message, the DBM attempts to find a registered endpoint that can terminate this call.

The web server interfaces with the DBM for viewing, adding, deleting, or modifying numbering plan configuration data. All changes to the numbering plan database are carried out on the standby database. Changes that the administrator makes to the numbering plan database do not affect call processing immediately. The database must first be cut over to the Main database.

Web server

Configuration of the Gatekeeper can be performed using a recommended web browser and accessing the Gatekeeper web server on the Succession Signaling Server. The administrator can view, modify, or delete all numbering plan configuration data. An administrator can also make changes in operation or restore the previous database if the changes are unsuitable. The Gatekeeper webpages in Element Manager also provide various diagnostic and traffic measurement tools.

vxWorks Shell

The Wind River vxWorks shell provides access to the operating system for maintenance and debug operations.

Network overview

With IP Peer Networking, there is one active Gatekeeper for each network zone. The Gatekeeper can run on any of the Succession Signaling Server platforms on any of the Succession 1000 or Succession 1000M nodes in the network. The Gatekeeper is configured with numbering plan information for every node in the network zone.

Coordinated endpoint configuration across multiple Gatekeeper zones

IP Peer Networking supports multiple H.323 zones. Separate Gatekeeper databases must be managed for each zone in a 1:1 relationship. Each Gatekeeper zone contains a Primary GK, optionally an Alternate GK, and

multiple Gateway endpoints. The reasons for implementing multiple Gatekeeper zones are:

1 to scale up to very large networks with hundreds of registered endpoints

2 to divide a network of any size into convenient administration zones, for example, Western Europe, North America

When a Succession 1000 or Succession 1000M system places an IP call to another node, the originating H.323 Gateway Signaling Proxy server sends an ARQ message to the Gatekeeper, specifying the destination telephone number. The Gatekeeper consults its internal numbering plan database and determines which node is the correct destination node. The Gatekeeper then sends an ACF message to the call originator and includes addressing information for the destination node.

If no numbering plan entries are found, the Gatekeeper queries all of the Gatekeepers on its list, using H.323 LRQ/LCF (Location Request/ Location Confirm) multicast protocol.

For example, if Node A places a call and sends an ARQ message to the Gatekeeper. The Gatekeeper consults its numbering plan database, determines that Node B is the correct destination, and returns the addressing information for Node B in an ACF message. Node A then sends the SETUP message directly to the H.323 Gateway Signaling Proxy Server on Node B.

If a Gatekeeper cannot resolve that destination address received in an incoming ARQ message, then it sends a LRQ message to other network zone Gatekeepers in order to resolve the number.

> ***Note:*** The Gatekeeper sending the LRQ message includes its own identification in the LRQ message and does not include the H323-ID of the gateway that sent the original ARQ message.

The peer Gatekeeper which resolves the number sends a LCF message with the destination Call Signaling address.

If a Gatekeeper cannot resolve the destination address in an incoming LRQ, it sends a Location Reject or a LRJ message to the originator of the LRQ message.

Incoming LRQ messages

When a Succession 3.0 Gatekeeper receives an incoming LRQ message, it checks to see if the Gatekeeper that sent the request is configured in its database. The information received in the **sourceInfo** field is used for authentication.

Table 7
How the Gatekeeper authenticates incoming LRQ messages

If the Gatekeeper sending the LRQ is a...	Then its sourceInfo field contains...	And the Gatekeeper has to check...
Succession 3.0 Gatekeeper	the alias address of the peer Gatekeeper which sent the LRQ message	(not applicable)
Succession 1000 Rel 2.0 Gatekeeper	the alias address of the Gateway	for the alias in the • network zone Gatekeeper list • endpoints list

If the information in the sourceInfo field cannot be authenticated, then the Succession 3.0 Gatekeeper rejects the incoming LRQ.

On receiving the incoming LRQ, the Gatekeeper parses the sourceInfo field. It searches for the source alias address as a URL ID type or an H323-ID type.

The Succession 3.0 Gatekeepers send the gatekeeper alias address along with the CDP domain information as a URL string. The format of the URL string is:

h323:gkH323ID;phone-context=cdpDomain

This URL string contains two variables which are configured at the far end:

- gkH323ID
- cdpDomain

This URL string is parsed for incoming LRQs and is used to extract the Gatekeeper alias name and the CDP domain information.

- The gatekeeper alias name is used for gatekeeper authentication
- The CDP domain information is used to search in the same CDP domain if the destination info was private.level0 type of number.

  Note: The cdpDomain is a string of characters that can be of any format. Typically, it would be something like "CDP-Canada.cdp.nt.com" to ensure uniqueness.

Outgoing LRQ messages

A Gatekeeper can be configured with a list of IP addresses of alternate gatekeepers in different network zone. The Gatekeeper can then send LRQ requests in an attempt to resolve ARQ requests which it cannot find registered matches for in its own numbering plan database.

The configuration of Network Zone Gatekeepers includes:

- an IP Address
- an H323 ID
- a CDP domain

See "Configuring Gatekeeper zones" on page 311.

This information is used for incoming LRQs and is also used to determined the Gatekeepers in which to send outgoing LRQs. If a Network Zone Gatekeeper is configured with a CDP domain, then it is sent an LRQ only if the endpoint sending the ARQ is also in the same CDP domain. If an ARQ request arrives, and there is no matching numbering plan entry for the destination phone number or there is a match but the matching entry (plus any alternates) is not currently registered, then the Gatekeeper sends an LRQ to all other gatekeepers on the network whose IP addresses have been configured.

Each Gatekeeper is configured with a Gatekeeper alias name which is an H323-ID. The outgoing LRQ message contains the Gatekeeper alias name in the sourceInfo field instead of the H323-ID received in the incoming ARQ message.

Gatekeeper purpose

IP Peer Networking uses optionally redundant Gatekeepers to support a centralized Network Numbering Plan. Each Gatekeeper has a zone that administers its own numbering plan, and requests out to other Gatekeepers for the numbering plan in their respective zones. A numbering plan specifies the format and structure of the numbers used within that plan. A numbering plan consists of decimal digits segmented into groups to identify specific elements used for identification, routing, and charging capabilities. A numbering plan does not include prefixes, suffixes, and additional information required to complete a call. The Dialing Plan contains this additional information. The Dialing Plan is implemented by the endpoints in a network. A Dialing Plan is a string or combination of digits, symbols, and additional information that defines the method by which the numbering plan is used. Dialing plans are divided into the following types:

- Private (on-net) dialing
- Public (off-net) dialing

For more information about numbering plans and dialing plans, see "Numbering plans" on page 117.

Gatekeeper discovery

Endpoints that require admission to the IP network and address translation must discover their Gatekeeper. Endpoints can be configured with the static IP address of the Gatekeeper running on the network's Primary Gatekeeper. This ensures that the IP address stays constant across reboots, and, therefore, the endpoints with statically configured Gatekeeper IP addresses can always discover the Gatekeeper. These endpoints send a message directly to the Gatekeeper over UDP/IP (User Datagram Protocol/Internet Protocol). This is the recommended approach; however, endpoints not configured with the IP address of the Gatekeeper, can use multicast to discover the IP address of their Gatekeeper.

The message requesting the IP address of the Gatekeeper contains the endpoint alias and the RAS signaling transport address of the endpoint. This is so the Gatekeeper knows where to send return messages. The message from the endpoint to the Gatekeeper also contains vendor information. This enables the Gatekeeper to determine the specific product and version that is

attempting discovery. The Gatekeeper only uses this information if the request for discovery is rejected.

Nortel Networks recommends that endpoints use the endpointAlias.h323-ID alias types.

The Gatekeeper contains a list of predefined endpoint aliases. The Gatekeeper attempts to match the H323-ID in the message from the endpoint with one of the endpoint aliases in the list. If it cannot find a match, it rejects the discovery request.

The Gatekeeper returns its RAS signaling transport address to the endpoint so the endpoint knows where to send RAS messages. The Gatekeeper also returns a list of Alternate Gatekeepers, if any are configured. Therefore, if the Gatekeeper is removed from service gracefully or if it cannot be reached by an endpoint, the endpoints can attempt to register with the Gatekeepers in the Alternate Gatekeepers list.

> ***Note:*** Gatekeeper Discovery using the Multicast approach is not recommended over large networks, because all routers between the endpoint requesting Gatekeeper discovery and the Gatekeeper must support Internet Group Management Protocol (IGMP).

Endpoint registration

After Gatekeeper discovery is complete, endpoints must register with the Gatekeeper. The Signaling Server platform, on which the H.323 Proxy Server for the node runs, has an IP address. This IP address is both the RAS signaling transport address and the call signaling transport address. The endpoints register with the Gatekeeper by sending a registration request message to the Gatekeeper.

Registering endpoints must provide vendor information, as well as its alias name in the registration request message. The Gatekeeper tracks the vendor information for management purposes. The administrator can determine the exact product and version of all registered endpoints using Gatekeeper Element Manager or the CLI. The Gatekeeper also uses this information if registration fails.

If the Gatekeeper accepts the registration request, it responds with a registration confirmation message. In this message, the Gatekeeper can include the IP address of an Alternate Gatekeeper (if one is configured). Endpoints also provide call signaling and RAS transport addresses in the registration request message. The Gatekeeper supports the receipt of multiple transport addresses and gives priority to the first address in each list.

> ***Note:*** IP Trunk 3.0 (or later) nodes always register multiple IP addresses due to the load-balancing architecture of the IP Trunk 3.0 (or later) nodes. The first IP address in the registration request is the node IP address and the remaining IP addresses are the IP addresses of the individual trunk cards in the node. When a call terminates on an IP Trunk 3.0 (or later) node, the Gatekeeper returns only the node IP address. The Gatekeeper knows that the endpoint is an IP Trunk 3.0 (or later) node, as its vendor information is provided in the request for registration message.

The Gatekeeper extracts the H323-ID from the incoming request for registration message and attempts to match it with one of the preconfigured endpoint H323-ID aliases in its internal database. If no match is found, the Gatekeeper rejects the registration request. If a match is found, the Gatekeeper accepts registration and extracts the call signaling and RAS transport addresses from the registration request message. The Gatekeeper updates its internal database with this information and then sends a registration confirmation message to the endpoint. If an Alternate Gatekeeper is configured, the Gatekeeper returns the Alternate Gatekeeper's IP address.

The Gatekeeper assigns the endpoint a unique Endpoint Identifier and returns this identifier in the registration confirmation message. This Endpoint Identifier is included in all subsequent RAS requests that the endpoint sends to the Gatekeeper. The Gatekeeper tracks the value of the assigned Endpoint Identifier for the duration of the endpoint's registration. The Gatekeeper can then match any incoming RAS request with the previously sent registration confirmation.

> ***Note:*** The Gatekeeper accepts registration request messages from an endpoint even if the Gatekeeper has not received a Gatekeeper discovery request from that particular endpoint.

Time-to-Live

The registration message includes Time-to-Live information. Endpoints periodically send registration request messages to the Gatekeeper in order to remain registered and so the Gatekeeper knows that the endpoints are alive.

An endpoint's registration with the Gatekeeper can expire. Registering endpoints must include Time-to-Live information in their registration request messages. The Gatekeeper responds with the same Time-to-Live information or the Time-to-Live information currently configured on the Gatekeeper if the Gatekeeper timer is shorter. This is a time-out in seconds. After this time, the registration expires. Before the expiration time, the endpoint sends a registration request message with the "Keep Alive" bit set. When the Gatekeeper receives this request, it extends the endpoints registration and resets the Time-to-Live timer.

If the Time-to-Live timer expires, the Gatekeeper unregisters the endpoint. The endpoint's entry in the internal database is updated to indicate that it is no longer registered and that the associated transport addresses are no longer valid.

Configure the Time-to-Live timer using the Gatekeeper webpages in Element Manager. Nortel Networks recommends that the timer be set to 30 seconds. Refer to Procedure 19, "Setting the RRQ Time-to-Live interval" on page 249.

Multiple registration requests

The Gatekeeper supports re-registration requests by an endpoint, provided that the information contained in the registration request is identical to that in the initial registration request. For example, if an endpoint crashes and then reboots after the boot sequence, it attempts to re-register with the Gatekeeper by sending another registration request message. The Gatekeeper accepts this registration by sending a confirmation message to the endpoint.

Registration requests when the Gatekeeper is out-of-service

The Gatekeeper can be taken out-of-service through the Gatekeeper webpages in Element Manager. If the Gatekeeper receives a registration request message from an endpoint while it is out-of-service, it rejects the registration request. However, the Gatekeeper sends the IP address of the Alternate Gatekeeper in the reject message.

Unregistration

An endpoint should be taken out-of-service prior to changing its IP address or performing software upgrades. Once out-of-service, an endpoint unregisters from the Gatekeeper by sending an unregister message. The Gatekeeper updates the endpoint's entry in the internal database to indicate that it is no longer registered and that the associated transport addresses are no longer valid.

If the endpoint does not send an unregister message to the Gatekeeper, the Gatekeeper automatically unregisters the endpoint when the Time-to-Live timer expires.

Gatekeeper webpages in Element Manager

Element Manager is a web-based configuration interface. Use the Gatekeeper webpages in Element Manager to configure the Gatekeeper. You can use Gatekeeper webpages to view, add, modify, or delete all numbering plan configuration data.

You can perform the following Gatekeeper configuration functions using Gatekeeper webpages:

- retrieve the current configuration database
- download a preconfigured database
- revert to the standby database
- configure a numbering plan
- add, modify, or delete preconfigured endpoint data
- add, modify, or delete numbering plan entries on a per-endpoint basis
- change system passwords

You can also perform the following Gatekeeper-specific performance monitoring functions using the Gatekeeper:

- **Monitor the state of endpoint registrations.**
  This shows the call signal and RAS IP addresses of all currently registered endpoints. If the endpoint provided multiple alias addresses or vendor information in the registration request message, this information is also shown.
- **View the traffic level history.**
  A log of the number of registration and admission requests handled each hour is kept. The traffic level history is tracked for each registered endpoint.
- **View the bandwidth usage history.**
  In every admission request, the originator provides a bandwidth field. The Gatekeeper logs the total bandwidth requested on an hourly basis.
- **View the alarm and exception log histories.**

The Gatekeeper webpages in Element Manager also provide access to more generic Succession Signaling Server platform debug services, including viewing the alarm and exception log histories.

Refer to “Configuring IP Peer Networking” on page 143 for information on how to perform the above functions.

Supported browsers

Element Manager supports Microsoft® Internet Explorer™ 6.0.2600 for the Windows™ operating systems.

Refer to “Logging in to the Gatekeeper webpages in Element Manager” on page 242 for information on logging in.

Security

The Gatekeeper webpages in Element Manager are password protected. The following are the two levels of access to Gatekeeper webpages:

- Guest access
- Administrator access

Guest access

If you log in to the Gatekeeper webpages as a guest, you can:

- view configuration data
- view output from the performance monitoring functions

As a guest user, you cannot modify any Gatekeeper configurations or settings, including the guest login user name and password. The default guest user name and password are as follows:

- default guest user name: **gkmon**
- default guest password: **gkmon**

Administrator access

If you log in to the Gatekeeper webpages in Element Manager as an administrator, you have full administrative access. You can update all configuration entries, and you have full write access to the database, including the ability to change all Gatekeeper-related system passwords. The default administrator user name and password are the following:

- default administrator user name: **gkadmin**
- default administrator password: **gkadmin**

Note: The Gatekeeper administrator user name and password are used only when accessing the Gatekeeper using Element Manager. Changing the Gatekeeper administrator user name and password does not change the user name and password for the Succession Signaling Sever shell.

Gatekeeper operating parameters

The Gatekeeper co-resides on the Succession Signaling Server with other applications. For large networks, if there is not enough capacity on the Succession Signaling Server to support Gatekeeper functionality in conjunction with other applications, a dedicated Succession Signaling Server can be required for the Gatekeeper. The Gatekeeper (Primary, Alternate, or Failsafe) cannot reside on an Alternate Succession Signaling Server. It has to be on a Primary (Leader) Succession Signaling Server.

The Gatekeeper has no knowledge of dialing plans implemented on endpoints. The Gatekeeper only has knowledge of numbering plans and deals only with fully qualified E.164/International numbers, fully qualified E.164/ National numbers, and fully qualified Private numbers.

Endpoints do not have to register the telephone numbers or range of telephone numbers that they support with the Gatekeeper. If endpoints register with this information, it is not used, but can be made available for management purposes through Element Manager.

Information regarding the numbers which an endpoint can terminate must be configured in the Gatekeeper. This ensures that the numbering plan for the entire network is managed from a central location and that endpoints cannot support numbers which are not preconfigured on the Gatekeeper. If an endpoint provides this number information when registering with the Gatekeeper, it is ignored.

Endpoints which register using RAS messages must provide an H323-ID or a similar alias (for example, URL-ID or e-mail ID).

The Gatekeeper only supports direct-routed call signaling and RAS messaging for call control. All endpoints registered with the Gatekeeper must use the ARQ mechanism and consult with the Gatekeeper for admission and address translation. The Gatekeeper does not pre-grant an ARQ for the call originator, but does pre-grant for the call terminator. This is because the Gatekeeper does not track call state, and has no easy way of correlating the ARQ between call originators and terminators.

All H.225/Q.931 call signaling messages and all H.245 call control messages are not directed to the Gatekeeper and are passed directly between endpoints.

This enables the Gatekeeper to be more scalable and to handle a larger number of simultaneous calls.

Each Gatekeeper can handle up to 60 000 calls per hour.

IP Peer Networking feature uses direct-routed call signaling; therefore, use of the Gatekeeper has no impact on MCDN or QSIG tunnelling. For example, if MCDN or QSIG is tunnelled between a Succession 1000 node and an IP Trunk 3.0 (or later) node, then the tunnelling takes place in the H.225/ Q.931 call signaling and is completely independent of the RAS which is routed to the Gatekeeper.

The Gatekeeper supports Overlap Sending according to H.323; however, allowable configuration items on the Gatekeeper must be taken into consideration.

The Gatekeeper generates SNMP traps and sends them to a configured SNMP host. The Gatekeeper uses the SNMP services provided by the Succession Signaling Server platform.

The Gatekeeper supports IP multicast for discovery and location request messages.

> ***Note:*** Gatekeeper Discovery using the Multicast approach is not recommended over large networks, because all routers between the endpoint requesting Gatekeeper discovery and the Gatekeeper must support Internet Group Management Protocol (IGMP).

The Gatekeeper does not support multiple customers. Multiple customers can be configured with each customer having their own unique dialing or numbering plan. If multiple customers are to be supported in a network, each customer must have their own Gatekeeper. As the Gatekeeper is a module running on the Succession Signaling Server, each customer must have their own Succession Signaling Server so they can have a dedicated H.323 Gateway and at least one dedicated Gatekeeper.

The Gatekeeper does not track the state of active calls, keep count of the total number of active calls, or generate Call Detail Recording (CDR) records. Therefore, all Disengage Request (DRQ) messages are automatically confirmed. The Gatekeeper does not have traffic management capabilities,

such as maximum calls allowed for each endpoint or maximum bandwidth allowed for each endpoint or zone.

Alternate routing based on the geographical zone of the call originator is not supported. This has implications for 911 handling. In order to provide different routing for 911 calls from different originating Succession 1000 or Succession 1000M nodes some form of digit manipulation is required. For example, if there are two nodes then one node could prefix 911 with 1 and the other node could prefix 911 with 2. The Gatekeeper could have two different numbering plan entries, one for 1911 and one for 2911 and provide different routing in this fashion.

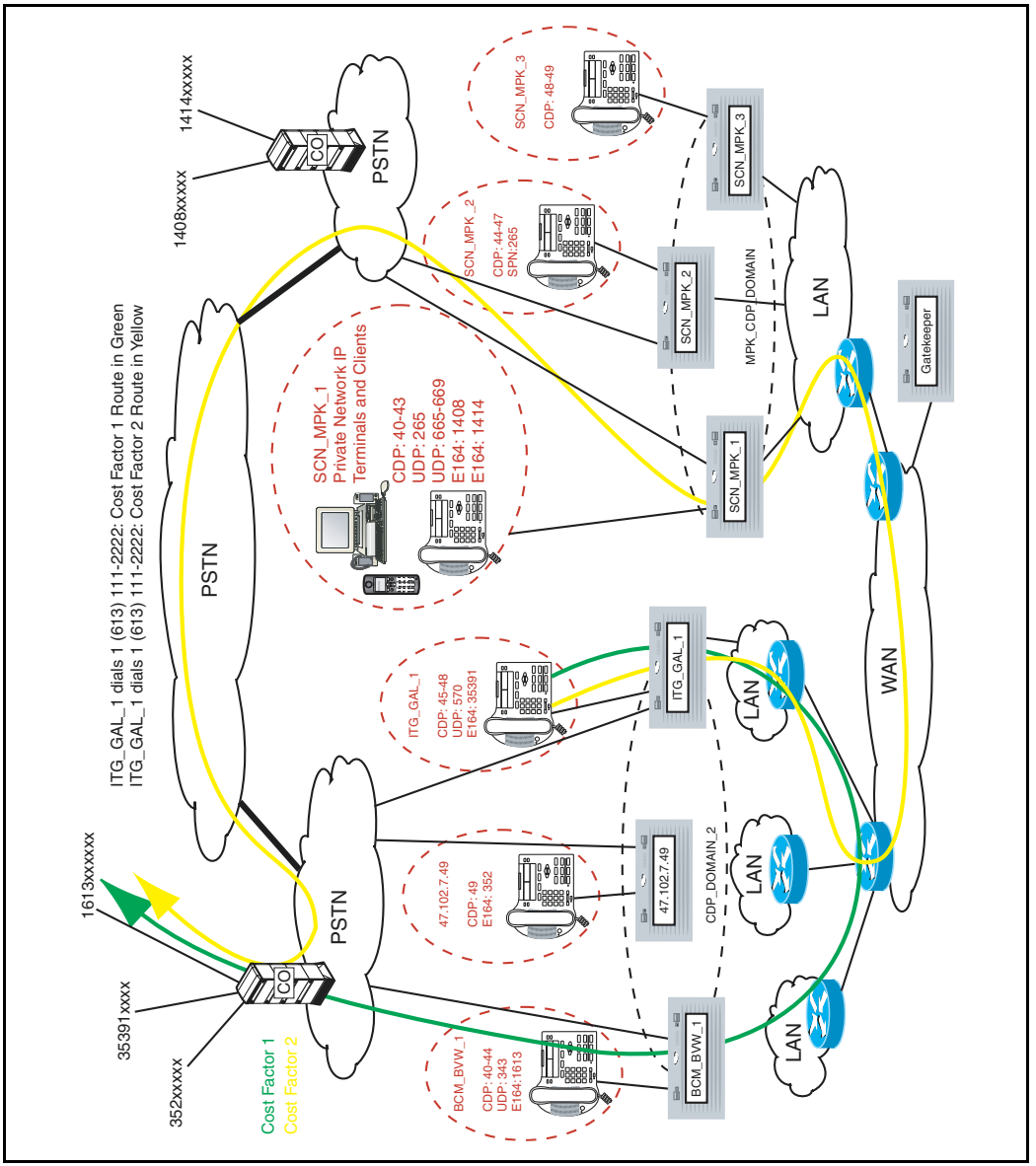
Zone management on the Succession Call Server provides an alternate mechanism for routing 911 calls, based on the Branch Office zone.

The Gatekeeper, like all Succession 1000 and Succession 1000M components, does not support the H.235 security protocol.

All number and cost factor pairs within a numbering plan table are unique for private numbering plans. When adding an alias for a predefined endpoint, the request is rejected if the administrator specifies an alias type and provides a number string and cost factor that is already in the numbering plan table for that alias type.

For example, Figure 27 on page 106 illustrates the configuration of a Succession 1000 System. SCN_MPK1 terminates privateNumber.level1RegionalNumber 265 with cost factor 1. BCM_BVW_1 also terminates this number but with a different cost factor, 2. If the administrator had attempted to configure this number on BCM_BVW_1 and had specified a cost factor of 1, the request would be rejected.

Figure 27
Example of all call routing plans



Number and cost factor pairs can be the same across different numbering plan tables. The numbering plan tables shown have only three columns for terminating route H323-ID and cost factor pairs. These are for illustrative purposes and in practice there can be as many alternate routes with different cost factors as required.

Similarly, configure the default routes according to alias type and CDP domain, as many alternate routes and associated cost factors can be required.

The Gatekeeper places the numbers in the numbering plan tables in ascending order. This accelerates the search when performing address translations.

When additional numbering plan entries are added using the Gatekeeper webpages in Element Manager, they are inserted in the middle of the table. For example, if an entry with publicNumber.internationalNumber alias type and numbering plan digits 1514 is added, it is inserted in the table between the 1414 and 1613 entries.

If an alias is added whose leftmost digits match an existing alias of the same type, it is placed below the existing entry in the table. For example, in the privateNumber.level1RegionalNumber table, the 2651 entry is below the 265 entry. This is similar to the ordering of entries in IP network routing tables, with more specific entries appearing below more general entries.

> ***Note:*** Tables generated in this example are represented in “Example–generated tables” on page 109.

When the Gatekeeper is resolving the IP address, if the number to be resolved begins with 2651XXX, the IP address of SCN_MPK_3 is returned (if it is registered). If the number to be resolved begins with 2652XXX, the IP address of SCN_MPK_1 is returned (if it is registered).

Ranges of leading digits can be configured (for example, a privateNumber.level1RegionalNumber entry of 665-669). This means that any numbers of this type beginning with 665, 666, 667, 668, or 669 are resolved to the IP address of SCN_MPK_1.

Leading digit ranges can be overridden by configuring more precise numbering plan entries or numbers with a greater number of leading digits.

For example, a privateNumber.level1RegionalNumber of 6651200# takes precedence over an entry of 665-669.

This means that the number 6651299 would resolve to the IP address of SCN_MPK_1, but 6651200 would resolve to the IP address of BCM_BVW_1. Note that due to the '#' character length requirement, 66512001 would not match the 6651200# numbering plan table entry and would resolve to SCN_MPK_1.

Endpoints that do not support RAS procedures have their IP address entered directly into the numbering plan table entry H323-ID field or the default route H323-ID field.

All H323-IDs are included in alphabetical order in the endpoint status table. This includes default endpoints.

The IP address field in the endpoint status table is only updated if it is known (that is, if the endpoint with the associated H323-ID has registered).

CDP numbering plan entries can be the same provided that the terminating endpoints belong to different CDP domains. For example, the CDP entries 40-43 for SCN_MPK_1 and 40-44 for BCM_BVW_1.

No special configuration items are present for ESN5 or Carrier Access Code support. If the Succession Signaling Server is unable to provide a fully qualified number in ARQ to the Gatekeeper and the number is prefixed with ESN5 prefix 100, then this prefix is placed before the existing entry in the numbering plan table.

National numbers are inserted into the publicNumber.internationalNumber table with the country code prefixed.

Example–generated tables

The configuration shown in Figure 27 on page 106 would result in the following tables:

Table 8
privateNumber.level1RegionalNumber numbering plan

Digits	Terminating Routes			
	H323-ID	Cost Factor	H323-ID	Cost Factor
265	SCN_MPK_1	1	BCM_BVW_1	2
2651	SCN_MPK_3	1		
343	BCM_BVW_1	1	SCN_MPK_1	2
570	ITG_GAL_1	1	47.102.7.49	2
665-669	SCN_MPK_1	1		
6651200#	BCM_BVW_1	1		

Table 9
privateNumber.plSNSpecificNumber numbering plan

Digits	Terminating Routes	
	H323-ID	Cost Factor
265	SCN_MPK_2	1

Table 10
publicNumber.internationalNumber numbering plan

Digits	Terminating Routes					
	H323-ID	Cost Factor	H323-ID	Cost Factor	H323-ID	Cost Factor
1408	SCN_MPK_1	1	BCM_BVW_1	2		
1414	SCN_MPK_1	1	SCN_MPK_2	2	ITG_GAL_1	3
1613	BCM_BVW_1	1	SCN_MPK_1	2		
352	47.102.7.49	1				
35391	ITG_GAL_1	1	47.102.7.49	2	SCN_MPK_1	3

Table 11
CDP Domain Table

CDP domain Name	Default Routes	
	H323-ID	Cost Factor
CDP_DOMAIN_2	47.85.2.100	1
MPK_CDP_DOMAIN		

Table 12
CDP_DOMAIN_2 numbering plan

Digits	Terminating Routes			
	H323-ID	Cost Factor	H323-ID	Cost Factor
40-44	BCM_BVW_1	1		
45-48	ITG_GAL_1	1		
49	47.102.7.49	1	47.102.7.50	2

Table 13
MPK_CDP_DOMAIN numbering plan

Digits	Terminating Routes	
	H323-ID	Cost Factor
40-43	SCN_MPK_1	1
44-47	SCN_MPK_2	1
48-49	SCN_MPK_3	1

Table 14
Default Route Table

Alias Type	Default Routes			
	H323-ID	Cost Factor	H323-ID	Cost Factor
publicNumber.internationalNumber	INTN_GW_1	1	INTN_GW_2	2
privateNumber.level1RegionalNumber	PRIV_GW	1		

Table 15
Endpoint Status Table

H323-ID	IP
BCM_BVW_1	
SCN_MPK_1	47.82.33.47
SCN_MPK_2	47.82.33.50
SCN_MPK_3	
INTN_GW_1	
INTN_GW_2	47.50.10.20
ITG_GAL_1	47.85.2.201
PRIV_GW	

Stand-alone Gatekeeper support for Meridian 1 and BCM nodes

Nortel Networks supports the use of a Succession 1000 H.323 Gatekeeper for Meridian 1 Release 25.40 and BCM 3.01 nodes.

The Succession 1000 H.323 Gatekeeper in a stand-alone configuration can be used to migrate numbering plans from node-based numbering plans to centralized Gatekeeper-based numbering plans. This provides increased functionality, as well as the flexibility to migrate a traditional Meridian 1 or BCM-based network to a Succession network.

In order to illustrate how the Succession 1000 H.323 Gatekeeper fits into a Meridian 1/BCM network using IP Trunks, it is useful to first look at how the Meridian1/BCM handles call admission control and numbering plan resolution.

Meridian 1/BCM node-based numbering plan

Figure 28 illustrates how the Meridian1/BCM handles call admission control and numbering plan resolution.

Figure 28
Meridian 1/BCM node-based numbering plan

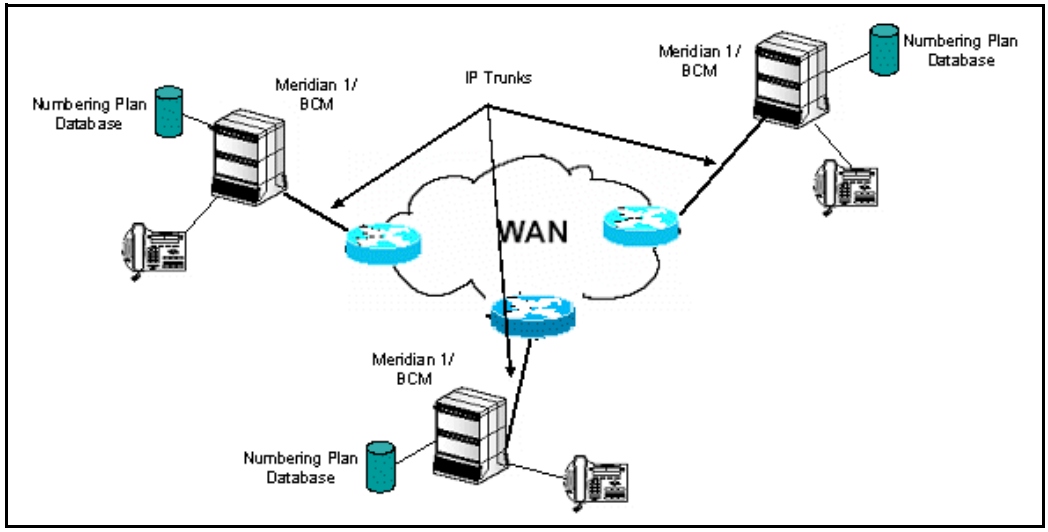


Figure 28 shows a Meridian 1/BCM network with the Meridian 1/BCM nodes equipped with IP Trunks. The IP Trunk routes are point-to-multipoint. Regardless of where the terminating node is located, all calls can be sent out over the same route. The calls can be routed to the correct destination over the packet-based IP network by the IP Trunk.

Every IP Trunk node in the network has its own numbering plan database. All IP Trunk nodes are configured with the following:

- The static IP address of every other IP Trunk node on the network.
- The numbering plan to route calls to the correct destination node.

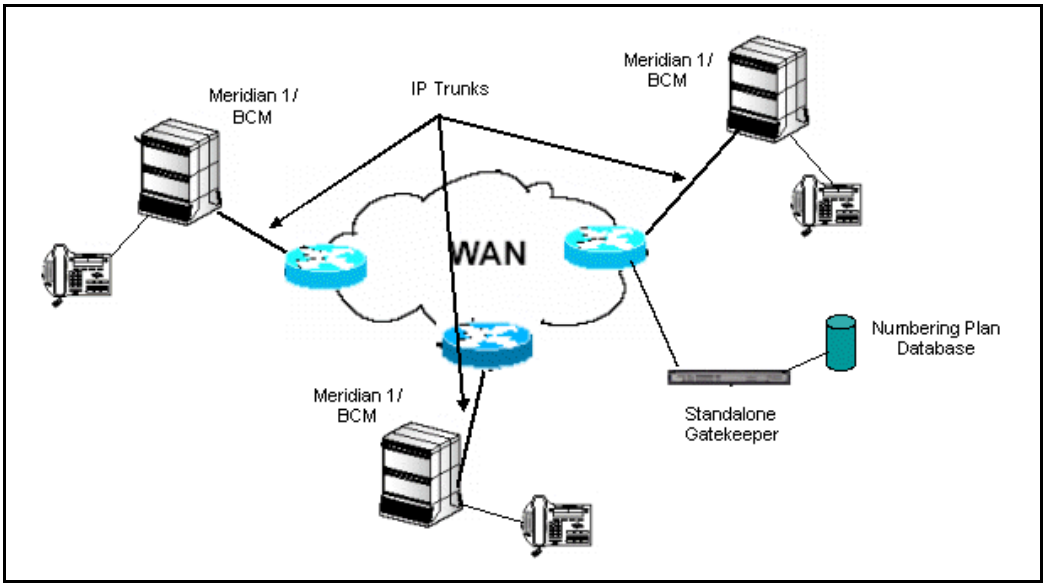
When the Meridian 1/BCM wishes to make an IP Trunk call, the following occurs:

1. The node consults its numbering plan.
2. The node determines where the destination is located.
3. The node retrieves the statically configured destination IP address.
4. The node routes the call directly to the destination node.

Gatekeeper-based numbering plan

In a Meridian 1/BCM network running IP Trunks and a stand-alone Succession 1000 H.323 Gatekeeper, the network numbering plan is centrally administered by the Gatekeeper as shown in Figure 29.

Figure 29
Gatekeeper-based numbering plan



The Succession 1000 H.323 Gatekeeper is configured with numbering plan information for every single Meridian 1/BCM node in the network zone.

The typical Meridian 1/BCM network is configured to use Gatekeeper Resolved signaling. With Gatekeeper Resolved signaling, the Gatekeeper provides address resolution, however, call set-up is performed directly between the nodes.

When a node wishes to place an IP call to another IP Trunk-enabled node, the originating node looks at its internal dialing plan table for address translation. If it cannot find a match, it then sends ARQ (Admission Request) to the Gatekeeper specifying the destination phone number. When configured to use Gatekeeper, the node automatically sends the ARQ to the Gatekeeper. The Gatekeeper consults its internal numbering plan database and determines which Meridian 1/BCM node is the correct destination node. The Gatekeeper then sends an Admission Confirm (ACF) to the call originator and includes addressing information for the destination node. Standard call setup is then performed between the two nodes.

Numbering plan information is stored centrally on the Gatekeeper for the entire network zone which greatly reduces the administrative overhead.

Note 1: For customers using a stand-alone gatekeeper, note that QoS Fallback to PSTN is not supported for IP Trunk destination nodes whose called telephone numbers are resolved by the Gatekeeper. Meridian 1 IP Trunk nodes that must use QoS Fallback to PSTN must continue to use the node-based Dial Plan table entries to resolve each other's telephone numbers. Gatekeeper number resolution can be used concurrently for any IP Trunk destination nodes that do not use QoS Fallback to PSTN.

In order to eliminate a single point of failure in their network, Nortel Networks recommends the deployment of both a primary and an alternate gatekeeper.

Numbering plans

Contents

This section contains information on the following topics:

Introduction

When setting up a Succession 1000 or Succession 1000M network, there are several numbering plans that can be used. This depends on customer preferences for dialing and configuration management requirements.

> ***Note:*** The numbering plan information required for the Succession Call Server software to internally route calls, such as routing information for locally accessible numbers, must be configured within each Succession Call Server.

"Numbering plan entry overview" on page 131 describes the implementation of the numbering plans. The sections below describe the following types according to their use:

- Uniform Dialing Plan
  - North American Numbering Plan
  - Flexible Numbering Plan
- Coordinated Dialing Plan
  - Transferable Directory Number
  - Group Dialing Plan
- Vacant Number Routing
- Special Numbering Plan

Private (on-net) numbering plans

Private (on-net) dialing refers to the dialing situations that occur when dialing telephones located within a local (private) network.

Uniform Dialing Plan

A Uniform Dialing Plan (UDP) enables users to dial all calls in a uniform manner, regardless of the location of the calling party or the route that the call takes. When using a Uniform Dialing Plan (UDP) to address private numbers, each location is assigned a Location Code (LOC). Each telephone has a Directory Number (DN) that is unique within the Succession Call Server (and Customer). To reach a user, you must know their Location Code and their DN. To reach an on-net location, the user dials the following:

Network Access Code (AC1 or AC2) + LOC + DN

For example, if:

- Network Access Code (AC1 or AC2) = 6
- LOC = 343
- DN = 2222

The user dials: 6 343 2222

The Gatekeeper must keep the Home Location (HLOC) code of every Gateway that is registered for UDP routing. To route a call, the H.323 Gateway passes the LOC and DN to the Gatekeeper to determine the IP addressing information of the desired Gateway. The Gatekeeper searches for the LOC within its database and returns the IP addressing information for the site. Then, the Gateway software can directly set up a call to the desired Gateway.

For more information on UDP, refer to *Basic Network Features* (553-3001-379).

For call routing information, see “UDP call routing operation” on page 140.

Coordinated Dialing Plan

With a Coordinated Dialing Plan (CDP), each location is allocated one or more Steering Codes that are unique within a CDP domain. Steering Codes are configured within a dialing plan and are part of the DN itself. They route calls on the network by a DN translator. The Gatekeeper has a list of Distant Steering Codes to route a call, while the Succession Call Server has a list of Local Steering Codes, which act like a HLOC.

Steering Codes enable you to reach Directory Numbers on a number of Succession Call Servers with a short dialing sequence. Each user's DN (including the Steering Code) must be unique within the CDP domain.

For example, a number of Succession Call Servers can be coordinated so that five-digit dialing can be performed within a campus environment. For example:

- **Call Server A:** Steering codes 3 and 4 (that is, DNs in the range 3xxxx and 4xxxx)
- **Call Server B:** Steering code 5 (that is, DNs in the range 5xxxx)

Within this group of Succession Call Servers, users can reach each other by dialing their unique DN. However, all DNs on Call Server A must be in the range 3xxxx or 4xxxx, whereas all DNs on Call Server B must be in the range 5xxxx.

> ***Note:*** If a user moves from one Succession Call Server to another, their DN must change in the CDP numbering plan (see "Transferable Directory Number" on page 121).

You can use CDP in conjunction with UDP. You use UDP by dialing AC1 or AC2 to reach UDP Location Codes, but use CDP by dialing CDP DNs within a CDP domain.

For a detailed description, refer to *Dialing Plans: Description* (553-3001-183).

For call routing, see "CDP call routing operation" on page 138.

Group Dialing Plan

Group Dialing Plan (GDP) enables coordinated dialing within a network using LOCs. Each group is assigned a LOC. From outside the group, you must dial the LOC as a prefix to the group CDP. In this case, the telephone's dialed number can be different when dialed from different locations.

For example, if:

- Network Access Code (AC1 or AC2) = 6
- LOC = 343
- DN = 3861

The user dials: 6 343 3861 from anywhere on the network, or the user dials only the DN (3861) from within the same CDP group.

Group Dialing Plans are part of Flexible Numbering Plans. For more detailed information, refer to *Dialing Plans: Description* (553-3001-183).

Transferable Directory Number

With Transferable Directory Numbers, each user is provided with a unique DN which does not change if they move to a different Succession Call Server. The Gatekeeper must keep track of each Transferable Directory Number in the network so that it knows which Gateway(s) to return when asked to resolve a Transferable Directory Number address.

For call routing information, see "Transferable DN call routing operation" on page 136.

Vacant Number Routing

In order to keep the Transferable Numbering Plan at a manageable level, Vacant Number Routing (VNR) was introduced with Succession CSE 1000 Release 2.0. This enables small sites, such as the Branch Office, to require minimal configuration to route calls through other Succession Call Servers or through the Gatekeeper. Instead of changing the numbering trees and steering codes at each location, all the routing information can be kept at one central location.

If a vacant number is dialed, the call is routed to the Gatekeeper. The Gatekeeper decides where the terminal is located. If the terminal cannot be located, then vacant number treatment at the terminating location is given. The DN is not treated as invalid at the location where vacant number dialing is in effect.

Vacant Number Routing must be configured on the Branch Office Succession System Controller (SSC). Refer to *Branch Office* (553-3001-214) for more information.

Succession 3.0 supports an enhancement to VNR. VNR enables data manipulation index (DMI) numbers for all trunk types so that an alternate route can be used for the VNR route. The VNR enhancement increases the flexible length of UDP digits from 10 to 19 and as a result, international calls can be made.

Based on the analysis of the dialed digits sets, TON/NPI for VTRK calls removes the NARS access code and the national or international prefix (dialed after NARS access code) so the Gatekeeper can route the call correctly.

This minimizes the configuration on the Branch Office. Only CDB NET data must be defined on the originating node (the Branch Office). There is no need to define NET data (in LD 90) and all UDP calls (International, National, NXX LOC) are working using VNR route.

> ***Note:*** LOC and NXX must use different NARS access codes. That is, if LOC is using AC2 then NXX must be defined for AC1. When defining CDB, you must only define dialing plans which use AC2. All others default to use AC1.

For more information on the VNR enhancement, refer to page 232.

Public (off-net) numbering plans

Public (off-net) dialing refers to dialing situations that occur when dialing a telephone that is not part of the local (private) network.

Uniform Dialing Plan

An off-net call using UDP is a call that does not terminate within the local (private) network; although, some on-net facilities can be used to complete a portion of the call routing. UDP uses network translators AC1 and AC2 to route calls. UDP uses Special Numbers (SPNs) to enable users to dial numbers of varying lengths.

For example, a UDP call is considered off-net if a user at LOC 343 dials the following:

AC1 or AC2 +1 + NPA +NXX + XXXX

For example, if:

- Network Access Code (AC1 or AC2) = 6
- NPA = 416
- NXX = 475
- XXXX = 7517

The user dials: 6 + 1 (416) 475-7517.

For call routing information, see “UDP call routing operation” on page 140.

North American Numbering Plan

The Succession Call Server supports North American Numbering Plan routing. The North American Numbering Plan is used to make North American public network calls through the private network. The North American Numbering Plan accommodates dialing plans based on a fixed number of digits. A user can dial AC1 or AC2 + NXX + XXXX for local calls or AC1 or AC2 + 1 + NPA + NXX + XXXX for toll calls.

For example, if:

- Network Access Code (AC1 or AC2) = 9
- NPA = 506
- NXX = 755
- XXXX = 8518

The user dials: 9 + 1 (506) 755-8518

Flexible Numbering Plan

Flexible Numbering Plan (FNP) accommodates dialing plans which are not based on a fixed number of digits (for example, International numbers). FNP uses SPNs to enable users to dial numbers of varying lengths. Also, the total number of digits dialed to reach a station can vary from station to station. FNP also enables flexibility for the length of location codes from node to node. An FNP can be used to support country-specific dialing plans. For example, to reach an international number from North America, a user can dial: AC1 or AC2 + 011 + Country Code + City Code + XXXXXX.

For example, if:

- Network Access Code (AC1 or AC2) = 9
- Country Code = 33
- City Code = 1
- XXXX = 331765

The user dials: 9 + 011 + 33 + 1 + 331765

For information on FNP operation and package dependencies, refer to *Dialing Plans: Description* (553-3001-183).

Special Numbering Plan

There exist SPNs for each country's dialing plan. In North America, the recognizable SPNs are 411, 611, 0, and 011 for international calling. The circuit switch or Gatekeeper recognizes the digits that are not part of, or do not comply with, the regular dialing plan, such that further dialing string analysis is rarely possible (this is referred to as a catch-all configuration).

Europe uses SPN dialing plans almost exclusively, because European numbering plans are not as rigid as North American plans.

Address translation and call routing

When an H.323-compliant entity on the network wants to place a call, it sends an admission request (ARQ) to the Gatekeeper. The endpoint includes the destination telephony number in this message. The destination information is an H.323 alias. The Gatekeeper extracts the destination alias and ensures that it is one of the supported types. The Gatekeeper then searches its numbering plan database to determine which endpoints on the network can terminate the telephone number and whether or not these endpoints are registered. The Gatekeeper returns the IP address of any endpoints which can terminate this number and are registered to the endpoint.

> ***Note:*** Endpoints that do not support RAS messaging do not register with the Gatekeeper.

Basic call routing

The routing of calls within Succession 1000 and Succession 1000M Large and Small System networks depends on the type of numbering plan in use and the number dialed. “Transferable DN call routing operation” on page 136 provides a description of how a call is routed from the call originator to the desired desktop or PSTN using the Transferable DN type of numbering plan. This is the most flexible numbering plan. It illustrates the configuration and operation of the routing software. The operation for “Private (on-net) numbering plans” on page 119 and “Public (off-net) numbering plans” on page 123 are described in “Numbering plans and routing” on page 134.

The H.323 Gatekeeper plays a key role in configuring numbering plans in a network. It provides IP address resolution based on dialed numbers.

Supported alias types

The Gatekeeper performs address translations on H.323 partyNumber alias types and on E.164 alias types. The partyNumber alias can be one of several subtypes according to the H.323 standard. The only partyNumber subtypes which the Gatekeeper supports are partyNumber.publicNumber and partyNumber.privateNumber. These also have subtypes. See Table 16 on page 126.

Table 16
Term explanations (Part 1 of 2)

H.323 signaling protocol	Succession 1000 and Succession 1000M term
publicNumber.internationalNumber (See Note 1)	E.164 International (UDP)
publicNumber.nationalNumber (See Note 1)	E.164 National (UDP)
publicNumber.subscriber	See Note 2.
publicNumber.unknown	See Note 3.
privateNumber.level1RegionalNumber (See Note 1.)	Uniform Dialing Plan Location Code (UDP LOC)
privateNumber.pISNSpecificNumber (See Note 1.)	Special Numbers (SPN)
privateNumber.localNumber (See Note 1.)	Coordinated Dialing Plan (CDP)
privateNumber.unknown	Unknown (UKWN) (See Note 4.)
e164	See Note 5.
Note 1: Only these alias types can be entered as numbering plan table entries using the web browser interface. The other alias types have no Type Of Number information.	
Note 2: Not supported by the Succession Gatekeeper. The Succession Call Server algorithmically coverts any public subscriber number to a supported type (for example, coverts a publicNumber.internationalNumber by adding the country code and area code).	
Note 3: Not supported by the Succession Call Server, but is supported by the Succession Gatekeeper for third-party interoperability. This is treated as a publicNumber.internationalNumber.	

Table 16
Term explanations (Part 2 of 2)

H.323 signaling protocol	Succession 1000 and Succession 1000M term
Note 4: Not supported by the Succession Call Server, but is supported by the Succession Gatekeeper for third-party interoperability. The Succession Call Server can generate privateNumber.unknown types with the limitation that INAC does not work. The Gatekeeper attempts to convert the number to privateNumber.localNumber (that is, CDP) or privateNumber.level1RegionalNumber (that is, UDP LOC) by analyzing the digits. If the Gatekeeper cannot determine which type to use based on digit analysis, it assumes that privateNumber.localNumber (that is, CDP) should be used.	
Note 5: Not supported by the Succession Call Server, but is supported by the Succession Gatekeeper for third-party interoperability. A default prefix can be configured on a per-Gatekeeper basis to distinguish between public and private numbers. For example, a prefix of “9” can be configured as the public number prefix. A prefix of “6” can be configured as the private default prefix. The Gatekeeper looks at the first digit. If it matches the public prefix (for example, “9”), it treats the subsequent digits as a publicNumber.internationalNumber. If the first digit matches the private prefix (for example, “6”), it treats the subsequent digits as a privateNumber.localNumber (that is, CDP) or privateNumber.level1RegionalNumber (that is, UDP LOC), depending on its digit examination.	

If the Gatekeeper receives an admission request message requesting translation for any other alias type (for example, publicNumber.subscriberNumber), it rejects the request.

The H.323 Proxy Server, which sends the admission request to the Gatekeeper, is responsible for mapping Numbering Plan Indicator (NPI)/ Type of Number (TON) values in the ISDN SETUP Called Party Number Information Element to one of the eight H.323 alias types listed in Table 16 on page 126.

Mapping between Succession 1000 and Succession 1000M NPI/TON and H.323 alias types

The Succession 1000 and Succession 1000M systems supports the NPI and (TON values shown in Tables 17 and 18). These values are for Universal ISDN Protocol Engine (UIPE)-formatted NPI/TON numbers.

Table 17
NPI values

NPI on Succession Call Server	UIPE-formatted description
0	UNKNOWN
1	E164
2	PRIVATE
3	E163

Table 18
TON values

TON	UIPE-formatted description
0	UNKNOWN
1	INTERNATIONAL
2	NATIONAL
3	SPECIAL
4	SUBSCRIBER
5	UNIFIED (UDP location code).
6	COORDINATED (CDP distant/trunk steering code)
Note: The Gatekeeper sees a trunk steering code as privateNumber.unknown, and so it converts it to privateNumber.localNumber in CDP	

Table 19 on page 129 shows the NPI/TON pairs, the corresponding call types and their corresponding H.323 alias types for which the Gatekeeper accepts

translation requests. The call type for outgoing routes can be manipulated by configuring a DMI in LD 86 and specifying the Call Type (CTYP).

If the H.323 Proxy Server receives a Q.931 setup message for an NPI/TON pair not included in Table 19, it must map the number according to one of the NPI/TON pairs/H.323 alias types which the Gatekeeper supports. This can require modifications to the called number dialing string.

CTYP is the mnemonic in the ESN overlays.

Table 19
NPI/TON to H.323 alias mapping

NPI UIPE	TON UIPE	CTYP	H.323 alias
E164 or E163	INTERNATIONAL	INTL	publicNumber.internationalNumber
	NATIONAL	NPA	publicNumber.nationalNumber
	UNKNOWN		publicNumber.unknown
PRIVATE	SPECIAL	SPN	privateNumber.pISNSpecificNumber
	UNIFIED (see Table 18 on page 128)	LOC	privateNumber.level1RegionalNumber
	COORDINATED (see Table 18 on page 128)	CDP	privateNumber.localNumber
	UNKNOWN	UKWN	privateNumber.unknown

The endpoints must correctly map the UIPE NPI/TON pairs to a valid partyNumber type that the Gatekeeper supports. The administrator must coordinate the numbering plan on the Gatekeeper with the mapping carried out by the endpoints.

LD 96 has been enhanced to show NPI/TON and ESN call types for D-Channel monitoring. Calling and Called number information for level 0 D-Channel tracing now includes the TON and ESN call types.

Table 20 shows Q.931 TON mapping.

Table 20
Q.931 TON mapping

NPI	TON
x000xxxx	Unknown
x001xxxx	International Number
x010xxxx	National Number
x011xxxx	Network Specific Number
x100xxxx	Subscriber Number
x110xxxx	Abbreviated Number
x101xxxx x111xxxx	Reserved for Extension

Table 21 shows the NPI/TON to ESN Call type mapping.

Table 21
NPI/TON to ESN Call type mapping

NPI	TON	ESN
0001 - E.164	010 - National	NPA
0001 - E.164	100 - Subscriber	NXX
1001 - PRIVATE	011 - Network Specific	SPN
1001 - PRIVATE	101 - Reserved	LOC
1001 - PRIVATE	110 - Abbreviated	CDP

Numbering plan entry overview

A numbering plan entry can be private or public. Private numbers can be configured using CDP, or UDP Location Code (LOC) entries. Public numbers can be configured using E.164 International or E.164 National entries.

When configuring a predefined endpoint on the Gatekeeper, the administrator must add the required numbering plan entries. The administrator adds the numbers or number ranges that the endpoint can terminate. For every numbering plan entry, the administrator must specify the alias type and the cost factor associated with the route. See “Configuring numbering plan entries” on page 272.

Using the cost factor to determine the entry or the path and endpoint, the Gatekeeper can match multiple entries to a dialed number. This enables alternate routing based on the cost of facilities. The Gatekeeper matches the number string with the most matching digits. For example, the following are defined as entries:

- 1613
- 161396
- 1613967

If a user dials “1613966”, the Gatekeeper matches entries with “161396”. See Table 22 for the cost factors associated with these entries.

Table 22
Cost factors

Entry	Cost factor
1613	1
161396	1
161396	2
1613967	1

In this case, the Gatekeeper returns the entries with the lowest cost entry first.

The administrator must also specify if the endpoint belongs to a CDP domain. If the endpoint does belong to a CDP domain, the administrator must specify the CDP domain name. However, before specifying an endpoint's CDP domain membership, the administrator must configure the CDP domain. The administrator does this by adding a new CDP domain and specifying its name. The alias type privateNumber.localNumber corresponds to a CDP number. When configuring a numbering plan entry for this alias type, the administrator must have previously specified the CDP domain to which the endpoint belongs.

Default endpoints can also be configured for each of the supported numbering plan alias types. These entries are configured by entering the H323-ID of the default endpoints and their associated cost factors.

> ***Note:*** For alias type privateNumber.localNumber (for example, CDP numbers), multiple default routes for each CDP domain can be configured. Each CDP domain must have its own default routes.

The Gatekeeper has one standard numbering plan table for each of the publicNumber.internationalNumber (CTYP = INTERNATIONAL), privateNumber.pISNSpecificNumber (CTYP = COORDINATED), and privateNumber.level1RegionalNumber (CTYP = UNIFIED) supported alias types.

> ***Note:*** Although publicNumber.nationalNumber aliases can be configured, there is no numbering plan table associated with this alias type, as these aliases are inserted in the publicNumber.internationalNumber table.

The Gatekeeper also has one numbering plan table for each CDP domain configured. Therefore, there are multiple numbering plan tables configured for the privateNumber.localNumber alias type. Each table contains lists of numbering plan entries with each entry containing the following information:

- leading digit string
- cost factor associated with the route to this endpoint

The Gatekeeper has a table for each of the standard alias types (internationalNumber.pISNSpecificNumber and level1RegionalNumber) which provides the default routes associated with each type. The tables

contain the H323-ID of the default routes or the IP address if the default route does not support RAS procedures and the cost factor associated with the route. There is also a table of default routes for each CDP domain.

Number Type support

The Gatekeeper enables address translation requests for publicNumber.nationalNumber and publicNumber.internationalNumber types. The Gatekeeper can be used for address translation across several countries; therefore, the Gatekeeper must be able to identify which country the request came from. The Gatekeeper must also be able to handle country codes correctly.

There is a system-wide configuration variable that specifies the default country code. For example, this variable could be set to “1” if the majority of the Gatekeeper traffic is within North America. There is also the option to configure a a country code for every endpoint that overrides the default system-wide country code. For example, if there is one Succession 1000 node in Galway, Ireland and all other nodes are in North America, the default system-wide country code could be set to “1” and the country code for the node in Galway could be set to “353”.

When configuring numbering plan table entries, the administrator can configure national number entries. When configuring a national number entry, either the system-wide country code or the endpoint-specific country code must be configured first. The Gatekeeper automatically prefixes the national numbering plan entry with the country code and then inserts this entry in the international numbering plan table. No table exists for national numbers. All national numbers are converted to international. When the Gatekeeper receives an admission request for a national number, the Gatekeeper determines the originator of the request, extracts the destination telephony number, prefixes the number with the relevant country code (either the country code for the endpoint or the system-wide country code), and resolves the number by searching in the international number table.

Note that the numbering plan entries in the Gatekeeper are strictly in conformance with the E.164 International standard, and that calls on Virtual Trunks which access the Gatekeeper must be correctly tagged.

For example, an endpoint can make an international call to 1-416-xxxxxxx. If this digit sequence is sent to the Gatekeeper, it must have a Call Type of "International", because the country Code ("1") is included. The same endpoint can make a call to 416-xxxxxxx, but in this case the Call Type must be "National", because the country code is not included. Both of these scenarios work correctly, as the Gatekeeper is set up to process both 416/ National and 1416/International.

However, it is not valid to send digits 1-416-xxxxxx with a Call Type of "National": the Gatekeeper is not able to recognize this, and the call is not routed.

Numbering plans and routing

When users attempt to make calls on a Succession 1000 or Succession 1000M system, they use dialed digits to indicate which telephone or service they would like to reach. Within the Succession Call Server, these digits are translated to determine whether the user is attempting to reach an internal telephone or service, or trying to reach another user or service outside of the Succession 1000 or Succession 1000M system. This is the first level of routing.

