Nortel Communication Server 1000

Network Routing Service Installation and Commissioning

NN43001-564

Document status: Standard
Document version: 01.01
Document date: 30 May 2007

Sourced in Canada

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

Revision history

May 2007

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

Contents

New in this Release

Network Routing Service

The Network Routing Service (NRS) provides routing to SIP and H.323 compliant devices. The network protocol component of the NRS is comprised of:

- SIP routing
- H.323 Gatekeeper (GK)
- Network Connection Service (NCS)

CS 1000 Release 5.0 NRS is offered in two versions: (1) a VxWorks-based NRS comprising a SIP Redirect Server, NCS and GK and a (2) a Linux-based NRS comprising a SIP Proxy Server and Redirect Server, NCS, and GK.

The VxWorks-based NRS application software can be run on any of the following server platforms: ISP1100 server (1 GB RAM minimum), CPPM-SS server, IBM or HP Commercial-Off-the-Shelf (COTS) server. On any of those four server platforms the VxWorks-based NRS can be configured to run either stand-alone or co-resident with other CS 1000 Signalling Server applications, i.e. UNIStim IP Phone Line Terminal Proxy (LTPS), IP Peer virtual trunk SIP or H.323 signaling Gateway (VTRK GW), IP Phone Application Server. There are no functional changes in the Vxworks-based NRS application in CS 1000 Rls 5.0, as compared with CS 1000 Rls 4.5.

The Linux-based NRS application software can be run on either IBM or HP COTS server. The CS 1000 Rls 5.0 Signalling Server applications cannot be run on the Nortel Linux-based COTS server. Therefore the Linux-based NRS can be configured to run only stand-alone

SIP Proxy

Communication Server (CS) 1000 Release 5.0 adds a transaction stateful SIP Proxy to the IP Peer Network.

A SIP Proxy acts as both a server and a client. A SIP Proxy receives requests, determines where to send the requests, and acting as a client on behalf of SIP endpoints, passes requests to another server.

A SIP Proxy makes the following features and functionality, which are provided by CS 1000 Release 5.0, possible:

1. Transport Layer Security (TLS).

   TLS provides the NRS with private, secure signaling, message authentication, confidentiality, and integrity through end-to-end encryption of media exchanged between two SIP endpoints.

2. Mixed transport layer protocol.

   A mixed transport layer protocol enables gateways using TCP, TLS over TCP, or UDP to interoperate.

3. SIP Proxy and Redirect mode

   By default the SIP Proxy and Redirect Server functions as a SIP Proxy. However, an endpoint can request transaction by transaction that the SIP Proxy act as a SIP Redirect Server.

   A SIP Redirect Server receives requests, but does not pass the requests to another server. Instead, a SIP Redirect Server sends a response back to the SIP endpoint, indicating the IP address of the called user.

4. SIP NRS Privacy within a Trusted Network

   The SIP Proxy asserts a network identity of a caller in a SIP session within an established trust domain as set forth in RFC 3323, RFC 3324 and RFC 3325. This allows the Proxy to convey privacy on behalf of a SIP endpoint within the trusted network. The proxy will withhold a particular SIP endpoint’s identity outside of the trust domain if indicated by the end user or by network policy. This notion of providing privacy Identification is needed in order to deliver, within the trust domain, such features as Caller ID, Caller Name and Number Blocking, and Calling Name and Number. In addition, the use of this feature allows a public and private name to be identified between trusted entities.

5. Multiple contacts for registration.

   Each endpoint will be able to register more than a single transport and IP address. Furthermore, endpoint identifiers can be reused across service domains.

6. Post-routing SIP URI modification.

7. Transaction forking.

NRS database

The Linux-based NRS provides real-time synchronization of the databases on the Primary and Secondary Network Routing Servers.

Enterprise Common Manager framework

The Nortel Enterprise Common Manager (ECM) framework provides:

- Private Certificate Authority.
- Secure Shell (SSH) access to the Command Line Interface.
- Centralized point of access for the management of users, passwords, system access, and security.
- ECM navigator provides an overview of network components from the host’s perspective.
- Single point of access to manage the entire network: Element Manager and the Linux-based NRS Manager are components of ECM.

NRS Manager

NRS Manager is a web-based management application used to configure, provision, and maintain the NRS. Key usability improvements introduced in the Linux-based NRS Manager are:

- Enhanced searching and sorting capabilities including wild cards and selectable scope of the search
- Capability to copy and move routing entries
- Simplified configuration for geographic redundancy
- Routing tests are fully integrated with endpoint and routing entry configuration
- SIP phone context mapping tools are fully integrated with endpoint and routing entry configuration
- Security infrastructure provided by the Enterprise Common Manager framework

How to Get Help

Getting help from the Nortel web site

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

www.nortel.com/support

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

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

Getting help over the telephone from a Nortel Solutions Center

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

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the telephone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Network Routing Service overview

Contents

This section contains information on the following topics:

Introduction

The convergence of voice, video and data on a single IP network reduces the costs and complexities of communication technology. There are two standards for call signaling and control of Voice over IP (VoIP): the IETF SIP protocol and the ITU-T H.323 protocol.

IP Peer Networking enables customers to distribute the functionality of CS 1000 systems over a Wide Area Network, using either Nortel SIP or H.323 Gateways, or third-party SIP or H.323 Gateways.

The Network Routing Service (NRS) provides routing services to both SIP and H.323-compliant devices. The NRS allows customers to manage a single network dialing plan for SIP, H.323, and mixed SIP/H.323 networks.

IP Peer Networking and NRS provide an integrated VoIP network for the delivery of voice, video, and data. The NRS is comprised of three components:

- network protocol component with a transport layer subcomponent
- database component
- NRS Manager

NRS Manager, a web-based management application, is used to configure, provision, and maintain the NRS.

NRS for CS 1000 Release 5.0 software is offered in two versions: a SIP Proxy NRS and a SIP Redirect Server NRS.

The SIP Proxy NRS is comprised of

1. network protocol component consisting of
    - SIP component

   - H.323 Gatekeeper component
   - Network Connection Service (NCS)

   The SIP component is comprised of a

   - SIP Proxy and Redirect Server
   - SIP Registrar
   - Transport Layer Security component

   By default the SIP Proxy and Redirect Server acts as a SIP Proxy. However, an endpoint can request transaction by transaction that the SIP Proxy and Redirect Server act as a SIP Redirect Server.

2. NRS Database component.

   The NRS Database component supports

   - a Routing and Location Service shared by the SIP Proxy and Redirect Server, the SIP Registrar, and the H.323 Gatekeeper
   - database synchronization

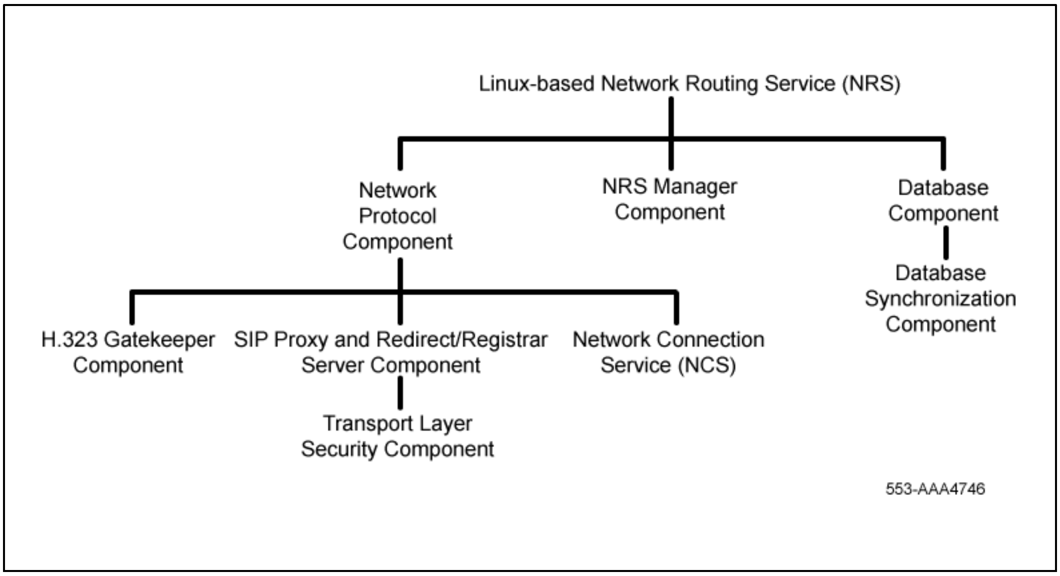
3. NRS Manager

The SIP Proxy NRS is hosted in a stand-alone mode on a dedicated server running the Linux™ real-time operating system.

The SIP Proxy NRS will be referred to as the Linux-based NRS.

Figure 1 "Linux-based NRS components" (page 22) shows a graphical view of the Linux-based NRS.

Figure 1
Linux-based NRS components


Linux-based Network Routing Service (NRS)
Network Protocol Component
NRS Manager Component
Database Component
Database Synchronization Component
H.323 Gatekeeper Component
SIP Proxy and Redirect/Registrar Server Component
Network Connection Service (NCS)
Transport Layer Security Component
553-AAA4746

The SIP Redirect Server NRS is comprised of

1. network protocol component consisting of
   - SIP component
   - H.323 Gatekeeper component
   - Network Connection Service (NCS)

   The SIP component is comprised of a
   - SIP Redirect Server
   - SIP Registrar
   - Transport Layer protocol component

2. NRS Database component.

   The NRS Database component supports
   - a Routing and Location Service shared by the SIP Redirect Server, the SIP Registrar, and the H.323 Gatekeeper
   - database synchronization

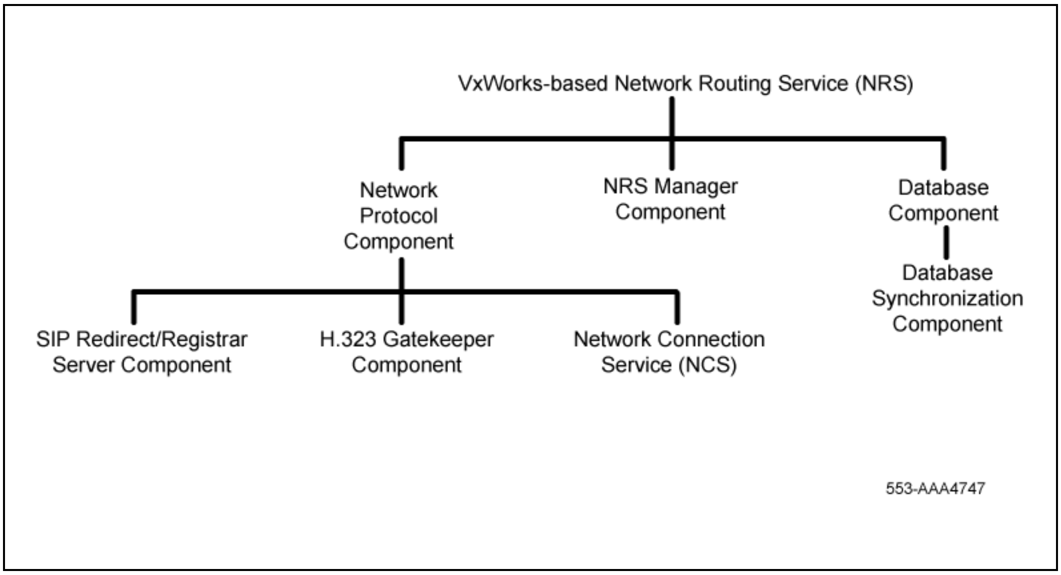
3. NRS Manager

The SIP Redirect Server NRS is hosted either co-resident with Signaling Server applications, or in a stand-alone mode on a dedicated server running the VxWorks™ real-time operating system.

The SIP Redirect Server NRS will be referred to as the VxWorks-based NRS.

Figure 2 "VxWorks-based NRS components" (page 23) shows a graphical view of the VxWorks-based NRS.

Figure 2
VxWorks-based NRS components


VxWorks-based Network Routing Service (NRS)
Network Protocol Component
NRS Manager Component
Database Component
Database Synchronization Component
SIP Redirect/Registrar Server Component
H.323 Gatekeeper Component
Network Connection Service (NCS)
553-AAA4747

Network protocol component

The NRS Network Protocol component is comprised of

- SIP Proxy and Redirect Server and a SIP Registrar, or a SIP Redirect Server and a SIP Registrar
- H.323 Gatekeeper
- Network Connection Service

and a transport layer subcomponent.

The SIP servers are network protocol components that serve SIP endpoints.

An H.323 Gatekeeper is a network protocol component that serves H.323 endpoints.

Session Initiation Protocol

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

The CS 1000 implementation of SIP complies with the standards described in the following Request for Comments (RFC) Internet Engineering Task Force (IETF) documents:

- RFC 3261 – SIP: Session Initiation Protocol
- RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 2806 – URLs for Telephone Calls
- RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3265 – Session Initiation Protocol (SIP)-Specific Event Notification
- RFC 3311 – The Session Initiation Protocol (SIP) UPDATE Method
- RFC 2976 – The SIP INFO Method
- RFC 3323
- RFC 3324
- RFC 3325

SIP entities

A SIP network is composed of five logical entities. The logical SIP entities are:

- User agent
- SIP Proxy Server
- SIP Redirect Server
- SIP Registrar Server
- Back-to-Back User Agent

User agent

A SIP user agent is an endpoint entity that initiates and terminates sessions by exchanging requests and responses. This document refers to SIP user agents as “SIP endpoints”. SIP endpoints are IP phones or SIP Gateways.

SIP Proxy Server

A SIP Proxy acts as both a server and a client. A SIP Proxy receives requests, determines where to send the requests, and acting as a client on behalf of SIP endpoints passes requests on to another server.

A SIP Proxy can be either a SIP stateful proxy server or a SIP stateless proxy server. A proxy server in a stateful mode remembers the incoming requests it receives, along with the responses it sends back and the outgoing requests it sends on. A proxy server acting in a stateless mode forgets all information once it has sent a request.

SIP Redirect Server

A SIP Redirect Server provides telephone number to IP address resolution. It translates telephone numbers recognized by Enterprise Business Network (EBN) voice systems to IP addresses in a SIP domain.

A SIP Redirect Server receives requests, but does not pass the requests onto another server. Instead, a SIP Redirect Server sends a response back to the SIP endpoint, indicating the IP address of the called user. Because the response includes the address of the called user, the caller can then directly contact the called party.

SIP Registrar

A SIP Registrar is a server that accepts REGISTER requests and updates the NRS database with the contact information specified in the request. A SIP Registrar accepts registration requests from SIP Phones, SIP Trunk Gateways, and other certified compatible third-party SIP endpoints.

Each endpoint will be able to register more than a single transport and IP address with the SIP Registrar deployed by the SIP Proxy. Furthermore, endpoint identifiers can be reused across service domains.

NRS SIP server implementation

The SIP standard does not specify how the functionality of the SIP server logical entities are implemented. They may be hosted on the same hardware platform or distributed across different servers. In the Network Routing Service, a single network server functions as both a SIP Proxy and Redirect Server and as a SIP Registrar, or as both a SIP Redirect Server and as a SIP Registrar. When emphasizing the network server’s dual functionality, it will be referred to as a SIP Proxy/Registrar Server or as a SIP Redirect/Registrar Server.

In the Linux-based Network Routing Service the SIP Registrar is co-resident with the SIP Proxy and Redirect Server on a dedicated server running the Linux™ real-time operating system. The SIP Proxy NRS is not co-resident with Signaling Server applications.

In the VxWorks-based Network Routing Service the SIP Registrar is co-resident with the SIP Redirect Server. The SIP Redirect Server is hosted either co-resident with Signaling Server applications, or in a stand-alone mode on a dedicated server running the VxWorks™ real-time operating system.

The SIP Proxy/Registrar Server and the SIP Redirect/Registrar Server are network protocol components of the Network Routing Service that serve SIP endpoints.

Back-to-Back User Agent

A SIP User Agent can act as a User Agent client and as a User Agent server. As a client a User Agent initiates SIP requests. As a server a User Agent returns a response. A Back-to-Back User Agent (B2BUA) processes a request on behalf of a client as a server. To determine how to answer a request, a B2BUA acts as a client and generates requests.

Unlike a SIP Proxy, a B2BUA must maintain call state and must participate in all requests sent on the calls it has established. A B2BUA can disconnect a call or alter SIP messages. A SIP Proxy can not.

The Multimedia Communication Server (MCS) 5100 is a SIP B2BUA.

SIP domains

SIP endpoints (User agents) are grouped into domains. A SIP domain is managed by a SIP Proxy/Registrar Server or by a SIP Redirect/Registrar Server. A SIP domain is an administrative unit in the NRS database. NRS SIP domains comprise SIP Service Domains and L1 and L0 Regional Domains.

A SIP service domain can and should map into a fully qualified DNS namespace domain. NRS does not have a DNS client. NRS interoperates with third party gateways that may have a DNS client.

L1 and L0 Regional Domains are SIP subdomains. L1 and L0 SIP subdomains are not part of the DNS namespace. L1 and L0 SIP subdomains are not DNS subdomains.

For more information on SIP domains see Figure 4 "Hierarchy of the NRS database components" (page 35) and "SIP Uniform Resource Identifiers" (page 38).

Location Service

Users may move between SIP endpoints and they may be addressable by multiple names. SIP deals with this complexity by distinguishing between an address of record (AOR) and contact addresses.

An AOR is a SIP, or SIPS, Uniform Resource Identifier (URI) that points to a domain with a location service. A contact address is an IP address or DNS name for a SIP device.

A User, User Agent or Service has a unique AOR. A user can have more than one contact address. A user is not limited to registering from a single device. Similarly, more than one user can be registered to a single device.

SIP registration expires unless refreshed. At periodic intervals SIP devices send REGISTER messages to inform the SIP Registrar of the device's current contact address. The SIP Registrar associates (or binds) the AOR in the REGISTER message with the contact address. The SIP Registrar writes the binding to a database. This database is called a location service. The location service contains a list of bindings of AORs to zero or more contact addresses. The NRS database is a location service.

The location service and routing tables in the NRS database are used by a SIP Proxy or a SIP Redirect Server for AOR-to-contact-address resolution.

A SIP endpoint registers with a SIP Registrar to get authorization to initiate a call and/or receive other services. The SIP Registrar updates the NRS database with the client contact information. The NRS database provides a location service that is used by the SIP Proxy or SIP Redirect Server to locate the SIP Trunk Gateway that serves the target of a SIP request. A SIP Trunk Gateway has a number of non-SIP lines and trunks behind it which do not have their own identity in the SIP domain. These non-SIP endpoints are accessed by mapping SIP URIs based on telephony Directory Numbers (DN) to one or more SIP Trunk Gateways. The location service is effectively a matching mechanism that allows a fully-qualified telephone number to be associated with a range of telephone numbers and the SIP Trunk Gateway that provides access to that DN range.

NRS purpose

The NRS:

- Populates the location and registration database.
- Populates routing tables.
- Adds SIP Proxy and Redirect Servers, or SIP Redirect Servers, to the customer network.
- Provides a translation database for telephone numbers contained within the SIP Uniform Resource Identifier (URI) in order to present a well-formed, syntactically-correct telephone number to the location service within the proxy.
- Linux-based NRS populates post-routing SIP URI modification tables.

Signaling Gateways

Signaling gateways translate signaling messages between one medium and another. They provide a bridge between analog or digital devices and IP networks.

Signaling gateways also provide bridge between one set of IP devices and another set of IP devices.

The IP Peer Network supports the following signaling gateways:

1. SIP gateway
2. H.323 gateway
3. ISDN (Integrated Services Digital Network) PRI (Primary Rate Interface) and ISDN BRI (Basic Rate Interface) to SIP conversion
4. PBX (Private Branch Exchange) to SIP conversion
5. T1/E1 to SIP conversion - bridge between PSTN and an IP network

SIP Gateway

SIP Gateway Signaling is an industry-standard, SIP-based, IP Peer solution that delivers a SIP interface for interoperability with standard SIP-based products.

- uses Virtual Trunks to enable direct, end-to-end paths between two SIP compatible IP devices.
- provides an interface between SIP networks and legacy ISDN and PSTN switched circuit networks. Gateways provide signaling mapping as well as transcoding between IP packet and circuit-switched formats.

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

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

CS 1000 supports SIP Gateway Signaling and SIP Services

SIP services

SIP Services, include

- Converged Desktop Service (CDS). SIP CDS integrates CS 1000 telephony features with Multimedia Communication Server (MCS) 5100 applications.

SIP CDS allows users to use their existing telephony system for voice communication and to use their PC for multimedia communication.

- Microsoft LCS 2500 Office Communicator.
- IBM Lotus Notes Converged Desktop.

H.323 protocol

H.323 is a signaling protocol for the real-time integration of voice, video, and data in a VoIP network.

The CS 1000 implementation of H.323 complies with the standards of the International Telecommunication Union (ITU) described in the following Recommendation documents of the ITU Telecommunication Standardization Sector (ITU-T):

- H.245
- H.225
- Registration Admission Status (RAS)
- Real-Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP)

H.323 entities

An H.323 network is composed of four H.323 entities defined by the ITU-T H.323 standard. The four H.323 entities are:

- H.323 terminal
- H.323 Gatekeeper
- Gatekeeper zone
- H.323 Gateway

H.323 terminal

An H.323 terminal is an endpoint that enables real-time communication with other H.323 terminals. This document refers to H.322 terminals as “H.323 endpoints”. H.323 endpoints are IP Phones and H.323 Gateways.

H.323 Gatekeeper

Gatekeepers manage H.323 endpoints in an H.323 network. H.323 endpoints register to a gatekeeper. H.323 endpoints communicate with gatekeepers using the Registration Admission Status (RAS) protocol.

An H.323 Gatekeeper is a network protocol component of the Network Routing Service that serves H.323 endpoints.

Gatekeeper zones

H.323 endpoints are grouped into zones. Each zone is managed by a gatekeeper. A gatekeeper zone is an administrative unit within an IP Peer Network. Separate NRS databases must be managed for each zone.

H.323 Gateway

An H.323 Gateway

- uses Virtual Trunks to enable direct, end-to-end paths between two H.323 compatible IP devices.
- provides an interface between H.323 IP networks and legacy ISDN and PSTN switched circuit networks. Gateways provide signaling mapping as well as transcoding between IP packet and circuit-switched formats.

SIP and H.323 interworking

Table 1 "Comparison of SIP and H.323 terminology" (page 30) summarizes SIP and H.323 interworking terminology.

Table 1
Comparison of SIP and H.323 terminology

NRS Server	In SIP, a SIP Proxy/Registrar or SIP Redirect/ Registrar Server In H.323 a Gatekeeper
Endpoint	SIP endpoint (SIP User Agent) H.323 endpoint (H.323 Terminal)
Address Format	SIP supports the URI (Universal Resource Indicator) address format
Endpoint Registration	In Linux-based NRS a SIP client registers to a SIP Proxy/Registrar to update the NRS database. In Vxworks-based NRS a SIP client registers to a SIP Redirect/Registrar Server to update the NRS database. An H.323 endpoint registers with a H.323 Gatekeeper to update the NRS database

The interworking between SIP-oriented services and H.323-oriented services is achieved through the CS 1000 Call Server.

Network Connection Service

The NCS is used to support the Media Gateway 1000B (MG 1000B), IP Line Virtual Office, Branch Office (including the SRG), and Geographic Redundancy features. The NCS provides an interface to the TPS, enabling the TPS to query the NRS using the UNIStim protocol.

- Network Connection Service (NCS) – The NCS is required for the IP Line Virtual Office, Branch Office (including the SRG), and Geographic Redundancy features. The NCS allows the Line TPS (LTPS) to query the NRS using the UNIStim protocol.

There are four areas in CS 1000 Element Manager and in NRS Manager for configuring the NCS:

- In Element Manager, the H.323 Gateway Settings contains the NCS configuration. See **IP Network > Node: Servers, Media Cards > Configuration > Edit > Signaling Servers > Signaling Server Properties > H323 GW Settings** in the Element Manager Navigator. For more information see .
- In VxWorks-based NRS Manager, NCS is configured in the following areas:
  - For configuration of the NRS server to support the NCS, see **Home > NRS Server Settings > NCS Settings** (see Procedure 79 "Configuring NRS Server Settings" (page 302)).
  - Configuration of Virtual Office and branch office (including the SRG) user redirection to the main office, see **Configuration > Gateway Endpoints** (see Procedure 87 "Adding a Gateway Endpoint" (page 320)).
  - Configuration of the Virtual Office Login, see **Configuration > Collaborative Servers** (see Procedure 94 "Viewing the Collaborative Servers" (page 341)).

SIP NRS Privacy within a Trusted Network

Within the Linux-based NRS the SIP Proxy asserts a network identity of a caller in a SIP session within an established trust domain as set forth in RFC 3323, RFC 3324 and RFC 3325. This allows the Proxy to convey privacy on behalf of a SIP endpoint within the trusted network. The proxy will withhold a particular SIP endpoint's identity outside of the trust domain if indicated by the end user or by network policy. This notion of providing privacy Identification is needed in order to deliver, within the trust domain, such features as Caller ID, Caller Name and Number Blocking, and Calling Name and Number. In addition, the use of this feature allows a public and private name to be identified between trusted entities.

NRS Failsafe

Within the Linux-based NRS, a failsafe mechanism, used to update CS1000 SIP Gateways configured with the failsafe function, has been deployed in CS 1000 Release 5.0. The failsafe function on the IP Peer Gateways is used as a mechanism by which the SIP Gateways stay in contact with the CS1000 switching agent when network connectivity has been lost to both the primary and secondary NRS service. In order to use proper routing data, the Linux-based NRS, at the prescribed time, will initiate an update session with the CS1000 SIP Gateway, format the SIP routing data from the NRS on Linux, and begin the transfer of the data to the gateway.

In order to perform the failsafe synchronization, the Linux-based NRS should update the solid data remotely to the failsafe server running on VxWorks. At intervals of every 6 hours, the failsafe mechanism synchronizes and updates the routing data with the NRS on Linux for registered failsafe supported gateways.

To reduce CPU load, the failsafe synchronization is only triggered if there is a change to the solid database on Linux. When Cut over and Commit database action is performed, only the changed data needs to be updated on the failsafe server running on VxWorks.

Since the failsafe mechanism is executed periodically, the Linux cron takes care to trigger the operation every 6 hours.

When the Linux cron starts the failsafe synchronization, it may get aborted for the following reasons:

1. When there is no failsafe server configured.
2. When there is no change done to solid database on Linux.
3. When the failsafe data entry is NULL.

Failsafe NRS synchronization

The Failsafe NRS synchronization script provides a manual command to invoke Failsafe NRS synchronization immediately, instead of waiting up to 6 hours for the Linux cron to invoke the scheduled Failsafe NRS synchronization.

CS 1000 Release 5.0 interoperability with NRS Release 4.5

CS Release 5.0 endpoints can register as SIP Gateways and H.323 Gatekeepers with NRS Release 4.5.

Database component

NRS Database

The NRS database is comprised of endpoints (IP phones, SIP gateways, H.322 gateways, and collaborative servers), routing tables containing routes to these endpoints and post-routing SIP URI modification tables.

The NRS database stores the central dialing plan in XML format for the SIP Proxy, the SIP Redirect Server and the H.323 Gatekeeper. The SIP Proxy, the SIP Redirect Server and the H.323 Gatekeeper access this common endpoint and gateway database.

The NRS allows for the configuration of multiple customers.

The advantages of the NRS database are:

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

The database component of the NRS is responsible for:

- configuring the numbering plan
- reading and updating the active and standby databases on disk
- resolving all registrations and requests which the NRS passes to the database

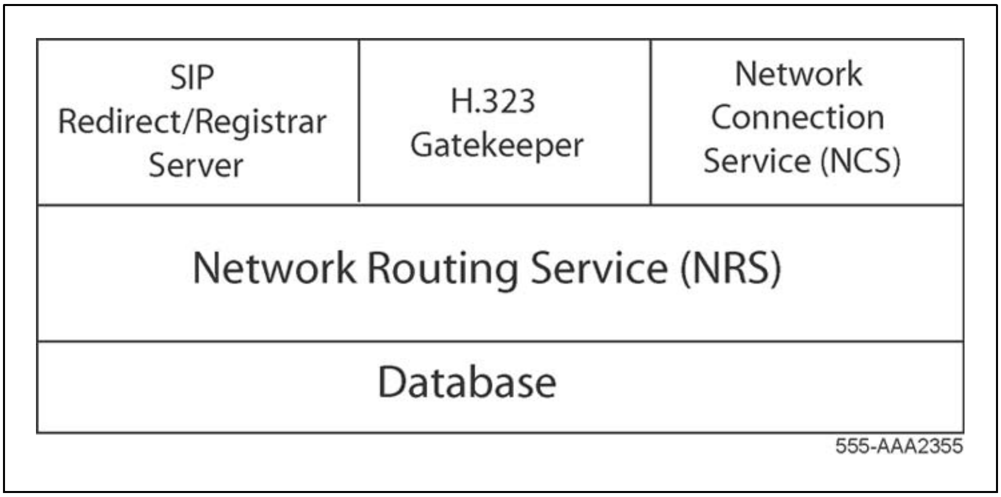
The NRS numbering plan configuration is stored in XML format in two databases on disk. The active database is used for call processing and the standby database is used for configuration changes.

The database component interfaces with the active and standby databases on disk. All call processing requests that the NRS passes to the database are resolved using the active database. The database uses the information that the NRS extracted from the request to search its database. For example, in the case of a SIP? message or an H.323 ARQ message, the database attempts to find a registered endpoint that can terminate the call.

The NRS Manager web server interfaces with the database for viewing, adding, deleting, or modifying numbering plan configuration data and routing entries. 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 active database. The database is cut over to the active database by executing a database **Cut over** command.

The NRS database provides a central database of addresses that are required to route calls across the network. The NRS database resides on the server hosting the Network Routing Service (see Figure 3 "NRS database and network protocol components" (page 34)).

Figure 3
NRS database and network protocol components


SIP Redirect/Registrar Server
H.323 Gatekeeper
Network Connection Service (NCS)
Network Routing Service (NRS)
Database
555-AAA2355

The SIP Proxy, the SIP Redirect Server and the H.323 Gatekeeper have access to the endpoint/location database.

- The SIP Proxy and the Redirect Server access the location database on CS 1000 systems to direct SIP Trunk Gateways within a networked environment.
- The H.323 Gatekeeper also accesses the central location database, but to direct H.323 Gateways.

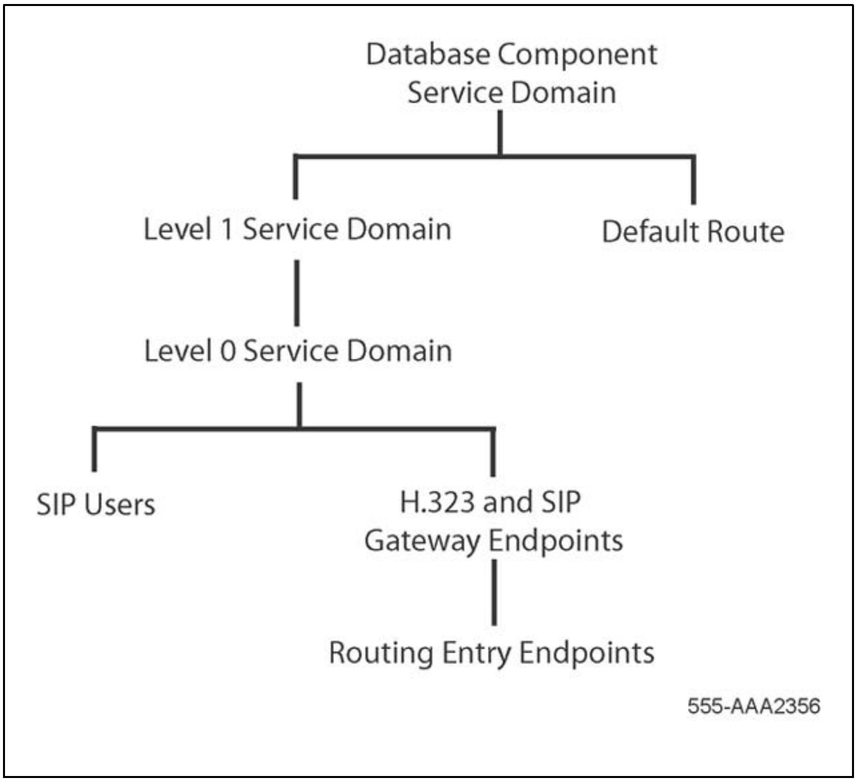
The routing data is the same for SIP and H.323. As a result, the SIP Proxy, the SIP Redirect Server and the H.323 Gatekeeper provide address-resolution functionality for the CS 1000 Call Server.

Figure 4 shows a hierarchical view of the database. The data is stored and organized in the database as described in Figure 4 "Hierarchy of the NRS database components" (page 35). The data is used by the SIP Proxy, the SIP Redirect Server and the H.323 Gatekeeper.

The routing data is the same for SIP and H.323. As a result, the SIP Proxy, the SIP Redirect Server and the H.323 Gatekeeper provide address-resolution functionality for the CS 1000 Call Server.

Figure 4 "Hierarchy of the NRS database components" (page 35) shows a hierarchical view of the database. The data is stored and organized in the database as described in “Hierarchical model of the Network Routing Service” on page 41. The data is used by the SIP Proxy, the SIP Redirect Server and the H.323 Gatekeeper.

Figure 4
Hierarchy of the NRS database components



Hierarchical model of the Network Routing Service

The NRS can support multiple customers and can provide routing services to several service provider networks. To do this, the NRS server uses the hierarchical model outlined in Table 2 "Hierarchical model of the Network Routing Service" (page 35). This model determines how information is stored and organized in the database. The data stored in the database is common to both H.323 and SIP.

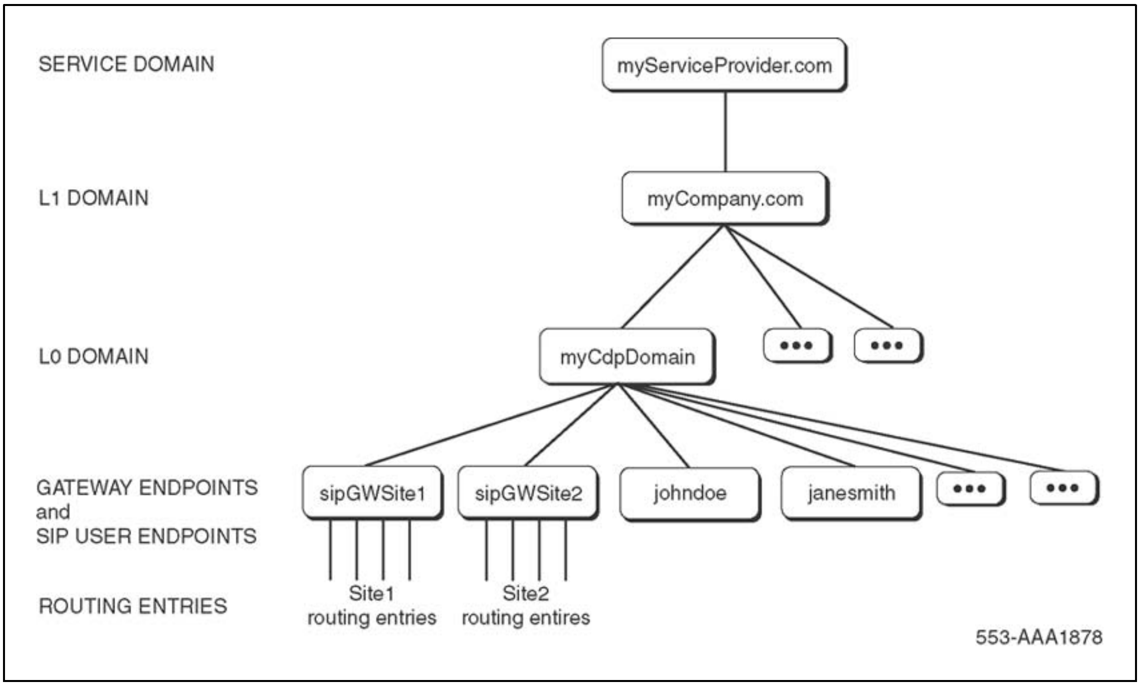
Table 2
Hierarchical model of the Network Routing Service

Level	Description
Service Domain	Represents a service provider network. A service domain maps into a SIP-domain. Example: myServiceProvider.com

Level	Description
Level 1 Regional Domain	Represents a subdomain in a Service Domain. ***Note 1:*** The Level 1 Regional Domain is also referred to as the L1-domain (in the context of the Network Routing Service). An L1-domain maps into an enterprise/customer network as well as a Meridian Uniform Dialing Plan (UDP) domain. The L1-domain should match across the UDP domain including E.164. Example: myCompany.com ***Note 2:*** UDP means all the call types in the dialing plan which include private (special numbers) and public (national, international, subscriber, and special numbers).
Level 0 Regional Domain	Represents a subdomain in a Level 1 Regional Domain. ***Note 1:*** The Level 0 Regional Domain is also referred to as the L0-domain (in the context of the Network Routing Service). An L0-domain maps to a site level as well as a Meridian Coordinated Dialing Plan (CDP) domain. The L0-domain should match across the CDP domain. Example: myCdpDomain ***Note 2:*** A site can be a street address, a campus, or a metropolitan area.
Gateway Endpoint	Represents a gateway. It exists within an L0 Domain. A site can have many endpoints. Example: sipGWSite1, sipGWSite2
User Endpoints	Represents a SIP Phone. It exists with the L0 domain. A site can have many SIP Phones. Example: johndoe, janesmith
Routing Entry	Represents a range of addresses (URIs) where a gateway can terminate calls. A routing entry exists within a gateway. These are the routing entries that the gateway supports.

Figure 5 "Hierarchical structure of the Network Routing Service" (page 37) shows the hierarchical structure of the Network Routing Service.

Figure 5
Hierarchical structure of the Network Routing Service



> ***Note:*** If there is no Service Domain, the Service Domain must be configured the same as the Level 1 Regional Domain.

For example:

- Bell Canada is the Service Provider.
- Nortel is the Level 1 Domain.
- Sites within Canada can make up the Level 0 Domains

  (such as Belleville or Ottawa).
- Switches at the sites are the Gateway Endpoints.

SIP authentication

The data that the SIP Proxy/Registrar and the SIP Redirect/Registrar Server needs to successfully perform authentication is configured in two ways:

- Group identity
  - — against an enterprise network (that is, the Level 1 Regional domain)
  - — against a site in the enterprise network (that is, the Level 0 Regional (CDP) Domain)
- Individual endpoint identity
  - — against a Gateway Endpoint

— against a SIP User Endpoint

If a gateway endpoint does not have individual identity configured, then the L0 Domain group identity data is used by the SIP Proxy/Registrar and the SIP Redirect/Registrar Server during the authentication procedure.

If neither the individual endpoint identity nor the L0 identity is provided, then L1 Domain identity is used.

Configuring authentication in the NRS

Authentication is configured using NRS Manager. Authentication can be configured at the following levels in the NRS:

Level 1 Domain and Level 0 Domain Authentication can be turned on or off at this level. If authentication is turned on, then all Gateway Endpoints and SIP User Endpoints require authentication.

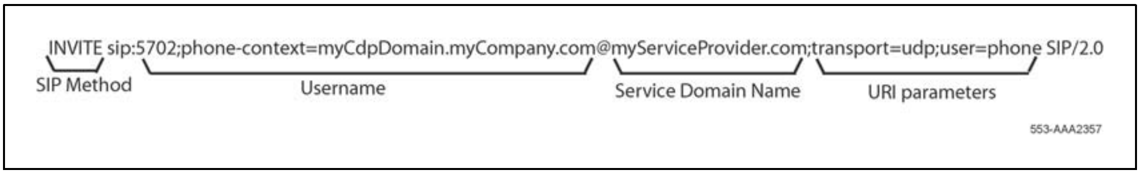
Gateway Endpoints and SIP User Endpoints Authentication can also be turned on or off at the Gateway Endpoint and SIP User Endpoint levels. This level provides three authentication options:

- Not configured — If this option is selected, then the endpoint uses the Level 1 or Level 0 Domain authentication (if Level 1 authentication is enabled).
- Authentication off — If authentication is turned off, then authentication is off for this endpoint even if Level 1 or Level 0 Domain authentication is enabled. This endpoint authentication setting overrides the Level 1 and Level 0 Domain authentication setting.
- Authentication on — If authentication is turned on, then authentication is on for this endpoint and the authentication overrides the Level 1 and Level 0 Domain authentication (if it is enabled). This endpoint authentication setting overrides the Level 1 and Level 0 Domain authentication setting.

SIP Uniform Resource Identifiers

The NRS supports SIP URIs (see Figure 6 "SIP URI example" (page 38)). A SIP URI is a user's SIP identity.

Figure 6
SIP URI example


INVITE sip:5702;phone-context=myCdpDomain.myCompany.com@myServiceProvider.com;transport=udp;user=phone SIP/2.0
SIP Method
Username
Service Domain Name
URI parameters
553-AAA2357

Where:

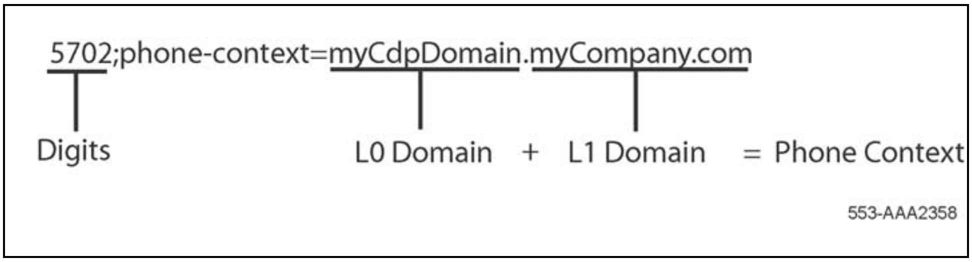
- **Username:** Specifies the actual subscriber information, which is used by the SIP Trunk Gateway to map to and from the NPI/TON field. The username field is parsed into a name and phone context (see Figure 7 "Username example" (page 39)).

  The subscriber information or the "username" part of the SIP URI (that is, the field before the @ symbol) is formatted as:

  digits;phone-context=[L0 subdomain name.L1 subdomain name]

  Where digits is the telephone number digits.

  Figure 7
  Username example


5702;phone-context=myCdpDomain.myCompany.com
Digits
L0 Domain + L1 Domain = Phone Context
553-AAA2358

  > ***Note:*** L0 and L1 Regional Domains are SIP subdomains. L0 and L1 SIP subdomains are not part of the DNS namespace. L0 and L1 SIP subdomains are not DNS subdomains.

- **Service Domain Name:** Each SIP domain is a collection of a group of users either within the same region or within the same organization. All users within the same domain share the same domain name, and each has a unique username within the domain. The domain name is well known by all SIP proxies. Typically, this is the host name after the @ symbol (for example, myServiceProvider.com).

  > ***Note:*** A SIP service domain can and should map into a fully qualified DNS namespace domain. NRS does not have a DNS client. NRS interoperates with third party gateways that may have a DNS client.

- **user=phone:** Indicates that the URI is for a telephone user.

Address lookup is based on the digits, phone context, and domain name:

sip:[number];phone-context=[L0 subdomain name.L1 subdomain name]
@[service domain];user=phone

The subdomain names are preconfigured data on both the SIP Trunk Gateway and SIP Redirect Server. The name explicitly maps a dialing plan to and from a SIP URI.

The ISDN NPI/TON field explicitly maps to the SIP phone-context attribute. The public numbering plans map to SIP URI by rules specified in RFC 2806 and RFC 3261. The exception is TON = unknown and TON = special number.

The private numbering plans, public/unknown numbers, and public/special numbers also have explicit one-to-one mappings to SIP URI. They must be defined by preconfigured subdomain names. The subdomain name must be defined on both Gateway and proxy/registrar.

The NRS also facilitates a translation database for phone numbers contained within the SIP URI, in order to present a well formed, syntactically correct phone number to the location service. Therefore, the NRS is designed to operate with both the phone-context and NPI/TON qualified numbers.

Example

Table 3 "Numbering plan mapping" (page 40) provides an example of the numbering plan mapping to clarify how different dialing plans are mapped to a SIP URI. Two methods can be used to configure the URI map — one for the NRS and one for the MCS 5100. Table 3 "Numbering plan mapping" (page 40) provides examples for both the NRS and MCS 5100.

Assume the following:

- The SIP Trunk Gateway has registered at a domain called myServiceProvider.com.
- A telephone user resides at sipGWSite1 and has ESN Location Code 343 with extension 3756. The Direct Inward Dialing (DID) number is 1-613-967-3756.

Refer to Figure 5 "Hierarchical structure of the Network Routing Service" (page 37) for the SIP address hierarchy tree.

Table 3
Numbering plan mapping

NPI/TON/DN	SIP URI
E.164/ International/ 1-613-967-3756	NRS example: sip:+16139673756@myServiceProvider.com;user=phone MCS 5100 example: sip:+16139673756@myServiceProvider.com;user=phone

NPI/TON/DN	SIP URI
	Note: Public international numbers do not have a phone context, as these numbers are globally unique within a domain. A "+" sign is automatically added by the gateway before the digits to indicate that the number is an international number.
E.164/National/ 613-967-3756	NRS example: sip:6139673756;phone-context=+1@myServiceProvider.com;user=phone MCS 5100 example: sip:6139673756;phone-context=mynation.national.e164.myrootdomain@myServiceProvider.com;user=phone
E.164/Subscriber/ 967-3756	NRS example: sip:9673756;phone-context=+1613@myServiceProvider.com;user=phone MCS 5100 example: sip:9673756;phone-context=myarea.mynation.local.e164.myrootdomain@myServiceProvider.com;user=phone
E.164/Unknown /9-1-613-967-3756	Not supported for the NRS. MCS 5100 example: sip:916139673756;phone-context=myarea.mynation.unknown.e164.myrootdomain@myServiceProvider.com;user=phone
E.164/ Special Number/ 911	Not supported for the NRS. MCS 5100 example: sip:911;phone-context=myarea.mynation.special.e164.myrootdomain@myServiceProvider.com;user=phone
Private/UDP/ 343-3756	NRS example: sip:3433756;phone-context=myCompany.com@myServiceProvider.com;user=phone MCS 5100 example: sip:3433756;phone-context=level1.private.myenterprise@myServiceProvider.com;user=phone
Private/CDP/ 3756	NRS example: sip:3756;phone-context=myCdpDomain.myCompany.com@myServiceProvider.com;user=phone MCS 5100 example: sip:3756;phone-context=mylocation.level0.private.myenterprise@myServiceProvider.com;user=phone

NPI/TON/DN	SIP URI
Private/ Special Number/ 911	NRS example: sip:911;phone-context=special.myCdpDomain.myCompany.com @myServiceProvider.com;user=phone MCS 5100 example: sip:911;phone-context=mylocation.special.private.myenterprise @myServiceProvider.com;user=phone
Private/ Unknown (Vacant Number Routing)/ 343-3756	No configuration is required for NRS. MCS 5100 example: sip:3433756; phone-context=mylocation.unknown.private.myenterprise @myServiceProvider.com;user=phone
Unknown/ Unknown/ 6-343-3756	No configuration is required for NRS. MCS 5100 example: sip:63433756; phone-context=mylocation.unknown.unknown. myrootdomain@myServiceProvider.com;user=phone

Database synchronization/operation component

The Network Routing Service can be redundantly instantiated across a cluster of Network Routing Servers sharing a distributed database. In CS 1000 Release 5.0 the cluster is comprised of a Primary Network Routing Server and a Secondary Network Routing Server.

> ***Note:*** In the VxWorks-based Network Routing Service the Secondary Network Routing Server is referred to as the Alternate Server.

The NRS database for each Network Routing Server has two schemas — an active schema and a standby schema.

- The active database is used for runtime location queries by SIP Proxy, Gatekeeper and Network Connection Service.
- The standby database is used by the administrator to modify the NRS database. An Administrator can only make changes to the standby database.

The database synchronization component has two functions:

1. Synchronization of the active and standby databases on a Network Routing Server.
2. Synchronization of the databases on the Primary and Secondary Network Routing Servers.

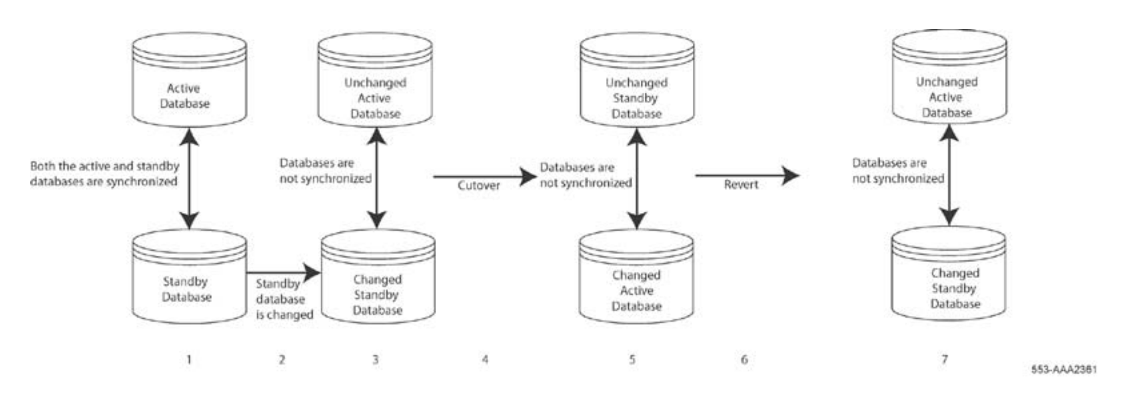
Synchronization of the active and standby databases on a Network Routing Server

Cut over and revert

Figure 8 "NRS database actions - Cut over and Revert" (page 43) shows both the active and standby database when **Cut over** and **Revert** database commands are issued.

1. The active and standby databases are synchronized.
2. A change is made to the standby database.
3. The standby database is changed and the active database is unchanged. The databases are not synchronized.
4. The database **Cut over** command is issued.
5. The changed database becomes the active database.
6. The database **Revert** command is issued. (Perhaps the Administrator wants to make more changes to the database.)
7. The changed database becomes the standby database.

Figure 8
NRS database actions - Cut over and Revert


Active Database
Unchanged Active Database
Unchanged Standby Database
Unchanged Active Database
Both the active and standby databases are synchronized
Databases are not synchronized
Cutover
Databases are not synchronized
Revert
Databases are not synchronized
Standby Database
Standby database is changed
Changed Standby Database
Changed Active Database
Changed Standby Database
1
2
3
4
5
6
7
553-AAA2381

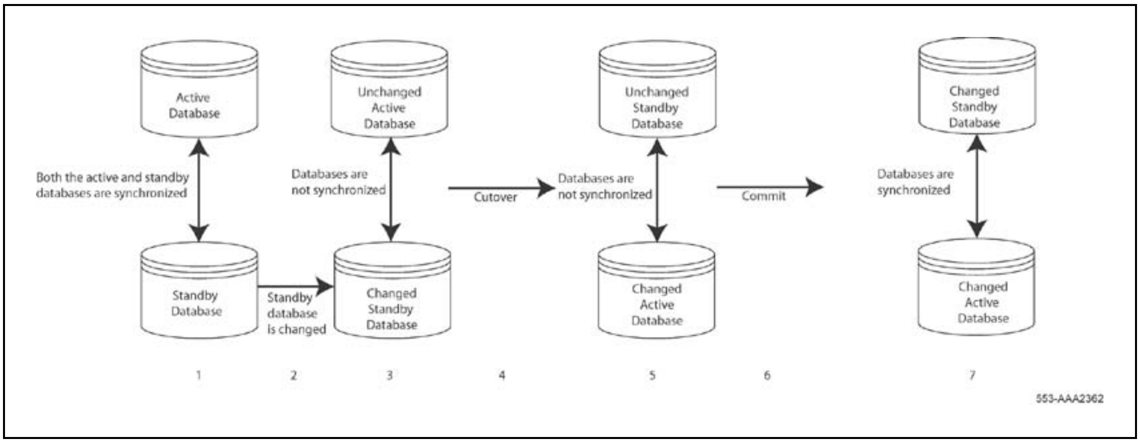
Cut over and commit

Figure 9 "NRS database actions - Cut over and Commit" (page 44) shows both the active and standby database when **Cut over** and **Commit** database commands are issued.

1. The active and standby databases are synchronized.
2. A change is made to the standby database.
3. The standby database is changed and the active database is unchanged. The databases are not synchronized.
4. The database **Cut over** command is issued.
5. The changed database becomes the active database.

6. The database **Commit** command is issued. (The administrator wants to submit the changes made to the database.)
7. The databases are synchronized. Both databases are changed.

Figure 9
NRS database actions - Cut over and Commit

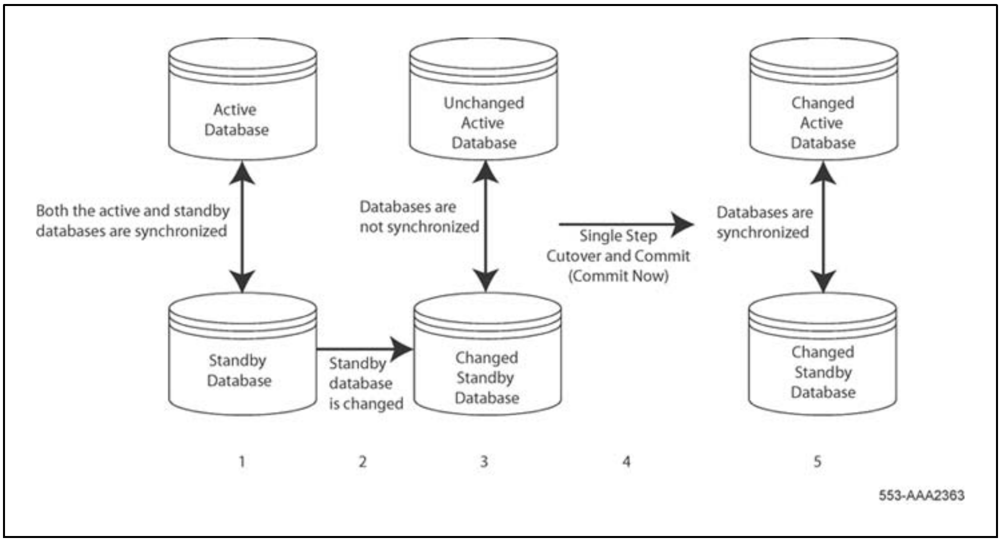

Active Database
Both the active and standby databases are synchronized
Standby Database
Standby database is changed
Unchanged Active Database
Databases are not synchronized
Changed Standby Database
Cutover
Unchanged Standby Database
Databases are not synchronized
Changed Active Database
Commit
Changed Standby Database
Databases are synchronized
Changed Active Database
1
2
3
4
5
6
7
553-AAA2362

Single-step Cut over and Commit

Figure 10 "NRS database actions - single-step Cut over and Commit" (page 45) shows both the active and standby database when a single-step **Cut over and Commit** database command is issued:

1. The active and standby databases are synchronized.
2. A change is made to the standby database.
3. The standby database is changed and the active database is unchanged. The databases are not synchronized.
4. The database single-step **Cut over and Commit** command is issued.
5. The databases are synchronized. Both databases are changed.

Figure 10
NRS database actions - single-step Cut over and Commit

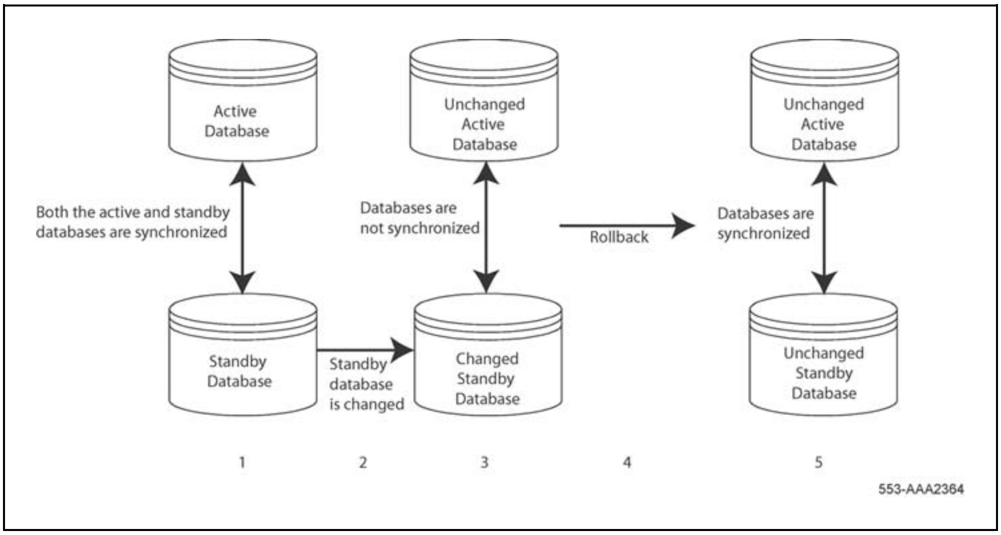

Active Database
Unchanged Active Database
Changed Active Database
Both the active and standby databases are synchronized
Databases are not synchronized
Single Step Cutover and Commit (Commit Now)
Databases are synchronized
Standby Database
Standby database is changed
Changed Standby Database
Changed Standby Database
1
2
3
4
5
553-AAA2363

Rollback

Figure 11 "NRS database actions - rollback" (page 46) shows both the active and standby database when a **Rollback** database command is issued:

1. The active and standby databases are synchronized.
2. A change is made to the standby database.
3. The standby database is changed and the active database is unchanged. The databases are not synchronized.
4. The database **Rollback** command is issued. (The administrator wants to undo the changes to the database.)
5. The databases are synchronized. Neither database is changed.

Figure 11
NRS database actions - rollback


Active Database
Both the active and standby databases are synchronized
Standby Database
Standby database is changed
Unchanged Active Database
Databases are not synchronized
Changed Standby Database
Rollback
Unchanged Active Database
Databases are synchronized
Unchanged Standby Database
1
2
3
4
5
553-AAA2364

To perform database actions using NRS Manager, refer to "Performing NRS database actions" (page 349).

Synchronization of the databases on the VxWorks-based Primary and Alternate Network Routing Servers.

The time interval between database synchronization of the Primary NRS and the Alternate NRS is a configurable parameter in the VxWorks-based NRS. The time interval between database synchronization of the Primary NRS and the Alternate NRS is in the range 1 to 24 hours.

> ***Note:*** The administrator can force a database synchronization through the CLI.

Synchronization of the databases on the Linux-based Primary and Secondary Network Routing Servers.

Synchronization of the Primary NRS database and the Secondary NRS database occurs in real-time in the Linux-based NRS.

NRS functionality

Contents

This section contains information on the following topics:

Introduction

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

The primary function of the NRS is to provide the following services:

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

> ***Note:*** The NRS can operate in stand-alone mode, without being connected to the Call Server.

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

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

Network overview

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

Coordinated endpoint configuration across multiple NRS zones

IP Peer Networking supports multiple SIP and H.323 zones. Separate NRS databases must be managed for each zone in a 1:1 relationship. Each NRS zone contains a Primary NRS, optionally an Alternate NRS, and multiple Gateway Endpoints or User Endpoints. The reasons for implementing multiple NRS zones are:

1. to scale up to very large networks with hundreds of registered endpoints
2. to divide a network of any size into convenient administration zones (for example, Western Europe and North America)

When a CS 1000 system places an IP call to another node, the originating Gateway signaling server sends a message to the NRS, specifying the destination telephone number. The NRS consults its internal numbering plan database and determines which node is the correct destination node.

SIP operation

The SIP Redirect Server allows SIP Trunk Gateways to communicate with other SIP Trunk Gateways across an enterprise. The SIP Trunk Gateway must keep information only about various lines and applications for which it is responsible, and it must have enough knowledge to contact the SIP Redirect Server. The SIP Redirect Server then redirects the SIP Trunk Gateway to where it needs to send its signaling.

A SIP Redirect Server receives requests but, rather than passing these requests onto another redirect server, it sends a response back to the originator of the request.

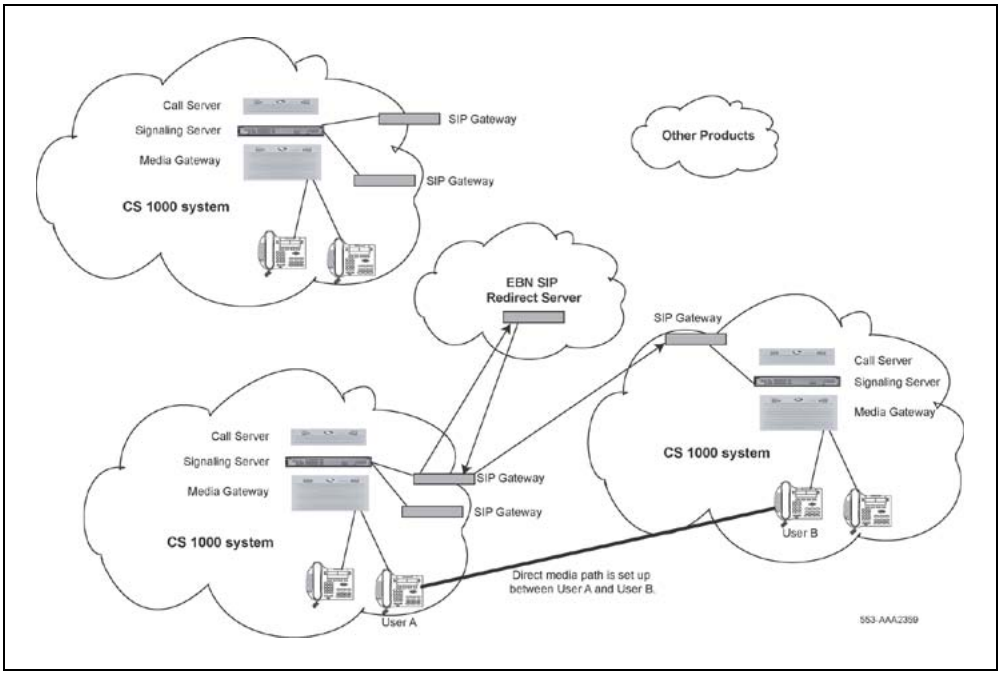
SIP Trunk Gateways, SIP Proxy Servers (for example, the MCS 5100), and SIP Phones forward calls to the contact address returned by the SIP Redirect Server. For instance, a SIP Trunk Gateway sends an INVITE message to the SIP Redirect Server. The SIP Redirect Server then sends a redirect message back to the originator with the addressing information for the destination node. The originator then sends an INVITE message directly to the SIP Trunk Gateway destination node.

For example, User A would like to contact User B across the enterprise network. The following sequence occurs:

- User A contacts its SIP Trunk Gateway. (That is, User A sends an address-resolution request to the SIP Trunk Gateway.)
- User A’s SIP Trunk Gateway contacts the EBN SIP Redirect Server.
- The EBN SIP Redirect Server executes a location look-up to see if its database contains an address match for the domain of User B.
- If a match is found, the SIP Redirect Server returns a response back to User A indicating the contact address required for User A to call the called party. (That is, the EBN SIP Redirect Server redirects User A’s SIP Trunk Gateway to User B’s SIP Trunk Gateway.)
- User A’s SIP Trunk Gateway uses the provided contact address and directly communicates with User B’s SIP Trunk Gateway.
- A direct media path is then set up between User A and User B.

Figure 12 "SIP Signaling and SIP Redirect Server" (page 50) shows how the SIP Redirect Server accepts a request from a SIP Trunk Gateway and sends the response back to the SIP Trunk Gateway. The SIP Trunk Gateway can then contact the called party’s SIP Trunk Gateway directly. Once the SIP Trunk Gateway contacts the called party’s SIP Trunk Gateway, a direct media path is set up between the caller and the called party.

Figure 12
SIP Signaling and SIP Redirect Server



If the SIP Redirect Server does not find any matching numbering plan entries, (a NULL entry is returned by the database), then the SIP Redirect Server transmits a SIP 404 (Not Found) response.

Similarly, if a request fails due to registration failure, a SIP 401 (Unauthorized) response is transmitted.

> ***Note:*** All redirect server logs use the existing RPT report log facility.

H.323 operation

An H.323 Gateway sends an ARQ message to the H.323 Gatekeeper. If a match is found for the called-party number digits in the ARQ, then the H.323 Gatekeeper sends an ACF message to the call originator and includes addressing information for the destination node.

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

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

If an H.323 Gatekeeper cannot resolve the destination address received in an incoming ARQ message, then it sends a LRQ message to other network zone H.323 Gatekeepers in order to resolve the number.

> ***Note:*** The H.323 Gatekeeper sending the LRQ message includes its own identification in the LRQ message and does not include the H323-ID of the gateway that sent the original ARQ message.

The peer H.323 Gatekeeper that resolves the number sends an LCF message with the destination Call Signaling address.

If an H.323 Gatekeeper cannot resolve the destination address in an incoming LRQ, it sends a Location Reject (LRJ) message to the originator of the LRQ message.

The behavior of the H.323 Gatekeeper (that sent the LRQ messages) depends on the responses from the remote H.323 Gatekeepers. When an LCF is received from a remote H.323 Gatekeeper, the local H.323 Gatekeeper immediately sends the ACF to the gateway at Node A. If an ARJ is received indicating "incomplete number", further digits are required. An immediate ARJ indicating the need for further digits is sent to Node A. Node A retries on receiving more digits. Otherwise, the local H.323 Gatekeeper waits until either all the remote Gateways have responded, or a timer expires indicating that one or more Gatekeepers could not reply. At this time, either an ARJ indicating call failure is returned, or an ACF indicating the default route is returned.

Incoming LRQ messages When an H.323 Gatekeeper receives an incoming LRQ message, it checks to see if the H.323 Gatekeeper that sent the request is configured in its database. The information received in the **sourceInfo** field is used for authentication.

Table 4
How the H.323 Gatekeeper authenticates incoming LRQ messages

If the H.323 Gatekeeper sending the LRQ is a...	Then its sourceInfo field contains...	And the H.323 Gatekeeper has to check...
CS 1000 Release 4.0 (or later) H.323 Gatekeeper or	the alias address of the peer H.323 Gatekeeper that sent the LRQ message	(not applicable)

If the H.323 Gatekeeper sending the LRQ is a...	Then its sourceInfo field contains...	And the H.323 Gatekeeper has to check...
Succession 3.0 H.323 Gatekeeper		
CS 1000 Release 2.0 H.323 Gatekeeper	the alias address of the H.323 Gateway	for the alias in the • network zone H.323 Gatekeeper list • endpoints list

If the information in the sourceInfo field cannot be authenticated, then the H.323 Gatekeeper rejects the incoming LRQ.

On receiving the incoming LRQ, the H.323 Gatekeeper parses the sourceInfo field. It searches for the source alias address as a URL ID type or an H323-ID type.

The H.323 Gatekeepers send the gatekeeper alias address along with the CDP domain information as a URL string. The format of the URL string is:

h323:gkH323ID;phone-context=cdpDomain

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

- gkH323ID
- cdpDomain

This URL string is parsed for incoming LRQs and is used to extract the H.323 Gatekeeper alias name and the CDP domain information.

- The H.323 Gatekeeper alias name is used for gatekeeper authentication.
- The CDP domain information is used to search in the same CDP domain if the destination info was private.level0 type of number.

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

Outgoing LRQ messages An H.323 Gatekeeper can be configured with a list of IP addresses of alternate H.323 Gatekeepers in different network zone. The H.323 Gatekeeper can then send LRQ requests in an attempt to resolve ARQ requests for which it cannot find registered matches in its own numbering plan database.

The configuration of H.323 Gatekeepers Collaborative Servers includes:

- an IP address
- an H.323 ID

- a CDP domain (Level 0 Domain)

See Procedure 93 "Adding a Collaborative Server" (page 337).

This information is used for incoming LRQs and is also used to determined the H.323 Gatekeepers in which to send outgoing LRQs. If a Network Zone H.323 Gatekeeper is configured with a CDP domain, then it is sent an LRQ only if the endpoint sending the ARQ is also in the same CDP domain. If an ARQ request arrives, and there is no matching numbering plan entry for the destination telephone number or there is a match but the matching entry (plus any alternates) is not currently registered, then the H.323 Gatekeeper sends an LRQ to all other H.323 Gatekeepers on the network whose IP addresses have been configured.

Each H.323 Gatekeeper is configured with an H.323 Gatekeeper alias name which is an H323-ID. The outgoing LRQ message contains the H.323 Gatekeeper alias name in the sourceInfo field instead of the H323-ID received in the incoming ARQ message.

NRS purpose

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

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

For more information about numbering plans and dialing plans, see "Numbering plans" (page 71).

H.323 Gatekeeper discovery

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

The message requesting the IP address of the H.323 Gatekeeper contains the endpoint alias and the RAS signaling transport address of the endpoint. This is so the H.323 Gatekeeper knows where to send return messages. The message from the endpoint to the H.323 Gatekeeper also contains vendor information. Thus, the H.323 Gatekeeper determines the specific product and version that is attempting discovery. The H.323 Gatekeeper only uses this information if the request for discovery is rejected.

Nortel recommends that endpoints use the endpoint Alias.h323-ID alias types.

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

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

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

H.323 Endpoint registration

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

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

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

> ***Note 1:*** IP Trunk 3.0 (or later) nodes always register multiple IP addresses due to the load-balancing architecture of the IP Trunk 3.0 (or later) nodes. The first IP address in the registration request is the node IP address and the remaining IP addresses are the IP addresses of the individual trunk cards in the node. When a call terminates on an IP Trunk 3.0 (or later) node, the Gatekeeper returns only the node IP address. The Gatekeeper knows that the endpoint is an IP Trunk 3.0 (or later) node, as its vendor information is provided in the request for registration message.
>
> ***Note 2:*** IP Trunk 3.0 (or later) nodes use multiple IP addresses when sending admission requests to the Gatekeeper. The card that is the RTP endpoint for the call uses its own IP address for the ARQ. However, to ensure that the node can carry out load-balancing, the node "Leader" IP address is sent to the Gatekeeper in the registration request; no other IP addresses are provided, to allow the IP Trunk node to control load balancing.
>
> The Gatekeeper knows that the IP Trunk 3.0 (or later) IP address used in the ARQ belongs to the node, since the Gatekeeper provides an endpoint identifier in the registration sequence, and this is included in all ARQs.

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

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

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

Time-to-Live

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

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

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

Configure the Time-to-Live timer using NRS Manager. Nortel recommends that the timer be configured to 30 seconds. Refer to Procedure 78 "Configuring system-wide settings" (page 300).

Multiple registration requests

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

Registration requests when the NRS is out-of-service

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

Unregistration

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

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

SIP registration

The SIP Registrar accepts REGISTER requests. A request is a SIP message sent from a client to a server to invoke a particular operation.

> ***Note:*** A response is a SIP message sent from a server to a client to indicate the status of a request sent from the client to the server.

Registration entails sending a REGISTER request to the SIP Registrar. The SIP Registrar acts as the front end to the location service (database) for a domain, reading and writing mappings based on the contents of REGISTER requests. This location service is then typically consulted by a SIP Redirect or Proxy Server that is responsible for routing requests for that domain.

The SIP Registrar places the information it receives (in the requests) into the location service for the domain it handles. The location service is used by the SIP Redirect and Proxy Servers to locate the SIP Trunk Gateway that serves the target of the request. A SIP Trunk Gateway has a number of non-SIP lines and trunks behind it which do not have their own identity in the SIP domain. These non-SIP endpoints are accessed by mapping SIP URIs based on telephony DNs to one or more SIP Trunk Gateways. The location service is a matching mechanism that allows a fully-qualified telephone number to be associated with a range of telephone numbers and the SIP Trunk Gateway that provides access to that DN range.

SIP endpoints are also known as User Agents. User Agents have two functions:

- act as User Agent Clients — initiate request
- act as User Agent Servers — process requests and generate responses to the requests

The SIP Registrar is a special type of User Agent Server.

The REGISTER request

A REGISTER request is used for registering contact information. The REGISTER request is used by SIP clients to notify a SIP network of its current IP address and the URLs for which it would like to receive a call. This SIP mechanism is used by called parties to register in order to receive incoming calls from proxies that serve that domain.

Dynamic registration

Dynamic registration facilitates the creation of a contact list for the authorized SIP Trunk Gateway Endpoints and SIP Phones (SIP User Endpoints).

Dynamic registration of SIP Trunk Gateway Endpoints SIP Trunk Gateway dynamic registration facilitates the creation of the contact list for the authorized Gateway endpoints. The gateways dynamically register their IP address with the SIP Redirect/Proxy Server (that is, with the SIP Registrar component). This eliminates some manual provisioning at the SIP Redirect Server. It also reduces the potential for error when manually entering the IP address of the SIP Trunk Gateway in the SIP Redirect Server.

Dynamic registration of SIP Phones (SIP User Endpoints) SIP Phone dynamic registration facilitates the creation of the contact list for the authorized SIP Phones. For more information about SIP Phone registration, refer to SIP Phone dynamic registration.

Database synchronization Database synchronization treats dynamically registered data the same way as the H.323 Gatekeeper:

- If the Alternate NRS database takes over, then registrations are lost.
- If the Failsafe NRS database takes over, then registrations are kept.

NRS Manager

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

You can perform the following NRS configuration functions using NRS Manager:

- configure a numbering plan
- add, modify, or delete preconfigured endpoint data
- add, modify, or delete numbering plan entries on a per-endpoint basis
- retrieve the current configuration database
- interwork with a preconfigured database

- revert to the standby database
- change system passwords

Security

NRS Manager is password-protected.

The NRS has two access levels:

- Administrator level
- Monitor level

Refer to *Security Management (NN43001-604)*, for detailed information on CS 1000 system security including protection of signaling and the media stream from privacy intrusions or disruption, and the administration and use of secure remote access.

Administrator access

A user with administration-level access can view and modify the NRS. Administrator-level access is the highest authority level. An administrator has the authority to manage the entire NRS.

The administrator has the ability to view, create, and modify the login names and passwords that are used for configuration and maintenance.

If you log in to NRS Manager as an administrator, you have full administrative access. You can update all configuration entries, and you have full write access to the database, including the ability to change all NRS passwords.

The NRS administrator username and password are used only when accessing NRS Manager. Changing the NRS administrator username and password does not change the username and password for the Signaling Server shell.

> **ATTENTION**
>
> **IMPORTANT!**
>
> Nortel recommends that default usernames and passwords be changed for increased network security.

Changing username and passwords The usernames and passwords used to access the NRS can be changed under the Administration tab in NRS Manager. See "Configuring and administering users" (page 373).

All user login names and passwords are recorded in the NRS database. The passwords are stored in an encrypted format.

Monitor access

A user with monitor-level access can only view existing NRS configuration data. The user cannot modify any NRS configurations or settings. A user with monitor access can only change their own password.

NRS Manager blocks certain navigation operations for monitor-access level users. If a user is a monitor-level user, then NRS Manager does not allow the user to change NRS provisioning operations.

If you log in to the NRS as a monitor, you can:

- view configuration data
- execute H.323 and SIP routing tests
- review reports

Note: CS 1000 Element Manager includes performance and traffic monitoring functions.

NRS operating parameters

The NRS can co-reside on the Signaling Server with other applications (co-resident mode). For large networks, if the Signaling Server does not have enough capacity to support the NRS functionality in conjunction with other applications, a dedicated Signaling Server can be required for the NRS (stand-alone mode). The NRS (Primary, Alternate, or Failsafe) cannot reside on an Alternate Signaling Server. It has to be on a Primary (Leader) Signaling Server.

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

The NRS can use prefix routing as long as the prefix is qualified. That is, you do not need 1-613-969-7944; 1-613-969 may be enough.

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

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

H.323 endpoints which register using RAS messages must provide an H323-ID or a similar alias (for example, URL-ID or e-mail ID).

The NRS supports only direct-routed call signaling and RAS messaging for call control.

- All H.323 endpoints registered with the H.323 Gatekeeper must use the ARQ mechanism and must consult with the H.323 Gatekeeper for admission and address translation. The H.323 Gatekeeper does not pre-grant an ARQ for the call originator, but does pre-grant for the call terminator. This is because the H.323 Gatekeeper does not track call state, and has no easy way of correlating the ARQ between call originators and terminators.
- All SIP endpoints registered with the SIP Redirect Server must use the SIP INVITE message.

All H.225/Q.931 call-signaling messages and all H.245 call-control messages are not directed to the NRS and are passed directly between endpoints. This approach enables the NRS to be more scalable and to handle a larger number of simultaneous calls.

Each NRS supports up to 100 000 calls per hour.

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

The NRS (H.323 Gatekeeper only) supports Overlap Sending according to H.323; however, allowable configuration items on the H.323 Gatekeeper must be taken into consideration. For more information about overlap signaling, refer to *IP Peer Networking Installation and Commissioning (NN43001-313)* .

The NRS (stand-alone mode only) generates SNMP traps and sends them to a configured SNMP host. The NRS uses the SNMP services provided by the Signaling Server platform.

The NRS supports IP multicast for discovery and location-request messages.

> ***Note:*** NRS/H.323 Gatekeeper Discovery using the Multicast approach is not recommended over large networks, because all routers between the endpoint requesting NRS discovery and the NRS must support Internet Group Management Protocol (IGMP).

The NRS supports multiple customers. Multiple customers can be configured with each customer having their own unique dialing or numbering plan.

The NRS does not track the state of active calls, keep count of the total number of active calls, or generate Call Detail Recording (CDR) records. Therefore, all Disengage Request (DRQ) messages are automatically confirmed. The NRS does not have traffic management capabilities, such as maximum calls allowed for each endpoint or maximum bandwidth allowed for each endpoint or zone.

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

Zone management on the Call Server provides an alternate mechanism for routing 911 calls, based on the branch office or SRG zone. For more information, refer to *Branch Office Installation and Commissioning (NN43001-314)*.

The NRS, like all CS 1000 components, does not support the H.235 security protocol.

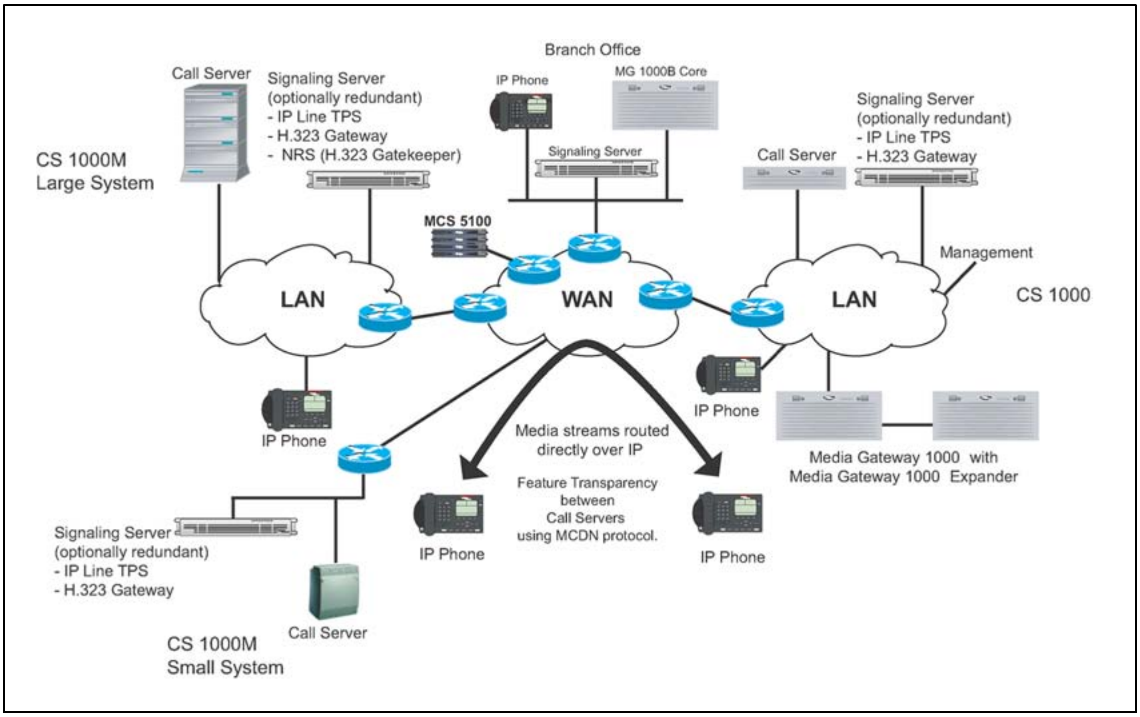
All number and cost factor pairs within a numbering plan table are unique for private numbering plans. When adding an H.323 alias for a predefined H.323 endpoint, the request is rejected if the administrator specifies an alias type and provides a number string and cost factor that is already in the numbering plan table for that alias type.

For example, Figure 13 "Example of all call routing plans" (page 63) illustrates the configuration of a CS 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 13
Example of all call routing plans



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

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

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

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

If an alias is added whose left most 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" (page 65).

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

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

Leading digit ranges can be overridden by configuring more precise numbering plan entries or numbers with a greater number of leading digits. For example, a privateNumber.level1RegionalNumber of 6651200# takes precedence over an entry of 665-669.

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

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

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

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

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

No special configuration items are present for ESN5 or Carrier Access Code support. If the Signaling Server is unable to provide a fully-qualified number in ARQ to the H.323 Gatekeeper and the number is prefixed with ESN5 prefix 100, then this prefix is placed before the existing entry in the numbering plan table.

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

Example generated tables

The configuration shown in Figure 13 "Example of all call routing plans" (page 63) would result in Table 5 "privateNumber.level1RegionalNumber numbering plan" (page 65) through Table 12 "Endpoint Status Table" (page 67).

Table 5
privateNumber.level1RegionalNumber numbering plan

	Terminating Routes			
Digits	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 6
privateNumber.pISNSpecificNumber numbering plan

Digits	Terminating Routes	
	H323-ID	Cost Factor
265	SCN_MPK_2	1

Table 7
publicNumber.internationalNumber numbering plan

	Terminating Routes					
Digits	H323-ID	Cost Fact or	H323-ID	Cost Fact or	H323-ID	Cost Fact or
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		

	Terminating Routes					
Digits	H323-ID	Cost Factor	H323-ID	Cost Factor	H323-ID	Cost Factor
352	47.102.7.49	1				
35391	ITG_GAL_1	1	47.102.7.49	2	SCN_MPK_1	3

Table 8
CDP domain table

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

Table 9
CDP_DOMAIN_2 numbering plan

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

Table 10
MPK_CDP_DOMAIN numbering plan

	Terminating Routes	
Digits	H323-ID	Cost Factor
40-43	SCN_MPK_1	1

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

Table 11
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 12
Endpoint Status Table

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

Stand-alone NRS support for Meridian 1 and BCM nodes

Nortel supports the use of an NRS for Meridian 1 Release 25.40 and Business Communications Manager (BCM) 3.6 nodes using H.323 endpoints that use IP Trunk 3.0 (or later).

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

To illustrate how the NRS fits into a Meridian 1/BCM network using IP Trunks, it is useful to first look at how the Meridian1/BCM handles call admission control and numbering plan resolution.

Meridian 1/BCM node-based numbering plan

Figure 14 "Meridian 1/BCM node-based numbering plan" (page 68) illustrates how the Meridian1/BCM handles call admission control and numbering plan resolution.

Figure 14
Meridian 1/BCM node-based numbering plan

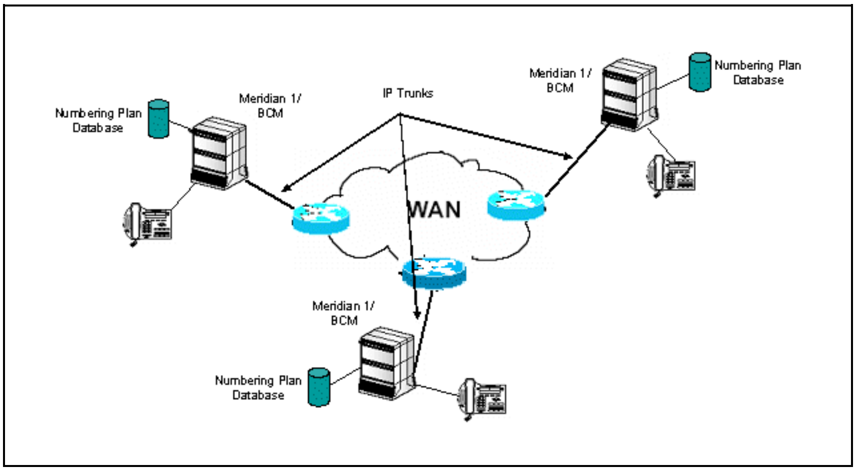


Figure 14 "Meridian 1/BCM node-based numbering plan" (page 68) shows a Meridian 1/BCM network with the Meridian 1/BCM nodes equipped with IP Trunks. The IP Trunk routes are point-to-multipoint. Regardless of where the terminating node is located, all calls can be sent out over the same route. The calls can be routed to the correct destination over the packet-based IP network by the IP Trunk.

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

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

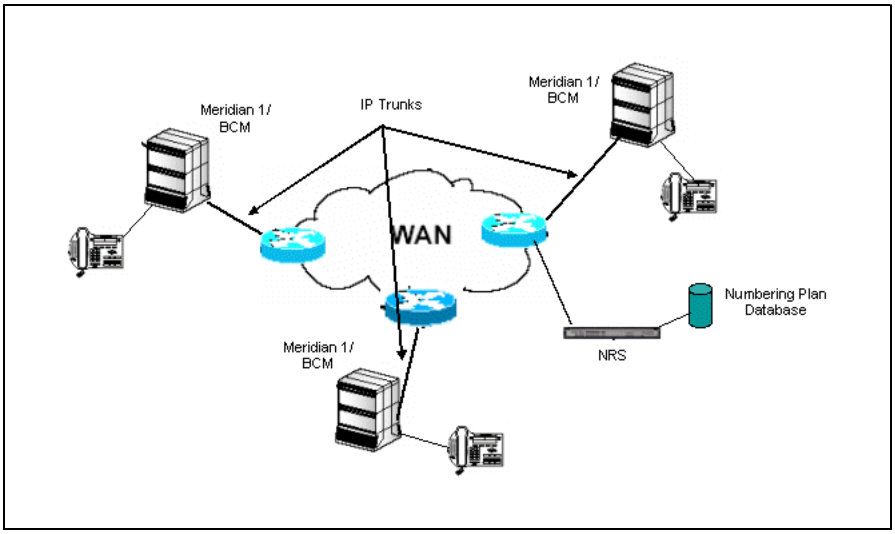
When the Meridian 1/BCM wishes to make an IP Trunk call, the following occurs:

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

NRS-based numbering plan

In a Meridian 1/BCM network running IP Trunks and a stand-alone NRS, the network numbering plan is centrally administered by the NRS, as shown in Figure 15 "NRS-based numbering plan" (page 69).

Figure 15
NRS-based numbering plan



The NRS is configured with numbering plan information for every Meridian 1/BCM node in the network zone.

The typical Meridian 1/BCM network is configured to use H.323 Gatekeeper Resolved signaling. With H.323 Gatekeeper Resolved signaling, the H.323 Gatekeeper provides address resolution; however, call setup is performed directly between the nodes.

When a node wishes to place an IP call to another IP Trunk-enabled node, the originating node looks at its internal dialing plan table for address translation. If the originating node cannot find a match, it then sends ARQ (Admission Request) to the H.323 Gatekeeper specifying the destination phone number. When configured to use H.323 Gatekeeper, the node automatically sends the ARQ to the H.323 Gatekeeper. The H.323 Gatekeeper consults its internal numbering plan database and determines which Meridian 1/BCM node is the correct destination node. The H.323 Gatekeeper then sends an Admission Confirm (ACF) to the call originator and includes addressing information for the destination node. Standard call setup is then performed between the two nodes.

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

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

In order to eliminate a single point of failure in their network, Nortel recommends the deployment of both a Primary and an Alternate NRS.

Numbering plans

Contents

This section contains information on the following topics:

Introduction

When configuring a CS 1000 network, several numbering plans can be used. The numbering plan depends on customer preferences for dialing and configuration management requirements.

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

"Numbering plan entry overview" (page 81) describes the implementation of the numbering plans. The sections below describe the following types according to their use:

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

Private (on-net) numbering plans

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

Uniform Dialing Plan

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

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

For example, if:

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

The user dials: 6 343 2222

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

For more information on UDP, refer to *Basic Network Features (NN43001-579)*.

For call routing information, see "UDP call-routing operation" (page 89).

Coordinated Dialing Plan

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

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

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

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

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

> ***Note:*** If a user moves from one Call Server to another, the user's DN must change in the CDP numbering plan (see "Transferable Directory Number" (page 74)).

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 (NN43001-283)*.

For call routing, see "CDP call routing operation" (page 87).

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 (NN43001-283)*.

Transferable Directory Number

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

For call routing information, see "Transferable DN call routing operation" (page 86).

Vacant Number Routing

Vacant Number Routing (VNR) is supported in order to keep the Transferable Numbering Plan at a manageable level. As a result, small sites, such as the branch office, require minimal configuration to route calls through other Call Servers or through the NRS. Instead of changing the numbering trees and steering codes at each location, all the routing information can be kept at one central location.

