Nortel Communication Server 1000

Network Routing Service Fundamentals

Release: 7.0
Document Revision: 02.01

www.nortel.com

NN43001-130

Nortel Communication Server 1000
Release: 7.0
Publication: NN43001-130
Document release date: 4 June 2010

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

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

All other trademarks are the property of their respective owners.

Contents

New in this Release 11

Redirect Server support on Linux-based NRS 11
Call processing capacity improvement 11
Same-cost routing 11
Source-based routing for Multimedia Convergence Manager 11
Service domain name can be configured as an IP Address in NRS Manager 12
Operation, Administration and Maintenance Transaction Audit and Security Event Logging 12
Access to NRS CLI command 12
Features 12
- IPv6 support 13
- Route cost modification 13
- Internal and external NRS for the High Scalability Solution 13
- Tertiary NRS server 13

Other 13
- Revision History 13
- Conventions 14

How to Get Help 17

Getting help from the Nortel web site 17
Getting help over the telephone from a Nortel Solutions Center 17
Getting help from a specialist by using an Express Routing Code 17
Getting help through a Nortel distributor or reseller 18

Network Routing Service overview 19

Contents 19
Introduction 21
Network protocol component 24
- Session Initiation Protocol 25
- SIP entities 25
- User agent 26
- SIP Proxy Server 26
- SIP Redirect Server 26
- SIP Registrar 26
- NRS SIP server implementation 26

Copyright © 2010 Nortel Networks. All Rights Reserved.

Back-to-Back User Agent 27
SIP domains 27
Location Service 27
NRS purpose 28
Signaling Gateways 28
SIP Gateway 29
SIP services 29
H.323 protocol 30
H.323 entities 30
H.323 terminal 30
H.323 Gatekeeper 30
Gatekeeper zones 31
H.323 Gateway 31
SIP and H.323 interworking 31
Network Connection Service 32
SIP NRS Privacy within a Trusted Network 32
Primary and Secondary NRS servers 32
Tertiary NRS server 33
Internal and external NRS for the High Scalability Solution 33
NRS Failsafe 33
Database component 35
NRS Database 35
Database synchronization and operation component 44
Synchronization of the active and standby databases on a Network Routing Server 46
NRS database redundancy 49
Source-based routing for Multimedia Convergence Manager 50
Same-cost routing 50
Feature interactions 51
Operation, Administration, and Maintenance Transaction Audit and Security Event Logging 52
Operation, Administration and Maintenance logging framework 52
Centralized Operation, Administration and Maintenance log storage and log file rotation 52
Log viewer interface 53
Support for an OSS Syslog server 54
Log message format 54
Logging events 55
Further information 56

NRS functionality **57**
Contents 57
Introduction 57
Network overview 58
NRS Manager 69

Copyright © 2010 Nortel Networks. All Rights Reserved.

NRS operating parameters 69
Standalone NRS support for Meridian 1 and BCM nodes 76

Numbering plans 81
Contents 81
Introduction 81
Address translation and call routing 87
Numbering plans and routing 94

SIP Phone support 101
Contents 101
Introduction 101
SIP IP Phone Startup 104
SIP Phone calls 105
SIP IP Phone Log on failure 114
SIP Phone dynamic registration 114
Installing a SIP Phone 115
Configuring a SIP Phone 115
SIP IP Phone logoff 116

Configure and manage the Network Routing Service 117
Contents 117
Introduction 119
Installation of Linux operating system, UCM Common Services and NRS application 120
CS 1000 task flow 121
Upgrade Linux-based NRS Release 5.0 or 5.5 to Release 7.0 123
Migration from Solid database to MySQL 124
Database application creation and operation 124
NRS database password interface change 125
Upgrade from Release 3.0 to Release 7.0 126
Upgrade from Release 4.0 or later to Release 7.0 126
Access NRS Manager through the UCM Common Services 126
Initial configuration of NRS on a new IP Peer network 127
Configure Gateway endpoints 129
Nortel recommendation for load-balancing across the Primary and Secondary Linux-based NRS servers 129
SIP Gateway switchover from Primary SPS to Secondary SPS 130
Configure NRS database user endpoints 131
Upgrade of an IP Peer Network from VxWorks-based NRS to Linux-based NRS 131
Recommended upgrade procedure 131
Re-use the existing NRS IP addresses for Linux-based NRS upgrade procedure 131
New NRS IP address assignments upgrade procedure 146
Recovery from failure of Linux-based NRS 148

Copyright © 2010 Nortel Networks. All Rights Reserved.

Operation and maintenance commands 149
Browser configuration 149
Log in to UCM Common Services and Access NRS Manager 151
NRS Manager interface 154
NRS Manager Navigator 154
Navigation of NRS Manager web pages 155
NRS Manager features 157
Mandatory fields on NRS Manager web pages 159
Numbering Plans inherited fields 160
Help and Logout links 161
Configuring IPv6 in NRSM 161
Log out of UCM Common Services 163
Configure the Primary and Secondary NRS Server Settings 163
Configure system-wide settings 175
Configure the NRS database 177
Switch between the Active and Standby databases 178
Manage a Service Domain 179
Add a Service Domain 180
View the Service Domain 181
Edit a Service Domain 183
Delete a Service Domain 184
Manage a Level 1 Domain (UDP) 186
Add an L1 Domain (UDP) 186
View an L1 Domain (UDP) 189
Edit an L1 Domain (UDP) 191
Delete an L1 Domain (UDP) 193
Manage a Level 0 Domain (CDP) 195
Add an L0 Domain (CDP) 195
View an L0 Domain (CDP) 198
Edit an L0 Domain (CDP) 200
Delete an L0 Domain (CDP) 202
Manage a Collaborative Server 204
Add a Collaborative Server 204
View a Collaborative Server 209
Edit a Collaborative Server 210
Delete a Collaborative Server 212
Manage a Gateway Endpoint 213
Add a Gateway Endpoint 213
View Gateway Endpoint Dynamic Registration Information 220
View the Gateway Endpoints 222
Edit the Gateway Endpoints 224
Delete the Gateway Endpoints 226
Manage Post-routing SIP URI Modification 227
Add Post-routing SIP URI Modification 227

Copyright © 2010 Nortel Networks. All Rights Reserved.

View Post-routing SIP URI Modification 229
Edit Post-routing SIP URI Modification 230
Delete Post-routing SIP URI Modification 231
Manage a User Endpoint 232
Unqualified number routing 233
Task summary 233
Add a User Endpoint (SIP Phone) 233
View User Endpoint Dynamic Registration Information 238
View the User Endpoints 239
Edit a User Endpoint 241
Delete a User Endpoint 243
SIP Phone Context 244
Manage a Routing Entry 245
Add a Routing Entry 245
View the Routing Entries 248
Edit a Routing Entry 250
Delete a Routing Entry 251
Copy a Routing Entry 253
Move Routing Entries 255
Search Routing Entries 258
Manage a Default Route 258
Add a Default Route 259
View Default Routes 260
Edit a Default Route 262
Delete a Default Route 263
Manage bulk export of routing entries 264
Bulk export of routing entries 265
Manage bulk import of routing entries 267
Recommendations 267
Bulk import of routing entries 268
Import CSV file specifications 271
Verify the numbering plan and save the NRS configuration 280
H.323 and SIP Routing Tests 281
Perform an H.323 Routing Test 281
Perform a SIP Routing Test 282
Enable, disable and restart the NRS Server 284
Disable the NRS server 285
Enable the NRS server 285
Restart the NRS Server 286
Perform NRS database actions 286
Perform a database Cut over 288
Revert the database changes 289
Perform database Roll back 289
Commit the database changes 290

Copyright © 2010 Nortel Networks. All Rights Reserved.

Backup the database 291
Automatically backup the database 291
Manually backup the database 292
Download the latest backup file 293
Download the latest backup log file 295
Restore the NRS database 296
Restore the database 297
Restore from the connected Signaling Server 298
Restore from a secure FTP site 300
Restore from a client machine 302
Download the latest restore log file 303
GK/NRS Data Upgrade 304
Migration overview 304

Passthrough End User License Agreement 309

Procedures

Procedure 1 Booting IPv4 or IPv6 SIP IP Phones 104
Procedure 2 Logging off from the SIP IP Phones 116
Procedure 3 Configuring the Internet Explorer browser settings 150
Procedure 4 Configuring the Windows Display settings 151
Procedure 5 Logging in to UCM Common Services and Accessing NRS Manager 151
Procedure 6 Logging out of UCM Common Services 163
Procedure 7 Configuring the Primary and Secondary NRS Server Settings for IPv4 and IPv6 166
Procedure 8 Configuring system-wide settings 175
Procedure 9 Switching between the Active and Standby databases 178
Procedure 10 Adding a Service Domain 180
Procedure 11 Viewing the Service Domains 182
Procedure 12 Editing a Service Domain 183
Procedure 13 Deleting a Service Domain 184
Procedure 14 Adding an L1 Domain 186
Procedure 15 Viewing an L1 Domain (UDP) 190
Procedure 16 Editing an L1 Domain (UDP) 191
Procedure 17 Deleting an L1 Domain (UDP) 193
Procedure 18 Adding an L0 Domain (CDP) 195
Procedure 19 Viewing an L0 Domain (CDP) 198
Procedure 20 Editing an L0 Domain (CDP) 200
Procedure 21 Deleting an L0 Domain (CDP) 202
Procedure 22 Adding a Collaborative Server 204
Procedure 23 Viewing a Collaborative Server 209
Procedure 24 Editing a Collaborative Server 210
Procedure 25 Deleting a Collaborative Server 212
Procedure 26 Adding a Gateway Endpoint 213
Procedure 27 Viewing Gateway Endpoint Dynamic Registration Information 220
Procedure 28 Viewing the Gateway Endpoints 222
Procedure 29 Editing the Gateway Endpoints 224
Procedure 30 Deleting the Gateway Endpoints 226

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 31 Adding Post-routing SIP URI Modification 227
Procedure 32 Viewing Post-routing SIP URI Modification 229
Procedure 33 Editing Post-routing SIP URI Modification 230
Procedure 34 Deleting Post-routing SIP URI Modification 231
Procedure 35 Adding a User Endpoint 233
Procedure 36 Viewing User Endpoint Dynamic Registration Information 238
Procedure 37 Viewing the User Endpoints 239
Procedure 38 Editing a User Endpoint 241
Procedure 39 Deleting a User Endpoint 243
Procedure 40 Mapping the SIP Phone Context 244
Procedure 41 Adding a Routing Entry 246
Procedure 42 Viewing the Routing Entries 248
Procedure 43 Editing a Routing Entry 250
Procedure 44 Deleting a Routing Entry 252
Procedure 45 Copying a Routing Entry 253
Procedure 46 Moving Routing Entries 255
Procedure 47 Searching Routing Entries 258
Procedure 48 Adding a Default Route 259
Procedure 49 Viewing Default Routes 261
Procedure 50 Editing a Default Route 262
Procedure 51 Deleting a Default Route 263
Procedure 52 Bulk export of routing entries 265
Procedure 53 Bulk import of routing entries 269
Procedure 54 Verifying the numbering plan 280
Procedure 55 Performing an H.323 Routing Test 281
Procedure 56 Performing a SIP Routing Test 282
Procedure 57 Disabling the NRS server 285
Procedure 58 Enabling the NRS server 286
Procedure 59 Restarting the NRS Server 286
Procedure 60 Cutting over the database 288
Procedure 61 Reverting the database changes 289
Procedure 62 Rolling back changes to the database 290
Procedure 63 Committing the database 290
Procedure 64 Backing up the database automatically 291
Procedure 65 Backing up the database manually 292
Procedure 66 Downloading the latest backup file 293
Procedure 67 Downloading the latest backup log file 296
Procedure 68 Restoring the database 297
Procedure 69 Restoring from the connected Signaling Server 298
Procedure 70 Restoring from a secure FTP site 301
Procedure 71 Restoring from a client machine 302
Procedure 72 Downloading the latest restore log file 303

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

New in this Release

The following sections detail what's new in Network Routing Service Fundamentals for Communication Server 1000 Release 7.0:

- "Features" (page 12)
- "Other" (page 13)

Redirect Server support on Linux-based NRS

The Linux-based NRS can be a SIP Proxy or as a SIP Redirect Server for each end point. Configuration of gateway and user endpoints is provided by the NRS Manager. Calls can occur between Proxy mode and Redirect Server mode endpoints.

The SIP Redirect Server mode offers a significant improvement in call capacity, but most advanced features (such as Post-Routing SIP URI modification) are not supported in Redirect Server mode.

Call processing capacity improvement

In CS 1000 Releases 4.0, 4.5, 5.0, 5.5 and 6.0, a Solid database server was used to store and retrieve the NRS routing data. In CS 1000 Release 7.0, MySQL Enterprise 5.1 server is used to store and query the NRS routing data. Migration from the Solid database to MySQL provides significant improvement in call processing capacity and system stability. MySQL migration does not affect the user interface.

Same-cost routing

When you perform a location query during server/client session setup, a target set consisting of multiple addresses can be produced with the same cost value. Same-cost routing provides load balancing by random selection among multiple gateway routes with the same cost factor.

Source-based routing for Multimedia Convergence Manager

Source-based routing interworks with Multimedia Convergence Manager (MCM). All calls (SIP sessions) originated by the Office Communications client go through the home CS 1000 where the originator DN belongs.

Copyright © 2010 Nortel Networks. All Rights Reserved.

If homing cannot occur on MCM by using the telephone number, MCM forces the SIP Proxy or SIP Redirect Server to perform the routing using the first SIP gateway endpoint instead of the telephone number.

Service domain name can be configured as an IP Address in NRS Manager

In CS 1000 Release 7.0, you can configure the Service Domain name as the Primary NRS Server TLAN IP address when required to interwork with third-party gateways that do not support a Service Domain name.

Operation, Administration and Maintenance Transaction Audit and Security Event Logging

The Operation, Administration, and Maintenance Transaction (OAM) Audit Log is a secure record of all system administrator OAM activities and security-related events. The OA&M Transaction Audit Log is maintained in a central location on the Nortel Unified Communications Management (UCM) Common Services. It can be forwarded to an external Operational Support System using the Linux syslog daemon.

The OA&M log records include security, operational, configuration and maintenance events of CS 1000 management applications. The security audit logs contain sufficient information for after-the-fact investigation, or analysis, of security incidents. The audit logs provide a way to accomplish several security-related objectives including individual accountability, reconstruction of past events, intrusion detection, and problem analysis.

Access to NRS CLI command

The maintenance and administration, system administration, and database administration CLI commands are renamed and moved to a new location under a new policy-based access method.

The maintenance and administration commands are accessible only by users who belong to the UCM Common Services maintenance and administration group (maintadmin).

The system administration commands are accessible only by users who belong to the UCM Common Services system administration group (systemadmin).

The database administration commands are accessible only by users who belong to the UCM Common Services database administration group (dbadmin).

Features

See the following sections for information about feature changes:

Copyright © 2010 Nortel Networks. All Rights Reserved.

IPv6 support

Support for IPv6 helps to configure single stack (IPv4 only) and dual stack (both IPv4 and IPv6) in NRSM. NRSM provides support for the IPv6 format for TLAN IPs in the User Interface. You can also add IPv6 endpoints.

For more information about how to configure IPv6 for the NRS Manager, see "Configuring IPv6 in NRSM" (page 161) in the "Configure and manage the Network Routing Service" (page 117) chapter.

Route cost modification

The NRSM code is modified to display an error message if a new routing entry is added that has the same DN type and DN prefix as another routing entry that is already present under the same Gateway Endpoint.

For more information about how to manage routing entries, see "Manage a Routing Entry" (page 245) in the "Configure and manage the Network Routing Service" (page 117) chapter.

Internal and external NRS for the High Scalability Solution

The High Scalability Solution introduces two Network Routing Service (NRS) servers for network routing—an internal NRS and an external NRS.

For more information about internal and external NRS for High Scalability, see "Internal and external NRS for the High Scalability Solution" (page 33) in the "Network Routing Service overview" (page 19) chapter.

Tertiary NRS server

A tertiary NRS server provides a third level of redundancy for the SIP Gateway (SIPGW) and replaces the existing failsafe operations to provide maximum flexibility and ease of deployment for a scalable solution.

For more information about the Tertiary NRS server, see "Tertiary NRS server" (page 33) in the "Network Routing Service overview" (page 19) chapter.

Other

Revision History

June 2010

Standard 2.01. This document is up-issued to support Nortel Communication Server 1000 Release 7.0.

June 2009

Standard 01.04. This document is up-issued to reflect changes in technical content.

Copyright © 2010 Nortel Networks. All Rights Reserved.

May 2009
Standard 01.03. This document is up-issued to reflect changes in technical content.

May 2009
Standard 01.02. This document is up-issued to reflect changes in technical content.

May 2009
Standard 01.01. This document is a new NTP for Communication Server 1000 Release 6.0. It was created to support a restructuring of the Documentation Library. This document is comprised of (1) information on the Linux-based Network Routing Service that was previously contained in *Network Routing Service Installation and Commissioning (NN43001-564)*, now retired and (2) a description of the operation and configuration of Communication Server 1000 Release 6.0 Network Routing Service.

Conventions

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

- Communication Server 1000E (CS 1000E)
- Communication Server 1000M (CS 1000M)

In this document, the following hardware is referred to generically as Media Gateway:

- Option 11C Mini Chassis (NTDK91) and Expander chassis (NTDK92) - legacy hardware
- Option 11C Cabinet (NTAK11) - legacy hardware
- MG 1000E Chassis (NTDU14) and Expander chassis (NTDU15)
- MG 1010 Chassis (NTC310)
- IPE module (NT8D37) with MG XPEC card (NTDW20)

In this document, the following hardware platforms are referred to generically as Server:

- Call Processor Pentium IV (CP PIV) card
- Common Processor Pentium Mobile (CP PM) card
- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers

Copyright © 2010 Nortel Networks. All Rights Reserved.

— IBM x360m server (COTS1)

— HP DL320 G4 server (COTS1)

— IBM x3350 server (COTS2)

— Dell R300 server (COTS2)

In this document, the generic term COTS refers to all COTS servers. The term COTS1 or COTS2 refers to the specific servers in the preceding list.