If the user is trying to reach a device that is internal to the Succession 1000 or Succession 1000M system, the Succession Call Server terminates the call as appropriate on the internal device. If the user is trying to reach a device outside the Succession 1000 or Succession 1000M system, there are several options that can be configured within the system.

The system administrator can choose to use one of the PBX Networking numbering plans, such as CDP, to help route the call to the appropriate trunk route, or the administrator can choose to use Vacant Number Routing (VNR), where any number that is not known to the Succession Call Server is routed out a specified trunk route. This enables a Gatekeeper to determine the final destination of the call from a central database.

Refer to *Dialing Plans: Description* (553-3001-183) for information on VNR operation.

Using a Gatekeeper for routing

Once the system determines that a user is attempting to reach a telephone or service using the IP network, the call is routed to the H.323 Gateway software, which uses the Gatekeeper to help with the routing of the call.

The basic role of a Gatekeeper is to perform address translation from an alias (in this case, a telephone number) to an IP signaling address, and to authorize the call in the H.323 network.

The Gatekeeper is the central location where the numbering plan information is configured. The identity of each endpoint (for example, a Succession 1000 system) is configured in the Gatekeeper with the numbers it can reach. For example, an entry could look like the following:

"Santa Clara-01"

PublicNumber = +1 408 XXX XXXX

PrivateNumber = Electronic Switched Network (ESN) 265 XXXX, ESN 655 XXXX

At power-up, an endpoint performs Gatekeeper Discovery using a configured Gatekeeper address. The endpoint then registers with its primary Gatekeeper at the address returned by the Gatekeeper Discovery process using the H.225.0 (RAS) protocol by sending its H323-ID and its IP address. In the example above, it would use the following:

"Santa_Clara-01"

Signaling IP address = 47.0.1.2

Upon receipt of the registration, the Gatekeeper matches the name "Santa_Clara-01" in the registration with the configured information in its database, and adds the IP address.

When a user behind an H.323 proxy wants to reach another user, its H.323 proxy sends a call request to its Gatekeeper. The Gatekeeper determines any endpoint(s) that are responsible for that particular user and returns its

signaling IP address(es) in the direct-routed model, which is the preferred model.

Using the same example, the user dials “62653756”. Its Succession Call Server determines that this call is destined to ESN 265 3756 based on the dialing prefix and routes the call to the H.323 Gateway. The H.323 Gateway sends an admission request to the Gatekeeper for PrivateNumber ESN 265 3756. The Gatekeeper then consults its database and performs the closest match (that is, “ESN 265 XXXX” in the “Santa_Clara-01” entry) and returns the IP address that was previously provided by “Santa_Clara-01” at registration time (that is, 47.0.1.2).

Transferable DN call routing operation

With the Transferable Directory Number type of CDP numbering plan, networks provide the ability to enable users to move from location to location while retaining their Directory Number. This capability is provided by a combination of Network Management and the call routing capabilities of the Succession Call Server software. The Gatekeeper must be updated to reflect the current location of the DNs.

> ***Note:*** Transferable Directory Numbers are usually used in conjunction with Vacant Number Routing (VNR).

Figure 30 on page 137 shows a network of Succession 1000 Systems in which each user wants to retain their unique seven-digit Directory Number. Table 23 on page 138 provides a summary of the DNs in Figure 30, as well as their associated Succession Call Server.

Each user in the network is associated with a Succession Call Server and its group of Gateways. The Gateways provide call processing features and redundancy. The Gatekeeper in Figure 30 is aware of the location of any user with a given Directory Number within the network. In this case, the user with Directory Number 22221 is located at Call Server A. When a user dials the last digit of this number, their Call Server determines whether the user is within its local database, and if so, handles the call directly.

For example, if the user with Directory Number 22222 dials 22221, Call Server A handles the call directly.

However, if the Directory Number is not within the local database of the initial Succession Call Server, the call is routed through the H.323 Gateway software on the Signaling Server in order to locate the user. This routing uses a feature called Network Number Resolution. Since the Gatekeeper knows where to locate any user with a Transferable Directory Number, it directs the call to the proper Succession Call Server.

For example, if the user with DN 22224 dials DN 22221, Call Server B routes the call to the H.323 Gateway software, which requests the location of the desired Succession Call Server from the Gatekeeper. The Gatekeeper responds with the H.323 address information of Call Server A, at which time Call Server B attempts a call setup to Call Server A and completes the call.

Figure 30
Transferable DN routing

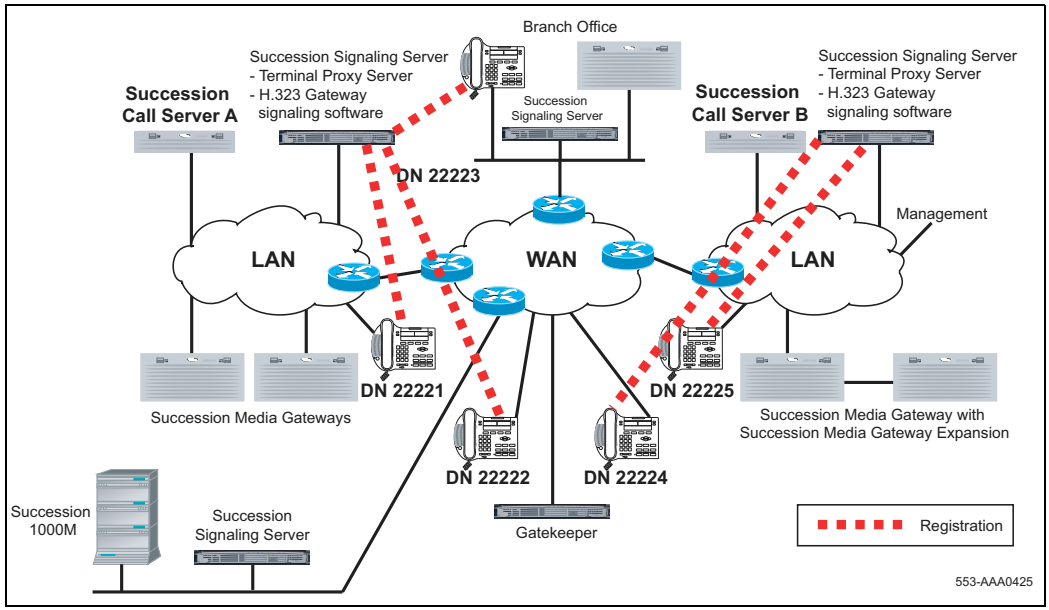


Table 23
DNs with their associated Succession Call Server

DN	Succession Call Server
22221	A
22222	A
22223	A
22224	B
22225	B

CDP call routing operation

The routing of calls in a CDP-type of numbering plan is the same as that for Transferable Directory Number, with the following exceptions:

- Only the Steering Codes must be stored in the Gatekeeper, since entire ranges of DNs are located within the same Succession Call Server.
- With CDP, Succession Call Servers and Branch Offices can be grouped into CDP domains, all sharing a CDP. This enables for more convenient number dialing within a complex, such as a campus with several Succession Call Servers. When configuring CDP numbers at the Gatekeeper, administrators must also specify to which CDP domain they belong.

Figure 31 on page 139 shows an example of CDP routing. Table 24 on page 140 shows the DNs with their associated Succession Call Server and CDP domain.

Figure 31
CDP call routing

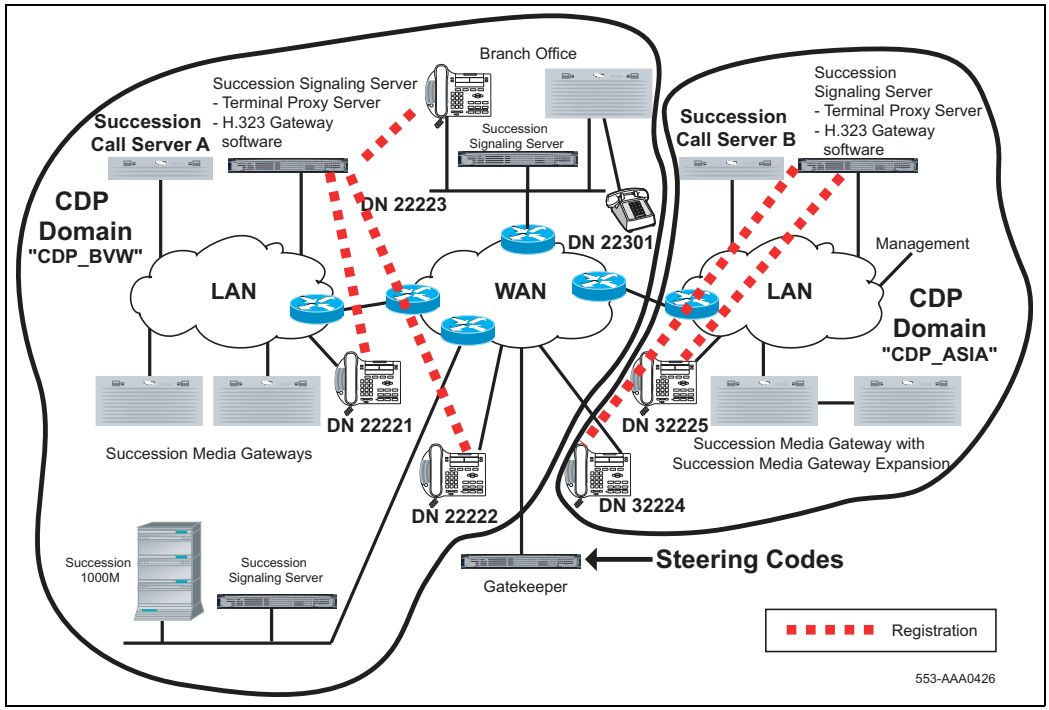


Table 24
DNs with their associated Succession Call Server and CDP domain

DN	Succession Call Server	CDP domain
22221	A	“CDP_BVW”
22222	A	“CDP_BVW”
22223	A	“CDP_BVW”
22301	Branch Office	“CDP_BVW”
32224	B	“CDP_ASIA”
32225	B	“CDP_ASIA”

UDP call routing operation

The routing of calls in a UDP private numbering plan is basically the same as that for Transferable Directory Number, except that only the Location Codes must be stored in the Gatekeeper, since the user uniquely identifies the specific location by dialing this code.

CDP and Transferable Directory Number numbering plans can co-exist within the same network. The dialing of a network access code (AC1 or AC2) enables the Succession Call Server to differentiate between calls that must be resolved using the UDP Type of Number (TON) and those that must be resolved using the CDP TON.

Note: Transferable Directory Numbers are considered CDP numbers.

Off-net call routing operation

When dialing calls to PSTN interfaces, the Succession Call Server determines that the call is destined off-net, based on digit analysis that must be configured at major Succession Call Servers in the network. This enables the Gateway software to request the location of public E.164 numbers from the Gatekeeper. The Gatekeeper is configured with a list of potential "alternate routes" that can be used to reach a certain number, each of which is configured with a Cost Factor to help determine the least-cost route for the call.

When a Gatekeeper replies to the H.323 Gateway with the address information for E.164 numbers, it provides a list of alternate gateways, sorted in order of cost. If a Gateway is busy when a call attempt is made, the originating Gateway tries the next alternative in the list. If none of the alternatives are available over the IP network, the originating Succession Call Server can be configured to step to the next member of its route list, which could be a PSTN or TIE alternate route.

For example, in the event of an IP network outage that does not enable voice calls to terminate over the IP network, calls are rerouted to any alternate PSTN or TIE routes.

Routing to and from a Branch Office H.323 WAN Gateway

Since Internet Telephone users can be located at a Branch Office equipped with a Branch Office Gateway, the routing of calls to the local gateway is important (especially when toll charges are applicable to calls made from the central Succession Call Server that is controlling the telephone). The administrator can configure digit manipulation for Internet Telephones that are located near a Branch Office H.323 WAN Gateway, in order to select a gateway that provides PSTN access local to the telephone.

Note: The Branch Office supports the various Succession 3.0 PSTN interfaces. Refer to *Electronic Switched Network: Signaling and Transmission Guidelines* (553-3001-180) for further information.

Calls from the PSTN to users within the network can either be routed using the various ESN numbering plan configurations, or can be routed using the Vacant Number Routing (VNR) feature. This enables small sites, such as those using the Branch Office H.323 WAN Gateway, to require minimal configuration to route calls through other Succession Call Servers or through the Gatekeeper.

Outgoing calls to access local PSTN resources can be routed using ESN, as well as zone parameters that enable digit insertion. The zone parameters enable calls made by a Branch Office user to be routed to the desired local PSTN facilities. Refer to *Branch Office* (553-3001-214) for further information.

Configuring IP Peer Networking

Contents

This section contains information on the following topics:

Description

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

- Command Line Interface (CLI)
- Element Manager

  Note: Element Manager has a set of dedicated webpages for maintaining the Gatekeeper

- Optivity Telephony Manager (OTM)

  Note: You can use OTM to launch Element Manager. Refer to *Optivity Telephony Manager: System Administration* (553-3001-330) for detailed information on OTM.

This chapter provides instructions on how to implement IP Peer Networking in your IP network. Gatekeeper functions are discussed in "Managing the Gatekeeper" on page 239.

For information on how to install system components and how to perform basic configuration, refer to

- *Small System: Installation and Configuration* (553-3011-210)
- *Large System: Installation and Configuration* (553-3021-210)
- *Succession 1000 System: Installation and Configuration* (553-3031-210)

For a description of system management, see *System Management* (553-3001-300).

For a detailed description of Element Manager, refer to *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232) and *Succession 1000 Element Manager: System Administration* (553-3001-332).

Once you have installed the various components and configured the basic information, you can then implement the IP Peer Networking feature. Implementing IP Peer Networking in a Succession 1000 or Succession 1000M network is similar to configuring a traditional circuit-switched network that uses a "star" topology. All Succession 1000 and Succession 1000M systems form the outer points of the star, with respect to address resolution (the systems form a grid with respect to media paths). These systems are configured to route network-wide calls into the IP network over a route configured with Virtual Trunks. The Virtual Trunks are configured to use the Gatekeeper. The Gatekeeper, in conjunction with the Gateway software at each site, acts as the center of the "star".

Element Manager and the Gatekeeper webpages in Element Manager enable you to configure and maintain certain aspects of the system through a web browser.

> ***Note 1:*** Element Manager must be installed on each Succession Signaling Server within the system.
>
> ***Note 2:*** Element Manager requires Internet Explorer 6.0.2600.

In addition to Element Manager and Gatekeeper webpages in Element Manager, you can perform a number of configuration functions through the Command Line Interface (CLI). You can access the CLI from a serial port, or by using the telnet or rlogin commands over a network connection.

You can also use OTM to access the web servers running on the Succession Signaling Server.

Task summary

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

1 Plan your Network Numbering Plan. Refer to *Dialing Plans: Description* (553-3001-183).

a Are you using Uniform Dialing Plan (UDP) or Coordinated Dialing Plan (CDP), or both?

b Are you also using Group Dialing Plan (GDP), North American Numbering Plan (NANP), or Flexible Numbering Plan (FNP)?

2 Perform basic installation, setup, and configuration of the various components, including the Succession Signaling Server. Refer to:

— *Small System: Installation and Configuration* (553-3011-210)

— *Large System: Installation and Configuration* (553-3021-210)

— *Succession 1000 System: Installation and Configuration* (553-3031-210)

— *Signaling Server: Installation and Configuration* (553-3001-212).

3 Configure the Primary, Alternate, and Failsafe Gatekeepers at installation and initial setup of the Succession Signaling Server. See *Succession 1000 System: Installation and Configuration* (553-3031-210).

Note: The Gatekeeper requires IP telephony node configuration files. These files are installed and configured during the Succession Signaling Server software installation (basic configuration step).

4 Configure the Customer Data Block with any desired networking settings and options, including ISDN. Use Element Manager or the Command Line Interface (LD 15). See “Configuring the Customer Data Block” on page 155 and “Feature Implementation” on page 219.

5 Configure the D-channel using Element Manager or the Command Line Interface (LD 17). See“Configuring D-channels” on page 159 and “Feature Implementation” on page 219.

6 Configure the zones.

7 Configure the Virtual Trunk routes using Element Manager or the Command Line Interface (LD 16). Configure the Route Data Blocks and associate the Virtual Trunk routes with the IP network by configuring the following parameters:

a route information

b network management information (for example, Access Restrictions)

c bandwidth zone

d protocol identifier

e associated Node ID

For the Element Manager procedure, see "Configuring the Virtual routes and trunks" on page 167. For the CLI procedure, see "Feature Implementation" on page 219.

8 Configure the Virtual Trunks using Element Manager (see "Configuring the Virtual routes and trunks" on page 167) or the Command Line Interface (LD 14) and "Feature Implementation" on page 219.

9 Use Element Manager or the Command Line Interface (CLI) to configure networking ("Configuring networking" on page 181) and numbering plan features ("Configuring call routing" on page 186) within the Succession Call Server, such as routing calls based on digits dialed. For example, CDP configuration for the dialing plan used on the Succession Call Server includes:

a ESN control block basics (LD 86): configure the dialing plan

b Network Control Block (LD 87): configure network access

c Route List Block (LD 86): create an entry for Virtual Trunk route

d Network Control Block (LD 15): enter CDP steering codes or UDP steering codes

10 Configure the codecs using Element Manager (see "Configuring codecs" on page 193).

11 Configure dialing plan information for calls that must be routed to circuit-switched trunks (for example, PSTN interfaces). See *Dialing Plans: Description* (553-3001-183) and *IP Trunk: Description, Installation, and Operation* (553-3001-363).

12 Enable the Gatekeeper using Element Manager, if not already enabled through the Signaling Server Install Tool. See "Enabling the Gatekeeper" on page 216.

Table 25 outlines the step required in setting up IP Peer Networking.

Table 25
Setting up the Succession 1000 and Succession 1000M Systems (Part 1 of 2)

Task	Refer to...
Plan your Network Numbering Plan.	*Dialing Plans: Description* (553-3001-183).
Perform basic installation, setup, and configuration of the various Succession 1000 components, including the Succession Signaling Server.	*Small System: Installation and Configuration* (553-3011-210) *Large System: Installation and Configuration* (553-3021-210) *Succession 1000 System: Installation and Configuration* (553-3031-210) *Signaling Server: Installation and Configuration* (553-3001-212)
Configure the Primary, Alternate, and Failsafe Gatekeepers at installation and initial setup of the Succession Signaling Server.	*Succession 1000 System: Installation and Configuration* (553-3031-210)
Configure the Customer Data Block with any desired networking settings and options, including ISDN. Use Element Manager or the Command Line Interface (LD 15).	"Configuring the Customer Data Block" on page 155 "Feature Implementation" on page 219.
Configure the D-channel using Element Manager or the Command Line Interface (LD 17).	"Configuring D-channels" on page 159 "Feature Implementation" on page 219.

Table 25
Setting up the Succession 1000 and Succession 1000M Systems (Part 2 of 2)

Task	Refer to...
Configure the Virtual Trunk routes using Element Manager or the Command Line Interface (LD 16). Configure the Route Data Blocks and associate the Virtual Trunk routes with the IP network by configuring the following parameters: • route information • network management information (for example, Access Restrictions) • bandwidth zone • protocol identifier • associated Node ID	"Configuring the Virtual routes and trunks" on page 167 for the Element Manager procedure. "Feature Implementation" on page 219 for the CLI procedure.
Configure the Virtual Trunks	"Configuring the Virtual routes and trunks" on page 167) for the Element Manager procedure. (LD 14) and "Feature Implementation" on page 219 for the Command Line Interface.
Configure networking and numbering plan features within the Succession Call Server, such as routing calls based on digits dialed.	"Configuring networking" on page 181 "Configuring call routing" on page 186
Configure the codecs using Element Manager	"Configuring codecs" on page 193
Configure dialing plan information for calls that must be routed to circuit-switched trunks (for example, PSTN interfaces).	*Dialing Plans: Description* (553-3001-183) and *IP Trunk: Description, Installation, and Operation* (553-3001-363)
Enable the Gatekeeper using Element Manager, if not already enabled through the Signaling Server Install Tool.	"Enabling the Gatekeeper" on page 216

Launching Element Manager

To log in to Element Manager, follow the steps in Procedure 1. Element Manager supports Microsoft Internet Explorer 6.0.2600 for the Windows operating systems.

Procedure 1
Launching Element Manager

1 Open the web browser.

2 Enter the **Succession Signaling Server Node IP address** in the Address Bar of the browser window and press **Enter** on the keyboard.

Note: The ELAN IP address may be required, instead of the Node IP address, to access to the Element Manager login webpage in secure environments.

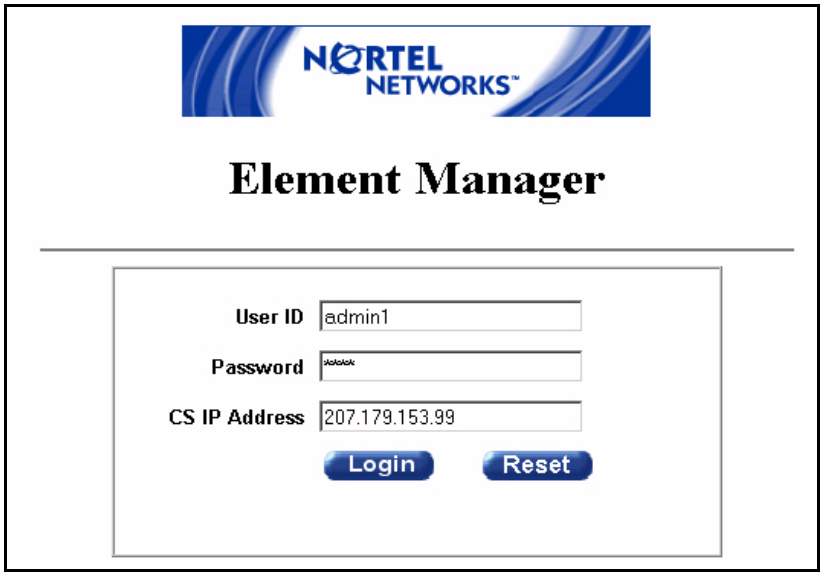
3 Element Manager opens and the **Login** webpage displays (see Figure 32 on page 152).

a. Enter the **User ID** and **Password** of the Succession Call Server.

The IP Address of the Succession Call Server is auto-filled in the **CS IP Address** field.

b. Click the **Login** button.

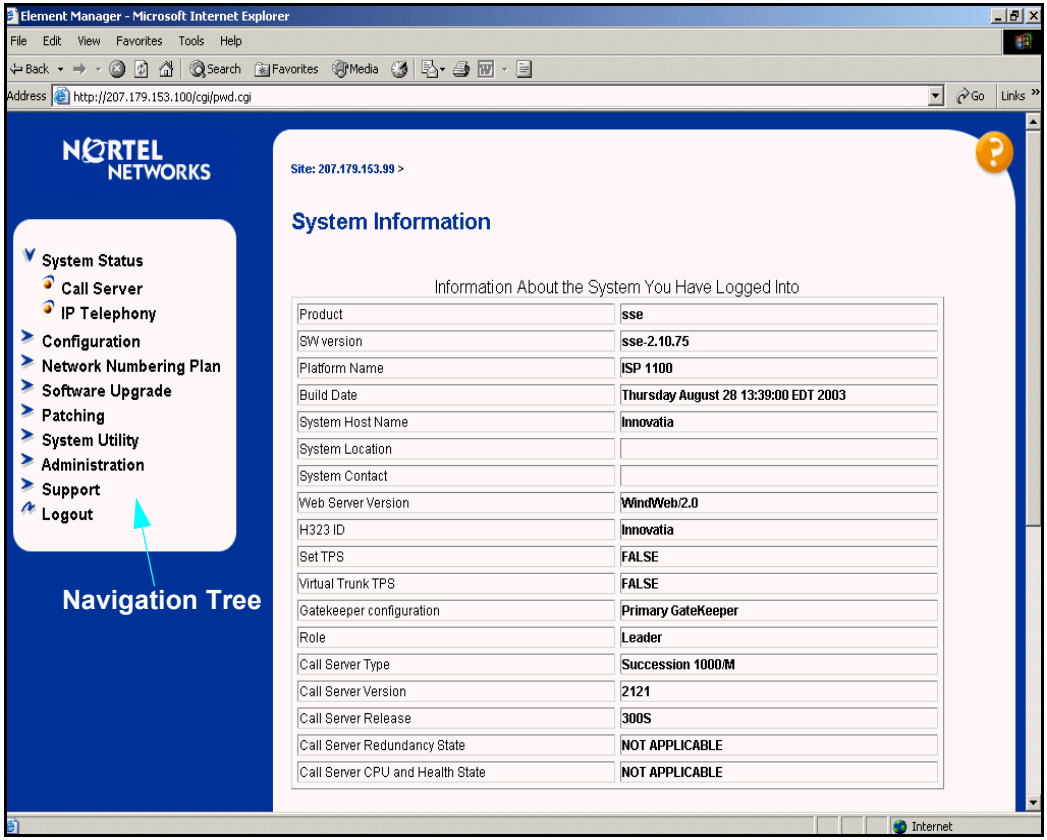
Figure 32
Element Manager–Login webpage



4 The **System Information** webpage displays (see Figure 33 on page 153).

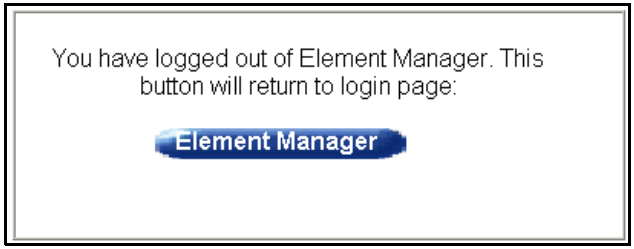
The **Navigation Tree** is located on the left side of the browser window. The **System Status** menu is expanded in Navigation Tree.

Figure 33
Element Manager–System Information



Note 1: To log out of Element Manager, click **Logout** at the bottom of the Navigation Tree. Figure 34 shows the message that is displayed when you log out. If you need to log back in to Element Manager, click the **Element Manager** button and you are returned to the **Login** screen (see Figure 32 on page 152).

Figure 34
Logged out of Element Manager



Note 2: Element Manager times out after a period of inactivity.

Users are logged out without any warning in all Element Manager webpages, with the exception of the **Edit** webpage (see Figure 69 on page 194). When you are working in the Edit webpage, a message displays that warns of the impending time-out action. Click the **OK** button (on the warning message) within the remaining time-out period (5 minutes) to reset the timer. If you do not respond within the 5 minute warning period, your session is cancelled and you must log in again. Any data modifications made on screen, but not submitted to the system, are lost.

Note 3: For additional information about Element Manager, refer to the following NTPs:

— *Succession 1000 Element Manager: Installation and Configuration* (553-3001-232)

— *Succession 1000 Element Manager: System Administration* (553-3001-332)

End of Procedure

Using Element Manager for configuration

Use the following sections in consecutive order.

Configuring the Customer Data Block

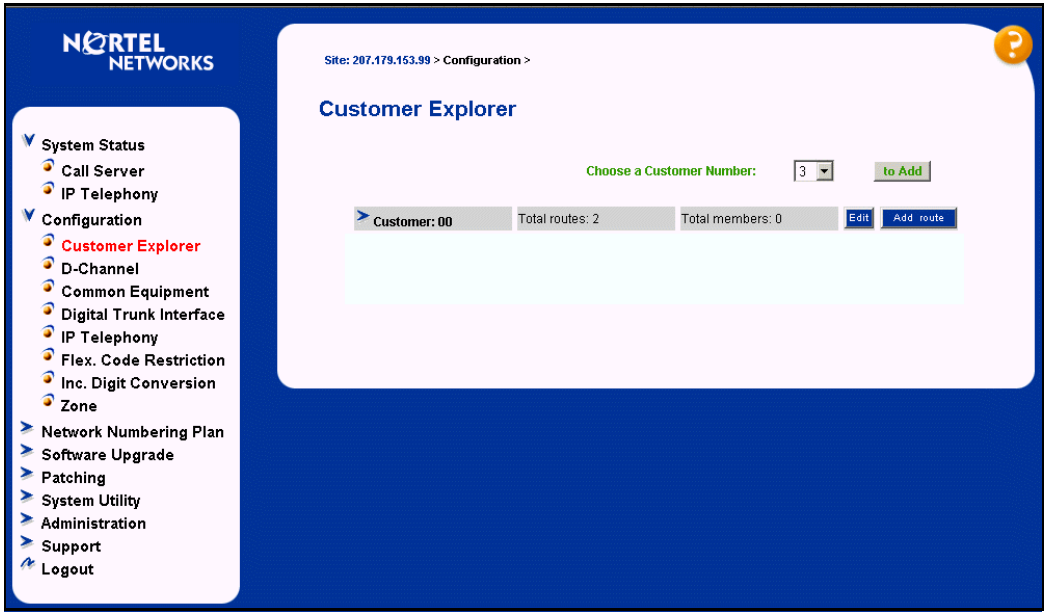
Procedure 2
Configuring the Customer Data Block and enable ISDN

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

1 Select **Configuration | Customer Explorer** from the Navigation Tree.

The **Customer Explorer** webpage displays as in Figure 35.

Figure 35
Customer Explorer

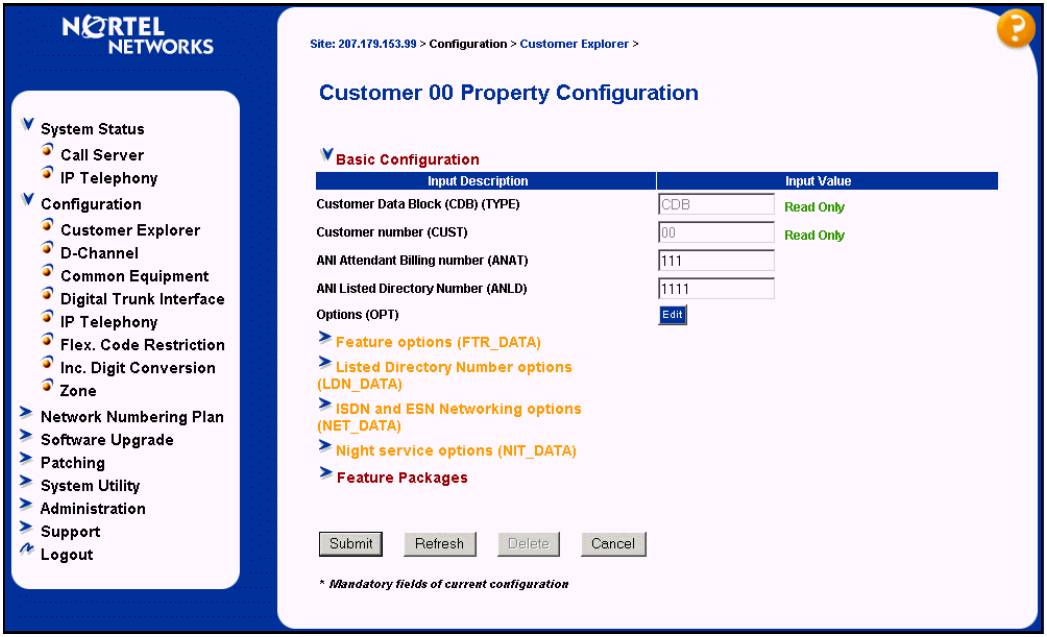


2 Click the **Edit** button associated with the customer (not the route) to open the **Customer xx Property Configuration** webpage where xx is the Customer number.

Figure 36 shows the Customer xx Property Configuration webpage.

3 Use the Customer Property Configuration webpage to configure Customer data.

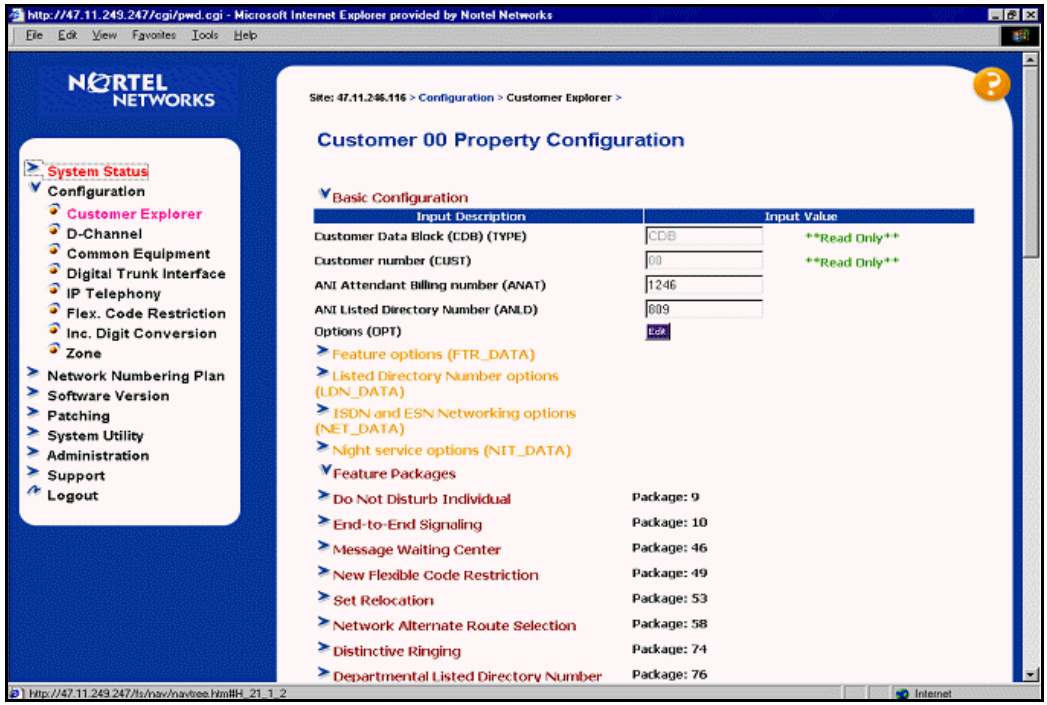
Figure 36
Customer xx Property Configuration webpage



4 Click **Feature Packages**.

The Feature Packages list expands as shown in Figure 37 on page 157.

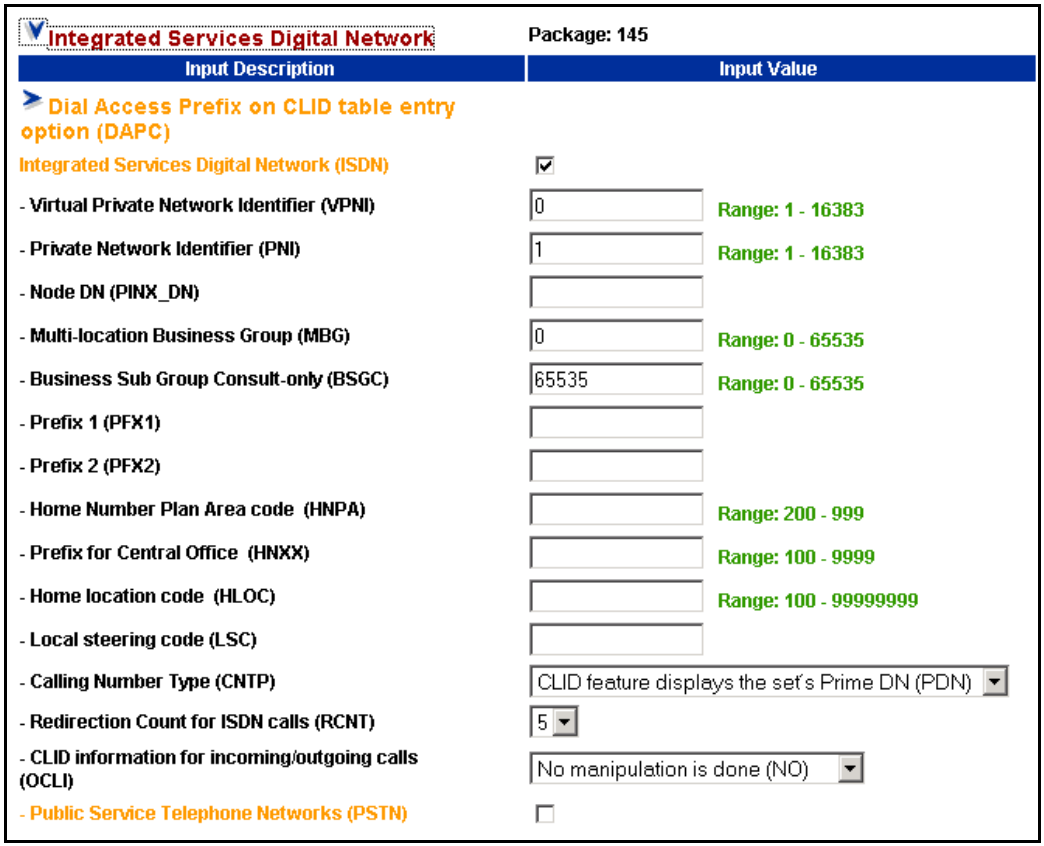
Figure 37
Customer Properties Feature Packages list



5 Scroll down the page and click **Integrated Services Digital Network Package:145**.

6 Check the **Integrate Services Digital Network (ISDN)** check box (see Figure 38 on page 158).

Figure 38
ISDN package options



7 Scroll to the bottom of the page and click the **Submit** button.

End of Procedure

Configuring D-channels

Procedure 3
Configuring D-channels

To configure D-channels, use Element Manager or LD 17 of the Command Line Interface.

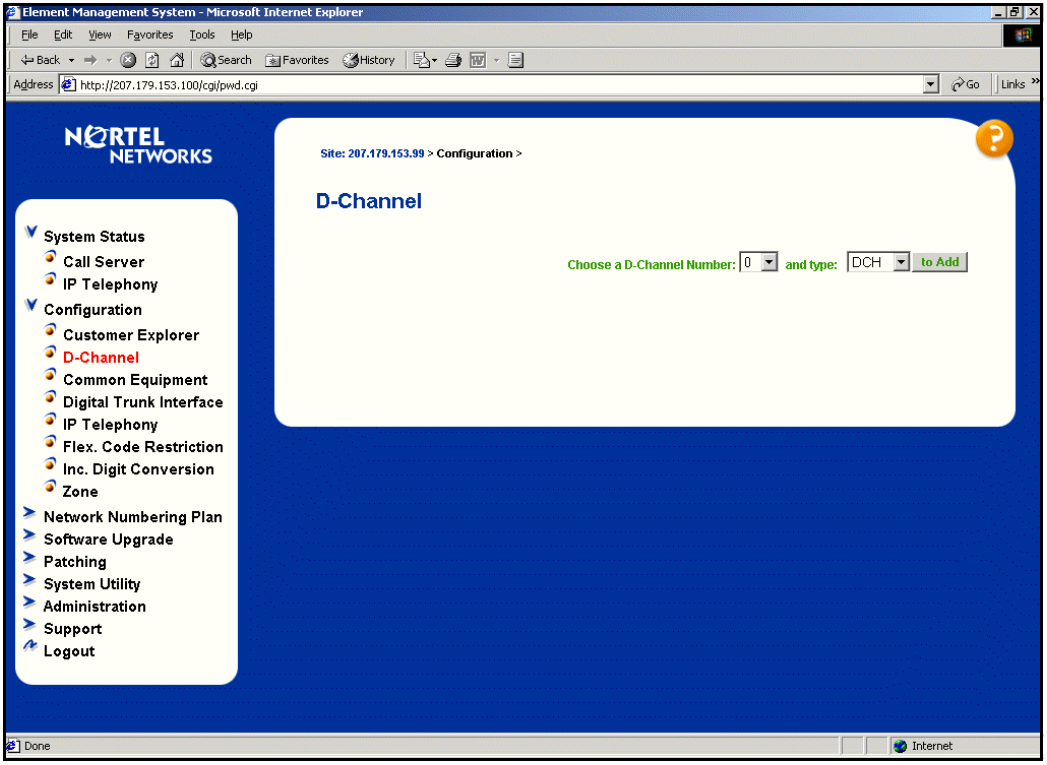
Figure 39 on page 160 and Figure 40 on page 161 show the D-Channel Configuration webpages in Element Manager. Use these webpages to configure D-channels.

1 Select **Configuration | D-Channel** from the Navigation Tree.

Note: The first time you access this screen, a message indicates that no D-channels have been configured.

The **D-Channel** screen displays as shown in Figure 39 on page 160.

Figure 39
D-Channel Configuration webpage



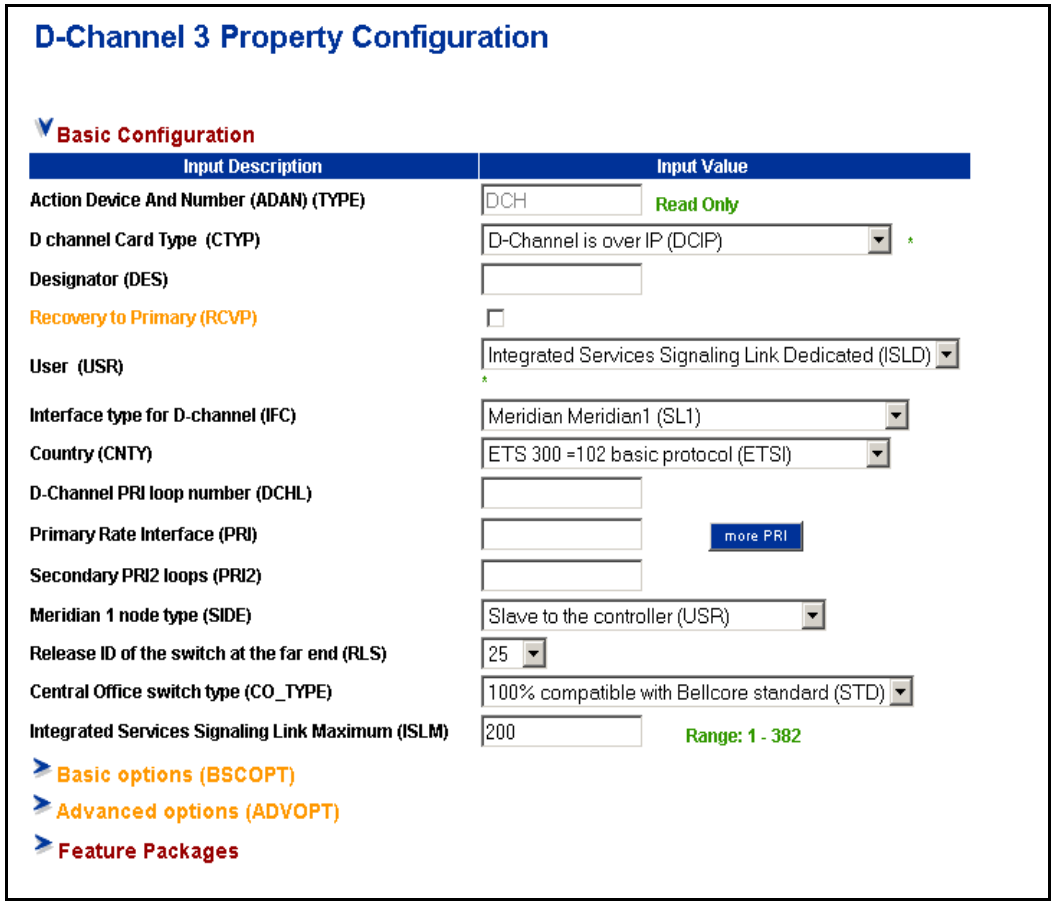
2 Input the D-channel number and click the **to Add** button.

The **D-Channel xx Property Configuration** screen displays as shown in Figure 40 on page 161.

Note 1: The D-Channel number is denoted by xx.

Note 2: Required fields are indicated with a green asterisk.

Figure 40
D-channel configuration webpage



3 Configure the following fields with the following values:

a. **D channel Card Type (CYTP)** = D-Channel is over IP (DCIP)

b. **User (USR)** = Integrated Services Signaling Link Dedicated (ISLD)

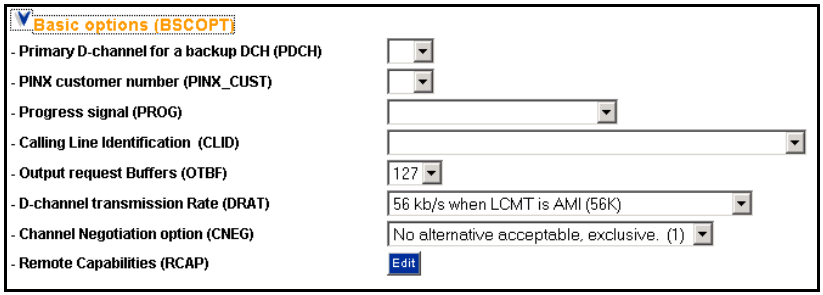
c. **Interface type for D-channel (IFC)** = Meridian Meridian1 (SL1)

4 If you are defining the Network Name Display:

a. Select the **Release ID of the switch at the far end (RLS)** from the drop-down list box.

b. Open the **Basic options (BSCOPT)** tab (see Figure 41).

Figure 41
D-channel - Basic options



c. Configure **Remote Capabilities (RCAP)** by clicking on the **Edit** button.

The **Remote Capabilities Configuration** webpage displays.

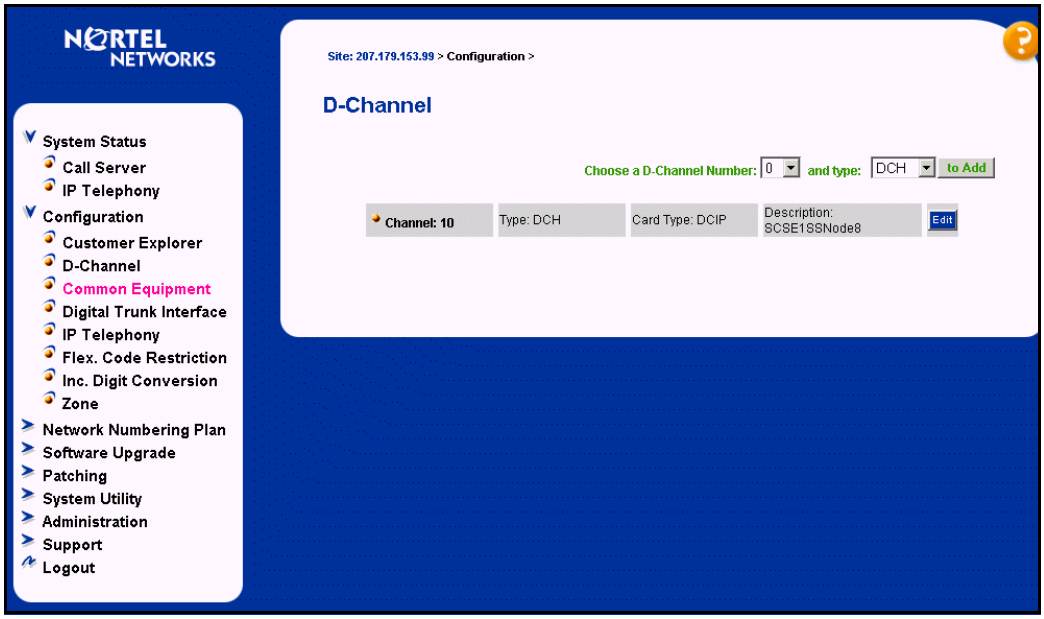
d. Scroll down the page and click the check box for **Network name Display method 2 (ND2)**.

e. Click the **Return - Remote Capabilities** button at the bottom of the page.

The **D-Channel xx Property Configuration** screen redisplays.

5 Click the **Submit** button to save the changes. The D-Channel screen redisplays (Figure 42 on page 163) with the changes.

Figure 42
D-channel configuration results



End of Procedure

Configuring zones

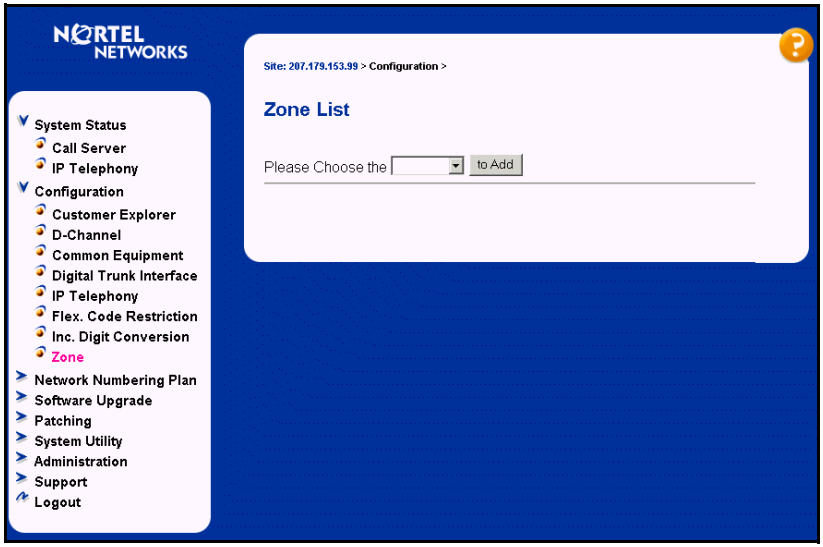
A zone is an area of a network that can be treated as a single entity with respect to the use of bandwidth for voice and signaling. Zones must be configured before the configuration of virtual routes.

Procedure 4
Configuring zones

1 Select **Configuration** | **Zone** from the Navigation Tree.

The **Zone List** pages displays (see Figure 43).

Figure 43
Zone List

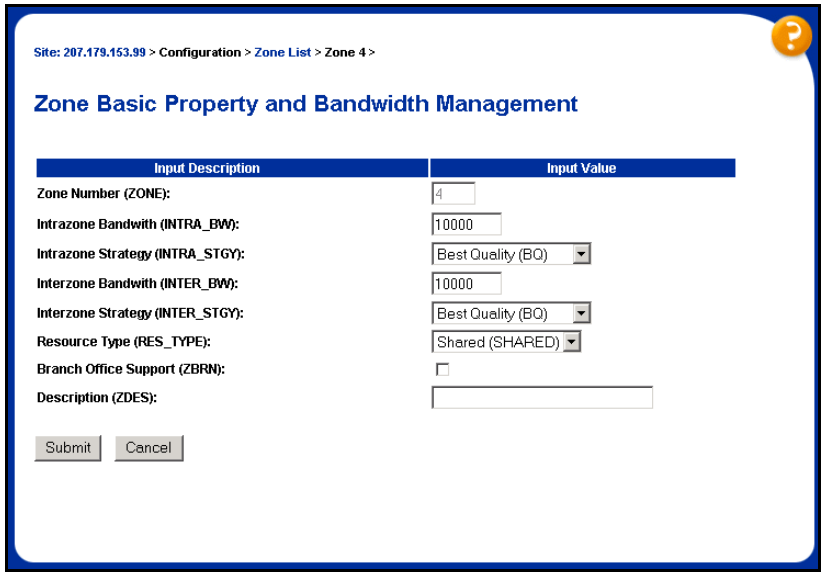


2 Choose a zone number from the drop-down list box.

3 Click the **to Add** button.

4 The **Zone Basic Property and Bandwidth Management** webpage displays (see Figure 44 on page 165).

Figure 44
Zone Basic Property and Bandwidth Management



Note: The **Zone Number (ZONE)** field is auto-filled based on the number selected on the Zone List webpage.

5 Enter the **Intrazone Bandwidth (INTRA _BW)**.

6 Select the **Intrazone Strategy (INTRA _STGY)** from the drop-down list box.

7 Enter the **Interzone Bandwidth (INTER _BW)**.

8 Select the **Interzone Bandwidth (INTER _BW)** from the drop-down list box.

9 Select the **Resource Type (RES_TYPE)** from the drop-down list box.

10 Enter a description of the zone in the **Description (ZDES)** text box.

11 Click the **Submit** button.

The Zone List redisplays and the new zone has been added (see Figure 45 on page 166).

Figure 45
Zone List with newly added zone

End of Procedure

Configuring the Virtual routes and trunks

Procedure 5
Configuring Virtual Trunk routes

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

Figures 46 shows the New Route Property webpage in Element Manager. Use this webpage to configure Virtual Trunk routes.

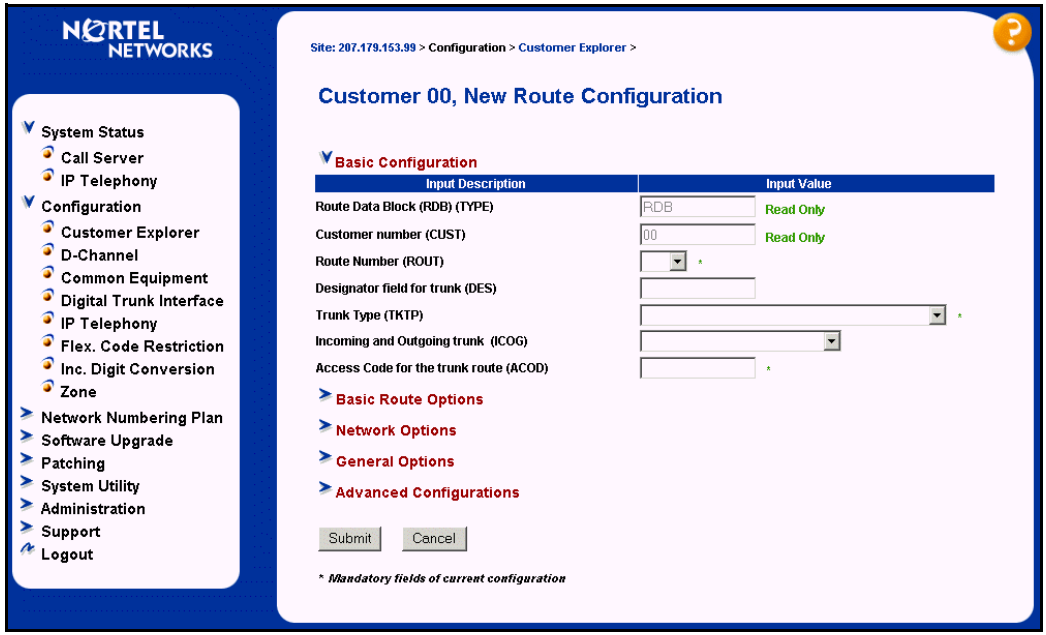
Note: The zone parameter makes the codec selections and calculates the bandwidth usage for calls to the trunk members of a given route.

1 Select **Configuration | Customer Explorer** from the Navigation Tree.

2 Click the **Add route** button associated with the customer.

The **Customer xx, New Route Configuration** webpage displays (where xx is the customer number). See Figure 46.

Figure 46
New Route Configuration webpage



3 Under **Basic Configuration**, fill in the required fields to create a new Virtual Trunk Route:

a. Select a **Route Number (ROUT)** from the drop-down list box.

b. Select the **Trunk Type (TKTP)** = TIE trunk data block (TIE).

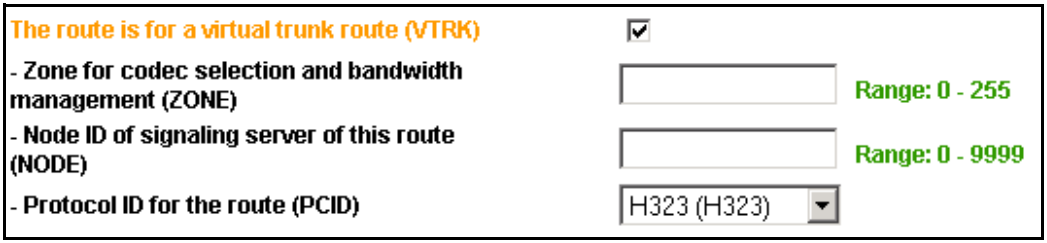
When TIE is select, the following three options appear:

- The route is for a virtual trunk route (VTRK)
- Digital Trunk Route (DTRK)
- Integrated Services Digital Network option (ISDN)

4 Check the box for **The route is for a virtual trunk route (VTRK)**.

Three fields display as shown in Figure 47.

Figure 47
Virtual trunk route



a. Enter a **ZONE** number.

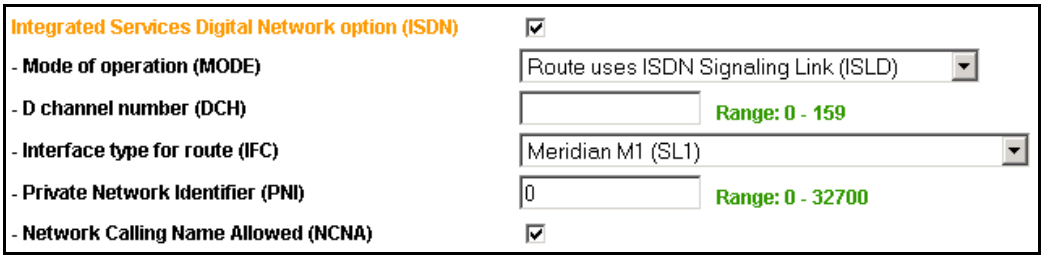
b. Enter the **NODE** ID (the node served by this Succession Signaling Server).

c. Confirm the Protocol ID for the route (**PCID**) = H32 (H323) (autofilled).

5 Check the box for **Integrated Services Digital Networks option (ISDN)**.

Four options are display as shown in Figure 48 on page 169.

Figure 48
ISDN option



a. Choose **MODE** = Route uses ISDN Signaling Link (ISLD).

b. Input the D channel number **(DCH)**.

c. Choose Interface type for route **(IFC)** = Meridian M1 (SL1).

d. Check the box for Network Calling Name Allowed **(NCNA)**.