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

Vacant Number Routing must be configured on the Media Gateway 1000B (MG 1000B) Core Small System Controller (SSC). Refer to *Branch Office Installation and Commissioning (NN43001-314)* for more information.

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

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

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

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

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

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" (page 89).

North American Numbering Plan

The Call Server supports North American Numbering Plan routing. The North American Numbering Plan is used to make North American public network calls through the private network. The North American Numbering

Plan accommodates dialing plans based on a fixed number of digits. A user can dial AC1 or AC2 + NXX + XXXX for local calls or AC1 or AC2 + 1 + NPA + NXX + XXXX for toll calls.

For example, if:

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

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

Flexible Numbering Plan

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

For example, if:

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

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

For information on FNP operation and package dependencies, refer to *Dialing Plans: Description (NN43001-283)*.

Special Numbering Plan

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

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

Address translation and call routing

H.323

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

> ***Note:*** Endpoints that do not support RAS messaging do not register with the H.323 Gatekeeper.

SIP

When a SIP-compliant entity on the network wants to place a call, it sends an INVITE message to the SIP Redirect Server by way of the SIP Trunk Gateway. The endpoint includes the destination telephony number in this message. The destination information is a SIP URI (see "SIP Uniform Resource Identifiers" (page 38)). The SIP Redirect Server searches its numbering plan database to determine which endpoints on the network can terminate the telephone number and whether or not these endpoints are registered. Address lookup is based on the digits, phone context, and domain name.

The SIP Redirect Server returns the IP address of any endpoints that can terminate this number and that are registered to the endpoint.

Basic call routing

The routing of calls within the CS 1000 networks depends on the type of numbering plan in use and the number dialed. "Transferable DN call routing operation" (page 86) 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" (page 72) and "Public (off-net) numbering plans" (page 75) are described in "Numbering plans and routing" (page 84).

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

Supported alias types (for H.323)

The H.323 Gatekeeper performs address translations on H.323 partyNumber alias types and on E.164 alias types. The partyNumber alias can be one of several subtypes according to the H.323 standard. The only partyNumber subtypes that the H.323 Gatekeeper supports are partyNumber.publicNumber and partyNumber.privateNumber. These also have subtypes. See Table 13 "H.323 term explanations" (page 78).

Table 13
H.323 term explanations

H.323 signaling protocol	CS 1000 term
publicNumber.internationalNumber (Note 1)	E.164 International (UDP)
publicNumber.nationalNumber (Note 1)	E.164 National (UDP)
publicNumber.subscriber	See Note 2.
publicNumber.unknown	See Note 3.
privateNumber.level1RegionalNumber (Note 1)	Uniform Dialing Plan Location Code (UDP LOC)
privateNumber.pISNSpecificNumber (Note 1)	Special Numbers (SPN)
privateNumber.localNumber (Note 1)	Coordinated Dialing Plan (CDP)
privateNumber.unknown	Unknown (UKWN) (Note 4)
e164	See Note 5.
Note: 1. Only these alias types can be entered as numbering plan table entries using the web browser interface. The other alias types have no Type Of Number (TON) information.	
Note: 2. Not supported by the H.323 Gatekeeper. The Call Server algorithmically converts any public subscriber number to a supported type (for example, converts a publicNumber.internationalNumber by adding the country code and area code).	
Note: 3. Not supported by the Call Server, but is supported by the H.323 Gatekeeper for third-party interoperability. This is treated as a publicNumber.internationalNumber.	
Note: 4. Not supported by the Call Server, but is supported by the NRS for third-party interoperability. The Call Server can generate privateNumber.unknown types with the limitation that INAC does not work. The NRS attempts to convert the number to privateNumber.localNumber (that is, CDP) or privateNumber.level1RegionalNumber (that is, UDP LOC) by analyzing the digits. If the NRS cannot determine which type to use based on digit analysis, it assumes that privateNumber.localNumber (that is, CDP) should be used.	
Note: 5. Not supported by the Call Server, but is supported by the NRS for third-party interoperability. A default prefix can be configured on a per-NRS basis to distinguish between public and private numbers. For example, a prefix of "9" can be configured as the public number prefix. A prefix of "6" can be configured as the private default prefix. The NRS looks at the first digit. If it matches the public prefix (for example, "9"), it treats the subsequent digits as a publicNumber.internationalNumber. If the first digit matches the private prefix (for example, "6"), it treats the subsequent digits as a privateNumber.localNumber (that is, CDP) or privateNumber.level1RegionalNumber (that is, UDP LOC), depending on its digit examination.	

If the H.323 Gatekeeper receives an admission-request message requesting translation for any other alias type (for example, publicNumber.subscriberNumber), it rejects the request.

The H.323 Proxy Server, which sends the admission request to the H.323 Gatekeeper, is responsible for mapping Numbering Plan Indicator (NPI)/Type of Number (TON) values in the ISDN SETUP Called Party Number Information Element to one of the eight H.323 alias types listed in Table 13 "H.323 term explanations" (page 78).

Mapping between CS 1000 NPI/TON and H.323 alias types The CS 1000 system supports the NPI and TON values shown in Table 14 "NPI values" (page 79) and Table 15 "TON values" (page 79). These values are for Universal ISDN Protocol Engine (UIPE)-formatted NPI/TON numbers.

Table 14
NPI values

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

Table 15
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 H.323 Gatekeeper sees a trunk steering code as privateNumber.unknown. The H.323 Gatekeeper then converts the code to privateNumber.localNumber in CDP.	

Table 16 "NPI/TON to H.323 alias mapping" (page 80) shows the NPI/TON pairs, the corresponding call types, and their corresponding H.323 alias types for which the H.323 Gatekeeper accepts translation requests. The call type for outgoing routes is manipulated by configuring a DMI in LD 86 and specifying the Call Type (CTYP).

If the H.323 Proxy Server receives a Q.931 SETUP message for an NPI/TON pair not included in Table 16 "NPI/TON to H.323 alias mapping" (page 80), it must map the number according to one of the NPI/TON pairs/H.323 alias types which the H.323 Gatekeeper supports. This process can require modifications to the called number dialing string.

CTYP is the mnemonic in the ESN overlays.

Table 16
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 15 "TON values" (page 79))	LOC	privateNumber.level1RegionalNumber
	COORDINATED (see Table 15 "TON values" (page 79))	CDP	privateNumber.localNumber
	UNKNOWN	UKWN	privateNumber.unknown

The endpoints must correctly map the UIPE NPI/TON pairs to a valid partyNumber type that the H.323 Gatekeeper supports. The administrator must coordinate the numbering plan on the H.323 Gatekeeper with the mapping carried out by the endpoints.

LD 96 shows NPI/TON and ESN call types for D-channel monitoring. Calling and Called number information for level 0 D-channel tracing includes the TON and ESN call types.

Table 17 "Q.931 TON mapping" (page 81) shows Q.931 TON mapping.

Table 17
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 18 "NPI/TON to ESN Call type mapping" (page 81) shows the NPI/TON to ESN Call type mapping.

Table 18
NPI/TON to ESN Call type mapping

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

Numbering plan entry overview

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

When configuring a predefined endpoint on the NRS, the administrator must add the required numbering plan entries. The administrator adds the numbers or number ranges that the endpoint can terminate. For every numbering plan entry, the administrator must specify the DN type, the default route, the DN prefix, and the cost factor associated with the route. See "Adding a Routing Entry" (page 327).

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

- 1613
- 161396
- 1613967

If a user dials "1613966", the NRS matches entries with "161396". See Table 19 "Cost factors" (page 82) for the cost factors associated with these entries.

Table 19
Cost factors

Entry	Cost factor
1613	1
161396	1
161396	2
1613967	1

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

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

Default endpoints can also be configured for each of the supported numbering plan types. These entries are configured by entering the DN type, the default route, the DN prefix, and their associated cost factors.

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

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

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

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

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

The NRS has a table for each of the standard alias types (internationalNumber.pISNSpecificNumber and level1RegionalNumber) which provides the default routes associated with each type. The tables contain the H323-ID of the default routes or the IP address if the default route does not support RAS procedures and the cost factor associated with the route. There is also a table of default routes for each CDP domain.

Number Type support

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

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

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

Note that the numbering plan entries in the NRS conform strictly to the E.164 International standard. Calls on Virtual Trunks that access the NRS must be tagged correctly.

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

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

Numbering plans and routing

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

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

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

Refer to *Dialing Plans: Description (NN43001-283)* for information on VNR operation.

Using an NRS for routing

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

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

The basic role of a SIP Redirect Server is to perform address translation from a SIP URI to an IP signaling address and to authorize the call in the SIP network.

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

"Santa Clara-01"
PublicNumber = +1 408 XXX XXXX
PrivateNumber = Electronic Switched Network (ESN) 265 XXXX, ESN 655 XXXX

At power-up, an H.323 endpoint performs Gatekeeper Discovery using a configured H.323 Gatekeeper address. The endpoint then registers with its primary H.323 Gatekeeper at the address returned by the Gatekeeper Discovery process using the H.225.0 (RAS) protocol by sending its H323-ID and its IP address. In the example above, it would use the following:

"Santa_Clara-01"
Signaling IP address = 47.0.1.2

Upon receipt of the registration, the H.323 Gatekeeper matches the name "Santa_Clara-01" in the registration with the configured information in its database, and adds the IP address.

When a user behind an H.323 proxy wants to reach another user, its H.323 proxy sends a call request to its H.323 Gatekeeper. The H.323 Gatekeeper determines any endpoint(s) that are responsible for that particular user and returns its signaling IP address(es) in the direct-routed model, which is the preferred model.

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

Transferable DN call routing operation

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

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

Figure 16 "Transferable DN routing" (page 87) shows a network of CS 1000 Systems in which each user wants to retain their unique seven-digit Directory Number. Table 20 "DNs with their associated Call Servers" (page 87) provides a summary of the DNs in Figure 16 "Transferable DN routing" (page 87), as well as their associated Call Server.

Each user in the network is associated with a Call Server and its group of SIP Trunk and/or H.323 Gateways. The Gateways provide call-processing features and redundancy. The NRS in Figure 16 "Transferable DN routing" (page 87) is aware of the location of any user with a given Directory Number within the network. In this case, the user with Directory Number 22221 is located at Call Server A. When a user dials the last digit of this number, their Call Server determines whether the user is within its local database, and if so, handles the call directly.

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

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

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

Figure 16
Transferable DN routing

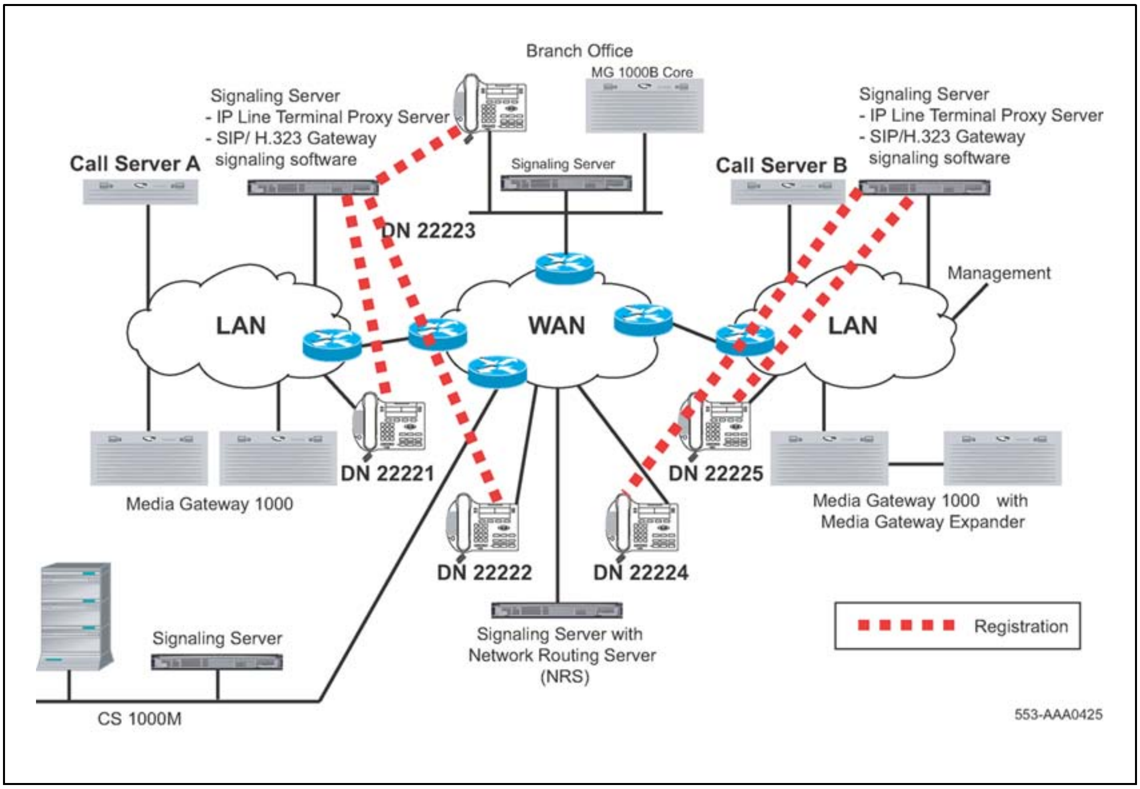


Table 20
DNs with their associated Call Servers

DN	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 NRS, because entire ranges of DNs are located within the same Call Server.
- With CDP, Call Servers and MG 1000B platform systems can be grouped into CDP domains, all sharing a CDP. This enables more convenient number dialing within a complex, such as a campus with several Call

Servers. When configuring CDP numbers at the NRS, administrators must also specify to which CDP domain they belong.

Figure 17 "CDP call routing" (page 88) shows an example of CDP routing. Table 21 "DNs with their associated Call Servers and CDP domains" (page 88) shows the DNs with their associated Call Servers and CDP domains.

Figure 17
CDP call routing

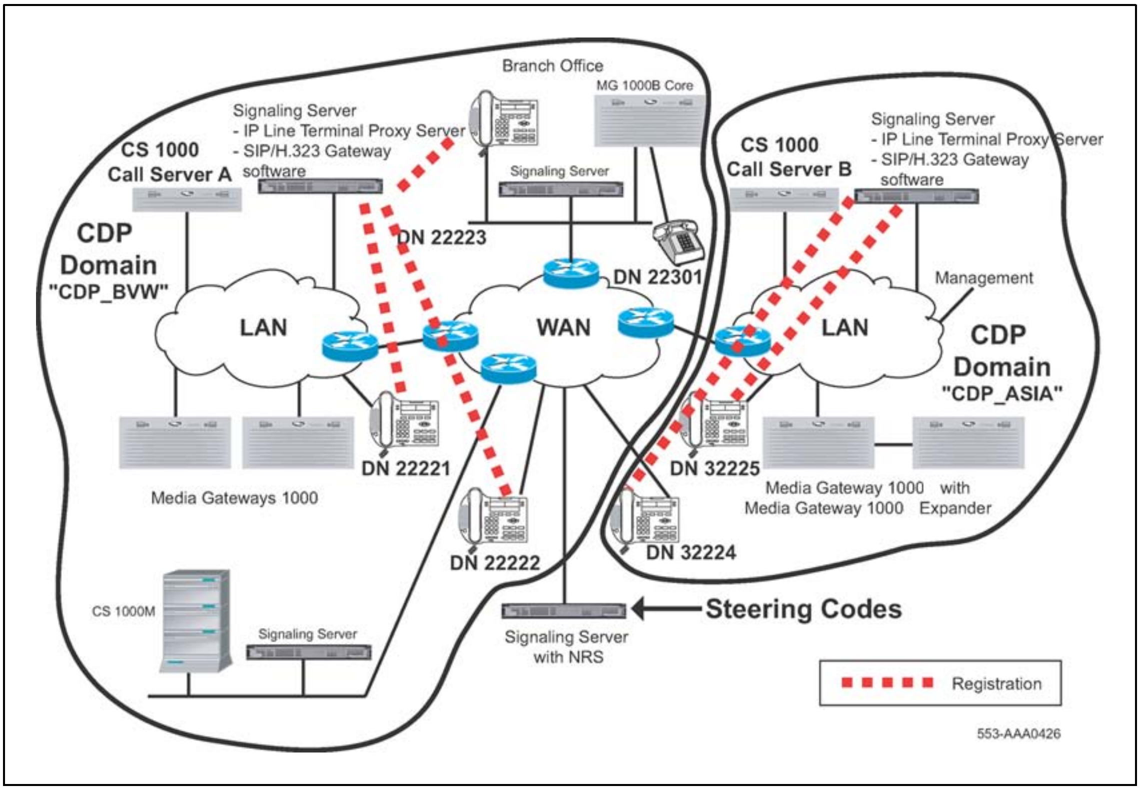


Table 21
DNs with their associated Call Servers and CDP domains

DN	Call Server	CDP domain
22221	A	"CDP_BVW"
22222	A	"CDP_BVW"
22223	A	"CDP_BVW"
22301	MG 1000B	"CDP_BVW"
32224	B	"CDP_ASIA"
32225	B	"CDP_ASIA"

UDP call-routing operation

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

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

> ***Note:*** Transferable Directory Numbers are considered CDP numbers.

Off-net call routing operation

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

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

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

Routing to and from a branch office or SRG

Because IP Phone users can be located at a branch office equipped with an MG 1000B Core or SRG, the routing of calls to the local gateway is important (especially when toll charges are applicable to calls made from the central Call Server that is controlling the telephone). The administrator can configure digit manipulation for IP Phones that are located near an MG 1000B Core or SRG, selecting a gateway that provides PSTN access local to the telephone.

> ***Note:*** The Branch Office feature (which includes the SRG) supports the various PSTN interfaces. Refer to *Electronic Switched Network:*

Signaling and Transmission Guidelines (NN43001-280) for further information.

Calls from the PSTN to users within the network can be routed either using the various ESN numbering plan configurations or using the Vacant Number Routing (VNR) feature. This process enables small sites, such as those using the MG 1000B Core, to require minimal configuration to route calls through other Call Servers or through the NRS.

Outgoing calls to access local PSTN resources can be routed using ESN, as well as zone parameters that enable digit insertion. The zone parameters enable calls made by a branch office or SRG user to be routed to the desired local PSTN facilities. Refer to *Branch Office Installation and Commissioning (NN43001-314)* for further information.

SIP Phone support

Contents

This section contains information on the following topics:

Introduction

Certified compatible third-party industry-standard SIP Phones are supported.

SIP Phones are configured on, and register to the NRS (specifically, the SIP Redirect Server), where they are configured as SIP user endpoints. As such, they communicate directly with the SIP Redirect Server, SIP Trunk Gateways, and other SIP Phones on the system. In contrast, IP Phones are configured on, and are controlled by, the Call Server.

IP Phones use the Unified Networks IP Stimulus Protocol (UNIStim) and are stimulus-based telephones. The features on an IP Phone are delivered by the Communication Server. SIP Phones use the Session Initiation Protocol which is an open industry standard-based signaling protocol. Some of the telephony features of the SIP Phones are delivered by the Communication Server. However, SIP Phones can have additional features that are available on the telephone itself. These features vary based on manufacturer and the model of the telephone.

A SIP Phone is a standards-based SIP device.

> ***Note:*** CS 1000 does not support Call Forward across NRS Collaborative Servers by third-party SIP Phones.

SIP Phone interaction

Table 22 "SIP Phone and CS 1000 component interaction" (page 92) shows the interaction between SIP Phones and components in the CS 1000 network.

Table 22
SIP Phone and CS 1000 component interaction

Component	Description
SIP Phone	SIP Phones are intelligent telephones which deliver many common business telephony features (for example, CLID, Conference, Transfer, MWI, and Name Display). See "SIP Phone features" (page 93) for more details. SIP Phones can also have other manufacturer-dependant features.
SIP Redirect Server	The NRS, specifically the SIP Redirect Server, provides the following: • a web-based interface (NRS Manager) for provisioning SIP Phones • registration and authentication for SIP Phones • routing definitions for all SIP traffic (including SIP Phones)
SIP Trunk Gateway	The SIP Trunk Gateway provides the following: • a signaling gateway for all SIP calls originating from and terminating to the CS 1000 system • standard SIP support for CLID, MWI, Name Display, and Call Redirection

Component	Description
CS 1000 Call Server	The Call Server provides call processing software which enables the following: • CDR using the tandem CDR feature • Trunk Access Restrictions using Class of Service (CLS) and Trunk Group Access Restrictions (TGAR) • SIP Access Port Licenses
TDM telephones and IP Phones, IP Trunk, and CallPilot	SIP Phones can interwork with the full suite of CS 1000 TDM and IP endpoints. CallPilot provides Unified Messaging for SIP Phones, including MWI.

SIP Phone features

The following is a list of features delivered through the CS 1000 system:

- Calling Line Identification (CLID)
- Network Call Party Name display
- Network Call Redirection
- Message Waiting Indication
- Network Class of Service Access controls
- Network Alternate Route Selection (NARS, UDP, CDP)
- Call Detail Recording (CDR) using Tandem CDR features

The following is a list of intelligent SIP Phone-based features supported by the CS 1000 system. The features are dependant on the SIP Phone.

- Conference calling
- Call hold
- Call waiting
- Call forwarding
- Call transfer
- Caller ID
- Call waiting caller ID

The following features are available through the user interface in a web server-based configuration:

- Speed dial from phone book
- Call logs

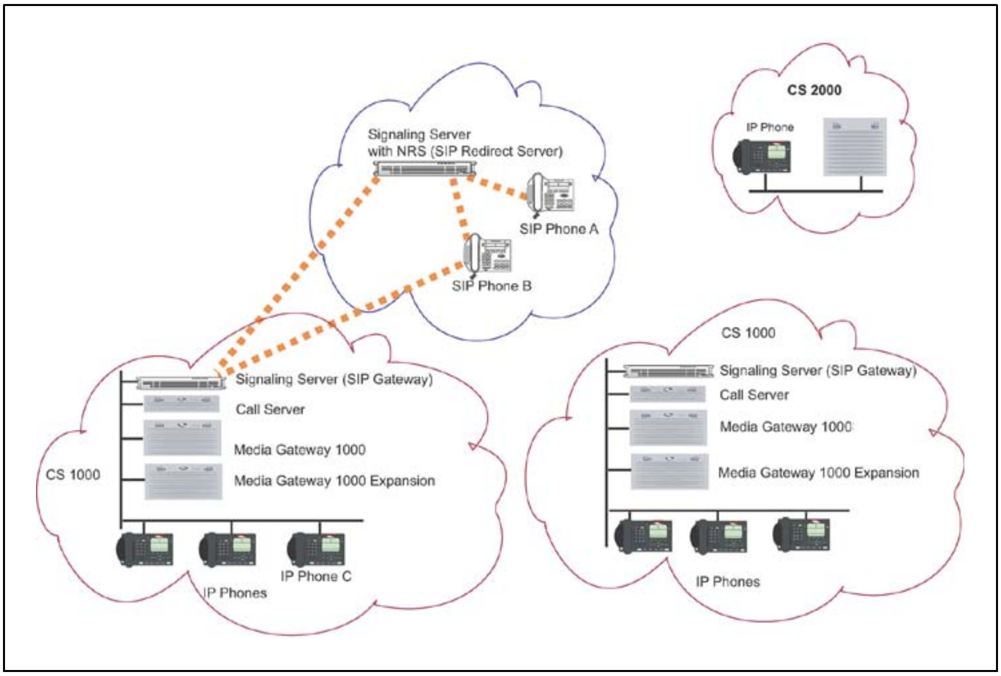
SIP-compliant telephones can interoperate with voice, data, video, and Internet applications and services that are SIP-enabled or provide full SIP support.

SIP Phones are configured on the Signaling Server using NRS Manager. See "Configuring a SIP Phone" (page 104).

SIP Phone calls

Figure 18 "SIP Phones and SIP Trunk Gateways in the network" (page 94) shows SIP Phone-to-SIP Phone connectivity and SIP Phone-to-SIP Trunk Gateway connectivity.

Figure 18
SIP Phones and SIP Trunk Gateways in the network



When two SIP Phones (SIP Phones A and B) want to communicate with each other, the originating SIP Phone must communicate directly with the SIP Redirect Server for authentication and address resolution. Then communication is established between the two SIP Phones. Refer to "SIP Phone-to-SIP Phone communication" (page 95) for the call flow between two SIP Phones in the same network.

When a SIP Phone (A) wants to communicate with another non-SIP telephone (for example, IP Phone C), then the SIP Trunk Gateway is involved. Refer to "SIP Trunk Gateway-to-SIP Phone communication" (page 98) for the call flow between a SIP Phone and another telephone using the SIP Trunk Gateway.

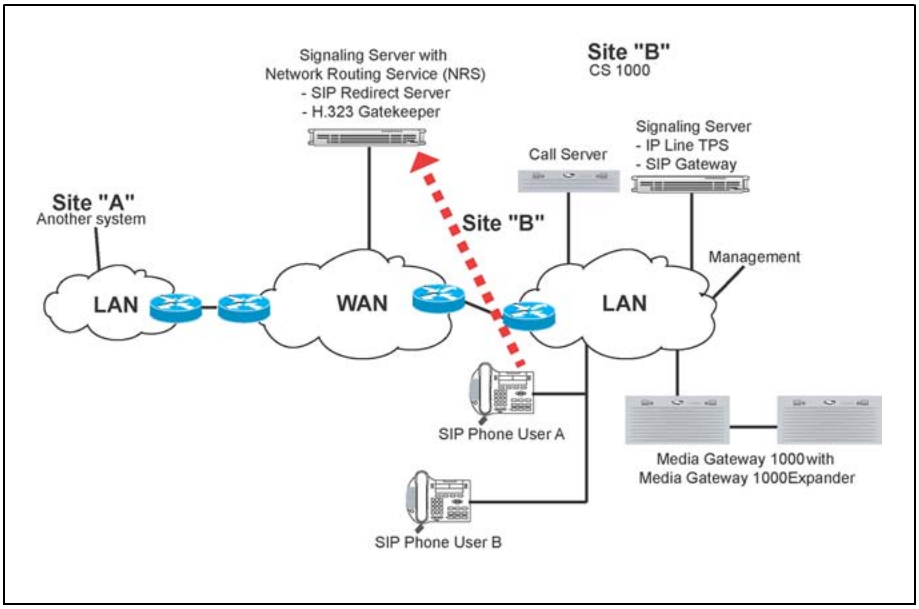
Note: The following call flows are not exhaustive descriptions of the protocol, and exclude some of the components in the CS 1000 system. They are examples for illustrative purposes only.

SIP Phone-to-SIP Phone communication

When SIP Phone User A wants to call SIP Phone User B, the following occurs:

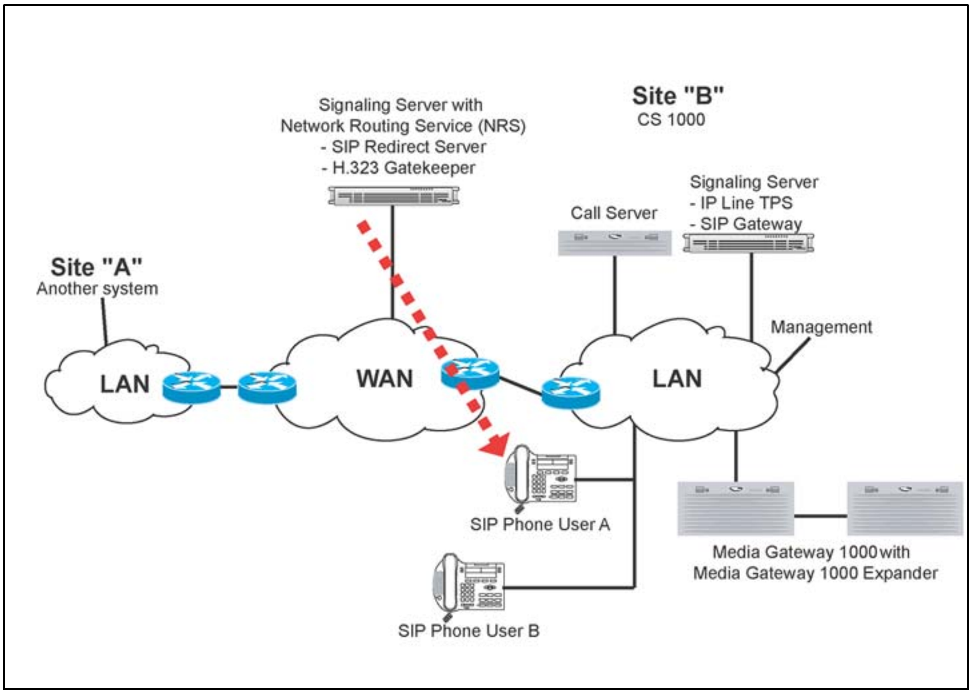
1. SIP Phone A sends an INVITE message to the NRS (specifically the SIP Redirect Server). See Figure 19 "SIP Phone A sends INVITE message to SIP Redirect Server" (page 95).

Figure 19
SIP Phone A sends INVITE message to SIP Redirect Server



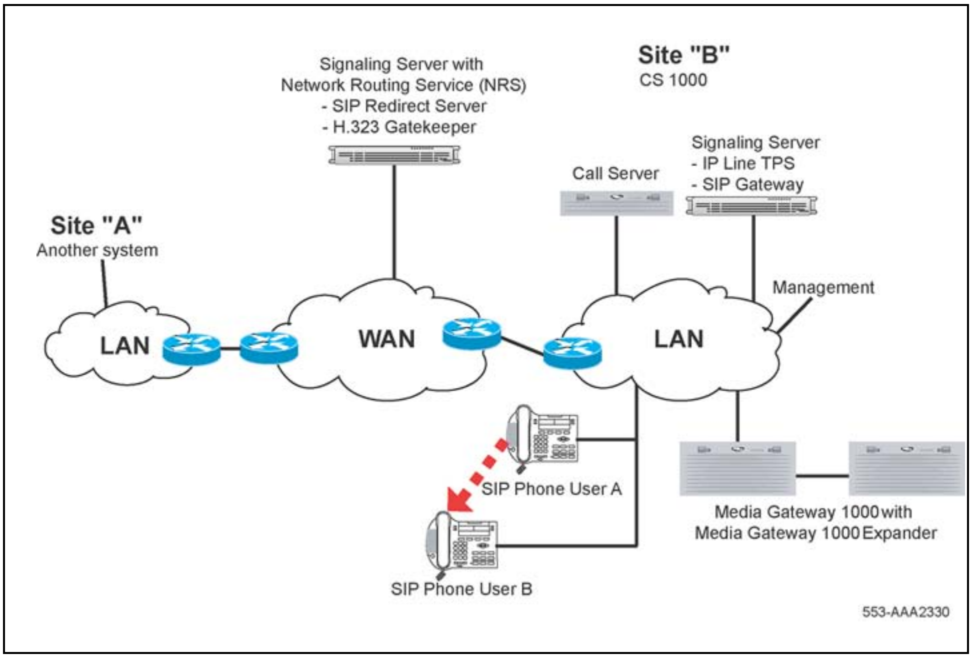
2. The SIP Redirect Server responds with a REDIRECT message and informs SIP Phone User A to directly contact SIP Phone User B. See Figure 20 "SIP Redirect Server responds to SIP Phone A" (page 96).

Figure 20
SIP Redirect Server responds to SIP Phone A



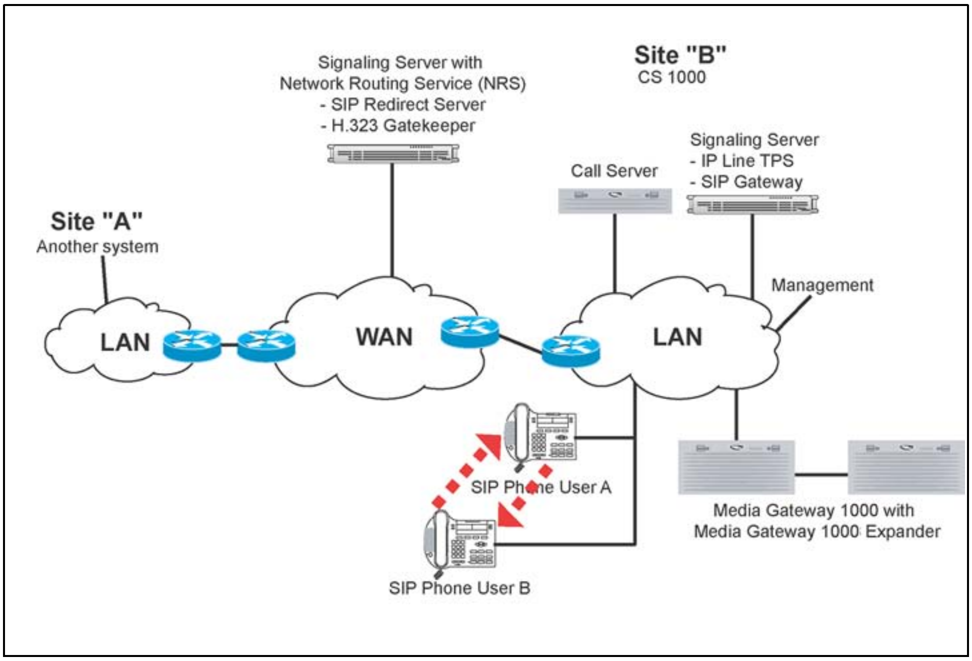
3. SIP Phone A sends an INVITE message directly to SIP Phone B. SIP Phone B rings. See Figure 21 "SIP Phone A sends INVITE message to SIP Phone B" (page 96).

Figure 21
SIP Phone A sends INVITE message to SIP Phone B



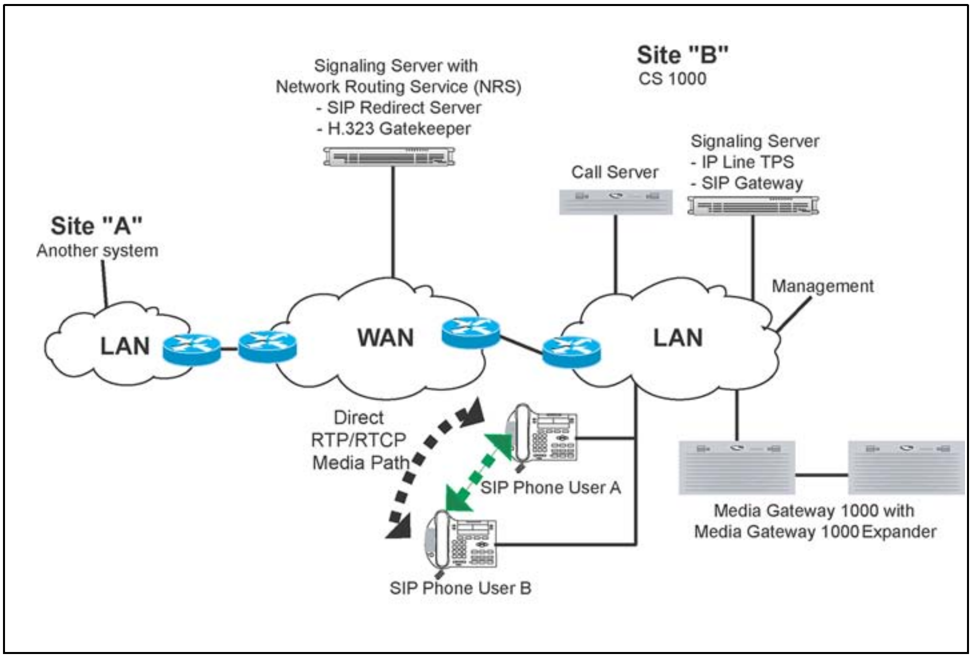
4. SIP Phone User B sends a SIP 200 OK message to SIP Phone User A. SIP Phone A replies by sending a 200 ACK message to SIP Phone B. See Figure 22 "SIP Phone B sends 200 OK message to SIP Phone A" (page 97).

Figure 22
SIP Phone B sends 200 OK message to SIP Phone A



5. The call is set up between the two SIP Phones, and two-way RTP messages are exchanged between SIP Phone A and SIP Phone B. See Figure 23 "SIP Phones start the direct IP media paths" (page 98).

Figure 23
SIP Phones start the direct IP media paths

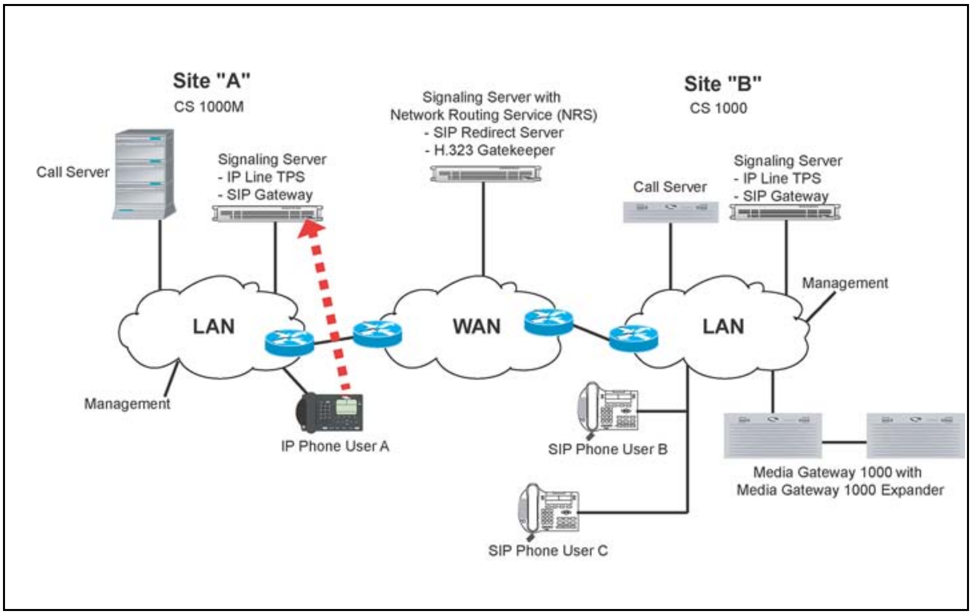


SIP Trunk Gateway-to-SIP Phone communication

When IP Phone User A wants to call SIP Phone User B, the following occurs:

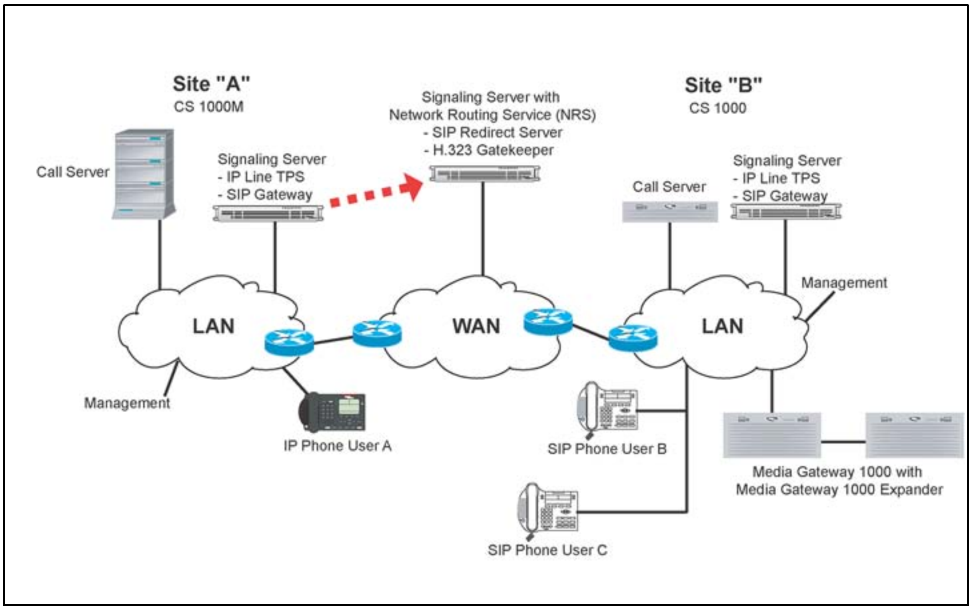
1. IP Phone A makes a call that is routed through Call Server A. See Figure 24 "IP Phone A sends message to SIP Trunk Gateway A" (page 98).

Figure 24
IP Phone A sends message to SIP Trunk Gateway A



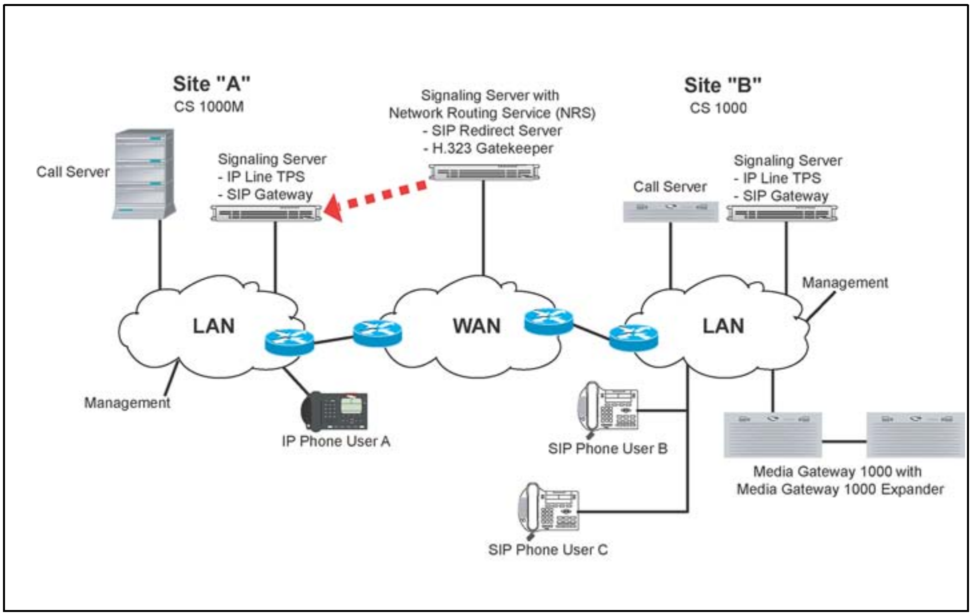
2. SIP Trunk Gateway A sends an INVITE message to the NRS (SIP Redirect Server). See Figure 25 "SIP Trunk Gateway A sends INVITE message to SIP Redirect Server" (page 99).

Figure 25
SIP Trunk Gateway A sends INVITE message to SIP Redirect Server



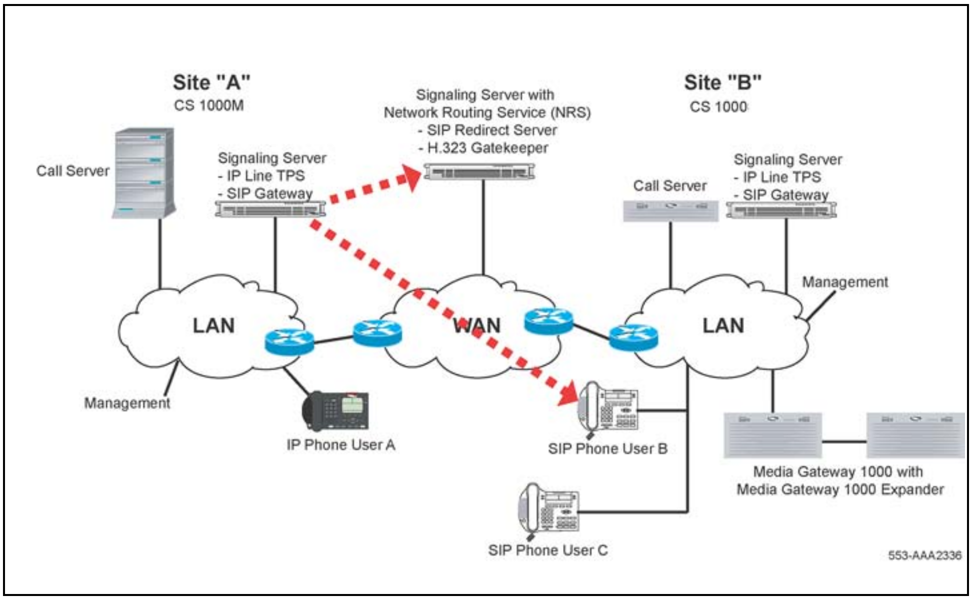
3. The SIP Redirect Server replies back to SIP Trunk Gateway A with a REDIRECT message. The SIP Redirect Server informs SIP Trunk Gateway A of the location of SIP Phone B. See Figure 26 "SIP Redirect Server replies to SIP Trunk Gateway A" (page 100).

Figure 26
SIP Redirect Server replies to SIP Trunk Gateway A



4. SIP Trunk Gateway A acknowledges the message from the SIP Redirect Server with an ACK message. SIP Trunk Gateway A then sends an INVITE message directly to SIP Phone B. See Figure 27 "SIP Trunk Gateway A sends INVITE message to SIP Phone B" (page 100).

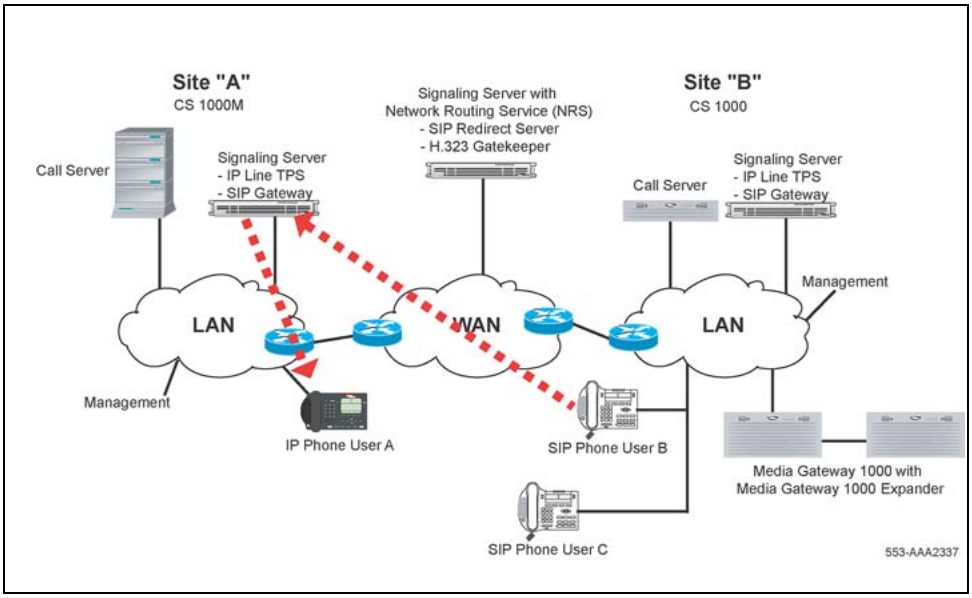
Figure 27
SIP Trunk Gateway A sends INVITE message to SIP Phone B



5. SIP Phone B sends a TRYING message and a Ringing message to the SIP Trunk Gateway A. SIP Trunk Gateway A then sends an Alerting

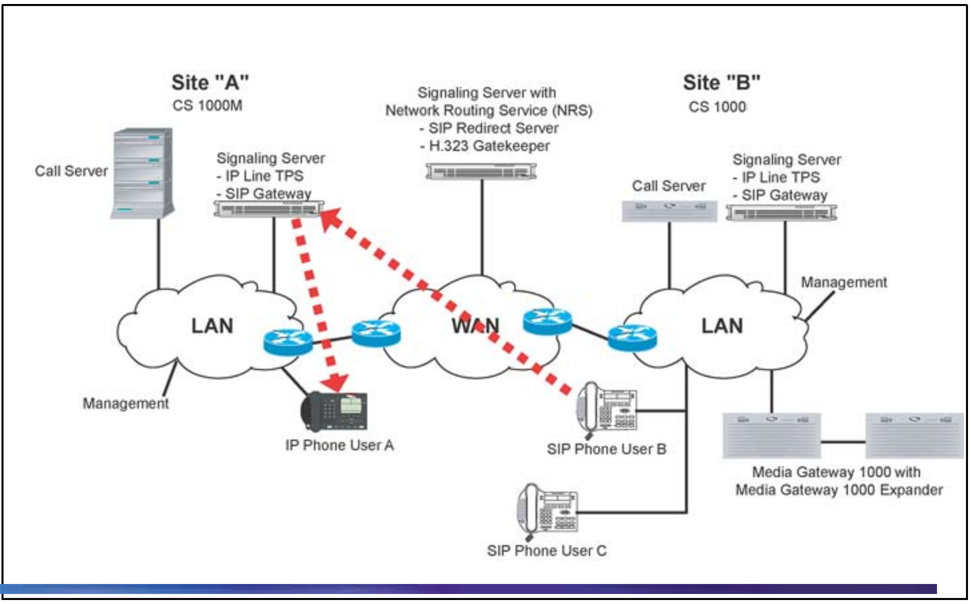
message to IP Phone A. See Figure 28 "SIP Phone B communicates with SIP Trunk Gateway A and SIP Trunk Gateway A communicates with IP Phone" (page 101).

Figure 28
SIP Phone B communicates with SIP Trunk Gateway A and SIP Trunk Gateway A communicates with IP Phone A



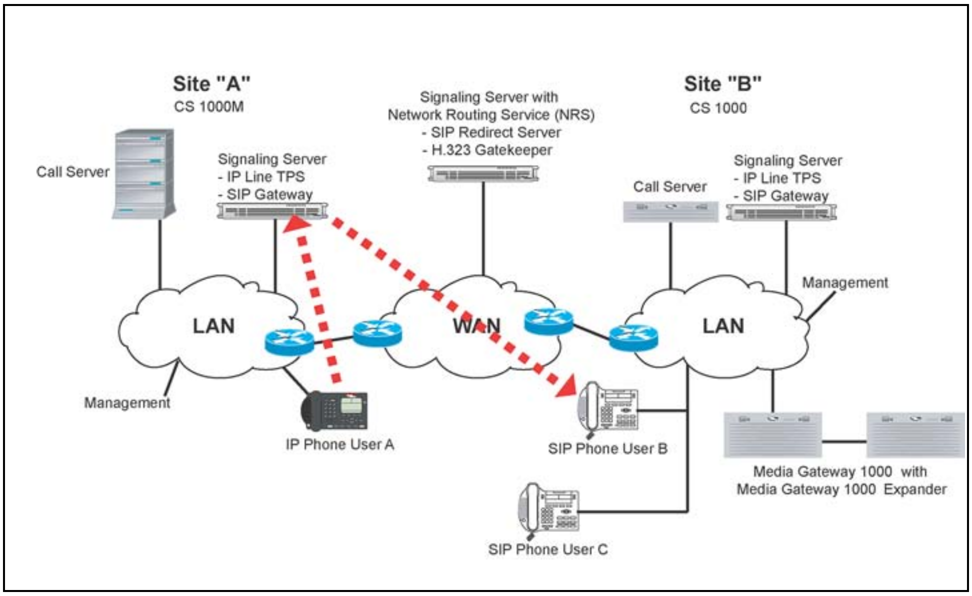
6. SIP Phone B sends a SIP 200 OK message to the SIP Trunk Gateway A. SIP Trunk Gateway A sends a Connect message to IP Phone A. See Figure 29 "SIP Trunk Gateway A communicates with SIP Phone B and IP Phone A" (page 101).

Figure 29
SIP Trunk Gateway A communicates with SIP Phone B and IP Phone A



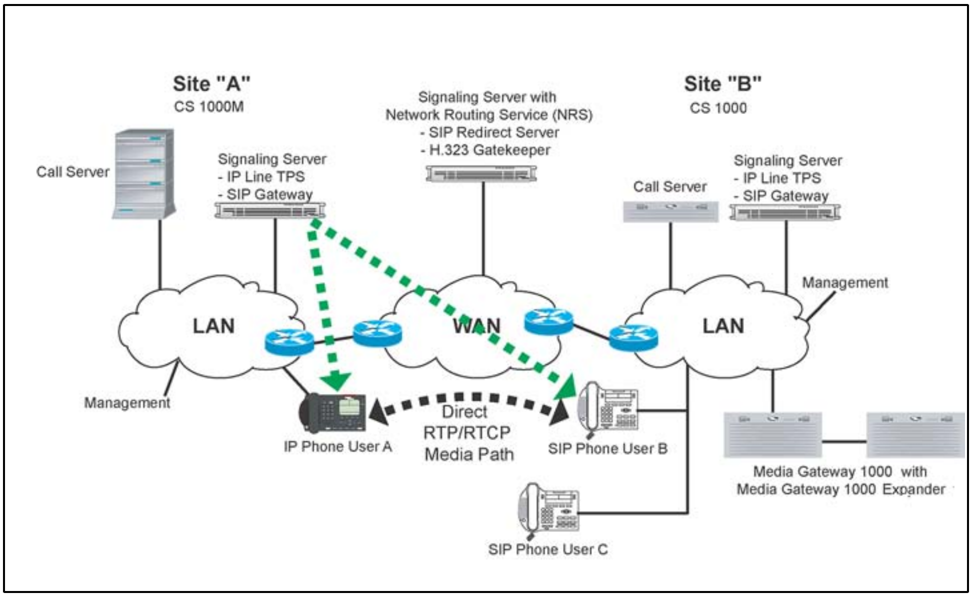
7. IP Phone User A responds to SIP Trunk Gateway A with a Connect ACK message. SIP Trunk Gateway A sends a SIP 200 ACK message to SIP Phone B. See Figure 30 "IP Phone A acknowledges SIP Trunk Gateway A and SIP Trunk Gateway A sends SIP 200 ACK message to SIP" (page 102).

Figure 30
IP Phone A acknowledges SIP Trunk Gateway A and SIP Trunk Gateway A sends SIP 200 ACK message to SIP Phone B



8. The call is set up between IP Phone A and SIP Phone B. Two-way RTP messages are exchanged between IP Phone A and SIP Phone B. See Figure 31 "Direct media path is set up between IP Phone A and SIP Phone B" (page 103).

Figure 31
Direct media path is set up between IP Phone A and SIP Phone B



SIP Phone dynamic registration

SIP Phone dynamic registration facilitates the creation of a contact list for the authorized SIP Phones. A SIP Phone client registers as an endpoint with the SIP Redirect Server (in the NRS). A phone number and a username are mandatory routing entries for the endpoint and are provided during provisioning in the NRS (see Procedure 1 "Adding a User Endpoint" (page 105)).

At registration, only one IP address of the SIP Phone is registered in the endpoint contact list. That is, if a SIP Phone provides more than one IP address in the registration message, then only one IP address (the first one) is stored on the NRS. Usually only one IP address is provided in the registration message; however, the number of provided IP addresses depends on the SIP Phone.

The SIP Redirect Server provides the phone context for SIP Phones when calling users behind the SIP Trunk Gateway.

> ***Note:*** SIP Phones typically do not qualify DN-based URIs with the phone context. Basic support for dealing with raw numbers (as they are dialed by the user) is provided by the SIP Redirect Server. The SIP Redirect Server provides support of unqualified DN-based URIs by performing a pretranslation in order to find the appropriate phone-context.

Assumptions

SIP Phones must support the following for the dynamic registration and establishment of the SIP Phone calls:

- REGISTER message
- 302 message
- Re-INVITE message
- REFER message
- SUBSCRIBE message
- NOTIFY message
- INFO message for end-to-end DTMF
- phone-context transfer from 302 message to INVITE message
- vendor information
- username and password
- static or DHCP assigned IP address
- Expires and Expires Refresh Time based on a 423 (Interval Too Brief) message

Log files

SIP Phones generate log files. SIP Phone user registration and deregistration generate informational report log entries. However, SIP Trunk Gateways generate both log files and SNMP alarms. SIP Trunk Gateway endpoint registration and deregistrations generate SNMP alarms, as well as report log entries.

Installing a SIP Phone

Follow the manufacturer's installation and configuration instructions to set up your SIP Phone.

Configuring a SIP Phone

A SIP Phone is configured as a User Endpoint using NRS Manager. A SIP Phone registers and communicates as an User Endpoint in the NRS.

Routing of unqualified numbers

To support routing of unqualified numbers dialed by SIP Phones, the NRS provides several types of dialing prefixes at the Level 1 regional domain, Level 0 regional domain, and for endpoints. The dialing prefixes include the following:

- E.164 International dialing access code (for example, 6011)
- E.164 National dialing access code (for example, 61)

- E.164 Local dialing access code (for example, 9)
- Level 1 Regional dialing access code (for example, 6)
- Level 0 Regional dialing access code (the default, if none of above match)

Up to two special numbers can be specified at L1 and/or L0.

Task summary

Before a SIP Phone can be added as a User Endpoint in the NRS, the Service Domain, Level 1 Regional Domain, and Level 0 Regional Domain must be configured. To complete these tasks, perform the following procedures:

In the Vxworks-based NRS see

- Procedure 81 "Adding a Service Domain" (page 310)
- Procedure 83 "Adding an L1 Domain (UDP)" (page 312)
- Procedure 85 "Adding an L0 Domain (CDP)" (page 316)

In the Linux-based NRS see

- Procedure 9 "Adding a Service Domain" (page 166)
- Procedure 13 "Adding an L1 Domain (UDP)" (page 172)
- Procedure 17 "Adding an L0 Domain (CDP)" (page 181)

To add a SIP Phone in Linux-based NRS as a User Endpoint, perform the steps in Procedure 34 "Adding a User Endpoint" (page 219).

Adding a User Endpoint (SIP Phone)

To add a SIP Phone as a User Endpoint in VxWorks-based NRS, see Procedure 1 "Adding a User Endpoint" (page 105).

Procedure 1
Adding a User Endpoint

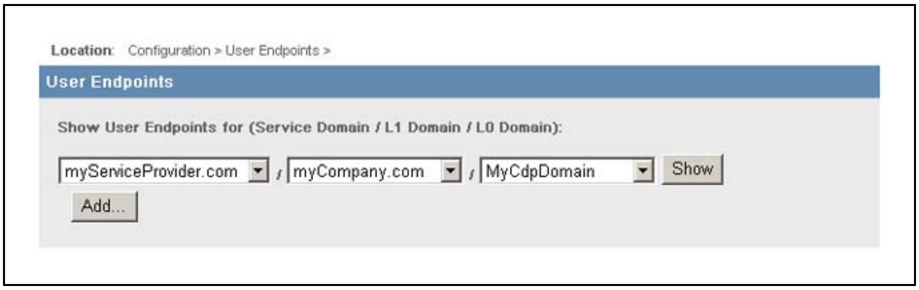
Step	Action
1	Log in to the VxWorks NRS Manager. See "Accessing NRS Manager" (page 290).
2	Click the **Configuration** tab. A dialog box displays indicating the status of the active and standby database. Click **OK**.
3	Ensure the **Standby DB view** is selected.

4 Click **User Endpoints** from the navigator.

> ***Note:*** User Endpoint configuration is currently supported only for SIP.

The **User Endpoints** web page opens, as shown in Figure 33 "Configured User Endpoints" (page 106).

Figure 32
User Endpoints web page



Location: Configuration > User Endpoints >

User Endpoints

Show User Endpoints for (Service Domain / L1 Domain / L0 Domain):

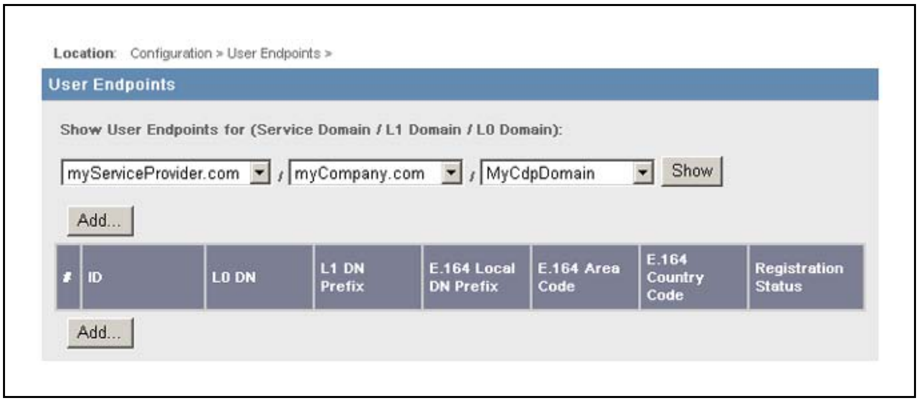
myServiceProvider.com / myCompany.com / MyCdpDomain

5 Select a Service Domain, LI Domain, and L0 Domain from the respective drop-down lists.

6 (Optional) Click **Show**.

The web page expands to display a list of configured User Endpoints for the selected Service Domain, L1 Domain, and L0 Domain. See Figure 33 "Configured User Endpoints" (page 106).

Figure 33
Configured User Endpoints



Location: Configuration > User Endpoints >

User Endpoints

Show User Endpoints for (Service Domain / L1 Domain / L0 Domain):

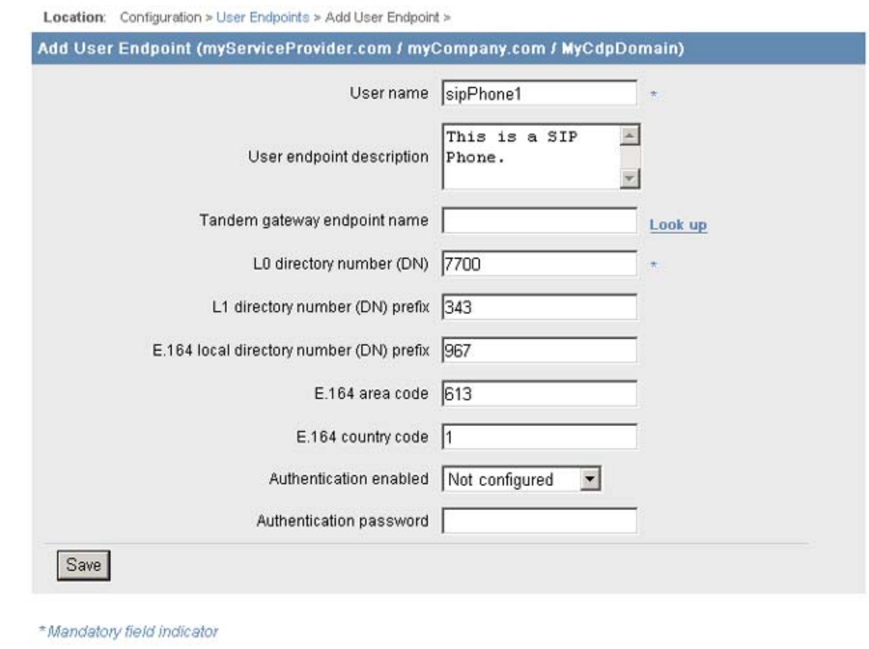
myServiceProvider.com / myCompany.com / MyCdpDomain

#	ID	L0 DN	L1 DN Prefix	E.164 Local DN Prefix	E.164 Area Code	E.164 Country Code	Registration Status

7 Click **Add....**

The **Add User Endpoint** web page opens, as shown in Figure 34 "Add User Endpoint web page" (page 107).

Figure 34
Add User Endpoint web page



Location: Configuration > User Endpoints > Add User Endpoint >

Add User Endpoint (myServiceProvider.com / myCompany.com / MyCdpDomain)

User name	sipPhone1 *
User endpoint description	This is a SIP Phone.
Tandem gateway endpoint name	Look up
L0 directory number (DN)	7700 *
L1 directory number (DN) prefix	343
E.164 local directory number (DN) prefix	967
E.164 area code	613
E.164 country code	1
Authentication enabled	Not configured
Authentication password	

* Mandatory field indicator

8 Enter a **User name** for the SIP Phone. The endpoint's username must be alphanumeric and can be up to 30 characters in length.

The username, together with the Service Domain names, becomes a string that is used to build the user's SIP URI:

[username]@[service_domain_name]

This SIP URI is used during SIP Phone registration. The username is used by the SIP authentication procedures.

9 Enter the **User endpoint description**. The endpoint's description must be alphanumeric (except single quotes) and can be up to 120 characters in length.

10 (Optional) Enter the **Tandem gateway endpoint name**.

A tandem gateway endpoint must be an existing endpoint on the network. It is usually a Gateway Endpoint. The tandem gateway endpoint name is used to tandem all calls originating from this User Endpoint. That is, all calls originating from this User Endpoint are forwarded to the tandem gateway endpoint, which then routes all the call to the appropriate destinations. This is useful for generating Call Records for originating User Endpoint calls.

Note 1: The tandem gateway endpoint name field is also present on the Gateway Endpoint web page.

Note 2: A tandem gateway endpoint must ONLY be configured if the customer wants all the outgoing calls from the SIP User Endpoint to tandem through a SIP Trunk Gateway Endpoint, in that case the SIP Trunk Gateway Endpoint name should be specified in the tandem endpoint box.

Note 3: To accurately add the SIP Trunk Gateway Endpoint name, a **Look up** link is provided to the right of the **Tandem gateway endpoint name** text box. Clicking the **Look up** link opens the **Look up path for Gateway Endpoints** web page .

11 Enter the **LO directory number (DN)** of the SIP Phone. The DN must be numeric and can be up to 30 numbers in length.

An example is 5000. The DN is the user’s DN. That is, the CDP number.

12 Enter the **L1 directory number (DN) prefix**. The DN prefix must be numeric and can be up to seven characters in length.

An example is 343. The L1 DN prefix together with the L0 DN creates the user’s DN which is unique within the parent L1 Regional Domain. That is, the UDP number. For example, 3435000.

L1 domain prefix + L0 DN = User’s DN
343 + 5000 = 3435000

13 Enter the **E.164 local directory number (DN) prefix**. The DN prefix must be numeric and can be up to seven characters in length.

An example is 967. The E.164 local DN prefix is the location code. The E.164 local prefix, together with the L0 DN, creates the user’s E.164 Local (subscriber) DN. For example, 9675000.

E.164 local prefix + L0 DN = User’s E.164 Local (subscriber) DN 967 + 5000 = 9675000

14 Enter the **E.164 area code**. The code must be numeric and can be up to 7 characters in length.

An example is 613. The E.164 area code together with both the E.164 local prefix and L0 DN creates the user’s national E.164 National DN. For example, 6139675000.

E.164 area code + E.164 local prefix + L0 DN = User’s E.164 National DN 613 + 967 + 5000 = 6139675000

15 Enter the **E.164 country code**. The code must be numeric and can be up to 7 characters in length.

An example is 1 (for North America). The E.164 country code, together with the E.164 area code, E.164 local prefix, and L0 DN, creates the user's E.164 International DN. For example, 16139675000.

E.164 country code + E.164 area code + E.164 local prefix + L0 DN = User's E.164 International DN
1 + 613 + 967 + 5000 = 16139675000

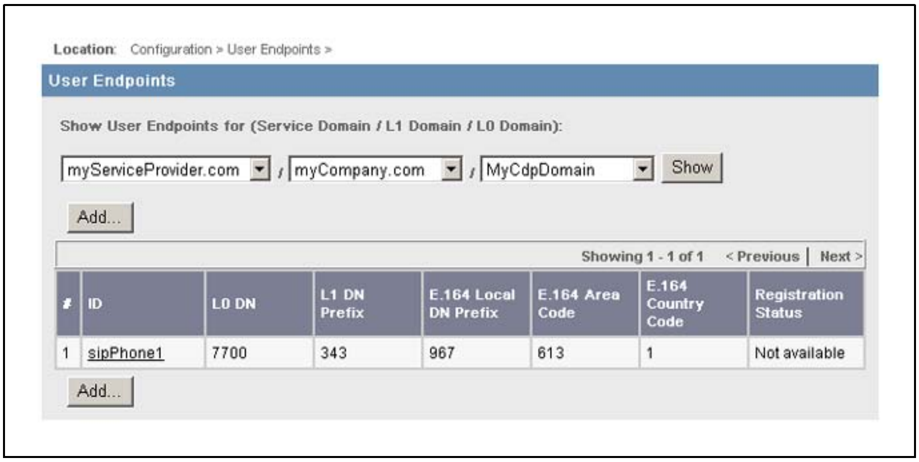
16 Select **Authentication** on from the **Authentication enabled** drop-down list, if you want to enable authentication for this endpoint.

17 If authentication is enabled in step 16, then enter the **Authentication password**. The password must be alphanumeric and can be up to 30 characters in length.

18 Click **Save**.

The **User Endpoints** web page opens, showing the newly added SIP Phone user endpoint. See Figure 35 "Added User Endpoints" (page 109).

Figure 35
Added User Endpoints



Location: Configuration > User Endpoints >

User Endpoints

Show User Endpoints for (Service Domain / L1 Domain / L0 Domain):

myServiceProvider.com / myCompany.com / MyCdpDomain

#	ID	L0 DN	L1 DN Prefix	E.164 Local DN Prefix	E.164 Area Code	E.164 Country Code	Registration Status
1	sipPhone1	7700	343	967	613	1	Not available

19 If required, click **Add...** to add additional SIP Phone user endpoints. Repeat step 7 to step 18.

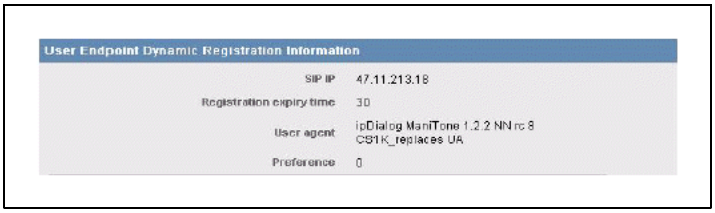
Any new endpoints are displayed in the **User Endpoints** web page.

> ***Note 1:*** A maximum of 50 user endpoints can be displayed on the **User Endpoints** web page.
>
> ***Note 2:*** If a User Endpoint is configured, then the supported protocol type is dynamic SIP. NRS Manager displays User Endpoint Dynamic Registration Information after the User Endpoint registers with the NRS (see Figure 36 "User Endpoint Dynamic Registration Information" (page 110)).

User Endpoint Dynamic Registration information includes the following: SIP IP, Registration expiry time, User agent, and Preference.

The **User Endpoint Dynamic Registration Information** web page is displayed only when NRS Manager is in Active database mode. Detailed dynamic registration information is displayed inside the **User Endpoints** web page.

Figure 36
User Endpoint Dynamic Registration Information



User Endpoint Dynamic Registration Information

SIP IP	47.11.213.18
Registration expiry time	30
User agent	ipDialog ManiTone 1.2.2 NN rc 8 CS1K_replaces UA
Preference	0

—End—

Configure and manage the Linux-based Network Routing Service

Contents

This section contains information on the following topics:

Introduction

The Network Routing Service (NRS) can be configured and maintained through a web interface called NRS Manager. The Linux-based NRS Manager is a component of the Nortel Enterprise Common Manager (ECM). The ECM provides security and navigation infrastructure services for the web-based management applications: Element Manager (EM) and NRS Manager.

It is best practice to configure both a Primary and Secondary NRS to assure high availability of the IP Telephony network.

It is best practice to configure both a Primary and a Backup Security Server per ECM security domain to assure a highly available authentication and authorization service for OA&M users who need to access managed systems/elements in the ECM security domain, as well as for auxiliary applications that rely on continuous availability of the ECM framework web services API to monitor and control the CS 1000.

ECM Framework is installed from the NRS application Install CD (or from the EM application Install CD). Installation of ECM Framework is the first part of every Nortel application Install CD. The **`appinstall`** command always begins by installing the ECM Framework, then goes on to install the specific Nortel application.

For example, before NRS data can be provisioned using NRS Manager:

1. The Nortel-customized Red Hat Enterprise Linux operating system must be installed on an IBM 306m (NTDU99AA) or on a HP DL320 G4 (NTDU97AA) stand-alone server.
2. The Primary NRS and the ECM framework must be installed, and the co-resident Primary Security Service must be installed if a new ECM

Security Domain will be created simultaneously with the installation of the Primary NRS. Alternatively, the Primary NRS can become a member of an existing ECM Security Domain. Optionally a co-resident Backup Security Service may be installed with the installation of the Primary NRS for an existing ECM Security Domain if a Backup Security Service does not already exist.

> ***Note:*** In CS 1000 Rls 5.0 the Linux-based NRS must run on a stand-alone Linux-base COTS server, even for a small IP Telephony network that does not require high availability of the NRS services. Linux-based NRS in Rls 5.0 does not run co-resident with Signaling Server applications on a CS 1000 system. For small CS 1000 networks that do not require high-availability, but do require some of the features introduced with the Linux-based NRS, the customer may choose to avoid the cost of provisioning a Secondary Linux-based NRS. A customer with similar requirements prior to CS 1000 Rls 5.0 would have relied on Primary and Secondary VxWorks-based NRS that are co-resident with Signaling Server applications on two geographically distributed CS 1000 systems.
>
> It is best practice to configure a Backup Security Service when one or more Nortel Linux-based servers are joined as members of an existing ECM Security Domain, to ensure continued access to ECM-based system management applications in case of failure of the ECM Primary Security service.
>
> It is best practice to configure a Secondary NRS for every NRS zone to ensure high-availability of the CS 1000 Rls 5.0 NRS.

3. Add he NRS Manager for the Primary and Secondary NRS servers as managed elements of the ECM.
4. Create user accounts and assign roles and permissions for access to the Primary and Secondary NRS servers from the ECM.

There is a bootable CD to install the Linux operating system and required third party software such as a Web server. There are two application CDs: the NRS CD and the EM CD. The NRS CD contains the NRS, the Primary Security Service and the Backup Security Service. The EM CD contains the EM, the Primary Security Service and the Backup Security Service.

Installation of Linux operating system, ECM framework and NRS application

There is one bootable CD to install the Nortel Linux-base operating system (RHEL 4.0), and to configure IP addresses for dual network interfaces, DNS name server IP addresses, Network Time Protocol, and Linux base built-in user accounts (**`root`** and **`nortel`**).

There are two Nortel application install CDs: the NRS CD and the EM CD. Either the NRS or the EM application, but not both, can be installed on the Nortel Linux base server in CS 1000 Rls 5.0.

The NRS CD contains

- the Network Routing Service application
- the ECM framework
- the ECM Security Service (configurable as Primary Security Service, Backup Security Service, or Security Domain Member)
- Solid database (configurable as Hotstandby primary Solid server, Hotstandby secondary Solid server, or Standalone Solid Server)
- NRS Manager

The EM CD contains

- the Element Manager application
- the ECM framework
- the ECM Security Service (configurable as Primary Security Service, Backup Security Service, or Security Domain Member)
- Solid database

The Linux-based NRS server must be enabled and properly configured before the NRS data can be provisioned using NRS Manager.

Refer to *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*, for detailed information on installing the Linux operating system, the NRS application and the NRS Manager, the ECM Framework, the Solid database, and the ECM Security Services.

Refer to *Enterprise Common Manager Fundamentals (NN43001-116)*, for detailed information on adding a managed element to the ECM, creating user accounts, and assigning roles and permissions for access to the NRS server from the ECM.

The NRS and EM are installed on stand-alone servers. The Primary Security Service and the Backup Security Service can be installed with either NRS or EM. The NRS server will usually have a heavier load than the EM server. To optimize the servers' load balance, Nortel ***recommends*** that, if both Linux-based EM and Linux-based NRS are installed, the Primary Security Service be installed on the EM server and the Backup Security Service be installed on the Primary NRS server. In this case the Secondary NRS will be a security client of the Primary and Backup Security servers.

If Linux-based EM is ***not*** being installed, Nortel ***recommends*** that the Primary Security Service be installed on the Primary NRS server and the Backup Security Service be installed on the Secondary NRS server.

> ***Note 1:*** An ECM security domain member server is a server that has the ECM installed, but does not have the Primary Security Service or the Backup Security Service installed. All ECM security domain member servers must have IP connectivity to either the Primary or Backup security server. If IP connectivity to both the Primary and Backup security servers is unavailable then the ECM security domain member server web pages are inaccessible.
>
> ***Note 2:*** If the Primary Security Service is installed on the EM server the NRS server must have IP connectivity to the EM server. If IP connectivity to the EM server is unavailable then the NRS Manager web pages are inaccessible. IP connectivity between an NRS server and the EM server will be assured if the servers are on the same LAN.

Refer to *Security Management (NN43001-604)*, for detailed information on CS 1000 system security including protection of signaling and the media stream from privacy intrusions or disruption, and the administration and use of secure remote access.

Access NRS Manager through the ECM

Access NRS Manager through the ECM. See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145) to access NRS Manager.

Configure your web browser and windows display before logging in to ECM. NRS Manager is supported only on Microsoft Internet Explorer version 6.0 (or later). See Procedure 2 "Configure the Internet Explorer browser settings" (page 144) to configure the Internet Explorer browser. See Procedure 3 "Configuring the Windows Display settings" (page 145) to configure the Windows display settings.

Initial configuration of Linux-based NRS on a new IP Peer network

This section provides a high-level overview of the initial configuration of the Linux-based NRS on a new IP Peer network. The main steps are:

- Accessing the NRS Manager.
- Configuring the Primary and Secondary NRS servers.
- Starting services.
- Configuring system wide NRS settings.
- Configuring the NRS database (the Solid database). The NRS database provides a central database of addresses that are required to route calls across the network.

- Logging out of the ECM.

In more detail, the initial configuration of the Linux-based NRS on a new IP Peer network task is comprised of:

1. **Accessing NRS manager.** See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).
2. **Configure the Primary and Secondary NRS server settings.** See Procedure 6 "Configuring the Primary and Secondary NRS Server Settings" (page 155).

   ATTENTION
   The Primary and Secondary NRS servers must be configured one by one. The user ***must*** be logged on the specific (either Primary or Secondary) server to configure it. See Step 4 of Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).

3. **Start services.**

   In the **NRS Manager Navigator** select **System > NRS Server**. The **NRS Server** web page opens, as shown in Figure 42 "NRS Server web page" (page 148). Click the **Restart** button on the **Service Status** pane of the **NRS Server** web page.
4. **Configure system wide settings.** See Procedure 7 "Configuring system-wide settings" (page 162).
5. **Build the NRS database.**

   The NRS database comprises

   - service domains, L1 domains and L0 domains
   - collaborative servers
   - gateway endpoints
   - routing entries
   - post-routing SIP URI modification table entries

     Note: This task is related to building the NRS database gateway endpoints. It is not related to building the NRS database user endpoints.

   ATTENTION
   The following steps **must** be performed in the order given.

   a. Create the Service Domain, Level 1 Domains (UDP), Level 0 Domains (CDP), which hold the endpoint numbering plans on the

NRS. This is complementary to the CDP configuration on the Call Server.

   i. See Procedure 9 "Adding a Service Domain" (page 166).

   ii. See Procedure 13 "Adding an L1 Domain (UDP)" (page 172).

   iii. See Procedure 17 "Adding an L0 Domain (CDP)" (page 181).

b. Add collaborative servers.

   - See Procedure 21 "Adding a Collaborative Server" (page 190).

c. Add gateway endpoints and endpoint prefixes. See Procedure 25 "Adding a Gateway Endpoint" (page 199).

d. Add the numbering plan entries for each gateway endpoint, including the Cost Factor for each entry.

   i. See Procedure 40 "Adding a Routing Entry" (page 231).

   ii. See Procedure 47 "Adding a Default Route" (page 244).

e. Post-routing SIP URI modification table entries

   i. See Procedure 30 "Adding Post-routing SIP URI Modification" (page 213).

   ii. See Procedure 32 "Editing Post-routing SIP URI Modification" (page 216).

   iii. See Procedure 33 "Deleting Post-routing SIP URI Modification" (page 217).

6. **Test the numbering plans** .

   a. See Procedure 52 "Performing an H.323 Routing Test" (page 250).

   b. See Procedure 53 "Performing a SIP Routing Test" (page 252).

7. **Perform database actions.** See "Performing NRS database actions" (page 255). To save the NRS configuration, refer to the procedures in this section.

   - See Procedure 57 "Cutting over the database" (page 257).
   - See Procedure 58 "Reverting the database changes" (page 258).
   - See Procedure 59 "Rolling back changes to the database" (page 259).
   - See Procedure 60 "Committing the database" (page 260).

8. **Back up the NRS database.** See "Backing up the database" (page 260).

- See Procedure 61 "Automatically backing up the database" (page 261).
- See Procedure 62 "Manually backing up the database" (page 262).

9. **Log out of ECM** . See Procedure 5 "Logging out of ECM " (page 155).
10. To return to the ECM web page without terminating the current ECM session see "Common Manager link" (page 154).

Configure Gateway endpoints

See the Element Manager procedures in *IP Peer Networking Installation and Commissioning (NN43001-313)* to configure H.323 and SIP gateway endpoints. When configuring the gateway endpoints see the "Nortel recommendation for load-balancing across the Primary and Secondary Linux-based NRS servers" (page 118).

Nortel recommendation for load-balancing across the Primary and Secondary Linux-based NRS servers

The Linux-based NRS has an active-active database model. In the active-active database model:

- Both the Primary and Secondary NRS can register endpoints.
- A registration event updates a common database shared by the Primary and Secondary NRS.
- Both the Primary and Secondary NRS can route calls to endpoints that are registered to either the Primary or Secondary NRS.

Load-balancing across the Primary and Secondary NRS servers can be implemented by configuring half of the gateway endpoints to target the Primary NRS server as their first choice for registration and half of the gateway endpoints to target the Secondary NRS server as their first choice for registration. The gateway will register with only one of the NRS servers.

There are two IP addresses assigned when configuring H.323 gateway settings: a **Primary gatekeeper IP address** and an **Alternate gatekeeper IP address**. In this context, the **Primary gatekeeper IP address** is the IP address of the gateway's' first choice for registration and the **Alternate gatekeeper IP address** is the IP address of the gateway's alternate choice for registration, if it's first choice is not in service.

Thus, to optimize load-balancing across the Primary and Secondary NRS servers when configuring the gateway endpoints, for half of the H.323 gateway endpoints enter the **IP address of the Primary NRS server** in the **Primary gatekeeper IP address** text box and enter the **IP address of the Secondary NRS server** in the **Alternate gatekeeper IP address** text box.

Reverse this assignment for the other half of the H.323 gateway endpoints. That is enter the **IP address of the Secondary NRS server** in the **Primary gatekeeper IP address** text box and enter the **IP address of the Primary NRS server** in the **Alternate gatekeeper IP address** text box.

Similarly, there are two IP addresses assigned when configuring SIP gateway settings: a **Primary Proxy/Re-direct IP address** and a **Secondary Proxy/Re-direct IP address**. In this context, the **Primary Proxy/Re-direct IP address** is the IP address of the gateway's first choice for registration and the **Secondary Proxy/Re-direct IP address** is the IP address of the gateway's alternate choice for registration, if it's first choice is not in service.

Thus to optimize load-balancing across the Primary and Secondary NRS servers when configuring the gateway endpoints, for half of the SIP gateway endpoints enter the **IP address of the Primary NRS server** in the **Primary Proxy/Re-direct IP address** text box and enter the **IP address of the Secondary NRS server** in the **Secondary Proxy/Re-direct IP address** text box.

Reverse this assignment for the other half of the SIP gateway endpoints. That is enter the **IP address of the Secondary NRS server** in the **Primary Proxy/Re-direct IP address** text box and enter the **IP address of the Primary NRS server** in the **Secondary Proxy/Re-direct IP address** text box.

Configure NRS database user endpoints

1. **SIP phones.** A SIP Phone registers and communicates as a user endpoint in the NRS. To add a User Endpoint, refer to Procedure 34 "Adding a User Endpoint" (page 219).
2. **View the SIP Phone Context.** See Procedure 39 "SIP Phone Context Mapping" (page 229) to view the SIP phone context.

Upgrade of an IP Peer Network from VxWorks-based NRS to Linux-based NRS with SIP Proxy

Recommended upgrade procedure

There are two upgrade paths of an existing IP Peer Network from VxWorks-based NRS to Linux-based NRS:

1. **Re-use the existing NRS IP addresses for Linux-based NRS servers**
2. **New NRS IP address assignments**

Nortel ***recommends*** following the upgrade procedures that **Re-use the existing NRS IP addresses for Linux-based NRS servers** in order to avoid configuration changes to all existing SIP and H.323 endpoints. The recommended procedure also allows rapid switchover from the existing VxWorks-based NRS to the new Linux-based NRS while minimizing IP Telephony service interruption.

You must follow the alternative upgrade procedures for **New NRS IP address assignments** (a) when the new Linux-based NRS must be installed at a different location with different IP address scopes, or (b) when the new Linux-based NRS must be installed as a Collaborating NRS zone parallel to the existing VxWorks-based NRS during a gradual upgrade process with gradual switchover of the SIP and H.323 endpoints to the new Linux-based NRS.

Re-use the existing NRS IP addresses for Linux-based NRS upgrade procedure

If the Linux-based NRS can be installed in the same physical location as the existing VxWorks-based NRS, there are several advantages to this upgrade path:

- All VxWorks-based SIP and H.323 endpoints can be simultaneously switched over to the Linux-based NRS by manipulating Layer 1 and Layer 2 network connections of the VxWorks-based and Linux-Based NRS. Consequently, the NRS service will not be interrupted due to the upgrade.
- Endpoints (virtual trunk Gateways and IP Phones) do not have to be manually re-configured to target new Primary and Secondary NRS IP addresses.
- Provided the endpoints have not been re-configured to use features that are unique to the Linux-base NRS (for example, network post-translation, TLS, or transport normalization), it is possible to revert all endpoints with minimum disruption to the VxWorks-based NRS by manipulating Layer 1 and Layer 2 network connections (such as moving the ethernet cables) on the VxWorks-based and Linux-based NRS servers.

  One might wish to revert to the VxWorks-based NRS, if service needs to be restored rapidly after a switch over to the Linux-based NRS due to a configuration mistake or missing software patches.

Overview of upgrade procedure

The following considerations determine how the upgrade procedure is implemented:

1. If the Linux-based NRS servers re-use existing IP addresses, it is necessary to ensure that duplicate IP addresses do not appear on the enterprise network during the upgrade.

   To ensure that duplicate IP addresses do not appear on the enterprise network during the upgrade, isolate the existing VxWorks-based Primary NRS from the enterprise network by unplugging it from the network.

This forces the endpoints to register to the VxWorks-based Alternate NRS. Network services will be maintained by the Alternate NRS during the upgrade. If the Alternate NRS were to fail, the Failsafe NRS, co-resident with CS 1000 gateway endpoints, provides system redundancy for the IP Peer network during the upgrade and migration to Linux-based NRS.

2. A Linux-based NRS application must be installed on an ECM security domain. An ECM security domain is defined by the ECM Primary Security server. An ECM security domain is comprised of the ECM Primary Security server, an optional ECM Backup Security server and any associated security domain member servers. An ECM security domain member server is a server that has the ECM framework and the Linux-based EM application or the Linux-based NRS application installed, but does not have the Primary Security Service or the Backup Security Service installed.

   If single sign-on is required for EM and NRS Manager than the Linux-based NRS servers and Linux-based EM must be members of the same ECM security domain.

   The Linux-based NRS and the Linux-based EM applications are installed on stand-alone servers. The ECM Primary Security Service can be installed with either NRS or EM. To optimize the servers' load balance Nortel **recommends** that, if both Linux-based EM and Linux-based NRS are installed, the Primary Security Service be installed on the EM server. If Linux-based EM is not being installed, Nortel **recommends** that the Primary Security Service be installed on the Primary NRS server.

3. By contrast, the VxWorks-based NRS is hosted either co-resident with Signaling Server applications, or in a stand-alone mode on a dedicated server running the VxWorks real-time operating system. VxWorks servers do not rely on ECM security domains for installation or operation.

   If the VxWorks-based NRS is co-resident with Signaling Server applications, the Signaling Server must be assigned a new TLAN host IP address that is not in use on the TLAN network.

Linux-based NRS dependency on ECM security domain

There must be network connectivity to the ECM Primary Security Service during the installation of the Primary and Secondary NRS. There are two configurations for the deployment of the ECM Primary Security Service:

1. Linux-based EM has not been installed and is not being installed now. The ECM Primary Security Service is being installed on the Linux-based Primary NRS server and the ECM Backup Security Service is being installed on the Linux-based Secondary NRS server.

2. Both the Linux-based EM and Linux-based NRS are being installed. The ECM Primary Security Service is being installed on the EM server and

the ECM Backup Security Service is being installed on the Linux-based Primary NRS server. The Linux-based Secondary NRS will be a security client of the ECM Primary and Backup Security servers.

Install Linux-based NRS by isolating VxWorks-based NRS from customer network: scenario 1

Follow this upgrade path if the Linux-based EM has not been installed and is not being installed now. The ECM Primary Security Service is being installed on the Linux-based Primary NRS server and the ECM Backup Security Service is being installed on the Linux-based Secondary NRS server.

This section provides a task summary of the main steps in the upgrade procedure.

1. **Log on to VxWorks-based Primary NRS**.

   See "Accessing NRS Manager" (page 290).

2. **Monitor the VxWorks-based IP Peer network.**

   View SIP gateways, H.323 gateways, user endpoints, collaborative servers, a representative sample of routes and the database backup log file. Carefully note which endpoints are registered and which endpoints are not registered.

   Follow the VxWorks-based procedures:

   Procedure 88 "Viewing the Gateway Endpoints" (page 326).

   Procedure 1 "Adding a User Endpoint" (page 105). (This procedure also shows how to view user endpoints).

   Procedure 94 "Viewing the Collaborative Servers" (page 341).

   Procedure 90 "Viewing the Routing Entries" (page 332).

   Procedure 108 "Downloading the latest backup log file" (page 360)

3. To ensure that the Alternate NRS is communicating with the Primary NRS and that the databases are synchronized, use the CLI command to invoke database synchronization.