In this document, the following cards are referred to generically as Gateway Controller:

- Media Gateway Controller (MGC) card (NTDW60 and NTDW98)
- Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card (NTDW20)
- Common Processor Media Gateway (CP MG) card (NTDW56 and NTDW59)

The following table shows CS 1000 Release 7.0 supported roles for common hardware platforms:

Table 1
Hardware platform supported roles

Hardware platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP IV	yes	no	no	no
CP PM	yes	yes	yes	no
CP DC	no	yes	yes	no
CP MG	no	yes	yes (see note)	yes (see note)
MGC	no	no	no	yes
MG XPEC	no	no	no	yes
COTS	no	yes	no	no
COTS2	no	yes	yes	no

Note: The CP MG card functions as a Server and the Gateway Controller while occupying slot zero in a chassis, cabinet, and MG 1010.

For information about CP MG, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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:

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Network Routing Service overview

Contents

This chapter contains the following topics:

"Introduction" (page 21)

"Network protocol component" (page 24)

"Session Initiation Protocol" (page 25)

"SIP entities" (page 25)

"User agent" (page 26)

"SIP Proxy Server" (page 26)

"SIP Redirect Server" (page 26)

"SIP Registrar" (page 26)

"NRS SIP server implementation" (page 26)

"Back-to-Back User Agent" (page 27)

"SIP domains" (page 27)

"Location Service" (page 27)

"NRS purpose" (page 28)

"Signaling Gateways" (page 28)

"SIP Gateway" (page 29)

Copyright © 2010 Nortel Networks. All Rights Reserved.

"SIP services" (page 29)

"H.323 protocol" (page 30)

"H.323 entities" (page 30)

"H.323 terminal" (page 30)

"H.323 Gatekeeper" (page 30)

"Gatekeeper zones" (page 31)

"H.323 Gateway" (page 31)

"SIP and H.323 interworking" (page 31)

"Network Connection Service" (page 32)

"SIP NRS Privacy within a Trusted Network" (page 32)

"Primary and Secondary NRS servers" (page 32)

"NRS Failsafe" (page 33)

"Database component" (page 35)

"NRS Database" (page 35)

"Hierarchical model of the Network Routing Service" (page 38)

"SIP authentication" (page 40)

"SIP Uniform Resource Identifiers" (page 41)

"Database synchronization and operation component" (page 44)

"Synchronization of the active and standby databases on a Network Routing Server" (page 46)

"NRS database redundancy" (page 49)

"Source-based routing for Multimedia Convergence Manager" (page 50)

"Same-cost routing" (page 50)

"Operation, Administration, and Maintenance Transaction Audit and Security Event Logging" (page 52)

"Operation, Administration and Maintenance logging framework" (page 52)

"Centralized Operation, Administration and Maintenance log storage and log file rotation" (page 52)

"Log viewer interface" (page 53)

Copyright © 2010 Nortel Networks. All Rights Reserved.

"Support for an OSS Syslog server" (page 54)
"Log message format" (page 54)
"Logging events" (page 55)
"Further information" (page 56)

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.

The Linux-based 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

The SIP Proxy and Redirect Server can operate in Redirect mode or Proxy mode for each endpoint. The NRS Manager provides configuration.

— SIP Registrar

— Transport Layer Security component

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

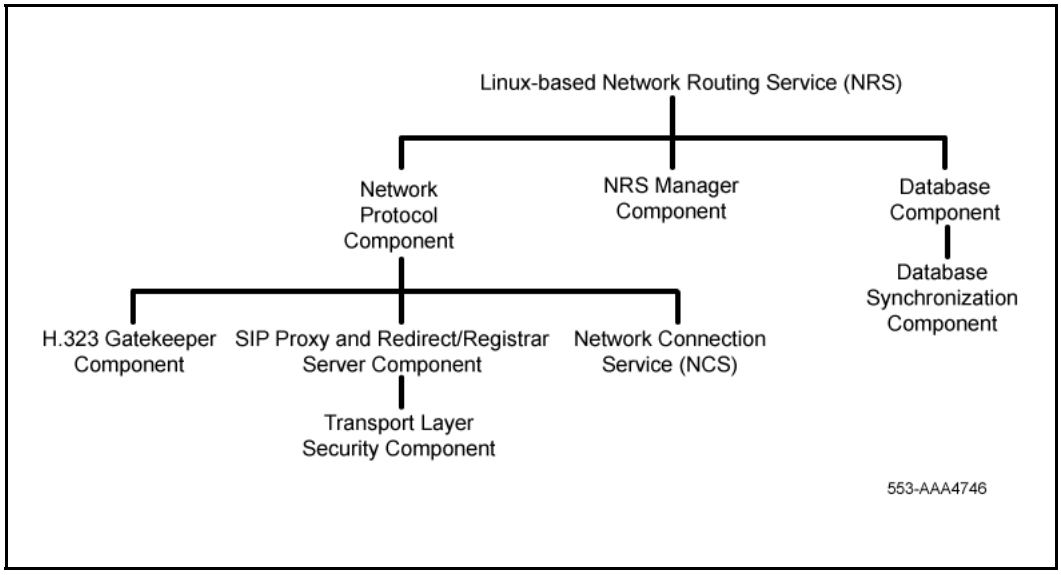
The Linux-based NRS is hosted either co-resident with Signaling Server applications or in stand-alone mode on a dedicated server running the Linux operating system.

The Linux-based NRS in Redirect mode can be used in Primary or Secondary configuration to handle SIP signaling between CS 1000 SIP gateways, as well as third-party SIP gateways and user endpoints. The Linux-based NRS in Redirect mode continues to support per-call redirect request and collaboration. However, the feature access codes used for per-call redirect take precedence over the endpoint configuration used in this mode.

Figure 1 "Linux-based NRS components" (page 23) shows a graphical view of the Linux-based NRS.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 1
Linux-based NRS components



NRS for CS 1000 Release 5.0 and Release 5.5 is offered in two versions:

- Linux-based NRS that supports a SIP Proxy
- VxWorks-based NRS that supports a SIP Redirect Server

In CS 1000 Release 7.0, the Linux-based NRS supports a SIP Server that can operate in Proxy or Redirect mode.

The CS 1000 Release 5.0 and 5.5 VxWorks-based NRS comprises

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

  The SIP component comprises
  - — SIP Redirect Server
  - — SIP Registrar
  - — Transport Layer protocol component
- NRS Database component.

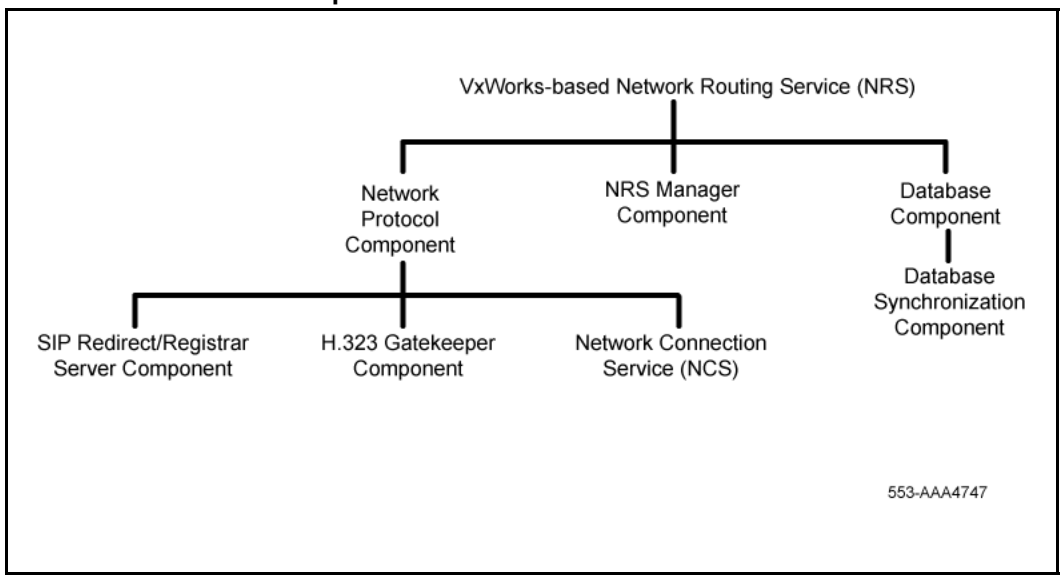
  The NRS Database component supports
  - — a Routing and Location Service shared by the SIP Redirect Server, the SIP Registrar, and the H.323 Gatekeeper
  - — database synchronization
- NRS Manager

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

Figure 2 "VxWorks-based NRS components" (page 24) shows a graphical view of the VxWorks-based NRS.

Figure 2
VxWorks-based NRS components



The VxWorks-based NRS is not offered in CS 1000 Release 7.0. For more information about the VxWorks-based NRS, see *Network Routing Service Installation and Commissioning* (NN43001-564).

Network protocol component

The NRS Network Protocol component comprises

- SIP Server
- SIP Registrar
- H.323 Gatekeeper
- Network Connection Service
- 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The SIP Proxy and Redirect Server in proxy mode is a stateful proxy server.

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 37) and “SIP Uniform Resource Identifiers” (page 41).

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 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 in SIP Proxy mode provides information for 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Signaling gateways also provide a 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

- Microsoft OCS 2007.
- 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.323 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 2 "Comparison of SIP and H.323 terminology" (page 31) summarizes SIP and H.323 interworking terminology.

Table 2
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	A SIP endpoint registers to a SIP Proxy/Registrar or 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 three 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.
- In NRS Manager, NCS is configured in the following areas:
- For configuration of the NRS server to support the NCS, see Procedure 7 “Configuring the Primary and Secondary NRS Server Settings for IPv4 and IPv6” (page 166).
- For configuration of Virtual Office and branch office (including the SRG) user redirection to the main office, see Procedure 26 “Adding a Gateway Endpoint” (page 213).

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.

Primary and Secondary NRS servers

All systems in the IP Peer network must register with the Network Routing Service (NRS). To eliminate a single point of failure in the IP Peer network, Nortel recommends deploying a Primary and Secondary NRS. The Secondary NRS provides Network Routing Service to the IP Peer network if the Primary NRS fails.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Tertiary NRS server

A tertiary NRS server provides a third level of redundancy for the SIP Gateway (SIPGW) and replaces the existing Failsafe operations to provide maximum flexibility and ease of deployment for a scalable solution. The tertiary NRS can run on any device on the network and operates in a one to many or a one-to-one mode. The tertiary NRS provides additional flexibility because it has an independent NRS database tailored to route SIP calls during a WAN outage. This is different from the failsafe NRS, which is a copy of the Primary NRS database. The data from the primary database may not be relevant in a WAN outage at a Survivable SIP Gateway and the failsafe NRS does not provide third level IP provisioning for the gateway on the management interface. The third level of redundancy does not apply to the H.323 gateway;if a system has a tertiary NRS defined for the SIP Gateway, the co-residing H.323 solution has only two levels of redundancy because the failsafe NRS cannot run on this system.

You can configure the tertiary NRS using the NRS Manager Web manager. For more information about configuring the SIP Trunk Gateway settings of the tertiary NRS server in Element Manager, see *IP Peer Networking Installation and Commissioning* (NN43001-313).

ATTENTION
If you attempt to enable Failsafe NRS, the Tertiary NRS server is disabled and the configuration values change to the default values.

Internal and external NRS for the High Scalability Solution

The High Scalability Solution uses two Network Routing Service (NRS) servers for network routing—an internal NRS and an external NRS. For small deployments, you can configure both the internal and the external NRS in the same server. The internal NRS is also the Network Connection Server for IP Phone redirection. The internal NRS is used to route Private numbers (CDP and UDP) within an HS system. The external NRS is used to route off-net E.164 numbers within an HS system and route E.164 and UDP calls to and from systems outside an HS system.

For more information about internal and external NRS and how to use each in the High Scalability Solution, see *Communication Server 1000E Planning and Engineering — High Scalability Solutions* (NN43041-221).

NRS Failsafe

Within the Linux-based NRS, a failsafe mechanism is used to update CS 1000 SIP Gateways configured with the failsafe function. The failsafe function on the IP Peer Gateways is used as a mechanism by which the SIP Gateways stay in contact with the CS 1000 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

the prescribed time, will initiate an update session with the CS 1000 SIP Gateway, format the SIP routing data from the NRS on Linux, and begin the transfer of the data to the gateway.

Because the failsafe mechanism is executed periodically, the Linux cron triggers the operation every 6 hours.

When failsafe synchronization starts, it can abort for the following reasons:

1. When there is no Failsafe Server configured.
2. When the failsafe data entry is NULL.

NRS database synchronization from Primary to Failsafe

If the Primary Network Routing Server fails, the Secondary Server takes the role of the Primary Server. If the Secondary Server fails, the Failsafe Server takes the role of the Primary Server. When the Failsafe Server becomes the Primary Server, the failsafe database has to be in the updated state. Failsafe synchronization between the Primary and Failsafe Servers supports the failsafe database in the updated state.

The failsafe synchronization in CS 1000 Release 7.0 is implemented by API functions, which create a database backup in XML format and load the backup files to the Failsafe Server. The Primary Server prepares the .XML database files on a periodic basis (the default is every 6 hours) and then initiates the transfer to all registered failsafe supported gateways.

The database synchronization from the Primary Server to the Failsafe Server is done through secure transfer, SFTP. For backward compatibility, FTP is used for Failsafe Servers running older versions of NRS (for example CS 1000 Releases 4.0, 4.5, 5.0 or 5.5). Although the support for failsafe synchronization is backward-compatible, there are some limitations to the database synchronization from the Primary Server to the Failsafe Server if the Failsafe Server is not running NRS Release 7.0:

- The Primary Server may have been configured with higher capacity than the Failsafe Server. The lower capacity Failsafe Server may not able to handle the synchronization request.
- The Primary NRS may have some endpoints configured as TLS support. If the Failsafe Server is running VxWorks-based NRS, the Failsafe Server ignores these endpoints and the associated routing entries because TLS are not supported by VxWorks-based NRS.

Copyright © 2010 Nortel Networks. All Rights Reserved.

For Failsafe deployment, you must configure the Failsafe servers and the Primary Server as members of the same UCM Common Services Security Domain

> ***Note:*** To address these limitations to the database synchronization from the Primary Server to the Failsafe Server, Nortel recommends that the Failsafe NRS and gateways be upgraded to the same version as the Primary NRS.

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 issue the command

```
/spcmd -D -d failsafe
```

Database component

NRS Database

The NRS database is comprised of endpoints (IP phones, SIP gateways, H.323 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:

Copyright © 2010 Nortel Networks. All Rights Reserved.

- 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

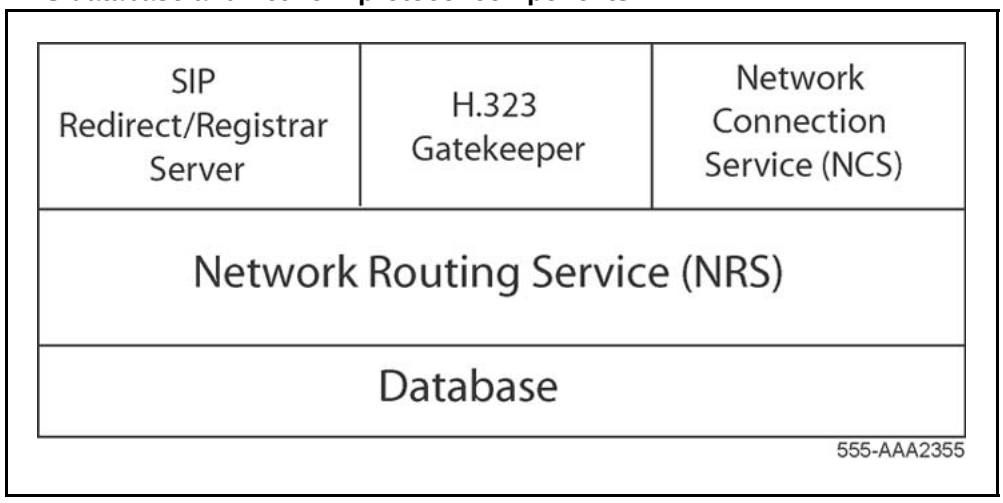
The NRS numbering plan configuration is stored in XML format in two databases on disk. The active database is used for call processing and the standby database is used for configuration changes.

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 36)).

Figure 3
NRS database and network protocol components



Copyright © 2010 Nortel Networks. All Rights Reserved.

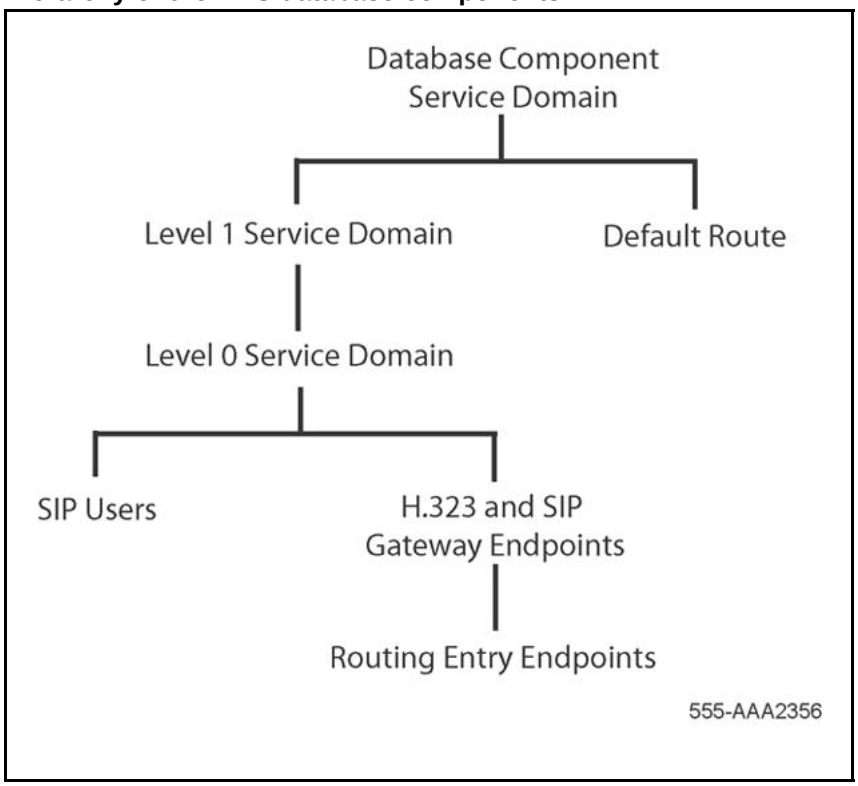
The SIP Proxy, the SIP Redirect Server and the H.323 Gatekeeper have access to the endpoint/location database.