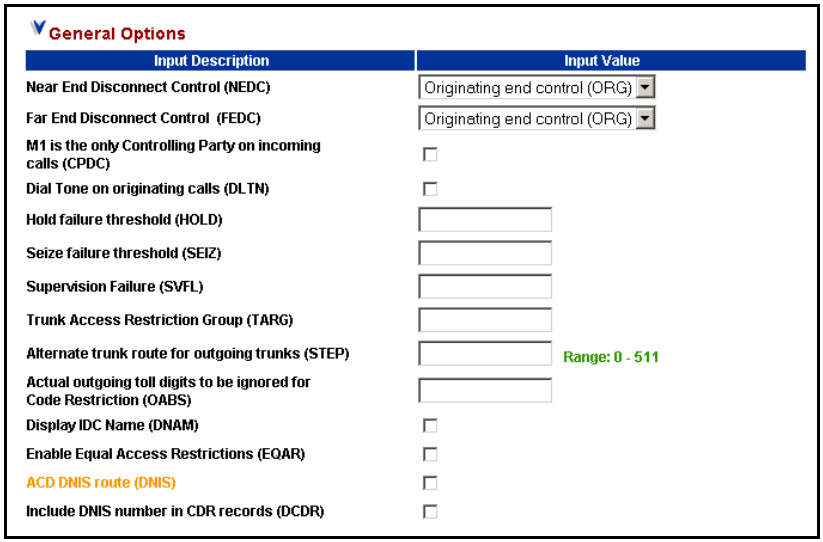
6 Check the box for Network Call Redirection **(NCRD)** (see Figure 49).

Figure 49
NCRD

7 Scroll up to the top of the page and enter the **Access Code for the trunk route (ACOD)**.

8 Click on **General Options** (see Figure 50 on page 170).

Figure 50
General Options



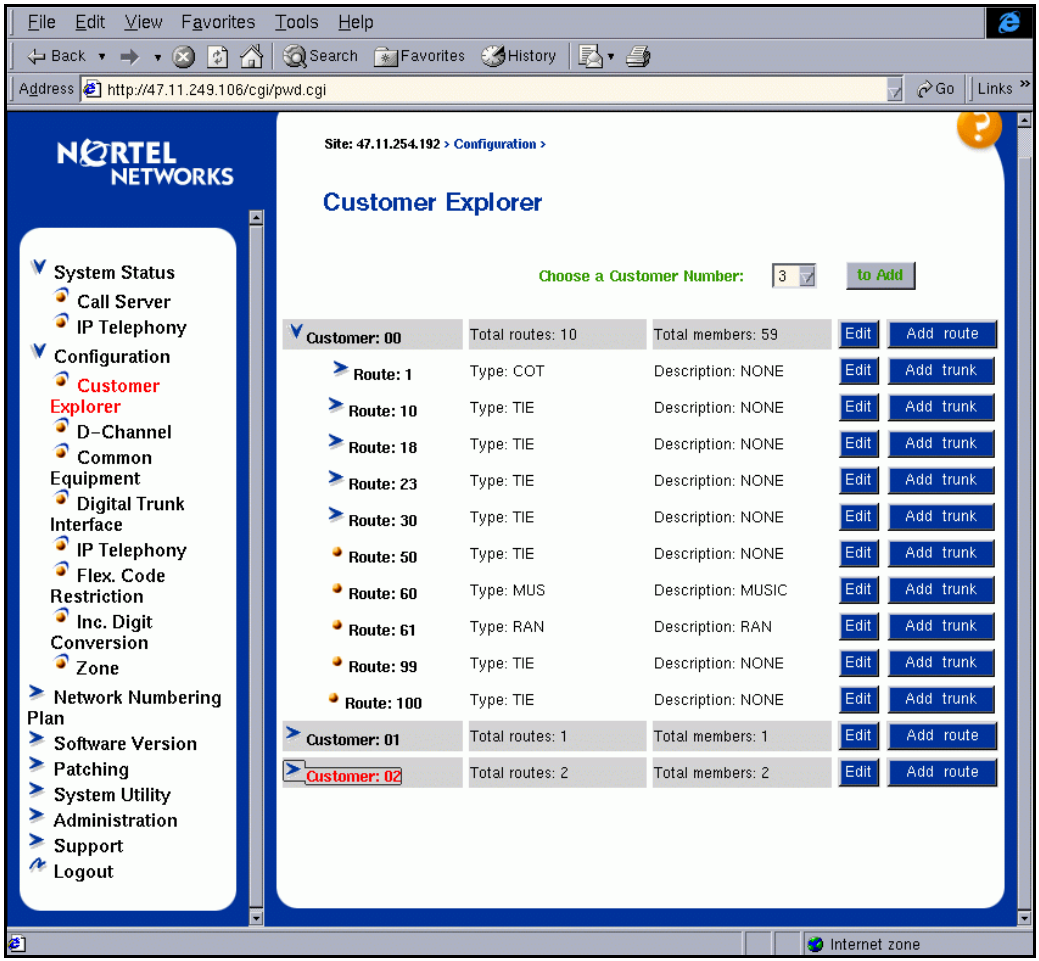
9 Enter the **Trunk Access Restriction Group (TARG)** value if you are configuring a single customer.

10 Enter the appropriate information in the text boxes and in **Basic Route Options**, **Network Options**, **General Options**, and **Advanced Configurations**.

11 Click the **Submit** button.

The **Customer Explorer** webpage displays as shown in Figure 51 on page 171. The newly configured route is displayed for the customer.

Figure 51
Result



End of Procedure

Configure virtual superloops for Internet Telephones (LD 97)

One or more virtual superloops must be configured to support Internet Telephone Virtual TNs (VTNs).

Large Systems

In Large Systems, virtual superloops contend for the same range of loops with phantom, standard and remote superloops, digital trunk loops and all service loops. Virtual superloops can reside in physically-equipped network groups or in virtual network groups.

Group maximums

Without FIBN, Package 365, there is a maximum of five network groups available, 0 – 4. With Package 365, there are a maximum of eight network groups, 0 – 7. For normal traffic engineering, provision up to 1024 VTNs on a single virtual superloop for a Large System. For non-blocking, do not exceed 120 VTNs on a single virtual superloop for a Large System.

Nortel Networks recommends that virtual superloops are configured starting in the highest non-physically equipped group available. Table 26 on page 173 lists the prompts and responses required to configure virtual superloops in LD 97.

Table 26
LD 97 – Configure virtual superloop for Large Systems.

Prompt	Response	Description
REQ	CHG	Change
TYPE	SUPL	Superloop
SUPL	Vxxx	V stands for a virtual superloop and xxx is the number of the virtual superloop xxx = 0 – 156 and multiple of four for a Large System without FIBN package 365 xxx = 0 – 252 and multiple of four for a Large System with FIBN package 365 xxx = 96 – 112 and multiple of four for a Small System and Succession 1000 system

Small Systems

In Small Systems, virtual superloops contend for the same range of superloops, 96 – 112, with phantom superloops.

Up to 128 VTNs can be configured on a single virtual superloop for a Small System, for a maximum number of 640 VTNs in each system.

In a Small System, mapping virtual superloops to virtual cards is the same as mapping phantom superloops to phantom cards. See Table 27 on page 174.

Table 27
Virtual superloop/virtual card mapping for Small Systems

SUPL	Card
96	61-64
100	65-68
104	69-72
108	73-76
112	77-80

Succession 1000 systems

Table 28 on page 174 lists the virtual superloop and virtual card mapping for the Succession 1000 system.

Table 28
Virtual superloop/virtual card mapping for Succession 1000 Systems

SUPL	Card	
96	61-64	81-84
100	65-68	85-88
104	69-72	89-92
108	73-76	93-96
112	77-80	97-99

LD 97 PRT TYPE SUPL prints the implicit virtual, phantom, or DECT cards for a virtual, phantom, or DECT superloop.

LD 21 LUU allows the user to list unused units of a specified type (iset, vtrk, phantom, DECT) in a specified range of (virtual, and so on) TNs. Similarly, LUC of a specified type (virtual, phantom, or DECT) prints a list of unused cards on configured superloops.

Procedure 6
Configuring Virtual Trunks

To configure Virtual Trunks in Element Manager, use the “New Member Property” pages.

Figures 52 to 54 show the New Member Property webpage in Element Manager. Use this webpage to configure Virtual Trunks.

1 Select **Configuration | Customer Explorer** from the Navigation Tree.

The **Customer Explorer** webpage displays.

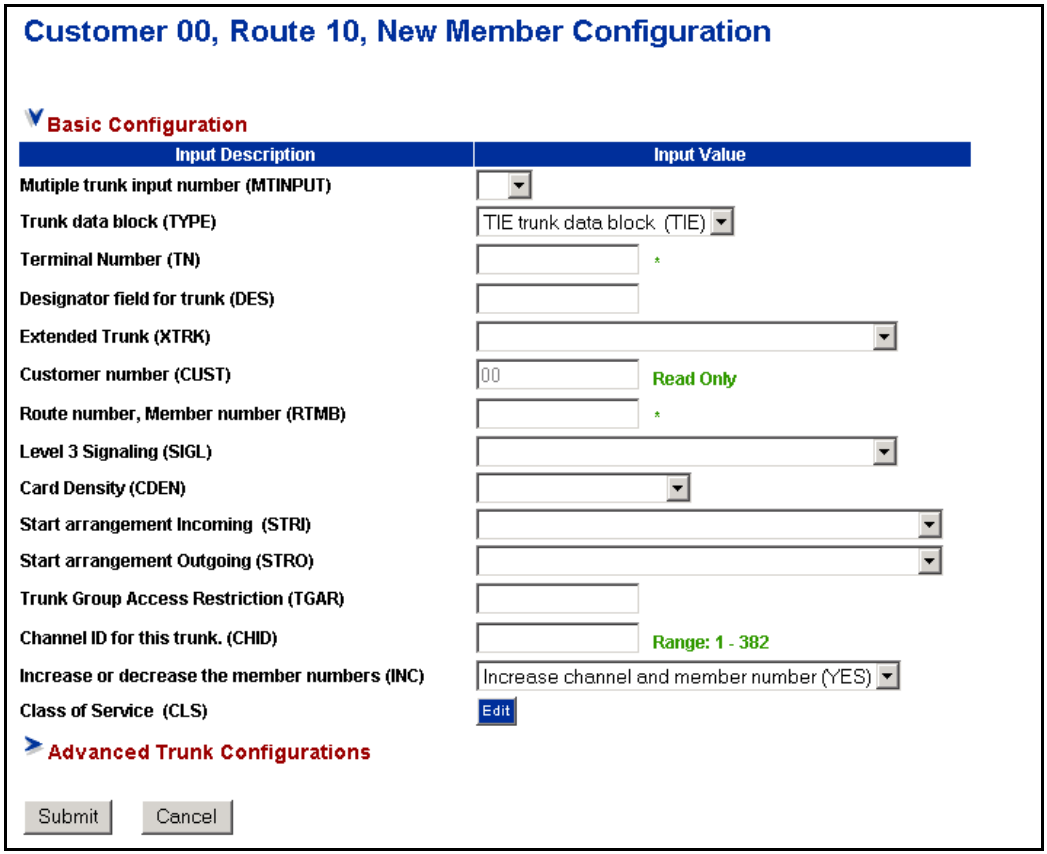
2 Click on the **Customer** for which you are configuring Virtual Trunks.

The customer list expands showing a list of configured routes (see Figure 51 on page 171).

3 Click the **Add trunk** button associated with route listing to add trunk members.

The **Customer xx, Route yy, New Member Configuration** webpage displays. The customer number is represented by xx and the route number by yy (see Figure 52 on page 176).

Figure 52
New Member Property webpage



4 Choose **Multiple trunk input number (MTINPUT)** if you are using more than one trunk.

Note: Designator field for trunk (DES) is a text string only, and has no impact on functionality.

5 Select **Trunk data block (TYPE)** = Tie trunk data block (TIE).

6 Select **Extended Trunk (XTRK)** = Virtual trunk (VTRK).

7 Set the **Trunk Group Access Restriction (TGAR)** value.

8 Set **Channel ID for this trunk (CHID)** = x (where x is in the range of 1-382).

Note 1: With ISL trunking, the traditional relationship, where CHID of the trunk at Site A must equal the CHID of the far end trunk at Site B, is no longer required. It is no longer point-to-point.

Note 2: Channel_ID: A numeric input is required. However, there is no requirement for the CHID of Site A to match the CHID of Site B, as required with traditional ISDN Signaling Link (ISL) trunking.

9 Fill the required fields:

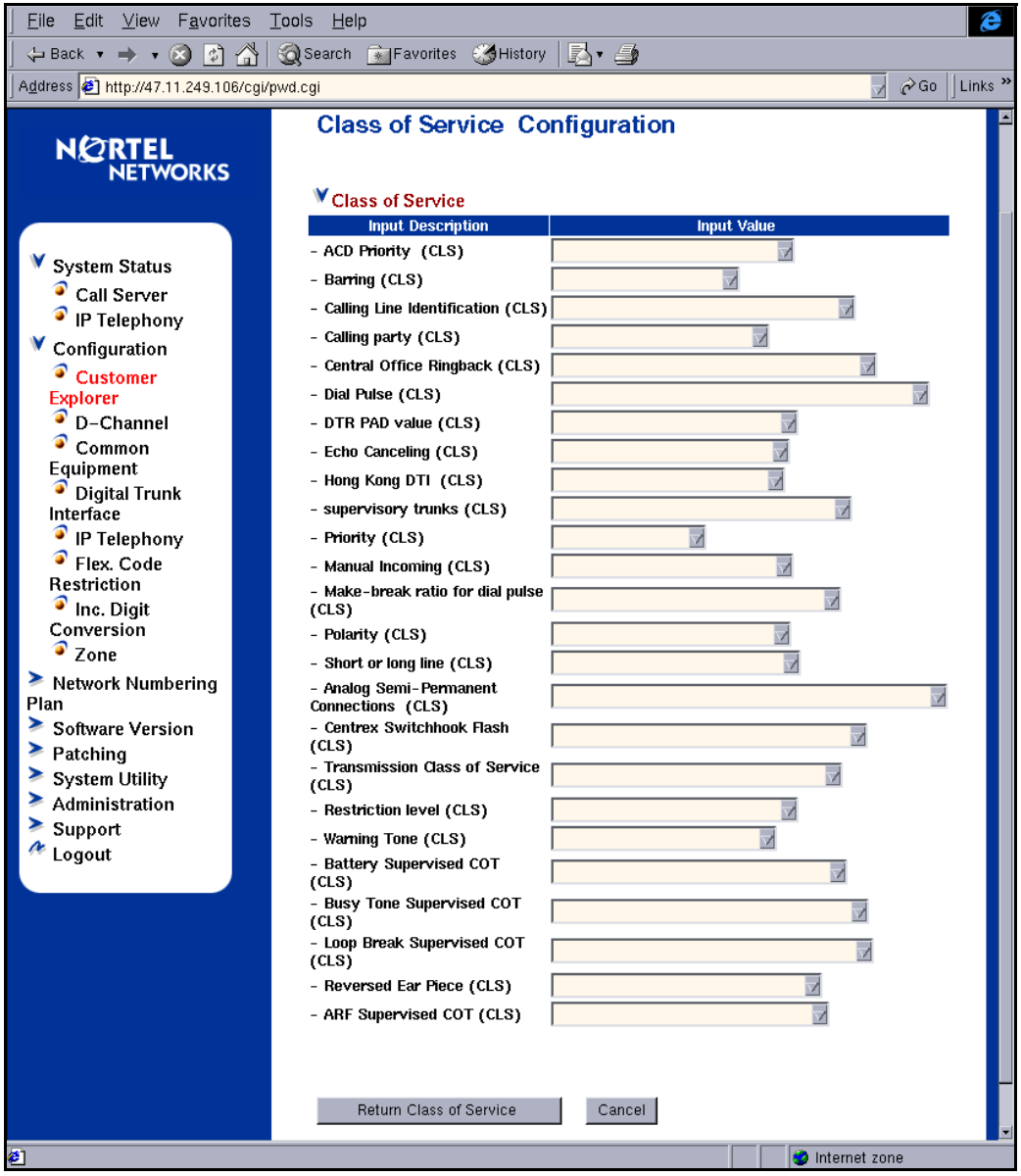
a. Terminal Number (TN)

b. Route Number, Member Number (RTMB)

10 To specify a **Class of Service (CLS)** for the trunk, click the **Edit** button.

The **Class of Service Configuration** pages displays (see Figure 53 on page 178). Select a Class of Service.

Figure 53
New Member Property webpage (continued)–Class of Service Configuration

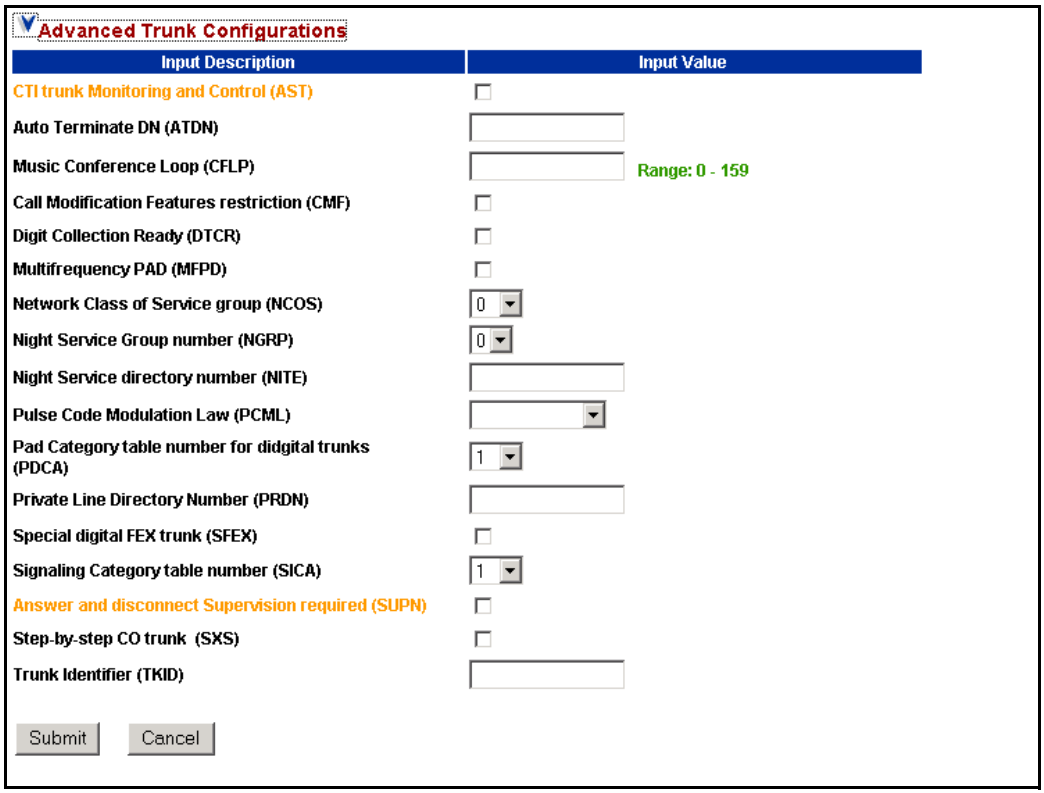


11 Select the Class of Service and then click the **Return Class of Service** button to return to the **New Member Configuration** webpage (Figure 52 on page 176).

12 Select **Advanced Trunk Configurations** (Figure 54).

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

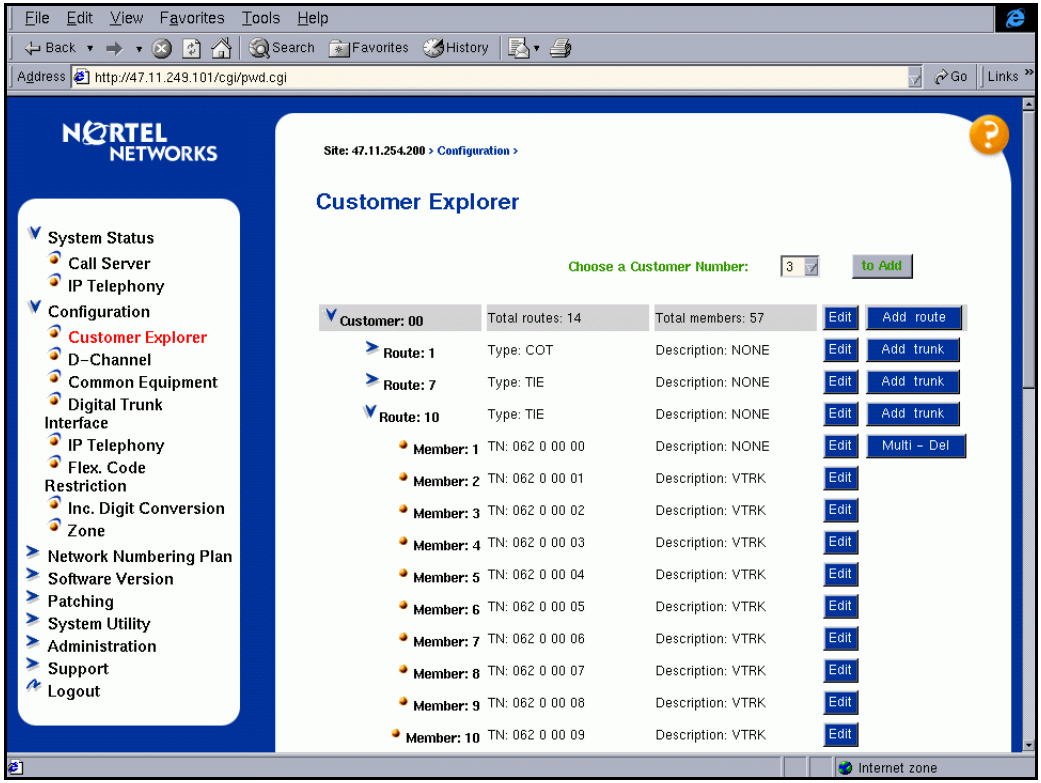
Figure 54
New Member Property webpage (continued)–Advanced Trunk Configuration



14 Click the **Submit** button to save the changes.

The **Customer Explorer** webpage redisplays showing the new trunk member (see Figure 55 on page 180).

Figure 55
Virtual Trunk routes



End of Procedure

Configuring networking

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

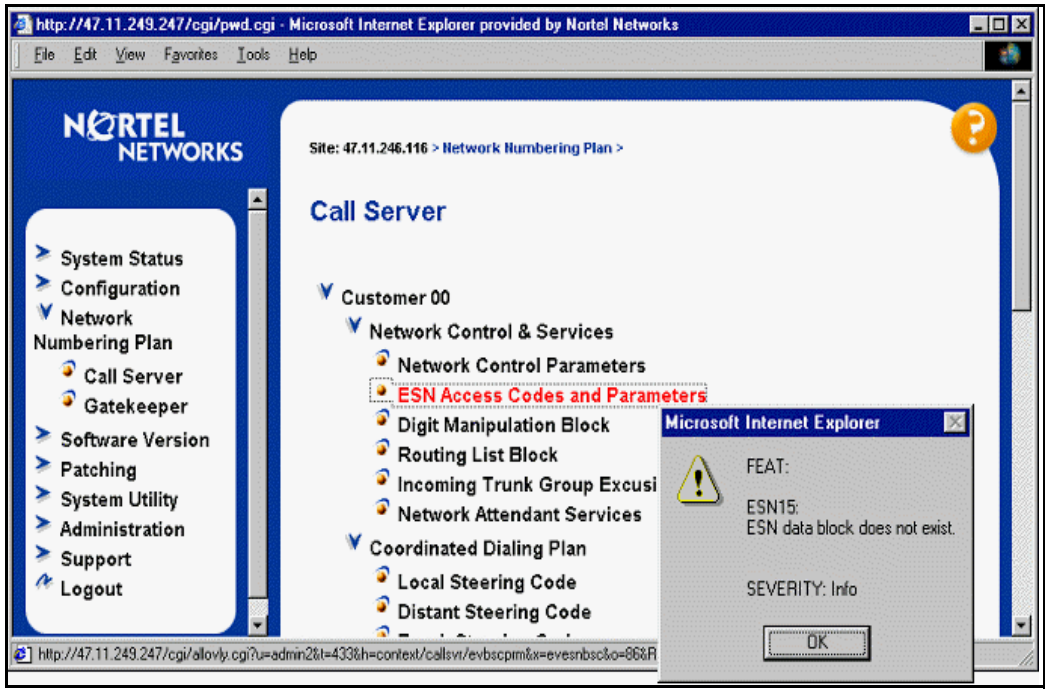
Procedure 7
Creating an ESN control block

1 Select **Networking Numbering Plan | Call Server** from the Navigation Tree.

The **Call Server** webpage displays (see Figure 56).

2 Under Network Control & Service, click **ESN Access Codes and Parameters (ESN)**.

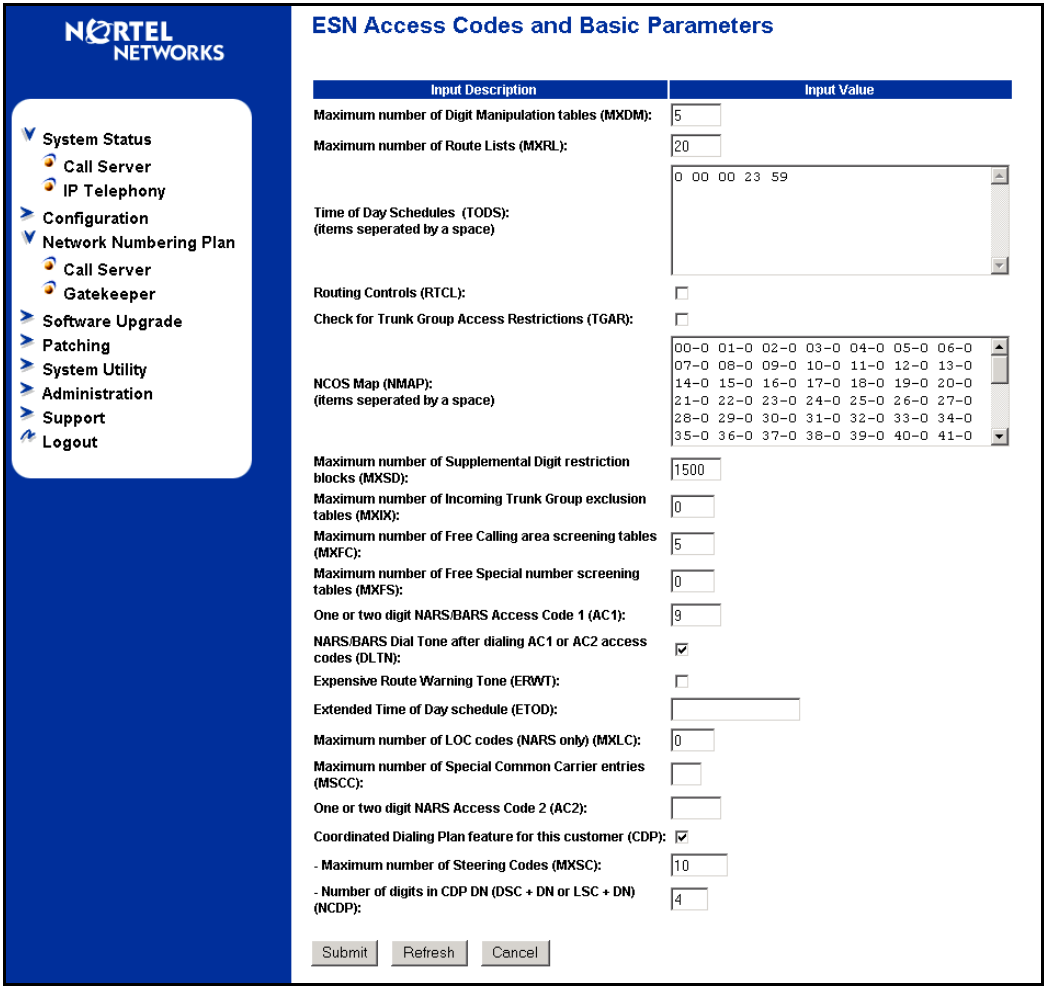
Figure 56
No ESN data block configured



3 If no ESN database is configured, a warning dialog box displays (Figure 56 on page 181). Click **OK** on the warning dialog box. The screen in Figure 57 displays.

If an ESN database is configured, the **ESN Access Codes and Basic Parameters** webpage displays (see Figure 57).

Figure 57
ESN data block configuration



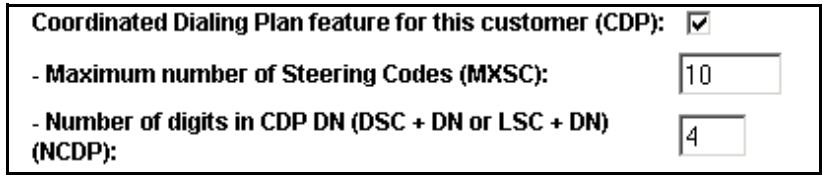
4 Define the parameters for the network. Include the **Maximum number of Route Lists (MXRL)**.

5 Scroll down the page and check the **Coordinated Dialing Plan feature for this customer (CDP)** checkbox (see Figure 58 on page 183).

   a. Configure the number of CDP steering codes (**Maximum number of Steering Codes (MXSC)**).

   b. Configure the number of digits of the CDP dialed number (**Number of digits in CDP DN (DSC + DN or LSC + DN) (NCDP)**).

Figure 58
ESN data block configuration (continued) – Coordinated Dialing Plan



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

The **Call Server** webpage redisplays (Figure 56 on page 181), this time without a warning dialog.

End of Procedure

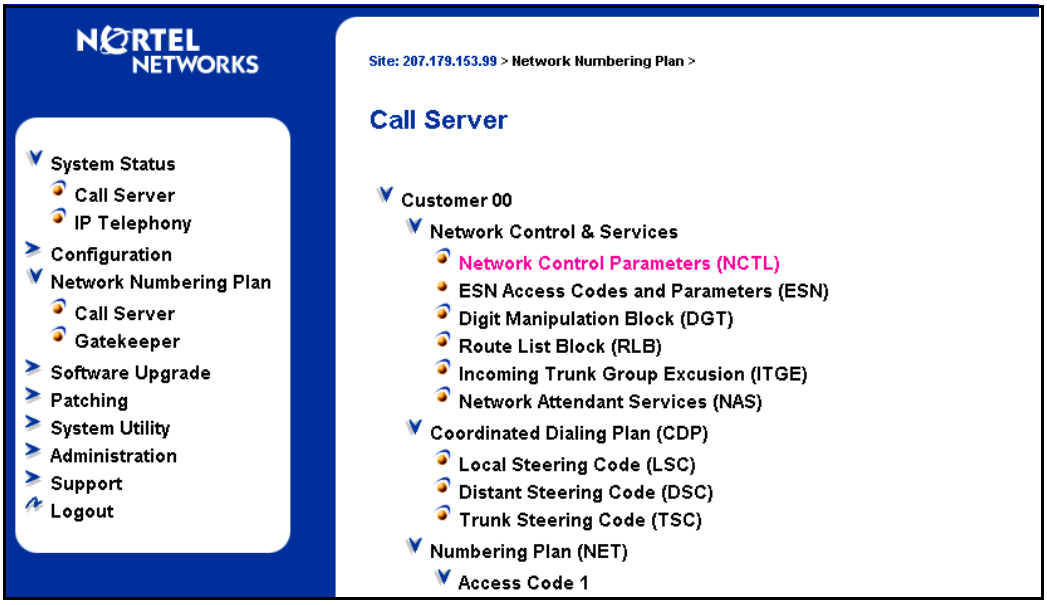
Procedure 8
Configuring network access

The default parameters for Network Control must be turned on.

1 Select **Network Numbering Plan | Call Server** from the Navigation Tree.

2 On the Call Server webpage, under Customer | Network Control & Service, select **Network Control Parameters (NCTL)**, as shown in Figure 59.

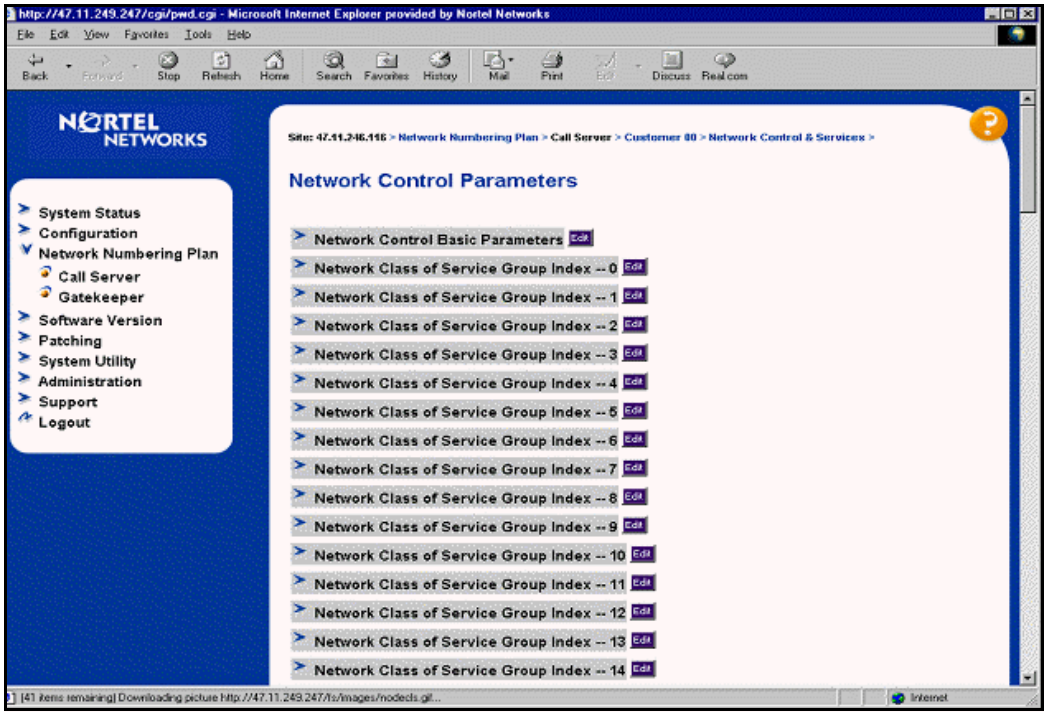
Figure 59
Network Control and Services



The **Network Control Parameters** webpage displays (see Figure 60 on page 185).

3 Click the **Edit** button to the right of **Network Control Basic Parameters** (see Figure 60).

Figure 60
Network Control Parameters webpage



The **Network Control Basic Parameters** webpage displays.

4 Accept the default parameters on the Network Control Basic Parameters webpage (Figure 60 on page 185) by clicking the **Submit** button at the bottom of the page.

The **Network Control Basic Parameters** webpage redisplays.

5 Scroll to the bottom of this page (Figure 60 on page 185) and accept the default Network Control Parameters by clicking **Submit**.

End of Procedure

Configuring call routing

Procedure 9
Configuring the Route List Block

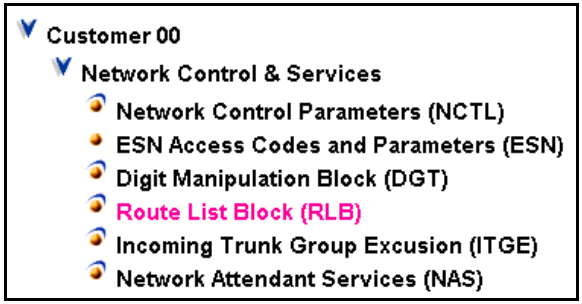
This procedure creates the Route List Block that routes calls over the Virtual Trunk route.

1 Select **Network Numbering Plan | Call Server** from the Navigation Tree.

The **Call Server** webpage displays.

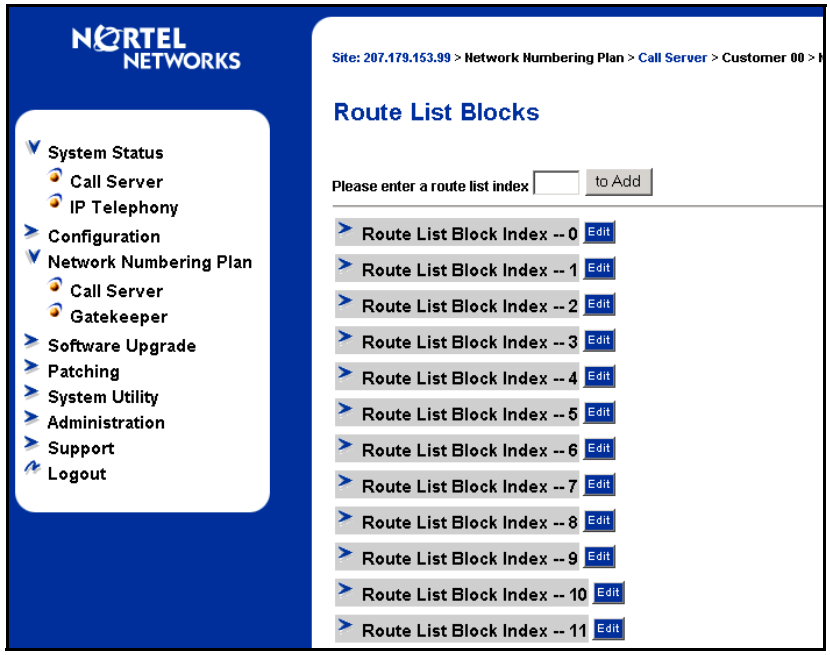
2 Under **Customer | Network Control & Services**, select **Route List Block (RLB)** (see Figure 61).

Figure 61
Route List Block (RLB)



The **Route List Blocks** webpage displays (see Figure 62 on page 187).

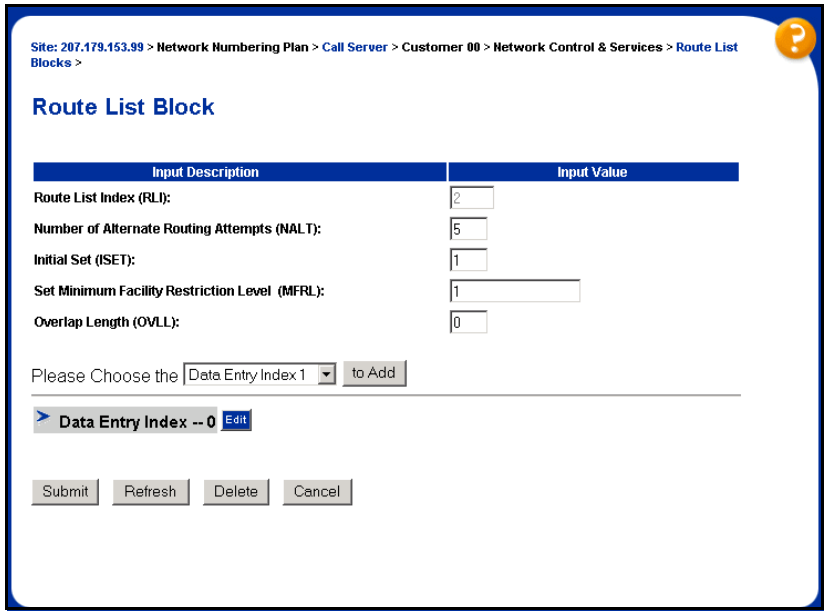
Figure 62
Route List Blocks



3 Enter the route list index number in the **Please enter a route list index** text box and click the **to Add** button.

The **Route List Block** webpage displays (see Figure 63 on page 188).

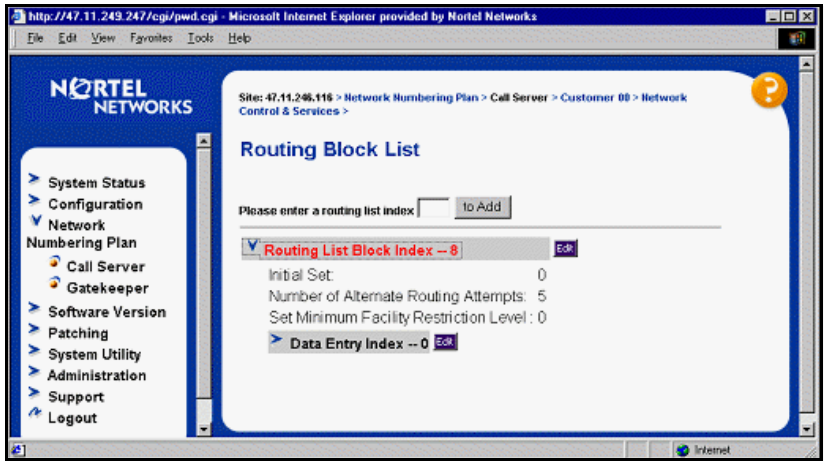
Figure 63
Route List Block



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

The new Route List Block is generated, and the initial Route List Blocks webpage redisplays (Figure 63 on page 188).

Figure 64
Resulting Route List Block



End of Procedure

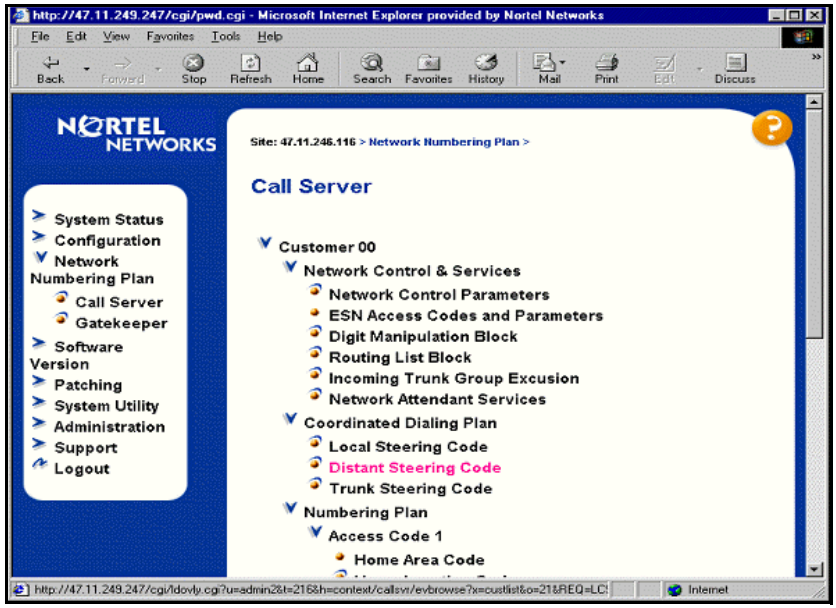
Procedure 10
Configuring Steering Codes

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

1 Select **Network Numbering Plan | Call Server** from the Navigation Tree.

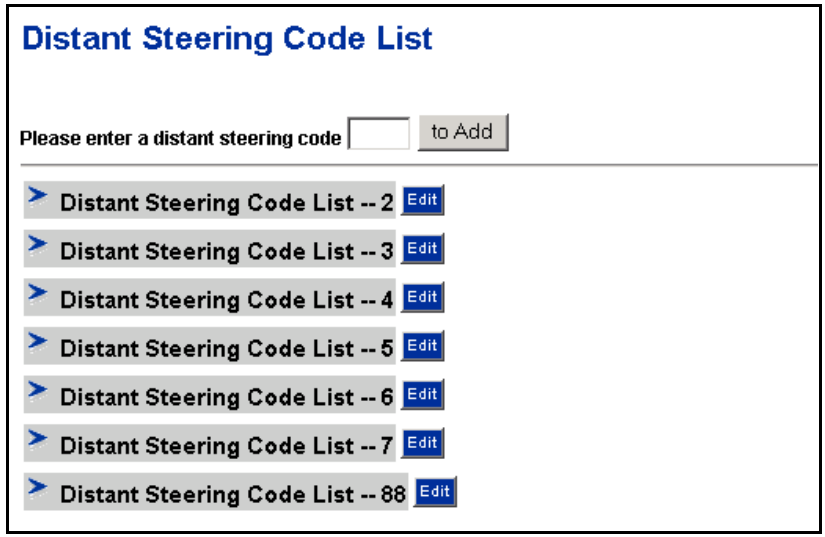
2 Under **Customer | Coordinated Dialing Plan (CDP)**, select **Distant Steering Codes (DSC)** (see Figure 65 on page 190).

Figure 65
Distant Steering Code



The **Distant Steering Code List** webpage displays. See Figure 66 on page 191.

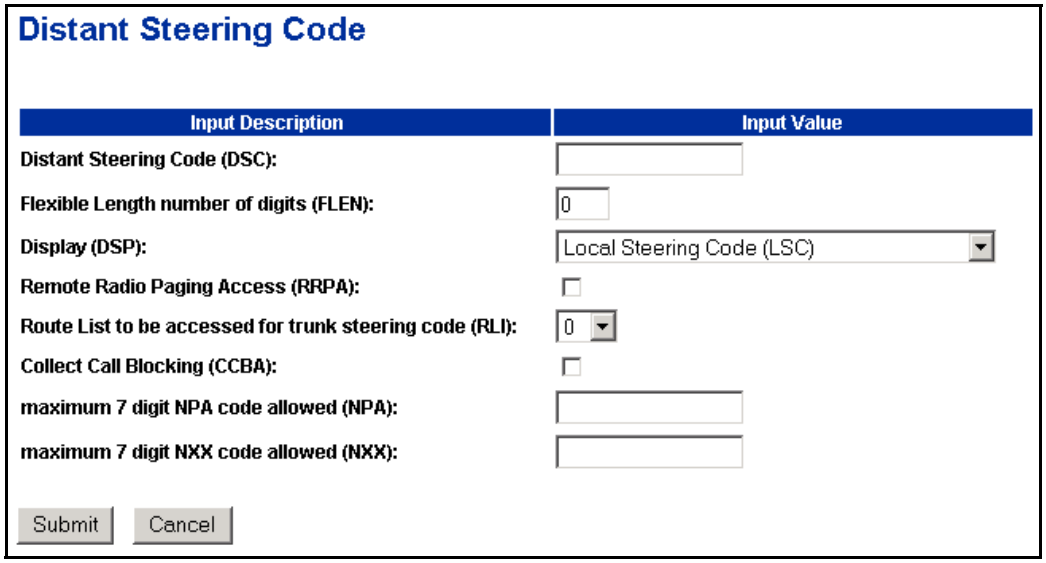
Figure 66
DIstant Steering Code List



3 Enter the steering code in the **Please enter a distant steering code** text box (Figure 66) and click the **to Add** button.

The **Distant Steering Code** webpage displays (see Figure 67 on page 192).

Figure 67
Distant Steering Code parameters



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

The Distant Steering Code List redisplays.

End of Procedure

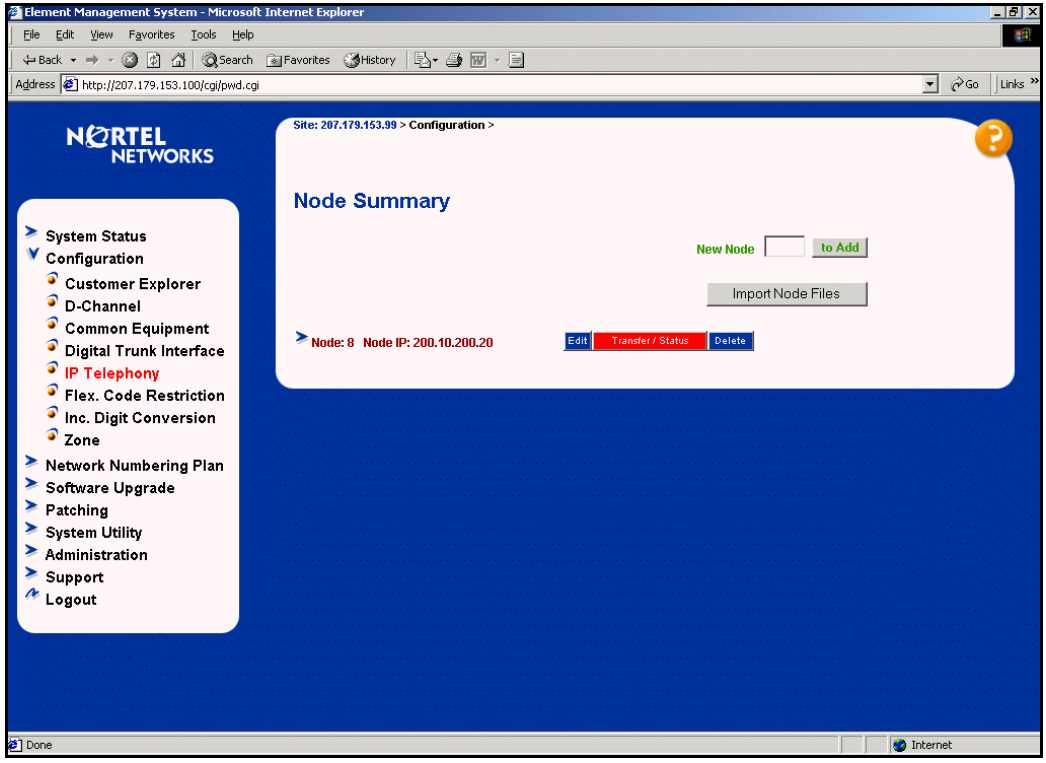
Configuring codecs

Procedure 11
Configuring codecs

1 Select **Configuration | IP Telephony** from the Navigation Tree.

The **Node Summary** webpage displays (see Figure 68).

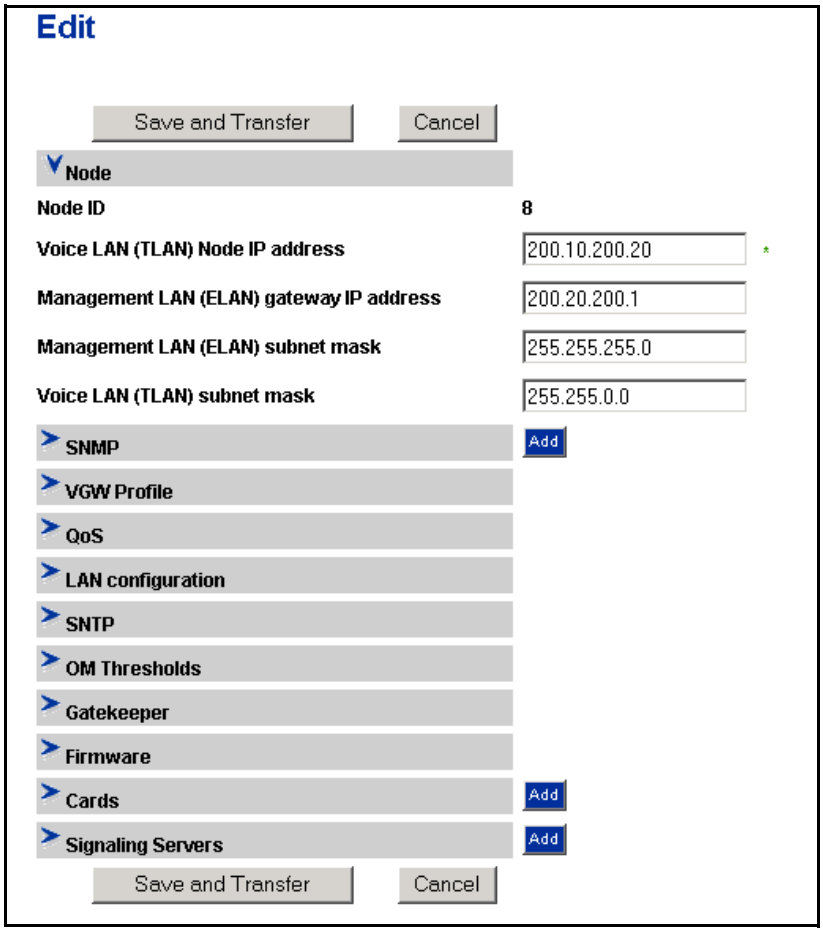
Figure 68
Node Summary



2 Click the **Edit** button.

The **Edit** webpage displays as shown in Figure 69.

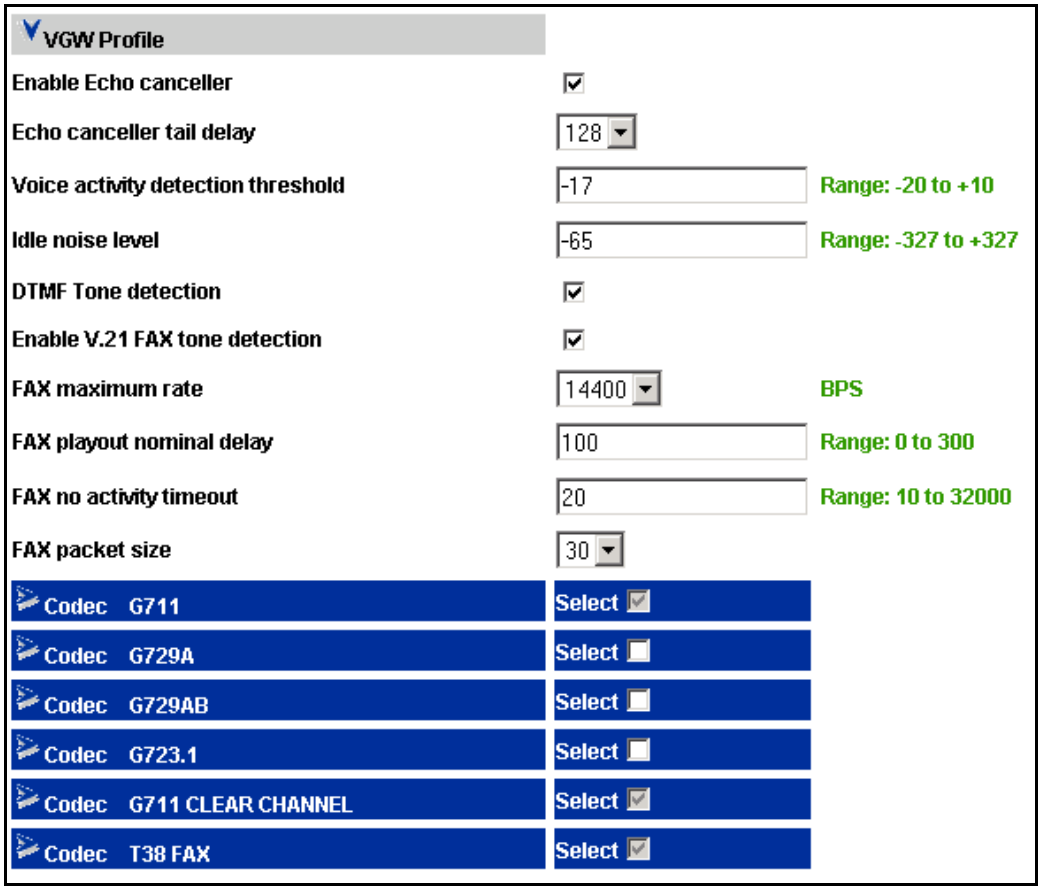
Figure 69
Edit



3 Click on **VGW Profile** to open its parameters as shown in Figure 70.

This area includes VGW Profile information and a list of codecs.

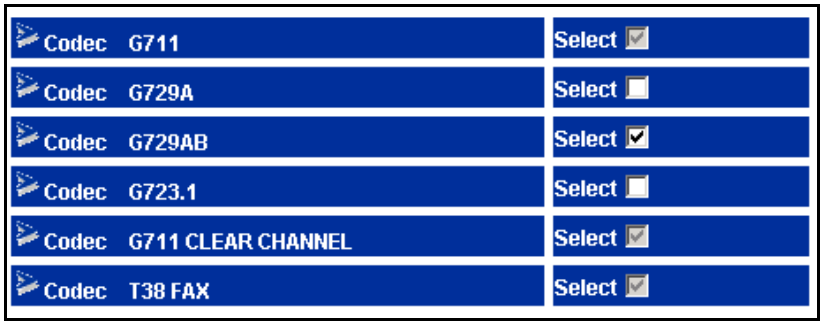
Figure 70
VGW Profile



4 To configure a codec, check the **Select** box to the right of the codec name. For example, in Figure 71 the G.729AB codec has been selected.

Note: The G.711, G.711 CLEAR CHANNEL, and T38 FAX codecs are automatically selected.

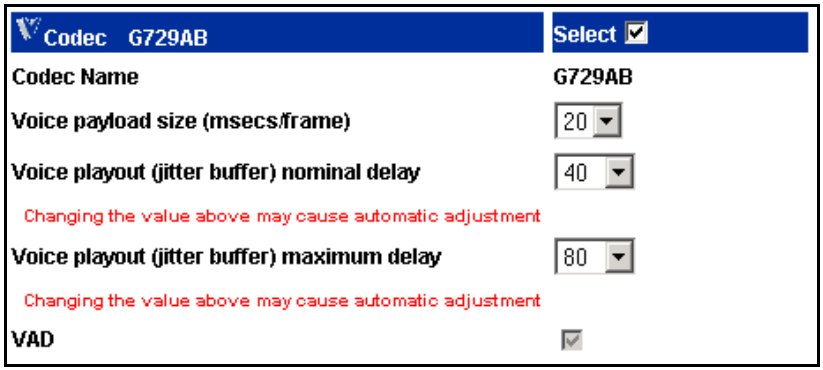
Figure 71
Example of a selected codec—G.729AB



5 Click on the codec name to modify the **Voice payload size (ms/frame)**, **Voice playout (jitter buffer) nominal delay**, and **Voice playout (jitter buffer) maximum delay** values of a codec.

Use the drop down lists to choose the values. See the example in Figure 72.