4. **Backup the VxWorks-based NRS database**. See "Backing up the database" (page 357).

5. **Gracefully disable the VxWorks-based Primary NRS server** forcing all endpoints to register with the VxWorks-based Alternate NRS. See Procedure 98 "Disabling the NRS server" (page 347).

6. **Log in to VxWorks-based Alternate NRS.** See "Accessing NRS Manager" (page 290).

   Verify that the SIP gateways, H.323 gateways and user endpoints have registered with the VxWorks-based Alternate NRS.

   Follow the VxWorks-based procedures:

Procedure 88 "Viewing the Gateway Endpoints" (page 326) .

Procedure 1 "Adding a User Endpoint" (page 105). (This procedure also shows how to view user endpoints).

7. **Disconnect the existing VxWorks-based Primary NRS from the enterprise network.**

   a. If the VxWorks-based Primary NRS server is in stand-alone mode (that is, not co-resident with Signaling Server applications), disconnect it from the enterprise network and connect the Linux-based Primary NRS server to the enterprise network.

   b. If the VxWorks-based Primary NRS is co-resident with Signaling Server applications, do not disconnect the Primary NRS from the enterprise network.

      Instead,

      i. Re-configure the Signaling Server with a newly assigned TLAN host IP address that is not in use on the TLAN network.

      ii. Reboot the Signaling Server. Doing so momentarily disrupts applications, such as

         - UNIStim terminal Proxy
         - SIP gateway
         - H.323 gateway

ATTENTION

You must complete step 7 before step 8

8. **Install the Linux-based Primary NRS server**.

   a. Install the Linux operating system on a COTS stand-alone server.

      There is a bootable CD to install the Linux operating system.

      Note: the VxWorks-based Primary NRS IP address must be assigned as the TLAN IP address of the Primary NRS during installation of the Linux operating system.

   b. Install the NRS and the ECM Primary Security Service. During the installation of the NRS application configure the Solid database server as **Hotstandby primary Solid server**.

      The NRS CD contains the NRS and ECM Primary Security Service.

      Refer to *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*, for detailed information on installing the Linux operating system, the ECM framework, the NRS and the ECM Primary Security Service.

9. **Add the NRS Manager for the Primary and Secondary NRS servers as managed elements of the ECM.**

   Refer to *Enterprise Common Manager Fundamentals (NN43001-116)*, for detailed information on adding a managed element to the ECM.

10. **Create user accounts and assign roles and permissions** for access to the Primary and Secondary NRS servers from the ECM.

    Refer to *Enterprise Common Manager Fundamentals (NN43001-116)*, for detailed information on creating user accounts, and assigning roles and permissions for access to the NRS servers from the ECM.

11. **Log in to NRS Manager for the Linux-based Primary NRS server**.

    See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).

12. **Restore the VxWorks-based NRS database** backed up in step 4. See the procedures in "Restoring the database" (page 266) to restore an NRS Release 5.0, 4.5 or 4.0 database. See "GK/NRS Data Upgrade" (page 273) to restore a 3.0 H.323 Gatekeeper.

    ATTENTION

    Restoring the previous release database should always be followed by cross checking changes in the Primary and Secondary NRS Server settings (see Figure 49 "Edit Server Configuration web page" (page 156)) and saving them in the new restored database.

13. To ensure that the correct database file has been restored and that it looks similar to the database that was backed up in step 4, review the restored database.

    Follow the Linux-based procedures:

    Procedure 27 "Viewing the Gateway Endpoints" (page 208)

    Procedure 41 "Viewing the Routing Entries" (page 234)

    Procedure 22 "Viewing a Collaborative Server" (page 195)

    Procedure 36 "Viewing the User Endpoints" (page 225)

14. **Configure the Linux-based Primary server settings**. See Procedure 6 "Configuring the Primary and Secondary NRS Server Settings" (page 155).

    - Assign the IP address of the VxWorks-based Primary NRS server to the Linux-based Primary NRS server. Assign the IP address of the VxWorks-based Alternate NRS server to the Linux-based Secondary NRS server. Choose **Primary** from the **server role** drop down list. See Figure 49 "Edit Server Configuration web page" (page 156).

- If the IP network NRS zone contains H.323 endpoints, configure H.323 Gatekeeper settings. See Figure 50 "H.323 Gatekeeper Settings section" (page 157).
- Configure SIP Server settings. See Figure 51 "SIP Server Settings section" (page 159).
- Configure Network Connection Server settings. See Figure 53 "Network Connection Server (NCS) Settings section" (page 161).

15. **Start services on the Primary NRS server.**

    In the **NRS Manager Navigator** select **System > NRS Server**. The **NRS Server** web page opens, as shown in Figure 42 "NRS Server web page" (page 148). Click the **Restart** button on the **Service Status** pane of the **NRS Server** web page.

    After services are started the Primary NRS will respond to polling and registration requests.

16. **Monitor the SIP gateway, H.323 gateway and user endpoints** on the Linux-based IP Peer network to ensure that they have registered with the Linux-based Primary NRS server.

    Follow the Linux-based procedures:

    Procedure 27 "Viewing the Gateway Endpoints" (page 208).

    Procedure 36 "Viewing the User Endpoints" (page 225)

    All gateways and end points should have registered with the Linux-based Primary NRS within five minutes.

    Carefully note which endpoints are registered and which endpoints are not registered.

    Compare this list of registered endpoints with the list of registered endpoints in step 2 to ensure that all SIP and H.323 endpoints that were registered to the VxWorks-based NRS are now registered to the Linux-based Primary NRS.

17. **Disconnect the existing VxWorks-based Alternate NRS from the enterprise network.**

    a. If the VxWorks-based Alternate NRS server is in stand-alone mode (that is not co-resident with Signaling Server applications), disconnect it from the enterprise network and connect the Linux-based Secondary NRS server to the enterprise network.

    b. If the VxWorks-based Alternate NRS is co-resident with Signaling Server applications, do not disconnect the Alternate NRS from the enterprise network.

Instead,

i. Re-configure the Signaling Server with a newly assigned TLAN host IP address that is not in use on the TLAN network.

ii. Reboot the Signaling Server. Doing so momentarily disrupts applications, such as

- UNIStim terminal Proxy
- SIP gateway
- H.323 gateway

ATTENTION

You must complete step 17 before step 18

ATTENTION

The IP Peer network will have a Linux-based Primary NRS server without a Linux-based Secondary NRS server or a VxWorks-based Alternate server deployed between the completion of step 18 and the completion of step 22. The network should not be left in this configuration. Coordinate the completion of the tasks in step 18 and step 21, to ensure that the network is not left in this configuration for a long period of time.

18. **Install the Linux-based Secondary NRS server**.

    a. Install the Linux operating system on a COTS stand-alone server.

    There is a bootable CD to install the Linux operating system.

    Note: the VxWorks-based Alternate NRS IP address must be assigned as the TLAN IP address of the Secondary NRS during installation of the Linux operating system.

    b. Install the NRS and the ECM Backup Security Service. During the installation of the NRS application configure the Solid database server as **Hotstandby secondary Solid server.**

    The NRS CD contains the NRS application and ECM Backup Security Service.

    Refer to *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*, for detailed information on installing the Linux operating system, the ECM framework, the NRS and the ECM Primary Security Service.

19. **Log in to NRS Manager for the Secondary NRS server.** See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).

20. **Configure the Linux-based Secondary server settings**. See Procedure 6 "Configuring the Primary and Secondary NRS Server Settings" (page 155).

    - Assign the IP address of the VxWorks-based Primary NRS server to the Linux-based Primary NRS server. Assign the IP address of the VxWorks-based Alternate NRS server to the Linux-based Secondary NRS server. Choose **Secondary** from the **server role** drop down list. See Figure 49 "Edit Server Configuration web page" (page 156).
    - If the IP network NRS zone contains H.323 endpoints, configure H.323 Gatekeeper settings. See Figure 50 "H.323 Gatekeeper Settings section" (page 157).
    - Configure SIP Server settings. See Figure 51 "SIP Server Settings section" (page 159).
    - Configure Network Connection Server settings. See Figure 53 "Network Connection Server (NCS) Settings section" (page 161).

21. **Start services on Secondary NRS server.**

    In the **NRS Manager Navigator** select **System > NRS Server**. The **NRS Server** web page opens, as shown in Figure 42 "NRS Server web page" (page 148). Click the **Restart** button on the **Service Status** pane of the **NRS Server** web page.

    Both the Linux-based Primary and Secondary NRS are in service. The endpoints should remain registered to the Primary NRS server. The Solid database synchronization link should be established between the Primary and Secondary NRS servers. The Solid databases on the Primary and Secondary servers should synchronize automatically.

22. **Ensure Linux-based Primary and Secondary NRS servers are synchronizing**.

    To ensure the NRS servers are synchronizing

    - Log onto the Primary NRS Manager. See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).
    - View the Gateway Endpoints on the Active Database. See Procedure 27 "Viewing the Gateway Endpoints" (page 208).
    - Note the number of Gateway Endpoints.
    - View the User Endpoints on the Active Database. See Procedure 36 "Viewing the User Endpoints" (page 225).
    - Note the number of User Endpoints
    - Log onto the Secondary NRS Manager. See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).

- View the Gateway Endpoints on the Active Database. See Procedure 27 "Viewing the Gateway Endpoints" (page 208).
- Note the number of Gateway Endpoints
- View the User Endpoints on the Active Database. See Procedure 36 "Viewing the User Endpoints" (page 225).
- Note the number of User Endpoints
- If the number of endpoints on the Primary NRS and the Secondary NRS databases are the same, then the databases are synchronized.

End of task summary for upgrade procedure.

Install Linux-based NRS by isolating VxWorks-based NRS from customer network: scenario 2

This section provides a task summary of the main steps in the upgrade procedure.

> ***Note:*** If Linux-based EM was installed with the ECM Primary Security Service prior to the installation of the Linux-based NRS, proceed directly to step 2.

1. Follow this upgrade path if the Linux-based EM and Linux-based NRS are being installed at the same time. The ECM Primary Security Service is being installed on the EM server and the ECM Backup Security Service is being installed on the Linux-based Primary NRS server. The Linux-based Secondary NRS will be a security client of the ECM Primary and Backup Security servers.

   Install and configure the Linux-based EM server

   a. Install the Linux operating system on a COTS stand-alone server.

      There is a bootable CD to install the Linux operating system.

      > ***Note:*** the VxWorks-based Primary NRS IP address must be assigned as the TLAN IP address of the Primary NRS during installation of the Linux operating system.

   b. Install the EM and the ECM Primary Security Service.

      The EM CD contains the EM and ECM Primary Security Service.

      Refer to *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*, for detailed information on installing the Linux operating system, the ECM framework, the NRS and the ECM Primary Security Service.

2. **Add the NRS Manager for the Primary and Secondary NRS servers as managed elements of the ECM.**

Refer to *Enterprise Common Manager Fundamentals (NN43001-116)*, for detailed information on adding a managed element to the ECM.

3. **Create user accounts and assign roles and permissions** for access to the Primary and Secondary NRS servers from the ECM.

   Refer to *Enterprise Common Manager Fundamentals (NN43001-116))*, for detailed information on creating user accounts, and assigning roles and permissions for access to the NRS servers from the ECM.

4. **Log on to VxWorks-based Primary NRS**. See "Accessing NRS Manager" (page 290).

5. **Monitor the VxWorks-based IP Peer network.**

   View SIP gateways, H.323 gateways, user endpoints, collaborative servers and a representative sample of routes. Carefully note which endpoints are registered and which endpoints are not registered.

   Follow VxWorks-based procedures:

   Procedure 88 "Viewing the Gateway Endpoints" (page 326).

   Procedure 1 "Adding a User Endpoint" (page 105). (This procedure also shows how to view user endpoints).

   Procedure 94 "Viewing the Collaborative Servers" (page 341).

   Procedure 90 "Viewing the Routing Entries" (page 332).

   Procedure 108 "Downloading the latest backup log file" (page 360).

6. To ensure that the Alternate NRS is communicating with the Primary NRS and that the databases are synchronized, use the CLI command to invoke database synchronization.

7. **Backup the VxWorks-based NRS database**. See "Backing up the database" (page 357).

8. **Gracefully disable the VxWorks-based Primary NRS server** forcing all endpoints to register with the VxWorks-based Alternate NRS. See Procedure 98 "Disabling the NRS server" (page 347).

9. **Log in to VxWorks-based Alternate NRS.** See "Accessing NRS Manager" (page 290).

   Verify that the SIP gateways, H.323 gateways and user endpoints have registered with the VxWorks-based Alternate NRS.

   Follow VxWorks-based procedures:

   Procedure 88 "Viewing the Gateway Endpoints" (page 326).

   Procedure 1 "Adding a User Endpoint" (page 105). (This procedure also shows how to view user endpoints).

10. **Disconnect the existing VxWorks-based Primary NRS from the enterprise network.**

    a. If the VxWorks-based Primary NRS server is in stand-alone mode (that is, not co-resident with Signaling Server applications), disconnect it from the enterprise network and connect the Linux-based Primary NRS server to the enterprise network.

    b. If the VxWorks-based Primary NRS is co-resident with Signaling Server applications, do not disconnect the Primary NRS from the enterprise network.

    Instead,

    i. Re-configure the Signaling Server with a newly assigned TLAN host IP address that is not in use on the TLAN network.

    ii. Reboot the Signaling Server. Doing so momentarily disrupts applications, such as

    - UNIStim terminal Proxy
    - SIP gateway
    - H.323 gateway

ATTENTION

You must complete step 10 before step 11.

11. **Install the Linux-based Primary NRS server**.

    a. Install the Linux operating system on a COTS stand-alone server.

    There is a bootable CD to install the Linux operating system.

    Note: the VxWorks-based Primary NRS IP address must be assigned as the TLAN IP address of the Primary NRS during installation of the Linux operating system.

    b. Install the NRS and the ECM Backup Security Service. During the installation of the NRS application configure the Solid database server as **Hotstandby primary Solid server**

    The NRS CD contains the NRS and ECM Primary Security Service.

    Refer to *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*, for detailed information on installing the Linux operating system, the ECM framework, the NRS and the ECM Backup Security Service.

12. **Log in to NRS Manager for the Linux-based Primary NRS server**.

    See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).

13. **Restore the VxWorks-based NRS database** backed up in step 7. See the procedures in "Restoring the database" (page 266) to restore an NRS Release 5.0, 4.5 or 4.0 database. See "GK/NRS Data Upgrade" (page 273) to restore a 3.0 H.323 Gatekeeper.

    ATTENTION
    Restoring the previous release database should always be followed by cross checking changes in the Primary and Secondary NRS Server settings (see Figure 49 "Edit Server Configuration web page" (page 156)) and saving them in the new restored database.

14. To ensure that the correct database file has been restored and that it looks similar to the database that was backed up in step 7, review the restored database.

    Follow Linux-based procedures to:

    Procedure 27 "Viewing the Gateway Endpoints" (page 208)

    Procedure 41 "Viewing the Routing Entries" (page 234)

    Procedure 22 "Viewing a Collaborative Server" (page 195)

    Procedure 36 "Viewing the User Endpoints" (page 225)

15. **Configure the Linux-based Primary server settings**. See Procedure 6 "Configuring the Primary and Secondary NRS Server Settings" (page 155).

    - Assign the IP address of the VxWorks-based Primary NRS server to the Linux-based Primary NRS server. Assign the IP address of the VxWorks-based Alternate NRS server to the Linux-based Secondary NRS server. Choose **Primary** from the **server role** drop down list. See Figure 49 "Edit Server Configuration web page" (page 156).
    - If the IP network NRS zone contains H.323 endpoints, configure H.323 Gatekeeper settings. See Figure 50 "H.323 Gatekeeper Settings section" (page 157).
    - Configure SIP Server settings. See Figure 51 "SIP Server Settings section" (page 159).
    - Configure Network Connection Server settings. See Figure 53 "Network Connection Server (NCS) Settings section" (page 161).

16. **Start services on the Primary NRS server.**

    In the **NRS Manager Navigator** select **System > NRS Server**. The **NRS Server** web page opens, as shown in Figure 42 "NRS Server web page" (page 148). Click the **Restart** button on the **Service Status** pane of the **NRS Server** web page.

After services are started the Primary NRS will respond to polling and registration requests.

17. **Monitor the SIP gateway, H.323 gateway and user endpoints** on the Linux-based IP Peer network to ensure that they have registered with the Linux-based Primary NRS server.

    Follow the Linux-based procedures:

    Procedure 27 "Viewing the Gateway Endpoints" (page 208).

    Procedure 36 "Viewing the User Endpoints" (page 225)

    All gateways and end points should have registered with the Linux-based Primary NRS within five minutes.

    Carefully note which endpoints are registered and which endpoints are not registered.

    Compare this list of registered endpoints with the list of registered endpoints in step 5 to ensure that all SIP endpoints that were registered to the VxWorks-based NRS are now registered to the Linux-based Primary NRS.

18. **Disconnect the existing VxWorks-based Alternate NRS from the enterprise network.**

    a. If the VxWorks-based Alternate NRS server is in stand-alone mode (that is not co-resident with Signaling Server applications), disconnect it from the enterprise network and connect the Linux-based Secondary NRS server to the enterprise network.

    b. If a Signaling Server is co-resident with the VxWorks-based Alternate NRS do not disconnect the VxWorks-based Alternate NRS from the enterprise network.

       Instead,

       i. Re-configure the Signaling Server with a newly assigned TLAN host IP address that is not in use on the TLAN network.

       ii. Reboot the Signaling Server. Doing so momentarily disrupts applications, such as

           - UNIStim terminal Proxy
           - SIP gateway
           - H.323 gateway

ATTENTION

Complete step 18 before step 19.

ATTENTION

The IP Peer network will have a Linux-based Primary NRS server without a Linux-based Secondary NRS server or a VxWorks-based Alternate server deployed between the completion of step 19 and the completion of step 23. The network should not be left in this configuration. Coordinate the completion of the tasks in step 19 and step 23, to ensure that the network is not left in this configuration for a long period of time.

19. **Install the Linux-based Secondary NRS server**.

    a. Install the Linux operating system on a COTS stand-alone server.

       There is a bootable CD to install the Linux operating system.

       > ***Note:*** the VxWorks-based Alternate NRS IP address must be assigned as the TLAN IP address of the Secondary NRS during installation of the Linux operating system.

    b. Install the NRS as an ECM security domain member, that is, without the ECM Primary or Backup Security service. The Secondary NRS will be a security client of the ECM Primary and Backup Security servers. During the installation of the NRS application configure the Solid database server as **Hotstandby secondary Solid server.**

       The NRS CD contains the NRS application.

       Refer to *Linux Platform Base and Applications Installation and Commissioning (NN43001-315))*, for detailed information on installing the Linux operating system, the ECM framework and the NRS.

20. **Log in to NRS Manager for the Secondary NRS server.** See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).

21. **Configure the Linux-based Secondary server settings**. See Procedure 6 "Configuring the Primary and Secondary NRS Server Settings" (page 155).

    - Assign the IP address of the VxWorks-based Primary NRS server to the Linux-based Primary NRS server. Assign the IP address of the VxWorks-based Alternate NRS server to the Linux-based Secondary NRS server. Choose **Secondary** from the **server role** drop down list. See Figure 49 "Edit Server Configuration web page" (page 156).
    - If the IP network NRS zone contains H.323 endpoints, configure H.323 Gatekeeper settings. See Figure 50 "H.323 Gatekeeper Settings section" (page 157).
    - Configure SIP Server settings. See Figure 51 "SIP Server Settings section" (page 159).

- Configure Network Connection Server settings. See Figure 53 "Network Connection Server (NCS) Settings section" (page 161).

22. **Start services on Secondary NRS server.**

    In the **NRS Manager Navigator** select **System > NRS Server**. The **NRS Server** web page opens, as shown in Figure 42 "NRS Server web page" (page 148). Click the **Restart** button on the **Service Status** pane of the **NRS Server** web page.

    Both the Linux-based Primary and Secondary NRS are in service. The endpoints should remain registered to the Primary NRS server. The Solid database synchronization link should be established between the Primary and Secondary NRS servers. The Solid databases on the Primary and Secondary servers should synchronize automatically.

23. **Ensure Linux-based Primary and Secondary NRS servers are synchronizing.**.

    To ensure the NRS servers are synchronizing

    - Log onto the Primary NRS Manager. See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).
    - View the Gateway Endpoints on the Active Database. See Procedure 27 "Viewing the Gateway Endpoints" (page 208).
    - Note the number of Gateway Endpoints.
    - View the User Endpoints on the Active Database. See Procedure 36 "Viewing the User Endpoints" (page 225).
    - Note the number of User Endpoints
    - Log onto the Secondary NRS Manager. See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).
    - View the Gateway Endpoints on the Active Database. See Procedure 27 "Viewing the Gateway Endpoints" (page 208).
    - Note the number of Gateway Endpoints
    - View the User Endpoints on the Active Database. See Procedure 36 "Viewing the User Endpoints" (page 225).
    - Note the number of User Endpoints
    - If the number of endpoints on the Primary NRS and the Secondary NRS databases are the same, then the databases are synchronized.

End of task summary for upgrade procedure.

New NRS IP address assignments upgrade procedure

1. Backup the VxWorks-based NRS (Release 4.0, 4.5 or 5.0) or H.323 Gatekeeper database. See "Backing up the database" (page 357).

2. Install and configure the Linux-based NRS Primary and Secondary servers with the new IP addresses. See "Introduction" (page 112) and "Installation of Linux operating system, ECM framework and NRS application" (page 113).

   This step has four substeps:

   a. Install the Linux operating system on a COTS stand-alone server. There is a bootable CD to install the Linux operating system.

   b. Install the Primary and Secondary NRS, the Primary Security Service and the Backup Security Service.

   c. Add the NRS Manager for the Primary and Secondary NRS servers as managed elements of the ECM.

   d. Create user accounts and assign roles and permissions for access to the Primary and Secondary NRS servers from the ECM.

   Refer to *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)*, for detailed information on installing the Linux operating system, the ECM framework and the NRS.

   Refer to *Enterprise Common Manager Fundamentals (NN43001-116)*, for detailed information on adding a managed element to the ECM, creating user accounts, and assigning roles and permissions for access to the NRS servers from the ECM.

3. **Log in to NRS Manager.** See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).

4. **Assign the new IP addresses to the Primary and Secondary NRS servers.** See Procedure 6 "Configuring the Primary and Secondary NRS Server Settings" (page 155).

   ATTENTION

   The primary and secondary NRS servers must be configured one by one. The user ***must*** be logged on the specific (either primary or secondary) server to configure it. See Step 4 of Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).

5. Restore the VxWorks-based NRS database backed up in step 1. If a Succession 3.0 H.323 Gatekeeper database is being restored see "GK/NRS Data Upgrade" (page 273). If an NRS Release 4.0, 4.5 or 5.0 database is being restored follow the procedures in "Restoring the database" (page 266).

> **ATTENTION**
> Restoring the previous release database should always be followed by cross checking changes in the Primary and Secondary NRS Server settings (see Figure 49 "Edit Server Configuration web page" (page 156)) and saving them in the new restored database.

6. **Start services.**

   In the **NRS Manager Navigator** select **System > NRS Server**. The **NRS Server** web page opens, as shown in Figure 42 "NRS Server web page" (page 148). Click the **Restart** button on the **Service Status** pane of the **NRS Server** web page.

7. Re-configure all endpoints to target the new IP addresses of the Primary and Secondary NRS servers.

> **ATTENTION**
> Re-configuring the endpoints to target the new IP addresses of the Primary and Secondary NRS servers interrupts the NRS service for parts of the IP Peer Network.

> **ATTENTION**
> Follow the "Nortel recommendation for load-balancing across the Primary and Secondary Linux-based NRS servers" (page 118) when re-configuring the **gateway** endpoints.

   a. See the Element Manager procedure in *IP Peer Networking Installation and Commissioning (NN43001-313)* to re-configure H.323 gateway endpoints.

   b. See the Element Manager procedure in *IP Peer Networking Installation and Commissioning (NN43001-313)* to re-configure SIP gateway endpoints.

   c. See Procedure 23 "Editing a Collaborative Server" (page 196) to re-configure collaborative servers.

   d. See BCM product documentation to re-configure BCM endpoints.

   e. See MCS 5100 product documentation to re-configure MCS 5100 endpoints.

   f. See *Nortel Converged Office Implementation Guide (NN43001-525)* to re-configure Nortel Multimedia Convergence Manager (MCM).

   g. Consult the manufacturer’s documentation to re-configure third party SIP phones .

End of task summary for upgrade procedure.

Recovery from failure of Linux-based NRS

To recover from a failure of Linux-based NRS

1. **Download** the latest **backup log** and the latest **backup file**.
   - See Procedure 64 "Downloading the latest backup log file" (page 265).
   - See Procedure 63 "Downloading the latest backup file" (page 263).
2. **Restore NRS database.**
   - See "Restoring the database" (page 266).

Operation and maintenance of Linux-based NRS

> **ATTENTION**
>
> A policy should be in place for automatic and manual backup of the NRS database. See Procedure 61 "Automatically backing up the database" (page 261) and Procedure 62 "Manually backing up the database" (page 262).

Access to NRS CLI commands

To access NRS CLI commands:

- Use a SSH client to log into the Linux-based NRS **nortel**l account. The **nortel** account password is set during the installation of the Linux operating system.
- Gatekeeper maintenance:

  To start the Operation, Administration, and Maintenance oam shell type the full pathname to the oam script

  ```
  /opt/nortel/gk/bin/oamShell
  ```

  To start the Problem Determination Tools pdt shell type the full pathname to the pdt shell script

  ```
  /opt/nortel/gk/bin/pdtShell
  ```

- To manually invoke Failsafe NRS database synchronization type in the full pathname to the database synchronization script

  ```
  /opt/nortel/sps/scripts/failsafe.pl main
  ```

SIP Proxy

Linux Commands

The following Linux commands are helpful in diagnosing SIP Proxy application issues:

- traceroute
- free

- ipcs
- ldconfig
- ping
- netstat
- ifconfig

Each of the above commands is described in the Linux man pages.

SIP Proxy Command

The syntax of the SIP Proxy `spcmd` command is:

usage: spcmd [cmd family] [[parameter <value>]...]

synopsis: spcmd -[H|L|O|R|S|V] -[s|t|u|v <defined value>]...

Table 23
spcmd Command Description

Family	Parameter	Description
-L	-v debug | info | all	Write debug, info, or all (i.e. both) logs in addition to the sipLogFile.
	-s on | off	Turn on/off the log types listed by the -v parameter. If no parameter is given, the default is set to on. Default is on.
-O	-v 400 | 401 | 407 | hw | ss	Display OM report for 400, 401, 407, or 3XX responses as well as the high water (hw) mark for internal queue memory usage and the number of SIP sessions (ss) that have been established.
-R	-s force | wait | now -t now | 1..99 -u min | sec	Execute a shutdown and restart of the application immediately or in some given time unit (min\sec) whether call are executing or not by either forcing the application or waiting for call processing to stop.

-S	-s force | wait -t now | 1..99 -u min | sec	Execute a switching of activity from the running application processing to stop where a timer value can be given.
- V	-v app | stack | all	Show the version of the application, oSIP stack, or both.

Table 24
Script Commands

Name	Parameters	Description
chkreg	None	Display endpoint registration information
gwshow	None	Display of Endpoint information
l0dshow	None	Display level 0 domain information
l1dshow	None	Display level 1 domain information
qyshow	None	Display routing query entry information
ryshow	None	Display routing entry information
sdmshow	None	Display service domain information
urshow	None	Display user domain information
failsafe.pl	None	Execute the failsafe sync immediately

NRS Application Monitor Subsystem

MONIT is an open source package used for monitoring the important daemon services automatically initiated at startup. If a malfunction occurs, MONIT provides actions such as alert, start, stop, and restart. In order to provide these actions, applications must be registered with MONIT, and the appropriate actions for each application must be specified.

The SIP Proxy application will be registered with the MONIT application upon installation and startup of the application. MONIT will query the applications and processes related to the SIP Proxy and determine if the application must be shutdown or restarted.

H.323 Gatekeeper

There are no functional changes in the H.323 Gatekeeper CLI commands in CS 1000 Rls 5.0, as compared with CS 1000 Rls 4.5.

Operation, Administration, and Maintenance oam commands

Gatekeeper

- gkDiscoveryTrace
- gkRegTrace
- gkCallTrace
- gkProtocolTrace
- gkTraceOff
- gkTraceOutput
- gkTraceSettings
- gkTraceTblClear
- gkTraceTblShow

nrsDB

- nrsGWEndpointShow
- nrsUserEPShow
- nrsCollaboratingServerShow
- nrsL0DomainShow
- nrsL1DomainShow
- nrsRoutingEntryShow
- nrsServiceDomainShow
- nrsCollaboratingServerQuery
- nrsGWEndpointQuery
- nrsUserEPQuery
- nrsL0DomainQuery
- nrsL1DomainQuery
- nrsServiceDomainQuery
- nrsDefaultRouteQuery
- nrsDBShow
- nrsDBSyncForce
- nrsDBStateShow

nrsomm

- NrsOmmShow
- NrsOmmAvShow

System

- swVersionShow

Problem Determination Tools pdt commands

Gatekeeper

- gkDiscoveryTrace
- gkRegTrace
- gkCallTrace
- gkProtocolTrace
- gkTraceOff
- gkTraceOutput
- gkTraceSettings
- gkTraceTblClear
- gkTraceTblShow

nrsDB

- nrsGWEndpointShow
- nrsUserEPShow
- nrsCollaboratingServerShow
- nrsL0DomainShow
- nrsL1DomainShow
- nrsRoutingEntryShow
- nrsServiceDomainShow
- nrsCollaboratingServerQuery
- nrsGWEndpointQuery
- nrsUserEPQuery
- nrsL0DomainQuery
- nrsL1DomainQuery
- nrsServiceDomainQuery
- nrsDefaultRouteQuery

- nrsDBShow
- nrsDBSyncForce
- nrsDBStateShow
- disNRS
- forcedisNRS
- enlNRS
- nrsGKTestQuery
- nrsSIPTestQuery

nrsomm

- NrsOmmShow
- NrsOmmAvShow

System

- syslogShow
- syslogLevelSet
- swVersionShow

Solid database commands

Database link synchronization

To ensure Linux-based Primary and Secondary database servers are synchronizing

- Log in to the **`nortel`** account on the Primary NRS server.

  To Log in to the nortel account access the Linux command line through a telnet or SSH client, or locally attach an EIA232 terminal to the COM port.

  The **`nortel`** account password is set during the installation of the Linux operating system.

- Run the command **`/opt/nortel/solid/bin/hsbchk`** from the Linux command line.

  The Primary and Secondary databases are in the process of synchronizing, if the state of the Primary database server is `"PRIMARY ACTIVE"`.

  The link between the database servers may be down and the databases may not be synchronizing, if the state of the database server is `"PRIMARY ALONE"`.

Failsafe NRS Synchronization

The Failsafe NRS synchronization script provides a manual command to invoke Failsafe NRS synchronization immediately, instead of waiting up to 6 hours for the Linux cron to invoke the scheduled Failsafe NRS synchronization. To manually invoke Failsafe NRS database synchronization type in the full pathname to the database synchronization script

```
/opt/nortel/sps/scripts/failsafe.pl main
```

Browser configuration

ATTENTION

Nortel discourages use of the Back, Forward, and Refresh buttons of the browser.

Use of the Back button is not recommended while the NRS Manager application is launched, because NRS Manager pages contain dynamic data content. NRS Manager provides a path for navigation purposes on top of every NRS Manager page.

Nortel recommends that the user click the navigation path to go back to the previous page (instead of using the Back button).

Configure the browser and display settings

Before you can use NRS Manager, the following tasks must be completed:

- Enable popups in the browser search utility (mandatory).
- Configure the Internet Explorer browser settings (mandatory).
- Configure the Windows Display settings (highly recommended).

  Note: The interface for the Internet Explorer browser settings and Windows Display settings may vary by browser version and by operating system.

Enable popups

If you are using a browser search utility (such as the GoogleTM search engine or the Yahoo!TM search engine), ensure that popups are enabled. Enabling pop-up windows is usually done at the search utility’s toolbar.

ATTENTION

Do not block pop-up windows if you are using a search utility (such as GoogleTM or Yahoo!TM search engines) in your browser.

Configure the browser settings

See Procedure 2 "Configure the Internet Explorer browser settings" (page 144) to configure the following Internet Explorer browser settings:

- Browser retrieve page information.

- Empty session information.
- Deselect the AutoComplete options.

Procedure 2
Configuring the Internet Explorer browser settings

Step	Action
1	Select **View > Text Size > Medium** to configure text size in the browser.
2	Select **Tools > Internet Options** in the Internet Explorer browser window. The **Internet Options** window opens.
3	Configure the browser retrieve page information: a. On the **General** tab under the **Temporary Internet files** section, click **Settings**. The **Settings** window opens. b. Under the **Check for newer versions of stored pages** section, select the **Every visit to the page** option. c. Click **OK**.
4	Configure the empty session information: a. Select the **Advanced** tab. b. Under **Security**, select **Empty Temporary Internet Files folder when browser is closed**.
5	Deselect the AutoComplete options. a. Select the **Content** tab. b. Under **Personal Information**, click **AutoComplete**. The **AutoComplete Settings** window opens. c. Under the **Use AutoComplete for** section, deselect **Forms** and **User names and passwords on forms**. Click **OK** (to close the **AutoComplete Settings** window) Click **OK** (to close the **Internet Options** window)

—End—

Configure the Windows Display settings

See Procedure 3 "Configuring the Windows Display settings" (page 145) to configure the Windows display settings.

Procedure 3
Configuring the Windows Display settings

Step	Action
1	Select **Start > Settings > Control Panel > Display**. The **Display Settings** window opens.
2	Select the **Settings** tab.
3	Select **True Color (32 bit)** from the **Colors** drop-down list.
4	Under **Screen area**, select **1280 by 1024 pixels**.
5	Click **OK**.

—End—

Log in to ECM and Access NRS Manager

Access NRS Manager through the ECM . See Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).

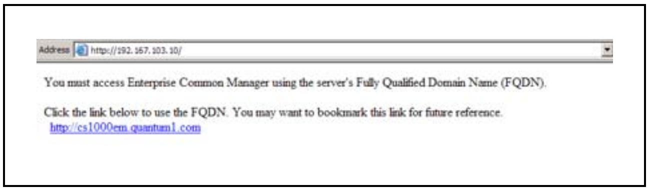
Two types of access privileges are supported:

- Administrative privileges — Administrators have full read/write privileges. An administrator can view and modify NRS configuration data.
- Monitor privileges — Monitors have read-only privileges. A Monitor can only view the NRS configuration data.

Procedure 4
Logging in to ECM and Accessing NRS Manager

Step	Action
1	Access the ECM using the Fully Qualified Domain Name (FQDN) of an ECM server that is a member of the security domain that the NRS server is a member of. ***Note:*** The link to the FQDN of the ECM server can be bookmarked in the Internet Explorer Favorites list. See Figure 37 "Link to FQDN" (page 146).

Figure 37
Link to FQDN



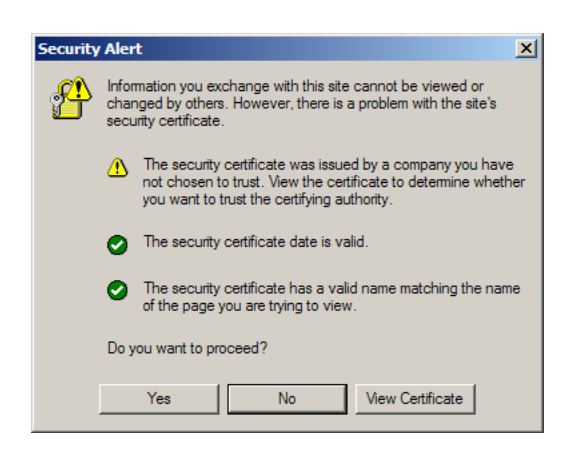
Address http://192.167.103.10/

You must access Enterprise Common Manager using the server's Fully Qualified Domain Name (FQDN).

Click the link below to use the FQDN. You may want to bookmark this link for future reference.
http://cs1000em.quantum1.com

The Security Alert web page opens. See Figure 38 "Security Alert web page" (page 146). Click the **Yes** button.

Figure 38
Security Alert web page



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

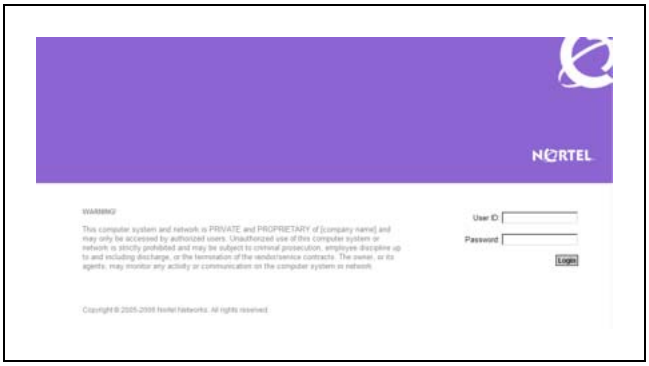
✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

2 The ECM log in web page opens. See Figure 39 "ECM log in web page" (page 146).

Figure 39
ECM log in web page



WARNING!

This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network.

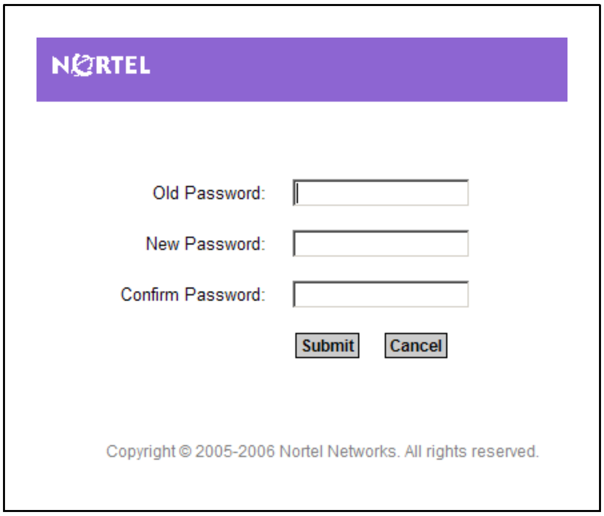
User ID:
Password:

Copyright © 2005-2006 Nortel Networks. All rights reserved.

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

If this is your first time logging in, you will prompted to change your password. See Figure 40 "Change Password web page" (page 147).

Figure 40
Change Password web page



Old Password:

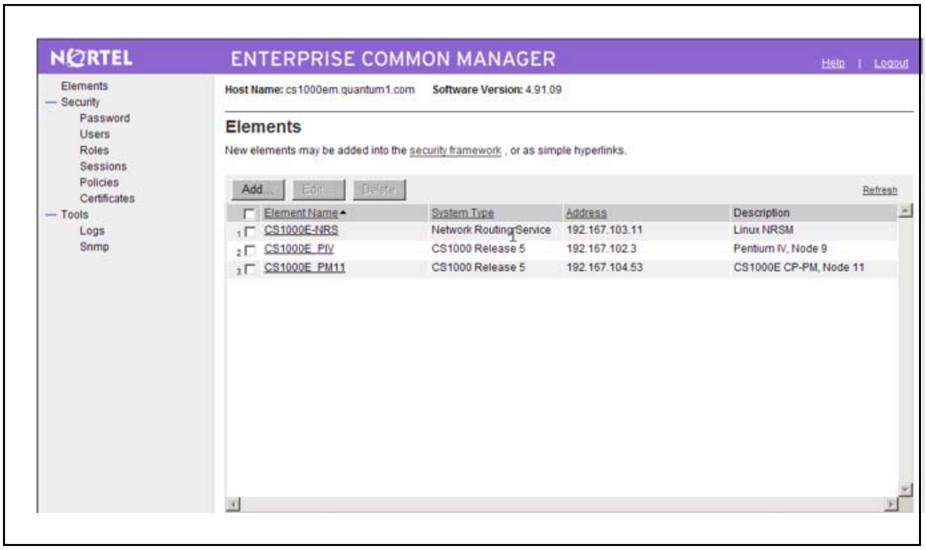
New Password:

Confirm Password:

Copyright © 2005-2006 Nortel Networks. All rights reserved.

3 The ECM Elements web page opens. See Figure 41 "ECM Elements web page" (page 147). Click the link to the NRS Manager in the **Element Name** column.

Figure 41
ECM Elements web page



Host Name: cs1000em.quantum1.com Software Version: 4.91.09

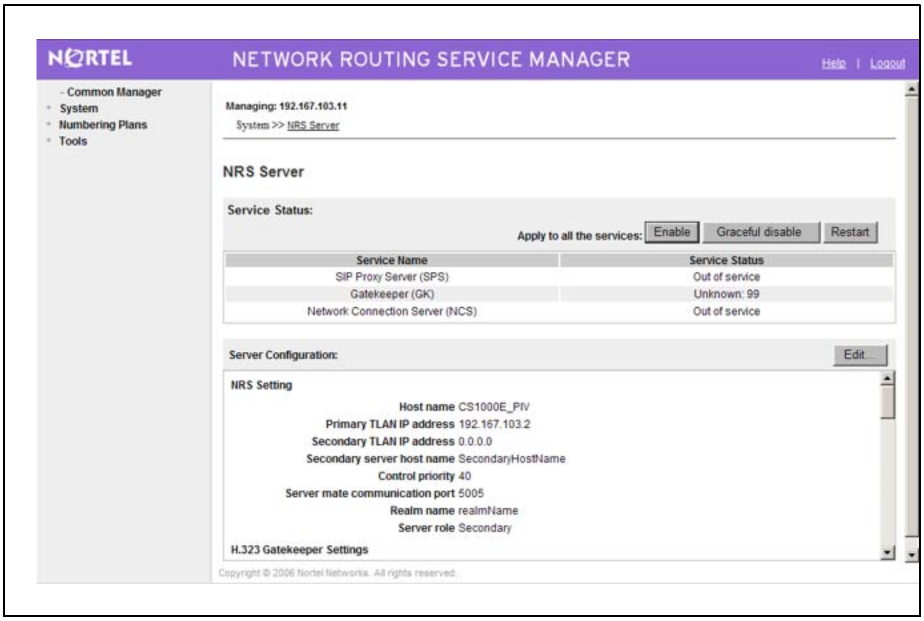
Elements

New elements may be added into the security framework , or as simple hyperlinks.

	Element Name	System Type	Address	Description
1 □	CS1000E-NRS	Network Routing Service	192.167.103.11	Linux NRSM
2 □	CS1000E_PIV	CS1000 Release 5	192.167.102.3	Pentium IV, Node 9
3 □	CS1000E_PM11	CS1000 Release 5	192.167.104.53	CS1000E CP-PM, Node 11

4 The NRS server web page opens, as shown in Figure 42 "NRS Server web page" (page 148).

Figure 42
NRS Server web page



Managing: 192.167.103.11

NRS Server

Service Status:

Apply to all the services:

Service Name	Service Status
SIP Proxy Server (SPS)	Out of service
Gatekeeper (GK)	Unknown: 99
Network Connection Server (NCS)	Out of service

Server Configuration:

NRS Setting

Host name CS1000E_PIV
Primary TLAN IP address 192.167.103.2
Secondary TLAN IP address 0.0.0.0
Secondary server host name SecondaryHostName
Control priority 40
Server mate communication port 5005
Realm name realmName
Server role Secondary

H.323 Gatekeeper Settings

Copyright © 2006 Nortel Networks. All rights reserved.

—End—

NRS Manager interface

NRS Manager Navigator

The **NRS Manager Navigator**, located on the left side of the NRS Manager web pages, contains links to other web pages. **Common Manager**, the root of the NRS Manager Navigator, is a link to the ECM web page. The **NRS Manager Navigator** is comprised of three main branches: **System**, **Numbering Plans**, and **Tools**. See Figure 42 "NRS Server web page" (page 148).

The **System** branch contains links to

- NRS Server
- Database
- System Wide Settings

The **Numbering Plans** branch contains links to

- Domains (Service, L1 and L0 Domains)
- Endpoints (Gateway and User Endpoints)
- Routes
- Network Post-Translation

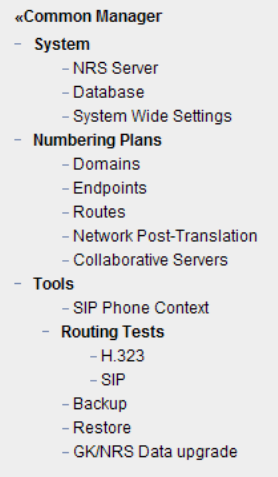
- Collaborative Servers

The **Tools** branch contains links to

- SIP Phone Context
- H.323 Routing Test
- SIP Routing Test
- (Database) Backup
- (Database) Restore
- GK/NRS Data upgrade

In Figure 43 "NRS Manager Navigator" (page 149), the NRS Manager Navigator is expanded to display all available links.

Figure 43
NRS Manager Navigator



Navigation of NRS Manager web pages

There are three navigation areas in NRS Manger web pages:

1. **NRS Manager Navigator**

   The NRS Manger navigation tree, shown in Figure 43 "NRS Manager Navigator" (page 149), is located on the left side of NRS Manger web pages. It contains links to other web pages. The web pages are opened by clicking a branch of the NRS Manger navigation tree.

2. **Navigation Path**.

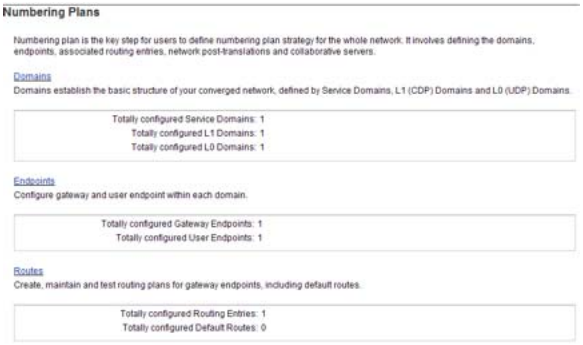
   The navigation path is located at the top of NRS Manger web pages. For example, to add an L0 Domain open the **Add L0 Domain** web page shown in Figure 75 "Add L0 Domain web page" (page 182). The navigation path for this web page is **Numbering Plans >> Domains >>**

L0 Domain. To open a parent web page click on a link in the navigation path.

3. **Numbering Plans web pages**.

   The **Numbering Plans** web page shown in Figure 44 "Numbering Plans web page" (page 150), contains links to Domain, Endpoints, Routes, Network Post-Translation and Collaborative Servers web pages. Click on a link to open a web page.

Figure 44
Numbering Plans web page



Numbering Plans

Numbering plan is the key step for users to define numbering plan strategy for the whole network. It involves defining the domains, endpoints, associated routing entries, network post-translations and collaborative servers.

Domains

Domains establish the basic structure of your converged network, defined by Service Domains, L1 (CDP) Domains and L0 (UDP) Domains.

Totally configured Service Domains: 1
Totally configured L1 Domains: 1
Totally configured L0 Domains: 1

Endpoints

Configure gateway and user endpoint within each domain.

Totally configured Gateway Endpoints: 1
Totally configured User Endpoints: 1

Routes

Create, maintain and test routing plans for gateway endpoints, including default routes.

Totally configured Routing Entries: 1
Totally configured Default Routes: 0

Each of the Numbering Plans component summary web pages contain links to other web pages. For example, the **Service Domains** web page, shown in Figure 58 "Service Domains pane" (page 166), contains columns entitled # of L1 Domains, # of L0 Domains, and # of Gateway Endpoints. Click on one of the links in those columns to go to the associated subcomponent summary page of a Service Domain.

Navigation examples

1. Go from **Add L0 Domain** web page to **Service Domains** web page.

   a. In the **NRS Manager Navigator** select **Numbering Plans > Domains.**

   Or

   b. Click on **Domains** in the **Numbering Plans >> Domains >> L0 Domain** navigation path.

2. Add a Gateway endpoint

   a. In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.**

   b. Ensure **Standby database** is selected.

   c. The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service

Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

d. Click the **Gateway Endpoints** button.

e. Click the **Add....** button.

Or

3. Add a Gateway endpoint from

- **Service Domains** web page shown in Figure 58 "Service Domains pane" (page 166).

  or

- **L1 Domains** web page shown in Figure 66 "L1 Domains (UDP) pane" (page 173).

  or

- **L0 Domains** web page shown in Figure 74 "L0 Domain (CDP) pane" (page 181).

a. Ensure **Standby database** is selected.

b. Click a link in the **# of Gateway Endpoints** column.

c. Select correct domain path from the **Limit results to Domain:** drop-down lists.

d. Click the **Add....** button.

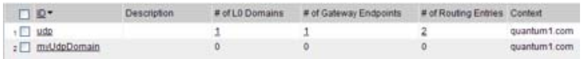
NRS Manager features

1. **Sort Numbering Plans** web pages by ascending or descending order.

   - The **ID** column in the Service Domains, L1 Domains, L0 Domains, Gateway Endpoints and User Endpoints web pages can be sorted by ascending or descending alphabetical order.
   - The **DN Prefix** column in the Routing Entries web page can be sorted by ascending or descending numerical order.
   - The **DN type** column in the Default Routes web page can be sorted by ascending or descending alphabetical order.
   - The **Originating Endpoint** column in the Network Post-Translation web page can be sorted by ascending or descending alphabetical order
   - The **Server Fully Qualified Domain** column in the Collaborative Servers web page can be sorted by ascending or descending alphabetical order.

Click on the column link to invert the sort order on the Numbering Plans web page. The Service Domains shown in Figure 45 "Descending Alphabetical sort order" (page 152) are sorted in descending alphabetical order.

Figure 45
Descending Alphabetical sort order



	□	ID▾	Description	# of L0 Domains	# of Gateway Endpoints	# of Routing Entries	Context
1	□	udp		1	1	2	quantum1.com
2	□	myUdpDomain		0	0	0	quantum1.com

2. **Filter by Domain**

   - The L1 Domains for all Service Domains can be displayed in the **L1 Domains (UDP)** web page. Or the L1 Domains for a specific Service Domain can be displayed in the **L1 Domains (UDP)** web page by selecting the Service Domain from the **Filter by Domain:** drop-down list.
   - The L0 Domains for all Service Domains and all L1 Domains can be displayed in the **L0 Domains (UDP)** web page. Or the L0 Domains for a specific Service Domain and/or L1 Domain can be displayed in the **L0 Domains (UDP)** web page by selecting the Service Domain and/or L1 Domain from the **Filter by Domain:** drop-down lists.
   - The Network Post-translations for all Service Domains can be displayed in the **Network Post-Translation** web page. Or the Network Post-translations for a specific Service Domain can be displayed in the **Network Post-Translation** web page by selecting the Service Domain from the **Filter by Domain:** drop-down list.

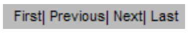
3. **Limit results to Domain**

   - The Gateway and User Endpoints for all Service Domains and all L1 Domains and all L0 Domains can be displayed in the **Endpoints** web page. Or the Gateway and User Endpoints for a specific Service Domain and/or L1 Domain and/or L0 Domain can be displayed in the **Endpoints** web page by selecting the Service Domain and/or L1 Domain and/or L0 Domain from the **Limit results to Domain** drop-down lists.
   - Routing entries for all Service Domains and all L1 Domains and all L0 Domains and all Gateway Endpoints can be displayed in the **Routing Entries** and **Default Routes** web pages. Or the Routing entries for a specific Service Domain and/or L1 Domain and/or L0 Domain and/or Gateway Endpoint can be displayed in the **Routing Entries** web page by selecting the Service Domain and/or L1 Domain and/or L0 domain from the **Limit results to Domain** drop-down lists and/or the Gateway Endpoint from the **Endpoint Name:** drop-down list.

4. **Pagination**

The entries tabulated on the Service Domains, L1 Domains (UDP), L0 Domains (CDP), Gateway and User Endpoints, Routing Entries and Default Routes, Network Post-Translation and Collaborative Servers web pages may not fit on one page. Navigate to the First, Previous, Next or Last page by using the pagination links on the right side of the web page footer, shown in Figure 46 "Pagination" (page 153).

Figure 46
Pagination



First| Previous| Next| Last

Mandatory fields on NRS Manager web pages

Mandatory fields on NRS Manger web pages are denoted by an *. All other fields on NRS Manager web pages are optional.

Numbering Plans inherited fields

The NRS database provides a central database of addresses that are required to route calls across the network. The NRS uses the hierarchical model outlined in Table 2 "Hierarchical model of the Network Routing Service" (page 29) to store an organize information in the database. In this hierarchical model

- an L1 domain is a subdomain of a Service domain
- an L0 domain is a subdomain of an L1 domain
- Gateway and User endpoints exist within an L0 domain
- a Routing entry represents a range of addresses (URIs) where a gateway can terminate calls. A routing entry exists within a Gateway

In provisioning the NRS, an L1 domain, an L0 domain and a Gateway endpoint can inherit configuration parameters from its parent. The inherited fields are:

- Endpoint authentication enabled
- Authentication password
- E.164 country code
- E.164 area code
- E.164 international dialing access code
- E.164 international dialing code length
- E.164 national dialing access code
- E.164 national dialing code length
- E.164 local (subscriber) dialing access code
- E.164 local (subscriber) dialing code length

- Private L1 domain (UDP location) dialing access code
- Private L1 domain (UDP location) dialing code length
- Special number
- Special number dialing code length
- Emergency service access prefix

Benefits of inherited fields

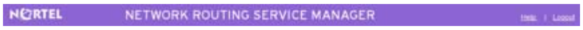
The benefits of inherited fields are:

- An inherited field that is provisioned in a parent component does not have to be explicitly provisioned in sublevel components
- An inherited field can be redefined in a sublevel component with a value that overwrites the value inherited from its parent

Help and Logout links

The **Help** and **Logout** links are located on the right side of the NRS Manager web page header. See Figure 47 "Help and Logout Links" (page 154).

Figure 47
Help and Logout Links



Help link

Select the **Help** link to access the **NRS Manager Help Files**.

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

Logout link

Select the **Logout** link to terminate the current Enterprise Common Manager session. See Procedure 5 "Logging out of ECM " (page 155).

Common Manager link

Select the **Common Manager** link on the **NRS Manager Navigator** to return to the ECM web page without terminating the current ECM session. See "The NRS Manager interface" (page 148).

Log out of ECM

See Procedure 5 "Logging out of ECM " (page 155) to log out of the ECM . Logging out of the ECM terminates the current session.

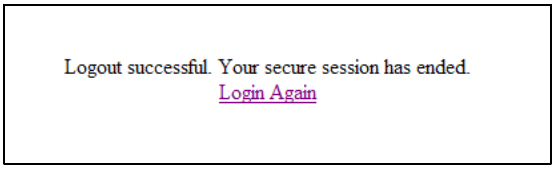
Procedure 5
Logging out of ECM

Step **Action**

1 Click the **Logout** link on the right side of the NRS Manager web page header.

The **Enterprise Common Manager Logout successful** web page opens.

Figure 48
Enterprise Common Manager Logout successful web page



Logout successful. Your secure session has ended.
Login Again

2 Close the browser window.

—End—

Configure the Primary and Secondary NRS Server Settings

The NRS Server Settings comprise:

- NRS Settings: These are generic settings applicable to H.323, SIP, and Network Connection Service.
- H.323 Gatekeeper Settings
- SIP Server Settings
- Network Connection Server (NCS) Settings

> **ATTENTION**
> The primary and secondary NRS servers must be configured one by one. The user ***must*** be logged on the specific (either primary or secondary) server to configure it. See Step 4 of Procedure 4 "Logging in to ECM and Accessing NRS Manager" (page 145).

Procedure 6
Configuring the Primary and Secondary NRS Server Settings

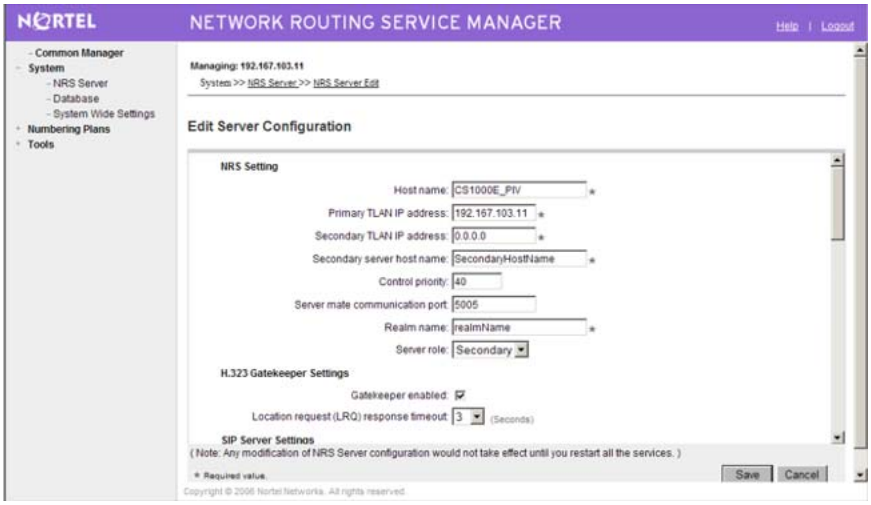
Step **Action**

1 In the **NRS Manager Navigator** select **System > NRS Server**.

The **NRS Server** web page opens, as shown in Figure 42 "NRS Server web page" (page 148).

2 To configure the **NRS Server Settings**, click the **Edit** button in the **Server Configuration** pane of the **NRS Server** web page. The **Edit Server Configuration** web page opens, as shown in Figure 49 "Edit Server Configuration web page" (page 156).

Figure 49
Edit Server Configuration web page



Managing: 192.167.103.11

Edit Server Configuration

NRS Setting

Host name: CS1000E_PIV *
Primary TLAN IP address: 192.167.103.11 *
Secondary TLAN IP address: 0.0.0.0 *
Secondary server host name: SecondaryHostName *
Control priority: 40
Server mate communication port: 5005
Realm name: realmName *
Server role: Secondary

H.323 Gatekeeper Settings

Gatekeeper enabled: ☑
Location request (LRQ) response timeout: 3 (Seconds)

SIP Server Settings

(Note: Any modification of NRS Server configuration would not take effect until you restart all the services.)

* Required value.

Copyright © 2006 Nortel Networks. All rights reserved.

3 Configure the **NRS Server Settings**:

a. **Host name:** Enter the Primary server host name in the text box. The host name must be alphanumeric and can be up to 20 characters in length.

b. **Primary TLAN IP address:** Enter the IP address of the Primary NRS (that is, the TLAN network interface IP address) in the text box. The default is 0.0.0.0.

c. **Secondary TLAN IP address:** Enter the IP address of the Secondary NRS (that is, the TLAN network interface IP address), in the text box. The default is 0.0.0.0.

d. **Secondary server host name:** Enter the Secondary server host name in the text box.

e. **Control priority:** Enter a value for the control priority in the text box. This is a priority bit setting inside the protocol that determines the signaling routing priority. The range is 0 to 63. The default value is 40. The control priority must be a numeric value.

f. **Server mate communication port:** Enter a value for the Server mate communication port in the text box. The Server mate communication port is numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 50005.

g. **Realm name:** Enter a value for the Realm name in the text box. The Realm name is alphanumeric and can be up to 20 characters in length.

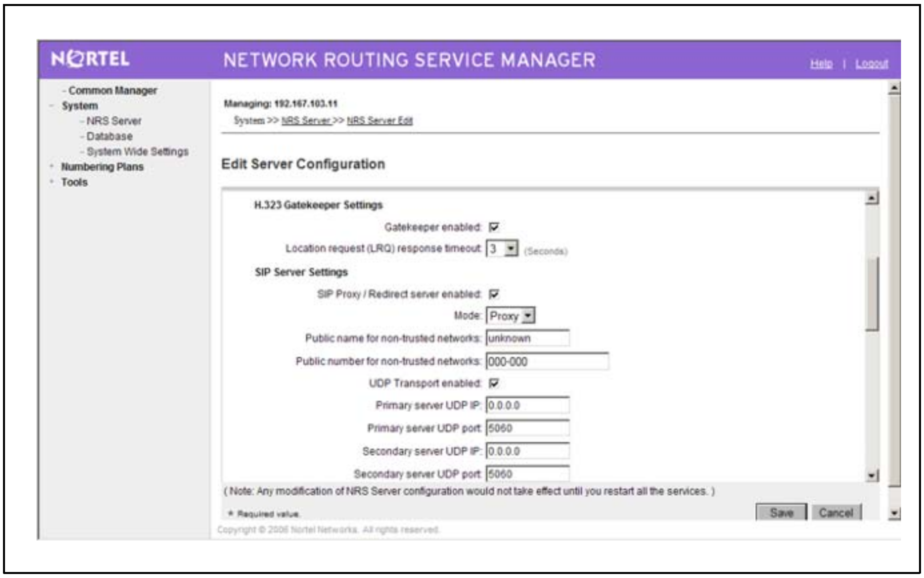
h. **Server role:** Choose **Primary** or **Secondary** from the drop down list.

4 To configure **H.323 Gatekeeper Settings** scroll down to the H.323 Gatekeeper Settings section of the Edit Server Configuration web page. See Figure 50 "H.323 Gatekeeper Settings section" (page 157).

a. Select the **Gatekeeper enabled** box.

b. Set the LRQ response timeout parameter by selecting a value from the **Location request (LRQ) response timeout [Seconds]** drop-down list. The minimum value is 1 second and the maximum value is 10 seconds. The default value is 3 seconds.

Figure 50
H.323 Gatekeeper Settings section



Managing: 192.167.103.11

System >> NRS Server >> NRS Server Edit

Edit Server Configuration

H.323 Gatekeeper Settings

Gatekeeper enabled: ☑

Location request (LRQ) response timeout: 3 (Seconds)

SIP Server Settings

SIP Proxy / Redirect server enabled: ☑

Mode: Proxy

Public name for non-trusted networks: unknown

Public number for non-trusted networks: 000-000

UDP Transport enabled: ☑

Primary server UDP IP: 0.0.0.0

Primary server UDP port: 5060

Secondary server UDP IP: 0.0.0.0

Secondary server UDP port: 5060

(Note: Any modification of NRS Server configuration would not take effect until you restart all the services.)

* Required value.

Copyright © 2006 Nortel Networks. All rights reserved.

5 To configure **SIP Server Settings** scroll down to the SIP Server Settings section of the Edit Server Configuration web page. See Figure 51 "SIP Server Settings section" (page 159).

a. Check the **SIP Proxy / Redirect server enabled** check box.

b. Select **Proxy** from the **Mode** drop-down list. This is the mode of the SIP Server. A SIP Proxy acts as both a server and a client. A SIP Proxy receives requests, determines where to send the requests, and acting as a client on behalf of SIP endpoints passes requests on to another server.

c. Enter **Public name for non-trusted networks** in the text box.

d. Enter **Public number for non-trusted networks** in the text box.

e. Select the transport protocol.

To enable UDP:

1. Select the **UDP transport enabled** check box.
2. Enter the **Primary server UDP IP** in the text box.
3. Enter the **Primary server UDP port** in the text box. The UDP port must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 5060.
4. Enter the **Secondary server UDP IP** in the text box.
5. Enter the **Secondary server UDP port** in the text box. The UDP port must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 5060.
6. Enter the **UDP maximum transmission unit (MTU)** in the text box. MTU is the maximum size of an Ethernet Layer 2 packet going out on the IP network. In this context, MTU is the maximum size of a SIP packet that is sent out on the UDP interface. The default value is 1500 bytes. The maximum value for MTU is 64K. When configuring the MTU, remember that there is a trade-off between packet size and the number of packets that have to be transmitted over the network.

To enable TCP:

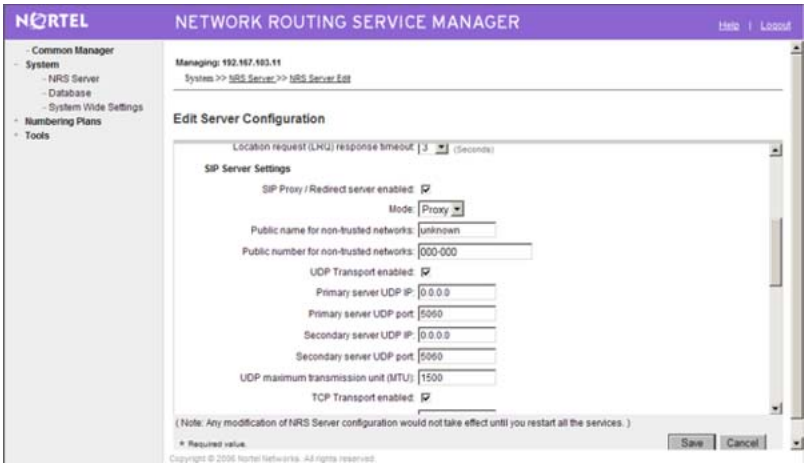
1. Select the **TCP transmission enabled** check box.
2. Enter the **Primary server TCP IP** in the text box.
3. Enter the **Primary server TCP port** in the text box. The TCP port must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 5060.
4. Enter the **Secondary server TCP IP** in the text box.
5. Enter the **Secondary server TCP port** in the text box. The TCP port must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 5060.
6. Enter the **TCP maximum transmission unit (MTU)** in the text box. MTU is the maximum size of an Ethernet Layer 2 packet going out on the IP network. In this context, MTU is

the maximum size of a SIP packet that is sent out on the TCP interface. The default value is 1500 bytes. The maximum value for MTU is 64K. When configuring the MTU, remember that there is a trade-off between packet size and the number of packets that have to be transmitted over the network.

To enable TLS:

1. Select the **TLS transmission enabled** check box.
2. Enter the **Primary server TLS IP** address in the text box.
3. Enter the **Primary server TLS port** in the text box. The TLS port must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 5061.
4. Enter the **Secondary server TLS IP** address in the text box.
5. Enter the **Secondary server TLS port** in the text box. The TLS port must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 5061.
6. Enter the **TLS maximum transmission unit (MTU)** in the text box. MTU is the maximum size of an Ethernet Layer 2 packet going out on the IP network. In this context, MTU is the maximum size of a SIP packet that is sent out on the TLS interface. The default value is 1500 bytes. The maximum value for MTU is 64K. When configuring the MTU, remember that there is a trade-off between packet size and the number of packets that have to be transmitted over the network.

Figure 51
SIP Server Settings section



Managing: 192.167.103.11
System >> NRS Server >> NRS Server Edit

Edit Server Configuration

Location request (LRQ) response timeout: 3 (Seconds)

SIP Server Settings

SIP Proxy / Redirect server enabled: ☑
Mode: Proxy
Public name for non-trusted networks: unknown
Public number for non-trusted networks: 000-000
UDP Transport enabled: ☑
Primary server UDP IP: 0.0.0.0
Primary server UDP port: 5060
Secondary server UDP IP: 0.0.0.0
Secondary server UDP port: 5060
UDP maximum transmission unit (MTU): 1500
TCP Transport enabled: ☑

(Note: Any modification of NRS Server configuration would not take effect until you restart all the services.)

* Required value.

Copyright © 2006 Nortel Networks. All rights reserved.

6 To configure **Transport Layer Security (TLS) Settings** scroll down to the Transport Layer Security (TLS) Settings section of the Edit Server Configuration web page. See Figure 52 "Transport Layer Security (TLS) Settings section" (page 160).

a. Enter **Maximum session cache** in text box.

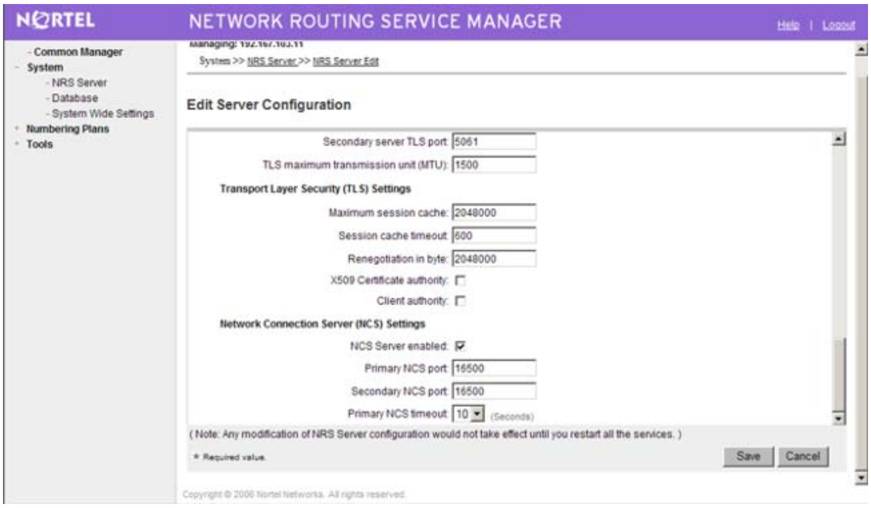
b. Enter **Session cache timeout** in text box.

c. Enter **Renegotiation in byte** in text box.

d. Select the **X509 Certificate authority** check box.

e. Select the **Client authority** check box.

Figure 52
Transport Layer Security (TLS) Settings section



Managing: 192.167.103.11

System >> NRS Server >> NRS Server Edit

Edit Server Configuration

Secondary server TLS port: 5061

TLS maximum transmission unit (MTU): 1500

Transport Layer Security (TLS) Settings

Maximum session cache: 2048000

Session cache timeout: 600

Renegotiation in byte: 2048000

X509 Certificate authority: ☐

Client authority: ☐

Network Connection Server (NCS) Settings

NCS Server enabled: ☑

Primary NCS port: 16500

Secondary NCS port: 16500

Primary NCS timeout: 10 (Seconds)

(Note: Any modification of NRS Server configuration would not take effect until you restart all the services.)

* Required value.

Copyright © 2006 Nortel Networks. All rights reserved.

7 To configure **Network Connection Server (NCS) Settings** scroll down to the Network Connection Server (NCS) Settings section of the Edit Server Configuration web page. See Figure 53 "Network Connection Server (NCS) Settings section" (page 161).

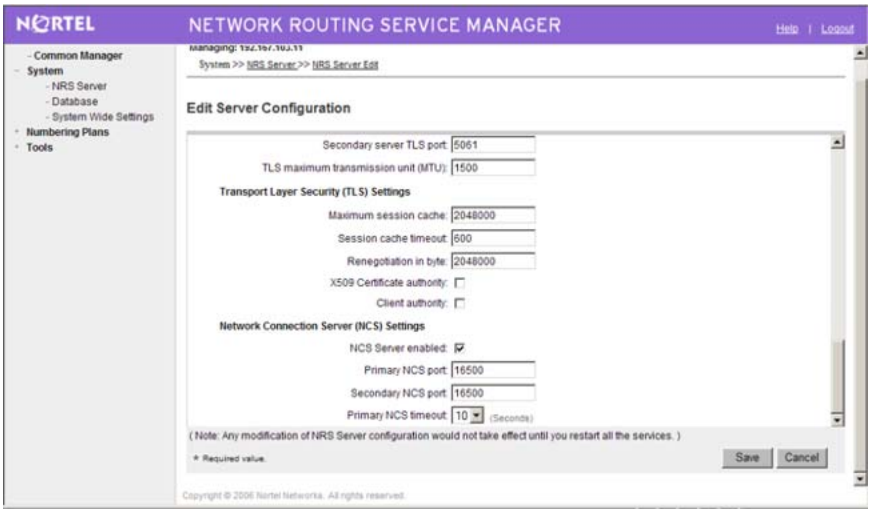
a. **Primary NCS port:** Enter a port number for the Primary NCS in the text box. The port number must be numeric and can be up to five digits in length. The range is 1024 to 65535. The default value is 16500.

b. **Secondary NCS port:** Enter a port number for the Secondary NCS in the text box. The port number must be numeric and up to five digits in length. The range is 1024 to 65535. The default value is 16500.

c. **Primary NCS timeout [Seconds]**: Select a timeout value for the Primary NCS from the drop-down list. The minimum value is 1 second and the maximum value is 30 seconds. The default value is 10 seconds.

Note: The NCS Settings are used for the Branch Office (including the Survivable Remote Gateway [SRG}), Virtual Office, and Geographic Redundancy features.

Figure 53
Network Connection Server (NCS) Settings section



Managing: 192.167.103.11

System >> NRS Server >> NRS Server Edit

Edit Server Configuration

Secondary server TLS port: 5061

TLS maximum transmission unit (MTU): 1500

Transport Layer Security (TLS) Settings

Maximum session cache: 2048000

Session cache timeout: 600

Renegotiation in byte: 2048000

X509 Certificate authority: □

Client authority: □

Network Connection Server (NCS) Settings

NCS Server enabled: ☑

Primary NCS port: 16500

Secondary NCS port: 16500

Primary NCS timeout: 10 (Seconds)

(Note: Any modification of NRS Server configuration would not take effect until you restart all the services.)

* Required value.

Copyright © 2006 Nortel Networks. All rights reserved.

8 Click the **Save** button.

9 The NRS Server web page reopens, as shown in Figure 42 "NRS Server web page" (page 148). Click the **Restart** button on the **Service Status** pane of the **NRS Server** web page.

—End—

Configure system-wide settings

The **System-wide settings** web page is used (1) to configure system-wide settings and (2) to schedule backup jobs. System-wide settings include:

- SIP registration and H.323 Gatekeeper registration Time-to-Live timer settings.
- H.323 Gatekeeper alias name.
- Automatic backup time setting.
- Whether automatic backup to an FTP site is enabled. If enabled, the IP address, path, and username for the FTP site must be provided.

See Procedure 7 "Configuring system-wide settings" (page 162) to configure system-wide settings.

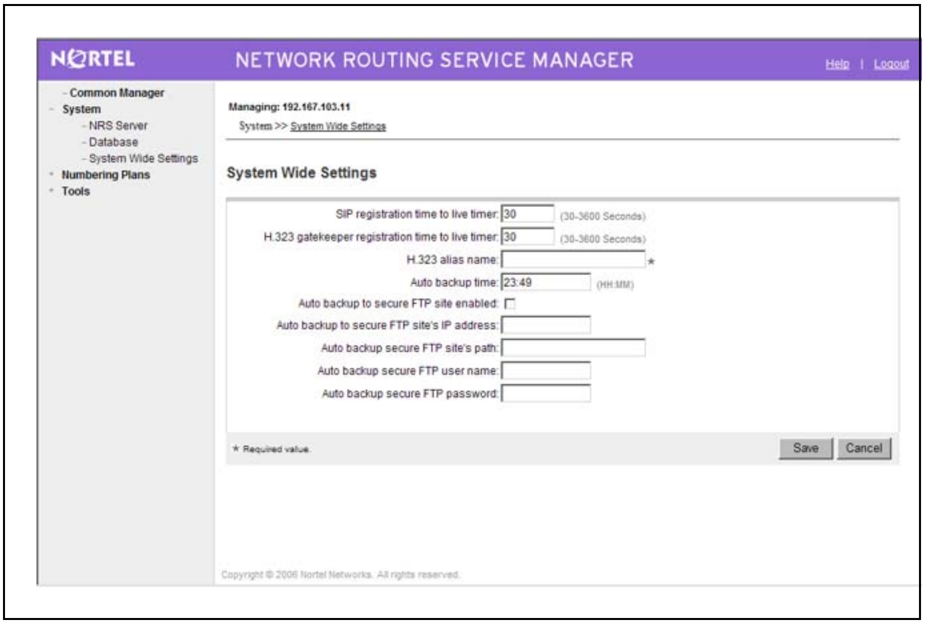
Procedure 7
Configuring system-wide settings

Step	Action

1 In the **NRS Manager Navigator** select **System > System Wide Settings**.

The **System Wide Settings** web page opens. See Figure 54 "System Wide Settings web page" (page 162).

Figure 54
System Wide Settings web page



Managing: 192.167.103.11

System >> System Wide Settings

System Wide Settings

SIP registration time to live timer: 30 (30-3600 Seconds)
H.323 gatekeeper registration time to live timer: 30 (30-3600 Seconds)
H.323 alias name: *
Auto backup time: 23:49 (HH:MM)
Auto backup to secure FTP site enabled: □
Auto backup to secure FTP site's IP address:
Auto backup secure FTP site's path:
Auto backup secure FTP user name:
Auto backup secure FTP password:

* Required value.

Copyright © 2006 Nortel Networks. All rights reserved.

2 Enter values for the Time-to-Live timers.

a. Enter a value in the **SIP registration time to live timer [Seconds]** text box. Nortel recommends that the timer be set to 30 seconds. The range is 30 to 3600 seconds.

b. Enter a value in the **H.323 gatekeeper registration time to live timer [Seconds]** text box. Nortel recommends that the timer be set to 30 seconds. The range is 30 to 3600 seconds.

3 Enter the alias name of the H.323 Gatekeeper in the **H.323 alias name** text box. This is a mandatory field. The alias name must be alphanumeric, can be up to 30 characters in length, and cannot have spaces.

To send out Location Requests (LRQ), the H.323 Gatekeeper must have an H.323 Gatekeeper alias name. An H.323 Gatekeeper alias name is also referred to as an H323-ID.

4 Enter the time when the database backup will automatically occur in the **Auto backup time [HH:MM]** text box.

5 Complete the following steps to automatically back up the NRS database to an FTP site.

a. Select the **Auto backup to secure FTP site enabled** check box.

b. Enter the IP address of the FTP site in the **Auto backup to secure FTP site’s IP address** text box.

c. Enter the path to the FTP site in the **Auto backup secure FTP site’s path** text box. The FTP site path must be alphanumeric and can be up to 120 characters in length.

d. Enter the user name used to access the FTP site in the **Auto backup secure FTP user name** text box. The FTP user name must be alphanumeric and can be up to 30 characters in length.

e. Enter the password used to access the FTP site in **Auto backup secure FTP password** text box. The FTP password must be alphanumeric and can be up to 24 characters in length but cannot include the single quote (’) symbol.

6 Click the **Save** button.

—End—

Configure the NRS database

The NRS (Solid) database is used by both the SIP Proxy/Redirect Server and the H.323 Gatekeeper. For more information on the NRS database see "Database component" (page 32).

Task summary list

See the procedures in this section to configure the NRS database.

- Procedure 8 "Switching between the Active and Standby databases" (page 164)
- Procedure 9 "Adding a Service Domain" (page 166)
- Procedure 13 "Adding an L1 Domain (UDP)" (page 172)
- Procedure 17 "Adding an L0 Domain (CDP)" (page 181)
- Procedure 25 "Adding a Gateway Endpoint" (page 199)
- Procedure 40 "Adding a Routing Entry" (page 231)

- Procedure 21 "Adding a Collaborative Server" (page 190)
- Procedure 57 "Cutting over the database" (page 257)
- Procedure 60 "Committing the database" (page 260)

  Note 1: To add a SIP Phone as a User Endpoint refer to Procedure 34 "Adding a User Endpoint" (page 219).

  Note 2: The standby database is used to modify the configuration data. Changes made to the standby database do not immediately effect call processing. Before changes made to the standby database effect call processing, the active and standby databases must be swapped by executing a database **Cut over** command.

Switch between the Active and Standby databases

The database has two schemas, Active and Standby. For more information see "Database synchronization/operation component" (page 42).

- The Active database is used for runtime location queries by SIP Proxy, Gatekeeper and NCS.
- The Standby database is used for administrator modifications.

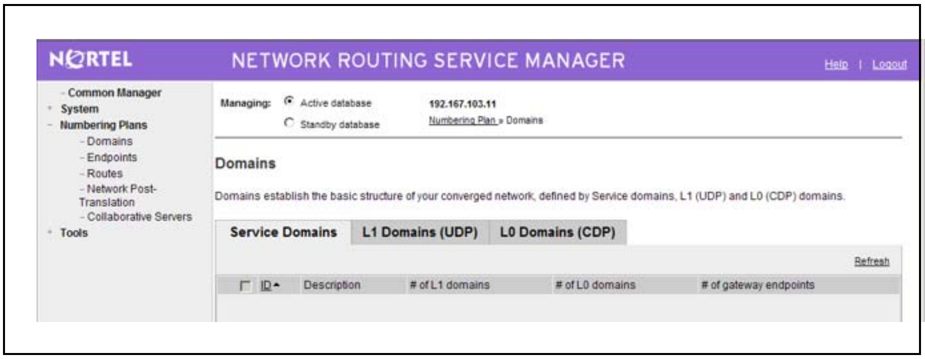
  Note: By default, the database is in Active database view when the **Domains** web page is first opened. To modify the database it must be in Standby database view. Only users with administrative authority can modify the database.

Below the NRS Manager header is an area for switching between the Active and Standby databases. See Procedure 8 "Switching between the Active and Standby databases" (page 164)to switch between the Active and Standby database.

Procedure 8
Switching between the Active and Standby databases

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).

Figure 55
Domains web page



Managing: ● Active database ○ Standby database

192.167.103.11

Numbering Plan » Domains

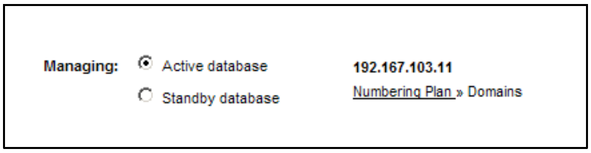
Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

□	ID▲	Description	# of L1 domains	# of L0 domains	# of gateway endpoints

2 Click **Standby database** to switch to the Standby database. See Figure 56 "Active database selected" (page 165). The Standby database is used for database modifications.

Figure 56
Active database selected



Managing: ● Active database ○ Standby database

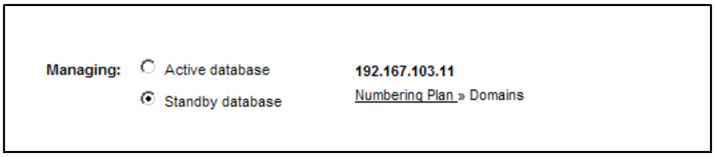
192.167.103.11

Numbering Plan » Domains

or

3 Click **Active database** to switch to the Active database. See Figure 57 "Standby database selected" (page 165). The Active database is used for database queries.

Figure 57
Standby database selected



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Domains

—End—

Note: Procedure 9 "Adding a Service Domain" (page 166) to Procedure 40 "Adding a Routing Entry" (page 231) use the example hierarchy (myServiceProvider.com, myCompany.com, and so on) provided in the "Network Routing Service overview" (page 19) chapter.

Manage a Service Domain

The Service Domain is a building block of the routable SIP URI. It represents the service domain name field in the URI (see "SIP Uniform Resource Identifiers" (page 38)). For more information on Service Domains see Figure 4 "Hierarchy of the NRS database components" (page 35).

Add a Service Domain

Use the following procedure to add a service domain.

Procedure 9
Adding a Service Domain

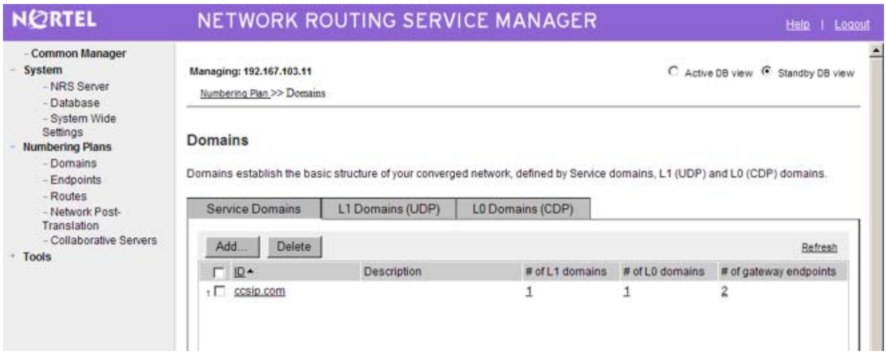
Step	Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 58 "Service Domains pane" (page 166).

Figure 58
Service Domains pane



Managing: 192.167.103.11

Domains

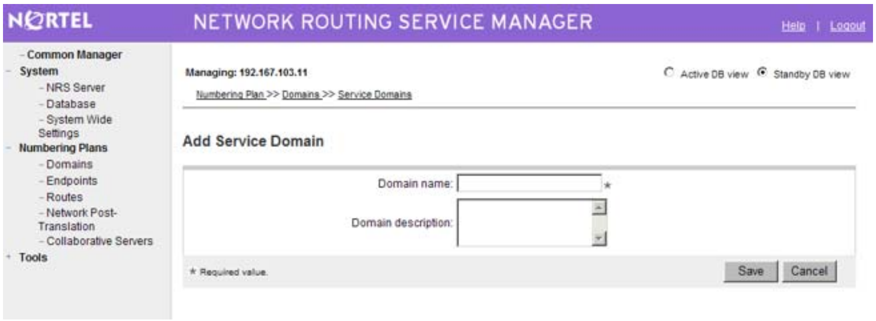
Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

	□	ID	Description	# of L1 domains	# of L0 domains	# of gateway endpoints
1	□	ccsip.com		1	1	2

3 Click the **Add...** button.

The **Add Service Domain** web page opens, as shown in Figure 59 "Add Service Domain web page" (page 167).

Figure 59
Add Service Domain web page



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Domains >> Service Domains

Add Service Domain

Domain name: *

Domain description:

* Required value.

4 Enter a **Domain name** for the Service Domain in the text box.

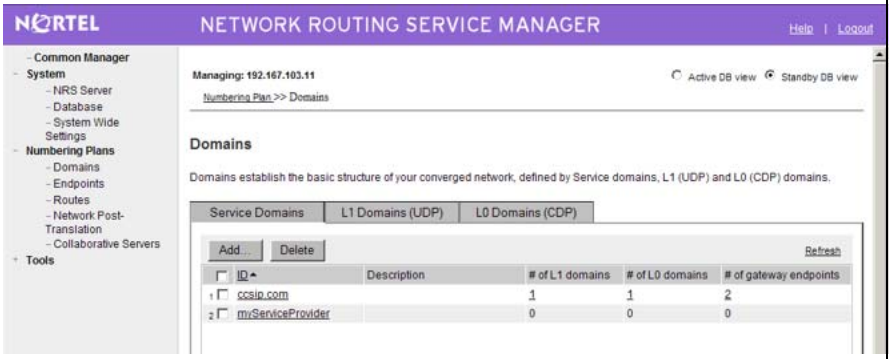
For example, enter myServiceProvider.com.

5 Enter a **Domain description** for the Service Domain in the text box.

6 Click the **Save** button. The standby database is updated.

The **Service Domains** web page opens, showing the newly added myServiceProvider.com Service Domain. See Figure 60 "Added Service Domain" (page 167).

Figure 60
Added Service Domain



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Domains

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

	☐	ID ▴	Description	# of L1 domains	# of L0 domains	# of gateway endpoints
1	☐	ccsip.com		1	1	2
2	☐	myServiceProvider		0	0	0

7 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

8 Test the configuration changes.

9 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

View the Service Domain

Use the following procedure to view the service domains.

Procedure 10
Viewing the Service Domains

Step **Action**

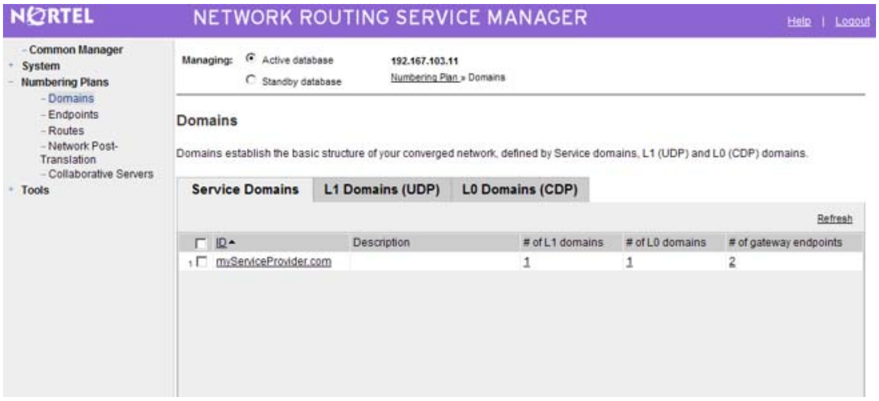
1 In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).

The Service Domains can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

2 Select the **Active** or **Standby** database. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The Active database is used for runtime queries. To modify the database it must be in Standby database view. Only Administrators can modify the standby database. One can switch between Active and Standby database views at any time.

The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 61 "Service Domains pane Active Database" (page 168).

Figure 61
Service Domains pane Active Database



Managing: ● Active database ○ Standby database

192.167.103.11

Numbering Plan » Domains

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

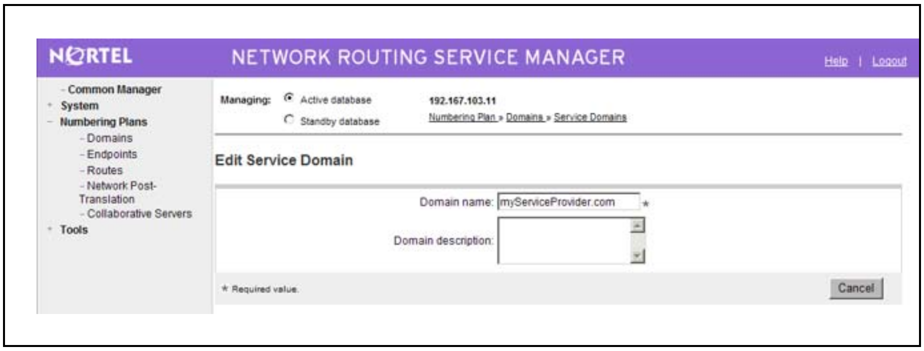
	□ ID▲	Description	# of L1 domains	# of L0 domains	# of gateway endpoints
1	□ myServiceProvider.com		1	1	2

3 Click a link in the **ID** column of the **Service Domains** pane.

The **Edit Service Domain** web page opens and displays the configured data for the selected Service Domain, as shown in Figure 62 "Edit Service Domains web page Active Database" (page 169).