- The SIP Proxy and the Redirect Server access the location database on CS 1000 systems to direct SIP Trunk Gateways within a network 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 "Hierarchy of the NRS database components" (page 37) 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" (page 38). 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



Copyright © 2010 Nortel Networks. All Rights Reserved.

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 3 "Hierarchical model of the Network Routing Service" (page 38). 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 3
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 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

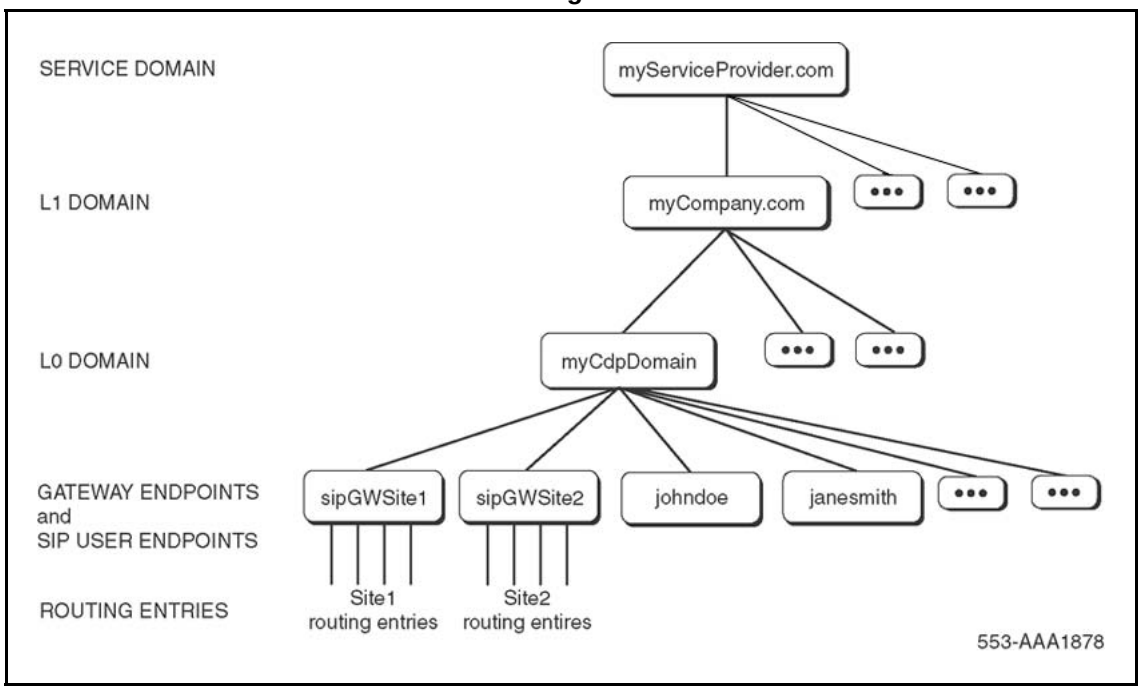
Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 3
Hierarchical model of the Network Routing Service (cont'd.)

Level	Description
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 39) 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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:

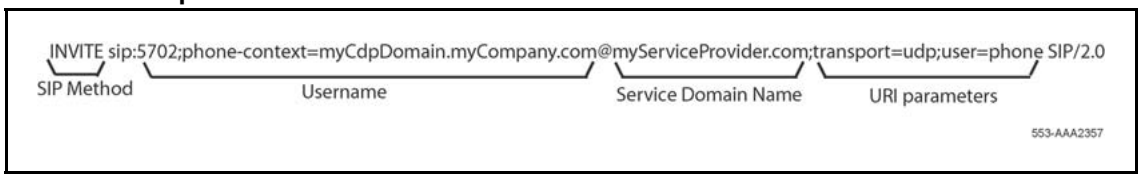
- Not configured — If this option is selected, then the endpoint uses the Level 1 or Level 0 Domain authentication (if Level 1 authentication is enabled).
- Authentication off — If authentication is turned off, then authentication is off for this endpoint even if Level 1 or Level 0 Domain authentication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

Copyright © 2010 Nortel Networks. All Rights Reserved.

SIP Uniform Resource Identifiers

The NRS supports SIP URIs (see Figure 6 "SIP URI example" (page 41)). A SIP URI is a user's SIP identity.

Figure 6
SIP URI example



Where:

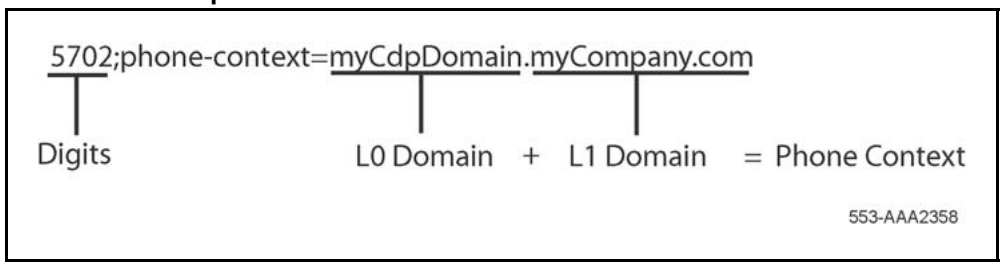
- **Username:** Specifies the actual subscriber information, which is used by the SIP Trunk Gateway to map to and from the NPI/TON field. The username field is parsed into a name and phone context (see Figure 7 "Username example" (page 41)).

  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



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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 4 "Numbering plan mapping" (page 43) 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 4 "Numbering plan mapping" (page 43) provides examples for both the NRS and MCS 5100.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

See Figure 5 "Hierarchical structure of the Network Routing Service" (page 39) for the SIP address hierarchy tree.

Table 4
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 ***Note:*** Public international numbers do not have a phone context, as these numbers are globally unique within a domain. A plus 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 4
Numbering plan mapping (cont'd.)

NPI/TON/DN	SIP URI
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
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 and operation component

You can deploy the Network Routing Service as a stand-alone server or as redundant servers that comprise a Primary Network Routing Server and a Secondary Network Routing Server.

Copyright © 2010 Nortel Networks. All Rights Reserved.

For the redundant deployment, you must configure both the Primary and Secondary NRS as members of the same UCM Common Services Security Domain.

For Failsafe deployment, you must configure the Failsave servers and the Primary server as members of the same UCM Common Services Security Domain.

In normal operational mode, the administrator must change configuration information on the Primary NRS server. The configuration information automatically synchronizes with the Secondary NRS server in real time. Database synchronization is one-directional from the Primary to the Secondary NRS server.

If the Primary NRS server is out of service, the administrator can make only temporary changes to the Secondary NRS Server. When the Primary NRS server returns to service, the Primary NRS Server synchronizes information with the Secondary NRS Server and overwrites the temporary configuration changes on the Secondary NRS Server. Configuration database changes must occur on the Primary NRS Server. Nortel does not recommend that you change the configuration data on the Secondary NRS Server because the temporary changes are overwritten when the Primary NRS Server returns to service.

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 or later the cluster is comprised of a Primary Network Routing Server and a Secondary Network Routing 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

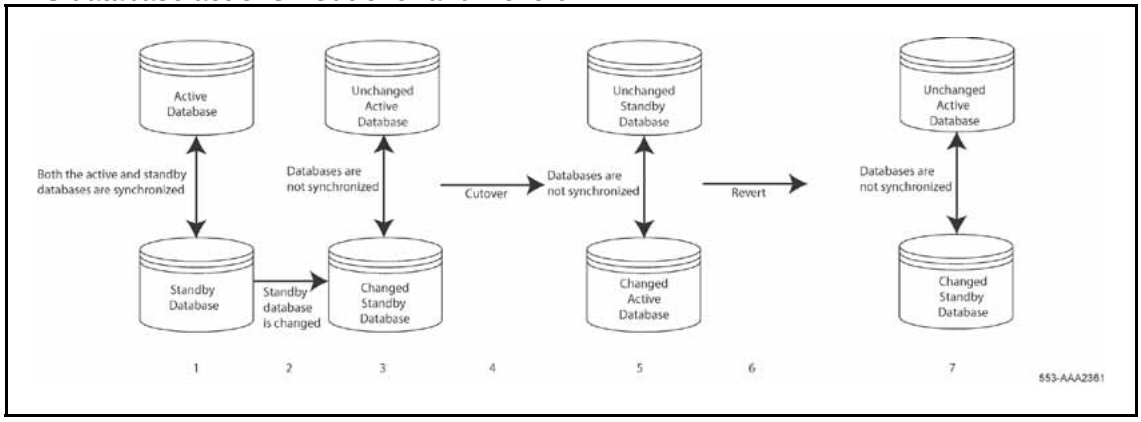
Synchronization of the active and standby databases on a Network Routing Server

Cut over and revert

Figure 8 "NRS database actions - Cut over and Revert" (page 46) 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



Cut over and commit

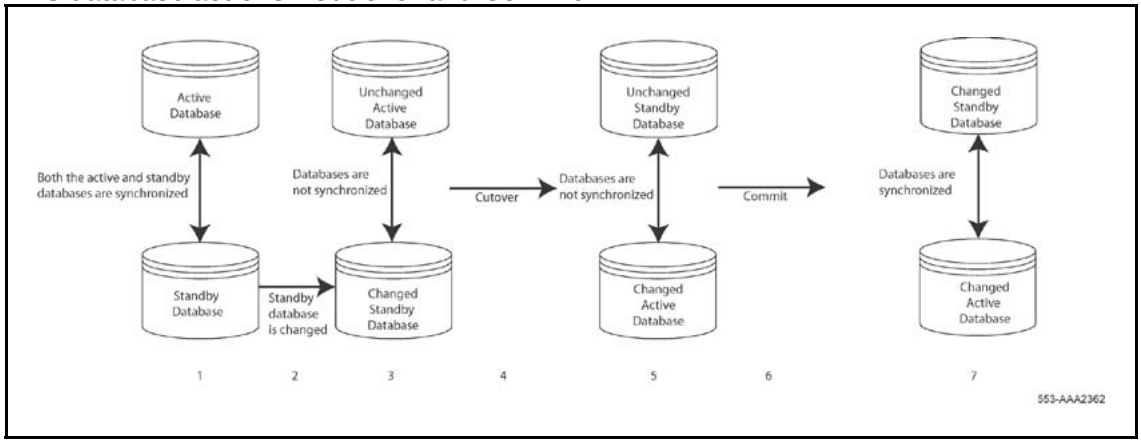
Figure 9 "NRS database actions - Cut over and Commit" (page 47) shows both the active and standby database when **Cut over** and **Commit** database commands are issued.

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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



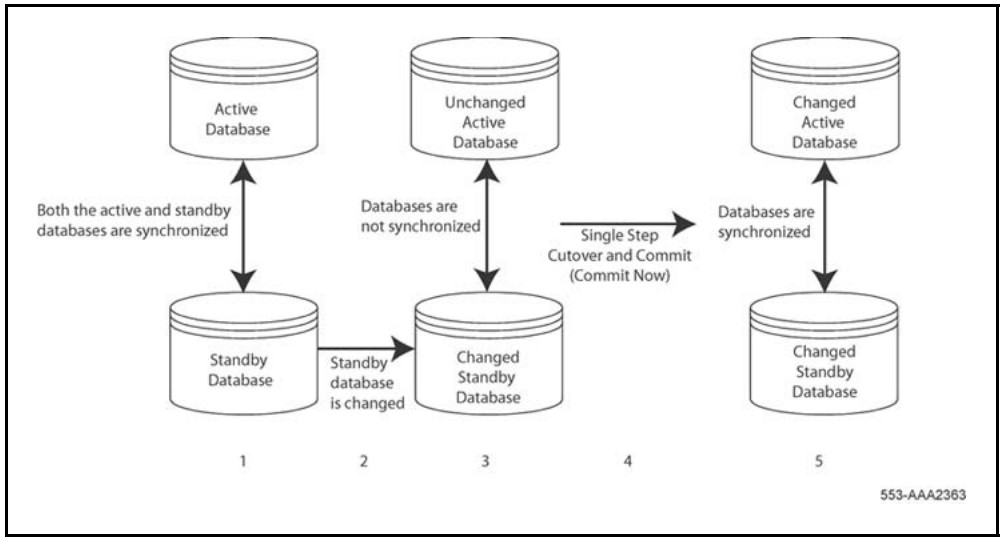
Single-step Cut over and Commit

Figure 10 "NRS database actions - single-step Cut over and Commit" (page 48) 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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



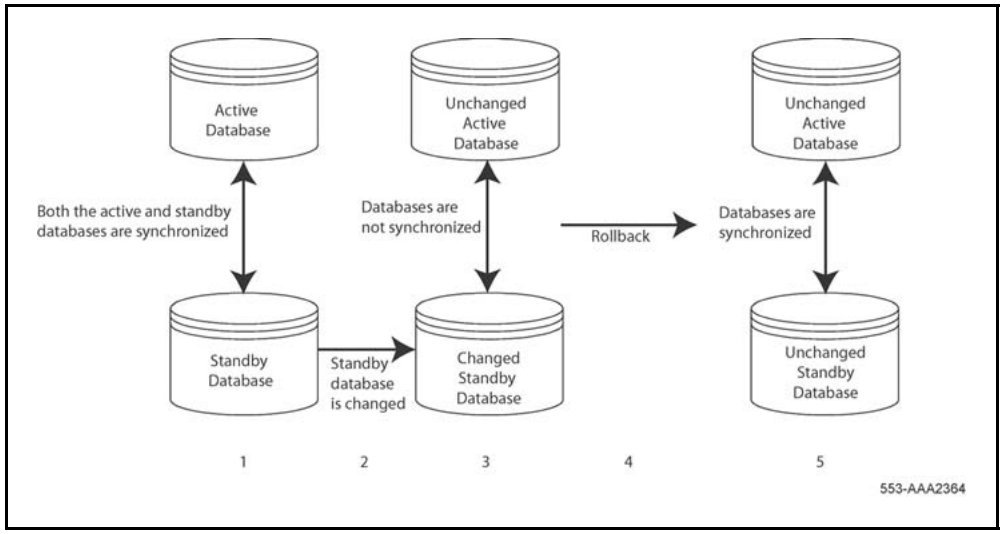
Rollback

Figure 11 "NRS database actions - rollback" (page 49) 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 11
NRS database actions - rollback



To perform database actions using NRS Manager, see "Perform NRS database actions" (page 286).

NRS database redundancy

In CS 1000 Release 5.0 or later, the Network Routing Service is redundantly deployed on a Primary Network Routing Server and a Secondary Network Routing Server.

Each node has a single MySQL server and multiple database clients including H.323 Gatekeeper, SIP Proxy Server, NRS Manager, and Network Connection Service. A registration event updates a common database shared by the Primary and Secondary Network Routing Servers.

The database clients perform local database access to the local MySQL server through a UNIX socket. The Linux-based NRS has an active-active database model. In the active-active database model, the administrator uses the NRS Manager to enter or change the configuration data on the Primary node. Database update on the Secondary node occurs by MySQL replication from the Primary to Secondary node. For dynamic or real-time data, the database update is one-way from the Primary to the Secondary node.

When both the Primary and Secondary nodes are in service, the database on the Secondary server is read-only. An administrator cannot change configuration information changes on the Secondary Server.

Copyright © 2010 Nortel Networks. All Rights Reserved.

An administrator can change configuration information changes on the Secondary Server only when the Primary Server is not in service and the Secondary Server can not connect with the Primary server. Changes on the Secondary Server are overwritten when the Primary Server comes into service.

You can set up only one of the three NRS roles (Primary, Secondary, or Failsafe) on an NRS server. A Failsafe NRS server does not support NRS Manager.

> ***Note:*** The SIP Proxy supports an active-active model to provide load balancing across the Primary and Secondary Linux-based NRS Servers. For full NRS redundancy, both the Primary and Secondary Servers must be matched hardware pairs. Support is unavailable for unmatched hardware pairs. Matched hardware pairs are CP PM-CP PM, or vendor matched COTS-COTS servers. Matched software configuration and engineering is also required for optimal performance.

Source-based routing for Multimedia Convergence Manager

Source-based routing interworks with Multimedia Convergence Manager (MCM). All calls (SIP sessions) originated by the Office Communications client go through the home CS 1000 where the originator DN belongs. If homing cannot occur on MCM by using the telephone number, MCM forces the SIP Proxy or SIP Redirect Server to perform the routing using the first SIP gateway endpoint instead of the telephone number.

> ***Note:*** The sip-gw-id flag on MCM must match the gateway name in the NRS endpoint table. Therefore, care must be maintained when configuring the two systems.

Same-cost routing

Same-cost routing provides load balancing by random selection among multiple gateway routes with the same cost factor. Because the gateways are randomly chosen for same-cost routes during call signaling, the signaling requests are load balanced over time. To configure multiple routes with the same cost, see Procedure 41 “Adding a Routing Entry” (page 246).

The NRS location service or gatekeeper randomly chooses one of the valid same cost routes to complete the call. If the endpoint with the least-cost route is unreachable or all channels are busy, the alternate endpoint (if registered) with a higher cost factor is used to complete the call.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Network Connection Service (NCS) is not treated as a special case when configuring same cost routing from NRS Manager. However, there is no randomized load-balancing of IP Phone registrations occurs across NCS endpoints with the same-cost value.