Figure 72
Example of G.729AB



6 Repeat step 4 and step 5 for each codec that needs configuration.

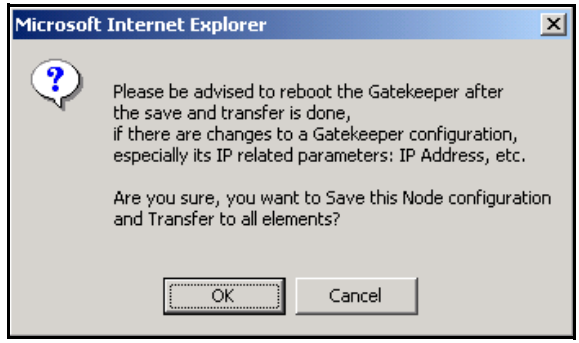
Note: For detailed information about configuring codecs, refer to *Data Networking for Voice over IP* (553-3001-160) and *IP Line: Description, Installation, and Operation* (553-3001-365).

7 Click the **Save and Transfer** button.

This saves the changes and transfers the node configuration files to all elements in the node (that is, the Succession Signaling Servers, Call Server, and Voice Gateway Media Cards).

A warning dialog box displays for rebooting the Gatekeeper if its parameters are changed (Figure 73).

Figure 73
Save and Transfer dialog box—reboot the Gatekeeper



8 Click the **OK** button.

A series of pages may display including the following:

- Transfer Progress webpage (see Figure 74 on page 198)
- Transfer Failure Report webpage (if applicable)
- Transfer / Status webpage (see Figure 75 on page 198) (This webpage shows if the transfer was successful or not, and allows the node information to be transferred again.)

Figure 74
Transfer Progress

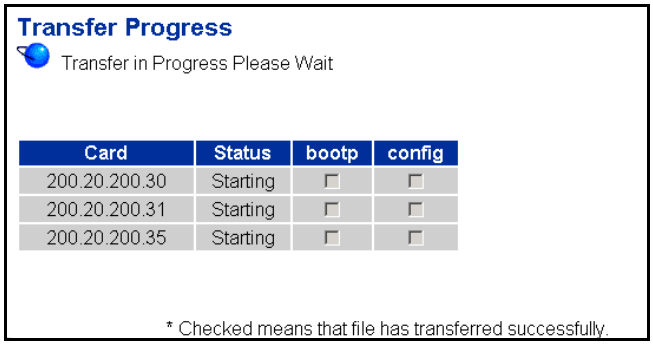
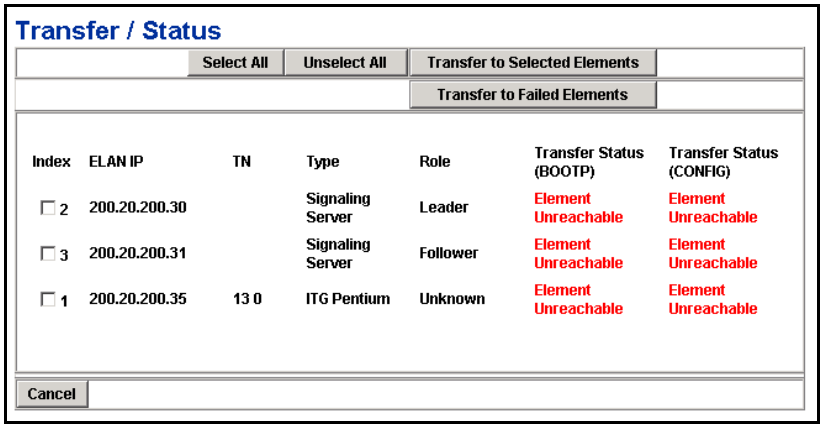


Figure 75
Transfer / Status



The Node Summary webpage (Figure 68 on page 193) redisplays if the transfer was successful.

Note: When on the Node Summary webpage, clicking the **Transfer / Status** button displays the Transfer / Status webpage (see Figure 75 on page 198). This sends the node configuration files to all IP Telephony components in the node.

- If any element within the Node fails to transfer either BOOTP or CONFIG files, the Transfer / Status button will be highlighted in red.
- The Transfer / Status button will be highlighted in yellow if the transfer status of the node elements is unavailable.

End of Procedure

Configuring QoS (DiffServ) values

Quality of Service (QoS) values are configured through Element Manager.

Procedure 12
Configuring QoS (DiffServ) values

1 Select **Configuration | IP Telephony** from the Navigation Tree.

The **Node Summary** webpage displays (see Figure 68 on page 193).

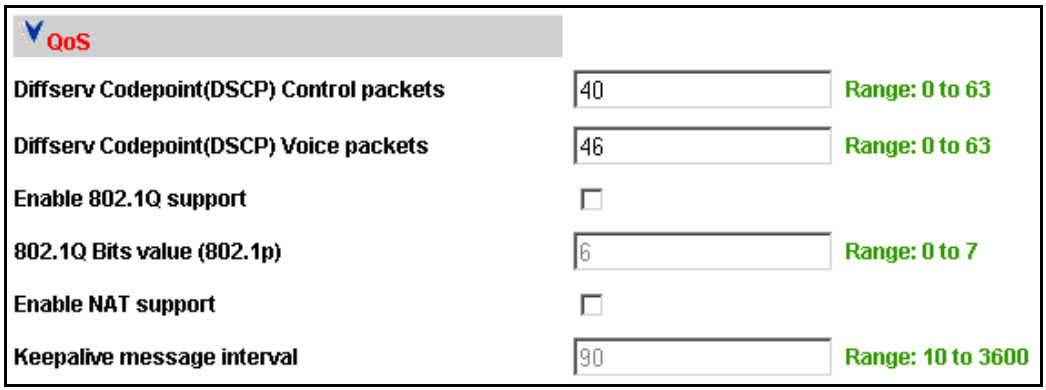
2 Click the **Edit** button.

The **Edit** webpage displays (see Figure 69 on page 194).

3 Click **QoS**.

The QoS sections expands (see Figure 76).

Figure 76
QoS



4 Enter the recommended values:

a. **Diffserv Codepoint (DSCP) Control packets**: A value of 40 - Class Selector 5 (CS5). The range is 0 – 63. This sets the priority of the signaling messaging.

b. **Diffserv CodePoint (DSCP) Voice packets**: A value of 46 Control DSCP - Expedited Forwarding (EF). The range is 0 – 63.

Note: The Differentiated Service (DiffServ) CodePoint (DSCP) determines the priorities of the management and voice packets in the IP Line network. The values are stored in IP telephony CONFIG.INI file. The values used in the IP packets are respectively **160** (40*4) and **184** (46*4).

5 Click the **Save and Transfer** button.

For more information about Differentiated Service (DiffServ) CodePoint (DSCP), see the *Data Networking for Voice over IP* (553-3001-160) and *IP Line: Description, Installation, and Operation* (553-3001-365).

End of Procedure

Configuring call types

To configure the call types and location codes HLOC, HNPA, LOC, NPA, NXX, SPN using Element Manager, follow the steps in Procedure 13.

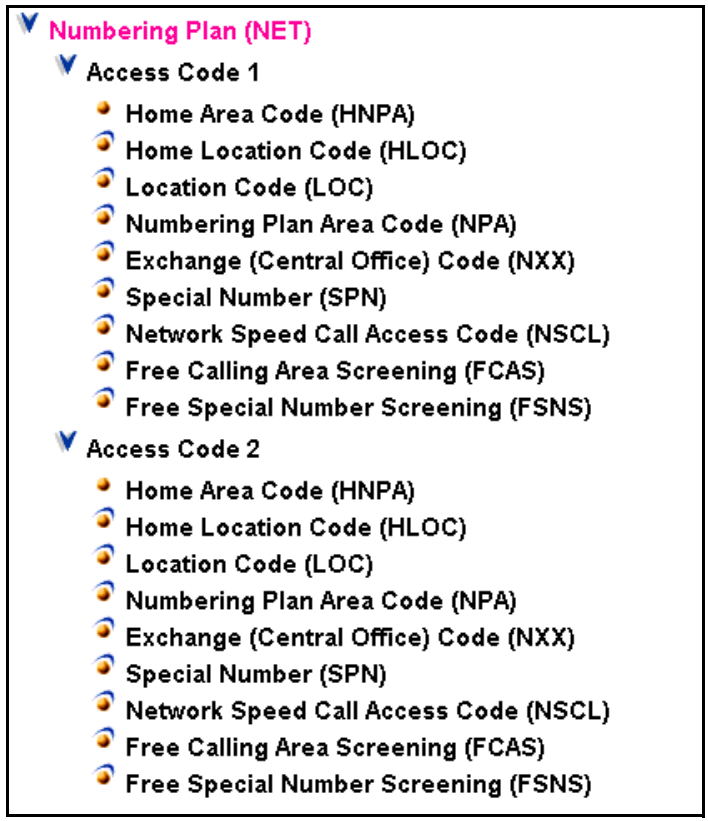
Procedure 13
Configuring call types

1 Select **Network Numbering Plan | Call Server** from the Navigation Tree.

2 Scroll to the **Numbering Plan (NET)** link (see Figure 77 on page 203).

To configure...	See...
Home Location Code (HLOC)	step 3 on page 204
Home Area Code (HNPA)	step 4 on page 205
Location Code (LOC)	step 5 on page 205
Numbering Plan Area Code (NPA)	step 6 on page 207
Exchange (Central Office) Code (NXX)	step 7 on page 209
Special Number (SPN)	step 8 on page 211

Figure 77
Numbering Plan (NET)



3 To configure Home Location Code, perform the following steps:

a. Click **Home Location Code (HLOC)** under Access Code 1 or Access Code 2.

The **Home Location Code List** webpage displays (see Figure 78).

b. Enter a code in the **home location code** text box.

c. Click the **to Add** button.

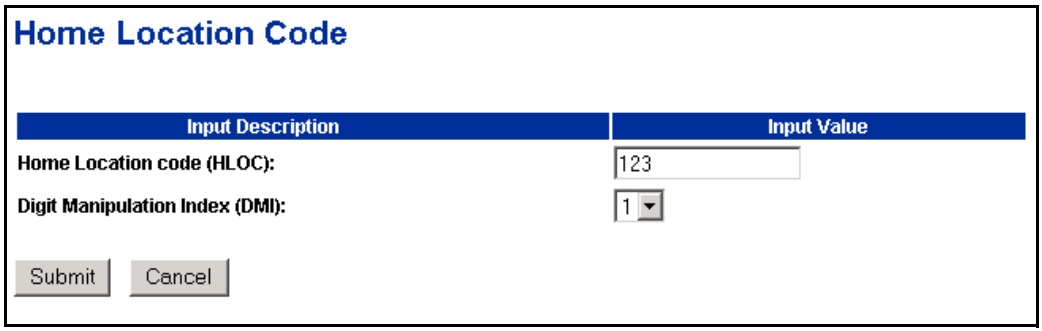
The **Home Location Code** webpage displays (see Figure 79) with the **Home Location code (HLOC)** auto-filled.

d. Select a **Digit Manipulation Index (DMI)**.

e. Click the **Submit** button.

Figure 78
Home Location Code List

Figure 79
Home Location Code



4 To configure Home Area Code (HNPA), perform the following steps:

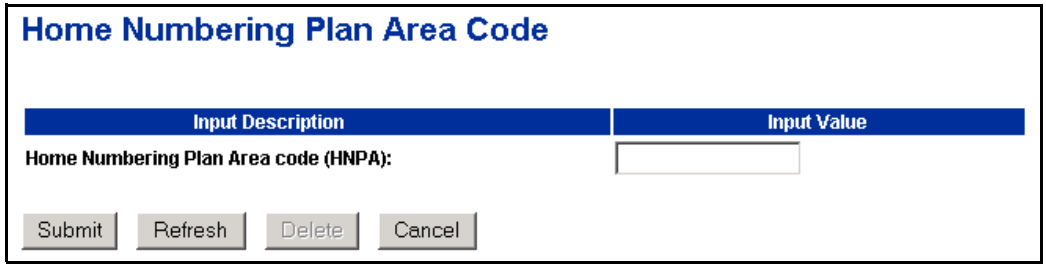
a. Click **Home Area Code (HNPA)** under Access Code 1 or Access Code 2

The **Home Numbering Plan Area Code** webpage displays (see Figure 80).

b. Enter the **Home Number Plan Area code (HNPA)** in the text box.

c. Click the **Submit** button.

Figure 80
Home Numbering Plan Area Code



5 To configure Location Code (LOC), perform the following steps:

a. Click **Location Code (LOC)** under Access Code 1 or Access Code 2.

The **Location Code List** webpage displays (see Figure 81 on page 206).

b. Enter a code in the **location code** text box.

c. Click the **to Add** button.

The **Location Code** webpage displays (see Figure 82 on page 206).

d. Fill the appropriate information.

e. Click the **Submit** button.

Figure 81
Location Code List

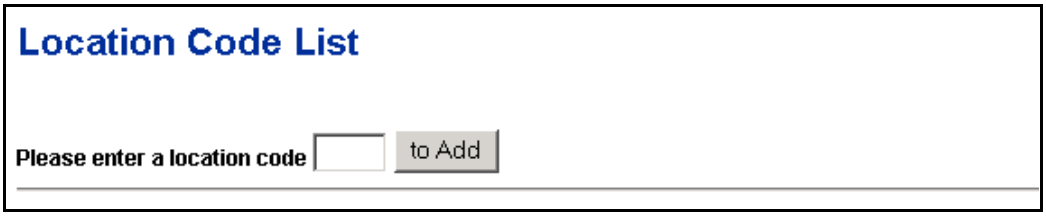
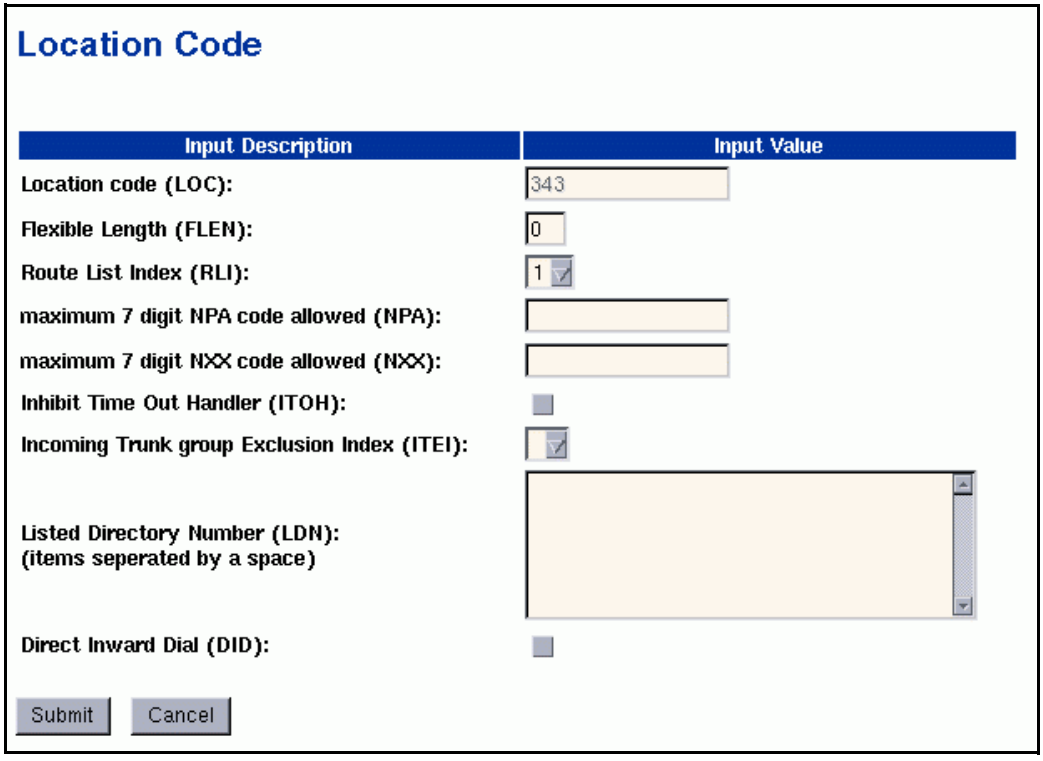


Figure 82
Location Code



6 To configure Number Plan Area Code (NPA), perform the following steps:

a. Click **Numbering Plan Area Code (NPA)** under Access Code 1 or Access Code 2.

The **Numbering Plan Area Code List** webpage displays (see Figure 83).

b. Enter an area code.

c. Click the **to Add** button.

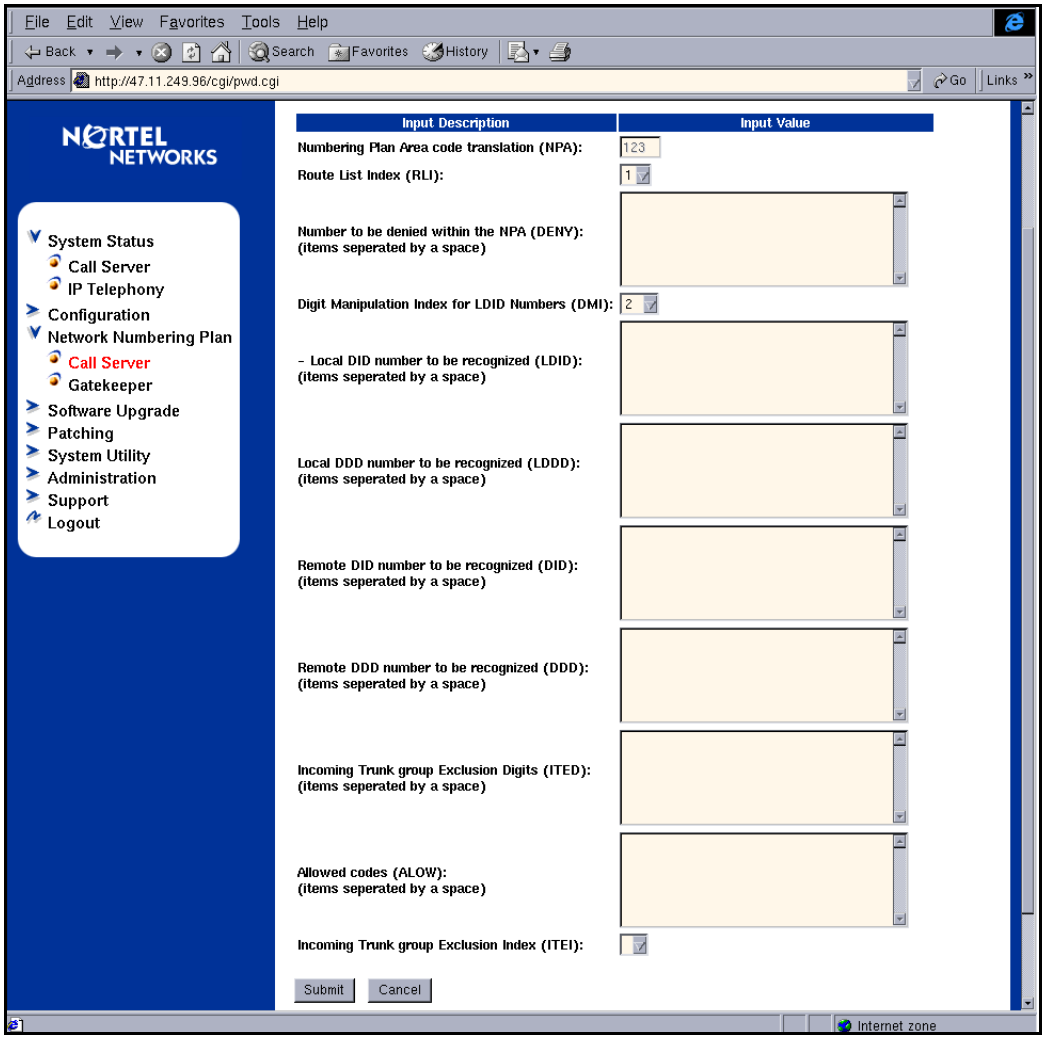
The **Numbering Plan Area Code** webpage displays (Figure 84 on page 208).

d. Fill the appropriate information.

e. Click the **Submit** button.

Figure 83
Numbering Plan Area Code List

Figure 84
Numbering Plan Area Code List (continued)



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

a. Click **Exchange (Central Office) Code (NXX)** under Access Code 1 or Access Code 2.

The **Exchange (Central Office) Code List** webpage displays (see Figure 85).

b. Enter the code.

c. Click the **to Add** button.

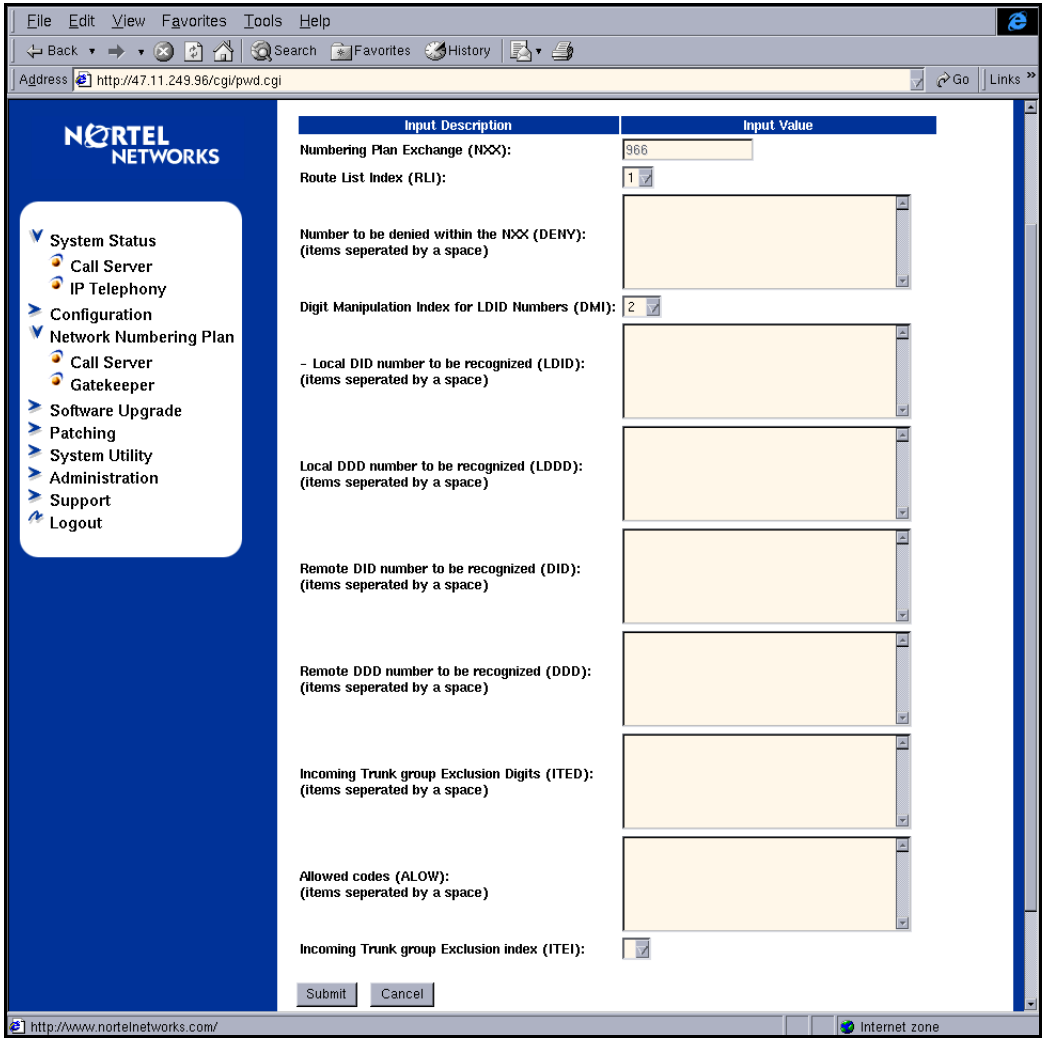
The **Exchange (Central Office) Code** webpage displays (see Figure 86 on page 210).

d. Fill the appropriate information.

e. Click the **Submit** button.

Figure 85
Exchange (Central Office) Code List

Figure 86
Exchange (Central Office) Code List (continued)



8 To configure Special Number (SPN), perform the following steps:

a. Click **Special Number (SPN)** under Access Code 1 or Access Code 2.

The **Special Number List** webpage displays (see Figure 87).

b. Enter the number.

c. Click the **to Add** button.

The **Special Number** webpage displays (see Figure 88 on page 212).

d. Fill the appropriate information.

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

Figure 87
Special Number List

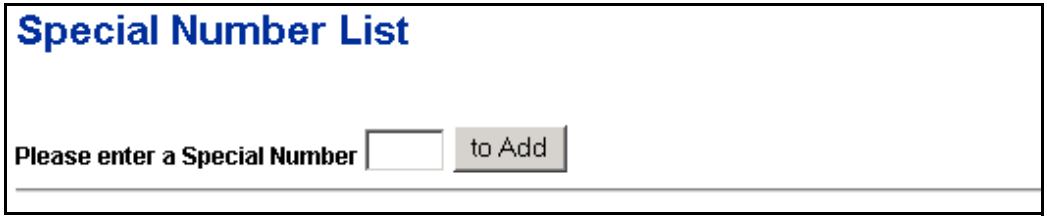
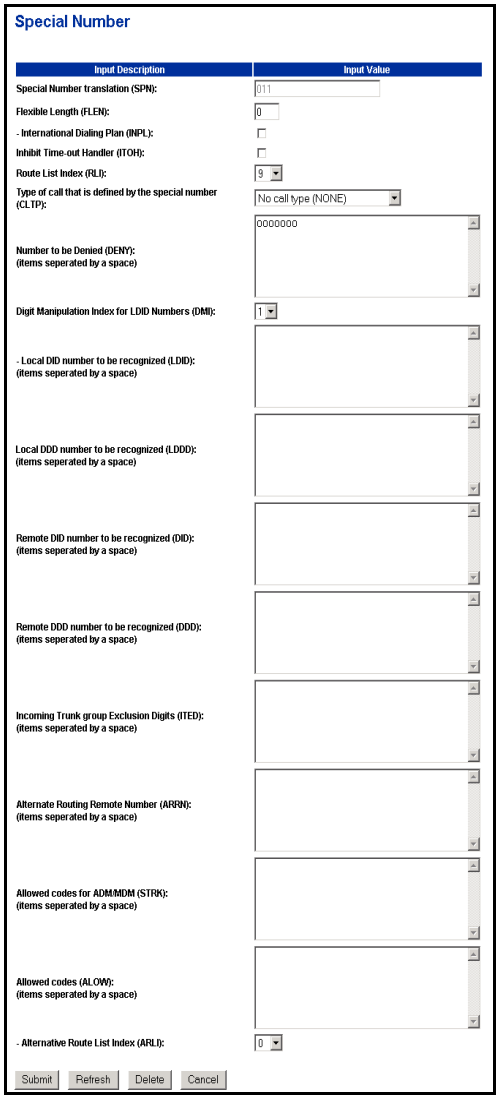


Figure 88
Special Number



End of Procedure

Configuring digit manipulation tables

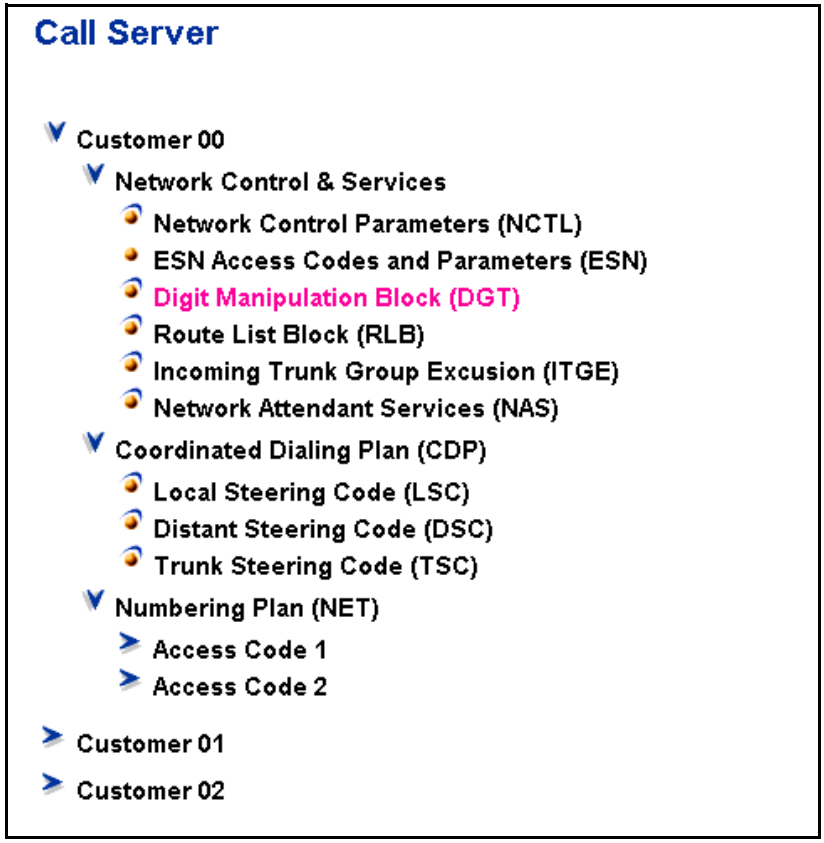
Procedure 14
Configuring digit manipulation tables

1 Select the **Network Numbering Plan | Call Server** from the Navigation Tree.

The **Caller Server** webpage displays.

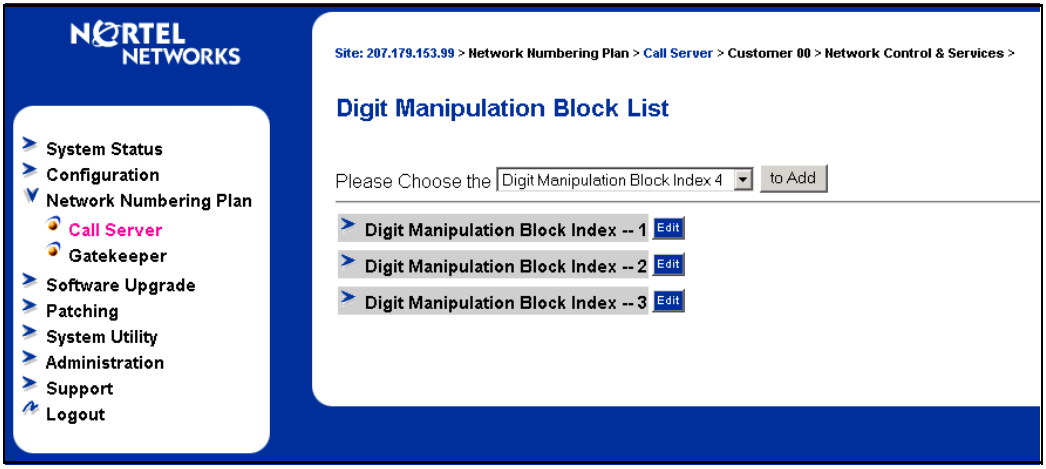
2 Under **Network Control & Services**, select **Digit Manipulation Block (DGT)** (see Figure 89).

Figure 89
Digit Manipulation Block (DGT)



The **Digit Manipulation Block List** webpage displays (see Figure 90).

Figure 90
Digit Manipulation Block List

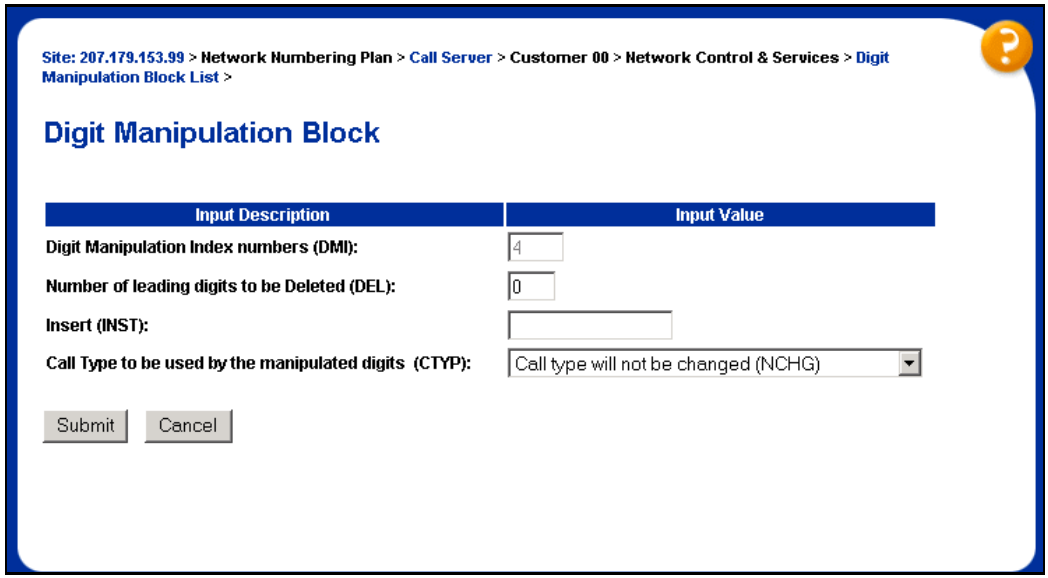


3 Select a **Digit Manipulation Block Index** number in the drop-down list box.

4 Click the **to Add** button.

The **Data Manipulation Block** webpage displays (see Figure 91 on page 215).

Figure 91
Digit Manipulation Block



5 Fill the appropriate information.

6 Click the **Submit** button.

End of Procedure

Enabling the Gatekeeper

This procedure is required for IP Peer Networking. It is a prerequisite for using the chapter "Managing the Gatekeeper" on page 239. The Gatekeeper can also be enabled during installation of the Succession Signaling Server software (Using the Install Tool, configure the Succession Signaling Server to enable the Gatekeeper application and the Gatekeeper IP addresses. See *Signaling Server: Installation and Configuration* (553-3001-212)).

Procedure 15
Enabling the Gatekeeper

Enable, change, or update the Gatekeeper configuration role (None, Primary, Alternate, or Failsafe) and the Gatekeeper IP addresses (Primary and Alternate) on the Leader Succession Signaling Server.

1 Select **Configuration | IP Telephony** from the Navigation Tree.

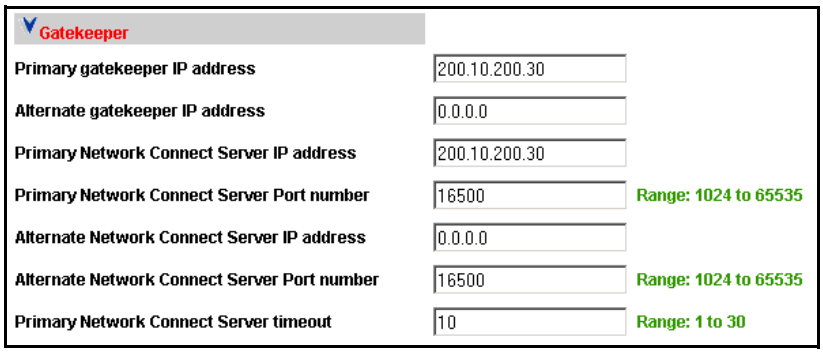
The **Node Summary** webpage displays.

2 Click the **Edit** button.

The **Edit** webpage displays.

3 Click on **Gatekeeper** to expand the options (see Figure 92).

Figure 92
Gatekeeper configuration



4 Enter the TLAN IP address (not the Node IP) of the Leader Succession Signaling Server running the Gatekeeper application for **Primary gatekeeper IP address**.

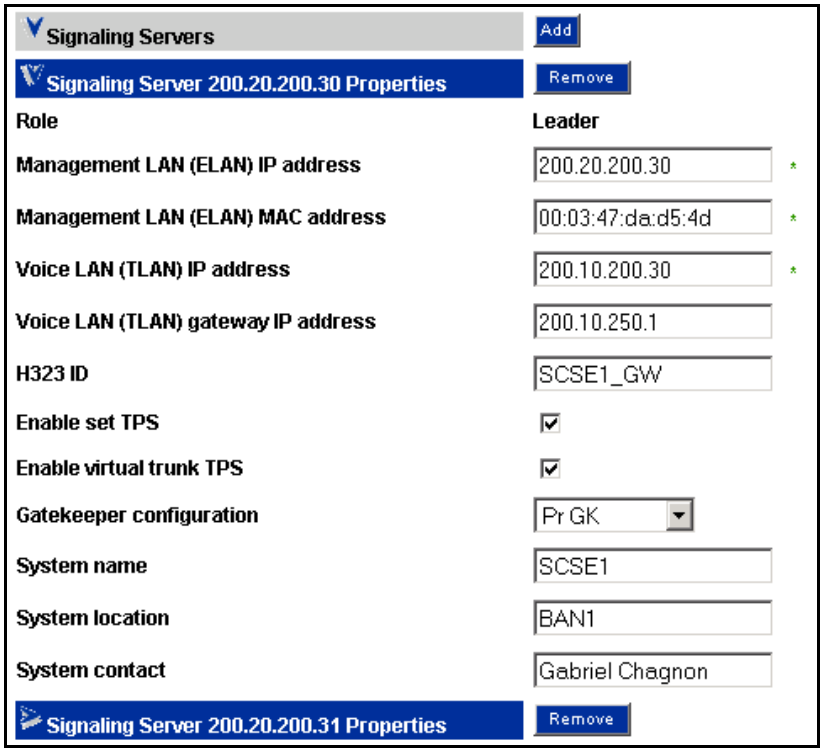
5 Enter the **Alternate gatekeeper IP address** if an Alternate Gatekeeper exists.

6 From the same Edit webpage, choose **Signaling Servers**.

Figure 93
Signaling Servers

7 Click on **Signaling Server xxx.xxx.xxx.xxx Properties** where xxx.xxx.xxx.xxx is the IP address for the selected Succession Signaling Server. Figure 94 on page 218 displays.

Figure 94
Enable Software Gatekeeper



8 In the H323 ID text box, enter any text string to describe the Virtual Trunk source.

9 Enable the Telephony Proxy Server by checking both of the following:

- **Enable set TPS**
- **Enable virtual trunk TPS**

10 Select the **Gatekeeper configuration** from the drop-down list box.

The options are No GK (no Gatekeeper), Pr GK (Primary Gatekeeper), Alt GK (Alternate Gatekeeper), and Failsafe GK (Failsafe Gatekeeper).

11 Click the **Save and Transfer** button to save the changes and transfer the properties to all nodes.

12 Click **Logout** at the bottom of the Navigation Tree to log out of Element Manager.

13 Reboot the Succession Signaling Server.

End of Procedure

Feature Implementation

If you are using the Command Line Interface (CLI), use the following implementation tables to configure the IP Peer Networking feature.

Task summary list

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

1 LD 17 – Configure D-channels.

2 LD 15 – Configure network settings and options.

3 LD 16 – Configure the route bandwidth zone.

4 LD 14 – Configure Virtual Trunks.

5 LD 86 – Configure dialing plan, networking, and ESN data.

6 LD 87 – Configure network access.

7 LD 86 – Configure the digit manipulation index.

8 LD 86 – Configure the Route List Block for the Virtual Trunk route.

9 LD 87 – Configure CDP steering codes.

10 LD 90 – Configure call types and location codes.

LD 17 – Configure D-channels. (Part 1 of 2)

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	ADAN	Action Device And Number
- ADAN	NEW DCH xx	Action Device And Number, where xx is 0-63.
CAB_TYPE	a...a	Cabinet Type Where a...a = • IP = IP Expansion Cabinet or Media Gateway • FIBR = Fiber Expansion Cabinet
- CTYP DCIP		Card Type D-channel over IP
- DES	x...x	Designator
BANR	YES	Enable security banner printing option
- IFC	SL1	Interface type for D-channel
CO_TYPE	aaa	Central Office switch type, where: • aaa = (STD) or ATT
- RCVP	YES	Auto-recovery to primary D-channel option.
- - ISLM	1-382	Integrated Services Signaling Link Maximum. The maximum number of ISL trunks controlled by the D-channel. There is no default value.
- OTBF	1-(32)-127	Output Request Buffers
- RLS	25	Release ID of the switch at the far end of the D-channel
- RCAP ND2		Remote Capabilities Network Name Display method 2

LD 17 – Configure D-channels. (Part 2 of 2)

Prompt	Response	Description
- OVLR	(NO)	Overlap Receiving
- OVLS	(NO)	Overlap Sending

LD 15 – Configure network settings and options. (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW CHG	Add data block Change existing data block
TYPE:	NET	ISDN and ESN Networking options
CUST	 0-99 0-31	Customer number For Large Systems For Small Systems and Succession 1000 systems
...		
OPT	a...a	Options
AC2	aaaa..aaaa	Enter call types that use Access Code 2 as defined in LD 86, for automatic insertion of UDP access code. Multiple responses are permitted. If a numbering plan is not entered here, it is automatically defaulted to AC1. Where aaaa = NPA = E.164 National number. NXX = E.164 Subscriber number. INTL = International number. SPN = Special Number. LOC = Location Code.
FNP	(YES)	Enable Flexible Numbering Plan for customer

LD 15 – Configure network settings and options. (Part 2 of 2)

Prompt	Response	Description
ISDN	YES	Integrated Services Digital Network
VPNI	1-16283	Virtual Private Network Identifier
- PNI	(0)-32700	Private Network Identifier
- CLID	(NO)	Do not enable Calling Line Identification option
CNTC	xx	Country code
NATC	xx	National access code
INTC	xxx	International access code

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

LD 16 – Configure the route bandwidth zone. (Part 1 of 3)

Prompt	Response	Description
REQ	NEW	Add a new route
TYPE	RDB	Route Data Block
CUST	xx	Customer number, as defined in LD 15
ROUT	 0-511 0-127	Route number For Large Systems For Small Systems and Succession 1000 systems
DES	x...x	Designator The designator field for the trunk groups. This designator can be 0-16 alphanumeric characters.
TKTP	 TIE	Trunk Type TIE trunk

LD 16 – Configure the route bandwidth zone. (Part 2 of 3)

Prompt	Response	Description
VTRK	YES	Virtual Trunk route, where: YES = This route is for Virtual Trunk NO = This route is not for Virtual Trunk (default)
ZONE	0-255	Zone for codec selection and bandwidth management
NODE	xxxx	Node ID Where the Node ID that matches the node of the Signaling Server. The Node ID can have a maximum of 4 numeric characters.
PCID	H323	Protocol ID for the H.323 route
ISDN	YES	Integrated Services Digital Network option
- MODE	ISLD	Mode of operation
- DCH	0-159	D-channel number
- IFC	SL1	Interface type for route (IFC responses are listed in *Software Input/Output: Administration* (553-3001-311))
- SRVC	a...a	Service type for AT&T ESS connections (SRVC responses are listed in *Software Input/Output: Administration* (553-3001-311))
- - PNI	(0)-32700	Private Network Identifier
- NCNA	(YES)	Network Calling Name Allowed

LD 16 – Configure the route bandwidth zone. (Part 3 of 3)

Prompt	Response	Description
- NCRD	YES	Network Call Redirection
- INAC	(NO) YES	Inserts the ESN access code to an incoming private network call. INAC enables an ESN access code to be automatically added to an incoming ESN call from a private network. If INAC = YES, then digit insertion (INST) for NARS or BARS calls is bypassed and Access Code 1 (AC1) is used for all call types. However, calls can be specifically defined to use Access Code 2 (AC2) in LD 15 at the AC2 prompt. INAC is prompted when the route type is either a TIE trunk or an IDA trunk with DPNSS1 signaling.

LD 14 – Configure Virtual Trunks. (Part 1 of 2)

Prompt	Response	**Description**
REQ	NEW NEW x	Create a trunk Create x trunks, where x = 1- 255 (to create that number of consecutive trunks)
TYPE	IPTI	IP TIE trunk data block
TN	 l s c u c u	Terminal Number of the first Virtual Trunk For Large Systems For Small Systems and Succession 1000 systems
DES	a....a	Virtual Trunk descriptor Designator field for trunk groups where a...a = 0-16 alphanumeric characters (DES is an optional entry)

LD 14 – Configure Virtual Trunks. (Part 2 of 2)

Prompt	Response	**Description**
XTRK		Extended Trunk
	VTRK	Virtual Trunk type
		Note: If you entered a virtual TN at the TN prompt, then the XTRK prompt only accepts the VTRK option.
CUST	xx	Customer number, as defined in LD 15
...		
RTMB		Route number and Member number
	0-511 1-510	For Large Systems
	0-127 1-510	For Small Systems and Succession 1000 systems
CHID	1-382	Channel ID for this trunk, dependent on the ISLM parameter (LD 17)
STRI	IMM	Start arrangement Incoming (a...a = DDL, IMM, MWNK, OWK, PTSD, SACK, RT, or WNK)
STRO	IMM	Start arrangement Outgoing (a...a = DDL, IMM, MWNK, OWK, PTSD, SACK, RT, or WNK)
SUPN	YES	Answer and disconnect Supervision required
		SUPN must equal YES for a COT with Virtual Network Service
...		
TKID	nnnnnnn	Trunk Identifier

LD 86 – Configure dialing plan, networking, and ESN data.

Prompt	Response	Description
REQ	NEW	Create new data block
FEAT	ESN	Electronic Switched Network
MXLC	x	Maximum number of Location Codes (NARS only) Where x = 0-1000
...		
CDP	YES	Coordinated Dialing Plan feature for this customer
- MXSC	x	Maximum number of Steering Codes Where x = • 0-8000 = Maximum number of Steering Codes for Small Systems and Succession 1000 Systems • 0-10000 = Maximum number of Steering Codes in North America • 0-32000 = Maximum number of Steering Codes outside North America
- NCDP	x	Number of digits to be included as part of the CDP DN (DSC + DN or LSC + DN) where x = 3-7.
AC1	x	One or two digit NARS/BARS Access Code 1
AC2	x	One or two digit NARS Access Code 2
DLTN	(YES)	NARS/BARS Dial Tone after dialing AC1 or AC2 access codes
ERWT	(YES)	Expensive Route Warning Tone
...		
TGAR	(NO)	Check for Trunk Group Access Restriction.

LD 87 – Configure network access.

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

LD 86 – Configure the digit manipulation index. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15
FEAT	DGT	Digit manipulation data block
DMI	xxxx	Digit Manipulation Index numbers Digit Manipulation Index with Flexible Numbering Plan (FNP) package 160 DMI is only prompted when the Directory Number Expansion (DNXP) package 150 is equipped and SDRR = LDID.
DEL	xx	Delete. Number of leading digits to be deleted.
INST	<cr>	Insert. Up to 31 leading digits can be inserted.

LD 86 – Configure the digit manipulation index. (Part 2 of 2)

Prompt	Response	Description
CTYP ...	<cr>	Call Type to be used by the manipulated digits. This call type must be recognized by the far end switch.

LD 86 – Configure the Route List Block for the Virtual Trunk route. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
FEAT	RLB	Route list block
...		
RLI		Route List Index to be accessed
	0-127 0-255 0-999	CDP and BARS NARS FNP
ENTR	xxx	Entry number for NARS/BARS Route list Where xxx = • 0-63 Entry number for NARS/BARS Route List • 0-6 Route list entry number for CDP • X Precede with x to remove
LTER	(NO)	Local Termination entry

LD 86 – Configure the Route List Block for the Virtual Trunk route. (Part 2 of 2)

Prompt	Response	Description
ROUT		Route number
	0-511	For Large Systems
	0-127	For Small Systems and Succession 1000 systems
DMI		Digit Manipulation Index
	0	No digit manipulation required
	1-31	CDP
	0-255	NARS and BARS
	0-999	FNP

LD 87 – Configure CDP steering codes. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
FEAT	CDP	Coordinated Dialing Plan
TYPE		Type of steering code
	DSC	Distant Steering Code
DSC	x..x	Distant Steering Code Up to 4 digits, up to 7 digits with Directory Number Expansion (DNXP) package 150.
- FLEN	(0)	Flexible Length number of digits
- DSP	(LSC)	Display (Local Steering Code)
- RRPA	(NO)	Remote Radio Paging Access

LD 87 – Configure CDP steering codes. (Part 2 of 2)

Prompt	Response	Description
- RLI		Route List to be accessed for Distant Steering Code. Cannot have non-zero entries or DMI.
	0-31	CDP
	0-127	BARS
	0-255	NARS
	0-999	Flexible Numbering Plan (FNP)
- CCBA	(NO)	Collect Call Blocking (CCB) Denied
- NPA	<cr>	North American Numbering Plan Routing code: maximum 7-digit National code enabled
- NXX	<cr>	North American Numbering Plan Routing code: maximum 7-digit subscriber code allowed

LD 90 – Configure call types and location codes. (Part 1 of 2)

Prompt	Response	Description
REQ	NEW	Create new data block
	CHG	Change existing data block
CUST	xx	Customer number, as defined in LD 15
FEAT	NET	Network Translator (Network translation tables)
TRAN		Translator
	AC1	Access Code 1 (NARS/BARS)
	AC2	Access Code 2 (NARS)
TYPE	LOC	Location Code
LOC	x...x	Location Code

LD 90 – Configure call types and location codes. (Part 2 of 2)

Prompt	Response	Description
- FLEN	(0)-10	Flexible Length Enter the maximum number of digits expected. When this number of digits is dialed, dialing is considered to be complete and end-of-dial processing begins. Default is zero (0) digits.
- RLI	0-999	Route List Index Enter Route List Index for this LOC.
…		

VNR enhancement

To configure the VNR enhancement, configure AC2, PFX1, VNR, RLI, CDPL, UDPL, CNTC, CATC, and INTC in LD 15.

LD 15 – Configure the VNR enhancement. (Part 1 of 6)

Prompt	Response	Description
REQ:	NEW	Add new data block to the system.
TYPE:	NET	ISDN and ESN networking options
CUST	 0-99 0-31	Customer number For Large Systems For Small Systems and Succession 1000 systems
OPT	 RTD	Options Coordinated Dialing Plan routing feature Denied
AC2	SPN LOC	Special Number; Location Code
FNP	(YES)	Enable Flexible Numbering Plan for customer.
ISDN	YES	Integrated Services Digital Network allowed for customer. ***Note:*** Prompted when ISDN signaling package 145 is equipped and either the Integrated Service Digital Network BRI Trunk Access (BRIT) package 233 is equipped or at least one PRA link is configured.
- VPNI	1-16283	Virtual Private Network Identifier
- CLID	YES	Allow Calling Line Identification option Calling Line Identification does not require ISDN.
- - ENTRY	xx	CLID entry to be configured. CLID entries must be between 0 and the value entered at the SIZE prompt - 1. Precede entry or entries with X to delete. ENTRY is repeated until a <cr> is entered.

LD 15 – Configure the VNR enhancement. (Part 2 of 6)

Prompt	Response	Description
- - - HLOC	100-9999999	Home Location Code (ESN) as defined in LD 90 1 to 7 digits with extended code. Prompted when ISDN=YES, or with Digital Private Network Signaling System 1 (DPNSS) package 123.
- - - LSC	0 .. x..x	Local Steering Code 1 to 7 digits. LSCs are required if the CDP DNs are longer than the local PDNs. The CLID sent for a CDP call is composed of the LSC defined in LD 15 plus the PDN of the calling set. Various ISDN network features depend on the CLID as the return address for sending feature control messages. Multiple LSCs may be defined in LD 87 for CDP but only one LSC can be defined here for the CLID. The LSC prompt appears only if the user has a five or six digit dialing plan, or if the DPNSS software package is equipped. LSC is prompted here if ISDN = NO, otherwise LSC is a subprompt of ISDN.
- PFX1	xxxx	Prefix 1. Prefix or area code for International PRA. First element of Calling Party Number. PFX1 + PFX2 + DN cannot exceed 8 numbers for AXE-10. Prompted with International Primary Rate Access (IPRA) package 202.
- PRX2	xxxx	Prefix 2. Central Office Prefix for International PRA. Second element of Calling Part Number. PFX1 + PFX2 + DN cannot exceed 8 numbers for AXE-10. Prompted with International Primary Rate Access (IPRA) package 202.

LD 15 – Configure the VNR enhancement. (Part 3 of 6)

Prompt	Response	Description
- RCNT	0-(5)	Redirection Count for ISDN calls Maximum number of inter-node hops allowed in a network redirection call, only enforced when ISDN = YES. This field must be set to greater than 0 for a network redirection to take place.
- PSTN	(NO)	Public Service Telephone Networks Limit the number of PSTNs allowed in a network connection to one PSTN. The default (NO) puts no limit on the number of PSTN connections.
- - TNDM	0-(15)-31	Tandem Threshold/Loop Avoidance Limit This is the value permitted in a network connection. If the value entered is greater than 25, then 25 will be used for DPNSS calls. Prompted when Integrated Services Digital Network (ISDN) package 245 and ISDN Supplementary Features (ISDN INTL SUP) package 161, or Digital Private Signaling System Network Services (DNWK) package 231 is equipped.
- - PCMC	0-(15)-31	Pulse Code Modulation Conversions permitted in a network connection, µ-Law to A- Law or A- Law to µ-Law, in a network connection
- SATD	0-(1)-5	Satellite Delays. Number of satellite delays allowed in a network connection
OCLI	NO	NO manipulation is done on outgoing CLID for calls forwarded to EuroISDN link.
TIDM	(NO)	Trunk Identity Meaningful

LD 15 – Configure the VNR enhancement. (Part 4 of 6)

Prompt	Response	Description
DASC	xxxx	Display Access Code Enter the access code which is to be placed on displays before Originating Line Identities (OLI) and Terminating Line Identities (TLI) are received from the ISDN. The default is no code, when creating a new data block. Prompted with Multi Language Wake Up (MLWU) package 206 and Integrated Digital Access (IDA) package 122.
ROPT	(NRO)	No Route Optimization This option may be used to suppress Route Optimization on switches which already have high traffic.
DITI	(NO)	DID to TIE connections allowed
TRNX	(NO)	Prevent transfer on ringing of supervised external trunks across a private network
EXTT	(NO)	Prevent connection of supervised external trunks via either call transfer or conference
FTOP	(FRES)	Flexible Trunk to Trunk Options. Flexible Trunk to Trunk Connections Restricted. FTT feature is inactive.

LD 15 – Configure the VNR enhancement. (Part 5 of 6)

Prompt	Response	Description
APAD	x y (0) (0)	Alternative Pad. Where: x = trunk pad selection and y = conference pad selection Valid inputs for x are: (0) = default North America 1 = Australia 2 = New Zealand 3 = Italy 4 = China EPE or EPE/IPE systems 5 = China pure IPE system 6-7 = future usage currently set to default Valid inputs for y are: (0) = default North America 1 = Alternative Conference pads selected The default = 0 when REQ = NEW. The default is the existing value when REQ = CHG.Alternative Conference pads are only provided on specific Conference cards.
DMWM	(NO)	Enable the output of DPNSSI Message Waiting Indication Non Specified Information error messages
MWNS	(NO)	Message Waiting Indication DPNSSI Non Specified Information string to recognize.
VNR	(YES)	Vacant Number Routing
- RLI	0-999	Route List Index as defined in LD 86
- CDPL	1-(10)	Flexible length of Vacant Number Routing (VNR) Coordinated Dialing Plan (CDP)

LD 15 – Configure the VNR enhancement. (Part 6 of 6)

Prompt	Response	Description
- UDPL	1-(19)	Uniform Plan Public Flexible length of Vacant Number Routing (VNR) Uniform Dialing Plan digits (UDP). Enter the maximum number of UDP digits expected by VNR.
NIT	2-(8)	Network Alternate Route Selection (NARS) Interdigit Timer
NAS_ATCL	(YES)	Network Attendant Service Attendant Control allowed
NAS_ACTV	NO	Network Attendant Service routing Activated
FOPT	0-(14)-30	Flexible Orbiting Prevention Timer The number of seconds in two second intervals that CFW should be suspended on a set that has just forwarded a call off-node. Odd entries are rounded up to the next valid entry. A response of 0 disables FOPT.
CNDN	0 .. x..x	Customer Calling Number Identification DN on outgoing Multifrequency Compelled Signaling (MFC) calls
- CNIP	(YES)	Calling Number Identification Presentation Send Customer Calling Number Identification (CNDN) + Trunk ID (TKID) if Calling Line ID (CLID) = NO in LD 17
CNAT	0 .. x..x	CNI Attendant DN on outgoing Multifrequency Compelled Signaling (MFC) calls.
CNTC	x	Country Code
NATC	x	National Access Code
INTC	xxx	International Access Code

LD 21 has been updated so that is prints which dialing plan is used with AC1. This helps identify which dialing plans use AC1 and which other dialing plans use AC2

LD 21 - Print the dialing plan.

Prompt	Response	Description
REQ	PRT	Print data block for the TYPE specified
TYPE	NET	ISDN and ESN networking options
CUST	xx	Customer number, as defined in LD 15

Managing the Gatekeeper

Contents

This section contains information on the following topics:

Task summary

This section is intended as a summary of how to manage the Gatekeeper database. The Gatekeeper database provides a central database of addresses that are required to route calls across the network. Many of the following steps, which are performed using the Gatekeeper webpages in Element Manager, can be taken out of the sequence presented below.

1 Log in to Gatekeeper webpages in Element Manager.

2 Configure Gatekeeper elements. Verify that the Gatekeeper is the Primary Gatekeeper and is active. See "Verifying that the Gatekeeper is the Primary Gatekeeper" on page 245.

3 Configure the System Wide Settings. See "Configuring the system-wide settings" on page 246.

4 Create the CDP domains, which holds the endpoint numbering plans on the Gatekeeper. It is complementary to the CDP configuration on the Succession Call Server. See "Configuring the CDP domains" on page 253.