> ***Note:*** See Procedure 11 "Editing a Service Domain" (page 169) to Edit the Service Domain.

Figure 62
Edit Service Domains web page Active Database



Managing: ● Active database ○ Standby database

192.167.103.11

Numbering Plan » Domains » Service Domains

Edit Service Domain

Domain name: myServiceProvider.com *

Domain description:

* Required value.

—End—

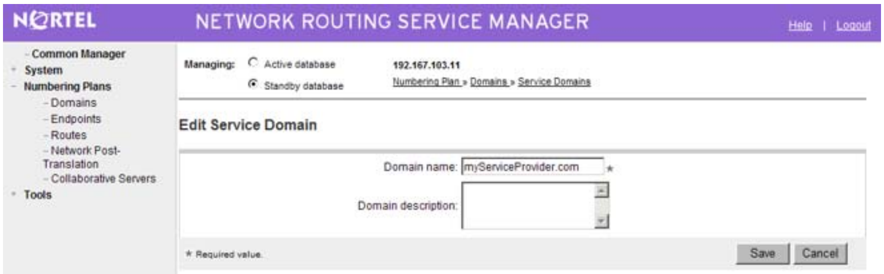
Edit a Service Domain

Use the following procedure to edit a service domain.

Procedure 11
Editing a Service Domain

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165). The Service Domains can be sorted in ascending or descending alphabetical order. See Sort web page by ID.
2	Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 58 "Service Domains pane" (page 166).
3	Click a link in the **ID** column of the **Service Domains** pane. The **Edit Service Domain** web page opens, as shown in Figure 63 "Edit Service Domain web page" (page 170).

Figure 63
Edit Service Domain web page



Managing: ○ Active database ● Standby database

192.167.103.11

Edit Service Domain

Domain name: myServiceProvider.com *

Domain description:

* Required value.

4 Modify the **Domain name** or the **Domain description** .

5 Click the **Save** button. The standby database is updated.

The **Service Domains** web page opens, as shown in Figure 58 "Service Domains pane" (page 166).

6 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

7 Test the configuration changes.

8 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Delete a Service Domain

Use the following procedure to delete a service domain.

Procedure 12
Deleting a Service Domain

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).

The Service Domains can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

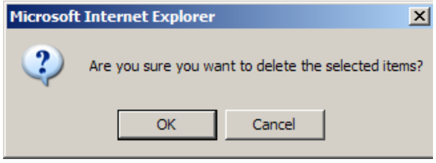
The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 58 "Service Domains pane" (page 166).

3 Select a check box beside one or more configured **Service Domains** in the **ID** column of the **Service Domains** pane.

4 Click **Delete**.

A **Confirmation Box** opens requesting confirmation before deleting the selected **Service Domain**.

Figure 64
Confirmation Box



Microsoft Internet Explorer

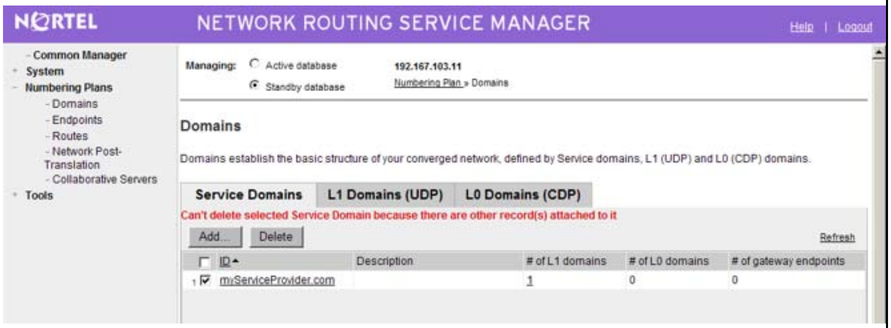
Are you sure you want to delete the selected items?

5 Click **OK**.

If there is ***not*** an associated **L1 Domain** or **Collaborative Server** configured, the standby database is updated and the **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 58 "Service Domains pane" (page 166).

If there is an associated **L1 Domain** or **Collaborative Server** configured, the **Service Domain** can not be deleted and an error message is displayed.

Figure 65
Delete Service domain error message



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Domains

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Can't delete selected Service Domain because there are other record(s) attached to it

	□ ID	Description	# of L1 domains	# of L0 domains	# of gateway endpoints
1	☑ myServiceProvider.com		1	0	0

The associated **L1 Domain** or **Collaborative Server** must be deleted before the **Service Domain** can be deleted.

See Procedure 16 "Deleting an L1 Domain (UDP)" (page 179) to delete the associated **L1 Domain**.

See Procedure 24 "Deleting a Collaborative Server" (page 197) to delete the associated **Collaborative Server**.

6 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state.

7 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes

—End—

Manage a Level 1 Domain (UDP)

The Level 1 (L1) Domain is a building block of the phone context for private addresses. It is the phone context root. For more information on phone context, see "SIP Uniform Resource Identifiers" (page 38). For more information on L1 Domains, see Figure 4 "Hierarchy of the NRS database components" (page 35).

Add an L1 Domain (UDP)

Use the following procedure to add an L1 Domain (UDP).

Procedure 13

Adding an L1 Domain (UDP)

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

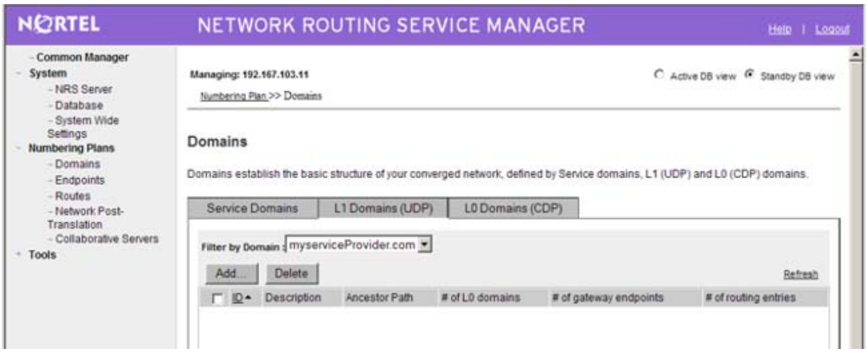
The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 58 "Service Domains pane" (page 166).

3 Click **L1 Domains (UDP)** button.

The **Domains** web page refreshes displaying the **L1 Domains (UDP)** pane, as shown in Figure 66 "L1 Domains (UDP) pane" (page 173).

The L1 Domains can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

Figure 66
L1 Domains (UDP) pane



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Domains

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

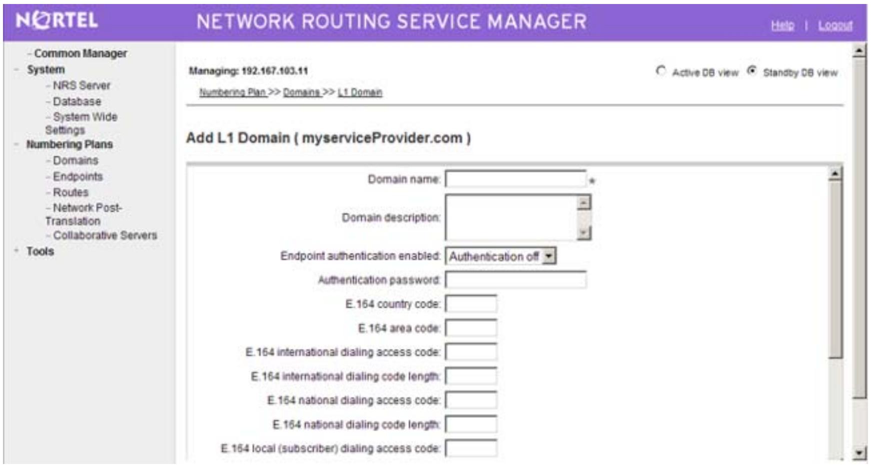
Filter by Domain : myserviceProvider.com

4 The **Filter by Domain:** drop-down list contains configured Service Domains. Select the **Service Domain**, where the new L1 subdomain will be added, from the drop-down list.

5 Click the **Add...** button.

The **Add L1 Domain** web page opens, as shown in Figure 67 "Add L1 Domain web page" (page 173).

Figure 67
Add L1 Domain web page



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Domains >> L1 Domain

Add L1 Domain (myserviceProvider.com)

Domain name: *

Domain description:

Endpoint authentication enabled: Authentication off

Authentication password:

E.164 country code:

E.164 area code:

E.164 international dialing access code:

E.164 international dialing code length:

E.164 national dialing access code:

E.164 national dialing code length:

E.164 local (subscriber) dialing access code:

6 Enter the **Domain name** of the L1 Domain in the text box. The name must be alphanumeric and can be up to 30 characters in length.

For example, enter myCompany.com.

7 Enter the **Domain description** in the text box. The description can include any character except single quotes and can be up to 120 characters in length.

> ***Note:*** An L1 Domain can inherit configuration parameters from its parent Service Domain. See "Numbering Plans inherited fields" (page 153).

8 Select **Authentication on** or **Authentication off** from the **Endpoint authentication enabled** drop-down list.

If **Authentication on** is selected, then all endpoints require authentication.

9 Enter the **Authentication password** in the text box, if **Authentication on** was selected in step 8. The password must be alphanumeric and can be up to 24 characters in length.

10 Enter the **E.164 country code** in the text box. The code must be numeric and can be up to 30 digits in length.

11 Enter the **E.164 area code** in the text box. The code must be numeric and can be up to 30 digits in length.

12 Any SIP endpoint that does not support SIP phone context should include prefix to dialed numbers in a prefix in the **E.164 international dialing access code** text box, so that NRS can resolve them. The code must be numeric and can be up to eight digits in length.

13 Enter the **E.164 international dialing code length** in the text box. The code length must be numeric and has to exceed the E.164 international dialing access code length.

14 Enter the **E.164 national dialing access code** in the text box. The code must be numeric and can be up to eight digits in length.

15 Enter the **E.164 national dialing access code length** in the text box. The code length must be numeric and has to exceed the E.164 national dialing access code length.

16 Enter the **E.164 local (subscriber) dialing access code** in the text box. The code must be numeric and can be up to eight digits in length.

17 Enter the **E.164 local (subscriber) dialing code length** in the text box. The code length must be numeric and has to exceed the E.164 local (subscriber) dialing access code length.

18 Enter the **Private L1 domain (UDP location) dialing access code** in the text box. The code must be numeric and can be up to eight digits in length.

19 Enter the **Private L1 domain (UDP location) dialing code length** in the text box. The code length must be numeric and has to exceed the Private L1 domain (UDP location) dialing access code length.

20 Enter the **Special number** in the text box. The number must be numeric and can be up to 30 digits in length.

21 Enter the **Special number dialing code length** in the text box. The code length must be numeric and equal to the Special number length.

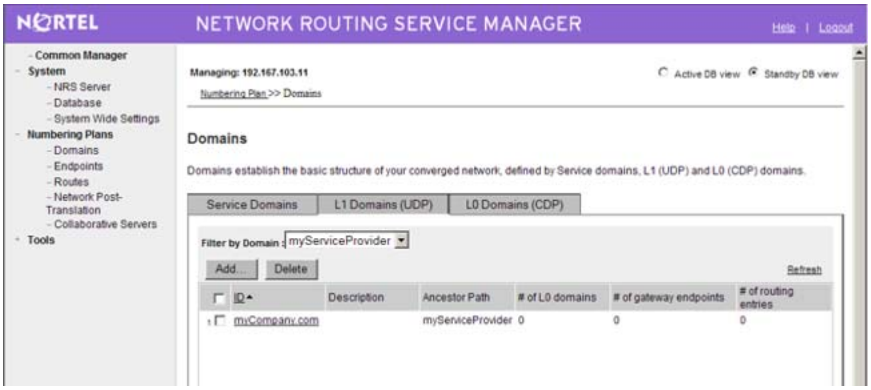
22 Enter the **Emergency service access prefix** in the text box. The number must be numeric and can be up to 30 digits in length.

23 Enter the **Special number label** in the text box. The label must be alphanumeric and can be up to 30 characters in length.

24 Click the **Save** button. The standby database is updated.

The **Domains** web page opens, showing the newly added myCompany.com L1 domain in the myServiceProvider.com Service Domain. See Figure 68 "Added L1 Domain" (page 175).

Figure 68
Added L1 Domain



Managing: 192.167.103.11

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Filter by Domain : myServiceProvider

	□ ID	Description	Ancestor Path	# of L0 domains	# of gateway endpoints	# of routing entries
1	□ myCompany.com		myServiceProvider	0	0	0

25 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

26 Test the configuration changes.

27 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

View an L1 Domain (CDP)

Use the following procedure to view an L1 Domain (CDP).

Procedure 14
Viewing an L1 Domain (CDP)

Step	Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).

2 Select the **Active** or **Standby** database. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The Active database is used for runtime queries. To modify the database it must be in Standby database view. Only Administrators can modify the standby database. One can switch between Active and Standby database views at any time.

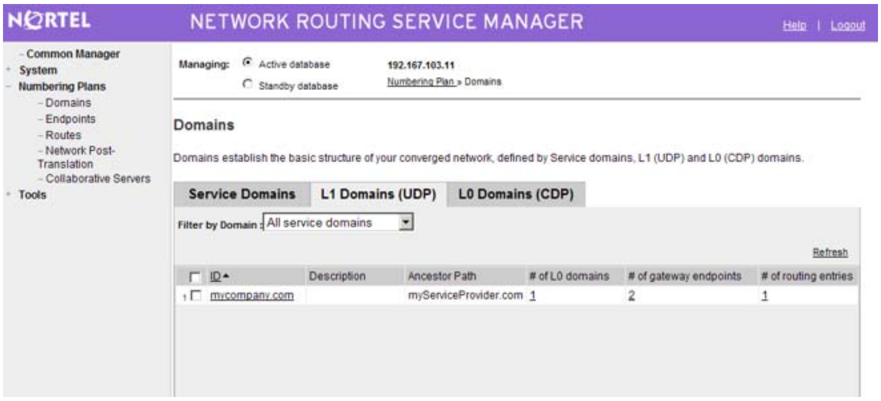
The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 61 "Service Domains pane Active Database" (page 168).

3 Click **L1 Domains (UDP)** button.

The **Domains** web page refreshes displaying the **L1 Domains (UDP)** pane, as shown in Figure 69 "L1 Domains (UDP) pane Active database" (page 176).

The L1 Domains can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

Figure 69
L1 Domains (UDP) pane Active database



Managing: ● Active database ○ Standby database

192.167.103.11
Numbering Plan » Domains

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Filter by Domain : All service domains

□	ID	Description	Ancestor Path	# of L0 domains	# of gateway endpoints	# of routing entries
□	mycompany.com		myServiceProvider.com	1	2	1

4 The **Filter by Domain:** drop-down list contains configured Service Domains. Select the **Service Domain**, that the L1 domain is a

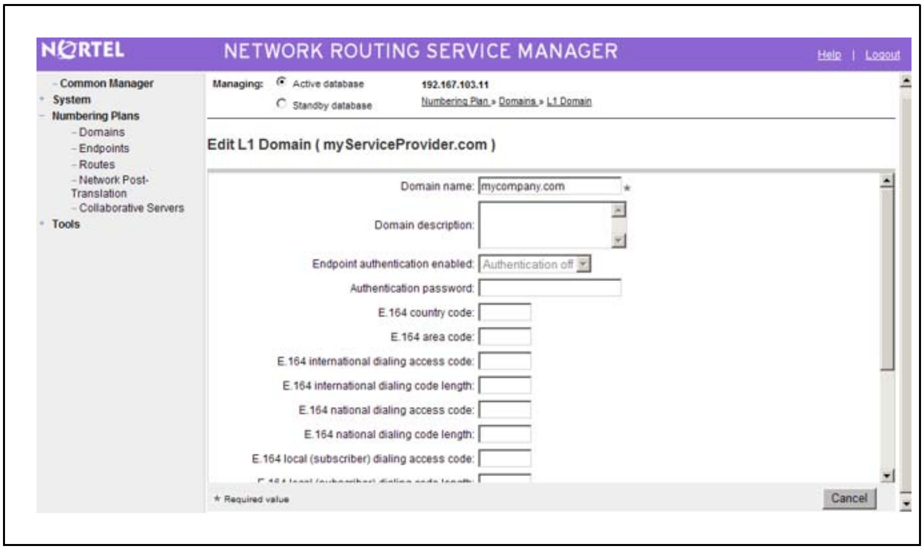
subdomain of, from the drop-down list. The **Domains** web page refreshes.

5 Click a **link** in the **ID** column of the L1 domains (UDP) web page.

The **Edit L1 Domain** web page opens and displays the configured data for the selected L1 Domain, as shown in Figure 70 "Edit L1 Domain (UDP) web page Active database" (page 177).

> ***Note:*** See Procedure 15 "Editing an L1 Domain (UDP)" (page 177) to Edit the L1 Domain.

Figure 70
Edit L1 Domain (UDP) web page Active database



Managing: ● Active database ○ Standby database

192.167.103.11

Numbering Plan » Domains » L1 Domain

Edit L1 Domain (myServiceProvider.com)

Domain name: mycompany.com *

Domain description:

Endpoint authentication enabled: Authentication off

Authentication password:

E.164 country code:

E.164 area code:

E.164 international dialing access code:

E.164 international dialing code length:

E.164 national dialing access code:

E.164 national dialing code length:

E.164 local (subscriber) dialing access code:

* Required value

—End—

Edit an L1 Domain (UDP)

Use the following procedure to edit an L1 Domain (UDP).

Procedure 15
Editing an L1 Domain (UDP)

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).
2	Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 58 "Service Domains pane" (page 166).

3 Click **L1 Domains (UDP)** button.

The **Domains** web page refreshes displaying the **L1 Domains (UDP)** pane, as shown in Figure 66 "L1 Domains (UDP) pane" (page 173).

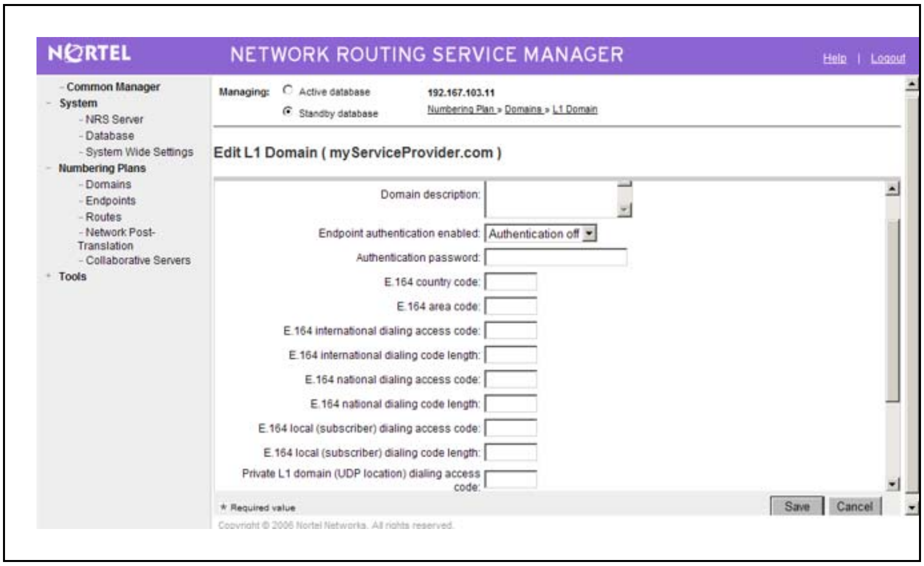
The L1 Domains can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

4 The **Filter by Domain:** drop-down list contains configured Service Domains. Select the **Service Domain**, where the L1 subdomain will be edited, from the drop-down list.

5 Click on a link in the **ID** column of the **L1 Domains (UDP)** pane.

The **Edit L1 Domain** web page opens, as shown in Figure 71 "Edit L1 Domain web page" (page 178).

Figure 71
Edit L1 Domain web page



Managing: ○ Active database ● Standby database 192.167.103.11

Edit L1 Domain (myServiceProvider.com)

Domain description:

Endpoint authentication enabled: Authentication off

Authentication password:

E.164 country code:

E.164 area code:

E.164 international dialing access code:

E.164 international dialing code length:

E.164 national dialing access code:

E.164 national dialing code length:

E.164 local (subscriber) dialing access code:

E.164 local (subscriber) dialing code length:

Private L1 domain (UDP location) dialing access code:

* Required value

Copyright © 2006 Nortel Networks. All rights reserved.

6 Modify the fields of the **Edit L1 Domain** web page as appropriate. See step 6 to step 23 of "Adding a Level 1 Domain (UDP)" (page 172).

> ***Note:*** An L1 Domain can inherit configuration parameters from its parent Service Domain. See "Numbering Plans inherited fields" (page 153).

7 Click the **Save** button.

The standby database is updated. The **Domains** web page opens displaying the **L1 Domains (UDP)** pane, as shown in Figure 66 "L1 Domains (UDP) pane" (page 173).

8 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

9 Test the configuration changes.

10 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Delete an L1 Domain (UDP)

Use the following procedure to delete an L1 Domain (UDP).

Procedure 16
Deleting an L1 Domain (UDP)

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 58 "Service Domains pane" (page 166).

3 Click **L1 Domains (UDP)** button.

The **Domains** web page refreshes displaying the **L1 Domains (UDP)** pane, as shown in Figure 66 "L1 Domains (UDP) pane" (page 173).

The L1 Domains can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

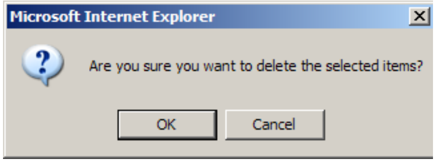
4 The **Filter by Domain:** drop-down list contains configured Service Domains. Select a **Service Domain** from the drop-down list.

5 Select a check box beside one or more configured **L1 Domains** in the **ID** column of the **L1 Domains (UDP)** pane.

6 Click the **Delete** button.

A **Confirmation Box** opens requesting confirmation before deleting the selected **L1 Domain**.

Figure 72
Confirmation Box



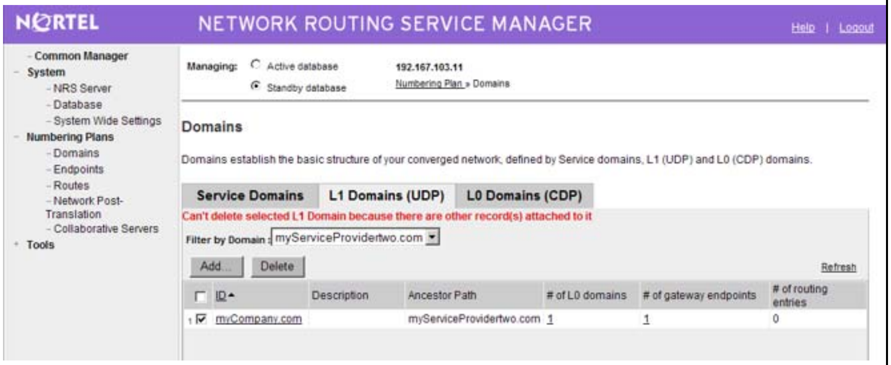
Are you sure you want to delete the selected items?

7 Click **OK**.

If there is ***not*** an associated **L0 Domain** or **Collaborative Server** configured, the standby database is updated and the **Domains** web page opens displaying the **L1 Domains (UDP)** pane, as shown in Figure 66 "L1 Domains (UDP) pane" (page 173).

If there is an associated **L0 Domain** or **Collaborative Server** configured, the **L1 Domain** can not be deleted and an error message is displayed. See Figure 73 "Delete L1 Domain error message" (page 180).

Figure 73
Delete L1 Domain error message



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Domains

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Can't delete selected L1 Domain because there are other record(s) attached to it

Filter by Domain : myServiceProvidertwo.com

	□	ID ▲	Description	Ancestor Path	# of L0 domains	# of gateway endpoints	# of routing entries
1	☑	myCompany.com		myServiceProvidertwo.com	1	1	0

The associated **L0 Domain** or **Collaborative Server** must be deleted before the **L1 Domain** can be deleted.

See Procedure 20 "Deleting an L0 Domain (CDP)" (page 188) to delete the associated **L0 Domain**.

See Procedure 24 "Deleting a Collaborative Server" (page 197) to delete the associated **Collaborative Server**.

8 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state.

9 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Manage a Level 0 Domain (CDP)

The Level 0 (L0) Domain is a building block of the phone context for private addresses. For more information on phone context, see "SIP Uniform Resource Identifiers" (page 38). For more information on L0 Domains, see Figure 4 "Hierarchy of the NRS database components" (page 35).

Add an L0 Domain (CDP)

Use the following procedure to add an L0 Domain (CDP).

Procedure 17
Adding an L0 Domain (CDP)

Step **Action**

1 In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).

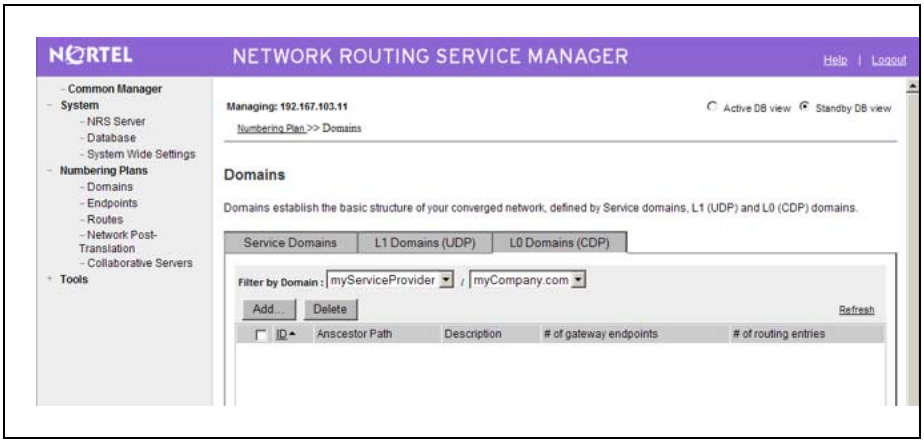
2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 58 "Service Domains pane" (page 166).

3 Click **L0 Domains (CDP)** button.

The **Domains** web page refreshes displaying the **L0 Domains (UDP)** pane, as shown in Figure 74 "L0 Domain (CDP) pane" (page 181).

Figure 74
L0 Domain (CDP) pane



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Domains

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

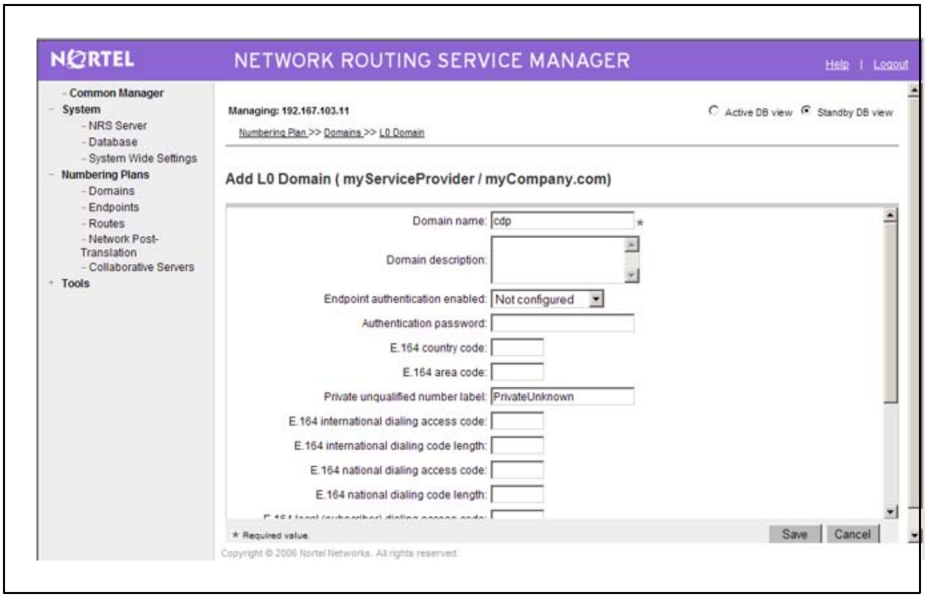
Filter by Domain : myServiceProvider / myCompany.com

4 The **Filter by Domain:** drop-down lists contain configured Service Domains and L1 Domains. Select the Service Domain and the L1 Domain, where the new L0 subdomain will be added, from the respective drop-down lists.

5 Click the **Add...** button.

The **Add L0 Domain** web page opens, as shown in Figure 75 "Add L0 Domain web page" (page 182).

Figure 75
Add L0 Domain web page



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Domains >> L0 Domain

Add L0 Domain (myServiceProvider / myCompany.com)

Domain name: cdp *

Domain description:

Endpoint authentication enabled: Not configured

Authentication password:

E.164 country code:

E.164 area code:

Private unqualified number label: PrivateUnknown

E.164 international dialing access code:

E.164 international dialing code length:

E.164 national dialing access code:

E.164 national dialing code length:

E.164 local (subscriber) dialing access code:

* Required value.

Copyright © 2006 Nortel Networks. All rights reserved.

6 Enter the **Domain name** of the L0 Domain in the text box. The name must be alphanumeric and up to 30 characters in length.

For example, enter myCdpDomain.

7 Enter the **Domain description** in the text box. The description can include any character except single quotes and can be up to 120 characters in length.

> ***Note:*** An L0 Domain can inherit configuration parameters from its parent L1 Domain. See "Numbering Plans inherited fields" (page 153).

8 Select **Not configured**, **Authentication on**, or **Authentication off** from the **Endpoint authentication enabled** drop-down list.

If **Authentication on** is selected, then all endpoints require authentication.

9 Enter the **Authentication password** in the text box, if **Authentication on** was selected in step 8. The password must be alphanumeric and up to 24 characters in length.

10 Enter the **E.164 country code** in the text box. The code must be numeric and can be up to 30 digits in length.

11 Enter the **E.164 area code** in the text box. The code must be numeric and can be up to 30 digits in length.

12 Enter the **Private unqualified number label** in the text box. The label must be alphanumeric and can be up to 30 characters in length. The first character in the label must be alphabetic.

13 Enter the **E.164 international dialing access code** in the text box. The code must be numeric and can be up to eight digits in length.

14 Enter the **E.164 international dialing code length** in the text box. The code length must be numeric and has to exceed the E.164 international dialing access code length.

15 Enter the **E.164 national dialing access code** in the text box. The code must be numeric and can be up to eight digits in length.

16 Enter the **E.164 national dialing code length** in the text box. The code length must be numeric and has to exceed the E.164 national dialing access code length.

17 Enter the **E.164 local (subscriber) dialing access code** in the text box. The code must be numeric and can be up to eight digits in length.

18 Enter the **E.164 local (subscriber) dialing code length** in the text box. The code must be numeric and has to exceed the E.164 local (subscriber) dialing access code length.

19 Enter the **Private L1 domain (UDP location) dialing access code** in the text box. The code must be numeric and can be up to eight digits in length.

20 Enter the **Private L1 domain (UDP location) dialing code length** in the text box. The code must be numeric and has to exceed the Private L1 domain (UDP location) dialing access code length.

21 Enter the **Special number** in the text box. The number must be numeric and can be up to 30 digits in length.

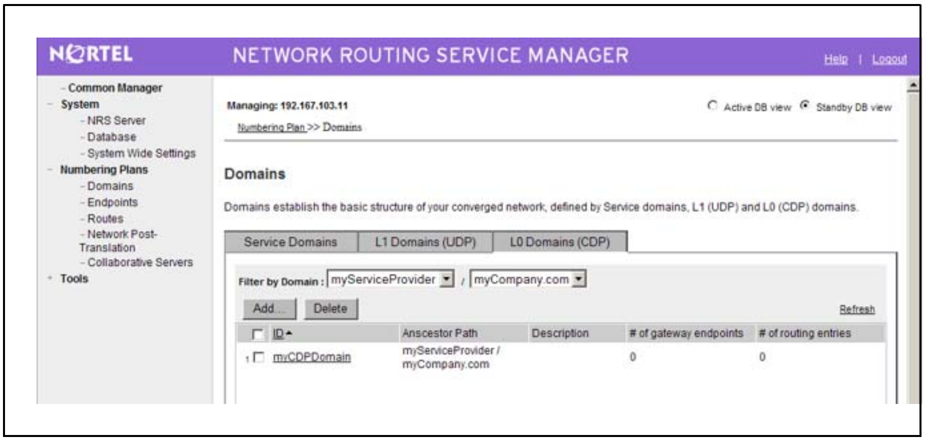
22 Enter the **Special number dialing code length** in the text box. The number must be numeric and equal to the Special number length.

23 Enter the **Emergency services access prefix** in the text box. The number must be numeric and can be up to 30 digits in length.

24 Click the **Save** button. The standby database is updated.

The **Domains** web page opens, showing the newly added myCdpDomain L0 domain. See Figure 76 "Added L0 Domain" (page 184).

Figure 76
Added L0 Domain



Managing: 192.167.103.11

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Filter by Domain : mySeviceProvider / myCompany.com

	□	ID▲	Anscestor Path	Description	# of gateway endpoints	# of routing entries
1	□	myCDPDomain	myServiceProvider / myCompany.com		0	0

25 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

26 Test the configuration changes.

27 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

View an L0 Domain (CDP)

Use the following procedure to view an L0 Domain (CDP).

Procedure 18
Viewing an L0 Domain (CDP)

Step **Action**

1 In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).

2 Select the **Active** or **Standby** database. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The Active database is used for runtime queries. To modify the database it must be in Standby database view. Only Administrators can modify the standby database. One can switch between Active and Standby database views at any time.

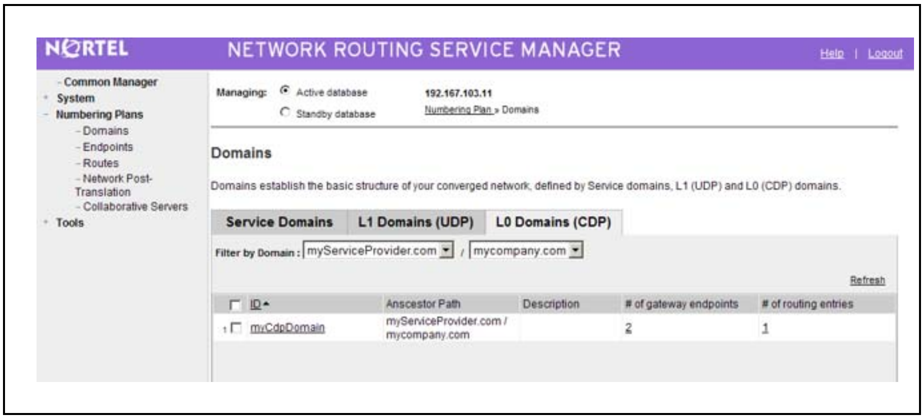
The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 61 "Service Domains pane Active Database" (page 168).

3 Click **L0 Domains (CDP)** button.

The **Domains** web page refreshes displaying the **L0 Domains (CDP)** pane, as shown in Figure 77 "L0 Domain (CDP) pane Active database" (page 185).

The L0 Domains can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

Figure 77
L0 Domain (CDP) pane Active database



NORTEL NETWORK ROUTING SERVICE MANAGER Help | Logout

- Common Manager
- System
- Numbering Plans
  - Domains
  - Endpoints
  - Routes
  - Network Post-Translation
  - Collaborative Servers
- Tools

Managing: ● Active database ○ Standby database

192.167.103.11
Numbering Plan » Domains

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Service Domains | L1 Domains (UDP) | L0 Domains (CDP)

Filter by Domain : myServiceProvider.com / mycompany.com

Refresh

	☐ ID	Anscestor Path	Description	# of gateway endpoints	# of routing entries
1	☐ myCdpDomain	myServiceProvider.com / mycompany.com		2	1

4 The **Filter by Domain:** drop-down lists contain configured Service Domains and L1 Domains. Select a Service Domain and L1 Domain from the drop-down lists.

The web page displays a list of configured L0 Domains.

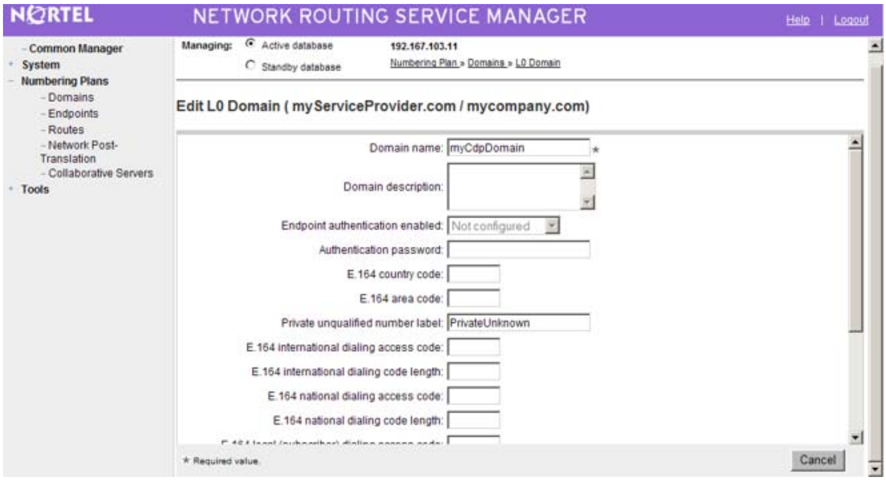
5 Click a **link** in the **ID** column of the L0 Domains (CDP) pane.

The **Edit L0 Domain** web page opens and displays the configured data for the selected L0 Domain.

See Figure 78 "Edit L0 Domain (CDP) web page Active database" (page 186).

> ***Note:*** See Procedure 19 "Editing an L0 Domain (CDP)" (page 186) to Edit the L0 Domain.

Figure 78
Edit L0 Domain (CDP) web page Active database



Managing: ● Active database ○ Standby database

192.167.103.11

Numbering Plan » Domains » L0 Domain

Edit L0 Domain (myServiceProvider.com / mycompany.com)

Domain name: myCdpDomain *

Domain description:

Endpoint authentication enabled: Not configured

Authentication password:

E.164 country code:

E.164 area code:

Private unqualified number label: PrivateUnknown

E.164 international dialing access code:

E.164 international dialing code length:

E.164 national dialing access code:

E.164 national dialing code length:

E.164 local (subscriber) dialing access code:

* Required value.

—End—

Edit an L0 Domain (CDP)

Use the following procedure to edit an L0 Domain (CDP).

Procedure 19
Editing an L0 Domain (CDP)

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).
2	Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 58 "Service Domains pane" (page 166).
3	Click **L0 Domains (CDP)** button. The **Domains** web page refreshes displaying the **L0 Domains (UDP)** pane, as shown in Figure 74 "L0 Domain (CDP) pane" (page 181). The L0 Domains can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

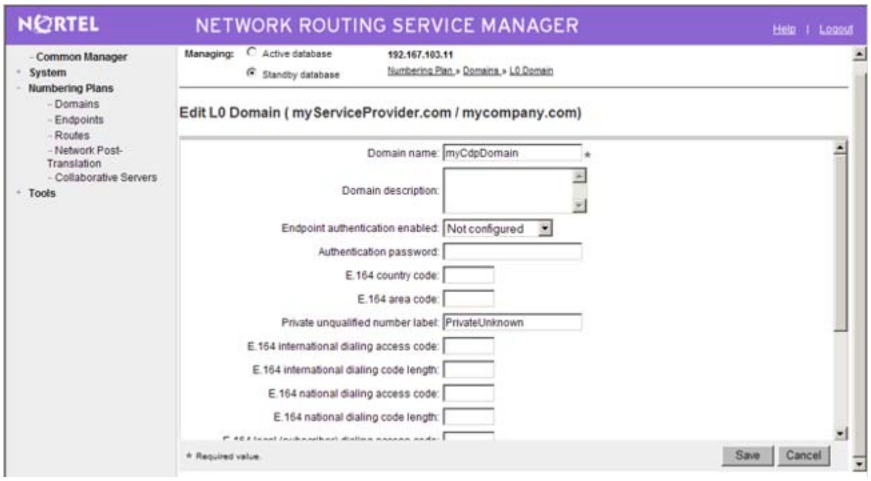
4 The **Filter by Domain:** drop-down lists contain configured Service Domains and L1 Domains. Select a Service Domain and L1 Domain from the drop-down lists.

The web page refreshes displaying a list of configured L0 Domains.

5 Click on a link in the **ID** column of the **L0 Domains (CDP)** pane.

The **Edit L0 Domain** web page opens, as shown in Figure 79 "Edit L0 Domain web page" (page 187).

Figure 79
Edit L0 Domain web page



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Domains » L0 Domain

Edit L0 Domain (myServiceProvider.com / mycompany.com)

Domain name: myCdpDomain *

Domain description:

Endpoint authentication enabled: Not configured

Authentication password:

E.164 country code:

E.164 area code:

Private unqualified number label: PrivateUnknown

E.164 international dialing access code:

E.164 international dialing code length:

E.164 national dialing access code:

E.164 national dialing code length:

E.164 local (subscriber) dialing access code:

* Required value.

6 Modify the fields of theEdit L0 Domain web page as appropriate. See step 6 to step 23 of Procedure 17 "Adding an L0 Domain (CDP)" (page 181).

> ***Note:*** An L1 Domain can inherit configuration parameters from its parent L0 Domain. See "Numbering Plans inherited fields" (page 153)

7 Click the **Save** button. The standby database is updated.

The **Domains** web page opens displaying the **L0 Domains (UDP)** pane, as shown in Figure 74 "L0 Domain (CDP) pane" (page 181).

8 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

9 Test the configuration changes.

10 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

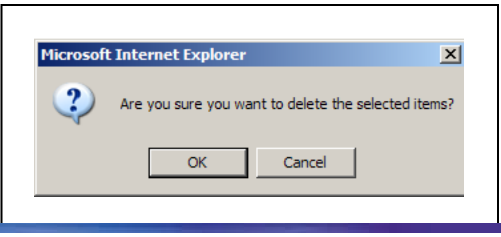
Delete an L0 Domain (CDP)

Use the following procedure to delete an L0 Domain (CDP).

Procedure 20
Deleting an L0 Domain (CDP)

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** web page opens, as shown in Figure 55 "Domains web page" (page 165).
2	Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 58 "Service Domains pane" (page 166).
3	Click **L0 Domains (CDP)** button. The **Domains** web page refreshes displaying the **L0 Domains (UDP)** pane, as shown in Figure 74 "L0 Domain (CDP) pane" (page 181). The L0 Domains can be sorted in ascending or descending alphabetical order. See Sort web page by ID.
4	The **Filter by Domain:** drop-down lists contain configured Service Domains and L1 Domains. Select a Service Domain and L1 Domain from the drop-down lists. The web page displays a list of configured L0 Domains.
5	Select a check box beside one or more configured **L0 Domains** in the **ID** column of the **L0 Domains (CDP)** pane.
6	Click **Delete**. A **Confirmation Box** opens requesting confirmation before deleting the selected **L0 Domain**.

Figure 80
Confirmation Box



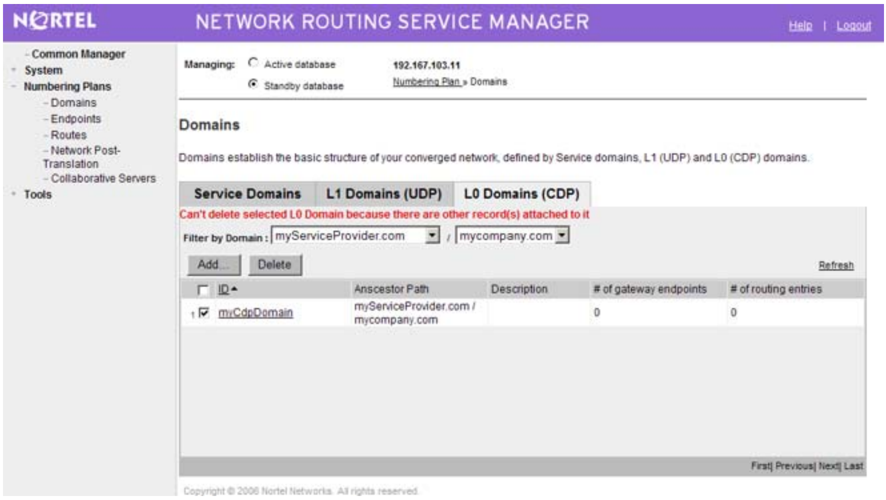
Are you sure you want to delete the selected items?

7 Click **OK**.

If there is ***not*** an associated **Collaborative Server** configured, the standby database is updated and the **Domains** web page opens displaying the **L0 Domains (UDP)** pane, as shown in Figure 74 "L0 Domain (CDP) pane" (page 181).

If there is an associated **Collaborative Server** configured, the **L0 Domain** can not be deleted and an error message is displayed, as shown in Figure 81 "Delete L0 Domain error message" (page 189).

Figure 81
Delete L0 Domain error message



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Domains

Domains

Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Can't delete selected L0 Domain because there are other record(s) attached to it

Filter by Domain : myServiceProvider.com / mycompany.com

	□ ID ▲	Anscestor Path	Description	# of gateway endpoints	# of routing entries
1	☑ myCdpDomain	myServiceProvider.com / mycompany.com		0	0

Copyright © 2006 Nortel Networks. All rights reserved.

The associated **Collaborative Server** must be deleted before the **L0 Domain** can be deleted.

See Procedure 24 "Deleting a Collaborative Server" (page 197)to delete the associated **Collaborative Server**.

8 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state.

9 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Manage a Collaborative Server

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

NRS Manager provides a utility for adding and viewing Collaborative Servers, either system-wide or in different network domains.

The configuration of a Collaborative Server as system-wide allows IP addresses to be shared by users across multiple domains. This also allows domains to be spread geographically.

NRS Collaborative Servers in different network domains can also be specified in the NRS.

If a request comes in from a gateway and the NRS cannot find a match in its database for the request, the NRS provides the IP address of a Collaborative Server to the gateway. The gateway can then send its request to the Collaborative Server.

> ***Note:*** Calls can only be made in the same domain, even though calls go through the Collaborative Server to find a match.

For more information about the Collaborative Server, refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*.

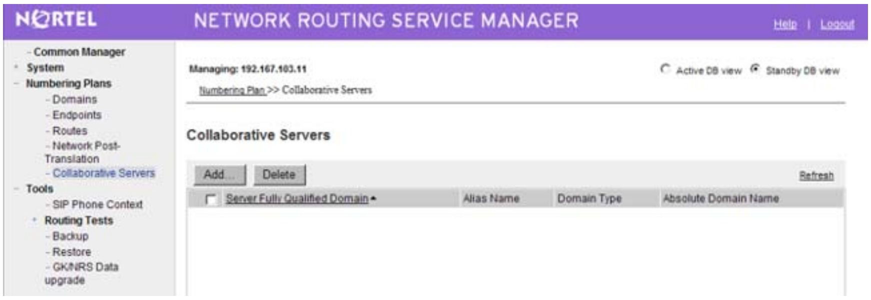
Add a Collaborative Server

Use the following procedure to add a Collaborative Server.

Procedure 21
Adding a Collaborative Server

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Collaborative Servers.** The **Collaborative Servers** web page opens, as shown in Figure 82 "Collaborative Servers web page" (page 190).

Figure 82
Collaborative Servers web page



Managing: 192.167.103.11

Collaborative Servers

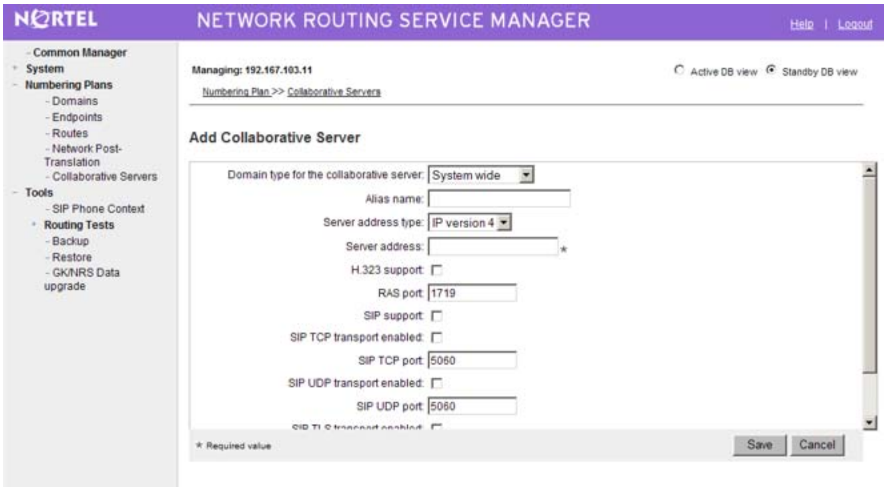
□	Server Fully Qualified Domain ▲	Alias Name	Domain Type	Absolute Domain Name

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164)

3 Click the **Add....** button.

The **Add Collaborative Server** web page opens, as shown in Figure 83 "Add Collaborative Server (System wide)" (page 191).

Figure 83
Add Collaborative Server (System wide)



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Add Collaborative Server

Domain type for the collaborative server: System wide
Alias name:
Server address type: IP version 4
Server address: *
H.323 support: □
RAS port: 1719
SIP support: □
SIP TCP transport enabled: □
SIP TCP port: 5060
SIP UDP transport enabled: □
SIP UDP port: 5060
SIP TLS transport enabled: □

* Required value

4 Select the **Domain type for Collaborative Server** from the drop-down list.

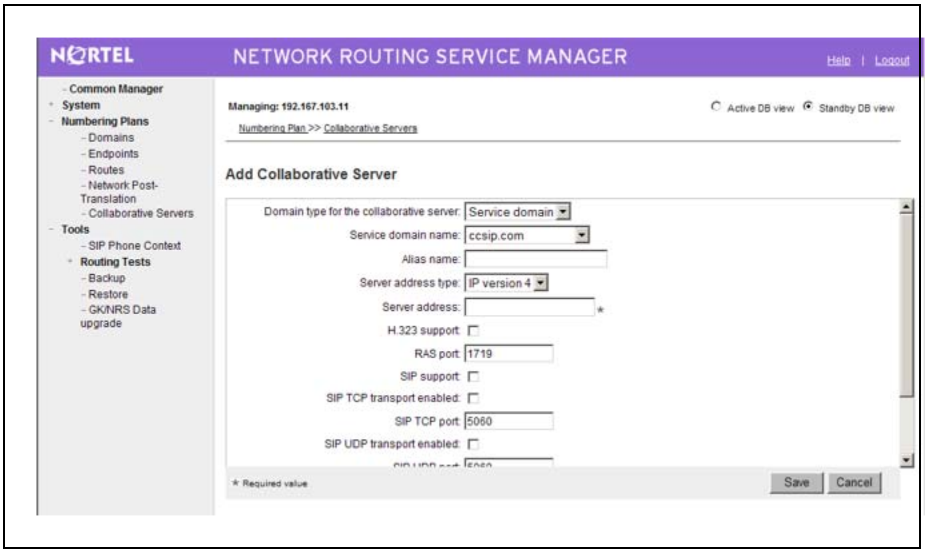
- Select **System wide** if the Collaborative Server is to be a system-wide server. See Figure 83 "Add Collaborative Server (System wide)" (page 191).
- Select **Service domain** if the Collaborative Server is to be a Service Domain server.

  An additional field **Service domain name** is displayed, as shown in Figure 84 "Add Collaborative Server (Service domain)" (page 192). Select the Service domain name from the drop-down list.
- Select **L1 domain** if the Collaborative Server is to be an L1 Domain server.

  Two additional fields are displayed: (1) **Service domain name** and (2) **L1 domain name** , as shown in Figure 85 "Add Collaborative Server (L1 Domain)" (page 192). Select the Service Domain name and the L1 Domain name from the drop-down lists.
- Select **L0 domain** if the Collaborative Server is to be an L0 Domain server.

Three additional fields are displayed: (1) **Service domain name**, (2) **L1 domain name** and (3) **L0 domain name**, as shown in Figure 86 "Add Collaborative Server (L0 Domain)" (page 193). Select the Service Domain name, the L1 Domain name and the L0 Domain name from the drop-down lists.

Figure 84
Add Collaborative Server (Service domain)



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

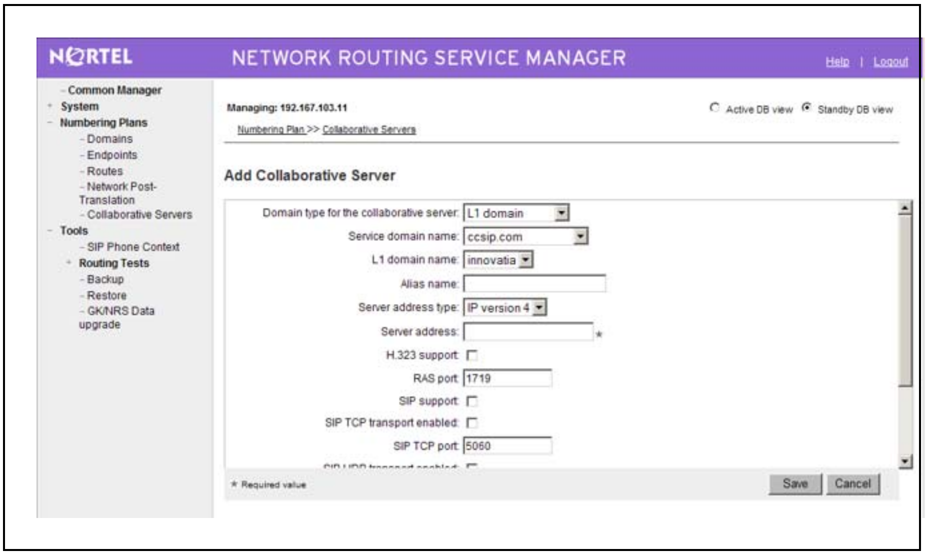
Numbering Plan >> Collaborative Servers

Add Collaborative Server

Domain type for the collaborative server: Service domain
Service domain name: ccsip.com
Alias name:
Server address type: IP version 4
Server address: *
H.323 support: □
RAS port: 1719
SIP support: □
SIP TCP transport enabled: □
SIP TCP port: 5060
SIP UDP transport enabled: □
SIP UDP port: 5060

* Required value

Figure 85
Add Collaborative Server (L1 Domain)



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

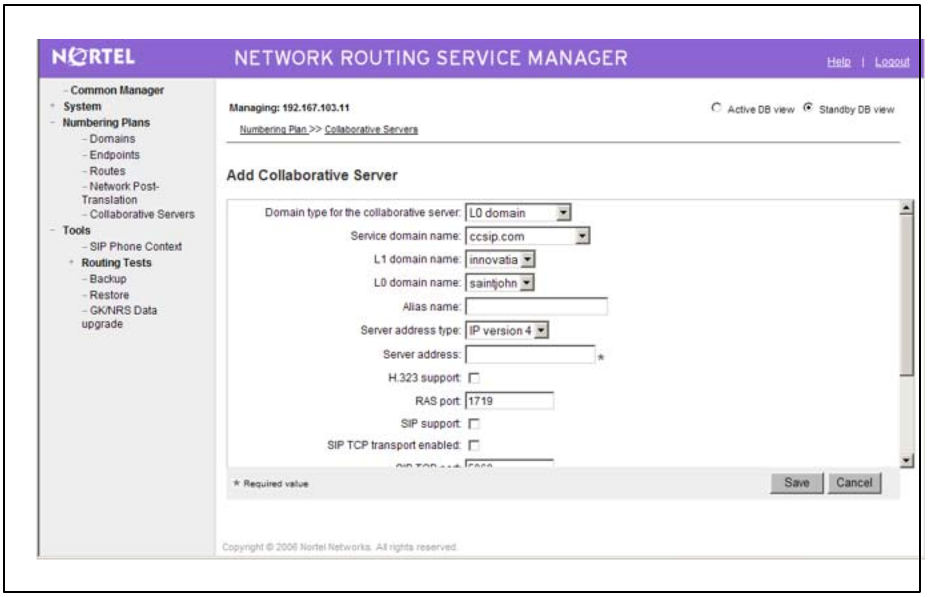
Numbering Plan >> Collaborative Servers

Add Collaborative Server

Domain type for the collaborative server: L1 domain
Service domain name: ccsip.com
L1 domain name: innovatia
Alias name:
Server address type: IP version 4
Server address: *
H.323 support: □
RAS port: 1719
SIP support: □
SIP TCP transport enabled: □
SIP TCP port: 5060
SIP UDP transport enabled: □

* Required value

Figure 86
Add Collaborative Server (L0 Domain)



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Collaborative Servers

Add Collaborative Server

Domain type for the collaborative server: L0 domain

Service domain name: ccsip.com

L1 domain name: innovatia

L0 domain name: saintjohn

Alias name:

Server address type: IP version 4

Server address: *

H.323 support: □

RAS port: 1719

SIP support: □

SIP TCP transport enabled: □

* Required value

5 Enter the **Alias name** of the collaborative server in the text box. The alias name must be alphanumeric and can be up to 30 characters in length. The name cannot include spaces.

6 **IP version 4** in the **Server address type** drop-down list is selected by default. This option has been added for future use.

7 Enter the IP address of the server in the **Server address** text box.

8 Select the protocol(s) supported by the server.

- If H.323 is supported, perform the following steps:
  1. Select the **H.323 support** check box.
  2. Enter the **RAS port** number. The port number must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port value is 1719.

- If SIP is supported, perform the following steps:
  1. Select the **SIP support** check box.
  2. Select the transport protocol:

     If SIP TCP is supported:

     - Select the **SIP TCP transport enabled** check box.
     - Enter the **SIP TCP port** number in the text box. The port number must be numeric and can be up to five digits in

length. The range is 0 to 65535. The default port value is 5060.

If SIP UDP is supported:

- Select the **SIP UDP transport enabled** check box.
- Enter the **SIP UDP port** number in the text box. The port number must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port value is 5060.

If SIP TLS is supported:

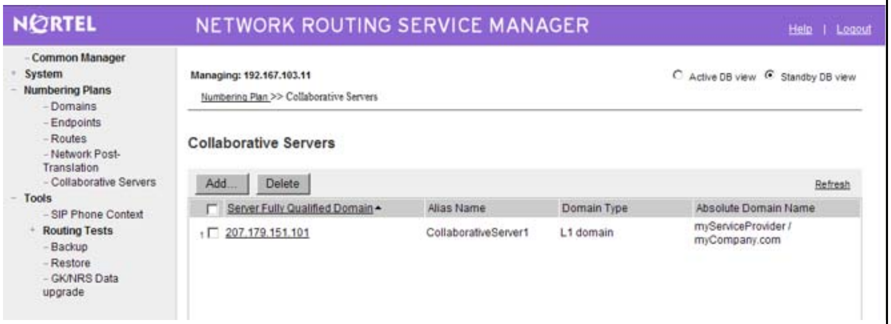
- Select the **SIP TLS transport enabled** check box.
- Enter the **SIP TLS port** number in the text box. The port number must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port value is 50601.

- If **End to end security** is supported, select the End to end security check box.

9 Click **Save**. The standby database is updated.

The **Collaborative Servers** web page opens with the newly added collaborative server, as shown in Figure 87 "Added Collaborative Server" (page 194).

Figure 87
Added Collaborative Server



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Collaborative Servers

Collaborative Servers

	Server Fully Qualified Domain	Alias Name	Domain Type	Absolute Domain Name
1 □	207.179.151.101	CollaborativeServer1	L1 domain	myServiceProvider / myCompany.com

10 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

11 Test the configuration changes.

12 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

View a Collaborative Server

Use the following procedure to view a Collaborative Server.

Procedure 22
Viewing a Collaborative Server

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Collaborative Servers.** The **Collaborative Servers** web page opens, displaying a list of configured Collaborative Servers as shown in Figure 82 "Collaborative Servers web page" (page 190).

The Collaborative Servers can be sorted in ascending or descending alphabetical order. See Sort web page by Server Fully Qualified Domain .

2 Select the **Active** or **Standby** database. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The Active database is used for runtime queries. To modify the database it must be in Standby database view. Only Administrators can modify the standby database. One can switch between Active and Standby database views at any time.

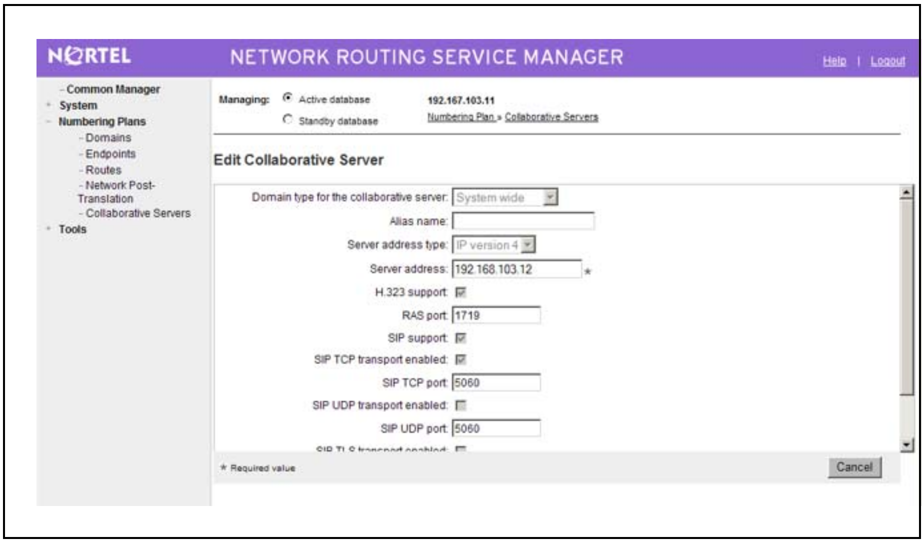
3 Click a **link** in the **Server Fully Qualified Domain** column of the Collaborative Servers web page.

The **Edit Collaborative Server** web page opens and displays the configured data for the selected Collaborative Server.

See Figure 88 "Edit Collaborative Server web page Active database" (page 196).

> ***Note:*** See Procedure 23 "Editing a Collaborative Server" (page 196) to Edit the Collaborative Server.

Figure 88
Edit Collaborative Server web page Active database



Managing: ● Active database ○ Standby database 192.167.103.11

Edit Collaborative Server

Domain type for the collaborative server: System wide

Alias name:

Server address type: IP version 4

Server address: 192.168.103.12 *

H.323 support: ☑

RAS port: 1719

SIP support: ☑

SIP TCP transport enabled: ☑

SIP TCP port: 5060

SIP UDP transport enabled: □

SIP UDP port: 5060

SIP TLS transport enabled: □

* Required value

—End—

Edit a Collaborative Server

Use the following procedure to edit a Collaborative Server.

Procedure 23
Editing a Collaborative Server

Step **Action**

1 In the **NRS Manager Navigator** select **Numbering Plans > Collaborative Servers.** The **Collaborative Servers** web page opens displaying a list of configured Collaborative Servers, as shown in Figure 82 "Collaborative Servers web page" (page 190).

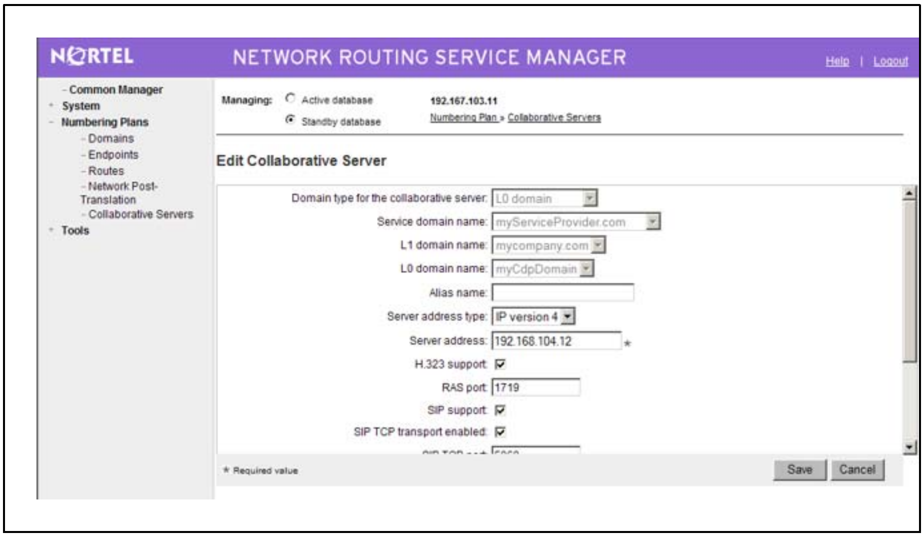
The Collaborative Servers can be sorted in ascending or descending alphabetical order. See Sort web page by Server Fully Qualified Domain .

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164)

3 Click a **link** in the **Server Fully Qualified Domain** column of the Collaborative Servers web page.

The **Edit Collaborative Server** web page opens and displays the configured data for the selected Collaborative Server, as shown in Figure 89 "Edit Collaborative Server web page" (page 197).

Figure 89
Edit Collaborative Server web page



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Collaborative Servers

Edit Collaborative Server

Domain type for the collaborative server: L0 domain

Service domain name: myServiceProvider.com

L1 domain name: mycompany.com

L0 domain name: myCdpDomain

Alias name:

Server address type: IP version 4

Server address: 192.168.104.12 *

H.323 support: ☑

RAS port: 1719

SIP support: ☑

SIP TCP transport enabled: ☑

* Required value

4 Modify the fields of the **Edit Collaborative Server** web page as appropriate. See step 5 to step 8 of Procedure 21 "Adding a Collaborative Server" (page 190).

5 Click **Save**. The standby database is updated.

The **Collaborative Servers** web page opens, as shown in Figure 82 "Collaborative Servers web page" (page 190).

6 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

7 Test the configuration changes.

8 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Delete a Collaborative Server

Use the following procedure to delete a Collaborative Server.

Procedure 24
Deleting a Collaborative Server

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Collaborative Servers.** The **Collaborative Servers** web page

opens displaying a list of configured Collaborative Servers, as shown in Figure 82 "Collaborative Servers web page" (page 190).

The Collaborative Servers can be sorted in ascending or descending alphabetical order. See Sort web page by Server Fully Qualified Domain .

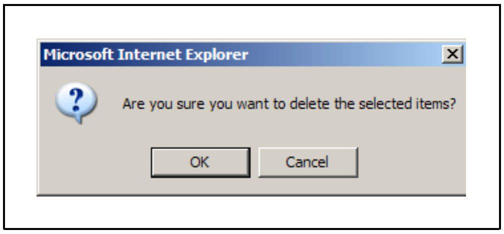
2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164)

3 Select a check box beside one or more **links** in the **Server Fully Qualified Domain** column of the Collaborative Servers web page.

4 Click **Delete**.

A **Confirmation Box** opens requesting confirmation before deleting the selected **Collaborative Server**. See .

Figure 90
Confirmation Box



Microsoft Internet Explorer

Are you sure you want to delete the selected items?

5 Click **OK**. The standby database is updated. The **Collaborative Servers** web refreshes displaying a list of configured collaborative servers, as shown in Figure 82 "Collaborative Servers web page" (page 190).

6 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state.

7 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Manage a Gateway Endpoint

See Procedure 25 "Adding a Gateway Endpoint" (page 199) to add a gateway endpoint.

Add a Gateway Endpoint

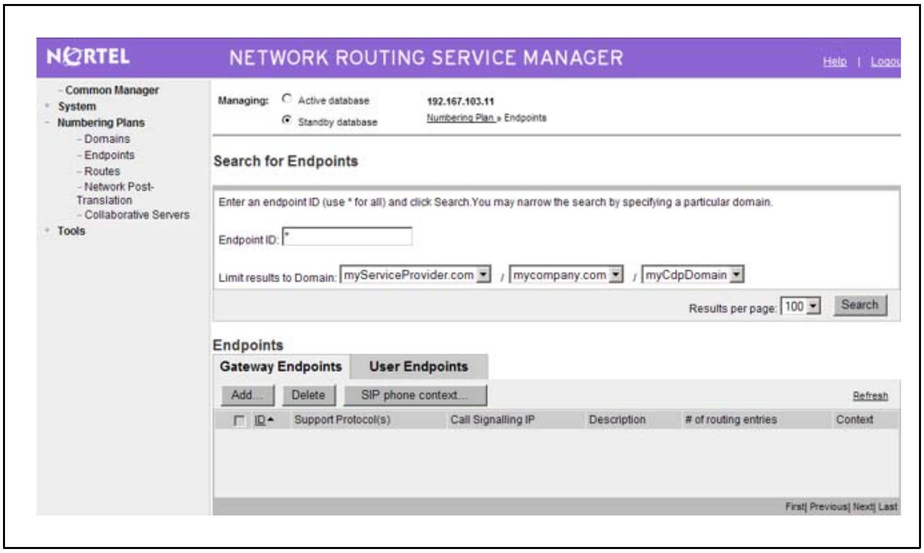
Use the following procedure to add a Gateway Endpoint.

Procedure 25
Adding a Gateway Endpoint

Step	Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).

Figure 91
Endpoints web page



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Endpoints

Search for Endpoints

Enter an endpoint ID (use * for all) and click Search.You may narrow the search by specifying a particular domain.

Endpoint ID: *

Limit results to Domain: myServiceProvider.com / mycompany.com / myCdpDomain

Results per page: 100

□	ID ▲	Support Protocol(s)	Call Signalling IP	Description	# of routing entries	Context

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

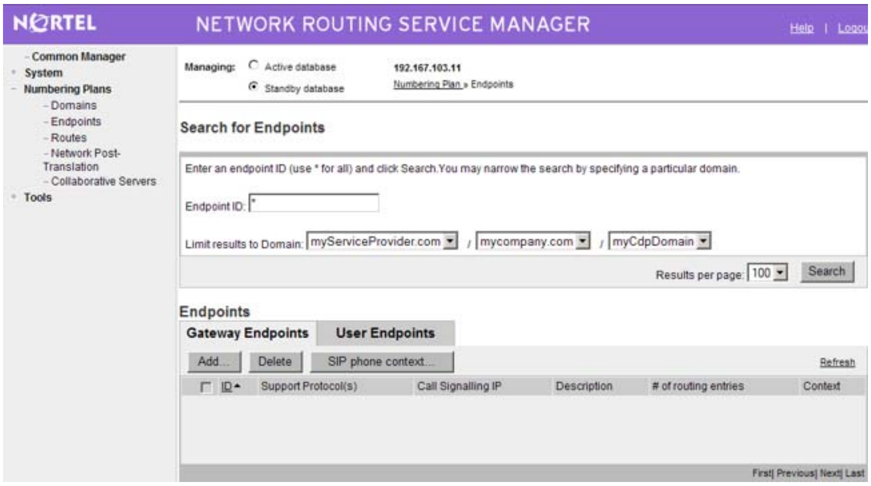
3 The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Click the **Gateway Endpoints** button.

The **Endpoints** web page refreshes displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 92 "Gateway Endpoints pane" (page 200).

The Gateway Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

Figure 92
Gateway Endpoints pane



NORTEL NETWORK ROUTING SERVICE MANAGER Help | Logou

- Common Manager
- System
- Numbering Plans
  - Domains
  - Endpoints
  - Routes
  - Network Post-Translation
  - Collaborative Servers
- Tools

Managing: ○ Active database ● Standby database 192.167.103.11

Numbering Plan » Endpoints

Search for Endpoints

Enter an endpoint ID (use * for all) and click Search.You may narrow the search by specifying a particular domain.

Endpoint ID: *

Limit results to Domain: myServiceProvider.com / mycompany.com / myCdpDomain

Results per page: 100 Search

Endpoints

Gateway Endpoints | User Endpoints

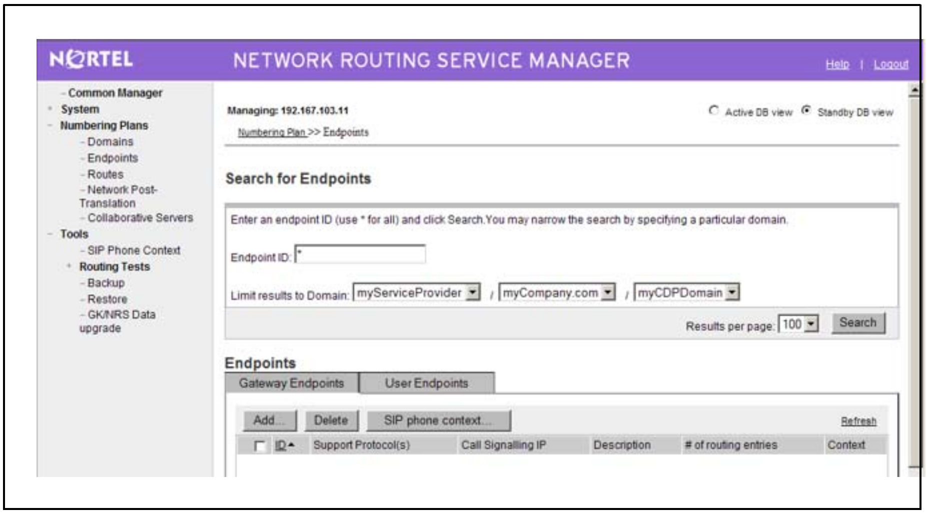
Add... Delete SIP phone context... Refresh

□	ID	Support Protocol(s)	Call Signalling IP	Description	# of routing entries	Context

First| Previous| Next| Last

5 (Optional) Click the **Search** button to display a list of configured Gateway Endpoints associated with the selected Service Domain, L1 domain, and L0 Domain, as shown in Figure 93 "Gateway Endpoints for selected Service Domain, L1 Domain and L0 Domain." (page 200).

Figure 93
Gateway Endpoints for selected Service Domain, L1 Domain and L0 Domain.



NORTEL NETWORK ROUTING SERVICE MANAGER Help | Logout

- Common Manager
- System
- Numbering Plans
  - Domains
  - Endpoints
  - Routes
  - Network Post-Translation
  - Collaborative Servers
- Tools
  - SIP Phone Context
  - Routing Tests
  - Backup
  - Restore
  - GK/NRS Data upgrade

Managing: 192.167.103.11 ○ Active DB view ● Standby DB view

Numbering Plan >> Endpoints

Search for Endpoints

Enter an endpoint ID (use * for all) and click Search.You may narrow the search by specifying a particular domain.

Endpoint ID: *

Limit results to Domain: myServiceProvider / myCompany.com / myCDPDomain

Results per page: 100 Search

Endpoints

Gateway Endpoints | User Endpoints

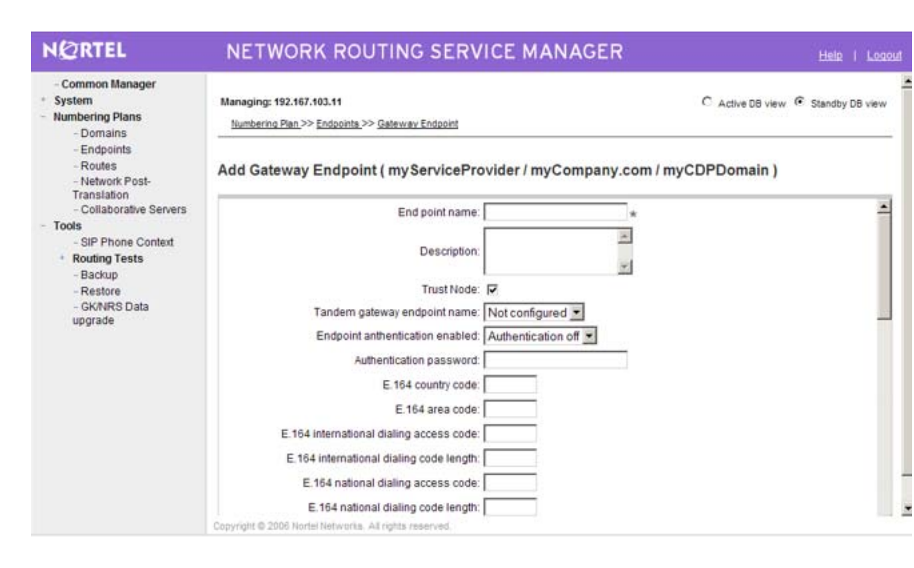
Add... Delete SIP phone context... Refresh

□	ID	Support Protocol(s)	Call Signalling IP	Description	# of routing entries	Context

6 Click the **Add....** button.

The **Add Gateway Endpoint** web page opens, as shown in Figure 94 "Add Gateway Endpoint web page" (page 201).

Figure 94
Add Gateway Endpoint web page



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Add Gateway Endpoint (myServiceProvider / myCompany.com / myCDPDomain)

End point name: *

Description:

Trust Node: ☑

Tandem gateway endpoint name: Not configured

Endpoint anthentication enabled: Authentication off

Authentication password:

E.164 country code:

E.164 area code:

E.164 international dialing access code:

E.164 international dialing code length:

E.164 national dialing access code:

E.164 national dialing code length:

Copyright © 2006 Nortel Networks. All rights reserved.

7 Enter the **Endpoint name** of the gateway in the text box. The name must be alphanumeric and can be up to 30 characters in length.

For example, enter sipGWSite1.

8 Enter a description of the endpoint in the **Description** text box. The description must be alphanumeric and can be up to 120 characters in length.

9 Enter the **Tandem gateway endpoint name** in the text box, if required. This indicates whether the endpoint is used to tandem calls from outside the network. The name must be alphanumeric and can be up to 30 characters in length.

> ***Note:*** A Gateway Endpoint can inherit configuration parameters from the L0 Domain that it exists within. See "Numbering Plans inherited fields" (page 153).

10 Select an option from the **Endpoint authentication enabled** drop-down list.

The three options are:

- **Not configured**: If this option is selected, then the gateway endpoint uses the L1 or L0 Authentication (if L1 or L0 authentication is enabled).
- **Authentication off**: If this option is selected, then authentication is off for this gateway endpoint even if L1 or L0 authentication is enabled.

- **Authentication on**: If this option is selected, then authentication is on for this gateway endpoint and the authentication overrides the L1 or L0 authentication (if it is enabled).

11 Enter the **Authentication password** in the text box, if **Authentication on** was selected in step 10. The password must be alphanumeric and can be up to 24 characters in length.

12 Enter the **E.164 country code** in the text box. The code must be numeric and can be up to eight digits in length.

13 Enter the **E.164 area code** in the text box. The code must be numeric and can be up to eight digits in length.

14 Enter the **E.164 international dialing access code** in the text box. The code must be numeric and can be up to eight digits in length.

15 Enter the **E.164 international dialing code length** in the text box. The code length must be numeric and has to exceed the E.164 international dialing access code length.

16 Enter the **E.164 national dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

17 Enter the **E.164 national dialing code length** in the text box. The code length must be numeric and has to exceed the E.164 national dialing access code length.

18 Enter the **E.164 local (subscriber) dialing access code** in the text box. The code must be numeric and can be up to eight digits in length.

19 Enter the **E.164 local (subscriber) dialing code length** in the text box. The code length must be numeric and has to exceed the E.164 local (subscriber) dialing access code length.

20 Enter the **Private L1 domain (UDP location) dialing access code** in the text box. The code must be numeric and can be up to eight digits in length.

21 Enter the **Private L1 domain (UDP location) dialing code length** in the text box. The code length must be numeric and has to exceed the Private L1 domain (UDP location) dialing access code length.

22 Enter the **Private special number 1** in the text box. The number must be numeric and can be up to 30 digits in length.

23 Enter the **Private special number 1 dialing code length** in the text box. The code length must be numeric and equal to the Private special number 1 length.

24 Enter the **Private special number 2** in the text box. The number must be numeric and can be up to 30 digits in length

25 Enter the **Private special number 2 dialing code length** in the text box. The code length must be numeric and equal to the Private special number 2 length.

26 Select **IP Version 4** from the **Static endpoint address type** drop-down list.

27 Enter the **Static endpoint address** in the text box.

This is the Node IP address of the Signaling Server. If a third-party gateway is being used, then it is the IP address of the gateway.

28 Select whether H.323 support is enabled from the **H.323 Support** drop-down list.

The three options are:

- H.323 not supported
- RAS H.323 endpoint
- Not RAS H.323 endpoint.

Note 1: If an H.323 Gateway Endpoint is configured with an H.323 Support type of RAS H.323 endpoint, then NRS Manager displays Endpoint Dynamic Registration information after the H.323 Gateway registers with the NRS.

Note 2: Endpoint Dynamic Registration information includes the following: Call Signaling IP, RAS IP, Alias name, t35Country code, t35Extension, Manufacturer code, Product ID, and Version ID.

Note 3: The H.323 **Endpoint Dynamic Registration Information** is displayed only when NRS Manager is in **Active database** view. The detailed dynamic registration information also is displayed only inside the Gateway Endpoint web page. See Procedure 26 "Viewing Gateway Endpoint Dynamic Registration Information" (page 206).

29 Configure SIP support.

a. Select an option from the **SIP Support** drop-down list. The three options are: SIP not supported, Static SIP endpoint, and Dynamic SIP endpoint.

b. If SIP support is enabled, select the transport protocol:

- If SIP TCP is supported, perform the following steps:

  - — Select the **SIP TCP transport enabled** check box.
  - — Enter the **SIP TCP port** number in the text box. The port number must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port value is 5060.

- If SIP UDP is supported, perform the following steps
  - — Select the **SIP UDP transport enabled** check box.
  - — Enter the **SIP UDP port** number in the text box. The port number must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port value is 5060.

- If SIP TLS is supported, perform the following steps:
  - — Select the **SIP TLS transport enabled** check box.
  - — Enter the **SIP TLS port** number in the text box. The port number must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port value is 50601.

Note: If a SIP Trunk Gateway Endpoint is configured with a SIP Support type of Dynamic SIP endpoint, then NRS Manager displays Endpoint Dynamic Registration Information for SIP after the SIP Trunk Gateway registers with the NRS.

Endpoint Dynamic Registration Information includes the following: SIP IP, Registration expiry time, User agent, and Preference.

The SIP **Endpoint Dynamic Registration Information** is displayed only when NRS Manager is in **Active DB view**. The detailed dynamic registration information also is displayed only inside the Gateway Endpoint web page. See Procedure 26 "Viewing Gateway Endpoint Dynamic Registration Information" (page 206).

30 If **End to end security** is supported, select the End to end security check box.

31 Select whether Redundancy is enabled from the **Redundancy enabled** drop-down list.

The three options are:

- Not configured
- Main Office

- Redundant Office

Geographic redundant gateways (Main Office and Redundant office endpoints) can be linked.

To set the main endpoint

- select **Main Office** from the **Redundancy enabled** drop-down list
- select the desired endpoint name in the **Redundant endpoint name** field

To set the redundant endpoint

- select **Redundant Office** from the **Redundancy enabled** drop-down list
- select the desired endpoint name in the **Main endpoint name** field

If two endpoints are linked (configured properly), NRS Manager will prompt the user to configure routes for the redundant endpoint with pre-set values when routes are added to the main endpoint. This feature enables the configuration of two routes (one for the main office endpoint and one for the redundant office endpoint) at the same time with pre-set values.

32 Select the **Network Connection Server is enabled** check box if this Gateway Endpoint supports the NCS for branch office or SRG user redirection to the main office, Virtual Office, or Geographic Redundancy.

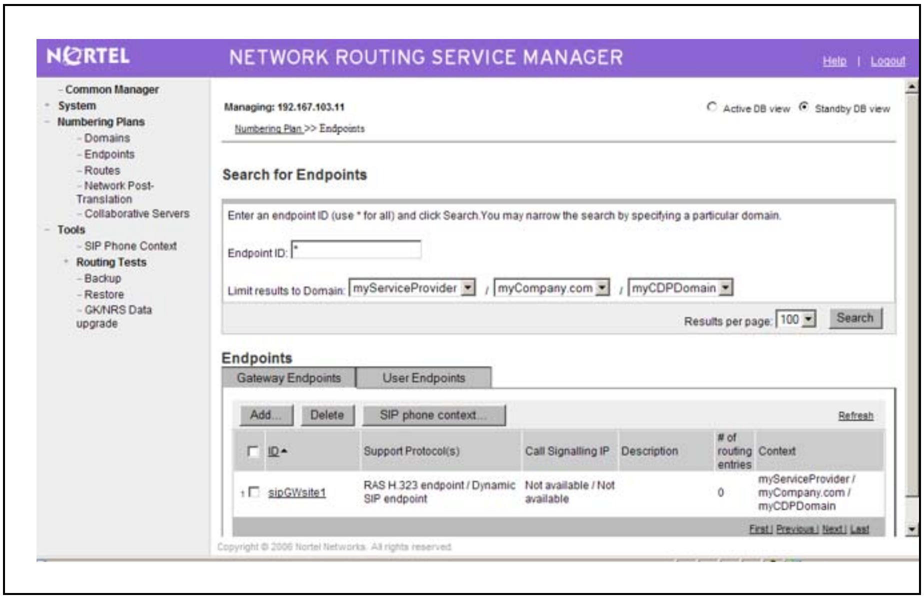
33 The **Main endpoint name** is dynamically generated based on the Gateway Endpoint configuration. The default selection is **Not configured**.

34 The **Redundant endpoint name** is dynamically generated based on the Gateway Endpoint configuration. The default selection is **Not configured**.

35 Click the **Save** button. The standby database is updated.

The **Gateway Endpoints** web page opens, showing the newly added sipGWSite1 endpoint. See Figure 95 "Gateway Endpoints web page for added Gateway Endpoint" (page 206).

Figure 95
Gateway Endpoints web page for added Gateway Endpoint



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Endpoints

Search for Endpoints

Enter an endpoint ID (use * for all) and click Search.You may narrow the search by specifying a particular domain.

Endpoint ID: *

Limit results to Domain: myServiceProvider / myCompany.com / myCDPDomain

Results per page: 100 Search

Endpoints

□	ID	Support Protocol(s)	Call Signalling IP	Description	# of routing entries	Context
1 □	sipGWsite1	RAS H.323 endpoint / Dynamic SIP endpoint	Not available / Not available		0	myServiceProvider / myCompany.com / myCDPDomain

First | Previous | Next | Last
Copyright © 2006 Nortel Networks. All rights reserved.

36 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

37 Test the configuration changes.

38 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

View Gateway Endpoint Dynamic Registration Information

Use the following procedure to view the Gateway Endpoint Dynamic Registration Information.

Procedure 26
Viewing Gateway Endpoint Dynamic Registration Information

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).

2 Ensure **Active database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

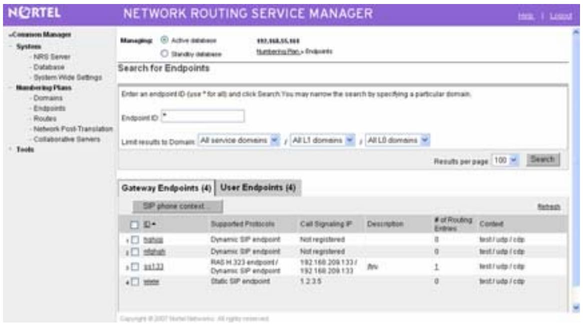
3 The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Click the **Gateway Endpoints** button.

The **Endpoints** web page refreshes displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 96 "Gateway Endpoints Summary web page" (page 207).

The Gateway Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

Figure 96
Gateway Endpoints Summary web page



Managing: ● Active database ○ Standby database 192.168.55.161
Numbering Plan > Endpoints

Search for Endpoints

Enter an endpoint ID (use * for all) and click Search. You may narrow the search by specifying a particular domain.

Endpoint ID: *

Limit results to Domain: All service domains / All L1 domains / All L0 domains

Results per page: 100 Search

Gateway Endpoints (4) | User Endpoints (4)

SIP phone context... Refresh

	□ ID ▲	Supported Protocols	Call Signaling IP	Description	# of Routing Entries	Context
1	□ hghgg	Dynamic SIP endpoint	Not registered		0	test / udp / cdp
2	□ nfghgh	Dynamic SIP endpoint	Not registered		0	test / udp / cdp
3	□ ss133	RAS H.323 endpoint / Dynamic SIP endpoint	192.168.209.133 / 192.168.209.133	/bv	1	test / udp / cdp
4	□ wwww	Static SIP endpoint	1.2.3.5		0	test / udp / cdp

Copyright © 2007 Nortel Networks. All rights reserved.

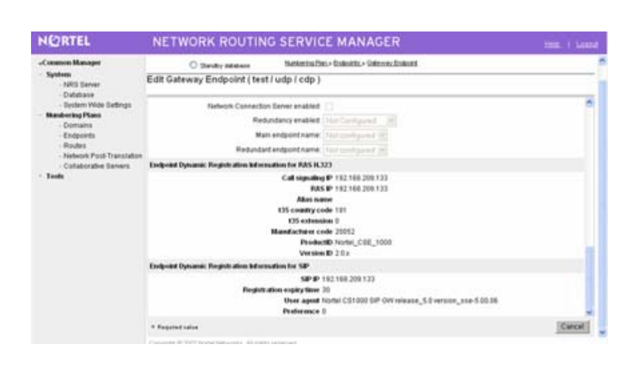
5 Click a **link** in the **ID** column of the **Endpoints** pane.