Even without same-cost load balancing, large-scale CS 1000 IP telephony solutions must often introduce routing prefixes to separate SIP or H.323 gateway routes, used for CDP and UDP LOC call traffic, from routes used for NCS-based features such as Branch Office, Geographic Redundancy, and Network-wide Virtual Office Login.

Table 5 "Same Cost Routing Matrix" (page 51) summarizes of same-cost routing support for each hierarchy in the numbering plan.

Table 5
Same Cost Routing Matrix

Routing Entry DN Type	Same Cost Routing Support in Release 5.5	Same Cost Routing Support in Release 6.0	Validation Scope in Release 6.0	Maximum number of Same Cost Routes in Release 6.0 (under the scope)
E.164 International	No	Yes	For each Service Domain	8
E.164 National	Yes	Yes	For each Service Domain	8 (no maximum same cost routes limitation in Release 5.5)
E.164 Local	Yes	Yes	For each Service Domain	8 (no maximum same cost routes limitation in Release 5.5)
Private L1	No	Yes	For each Layer 1 Domain	8
Private L0	No	Yes	For each Layer 0 Domain	8
Private Special	No	Yes	For each Layer 1 Domain	8

Note 1: No routing occurs under the same gateway endpoint.

Note 2: For 911 calls, the administrator should use special prefix in front of Private Special DN Prefix to identify the routing location.

Feature interactions

When the chosen same-cost route fails, and no higher cost routes are configured, then the call fails.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Operation, Administration, and Maintenance Transaction Audit and Security Event Logging

The Operation, Administration, and Maintenance Transaction (OA&M) Audit Log is a secure record of all system administrator OA&M activities and security-related events. The OA&M Transaction Audit Log is maintained in a central location on the Nortel Unified Communications Management Common Services (UCM Common Services). The log can be forwarded to an external Operational Support System (OSS) using the Linux syslog daemon.

The OA&M log records include security, operational, configuration, and maintenance events of CS 1000 management applications. The security audit logs contain sufficient information for after-the-fact investigation, or analysis, of security incidents. The audit logs provide a way to accomplish several security-related objectives including individual accountability, reconstruction of past events, intrusion detection, and problem analysis.

The OA&M logs are generated and stored in each backup and member UCM Common Services server. During software installation, the syslog daemon on the backup and member servers are configured to forward the OA&M logs to the central syslog daemon running on the primary UCM Common Services server for consolidation.

The Operation, Administration, and Maintenance Transaction Audit Log feature provides

- OA&M logging framework
- Central OA&M log storage and log file rotation
- Log viewer interface
- Support for a OSS Syslog server

Operation, Administration and Maintenance logging framework

NRS Manager uses the OA&M logging framework to insert a message with a standard format into the OA&M logs. the Linux syslog daemon generates NRS application logs and OA&M logs. Logs from the backup and member servers are forwarded to the centralized syslog daemon running on the primary UCM Common Services server for consolidation.

Centralized Operation, Administration and Maintenance log storage and log file rotation

Nortel recommends that you store all CS 1000 Release 7.0 Nortel application log files in `/var/log/nortel`. This partition is allocated 10 percent of the total hard disk space during the Linux base installation. You

Copyright © 2010 Nortel Networks. All Rights Reserved.

cannot change the size of the partition. The Alarm Script of the Linux base monitors the partitions for storage. The Alarm Script issues a message to the Linux console if the partition is near storage capacity.

Two OA&M log files containing all security -related events (security.log) and administration events (oam.log) are stored in the **`/var/log/nortel/`**
`OAM` directory of the Primary Server.

The files are configured for 30-day rotation. Each day, the files are created with the date appended to the file name to provide a 30-day archive of all generated log files. The archived log files are stored in compressed format. The naming convention for the archived files is xxx.log-YYYYMMDD.gz.

Log rotation is configured to start one day after server installation. For example, if you install the server on January 1, then logs generated on January 1 and January 2 are in the files created on the January 1. Beginning January 3, the OA&M log files are rotated daily. The OA&M log file generated on January 3 contain the logs from January 1 and January 2.

Note 1: If you need more than a 30-day history of OA&M logs, the logs can be forwarded to external storage using the syslog protocol.

Note 2: If the server is down, OA&M logs are not consolidated on the Primary UCM Common Services Server. No automatic failover and re consolidation of the log messages occur when the Primary Server starts. Nortel recommends that you manually perform a FTP the OA&M log files from the local servers to the primary UCM Common Services server and append them to the OA&M file for that day.

Log viewer interface

A log viewer interface is provided on the primary, backup, and member UCM Common Services servers. On the primary UCM Common Services server, you can use the log viewer to access the consolidated OA&M logs forwarded from the backup and member servers in the security domain. From the Base Manager, use the log viewer to access the local OA&M logs on the backup and member servers.

You cannot use the log viewer interface to view NRS Manager or SIP Proxy logs because the NRS Manager and SIP Proxy log formats are different from the OA&M log format.

You can use the log viewer to view log files smaller than 5 MB. A 5-MB log file can contain approximately 50 000 log events. If the log file size is larger than 5 MB, a link to export and download the file appears.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Support for an OSS Syslog server

The consolidated OA&M logs from the primary UCM Common Services server can be forwarded in real-time to an external third-party Operation Support System (OSS) syslog server for monitoring and analysis. The local OA&M logs can not be forwarded from backup and member UCM Common Services servers to an external third-party OSS syslog server. Application logs cannot be forwarded from the primary, backup, or member UCM Common Services servers to an external third-party OSS syslog server.

Log message format

OA&M logs summarize security and administration-related events on CS 1000 systems. OA&M logs record who did what, when, and whether the action was successful.

The log record format is as follows:

Priority Time-Generated Time-Reported Hostname Message [UserName: Remote network device identity /managed element IP /X.500 Object Identifier: Severity: MessageString - Result]

- Priority represents the priority of the syslog message
- Time-Generated represents the time at which the message arrived at the consolidation point
- Time-Reported represents the time of the event.
- Hostname represents the host name of the Linux server. If the host name is not available, it shows the IP address of the Linux server.

The message fields areas follows:

- Username defines the UCM Common Services user name of the administrator or the server invoking the request.
- Remote network device identity represents the remote network device identity, managed element IP address, or X.500 Object Identifier.
- Severity represents the syslog level of the message.
- MessageString represents the body that specifies the log message content.
- Result includes the result of the action performed, indicating whether it is successful.

Sample OA&M audit log messages include the following:

Copyright © 2010 Nortel Networks. All Rights Reserved.

- local3.info Aug 26 12:34:27 Aug 26 12:34:27 hpss1 admin: 192.168.55.173: Info: Restart SIP Proxy Server – SUCCESS
- local3.alert Aug 26 12:34:27 Aug 26 12:34:27 hpss1 admin: 192.168.55.173: Alert: Restart Gatekeeper service – FAIL

Logging events

The following log files are viewable by the log viewer:

- Application logs are generated by applications that use the Linux syslog daemon to log messages.
  - Line TPS
  - SIP Line Gateway
  - SIP Signaling Gateway
  - NRS Routing components (Network Connection Server, H.323 Gatekeeper)
  - Management Bundle
  - Linux Base
  - Co-resident Signaling Server
  - any other Nortel-specific application
- OA&M security-related events are recorded in security.log files. Examples of security events include the following:
  - Security policy changes
  - Log on successes and failures
  - Certificate changes
  - User Account Creation and Illegal (failed) Login Events
  - Any OA&M security event where security administrator privilege (or flag) is enabled or required

  OA&M administration events are recorded in oam.log files. Examples of administration events include the following:
  - Operational Events: captures queries for status and enabling or disabling resources.
  - Configuration Events: captures all feature or functional provisioning and modifications.
  - Maintenance Events: captures all upgrades, backups, restores and patching.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Further information

For further information about installing OA&M Transaction Audit and Security Event Logging, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315). For further information about configuring of OA&M Transaction Audit and Security Event Logging, see *Security Management Fundamentals* (NN43001-604).

Copyright © 2010 Nortel Networks. All Rights Reserved.

NRS functionality

Contents

This chapter contains the following topics:

"Introduction" (page 57)

"Network overview" (page 58)

- "Coordinated endpoint configuration across multiple NRS zones" (page 58)
- "NRS purpose" (page 63)
- "H.323 Gatekeeper discovery" (page 64)
- "H.323 Endpoint registration" (page 65)

"NRS Manager" (page 69)

- "Security" (page 69)

"NRS operating parameters" (page 69)

"Standalone NRS support for Meridian 1 and BCM nodes" (page 76)

- "Meridian 1/BCM node-based numbering plan" (page 77)
- "NRS-based numbering plan" (page 78)

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

The NRS can co-reside on the Signaling Server with other applications (co-resident mode) or operate in stand-alone mode.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

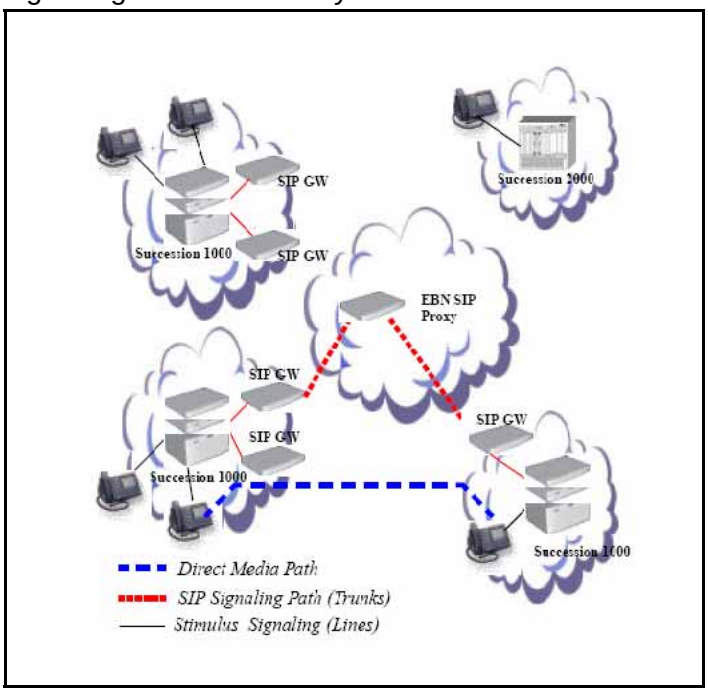
SIP operation

The SIP Proxy and 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 Proxy and Redirect Server. The SIP Proxy and Redirect Server then redirects the SIP Trunk Gateway to where it needs to send signaling.

The SIP Proxy Server acts as both server and client for the purpose of making requests on behalf of other SIP endpoints. The proxy accepts an incoming request, performs a look up on the Request-URI through some form of a location service, and then forwards the request to the retrieved location(s). Within this model, the proxy will maintain the state of the call through the final response of a transaction.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The following figure describes how the corporate network utilizes SIP signalling and a SIP Proxy server.



The SIP Trunk Gateways contact either the Proxy server or the Redirect server. The SIP Gateways cannot contact both the servers.

The SIP Redirect Server in Redirect mode receives requests but, rather than passing these requests to another SIP server, it returns a response back to the originator of the request.

SIP Trunk Gateways and SIP IP Phones forward calls to the contact address returned by the SIP Proxy and Redirect Server in Redirect mode as described in this example:

1. A SIP Trunk Gateway sends an INVITE message to the SIP Proxy and Redirect Server in Redirect mode.
2. The SIP Server returns a redirect message to the originator with the addressing information for the destination node.
3. The originator sends an INVITE message directly to the SIP Trunk Gateway destination node.

For example, User A contacts User B across the enterprise network. The following sequence occurs:

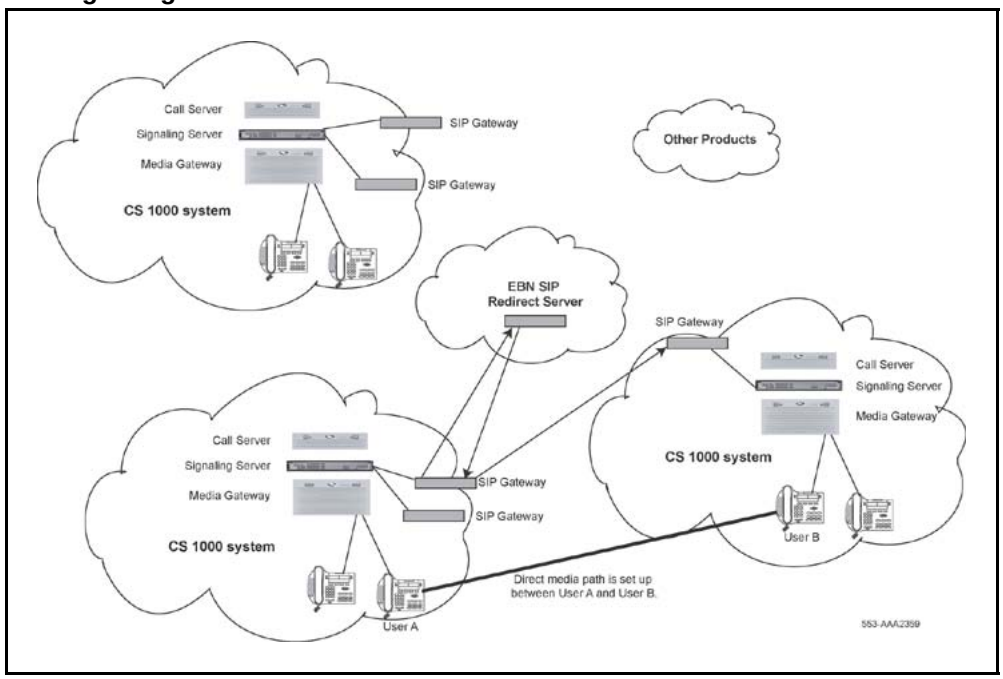
1. User A contacts the SIP Trunk Gateway. (That is, User A sends an address-resolution request to the SIP Trunk Gateway.)
2. The User A's SIP Trunk Gateway contacts the EBN SIP Proxy and Redirect Server in Redirect mode.

Copyright © 2010 Nortel Networks. All Rights Reserved.

3. The EBN SIP Proxy and Redirect Server in Redirect mode performs a location lookup to determine whether the database contains an address match for the domain of User B.
4. If a match is found, the SIP Proxy and Redirect Server in Redirect mode 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 Proxy and Redirect Server in Redirect mode redirects User A's SIP Trunk Gateway to User B's SIP Trunk Gateway.)
5. User A's SIP Trunk Gateway uses the provided contact address and directly communicates with User B's SIP Trunk Gateway.
6. A direct media path is then set up between User A and User B.

Figure 12 "SIP Signaling and SIP Redirect Server" (page 60) shows how the SIP Proxy and Redirect Server in Redirect mode accepts a request from a SIP Trunk Gateway and returns the response to the SIP Trunk Gateway. The SIP Trunk Gateway can then contact the called party's SIP Trunk Gateway directly. After 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 Proxy and Redirect Server in Redirect mode finds no matching numbering plan entries, (the database returns a NULL entry), then the SIP Server transmits a SIP 404 (Not Found) response.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 6
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 Succession 3.0 H.323 Gatekeeper	the alias address of the peer H.323 Gatekeeper that sent the LRQ message	(not applicable)
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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

- 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 22 “Adding a Collaborative Server” (page 204).

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 NRS to support a centralized Network Numbering Plan. Each NRS has a zone that administers its own numbering plan and requests other NRS 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 81).

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

load balancing.The Gatekeeper knows that the IP Trunk 3.0 (or later) IP address used in the ARQ belongs to the node, because 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Configure the Time-to-Live timer using NRS Manager. Nortel recommends that the timer be configured to 30 seconds. See Procedure 8 “Configuring system-wide settings” (page 175).

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 or Proxy Server (that is, with the SIP Registrar component). This eliminates some manual provisioning at the SIP Server. It also reduces the potential for error when manually entering the IP address of the SIP Trunk Gateway in the SIP 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, see “SIP Phone dynamic registration” (page 114).

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

NRS Manager has two access levels:

- Administrator 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.

For detailed information about 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, see *Security Management Fundamentals* (NN43001-604).

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 Proxy and 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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, see *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, see *Branch Office Installation and Commissioning* (NN43001-314).

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

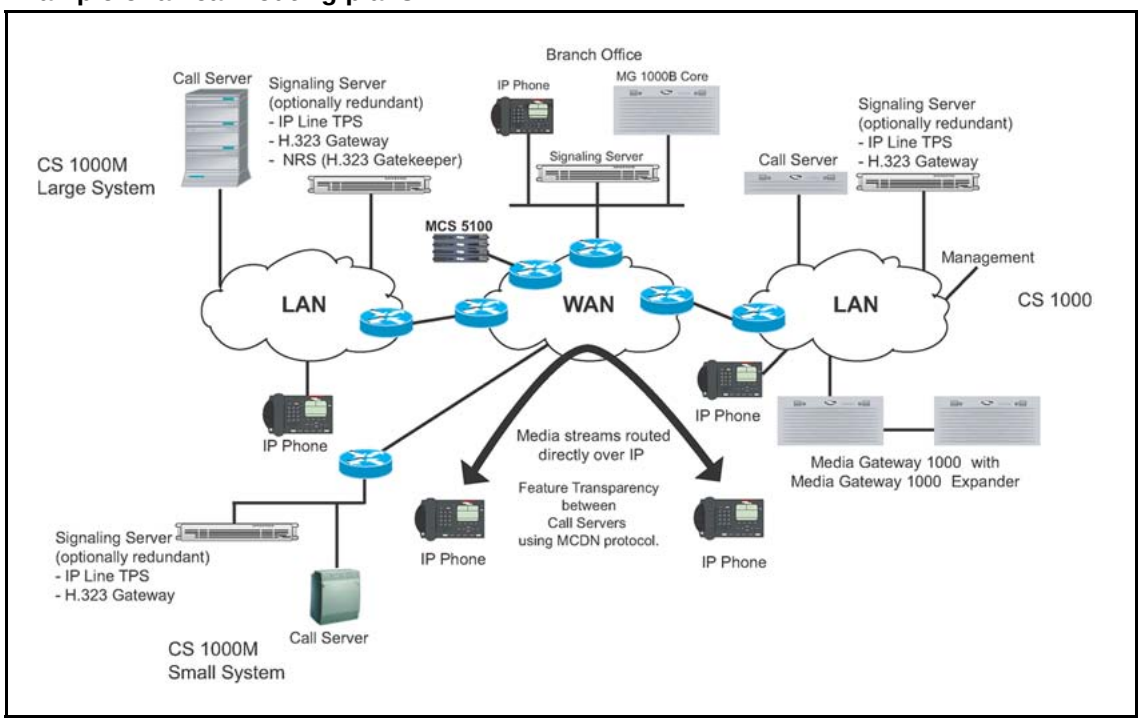
All number and cost factor pairs within a numbering plan table are unique for private numbering plans. When adding an H.323 alias for a predefined H.323 endpoint, the request is rejected if the administrator specifies an alias type and provides a number string and cost factor that is already in the numbering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

For example, Figure 13 "Example of all call routing plans" (page 72) 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



Copyright © 2010 Nortel Networks. All Rights Reserved.