5 Add the endpoints. See "Configuring endpoints" on page 259.

6 Add the endpoint prefixes. See "Selecting endpoint number prefixes" on page 268.

7 Add the numbering plan entries for each endpoint, including the Cost Factor for each entry. See "Configuring numbering plan entries" on page 272.

8 Perform database cutover. See "Performing database cutover" on page 282.

9 Test the numbering plans. See "Testing numbering plans" on page 287.

10 Back up the Gatekeeper database. See "Backing up the Gatekeeper" on page 290.

11 Log out of the Gatekeeper webpages in Element Manager. See "Logging out" on page 296.

Configuring the Gatekeeper database

Use the Gatekeeper webpages in Element Manager to configure the Gatekeeper database. For an overview on what the Gatekeeper webpages can accomplish, see “Gatekeeper webpages in Element Manager” on page 100.

Network configuration overview

Each network zone can have one Primary Gatekeeper. Each network zone can also have one Alternate Gatekeeper and multiple Failsafe Gatekeepers for each network zone.

A network zone is a logical grouping of nodes (this also includes IP Line or IP Trunk, BCM, and third-party gateways or endpoints). Network zones can have geographical significance in their administrative capacity. For example, a company can have one network zone covering North America and one covering Europe.

All nodes within a network zone are configured with the IP addresses of the Primary and Alternate Gatekeepers in that zone. It is the H.323 Proxy Server that makes use of the Gatekeeper IP address configuration, as it is the H.323 Proxy Server that communicates with the Gatekeeper. Every H.323 Proxy Server is also configured with a unique H.323 alias identifier. The alias is a network-wide unique identifier.

Configure all nodes within a network zone on the zone’s Gatekeeper. Configure each node’s H.323 Proxy Server and H.323 alias identifier on the Gatekeeper. Add each node individually to the Gatekeeper configuration. Then, add all routes which each node can terminate. For example, if your network can terminate six different routes, add the six numbering plan entries, their associated type of number information, and cost factors to the Gatekeeper’s configuration database. Repeat this procedure for every numbering plan entry and for every node in the network zone.

If there are multiple zones in the network, configure the Gatekeeper in each zone with the IP address of the Gatekeepers in other network zones. This enables interzone calls to be made. If a node wishes to place a call to a node outside its zone, the Gatekeeper can query Gatekeepers in other zones to determine where the terminating node is located.

Logging in to the Gatekeeper webpages in Element Manager

To log in to the Gatekeeper webpages in Element Manager, follow the steps in Procedure 16. Gatekeeper Element Manager supports Microsoft Internet Explorer 6.0.2600 for the Windows operating systems.

You can also use OTM to access the Element Manager.

Procedure 16
Logging in to the Gatekeeper webpages in Element Manager

1 Enter the Gatekeeper's URL in the **Address** Bar of the web browser on the network.

The Gatekeeper address is configured at each H.323 Gateway (that is, the Succession Signaling Server).

The URL is the Succession Signaling Server's TLAN IP address followed by *gk.* For example: http://47.39.2.50/gk/

Note: You must include *gk* as part of the URL, because the Gatekeeper resides on the Succession Signaling Sever platform with other applications. (For example, the TPS also uses a web-based configuration interface, so its URL could be: http://47.39.2.50/tps)

The **Enter Network Password** login dialog box displays (see Figure 95 on page 243).

Note: If you are already logged in to Element Manager, you can access the Gatekeeper webpages.

— Select **Network Numbering Plan** | **Gatekeeper** from the Navigation Tree.

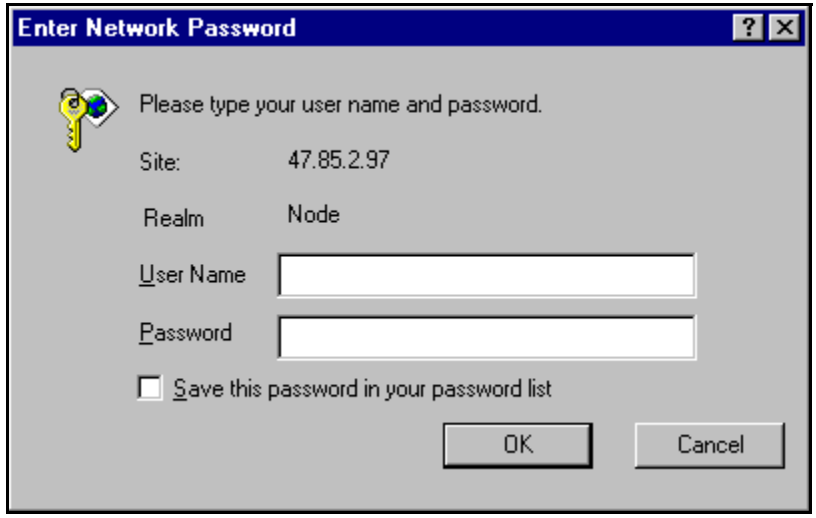
— Enter the **Gatekeeper IP Address** in the text box.

— Click the **Next** button.

— When the login window displays (see Figure 95 on page 243), enter the **User Name** and **Password**.

— Click the **OK** button.

Figure 95
Enter Network Password login dialog box



2 Enter your user name in the **User Name** text box (the default user name is *gkadmin*).

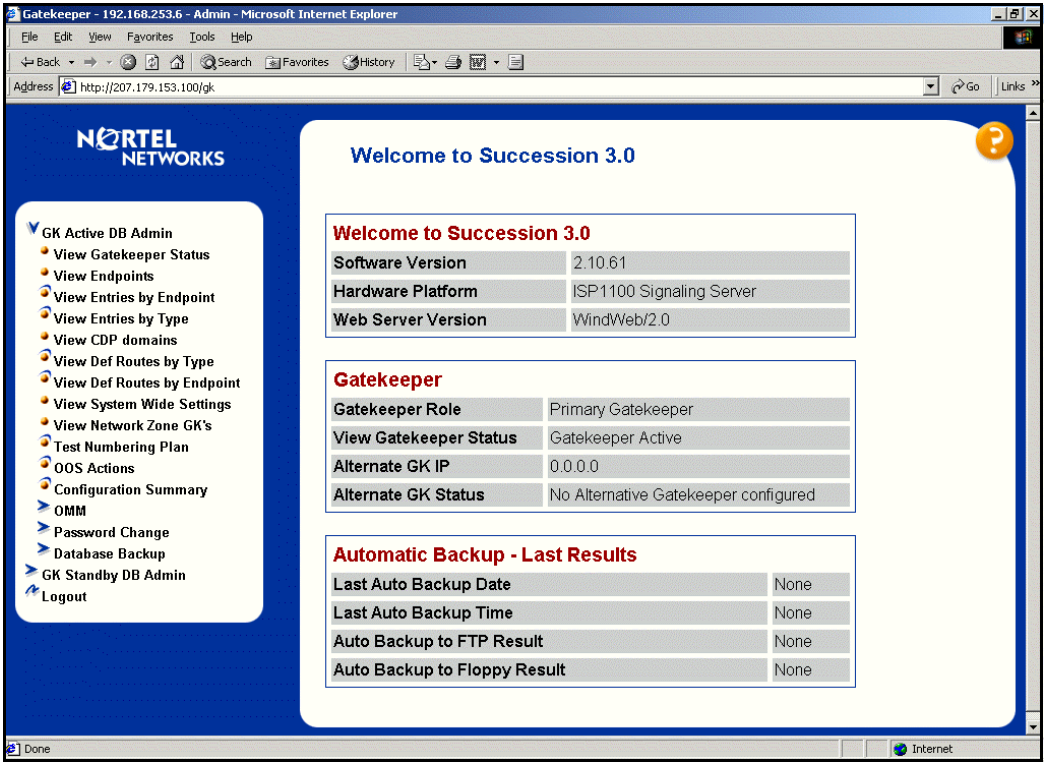
3 Enter your password in the **Password** text box (the default password is *gkadmin*).

4 Click the **OK** button.

If login is successful, the **Welcome** webpage displays (see Figure 96 on page 244).

If login is unsuccessful, an error message displays, and then the **Enter Network Password** dialog box redisplays.

Figure 96
Welcome webpage



End of Procedure

Verifying that the Gatekeeper is the Primary Gatekeeper

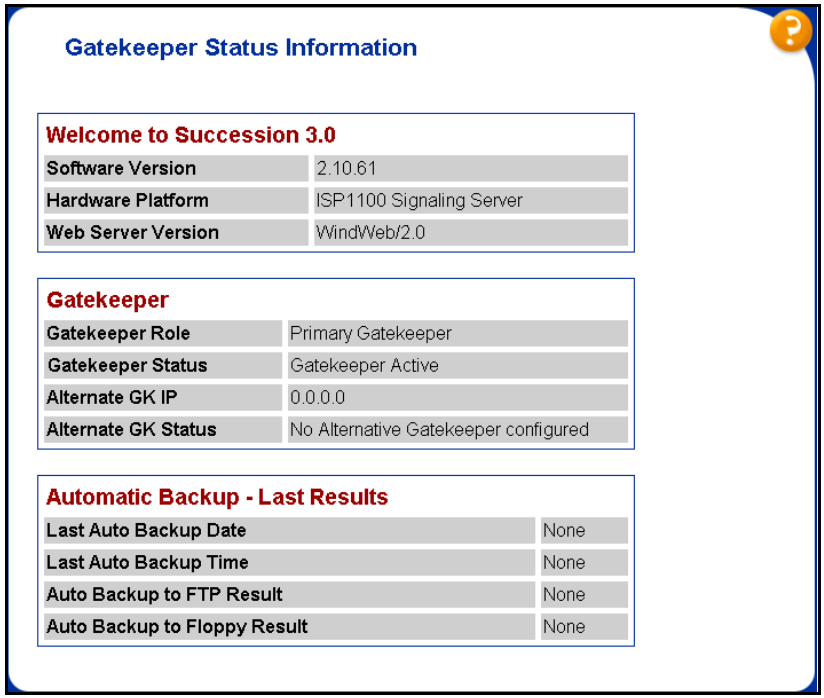
To verify that the Gatekeeper you are configuring is the Primary Gatekeeper and that it is active, follow the steps in Procedure 17.

Procedure 17
Verifying that the Gatekeeper is the Primary Gatekeeper

1 Select **GK Active DB Admin | View Gatekeeper Status** from the Navigation Tree.

The **Gatekeeper Status Information** webpage displays (see Figure 97).

Figure 97
Gatekeeper Status Information webpage



2 In the **Gatekeeper** section (in the middle of the webpage):

   a. Ensure that the **Gatekeeper Role** = Primary Gatekeeper.

   b. Ensure that **Gatekeeper Status** = Gatekeeper Active.

End of Procedure

Configuring the system-wide settings

The system-wide settings include:

- system-wide number prefixes
- the RRQ Time-to-Live interval
- the Gatekeeper alias name
- if the Alternate Gatekeeper is to be in permanent service
- database and registration synchronization poll interval

Use the procedures outlined in Table 29 to configure the system-wide settings.

Table 29
Procedures for configuring the system-wide settings

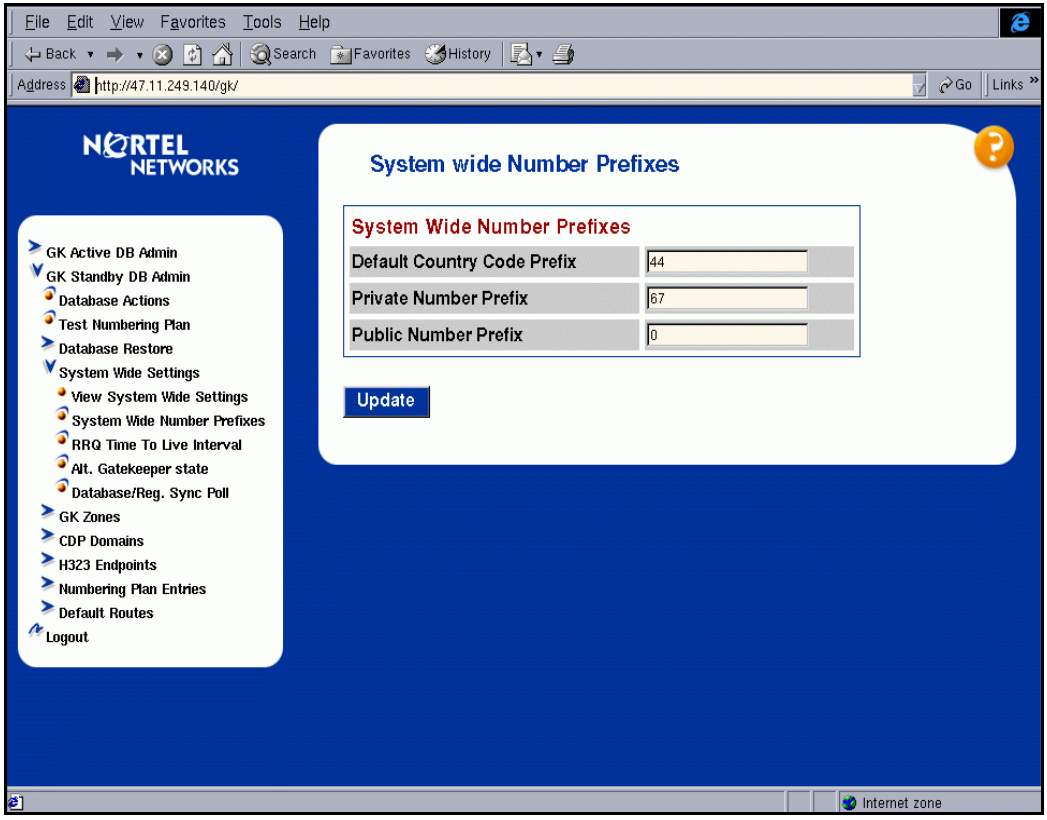
To configure the...	Use...
System-Wide Number Prefixes	Procedure 18 on page 247
RRQ Time-to-Live interval	Procedure 19 on page 249
Gatekeeper Alias Name	Procedure 20 on page 250
Database and Registration Synchronization Poll Interval	Procedure 21 on page 251
Alternate Gatekeeper to be in permanent service	Procedure 22 on page 252

Procedure 18
Selecting the System Wide Number Prefixes

1 Select **GK Standby DB Admin | System Wide Settings | System Wide Number Prefixes** from the Navigation Tree.

The **System wide Number Prefixes** webpage displays (see Figure 98).

Figure 98
System wide Number Prefixes

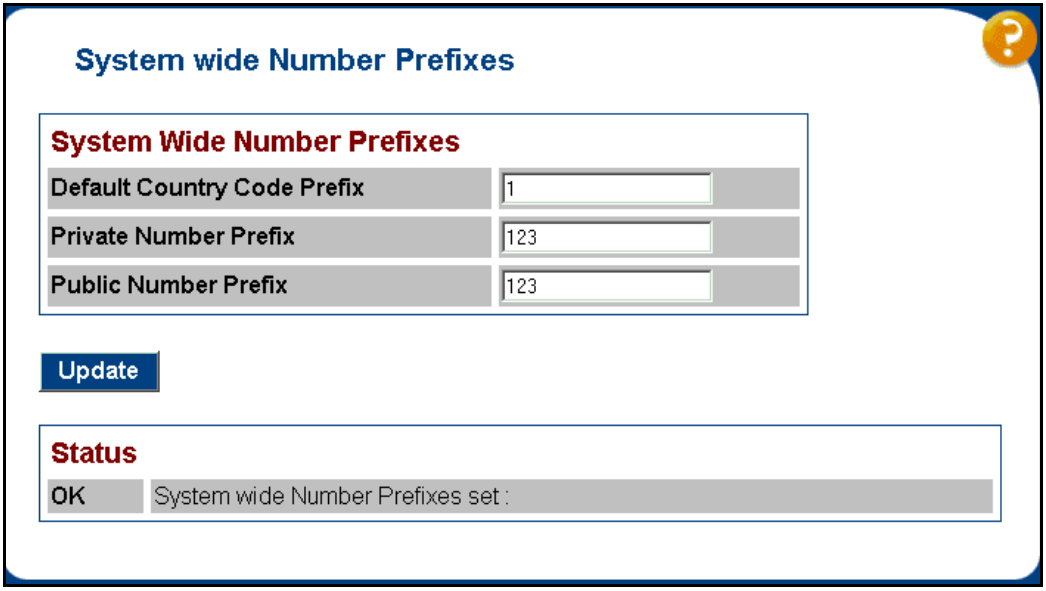


2 Enter the **Default Country Code Prefix**, the **Private Number Prefix**, and the **Public Number Prefix** in the appropriate text boxes.

3 Click the **Update** button.

The status of the request is displayed at the bottom of the webpage (see Figure 99).

Figure 99
System wide Number Prefixes—Status



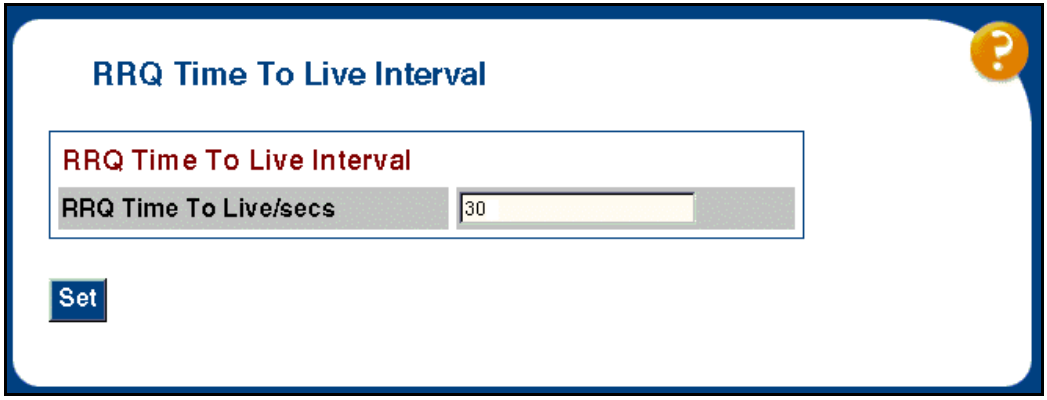
End of Procedure

Procedure 19
Setting the RRQ Time-to-Live interval

1 Select **GK Standby DB Admin | System Wide Settings | RRQ Time to Live Interval** from the Navigation Tree.

The **RRQ Time To Live Interval** webpage displays (see Figure 100).

Figure 100
RRQ Time-to-Live Interval webpage



2 Enter the RRQ Time-to-Live Interval (in seconds) in the **RRQ Time To Live/secs** text box. Nortel Networks recommends that the timer be set to 30 seconds.

3 Click the **Set** button.

The status of the request is displayed at the bottom of the page.

End of Procedure

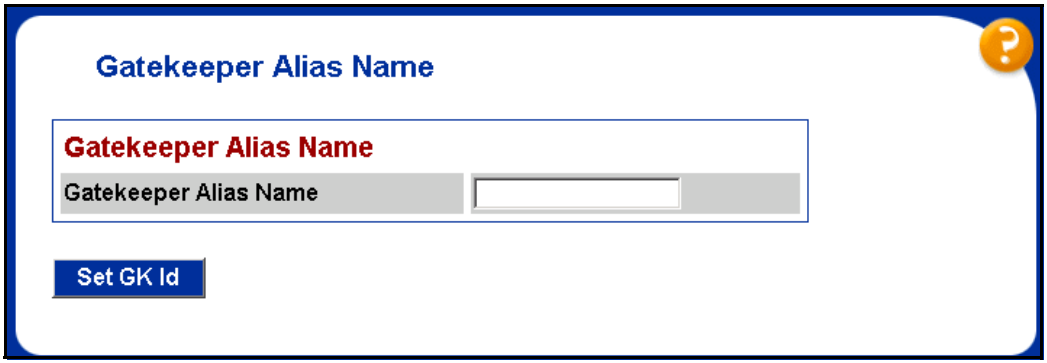
Procedure 20
Setting the Gatekeeper Alias Name

In order for the Gatekeeper to send out Location Requests (LRQ), the Gatekeeper must have a Gatekeeper alias name which is an H323-ID. The default value assigned to this parameter is the same as the “HostName” value configured in the Succession Signaling Server’s config.ini file.

1 Select **GK Standby DB Admin | System Wide Settings | Gatekeeper Alias Name** from the Navigation Tree.

The **Gatekeeper Alias Name** webpage displays (see Figure 101).

Figure 101
Gatekeeper Alias Name



2 Enter the alias name in the **Gatekeeper Alias Name** text box.

3 Click the **Set GK Id** button.

The status of the request is displayed at the bottom of the page.

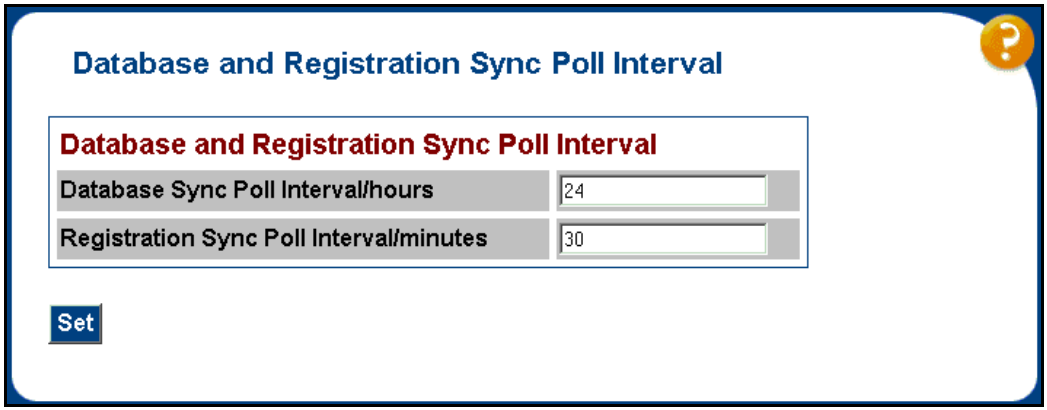
End of Procedure

Procedure 21
Setting the Database and Registration Synchronization Poll Interval

1 Select **GK Standby DB Admin | System Wide Settings | Database/Reg. Sync Poll** from the Navigation Tree.

The **Database and Registration Sync Poll Interval** webpage displays (see Figure 102).

Figure 102
Database and Registration Sync Poll Interval



2 Enter the database synchronization poll interval in hours in the **Database Sync Poll Interval/ hours** text box. This is the time interval between database synchronization with Alternate or Failsafe Gatekeeper. The range is 1 to 24 hours.

3 Enter the registration synchronization poll interval in minutes in the **Registration Sync Poll Interval/minutes** text box. This is the time interval between synchronization of endpoint registration information from Active Gatekeeper (Primary or Alternate) to the Failsafe Gatekeepers. The range is 10 minutes to 1440 minutes (24 hours). The default is 30 minutes.

4 Click the **Set** button.

The status of the request is displayed at the bottom of the page.

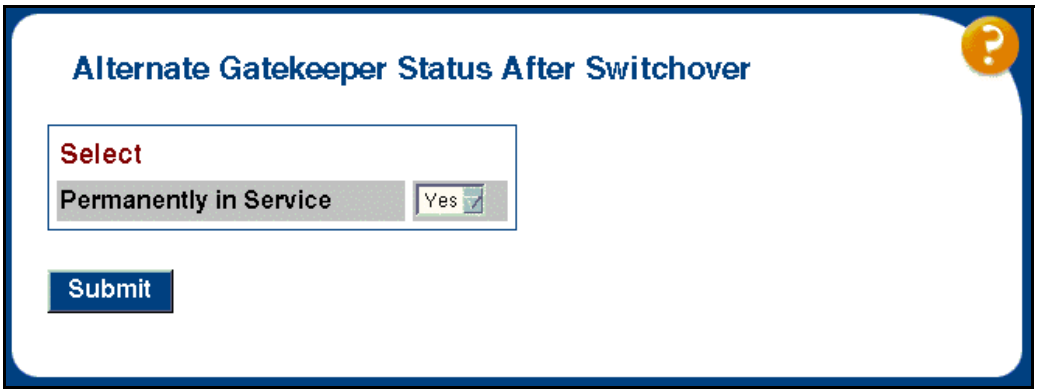
End of Procedure

Procedure 22
Putting the Alternate Gatekeeper in permanent service

1 Select **GK Standby DB Admin | System Wide Settings | Alternate Gatekeeper State** from the Navigation Tree.

The A**lternate Gatekeeper After Switchover Status** webpage displays (see Figure 103).

Figure 103
Alternate Gatekeeper Status After Switchover webpage



2 Select whether or not you want the Alternate Gatekeeper to be **Permanently in Service** from the drop-down list box.

Select **Yes** if the alternate Gatekeeper is to remain in service after a switchover, even if the Primary Gatekeeper recovers. Select **No** if the alternate Gatekeeper will switchover functions to the Primary Gatekeeper after the Primary Gatekeeper recovers.

3 Click the **Submit** button.

The status of the request is displayed at the bottom of the page.

End of Procedure

Configuring the CDP domains

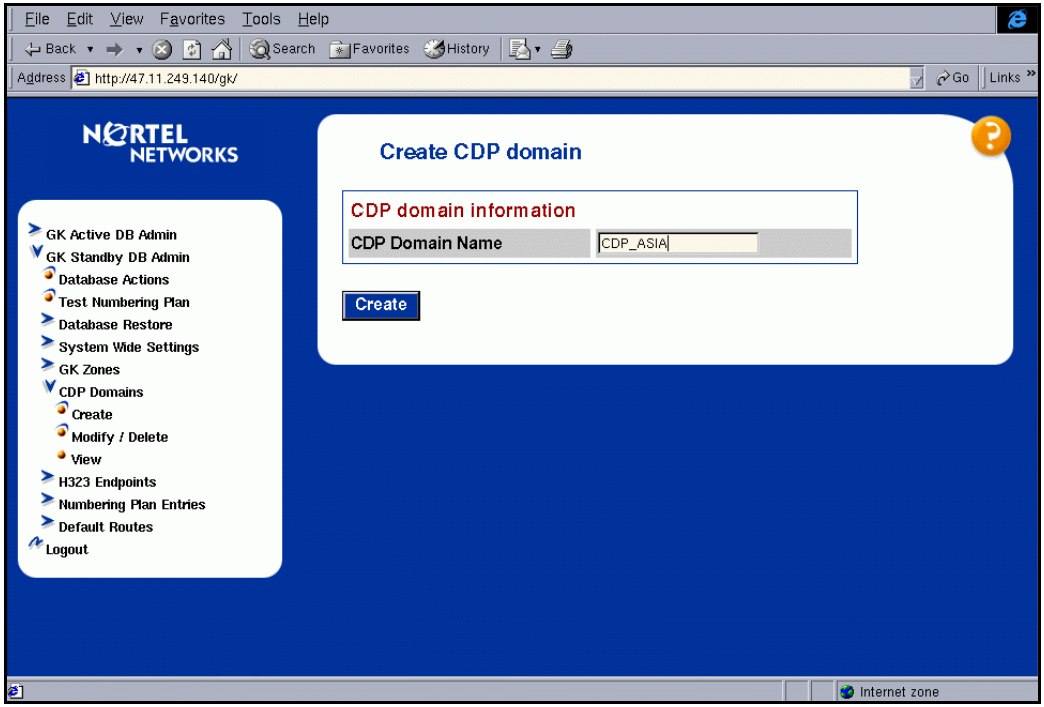
If CDP is used in conjunction with UDP or any other numbering plan, configure the CDP domains first. An endpoint can have both CDP and UDP configured.

Procedure 23
Creating a CDP domain

1 Select **GK Standby DB Admin | CDP Domains | Create** from the Navigation Tree.

The **Create CDP domain** webpage displays (see Figure 104).

Figure 104
Create CDP Domain webpage



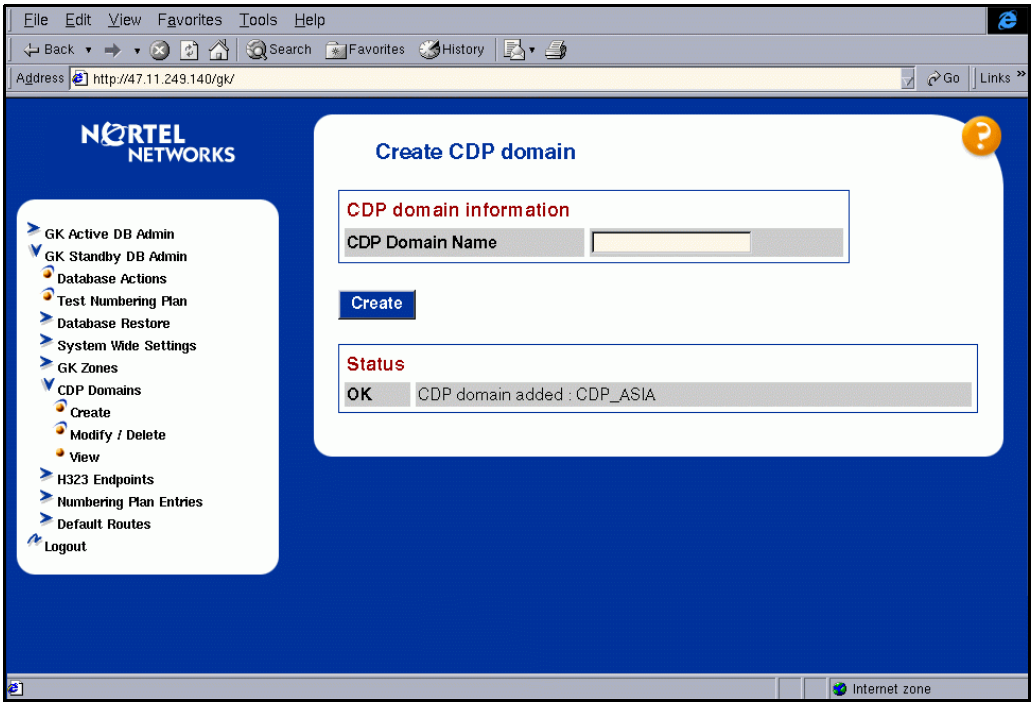
2 In the **CDP Domain Name** text box, enter the name of the CDP domain that you are creating (from the example in Figure 27 on page 106, “CDP_DOMAIN_2” or “MPK_DCP_DOMAIN”).

Note: The CDP domain name must be between 1 and 32 alphanumeric characters in length.

3 Click the **Create** button.

The status of the request is displayed at the bottom of the Create CDP domain webpage (see Figure 105).

Figure 105
Create CDP domain confirmation webpage



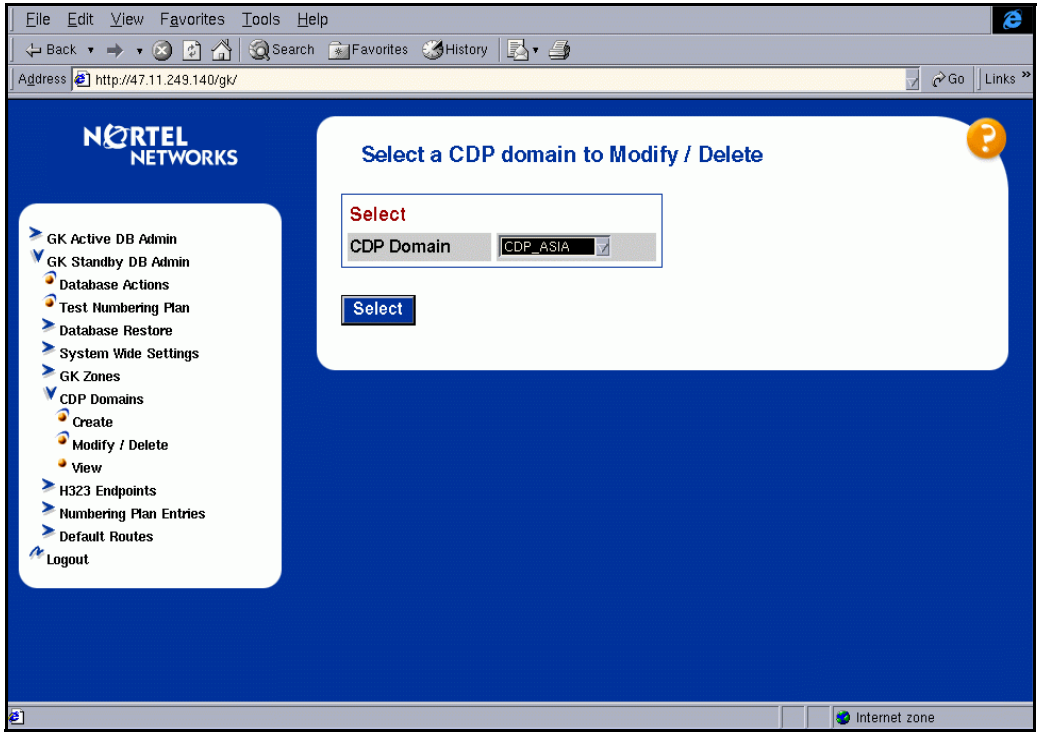
End of Procedure

Procedure 24
Modifying a CDP domain

1 Select **GK Standby DB Admin | CDP Domain | Modify / Delete** from the Navigation Tree.

The **Select a CDP domain to Modify / Delete** webpage displays (see Figure 106).

Figure 106
Select a CDP domain to Modify / Delete webpage

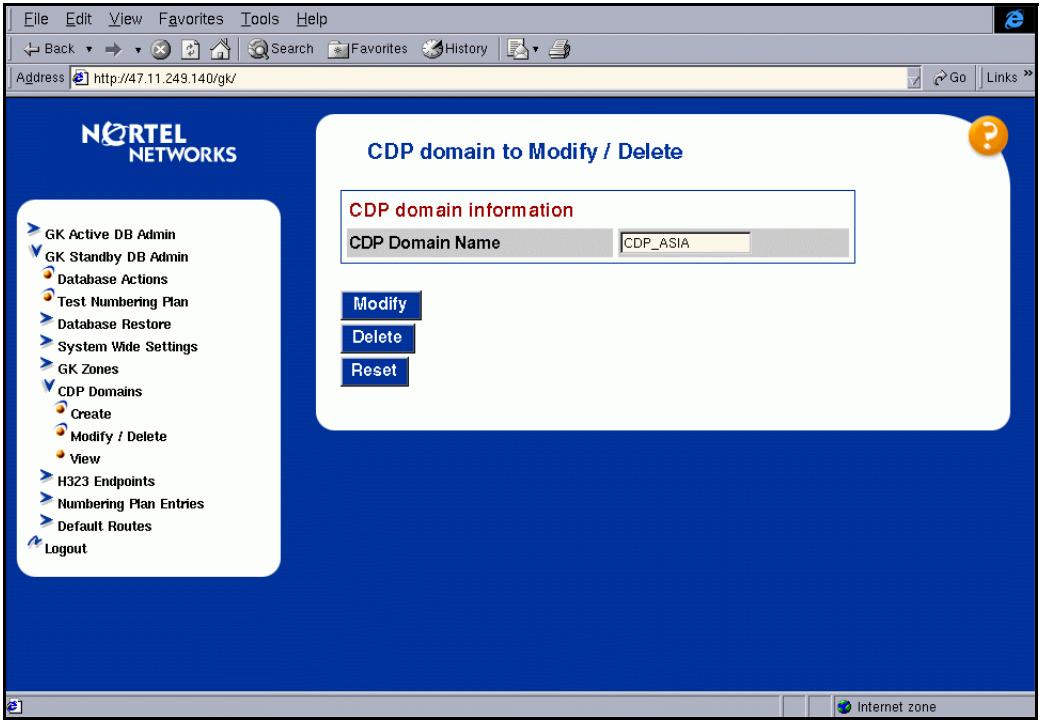


2 Select the CDP domain that you want to modify from **CDP Domain** drop-down list box.

3 Click the **Select** button.

The **CDP domain to Modify / Delete** webpage displays with the selected CDP domain in a text box (see Figure 107 on page 256).

Figure 107
CDP domain to Modify / Delete



4 Change the name of the domain in the **CDP Domain** Name text box.

Note: You can click **Reset** to restore the previous CDP domain name in the text box.

5 Click the **Modify** button. This changes the CDP domain to the name entered in the text box.

A status message displays confirming the change.

End of Procedure

Procedure 25
Deleting a CDP domain

1 Select **GK Standby DB Admin | CDP Domain | Modify / Delete** from the Navigation Tree.

The **Select a CDP domain to Modify/Delete** webpage displays (see Figure 106 on page 255).

2 Select the CDP domain that you want to delete from the **CDP Domain** drop-down list box.

3 Click the **Select** button.

A webpage displays with the selected CDP domain in a text box (see Figure 107 on page 256).

4 Verify that the CDP domain name in the CDP Domain Name text box is the CDP domain that you want to delete.

5 Click the **Delete** button.

A status message displays confirming that the domain has been removed.

End of Procedure

Viewing configured CDP domains

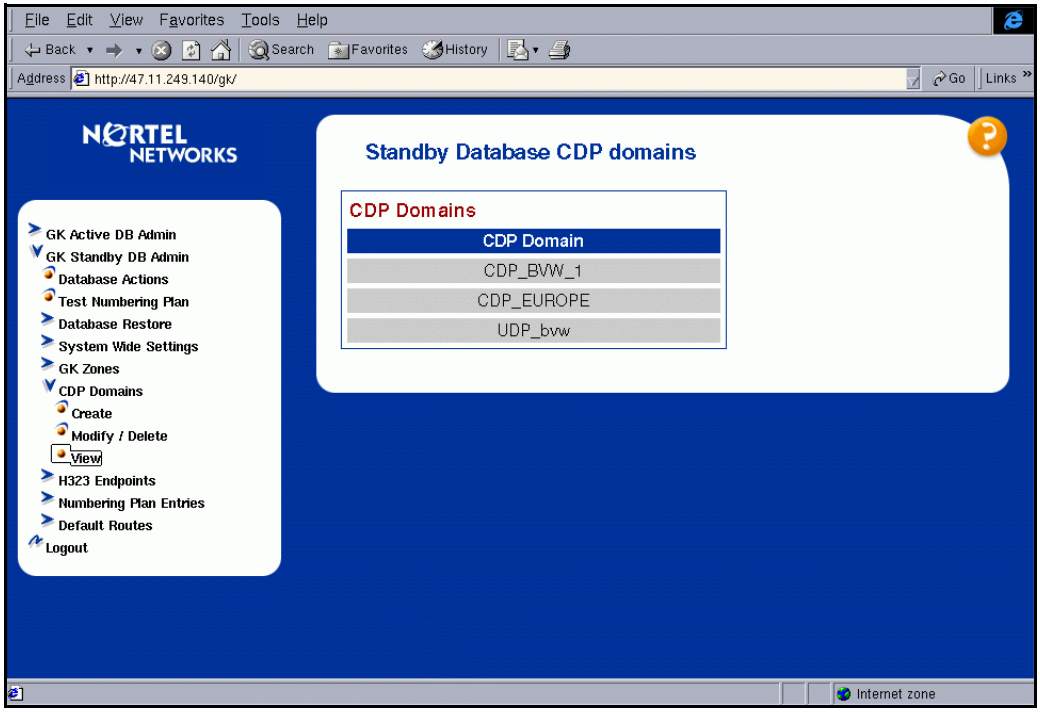
To view all configured CDP domains, follow the steps in Procedure 26.

Procedure 26
Viewing configured CDP domains

1 Select **GK Standby DB Admin | CDP Domains | View** from the Navigation Tree.

The **Standby Database CDP domains** webpage displays (see Figure 108) and displays a list of configured CDP domains.

Figure 108
List of CDP Domains webpage



End of Procedure

Configuring endpoints

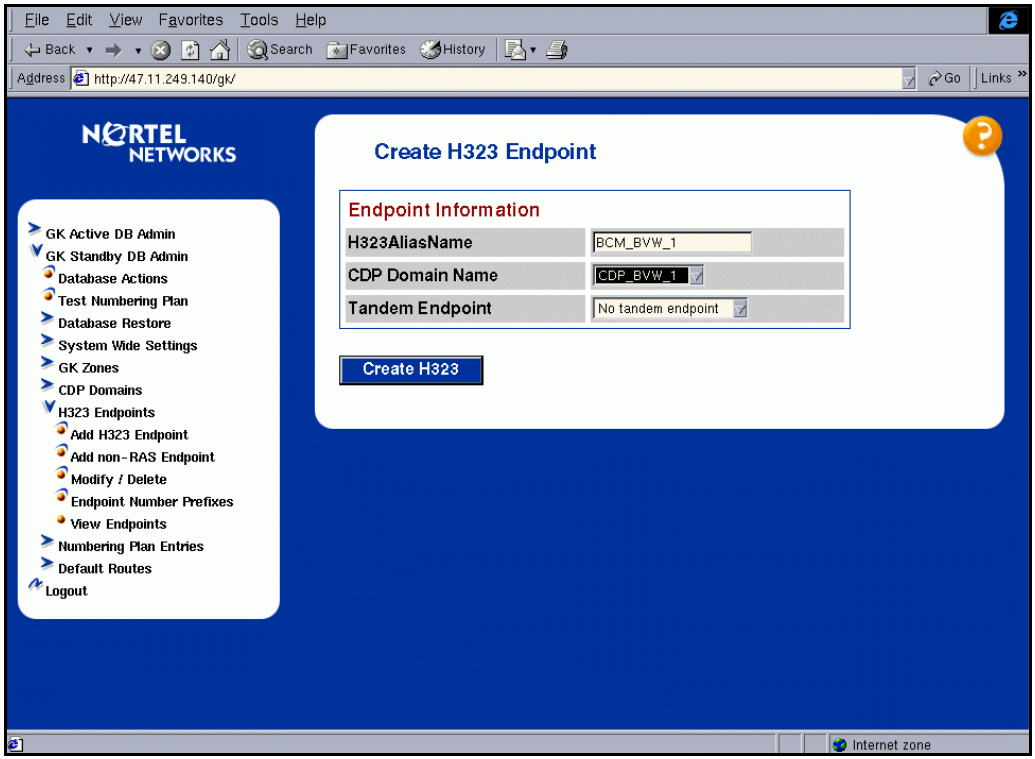
Procedure 27
Creating an H.323 Endpoint

The examples configured in this procedure are stated under the assumption the system-wide settings are complete (Procedure 18 on page 247).

1 Select **GK Standby DB Admin | H323 Endpoints | Add H323 Endpoint** from the Navigation Tree.

The **Create H323 Endpoint** webpage displays (see Figure 109).

Figure 109
Create H323 Endpoint webpage



2 Enter the H.323 alias of the endpoint that you are configuring In the **H323AliasName** text box.

   a. From the example in Figure 27 on page 106, create:

      i. BCM_BVW_1, ITG_GAL_1 H.323 endpoints, belonging to CDP_DOMAIN_2, or

      ii. SCN_MPK_1, SCN_MPK_2, SCN_MPK_3 H.323 endpoints belonging to MPK_CDP_DOMAIN.

   Note 1: The endpoint name (H323AliasName) MUST be the same as the H323-ID specified for the Succession Signaling Server. H.323 aliases are case-sensitive.

   Note 2: The H323AliasName must be a unique name that identifies this endpoint and is 1 - 32 characters in length.

   Note 3: ITG_GAL_1 must be running IP Line 3.1 software.

   b. From the example in Figure 30 on page 137, create Call_Server_A, Call_Server_B, and Branch_Office endpoints.

3 From the **CDP Domain Name** drop-down list box, select the CDP domain to which the endpoint belongs (if it belongs to a CDP domain).

   Note: If the CDP domain that you require is not displayed in the drop-down list box, then it has not been configured. Configure the domain using Procedure 23 on page 253.

4 If this endpoint has a tandem node, select its tandem from the **Tandem Endpoint** drop-down list. This indicate whether the endpoint is used to tandem calls from outside the network.

5 Click the **Create H323** button.

   The Gatekeeper updates the webpage with the result of the operation, indicating whether or not the endpoint was successfully created.

6 Repeat this procedure as often as necessary to create all endpoints.

End of Procedure

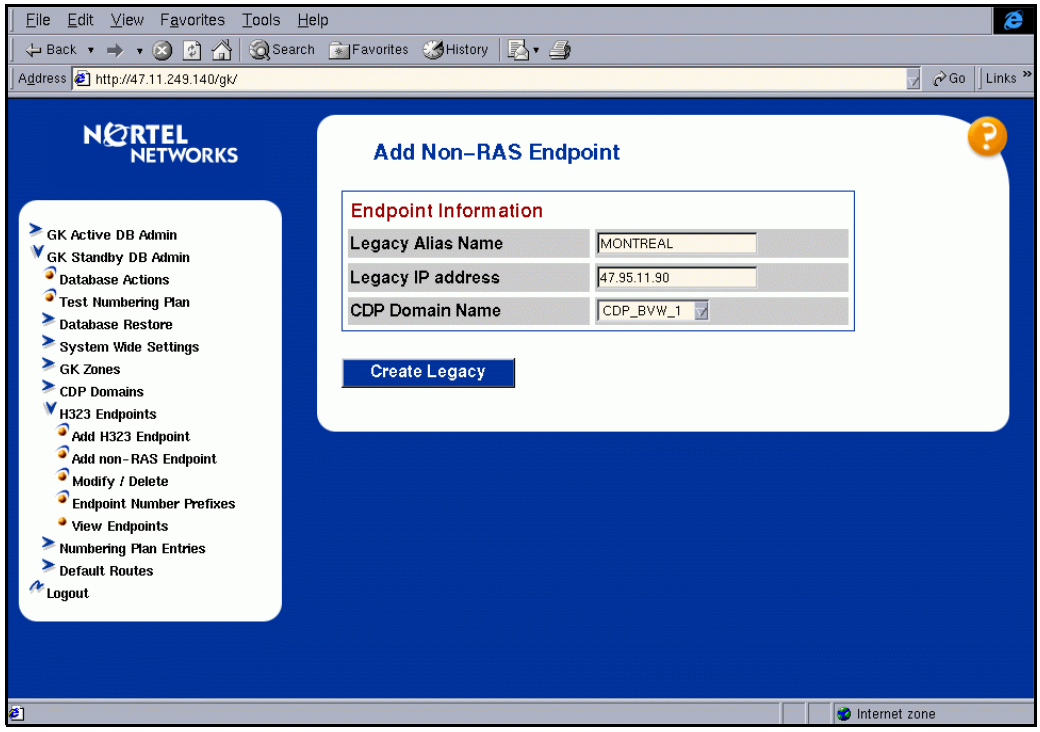
Procedure 28
Adding a non-RAS endpoint

This procedure is normally used for legacy devices because the Gatekeeper uses RAS protocol.

1 Select **GK Standby DB Admin | H323 Endpoints | Add non-RAS Endpoint** from the Navigation Tree.

The **Add Non-RAS Endpoint** webpage displays (see Figure 110).

Figure 110
Add Non-RAS Endpoint webpage



2 Enter the alias name in the **Legacy Alias Name** text box.

Note: The endpoint name can be between 1-32 alphanumeric characters.

From the example in Figure 27 on page 106, from CDP_DOMAIN_2, enter the name “47.102.7.49”.

3 Enter the legacy IP address in the **Legacy IP address** text box.

From the example in Figure 27 on page 106, enter “47.102.7.49”.

4 Select the **CDP domain Name** from the drop-down list box containing all configured CDP domains.

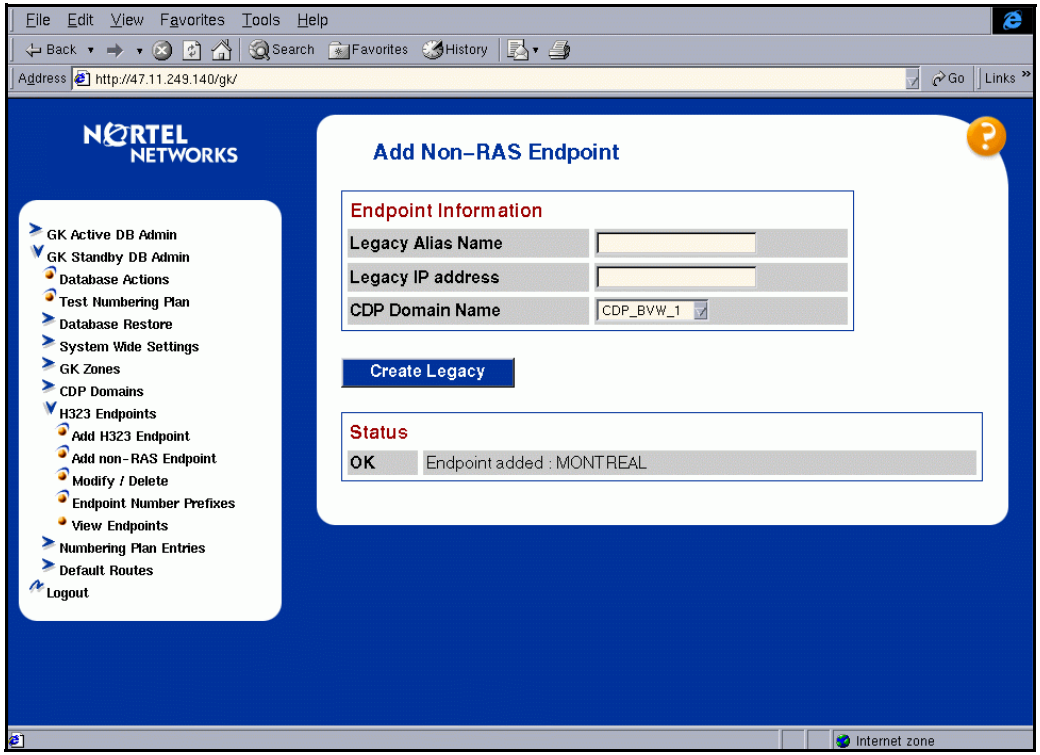
From the example in Figure 27 on page 106, choose CDP_DOMAIN_2.

5 Click the **Create Legacy** button.

The Gatekeeper updates the webpage with the result of the action, indicating whether or not the endpoint was added successfully (see Figure 111 on page 263).

6 Repeat this procedure as often as necessary to create all endpoints.

Figure 111
Add non-RAS Endpoint confirmation



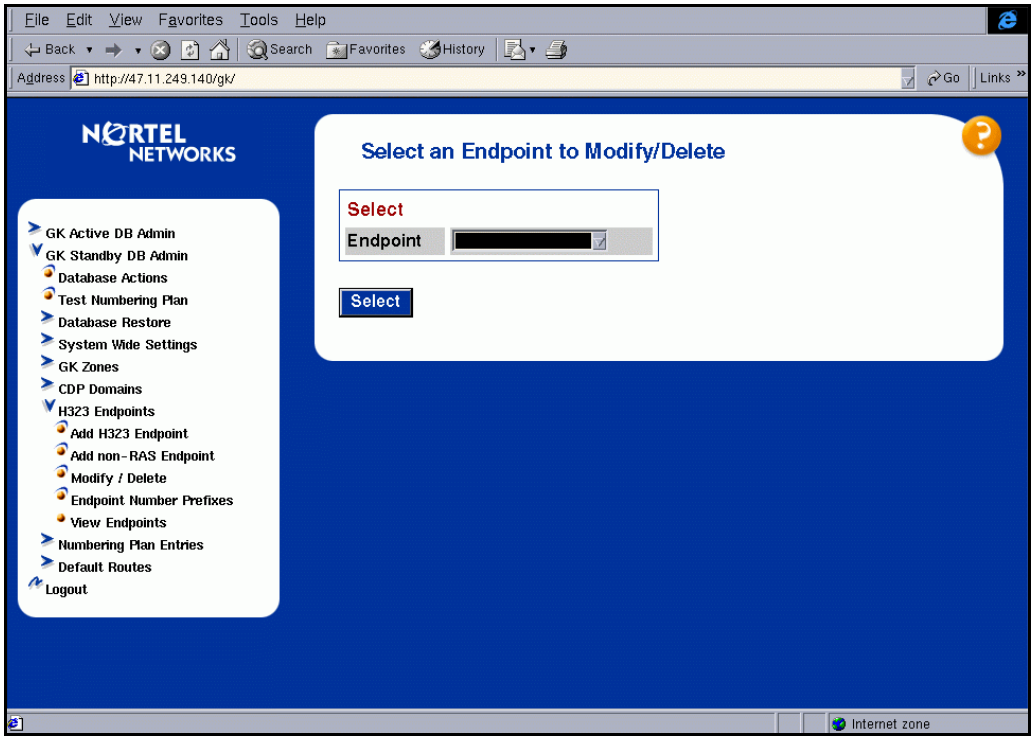
End of Procedure

Procedure 29
Modifying an endpoint

1 Select **GK Standby DB Admin | H323 Endpoints | Modify / Delete** from the Navigation Tree.

The **Select an Endpoint to Modify/Delete** webpage displays (see Figure 112).

Figure 112
Select an Endpoint to Modify/Delete webpage



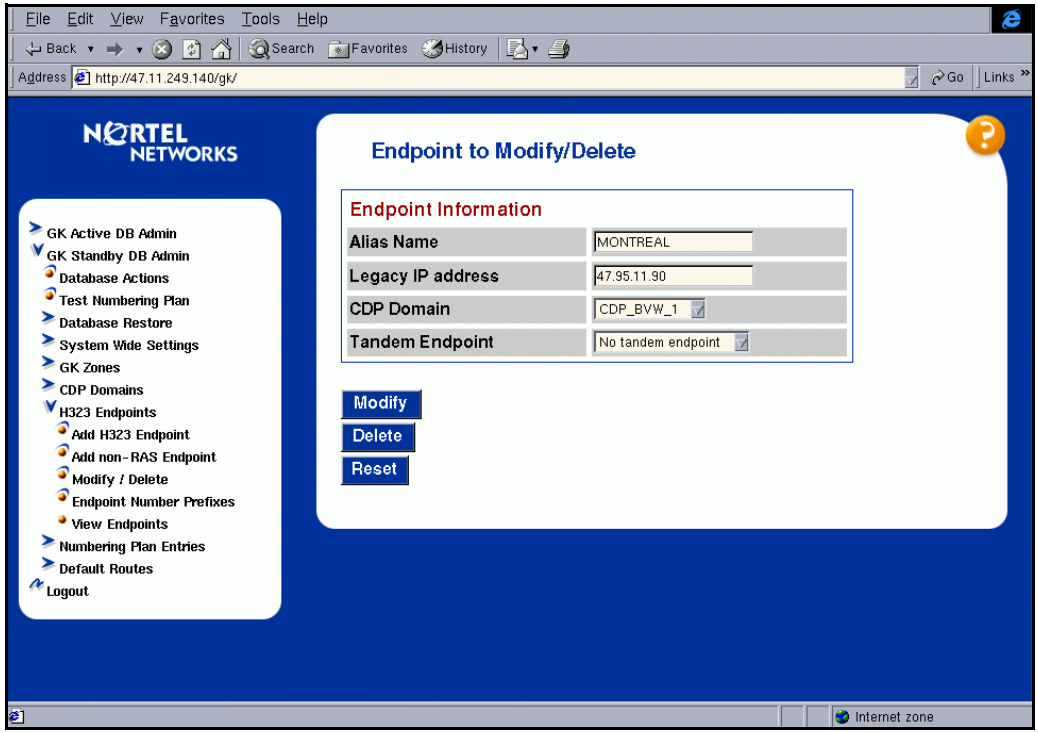
2 From the **Endpoint** drop-down list box, select the endpoint that you want to change.

Note: The Endpoint drop-down list box contains all of the endpoints that are configured in the Gatekeeper.

3 Click the **Select** button.

The **Endpoint to Modify/Delete** webpage displays with all the endpoint information (see Figure 113).

Figure 113
Endpoint to Modify/Delete webpage



4 Verify that the endpoint in the Endpoint in the Alias Name text box is the endpoint that you want to change.

5 Change the information accordingly.

Note: You can click **Reset** to restore the previous information in the text boxes.

6 Click the **Modify** button.

The Gatekeeper updates the webpage with the result of the action, indicating whether or not the endpoint was modified successfully.

End of Procedure

Procedure 30
Deleting an endpoint

1 Select **GK Standby DB Admin | H323 Endpoints | Modify / Delete** from the Navigation Tree.

The **Select an Endpoint to Modify/Delete** webpage displays (see Figure 112 on page 264).

2 Select the endpoint that you want to delete from the **Endpoint** drop-down list box.

Note: The Endpoint drop-down list box contains all of the endpoints that are configured in the Gatekeeper.

3 Click the **Select** button.

The **Endpoint to Modify/Delete** webpage displays (see Figure 113 on page 265).

4 Verify that the endpoint in the Alias Name text box is the endpoint that you want to delete.

5 Click the **Delete** button.

The **Select an Endpoint to Modify/Delete** webpage redisplays and indicates whether the endpoint has been successfully removed.

End of Procedure

Procedure 31
Viewing configured endpoints

There are two locations to view information on all configured endpoints. Each configured endpoint is listed with its associated CDP domain (if any) and its IP address if it is a non-RAS endpoint (that is, a legacy endpoint).

1 Select **GK Active DB Admin | View Endpoints** from the Navigation Tree.

Note: If you click **GK Active DB Admin | View Endpoints**, the Gatekeeper Active Database Endpoints webpage displays (see Figure 114). An **Endpoint Summary** and a list of all **Endpoints** configured in the Gatekeeper are shown on this webpage. This includes third-party endpoints, endpoints that do not support RAS messages, and other Nortel Networks endpoints, such as BCM.