The **Edit Gateway Endpoint** web page opens and displays the configured data for the selected Gateway Endpoint, as shown in Figure 99 "Edit Gateway Endpoint web page Active database" (page 210).

> ***Note 1:*** If an H.323 Gateway Endpoint is configured with an H.323 Support type of RAS H.323 endpoint, then NRS Manager displays Endpoint Dynamic Registration information after the H.323 Gateway registers with the NRS. Endpoint Dynamic Registration information includes the following: Call Signaling IP, RAS IP, Alias name, t35Country code, t35Extension, Manufacturer code, Product ID, and Version ID.
>
> ***Note 2:*** If a SIP Trunk Gateway Endpoint is configured with a SIP Support type of Dynamic SIP endpoint, then NRS Manager displays Endpoint Dynamic Registration Information for SIP after the SIP Trunk Gateway registers with the NRS. Endpoint Dynamic Registration Information includes the following: SIP IP, Registration expiry time, User agent, and Preference.

6 Scroll down the page to display **Endpoint Dynamic Registration Information for RAS H.323** and **Endpoint Dynamic Registration Information for SIP**, as shown in Figure 97 "Gateway Endpoints Property web page" (page 208).

Figure 97
Gateway Endpoints Property web page



Edit Gateway Endpoint (test / udp / cdp)

Network Connection Server enabled: □
Redundancy enabled: Not Configured
Main endpoint name: Not configured
Redundant endpoint name: Not configured

Endpoint Dynamic Registration Information for RAS H.323

Call signaling IP 192.168.209.133
RAS IP 192.168.209.133
Alias name
E35 country code 101
E35 extension 0
Manufacturer code 20052
ProductID Nortel_CSE_1000
Version ID 2.0.x

Endpoint Dynamic Registration Information for SIP

SIP IP 192.168.209.133
Registration expiry time 30
User agent Nortel CS1000 SIP GW release_5.0 version_sse-5.00.06
Preference 0

* Required value

Copyright © 2007 Nortel Networks. All rights reserved.

—End—

View the Gateway Endpoints

Use the following procedure to view the Gateway Endpoints.

Procedure 27
Viewing the Gateway Endpoints

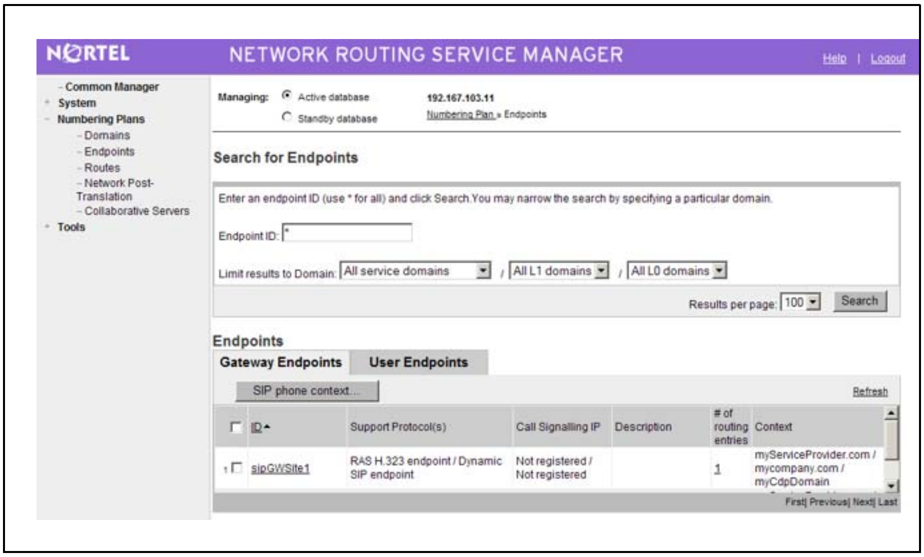
Step	Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).

2 Select the **Active** or **Standby** database. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The Active database is used for runtime queries. To modify the database it must be in Standby database view. Only Administrators can modify the standby database. One can switch between Active and Standby database views at any time.

The **Endpoints** web page refreshes, as shown in Figure 98 "Endpoints web page Active database" (page 209).

Figure 98
Endpoints web page Active database



Managing: ● Active database ○ Standby database 192.167.103.11

Enter an endpoint ID (use * for all) and click Search.You may narrow the search by specifying a particular domain.

Endpoint ID: *

Limit results to Domain: All service domains / All L1 domains / All L0 domains

Results per page: 100

□	ID▲	Support Protocol(s)	Call Signalling IP	Description	# of routing entries	Context
1 □	sipGWSite1	RAS H.323 endpoint / Dynamic SIP endpoint	Not registered / Not registered		1	myServiceProvider.com / mycompany.com / myCdpDomain

3 The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Click the **Gateway Endpoints** button. The **Endpoints** web page refreshes displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 92 "Gateway Endpoints pane" (page 200).

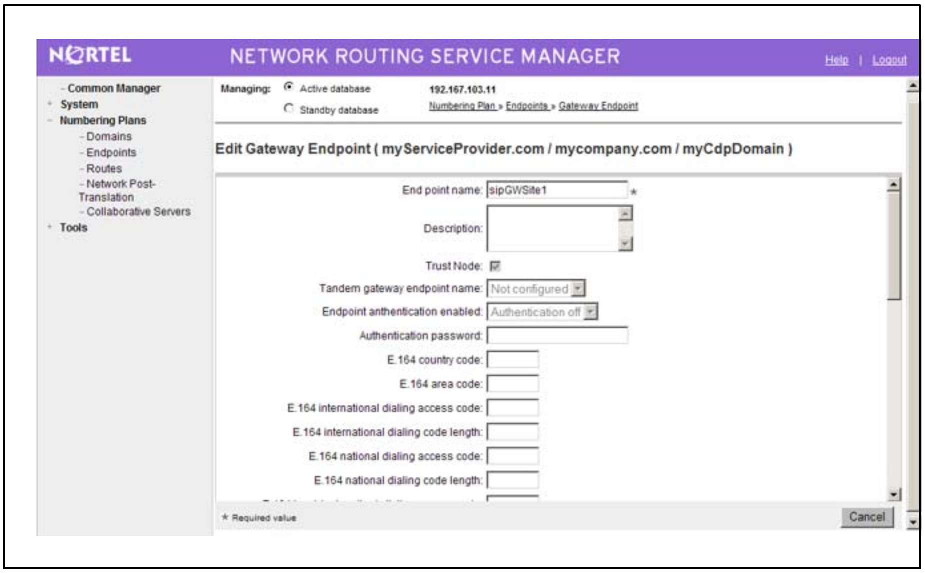
The Gateway Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

5 Click a **link** in the **ID** column of the **Endpoints** pane.

The **Edit Gateway Endpoint** web page opens and displays the configured data for the selected Gateway Endpoint, as shown in Figure 99 "Edit Gateway Endpoint web page Active database" (page 210).

> ***Note:*** See Procedure 28 "Editing the Gateway Endpoints" (page 210) to Edit the Gateway Endpoint.

Figure 99
Edit Gateway Endpoint web page Active database



Managing: ● Active database ○ Standby database

192.167.103.11

Edit Gateway Endpoint (myServiceProvider.com / mycompany.com / myCdpDomain)

End point name: sipGWSite1 *

Description:

Trust Node: ☑

Tandem gateway endpoint name: Not configured

Endpoint anthentication enabled: Authentication off

Authentication password:

E.164 country code:

E.164 area code:

E.164 international dialing access code:

E.164 international dialing code length:

E.164 national dialing access code:

E.164 national dialing code length:

* Required value

—End—

Edit the Gateway Endpoints

Use the following procedure to edit the Gateway Endpoints.

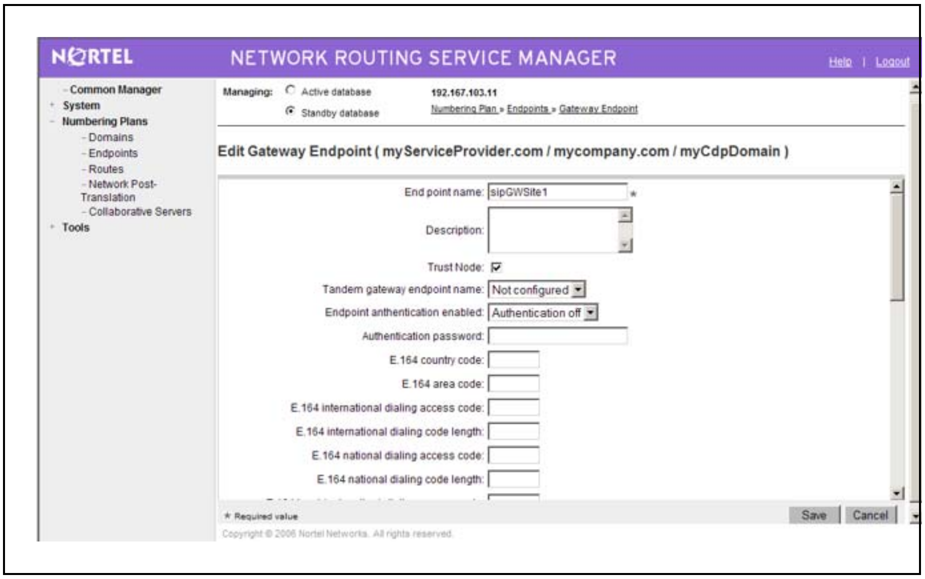
Procedure 28
Editing the Gateway Endpoints

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).
2	Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).
3	The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.
4	Click the **Gateway Endpoints** button. The **Endpoints** web page refreshes displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 92 "Gateway Endpoints pane" (page 200).

The Gateway Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

5 Click a **link** in the **ID** column of the Endpoints pane. The **Edit Gateway Endpoint** web page opens and displays the configured data for the selected Gateway Endpoint, as shown in Figure 100 "Edit Gateway Endpoint web page" (page 211).

Figure 100
Edit Gateway Endpoint web page



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Endpoints » Gateway Endpoint

Edit Gateway Endpoint (myServiceProvider.com / mycompany.com / myCdpDomain)

End point name: sipGWSite1 *

Description:

Trust Node: ☑

Tandem gateway endpoint name: Not configured

Endpoint anthentication enabled: Authentication off

Authentication password:

E.164 country code:

E.164 area code:

E.164 international dialing access code:

E.164 international dialing code length:

E.164 national dialing access code:

E.164 national dialing code length:

* Required value

Copyright © 2006 Nortel Networks. All rights reserved.

Note: A Gateway Endpoint can inherit configuration parameters from the L0 Domain that it exists within . See "Numbering Plans inherited fields" (page 153).

6 Modify the fields of the **Edit Gateway Endpoint** web page as appropriate. See step 7 to step 34 of Procedure 25 "Adding a Gateway Endpoint" (page 199).

7 Click the **Save** button. The standby database is updated. The **Endpoints** web page opens displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 92 "Gateway Endpoints pane" (page 200).

8 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

9 Test the configuration changes.

10 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

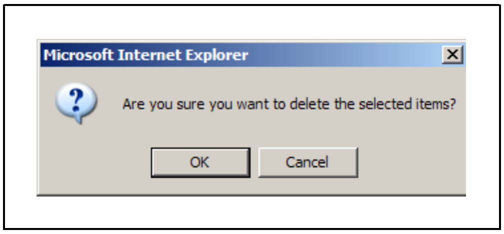
Delete the Gateway Endpoints

Use the following procedure to delete the Gateway Endpoints.

Procedure 29
Deleting the Gateway Endpoints

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).
2	Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).
3	The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.
4	Click the **Gateway Endpoints** button. The **Endpoints** web page opens displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 92 "Gateway Endpoints pane" (page 200). The Gateway Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by ID.
5	Select a check box beside one or more **links** in the **ID** column of the Endpoints pane.
6	Click **Delete**. A **Confirmation Box** opens requesting confirmation before deleting the selected **Gateway Endpoint**, as shown in Figure 101 "Confirmation Box" (page 212).

Figure 101
Confirmation Box



Microsoft Internet Explorer

Are you sure you want to delete the selected items?

7 Click **OK**. The standby database is updated. The **Endpoints** web page refreshes displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 92 "Gateway Endpoints pane" (page 200).

8 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state.

9 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Manage Post-routing SIP URI Modification

Add Post-routing SIP URI Modification

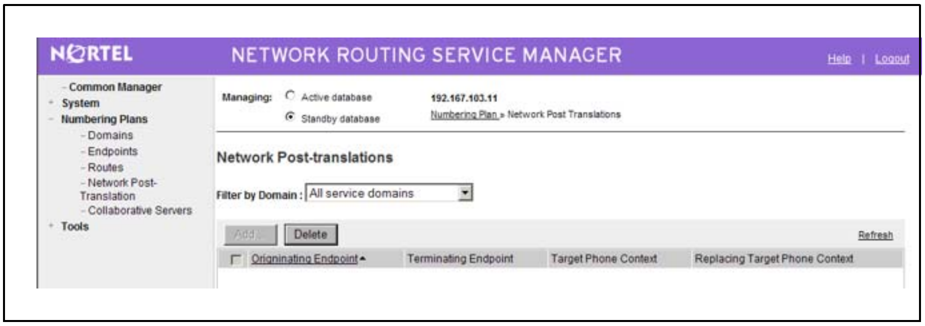
Use the following procedure to add Post-routing SIP URI Modification.

Procedure 30
Adding Post-routing SIP URI Modification

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Network Post-Translation.** The **Network Post-translations** web page opens, as shown in Figure 102 "Network Post-translations web page" (page 213).

Figure 102
Network Post-translations web page



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Network Post Translations

Network Post-translations

Filter by Domain : All service domains

□	Originating Endpoint ▲	Terminating Endpoint	Target Phone Context	Replacing Target Phone Context

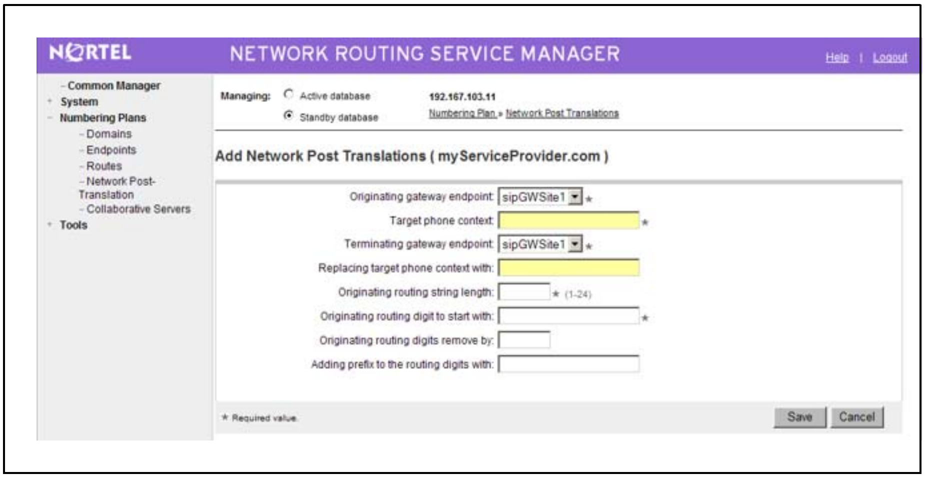
2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

3 Select a **Service domain** from the **Filter by Domain:** drop-down list.

4 Click the **Add....** button.

The **Add Network Post Translations** web page opens, as shown in Figure 103 "Add Network Post Translations web page" (page 214).

Figure 103
Add Network Post Translations web page



Managing: ○ Active database ● Standby database 192.167.103.11

Add Network Post Translations (myServiceProvider.com)

Originating gateway endpoint:	sipGWSite1 *
Target phone context:	*
Terminating gateway endpoint:	sipGWSite1 *
Replacing target phone context with:	
Originating routing string length:	* (1-24)
Originating routing digit to start with:	*
Originating routing digits remove by:	
Adding prefix to the routing digits with:	

* Required value.

5 Select an **Originating gateway endpoint** from the drop down list.

6 Enter a **Target phone context** in the text box. The name must be alphanumeric and can be up to 64 characters in length.

7 Select a **Terminating gateway endpoint** from the drop down list.

8 Enter a **Replacing target phone context with** in the text box. The name must be alphanumeric and can be up to 64 characters in length.

9 Enter an **Originating routing string length** in the text box. The string length must be numeric and can be up to 5 digits in length.

10 Enter an **Originating routing digit to start with** in the text box. The parameter must be numeric and can be up to 24 digits in length.

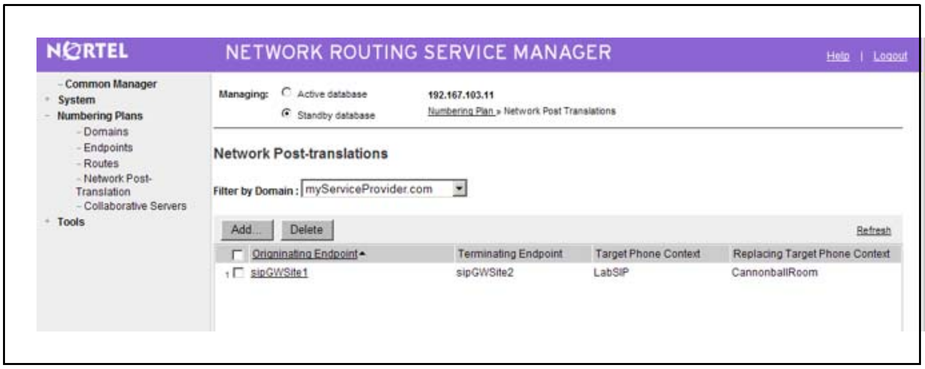
11 Enter an **Originating routing digits to remove by** in the text box. The parameter must be numeric and ***can not*** exceed the value of the **Originating routing string length** in step 9.

12 Enter a **Adding prefix to the routing digits with** in the text box. The parameter must be numeric and can be up to 64 digits in length. The parameter ***can not*** contain a leading + character.

13 Click the **Save** button. The standby database is updated.

The **Network Post-translations** web page opens displaying the added Network Post-translation, as shown in Figure 104 "Added Network Post-translations web page" (page 215).

Figure 104
Added Network Post-translations web page



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Network Post Translations

Network Post-translations

Filter by Domain : myServiceProvider.com

	□	Originating Endpoint▲	Terminating Endpoint	Target Phone Context	Replacing Target Phone Context
1	□	sipGWSite1	sipGWSite2	LabSIP	CannonballRoom

14 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

15 Test the configuration changes.

16 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

View Post-routing SIP URI Modification

Use the following procedure to view Post-routing SIP URI Modification.

Procedure 31
Viewing Post-routing SIP URI Modification

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Network Post-Translation.** The **Network Post-translations** web page opens, as shown in Figure 102 "Network Post-translations web page" (page 213).

2 Select the **Active** or **Standby** database. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The Active database is used for runtime queries. To modify the database it must be in Standby database view. Only Administrators can modify the standby database. One can switch between Active and Standby database views at any time. The **Network Post-translations** web page refreshes, as shown in Figure 102 "Network Post-translations web page" (page 213).

3 Select a **Service domain** from the **Filter by Domain:** drop-down list.

4 Click the **Refresh** link.

The **Network Post-translations** web page refreshes displaying a list of **Originating Endpoints**.

The Originating Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by Originating Endpoint.

5 Click a **link** in the **Originating Endpoint** column of the **Network Post-translations** web page.

The **Edit Network Post Translations** web page opens, as shown in Figure 105 "Edit Network Post Translations web page" (page 217), and displays the configured data for the selected Network Post Translation.

—End—

Edit Post-routing SIP URI Modification

Use the following procedure to edit Post-routing SIP URI Modification.

Procedure 32
Editing Post-routing SIP URI Modification

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Network Post-Translation.** The **Network Post-translations** web page opens, as shown in Figure 102 "Network Post-translations web page" (page 213).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

3 Select a **Service domain** from the **Filter by Domain:** drop-down list.

4 Click the **Refresh** link.

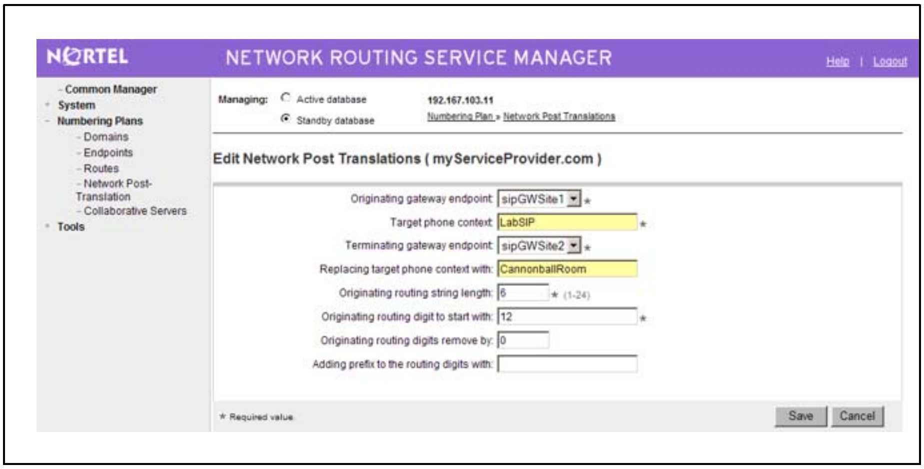
The **Network Post-translations** web page refreshes displaying a list of **Originating Endpoints**.

The Originating Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by Originating Endpoint.

5 Click a **link** in the **Originating Endpoint** column of the *Network Post-translations* web page.

The **Edit Network Post Translations** web page opens, as shown in Figure 105 "Edit Network Post Translations web page" (page 217), and displays the configured data for the selected Network Post Translation.

Figure 105
Edit Network Post Translations web page



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Network Post Translations

Edit Network Post Translations (myServiceProvider.com)

Originating gateway endpoint: sipGWSite1 *

Target phone context: LabSIP *

Terminating gateway endpoint: sipGWSite2 *

Replacing target phone context with: CannonballRoom

Originating routing string length: 6 * (1-24)

Originating routing digit to start with: 12 *

Originating routing digits remove by: 0

Adding prefix to the routing digits with:

* Required value.

6 Modify the fields of the**Edit Network Post Translations** web page as appropriate. See step 5 to step 12 of Procedure 30 "Adding Post-routing SIP URI Modification" (page 213).

7 Click the **Save** button. The standby database is updated.

The **Network Post-translations** web page opens, as shown in Figure 102 "Network Post-translations web page" (page 213).

8 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

9 Test the configuration changes.

10 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Delete Post-routing SIP URI Modification

Use the following procedure to delete Post-routing SIP URI Modification.

Procedure 33
Deleting Post-routing SIP URI Modification

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Network Post-Translation.** The **Network Post-translations** web page opens, as shown in Figure 102 "Network Post-translations web page" (page 213).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

3 Select a **Service domain** from the **Filter by Domain:** drop-down list.

4 Click the Refresh link.

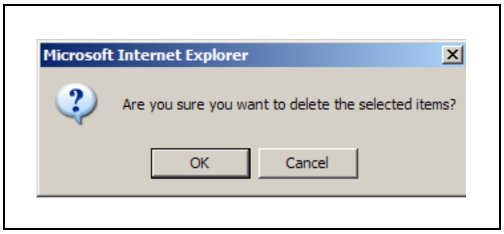
The **Network Post-translations** web page refreshes displaying a list of **Originating Endpoints**.

The Originating Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by Originating Endpoint.

5 Select a check box beside one or more **links** in the **Originating Endpoint** column of the Network Post-translations web page.

6 Click the **Delete** button. A **Confirmation Box** opens, as shown in Figure 106 "Confirmation Box" (page 218), requesting confirmation before deleting the selected **Network Post Translation**.

Figure 106
Confirmation Box


Microsoft Internet Explorer

Are you sure you want to delete the selected items?

7 Click **OK**. The standby database is updated.

The **Network Post-translations** web page opens, as shown in Figure 102 "Network Post-translations web page" (page 213).

8 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

9 Test the configuration changes.

10 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Manage a User Endpoint

A SIP Phone registers and communicates as a user endpoint in the NRS. To add a User Endpoint, refer to Procedure 34 "Adding a User Endpoint" (page 219).

Unqualified number routing

To support routing of unqualified numbers dialed by SIP Phones, the NRS provides several types of dialing prefixes at the Level 1 regional domain, Level 0 regional domain, and for endpoints. The dialing prefixes include the following:

- E.164 International dialing access code (for example, 6011)
- E.164 National dialing access code (for example, 61)
- E.164 Local dialing access code (for example, 9)
- Level 1 Regional dialing access code (for example, 6)
- Level 0 Regional dialing access code (the default, if none of above match)

Up to two special numbers can be specified at L1 and/or L0.

Task summary

Before a SIP Phone can be added as a User Endpoint in the NRS, the Service Domain, Level 1 Regional Domain, and Level 0 Regional Domain must be configured. To complete these tasks, see

- Procedure 9 "Adding a Service Domain" (page 166)
- Procedure 13 "Adding an L1 Domain (UDP)" (page 172)
- Procedure 17 "Adding an L0 Domain (CDP)" (page 181)

Add a User Endpoint

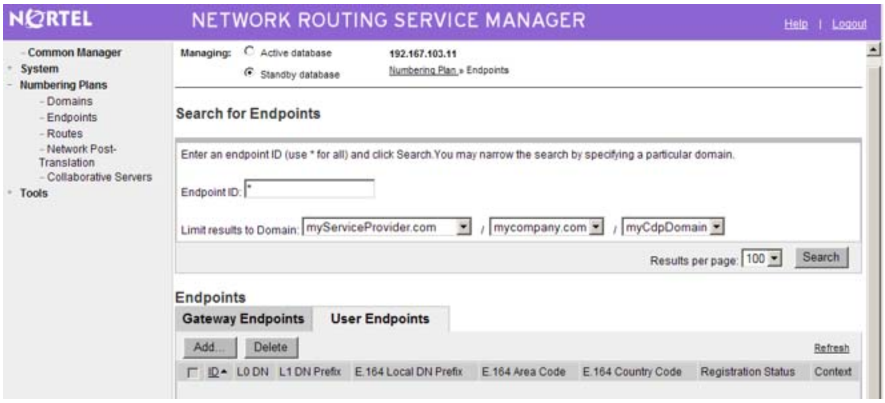
Use the following procedure to add a User Endpoint.

Procedure 34
Adding a User Endpoint

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).
2	Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).
3	The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Click the **User Endpoints** button. The **Endpoints** web page opens displaying a list of configured User Endpoints in the Endpoints pane, as shown in Figure 107 "User Endpoints pane" (page 220).

Figure 107
User Endpoints pane



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Endpoints

Search for Endpoints

Enter an endpoint ID (use * for all) and click Search.You may narrow the search by specifying a particular domain.

Endpoint ID: *

Limit results to Domain: myServiceProvider.com / mycompany.com / myCdpDomain

Results per page: 100 Search

Endpoints

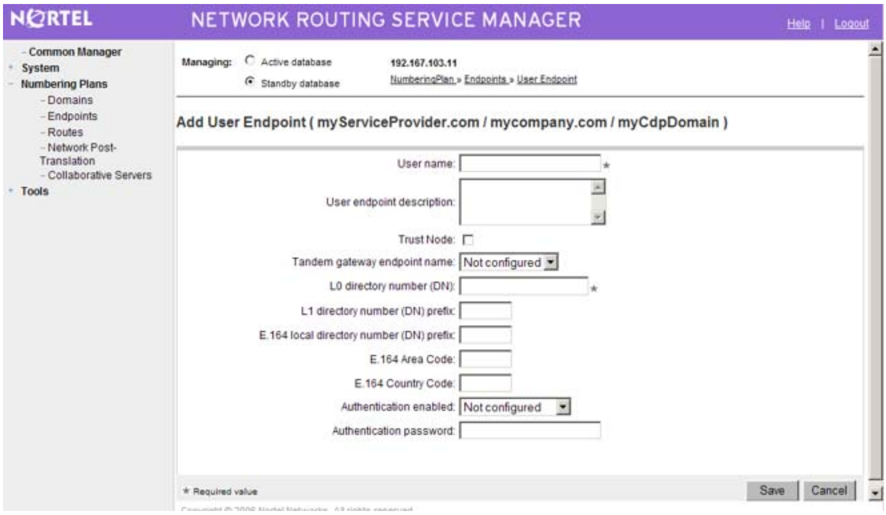
Gateway Endpoints | User Endpoints

Add... Delete Refresh

□	ID	L0 DN	L1 DN Prefix	E.164 Local DN Prefix	E.164 Area Code	E.164 Country Code	Registration Status	Context

5 Click the **Add....** button. The **Add User Endpoint** web page opens, as shown in Figure 108 "Add User Endpoint web page" (page 220).

Figure 108
Add User Endpoint web page



Managing: ○ Active database ● Standby database

192.167.103.11

NumberingPlan » Endpoints » User Endpoint

Add User Endpoint (myServiceProvider.com / mycompany.com / myCdpDomain)

User name: *

User endpoint description:

Trust Node: □

Tandem gateway endpoint name: Not configured

L0 directory number (DN): *

L1 directory number (DN) prefix:

E.164 local directory number (DN) prefix:

E.164 Area Code:

E.164 Country Code:

Authentication enabled: Not configured

Authentication password:

* Required value

Save Cancel

6 Enter a **User name** for the endpoint. The endpoint's user name must be alphanumeric and can be up to 30 characters in length.

The user name, together with the Service Domain names, becomes a string that is used to build the user's SIP URI:

Example: [username]@[service_domain_name]

This SIP URI is used during SIP Phone registration. The username is used by the SIP authentication procedures.

7 Enter the **User endpoint description**. The endpoint's description must be alphanumeric (except single quotes) and can be up to 120 characters in length.

8 Check the **Trust Node:** check box.

9 Enter the **Tandem gateway endpoint name**. The name must be alphanumeric and can be up to 30 characters in length

A tandem gateway endpoint must be an existing endpoint on the network. It is usually a Gateway Endpoint. The tandem gateway endpoint name is used to tandem all calls originating from this User Endpoint. That is, all calls originating from this User Endpoint are forwarded to the tandem gateway endpoint, which then routes all the call to the appropriate destinations. This is useful for generating Call Records for originating User Endpoint calls.

> ***Note:*** A tandem gateway endpoint must ONLY be configured if the customer wants all the outgoing calls from the SIP User Endpoint to tandem through a SIP Trunk Gateway Endpoint, in that case the SIP Trunk Gateway Endpoint name should be specified in the tandem endpoint box.

10 Enter the **L0 directory number (DN)** of the User Endpoint. The DN must be numeric and can be up to 30 digits in length.

An example is 5000. The DN is the user's DN. That is, the CDP number.

11 Enter the **L1 directory number (DN) prefix**. The DN prefix must be numeric and can be up to eight digits in length.

An example is 343. The L1 DN prefix together with the L0 DN creates the user's DN which is unique within the parent L1 Regional Domain. That is, the UDP number. For example, 3435000.

L1 domain prefix + L0 DN = User's DN
343 + 5000 = 3435000

12 Enter the **E.164 local directory number (DN) prefix**. The DN prefix must be numeric and can be up to eight digits in length.

An example is 967. The E.164 local DN prefix is the location code. The E.164 local prefix, together with the L0 DN, creates the user's E.164 Local (subscriber) DN. For example, 9675000.

E.164 local prefix + L0 DN = User's E.164 Local (subscriber) DN 967 + 5000 = 9675000

13 Enter the **E.164 area code**. The code must be numeric and can be up to eight digits in length.

An example is 613. The E.164 area code together with both the E.164 local prefix and L0 DN creates the user's national E.164 National DN. For example, 6139675000.

E.164 area code + E.164 local prefix + L0 DN = User's E.164 National DN 613 + 967 + 5000 = 6139675000

14 Enter the **E.164 country code**. The code must be numeric and can be up to eight digits in length.

An example is 1 (for North America). The E.164 country code, together with the E.164 area code, E.164 local prefix, and L0 DN, creates the user's E.164 International DN. For example, 16139675000.

E.164 country code + E.164 area code + E.164 local prefix + L0 DN = User's E.164 International DN
1 + 613 + 967 + 5000 = 16139675000

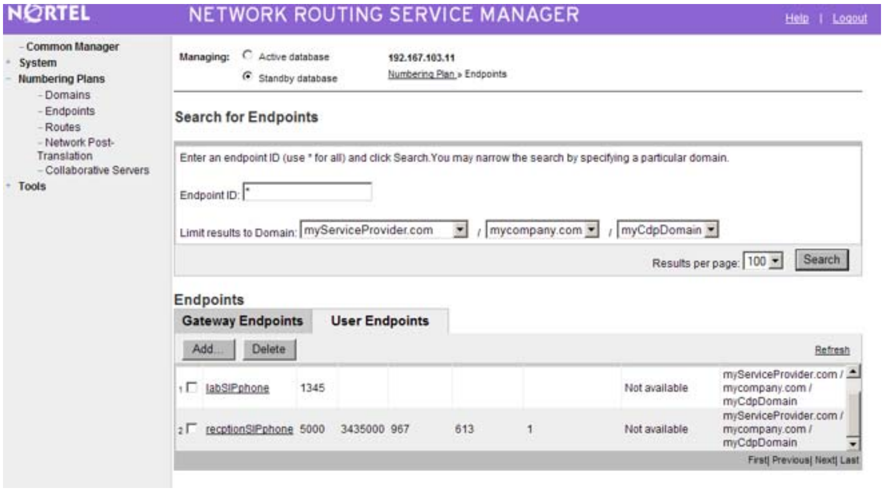
15 Select **Authentication** on from the **Authentication enabled** drop-down list, if you want to enable authentication for this endpoint.

16 If authentication is enabled in , then enter the **Authentication password**. The password must be alphanumeric and can be up to 24 characters in length.

17 Click the **Save** button. The standby database is updated.

The **Endpoints** web page opens, showing the newly added User Endpoint in the **User Endpoints** pane. See Figure 109 "Added User Endpoints" (page 223).

Figure 109
Added User Endpoints



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Endpoints

Search for Endpoints

Enter an endpoint ID (use * for all) and click Search.You may narrow the search by specifying a particular domain.

Endpoint ID: *

Limit results to Domain: myServiceProvider.com / mycompany.com / myCdpDomain

Results per page: 100

Endpoints

1	□	labSIPphone	1345					Not available	myServiceProvider.com / mycompany.com / myCdpDomain
2	□	recptionSIPphone	5000	3435000	967	613	1	Not available	myServiceProvider.com / mycompany.com / myCdpDomain

18 If required, click **Add...** to add additional User Endpoints. Repeat step 6 to step 17.

Any new endpoints are displayed in the **User Endpoints** web page.

> ***Note 1:*** A maximum of 100 user endpoints can be displayed on the **User Endpoints** web page.
>
> ***Note 2:*** If a User Endpoint is configured, then the supported protocol type is dynamic SIP. NRS Manager displays User Endpoint Dynamic Registration Information after the User Endpoint registers with the NRS.
>
> User Endpoint Dynamic Registration information includes the following: SIP IP, Registration expiry time, User agent, and Preference.
>
> The **User Endpoint Dynamic Registration Information** is displayed only when NRS Manager is in Active database mode. Detailed dynamic registration information is displayed inside the **User Endpoints Property** web page. See Procedure 35 "Viewing User Endpoint Dynamic Registration Information" (page 224).

19 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

20 Test the configuration changes.

21 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

View User Endpoint Dynamic Registration Information

Use the following procedure to view the User Endpoint Dynamic Registration Information.

Procedure 35
Viewing User Endpoint Dynamic Registration Information

Step Action

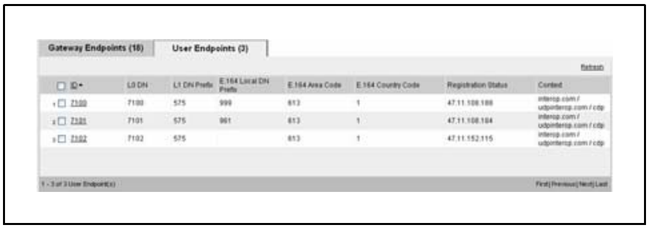
1 In the **NRS Manager Navigator** select **Numbering Plans > Endpoints**. The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).

2 Ensure **Active database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

3 The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Click the **User Endpoints** button. The **Endpoints** web page refreshes displaying a list of configured User Endpoints in the Endpoints pane, as shown in Figure 110 "User Endpoints Summary web page" (page 224). The User Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

Figure 110
User Endpoints Summary web page



	□ ID ▾	L0 DN	L1 DN Prefix	E.164 Local DN Prefix	E.164 Area Code	E.164 Country Code	Registration Status	Contact
1	□ 7100	7100	575	999	613	1	47.11.108.188	interop.com / udpinterop.com / cdp
2	□ 7101	7101	575	961	613	1	47.11.108.184	interop.com / udpinterop.com / cdp
3	□ 7102	7102	575		613	1	47.11.152.115	interop.com / udpinterop.com / cdp

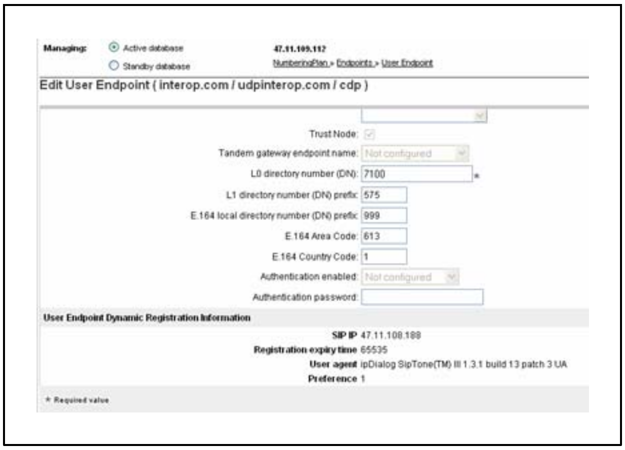
5 Click a **link** in the **ID** column of the **Endpoints** pane.

The **Edit User Endpoint** web page opens and displays the configured data for the selected User Endpoint, as shown in Figure 111 "User Endpoints Property web page" (page 225).

Note: If a User Endpoint is configured, then the supported protocol type is dynamic SIP. NRS Manager displays User Endpoint Dynamic Registration Information after the User Endpoint registers with the NRS

User Endpoint Dynamic Registration information includes the following: SIP IP, Registration expiry time, User agent, and Preference.

Figure 111
User Endpoints Property web page



Managing: ● Active database ○ Standby database

47.11.109.112

NumberingPlan > Endpoints > User Endpoint

Edit User Endpoint (interop.com / udpinterop.com / cdp)

Trust Node:	☑
Tandem gateway endpoint name:	Not configured
L0 directory number (DN):	7100 *
L1 directory number (DN) prefix:	575
E.164 local directory number (DN) prefix:	999
E.164 Area Code:	613
E.164 Country Code:	1
Authentication enabled:	Not configured
Authentication password:	

User Endpoint Dynamic Registration Information

SIP IP	47.11.108.188
Registration expiry time	65535
User agent	ipDialog SipTone(TM) III 1.3.1 build 13 patch 3 UA
Preference	1

* Required value

6 Scroll down the page to display **User Endpoint Dynamic Registration Information**.

—End—

View the User Endpoints

Use the following procedure to view the User Endpoints.

Procedure 36
Viewing the User Endpoints

Step	Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Endpoints**. The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).

2 Select the **Active** or **Standby** database. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The Active database is used for runtime queries. To modify the database it must be in Standby database view. Only Administrators can modify the standby database. One can switch between Active and Standby database views at any time. The **Endpoints** web page refreshes, as shown in Figure 98 "Endpoints web page Active database" (page 209).

3 The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

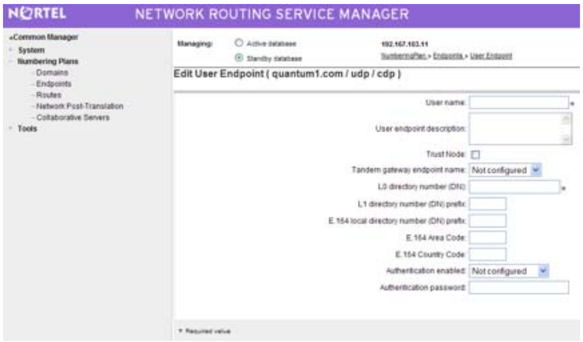
4 Click the **User Endpoints** button. The **Endpoints** web page refreshes displaying a list of configured User Endpoints in the Endpoints pane, as shown in Figure 107 "User Endpoints pane" (page 220). The User Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

5 Click a **link** in the **ID** column of the **Endpoints** pane.

The **Edit User Endpoint** web page opens and displays the configured data for the selected User Endpoint, as shown in Figure 112 "Edit User Endpoint web page Active database" (page 226).

> ***Note:*** See Procedure 37 "Editing a User Endpoint" (page 227) to Edit the User Endpoint.

Figure 112
Edit User Endpoint web page Active database



Managing: ○ Active database ● Standby database 192.167.103.11

Edit User Endpoint (quantum1.com / udp / cdp)

User name: *
User endpoint description:
Trust Node: □
Tandem gateway endpoint name: Not configured
L0 directory number (DN): *
L1 directory number (DN) prefix:
E.164 local directory number (DN) prefix:
E.164 Area Code:
E.164 Country Code:
Authentication enabled: Not configured
Authentication password:

* Required value

—End—

Edit a User Endpoint

Use the following procedure to edit a User Endpoint.

Procedure 37
Editing a User Endpoint

Step	Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

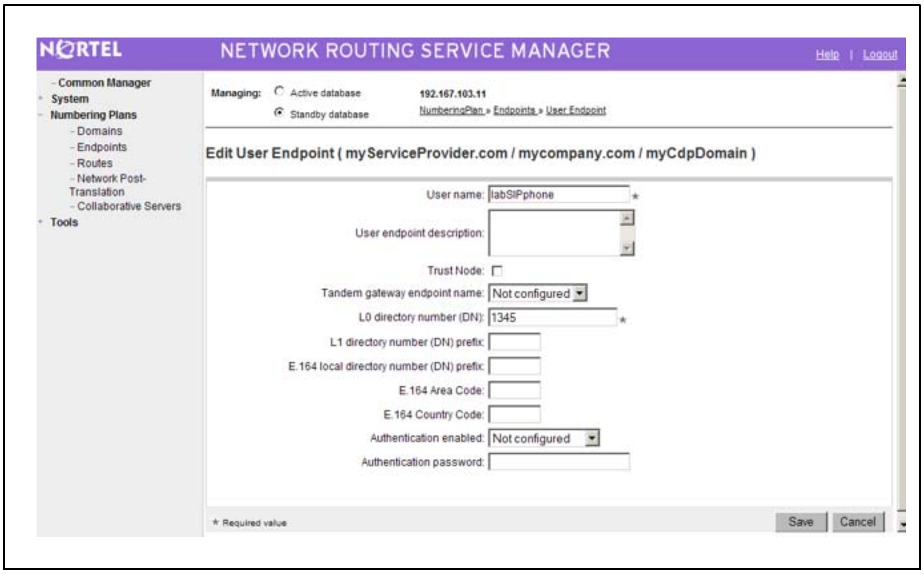
3 The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Click the **User Endpoints** button. The **Endpoints** web page opens displaying a list of configured User Endpoints in the Endpoints pane, as shown in Figure 107 "User Endpoints pane" (page 220).

The User Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

5 Click a **link** in the **ID** column of the Endpoints pane. The **Edit User Endpoint** web page opens and displays the configured data for the selected User Endpoint, as shown in Figure 113 "Edit User Endpoint web page" (page 227).

Figure 113
Edit User Endpoint web page



Managing: ○ Active database ● Standby database

192.167.103.11

NumberingPlan » Endpoints » User Endpoint

Edit User Endpoint (myServiceProvider.com / mycompany.com / myCdpDomain)

User name: labSIPphone *

User endpoint description:

Trust Node: □

Tandem gateway endpoint name: Not configured

L0 directory number (DN): 1345 *

L1 directory number (DN) prefix:

E.164 local directory number (DN) prefix:

E.164 Area Code:

E.164 Country Code:

Authentication enabled: Not configured

Authentication password:

* Required value

6 Modify the fields of the **Edit User Endpoint** web page as appropriate. See step 6 to step 17 of Procedure 34 "Adding a User Endpoint" (page 219).

7 Click the **Save** button. The standby database is updated. The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199)

8 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

9 Test the configuration changes.

10 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Delete a User Endpoint

Use the following procedure to delete a User Endpoint.

Procedure 38
Deleting a User Endpoint

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

3 The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

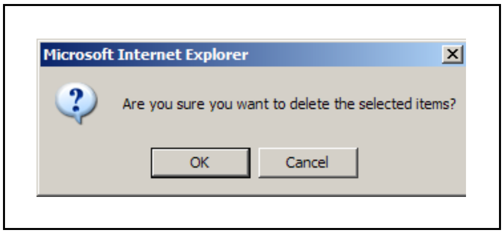
4 Click the **User Endpoints** button. The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199)

The User Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

5 Select a check box beside one or more **links** in the **ID** column of the Endpoints pane.

6 Click **Delete**. A **Confirmation Box** opens, as shown in Figure 114 "Confirmation Box" (page 229), requesting confirmation before deleting the selected **User Endpoint**.

Figure 114
Confirmation Box



Microsoft Internet Explorer

Are you sure you want to delete the selected items?

7 Click **OK**. The standby database is updated. The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).

8 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state.

9 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

SIP Phone Context

The SIP Phone Context web page provides a view of SIP phone-context constructions under a configured Service Domain, Level 1 Domain and Level 0 Domain or Gateway Endpoint. The SIP Phone Context web page is opened by selecting **Tools > SIP Phone Context** in the NRS Manager Navigator.

Procedure 39
Mapping the SIP Phone Context

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** web page opens, as shown in Figure 91 "Endpoints web page" (page 199).

2 Select **Standby database** or **Active database**. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

3 The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Click the **Gateway Endpoints** button. The **Endpoints** web page refreshes displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 92 "Gateway Endpoints pane" (page 200).

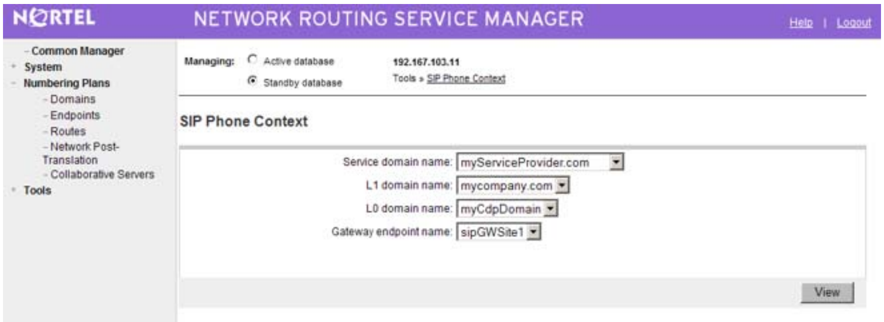
The Gateway Endpoints can be sorted in ascending or descending alphabetical order. See Sort web page by ID.

5 Select a check box beside a **link** in the **ID** column of the Endpoints pane.

6 Click the **SIP phone context** button.

The **SIP Phone Context** web page opens, as shown in Figure 115 "SIP Phone Context web page" (page 230).

Figure 115
SIP Phone Context web page



Managing: ○ Active database ● Standby database

192.167.103.11

Tools » SIP Phone Context

SIP Phone Context

Service domain name: myServiceProvider.com

L1 domain name: mycompany.com

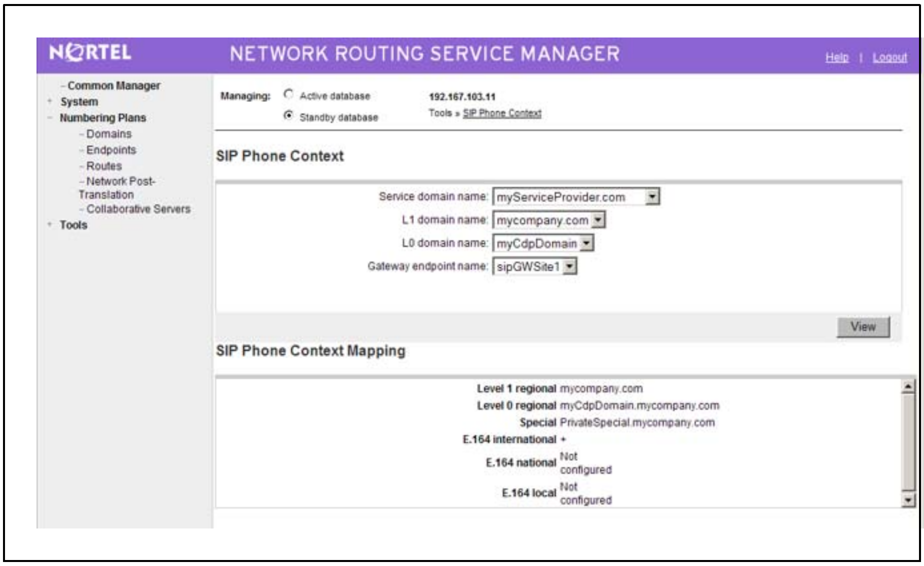
L0 domain name: myCdpDomain

Gateway endpoint name: sipGWSite1

7 Click the **View** button.

The SIP Phone Context web page expands to display the **SIP Phone Context Mapping** pane, as shown in Figure 116 "SIP Phone Context Mapping web page" (page 231).

Figure 116
SIP Phone Context Mapping web page



Managing: ○ Active database ● Standby database

192.167.103.11

Tools » SIP Phone Context

SIP Phone Context

Service domain name: myServiceProvider.com

L1 domain name: mycompany.com

L0 domain name: myCdpDomain

Gateway endpoint name: sipGWSite1

SIP Phone Context Mapping

Level 1 regional	mycompany.com
Level 0 regional	myCdpDomain.mycompany.com
Special	PrivateSpecial.mycompany.com
E.164 international	+
E.164 national	Not configured
E.164 local	Not configured

—End—

Manage a Routing Entry

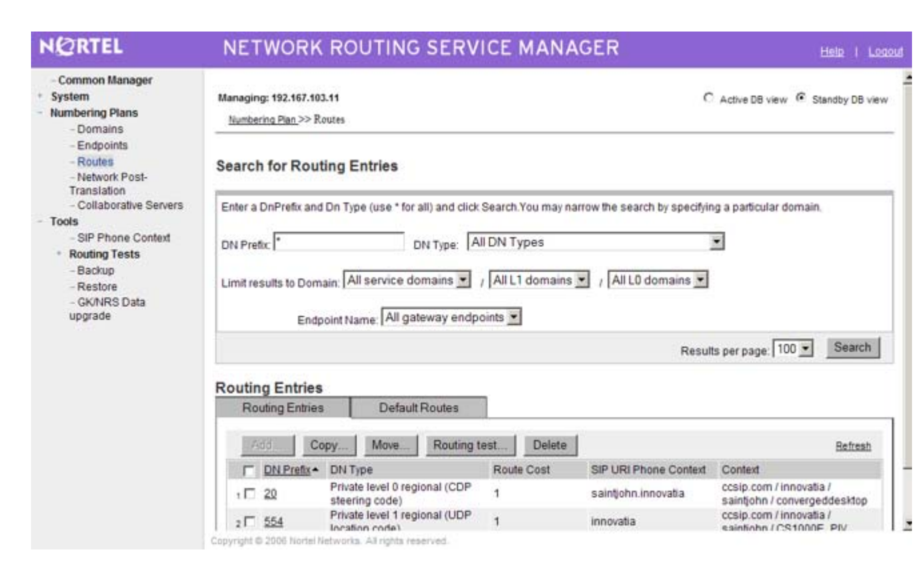
Add a Routing Entry

Use the following procedure to add a Routing Entry.

Procedure 40
Adding a Routing Entry

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).

Figure 117
Routes web page



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Routes

Search for Routing Entries

Enter a DnPrefix and Dn Type (use * for all) and click Search.You may narrow the search by specifying a particular domain.

DN Prefix: * DN Type: All DN Types

Limit results to Domain: All service domains / All L1 domains / All L0 domains

Endpoint Name: All gateway endpoints

Results per page: 100

Routing Entries

	□ DN Prefix▲	DN Type	Route Cost	SIP URI Phone Context	Context
1	□ 20	Private level 0 regional (CDP steering code)	1	saintjohn.innovatia	ccsip.com / innovatia / saintjohn / convergeddesktop
2	□ 554	Private level 1 regional (UDP location code)	1	innovatia	ccsip.com / innovatia / saintjohn / CS1000E_PIV

Copyright © 2006 Nortel Networks. All rights reserved.

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

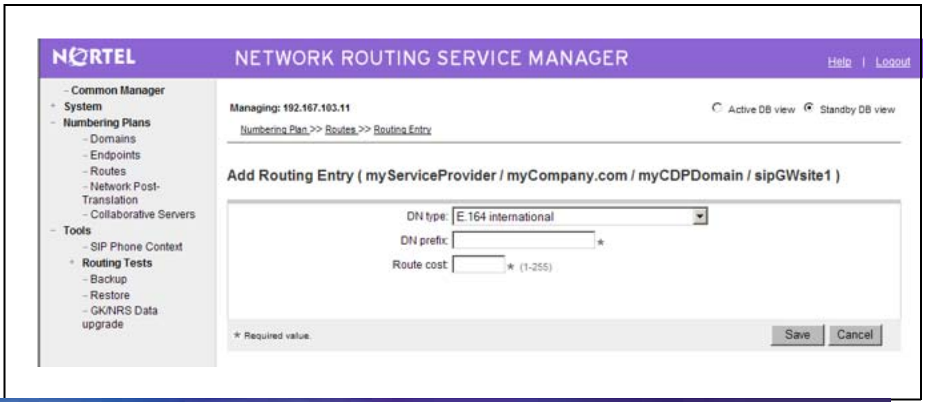
3 The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.

5 Click the **Routing Entries** button.

6 Click the **Add** button. The **Add Routing Entry** web page opens, as shown in Figure 118 "Add Routing Entry web page" (page 232).

Figure 118
Add Routing Entry web page



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Routes >> Routing Entry

Add Routing Entry (myServiceProvider / myCompany.com / myCDPDomain / sipGWsite1)

DN type: E.164 international

DN prefix: *

Route cost: * (1-255)

* Required value.

7 Select the DN type from the **DN Type** drop-down list. The six choices are E.164 international, E.164 national, E.164 local (subscriber), Private level 1 regional (UDP location code), Private level 0 regional (CDP steering code), and Private special.

8 Enter the **DN prefix** in the text box. The DN prefix can include 0-9, #, -, ?. The prefix can be up to 30 characters in length; however, the first character must be numeric.

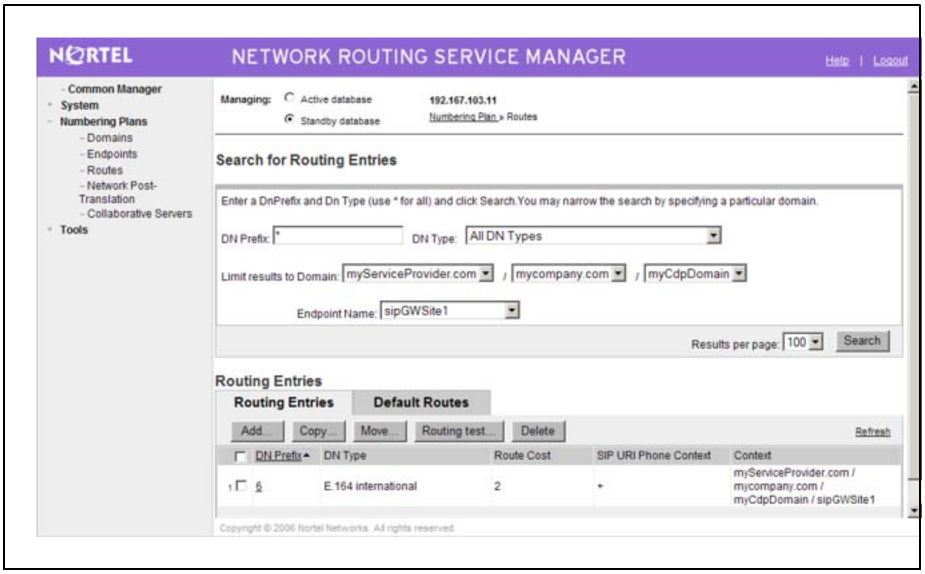
9 Enter the **Route cost** in the text box. The range is 1-255. The cost must be numeric and can be up to three digits in length.

The Route Cost is used to define least-cost routing. Higher numbers indicate higher costs.

10 Click the **Save** button. The standby database is updated.

The **Routes** web page opens, displaying the newly added routing entry in the Routing Entries pane, as shown in Figure 119 "Added Routing Entry" (page 233).

Figure 119
Added Routing Entry



Managing: ○ Active database ● Standby database 192.167.103.11

Search for Routing Entries

Enter a DnPrefix and Dn Type (use * for all) and click Search.You may narrow the search by specifying a particular domain.

DN Prefix: *   DN Type: All DN Types

Limit results to Domain: myServiceProvider.com / mycompany.com / myCdpDomain

Endpoint Name: sipGWSite1

Results per page: 100   Search

Routing Entries

	DN Prefix	DN Type	Route Cost	SIP URI Phone Context	Context
1 □	6	E.164 international	2	+	myServiceProvider.com / mycompany.com / myCdpDomain / sipGWSite1

11 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

12 Test the configuration changes.

13 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

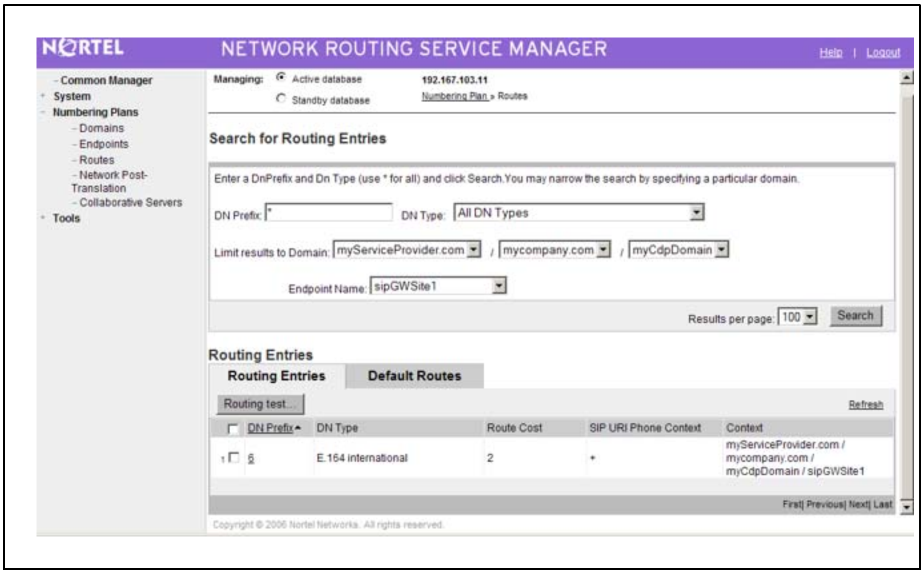
View the Routing Entries

Use the following procedure to view the Routing Entries.

Procedure 41
Viewing the Routing Entries

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).
2	Select the **Active** or **Standby** database. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The Active database is used for runtime queries. To modify the database it must be in Standby database view. Only Administrators can modify the standby database. One can switch between Active and Standby database views at any time. The **Routes** web page refreshes.
3	Enter a **DN Prefix** in the text box.
4	Select the DN type(s) from the **DN Type** drop-down list. The seven choices are All DN Types, E.164 international, E.164 national, E.164 local (subscriber), Private level 1 regional (UDP location code), Private level 0 regional (CDP steering code), and Private special.
5	The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.
6	Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.
7	Click the **Routing Entries** button.
8	Click **Search**. The web page refreshes to display a list of configured Routing Entries, as shown in Figure 120 "Search for Routing Entries web page" (page 235). The Routing Entries can be sorted in ascending or descending numerical order. See Sort web page by DN Prefix.

Figure 120
Search for Routing Entries web page



Managing: ● Active database ○ Standby database 192.167.103.11

Search for Routing Entries

Enter a DnPrefix and Dn Type (use * for all) and click Search.You may narrow the search by specifying a particular domain.

DN Prefix: * DN Type: All DN Types

Limit results to Domain: myServiceProvider.com / mycompany.com / myCdpDomain

Endpoint Name: sipGWSite1

Results per page: 100

Routing Entries

	□	DN Prefix	DN Type	Route Cost	SIP URI Phone Context	Context
1	□	6	E.164 international	2	*	myServiceProvider.com / mycompany.com / myCdpDomain / sipGWSite1

Copyright © 2006 Nortel Networks. All rights reserved.

—End—

Edit a Routing Entry

Use the following procedure to edit a Routing Entry.

Procedure 42
Editing a Routing Entry

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

3 The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.

5 Click the **Routing Entries** button.

6 Click **Search**.

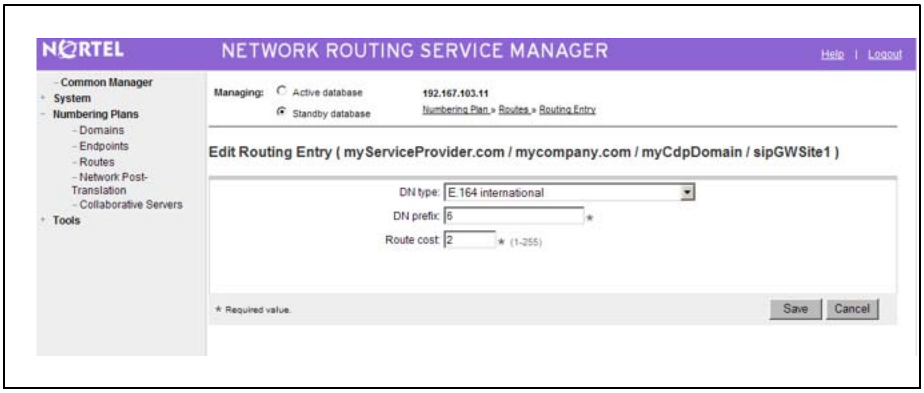
The web page refreshes to display a list of configured Routing Entries, as shown in Figure 120 "Search for Routing Entries web page" (page 235).

The Routing Entries can be sorted in ascending or descending numerical order. See Sort web page by DN Prefix.

7 Click a **link** in the **DN Prefix** column of the Routing Entries pane.

The **Edit Routing Entry** web page opens, as shown in Figure 121 "Edit Routing Entry web page" (page 236).

Figure 121
Edit Routing Entry web page



Managing: ○ Active database ● Standby database 192.167.103.11

Edit Routing Entry (myServiceProvider.com / mycompany.com / myCdpDomain / sipGWSite1)

DN type: E.164 international

DN prefix: 6 *

Route cost: 2 * (1-255)

* Required value.

8 Modify the **DN Type**, **DN Prefix** or **Route Cost**.

9 Click the **Save** button. The standby database is updated. The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).

10 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

11 Test the configuration changes.

12 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

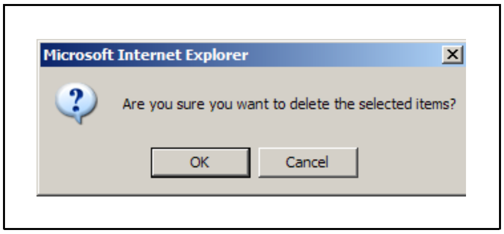
Delete a Routing Entry

Use the following procedure to delete a Routing Entry.

Procedure 43
Deleting a Routing Entry

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).
2	Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).
3	The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.
4	Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.
5	Click the **Routing Entries** button.
6	Click **Search**. The web page refreshes to display a list of configured Routing Entries, as shown in Figure 120 "Search for Routing Entries web page" (page 235). The Routing Entries can be sorted in ascending or descending numerical order. See Sort web page by DN Prefix.
7	Select a check box beside one or more **links** in the **DN Prefix** column of the Routing Entries pane.
8	Click the **Delete** button. A **Confirmation Box** opens, as shown in Figure 122 "Confirmation Box" (page 237), requesting confirmation before deleting the selected **Routing Entry**.

Figure 122
Confirmation Box



Microsoft Internet Explorer

Are you sure you want to delete the selected items?

Step	Action
9	Click **OK**. The standby database is updated. The **Routes** web page refreshes, as shown in Figure 117 "Routes web page" (page 232).

10 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state.

11 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Copy a Routing Entry

Use the following procedure to copy a Routing Entry.

Procedure 44
Copying a Routing Entry

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

3 The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.

5 Click the **Routing Entries** button.

6 Click **Search**.

The web page refreshes to display a list of configured Routing Entries, as shown in Figure 120 "Search for Routing Entries web page" (page 235).

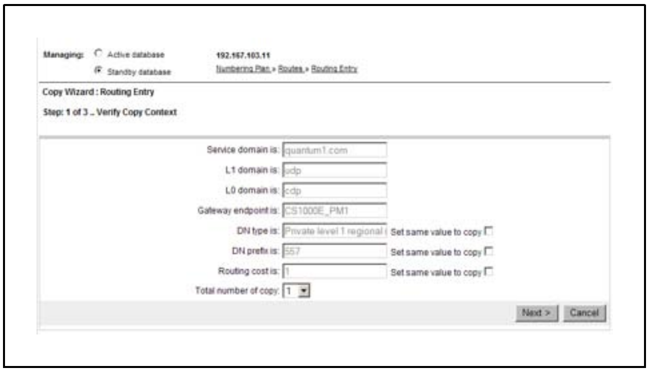
The Routing Entries can be sorted in ascending or descending numerical order. See Sort web page by DN Prefix.

7 Select a check box beside a **link** in the **DN Prefix** column of the Routing Entries pane.

8 Click **Copy**.

The **Copy Wizard: Routing Entry Verify Copy Context** web page opens, as shown in Figure 123 "Copy Wizard: Routing Entry Verify Copy Context web page" (page 239).

Figure 123
Copy Wizard: Routing Entry Verify Copy Context web page



Managing: ○ Active database ● Standby database
192.167.103.11
Numbering Plan » Routes » Routing Entry

Copy Wizard : Routing Entry

Step: 1 of 3 .. Verify Copy Context

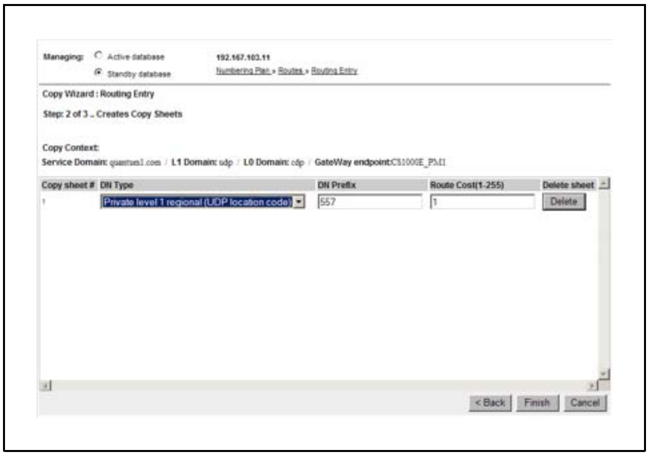
Service domain is: quantum1.com
L1 domain is: udp
L0 domain is: cdp
Gateway endpoint is: CS1000E_PM1
DN type is: Private level 1 regional (Set same value to copy □
DN prefix is: 557 Set same value to copy □
Routing cost is: 1 Set same value to copy □
Total number of copy: 1

9 Select **Total number of copy** from the drop down list.

10 Click **Next**.

The **Copy Wizard: Routing Entry Creates Copy Sheets** web page opens, as shown in Figure 124 "Copy Wizard: Routing Entry Creates Copy Sheets web page" (page 239).

Figure 124
Copy Wizard: Routing Entry Creates Copy Sheets web page



Managing: ○ Active database ● Standby database
192.167.103.11
Numbering Plan » Routes » Routing Entry

Copy Wizard : Routing Entry

Step: 2 of 3 .. Creates Copy Sheets

Copy Context:
Service Domain: quantum1.com / L1 Domain: udp / L0 Domain: cdp / GateWay endpoint:CS1000E_PM1

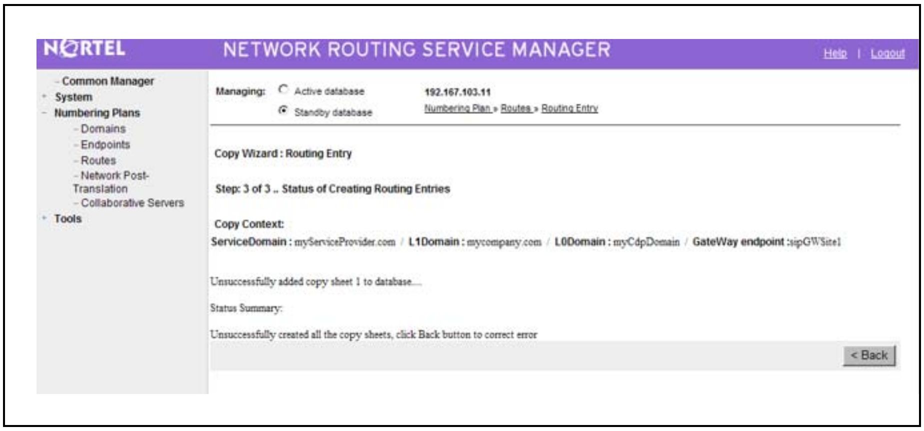
Copy sheet #	DN Type	DN Prefix	Route Cost(1-255)	Delete sheet
1	Private level 1 regional (UDP location code)	557	1	Delete

11 Modify the copy sheet(s).

12 Click **Finish**. The standby database is updated.

The **Copy Wizard: Routing Entry Status of Creating Routing Entries** web page opens, as shown in Figure 125 "Copy Wizard: Routing Entry Status of Creating Routing Entries web page" (page 240).

Figure 125
Copy Wizard: Routing Entry Status of Creating Routing Entries web page



Managing: ○ Active database ● Standby database

192.167.103.11

Copy Wizard : Routing Entry

Step: 3 of 3 .. Status of Creating Routing Entries

Copy Context:
ServiceDomain : myServiceProvider.com / L1Domain : mycompany.com / L0Domain : myCdpDomain / GateWay endpoint :sipGWSite1

Unsuccessfully added copy sheet 1 to database....

Status Summary:

Unsuccessfully created all the copy sheets, click Back button to correct error

13 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

14 Test the configuration changes.

15 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Move Routing Entries

Use the following procedure to move a Routing Entries.

Procedure 45
Moving Routing Entries

Step **Action**

1 In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

3 The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.

5 Click the **Routing Entries** button.

6 Click **Search**.

The web page refreshes to display a list of configured Routing Entries, as shown in Figure 120 "Search for Routing Entries web page" (page 235).

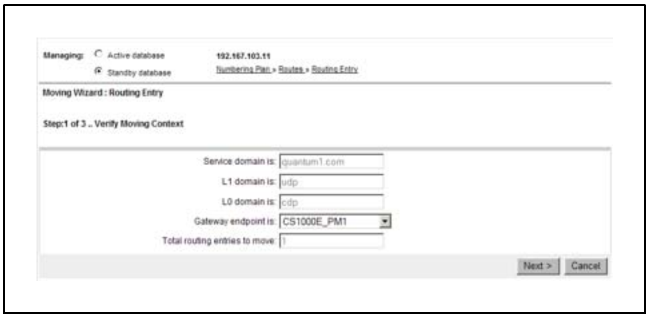
The Routing Entries can be sorted in ascending or descending numerical order. See Sort web page by DN Prefix.

7 Select a check box beside one, or up to ten, **links** in the **DN Prefix** column of the Routing Entries pane.

8 Click **Move**.

The **Moving Wizard: Routing Entry Verify Moving Context** web page opens, as shown in Figure 126 "Moving Wizard: Routing Entry Verify Moving Context web page" (page 241).

Figure 126
Moving Wizard: Routing Entry Verify Moving Context web page



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Routes » Routing Entry

Moving Wizard : Routing Entry

Step:1 of 3 .. Verify Moving Context

Service domain is: quantum1.com

L1 domain is: udp

L0 domain is: cdp

Gateway endpoint is: CS1000E_PM1

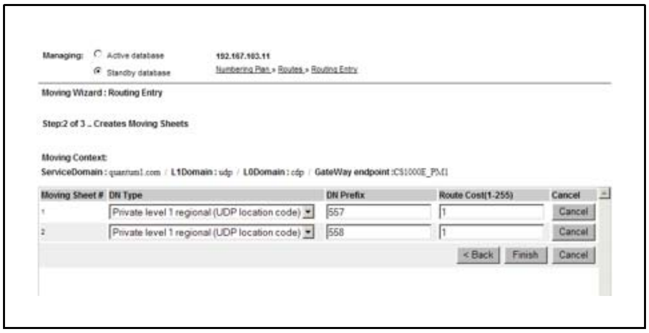
Total routing entries to move: 1

9 Choose the destination endpoint from the **Gateway endpoint is** drop-down list.

10 Click **Next**.

The **Moving Wizard: Routing Entry Creates Moving Sheets** web page opens, as shown in Figure 127 "Moving Wizard: Routing Entry Creates Moving Sheets web page" (page 242).

Figure 127
Moving Wizard: Routing Entry Creates Moving Sheets web page



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Routes » Routing Entry

Moving Wizard : Routing Entry

Step:2 of 3 .. Creates Moving Sheets

Moving Context:
ServiceDomain : quantum1.com / L1Domain : udp / L0Domain : cdp / GateWay endpoint :CS1000E_PM1

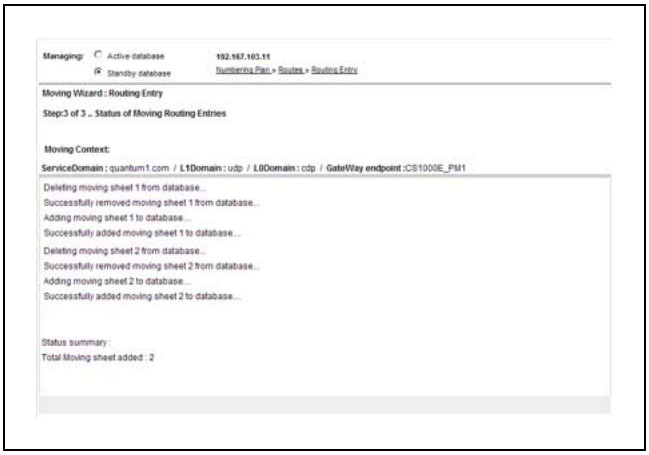
Moving Sheet #	DN Type	DN Prefix	Route Cost(1-255)	Cancel
1	Private level 1 regional (UDP location code)	557	1	Cancel
2	Private level 1 regional (UDP location code)	558	1	Cancel

11 Modify the copy sheet(s).

12 Click **Finish**. The standby database is updated.

The **Moving Wizard: Routing Entry Status of Moving Routing Entries** web page opens, as shown in Figure 128 "Moving Wizard: Routing Entry Status of Moving Routing Entries web page" (page 242).

Figure 128
Moving Wizard: Routing Entry Status of Moving Routing Entries web page



Managing: ○ Active database ● Standby database

192.167.103.11

Numbering Plan » Routes » Routing Entry

Moving Wizard : Routing Entry

Step:3 of 3 .. Status of Moving Routing Entries

Moving Context:
ServiceDomain : quantum1.com / L1Domain : udp / L0Domain : cdp / GateWay endpoint :CS1000E_PM1

```
Deleting moving sheet 1 from database...
Successfully removed moving sheet 1 from database...
Adding moving sheet 1 to database...
Successfully added moving sheet 1 to database...
Deleting moving sheet 2 from database...
Successfully removed moving sheet 2 from database...
Adding moving sheet 2 to database...
Successfully added moving sheet 2 to database...


Status summary :
Total Moving sheet added : 2
```

13 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

14 Test the configuration changes.

15 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Search Routing Entries

Use the following procedure to search Routing Entries by DN Prefix.

Procedure 46
Searching Routing Entries

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).
2	Select **Standby database** or **Active database**. See Procedure 8 "Switching between the Active and Standby databases" (page 164).
3	Select the **Routing Entries** button.
4	Enter a **DN Prefix** in the text box. Specify***** (wild card) for all prefixes, DN digits combined with the wild card or DN digits.
5	Select the **All DN Types** from the **DN Type** drop-down list.
6	The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.
7	Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list.
8	Click **Search**. The web page refreshes to display a list of configured Routing Entries, as shown in Figure 120 "Search for Routing Entries web page" (page 235). The Routing Entries can be sorted in ascending or descending numerical order. See Sort web page by DN Prefix.

—End—

Manage a Default Route

If the routing entry DN prefix in an incoming H.323/SIP signaling request does not match a DN prefix Gateway Endpoint routing entry recorded in the NRS database, the default route is returned to the gateway.

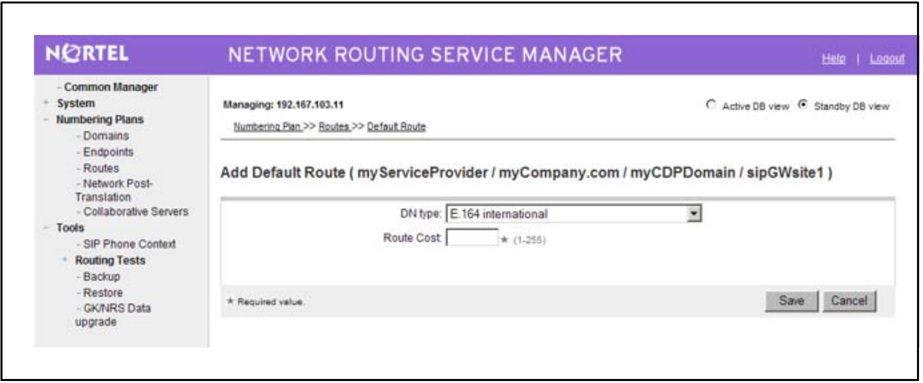
Add a Default Route

Use the following procedure to add a Default Route.

Procedure 47
Adding a Default Route

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).
2	Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).
3	The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.
4	Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.
5	Click the **Default Routes** button. The **Routes** web page refreshes to display a list of configured default routes,
6	Click the **Add** button. The **Add Default Route** web page opens, as shown in Figure 129 "Add Default route web page" (page 244).

Figure 129
Add Default route web page



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Numbering Plan >> Routes >> Default Route

Add Default Route (myServiceProvider / myCompany.com / myCDPDomain / sipGWsite1)

DN type: E.164 international

Route Cost: * (1-255)

* Required value.

Step	Action
7	Select the **DN type** from the drop down list. The six options are E.164 international, E.164 national, E.164 local (subscriber), Private level 1 regional (UDP location code), Private level 0 regional (CDP steering code), and Private special.

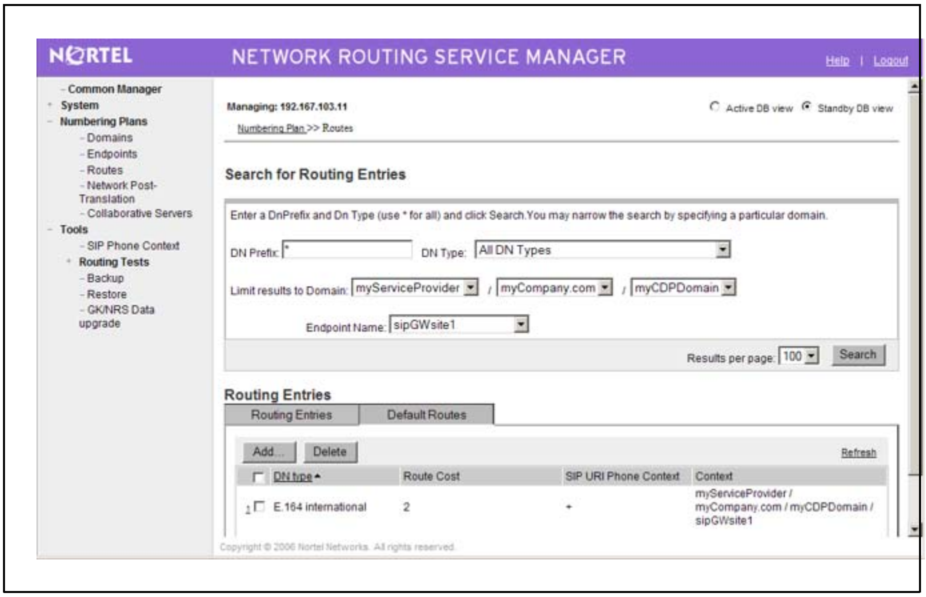
The DN type attribute determines how the phone context value, that is used to qualify the DN prefix, is built from the building blocks configured for the routing entry parents.

> ***Note:*** Each DN type has only one default route.

8 Enter the **Route cost**. The range is 1-255. The cost must be numeric and can be up to three digits in length.

9 Click the **Save** button. The standby database is updated. The **Routes** web page opens displaying the new default route, as shown in Figure 130 "Added Default route" (page 245).

Figure 130
Added Default route



Managing: 192.167.103.11

○ Active DB view ● Standby DB view

Search for Routing Entries

Enter a DnPrefix and Dn Type (use * for all) and click Search.You may narrow the search by specifying a particular domain.

DN Prefix: * DN Type: All DN Types

Limit results to Domain: myServiceProvider / myCompany.com / myCDPDomain

Endpoint Name: sipGWsite1

Results per page: 100

Routing Entries

		DN type	Route Cost	SIP URI Phone Context	Context
	□				
1	□	E.164 international	2	*	myServiceProvider / myCompany.com / myCDPDomain / sipGWsite1

Copyright © 2006 Nortel Networks. All rights reserved.

10 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

11 Test the configuration changes.

12 See Procedure 60 "Committing the database" (page 260)to update the database with the configuration changes.

—End—

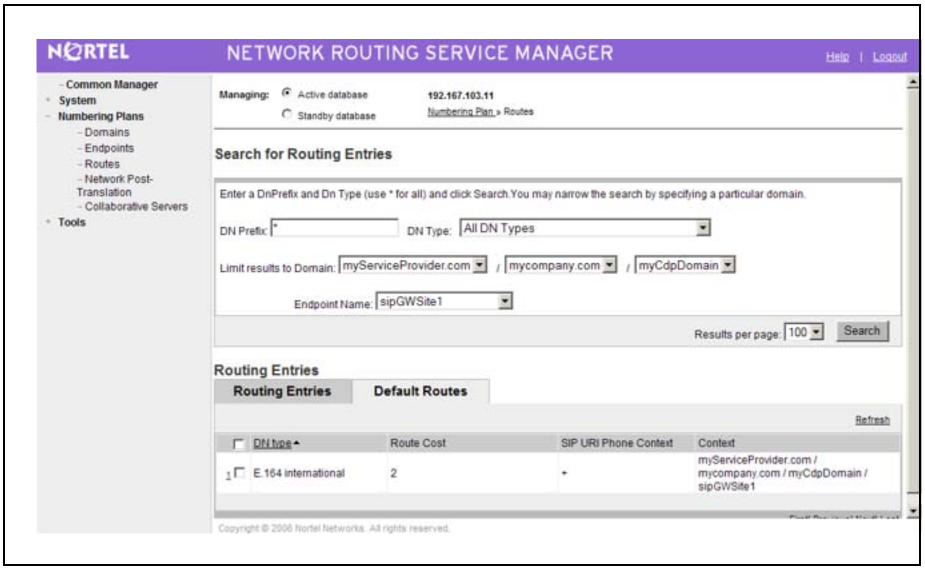
View Default Routes

Use the following procedure to view Default Routes.

Procedure 48
Viewing Default Routes

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).
2	Select the **Active** or **Standby** database. See Procedure 8 "Switching between the Active and Standby databases" (page 164). The Active database is used for runtime queries. To modify the database it must be in Standby database view. Only Administrators can modify the standby database. One can switch between Active and Standby database views at any time. The **Routes** web page refreshes.
3	Enter a **DN Prefix** in the text box.
4	Select the DN type(s) from the **DN Type** drop-down list. The seven choices are All DN Types, E.164 international, E.164 national, E.164 local (subscriber), Private level 1 regional (UDP location code), Private level 0 regional (CDP steering code), and Private special.
5	The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.
6	Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.
7	Click the **Default Routes** button.
8	Click **Search**. The web page expands to display a list of configured Default Route(s), as shown in Figure 131 "Search for Default Routes web page" (page 247). The Default Routes can be sorted in ascending or descending alphabetical order. See Sort web page by DN type.

Figure 131
Search for Default Routes web page



Managing: ● Active database ○ Standby database 192.167.103.11

Search for Routing Entries

Enter a DnPrefix and Dn Type (use * for all) and click Search.You may narrow the search by specifying a particular domain.

DN Prefix: * DN Type: All DN Types

Limit results to Domain: myServiceProvider.com / mycompany.com / myCdpDomain

Endpoint Name: sipGWSite1

Results per page: 100

Routing Entries

		DN type	Route Cost	SIP URI Phone Context	Context
	□				
1	□	E.164 international	2	+	myServiceProvider.com / mycompany.com / myCdpDomain / sipGWSite1

Copyright © 2006 Nortel Networks. All rights reserved.

—End—

Edit a Default Route

Use the following procedure to edit a Default Route.

Procedure 49
Editing a Default Route

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).
2	Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).
3	The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.
4	Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.
5	Click the **Default Routes** button.
6	Click **Search**.

The web page expands to display a list of configured Default Route(s), as shown in Figure 131 "Search for Default Routes web page" (page 247).

The Default Routes can be sorted in ascending or descending alphabetical order. See Sort web page by DN type.

7 Click a **link** in the **DN Type** column of the Default Routes pane.

The **Edit Default Route** web page opens.

8 Modify the **DN Type** or **Route Cost**.

9 Click the **Save** button. The standby database is updated. The **Routes** web page opens displaying the modified default route, as shown in Figure 117 "Routes web page" (page 232)

10 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state. The configuration changes can now be tested.

11 Test the configuration changes.

12 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Delete a Default Route

Use the following procedure to delete a Default Route.

Procedure 50
Deleting a Default Route

Step Action

1 In the **NRS Manager Navigator** select **Numbering Plans > Routes.**The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).

2 Ensure **Standby database** is selected. See Procedure 8 "Switching between the Active and Standby databases" (page 164).

3 The **Limit results to Domain:** drop-down lists, in the **Search for Routing Entries** pane, contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.

5 Click the **Default Routes** button.

6 Click **Search**.

The web page expands to display a list of configured Default Route(s), as shown in Figure 131 "Search for Default Routes web page" (page 247).

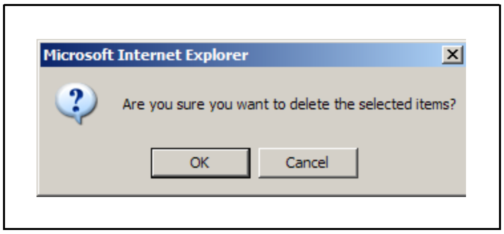
The Default Routes can be sorted in ascending or descending alphabetical order. See Sort web page by DN type.

7 Select a check box beside one or more **links** in the **DN Type** column of the Default Routes pane.

8 Click **Delete**.

A **Confirmation Box** opens, as shown in Figure 132 "Confirmation Box" (page 249), requesting confirmation before deleting the selected **Default Route**.

Figure 132
Confirmation Box



Microsoft Internet Explorer

Are you sure you want to delete the selected items?

9 Click **OK**. The standby database is updated. The **Routes** web page opens, as shown in Figure 117 "Routes web page" (page 232).

10 See Procedure 57 "Cutting over the database" (page 257) to place the database in a Switched Over state.

11 See Procedure 60 "Committing the database" (page 260) to update the database with the configuration changes.

—End—

Verify the numbering plan and save the NRS configuration

You should verify your numbering plan after it is configured in the NRS.

Use the following procedure to verify the numbering plan.

Procedure 51
Verifying the numbering plan

Step	Action
1	Perform a database **Cut over**. Cutting over places the database on the network. See Procedure 57 "Cutting over the database" (page 257).
2	Perform the routing tests. • See Procedure 52 "Performing an H.323 Routing Test" (page 250). • See Procedure 53 "Performing a SIP Routing Test" (page 252).
3	If the routing tests succeed, perform a database **Commit**. See Procedure 60 "Committing the database" (page 260).
4	If there are problems with the network testing, use the database **Revert** command to undo the **Cut over.** See Procedure 58 "Reverting the database changes" (page 258) If you want to undo the latest provisioning changes, use a database **Rollback** command to synchronize the Standby database with the previous Active database. See Procedure 59 "Rolling back changes to the database" (page 259)

—End—

H.323 and SIP Routing Tests

To ascertain if a numbering plan entry exists in the active or standby database:

- See Procedure 52 "Performing an H.323 Routing Test" (page 250) to perform an H.323 Routing Test.
- See Procedure 53 "Performing a SIP Routing Test" (page 252) to perform a SIP Routing Test.