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 74).

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 octothorpe 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 72) would result in Table 7 "privateNumber.level1RegionalNumber numbering plan" (page 74) through Table 14 "Endpoint Status Table" (page 76).

Table 7
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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 7
privateNumber.level1RegionalNumber numbering plan (cont'd.)

Digits	Terminating Routes			
	H323-ID	Cost Factor	H323-ID	Cost Factor
665-669	SCN_MPK_1	1		
6651200#	BCM_BVW_1	1		

Table 8
privateNumber.pISNSpecificNumber numbering plan

Digits	Terminating Routes	
	H323-ID	Cost Factor
265	SCN_MPK_2	1

Table 9
publicNumber.internationalNumber numbering plan

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

Table 10
CDP domain table

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

Table 11
CDP_DOMAIN_2 numbering plan

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 12
MPK_CDP_DOMAIN numbering plan

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

Table 13
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 14
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	

Standalone 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 77) illustrates how the Meridian1/BCM handles call admission control and numbering plan resolution.

Figure 14
Meridian 1/BCM node-based numbering plan

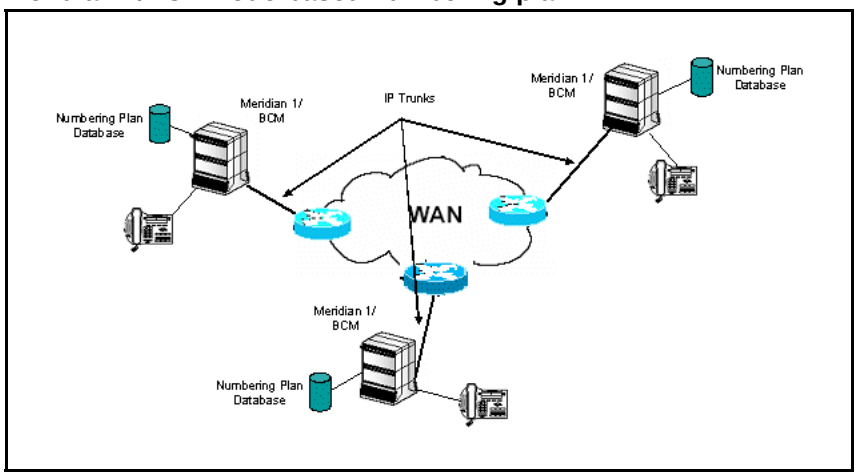


Figure 14 "Meridian 1/BCM node-based numbering plan" (page 77) shows a Meridian 1/BCM network with the Meridian 1/BCM nodes equipped with IP Trunks. The IP Trunk routes are point-to-multipoint. Regardless of where the terminating node is located, all calls can be sent out over the same route. The calls 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:

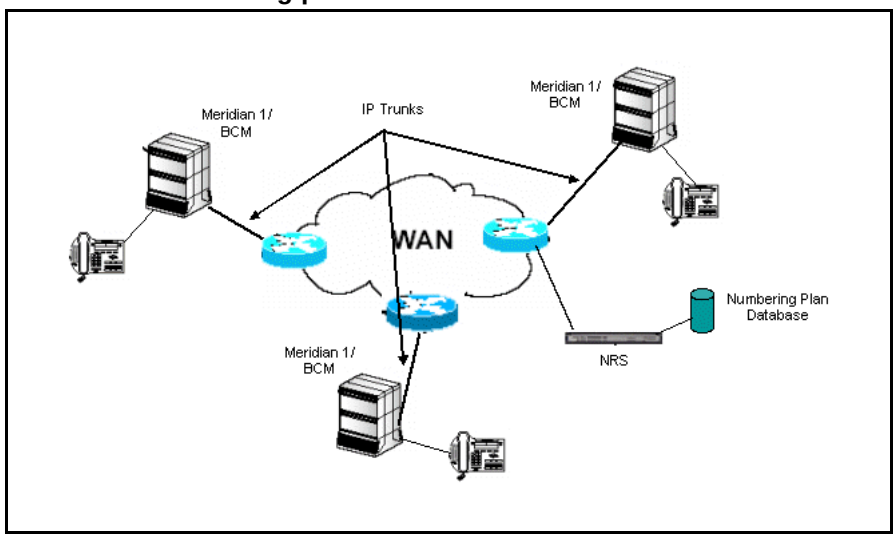
1. The node consults its numbering plan.
2. The node determines where the destination is located.
3. The node retrieves the statically configured destination IP address.
4. The node routes the call directly to the destination node.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 78).

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Numbering plans

Contents

This chapter contains the following topics:

"Introduction" (page 81)

"Private (on-net) numbering plans" (page 82)

"Public (off-net) numbering plans" (page 85)

"Address translation and call routing" (page 87)

"H.323" (page 87)

"SIP" (page 87)

"Basic call routing" (page 87)

"Numbering plan entry overview" (page 91)

"Numbering plans and routing" (page 94)

"Using an NRS for routing" (page 94)

"Transferable DN call routing operation" (page 96)

"CDP call routing operation" (page 97)

"UDP call-routing operation" (page 98)

"Off-net call routing operation" (page 99)

"Routing to and from a branch office or SRG" (page 99)

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

"Numbering plan entry overview" (page 91) 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 Location Code and DN of the user. 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

For call routing information, see "UDP call-routing operation" (page 98).

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 84)).

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, see *Dialing Plans: Description* (NN43001-283).

For call routing, see "CDP call routing operation" (page 97).

Copyright © 2010 Nortel Networks. All Rights Reserved.

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, see *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 96).

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.

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

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 98).

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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, see *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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 places a call, it sends an INVITE message to the SIP Proxy and Redirect Server by way of the SIP Trunk Gateway. The endpoint includes the destination telephone number in the message. The destination information is a SIP URI (see "SIP Uniform Resource Identifiers" (page 41)). The SIP Proxy and Redirect Server searches the numbering plan database to determine which endpoints on the network can terminate the telephone number and whether these endpoints are registered. Address lookup is based on the digits, phone context, and domain name.

The SIP Proxy and 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 96) 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 82) and "Public (off-net) numbering plans" (page 85) are described in "Numbering plans and routing" (page 94).

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 15 "H.323 term explanations" (page 88).

Table 15
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.	

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 15 "H.323 term explanations" (page 88).

Mapping between CS 1000 NPI/TON and H.323 alias types The CS 1000 system supports the NPI and TON values shown in Table 16 "NPI values" (page 89) and Table 17 "TON values" (page 89). These values are for Universal ISDN Protocol Engine (UIPE)-formatted NPI/TON numbers.

Table 16
NPI values

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

Table 17
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 18 "NPI/TON to H.323 alias mapping" (page 90) 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).

Copyright © 2010 Nortel Networks. All Rights Reserved.

If the H.323 Proxy Server receives a Q.931 SETUP message for an NPI/TON pair not included in Table 18 "NPI/TON to H.323 alias mapping" (page 90), 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 18
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 17 "TON values" (page 89))	LOC	privateNumber.level1RegionalNumber
	COORDINATED (see Table 17 "TON values" (page 89))	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 19 "Q.931 TON mapping" (page 90) shows Q.931 TON mapping.

Table 19
Q.931 TON mapping

NPI	TON
x000xxxx	Unknown
x001xxxx	International Number
x010xxxx	National Number
x011xxxx	Network Specific Number
x100xxxx	Subscriber Number

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 19
Q.931 TON mapping (cont'd.)

NPI	TON
x110xxxx	Abbreviated Number
x101xxxx x111xxxx	Reserved for Extension

Table 20 "NPI/TON to ESN Call type mapping" (page 91) shows the NPI/TON to ESN Call type mapping.

Table 20
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 Procedure 41 “Adding a Routing Entry” (page 246).

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

If a user dials 1613966, the NRS matches entries with 161396. See Table 21 "Cost factors" (page 92) for the cost factors associated with these entries.

Table 21
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 routes can also be configured for each of the supported numbering plan types. These entries are configured by entering the DN type 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

For information about VNR operation, see *Dialing Plans: Description* (NN43001-283).

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The basic role of a SIP Proxy and 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).

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 97) shows a network of CS 1000 Systems in which each user wants to retain their unique seven-digit Directory Number. Table 22 "DNs with their associated Call Servers" (page 97) provides a summary of the DNs in Figure 16 "Transferable DN routing" (page 97), 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 97) 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 16
Transferable DN routing

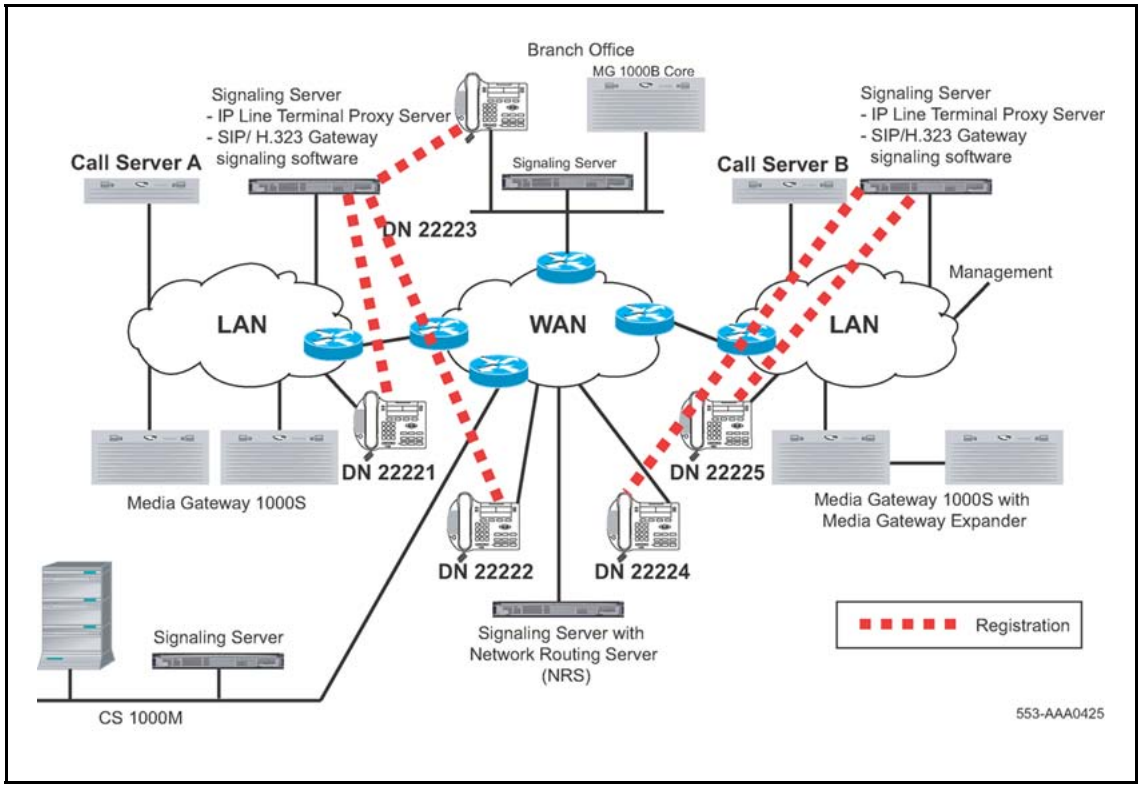


Table 22
DNs with their associated Call Servers

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 17 "CDP call routing" (page 98) shows an example of CDP routing. Table 23 "DNs with their associated Call Servers and CDP domains" (page 98) shows the DNs with their associated Call Servers and CDP domains.

Figure 17
CDP call routing

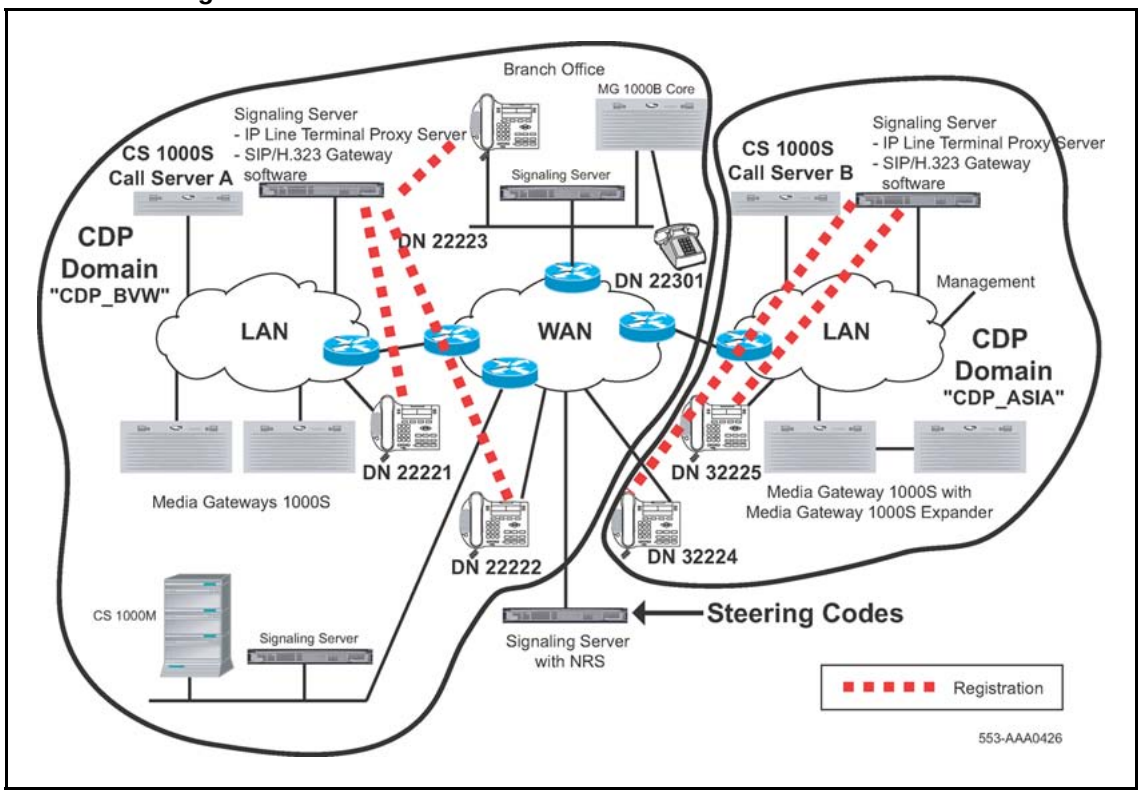


Table 23
DNs with their associated Call Servers and CDP domains

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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. *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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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. For more information, see *Branch Office Installation and Commissioning* (NN43001-314).

Copyright © 2010 Nortel Networks. All Rights Reserved.

SIP Phone support

Contents

This chapter contains the following topics:

"Introduction" (page 101)
- "SIP Phone interaction" (page 102)
- "SIP Phone features" (page 103)

"SIP IP Phone Startup" (page 104)

"SIP Phone calls" (page 105)
- "SIP Phone-to-SIP Phone communication" (page 106)
- "SIP Trunk Gateway-to-SIP Phone communication" (page 109)

"SIP Phone dynamic registration" (page 114)
- "Assumptions" (page 114)
- "Log files" (page 115)

"Installing a SIP Phone" (page 115)

"Configuring a SIP Phone" (page 115)
- "Routing of unqualified numbers" (page 115)
- "Task summary" (page 116)

Introduction

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

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 IP Phones use the Session Initiation Protocol which is an open industry standard-based signaling protocol. Some of the telephony features of the SIP IP Phones are delivered by the Communication Server. However, SIP IP 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 IP Phone is a standards-based SIP device.

CS 1000 does not support Call Forward across NRS Collaborative Servers by third-party SIP IP Phones.

In CS 1000 Release 6.0, SIP Phones are supported only on the SIP Line Gateway — not on the trunk registering to the SIP Proxy Server.

With the introduction of CS 1000 Release 6.0 SIP Line Service and support of SIP IP Phones directly connected to the CS 1000 with Release 6.0 SLG and SIPL universal extensions, only the MC 3100, OCS and SIP DECT are supported with the SIP Proxy Server. For further information, see *SIP Line Fundamentals* (NN43001-508) .

SIP Phone interaction

Table 24 "SIP Phone and CS 1000 component interaction" (page 102) shows the interaction between SIP Phones and components in the CS 1000 network.

Table 24
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 103) for more details. SIP Phones can also have other manufacturer-dependant features.
SIP Proxy Server	The NRS, specifically the SIP Proxy 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)

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 24
SIP Phone and CS 1000 component interaction (cont'd.)

Component	Description
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
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
- Local or trunk call between Dual stack
- Local or trunk call between Dual stack and IPv4

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

- 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 115).

SIP IP Phone Startup

You can start the dual stack SIP IP Phone—IPv4 or IPv6 ANAT—according to the requirement. To start the IPv4 or IPv6 SIP IP Phone, use the following procedure.

Procedure 1
Booting IPv4 or IPv6 SIP IP Phones

Step	Action
1	Install dual stack software on the SIP IP Phone with IPv4 or IPv6 ANAT preference.
2	Select **Enable IPv6 for IPv6** preference.
3	Clear **Enable IPv6** for IPv4 preference.
4	Configure the **Server Settings** with the IPv6 or IPv4 SLG IP address according to the SLG capabilities.
5	Set **Port** as 5070.
6	In the **Device Settings** for dual stack preference, enter both IPv6 and IPv4 addresses.
7	Enter the **Username** and **Password** to log on to the SIP IP Phone.