2 Select **GK Standby DB Admin | H323 Endpoints | View Endpoints** from the Navigation Tree (see Figure 115 on page 268).

Each configured endpoint is listed with its associated CDP domain (if any) and its IP address if it is a non-RAS endpoint (that is a legacy endpoint).

Figure 114
Active Database Endpoints webpage

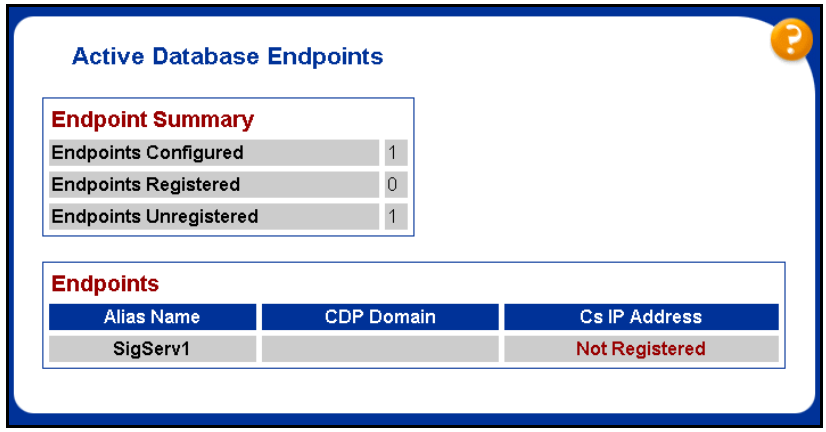
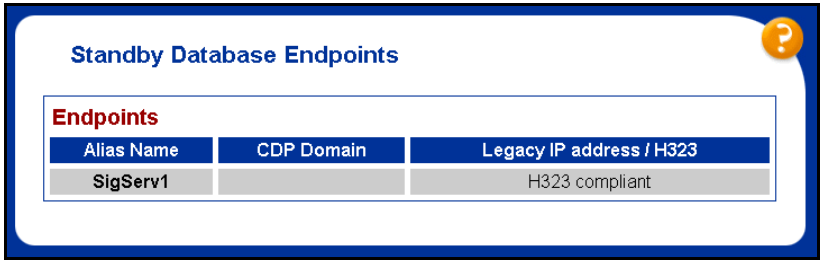


Figure 115
Standby Database Endpoints webpage



End of Procedure

Selecting endpoint number prefixes

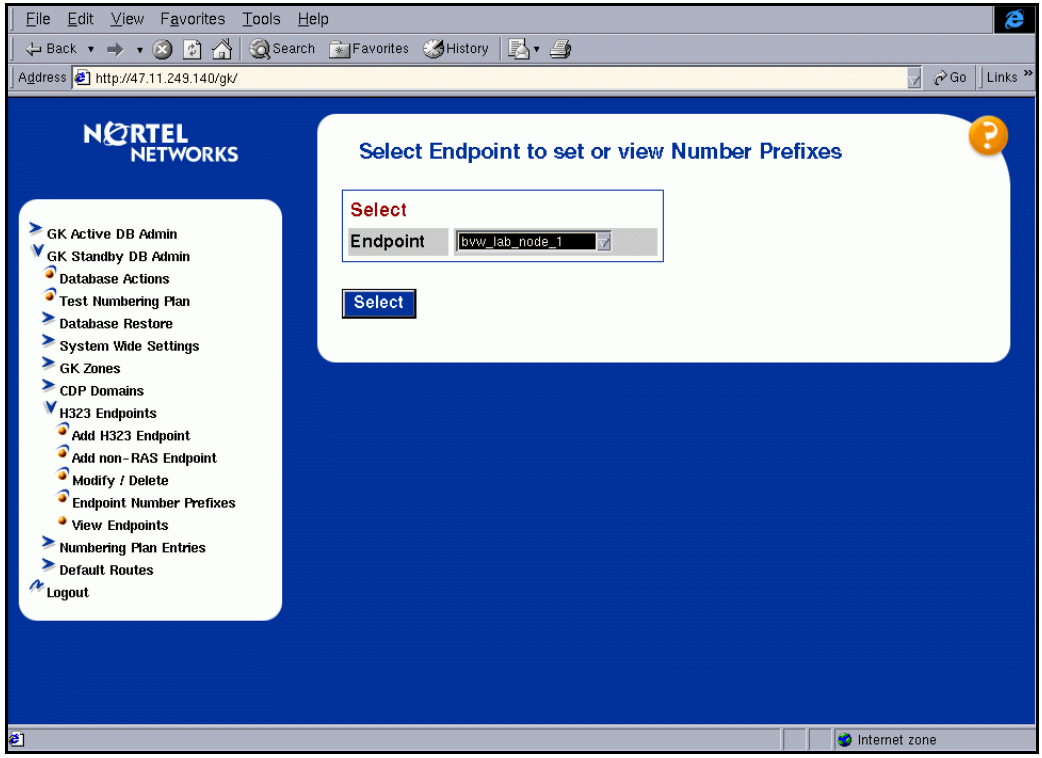
To select the endpoint number prefixes, follow the steps in Procedure 32 on page 268.

Procedure 32
Selecting endpoint number prefixes

1 Select **GK Standby DB Admin | H323 Endpoints | Endpoint Number Prefixes** from the Navigation Tree.

The **Select Endpoint to set or view Number Prefixes** webpage displays (see Figure 116 on page 269).

Figure 116
Select an Endpoint to set or view Number Prefixes webpage

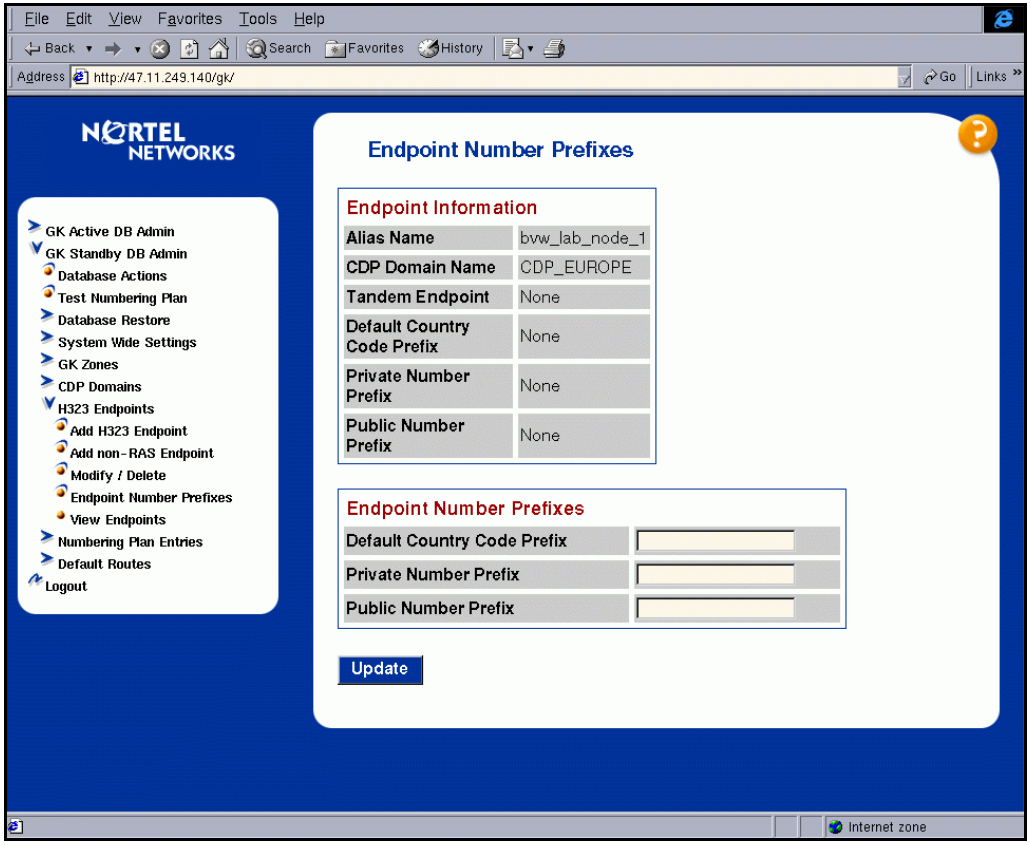


2 Select the Endpoint for which you want to set the number prefixes from the **Endpoint** drop-down list box.

3 Click the **Select** button.

The **Endpoint Number Prefixes** webpage displays (see Figure 117 on page 270).

Figure 117
Endpoint Number Prefixes webpage

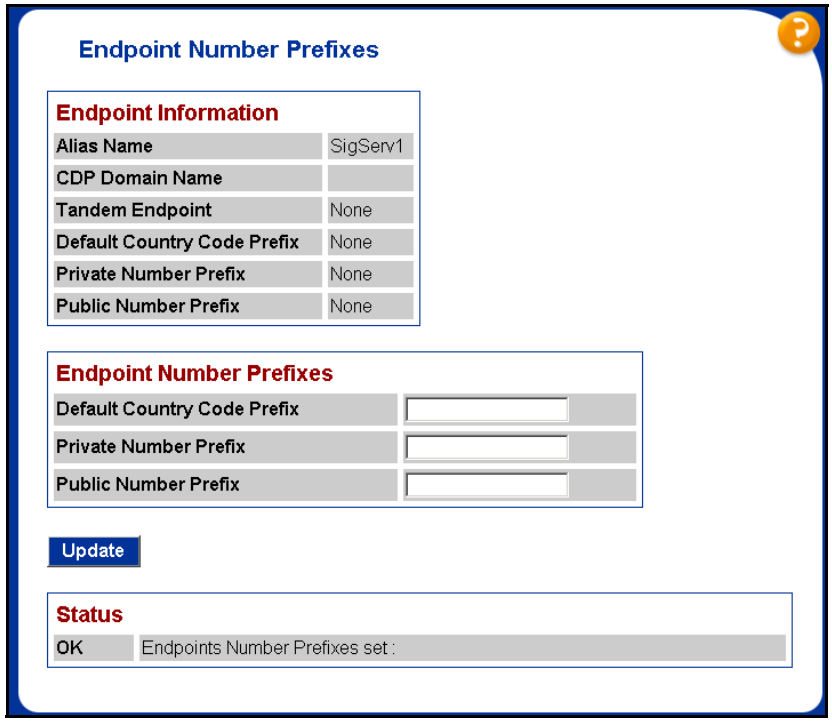


4 Enter the **Default Country Code Prefix**, the **Private Number Prefix**, and the **Public Number Prefix** in the appropriate text boxes.

5 Click the **Update** button.

The status of the update is displayed at the bottom of the webpage (see Figure 118 on page 271).

Figure 118
Endpoint Number Prefixes confirmation webpage



End of Procedure

Configuring numbering plan entries

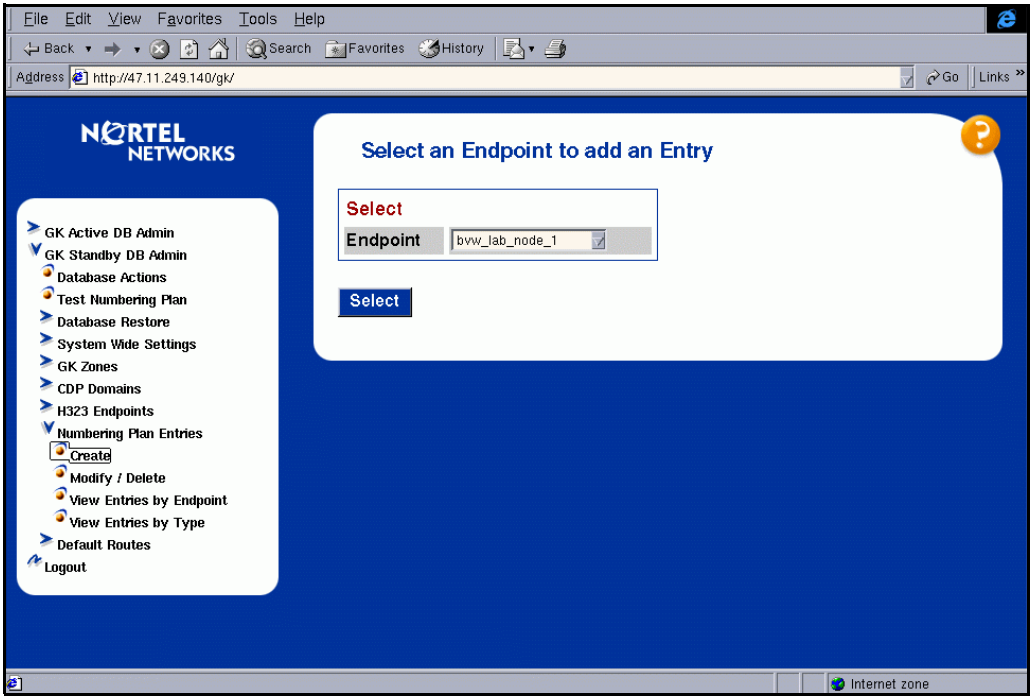
Procedure 33
Configuring numbering plan entries

This procedure uses examples shown in this book. Substitute the examples according to the numbering plan you have planned for your system.

1 Select **GK Standby DB Admin | Numbering Plan Entries | Create** from the Navigation Tree.

The **Select an Endpoint to add an Entry** webpage displays (see Figure 119).

Figure 119
Select an Endpoint to add an Entry webpage



2 Select the **Endpoint** to which you want to add a numbering plan entry from the drop-down list box.

From the example in Figure 27 on page 106, select the following CDP endpoints:

a. BCM_BVW_1

b. 47.102.7.49

c. ITG_GAL_1

d. SCN_MPK_1

e. SCN_MPK_2

f. SCN_MPK_3

Otherwise, select the following for the UDP endpoints:

a. BCM_BVW_1

b. 47.102.7.49

c. ITG_GAL_1

d. SCN_MPK_1

e. SCN_MPK_3

Note: There is no need to make a difference between CDP endpoints and UDP endpoints. The same endpoint can have both CDP and UDP configured. This example is split up for illustrative purposes.

From the example in Figure 30 on page 137, select the following for the Transferable DN endpoints:

a. Call_Server_A

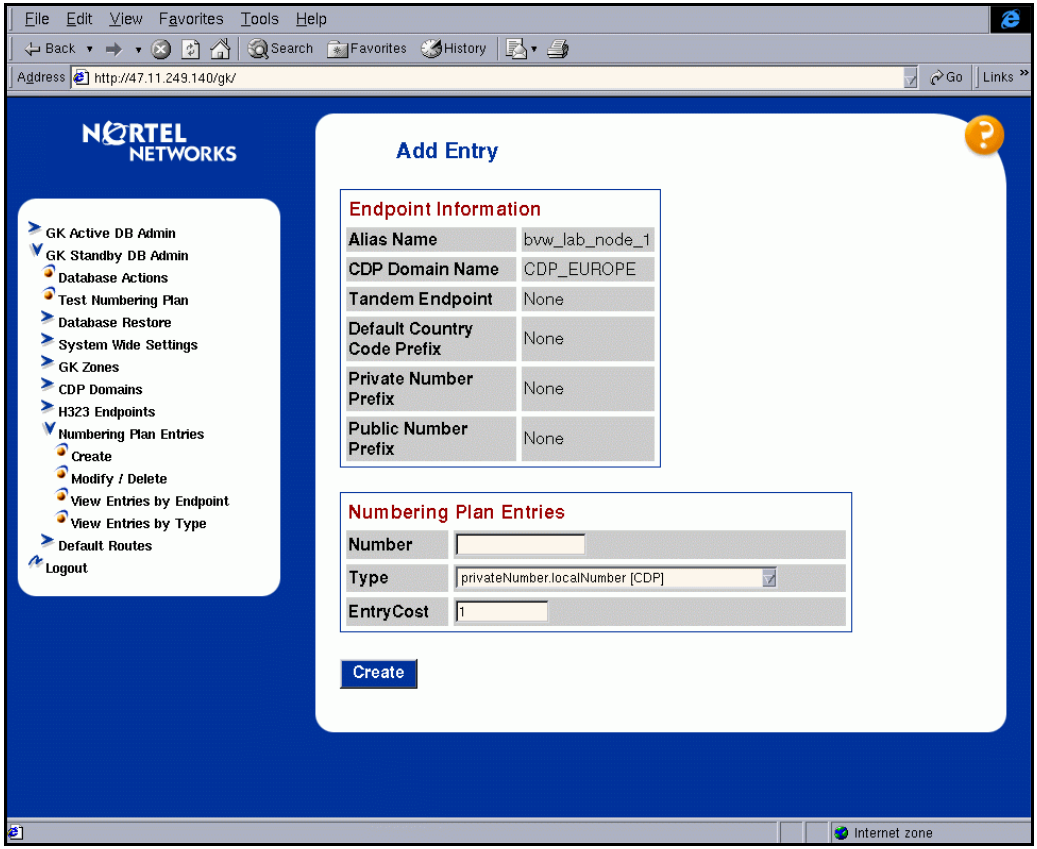
b. Call_Server_B

c. Branch_Office H.323

3 Click the **Select** button.

The **Add Entry** webpage displays (see Figure 120 on page 274).

Figure 120
Add Entry webpage



4 Enter the entry number in the **Number** text box.

From the example in Figure 27 on page 106, configure the following entry numbers with respect to the endpoints in step 2 on page 273:

a. 40-44

b. 49

c. 45-48

d. 40-43

e. 44-47

f. 48-49

From the example in Figure 27 on page 106, configure the following entry numbers with respect to the UDP endpoints in step 2 on page 273:

a. 343; 265; 6651200# (repeat this step for each number)

b. 570

c. 570

d. 265; 343; 665-669 (repeat this step for each number)

e. 2651

5 Select the entry type from the **Type** drop-down list box.

From the example in Figure 27 on page 106, select entry type:

a. privateNumber.localNumber[CDP] for the CDP endpoints

b. privateNumber.level1RegionalNumber[UDP] for the UDP endpoints

c. publicNumber.internationalNumber for International Numbers endpoints

d. publicNumber.nationalNumber for National Numbers endpoints

e. privateNumber.pISNSpecificNumber[SPECIAL] for SPN endpoints

From the example in Figure 30 on page 137, select entry type:

f. privateNumber.localNumber[CDP] for Transferable DN endpoints

6 Enter the entry cost in the **Entry Cost** text box.

From the example in Figure 27 on page 106, enter “1” for each CDP endpoint.

From the example in Figure 27 on page 106, enter the following costs with respect to the UDP endpoints in step 2 on page 273:

a. 1; 2; 1 (repeat this step for each number)

b. 2

c. 1

d. 1; 2; 1 (repeat this step for each number)

e. 1

7 From the example in Figure 27 on page 106, configure the following entry numbers and costs with respect to the International Number endpoints:

   a. (BCM_BVW_1) Number = +1 613, EntryCost = 1; Number +1 408, EntryCost = 2

   b. (47.102.7.49) Number = +352, EntryCost = 1;

   c. (ITG_GAL_1) Number = +353 91, EntryCost = 2; Number = +1 414, EntryCost = 3

   d. (SCN_MPK_1) Number = +1 408, EntryCost = 1; Number = +1 613, EntryCost = 2; Number = +353 91, EntryCost = 3

8 From the example in Figure 27 on page 106, configure the following entry numbers and costs with respect to the National Number endpoints:

   a. (SCN_MPK_1) Number = 414, EntryCost = 1

   b. (SCN_MPK_2) Number = 414, EntryCost = 2

9 From the example in Figure 27 on page 106, configure the following entry numbers and costs with respect to the SPN endpoints:

   (SCN_MPK_2) Number = 265, EntryCost = 1

10 From the example in Figure 30 on page 137, configure the following entry numbers and costs with respect to the Transferable DN endpoints:

   From the example in Figure 30 on page 137, configure the following entry numbers with respect to the Transferable DN endpoints:

   a. (Call_Server_A) Number = 22221#, EntryCost = 1; Number = 22222#, EntryCost = 1; Number = 22223#, Number = 22223#

   b. (Call_Server_B) Number = 22224#, EntryCost = 1; 22225#, EntryCost = 1

11 Click the **Create** button.

   The Gatekeeper updates the webpage with the result of the action, indicating whether or not the entry was created successfully.

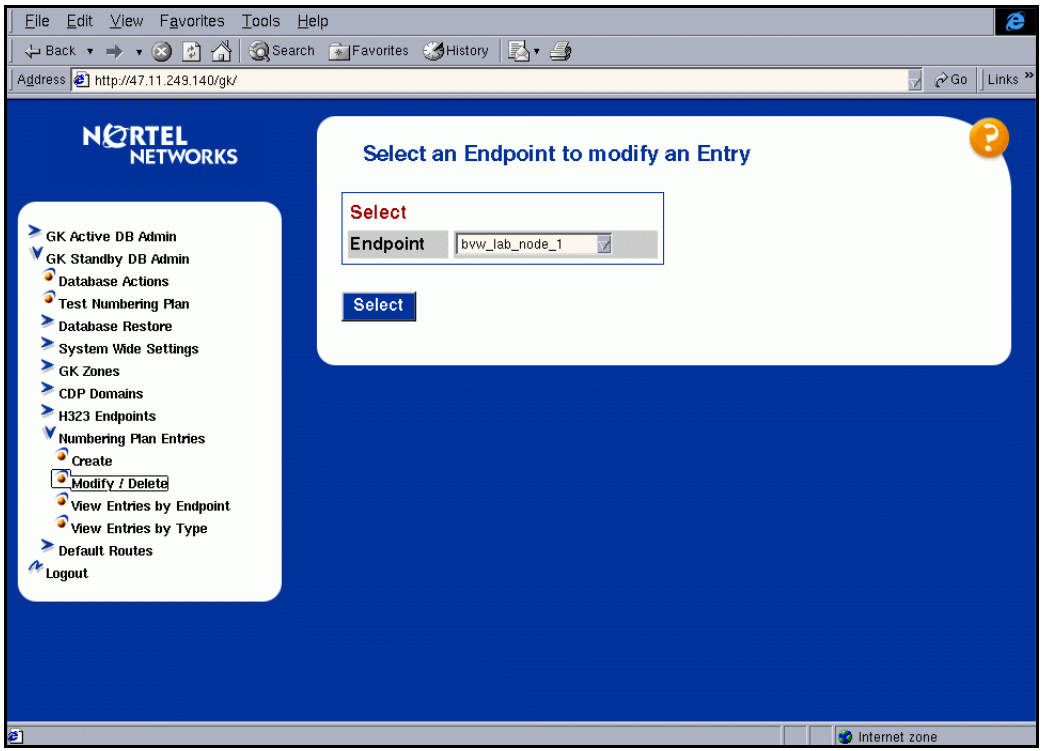
End of Procedure

Procedure 34
Modifying a numbering plan entry

1 Select **GK Standby DB Admin | Numbering Plan Entries | Modify / Delete** from the Navigation Tree.

The **Select an Endpoint to modify an Entry** webpage displays (see Figure 121).

Figure 121
Modify an Entry

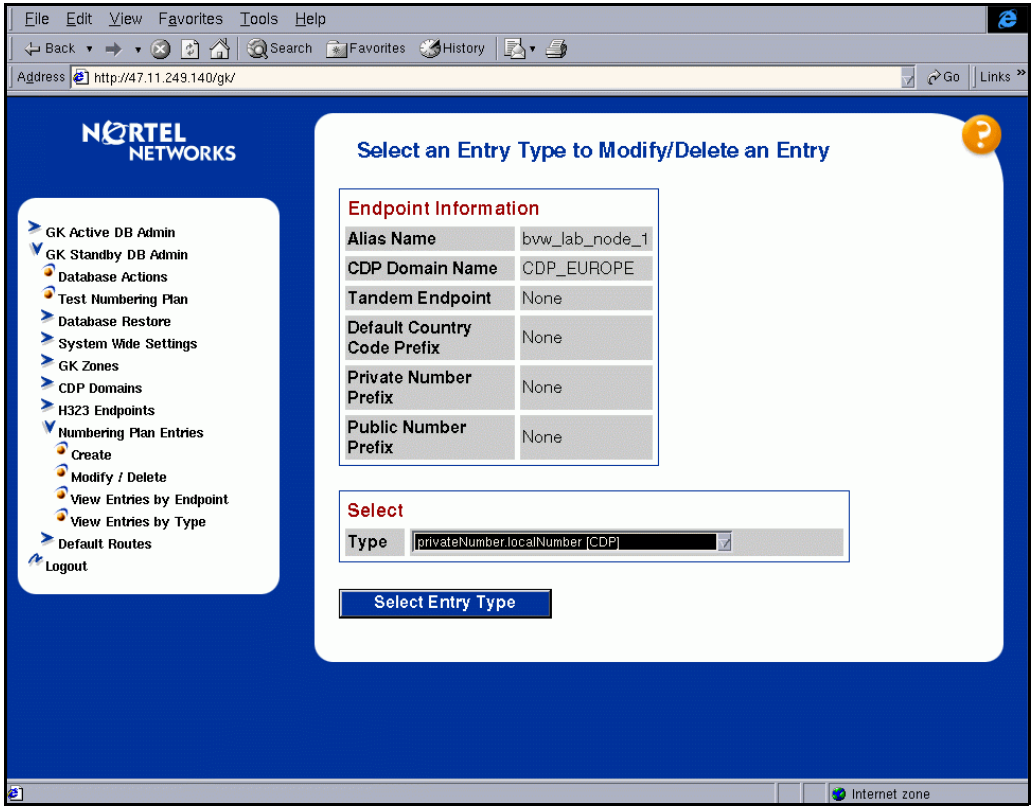


2 From the **Endpoint** drop-down list box, select the endpoint you want to change.

3 Click the **Select** button.

The **Select an Entry Type to Modify/Delete and Entry** webpage displays (see Figure 122 on page 278).

Figure 122
Select Type

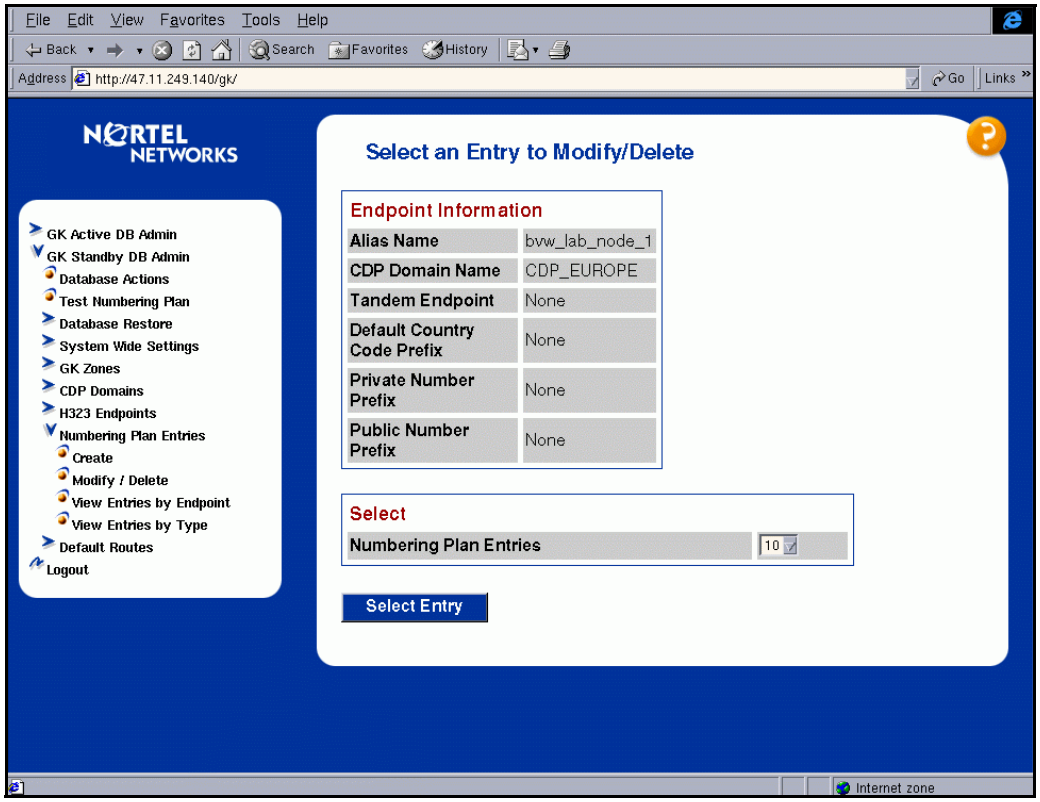


4 Under the **Select** section, select the numbering plan type you want to modify from the **Type** drop-down list box.

5 Click the **Select Entry Type** button.

The screen in Figure 123 on page 279 displays.

Figure 123
Entry to Modify/Delete

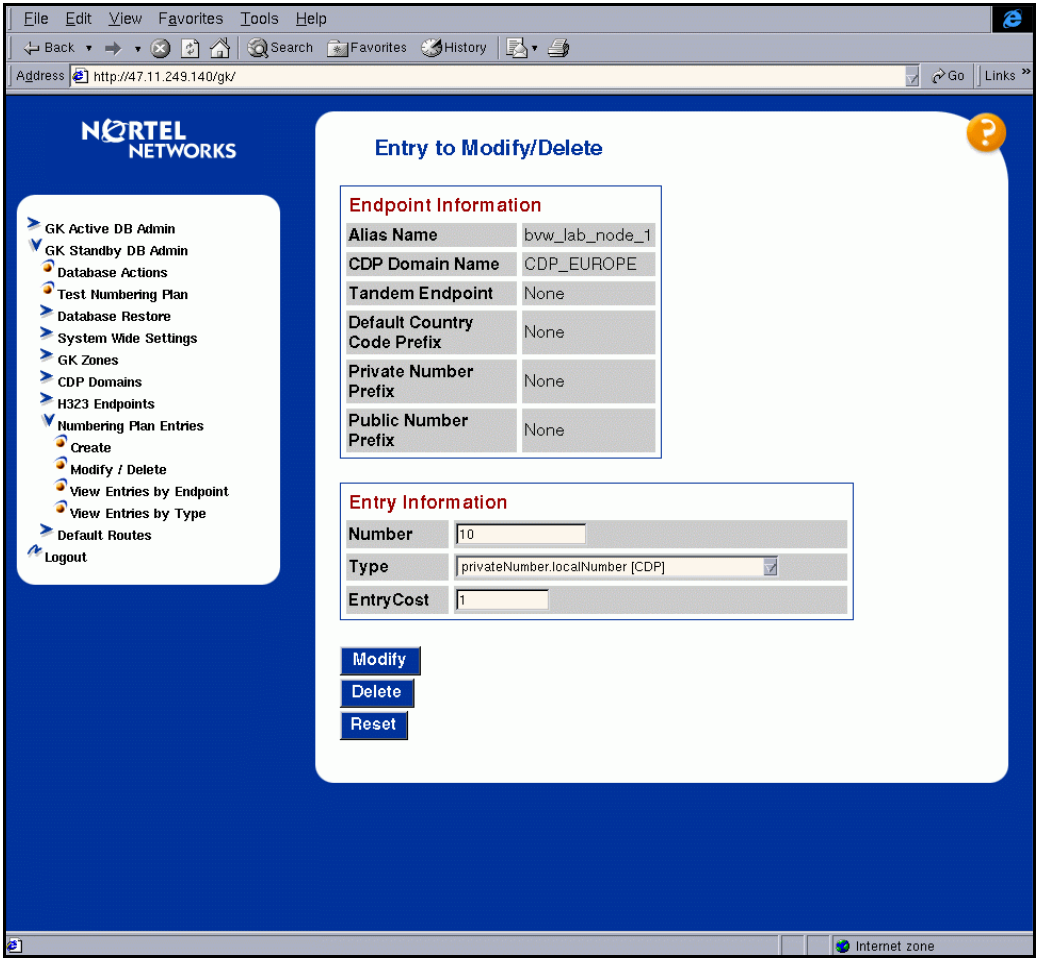


6 From the **Numbering Plan Entries** drop-down list box, select the entry you want to change.

7 Click the **Select Entry** button.

The screen in Figure 124 on page 280 displays.

Figure 124
Entry to Modify/Delete



8 Change the numbering plan entry information as required.

Note: You can click **Reset** to restore the previous information.

9 Click the **Modify** button. The status of the request is displayed at the bottom of the webpage.

End of Procedure

Procedure 35
Deleting an endpoint entry

1 Select **GK Standby DB Admin | Numbering Plan Entries | Modify / Delete** from the Navigation Tree.

The **Select an Endpoint to modify an Entry** webpage displays (see Figure 121 on page 277).

2 From the **Endpoint** drop-down list box, select the endpoint you want to change.

3 Click the **Select** button.

The **Select an Entry Type to Modify/Delete and Entry** webpage displays (see Figure 122 on page 278).

4 From the **Type** drop-down list, select the entry you want to delete.

5 Click the **Select Entry Type** button.

The **Select an Entry to Modify/Delete** webpage displays (see Figure 123 on page 279).

6 Select the entry you want to change from the **Numbering Plan Entries** drop-down list box.

7 Click the **Select Entry** button.

The **Entry to Modify/Delete** webpage displays (see Figure 124 on page 280).

8 Select the entry type from the Type drop-down list box.

9 Click the **Delete** button.

The status of the request is display at the bottom of the webpage.

End of Procedure

Performing database cutover

To perform database cutover, follow the steps in Procedure 36.

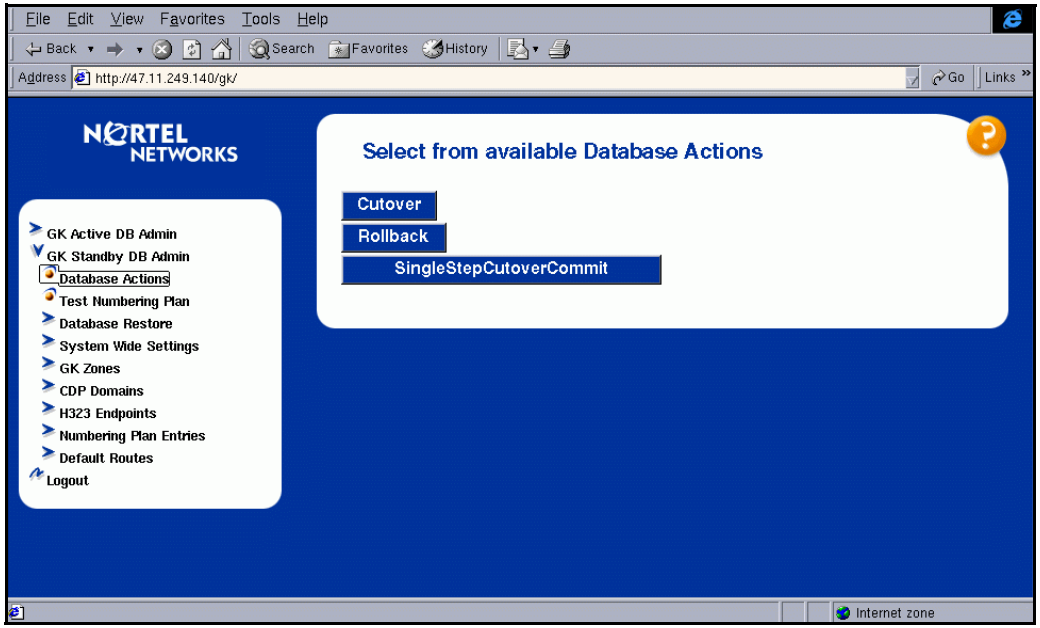
Procedure 36
Performing database cutover

1 Select **GK Standby DB Admin | Database Actions** from the Navigation Tree.

The **Select from available Database Actions** webpage displays (see Figure 125).

Note: If the databases are synchronized, a "Databases are in-sync" message displays.

Figure 125
Select from available Database Actions



2 Choose one of the following:

a. Click the **Cutover** button.

This swaps the primary and standby databases, so configuration changes take effect.

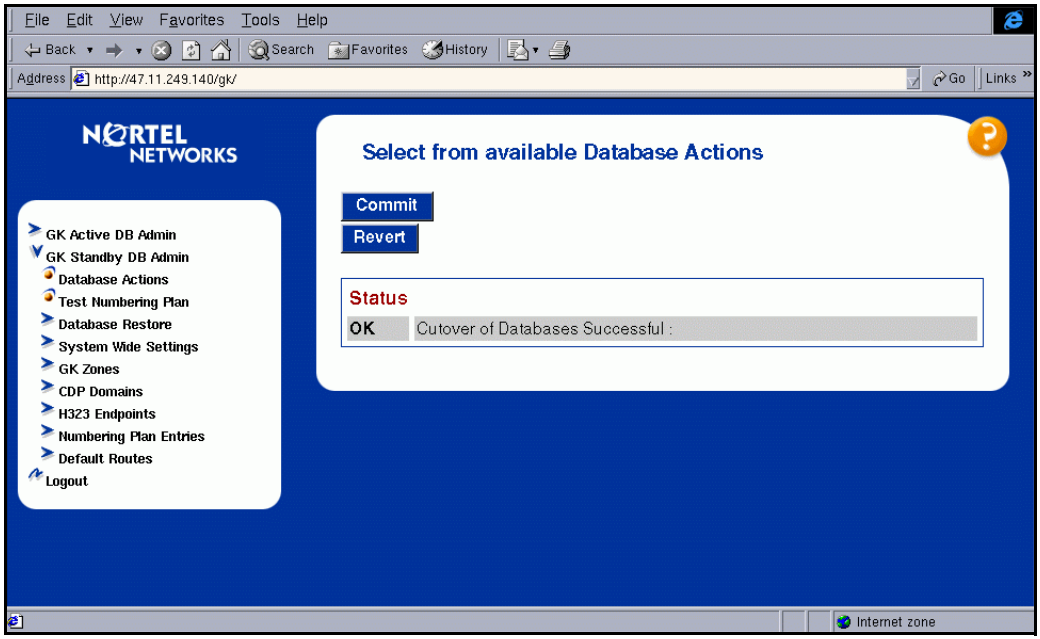
A confirmation webpage displays (see Figure 126 on page 283). Go to step 3 on page 284.

b. Click the **SingleStepCutoverCommit** button.

This swaps the primary and standby databases and synchronizes both the databases with the new configuration. You cannot Rollback to a previous configuration.

A confirmation message displays confirming the cutover (see Figure 127 on page 284).

Figure 126
Cutover confirmation webpage



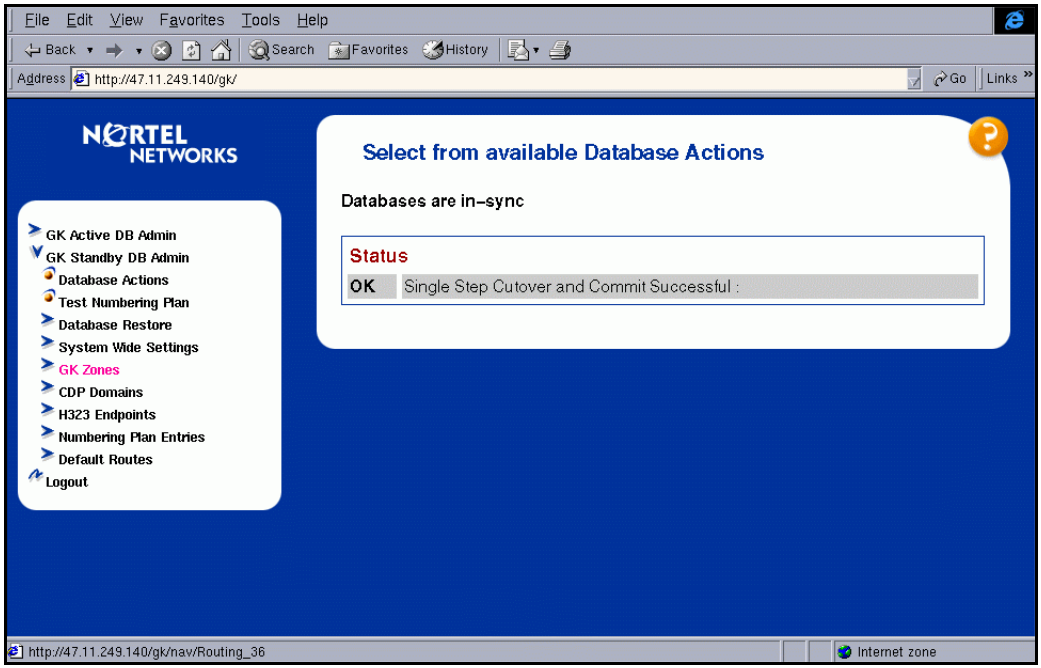
3 Choose one of the following:

a. Click **Commit** to complete the cutover.

> **CAUTION**
>
> If a database has 2000 endpoints, and a change is made to the database and then the change is committed, do not reboot the system (for any reason) for five minutes. Otherwise, some endpoints can be missing from the active database.
>
> If this is the case, the database administrator can recover the missing information by making a change in the standby database and then committing the database.

b. Click **Revert** to revert to the previous active database.

Figure 127
Single Step Cutover and Commit confirmation webpage



4 After database cutover, follow “Viewing configured endpoints” on page 267 to verify how the endpoints register at the Gatekeeper.

5 After database cutover, you can perform the inverse operation to see how the Gatekeeper registers at the endpoints. To do this, log into the Succession Signaling Server at the VxWorks shell (see the *Signaling Server: Installation and Configuration* (553-3001-212) for the procedure) and enter the following command:

```
->npmShow
```

The command shows (see the example in Figure 128 on page 286):

- the Network Protocol Module (NPM) software status (this is the H.323 Gateway Signaling software)
- the active Gatekeeper
- the Gatekeeper registration status, Time-to-Live, and re-registration timers
- the number of busy, idle, and total channels
- the RadVision stack version
- the channel tracing indication (for debug messages related to a specific channel)
- various information about the busy channels (information is truncated in the example)

Figure 128
npmShow command results

Npm status:	Active
Active GateKeeper:	47.11.249.140 (primary)
GateKeeper registration status:	registered, TTL: 295 secs, re-register: 20 secs
Channels Busy / Idle / Total:	4 / 196 / 200
Stack version:	RadVision 3.0.9.5
Channel tracing:	-1

Chan	Direction	Call State	RxState	TxState	Codec	AirTime	FS	MS	Fax
1	Terminate	Offering	-na-	-na	-none-	8	yes	s	no
2	Terminate	Connected	Connected	Connected	G_711_u_law_20MS_NOVAD	5	yes	m	no
3	Originate	RingBack	-na-	-na-	-none-	15	no	s	no
4	Originate	Connected	Connected	Connected	G_711_u_law_20MS_NOVAD	4	yes	s	no

End of Procedure

Database integrity

Prior to Succession 3.0, a user could not access the database using Element Manager while a Commit, SingleStepCommit, or Rollback operation was in progress. This restriction guaranteed the database integrity (that is, the user could not add or view an Endpoint when a Commit was in progress).

Succession 3.0 Software can process commands from Element Manager while either of these operations are in progress. However, to maintain database integrity, checks are performed to see if a Commit, SingleStepCommit, or Rollback operation is in progress. If a user clicks a button in Element Manager that issues a command which requires database access, and any one of the operations is in progress, appropriate status messages are displayed (Figure 129 shows a status message).

Figure 129
Database status

Testing numbering plans

To test numbering plan entries, follow the steps in Procedure 37.

Procedure 37
Testing numbering plan entries

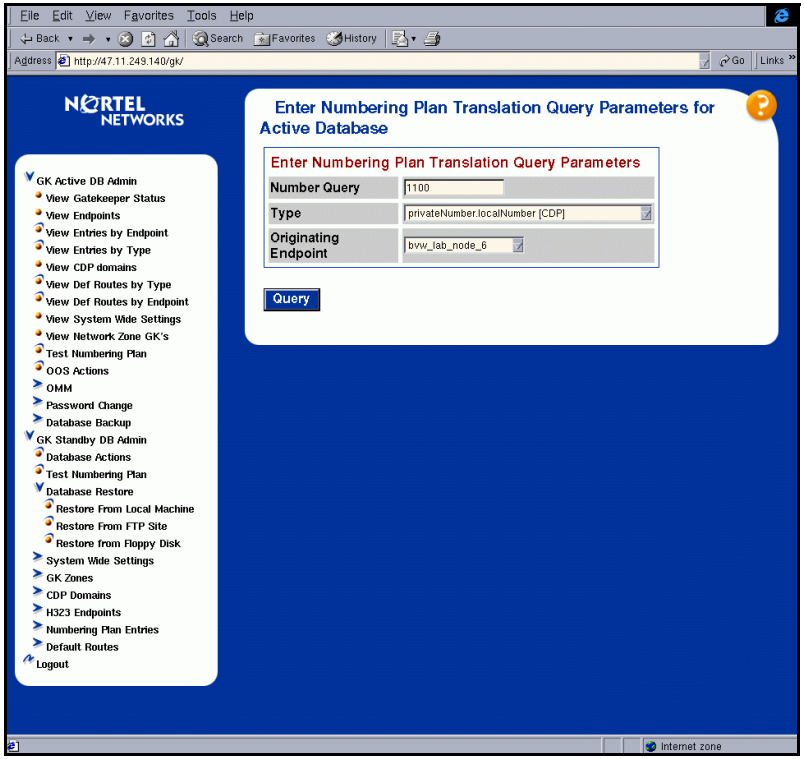
1 Select **GK Standby DB Admin | Test Numbering Plan** from the Navigation Tree.

or

Select **GK Active DB Admin | Test Numbering Plan** from the Navigation Tree if the test is against the active database.

The **Enter Numbering Plan Translation Query Parameters for [Active or Standby] Databases** webpage displays. Figure 130 shows the webpage for the Active Database.

Figure 130
Enter Numbering Plan Translation Query Parameters for Active Database webpage



2 Enter the telephone number in the **Number Query** text box.

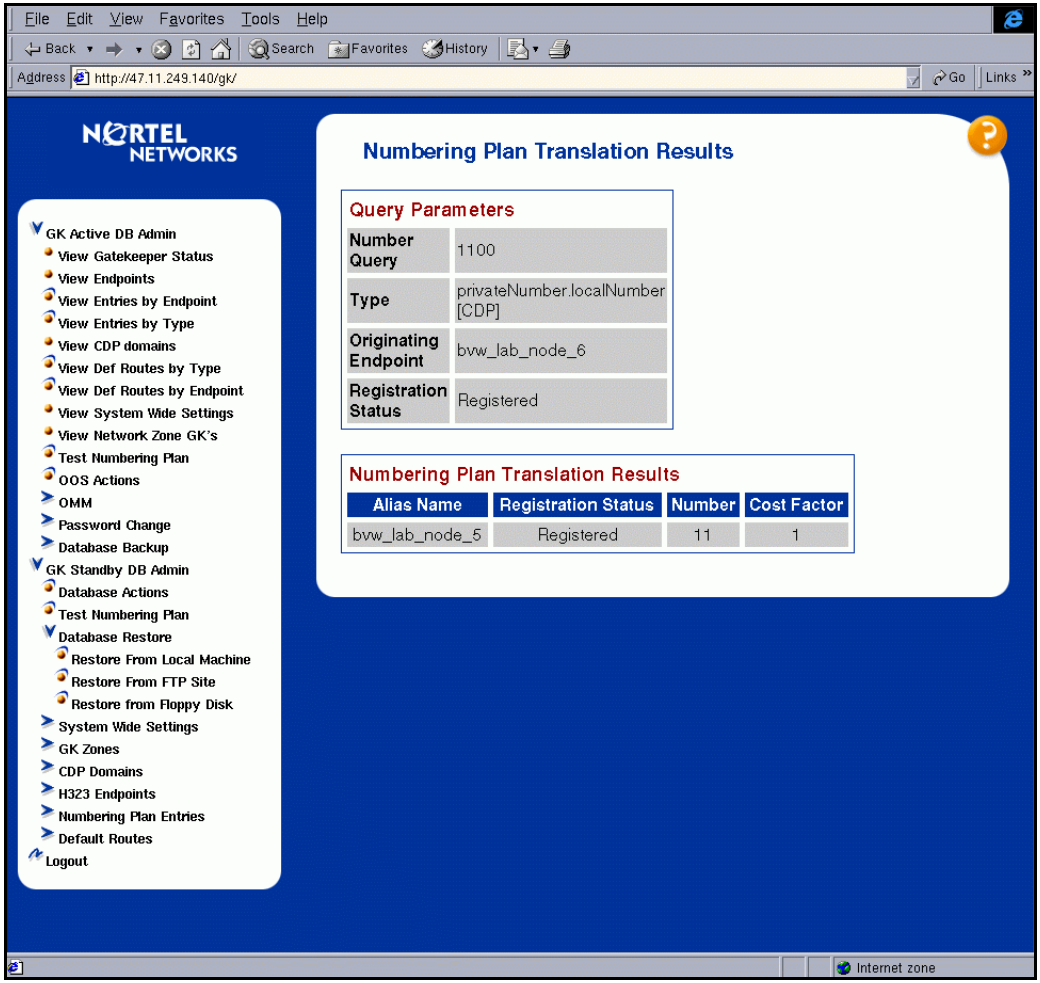
3 Select the alias type from the **Type** drop-down list box.

4 Select the endpoint where the call originates from the **Originating Endpoint** drop-down list box.

5 Click the **Query** button to see if the number is configured on the selected endpoint.

The **Numbering Plan Translation Results** webpage displays (see Figure 131).

Figure 131
Numbering Plan Translation Results webpage



End of Procedure

Backing up the Gatekeeper

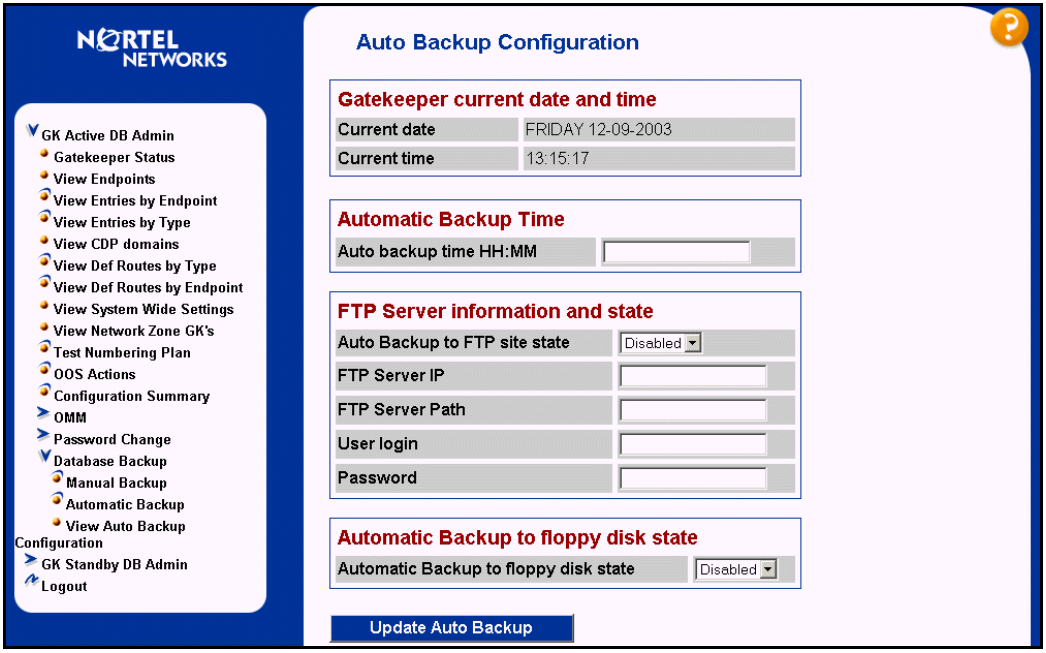
Element Manager provides a facility for backing up the Gatekeeper.

Procedure 38
Backing up the Gatekeeper

1 Select **GK Active DB Admin | Database Backup | Automatic Backup** from the Navigation Tree.

The **Auto Backup Configuration** webpage displays (see Figure 132).

Figure 132
Automatic Backup Configuration webpage



2 Enter the **Automatic Backup Time** information:

   a. Enter the hour (HH) and minute (MM) that you want Gatekeeper to produce a backup file in the **Auto backup time HH:MM** text box. Use 24-hour format (for example, 13:01).

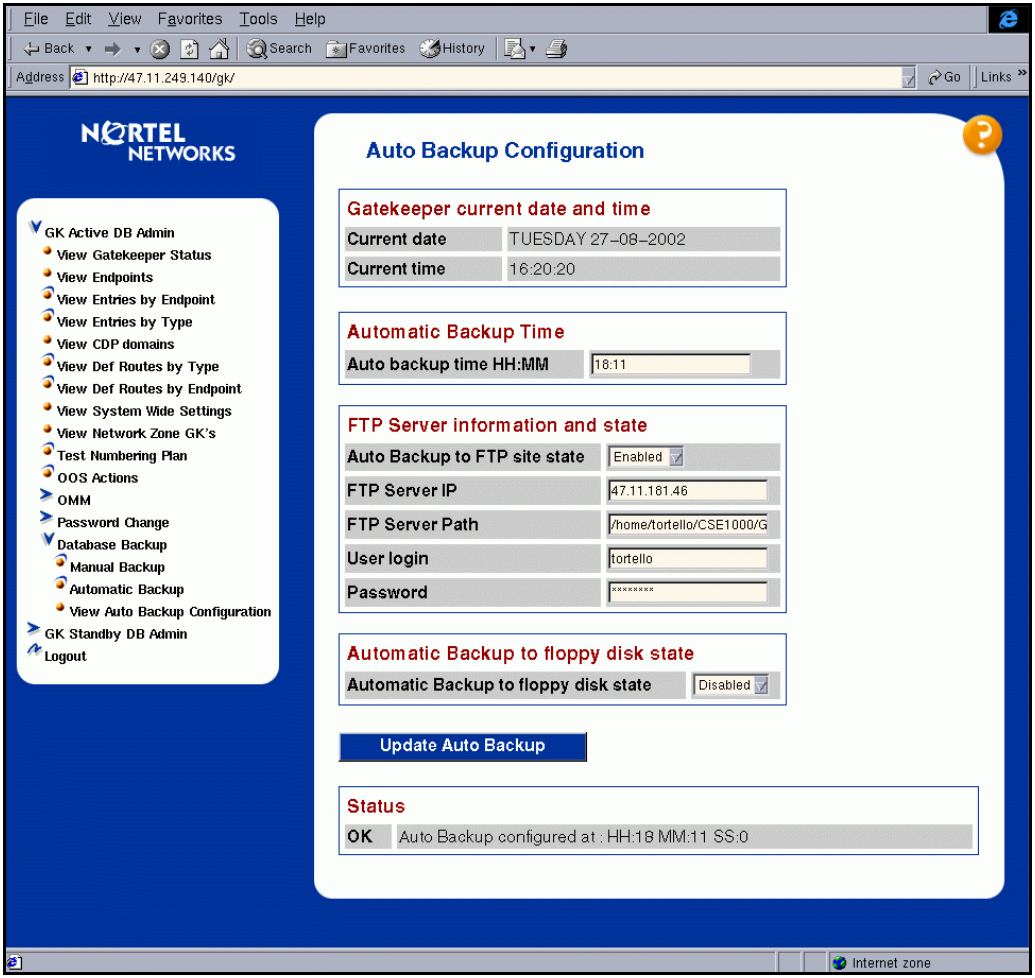
3 Specify the storage location for the backup file. The backup files can be transfer to an FTP server, to a floppy disk, or to both.

   - If you want to back up to the FTP server, enter the **FTP Server information and state** parameters:
     - **Auto backup to FTP site state**: If Enabled, the Gatekeeper transfers the backup file to the defined FTP server.
     - **FTP Server IP**: Enter the IP address of the FTP server.
     - **FTP Server Path**: Enter the network path to the FTP server.
     - **User login**: Enter the user ID of an active account on the FTP server.
     - **Password**: Enter the password for the FTP server account.
   - If **Automatic Backup to floppy disk state** is enabled, the Gatekeeper sends the backup file to the floppy-disk drive on your local machine. Make sure a disk is present to accept the file.

4 Click the **Update Auto Backup** button.

   The status area displays at the bottom of the webpage in Figure 133 on page 292.