Perform an H.323 Routing Test

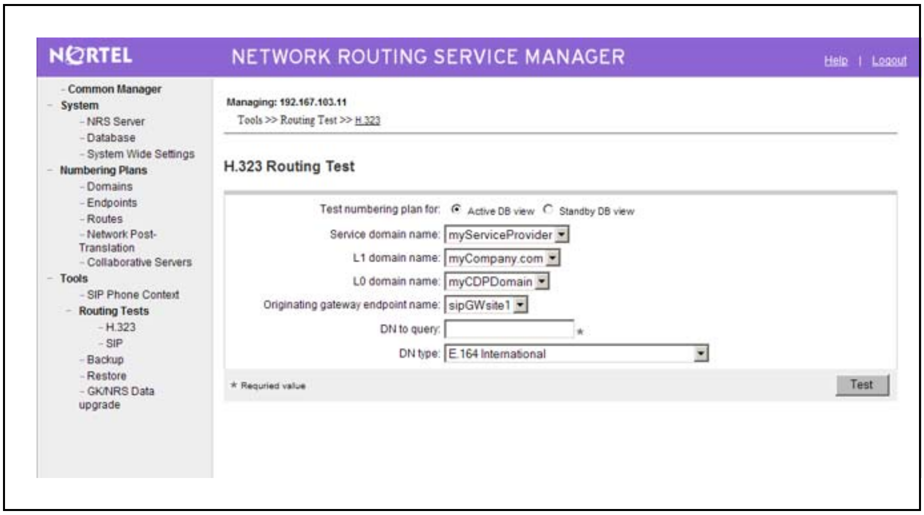
Use the following procedure to perform an H.323 Routing Test.

Procedure 52
Performing an H.323 Routing Test

Step	Action
1	In the **NRS Manager Navigator** select **Tools > Routing Tests > H.323.**

The **H.323 Routing Test** web page opens, as shown in Figure 133 "H.323 routing Test" (page 251).

Figure 133
H.323 routing Test



Managing: 192.167.103.11

Tools >> Routing Test >> H.323

H.323 Routing Test

Test numbering plan for: ● Active DB view ○ Standby DB view

Service domain name: myServiceProvider

L1 domain name: myCompany.com

L0 domain name: myCDPDomain

Originating gateway endpoint name: sipGWsite1

DN to query: *

DN type: E.164 International

* Requried value

2 Select **Active database** or **Standby database**. See Procedure 8 "Switching between the Active and Standby databases" (page 164)

3 Select the **Service domain name** from the drop-down list.

4 Select the **L1 domain name** from the drop-down list.

5 Select the **L0 domain name** from the drop-down list.

6 Select the **Originating gateway endpoint name** from the drop-down list.

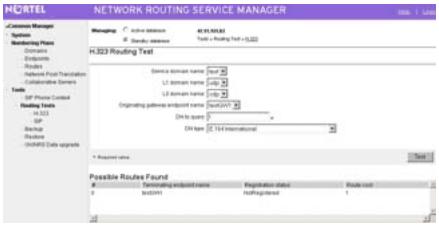
7 Enter a numbering plan entry you want to check in the **DN to query** text box.

8 Select a number type from the **DN type** drop-down list.

9 Click **Test**.

The results of the H.323 Routing Test are displayed, as shown in Figure 134 "H.323 Routing Test results" (page 252).

Figure 134
H.323 Routing Test results



Managing: ○ Active database ● Standby database

Tools » Routing Test » H.323

H.323 Routing Test

Service domain name: test

L1 domain name: udp

L0 domain name: cdp

Originating gateway endpoint name: testGW1

DN to query: 1 *

DN type: E.164 International

* Required value

Possible Routes Found

#	Terminating endpoint name	Registration status	Route cost
0	testGW1	NotRegistered	1

—End—

Perform a SIP Routing Test

Use the following procedure to perform a SIP Routing Test.

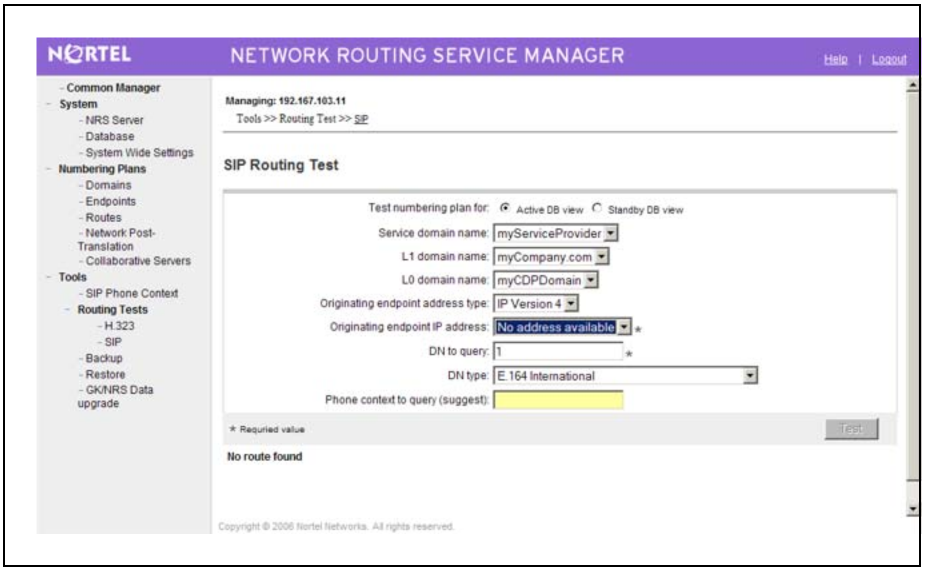
Procedure 53
Performing a SIP Routing Test

Step Action

1 In the **NRS Manager Navigator** select **Tools > Routing Tests > SIP.**

The **SIP Routing Test** web page opens, as shown in Figure 135 "SIP Routing Test" (page 252).

Figure 135
SIP Routing Test



Managing: 192.167.103.11

Tools >> Routing Test >> SIP

SIP Routing Test

Test numbering plan for: ● Active DB view ○ Standby DB view

Service domain name: myServiceProvider

L1 domain name: myCompany.com

L0 domain name: myCDPDomain

Originating endpoint address type: IP Version 4

Originating endpoint IP address: No address available *

DN to query: 1 *

DN type: E.164 International

Phone context to query (suggest):

* Requried value

No route found

Copyright © 2006 Nortel Networks. All rights reserved.

2 Select **Active database** or **Standby database**. See Procedure 8 "Switching between the Active and Standby databases" (page 164)

3 Select the Service Domain from the **Service domain name** drop-down list.

4 Select the L1 Domain name from the **L1 domain name** drop-down list.

5 Select the L0 Domain name from the **L0 domain name** drop-down list.

6 Ensure IP version 4 is selected from the **Originating endpoint address type** drop-down list.

7 Select the **Originating gateway endpoint name** from the drop-down list.

8 Enter a numbering plan entry you want to check in the **DN to query** text box.

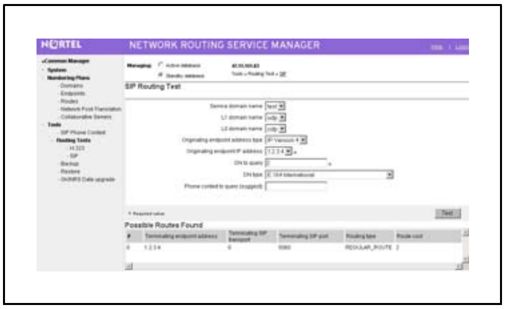
9 Select the DN type you want to check from the **DN type** drop-down list.

10 Enter the **Phone context to query** in the text box.

11 Click **Test**.

The results of the SIP Routing Test are displayed, as shown in Figure 136 "SIP Routing Test results" (page 253).

Figure 136
SIP Routing Test results



SIP Routing Test

Service domain name: test
L1 domain name: cdp
L0 domain name: cdp
Originating endpoint address type: IP Version 4
Originating endpoint IP address: 1.2.3.4 *
DN to query: 2 *
DN type: E.164 International
Phone context to query (suggest):

* Required value

Possible Routes Found

#	Terminating endpoint address	Terminating SIP transport	Terminating SIP port	Routing type	Route cost
0	1.2.3.4	0	5060	REGULAR_ROUTE	1

—End—

Enable, disable and restart the NRS Server

Actions to:

- Forcefully disable the NRS server (nrsForceDisableServer)
- Gracefully disable the NRS server (nrsDisableServer) This command should not interrupt the existing calls.

- Enable the NRS server (nrsEnableServer)

can be performed using NRS Manager or the Command Line Interface (CLI).

The NRS can be taken out-of-service to perform maintenance or to place an Alternate NRS into service.

> ***Note:*** Only users with administrator privileges can execute the NRS server action commands.

See Procedure 54 "Disabling the NRS server" (page 254) to take the NRS out-of-service (disabling the NRS server).

See Procedure 55 "Enabling the NRS server" (page 255) to bring the NRS back in to service.

See Procedure 56 "Restarting the NRS Server" (page 255) to restart the NRS.

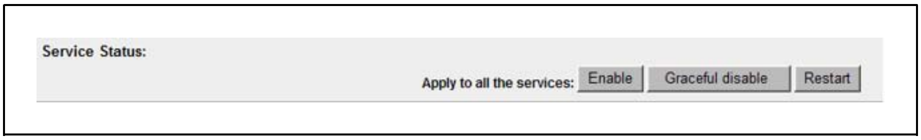
Disable the NRS server

Use the following procedure to disable the NRS server.

Procedure 54
Disabling the NRS server

Step	Action
1	In the **NRS Manager Navigator** select **System > NRS Server.** The **NRS Server** web page opens, as shown in Figure 42 "NRS Server web page" (page 148)
2	Select **Graceful disable** from the **Service Status** pane of the **NRS Server** web page. See Figure 137 "Service Status pane" (page 254).

Figure 137
Service Status pane



Step	Action
3	The nrsDisableServer command is issued.

—End—

Enable the NRS server

Use the following procedure to enable the NRS server.

Procedure 55
Enabling the NRS server

Step	Action
1	In the **NRS Manager Navigator** select **System > NRS Server.** The **NRS Server** web page opens, as shown in Figure 42 "NRS Server web page" (page 148)
2	Select **Enable** from the **Service Status** pane of the **NRS Server** web page. See Figure 137 "Service Status pane" (page 254).
3	The nrsEnableServer command is issued.

—End—

Restart the NRS Server

Use the following procedure to restart the NRS Server.

Procedure 56
Restarting the NRS Server

Step	Action
1	In the **NRS Manager Navigator** select **System > NRS Server.** The **NRS Server** web page opens, as shown in Figure 42 "NRS Server web page" (page 148)
2	Click the **Restart** button in the **Service Status** pane of the **NRS Server** web page. See Figure 137 "Service Status pane" (page 254).

—End—

Perform NRS database actions

The NRS database has two schemas: an active schema and a standby schema

- The active database is used for runtime queries.
- The standby database is used to modify the configuration data. Changes can be made only to the standby database.

The following database commands can be performed using NRS Manager:

- **Cut over** : Swaps the active and standby databases by interchanging the active and standby database access pointers. The active and standby databases must be swapped before configuration changes can take effect.

- **Commit**: Copies data *from* the active database *to* the standby database. Synchronizes the standby database with the active database. Overwrites the previous configuration data with the new configuration data.
- **Revert**: After a Cut over, a revert interchanges the active and standby database access pointers. The active and standby databases are swapped.
- **Roll back** : Before a Commit, a roll back undoes changes made to the standby database. A Roll Back copies data *from* the active database *to* the standby database. As a result, any changes made during the latest provisioning to the standby database are erased. The standby database is synchronized with the active database. This operation is available after a Cut over and before a Commit.

  Note: Only users with administrator privileges can execute the database action commands.

Database commands are executed from the **Database** web page. The database has three states: Committed, Switched Over and Changed. The current database status is displayed in the **Database status** pane of the **Database** web page as shown in Figure 138 "Database status: Changed" (page 257). Depending on the database status, some commands may not be available.

For example:

- If the database is in the **Committed** state, no commands are available.
- If the database is in the **Switched Over** state, the available commands are **Commit**, **Revert**, and **Roll back**.
- If the database is in the **Changed** state, the available commands are **Cut over** and **Roll back**.

For information about database commands, refer to "Database synchronization/operation component" (page 42).

To perform a:

- database **Cut over**, see Procedure 57 "Cutting over the database" (page 257).
- database **Revert**, see Procedure 58 "Reverting the database changes" (page 258).
- database **Commit**, see Procedure 60 "Committing the database" (page 260).

- database **Roll back**, see Procedure 59 "Rolling back changes to the database" (page 259).

Perform a database Cut over

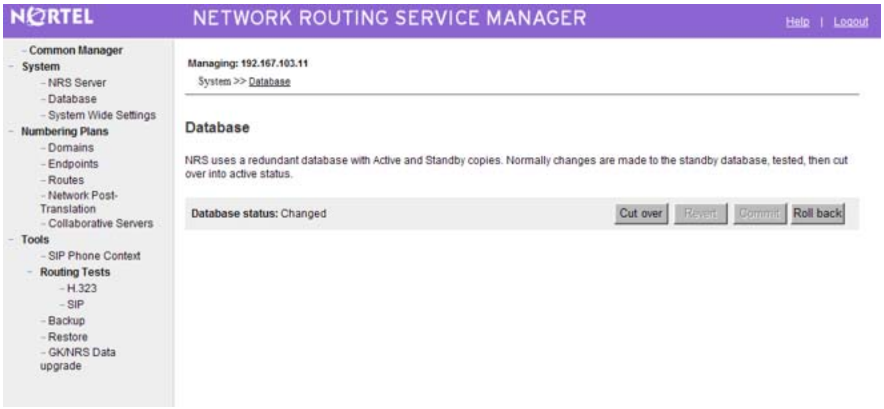
Cutting over a database switches the active and standby database access pointer. This swaps the primary and standby databases, so configuration changes take effect.

See Procedure 57 "Cutting over the database" (page 257) to perform a database cut over.

Procedure 57
Cutting over the database

Step	Action
1	In the **NRS Manager Navigator** select **System > Database.** The **Database** web page opens, as shown in Figure 138 "Database status: Changed" (page 257).

Figure 138
Database status: Changed



Managing: 192.167.103.11

System >> Database

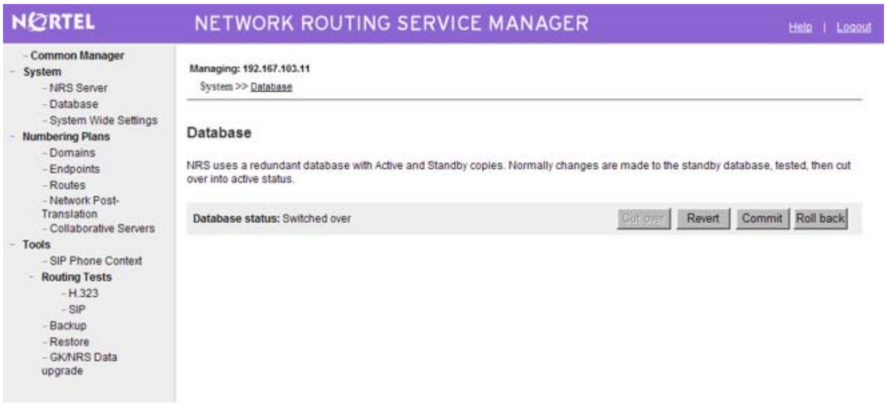
Database

NRS uses a redundant database with Active and Standby copies. Normally changes are made to the standby database, tested, then cut over into active status.

Database status: Changed

2	Click the **Cut over** button. The Cut over command is issued, and the database is placed into a *Switched over* state, as shown in Figure 139 "Database status: Switched over" (page 258).

Figure 139
Database status: Switched over



Managing: 192.167.103.11
System >> Database

Database

NRS uses a redundant database with Active and Standby copies. Normally changes are made to the standby database, tested, then cut over into active status.

Database status: Switched over

3 Perform a database **Commit** to save the changes after the cut over. See Procedure 60 "Committing the database" (page 260). If you do not want to save the changes to the database, perform a database Revert (see Procedure 58 "Reverting the database changes" (page 258)) or database Roll back (see Procedure 59 "Rolling back changes to the database" (page 259)).

—End—

Revert the database changes

After a database **Cut over**, the **Revert** command interchanges the active and standby database access pointers. The active and standby databases are swapped.

See Procedure 58 "Reverting the database changes" (page 258) to interchange the active and standby database access pointers .

Procedure 58
Reverting the database changes

Step	Action
1	In the **NRS Manager Navigator** select **System > Database.** The **Database** web page opens. The Database status is *Switched over*, as shown in Figure 139 "Database status: Switched over" (page 258).
2	Click the**Revert** button. The Revert command is issued, and the database is placed into a *Changed* state, as shown in Figure 138 "Database status: Changed" (page 257).

—End—

Perform database Roll back

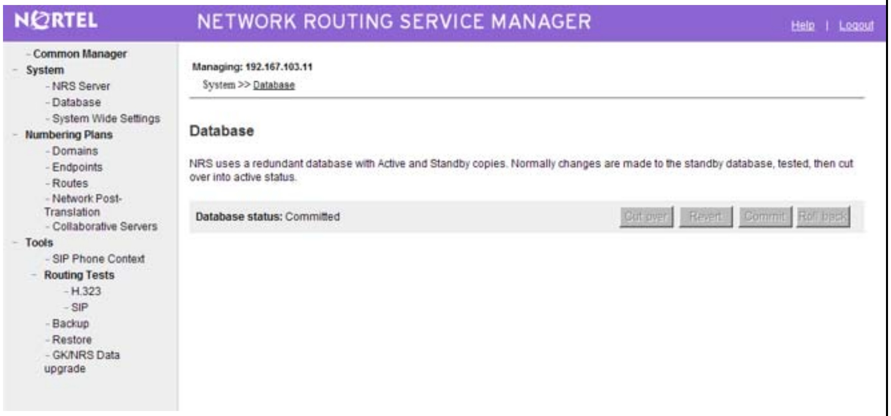
The **Roll back** command copies the active database to the standby database. As a result, any changes made during the latest provisioning to the standby database are erased. The standby database is synchronized with the active database. The **Roll back** command is available if the database is in the *Changed* or *Switched Over* state.

To roll back changes made to the standby database, perform Procedure 59 "Rolling back changes to the database" (page 259).

Procedure 59
Rolling back changes to the database

Step	Action
1	In the **NRS Manager Navigator** select **System > Database.** The **Database** web page opens. The Database status is *Switched over*, as shown in Figure 139 "Database status: Switched over" (page 258).
2	Select the **Roll back** button. The Roll back command is issued, and the database is placed into a *Committed* state, as shown in Figure 140 "Database status: Committed" (page 259).

Figure 140
Database status: Committed



Managing: 192.167.103.11
System >> Database

Database

NRS uses a redundant database with Active and Standby copies. Normally changes are made to the standby database, tested, then cut over into active status.

Database status: Committed

—End—

Commit the database changes

After a database **Cut over**, the **Commit** command copies data *from* the active database *to* the standby database. The previous configuration data is overwritten with the new configuration data. The standby database is synchronized with the active database.

See Procedure 60 "Committing the database" (page 260) to perform a database **Commit**.

Procedure 60

Committing the database

Step	Action
1	In the **NRS Manager Navigator** select **System > Database.** The **Database** web page opens. The Database status is *Switched over*, as shown in Figure 139 "Database status: Switched over" (page 258).
2	Select the **Commit** button. The **Commit** command is issued, and the database is placed into a *Committed* state, as shown in Figure 140 "Database status: Committed" (page 259).

—End—

Backup the database

NRS Manager provides a facility for backing up the NRS database.

The database can be automatically backed up or manually backed up.

- See the **automatic backup** option in Procedure 7 "Configuring system-wide settings" (page 162) to configure the backup time and location.
- The **manual backup** option allows you to immediately back up the database.

Note 1: Autobackup settings are saved during a database backup and are not changed during a database restore.

Note 2: Only users with administrator privileges can execute the database backup commands.

Automatically backup the database

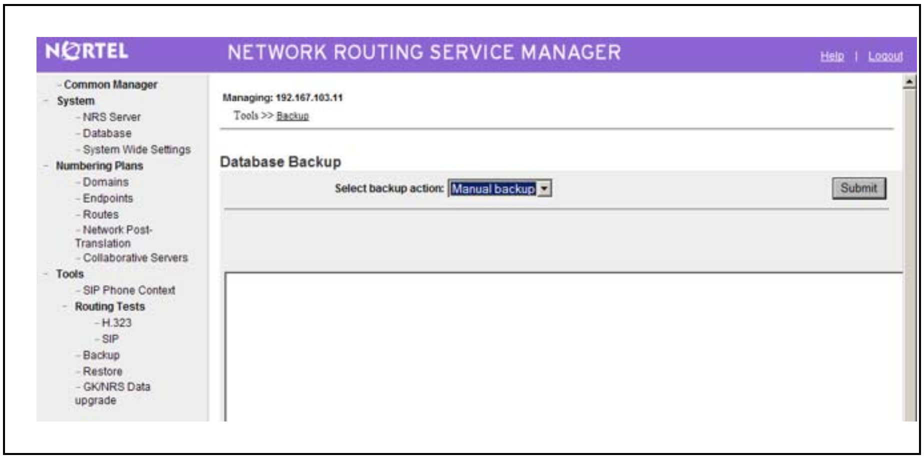
Use the following procedure to automatically backup the database.

Procedure 61
Backing up the database automatically

Step	Action

1 In the **NRS Manager Navigator** select **Tools > Backup.** The **Database Backup** web page opens, as shown in Figure 141 "Database Backup web page" (page 261).

Figure 141
Database Backup web page



Select backup action: Manual backup

2 Select **Auto backup** from the **Select backup action** drop-down list.

3 Click the **Submit** button.

The **System Wide Settings** web page opens, as shown in Figure 54 "System Wide Settings web page" (page 162).

4 Perform the following steps from Procedure 7 "Configuring system-wide settings" (page 162):

- step 3
- step 4
- step 5
- step 6

—End—

Manually backup the database

Use the following procedure to manually backup the database.

Procedure 62
Backing up the database manually

Step **Action**

1 In the **NRS Manager Navigator** select **Tools > Backup.** The **Database Backup** web page open, as shown in Figure 141 "Database Backup web page" (page 261).

2 Select **Manual backup** from the **Select backup action** drop-down list.

3 Click the **Submit** button.

A summary of the manual backup is displayed in the text area of the **Database Backup** web page, as shown in Figure 142 "Manual back up" (page 262).

Two links appear on the screen:

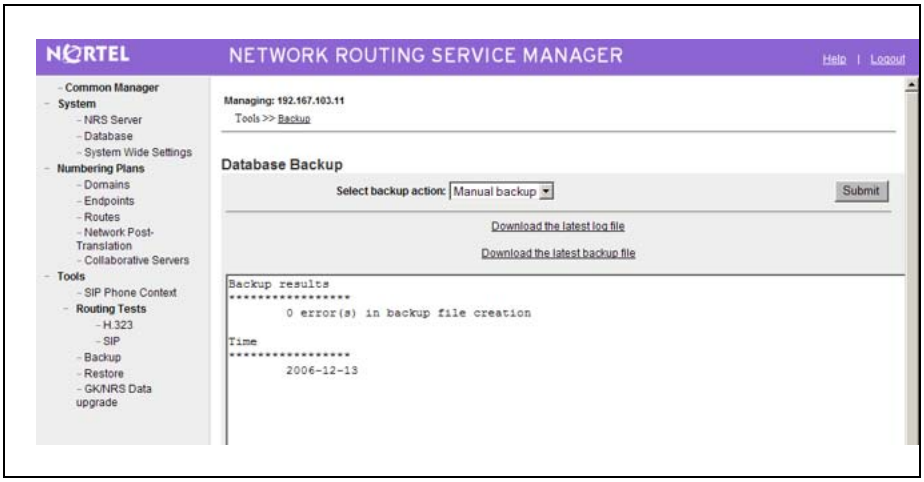
- **Download the latest log file**.

  See Procedure 64 "Downloading the latest backup log file" (page 265) to download the latest backup log file.

- **Download the latest backup file**.

  See Procedure 63 "Downloading the latest backup file" (page 263) to download the latest backup file.

Figure 142
Manual back up



Managing: 192.167.103.11

Database Backup

Select backup action: Manual backup

```
Backup results
*****************
        0 error(s) in backup file creation

Time
*****************
        2006-12-13
```

—End—

Download the latest backup file

Use the following procedure to download the latest backup file.

Procedure 63
Downloading the latest backup file

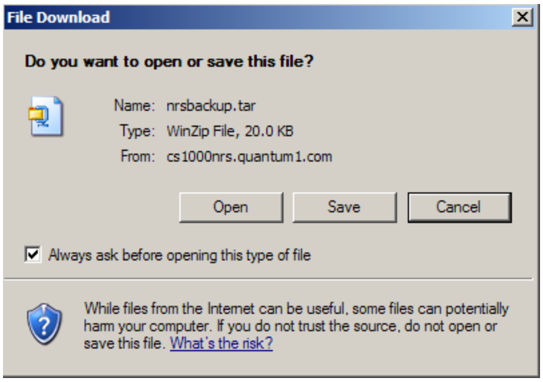
Step Action

1 See Procedure 62 "Manually backing up the database" (page 262)

2 Click the **Download the latest backup file** link on the **Database Backup** web page. See Figure 142 "Manual back up" (page 262).

The **File Download** dialog box opens.

Figure 143
File Download dialog box



Do you want to open or save this file?

Name: nrsbackup.tar
Type: WinZip File, 20.0 KB
From: cs1000nrs.quantum1.com

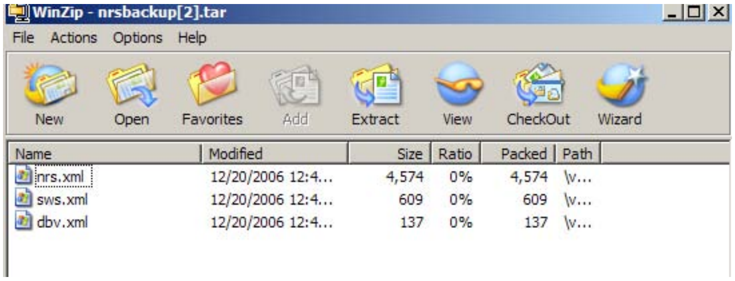
☑ Always ask before opening this type of file

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

The **File Download** dialog box provides the option to open the latest backup file or download and save the latest backup file to the user's local client (PC).

3 Click **Open** to view the latest backup file.

Figure 144
Latest backup file



Name	Modified	Size	Ratio	Packed	Path
nrs.xml	12/20/2006 12:4...	4,574	0%	4,574	\v...
sws.xml	12/20/2006 12:4...	609	0%	609	\v...
dbv.xml	12/20/2006 12:4...	137	0%	137	\v...

The file is a compressed file that contains multiple backup files. The name of the compressed file is nrsback.tar

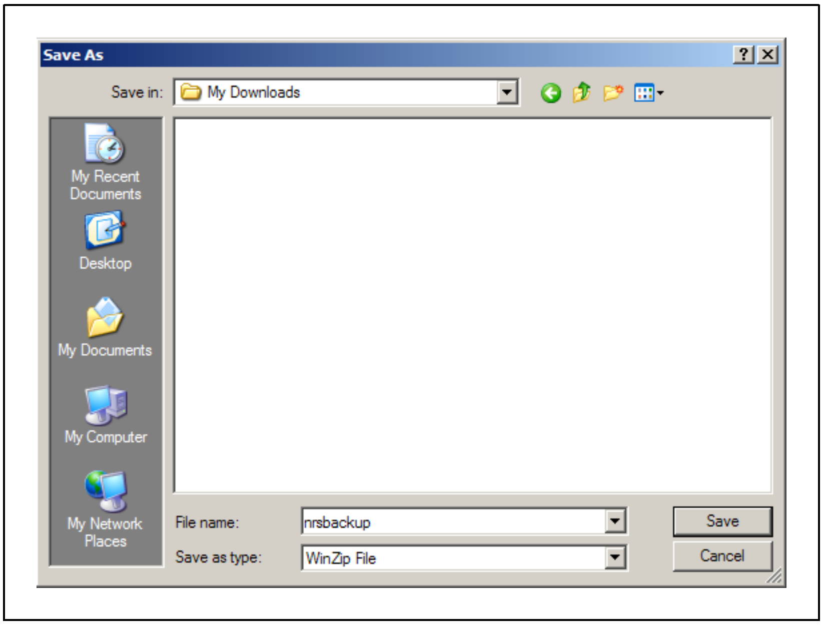
Select a file from the **Name** column. Click the **Extract** icon to download the selected file.

Or

4 Click **Save** to save the file to a local client.

The **Save As** dialog box opens.

Figure 145
Save As dialog box



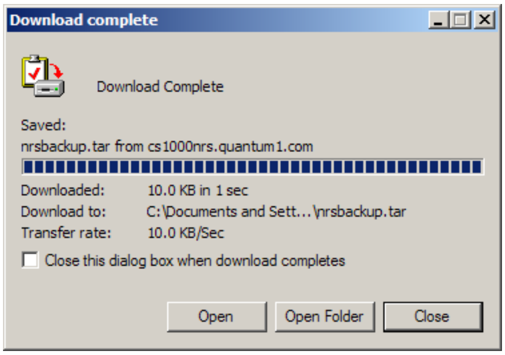
File name: nrsbackup

Save as type: WinZip File

5 Select a folder from the **Save in** drop down list. Enter a file name in the **File name** text box. Click **Save**.

The **Download complete** window opens.

Figure 146
Download complete window



Download Complete

Saved:
nrsbackup.tar from cs1000nrs.quantum1.com

Downloaded:	10.0 KB in 1 sec
Download to:	C:\Documents and Sett...\nrsbackup.tar
Transfer rate:	10.0 KB/Sec

□ Close this dialog box when download completes

—End—

Download the latest backup log file

Use the following procedure to download the latest backup log file.

Procedure 64
Downloading the latest backup log file

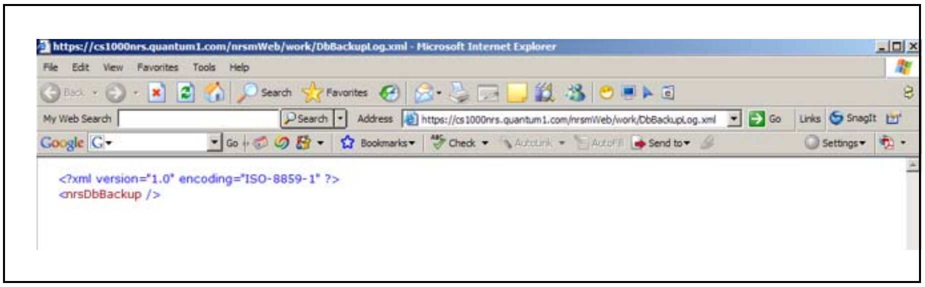
Step	Action

1 See Procedure 62 "Manually backing up the database" (page 262)

2 Click **Download the latest log file** link on the **Database Backup** web page. See Figure 142 "Manual back up" (page 262).

A window opens containing the latest backup log file, as shown in Figure 144 "Latest backup file" (page 263). The name of the log file is DbBackupLog.xml. The DbBackupLog.xml file contains information about the backup. For example, if there were errors during the back up process.

Figure 147
Backup log file



Address: https://cs1000nrs.quantum1.com/nrsmWeb/work/DbBackupLog.xml

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<nrsDbBackup />
```

3 The backup log file can be saved using the **File > Save As...** menu option.

—End—

Restore the NRS database

The database can be restored:

- From the connected Signaling Server
- From a secure FTP site
- From the client machine

Note 1: Autobackup settings are saved during a database backup and are not changed during a database restore.

Note 2: Only users with administrator privileges can execute the database restore commands.

Upon executing the database restore operation on the same database, the ID (that is, Primary Key) is changed in the standby schema. As a result, during Cut over (just before swapping the active and standby schema), it removes the old registration details and updates the new registration entries because of data mismatch. So, all the endpoints will be deregistered for a limited time until the next re-registration occurs. This action functions in the same manner as Release 4.0/4.5. To minimize the impact of the operation due to the execution of the database restore and Cut over, the following steps should be followed:

1. Set the re-registration time to 30 seconds, and wait for the original time period to expire.
2. Perform the database restore and Cut over and wait for 30 seconds
3. If desired, return the re-registration time back to its original value

For instance, if the original registration period is set to five minutes, perform the following steps:

1. Change the re-registration period to 30 seconds and wait for five minutes.
2. Execute the database restore and Cut over operations and wait for 30 seconds.
3. Change the re-registration period back to five minutes.

Restore the database

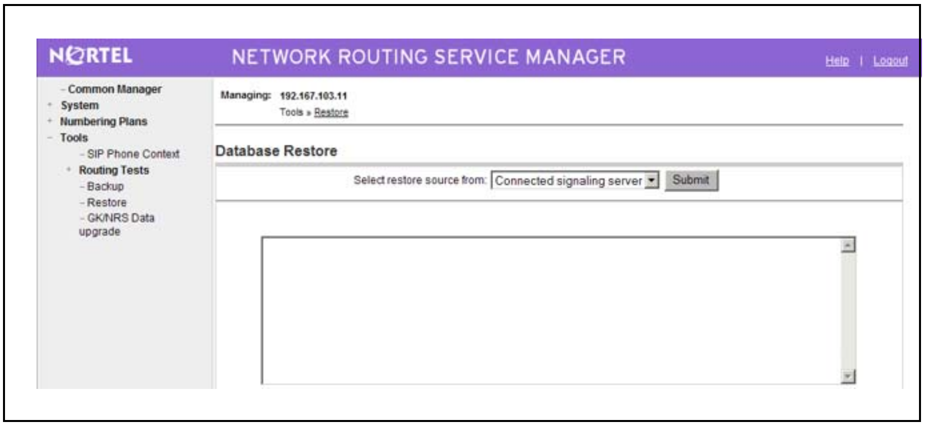
Use the following procedure to restore the database.

Procedure 65
Restoring the database

Step	Action

1 In the **NRS Manager Navigator** select **Tools > Restore.** The **Database Restore** web page opens, as shown in Figure 148 "Database Restore web page" (page 267).

Figure 148
Database Restore web page



Managing: 192.167.103.11

Database Restore

Select restore source from: Connected signaling server

2 The database can be restored from three source locations:

- From the **Connected Signaling Server**.
  See Procedure 66 "Restoring from the connected Signaling Server" (page 268) to restore the database from the Connected Signaling Server.
- From a secure **FTP site**.
  See Procedure 67 "Restoring from a secure FTP site" (page 269)to restore the database from a secure FTP site.
- From the **Client machine**.
  See Procedure 68 "Restoring from a client machine" (page 270) to restore the database from the Client machine.

—End—

Restore from the connected Signaling Server

Use the following procedure to restore from the connected Signaling Server.

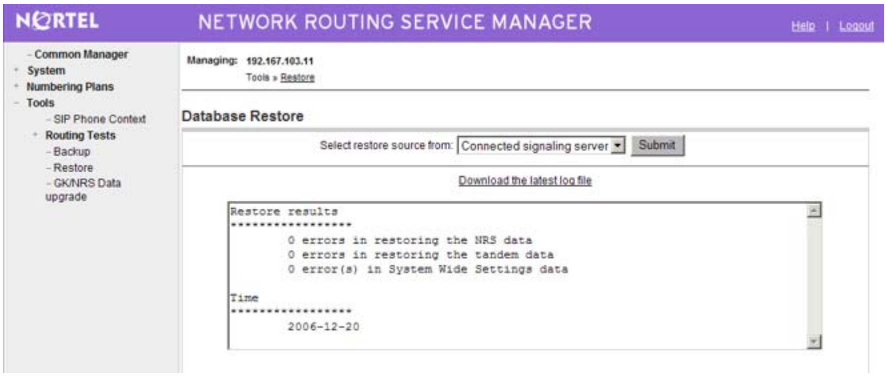
Procedure 66
Restoring from the connected Signaling Server

Step	Action
1	In the **NRS Manager Navigator** select **Tools > Restore.** The **Database Restore** web page opens, as shown in Figure 148 "Database Restore web page" (page 267).
2	Select **Connected Signaling Server** from the **Select restore source from** drop-down list. See Figure 148 "Database Restore web page" (page 267).
3	Click the **Submit** button.

A message displays in the text area of the **Database Restore** web page showing a summary of the database restore from the Signaling Server. See Figure 149 "Database Restore from connected Signaling Server" (page 268).

The **Download the latest log file** link also appears on the web page. See Procedure 69 "Downloading the latest restore log file" (page 272) for downloading the restore log file.

Figure 149
Database Restore from connected Signaling Server



Managing: 192.167.103.11
Tools » Restore

Database Restore

Select restore source from: Connected signaling server

```
Restore results
*****************
        0 errors in restoring the NRS data
        0 errors in restoring the tandem data
        0 error(s) in System Wide Settings data

Time
*****************
        2006-12-20
```

—End—

Restore from a secure FTP site

Use the following procedure to restore from a secure FTP site.

Procedure 67
Restoring from a secure FTP site

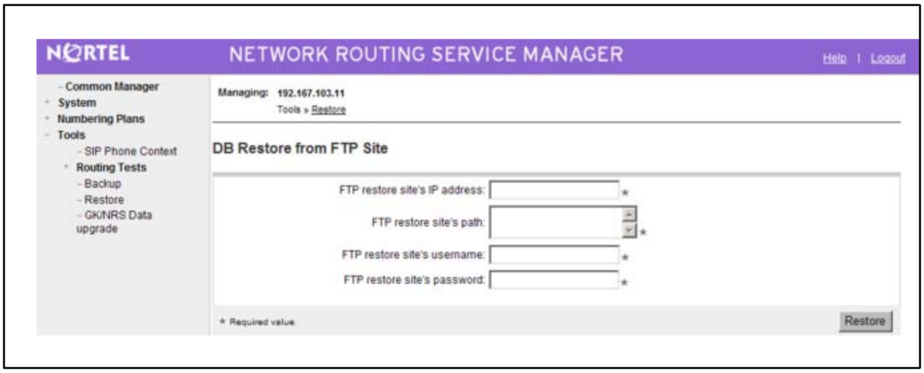
Step **Action**

1 In the **NRS Manager Navigator** select **Tools > Restore.** The **Database Restore** web page opens, as shown in Figure 148 "Database Restore web page" (page 267).

2 Select **FTP site** from the **Select restore source from** drop-down list.

3 Click the **Submit** button. The **DB Restore from FTP Site** web page opens, as shown in Figure 150 "Database Restore from FTP site" (page 269).

Figure 150
Database Restore from FTP site



Managing: 192.167.103.11

4 Enter the **FTP restore site’s IP address** in the text box.

5 Enter the **FTP restore site’s path** in the text box.

6 Enter the **FTP restore site’s username** in the text box.

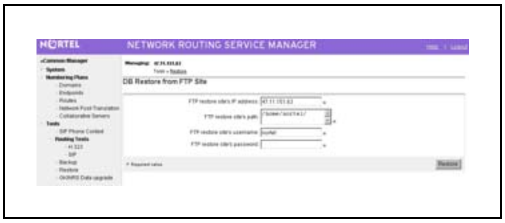
7 Enter the **FTP restore site’s password** in the text box.

8 Click **Restore**.

A message is displayed in the text area of the DB Restore from FTP Site web page, showing a summary of the database restore from the FTP site. See Figure 151 "Database Restore from FTP site results" (page 270).

The **Download the latest log file** link also appears on the web page. See Procedure 69 "Downloading the latest restore log file" (page 272) for downloading the restore log file.

Figure 151
Database Restore from FTP site results



Managing: 47.11.151.83
Tools » Restore

DB Restore from FTP Site

FTP restore site's IP address: 47.11.151.83 *
FTP restore site's path: /home/nortel/ *
FTP restore site's username: nortel *
FTP restore site's password: *

* Required value

—End—

Restore from a client machine

Use the following procedure to restore from a client machine.

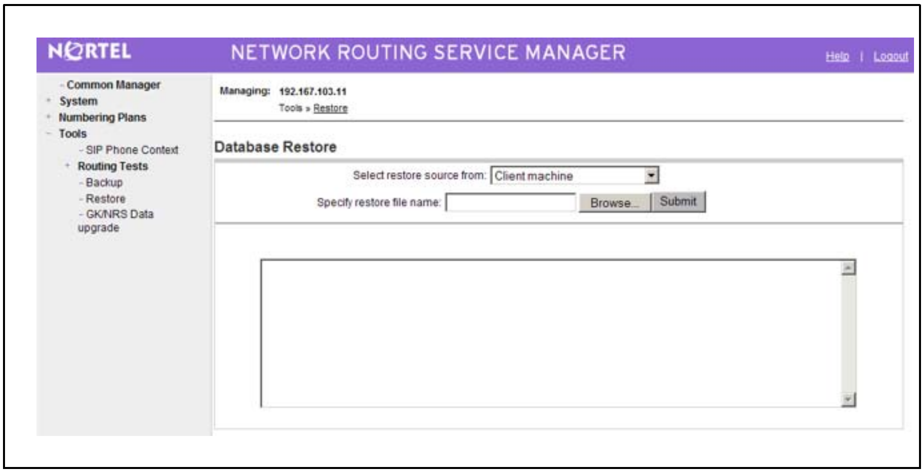
Procedure 68
Restoring from a client machine

Step	Action

1 In the **NRS Manager Navigator** select **Tools > Restore.** The **Database Restore** web page opens, as shown in Figure 148 "Database Restore web page" (page 267).

2 Select **Client machine** from the **Select restore source from** drop-down list. See Figure 148 "Database Restore web page" (page 267). The **Database Restore** web page opens, as shown in Figure 152 "Database Restore from client machine" (page 270).

Figure 152
Database Restore from client machine



Managing: 192.167.103.11
Tools » Restore

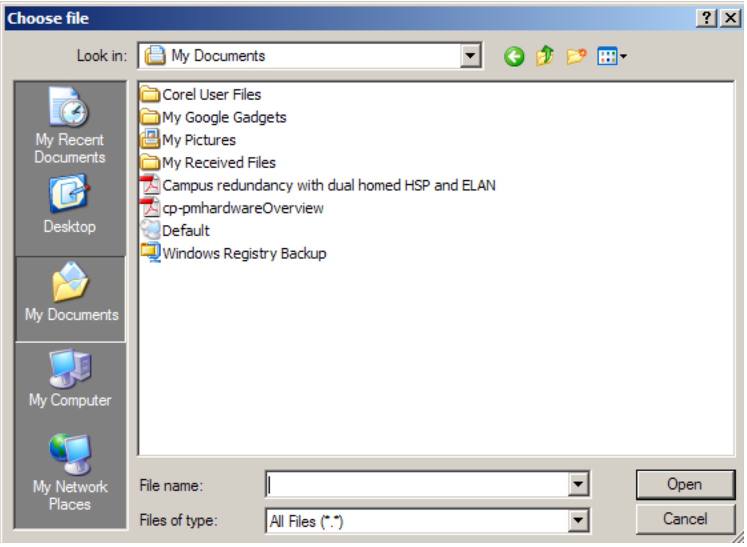
Database Restore

Select restore source from: Client machine
Specify restore file name:

3 The **Database Restore** web page contains a **Specify restore file name** text box and a **Browse** button. Click **Browse** to navigate to the folder containing the backup file.

The **Choose file** dialog window opens.

Figure 153
Choose file dialog window



Files of type: All Files (*.*)

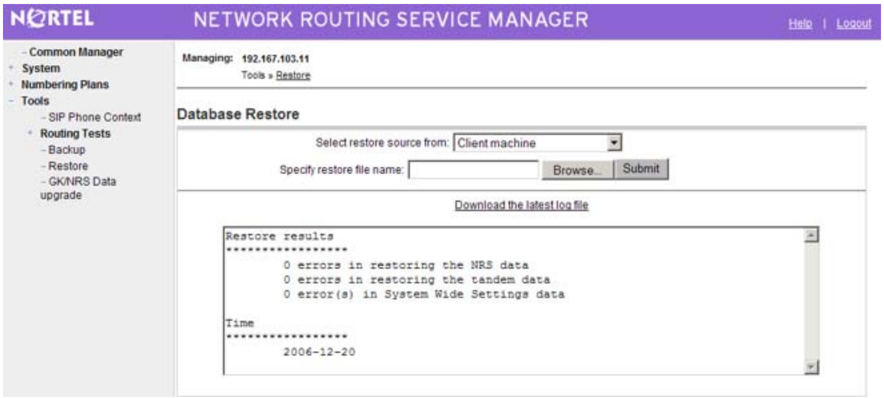
4 Select the backup file, and click **Open**.

The **Specify restore file name** text box auto-fills with the path and filename of the backup file.

5 Click the **Submit** button.

A message is displayed in the text area of the **Database Restore** web page showing a summary of the database restore from the client machine. See Figure 154 "Database Restore client machine results" (page 271).

Figure 154
Database Restore client machine results



Managing: 192.167.103.11

Select restore source from: Client machine

```
Restore results
*****************
        0 errors in restoring the NRS data
        0 errors in restoring the tandem data
        0 error(s) in System Wide Settings data

Time
*****************
        2006-12-20
```

The **Download the latest log file** link also appears on the web page. See Procedure 69 "Downloading the latest restore log file" (page 272) to download the restore log file.

—End—

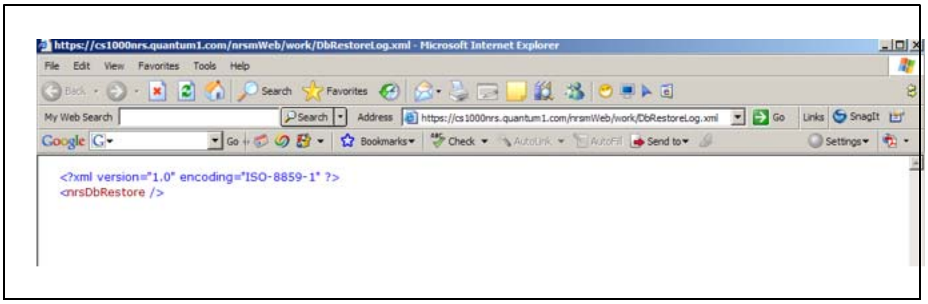
Download the latest restore log file

Use the following procedure to download the latest restore log file.

Procedure 69
Downloading the latest restore log file

Step	Action
1	NRS Manager provides the option to restore the database from three source locations: • See Procedure 66 "Restoring from the connected Signaling Server" (page 268) to restore the database from the **Connected Signaling Server**. • See Procedure 67 "Restoring from a secure FTP site" (page 269)to restore the database from a secure **FTP site**. • See Procedure 68 "Restoring from a client machine" (page 270) to restore the database from the **Client machine**.
2	Click the **Download the latest log file** link to view the Restore log file. A window opens containing the latest restore log file, as shown in Figure 155 "Restore log file" (page 272). The name of the log file is DbRestoreLog.xml. The DbRestoreLog.xml file contains information about the database restore.

Figure 155
Restore log file



https://cs1000nrs.quantum1.com/nrsmWeb/work/DbRestoreLog.xml - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
My Web Search Search Address https://cs1000nrs.quantum1.com/nrsmWeb/work/DbRestoreLog.xml Go Links SnagIt
Google G Go Bookmarks Check AutoLink AutoFill Send to Settings

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<nrsDbRestore />
```

Step	Action
3	The restore log file can be saved, using the **File > Save As...** menu option.

—End—

GK/NRS Data Upgrade

The **Tools > GK/NRS Data Upgrade** link in the **NRS Manager Navigator** is used to upgrade a Succession 3.0 H.323 Gatekeeper to a CS 1000 Release 4.0 (or later) NRS. If required, this procedure must be completed as part of your upgrade procedures.

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

Migration overview

It is best practice to configure both a Primary and Secondary NRS to assure high availability of the IP Telephony network.

It is best practice to configure both a Primary and a Backup Security Server per ECM security domain to assure a highly available authentication and authorization service for OA&M users who need to access managed systems/elements in the ECM security domain, as well as for auxiliary applications that rely on continuous availability of the ECM framework web services API to monitor and control the CS 1000.

To migrate your system, you must convert the Succession 3.0 H.323 Gatekeeper database into a CS 1000 Release 4.0 (or later) NRS database. This involves the following tasks:

- Backing up the Succession 3.0 H.323 Gatekeeper database using Element Manager to ftp site or management PC.
- Installing and configuring the Linux-based NRS Primary and Secondary servers with the new IP addresses. See "Introduction" (page 112) and "Installation of Linux operating system, ECM framework and NRS application" (page 113).

  This step has four substeps:

  1. Install the Linux operating system on IBM 306m (NTDU99AA) or on HP DL320 G4 (NTDU97AA) stand-alone servers.
  2. Install the Primary and Secondary NRS, the Primary Security Service and the Backup Security Service.
  3. Add the NRS Manager for the Primary and Secondary NRS servers as managed elements of the ECM.
  4. Create user accounts and assign roles and permissions for access to the Primary and Secondary NRS servers from the ECM.

Refer to *Linux Platform Base and Applications Installation and Commissioning (NN43001-315)* for detailed information on installing the Linux operating system, the ECM framework, the NRS and the Primary and Backup Security Services.

Refer to *Enterprise Common Manager Fundamentals (NN43001-116)* for detailed information on adding a managed element to the ECM, creating user accounts, and assigning roles and permissions for access to the NRS server from the ECM.

- Adding a Service Domain and Level 1 domain using NRS Manager. (These two domains do not exist in the Release 3.0 Gatekeeper.) See Procedure 9 "Adding a Service Domain" (page 166) to add a Service Domain . See "Adding a Level 1 Domain (UDP)" (page 172) to add a Level 1 Domain.
- Using the **Tools > GK/NRS Data Upgrade** link in the **NRS Manager Navigator** to convert the H.323 Gatekeeper database to the CS 1000 Release 4.0 (or later) NRS database using NRS Manager.
- Performing database **Cut over** and database **Commit** commands.

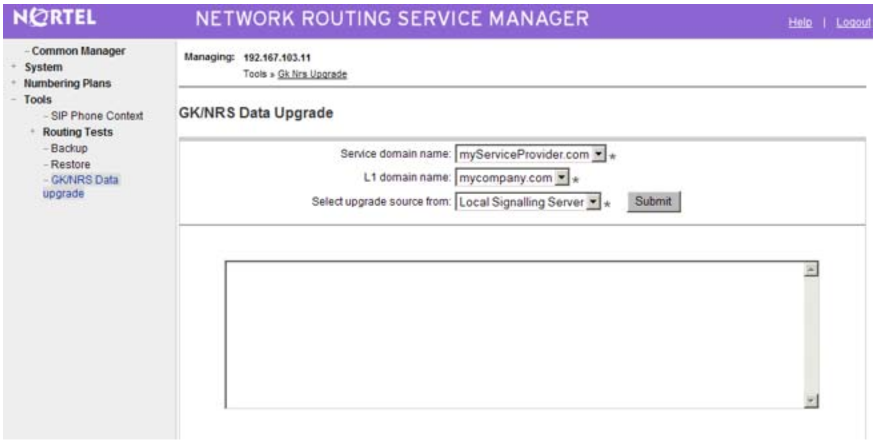
  The converted H.323 Gatekeeper database is stored in the NRS standby database. Changes made to the standby database do not immediately effect call processing. Before changes made to the standby database effect call processing, database **Cut over** and **Commit** commands must be executed. See "Performing NRS database actions" (page 255).

  See Procedure 57 "Cutting over the database" (page 257) to perform a database **Cut over** . See Procedure 60 "Committing the database" (page 260) to perform a database **Commit**.

  Note: Only users with administrator privileges can execute Gatekeeper/NRS (GK/NRS) data conversion.

Figure 156 "GK/NRS Data Upgrade web page" (page 275) and Figure 157 "GK/NRS Data Upgrade results" (page 275) are only for illustration purposes, to show the user interface for the Gatekeeper to NRS Upgrade area in NRS Manager.

**Figure 156
GK/NRS Data Upgrade web page**



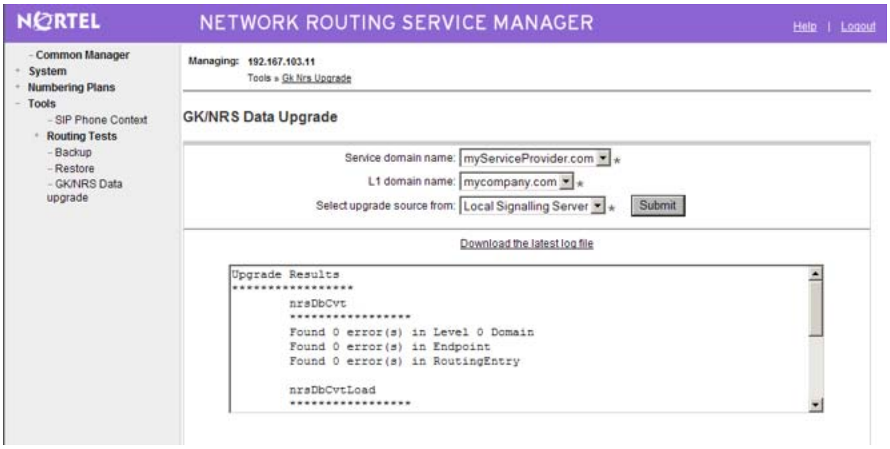
Managing: 192.167.103.11

Service domain name: myServiceProvider.com *

L1 domain name: mycompany.com *

Select upgrade source from: Local Signalling Server *

**Figure 157
GK/NRS Data Upgrade results**



Managing: 192.167.103.11

Service domain name: myServiceProvider.com *

L1 domain name: mycompany.com *

Select upgrade source from: Local Signalling Server *

```
Upgrade Results
*****************
        nrsDbCvt
        *****************
        Found 0 error(s) in Level 0 Domain
        Found 0 error(s) in Endpoint
        Found 0 error(s) in RoutingEntry

        nrsDbCvtLoad
        *****************
```

Configure and manage the VxWorks-based Network Routing Service

Contents

This section contains information on the following topics:

Introduction

The Network Routing Service (NRS) can be configured and maintained through a web interface called NRS Manager. NRS Manager is a multi-customer user interface. The NRS includes a Service Domain level that is used to support multiple customers.

> ***Note:*** NRS Manager replaces the Succession 3.0 H.323 Gatekeeper web pages in CS 1000 Element Manager in CS 1000 Release 4.0 and later.

The NRS can also be accessed directly from the Command Line Interface of the Signaling Server. This does not provide access to NRS Manager, but does allow users to run NRS-specific CLI commands listed in Command Line Interface commands.

Browser configuration

Your web browser must be properly configured before using NRS Manager.

Supported browser

NRS Manager is supported only on Microsoft Internet Explorer version 6.0 (or later).

> **ATTENTION**
>
> Nortel discourages use of the Back, Forward, and Refresh buttons of the browser.
>
> Use of the Back button is not recommended while the NRS Manager application is launched, because NRS Manager pages contain dynamic data content. NRS Manager provides a path for navigation purposes on top of every NRS Manager page.
>
> Nortel recommends that the user click the navigation path to go back to the previous page (instead of using the Back button).

Configuring the browser and display settings

Before you can use NRS Manager, the following tasks must be completed:

- Enable popups in the browsers search utility (mandatory).
- Configure the Internet Explorer browser settings (mandatory).
- Configure the Windows Display settings (highly recommended).

Note: The interface for the Internet Explorer browser settings and Windows Display settings may vary by browser version and by operating system.

Enabling popups

If you are using a browser search utility (such as the Google™ search engine or the Yahoo!™ search engine), ensure that popups are enabled. Enabling pop-up windows is usually done at the search utility's toolbar.

> **ATTENTION**
>
> Do not block pop-up windows if you are using a search utility (such as Google™ or Yahoo!™ search engines) in your browser.

Configuring the browser settings

Follow Procedure 70 "Configure the Internet Explorer browser settings" (page 280) to configure the following Internet Explorer browser settings:

- Browser retrieve page information.
- Empty session information.
- Deselect the AutoComplete options.

Procedure 70
Configure the Internet Explorer browser settings

Step	Action

1 Select **View > Text Size > Medium** to configure text size in the browser.

2 Select **Tools > Internet Options** in the Internet Explorer browser window.

The **Internet Options** window opens.

3 Configure the browser retrieve page information:

a. On the **General** tab under the **Temporary Internet files** section, click **Settings**.

The **Settings** window opens.

b. Under the **Check for newer versions of stored pages** section, select the **Every visit to the page** option.

c. Click **OK**.

4 Configure the empty session information:

a. Select the **Advanced** tab.

b. Under **Security**, select **Empty Temporary Internet Files folder when browser is closed**.

5 Deselect the AutoComplete options.

a. Select the **Content** tab.

b. Under **Personal Information**, click **AutoComplete**.

The **AutoComplete Settings** window opens.

c. Under the **Use AutoComplete for** section, deselect **Forms** and **User names and passwords on forms**.

Click **OK** (to close the **AutoComplete Settings** window)

Click **OK** (to close the **Internet Options** window)

—End—

Configuring the Windows Display settings

Follow Procedure 71 "Configuring the Windows Display settings" (page 281) to configure the Windows display settings.

Procedure 71
Configuring the Windows Display settings

Step	Action
1	Select **Start > Settings > Control Panel > Display**. The **Display Settings** window opens.
2	Select the **Settings** tab.
3	Select **True Color (32 bit)** from the **Colors** drop-down list.
4	Under **Screen area**, select **1280 by 1024 pixels**.
5	Click **OK**.

—End—

Enabling and configuring the NRS server

The NRS server must be enabled and properly configured before any NRS data can be provisioned using NRS Manager.

ATTENTION

The Network Routing Service can be redundantly installed across a cluster of Network Routing Servers sharing a distributed database.

In CS 1000 Release 5.0 the cluster is comprised of a Primary Network Routing Server and an Alternate Network Routing Server. Optionally, a Failsafe Network Routing Server can be co-resident with an IP Peer Gateway (H.323 or SIP) on a Signaling Server in an IP telephony node.

The Primary, Alternate and (optional) Failsafe Network Routing Servers must host the same major software release. For example, all servers must host release 4.50.xx or 5.00.xx. Network Routing Servers hosting different major software releases cannot synchronize the NRS databases.

Refer to Signaling Server: Installation and Configuration (553-3001-212) for detailed information on the Network Routing Server installation procedures

The VxWorks-based NRS server can be configured in two modes:

- Stand-alone mode — The host Signaling Server is not registered to a Call Server. During installation of the Signaling Server, ensure that the Call Server IP address is configured as 0.0.0.0.

  Note: During installation of the Signaling Server in stand-alone mode (using the Signaling Server Software Install Tool), the administrator is not prompted to enter the Call Server IP address. Instead, the Call Server IP address defaults to 0.0.0.0. During the installation, the parameter confirmation screen displays the IP address as 0.0.0.0.

- Co-resident mode — The NRS is co-resident on a Signaling Server that is registered to a Call Server. The Signaling Server can also run other applications, such as the IP Line TPS and the Virtual Trunk applications.

Stand-alone mode

Procedure 72
Enabling and configuring the NRS server in stand-alone mode

Step	Action

1 Enable the NRS and configure the NRS server settings using the Signaling Server Software Install Tool.

Refer to *Signaling Server: Installation and Configuration (553-3001-212)* for detailed information on the Signaling Server Software Install Tool and for detailed installation procedures for configuring a stand-alone Signaling Server.

The following is a summary of the tasks required for the installation of a stand-alone Signaling Server. Follow the detailed procedures presented in *Signaling Server: Installation and Configuration (553-3001-212)* for complete instructions.

a. Perform the introductory steps for the Signaling Server installation.

b. Configure the Signaling Server as a Leader, when prompted.

c. Configure stand-alone mode (NRS only — no Call Server) for the Signaling Server.

d. Select whether the NRS supports the SIP Redirect Server, the H.323 Gatekeeper, or both.

e. Select the type of NRS — Primary or Alternate.

f. Enter the following:

   1. Enter the hostname.

   2. Enter the ELAN network interface IP address, subnet mask, and gateway IP address.

   3. Enter the TLAN network interface IP address, subnet mask, and gateway IP address.

g. The Call Server IP address defaults to 0.0.0.0. for a stand-alone Signaling Server.

h. Enter the IP address of the NRS (Primary or Alternate NRS IP address).

2 Restart the Signaling Server after proper configuration of the Signaling Server.

If the Signaling Server restarts successfully, the NRS is configured with the default settings.

3 Log in to the NRS Manger using the default user ID and password. See Procedure 75 "Logging in to NRS Manager using the browser address field" (page 291).

4 Configure the NRS Server Settings in NRS Manager. See Procedure 79 "Configuring NRS Server Settings" (page 302).

5 Log out of the NRS. See Procedure 76 "Logging out of NRS Manager" (page 298).

6 Restart the Signaling Server.

If the Signaling Server boots successfully, then the NRS server is properly configured.

—End—

Co-resident mode

Procedure 73
Enabling and configuring the NRS server in co-resident mode

Step Action

Note: If the Signaling Server has been configured in co-resident mode, proceed directly to step 3.

1 Enable the NRS and configure the NRS server settings using the Signaling Server Software Install Tool.

Refer to *Signaling Server: Installation and Configuration (553-3001-212)* for detailed information on the Signaling Server Software Install Tool and for detailed installation procedures for configuring a co-resident Signaling Server.

The following is a summary of the tasks required for the installation of a co-resident Signaling Server. Follow the detailed procedures presented in *Signaling Server: Installation and Configuration (553-3001-212)* for complete instructions.

a. Perform the introductory steps for the Signaling Server installation.

b. Configure the Signaling Server as a Leader, when prompted.

c. Select co-resident mode (LTPS + VTRK + NRS) for the Signaling Server.

d. Select whether the NRS supports the SIP Redirect Server, the H.323 Gatekeeper, or both. (The option to configure no NRS is also available.)

e. Select the type of NRS — Primary, Alternate or Failsafe.

f. Enter the following:

   1. Enter the hostname.

   2. Enter the ELAN network interface IP address, subnet mask, and gateway IP address.

   3. Enter the TLAN network interface IP address, subnet mask, and gateway IP address.

g. Enter the IP address of the NRS (Primary and/or Alternate NRS IP address).

2 Restart the Signaling Server after proper configuration of the Signaling Server. See Warm restarting the Signaling Server.

3 Log in to Element Manager. See Launching Element Manager.

4 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the navigator.

The **Node Configuration** web page opens.

5 Click **Edit**.

The **Edit** web page opens.

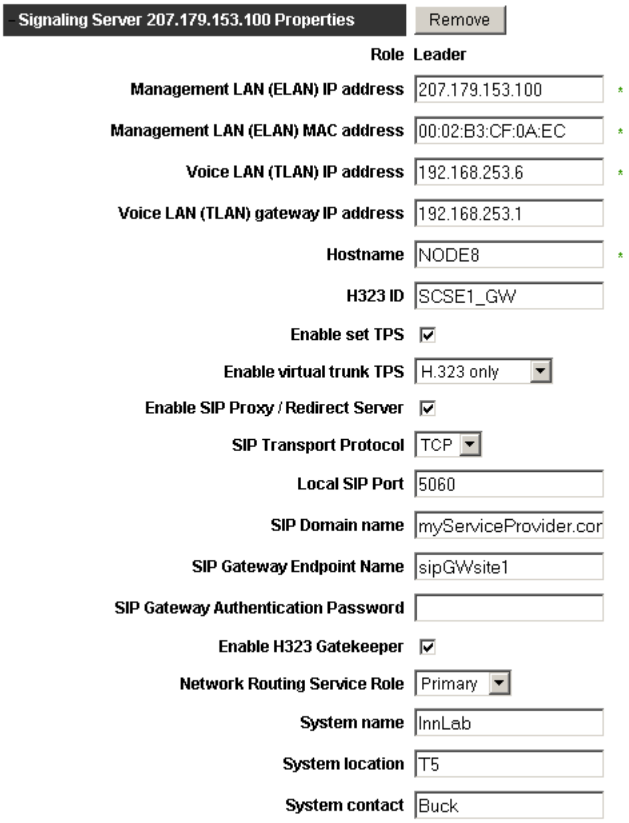
6 Click **Signaling Servers** to expand the section.

A list of Signaling Servers opens.

7 Select the appropriate **Signaling Server xxx.xxx.xxx.xxx Properties**.

The properties for that Signaling Server display, as shown in Figure 158 "Signaling Server xxx.xxx.xxx.xxx properties" (page 285).

Figure 158
Signaling Server xxx.xxx.xxx.xxx properties



Signaling Server 207.179.153.100 Properties   Remove

Role	Leader	
Management LAN (ELAN) IP address	207.179.153.100	*
Management LAN (ELAN) MAC address	00:02:B3:CF:0A:EC	*
Voice LAN (TLAN) IP address	192.168.253.6	*
Voice LAN (TLAN) gateway IP address	192.168.253.1	
Hostname	NODE8	*
H323 ID	SCSE1_GW	
Enable set TPS	☑	
Enable virtual trunk TPS	H.323 only	
Enable SIP Proxy / Redirect Server	☑	
SIP Transport Protocol	TCP	
Local SIP Port	5060	
SIP Domain name	myServiceProvider.cor	
SIP Gateway Endpoint Name	sipGWsite1	
SIP Gateway Authentication Password		
Enable H323 Gatekeeper	☑	
Network Routing Service Role	Primary	
System name	InnLab	
System location	T5	
System contact	Buck	

8 To enable the NRS, do the following:

a. Enable the SIP Proxy/Redirect Server and/or the H.323 Gatekeeper, as appropriate:

- Select the **Enable SIP Proxy / Redirect Server** check box to enable the SIP Redirect Server (see Figure 159 "Enabling the SIP Redirect Server" (page 285)).

  Figure 159
  Enabling the SIP Redirect Server

  Enable SIP Proxy / Redirect Server ☑

  Note 1: CS 1000 VxWorks-based NRS does not support the SIP Proxy Server.

  Note 2: The SIP Trunk Gateway must also be configured, see Enabling and configuring the SIP Trunk Gateway.

- Select the **Enable H.323 Gatekeeper** check box to enable the H.323 Gatekeeper (see Figure 160 "Enabling the H.323 Gatekeeper" (page 286)).

  Figure 160
  Enabling the H.323 Gatekeeper

  Enable H323 Gatekeeper ☑

  > ***Note:*** The H.323 Gateway must also be configured, see Enabling and configuring the H.323 Gateway.

b. Select the role of the NRS from the **Network Routing Service Role** drop-down list.

   The three options are Primary, Alternate, and Failsafe.

9 Configure the other required Signaling Server properties.

10 Click **Save and Transfer** to save the changes and transfer the properties to all nodes.

11 Click **Logout** at the bottom of the navigator to log out of Element Manager.

12 Restart the Signaling Server. See Warm restarting the Signaling Server.

13 After a successful restart of the Signaling Server, log in to NRS Manager using the default user ID and password. See Procedure 75 "Logging in to NRS Manager using the browser address field" (page 291).

14 Configure the NRS Server Settings in NRS Manager. See Procedure 79 "Configuring NRS Server Settings" (page 302).

15 Log out of the NRS. See Procedure 76 "Logging out of NRS Manager" (page 298).

16 Restart the Signaling Server.

If the Signaling Server boots successfully, then the NRS server is properly configured.

—End—

Changing a co-resident NRS server to a stand-alone NRS server

Use the Signaling Server Software Install Tool to change a co-resident NRS server to a stand-alone NRS.

Task summary

This section provides a high-level overview of the Configuring and Managing the VxWorks-based NRS task. The main steps are:

- Accessing the NRS Manager.
- Configuring the NRS.
- Configuring the Primary and Alternate NRS servers.
- Configuring and managing the NRS database. The NRS database provides a central database of addresses that are required to route calls across the network.
- Procedures for performing other tasks in the NRS including testing routes, enabling/disabling the NRS server, viewing the SIP Phone Context, and viewing database reports.
- Administering NRS Manager users.
- Logging out of NRS Manager.

In more detail, the Configuring and Managing the VxWorks-based NRS task is comprised of:

Step	Action
1	**Log in to NRS Manager.** See "Accessing NRS Manager" (page 290). You can log in two ways: • See Procedure 74 "Logging in to NRS Manager from Element Manager" (page 290) • See Procedure 75 "Logging in to NRS Manager using the browser address field" (page 291)
2	**Verify that the NRS is the Primary NRS and is active**. See Procedure 77 "Verifying that the NRS is the Primary NRS and is active" (page 299)
3	**Configure System Wide Settings**. See Procedure 78 "Configuring system-wide settings" (page 300)
4	**Configure the Primary and Alternate NRS Server Settings**. See Procedure 79 "Configuring NRS Server Settings" (page 302)
5	**Build the NRS database.** The NRS database comprises • service domains, L1 domains and L0 domains

- collaborative servers
- gateway endpoints
- routing entries

Note: The following steps **must** be performed in the order given.

a. Create the Service Domain, Level 1 Domains (UDP), Level 0 Domains (CDP), which hold the endpoint numbering plans on the NRS. This is complementary to the CDP configuration on the Call Server.

   1. See "Adding a Service Domain" (page 310)
   2. See "Adding a Level 1 Domain (UDP)" (page 312)
   3. See "Adding a Level 0 Domain (CDP)" (page 316)

b. Add collaborative servers.

   Note: You do not have to configure Gateway Endpoint, User Endpoints, or Routing Entries before you configure the Collaborative Servers.

   1. See Procedure 93 "Adding a Collaborative Server" (page 337)
   2. See Procedure 94 "Viewing the Collaborative Servers" (page 341)

c. Add the endpoints and add the endpoint prefixes.

   1. See "Adding a Gateway Endpoint" (page 320)
   2. See Procedure 1 "Adding a User Endpoint" (page 105)

d. Add the numbering plan entries for each endpoint, including the Cost Factor for each entry.

   1. See Procedure 89 "Adding a Routing Entry" (page 327)
   2. See Procedure 91 "Adding a Default Route" (page 333)

e. **Verify the numbering plan configuration**. See "Verifying the numbering plan and saving the NRS configuration" (page 342)

f. **Perform database actions**. See "Performing NRS database actions" (page 349) To save the NRS configuration, refer to the procedures in this section.

6 **Test the numbering plans** (see "H.323 and SIP Routing Tests" (page 342)).

- See Procedure 96 "Performing an H.323 Routing Test" (page 343)
- See Procedure 97 "Performing a SIP Routing Test" (page 344)

7 **Perform server actions** (see "Enabling and disabling the NRS Server" (page 347)).

- See Procedure 98 "Disabling the NRS server" (page 347)
- See Procedure 99 "Enabling the NRS server" (page 348)

8 **Perform database actions** (see "Performing NRS database actions" (page 349)).

- See Procedure 100 "Cutting over the database" (page 351)
- See Procedure 101 "Reverting the database changes" (page 352)
- See Procedure 102 "Rolling back changes to the database" (page 353)
- See Procedure 103 "Committing the database" (page 354)
- See Procedure 104 "Cutting over and committing changes to the database" (page 356)

9 **Back up the NRS database**. See "Backing up the database" (page 357)

- See Procedure 105 "Automatically backing up the database" (page 357)
- See Procedure 106 "Manually backing up the database" (page 358)

The NRS database can also be restored, if required. See "Restoring the database" (page 361)

- See Procedure 110 "Restoring from the connected Signaling Server" (page 362)
- See Procedure 111 "Restoring from an FTP site" (page 363)
- See Procedure 112 "Restoring from a client machine" (page 364)

10 If necessary, **convert** the Succession 3.0 Gatekeeper **database** to a CS 1000 Release 4.0 (or later) NRS database. See "GK/NRS Data Upgrade" (page 366) and refer to the Upgrades NTPs for detailed information.

11 **View the SIP Phone Context**. See "SIP Phone Context" (page 368).

12 **View reports** on the status of the database. See "Viewing the database reports" (page 370).

13 **Administer users** of the NRS (see "Configuring and administering users" (page 373)).

- See "Creating new users" (page 373)
- See "Viewing configured users" (page 375)
- See "Editing or deleting configured users" (page 376)

14 **Log out of NRS Manager**. See Procedure 76 "Logging out of NRS Manager" (page 298)

—End—

Accessing NRS Manager

Access NRS Manager in one of the following two ways:

- Click the **Network Routing Service** link in the navigator within Element Manager. See Procedure 74 "Logging in to NRS Manager from Element Manager" (page 290).
- Enter the IP address of NRS Manager in the browser’s address field. See Procedure 75 "Logging in to NRS Manager using the browser address field" (page 291).

  Note: To access the NRS directly from the Signaling Server, see "Accessing the NRS directly from the Signaling Server" (page 378).

To log in to the NRS from Element Manager, follow the steps in Procedure 74 "Logging in to NRS Manager from Element Manager" (page 290).

Procedure 74
Logging in to NRS Manager from Element Manager

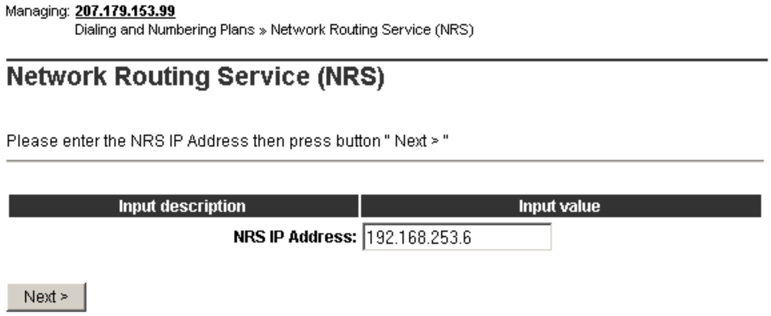
Step **Action**

1 Log in to Element Manager.

2 Select **Dialing and Numbering Plans > Network Routing Service** from the navigator.

The **Network Routing Service (NRS)** web page opens (see Figure 161 "Network Routing Service (NRS) configuration web page" (page 291)).

Figure 161
Network Routing Service (NRS) configuration web page



Managing: 207.179.153.99
Dialing and Numbering Plans » Network Routing Service (NRS)

Network Routing Service (NRS)

Please enter the NRS IP Address then press button " Next > "

Input description	Input value
NRS IP Address:	192.168.253.6

3 Enter the IP address of the NRS in the **NRS IP Address** text box.

> ***Note:*** The IP address that automatically appears may not be the IP address of the NRS. The displayed address is the address defined in Element Manager for the H.323 Gatekeeper or SIP Redirect Server.

4 Click **Next>**.

The **Network Routing Service** login window opens (see Figure 162 "NRS Manager login web page" (page 292))

5 Go to step 4 of Procedure 75 "Logging in to NRS Manager using the browser address field" (page 291).

—End—

Procedure 75
Logging in to NRS Manager using the browser address field

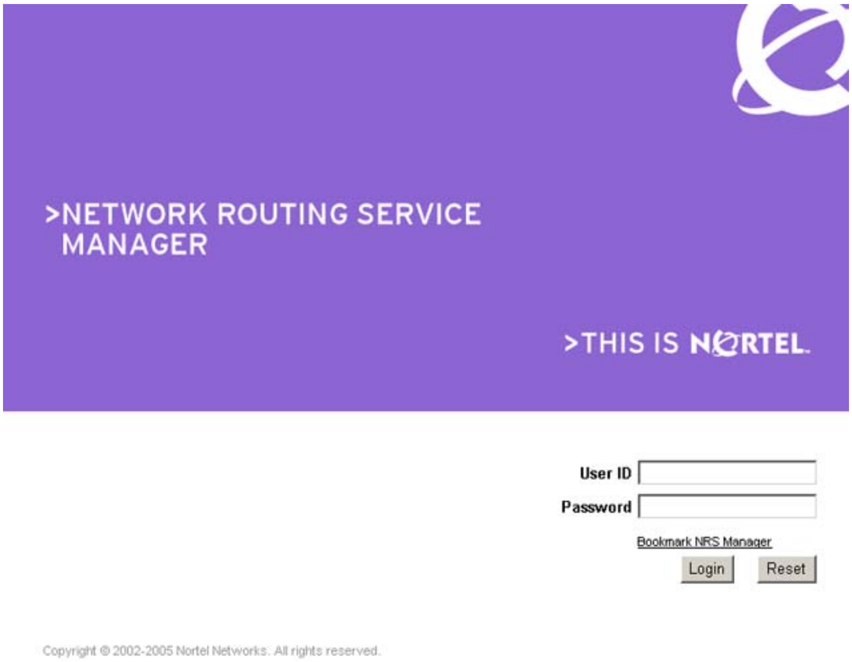
Step Action

1 Open the Microsoft Internet Explorer 6.0 (or later) browser.

2 Type the URL for NRS Manager into the address field of the browser. The URL has the following format:
http://[Signaling_Server_ELAN_network_interface_IP_address]/nrs/

3 The NRS Manager Login web page displays (see Figure 162 "NRS Manager login web page" (page 292)).

Figure 162
NRS Manager login web page


>NETWORK ROUTING SERVICE MANAGER
>THIS IS NORTEL
User ID
Password
Bookmark NRS Manager
Login
Reset
Copyright © 2002-2005 Nortel Networks. All rights reserved.

> ***Note:*** The H.323 Gatekeeper or SIP Redirect Server must be enabled before you can log into NRS Manager. If the H.323 Gatekeeper or the SIP Redirect Server are not enabled, the web page turns white, and the following error message is displayed:

```
Error code is WC0030:
Error:  Network Routing Service (NRS) Manager is not
accessible when neither Gatekeeper nor SIP Proxy/Redire
ct applications are enabled.
Please close the IE window.  Enable the application(s).
Reboot the Signaling Server, then access NRS Manager
again.
```

> ***Note 1:*** To enable the H.323 Gatekeeper or SIP Redirect Server, refer to Procedure 72 "Enabling and configuring the NRS server in stand-alone mode" (page 282) or Procedure 73 "Enabling and configuring the NRS server in co-resident mode" (page 283).
>
> ***Note 2:*** To add a bookmark to your Internet Explorer Favorites list, click the **Bookmark NRS Manager** link on the login page before logging in.

4 Enter the **`User ID`** and **`Password`** to log in.

A username and password must be provided to prevent unauthorized access.

ATTENTION

Nortel recommends that you log in to NRS Manager using the default User ID and Password when configuring the NRS server. When the NRS server configuration is complete, change the User ID and Password for increased system security.

The default values are:

- User ID — `admin`
- password — `admin`

  Note: NRS Manager is not available directly from the Signaling Server. To log in to the NRS from the Signaling Server, see "Accessing the NRS directly from the Signaling Server" (page 378).

Security is implemented through authentication and database access privileges. A username and password is required to access the NRS database. The username and password are stored (in encrypted format) in the same database as the SIP Redirect Server or Proxy Server data. The authentication parameters are configurable in the Element Manager but the NRS does the authentication.

Two types of access privileges are supported:

- Administrative privileges — Administrators have full read/write privileges. An administrator can view and modify NRS configuration data.
- Monitor privileges — Monitors have read-only privileges. A Monitor can only view the NRS configuration data.

  Note 1: Once logged in, an administrator can create new users using Procedure 117 "Creating new users" (page 374).

  Note 2: An administrator must create each monitor user individually. There is no default User ID and password for a monitor.

  Note 3: After 60 minutes of inactivity the session times out and the user is logged out of NRS Manager. The default session timeout is 60 minutes. The session timeout parameter is configurable using the CLI.

5 Click **Login**.

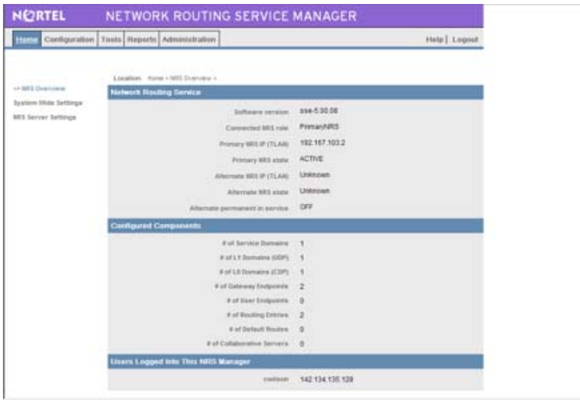
If login is successful, the User ID and Password are securely transferred from the web client to the NRS web server. The web server verifies the User ID and Password. If the User ID and Password are valid the **NRS Overview** web page opens. (See Figure 163 "NRS Overview web page" (page 294))

NRS Manager allows you to navigate to specific components of the NRS, and allows you to configure and maintain those components.

If the login is not successful, you may have entered an incorrect User ID or Password.

> ***Note:*** The **Reset** button clears the User ID and Password text boxes.

Figure 163
NRS Overview web page



Network Routing Service

Software version	sse-5.00.08
Connected NRS role	PrimaryNRS
Primary NRS IP (TLAN)	192.167.103.2
Primary NRS state	ACTIVE
Alternate NRS IP (TLAN)	Unknown
Alternate NRS state	Unknown
Alternate permanent in service	OFF

Configured Components

# of Service Domains	1
# of L1 Domains (UDP)	1
# of L0 Domains (CDP)	1
# of Gateway Endpoints	2
# of User Endpoints	0
# of Routing Entries	2
# of Default Routes	0
# of Collaborative Servers	0

Users Logged Into This NRS Manager

cwilson	142.134.135.128

An overview of the NRS is displayed in the main area of the **NRS Overview** web page:

- **Network Routing Service**:

  The upper part of the web page provides the following information about the NRS:

  — The software version

  — The role of the connected NRS

  — The IP address of the Primary NRS

  — The state of the Primary NRS

  — The IP address of the Alternate NRS

  — The state of the Alternate NRS

  — Whether the Alternate NRS is permanently in service

- **Configured Components**

The middle part of the web page provides the number of configured components of the NRS:

- Number of Service domains
- Number of Level 1 Domains (this maps to UDP)
- Number of Level 0 Domains (this maps to CDP)
- Number of Gateway Endpoints
- Number of User Endpoints
- Number of Routing Entries
- Number of Default Endpoints
- Number of Collaborative Servers

- **Users Logged into this NRS Manager**

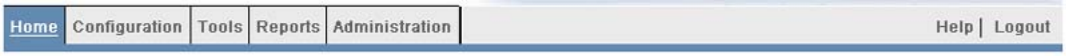
  The lower part of the web page provides a list of logged-in users and their IP Addresses.

—End—

The NRS Manager interface

The **NRS Manager toolbar** is located in the NRS Manager web page header. The toolbar has a set of five tabs for configuring and maintaining the NRS. **Help** and **Logout** links are also provided in the header of the NRS Manager web page. See Figure 164 "NRS Manager toolbar" (page 295).

Figure 164
NRS Manager toolbar



The **navigator** located on the left side of the NRS manager web pages contains links to other web pages. In theFigure 163 "NRS Overview web page" (page 294) the navigator contains links to the **NRS Overview**, the **System Wide Settings** and the **NRS Server Settings** web pages.

NRS Manager toolbar

The NRS Manager toolbar has five tabs, as shown in Figure 164 "NRS Manager toolbar" (page 295).

Home tab

Selecting the **Home** tab opens the **NRS Overview** web page. The **NRS Overview** web page provides summary information about the NRS, the number of configured components and a list of users logged in to the NRS Manager. The navigator on the **Home** web pages contains links to the

- NRS Overview
- System Wide Settings
- NRS Server Settings

web pages.

See "Home tab" (page 298).

Configuration tab

Selecting the **Configuration** tab opens the **Service Domains** configuration web page. The **Configuration** web pages are used to modify the NRS database. The navigator on the **Configuration** web pages contains links to the

- Service Domains
- L1 Domains (UDP)
- L0 Domains (CDP)
- Gateway Endpoints
- User Endpoints
- Routing Entries
- Default Routes
- Collaborative Servers

web pages.

See "Configuration tab" (page 307).

Tools tab

Selecting the **Tools** tab opens the **H.323 Routing Test tool** web page. The **Tools** web pages provides a group of tools for performing the following:

- H.323 and SIP routing tests against the active and standby databases
- server actions such as enabling and disabling the database
- database-related actions such as cut over, commit, revert, rollback, and single-step cut over and commit
- database backups and restores

- database conversion/upgrade (such as converting the Succession 3.0 H.323 Gatekeeper database to the CS 1000 Release 4.0 (or later) NRS database)
- SIP Phone context

The navigator on the **Tools** web pages contains links to the

- H.323 routing Test
- SIP Routing Test
- Server Actions
- Database Actions
- Database Backup
- Database Restore
- GK/NRS Data Upgrade
- SIP Phone Context
- SSL/TLS Configuration

web pages.

See "Tools tab" (page 342).

Reports tab

Selecting the **Reports** tab opens the **Database Report** web page. The **Reports** web page provides three types of database reports:

- Last database synchronized for the Alternate NRS (if configured)
- Last database synchronized for the Failsafe NRS (if configured)
- Current database status.

See "Reports tab" (page 370).

Administration tab

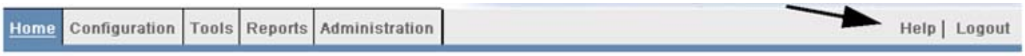
Selecting the **Administration** tab opens the **Users** web page. Open the **Users** web page to administer, configure, and view users. Users can be added and user privileges can be modified.

See "Administration tab" (page 373).

Help and Logout links

The **Help** and **Logout** links are located on the right side of the NRS Manager web page header (see Figure 165 "Help and Logout links" (page 298)).

Figure 165
Help and Logout links



Help link

Select the **Help** link to access the **NRS Manager Help Files** .

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

Logout link

Select the **Logout** link to terminate the current session. See "Logging out of NRS Manager" (page 298).

Logging out of NRS Manager

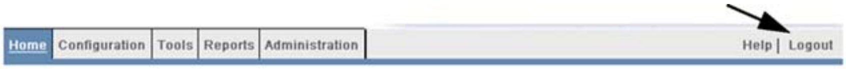
Follow the steps in Procedure 76 "Logging out of NRS Manager" (page 298) to log out of NRS Manager. Logging out of NRS Manager terminates the current session.

Procedure 76
Logging out of NRS Manager

Step Action

1 Click **Logout** (see Figure 166 "Logout link" (page 298)).

Figure 166
Logout link



The **Network Routing Service Manager** logout web page opens.

2 Close the browser window.

—End—

Home tab

Verifying that the NRS is the Primary NRS and is active

To verify that the NRS is the Primary NRS and that it is active, follow Procedure 77 "Verifying that the NRS is the Primary NRS and is active" (page 299).

Procedure 77
Verifying that the NRS is the Primary NRS and is active

Step	Action

1 Select the **Home** tab from the NRS Manager toolbar.

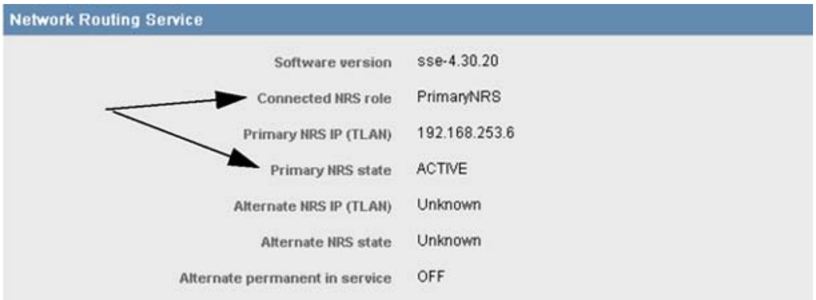
The **NRS Overview** web page opens, as shown in Figure 163 "NRS Overview web page" (page 294).

2 In the **Network Routing Service** section (the top section of the **NRS Overview** web page), shown in Figure 167 "Network Routing Service section" (page 299):

a. Ensure that **Connected NRS Role** = PrimaryNRS.

b. Ensure that **Primary NRS State** = Active.

Figure 167
Network Routing Service section



Network Routing Service

Software version	sse-4.30.20
Connected NRS role	PrimaryNRS
Primary NRS IP (TLAN)	192.168.253.6
Primary NRS state	ACTIVE
Alternate NRS IP (TLAN)	Unknown
Alternate NRS state	Unknown
Alternate permanent in service	OFF

—End—

Configuring system-wide settings

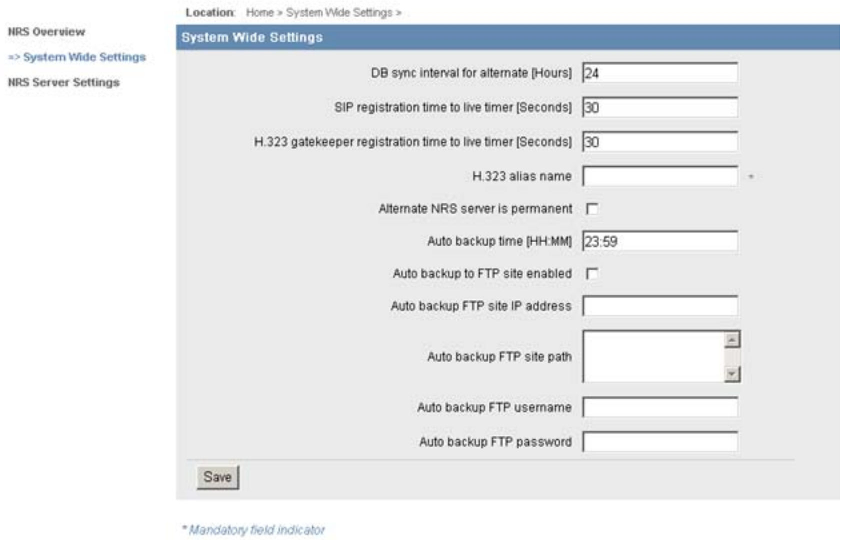
The **System-wide settings** web page is used (1) to configure system-wide settings and (2) to schedule backup jobs. System-wide settings include:

- Database synchronization interval for the Alternate and Failsafe NRS databases.
- SIP registration and H.323 Gatekeeper registration Time-to-Live timer settings.
- H.323 Gatekeeper alias name.
- Whether the Alternate NRS server is permanently in service.
- Automatic backup time setting.
- Whether automatic backup to an FTP site is enabled. If enabled, the IP address, path, and username for the FTP site must be provided.