--End--

Use the following settings to configure ANAT preference config file:

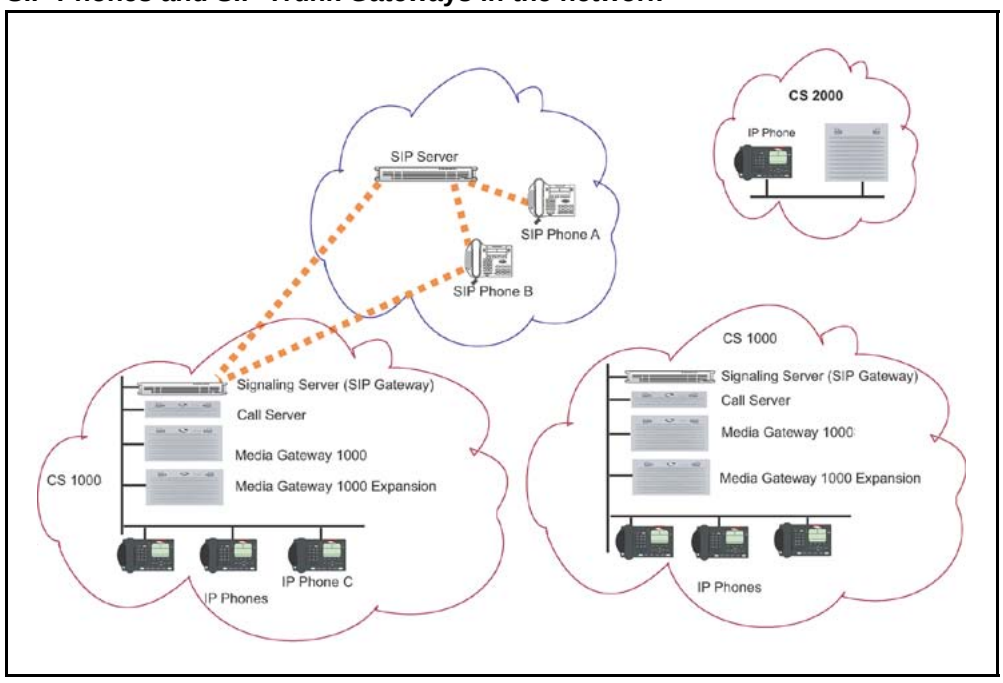
Copyright © 2010 Nortel Networks. All Rights Reserved.

```
************************************************
# Enable/Disable IPv6 settings
************************************************
IPV6_ENABLE Yes
PREFER_IPV6 Yes (For setting the ANAT preference)
IPV6_ENABLE_GUI Yes
```

SIP Phone calls

Figure 18 "SIP Phones and SIP Trunk Gateways in the network" (page 105) 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 Server for authentication and address resolution. Then communication is established between the two SIP Phones. See “SIP Phone-to-SIP Phone communication” (page 106) for the call flow between two SIP Phones in the same network.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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. See "SIP Trunk Gateway-to-SIP Phone communication" (page 109) 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.

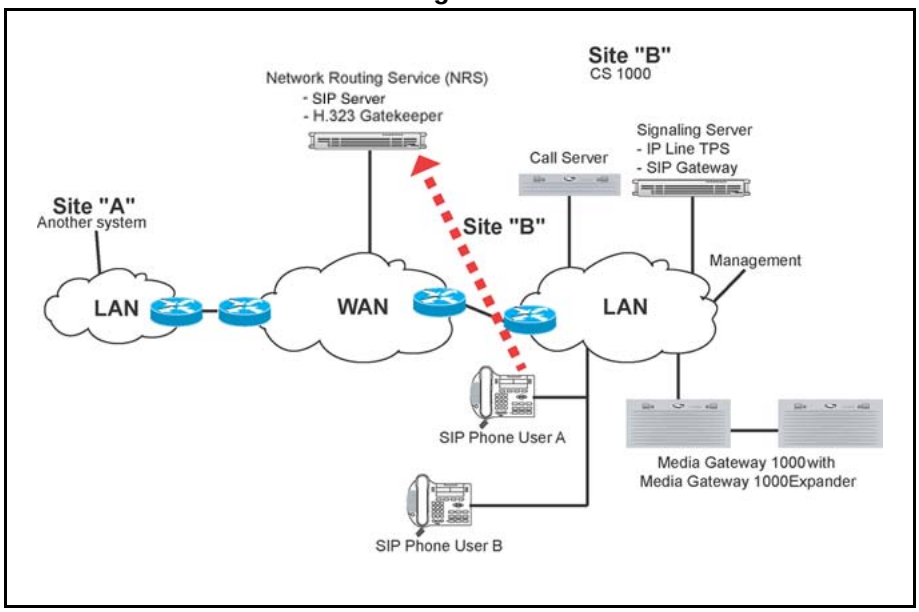
SIP Phone-to-SIP Phone communication

The following example pertains to the SIP Proxy in Redirect mode. When SIP Phone User A wants to call SIP Phone User B, the following occurs:

Note: The SIP Proxy Server is configured with IPv4 and IPv6 addresses. The Proxy Server has the dual stack IP address and handles incoming calls over the IPv4 or IPv6 interface. It forwards the call over the IPv4 or IPv6 interface depending on the far-end capability.

1. SIP Phone A sends an INVITE message to the NRS (specifically the SIP Server). See Figure 19 "SIP Phone A sends INVITE message to SIP Server" (page 106).

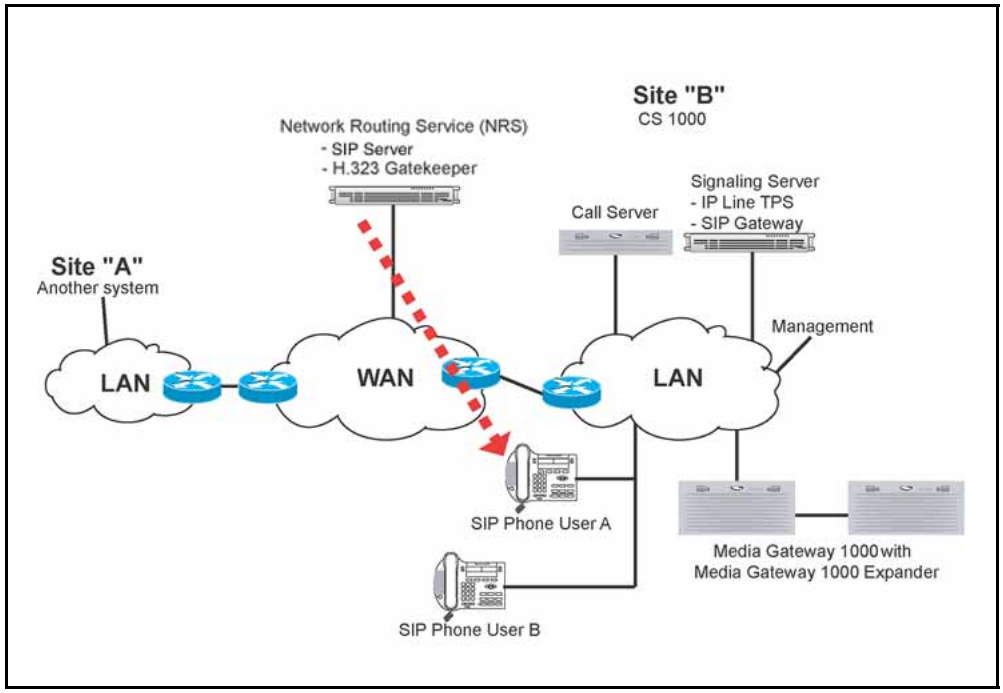
Figure 19
SIP Phone A sends INVITE message to SIP Server



2. The SIP Server responds with a REDIRECT message and informs SIP Phone User A to directly contact SIP Phone User B. See Figure 20 "SIP Server responds to SIP Phone A" (page 107).

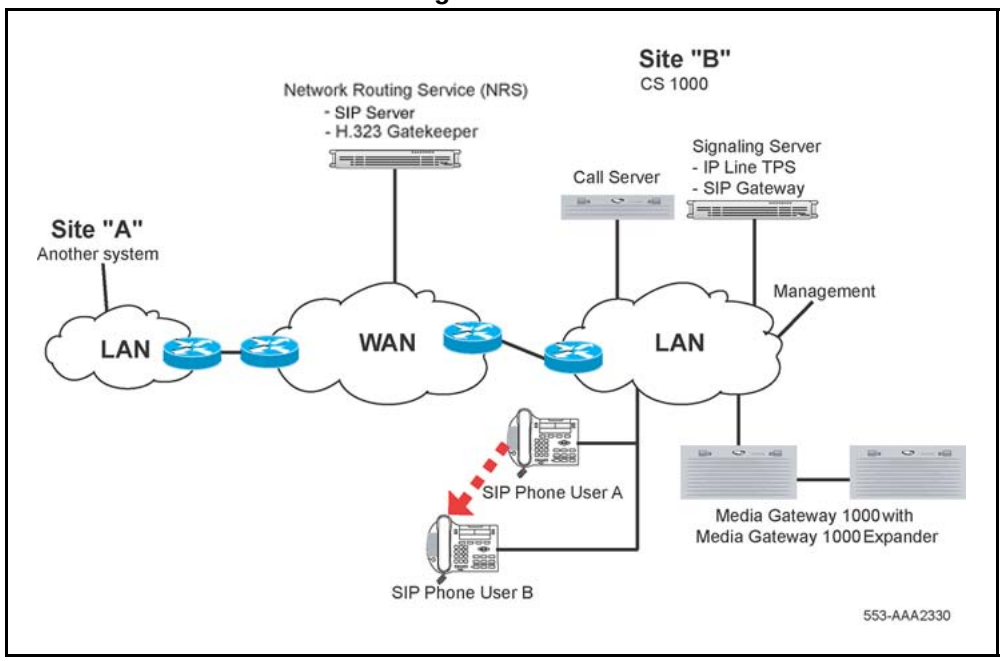
Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 20
SIP 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 107).

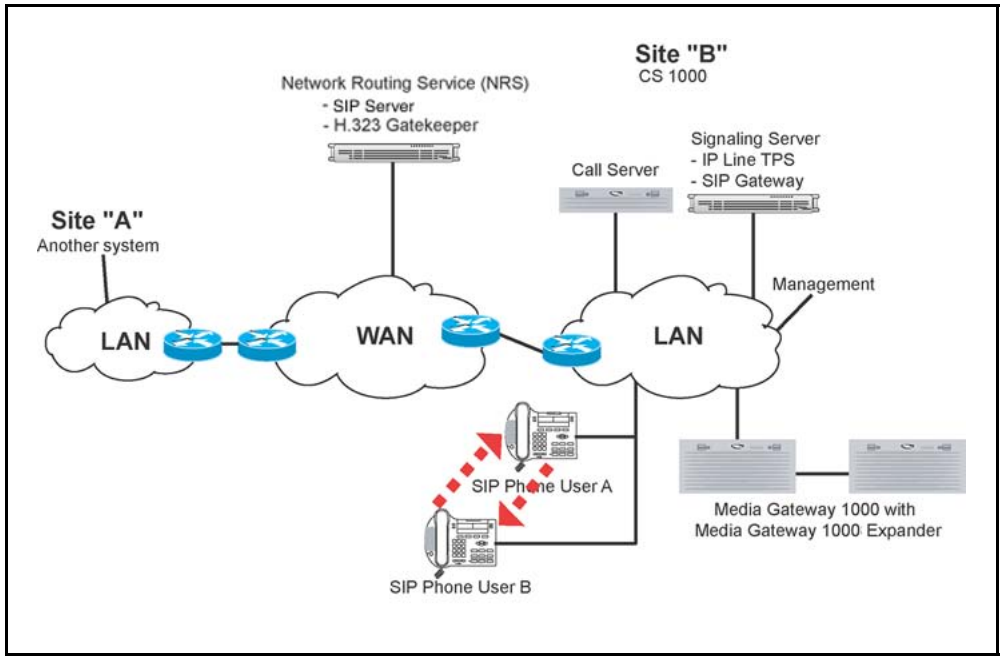
Figure 21
SIP Phone A sends INVITE message to SIP Phone B



Copyright © 2010 Nortel Networks. All Rights Reserved.

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 108).

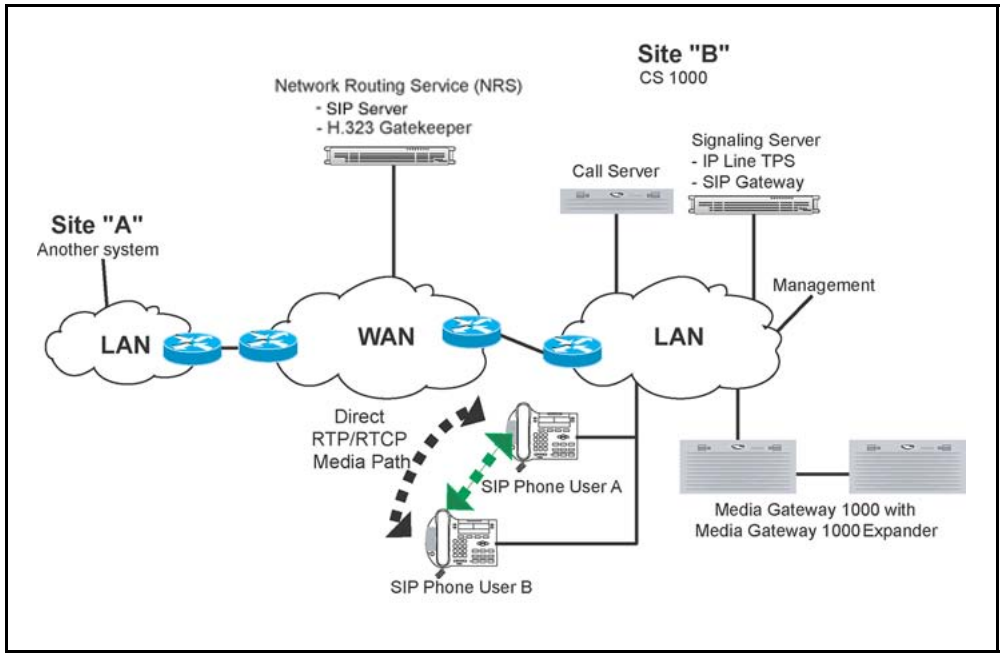
Figure 22
SIP Phone B sends 200 OK message to SIP Phone A



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 109).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 23
SIP Phones start the direct IP media paths



When SIP Phone A sends an INVITE message to the NRS, the server returns a message to the SIP Phone A user to directly contact SIP Phone B. Now when SIP Phone A calls SIP Phone B, the call is connected directly and the conversation can start.

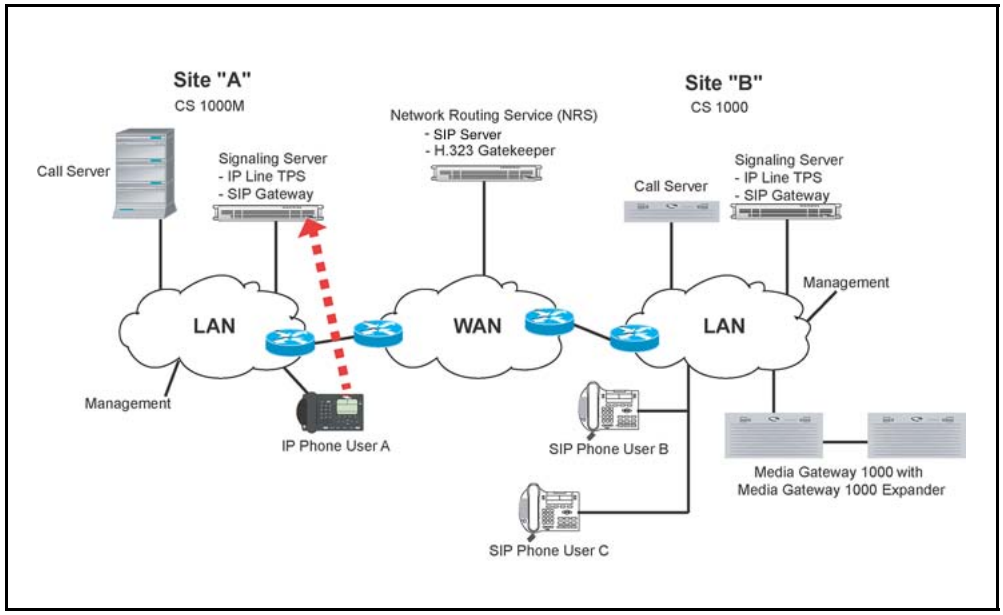
SIP Trunk Gateway-to-SIP Phone communication

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 110).

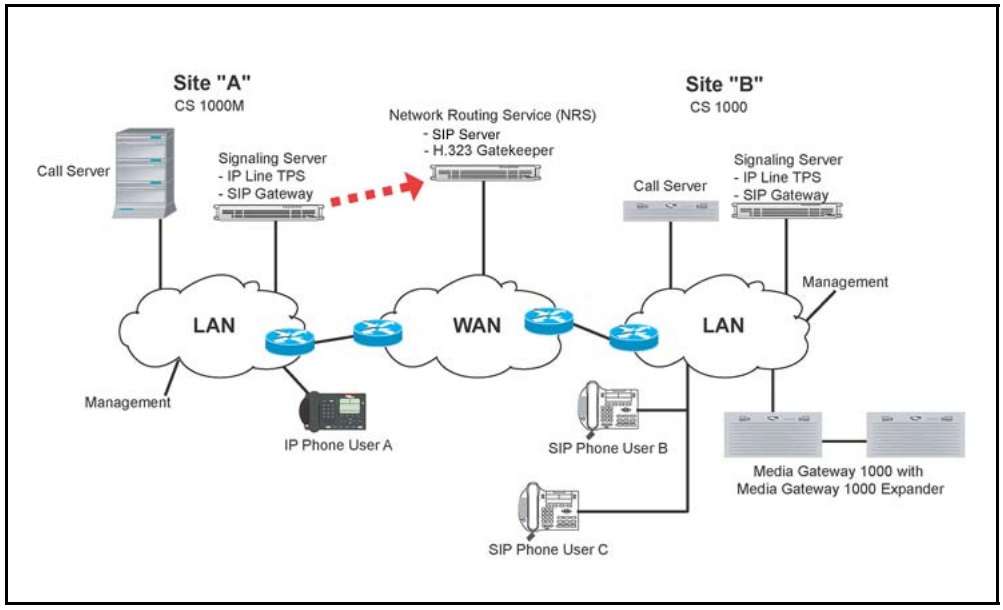
Copyright © 2010 Nortel Networks. All Rights Reserved.