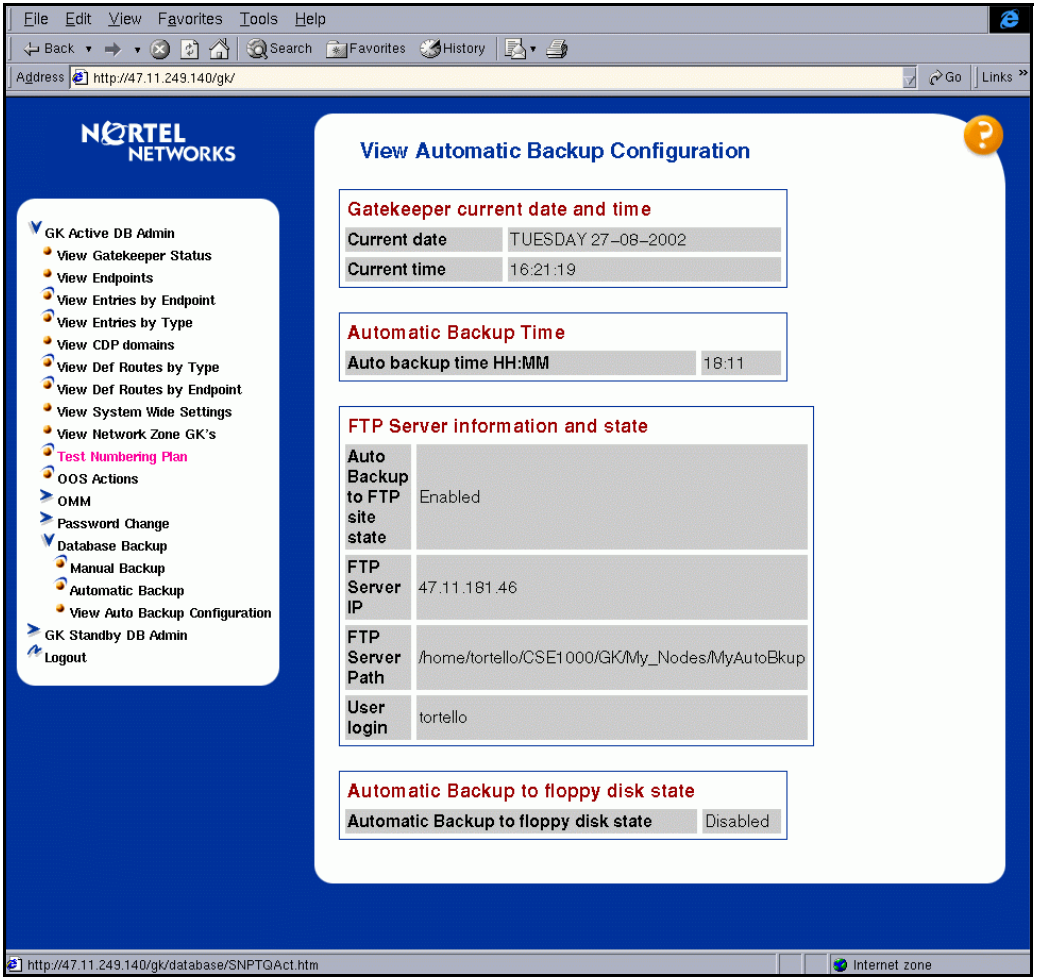
Figure 133
Update Auto Backup



5 To view the Automatic Backup Configuration parameters, click the **GK Active DB Admin | Database Backup | View Automatic Backup Configuration**.

The **View Automatic Backup Configuration** webpage displays as shown in Figure 134 on page 293.

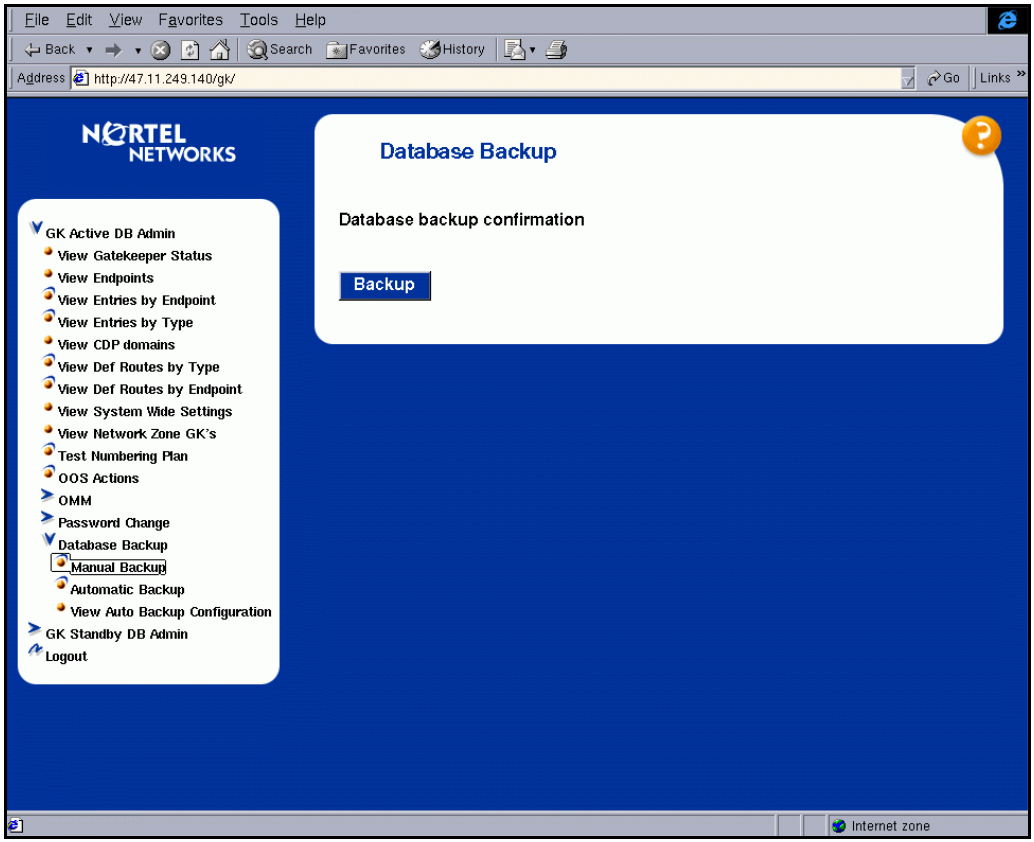
Figure 134
View Automatic Backup Configuration



6 If you wish to perform a manual backup of the database, select **GK Active DB Admin | Database Backup | Manual Backup** from the Navigation Tree.

The Database Backup webpage displays as in Figure 135.

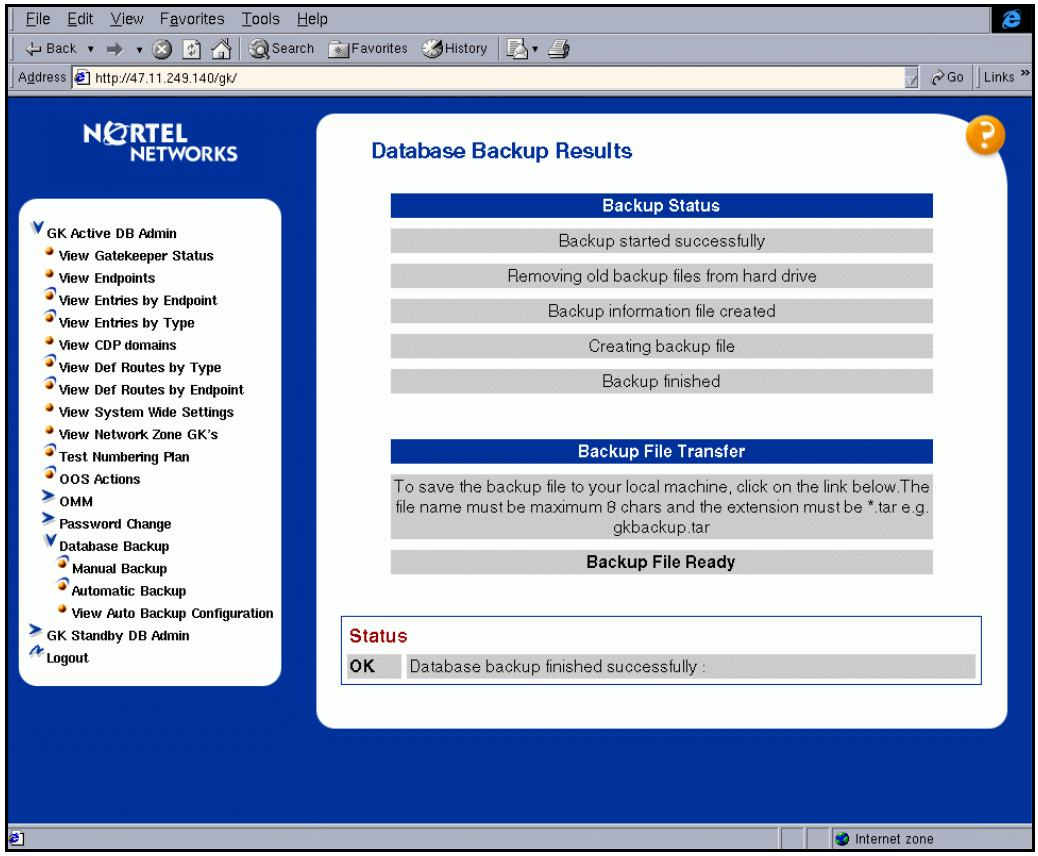
Figure 135
Manual database backup



7 Click the **Backup** button.

The **Database Backup Results** webpage displays as shown in Figure 136 on page 295.

Figure 136
Manual Database Backup Results



End of Procedure

Logging out

To log out of the Gatekeeper webpages in Element Manager, follow the steps in Procedure 39.

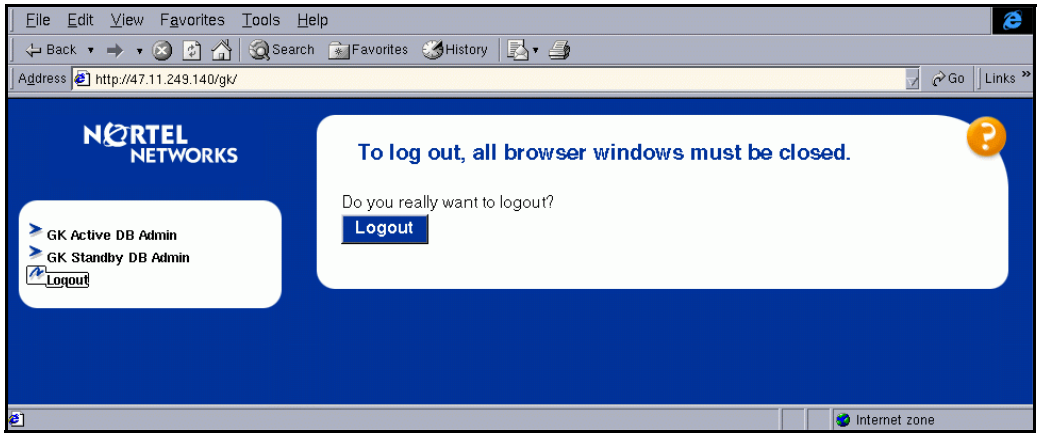
Procedure 39
Logging out of the Gatekeeper webpage in Element Manager

1 Select **Logout** from the Navigation Tree.

The Logout webpage displays (see Figure 137).

Note: All browser windows must be closed in order to log out.

Figure 137
Logout webpage



2 Click the **Logout** button.

A dialog box displays confirming if you want to close the window (see Figure 138 on page 297).

Figure 138
Close window dialog box

3 Click the **Yes** button.

The browser window closes.

End of Procedure

Gatekeeper tasks

Contents

This section contains information on the following topics:

Configuring default routes

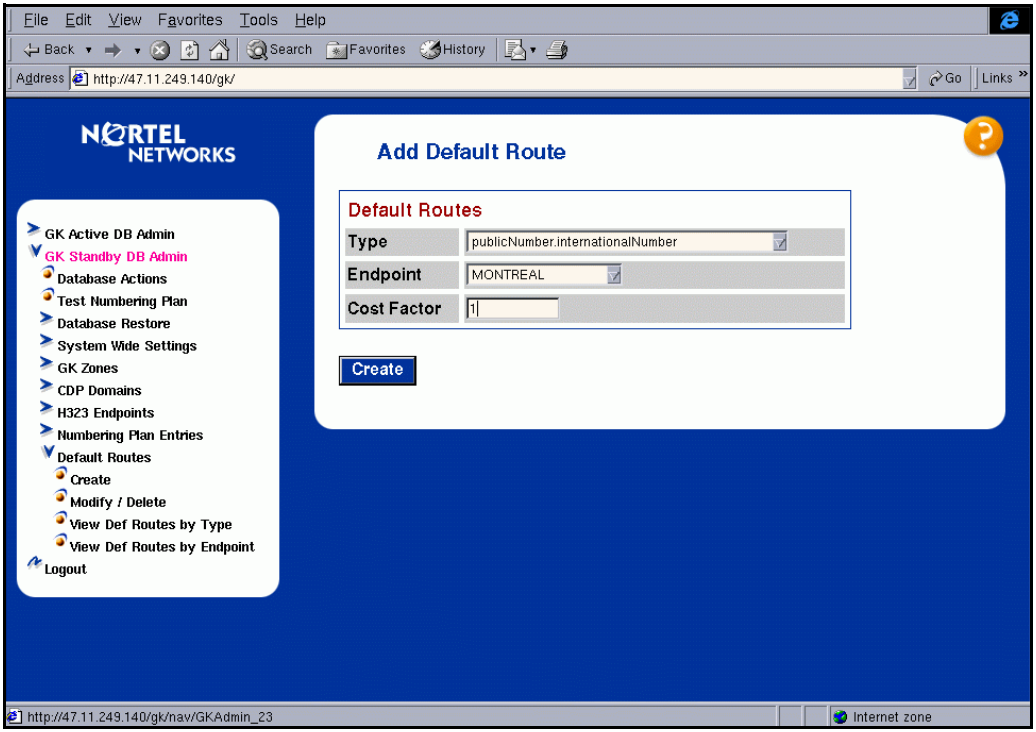
Procedure 40
Adding a default route

1 Log in to the Gatekeeper webpages in Element Manager (see Procedure 16 on page 242).

1 Select **GK Standby DB Admin | Default Routes | Create** from the Navigation Tree.

The **Add Default Route** webpage displays (see Figure 139 on page 300).

Figure 139
Add Default Route webpage



2 Select the alias type from the **Type** drop-down list box.

3 Select the endpoint from the **Endpoint** drop-down list box.

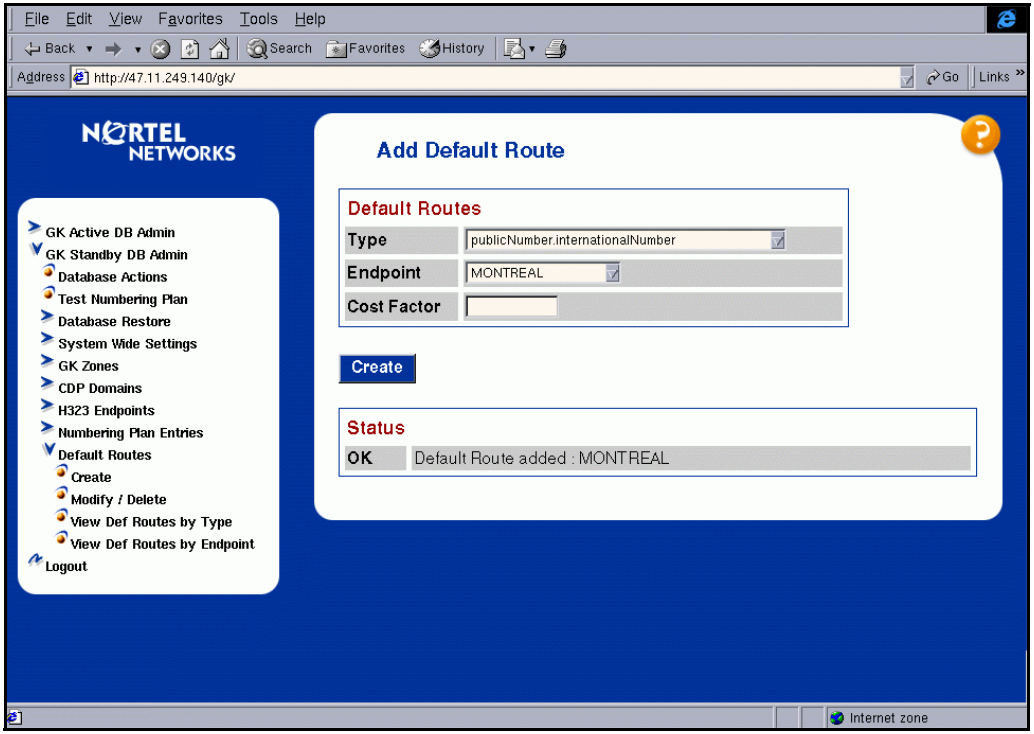
4 Enter the cost factor in the **Cost Factor** text box. The range is 1-225.

Note: This is the number used to define least cost routing. Higher numbers indicate higher costs.

5 Click the **Create** button.

The status display at the bottom of the webpage with a confirmation of whether or not the default route was added (see Figure 140 on page 301).

Figure 140
Add Default Route confirmation webpage



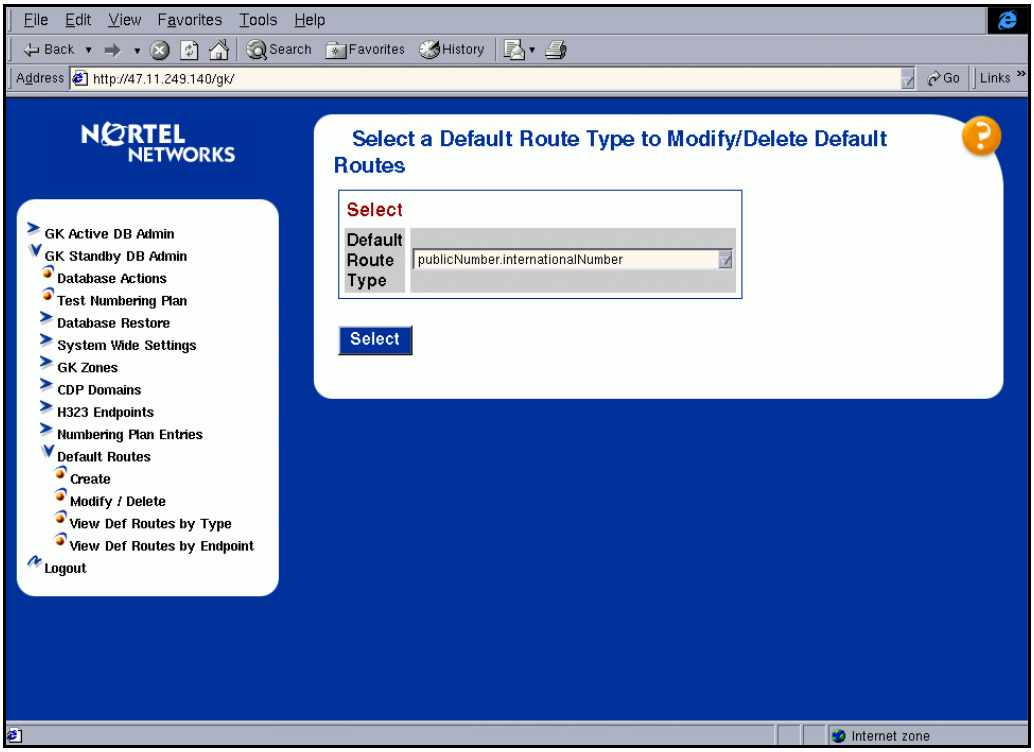
End of Procedure

Procedure 41
Modifying a default route

1 Select **GK Standby DB Admin | Default Routes | Modify / Delete** from the Navigation Tree.

The **Select a Default Route Type to Modify/Delete Default Routes** webpage displays (see Figure 141).

Figure 141
Select a Default Route Type to Modify/Delete Default Routes webpage

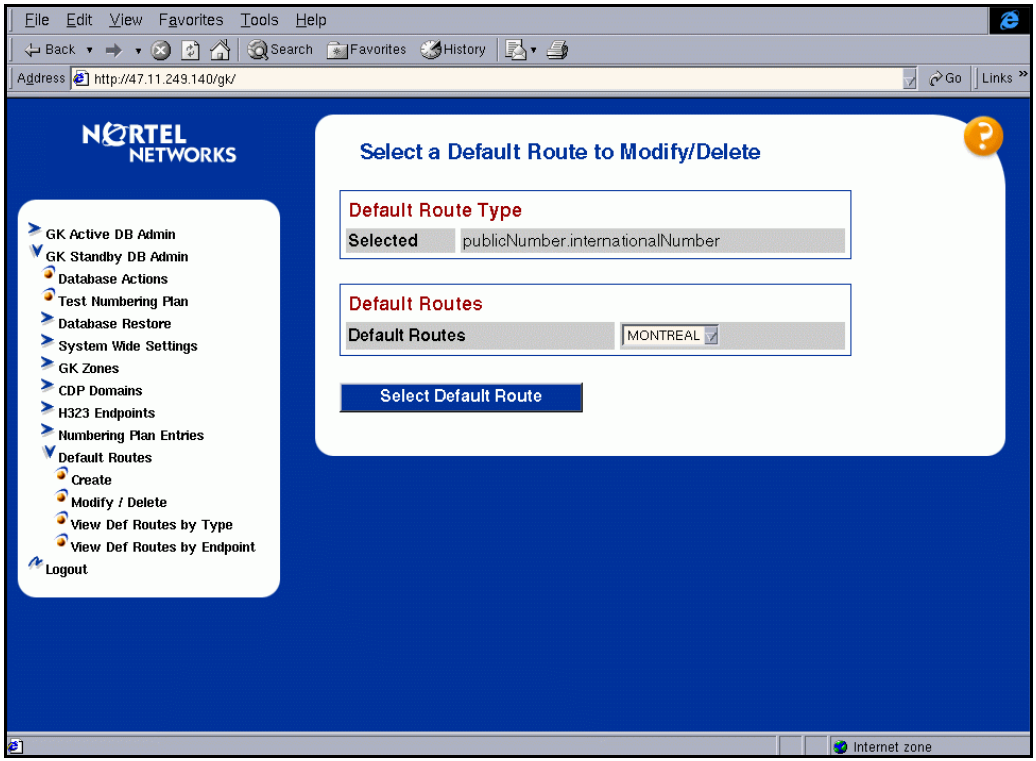


2 Select the default route type from the **Default Route Type** drop-down list box.

3 Click the **Select** button.

The **Select a Default Route to Modify/Delete** webpage displays (see Figure 142 on page 303).

Figure 142
Select a Default Route to Modify/Delete webpage

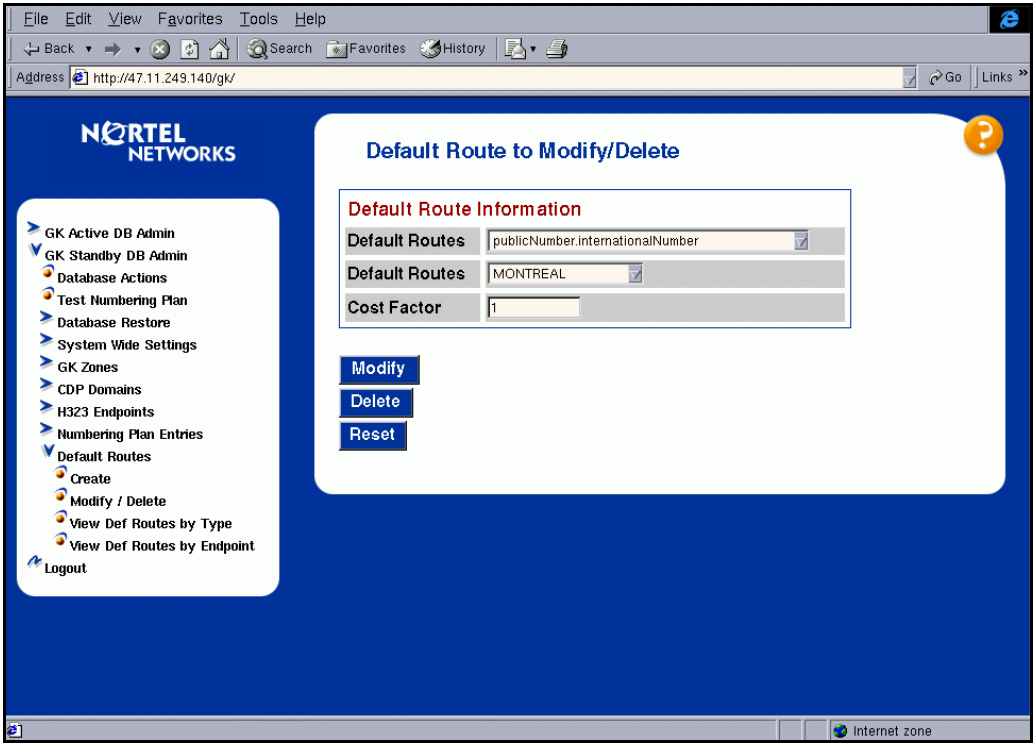


4 Select the default route from the **Default Routes** drop-down list box.

5 Click the **Select Default Route** button.

The **Default Route to Modify/Delete** webpage displays (see Figure 143 on page 304).

Figure 143
Default Route to Modify/Delete



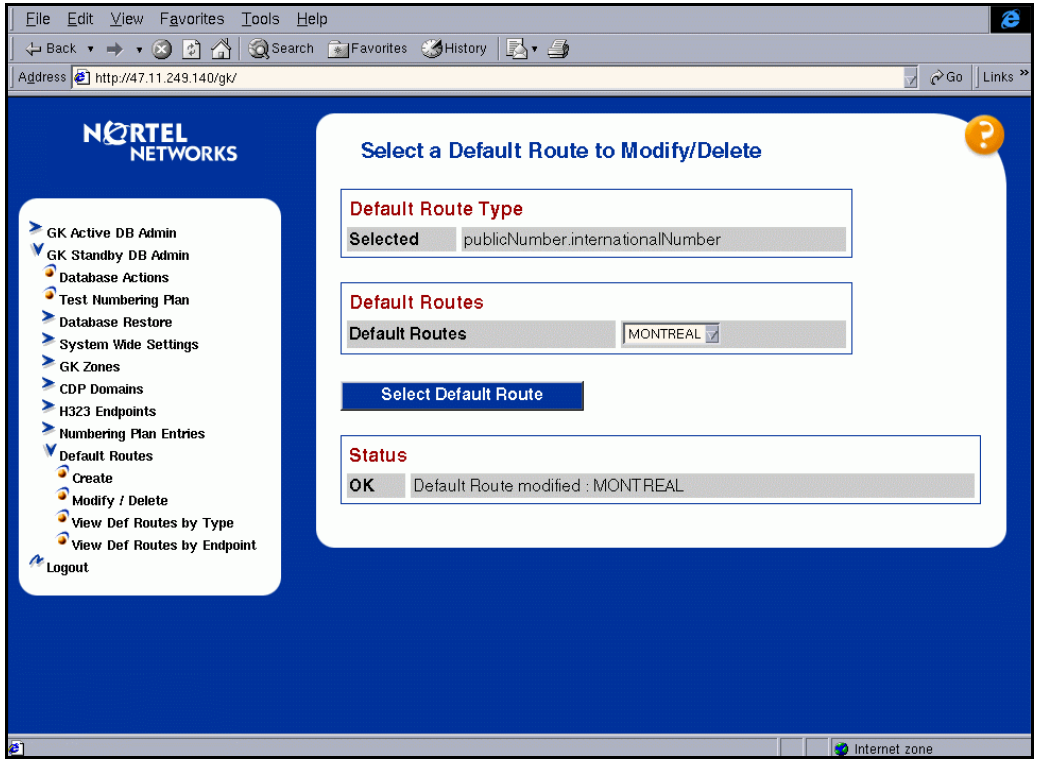
6 Modify the default route information as required.

Note: You can click **Reset** modifications to restore the previous information.

7 Click the **Modify** button.

The webpage refreshes and the status is shown at the bottom of the webpage (see Figure 144 on page 305).

Figure 144
Default route modification confirmation webpage



End of Procedure

Procedure 42
Deleting a default route

1 Click **GK Standby CD Admin | Database Actions | Default Routes | Modify / Delete**.

The **Select a Default Route Type to Modify/Delete Default Routes** webpage displays (see Figure 141 on page 302).

2 Select the default route type from the **Default Route Type** drop-down list box (see Figure 141 on page 302).

3 Click the **Select** button.

The **Select a Default Route to Modify/Delete** webpage displays (see Figure 142 on page 303).

4 Select the default route from the **Default Routes** drop-down list box.

5 Click the **Select Default Route** button.

The **Default Route to Modify/Delete** webpage displays (see Figure 143 on page 304).

6 Verify that the default route selected is the default route that you want to delete.

7 Click the **Delete** button.

The webpage refreshes with a confirmation of whether or not the default route was deleted (see Figure 144 on page 305).

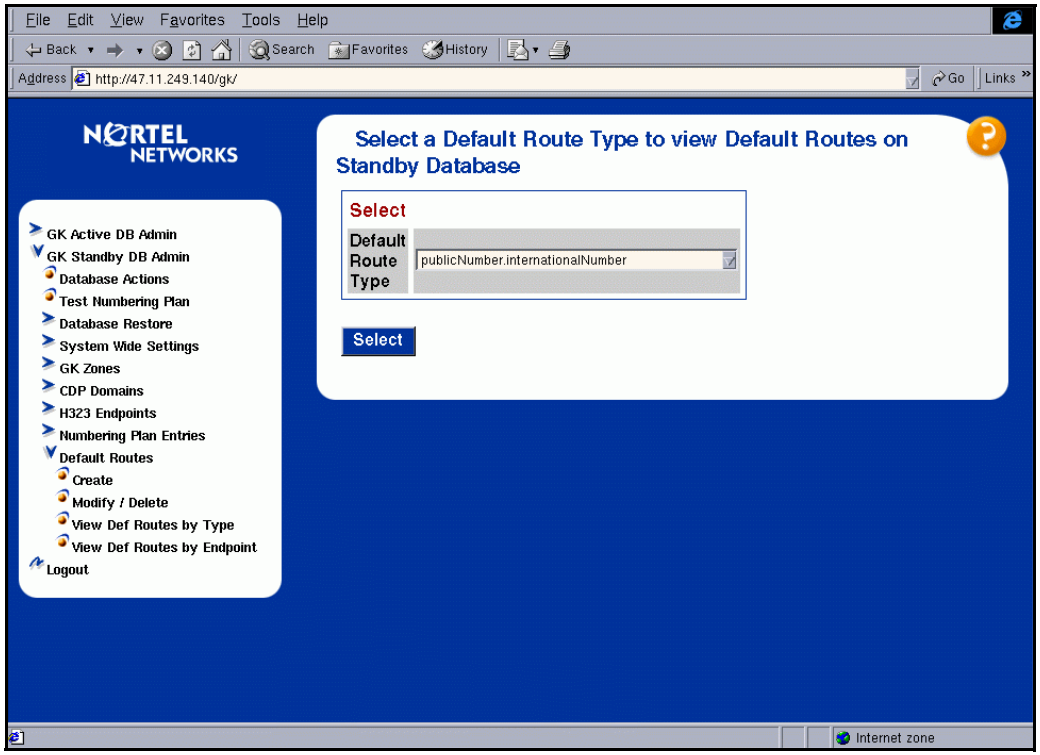
End of Procedure

Procedure 43
Viewing configured default routes by type

1 Select **GK Standby CD Admin | Default Routes | View Def Routes by Type** from the Navigation Tree.

The **Select a Default Route Type to view Default Routes on Standby Database** webpage displays (see Figure 145).

Figure 145
Select a Default Route Type to view Default Routes on Standby Database webpage

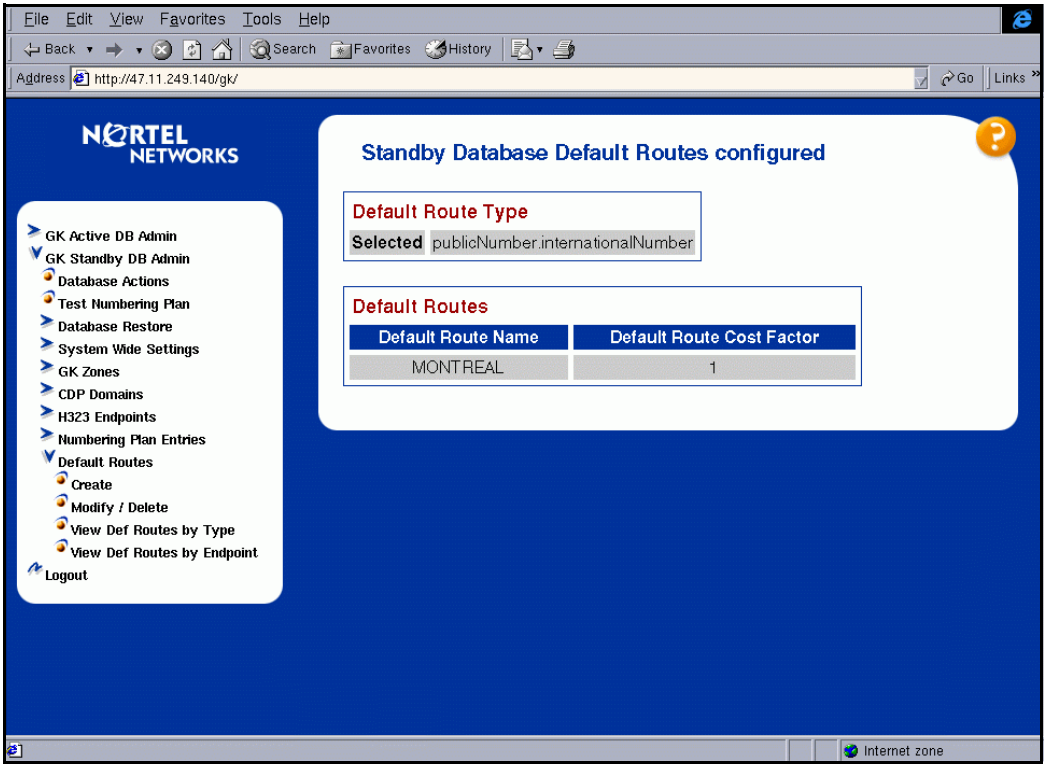


2 Select the route type from the **Default Route Type** drop-down list box.

3 Click the **Select** button.

The **Standby Database Default Routes configured** webpage displays (Figure 146 on page 308) displaying all of the default route names for the type you selected. This webpage also displays the associated default route cost factors.

Figure 146
Standby Database Default Routes configured webpage



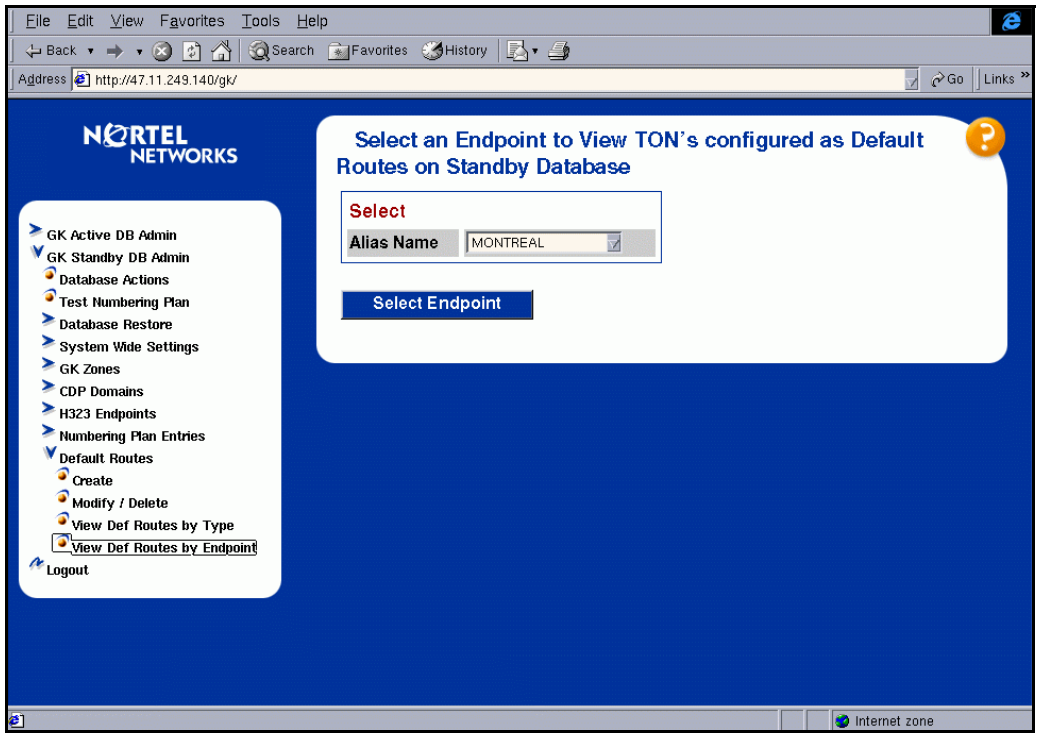
End of Procedure

Procedure 44
Viewing configured default routes by endpoint type

1 Select **GK Standby CD Admin | Default Routes | View Def Routes by Endpoint** from the Navigation Tree.

The **Select a Default Endpoint to View TON's configured as Default Routes on Standby Database** webpage displays (see Figure 147).

Figure 147
Select an Endpoint to view TONs configured as Default Routes on Standby Database

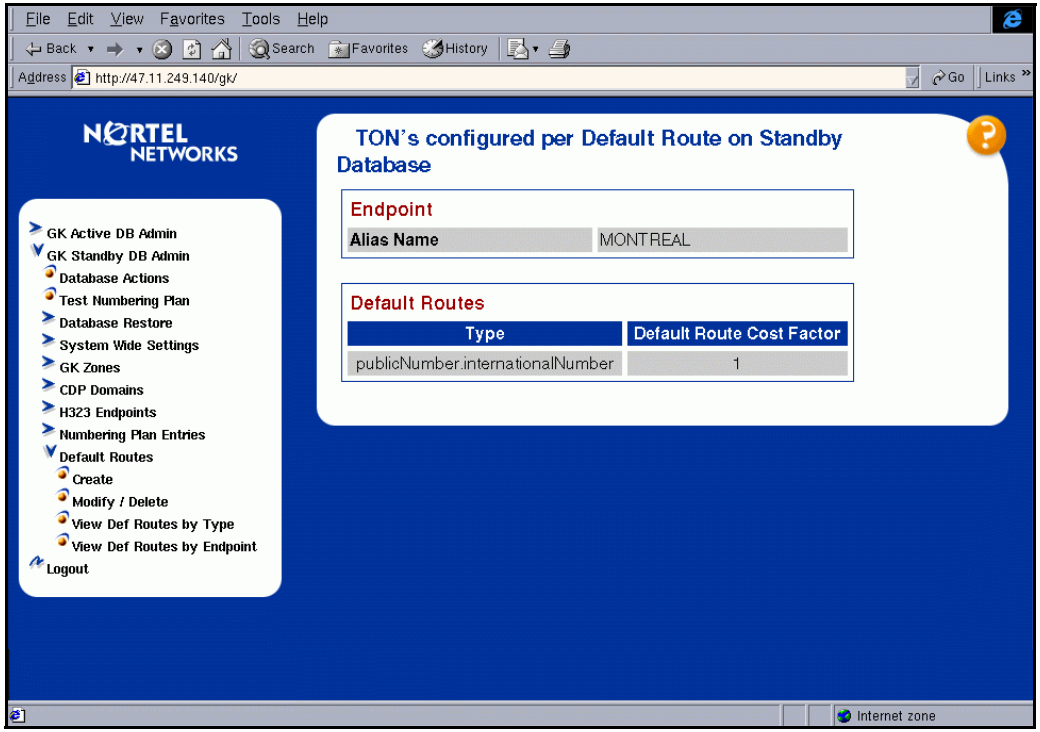


2 Select the **Alias Name** from the drop-down list box.

3 Click the **Select Endpoint** button.

The **TONs configured per Default Route on Standby Database** webpage displays (Figure 148 on page 310).

Figure 148
TONs configured per Default Route on Standby Database webpage



End of Procedure

Configuring Gatekeeper zones

A list of gatekeepers in different network zones can be specified in your Gatekeeper. Your Gatekeeper can contact gatekeepers (in other network zones) in order to resolve admission requests (ARQ) for which it cannot find matches in its own numbering plan database. For Succession 3.0, the user can provision the Gatekeeper's alias name and CDP DOMAIN, along with the IP address.

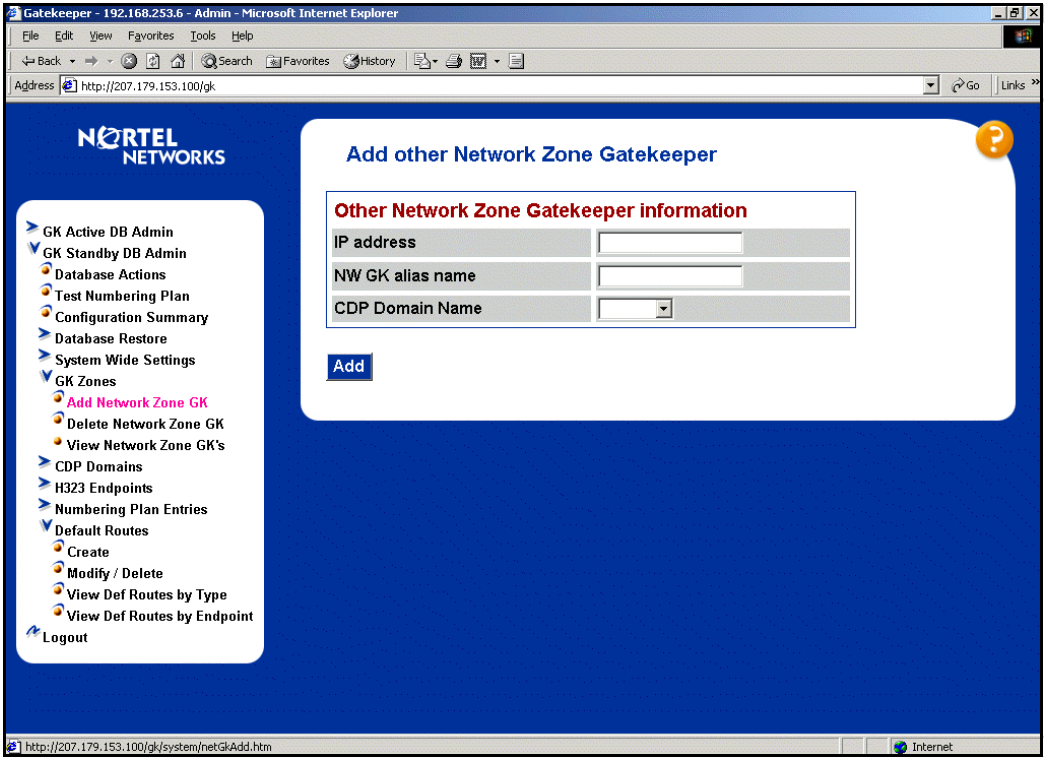
To add a Gatekeeper zone, follow the steps in Procedure 45.

Procedure 45
Adding a network zone

1 Select **GK Standby DB Admin | GK Zones | Add Network Zone GK** from the Navigation Tree.

The **Add other Network Zone Gatekeeper** webpage displays (see Figure 149 on page 312).

Figure 149
Add other Network Zone Gatekeeper webpage



Note: The **IP address** and **NW GK alias name** are required to add a Gatekeeper. The **CDP Domain Name** is not required, unless you want to restrict the network zone gatekeeper to a specific CDP domain.

Since the gatekeepers service multiple zones and the LRQ message contains the relevant CDP DOMAIN for the call, it is not advisable to restrict the network zone operation by provisioning a specific CDP DOMAIN against a Gatekeeper.

To add a third party Gatekeeper, Nortel Networks recommends associating a CDP DOMAIN with the third-party Gatekeeper. This gatekeeper will not be able to understand CDP DOMAIN information sent in the LRQ message and the administrator would like to associate each third party gatekeeper to only one CDP DOMAIN as third party Gatekeepers cannot support multiple CDP DOMAINS.

2 Enter the **IP address** of the Gatekeeper you want to add to the list of Gatekeepers in other network zones.

3 Enter the Gatekeeper alias name (H323-ID) in the **NW GK alias name** text box. This field is mandatory for Succession 3.0 Gatekeeper and third-party gatekeepers.

4 If required, select the CDP domain associated with the Network zone Gatekeeper from the **CDP Domain Name** drop-down list box. This is primarily for third-party gatekeepers.

5 Click the **Add** button.

The webpage refreshes with a confirmation of the operation.

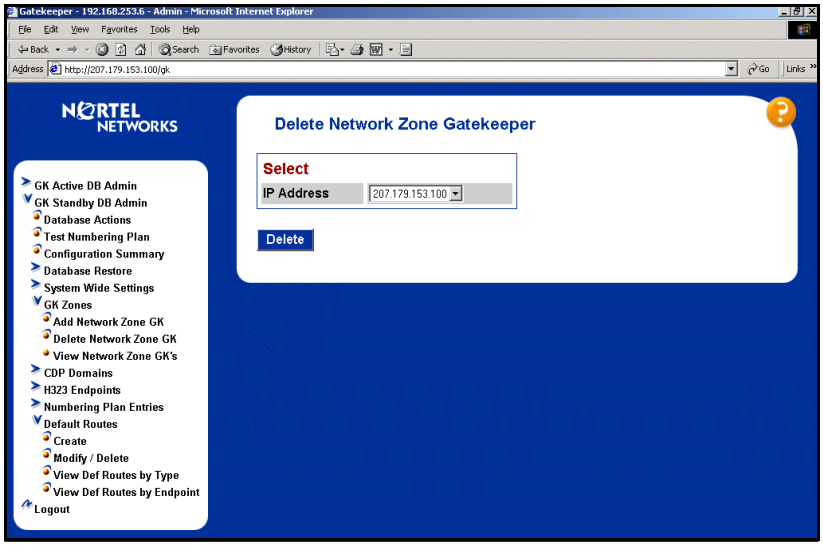
End of Procedure

Procedure 46
Deleting a Gatekeeper zone

1 Select **GK Standby DB Admin | GK Zones | Delete Network Zone GK** from the Navigation Tree.

The **Delete Network Zone Gatekeeper** webpage displays (see Figure 150 on page 314).

Figure 150
Delete Network Zone Gatekeeper webpage

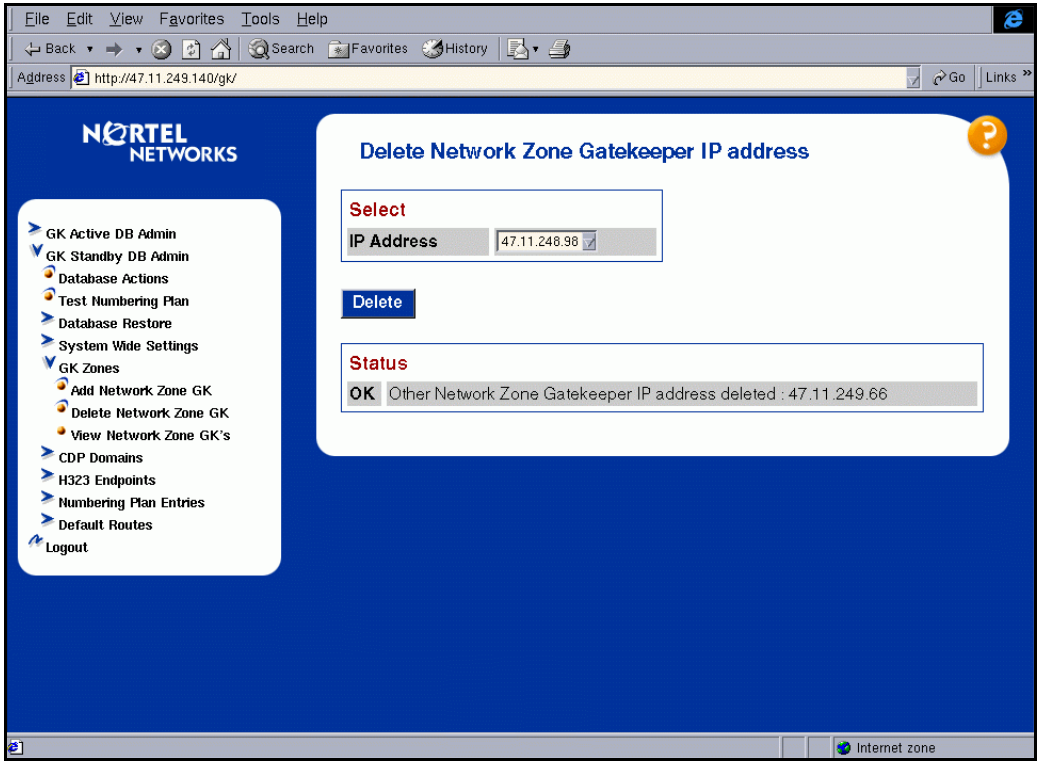


2 Select the IP address of the Network Gatekeeper Zone to be deleted from the **IP Address** drop-down list box.

3 Click the **Delete** button.

The webpage refreshes, confirming the deletion (see Figure 151 on page 315).

Figure 151
Delete Network Zone Gatekeeper confirmation webpage



End of Procedure

Taking the Gatekeeper out-of-service

The Gatekeeper can be taken out of service to perform maintenance, or to place an Alternate Gatekeeper into service.

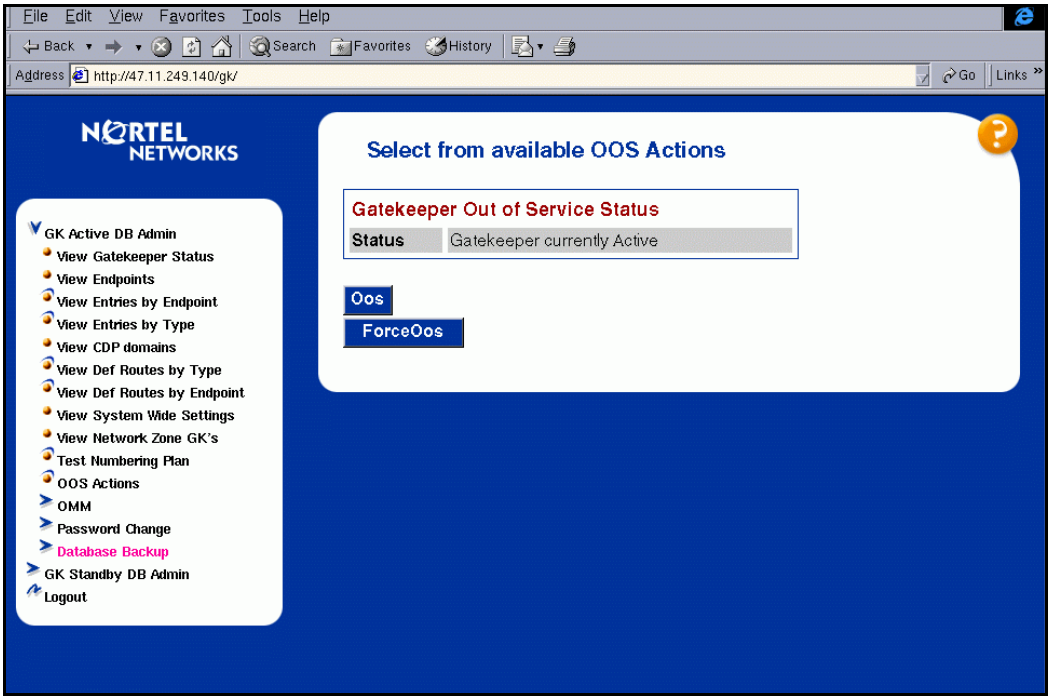
To take the Gatekeeper out-of-service, follow the steps in Procedure 47.

Procedure 47
Taking the Gatekeeper out-of-service (OOS)

1 Select **GK Active DB Admin | OOS Actions** from the Navigation Tree.

The **Select from available OOS Actions** webpage displays (see Figure 152).

Figure 152
Select from available OOS Actions webpage



2 Choose one of the following:

- Click the **Oos** button to take the Gatekeeper out-of-service only if the Alternate Gatekeeper is running (This performs a graceful shutdown of service).

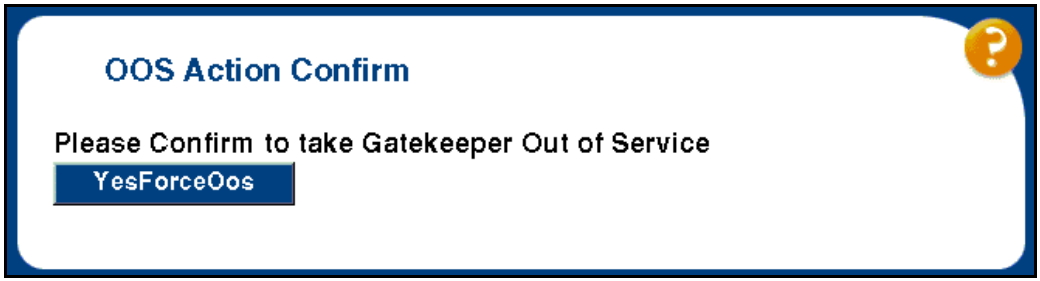
  The **OOS Action Confirm** webpage displays (see Figure 153).

Figure 153
OOS Action Confirm webpage

- Click the **ForceOos** button to take the Gatekeeper out-of-service, regardless of whether or not the Alternate Gatekeeper is running (This performs an immediate shut-down of service).

  The **OOS Action Confirm** webpage displays (see Figure 154).

Figure 154
OOS Action Confirm webpage

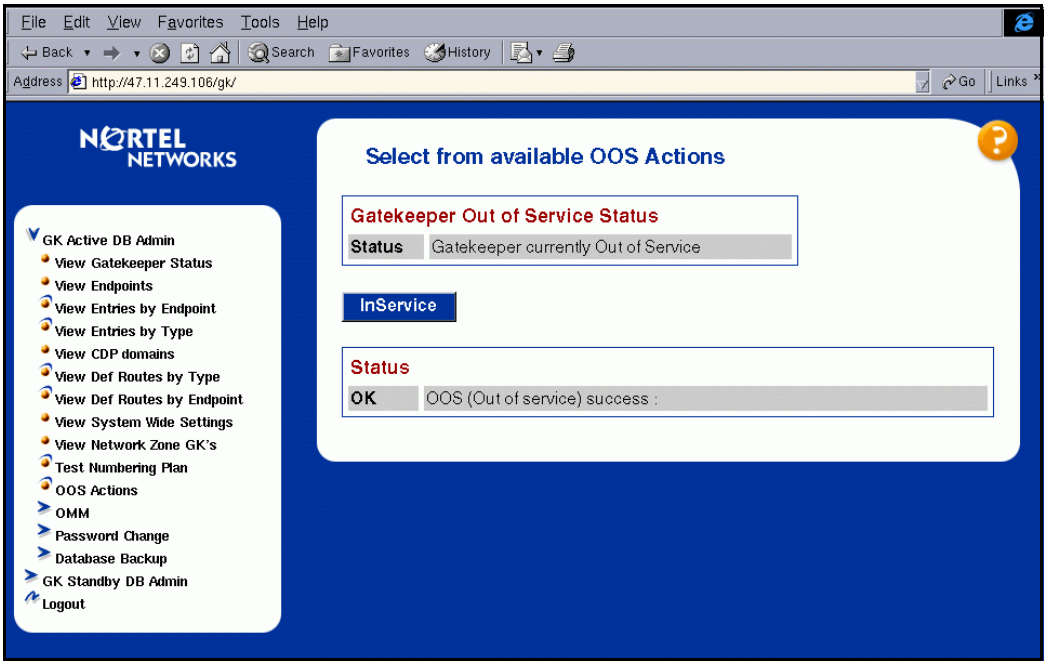


3 Depending on the option chosen in step 2 on page 317, choose one of the following:

- Click the **YesTakeOOS** button.
- Click **YesForceOOS** button.

A webpage displays confirming the status of the operation (see Figure 155).

Figure 155
OOS confirmation webpage



4 Click the **InService** button if you want to bring the Primary Gatekeeper back into service.

A status message display at the bottom **Select from available OOS Actions** webpage (see Figure 152 on page 316).

End of Procedure

Viewing traffic reports

To view traffic reports, follow the steps in Procedure 48.

Procedure 48
Viewing traffic reports

1 Select **GK Active DB Admin | OMM** from the Navigation Tree. Then select either of the following:

- **View Last Hour Report** to view traffic metrics for the last hour (see Figure 156).
- **View Average Report** to view a report showing averages for the time the system has been up and running (see Figure 157 on page 320).