Follow Procedure 78 "Configuring system-wide settings" (page 300) to configure system-wide settings.

Procedure 78
Configuring system-wide settings

Step	Action
1	Select the **Home** tab on the NRS Manager toolbar.
2	Click **System Wide Settings** in the navigator. The **Setting Wide Settings** web page opens (see Figure 168 "System Wide Settings" (page 300)).



Location: Home > System Wide Settings >

System Wide Settings

DB sync interval for alternate [Hours]	24
SIP registration time to live timer [Seconds]	30
H.323 gatekeeper registration time to live timer [Seconds]	30
H.323 alias name	*
Alternate NRS server is permanent	□
Auto backup time [HH:MM]	23:59
Auto backup to FTP site enabled	□
Auto backup FTP site IP address	
Auto backup FTP site path	
Auto backup FTP username	
Auto backup FTP password	

* Mandatory field indicator

Figure 168
System Wide Settings

3 Enter a value in the **DB sync interval for alternate [Hours]** text box. This is the time interval between database synchronization of the Primary NRS and the Alternate NRS. The range is 1 to 24 hours.

4 Enter values for the Time-to-Live timers.

a. Enter a value in the **SIP registration time to live timer [Seconds]** text box. Nortel recommends that the timer be set to 30 seconds. The range is 30 to 3600 seconds.

b. Enter a value in the **H.323 gatekeeper registration time to live timer [Seconds]** text box. Nortel recommends that the timer be set to 30 seconds. The range is 30 to 3600 seconds.

5 Enter the alias name of the H.323 Gatekeeper in the **H.323 alias name** text box. This is a mandatory field. The alias name must be alphanumeric, can be up to 30 characters in length, and cannot have spaces.

To send out Location Requests (LRQ), the H.323 Gatekeeper must have an H.323 Gatekeeper alias name. An H.323 Gatekeeper alias name is also referred to as an H323-ID. The default value of this parameter is the “HostName” value configured in the Signaling Server’s config.ini file.

6 Select the **Alternate NRS server is permanent** check box if you want the Alternate NRS Server to be permanently in service.

Select the check box if the Alternate NRS Server is to remain in service after a switchover, even if the Primary NRS recovers. Clear the check box if the Alternate NRS will switchover functions to the Primary NRS Server after the Primary NRS Server recovers.

7 Enter the time when the database backup will automatically occur in the **Auto backup time [HH:MM]** text box.

8 If you want to automatically back up the NRS database to an FTP site, then complete the following steps:

a. Select the **Auto backup to FTP site enabled** check box.

b. Enter the IP address of the FTP site in the **Auto backup FTP site IP address** text box.

c. Enter the path to the FTP site in the **Auto backup FTP site path** text box. The FTP site path must be alphanumeric and can be up to 120 characters in length.

d. Enter the username used to access the FTP site in the **Auto backup FTP username** text box. The FTP username must be alphanumeric and can be up to 30 characters in length.

e. Enter the password used to access the FTP site in **Auto backup FTP password** text box. The FTP password must be alphanumeric and can be up to 30 characters in length but cannot include the single quote (’) symbol. The FTP username must be alphanumeric and can be up to 30 characters in length.

9 Click Save.

—End—

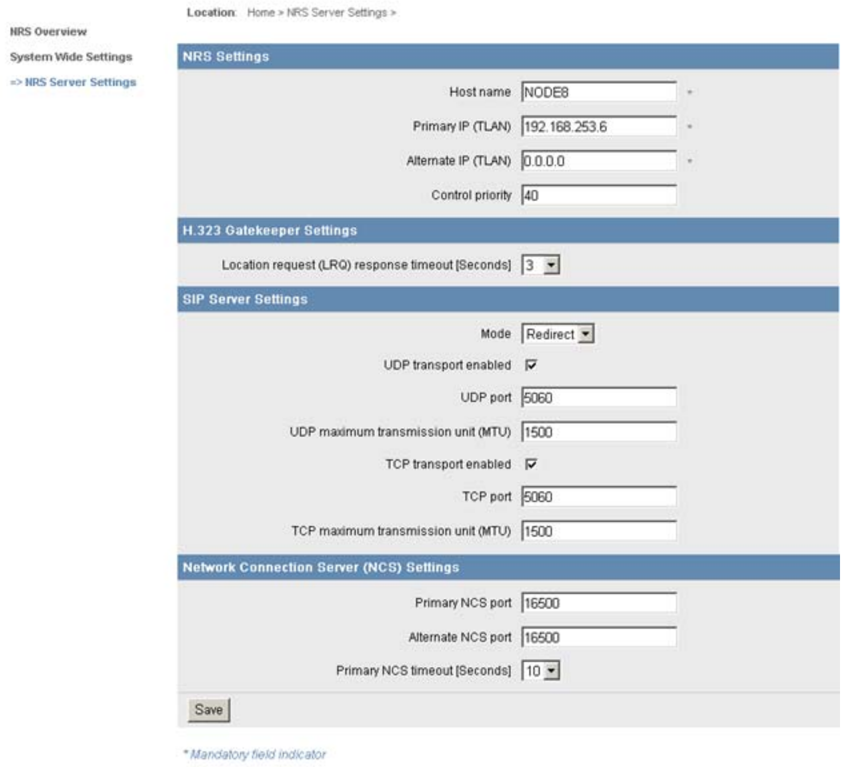
Configuring the Primary and Alternate NRS Server Settings

Procedure 79
Configuring NRS Server Settings

Step	Action
1	Select the **Home** tab on the NRS Manager toolbar.
2	Click **NRS Server Settings** in the navigator.

The **NRS Server Settings** web page opens (see Figure 169 "NRS Server Settings" (page 302)).

Figure 169
NRS Server Settings



Location: Home > NRS Server Settings >

NRS Overview
System Wide Settings
=> NRS Server Settings

NRS Settings

Host name	NODE8	*
Primary IP (TLAN)	192.168.253.6	*
Alternate IP (TLAN)	0.0.0.0	*
Control priority	40	

H.323 Gatekeeper Settings

Location request (LRQ) response timeout [Seconds]	3

SIP Server Settings

Mode	Redirect
UDP transport enabled	☑
UDP port	5060
UDP maximum transmission unit (MTU)	1500
TCP transport enabled	☑
TCP port	5060
TCP maximum transmission unit (MTU)	1500

Network Connection Server (NCS) Settings

Primary NCS port	16500
Alternate NCS port	16500
Primary NCS timeout [Seconds]	10

* Mandatory field indicator

The NRS Server Settings comprise:

- NRS Settings — These are generic settings applicable to H.323, SIP, and Network connection Service.
- H.323 Gatekeeper Settings
- SIP Server Settings
- Network Connection Server (NCS) Settings

- SNMP Settings — These settings are available only when the connected NRS is in stand-alone mode. If the connected NRS is in coresident mode, the SNMP Settings section is not displayed in NRS Manager. In co-resident mode, the SNMP parameters are configured using Element Manager. For more information, refer to *Simple Network Management Protocol: Description and Maintenance (553-3001-519)*.

3 To configure the **NRS Settings** (see Figure 170 "NRS Settings section" (page 303))

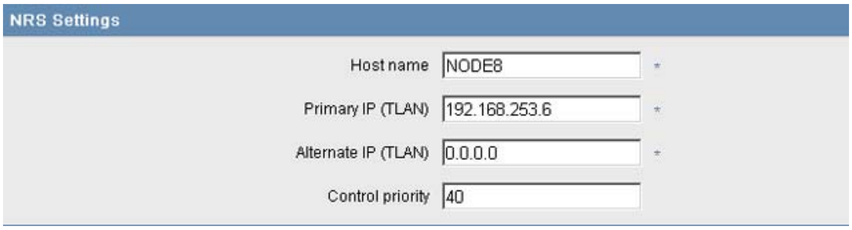
a. **Host name:** Enter the name of the connected host Signaling Server in the text box. The host name must be alphanumeric and can be up to 20 characters in length.

b. **Primary IP (TLAN):** Enter the IP address of the Primary NRS (that is, the TLAN network interface IP address) in the text box. The default is 0.0.0.0.

c. **Alternate IP (TLAN):** If the Alternate NRS is configured, enter the IP address of the Alternate NRS (that is, the TLAN network interface IP address), in the text box. The default is 0.0.0.0.

d. **Control priority:** Enter a value for the control priority in the text box. This is a priority bit setting inside the protocol that determines the signaling routing priority. The range is 0 to 63. The default value is 40. The control priority must be a numeric value.

Figure 170
NRS Settings section



NRS Settings

Host name: NODE8 *

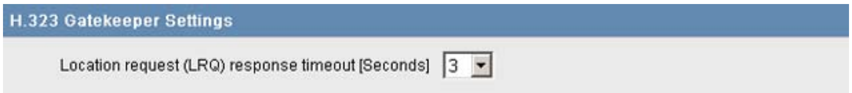
Primary IP (TLAN): 192.168.253.6 *

Alternate IP (TLAN): 0.0.0.0 *

Control priority: 40

4 To configure **H.323 Gatekeeper Settings** (see Figure 171 "H.323 Gatekeeper Settings section" (page 304)) set the LRQ response timeout parameter by selecting a value from the **Location request (LRQ) response timeout [Seconds]** drop-down list. The default value is 3 seconds. The minimum value is 1 second and the maximum value is 10 seconds.

Figure 171
H.323 Gatekeeper Settings section



H.323 Gatekeeper Settings

Location request (LRQ) response timeout [Seconds] 3

5 To configure **SIP Server Settings** (see Figure 172 "SIP Server Settings section" (page 305)) configure the following:

a. Select **Redirect** from the **Mode** drop-down list. This is the mode of the SIP Server. A redirect server receives requests, but rather than passing the request onto another server, it sends a response to the caller indicating the address of the called user. This provides the address for the caller to contact the called party directly.

b. Select the transport protocol.

Two options are available when selecting the transport protocol:

- UDP only
- Both UDP and TCP.

TCP cannot be enabled without enabling UDP.

To enable UDP:

1. Select the **UDP transport enabled** check box.
2. Enter the **UDP port** in the text box. The default port number is 5060. The UDP port must be numeric and can be up to five digits in length.
3. Enter the **UDP maximum transmission unit (MTU)** in the text box. MTU is the maximum size of an Ethernet Layer 2 packet going out on the IP network. In this context, MTU is the maximum size of a SIP packet that is sent out on the UDP interface. The default value is 1500 bytes. The maximum value for MTU is 64K. When configuring the MTU, remember that there is a trade-off between packet size and the number of packets that have to be transmitted over the network.

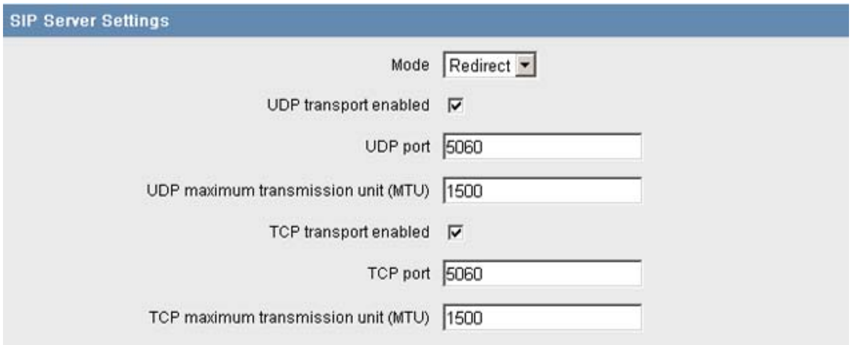
   Note: To enable TCP, UDP must also be enabled.

To enable TCP:

1. Select the **TCP transmission enabled** check box.
2. Enter the **TCP port** number in the text box. The default port number is 5060. The TCP must be numeric and can be up to five digits in length.

3. Enter the **TCP maximum transmission unit (MTU)** in the text box. MTU is the maximum size of an Ethernet Layer 2 packet going out on the IP network. In this context, MTU is the maximum size of a SIP packet that is sent out on the TCP interface. The default value is 1500 bytes. The maximum value for MTU is 64K. When configuring the MTU, remember that there is a trade-off between packet size and the number of packets that have to be transmitted over the network.

Figure 172
SIP Server Settings section



SIP Server Settings

Mode: Redirect ▾

UDP transport enabled: ☑

UDP port: 5060

UDP maximum transmission unit (MTU): 1500

TCP transport enabled: ☑

TCP port: 5060

TCP maximum transmission unit (MTU): 1500

6 To configure **Network Connection Server (NCS) Settings** (see Figure 173 "Network Connection Server (NCS) Settings section of NRS Server Settings web page" (page 306))

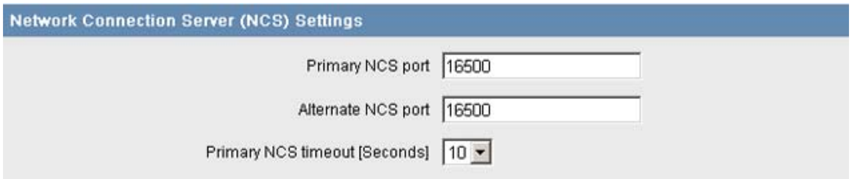
a. **Primary NCS port:** Enter a port number for the Primary NCS in the text box. The port number must be numeric and up to five digits in length. The range is 1024 to 65535. The default value is 16500.

b. **Alternate NCS port:** Enter a port number for the Alternate NCS in the text box. The port number must be numeric and up to five digits in length. The range is 1024 to 65535. The default value is 16500.

c. **Primary NCS timeout [Seconds]**: Select a timeout value for the Primary NCS from the drop-down list. The default value is 10 seconds. The minimum value is 1 second and the maximum value is 30 seconds.

Note: The NCS Settings are used for the Branch Office (including the Survivable Remote Gateway [SRG}), Virtual Office, and Geographic Redundancy features.

Figure 173
Network Connection Server (NCS) Settings section of NRS Server Settings web page



Network Connection Server (NCS) Settings

Primary NCS port: 16500

Alternate NCS port: 16500

Primary NCS timeout [Seconds]: 10 ▾

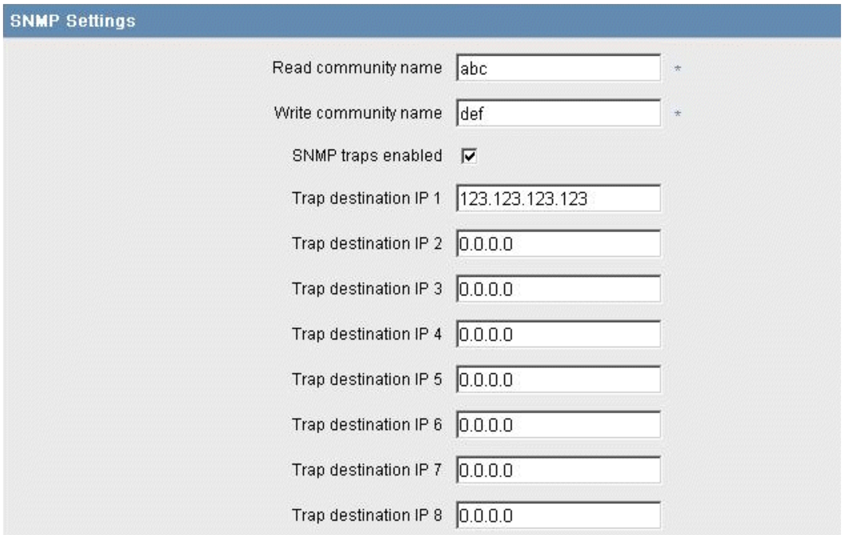
7 If the NRS is in stand-alone mode, that is not connected to a Call Server (see "Stand-alone mode" (page 282)) go to step 8 and configure the SNMP Settings.

If the NRS is in co-resident mode (see "Enabling and configuring the NRS server" (page 281)) the SNMP Settings are not displayed in NRS Manager. Go to step 9.

8 To configure the **SNMP Settings** (see Figure 174 "SNMP Settings" (page 306))

> ***Note:*** The SNMP settings are available only if the NRS is in stand-alone mode, that is not connected to a Call Server.

Figure 174
SNMP Settings



SNMP Settings

Read community name: abc *

Write community name: def *

SNMP traps enabled: ☑

Trap destination IP 1: 123.123.123.123

Trap destination IP 2: 0.0.0.0

Trap destination IP 3: 0.0.0.0

Trap destination IP 4: 0.0.0.0

Trap destination IP 5: 0.0.0.0

Trap destination IP 6: 0.0.0.0

Trap destination IP 7: 0.0.0.0

Trap destination IP 8: 0.0.0.0

a. **Read community name:** Enter the read community name in the text box. The name must be alphanumeric and can be up to 32 characters in length.

b. **Write community name:** Enter the read/write community name in the text box. The name must be alphanumeric and can be up to 32 characters in length.

Note: The read community name and the write community name control access to the Management Information Base (MIB). For detailed information, refer to **Simple Network Management Protocol: Description and Maintenance (553-3001-519)**.

c. **SNMP traps enabled:** Select the check box to enable SNMP traps if configuring one or more SNMP management IP addresses to receive SNMP traps from cards in the IP Telephony node.

d. **Trap destination IP 1** to **Trap destination IP 8**: If SNMP traps are enabled, the SNMP traps are sent to the IP address entered in the text boxes. Up to eight SNMP trap servers can be defined. The default IP address is 0.0.0.0

9 Click **Save**.

—End—

Configuration tab

The **Configuration** web pages, opened by selecting the configuration tab on the NRS Manager toolbar, are used to configure the NRS database. The database is used by both the SIP Redirect Server and the H.323 Gatekeeper.

Configuring the NRS database

Follow the procedures in this section to configure the NRS database.

Task summary list

Follow the procedures in this section to configure the NRS database.

- Procedure 80 "Switching between the active and standby databases" (page 308)
- Procedure 81 "Adding a Service Domain" (page 310)
- Procedure 83 "Adding an L1 Domain (UDP)" (page 312)
- Procedure 85 "Adding an L0 Domain (CDP)" (page 316)
- Procedure 87 "Adding a Gateway Endpoint" (page 320)
- Procedure 89 "Adding a Routing Entry" (page 327)
- Procedure 93 "Adding a Collaborative Server" (page 337)
- Procedure 104 "Cutting over and committing changes to the database" (page 356)

Note 1: To add a SIP Phone refer to Procedure 1 "Adding a User Endpoint" (page 105).

Note 2: The standby database is used to modify the configuration data. Changes made to the standby database do not immediately affect call processing. Before changes made to the standby database affect call processing, the active and standby databases must be swapped by executing a database **Cut over** command.

See Procedure 104 "Cutting over and committing changes to the database" (page 356).

See “Switching between the active and standby databases” on page 333, “Performing NRS database actions” on page 381, and Procedure 114 on page 388.

Changes can be saved individually or in batches, depending on the administrator’s preference.

Switching between the active and standby databases

The database has two schemas, active and standby.

- The active database is used for runtime queries.
- The standby database is used for administrator modifications.

  Note: By default, the database is in active database view when the **Configuration** web pages are first opened. To modify the database it must be in standby database view. Only users with administrative authority can modify the database.

To the right of the NRS Manager toolbar is an area for switching between the active and standby databases (see Figure 176 "Active DB view selected" (page 309)).

Follow Procedure 80 "Switching between the active and standby databases" (page 308) to switch between the active and standby database.

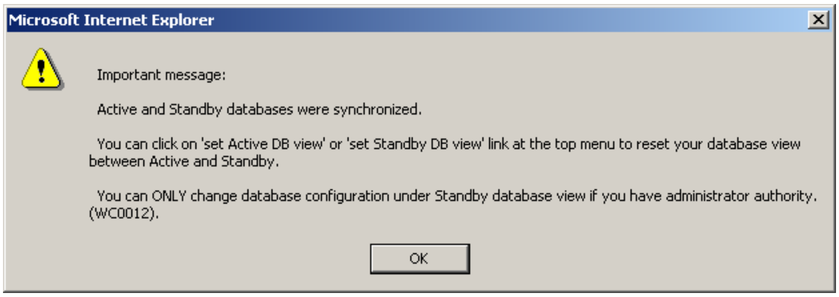
Procedure 80
Switching between the active and standby databases

Step	Action
1	Click the **Configuration** tab on the NRS Manager toolbar.

If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

Note: The dialog box only opens the first time that the Configuration web pages are opened.

Figure 175
Configuration tab message



Important message:

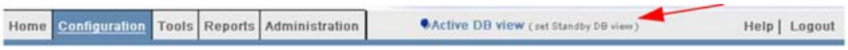
Active and Standby databases were synchronized.

You can click on 'set Active DB view' or 'set Standby DB view' link at the top menu to reset your database view between Active and Standby.

You can ONLY change database configuration under Standby database view if you have administrator authority. (WC0012).

2 Click **set Standby DB view** to switch to the standby database (see Figure 176 "Active DB view selected" (page 309)). The standby database is used for database modifications.

Figure 176
Active DB view selected

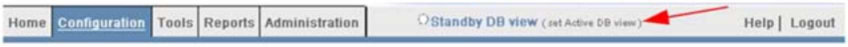


When the database is in standby database view, **Standby DB view** is bold (see Figure 177 "Switching between active and standby database view" (page 309)).

or

3 Click **set Active DB view** to switch to the active database (see Figure 177 "Switching between active and standby database view" (page 309)). The active database is used for database queries.

Figure 177
Switching between active and standby database view



When the database is in active database view, **Active DB view** is bold (see Figure 176 "Active DB view selected" (page 309)).

—End—

Note: Procedure 81 "Adding a Service Domain" (page 310) to Procedure 89 "Adding a Routing Entry" (page 327) use the example hierarchy (myServiceProvider.com, myCompany.com, and so on) provided in the "Contents" (page 19).

Adding a Service Domain

The Service Domain is a building block of the routable SIP URI. It represents the service domain name field in the URI (see "SIP Uniform Resource Identifiers" (page 38)).

Procedure 81

Adding a Service Domain

Step	Action
1	Select the **Configuration** tab on the NRS Manger toolbar.

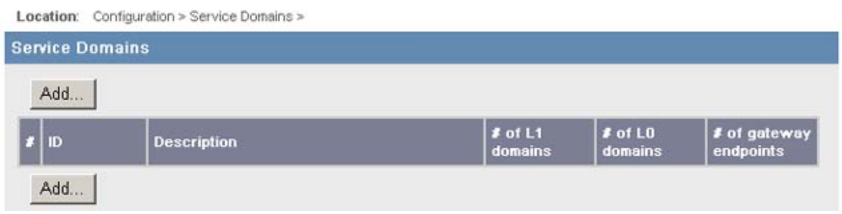
If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

> ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Standby DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

The **Service Domains** web page opens, as shown in Service Domains web page.

Figure 178
Service Domains web page



Location: Configuration > Service Domains >

Service Domains

Add...

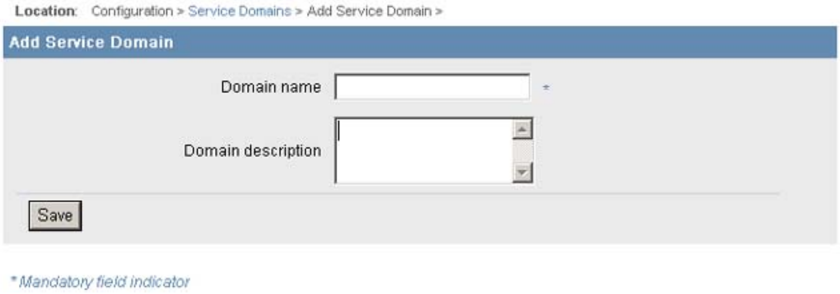
#	ID	Description	# of L1 domains	# of L0 domains	# of gateway endpoints

Add...

3 Click **Add...**.

The **Add Service Domain** web page opens, as shown in Figure 179 "Add Service Domain web page" (page 311).

Figure 179
Add Service Domain web page


Location: Configuration > Service Domains > Add Service Domain >
Add Service Domain
Domain name *
Domain description
Save
* Mandatory field indicator

4 Enter a **Domain name** for the Service Domain in the text box.

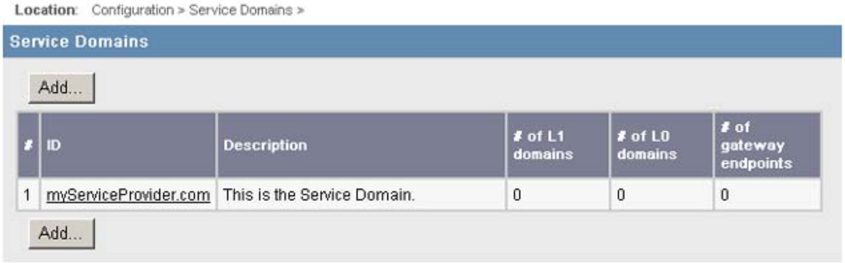
For example, enter myServiceProvider.com.

5 Enter a **Domain description** for the Service Domain in the text box.

6 Click **Save**.

The **Service Domains** web page opens, showing the newly added myServiceProvider.com Service Domain. See Figure 180 "Added Service Domain" (page 311).

Figure 180
Added Service Domain



#	ID	Description	# of L1 domains	# of L0 domains	# of gateway endpoints
1	myServiceProvider.com	This is the Service Domain.	0	0	0

—End—

Procedure 82
Viewing the Service Domains

Step **Action**

1 Select the **Configuration** tab on the NRS Manager toolbar.

If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

> ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Active DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

The **Service Domains** web page opens and displays a list of configured Service Domains.

3 Click a **link** in the **ID** column of the **Service Domains** web page.

The **View Service Domain Property** web page opens and displays a domain description for the selected Service Domain.

—End—

Adding a Level 1 Domain (UDP)

The Level 1 (L1) Domain is a building block of the phone context for private addresses. It is the phone context root. For more information on phone context, refer to "SIP Uniform Resource Identifiers" (page 38).

Procedure 83

Adding an L1 Domain (UDP)

Step Action

1 Select the **Configuration** tab on the NRS Manager toolbar.

If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

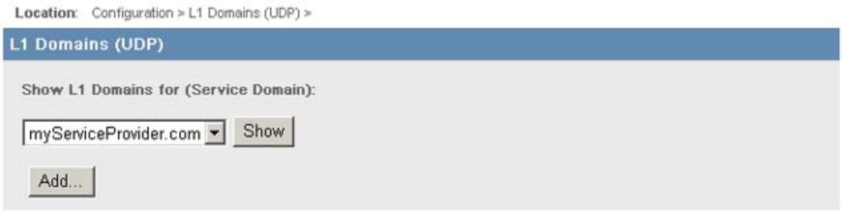
> ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Standby DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

3 Click **L1 Domains (UDP)** from the navigator.

The **L1 Domains (UDP)** web page opens, as shown in Figure 181 "L1 Domains (UDP) web page" (page 313). The drop-down list contains configured Service Domains.

Figure 181
L1 Domains (UDP) web page

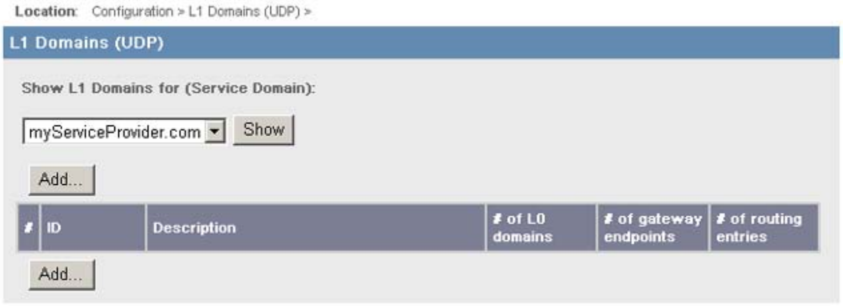

Location: Configuration > L1 Domains (UDP) >
L1 Domains (UDP)
Show L1 Domains for (Service Domain):
Show
Add...

Show L1 Domains for (Service Domain): myServiceProvider.com

4 Select the **Service Domain**, where the new L1 subdomain will be added, from the drop-down list.

5 (Optional) Click **Show** to display a list of configured L1 Domains for the selected Service Domain. See Figure 182 "L1 Domains (UDP) web page for selected Service Domain" (page 313).

Figure 182
L1 Domains (UDP) web page for selected Service Domain


Location: Configuration > L1 Domains (UDP) >
L1 Domains (UDP)
Show L1 Domains for (Service Domain):
Show
Add...
Add...

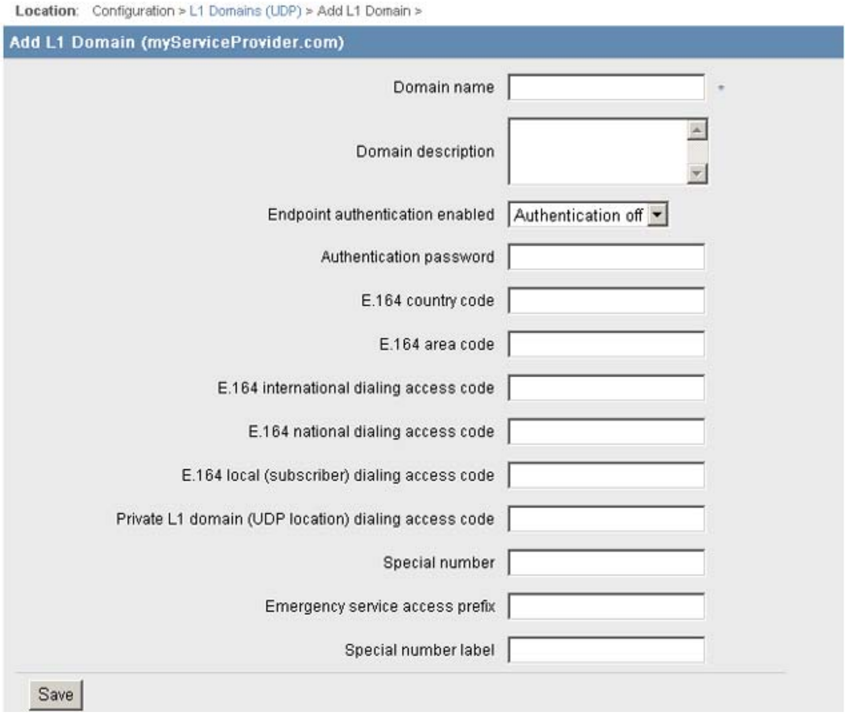
Show L1 Domains for (Service Domain): myServiceProvider.com

#	ID	Description	# of L0 domains	# of gateway endpoints	# of routing entries

6 Click **Add...**.

The **Add L1 Domain** web page opens, as shown in Figure 183 "Add L1 Domain web page" (page 314).

Figure 183
Add L1 Domain web page



Location: Configuration > L1 Domains (UDP) > Add L1 Domain >

Add L1 Domain (myServiceProvider.com)

Domain name	*
Domain description	
Endpoint authentication enabled	Authentication off
Authentication password	
E.164 country code	
E.164 area code	
E.164 international dialing access code	
E.164 national dialing access code	
E.164 local (subscriber) dialing access code	
Private L1 domain (UDP location) dialing access code	
Special number	
Emergency service access prefix	
Special number label	

7 Enter the **Domain name** of the L1 Domain in the text box. The name must be alphanumeric and can be up to 30 characters in length.

For example, enter myCompany.com.

8 Enter the **Domain description** in the text box. The description can include any character except single quotes and can be up to 120 characters in length.

9 Select **Authentication on** or **Authentication off** from the **Endpoint authentication enabled** drop-down list.

If **Authentication on** is selected, then all endpoints require authentication.

10 Enter the **Authentication password** in the text box, if **Authentication on** was selected in step 8. The password must be alphanumeric and up to 30 characters in length.

11 Enter the **E.164 country code** in the text box. The code must be numeric and can be up to seven characters in length.

12 Enter the **E.164 area code** in the text box. The code must be numeric and can be up to seven characters in length.

13 Enter the **E.164 international dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

14 Enter the **E.164 national dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

15 Enter the **E.164 local (subscriber) dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

16 Enter the **Private L1 domain (UDP location) dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

17 Enter the **Special number** in the text box. The number must be numeric and can be up to 30 characters in length.

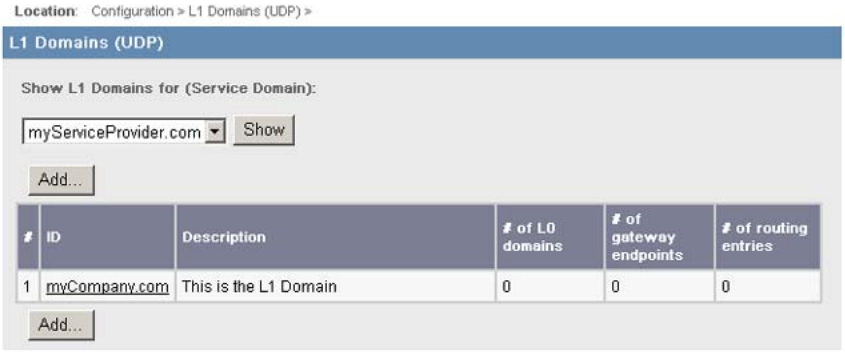
18 Enter the **Emergency service access prefix** in the text box. The number must be numeric and can be up to 30 characters in length.

19 Enter the **Special number label** in the text box. The label must be alphanumeric and can be up to 30 characters in length. The first character in the label must be alphabetic.

20 Click **Save**.

The **L1 Domains (UDP)** web page opens, showing the newly added myCompany.com L1 domain in the myServiceProvider.com Service Domain. See Figure 184 "Added L1 Domain" (page 315).

Figure 184
Added L1 Domain



Location: Configuration > L1 Domains (UDP) >

L1 Domains (UDP)

Show L1 Domains for (Service Domain): myServiceProvider.com

#	ID	Description	# of L0 domains	# of gateway endpoints	# of routing entries
1	myCompany.com	This is the L1 Domain	0	0	0

—End—

Procedure 84
Viewing the L1 Domains (UDP)

Step	Action
1	Select the **Configuration** tab on the NRS Manager toolbar. If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**. ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.
2	Ensure the **Active DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).
3	Click **L1 Domains (UDP)** in the navigator. The **L1 Domains (UDP)** web page opens and displays a drop-down list of configured Service Domains.
4	Select a Service Domain from the drop-down list.
5	Click **Show**. The web page expands to display a list of configured L1 Domains.
6	Click a **link** in the **ID** column of the L1 domains (UDP) web page. The View **L1 domain Property** web page opens and displays the configured data for the selected L1 Domain (UDP).

—End—

Adding a Level 0 Domain (CDP)

The Level 0 (L0) Domain is a building block of the phone context for private addresses. For more information on phone context, refer to "SIP Uniform Resource Identifiers" (page 38).

Procedure 85
Adding an L0 Domain (CDP)

Step	Action
1	Select the **Configuration** tab on the NRS Manager toolbar. If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

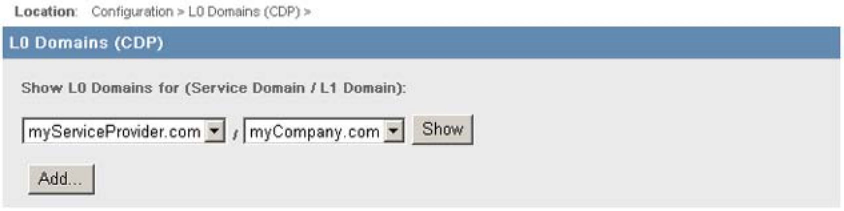
Note: The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Standby DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

3 Click **L0 Domains (CDP)** in the navigator.

The **L0 Domains (CDP)** web page opens, as shown in Figure 185 "L0 Domain (CDP) web page" (page 317). The two drop-down lists contain configured Service Domains and L1 Domains.

Figure 185
L0 Domain (CDP) web page



Location: Configuration > L0 Domains (CDP) >

L0 Domains (CDP)

Show L0 Domains for (Service Domain / L1 Domain):

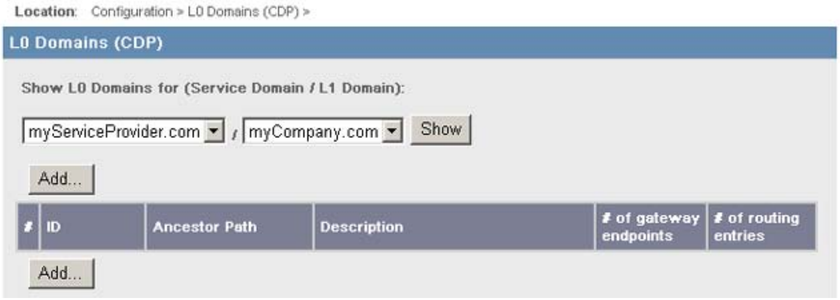
myServiceProvider.com / myCompany.com Show

Add...

4 Select the Service Domain and the L1 Domain from the respective drop-down lists.

5 (Optional) Click **Show** to display a list of configured L0 Domains for the selected Service Domain and L1 Domain. See Figure 186 "L0 Domains (CDP) web page for selected Service Domain / L1 Domain" (page 317).

Figure 186
L0 Domains (CDP) web page for selected Service Domain / L1 Domain



Location: Configuration > L0 Domains (CDP) >

L0 Domains (CDP)

Show L0 Domains for (Service Domain / L1 Domain):

myServiceProvider.com / myCompany.com Show

Add...

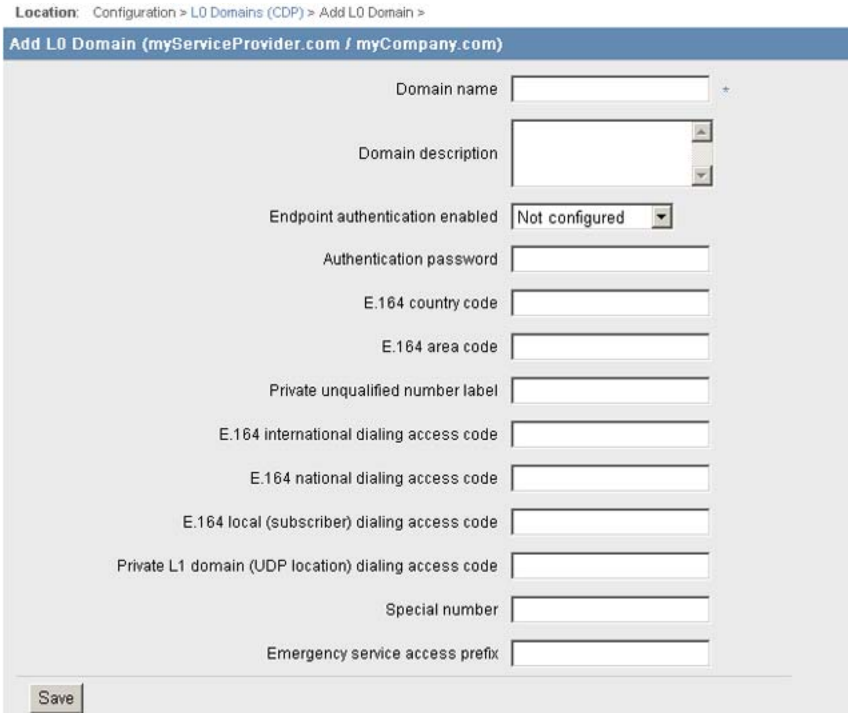
#	ID	Ancestor Path	Description	# of gateway endpoints	# of routing entries

Add...

6 Click **Add...**.

The **Add L0 Domain** web page opens, as shown in Figure 187 "Add L0 Domain web page" (page 318).

Figure 187
Add L0 Domain web page



Location: Configuration > L0 Domains (CDP) > Add L0 Domain >

Add L0 Domain (myServiceProvider.com / myCompany.com)

Domain name *

Domain description

Endpoint authentication enabled: Not configured

Authentication password

E.164 country code

E.164 area code

Private unqualified number label

E.164 international dialing access code

E.164 national dialing access code

E.164 local (subscriber) dialing access code

Private L1 domain (UDP location) dialing access code

Special number

Emergency service access prefix

7 Enter the **Domain name** of the L0 Domain in the text box. The name must be alphanumeric and up to 30 characters in length.

For example, enter myCdpDomain.

8 Enter the **Domain description** in the text box. The description can include any character except single quotes and can be up to 120 characters in length.

9 Select **Not configured**, **Authentication on**, or **Authentication off** from the **Endpoint authentication enabled** drop-down list.

If **Authentication on** is selected, then all endpoints require authentication.

10 Enter the **Authentication password** in the text box, if **Authentication on** was selected in step 8. The password must be alphanumeric and up to 30 characters in length.

11 Enter the **E.164 country code** in the text box. The code must be numeric and can be up to seven characters in length.

12 Enter the **E.164 area code** in the text box. The code must be numeric and can be up to seven characters in length.

13 Enter the **Private unqualified number label** in the text box. The label must be alphanumeric and can be up to 30 characters in length. The first character in the label must be alphabetic.

14 Enter the **E.164 international dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

15 Enter the **E.164 national dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

16 Enter the **E.164 local (subscriber) dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

17 Enter the **Private L1 domain (UDP location) dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

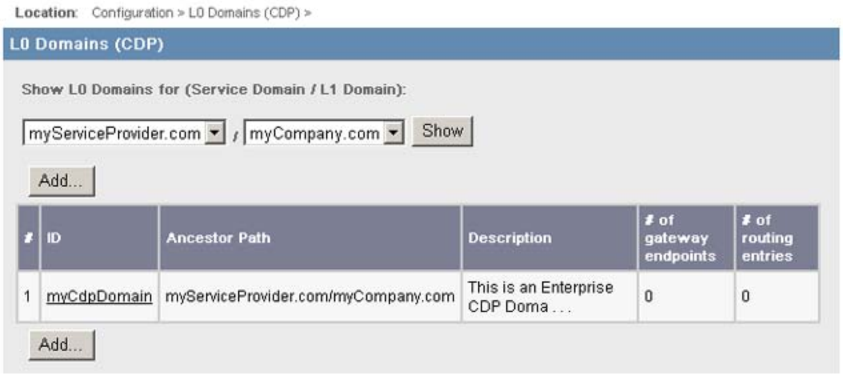
18 Enter the **Special number** in the text box. The number must be numeric and can be up to 30 characters in length.

19 Enter the **Emergency services access prefix** in the text box. The number must be numeric and can be up to 30 characters in length.

20 Click **Save**.

The **L0 Domains (CDP)** web page opens, showing the newly added myCdpDomain L0 domain. See Figure 188 "Added L0 Domain" (page 319).

Figure 188
Added L0 Domain



Location: Configuration > L0 Domains (CDP) >

L0 Domains (CDP)

Show L0 Domains for (Service Domain / L1 Domain):

myServiceProvider.com / myCompany.com

#	ID	Ancestor Path	Description	# of gateway endpoints	# of routing entries
1	myCdpDomain	myServiceProvider.com/myCompany.com	This is an Enterprise CDP Doma . . .	0	0

—End—

Procedure 86
Viewing the L0 Domains (CDP)

Step	Action
1	Select the **Configuration** tab on the NRS Manager toolbar. If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**. ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.
2	Ensure the **Active DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).
3	Click **L0 Domains (CDP)** in the navigator. The **L0 Domains (CDP)** web page opens and displays two drop-down lists: Service Domain / L1 Domain.
4	Select a Service Domain and L1 Domain from the drop-down lists.
5	Click **Show**. The web page expands to display a list of configured L0 Domains.
6	Click a **link** in the **ID** column of the L0 domains (CDP) web page. The View **L0 domain Property** web page opens and displays the configured data for the selected L0 Domain (CDP).

—End—

Adding a Gateway Endpoint

Follow Procedure 87 "Adding a Gateway Endpoint" (page 320) to add a gateway endpoint.

Procedure 87
Adding a Gateway Endpoint

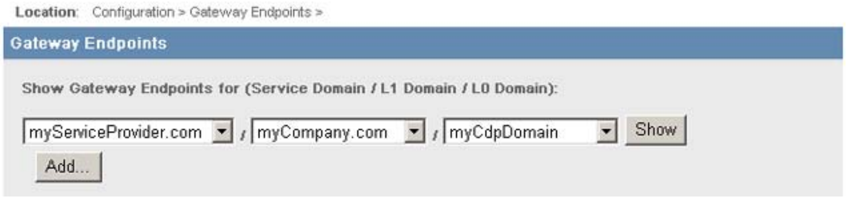
Step	Action
1	Select the **Configuration** tab on the NRS Manager toolbar. If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**. ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Standby DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

3 Click **Gateway Endpoints** in the navigator.

The **Gateway Endpoints** web page opens, as shown in Figure 189 "Gateway Endpoints web page" (page 321). The three drop-down lists contain configured Service Domains, L1 Domains, and L0 Domains.

Figure 189
Gateway Endpoints web page



Location: Configuration > Gateway Endpoints >

Gateway Endpoints

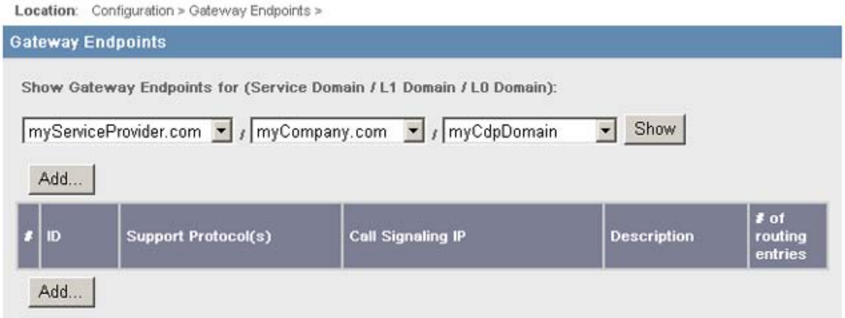
Show Gateway Endpoints for (Service Domain / L1 Domain / L0 Domain):

myServiceProvider.com / myCompany.com / myCdpDomain

4 Select the Service Domain, the L1 Domain, and L0 Domain from the respective drop-down lists.

5 (Optional) Click **Show** to display a list of configured Gateway Endpoints associated with the selected Service Domain, L1 Domain, and L0 Domain. See Figure 190 "Gateway Endpoints web page for selected Service Domain / L1 Domain / L0 Domain" (page 321).

Figure 190
Gateway Endpoints web page for selected Service Domain / L1 Domain / L0 Domain



Location: Configuration > Gateway Endpoints >

Gateway Endpoints

Show Gateway Endpoints for (Service Domain / L1 Domain / L0 Domain):

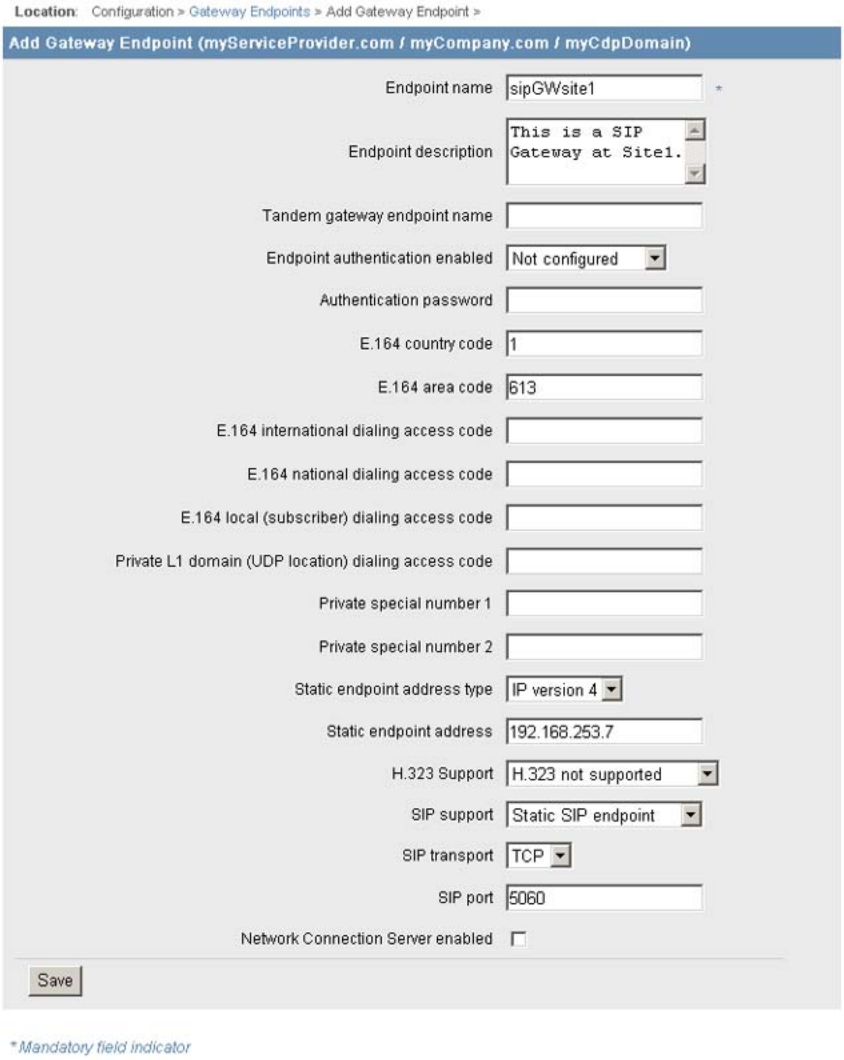
myServiceProvider.com / myCompany.com / myCdpDomain

#	ID	Support Protocol(s)	Call Signaling IP	Description	# of routing entries

6 Click **Add...**.

The **Add Gateway Endpoint** web page opens, as shown in Figure 191 "Add Gateway Endpoint web page" (page 322).

Figure 191
Add Gateway Endpoint web page



Location: Configuration > Gateway Endpoints > Add Gateway Endpoint >

Add Gateway Endpoint (myServiceProvider.com / myCompany.com / myCdpDomain)

Endpoint name	sipGWsite1 *
Endpoint description	This is a SIP Gateway at Site1.
Tandem gateway endpoint name	
Endpoint authentication enabled	Not configured
Authentication password	
E.164 country code	1
E.164 area code	613
E.164 international dialing access code	
E.164 national dialing access code	
E.164 local (subscriber) dialing access code	
Private L1 domain (UDP location) dialing access code	
Private special number 1	
Private special number 2	
Static endpoint address type	IP version 4
Static endpoint address	192.168.253.7
H.323 Support	H.323 not supported
SIP support	Static SIP endpoint
SIP transport	TCP
SIP port	5060
Network Connection Server enabled	□

**Mandatory field indicator*

7 Enter the **Endpoint name** of the gateway in the text box. The name must be alphanumeric and can be up to 30 characters in length.

For example, enter sipGWSite1.

8 Enter a description of the endpoint in the **Endpoint description** text box. The description must be alphanumeric and can be up to 120 characters in length.

9 Enter the **Tandem gateway endpoint name** in the text box, if required. This indicates whether the endpoint is used to tandem calls from outside the network. The name must be alphanumeric and can be up to 30 characters in length.

10 Select an option from the **Endpoint authentication enabled** drop-down list.

The three options are:

- **Not configured**: If this option is selected, then the gateway endpoint uses the L1 or L0 Authentication (if L1 or L0 authentication is enabled).
- **Authentication off**: If this option is selected, then authentication is off for this gateway endpoint even if L1 or L0 authentication is enabled.
- **Authentication on**: If this option is selected, then authentication is on for this gateway endpoint and the authentication overrides the L1 or L0 authentication (if it is enabled).

11 Enter the **Authentication password** in the text box, if **Authentication on** was selected in step 9. The password must be alphanumeric and can be up to 30 characters in length.

12 Enter the **E.164 country code** in the text box. The code must be numeric and can be up to seven characters in length.

13 Enter the **E.164 area code** in the text box. The code must be numeric and can be up to seven characters in length.

14 Enter the **E.164 international dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

15 Enter the **E.164 national dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

16 Enter the **E.164 local (subscriber) dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

17 Enter the **Private L1 domain (UDP location) dialing access code** in the text box. The code must be numeric and can be up to seven characters in length.

18 Enter the **Private special number 1** in the text box. The number must be numeric and can be up to 30 characters in length.

19 Enter the **Private special number 2** in the text box. The number must be numeric and can be up to 30 characters in length

20 Select **IP Version 4** from the **Static endpoint address type** drop-down list.

21 Enter the **Static endpoint address** in the text box.

This is the Node IP address of the Signaling Server. If a third-party gateway is being used, then it is the IP address of the gateway.

22 Select whether H.323 support is enabled from the **H.323 Support type** drop-down list.

The three options are:

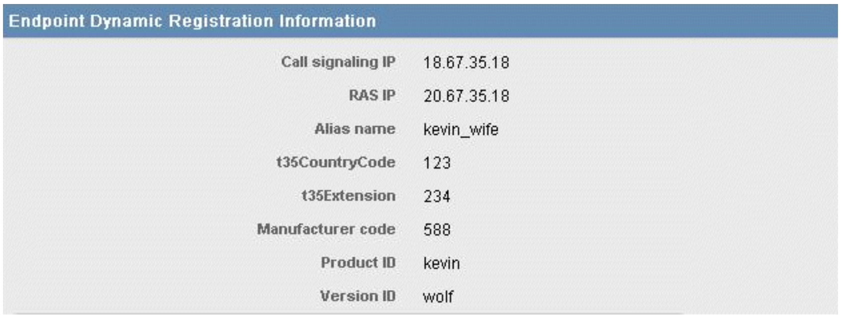
- H.323 not supported
- RAS H.323 endpoint
- Not RAS H.323 endpoint.

Note 1: If an H.323 Gateway Endpoint is configured with an H.323 Support type of RAS H.323 endpoint, then NRS Manager displays Endpoint Dynamic Registration information after the H.323 Gateway registers with the NRS.

Note 2: Endpoint Dynamic Registration information includes the following: Call Signaling IP, RAS IP, Alias name, t35Country code, t35Extension, Manufacturer code, Product ID, and Version ID.

Note 3: The H.323 **Endpoint Dynamic Registration Information** web page (see Figure 192 "H.323 Endpoint Dynamic Registration Information web page" (page 324)) is displayed only when NRS Manager is in **Active DB view**. The detailed dynamic registration information also is displayed only inside the Gateway Endpoint web page.

Figure 192
H.323 Endpoint Dynamic Registration Information web page



Endpoint Dynamic Registration Information

Call signaling IP	18.67.35.18
RAS IP	20.67.35.18
Alias name	kevin_wife
t35CountryCode	123
t35Extension	234
Manufacturer code	588
Product ID	kevin
Version ID	wolf

23 Configure SIP support.

a. Select an option from the **SIP Support type** drop-down list. The three options are: SIP not supported, Static SIP endpoint, and Dynamic SIP endpoint.

b. If SIP support is enabled, select the transport protocol from the **SIP transport** drop-down list. The two options are: TCP and UDP. TCP is selected by default.

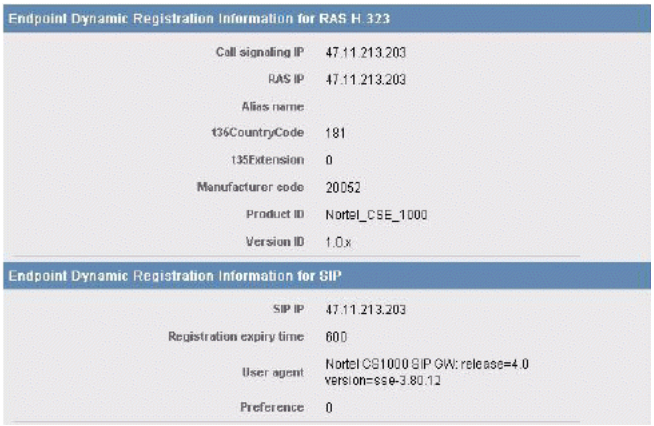
c. If SIP support is enabled, enter a port number in the **SIP port** text box. The value must be numeric and can be up to 5 digits in length. The range is 0 to 65535. The default port number is **5060** .

Note: If a SIP Trunk Gateway Endpoint is configured with a SIP Support type of Dynamic SIP endpoint, then NRS Manager displays Endpoint Dynamic Registration Information for SIP after the SIP Trunk Gateway registers with the NRS.

Endpoint Dynamic Registration Information includes the following: SIP IP, Registration expiry time, User agent, and Preference.

The SIP **Endpoint Dynamic Registration Information** web page (see Figure 193 "SIP Endpoint Dynamic Registration Information web page" (page 325)) is displayed only when NRS Manager is in **Active DB view**. The detailed dynamic registration information also is displayed only inside the Gateway Endpoint web page.

Figure 193
SIP Endpoint Dynamic Registration Information web page



Endpoint Dynamic Registration Information for RAS H.323

Call signaling IP	47.11.213.203
RAS IP	47.11.213.203
Alias name	
t36CountryCode	181
t35Extension	0
Manufacturer code	20052
Product ID	Nortel_CSE_1000
Version ID	1.0.x

Endpoint Dynamic Registration Information for SIP

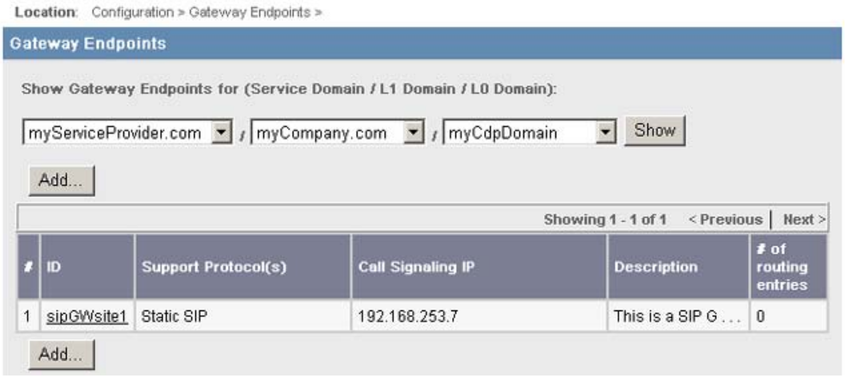
SIP IP	47.11.213.203
Registration expiry time	600
User agent	Nortel CS1000 SIP GW: release=4.0 version=sse-3.80.12
Preference	0

24 Select the **Network Connection Server is enabled** check box if this Gateway Endpoint supports the NCS for branch office or SRG user redirection to the main office, Virtual Office, or Geographic Redundancy.

25 Click **Save**.

The **Gateway Endpoints** web page opens, showing the newly added sipGWSite1 endpoint. See Figure 194 "Gateway Endpoints web page for added Gateway Endpoint" (page 326).

Figure 194
Gateway Endpoints web page for added Gateway Endpoint



Location: Configuration > Gateway Endpoints >

Gateway Endpoints

Show Gateway Endpoints for (Service Domain / L1 Domain / L0 Domain):

myServiceProvider.com / myCompany.com / myCdpDomain [Show]

[Add...]

Showing 1 - 1 of 1 < Previous | Next >

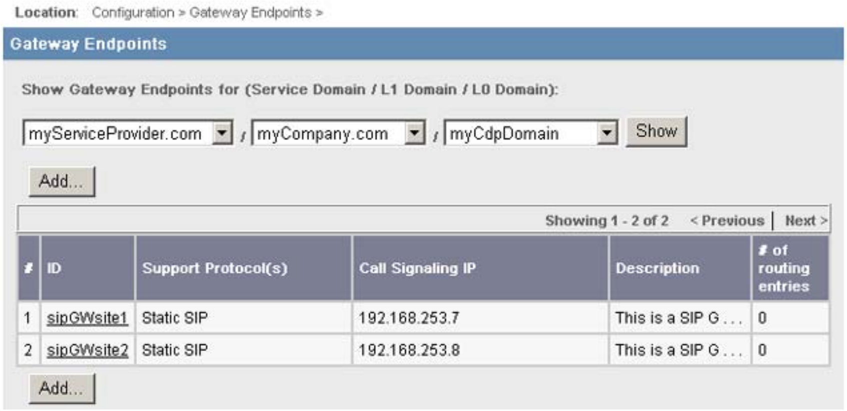
#	ID	Support Protocol(s)	Call Signaling IP	Description	# of routing entries
1	sipGWsite1	Static SIP	192.168.253.7	This is a SIP G . . .	0

[Add...]

26 If required, click **Add...** to add additional gateway endpoints. Repeat step 6 to step 24.

Any new endpoints are displayed in the **Gateway Endpoints** web page (see Figure 195 "Gateway Endpoints" (page 326)).

Figure 195
Gateway Endpoints



Location: Configuration > Gateway Endpoints >

Gateway Endpoints

Show Gateway Endpoints for (Service Domain / L1 Domain / L0 Domain):

myServiceProvider.com / myCompany.com / myCdpDomain [Show]

[Add...]

Showing 1 - 2 of 2 < Previous | Next >

#	ID	Support Protocol(s)	Call Signaling IP	Description	# of routing entries
1	sipGWsite1	Static SIP	192.168.253.7	This is a SIP G . . .	0
2	sipGWsite2	Static SIP	192.168.253.8	This is a SIP G . . .	0

[Add...]

—End—

Procedure 88
Viewing the Gateway Endpoints

Step	Action
1	Select the **Configuration** tab on the NRS Manager toolbar.

If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

> ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Active DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

3 Click **Gateway Endpoints** in the navigator.

The **Gateway Endpoints** web page opens and displays three drop-down lists: Service Domain / L1 Domain / L0 Domain.

4 Select a Service Domain, L1 Domain, and L0 Domain from the drop-down lists.

5 Click **Show**.

The web page expands to display a list of configured Gateway Endpoints.

6 Click a **link** in the **ID** column of the gateway Endpoints web page.

The **View Gateway Endpoint Property** web page opens and displays the configured data for the selected Gateway Endpoint.

—End—

Adding a User Endpoint

To add a User Endpoint (that is, a SIP Phone), refer to Procedure 1 "Adding a User Endpoint" (page 105).

Adding a Routing Entry

Procedure 89

Adding a Routing Entry

Step Action

1 Select the **Configuration** tab on the NRS Manager toolbar.

If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

> ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

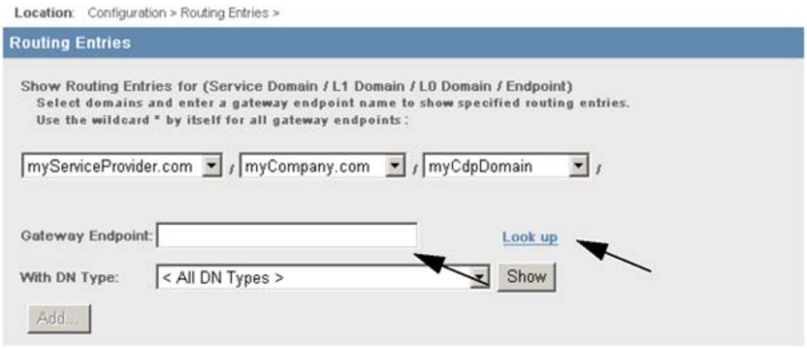
2 Ensure the **Standby DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

3 Click **Routing Entries** in the navigator.

The **Routing Entries** web page opens, as shown in Figure 196 "Routing Entries web page" (page 328).

> ***Note:*** The **Gateway Endpoint** field is empty.

Figure 196
Routing Entries web page



Location: Configuration > Routing Entries >

Routing Entries

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified routing entries.
Use the wildcard * by itself for all gateway endpoints :

myServiceProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint:

With DN Type: < All DN Types >

4 Fill the **Gateway Endpoint** text box using one of the following three methods:

a. Enter * in the **Gateway Endpoint** text box.

Click the **Show** button and the **Routing Entries** web page expands to display all Gateway Endpoints.

Cut and paste an entry from the **Gateway Endpoint** column into the **Gateway Endpoint** text box.

or

b. Click the **Look up** link to open the **Look up path for gateway endpoints** web page, as shown in Figure 197 "Lookup path for gateway endpoints web page - Page-by-Page search" (page 329). The **Look up** utility allows you to search for Gateway Endpoint in two ways: **Page-by-Page** and **Name prefix**.

- The **Page-by-Page** search is the default method, and the results are displayed in the **Look up path for gateway endpoints** web page, as shown in Figure 197 "Lookup path for gateway endpoints web page - Page-by-Page search" (page 329).

  Click a **link** in the **ID** column and the **Gateway Endpoint** text box auto-fills with the selected Gateway Endpoint, as shown in Figure 200 "Results of Gateway Endpoint look up" (page 330).

- To perform a Name prefix search, select **Name prefix** from the drop-down list. In the text box, enter an alphanumeric string for the first few characters in the name of Gateway Endpoints as shown in Figure 198 "Name prefix search entry" (page 329).

  Click **Search**, and all Gateway Endpoints whose name begins with the alphanumeric string entered in the text box are displayed, as shown in Figure 199 "Results of Name prefix search" (page 330).

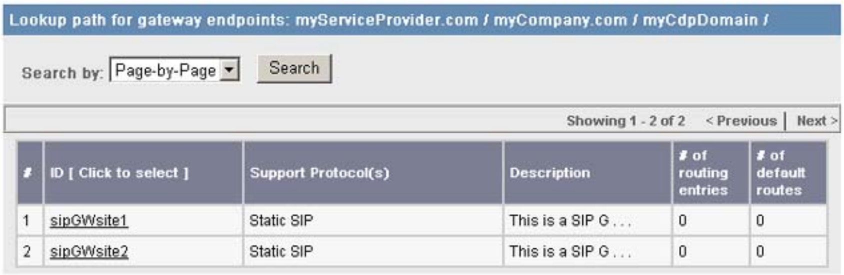
  Click a **link** in the **ID** column and the **Gateway Endpoint** text box auto-fills with the selected Gateway endpoint, as shown in Figure 200 "Results of Gateway Endpoint look up" (page 330)

or

c. To perform a **Name Prefix** search enter an alphanumeric string for the first few characters in the name of Gateway Endpoints, in the **Gateway Endpoint** text box. Click the **Look up** link, and all gateway Endpoints whose name begins with the alphanumeric string entered in the text box are displayed, as shown in Figure 199 "Results of Name prefix search" (page 330)

   Click a **link** in the **ID** column and the **Gateway Endpoint** text box auto-fills with the selected Gateway endpoint, as shown in Figure 200 "Results of Gateway Endpoint look up" (page 330)

Figure 197
Lookup path for gateway endpoints web page - Page-by-Page search



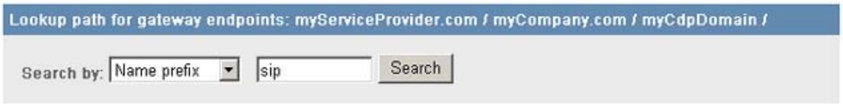
Lookup path for gateway endpoints: myServiceProvider.com / myCompany.com / myCdpDomain /

Search by: Page-by-Page

Showing 1 - 2 of 2

#	ID [Click to select]	Support Protocol(s)	Description	# of routing entries	# of default routes
1	sipGWsite1	Static SIP	This is a SIP G . . .	0	0
2	sipGWsite2	Static SIP	This is a SIP G . . .	0	0

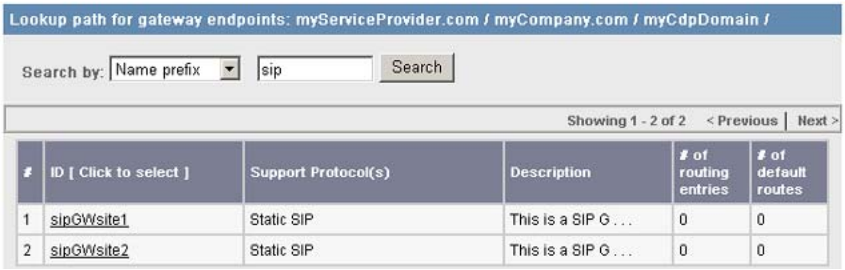
Figure 198
Name prefix search entry



Lookup path for gateway endpoints: myServiceProvider.com / myCompany.com / myCdpDomain /

Search by: Name prefix sip

Figure 199
Results of Name prefix search



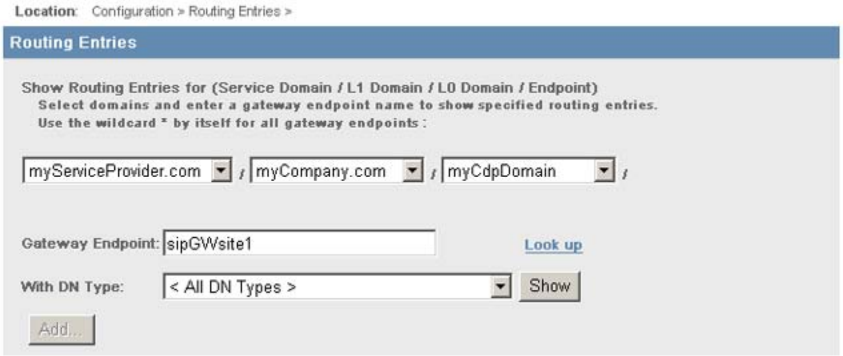
Lookup path for gateway endpoints: myServiceProvider.com / myCompany.com / myCdpDomain /

Search by: Name prefix ▾ sip Search

Showing 1 - 2 of 2 < Previous | Next >

#	ID [Click to select]	Support Protocol(s)	Description	# of routing entries	# of default routes
1	sipGWsite1	Static SIP	This is a SIP G . . .	0	0
2	sipGWsite2	Static SIP	This is a SIP G . . .	0	0

Figure 200
Results of Gateway Endpoint look up



Location: Configuration > Routing Entries >

Routing Entries

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified routing entries.
Use the wildcard * by itself for all gateway endpoints :

myServiceProvider.com ▾ / myCompany.com ▾ / myCdpDomain ▾ /

Gateway Endpoint: sipGWsite1 Look up

With DN Type: < All DN Types > ▾ Show

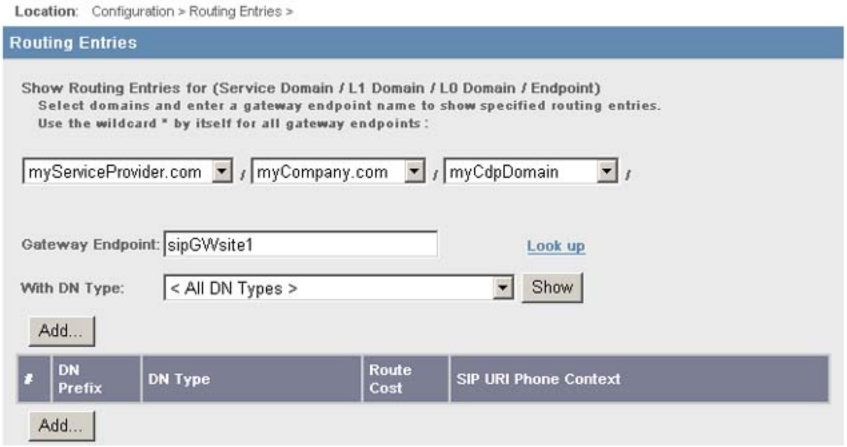
Add...

5 Select the DN type(s) from the **With DN Type** drop-down list. The seven choices are <All DN Types>, E.164 international, E.164 national, E.164 local (subscriber), Private level 1 regional (UDP location code), Private level 0 regional (CDP steering code), and Private special.

6 Click **Show**.

The web page expands to display a list of DNs of the type selected in Step 4, that are configured for the endpoint(s) in the Gateway Endpoint text box. See Figure 201 "DNs of selected type associated with selected Endpoint(s)" (page 331).

Figure 201
DNs of selected type associated with selected Endpoint(s)



Location: Configuration > Routing Entries >

Routing Entries

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified routing entries.
Use the wildcard * by itself for all gateway endpoints :

myServiceProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint: sipGWsite1

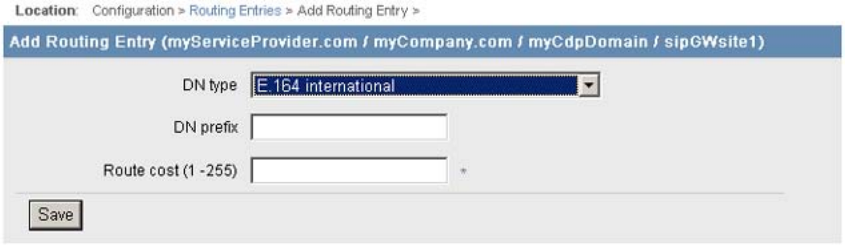
With DN Type: < All DN Types >

#	DN Prefix	DN Type	Route Cost	SIP URI Phone Context

7 Click **Add....**

The **Add Routing Entry** web page opens, as shown in Figure 202 "Add Routing Entry" (page 331).

Figure 202
Add Routing Entry



Location: Configuration > Routing Entries > Add Routing Entry >

Add Routing Entry (myServiceProvider.com / myCompany.com / myCdpDomain / sipGWsite1)

DN type: E.164 international

DN prefix:

Route cost (1 -255): *

8 Select the **DN type** from the drop-down list.

The six options are E.164 international, E.164 national, E.164 local (subscriber), Private level 1 regional (UDP location code), Private level 0 regional (CDP steering code), and Private special.

The DN type attribute determines how the phone context value, that is used to qualify the DN prefix, is built from the building blocks configured for the routing entry parents.

9 Enter the **DN prefix** in the text box. The DN prefix can include 0-9, #, -, ?. The prefix can be up to 30 characters in length; however, the first character must be numeric.

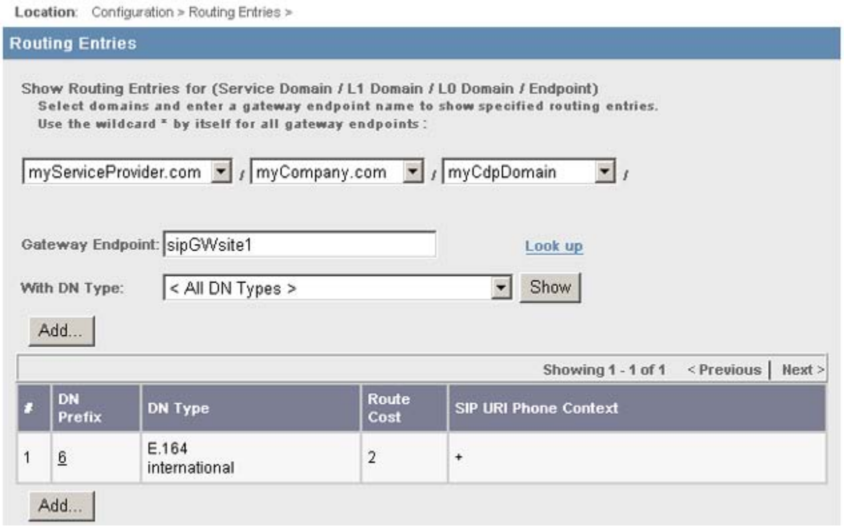
10 Enter the **Route cost** in the text box. The range is 1-255. The cost must be numeric and can be up to three characters in length.

This number is used to define least-cost routing. Higher numbers indicate higher costs.

11 Click **Save**.

The **Routing Entries** web page opens, displaying the newly added routing entry, as shown in Figure 203 "Added Routing Entry" (page 332).

Figure 203
Added Routing Entry



Location: Configuration > Routing Entries >

Routing Entries

Show Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified routing entries.
Use the wildcard * by itself for all gateway endpoints :

mySeviceProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint: sipGWsite1

With DN Type: < All DN Types >

#	DN Prefix	DN Type	Route Cost	SIP URI Phone Context
1	6	E.164 international	2	+

—End—

Procedure 90
Viewing the Routing Entries

Step	Action

1 Select the **Configuration** tab on the NRS Manager toolbar.

If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

> ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Active DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

3 Click **Routing Entries** in the navigator.

The **Routing Entries** web page opens and displays three drop-down lists: Service Domain / La Domain / L0 Domain.

4 Select a Service Domain, L1 Domain, and L0 Domain from the three drop-down lists, respectively.

5 Fill the **Gateway Endpoint** text using one of the methods described in Procedure 89 "Adding a Routing Entry" (page 327), Step 3.

6 Select the DN type from the **With DN Type** drop-down list.

7 Click **Show**.

The web page expands to display a list of configured Routing Entries.

—End—

Adding Default Routes

If the routing entry DN prefix in an incoming H.323/SIP signaling request does not match a DN prefix Gateway Endpoint routing entry recorded in the NRS database, the default route is returned to the gateway.

Procedure 91

Adding a Default Route

Step Action

1 Select the **Configuration** tab on the NRS Manager toolbar.

If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

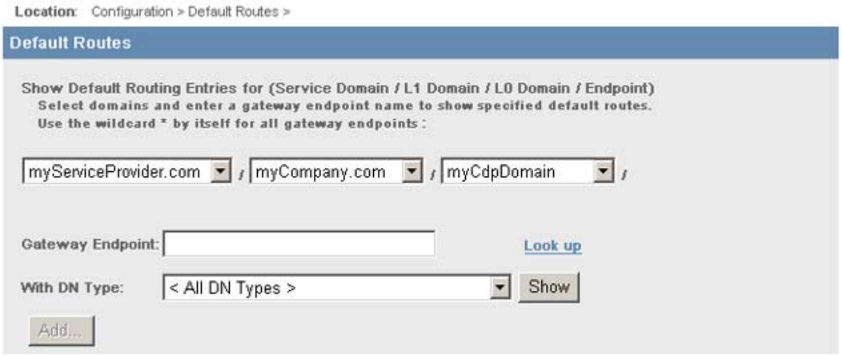
> ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Standby DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

3 Click **Default Routes** in the navigator.

The **Default Routes** web page opens, as shown in Figure 204 "Default Routes web page" (page 334).

Figure 204
Default Routes web page



Location: Configuration > Default Routes >

Default Routes

Show Default Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified default routes.
Use the wildcard * by itself for all gateway endpoints :

myServiceProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint: Look up

With DN Type: < All DN Types > Show

4 Fill the **Gateway Endpoint** text box using one of the methods described in Procedure 89 "Adding a Routing Entry" (page 327), Step 3.

5 Select the DN type from the **With DN Type** drop-down list.

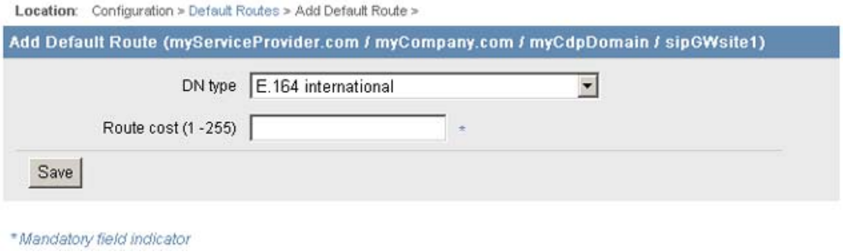
6 Click **Show**.

The web page expands to display a list of DNs, of the type selected in step 6, that are configured for the endpoint(s) in the Gateway Endpoint text box.

7 Click **Add....**

The **Add Default Route** web page opens, as shown in Figure 205 "Add Default Route web page" (page 334).

Figure 205
Add Default Route web page



Location: Configuration > Default Routes > Add Default Route >

Add Default Route (myServiceProvider.com / myCompany.com / myCdpDomain / sipGWsite1)

DN type E.164 international

Route cost (1 -255) *

* Mandatory field indicator

8 Select the **DN type**.

The six options are E.164 international, E.164 national, E.164 local (subscriber), Private level 1 regional (UDP location code), Private level 0 regional (CDP steering code), and Private special.

The DN type attribute determines how the phone context value, that is used to qualify the DN prefix, is built from the building blocks configured for the routing entry parents.

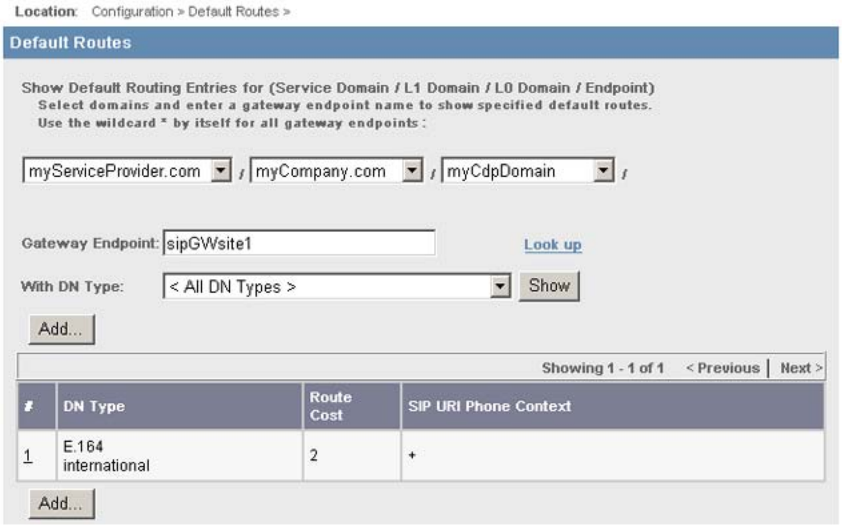
> ***Note:*** Each DN type has only one default route.

9 Enter the **Route cost**. The range is 1-255. The cost must be numeric and can be up to three characters in length.

10 Click **Save**.

The **Default Routes** web page opens showing the new default route. See Figure 206 "Added Default Route" (page 335).

Figure 206
Added Default Route



Location: Configuration > Default Routes >

Default Routes

Show Default Routing Entries for (Service Domain / L1 Domain / L0 Domain / Endpoint)
Select domains and enter a gateway endpoint name to show specified default routes.
Use the wildcard * by itself for all gateway endpoints :

myServiceProvider.com / myCompany.com / myCdpDomain /

Gateway Endpoint: sipGWsite1

With DN Type: < All DN Types >

Showing 1 - 1 of 1

#	DN Type	Route Cost	SIP URI Phone Context
1	E.164 international	2	+

—End—

Procedure 92
Viewing Default Routes

Step Action

1 Select the **Configuration** tab on the NRS Manager toolbar.

If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

> ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Active DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

3 Click **Default Routes** in the navigator.

The **Default Routes** web page opens and displays three drop-down lists: Service Domain / L1 Domain / L0 Domain.

4 Select a Service Domain, L1 Domain, and L0 Domain from the three drop-down lists, respectively.

5 Fill the **Gateway Endpoint** text using one of the methods described in Procedure 89 "Adding a Routing Entry" (page 327), Step 3.

6 Select the DN type from the **With DN Type** drop-down list.

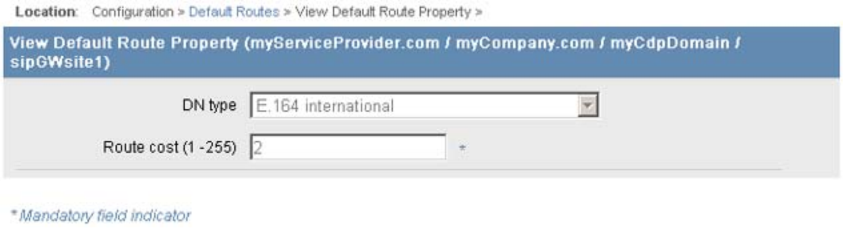
7 Click **Show**.

The web page expands to display a list of configured default routes.

8 Click a **link** in the # column of the Default Routes web page and the **View Default Route Property** web page opens, as shown in Figure 207 "View Default Route Property web page" (page 336).

You can edit the properties of the Default Route on this web page, or delete the Default Route altogether.

Figure 207
View Default Route Property web page



Location: Configuration > Default Routes > View Default Route Property >

View Default Route Property (myServiceProvider.com / myCompany.com / myCdpDomain / sipGWsite1)

DN type: E.164 international

Route cost (1 -255): 2 *

* Mandatory field indicator

—End—

Adding a Collaborative Server

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

NRS Manager provides a utility for adding and viewing Collaborative Servers, either system-wide or in different network domains.

The configuration of a Collaborative Server as “system-wide” allows IP addresses to be shared by users across multiple domains. This also allows domains to be spread geographically.

NRS Collaborative Servers in different network domains can also be specified in the NRS.

If a request comes in from a gateway and the NRS cannot find a match in its database for the request, the NRS provides the IP address of a Collaborative Server to the gateway. The gateway can then send its request to the Collaborative Server.

> ***Note:*** Calls can only be made in the same domain, even though calls go through the Collaborative Server to find a match.

For more information about the Collaborative Server, refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*.

Procedure 93
Adding a Collaborative Server

Step **Action**

1 Select the **Configuration** tab on the NRS Manager toolbar.

If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

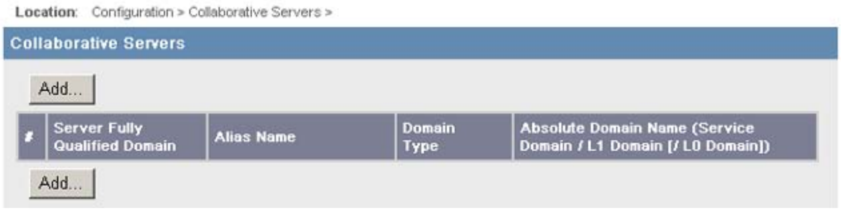
> ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Standby DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

3 Click **Collaborative Server** in the navigator.

The **Collaborative Servers** web page opens, as shown in Figure 208 "Collaborative Servers web page" (page 337).

Figure 208
Collaborative Servers web page



Location: Configuration > Collaborative Servers >

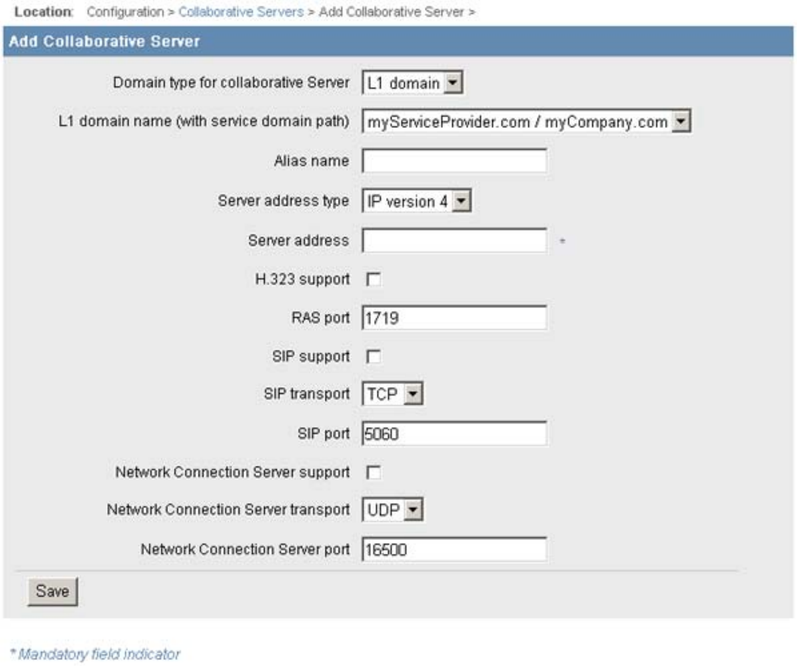
Collaborative Servers

#	Server Fully Qualified Domain	Alias Name	Domain Type	Absolute Domain Name (Service Domain / L1 Domain [/ L0 Domain])

4 Click **Add....**

The **Add Collaborative Server** web page opens, as shown in Figure 209 "Add Collaborative Server (with L1 Domain)" (page 338).

Figure 209
Add Collaborative Server (with L1 Domain)



Location: Configuration > Collaborative Servers > Add Collaborative Server >

Add Collaborative Server

Domain type for collaborative Server	L1 domain
L1 domain name (with service domain path)	myServiceProvider.com / myCompany.com
Alias name	
Server address type	IP version 4
Server address	*
H.323 support	□
RAS port	1719
SIP support	□
SIP transport	TCP
SIP port	5060
Network Connection Server support	□
Network Connection Server transport	UDP
Network Connection Server port	16500

Mandatory field indicator

5 Select the **Domain type for Collaborative Server** from the drop-down list.

- Select **System wide** if the Collaborative Server is to be a system-wide server. See Figure 210 "Add Collaborative Server (system-wide)" (page 339).

- Select **Service domain** if the Collaborative Server is to be a Service Domain server.

  An additional field **Service domain name** is displayed, prompting for the name of the Service domain. Select the name of the Service domain from the drop-down list.

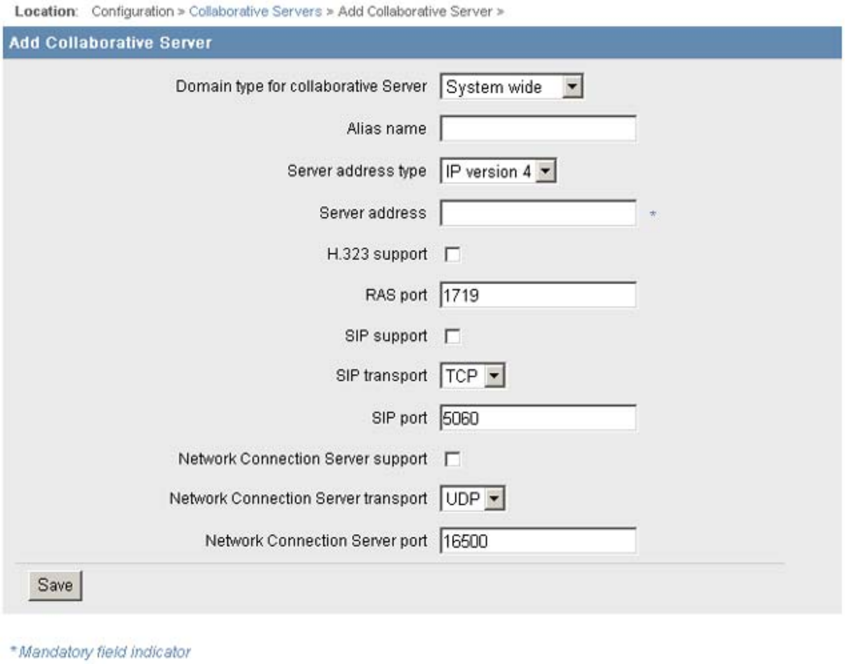
- Select **L1 domain** if the Collaborative Server is to be an L1 Domain server.