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 Server). See Figure 25 "SIP Trunk Gateway A sends INVITE message to SIP Server" (page 110).

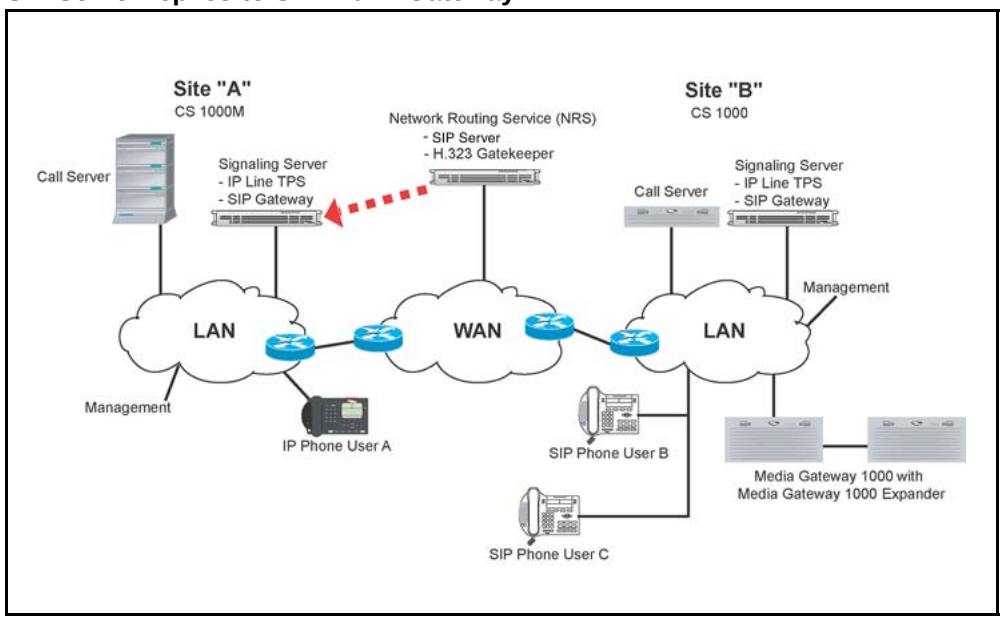
Figure 25
SIP Trunk Gateway A sends INVITE message to SIP Server



3. The SIP Server replies back to SIP Trunk Gateway A with a REDIRECT message. The SIP Server informs SIP Trunk Gateway A of the location of SIP Phone B. See Figure 26 "SIP Server replies to SIP Trunk Gateway A" (page 111).

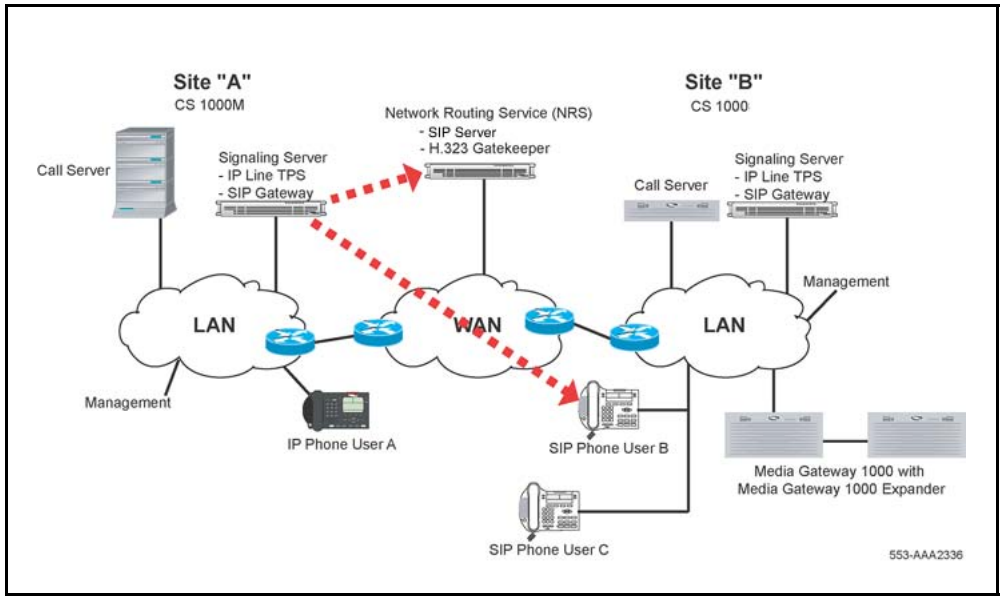
Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 26
SIP Server replies to SIP Trunk Gateway A



4. SIP Trunk Gateway A acknowledges the message from the SIP 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 111).

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

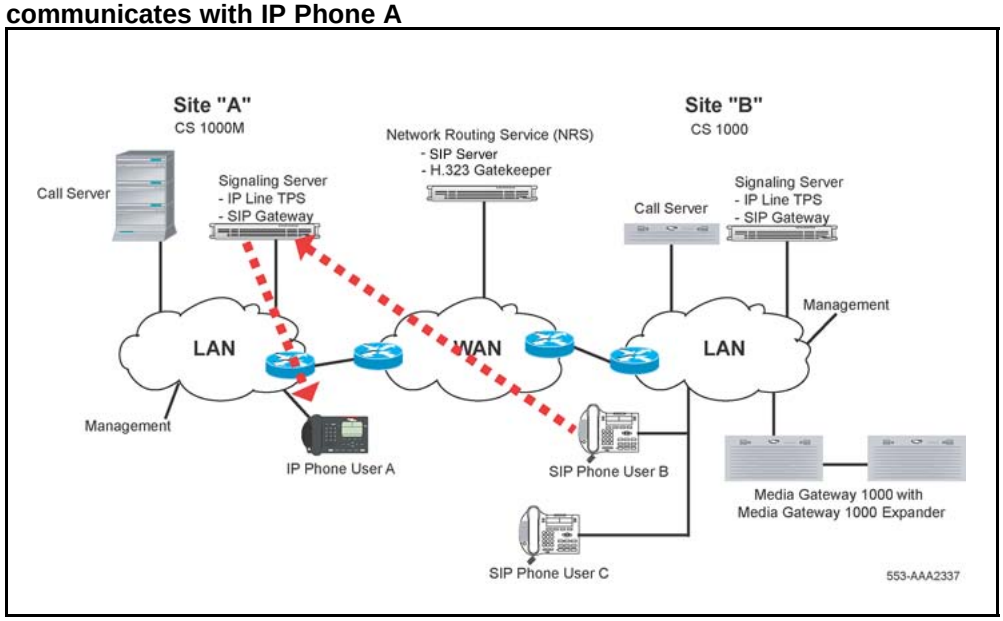


5. SIP Phone B sends a TRYING message and a Ringing message to the SIP Trunk Gateway A. SIP Trunk Gateway A then sends an Alerting message to IP Phone A. See Figure 28 "SIP Phone B communicates

Copyright © 2010 Nortel Networks. All Rights Reserved.

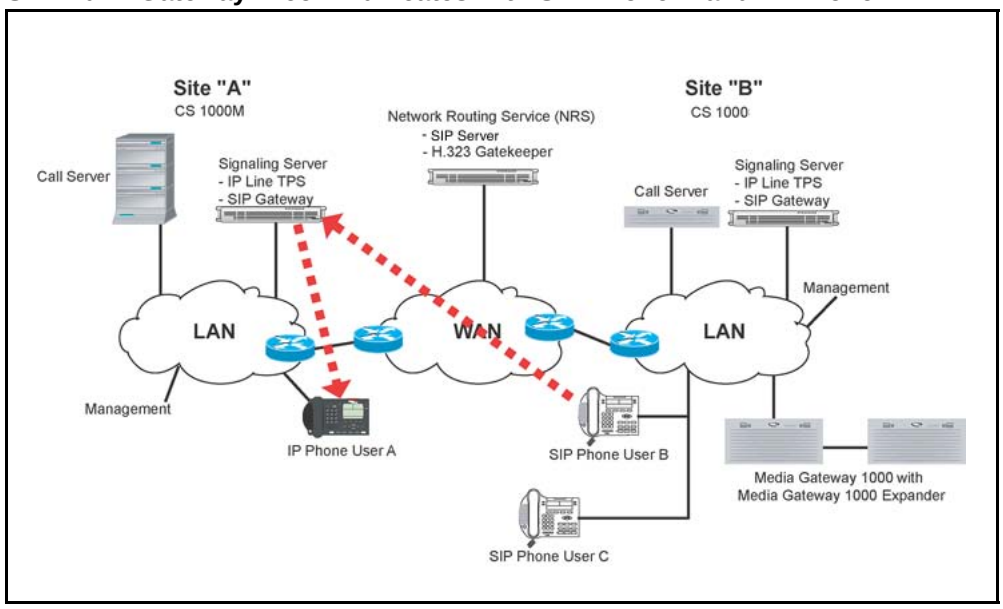
with SIP Trunk Gateway A and SIP Trunk Gateway A communicates with IP Phone A" (page 112).

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 112).

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

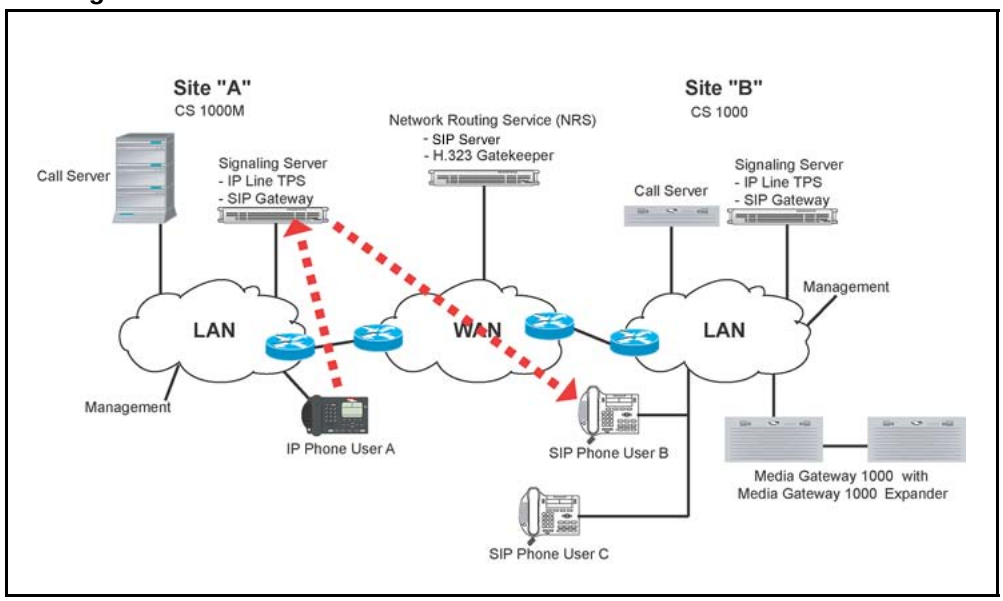


7. IP Phone User A responds to SIP Trunk Gateway A with a Connect ACK message. SIP Trunk Gateway A sends a SIP 200 ACK message

Copyright © 2010 Nortel Networks. All Rights Reserved.

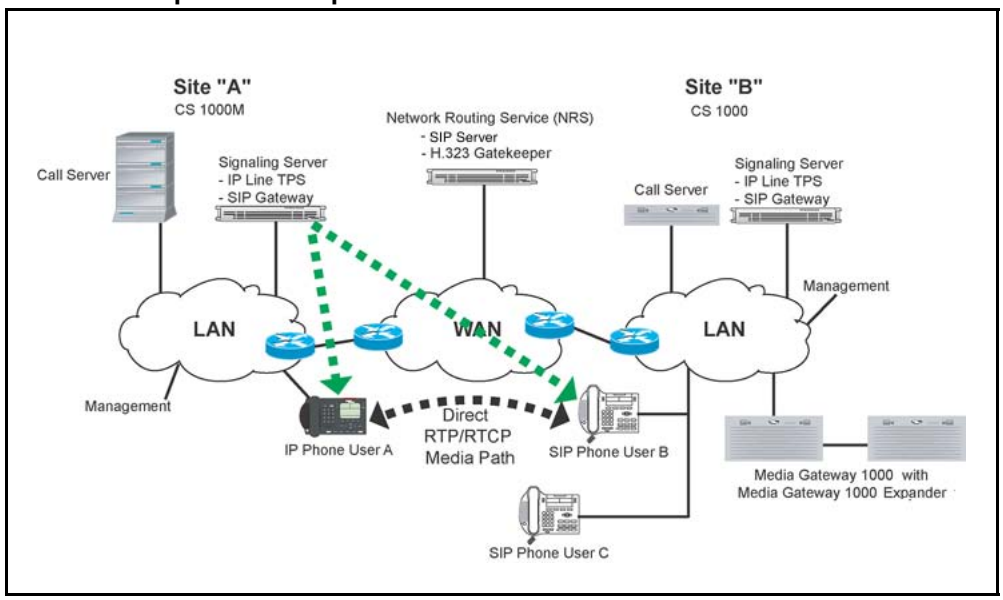
to SIP Phone B. See Figure 30 "IP Phone A acknowledges SIP Trunk Gateway A and SIP Trunk Gateway A sends SIP 200 ACK message to SIP Phone B" (page 113).

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 113).

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



Copyright © 2010 Nortel Networks. All Rights Reserved.

SIP IP Phone Log on failure

The user fails to log on to the SIP IP Phone due to the following reasons:

- user is not configured
- user is a client and the client type is not registered
- other internal errors

The SLG forwards the 404 not found message to SIP IP Phone. This is common for both IPv4 and dual stack phones.

The SLG also displays the status of the SIP Phone.

SIP Phone dynamic registration

SIP Phone dynamic registration helps create a contact list for the authorized SIP Phones. A SIP Phone registers as an endpoint with the SIP Proxy and Redirect Server (in the NRS). A telephone number and a user name are mandatory routing entries for the endpoint and are provided during provisioning in the NRS. See Procedure 35 “Adding a User Endpoint” (page 233).

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 Proxy and Redirect Server provides the phone context for SIP Phones for user calls from 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 Proxy and Redirect Server. The SIP Proxy and 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

- 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.

Note: You can determine if the SIP Phone is registered successfully by checking for the SIP line messages in the RLM table.

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)

Copyright © 2010 Nortel Networks. All Rights Reserved.

- 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 Linux-based NRS see

- Procedure 10 “Adding a Service Domain” (page 180)
- Procedure 14 “Adding an L1 Domain” (page 186)
- Procedure 18 “Adding an L0 Domain (CDP)” (page 195)

To add a SIP Phone in Linux-based NRS as a User Endpoint, perform the steps in Procedure 35 “Adding a User Endpoint” (page 233).

SIP IP Phone logoff

To log off the IPv4 or IPv6 SIP IP Phones, perform the Procedure 2 “Logging off from the SIP IP Phones” (page 116).

Procedure 2
Logging off from the SIP IP Phones

Step	Action
1	Press either the **Servcs** Context-sensitive soft key or the **Services** fixed key, select **System** , and then select **Logout** from the menu.
2	Press the **Logout** Context-sensitive soft key to complete the logoff process.
	--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Configure and manage the Network Routing Service

Contents

This chapter contains the following topics:

"Introduction" (page 119)

"Installation of Linux operating system, UCM Common Services and NRS application" (page 120)

"CS 1000 task flow" (page 121)

"Upgrade Linux-based NRS Release 5.0 or 5.5 to Release 7.0" (page 123)

"Migration from Solid database to MySQL" (page 124)

"Access NRS Manager through the UCM Common Services" (page 126)

"Initial configuration of NRS on a new IP Peer network" (page 127)

"Configure NRS database user endpoints" (page 131)

"Configuring IPv6 in NRSM" (page 161)

"Upgrade of an IP Peer Network from VxWorks-based NRS to Linux-based NRS" (page 131)

"Recovery from failure of Linux-based NRS" (page 148)

"Operation and maintenance commands" (page 149)

"Browser configuration" (page 149)

"Log in to UCM Common Services and Access NRS Manager" (page 151)

"NRS Manager interface" (page 154)

"Log out of UCM Common Services" (page 163)

Copyright © 2010 Nortel Networks. All Rights Reserved.

"Configure the Primary and Secondary NRS Server Settings" (page 163)

"Configure system-wide settings" (page 175)

"Configure the NRS database" (page 177)

"Switch between the Active and Standby databases" (page 178)

"Manage a Service Domain" (page 179)

"Manage a Level 1 Domain (UDP)" (page 186)

"Manage a Level 0 Domain (CDP)" (page 195)

"Manage a Collaborative Server" (page 204)

"Manage a Gateway Endpoint" (page 213)

"Manage Post-routing SIP URI Modification" (page 227)

"Manage a User Endpoint" (page 232)

"SIP Phone Context " (page 244)

"Manage a Routing Entry" (page 245)

"Manage a Default Route" (page 258)

"Manage bulk export of routing entries" (page 264)

"Manage bulk import of routing entries" (page 267)

"Verify the numbering plan and save the NRS configuration" (page 280)

"H.323 and SIP Routing Tests" (page 281)

"Enable, disable and restart the NRS Server" (page 284)

"Perform NRS database actions" (page 286)

"Backup the database" (page 291)

"Restore the NRS database" (page 296)

"GK/NRS Data Upgrade" (page 304)

Copyright © 2010 Nortel Networks. All Rights Reserved.