Figure 156
OMM-Last Hour Report webpage

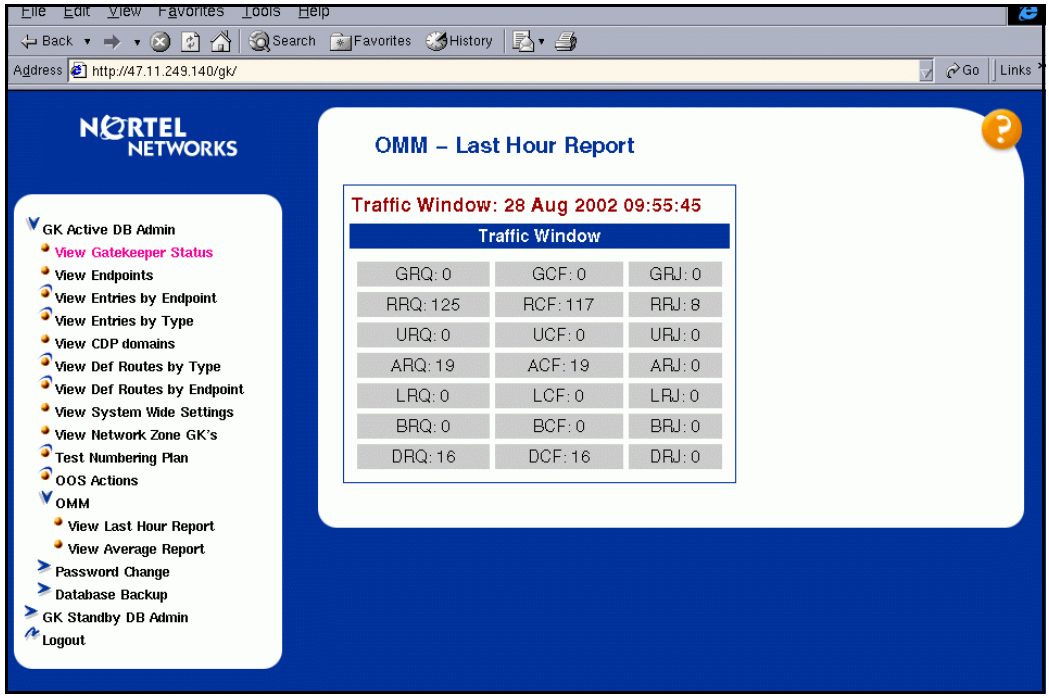
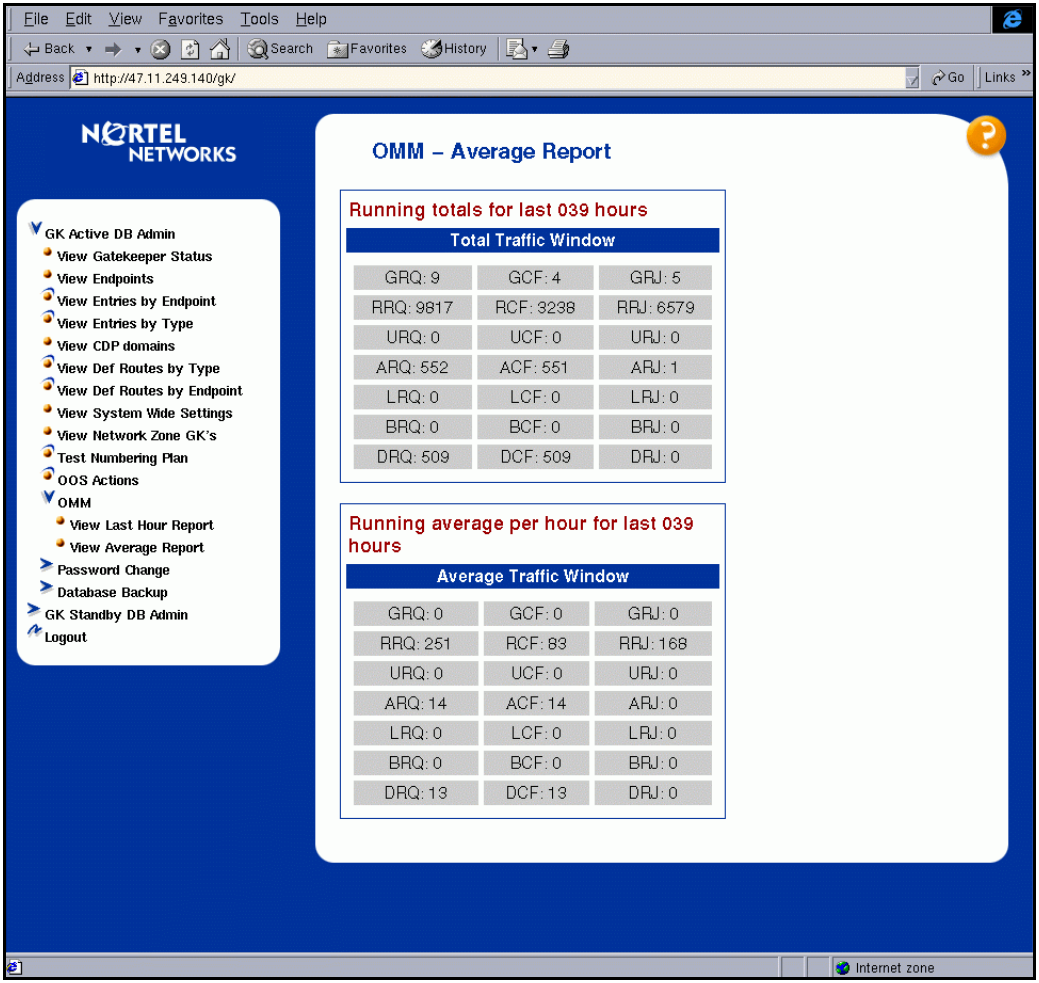


Figure 157
OMM-Average Report webpage



End of Procedure

Performing database rollback

To delete all changes made on the database, complete Procedure 49.

The rollback procedures swap the primary and standby databases to revert back to the previous configuration. This operation is available after a Cutover and a Commit are performed.

Procedure 49
Performing database rollback

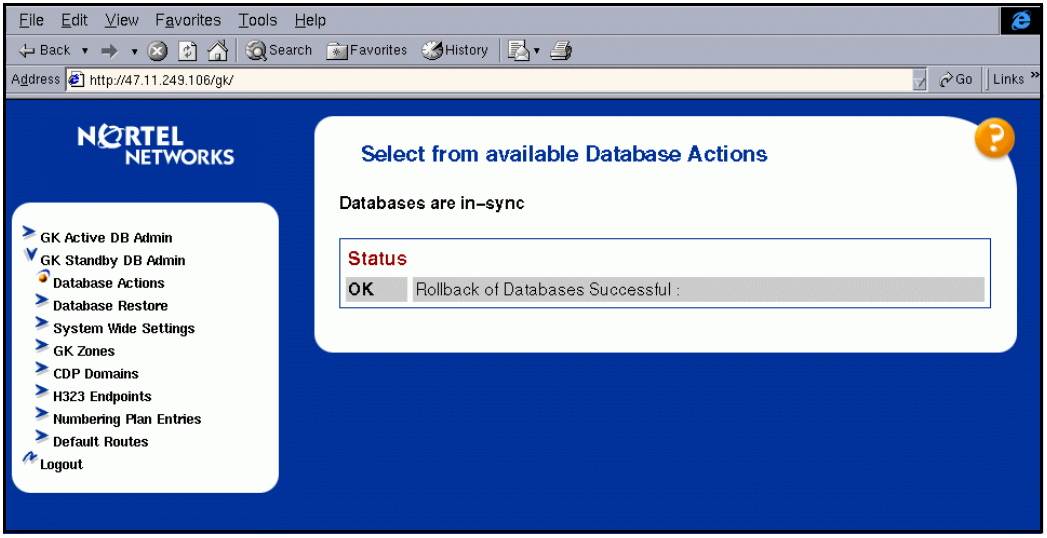
1 Select **GK Standby DB Admin | Database Actions** from the Navigation Tree.

The **Select from available Database Actions** webpage displays (see Figure 125 on page 282).

2 Click the **Rollback** button.

A status message displays indicating if the rollback operation was successful or not (see Figure 158).

Figure 158
Rollback status webpage



End of Procedure

IP Peer internetworking

Contents

This section contains information on the following topics:

Nortel Networks products internetworking

A Succession 1000M System internetworks with other Nortel Networks products. This chapter discusses internetworking between Succession 1000M System and the following products:

- Meridian 1 IE (IP Trunk Release 3.0 or later)
- Succession Business Communication Manager (BCM) Release 3.01

Meridian 1 IE (IP Trunk Release 3.0 or later)

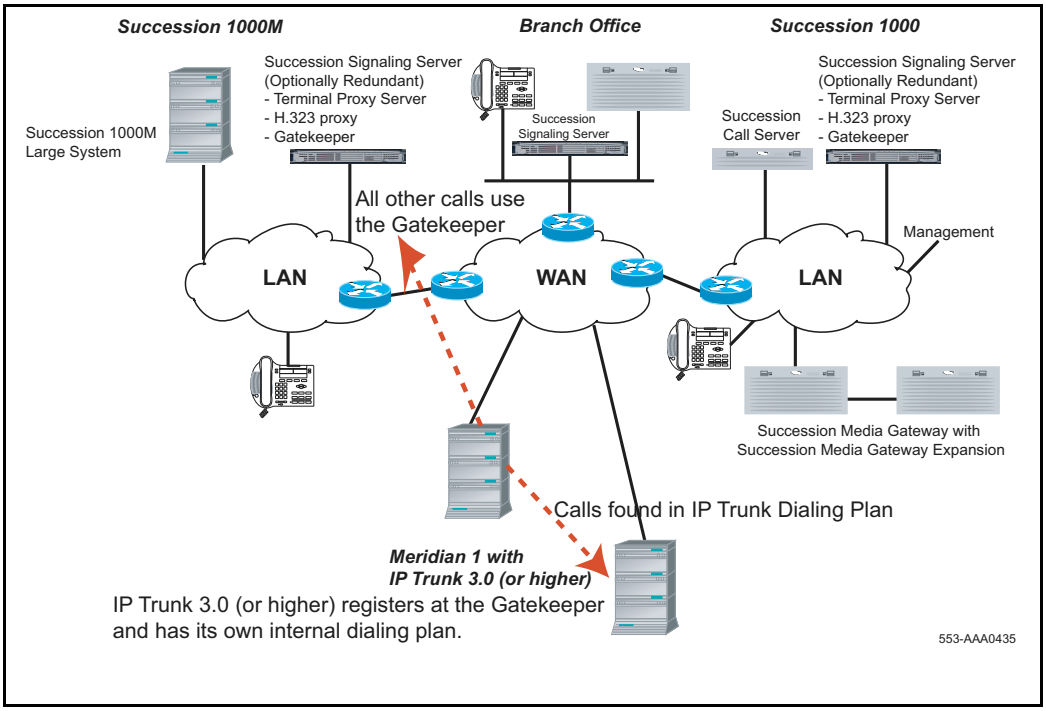
Succession 3.0 networks with Meridian 1 Release 25.xx or later. Nortel Network's Meridian Customer Defined Network (MCDN) protocol over PRI trunks provide the rich feature set currently available to networks of Meridian 1 Systems.

Any existing IP Trunks in the system must be upgraded to IP Trunk 3.0 (or later) in order to interwork with an IP Peer Networking node.

IP Peer Networking Phase 2 interworks with IP Trunk 3.0 (or later). It also supports all the MCDN features that IP Trunk 3.0 (or later) supports including Trunk Route Optimization.

With IP Trunk, the numbering plan is configured for each site. With IP Peer Networking, the Gatekeeper maintains the numbering plan for all sites. IP Trunk 3.0 (or later) maintains a point-to-point configuration. If a call is routed using IP Trunk 3.0 (or later) and the path is found, then the session is established. If the route path is not found, the lookup process is handed off to the Gatekeeper to resolve the route path. See Figure 159 on page 324.

Figure 159
IP Peer to Meridian 1 IP Trunk 3.0 (or later) Interworking



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

1 The ITG-Pentium 24-port and Succession Media Card 32-port trunk cards must be upgraded to IP Trunk 3.0 (or later) software. This upgrade supports MCDN features and Gatekeeper registration. Use OTM 2.1 to perform the upgrade. Refer to *Optivity Telephony Manager: System Administration* (553-3001-330) for information on installing, upgrading, and configuring IP Trunk 3.0 (or later) parameters.

2 Configure the IP Trunk 3.0 (or later) node to register with the Succession 1000M Gatekeeper, using the OTM 2.1 Gatekeeper Properties dialog window shown in Figure 160 on page 326. This dialog window enables the administrator to link an IP Trunk 3.0 (or later) endpoint to a Gatekeeper zone (automatically providing Primary and Alternate Gatekeepers). This window is also used to manually provision a Gatekeeper for the node. Refer to *Optivity Telephony Manager: System Administration* (553-3001-330) for information on how to configure the IP Trunk 3.0 (or later) options.

Figure 160
Gatekeeper Properties dialog window

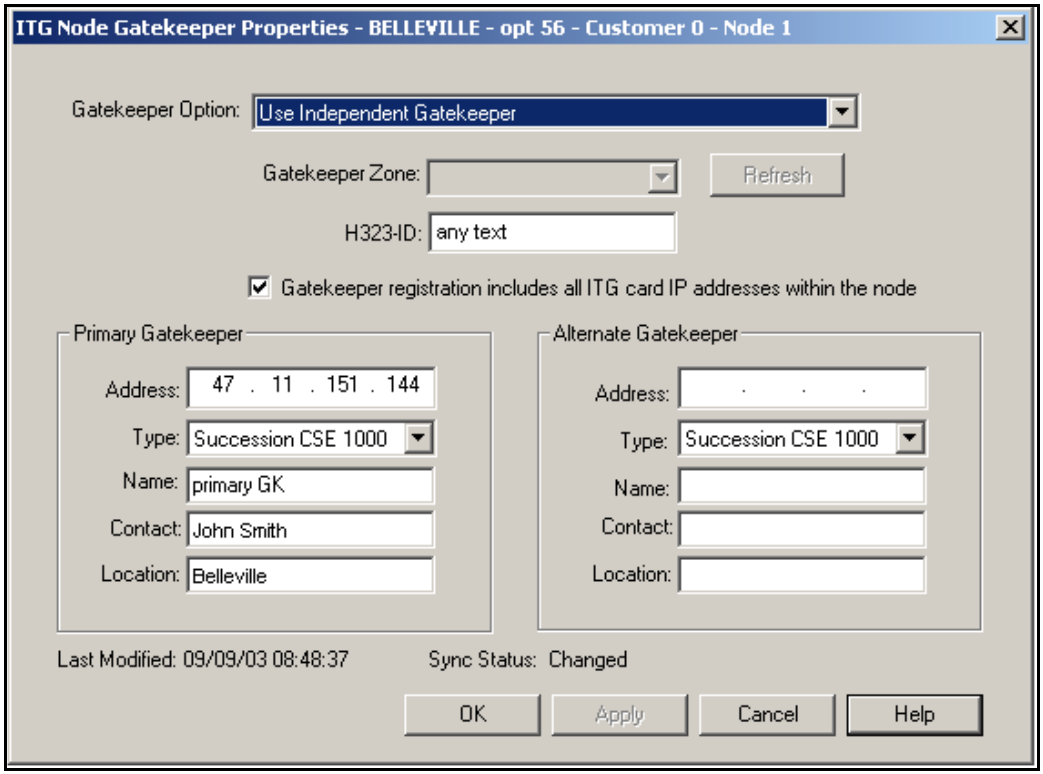


Figure 161
Gatekeeper Option drop-down list box

If configured appropriately, the IP Trunk 3.0 (or later) node uses Registration, Admission, and Status signaling (RAS) messaging to register with the Gatekeeper. The IP Trunk 3.0 (or later) x node then processes calls by scanning its DN information and routing unresolved calls to the Gatekeeper, using the Address Translation Protocol Module (ATPM).

OTM 2.1 enables the user to configure the IP address of a Succession 1000 or Succession 1000M node, with a capability of "CSE" in the ATPM dialing plan table. This enables the IP Trunk 3.0 (or later) node to directly call the Succession 1000 and Succession 1000M node.

> ***Note:*** In earlier software releases, the Succession software was known as Succession Communication Server for Enterprise (CSE) 1000. The CSE acronym has be removed from the software name, however, the CSE acronym remains in the ATPM dialing plan table.

The IP Trunk 3.0 (or later) node is subordinate to the Gatekeeper for all calls requiring the Gatekeeper. The IP Trunk 3.0 (or later) node:

1 registers with the Gatekeeper, according to H.323 protocol

2 requests admission

3 accepts the reply, according to H.323 protocol

4 proceeds to handle the call as required, based on the returned message

> ***Note:*** IP Trunk 3.0 (or later) supports the Succession Media Card 32-port trunk card and/or the ITG-Pentium 24-port trunk card.

Refer to *IP Trunk: Description, Installation, and Operation* (553-3001-363) for information on how to install, configure, and operate IP Trunk 3.0 (or later) functions, as well as information on IP Trunk signaling support (for example, MCDN, non-call associated signaling, and ESN5).

Succession Business Communication Manager Release 3.01

IP Peer Networking Phase 2 interoperates with Succession Business Communication Manager (BCM) Release 3.01. Succession BCM 3.01 has been enhanced with many additional MCDN features including the following:

- Network Call Transfer
- Network Call Redirection Information
- Message Waiting Indication
- ISDN Call Connection Limitation
- Trunk Route Optimization
- Trunk Anti-Tromboning
- Camp-On
- Break-In

For interworking between Succession BCM and a system running the Succession 3.0 Software, upgrade the Succession BCM to version 3.01 software.

A Succession BCM endpoint is configured on the Gatekeeper the same way that a Succession 1000 or Succession 1000M endpoint is configured. Configure the following on the Succession BCM so that it can interwork with the Succession 3.0 system:

- **Unified Manager: Services | IP telephony | H.323 Trunks | Call Signaling** should be set to **GatekeeperRouted** or **GatekeeperResolved**
- **Unified Manager: Services | IP telephony | H.323 Trunks | Gatekeeper IP** should be set to IP address of the Gatekeeper
- **Unified Manager: Services | IP telephony | H.323 Trunks | Alias Names** should be set to the Alias name that was used when the H.323 Endpoint for the BCM was created on the Gatekeeper

In order to make a Succession BCM 3.01 to Succession 1000 or Succession 1000M Large or Small System call, ensure that the Succession BCM routes and dialing plan (used to reach the Succession 1000 or Succession 1000M Large or Small System) matches the numbering plan entry assigned to the Succession 1000 or Succession 1000M Large or Small System through the Gatekeeper Element Manager.

Similarly, to make a Succession 1000 or Succession 1000M Large or Small System to Succession BCM 3.01 call, ensure that the numbering plan entry assigned to the BCM (through the Gatekeeper Element Manager) matches the dialing plan information configured on the Succession 1000 or Succession 1000M Large or Small Systems.

IP Peer upgrades

Contents

This section contains information on the following topics:

Introduction

Table 30 lists the four procedures in this chapter that are used when upgrading

- Meridian 1 IE to Succession 1000M
- Meridian 1 IE Succession 3.0 to Succession 1000M

Table 30
IP Peer upgrade procedures

Procedures	
Procedure 50	"Configuring H323-ID endpoints for IP Trunk 3.0 (or later) and BCM 3.01 on the Gatekeeper" on page 334
Procedure 51	"Configuring Network Numbering Plan for IP Trunk 3.0 (or later) and BCM 3.01 on the Gatekeeper" on page 337
Procedure 52	"Configuring IP Trunk Network to register with Gatekeeper and to use Gatekeeper Numbering Plan" on page 341
Procedure 53	"Configuring and cutting over an upgraded Succession 1000M system to use IP Peer Virtual Trunks" on page 346

For detailed information about the upgrade scenarios. Refer to

- *Small System: Upgrade Procedures* (553-3011-258)
- *Large System: Upgrade Procedures* (553-3021-258)

In general, the first three procedures are used to migrate a network of IP Trunk 3.0 (or later) nodes and BCM 3.01 systems from using the node-based Dialing Plan resolution to using the Gatekeeper Network Numbering Plan resolution.

Node-based Dialing Plan resolution uses destination endpoints identified by statically configured IP addresses. While Gatekeeper Network Numbering Plan resolution uses origination and destination endpoints identified by H323-IDs or H323AliasNames configured in the Gatekeeper.

The Gatekeeper dynamically obtains the call signaling IP address of each endpoint when the endpoint registers with the Gatekeeper using its preconfigured H323-ID.

Currently, the migration procedures are not automated. To migrate to the Gatekeeper Network Numbering plan, do one of the following:

- Inspect the IP Trunk Dialing Plan data, and then manually copy and paste the data from the OTM IP Trunk Service Properties sheets to the Gatekeeper endpoint and numbering plan database
- Use FTP to obtain the IP Trunk Dialing Plan text file (dptable.1) from the IP Trunk card. The path to the text file is /C:/table/dptable.1.

  Inspect the dptable.1 text file. Manually copy the dialing plan data from the opened text file and then paste the data in to the Gatekeeper endpoint and numbering plan database.

  Note: Consult the *IP Trunk 3.0 Expert Guide* to interpret the format of the data in the dptable.1 text file.

Configuring H323-ID endpoints for IP Trunk 3.0 (or later) and BCM 3.01 on the Gatekeeper

You must create an endpoint H323-ID for the selected IP Trunk node and assign it to the appropriate CDP Domain for each destination Node name that exists in the Dial Plan for the selected IP Trunk node.

Keep notes to track your progress. Note any discrepancies, which may include:

- Endpoints whose node capability is not SL1 or SL1ESN5 (for example, H.323V2, ISGF, ESGF, CSE)
- Nodes that have Quality of Service (QoS) Monitoring enabled (QoS Monitoring is not supported by Gatekeeper)

Procedure 50
Configuring H323-ID endpoints for IP Trunk 3.0 (or later) and BCM 3.01 on the Gatekeeper

1 Log in to OTM.

2 From the OTM Navigator, select **Services | ITG ISDN Trunk**.

3 Select an IP Trunk node that meets the following two criteria:

- The node currently has a typical Dialing Plan for the IP Trunk network.
- The node is migrating to a Gatekeeper-based Network Numbering Plan.

4 Select **Configuration | Node | Dialing Plan** (or right-click on the node and select **Dialing Plan**) to open the Dialing Plan for the selected node.

5 Sort by node name.

6 Using the same OTM PC, open the Internet Explorer 6.0.2600 web browser.

7 In the browser's **Address** field, enter the ELAN or TLAN IP address to access the **Gatekeeper** pages in Element Manager.

For example: http://<Succession Signaling Server IP address>/gk

8 Log in to the **Gatekeeper** pages in Element Manager using:

User = gkadmin

Password = gkadmin

A welcome webpage is displayed.

9 Select **GK Standby DB Admin | CDP Domains | Create** from the Navigation Tree at the left of the webpage.

The **Create CDP domain** webpage is displayed.

a. In the **CDP Domain Name** text box, enter a CDP domain name that describes the campus or network that shares a coordinated Dialing Plan.

b. Click the **Create** button to save the CDP domain.

10 Select **GK Standby DB Admin | H323 Endpoints | Add H323 Endpoint** from the Navigation Tree. (This is in preparation for the Copy and Paste steps that follow.)

The **Create H323 Endpoint** webpage is displayed.

11 Return to OTM.

Note: Do not close the **Gatekeeper** pages in Element Manager.

12 In the **OTM ITG Dialing Plan** window, double-click on the first destination node in the dialing plan.

A property sheet for the **Destination Node** in this dialing plan opens.

13 In the **General** tab, edit the **Node Name** to create a consistent format for the H323-IDs so that the type of endpoint is clearly indicated.

For example:

Rich_Gal-C_IPT

Rich_Gal-C_IPP-GW

Rich_Card_BCM

where:

Rich = Site Name
Gal = System Name
IPT (IP Trunk 3.0 (or later)), IPP-GW (IP Peer VTRK Gateway), BCM (BCM 3.01) = Type of endpoint

14 Click the **Apply** button to save the edited node name.

15 Copy the edited node name to the Clipboard.

16 Close the Destination Node property sheet.

17 Return to the **Gatekeeper** pages in Element Manager. The Create H323 Endpoint webpage is displayed.

18 Paste the edited node name into the **H323AliasName** text box for the IP Trunk 3.0 (or later) endpoint that you are adding to the Gatekeeper database.

If this endpoint uses CDP Steering Codes in the dialing plan, then select the appropriate **CDP Domain Name** from the drop-down list box.

19 Click the **Create H323** button to save the H323AliasName or H323-ID in the Gatekeeper database.

20 Repeat step 11 to step 19 to add an Endpoint H323-ID for every destination node that appears in the Dialing Plan for the selected IP Trunk node.

21 Once you have added an Endpoint H323-ID for every destination node, you must then add an Endpoint H323-ID for the IP Trunk node of the Dialing Plan from which you have been working.

a. Close the Dialing Plan from which you have been working.

b. Select another IP Trunk node that has a typical Dialing Plan and open the Dialing Plan.

c. Find the destination Node name for the node whose Dialing Plan you were previously working from.

d. Perform step 11 to step 19.

22 Select **Gatekeeper Standby DB | H323 Endpoints | View Endpoints** from the Navigation Tree to view the newly added Endpoints.

23 Note any discrepancies while you inspect and compare the Dialing Plan of at least two typical nodes in OTM.

Investigate and resolve any discrepancies. Discrepancies may include:

- Endpoints whose node capability is not SL1 or SL1ESN5 (for example, H.323V2, ISGF, ESGF, CSE)
- Nodes that have Quality of Service (QoS) Monitoring enabled (QoS Monitoring is not supported by Gatekeeper)

Note: Contact Technical Support if you require assistance to resolve discrepancies.

24 In the **Gatekeeper** pages of Element Manager, add Endpoint H323-IDs for any new destination node names not found in the first typical Dialing Plan selected.

25 Verify that you have added an Endpoint H323-ID in the Gatekeeper for each destination node in the Dialing Plans of the IP Trunk 3.0 (or later) network (may include BCM 3.01 destination nodes).

End of Procedure

Configuring Network Numbering Plan for IP Trunk 3.0 (or later) and BCM 3.01 on the Gatekeeper

Procedure 51 assumes that Procedure 50 “Configuring H323-ID endpoints for IP Trunk 3.0 (or later) and BCM 3.01 on the Gatekeeper” on page 334 have been completed.

In general, Procedure 51 details the steps for configuring the Network Numbering Plan for existing IP Trunk 3.0 (or later) nodes and BCM 3.01 systems in Gatekeeper.

Keep notes to track your progress. Note any discrepancies, which may include:

- Digits deleted and inserted
  (The Gatekeeper does not provide digit manipulation capability.)
- Exchange (Central Office) Code (NXX) Dial Plan entry types
  (The Gatekeeper does not support NXX Dial Plan types.)

To work around these discrepancies, you must create additional Digit Manipulation Tables and Route List Blocks on the host Meridian 1 system, and modify CDP and UDP network translations. Enter the manipulated number in Gatekeeper Numbering Plan.

Procedure 51
Configuring Network Numbering Plan for IP Trunk 3.0 (or later) and BCM 3.01 on the Gatekeeper

1. Log in to OTM.
2. From the OTM Navigator, select **Services | ITG ISDN Trunk**.
3. Select an IP Trunk node that meets the following two criteria:
   - The node currently has a typical Dialing Plan for the IP Trunk network.
   - The node is migrating to a Gatekeeper-based Network Numbering Plan.
4. Select the IP Trunk node used in Procedure 50 on page 334.
5. Select **Configuration | Node | Dialing Plan** (or right-click on the node and select Dialing Plan) to open the Dialing Plan for the selected node.
6. Sort by node name.

7 Using the same OTM PC, open the Internet Explorer 6.0.2600 web browser.

8 In the browser's **Address** field, enter the ELAN or TLAN IP address followed by "/gk" to access the **Gatekeeper** pages in Element Manager and click Go.

For example: http://<Host Succession Signaling Server IP address>/gk

9 Log in to the **Gatekeeper** pages in Element Manager using:

User = gkadmin

Password = gkadmin

10 Select **GK Standby DB Admin | Numbering Plan Entries | Create** from the Navigation Tree.

The **Select an Endpoint to add an Entry** webpage displays.

Leave this webpage open in preparation for the copy and paste steps that follow.

11 In OTM, double-click the first destination node in the Dialing Plan.

The **ITG Dialing Plan - Remote Node Properties** sheet displays.

Note: When repeating step 11 to step 13, double-click the next destination node when you have copied and paste all the Dial Plan entries in the previous destination nodes **Digits Dialed** tab of the Remote Node Properties sheet.

12 Select the **Digits Dialed** tab located on the ITG Dialing Plan - Remote Node Properties sheet.

a. Select the first item in the list of Dial Plan entries.

Note 1: When repeating step 12 to step 14, select the next Dial Plan entry.

b. Copy the Dial Plan digits to the Clipboard.

Note 2: Take note of the Dialing Plan type. You will use the Dialing Plan type information in the next step.

If there are more Dial Plan entries, leave the Properties sheet open for later use. Otherwise, click **Cancel** to close.

13 Select **GK Standby DB Admin | Numbering Plan Entries | Create** from the Navigation Tree.

The **Select an Endpoint to add an Entry** webpage is displayed.

a. Select the corresponding Endpoint from the **Endpoint** drop-down list box.

b. Click the **Select** button.

The **Add Entry** webpage appears.

c. In the **Numbering Plan Entries** area:

i. Paste the Dialing Plan digits into the **Number** text box.

ii. Select the type of number from the **Type** drop-down list box that corresponds to the OTM Dial Plan type.

iii. Click the **Create** button to add the entry to the Gatekeeper Numbering Plan for this Endpoint.

14 Repeat step 11 to step 13 until you have copied and pasted the last Dialing Plan entry for the last destination Node in the OTM Dialing Plan.

Note: Remember to take note of the Dialing Plan type for each Dial Plan entry you are copying.

15 Once you have added each Dialing Plan entry for each destination Node in the Dialing Plan for the typical IP trunk node whose Dialing Plan you have been working from, you must then add the Dial Plan entries for the destination Node whose Dialing Plan you have been working from:

a. Close the Dialing Plan for the node from which you have been working.

b. Right-click on another typical node and open its Dialing Plan.

c. Find the destination node for the first node you were working from, and double-click to open the Remote Node Properties sheet.

d. Perform step 11 to step 13 until you have copied and pasted all the Dial Plan entries for the destination node of the first node that you were working from.

16 Select **Standby DB Admin | NumberingPlanEntries | View Entries by Endpoint** from the Navigation Tree.

The **Select an Endpoint to view Entries on Standby Database** webpage displays.

a. Select an endpoint to view from the **Endpoint** drop-down list box.

b. Click the **Select** button.

The **View Standby Database Endpoint Entries** webpage displays with the endpoint information.

c. Compare the entries contained on the **View Standby Database Endpoint Entries** webpage for the selected endpoint to the ITG Dialing Plan table entry for the corresponding destination Node.

d. Repeat step a to step c, selecting the next endpoint until you have viewed and compared all the entries for the endpoints and all the destination Nodes.

17 Select **GK Standby DB Admin | Database Actions**.

18 Click the **SingleStepCutoverCommit** button.

The Endpoint and Numbering Plan database is copied to **GK Active DB Admin**. The database is used by the Gatekeeper to register endpoints and to resolve the telephone numbers in Admission Request (ARQ) messages from Endpoints.

End of Procedure

Configuring IP Trunk Network to register with Gatekeeper and to use Gatekeeper Numbering Plan

Procedure 52 assumes that the following procedures have been completed:

- Procedure 50 “Configuring H323-ID endpoints for IP Trunk 3.0 (or later) and BCM 3.01 on the Gatekeeper” on page 334
- Procedure 51 “Configuring Network Numbering Plan for IP Trunk 3.0 (or later) and BCM 3.01 on the Gatekeeper” on page 337

Note: A similar procedure must be performed on BCM 3.01 systems.

CAUTION — Service Interruption

To avoid service interruption, do not perform this procedure during high traffic volume.

Procedure 52
Configuring IP Trunk Network to register with Gatekeeper and to use Gatekeeper Numbering Plan

1 Log in to OTM.

2 From the OTM Navigator, select **Services | ITG ISDN Trunk**.

3 You must disable **QOS Fallback to PSTN** in the Dialing Plans of all IP Telephony nodes that are being migrated to use the Gatekeeper:

   a. In OTM, open the Dialing Plan for each node.

   b. Open each destination node in the Dialing Plan of each node, and uncheck the **QOS Fallback PSTN** feature.

   c. Click the **OK** button to save.

   d. Change all the Dialing Plans for every node to be migrated before you click the **Synchronize/Transmit** button.

4 Select the first IP Trunk node to be reconfigured to use the Gatekeeper Numbering Plan.

5 Right-click the node and select **Gatekeeper**.

   The **ITG Node Gatekeeper Properties** sheet displays (see Figure 160 on page 326).

6 Select the appropriate **Gatekeeper Option** from the drop-down list box.

Note: If OTM 2.1 Navigator has been configured with Gatekeeper zones, then select **Use Gatekeeper Zone information from OTM Navigator**. Otherwise, select **Use independent Gatekeeper**.

If **Use Gatekeeper Zone information from OTM Navigator** was selected, then:

a. Select the zone from the **Gatekeeper Zone** drop-down list box.

b. Enter the H323-ID for this IP Trunk 3.0 (or later) Endpoint in the **H323-ID** text box. The Endpoint H323-ID must match the H323AliasName previously configured on the Gatekeeper for this IP Trunk 3.0 (or later) H323 Endpoint. For example: “Host Meridian 1 system_IPT”.

c. Click the **OK** button.

Note: To determine the previously configured H323-ID, log in to the **Gatekeeper** pages Element Manager and select **GK Standby DB Admin** | **H323 Endpoints** | **View Endpoints** from the Navigation Tree. Select the endpoint corresponding with the IP Trunk node you are configuring. Click on **AliasName** and copy, then paste into the OTM H323-ID field.

If **Use independent Gatekeeper** was selected, then:

a. Copy and paste the H323-ID from OTM into the **H323-ID** text box

b. Under **Primary Gatekeeper**:

i. Enter the IP address for Primary Gatekeeper in the **Address** text box.

ii. Select **CSE1000** from the **Type** drop-down list box.

iii. Enter the Site and System name of the Primary Gatekeeper in the **Name** text box.

iv. Enter the contact name for the Primary Gatekeeper in the **Contact** text box.

v. Enter the location of the Primary Gatekeeper in the **Location** text box.

c. Repeat for the **Alternate Gatekeeper**.

d. Click the **OK** button.

7 Right-click on the node to be reconfigured.

a. Select the **Synchronize | Transmit** button.

The **ITG-Transmit Options** window appears.

b. Click the **Dialing Plan** check box.

c. Click the **Start Transmit** button.

Monitor the **Transmit Control** window for successful transmission of Dialing Plans.

8 Verify the Endpoint has registered with Gatekeeper using the **Gatekeeper** pages in Element Manager:

a. Select **GK Active DB Admin | View Endpoints** from the Navigation Tree.

A list of all registered endpoints is displayed.

b. Verify the present node appears in the list.

If the present node does not appear in the list, you may have:

— incorrectly entered the Alias Name into the OTM H323-ID field

— incorrectly entered the Primary (or Alternate) Gatekeeper IP address

— unsuccessfully disabled and transmitted the Dialing Plan

Note: The CLI can also be used to verify that the endpoint has registered with the Gatekeeper. Log in to the ITG shell of the IP Trunk Leader card and enter the **gkShow** command. A list of all registered endpoints is displayed.

9 Backup the Dialing Plan file (C:/table/dptable.1) for the IP Trunk node that you are reconfiguring. Use FTP to obtain dptable.1 file and copy it to an appropriately named folder on the OTM Server.

The default FTP log is:

User = itgadmin

Password = itgadmin

If you need to restore the Dialing Plan entries for this node:

a. Use FTP to put the file back on the IP Trunk active Leader card.

b. In OTM's ITG ISDN Trunk service, right-click on the node and select Synchronize | Retrieve.

c. Click the **Dialing plan** check box, and click the **Start retrieve** button.

d. After successfully retrieving the Dialing plan, you must click the **Transmit Dialing plan** button to restore the original Dialing Plan.

10 In OTM, right-click on the node to be reconfigured then:

a. Select **Dialing Plan**.

The **ITG Dialing Plan** window displays for the selected node.

b. Select **Edit | Select All**.

c. Repeatedly press the **Delete** key until all destination nodes are deleted from the Dialing Plan.

d. Close the **Dialing Plan** window.

e. Right-click the node and click the **Synchronize | Transmit** button.

The **ITG - Transmit Options** dialogue box appears.

f. Click the option for **Dialing Plan**, then click the **Start Transmit** button.

g. Monitor the progress in the **Transmit Control** window.

11 Verify the Gatekeeper Dialing Plan is functioning correctly for calls originating from the reconfigured IP Trunk node by placing test calls from the host system to various destination nodes using all Numbering Plan types and numbers configured on the network.

If the test calls are successful, then repeat configuration step 3 to step 10 until all nodes in the ISDN IP Trunk service have been reconfigured, tested, and verified.

If the test calls are not successful, use the **LD 96: D-channel Diagnostic** to determine what dialed digits and call types are being sent to the Succession Call Server. Verify that the dialed digits and call types are present on the Gatekeeper and that the destination endpoint is registered with the Gatekeeper. You may need to configure appropriate digit manipulation and new RLIs on the host system.

At this point, you have successfully migrated the IP Trunk 3.0 (or later) network to the Gatekeeper Numbering Plan.

Note: A similar procedure must be performed for BCM 3.01 systems.

End of Procedure

Configuring and cutting over an upgraded Succession 1000M system to use IP Peer Virtual Trunks

IMPORTANT!

Ensure that you have completed all the required procedures prior to beginning Procedure 53 on page 346.

Refer to the following NTPs:

- *Small System: Upgrade Procedures* (553-3011-258)
- *Large System: Upgrade Procedures* (553-3021-258)

If...	Then...
The upgraded Succession 1000M system belongs to a large IP Trunk network...	Ensure you have completed a Pre- or Post-upgrade migration of the IP Trunk 3.0 (or later) and BCM 3.01 network to use the Gatekeeper-resolved Network Numbering Plan.
The upgraded Succession 1000M system belongs to a small IP Trunk network (for example, 2 to 4 systems), and you have chosen the “No migration” method...	Ensure you scheduled a sufficient maintenance window and provided for sufficient technician resources to simultaneously reconfigure and cut over all the upgraded Succession 1000M systems in a single maintenance window.

Procedure 53
Configuring and cutting over an upgraded Succession 1000M system to use IP Peer Virtual Trunks

1 Verify the Gatekeeper registration state of the IPP Gateway using one of the following methods:

- Use the Succession Signaling Server command `oam> npmShow`.
- Use the **Gatekeeper** pages in Element Manager and select **GK Active DB Admin** | **View Endpoints** from the Navigation Tree.

If...	Then...
IPP Gateway is not registered with Gatekeeper...	• Verify Gateway H323-ID matches the Gatekeeper H323AliasName using **GK Active DB Admin**. • Verify the Primary and Alternate Gatekeeper IP address using **Element Manager**. — Click **Configuration**	**IP Telephony** from the Navigation Tree. — Click the **Edit** button associated with the Node. The **Edit** webpage displays. — Click **Gatekeeper** to display the Primary Gatekeeper and Alternate Gatekeeper IP addresses. The Primary Gatekeeper and Alternate Gatekeeper IP addresses must equal the Host Succession Signaling Server's TLAN IP address for each Gatekeeper.
The registration is successful...	Perform outgoing calls from this node using route ACOD. ***Note:*** Configure RDB ISDN CTYP = CDP or LOC to match Type of Number of Gatekeeper numbering plan entries for outgoing test calls.

2 Identify all Route List Blocks (RLB) containing an IP Trunk route entry that are currently used by CDP Steering Codes and UDP NARS network translations.

Note 1: These RLBs must be changed to allow the upgraded Succession 1000M System to use IP Peer Virtual IP Trunk Gateway to make incoming and outgoing VoIP trunk calls with IP Trunk 3.0 (or later) and BCM 3.01 nodes.

Note 2: By changing the RLBs that contain an IP Trunk route entry, you can avoid making extensive changes to the CDP and UDP network translations.

3 Change the identified RLBs to insert an IP Peer Gateway Virtual IP trunk route (IPP-GW VTRK) entry before the IP Trunk route entry.

a. Configure SBOC = RRA for the IPP-GW VTRK entry.

b. Configure FRL = 7 for the IPP-GW VTRK entry if you prefer to make test calls only from terminals with an Network Class of Service (NCOS) containing an FRL = 7. This prevents normal users from using the IPP-GW VTRK route for outgoing calls while you are testing the Network Numbering Plan and routing plan.

Note: You can instantly revert to using the IP Trunk route for outgoing calls by removing the IPP-GW VTRK entry from the RLB (`REQ CHG... ENTR Xnn`).

4 Make test calls from the upgraded Succession 1000M System using the IPP-GW to endpoints in the IP Trunk 3.0 (or later)/BCM 3.01/IPP-GW Network:

a. Make outgoing test calls for all ESN Call Types (CTYP) that use the IPP-GW VTRK/IPT 3.0 (or later) RLBs.

b. Verify that the IPP-GW route is being used for outgoing calls (On Hold/Off Hold displays Route ACOD).

5 Make incoming test calls from endpoints in the IPT 3.0 (or later)/BCM 3.01/IPP-GW Network.

Use LD 80 to verify that the IP Trunk route is still being used for incoming calls. The LD 80 commands are `TRAC` or `TRAK`.

6 Test Non-Call-Associated Signaling (NCAS) features to endpoints in the IPT 3.0 (or later)/BCM 3.01/IPP-GW Network.

Use `MIK/MCK` to turn MWI on/off over the network.

7 Using the Gatekeeper pages in Element Manager, change the Numbering Plan entries for the IP Trunk node on the upgraded Succession 1000M System.

For H323AliasName = “upgraded_system_IPT”, change Cost Factor (Entry Cost) = 1 to Cost Factor (Entry Cost) = 2.

8 Using Gatekeeper pages in Element Manager, duplicate the Numbering Plan entries from the IP Trunk node (H323AliasName = “upgraded_system_IPT”) to the IP Peer VTRK Gateway on the upgraded Succession 1000M System (H323AliasName = “upgraded_system_IPP-GW”) with Cost Factor (Entry Cost) = 1 for the Numbering Plan entries on H323 Endpoint “upgraded_system_IPP-GW”.

a. Select **GK Standby DB Admin** | **Database Actions** from the Navigation Tree.

b. Click the **Cutover** button.

The Numbering Plan entry changes are copied to **GK Active DB Admin** and immediately applied to the operation of the Gatekeeper. The first choice route on the Gatekeeper for Numbering Plan entries destined for the upgraded Succession 1000M System has now been changed to the H323 Endpoint “upgraded_system_IPP-GW”.

Note: As long as you have not yet clicked the **Commit** button under **GK Standby DB Admin** | **Database Actions**, you can instantly revert to the previous Gatekeeper configuration and stop incoming calls from using the IP Peer Gateway Virtual Trunk route.

9 Make incoming test calls from endpoints in the IPT 3.0 (or later)/BCM 3.01/IPP-GW Network.

Use LD 80 to verify that the IP Peer Gateway Virtual Trunk route is still being used for incoming calls. The LD 80 commands are `TRAC` or `TRAK`.

10 Test Non-Call Associated Signaling (NCAS) Features.

Use `MIK/MCK` to turn MWI on/off over the network.

a. Disable D-Channel for the IP Trunk Route to ensure that all outgoing and incoming calls use the IP Peer Gateway Virtual Trunk route.

b. Make incoming and outgoing test calls to all ESN Call Types that are used in the network numbering plan.

c. Test NCAS features.

The IP Trunk 3.0 (or later) route is no longer required in the upgraded Succession 1000M System, provided that:

- all nodes in the network have been upgraded to IP Trunk 3.0 (or later), BCM 3.01, and Succession 3.0 Software with IP Peer Networking.
- all nodes have migrated to Gatekeeper numbering plan resolution.

Unused IP Trunk 3.0 (or later) cards can be converted to Voice Gateway Media Cards (VGMC). Refer to the following NTPs for this procedure:

- *Small System: Upgrade Procedures* (553-3011-258)
- *Large System: Upgrade Procedures* (553-3021-258)

End of Procedure

Maintenance

Contents

This section contains information on the following topics:

Command Line Interface (CLI) commands

Virtual Trunk CLI commands

Table 31 includes the CLI commands used when working with Virtual Trunks.

Table 31
Virtual Trunk CLI commands

CLI Command	Description
DSRM <cust #> <route #>	Disables all route members in a customer's route. This command: • disconnects all active calls associated with the trunks • disables all route members on the call server • unregisters all trunks • removes them from the RLM table On the Succession Signaling Server, all trunks will be removed from the Succession Signaling Server list.
ENRM <cust #> <route #>	Enables all the route members (virtual trunks) This command: • enables all route members in a customer's route • enables all route members • register the member • puts the members into the RLM table On the Succession Signaling Server, all trunks will be put on the Succession Signaling Server list.
STVT <cust#> <rout#> start_mb# end_mb#	Displays the virtual trunk status specified by customer number, route number, and starting and ending member number.

Gatekeeper CLI commands

Table 32 includes the CLI commands used when working with the Gatekeeper.

Table 32
Gatekeeper CLI commands

CLI Command	Description
gkDbmCliLimitsShow	Shows the current values of the limits on the number of CDP domains, endpoints, entries, and default routes.
gkDbmCliLimitsSet	Sets user specified limits on CDP domains, endpoints, entries, and default routes.
gkDbmCliLimitsReset	Resets the limits to the standard default values.

D-channel CLI command

Table 33 includes a CLI command which displays the D-channel menu.

Table 33
D-channel CLI commands

CLI Command	Description
DCHmenu	Displays a menu to perform various information retrieval operations for the D-channel. The output for DCHmenu: oam->DCHmenu Please select one of the DCHmenu options: 0 - Print menu (default) 1 - Print current DCH state 2 - Print current DCH configuration 3 - Print application error log 4 - Print link error log 5 - Print protocol error log 6 - Print message log 7 - Enable printing all messages processed by UIPC 8 - Enable error printing 9 - Enable info printing 10 - Enter manual message mode 11 - Print b channel control blocks 99 - Exit menu Please enter your DCHmenu choice (0 to print the menu): 1

H.323 CLI commands

Table 34 includes CLI commands used for the H.323 debug logs.

Table 34
H.323 CLI commands

CLI Command	Description
VTrkCallTrace H323 (chanID,onFlag)	Turns on H.323 debug log message for one channel for call associated signaling. Multiple traces can be up to 3 channels. • The channel must be registered before the CLI can be issued. • onFlag is used to turn on/off debug trace tool. Output format: oam->VTrkCallTrace H323 4,1 20/06/02 12:54:52 LOG0007 NPM: ISDN Call Setup msg rcvd: msgPtr=0xc0d9b0c 20/06/02 12:54:52 LOG0007 NPM: npmOutCallSetup: SESSION 0xbf3ca74, chid 4; uu_msg_length 82 20/06/02 12:54:52 LOG0007 NPM: npmOutCallSetup: Called 1003; Calling 5100 20/06/02 12:54:52 LOG0007 NPM: CHID 4: npmOutCallSetup: Calling num: 5100, Called num: 1003, ESN5 prefix 20/06/02 12:54:52 LOG0007 NPM: npmTunneledUIPEInsert: chid 4 ISDN setup:msg 0xc0d9b0c length 82
VTrkNonCallTrace H323 (chanID,onFlag)	Turns on H.323 debug log message for one channel for non-call associated signaling. Multiple traces can be up to 3 channels. • The channel must be registered before the CLI can be issued. • onFlag is used to turn on/off debug trace tool. Output format is the same as VTrkCallTrace H323(chanID,onFlag).

STAT CLI commands

Table 35 includes the STAT LINK and STAT SERV CLI commands (LD 117). These commands display the link information of the connected services. These command are applicable to the Call Server.

Table 35
STAT CLI commands

CLI Command	Description
stat link ip <IP address>	Displays the link information and link status of the server with the specified IP address or contained specified subnet.
stat link srv ss	Displays the link information and link status of the Succession Signaling Servers.
stat link name <hostname>	Displays the link information and link status of the server with the specified hostname.
stat link node <node ID>	Displays the link information and link status of the server with the specified node ID.
stat serv ip <IP address>	Displays the information of the server with the specified IP address or contained specified subnet.
stat serv app <applicationType>	Displays the information of the server running the specified application. Where application type can be: • LTPS (Line TPS) • VGW (Voice Gateway) • H323 (H323 Virtual Trunk) • GK (Gatekeeper)
stat serv node <node ID>	Displays the information of the server with the specified node ID.
stip tn <tn>	Displays the IP information and status of the specified TN.
stip type ipti	Displays the IP information and status of all TNs that are of IPTI (Virtual Trunk and ITG Trunk) type

Graceful disable commands

Table 36 includes graceful disable CLI commands applicable to the Succession Signaling Server. They are issued from the oam shell.

Table 36
Graceful Disable commands (Part 1 of 2)

CLI Command	Description
vtrkShow	Displays information and status of virtual trunk channels.
disServices	Causes the server to gracefully switch the registered resources to the other services in the same node.
disTPS	Causes the line LTPS to gracefully switch the registered sets to the other cards located in the same node.
disVTRK	Causes the virtual trunk to gracefully switch the registered virtual trunks to other SS located in the same node.
disGK	Puts the local gatekeeper out of service and puts the alternative gatekeeper in service (if available).
forcedisServices	Forces the server to switch the registered resources to the other services in the same node.
forcedisTPS	Forces all registered line LTPS to unregister from the local server.
forcedisVTRK	Forces all registered virtual trunks to unregister from the local server.
forcedisGK	Forces the local gatekeeper to be put out of service.
enlServices	Causes all the services to accept registration of resources.
enlTPS	Causes line TPS application to be enabled and to accept set registrations.
enlVTRK	Causes the virtual trunk application to be enabled and to accept virtual trunk registrations.

Table 36
Graceful Disable commands (Part 2 of 2)

CLI Command	Description
enlGK	Causes the local gatekeeper to be put in service. The local gatekeeper becomes the active Gatekeeper when it is: • the Primary Gatekeeper • the Alternate Gatekeeper and Primary Gatekeeper is out of service • the Fail Safe Gatekeeper and both Primary Gatekeeper and Alternate Gatekeeper are out of service The local gatekeeper becomes the standby Gatekeeper when it is: • the Alternative Gatekeeper and the Primary Gatekeeper is in service (active) • the Fail Safe Gatekeeper and either the Primary Gatekeeper or Alternate Gatekeeper is active
loadBalance	Causes the service to attempt to balance the registration load of sets between this service and the rest of the node services.
servicesStatusShow	Shows the status of services (tps/iset/vtrk/gk)
soHelpMenu	Displays the above commands.

Succession Signaling Server error logging and SNMP alarms

SNMP alarms

When the IP Peer Gateway and Gatekeeper applications generate alarms, these alarms are output from the Succession Signaling Server. When an error or specific event occurs, SNMP sends an alarm trap to OTM or any SNMP manager that is configured in the SNMP section of the Node Properties in Element Manager.

For example, an SNMP alarm is generated if the Succession Signaling Server loses the link to the Succession Call Server.

OTM receives SNMP traps from the Succession 1000 and Succession 1000M Large and Small Systems and stores them in a circular log file on the OTM Server. The OTM Alarm Notification application monitors incoming traps and notifies the appropriate users of important events and alarms. For more information about OTM alarm management, refer to *Succession 1000 System: Maintenance* (553-3031-500).

HPOpenView or Optivity NMS are examples of SNMP managers.

Error logging

An SNMP alarm places a system error message into the Succession Signaling Server's error log file. The error log file can be viewed using Element Manager. The file can also be viewed in any text browser once the file is uploaded to an FTP host using the LogFilePut command.

Use Procedure 54 on page 359 to view the error log in Element Manager.

Procedure 54
Viewing the error log file in Element Manager

1. Select **System Status** from the Navigation Tree.
2. Select **IP Telephony**. The **IP Telephony information** pages displays.
3. Expand the node containing the associated Succession Signaling Server.

4 Click the **RPT LOG** button. The RPT LOG button launches the **Report Utility** webpage for Signaling Servers. For more information about this page, refer to *Succession 1000 Element Manager: System Administration* (553-3001-332) /*Succession 1000 Element Manager: Installation and Configuration* (553-3001-232).

End of Procedure

The System Status webpage provides status information about the system and access to diagnostic tools. These tools enable users to issue commands to maintain Succession 1000 components and Succession 1000M components. Use features on the System Status webpage to perform maintenance tasks, troubleshooting, and problem resolution.

Error message format

ITG messages are generated from the Voice Gateway Media Cards and the Succession Signaling Server. ITS messages are generated from the Internet Telephone and are reported through the Succession Signaling Server.

The format of the ITG and ITS error messages is ITGsxxx or ITSsxxx, where sxxx is a four digit number. For example, ITG0351.

The first digit of the four digit number in the error message represents the severity category of the message. The severity categories are:

1 = Critical
2 = Major
3 = Minor
4 = Warning
5 = Cleared (Info)
6 = Indeterminate (Info)

Note: Message numbers beginning with 0 do not follow this format.

For a detailed list of the ITG and ITS error messages, refer to *Software Input/ Output: System Messages* (553-3001-411).

Appendix A: ISDN/H.323 mapping tables

Nortel Networks proprietary Private UDP numbers (ESN LOC) are encoded as Private Level 1 Regional numbers in H.323. CDP numbers are encoded as Private Level 0 Regional numbers in H.323. In H.225.0 (Q.931) messages, public numbers (E.164) are encoded in the Information Element (IE). Private numbers are encoded in the User to User Information Element (UUIE). On reception, both the IE and UUIE are accepted. If both are included, preference is given to the proper format (that is, the IE for public numbers and the UUIE for private numbers). The numbers in the Signaling Server are encoded using the Universal ISDN Protocol Engine (UIPE) format (which is different from Q.931/MCDN/H.323). Tables 37 to 46 describe the mapping.

Table 37
Mapping from UIPE to H.225.0 for NPI

Numbering Plan Indicator (NPI)	UIPE	H.225.0 IE NPI	H.225.0 UUIE NPI
Unknown	0000 (0)	1001 (9)	privateNumber
ISDN/Telephony (E.164)	0001 (1)	0001 (1)	publicNumber
Private	0010 (2)	1001 (9)	privateNumber
Telephony (E.163)	0011 (3)	0001 (1)	publicNumber
Telex (F.69)	0100 (4)	0100 (4)	N/A
Data (X.121)	0101 (5)	0011 (3)	N/A
National Standard	0110 (6)	1000 (8)	N/A

Table 38
Mapping from UIPE to H.225.0 for TON (NPI = E.164/E.163)

TON (NPI=E.164/E.163)	UIPE TON	H.225.0 IE TON	H.225.0 UUIE TON
Unknown	000 (0)	000 (0)	unknown
International number	001 (1)	001 (1)	internationalNumber
National number	010 (2)	010 (2)	nationalNumber
Special number	011 (3)	011 (3)	networkSpecificNumber
Subscriber number	100 (4)	100 (4)	subscriberNumber

Table 39
Mapping from UIPE to H.225.0 for TON (NPI = Private)

TON (NPI = Private)	UIPE TON	H.225.0 IE TON	H.225.0 UUIE TON
Unknown	000 (0)	000 (0)	unknown
ESN LOC (UDP)	101 (5)	000 (0)	level1RegionalNumber
ESN CDP	110 (6)	000 (0)	localNumber
ESN Special Number	011 (3)	000 (0)	pISNSpecificNumber
Note: When NPI = Private, the number digits are encoded in the privateNumber of PartyNumber, which includes the Type of Number (TON). The TON in the H.225.0 IE are ignored on receipt and coded as Unknown (that is, 0000.) In H.323 version 4, “publicNumber” is renamed “e164Number”.			

Table 40
Mapping from H.225.0 Information Element to UIPE for NPI (Part 1 of 2)

NPI	H.225.0 IE NPI	UIPE NPI
ISDN/Telephony (E.164)	0001 (1)	0001(1)
Private	1001 (9)	0010 (2)
Telephony (E.163)	0010 (2)	0011 (3)

Table 40
Mapping from H.225.0 Information Element to UIPE for NPI (Part 2 of 2)

NPI	H.225.0 IE NPI	UIPE NPI
Telex (F.69)	0100 (4)	0100 (4)
Data (X.121)	0011 (3)	0101 (5)
National Standard	1000 (8)	0110 (6)
Unknown	all others	0000 (0)

Table 41
Mapping from H.225.0 Information Element to UIPE for TON (NPI = E.164/E.163)

TON (NPI = E.164/E.163)	H.225.0 IE TON	UIPE TON
International number	001 (1)	001 (1)
National number	010 (2)	010 (2)
Network specific number	011 (3)	011 (3)
Subscriber number	100 (4)	100 (4)
Unknown	all others	000 (0)

Table 42
Mapping from H.225.0 Information Element to UIPE for TON (NPI = Private)

TON (NPI = Private)	H.225.0 IE TON	UIPE TON
Level 1 Regional Number	010 (2)	101 (5)
Local Number/ Level 0 Regional	100 (4)	110 (6)
PISN Specific Number	011 (3)	011 (3)
Unknown	all others	000 (0)
Note: When NPI = Private, precedence is given to any number in the H.225.0 UUIE. The H.225.0 IE is only used if the H.225.0 UUIE is not present. The Presentation Indicator and Screening Indicator are always in the information H.225.0 IE. The H.225.0 UUIE is only used if the H.225.0 IE is not present. In H.323 version 4, “publicNumber” is renamed “e164Number”.		

Table 43
Mapping from H.225.0 UUIE to UIPE for NPI

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

Table 44
Mapping from H.225.0 UUIE to UIPE for TON (NPI = E.164/E.163)

TON (NPI = E.164/E.163)	H.225.0 UUIE TON	UIPE TON
International number	internationalNumber	001 (1)
National number	nationalNumber	010 (2)
Network specific number	networkSpecificNumber	011 (3)
Subscriber number	subscriberNumber	100 (4)
Unknown	all others	000 (0)

Table 45
Mapping from H.225.0 UUIE to UIPE for TON (NPI = Private)

TON (NPI = Private)	H.225.0 UUIE TON	UIPE TON
Level 1 Regional Number	level1 RegionalNumber	101 (5)
Local Number/ Level 0 Regional	localNumber	110 (6)
PISN Specific Number	pISNSpecificNumber	011 (3)
Unknown	all others	000 (0)

Table 46
Mapping from H.225.0 UUIE to UIPE for Unqualified Number

Unqualified Number	H.225.0 UUIE	UIPE NPI	UIPE TON
Dialed Digits	e164	0000 (0)	0000 (0)
Note: In H.323 version 4, “e164” is renamed “dialedDigits”. In H.323 version 4, “publicNumber” is renamed “e164Number”.			

Succession 1000, Succession 1000M

IP Peer Networking

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.
SL-1, Meridian 1, and Succession are trademarks of Nortel Networks. VxWorks is a trademark of Wind River Systems, Inc. Windows NT, Windows 2000, and Microsoft Internet Explorer are trademarks of Microsoft Corporation.
Publication number: 553-3001-213
Document release: Standard 1.00
Date: October 2003
Produced in Canada

NORTEL NETWORKS™