  An additional field **L1 domain name (with service domain path)** is displayed, prompting for the name of the L1 domain. Select the Service Domain / L1 Domain name from the drop-down list.

- Select **L0 domain** if the Collaborative Server is to be an L0 Domain server.

Two additional fields are displayed: (1) **L1 domain name (with service domain path**) prompting for the name of the L1 domain. and (2) **L0 Domain** prompting for the name of the L0 domain. See Figure 211 "Add Collaborative Server (with L0 Domain)" (page 340). Select the name of the L0 Domain from the drop-down list for the second field.

Figure 210
Add Collaborative Server (system-wide)



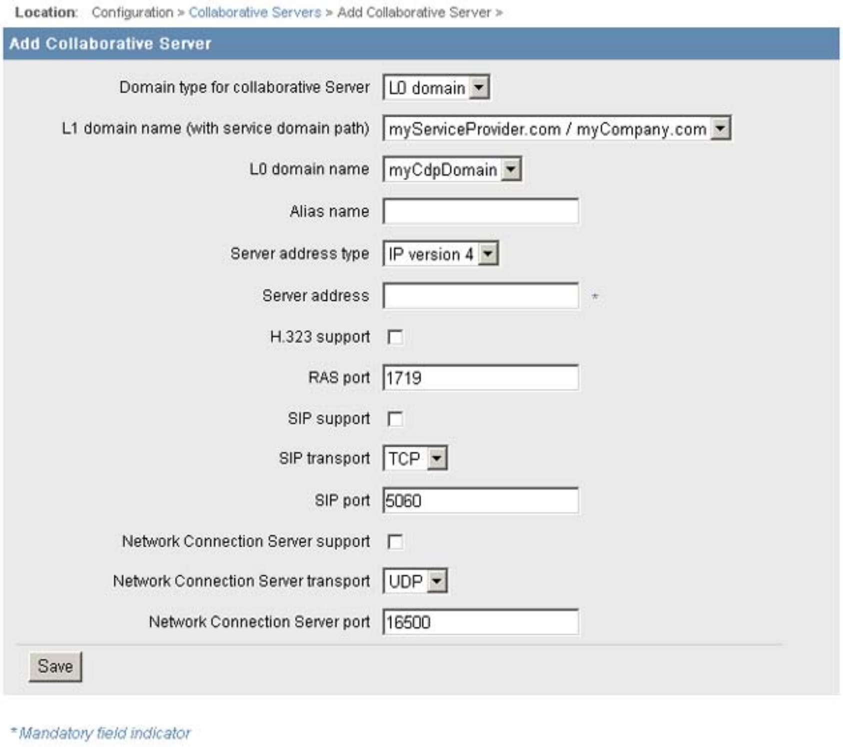
Location: Configuration > Collaborative Servers > Add Collaborative Server >

Add Collaborative Server

Domain type for collaborative Server	System wide ▾
Alias name	
Server address type	IP version 4 ▾
Server address	*
H.323 support	□
RAS port	1719
SIP support	□
SIP transport	TCP ▾
SIP port	5060
Network Connection Server support	□
Network Connection Server transport	UDP ▾
Network Connection Server port	16500

** Mandatory field indicator*

Figure 211
Add Collaborative Server (with L0 Domain)



Location: Configuration > Collaborative Servers > Add Collaborative Server >

Add Collaborative Server

Domain type for collaborative Server	L0 domain
L1 domain name (with service domain path)	myServiceProvider.com / myCompany.com
L0 domain name	myCdpDomain
Alias name	
Server address type	IP version 4
Server address	*
H.323 support	□
RAS port	1719
SIP support	□
SIP transport	TCP
SIP port	5060
Network Connection Server support	□
Network Connection Server transport	UDP
Network Connection Server port	16500

* Mandatory field indicator

6 Enter the **Alias name** of the collaborative server in the text box. The alias name must be alphanumeric and can be up to 30 characters in length. The name cannot include spaces.

7 Select **IP version 4** from the **Server address type** drop-down list.

8 Enter the TLAN IP address of the server in the **Server address** text box.

9 Select the protocol(s) supported by the server.

- If H.323 is supported, perform the following steps:
  1. Select the **H.323 support** check box.
  2. Enter the **RAS port** number. The port number must be numeric and can be up to five characters in length.
- If SIP is supported, perform the following steps:
  1. Select the **SIP support** check box.
  2. Select the transport protocol from the **SIP transport** drop-down list. TCP is the default.

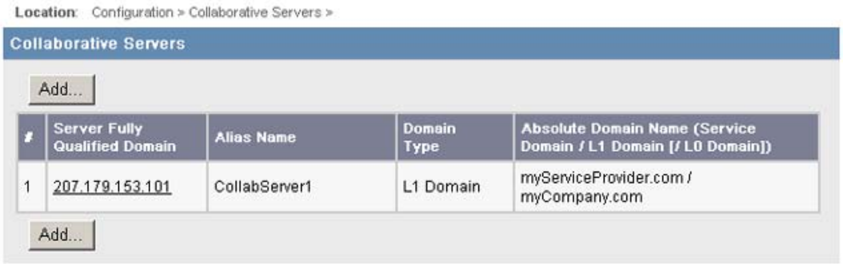
3. Enter the **SIP port** number in the text box. The port number must be numeric and can be up to five digits in length.

10 Ensure that the **Network Connection Server support** check box is **not** selected. The Collaborative Server does not support the Network Connection Service (NCS).

11 Click **Save**.

The **Collaborative Servers** web page opens with the newly added collaborative server, as shown in Figure 212 "Added Collaborative Server" (page 341).

Figure 212
Added Collaborative Server



Location: Configuration > Collaborative Servers >

Collaborative Servers

#	Server Fully Qualified Domain	Alias Name	Domain Type	Absolute Domain Name (Service Domain / L1 Domain [/ L0 Domain])
1	207.179.153.101	CollabServer1	L1 Domain	myServiceProvider.com / myCompany.com

12 If required, click **Add....** to add additional collaborative servers. repeat step 5 to step 11.

—End—

Procedure 94
Viewing the Collaborative Servers

Step Action

1 Select the **Configuration** tab on the NRS Manager toolbar.

If a dialog box displays indicating the status of the active and standby database (see Figure 175 "Configuration tab message" (page 309)) click **OK**.

> ***Note:*** The dialog box only opens the first time that the Configuration web pages are opened.

2 Ensure the **Active DB view** is selected. (See Procedure 80 "Switching between the active and standby databases" (page 308)).

3 Click **Collaborative Server** in the navigator.

The **Collaborative Server** web page opens and displays a list of configured Collaborative Servers in different network zones.

—End—

Verifying the numbering plan and saving the NRS configuration

You should verify your numbering plan after it is configured in the NRS.

Procedure 95

Verifying the numbering plan

Step	Action
1	Perform a database **Cut over**. Cutting over places the database on the network. See Procedure 100 "Cutting over the database" (page 351).
2	Perform the routing tests. • See Procedure 96 "Performing an H.323 Routing Test" (page 343). • See Procedure 97 "Performing a SIP Routing Test" (page 344).
3	If the routing tests succeed, perform a database **Commit**. See Procedure 103 "Committing the database" (page 354).
4	If there are problems with the network testing, use the database **Revert** command to undo the **Cut over.** See Procedure 101 "Reverting the database changes" (page 352) If you want to undo the latest provisioning changes, use a database rollback command to resynchronize the Standby database with the previous Active database. See Procedure 102 "Rolling back changes to the database" (page 353)

—End—

Tools tab

H.323 and SIP Routing Tests

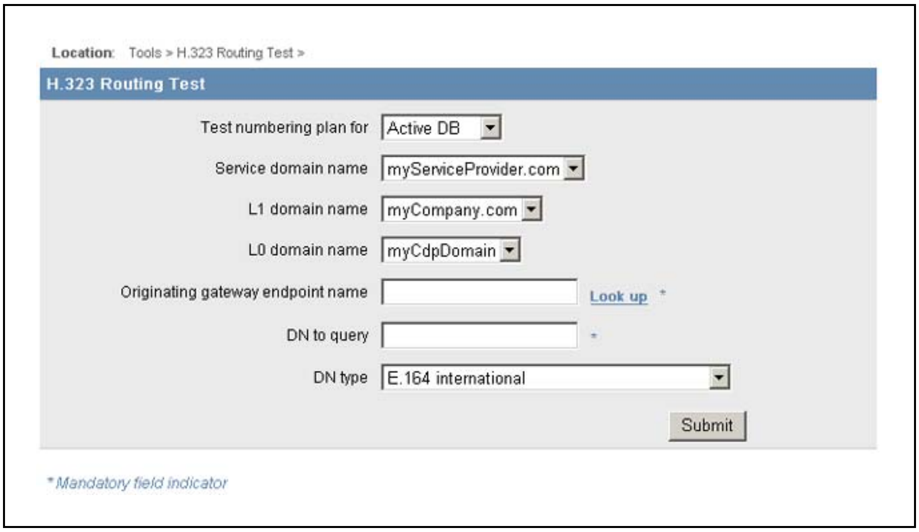
To ascertain if a numbering plan entry exists in the active or standby database:

- Follow Procedure 96 "Performing an H.323 Routing Test" (page 343) to perform an H.323 Routing Test.
- Follow Procedure 97 "Performing a SIP Routing Test" (page 344) to perform a SIP Routing Test.

Procedure 96
Performing an H.323 Routing Test

Step	Action
1	Click the **Tools** tab on the NRS Manager toolbar. The **H.323 Routing Test** web page opens, as shown in H.323 Routing Test.

Figure 213
H.323 routing Test



Location: Tools > H.323 Routing Test >

H.323 Routing Test

Test numbering plan for: Active DB

Service domain name: myServiceProvider.com

L1 domain name: myCompany.com

L0 domain name: myCdpDomain

Originating gateway endpoint name: *

DN to query: *

DN type: E.164 international

*Mandatory field indicator

Step	Action
2	Select **Active DB** or **Standby DB** from the **Test numbering plan for** drop-down list.
3	Select the **Service domain name** from the drop-down list.
4	Select the **L1 domain name** from the drop-down list.
5	Select the **L0 domain name** from the drop-down list.
6	Enter the **Originating gateway endpoint name** using the **Lookup** link. Click the **Look up** link to open the **Look up path for gateway endpoints** web page. The **Look up** utility allows you to search for Gateway Endpoints in two ways: **Page-by-Page** and **Name prefix**. a. The **Page-by-Page** search is the default method. Click **Search**, on the **Look up path for gateway endpoints** web page. The **Look up path for gateway endpoints** web page expands, and the results are displayed. or

b. Select **Name prefix** from the drop-down list to perform a Name prefix search. In the text box, enter an alphanumeric string for the first few characters in the name of Gateway Endpoints.

   Click **Search**, and all Gateway Endpoints whose name begins with the alphanumeric string entered in the text box are displayed.

7 Click a **link** in the **ID** column of the **Look up path for gateway endpoints** web page and the **Originating gateway endpoint name** text box auto-fills with the selected Gateway Endpoint.

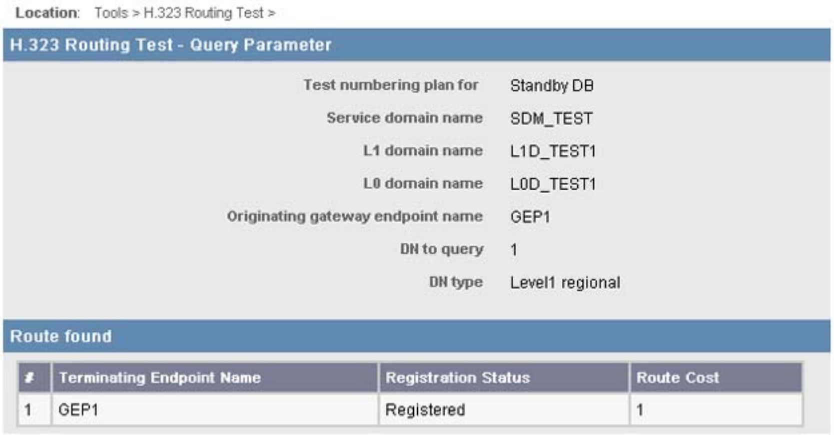
8 Enter a numbering plan entry you want to check in the **DN to query** text box.

9 Select a number type from the **DN type** drop-down list.

10 Click **Submit**.

The results of the H.323 Routing Test are displayed, as shown in Figure 214 "H.323 Routing Test - results" (page 344).

Figure 214
H.323 Routing Test - results



Location: Tools > H.323 Routing Test >

H.323 Routing Test - Query Parameter

Test numbering plan for	Standby DB
Service domain name	SDM_TEST
L1 domain name	L1D_TEST1
L0 domain name	L0D_TEST1
Originating gateway endpoint name	GEP1
DN to query	1
DN type	Level1 regional

Route found

#	Terminating Endpoint Name	Registration Status	Route Cost
1	GEP1	Registered	1

—End—

Procedure 97
Performing a SIP Routing Test

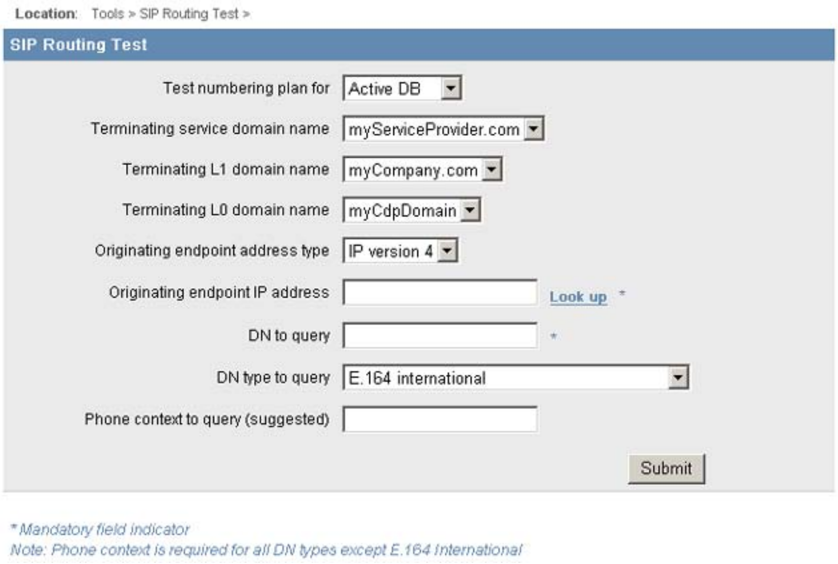
Step Action

1 Click the **Tools** tab on the NRS Manager toolbar.

2 Click **SIP Routing Test** in the navigator.

The **SIP Routing Test** web page opens, as shown in Figure 215 "SIP Routing Test" (page 345).

Figure 215
SIP Routing Test



Location: Tools > SIP Routing Test >

SIP Routing Test

Test numbering plan for	Active DB ▾
Terminating service domain name	myServiceProvider.com ▾
Terminating L1 domain name	myCompany.com ▾
Terminating L0 domain name	myCdpDomain ▾
Originating endpoint address type	IP version 4 ▾
Originating endpoint IP address	Look up *
DN to query	*
DN type to query	E.164 international ▾
Phone context to query (suggested)	

Submit

Mandatory field indicator
Note: Phone context is required for all DN types except E.164 International

3 Select **Active DB** or **Standby DB** from the **Test numbering plan for** drop-down list.

4 Select the Service Domain from the **Terminating service domain name** drop-down list.

5 Select the L1 Domain name from the **Terminating L1 domain name** drop-down list.

6 Select the L0 Domain name from the **Terminating L0 domain name** drop-down list.

7 Ensure IP version 4 is selected from the **Originating endpoint address type** drop-down list.

8 Enter the **Originating gateway endpoint name** using the **Lookup** link.

Click the **Look up** link to open the **Look up path for gateway endpoints** web page.

The **Look up** utility allows you to search for Gateway Endpoints in two ways: **Page-by-Page** and **Name prefix**.

a. The **Page-by-Page** search is the default method.

Click **Search**, on the **Look up path for gateway endpoints** web page. The **Look up path for gateway endpoints** web page expands, and the results are displayed.

or

b. Select **Name prefix** from the drop-down list to perform a Name prefix search. In the text box, enter an alphanumeric string for the first few characters in the name of Gateway Endpoints.

Click **Search**, and all Gateway Endpoints whose name begins with the alphanumeric string entered in the text box are displayed.

9 Click a **link** in the **SIP Endpoint IP** column of the **Look up path for gateway endpoints** web page and the **Originating endpoint IP address** text box auto-fills with the selected SIP Endpoint IP address.

10 Enter a numbering plan entry you want to check in the **DN to query** text box.

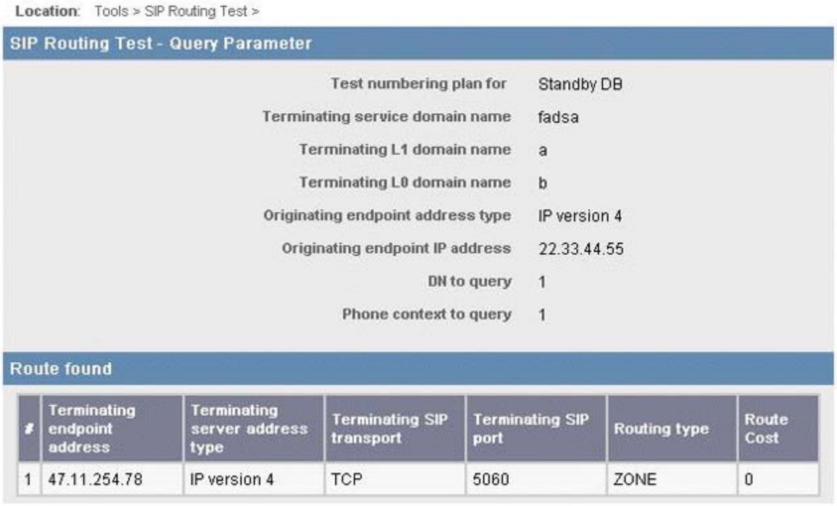
11 Select the DN type you want to check from the **DN type to query** drop-down list.

12 Enter the **Phone context to query**.

13 Click **Submit**.

The results of the SIP Routing Test are displayed (see Figure 216 "SIP Routing Test - results" (page 346)).

Figure 216
SIP Routing Test - results



Location: Tools > SIP Routing Test >

SIP Routing Test - Query Parameter

Test numbering plan for	Standby DB
Terminating service domain name	fadsa
Terminating L1 domain name	a
Terminating L0 domain name	b
Originating endpoint address type	IP version 4
Originating endpoint IP address	22.33.44.55
DN to query	1
Phone context to query	1

Route found

#	Terminating endpoint address	Terminating server address type	Terminating SIP transport	Terminating SIP port	Routing type	Route Cost
1	47.11.254.78	IP version 4	TCP	5060	ZONE	0

—End—

Enabling and disabling the NRS Server

Actions to:

- Forcefully disable the NRS server (nrsForceDisableServer)
- Gracefully disable the NRS server (nrsDisableServer) This command should not interrupt the existing calls.
- Enable the NRS server (nrsEnableServer)

can be performed using NRS Manager or the Command Line Interface (CLI).

The NRS can be taken out-of-service to perform maintenance or to place an Alternate NRS into service.

> ***Note:*** Only users with administrator privileges can execute the NRS server action commands.

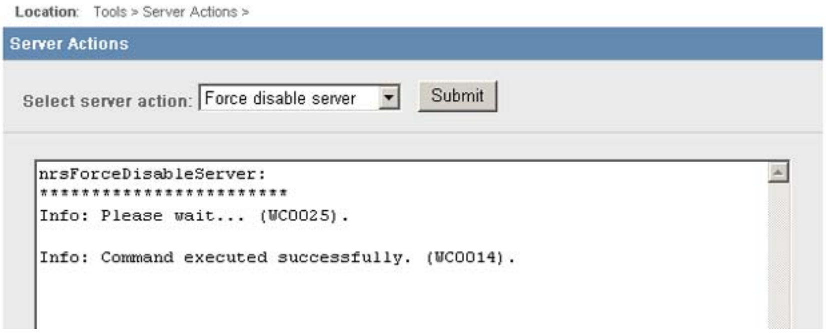
To take the NRS out-of-service (disabling the NRS server), follow the steps in Procedure 98 "Disabling the NRS server" (page 347). To bring the NRS back in to service, follow the steps in Procedure 99 "Enabling the NRS server" (page 348).

Procedure 98

Disabling the NRS server

Step	Action
1	Click the **Tools** tab on the NRS Manager toolbar.
2	Click **Server Actions** in the navigator. The **Server Actions** web page opens.
3	Select **Graceful disable server** or **Forceful disable server** from the **Select server action** drop-down list.
4	Click **Submit**. The nrsDisableServer or nrsForceDisableServer command is issued. The results are written in the text area of the **Server Actions** web page, as shown in Figure 217 "Disabling the server" (page 348).

Figure 217
Disabling the server


Location: Tools > Server Actions >
Server Actions
Select server action: Force disable server
Submit

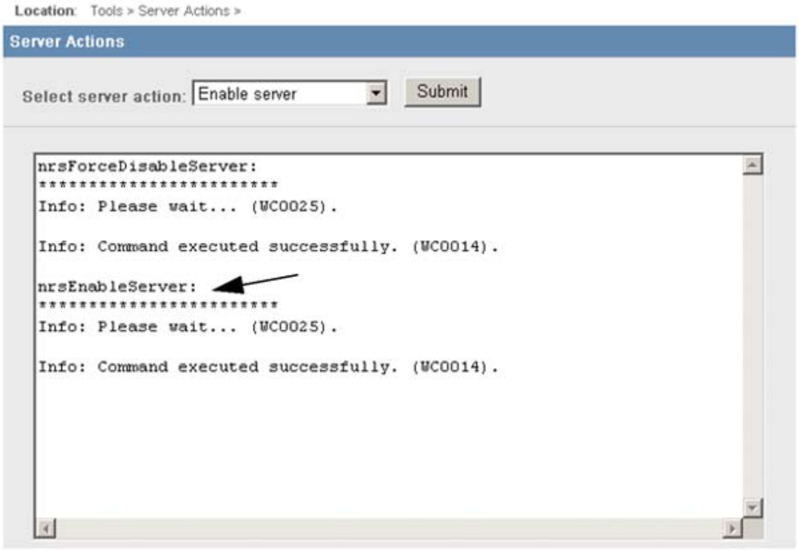
```
nrsForceDisableServer:
************************
Info: Please wait... (WC0025).

Info: Command executed successfully. (WC0014).
```

—End—

Procedure 99
Enabling the NRS server

Step	Action
1	Click the **Tools** tab on the NRS Manager toolbar.
2	Click **Server Actions** in the navigator. The **Server Actions** web page opens.
3	Select **Enable server** from the **Select server action** drop-down list.
4	Click **Submit**. The nrsEnableServer command is issued. The results are written in the text area of the Server Actions web page, as shown in Figure 218 "Enabling the server" (page 349).

Figure 218
Enabling the server


Location: Tools > Server Actions >
Server Actions
Select server action: Enable server
Submit

```
nrsForceDisableServer:
************************
Info: Please wait... (WC0025).

Info: Command executed successfully. (WC0014).

nrsEnableServer:
************************
Info: Please wait... (WC0025).

Info: Command executed successfully. (WC0014).
```

—End—

Performing NRS database actions

The NRS database has two schemas — an active schema and a standby schema

- The active database is used for runtime queries.
- The standby database is used to modify the configuration data. Changes can be made only to the standby database.

The following database commands can be performed using NRS Manager:

- **Cut over** — Swaps the active and standby databases by interchanging the active and standby database access pointers. The active and standby databases must be swapped before configuration changes can take effect. See Step 4 in Figure 74 from IP Peer NTP.
- **Commit** — Copies data *from* the active database *to* the standby database. Synchronizes the standby database with the active database. Overwrites the previous configuration data with the new configuration data. See Step 6 in Figure 75 from IP Peer NTP.
- **Revert** — After a Cut over, a revert interchanges the active and standby database access pointers. The active and standby databases are swapped. See Step 6 in Figure 74 from IP Peer NTP.

- **Roll back** — Before a Commit, a roll back undoes changes made to the standby database. A Roll Back copies data *from* the active database *to* the standby database. As a result, any changes made during the latest provisioning to the standby database are erased. The standby database is synchronized with the active database. This operation is available after a Cut over and before a Commit. See Step 4 in Figure 77 from IP Peer NTP.
- **Cut over and Commit** — The active and standby databases are swapped and synchronized with the new data configuration in a single step. The Standby database can not Roll back to a previous data configuration after a Cut over and Commit. See Step 4 in Figure 77 from IP Peer NTP.

  Note: Only users with administrator privileges can execute the database action commands.

For more information, refer to "Database synchronization/operation component" (page 42).

Database commands are executed from the **DB Actions** web page. The database has three states: Committed, Switched Over and Changed. The current database status is displayed in the title of the **DB Actions** web page as shown in Figure 219 "Database State: Changed" (page 351). Depending on the database status, some commands may not be in the **Select database action** drop-down list.

For example:

- If the database is in the **Committed** state, no commands are available.
- If the database is in the **Switched Over** state, the available commands in the **Select database action** drop-down list are Commit, Revert, and Roll back.
- If the database is in the **Changed** state, the available commands in the **Select database action** drop-down list are Cut over, Roll back, and Cut over & Commit.

For information about database commands, refer to "Database synchronization/operation component" (page 42).

To perform a:

- database cut over, see Procedure 100 "Cutting over the database" (page 351)
- database revert, see Procedure 101 "Reverting the database changes" (page 352)
- database commit, see Procedure 103 "Committing the database" (page 354)

- database cut over and commit, see Procedure 104 "Cutting over and committing changes to the database" (page 356)
- database roll back, see Procedure 102 "Rolling back changes to the database" (page 353)

Performing a database cut over

Cutting over a database switches the active and standby database access pointer. This swaps the primary and standby databases, so configuration changes take effect.

To perform a database cut over, follow the steps in Procedure 100 "Cutting over the database" (page 351).

Procedure 100
Cutting over the database

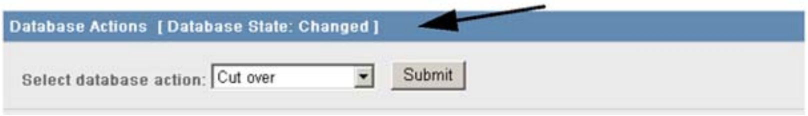
Step Action

1 Click the **Tools** tab on the NRS Manager toolbar.

2 Click **Database Actions** in the navigator.

The **Database Actions** web page opens. The database is in the Changed states, as shown in Figure 219 "Database State: Changed" (page 351).

Figure 219
Database State: Changed



Database Actions [Database State: Changed]

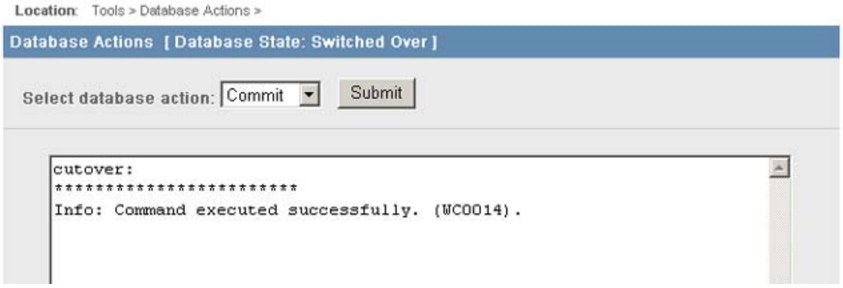
Select database action: Cut over

3 Select **Cut over** from the **Select database action** drop-down list.

4 Click **Submit**.

The Cut over command is issued, and the database is placed into a Switched Over state. Text is written in the text area of the Database Actions web page indicating that the Cut over command executed successfully, as shown in Figure 220 "Database Actions Cut over" (page 352).

Figure 220
Database Actions Cut over


Location: Tools > Database Actions >
Database Actions [Database State: Switched Over]
Submit

Select database action: Commit

```
cutover:
************************
Info: Command executed successfully. (WC0014).
```

5 To save the changes after the cut over, perform a Commit (see Procedure 103 "Committing the database" (page 354)). If you do not want to save the changes to the database, perform a Revert (see Procedure 101 "Reverting the database changes" (page 352)) or Roll back (see Procedure 102 "Rolling back changes to the database" (page 353)).

—End—

Reverting the database changes

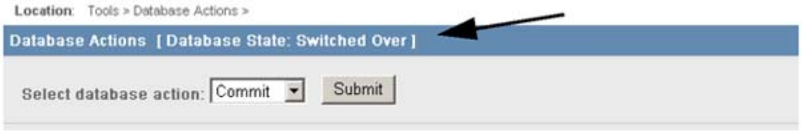
After a database Cut over, the Revert command interchanges the active and standby database access pointers. The active and standby databases are swapped.

To interchange the active and standby database access pointers, follow the steps inProcedure 101 "Reverting the database changes" (page 352).

Procedure 101
Reverting the database changes

Step	Action
1	Click the **Tools** tab on the NRS Manager toolbar.
2	Click **Database Actions** in the navigator. The **Database Actions** web pages opens. The database is in Switched Over state, as shown in Figure 221 "Database State: Switched Over" (page 352).

Figure 221
Database State: Switched Over


Location: Tools > Database Actions >
Database Actions [Database State: Switched Over]
Submit

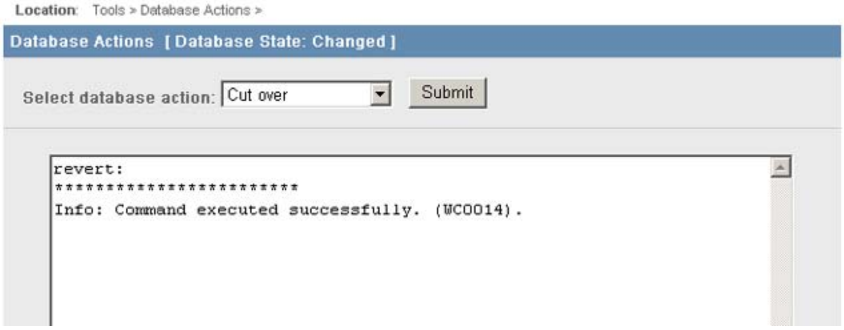
Select database action: Commit

3 Select **Revert** from the **Select database action** drop-down list.

4 Click **Submit**.

The Revert command is issued, and the database is placed into a Changed state. Text is written in the text area of the Database Actions web page indicating that the Revert command executed successfully, as shown in Figure 222 "Database Actions revert" (page 353)).

Figure 222
Database Actions revert


Location: Tools > Database Actions >
Database Actions [Database State: Changed]
Select database action: Cut over
Submit

```
revert:
************************
Info: Command executed successfully. (WC0014).
```

—End—

Performing database rollback

The Roll back command copies the active database to the standby database. As a result, any changes made during the latest provisioning to the standby database are erased. The standby database is synchronized with the active database. The Roll back command is available if the database is in the Changed or Switched Over state.

To roll back changes made to the standby database, perform Procedure 102 "Rolling back changes to the database" (page 353).

Procedure 102
Rolling back changes to the database

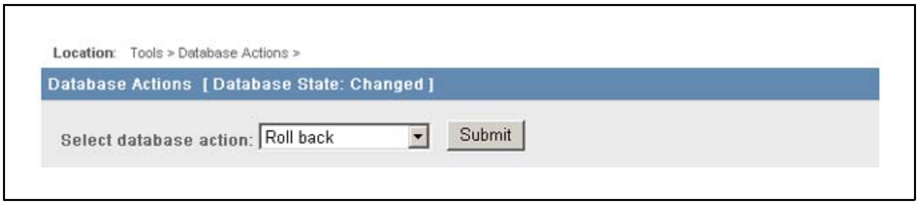
Step Action

1 Click the **Tools** tab on the NRS Manager toolbar.

2 Click **Database Actions** in the navigator.

The Database Actions web page opens. The database is in the Changed state, as shown in Figure 223 "Database Actions Roll back" (page 354)

Figure 223
Database Actions Roll back



Location: Tools > Database Actions >

Database Actions [Database State: Changed]

Select database action: Roll back

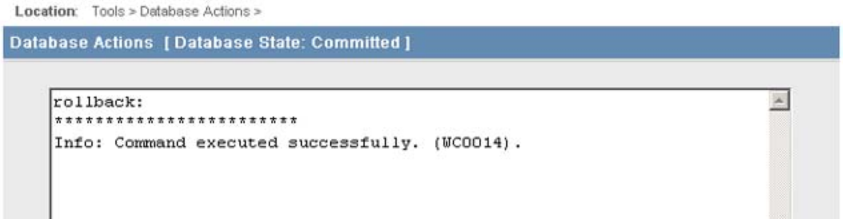
3 Select **Roll back** from the Select **database action** drop-down list.

4 Click **Submit**.

The Roll back command is issued, and the database is placed into a Committed state. Text is written in the text area of the Database Actions web page indicating that the Roll back command executed successfully, as shown in Figure 224 "Database Actions Roll back (successful)" (page 354)).

The **Select database action** drop-down list is also removed from the web page.

Figure 224
Database Actions Roll back (successful)



Location: Tools > Database Actions >

Database Actions [Database State: Committed]

```
rollback:
*************************
Info: Command executed successfully. (WC0014).
```

—End—

Committing the database changes

After Cut over, the Commit command copies data *from* the active database *to* the standby database. The previous configuration data is overwritten with the new configuration data. The standby database is synchronized with the active database.

To perform a database commit, follow the steps in Procedure 103 "Committing the database" (page 354).

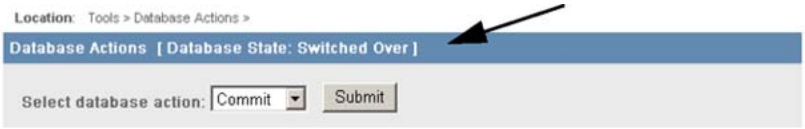
Procedure 103
Committing the database

Step	Action
1	Click the **Tools** tab on the NRS Manager toolbar.

2 Click **Database Actions** in the navigator.

The **Database Actions** web page opens. The database is in Switched Over state, as shown in Figure 225 "Database State: Switched Over" (page 355).

Figure 225
Database State: Switched Over



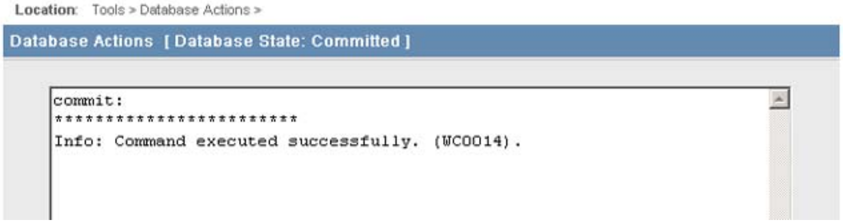
Location: Tools > Database Actions >
Database Actions [Database State: Switched Over]
Select database action: Commit
Submit

3 Select **Commit** from the **Select database action** drop-down list.

4 Click **Submit**.

The Commit command is issued, and the database is placed into a Committed state. Text is written in the text area of the Database Actions web page indicating that the Commit command executed successfully, as shown in Figure 226 "Database Actions Commit" (page 355)).

Figure 226
Database Actions Commit



Location: Tools > Database Actions >
Database Actions [Database State: Committed]

```
commit:
************************
Info: Command executed successfully. (WC0014).
```

—End—

Saving changes to the database with a single-step cutover and commit

After the service domain, L1 domains, L0 domains, gateway endpoints, and routing entries are configured and tested, the changes must be saved to the database. The changes can be saved in a single step using the **Cut over & Commit** command.

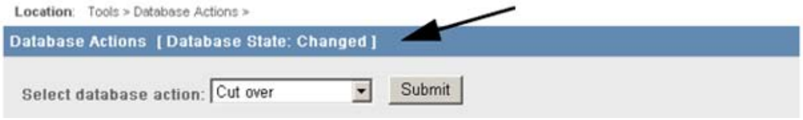
To perform a single-step cut over and commit, follow the steps in Procedure 104 "Cutting over and committing changes to the database" (page 356).

Procedure 104
Cutting over and committing changes to the database

Step	Action
1	Click the **Tools** tab on the NRS Manager toolbar.
2	Click **Database Actions** in the navigator.

The **Database Action** web page opens. The database is in the changed state, as shown in Figure 227 "Database State: Changed" (page 356).

Figure 227
Database State: Changed

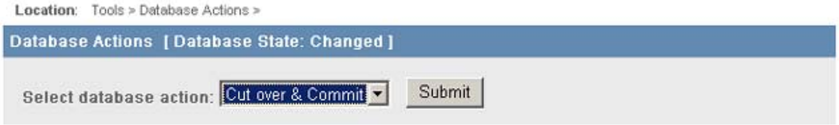


Location: Tools > Database Actions >
Database Actions [Database State: Changed]
Submit

Select database action: Cut over

3 Select **Cut over & Commit** from the **Select database action** drop-down list, as shown in Figure 228 "Database Actions Cut over and Commit" (page 356).

Figure 228
Database Actions Cut over and Commit



Location: Tools > Database Actions >
Database Actions [Database State: Changed]
Submit

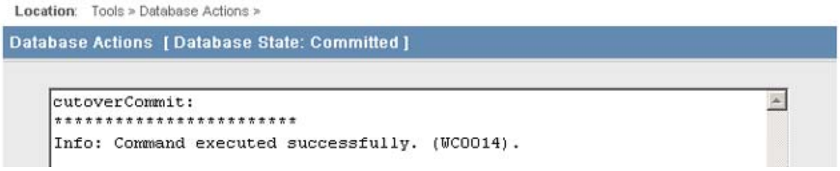
Select database action: Cut over & Commit

4 Click **Submit**.

The Cut over & Commit command is issued, and the database is placed into a Committed state. Text is written in the text area of the Database Actions web page indicating that the Cut over & Commit command executed successfully, as shown in Figure 229 "Database Actions Cut over and Commit (successful)" (page 356).

The **Select database action** drop-down list is also removed from the web page.

Figure 229
Database Actions Cut over and Commit (successful)



Location: Tools > Database Actions >
Database Actions [Database State: Committed]

```
cutoverCommit:
************************
Info: Command executed successfully. (WC0014).
```

—End—

Backing up the database

NRS Manager provides a facility for backing up the NRS database.

The database can be automatically backed up or manually backed up.

- The **automatic backup** option allows you to configure the backup time and location using **system-wide settings**. See Procedure 78 "Configuring system-wide settings" (page 300)
- The **manual backup** option allows you to immediately back up the database.

  Note: Only users with administrator privileges can execute the database backup commands.

Procedure 105
Automatically backing up the database

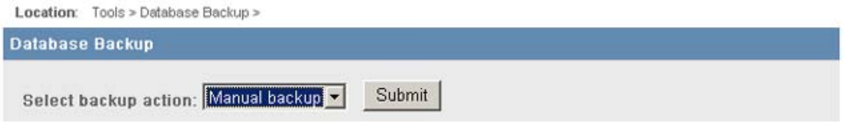
Step Action

1 Click the **Tools** tab on the NRS Manager toolbar.

2 Click **Database Backup** in the navigator.

The **Database Backup** web page opens, as shown in Figure 230 "Database Backup web page" (page 357).

Figure 230
Database Backup web page



Location: Tools > Database Backup >

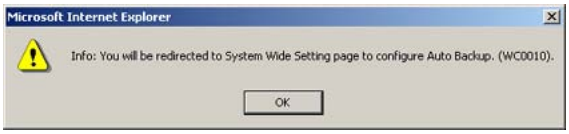
Database Backup

Select backup action: Manual backup

3 Select **Auto backup** from the **Select backup action** drop-down list.

A dialog box opens indicating that you will be redirected to the **System Wide Settings** web page (see Figure 231 "Automatically back up the database - redirection to System Wide Settings" (page 357)).

Figure 231
Automatically back up the database - redirection to System Wide Settings



Microsoft Internet Explorer

Info: You will be redirected to System Wide Setting page to configure Auto Backup. (WC0010).

4 Click **OK**.

The **System Wide Settings** web page opens (see Figure 168 "System Wide Settings" (page 300)).

5 Perform the following steps from Procedure 78 "Configuring system-wide settings" (page 300):

- step 7
- step 8
- step 9

—End—

Procedure 106
Manually backing up the database

Step Action

1 Click the **Tools** tab on the NRS Manager toolbar.

2 Click **Database Backup** in the navigator.

The Database Backup web page opens, as shown in Figure 230 "Database Backup web page" (page 357). **Manual backup** is automatically selected in the **Select backup action** drop-down list.

3 Click **Submit**.

A summary of the manual backup is displayed in the text area of the Database Backup web page, as shown in Figure 232 "Manual back up." (page 359)).

Two links appear on the screen:

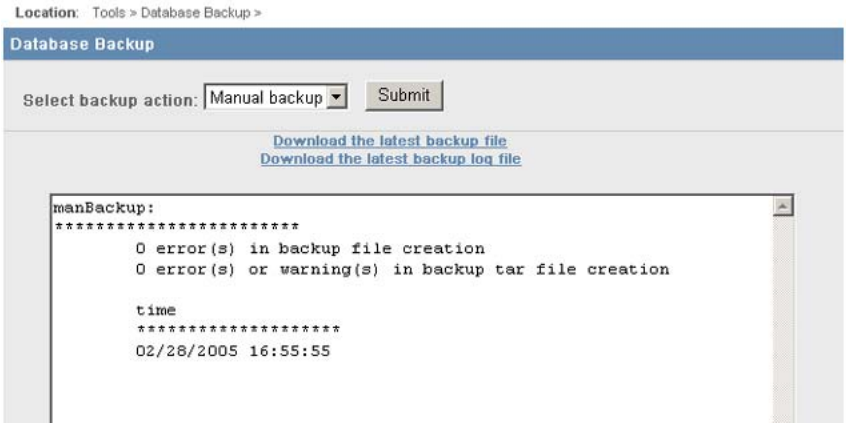
- **Download the latest backup file**

  (To download the latest backup file, follow Procedure 107 "Downloading the latest backup file" (page 359)).

- **Download the latest backup log file**

  (To download the latest backup log file, follow Procedure 108 "Downloading the latest backup log file" (page 360)).

Figure 232
Manual back up.


Location: Tools > Database Backup >
Database Backup
Select backup action:
Manual backup
Submit
Download the latest backup file
Download the latest backup log file

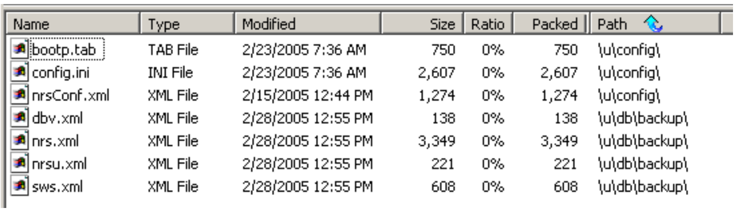
```
manBackup:
************************
        0 error(s) in backup file creation
        0 error(s) or warning(s) in backup tar file creation

        time
        ********************
        02/28/2005 16:55:55
```

—End—

Procedure 107
Downloading the latest backup file

Step	Action
1	Follow the steps in Procedure 106 "Manually backing up the database" (page 358)
2	Click the **Download the latest backup file** link on the **Database Backup** web page. (See Figure 232 "Manual back up." (page 359)). The **File Download** dialog box opens. The **File Download** dialog box provides the option to view the latest backup file or download and save the latest backup file to the user's local client (PC).
3	Click **Open** to view the latest backup file or click **Save** to save the file to a local client. The file is a compressed file that contains multiple backup files. The name of the compressed file is nrsback.tar (see Figure 233 "NRS backup files" (page 360)).

Figure 233
NRS backup files



Name	Type	Modified	Size	Ratio	Packed	Path
bootp.tab	TAB File	2/23/2005 7:36 AM	750	0%	750	\u\config\
config.ini	INI File	2/23/2005 7:36 AM	2,607	0%	2,607	\u\config\
nrsConf.xml	XML File	2/15/2005 12:44 PM	1,274	0%	1,274	\u\config\
dbv.xml	XML File	2/28/2005 12:55 PM	138	0%	138	\u\db\backup\
nrs.xml	XML File	2/28/2005 12:55 PM	3,349	0%	3,349	\u\db\backup\
nrsu.xml	XML File	2/28/2005 12:55 PM	221	0%	221	\u\db\backup\
sws.xml	XML File	2/28/2005 12:55 PM	608	0%	608	\u\db\backup\

—End—

Procedure 108
Downloading the latest backup log file

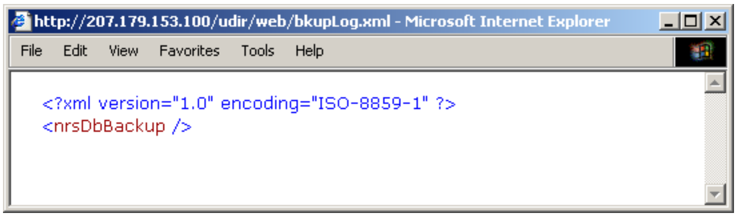
Step Action

1 Follow the steps in Procedure 106 "Manually backing up the database" (page 358)

2 Click **Download the latest backup log file** link on the **Database Backup** web page. (See Figure 232 "Manual back up." (page 359)).

A window opens containing the latest backup log file, as shown in Figure 234 "Backup log file" (page 360). The name of the log file is bkLog.xml. The bkLog.xml file contains information about the backup. For example, if there were errors during the back up process.

Figure 234
Backup log file


http://207.179.153.100/udir/web/bkupLog.xml - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<nrsDbBackup />
```

3 The backup log file can be saved using the **File > Save As...** menu option.

—End—

Restoring the database

NRS Manager provides the option to select a restore source to complete the database restore action. Restore sources include:

- From the connected Signaling Server
- From an FTP site
- From the client machine

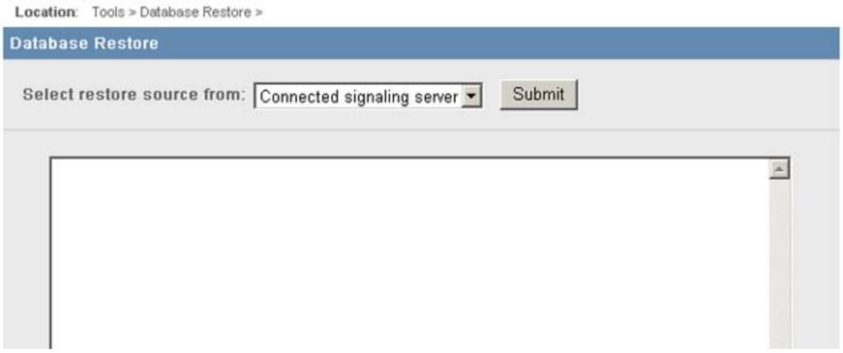
Note: Only users with administrator privileges can execute the database restore commands.

Procedure 109
Restoring the database

Step	Action
1	Click the **Tools** tab on the NRS Manager toolbar.
2	Click **Database Restore** in the navigator.

The **Database Restore** web page opens, as shown in Figure 235 "Database Restore web page" (page 361).

Figure 235
Database Restore web page



Location: Tools > Database Restore >
Database Restore
Select restore source from: Connected signaling server
Submit

The database can be restored from three source locations:

- From the **Connected Signaling Server**
  (To restore the database from the Connected Signaling Server, follow Procedure 110 "Restoring from the connected Signaling Server" (page 362)).
- From an **FTP site**
  (To restore the database from an FTP site, follow Procedure 111 "Restoring from an FTP site" (page 363)).
- From the **Client machine**
  (To restore the database from the Client machine, follow Procedure 112 "Restoring from a client machine" (page 364)).

—End—

Procedure 110
Restoring from the connected Signaling Server

Step	Action

1 Follow the steps in Procedure 109 "Restoring the database" (page 361)

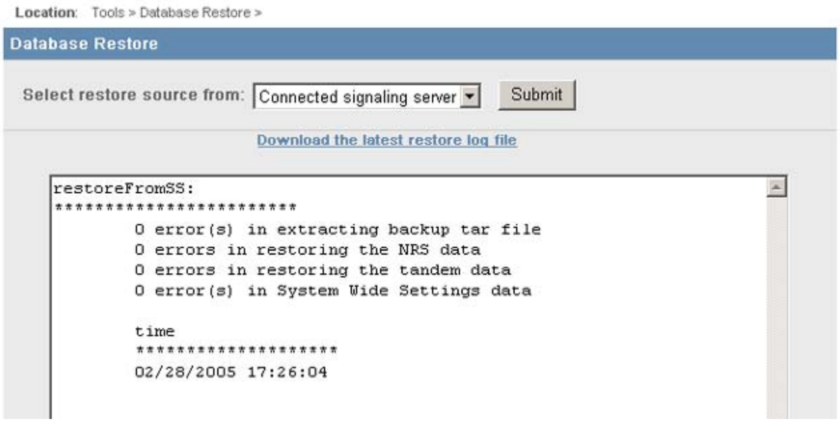
2 Select **Connected Signaling Server** from the **Select restore source from** drop-down list. (See Figure 235 "Database Restore web page" (page 361)).

3 Click **Submit**.

A message displays in the text area of the Database Restore web page showing a summary of the database restore from the Signaling Server. (See Figure 236 "Database Restore - from connected Signaling Server" (page 362)).

The **Download the latest restore log file** link also appears on the web page. See Procedure 113 "Downloading the latest restore log file" (page 365) for downloading the restore log file.

Figure 236
Database Restore - from connected Signaling Server


Location: Tools > Database Restore >
Database Restore
Submit
Download the latest restore log file

Select restore source from: Connected signaling server

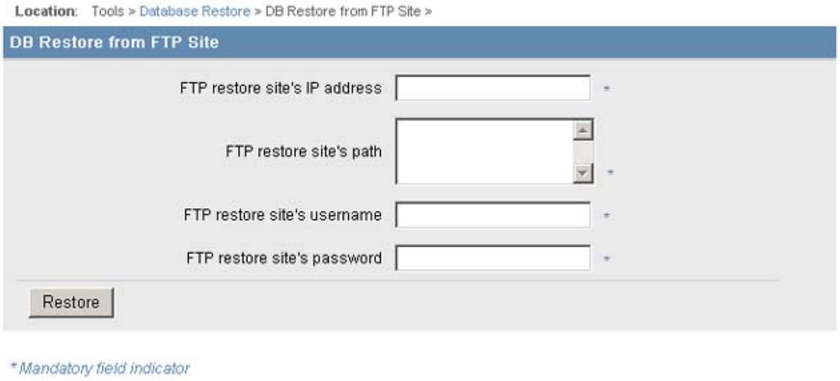
```
restoreFromSS:
*************************
        0 error(s) in extracting backup tar file
        0 errors in restoring the NRS data
        0 errors in restoring the tandem data
        0 error(s) in System Wide Settings data

        time
        *********************
        02/28/2005 17:26:04
```

—End—

Procedure 111
Restoring from an FTP site

Step	Action
1	Follow the steps in Procedure 109 "Restoring the database" (page 361)
2	Select **FTP site** from the **Select restore source from** drop-down list (see Figure 235 "Database Restore web page" (page 361)). The **DB Restore from FTP Site** web page opens (see Figure 237 "Database Restore - from FTP site" (page 363)). a. Enter the **FTP restore site's IP address** in the text box. b. Enter the **FTP restore site's path** in the text box. c. Enter the **FTP restore site's username** in the text box. d. Enter the **FTP restore site's password** in the text box.

Figure 237
Database Restore - from FTP site



Location: Tools > Database Restore > DB Restore from FTP Site >

DB Restore from FTP Site

FTP restore site's IP address *

FTP restore site's path *

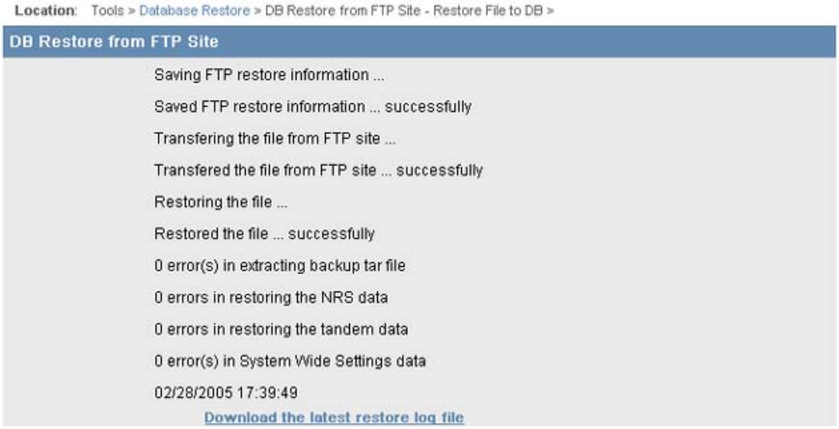
FTP restore site's username *

FTP restore site's password *

* Mandatory field indicator

Step	Action
3	Click **Restore**. A message is displayed in the text area of the DB Restore from FTP Site web page, showing a summary of the database restore from the FTP site. See Figure 238 "Database Restore - from FTP site - results" (page 364). The **Download the latest restore log file** link also appears on the web page. See Procedure 113 "Downloading the latest restore log file" (page 365) for downloading the restore log file.

Figure 238
Database Restore - from FTP site - results



Location: Tools > Database Restore > DB Restore from FTP Site - Restore File to DB >

DB Restore from FTP Site

```
Saving FTP restore information ...
Saved FTP restore information ... successfully
Transfering the file from FTP site ...
Transfered the file from FTP site ... successfully
Restoring the file ...
Restored the file ... successfully
0 error(s) in extracting backup tar file
0 errors in restoring the NRS data
0 errors in restoring the tandem data
0 error(s) in System Wide Settings data
02/28/2005 17:39:49
```

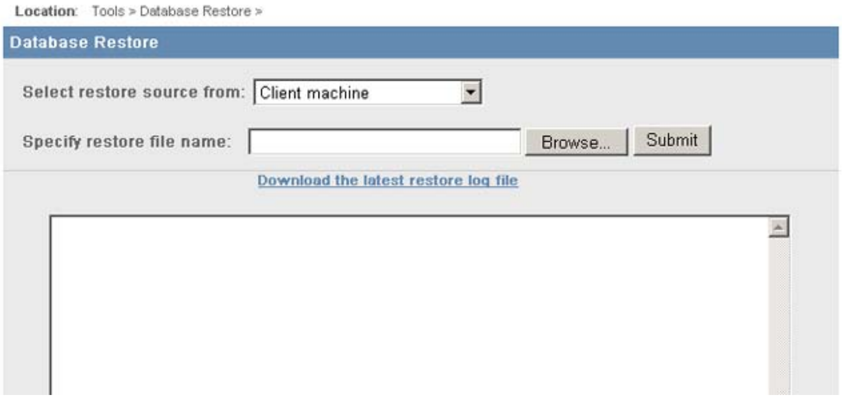
—End—

Procedure 112
Restoring from a client machine

Step	Action
1	Follow the steps in Procedure 109 "Restoring the database" (page 361)
2	Select **Client machine** from the **Select restore source from** drop-down list (see Figure 235 "Database Restore web page" (page 361)).

The **Database Restore** web page opens, as shown in Figure 239 "Database Restore - from client machine" (page 364). The web page contains a **Specify restore file name** text box and a **Browse** button.

Figure 239
Database Restore - from client machine



Location: Tools > Database Restore >

Database Restore

Select restore source from: Client machine

Specify restore file name:

3 Click **Browse** to navigate to the folder containing the backup file.

The **Choose file** dialog window opens.

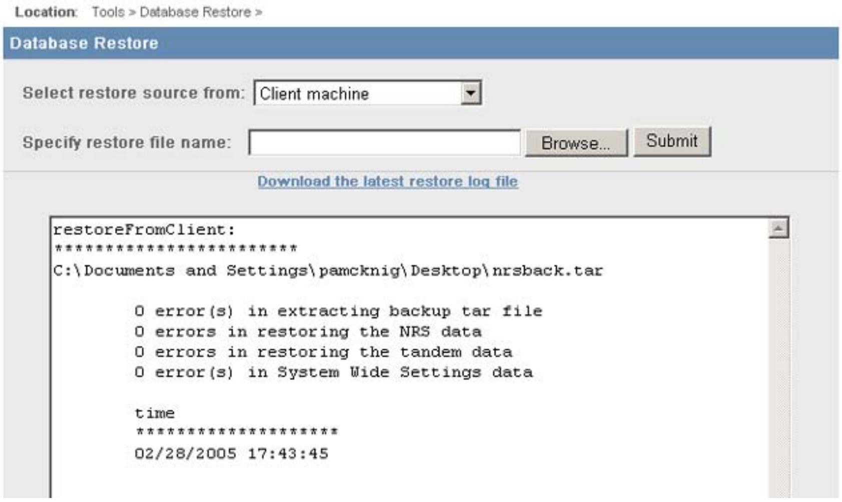
4 Select the backup file, and click **OK**.

The **Specify restore file name** text box auto-fills with the path and filename of the backup file.

5 Click **Submit**.

A message is displayed in the text area of the Database Restore window showing a summary of the database restore from the client machine. See Figure 240 "Database Restore - client machine - results" (page 365).

Figure 240
Database Restore - client machine - results


Location: Tools > Database Restore >
Database Restore
Browse...
Submit
Download the latest restore log file

Select restore source from: Client machine

Specify restore file name:

```
restoreFromClient:
*************************
C:\Documents and Settings\pamcknig\Desktop\nrsback.tar

        0 error(s) in extracting backup tar file
        0 errors in restoring the NRS data
        0 errors in restoring the tandem data
        0 error(s) in System Wide Settings data

        time
        ********************
        02/28/2005 17:43:45
```

The **Download the latest restore log file** link also appears on the web page. See Procedure 113 "Downloading the latest restore log file" (page 365) for downloading the restore log file.

—End—

Procedure 113
Downloading the latest restore log file

Step **Action**

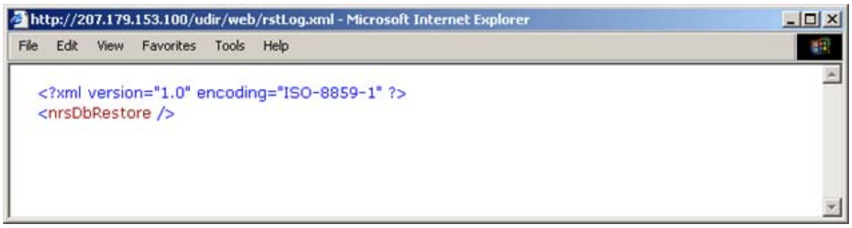
1 NRS Manager provides the option to restore the database from three source locations:

- Follow Procedure 110 "Restoring from the connected Signaling Server" (page 362) to restore the database from the **Connected Signaling Server**
- Follow Procedure 111 "Restoring from an FTP site" (page 363) to restore the database from an **FTP site**
- Follow Procedure 112 "Restoring from a client machine" (page 364) to restore the database from the **Client machine**

2 Click the **Download the latest restore log file** link to view the Restore log file.

A window opens containing the latest restore log file, as shown inFigure 241 "Restore log file" (page 366). The name of the log file is rstLog.xml. The rstLog.xml file contains information about the database restore.

Figure 241
Restore log file



http://207.179.153.100/udir/web/rstLog.xml - Microsoft Internet Explorer
File Edit View Favorites Tools Help

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<nrsDbRestore />
```

3 The restore log file can be saved, using the **File > Save As...** menu option.

—End—

GK/NRS Data Upgrade

The **GK/NRS Data Upgrade** link on the Tools web page is used to upgrade a Succession 3.0 H.323 Gatekeeper to a CS 1000 Release 4.0 (or later) NRS. If required, this procedure must be completed as part of your upgrade procedures.

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

Migration overview

To migrate your system, you must convert the Succession 3.0 H.323 Gatekeeper database into a CS 1000 Release 4.0 (or later) NRS database. This involves the following tasks:

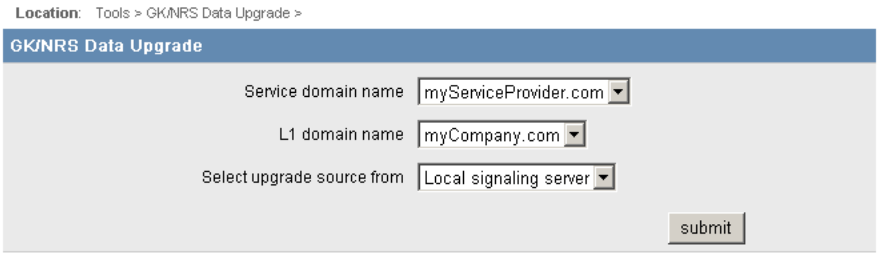
- backing up the Succession 3.0 H.323 Gatekeeper database using Element Manager
- verifying that the backup files (.tar file) exist
- upgrading the Signaling Server software from Succession 3.0 to CS 1000 Release 4.0 (or later)
- reconfiguring the Signaling Server
- creating a Service Domain and Level 1 domain using NRS Manager (These two domains do not exist in the Succession 3.0 Gatekeeper.)
- converting the H.323 Gatekeeper database to the CS 1000 Release 4.0 (or later) NRS database using NRS Manager
- performing a database Cut over and Commit

  The converted H.323 Gatekeeper database is stored in the NRS standby database. Changes made to the standby database do not immediately affect call processing. Before changes made to the standby database affect call processing, database Cut over and Commit commands must be executed. See "Performing NRS database actions" (page 349).

  Note: Only users with administrator privileges can execute Gatekeeper/NRS (GK/NRS) data conversion.

Figure 242 "GK/NRS Data Upgrade web page" (page 367) and Figure 243 "GK/NRS Data Upgrade - results" (page 368) are only for illustration purposes, to show the user interface for the Gatekeeper to NRS Upgrade area in NRS Manager.

Figure 242
GK/NRS Data Upgrade web page



Location: Tools > GK/NRS Data Upgrade >

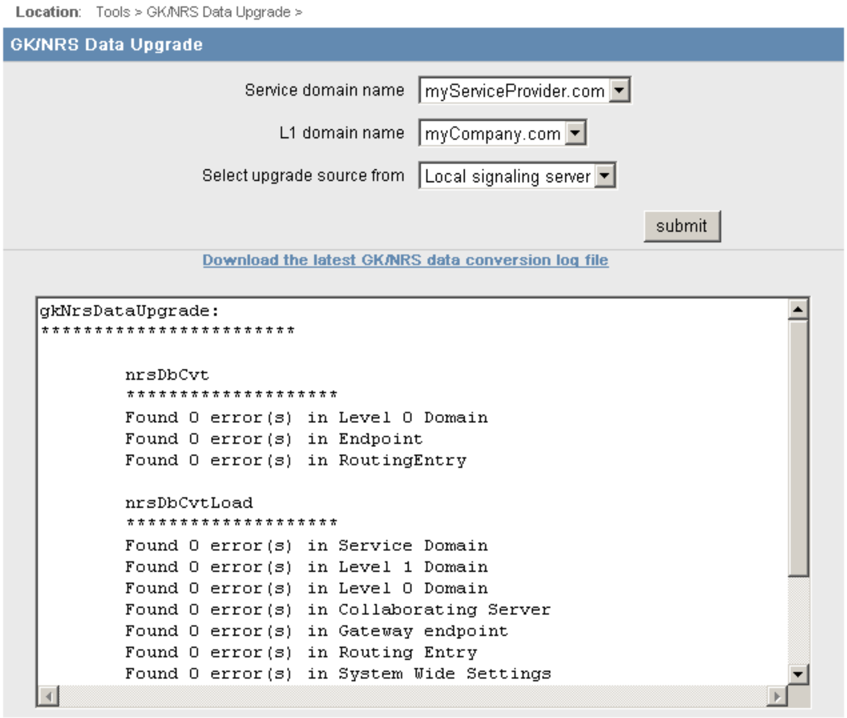
GK/NRS Data Upgrade

Service domain name: myServiceProvider.com

L1 domain name: myCompany.com

Select upgrade source from: Local signaling server

Figure 243
GK/NRS Data Upgrade - results


Location: Tools > GK/NRS Data Upgrade >
GK/NRS Data Upgrade
submit
Download the latest GK/NRS data conversion log file

Service domain name: mySeviceProvider.com
L1 domain name: myCompany.com
Select upgrade source from: Local signaling server

```
gkNrsDataUpgrade:
************************


        nrsDbCvt
        ********************
        Found 0 error(s) in Level 0 Domain
        Found 0 error(s) in Endpoint
        Found 0 error(s) in RoutingEntry

        nrsDbCvtLoad
        ********************
        Found 0 error(s) in Service Domain
        Found 0 error(s) in Level 1 Domain
        Found 0 error(s) in Level 0 Domain
        Found 0 error(s) in Collaborating Server
        Found 0 error(s) in Gateway endpoint
        Found 0 error(s) in Routing Entry
        Found 0 error(s) in System Wide Settings
```

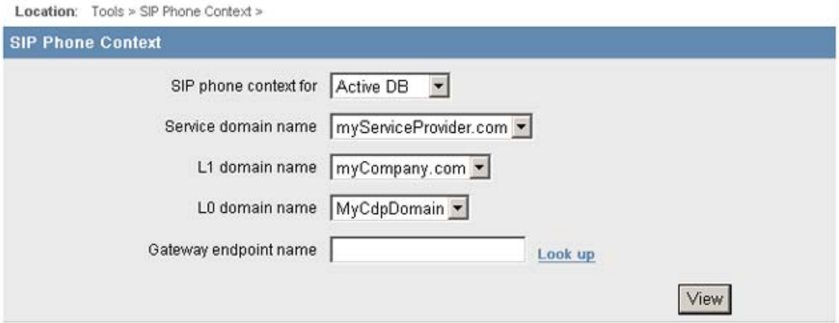
SIP Phone Context

The SIP Phone Context web page provides a view of SIP phone-context constructions under a configured Level 0 Domain or Gateway Endpoint.

Procedure 114
SIP Phone Context

Step	Action
1	Click the **Tools** tab on the NRS Manager toolbar.
2	Click **SIP Phone Context** in the navigator. The **SIP Phone Context** web page opens, as shown in Figure 244 "SIP Phone Context web page" (page 369).

Figure 244
SIP Phone Context web page



Location: Tools > SIP Phone Context >

SIP Phone Context

SIP phone context for: Active DB

Service domain name: myServiceProvider.com

L1 domain name: myCompany.com

L0 domain name: MyCdpDomain

Gateway endpoint name:

3 Select **Standby DB** or **Active DB** from the **SIP phone context for** drop-down list.

4 Select the **Service domain name** from the drop-down list.

5 Select the **L1 domain name** from the drop-down list.

6 Select the **L0 domain name** from the drop-down list.

7 If the selected **L0 domain name** has configured Gateway Endpoints, the **Look up** link appears beside the **Gateway endpoint name** text box.

The Gateway endpoint name field is optional.

- If you do not select a Gateway Endpoint name and click **View**, then the SIP Phone Context Mapping information is displayed based on L0 domain configuration (which also applies to the User Endpoint configuration).
- If you select a Gateway Endpoint name and click **View**, then the SIP Phone Context Mapping information is displayed based on Gateway Endpoint configuration.

8 To select a Gateway Endpoint name, click the **Look up** link to open the **Look up path for gateway endpoints** web page.

The **Look up** utility allows you to search for Gateway Endpoints in two ways: **Page-by-Page** and **Name prefix**. (See Procedure 97 "Performing a SIP Routing Test" (page 344))

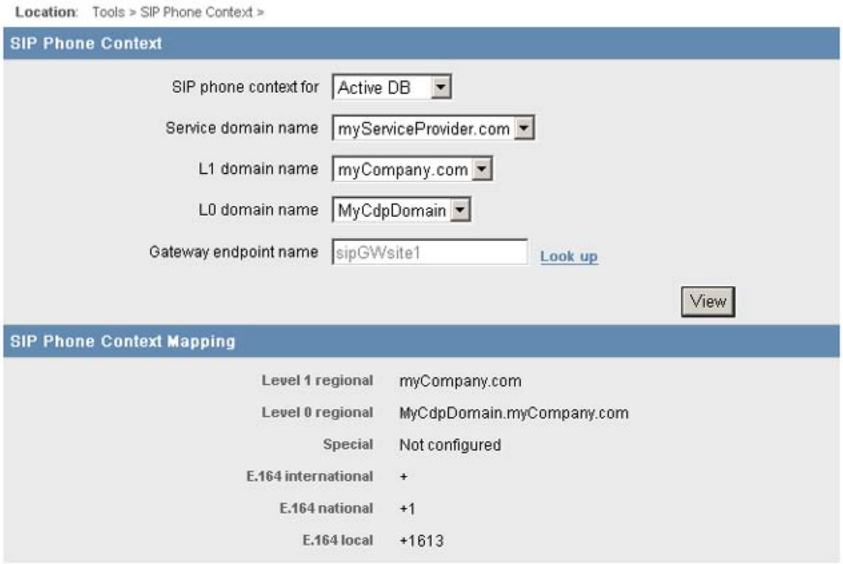
Click a **link** in the **ID** column of the **Lookup path for Gateway endpoints** web page and the **Gateway endpoint name** text box auto-fills with the selected Gateway Endpoint.

You cannot enter an endpoint name directly in the **Gateway endpoint name** text box.

9 Click **View**.

The SIP Phone Context web page expands to display the**SIP Phone Context Mapping** area, as shown in Figure 245 "SIP Phone Context Mapping" (page 370).

Figure 245
SIP Phone Context Mapping



Location: Tools > SIP Phone Context >

SIP Phone Context

SIP phone context for: Active DB
Service domain name: myServiceProvider.com
L1 domain name: myCompany.com
L0 domain name: MyCdpDomain
Gateway endpoint name: sipGWsite1

SIP Phone Context Mapping

Level 1 regional	myCompany.com
Level 0 regional	MyCdpDomain.myCompany.com
Special	Not configured
E.164 international	+
E.164 national	+1
E.164 local	+1613

—End—

SSL/TLS Configuration

The SSL/TLS Configuration utility in NRS Manager configures the SSL/TLS certificate to enforce system security. Refer to *Element Manager: System Administration (553-3001-332)* for information on this function.

Reports tab

Viewing the database reports

NRS Manager provides three database reports. The report types are:

- Last database synchronization for the Alternate NRS
- Last database synchronization for the Failsafe NRS
- Current database status

Note: Alternate and Failsafe NRS servers must exist for Procedure 115 "Viewing the last database synchronization for the Alternate or Failsafe NRS" (page 371) and Procedure 116 "Viewing the current database status" (page 372).

Last database synchronization

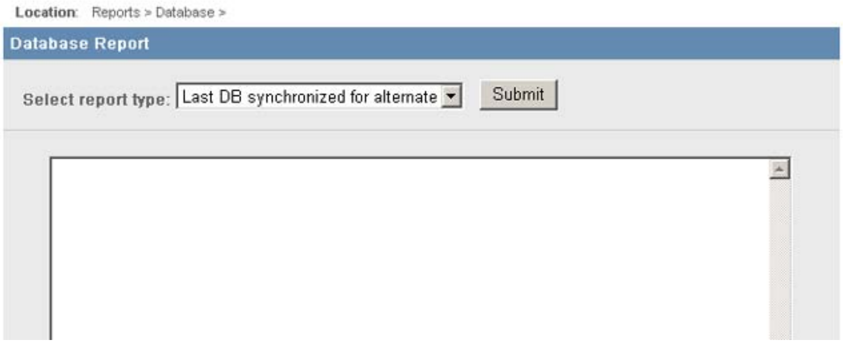
Follow Procedure 115 "Viewing the last database synchronization for the Alternate or Failsafe NRS" (page 371) to view the last database synchronization.

Procedure 115

Viewing the last database synchronization for the Alternate or Failsafe NRS

Step	Action
1	Click the **Reports** tab on the NRS Manager toolbar. The **Database Report** web page opens, as shown in Figure 246 "Last DB synchronized" (page 371)
2	Select **Last DB synchronized for alternate** or **Last DB synchronized for failsafe** from the **Select report type** drop-down list.

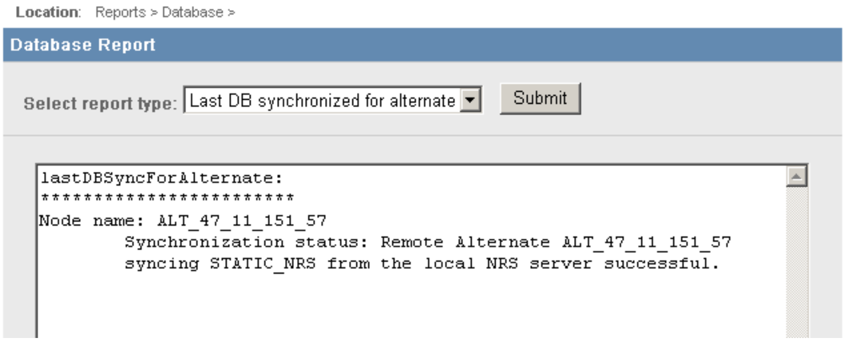
Figure 246
Last DB synchronized



Select report type: Last DB synchronized for alternate

Step	Action
3	Click **Submit**. Figure 247 "Last DB synchronized for Alternate - results" (page 371) shows the results of the last database synchronization for the Alternate NRS.

Figure 247
Last DB synchronized for Alternate - results



Select report type: Last DB synchronized for alternate

```
lastDBSyncForAlternate:
************************
Node name: ALT_47_11_151_57
        Synchronization status: Remote Alternate ALT_47_11_151_57
        syncing STATIC_NRS from the local NRS server successful.
```

—End—

Current database status

Follow Procedure 116 "Viewing the current database status" (page 372) to view the current database status.

Procedure 116
Viewing the current database status

Step	Action

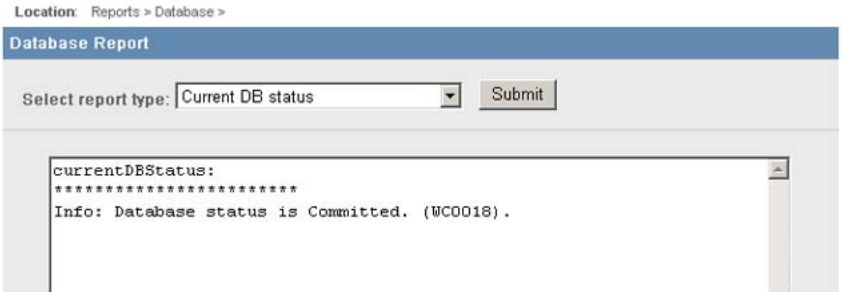
1 Click the **Reports** tab on the NRS Manager toolbar.

The **Database Report** web page opens, as shown in Figure 246 "Last DB synchronized" (page 371).

2 Select **Current DB status** from the **Select report type** drop-down list.

3 Click **Submit**.

Figure 248
Viewing the current database status



Select report type: Current DB status

```
currentDBStatus:
************************
Info: Database status is Committed. (WC0018).
```

There are three database states:

- **Changed** — The configuration data in the standby database has been modified. The active and standby databases are not synchronized. See Step 3 in Figure 74 of IP Peer.
- **Switched Over** — A Cut over command has been executed after the configuration data in the standby database has been modified. The active and standby databases have been swapped by interchanging the active and standby database access pointers. The standby database is now unchanged and the active database contains the modified configuration data. The active and standby databases are not synchronized. See Step 5 in Figure 74 of IP Peer.

- **Committed** — A Commit or Rollback command has been executed after the configuration data in the standby database has been modified. The active and standby databases are synchronized. See Step 7 in Figure 75 of IP Peer, or Step 5 in Figure 76 or Step 5 in Figure 77 in IP Peer.

—End—

Administration tab

Configuring and administering users

Open the **Users** web page to administer, configure, and view users. Click the **Administration** tab on the NRS Manager toolbar to open the Users web page.

NRS Manager supports two types of access privileges:

- Administrative privileges — Administrators have full read/write privileges. An administrator can view and modify NRS configuration data.
- Monitor privileges — Monitors have read-only privileges. A monitor can only view the NRS configuration data.

An administrator can view, create, and modify the login names and passwords which are used for configuration and maintenance of the NRS.

If the currently logged-in user has administrator-level access, the user:

- can only change their own properties.
- cannot delete themselves
- cannot change their user access level

Another administrator account must be used to modify an administrator account.

> ***Note:*** Administrator-level users for an NRS running on a stand-alone Signaling Server can also be configured and managed using the CLI commands given in Stand-alone NRS CLI commands.

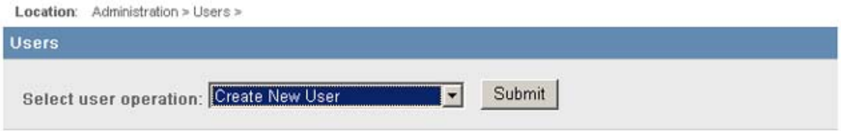
Creating new users

Follow the steps in Procedure 117 "Creating new users" (page 374) to create new users.

Procedure 117
Creating new users

Step	Action
1	Click the **Administration** tab on the NRS Manager toolbar. The **Users** web page opens, as shown in Figure 249 "Users web page" (page 374).
2	Select **Create New User** from the **Select user operation** drop-down list.

Figure 249
Users web page

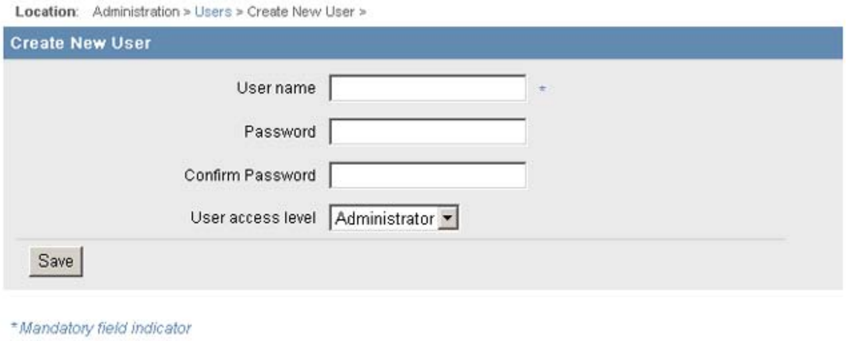


Location: Administration > Users >

Select user operation: Create New User

Step	Action
3	Click **Submit**. The **Create New User** web pages opens, as shown in Figure 250 "Create New User web page" (page 374).

Figure 250
Create New User web page



Location: Administration > Users > Create New User >

User name *

Password

Confirm Password

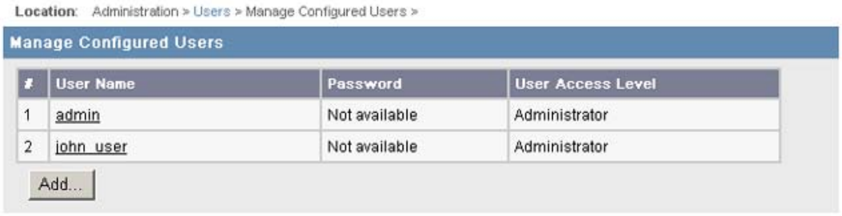
User access level: Administrator

*Mandatory field indicator

Step	Action
4	Enter a **User name** in the text box. The username is alphanumeric and can be up to 30 characters in length. The username cannot have spaces and the first character must be a letter.
5	Enter a **Password** in the text box. The password is alphanumeric and can be up to 24 characters in length.
6	Re-enter the password in the **Confirm Password** text box.
7	Select the access level of Administrator or Monitor from the **User access level** drop-down list.
8	Click **Save**.

The **Manage Configured Users** web page opens, as shown in Figure 251 "Manage Configured Users web page" (page 375).

Figure 251
Manage Configured Users web page



Location: Administration > Users > Manage Configured Users >

Manage Configured Users

#	User Name	Password	User Access Level
1	admin	Not available	Administrator
2	john_user	Not available	Administrator

—End—

Viewing configured users

Follow the steps in Procedure 118 "Viewing configured users" (page 375) to view configured users.

Procedure 118
Viewing configured users

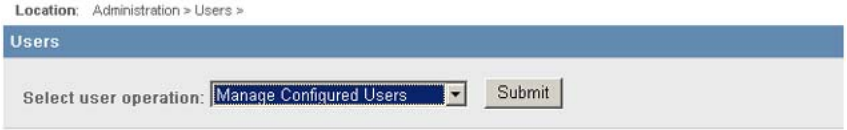
Step	Action

1 Click the **Administration** tab on the NRS Manager toolbar.

The Users web page opens, as shown in Figure 249 "Users web page" (page 374)

2 Select **Manage Configured Users** from the **Select user operation** drop-down list.

Figure 252
Users web page



Location: Administration > Users >

Users

Select user operation: Manage Configured Users

3 Click **Submit**.

The **Manage Configured Users** web pages opens. A list of configured users is displayed, as shown in Figure 251 "Manage Configured Users web page" (page 375).

> ***Note:*** You can create new users from the View Configured Users web pages by clicking **Add....** The Create New User web page opens, as shown in Figure 250 "Create New User web

page" (page 374). Follow the steps in Procedure 117 "Creating new users" (page 374) to configure the new user.

—End—

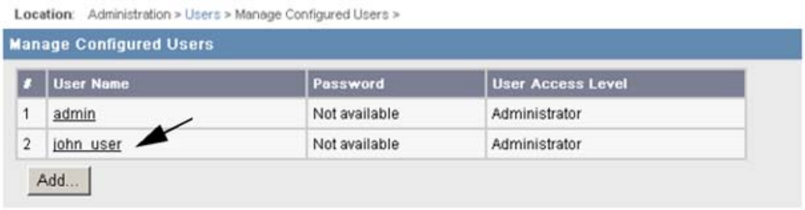
Editing or deleting configured users

Follow Procedure 119 "Editing or deleting configured users" (page 376) to edit a user’s username, password, or access level. Procedure 119 "Editing or deleting configured users" (page 376) can also be used to delete users.

Procedure 119
Editing or deleting configured users

Step	Action
1	Click the **Administration** tab on the NRS Manager toolbar. The **Users** web page opens, as shown in Figure 249 "Users web page" (page 374)
2	Select **Manage Configured Users** from the **Select user operation** drop-down list.
3	Click **Submit**. The **Manage Configured Users** web page opens, as shown in Manage Configured Users web page. A list of configured users is displayed.

Figure 253
Manage Configured Users web page



Location: Administration > Users > Manage Configured Users >

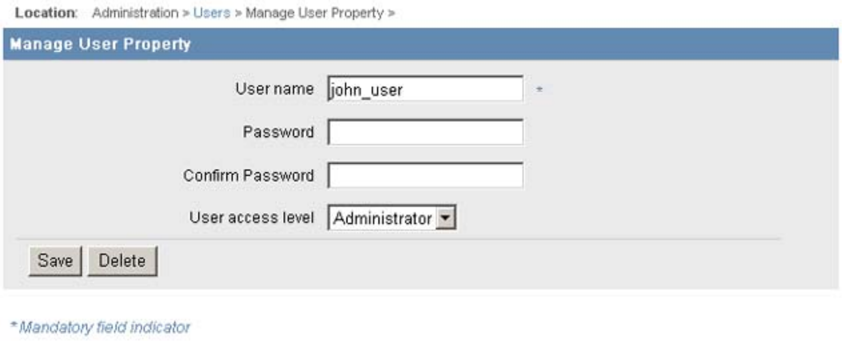
Manage Configured Users

#	User Name	Password	User Access Level
1	admin	Not available	Administrator
2	john_user	Not available	Administrator

4 Click a **link** in the **User Name** column.

The **Manage User Property** web page opens, as shown in Figure 254 "Manage User Property web page" (page 377). The web page includes two buttons: **Save** and **Delete**.

Figure 254
Manage User Property web page



Location: Administration > Users > Manage User Property >

Manage User Property

User name: john_user *

Password:

Confirm Password:

User access level: Administrator

* Mandatory field indicator

5 To edit the user’s **Password** enter a password in the text box. The password is alphanumeric and can be up to 30 characters in length.

Re-enter the password in the **Confirm Password** text box.

Select the access level of Administrator or Monitor from the **User access level** drop-down list.

> ***Note:*** The username cannot be changed. If you want to change a user’s username, delete the user and then recreate the user with the new username.

6 Click **Save**.

The **Manage Configured User** web page re-opens.

7 To delete a user, click **Delete**.

The **Manage Configured Users** web page re-opens and the user is no longer displayed in the list of configured users.

—End—

Changing your password

Follow Procedure 120 "Changing your password" (page 377) to change your password.

Procedure 120
Changing your password

Step	Action

1 Click the **Administration** tab on the NRS Manager toolbar.

The **Users** web page opens, as shown in Figure 252 "Users web page" (page 375)

2 Select **Manage Configured Users** from the **Select user operation** drop-down list.

3 Click **Submit**.

The **Manage Configured Users** web page opens, as shown in Manage Configured Users web page.

4 Click a **link** in the **User Name** column.

The **Manage user Property** web page opens, as shown in Figure 254 "Manage User Property web page" (page 377)

5 Enter a new password in the **Password** text box.

6 Re-enter your new password in the **Confirm Password** text box. The password is alphanumeric and can be up to 30 characters in length.

7 Click **Save**.

The **User** web page re-opens.

—End—

Accessing the NRS directly from the Signaling Server

The NRS can be accessed directly from the Signaling Server using a maintenance terminal. Follow the login procedure given in *Signaling Server: Installation and Configuration (553-3001-212)*.

Use the following login credentials:

- User ID: `admin`
- Password: `cseadmin` or `<current>`

  If you use the default password, you are prompted to change your password. If this is not your first login from the Signaling Server, and you have already changed your password, enter your new password (`<current>` above).

  Note: You cannot access NRS Manager from the Signaling Server using this access method.

After you have logged in, you can use the Signaling Server CLI commands listed in Command Line Interface commands. These commands include NRS-specific commands listed in NRS database CLI commands and Stand-alone NRS CLI commands.

Appendix Passthrough End User License Agreement

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

This section governs the use of the Red Hat Software and any updates to the Red Hat Software, regardless of the delivery mechanism and is governed by the laws of the state of New York in the U.S.A. The Red Hat Software is a collective work under U.S. Copyright Law. Subject to the following terms, Red Hat, Inc. ("Red Hat") grants to the user ("Customer") a license to this collective work pursuant to the GNU General Public License. Red Hat Enterprise Linux (the "Red Hat Software") is a modular operating system consisting of hundreds of software components. The end user license agreement for each component is located in the component's source code. With the exception of certain image files identified below, the license terms for the components permit Customer to copy, modify, and redistribute the component, in both source code and binary code forms. This agreement does not limit Customer's rights under, or grant Customer rights that supersede, the license terms of any particular component. The Red Hat Software and each of its components, including the source code, documentation, appearance, structure and organization are owned by Red Hat and others and are protected under copyright and other laws. Title to the Red Hat Software and any component, or to any copy, modification, or merged portion shall remain with the aforementioned, subject to the applicable license. The "Red Hat" trademark and the "Shadowman" logo are registered trademarks of Red Hat in the U.S. and other countries. This agreement does not permit Customer to distribute the Red Hat Software using Red Hat's trademarks. If Customer makes a commercial redistribution of the Red Hat Software, unless a separate agreement with Red Hat is executed or other permission granted, then Customer must modify any files identified as “REDHAT-LOGOS” and “anaconda-images” to remove all images containing the “Red Hat” trademark or the “Shadowman” logo. As required by U.S. law, Customer represents and warrants that it: (a) understands that the Software is subject to export controls under the U.S. Commerce Department’s Export Administration Regulations (“EAR”); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria); (c) will not export, re-export, or transfer the Software to any prohibited destination, entity, or individual without the necessary export license(s) or authorizations(s) from the U.S. Government; (d) will not use or transfer the Red Hat Software for use in any sensitive nuclear, chemical or biological weapons, or missile technology end-uses unless authorized by the U.S. Government by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Software to eligible end users, it will, as required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department’s Bureau of Industry & Security (BIS), which include the name and address (including country) of each transferee; and (f) understands that countries other than the United States may restrict the import, use, or export of encryption products and that it shall be solely responsible for compliance with any such import, use, or export restrictions. Red Hat may distribute third party software programs with the Red Hat Software that are not part of the Red Hat Software. These third party programs are subject to their own license terms. The license terms either accompany the programs or can be viewed at http://www.redhat.com/licenses/. If Customer does not agree to abide by the applicable license terms for such programs, then Customer may not install them. If Customer wishes to install the programs on more than one system or transfer the programs to another party, then Customer must contact the licensor of the programs. If any provision of this agreement is held to be unenforceable, that shall not affect the enforceability of the remaining provisions. Copyright © 2003 Red Hat, Inc. All rights reserved. "Red Hat" and the Red Hat "Shadowman" logo are registered trademarks of Red Hat, Inc. "Linux" is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners.

Nortel Communication Server 1000

Network Routing Service Installation and Commissioning

Publication: NN43001-564
Document status: Standard
Document version: 01.01
Document date: 30 May 2007

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

Sourced in Canada

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