Introduction

> ***Note:*** When components of an IP Peer network are upgraded to CS 1000 Release 5.0 or later, the Network Routing Servers must be running the highest release software installed on the network.

The Network Routing Service (NRS) can be configured and maintained through a web interface called NRS Manager. The Linux-based NRS Manager can be deployed on the Nortel Unified Communications Management Common Services (UCM Common Services). The UCM Common Services provides security and navigation infrastructure services for the web-based management applications: Element Manager (EM), Subscriber Manager 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 UCM Common Services Security Domain to assure a highly available authentication and authorization service for OA&M users who need to access managed systems/elements in the UCM Common Services Security Domain, as well as for auxiliary applications that rely on continuous availability of the UCM Common Services web services API to monitor and control the CS 1000.

The Nortel Linux platform uses Centralized Deployment Manager to remotely deploy Nortel application software from the UCM Common Services Primary Security server to other Linux servers in the same security domain.

The UCM Common Services base application provides the necessary system functions and must be successfully installed for the EM, Subscriber Manager, and NRS Manager applications to work. The UCM Common Services base application resides on the Linux base installation media and is installed automatically the first time the system starts after base installation. The success or failure of the base applications installation appears in an on-screen message. If the base application installation fails, you must reinstall the Linux base.

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

1. The Nortel-customized Red Hat Enterprise Linux operating system must be installed.
2. The Primary NRS and the UCM Common Services must be installed, and the co-resident Primary Security Service must be installed if a new UCM Common Services Security Domain will be created

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

Note 1: Nortel recommends that you configure a Backup Security Service when one or more Nortel Linux-based servers are joined as members of an existing UCM Common Services Security Domain. This ensures continued access to UCM Common Services system management applications in case the UCM Common Services Primary Security service fails.

Note 2: Nortel recommends that you configure a Secondary NRS for every NRS zone to ensure high-availability of the CS 1000 NRS.

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

Installation of Linux operating system, UCM Common Services and NRS application

For information about installing the Linux operating system, the NRS application and the NRS Manager, the UCM Common Services, the MySQL database, and the UCM Common Services Security Services, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

For information about adding a managed element to the UCM Common Services, creating user accounts, and assigning roles and permissions for access to the NRS server from the UCM Common Services, see *Unified Communications Management* (NN43001-116).

The NRS and EM are installed on dedicated 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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:*** A UCM Common Services Security Domain member server is a server that has the UCM Common Services installed, but does not have the Primary Security Service or the Backup Security Service installed. All UCM Common Services 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 UCM Common Services Security Domain member server web pages are inaccessible.
>
> ***Note 2:*** If the Primary Security Service is installed on the Element Manager server, then 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 is ensured if the servers are on the same LAN.

For information about 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, see *Security Management Fundamentals* (NN43001-604).

CS 1000 task flow

This section provides a high-level task flow for the installation or upgrade of a CS 1000 system. The task flow indicates the recommended sequence of events to follow when configuring a system and provides the NTP number that contains the detailed procedures required for the task.

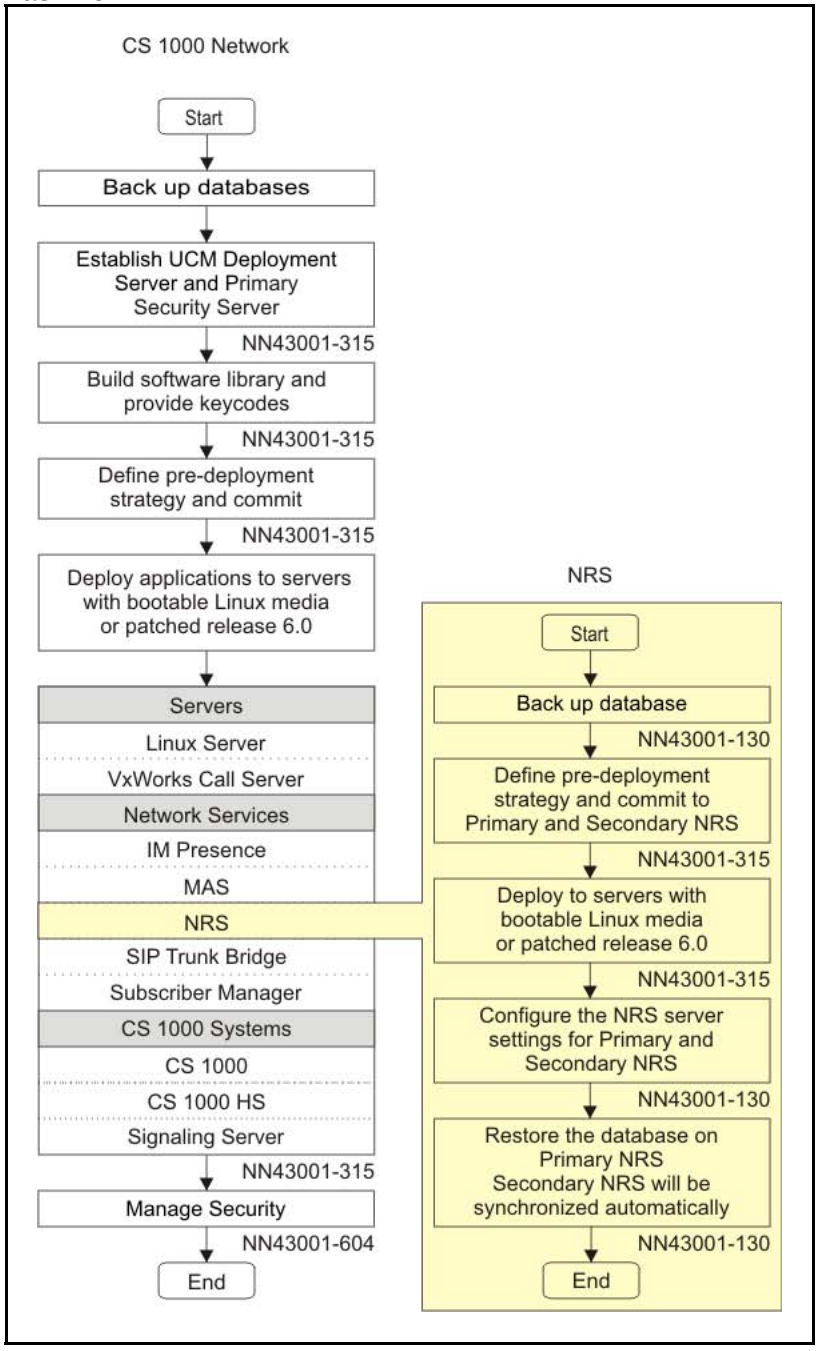
For more information, see the following NTPs, which are referenced in the task flow diagram:

- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Branch Office Installation and Commissioning* (NN43001-314)
- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *SIP Line Fundamentals* (NN43001-508)
- *Security Management Fundamentals* (NN43001-604)
- *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310)
- *CS 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458)

Copyright © 2010 Nortel Networks. All Rights Reserved.

- *Communication Server 1000E Installation and Commissioning* (NN43041-310)
- *Communication Server 1000E - Upgrade Procedures* (NN43041-458)

Figure 32
Task flow



Copyright © 2010 Nortel Networks. All Rights Reserved.

Upgrade Linux-based NRS Release 5.0 or 5.5 to Release 7.0

Nortel recommends that you do not upgrade NRS while traffic runs on a server that has NRS hosted co-resident with Signaling Server applications. The operation can take a large amount of time depending on the amount of information and the traffic rate.

> ***Note:*** 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 or later.

See "Backup the database" (page 291) for detailed information on backing up the NRS database.

For information about upgrading the Linux operating system, the NRS application and the NRS Manager, the UCM Common Services, the MySQL database, and the UCM Common Services Security Services, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

For information about restoring the NRS database, see "Restore the NRS database" (page 296).

> ***Note:*** The Linux-based NRS for CS 1000 Release 7.0 can operate in Redirect mode or Proxy mode. During the upgrade from Linux-based NRS Release 5.0 or 5.5 to Release 7.0, the SIP mode of operation is Proxy mode. In general, the NRS application is much faster in Redirect mode, but Redirect mode does not support most advanced features (such as Post-routing SIP URI modification). Third-party devices that do not support SIP 302 messages may not work in Redirect mode. Proxy mode is the preferred mode of operation.
>
> To configure a SIP endpoint in Redirect mode, make sure that the endpoint can handle the SIP redirect messages (like 300 or 302) and the network transport type (UDP, TCP, or TLS) used by the originator that the destination endpoint can support. For example, if the originator gateway with TLS network transport type is redirected to directly call a gateway that only supports UDP, the call is not successful. If you are not sure what your gateway supports, select the Proxy mode to resolve these issues.
>
> The SIP mode of operation for both gateway and user endpoints is configurable with NRS Manager. To edit a gateway endpoint, see Procedure 29 "Editing the Gateway Endpoints" (page 224). To edit a user endpoint, see Procedure 38 "Editing a User Endpoint" (page 241).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Migration from Solid database to MySQL

In CS 1000 Releases 4.0, 4.5, 5.0, and 5.5, a Solid database server was used to store and retrieve the NRS routing data. In CS 1000 Release 6.0, MySQL Enterprise 5.1 server is used to store and query the NRS routing data. Migration from the Solid database to MySQL provides significant improvement in call processing capacity and system stability.

The Solid RPM package is replaced by two groups of RPMs. One group is the MySQL third-party RPM. The other group is the Nortel application RPM, which is renamed from Solid to dbcom. The two groups of RPMs are part of the Nortel application image and are included in the Linux application.

MySQL migration has no effect on the user interface.

Note 1: When you upgrade the Solid database to MySQL, the database server TCP port changes from 1313 to 3306.

Note 2: When you upgrade the Solid database to MySQL, all Solid database utilities are removed.

Database application creation and operation

The dbcom application creation is based on the original Solid RPM creation and follows the Linux base RPM guidelines. The current Linux base appinstall and appstart are used for the MySQL installation and operation. After you install the application, the following default database configuration, accounts and passwords are loaded.

- NRS/NRS Manager: the account name nrs with the default password from the Secret Manager (SM) has full privileges on the databases NRS_A, NRS_B, and NRS_D. The databases is empty initially.
- PD: the account name pd with the default password from the Secret Manager (SM) has full privileges on the database pddb. The database is empty initially.
- EM/BCC: the account name mgmt with the default password from the Secret Manager (SM) has full privileges and it can create the databases on demand. The default empty databases are systemdatabase and template_database.

Similar to operation of the Solid database, the following commands are supported under the nortel account and are used to start, stop, restart, and check the status of the MySQL database engine:

- **`appstart dbcom start`**
- **`appstart dbcom stop`**

Copyright © 2010 Nortel Networks. All Rights Reserved.

- **appstart dbcom restart**
- **appstart dbcom status**

NRS database password interface change

For an NRS upgrade to CS 1000 Release 7.0, or a new CS 1000 Release 7.0 NRS installation, the existing default passwords are utilized. However, in CS 1000 Release 6.0, for additional password security, the system administrator can use a shell script utility to change the password for each database application. Only the nortel user can use this script; it is intended for an experienced system administrator or expert user. The password change requires that you restart the application to activate the new password.

Usage: dbcom_passwd [nrs | pd | mgmt | dbroot] [password]

nrs (NRS application including SIP Proxy Server, Gatekeeper, Network Connection Service, Jboss, Failsafe and Replication)

pd (Personal Directory application)

mgmt (Management application including BCC)

dbroot (MySQL root user)

The script accepts two arguments:

1. the name of the component for which the password is changed
2. the new password

Example: **dbcom_passwd "nrs" "new-password"**

In this example the database password for the nrs component changes to new-password. The commands require confirmation before changing the password and warns that the nrs application restart. To proceed with the password change, you must provide the current password. The first time, you can enter the default password of 2tdp22ler.

To activate the new password, the script automatically restarts the target application, with the exception of dbroot. For the NRS application, all components (SIP Proxy Server, Gatekeeper, Network Connection Service, Jboss-Quantum, and dbcom component) restart. Only a Nortel user can use the script, which requires entry of the existing password before a new password can be accepted.

Copyright © 2010 Nortel Networks. All Rights Reserved.

For the NRS, the password change occurs only on the targeted NRS server. For redundant configurations, no password synchronization occurs between the primary and secondary servers. You must manually update the same password for each application on each server. For example changing the NRS application password on the primary server must be followed by changing the password on the secondary server. The NRS database password on the primary and secondary server must be the same for successful MySQL database replication between the two servers.

> ***Note:*** To change the database password the current password must be supplied. If the current password is unknown, the only way to recover is to reinstall the software. The database password is encrypted and stored locally on each system. No backup or recovery procedure exists to extract the password when it changes from the default setting.

Upgrade from Release 3.0 to Release 7.0

If you upgrade a Succession 3.0 H.323 Gatekeeper database , see "GK/NRS Data Upgrade" (page 304).

Upgrade from Release 4.0 or later to Release 7.0

Backup the NRS database.

For detailed information about backing up a Linux-based NRS database, see "Backup the database" (page 291). For detailed information about backing up a VxWorks-based NRS database, see the VxWorks-based procedure in *Network Routing Service Installation and Commissioning* (NN43001-564).

The database file is processed to accommodate database structure changes.

Perform the procedures in "Restore the NRS database" (page 296), to restore the database.

Access NRS Manager through the UCM Common Services

Access NRS Manager through the UCM Common Services. See Procedure 5 "Logging in to UCM Common Services and Accessing NRS Manager" (page 151) to access NRS Manager.

Configure your Web browser and Windows display before you log on to UCM Common Services. NRS Manager is supported only on Microsoft Internet Explorer Version 6.0 (or later). See Procedure 3 "Configuring the Internet Explorer browser settings" (page 150) to configure the Internet Explorer browser. See Procedure 4 "Configuring the Windows Display settings" (page 151) to configure the Windows display settings.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Initial configuration of 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 MySQL database). The NRS database provides a central database of addresses that are required to route calls across the network.
- Logging off the UCM Common Services.

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

1. **Accessing NRS manager.** See Procedure 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151) .
2. **Configure the Primary and Secondary NRS server settings.** See Procedure 7 “Configuring the Primary and Secondary NRS Server Settings for IPv4 and IPv6” (page 166).

   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 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

3. **Start services.**

   In the **NRS Manager Navigator** select **System > NRS Server**. The **NRS Server** web page opens. Click the **Restart** button on the **Service Status** pane of the **NRS Server** web page.
4. **Configure system wide settings.** See Procedure 8 “Configuring system-wide settings” (page 175).
5. **Build the NRS database.**

   The NRS database comprises

   — service domains, L1 domains and L0 domains

   — collaborative servers

   — gateway endpoints

Copyright © 2010 Nortel Networks. All Rights Reserved.

— 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 10 “Adding a Service Domain” (page 180).

   ii. See Procedure 14 “Adding an L1 Domain” (page 186).

   iii. See Procedure 18 “Adding an L0 Domain (CDP)” (page 195).

b. Add collaborative servers.

   – See Procedure 22 “Adding a Collaborative Server” (page 204).

c. Add gateway endpoints and endpoint prefixes. See Procedure 26 “Adding a Gateway Endpoint” (page 213).

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

   i. See Procedure 41 “Adding a Routing Entry” (page 246).

   ii. See Procedure 48 “Adding a Default Route” (page 259).

e. Post-routing SIP URI modification table entries

   i. See Procedure 31 “Adding Post-routing SIP URI Modification” (page 227).

   ii. See Procedure 33 “Editing Post-routing SIP URI Modification” (page 230).

   iii. See Procedure 34 “Deleting Post-routing SIP URI Modification” (page 231).

6. **Test the numbering plans** .

   a. See Procedure 55 “Performing an H.323 Routing Test” (page 281).

   b. See Procedure 56 “Performing a SIP Routing Test” (page 282).

7. **Perform database actions.** See “Perform NRS database actions” (page 286). To save the NRS configuration, see the following procedures in this section.

Copyright © 2010 Nortel Networks. All Rights Reserved.

— See Procedure 60 “Cutting over the database” (page 288).

— See Procedure 61 “Reverting the database changes” (page 289).

— See Procedure 62 “Rolling back changes to the database” (page 290).

— See Procedure 63 “Committing the database” (page 290).

8. **Back up the NRS database**. See “Backup the database” (page 291).

   — See Procedure 64 “Backing up the database automatically” (page 291).

   — See Procedure 65 “Backing up the database manually” (page 292).

9. **Log out of UCM Common Services**. See Procedure 6 “Logging out of UCM Common Services ” (page 163)

10. To return to the UCM web page without terminating the current UCM Common Services session see “UCM Network Services link” (page 161).

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 129).

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

SIP Gateway switchover from Primary SPS to Secondary SPS

Primary and Secondary SPS fallback or switchover feature works for dual stack and IPv4 nodes only. Release 7.0 introduces Global unicast IPv6 addressing support over the Primary and Secondary SPS. If the SIP Gateway is registered to Primary SPS over IPv6 running on node 2, then the secondary SPS is configured on node 1 where the SIP Gateway is active. When the Primary SPS goes down, the status of the SIP Gateway is displayed as not registered. Later, the Secondary SPS takes over and the SIP Gateway registers to the Secondary SPS over IPv6.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Once the Primary SPS link is active again, the SIP Gateway registers back to the Primary SPS over IPv6. Thus the SIP Gateway switches from Primary SPS to Secondary SPS and back to Primary SPS over IPv6.

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, see Procedure 35 “Adding a User Endpoint” (page 233).
2. **View the SIP Phone Context.** See Procedure 40 “Mapping the SIP Phone Context” (page 244) to view the SIP phone context.

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

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 a UCM Common Services Security Domain. A UCM Common Services Security Domain is defined by the UCM Common Services Primary Security server. A UCM Common Services Security Domain is comprised of the UCM Common Services Primary Security server, an optional UCM Common Services Backup Security server and any associated Security Domain member servers. A UCM Common Services Security Domain member server is a server that has the UCM Common Services 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 UCM Common Services Security Domain.

The Linux-based NRS and the Linux-based EM applications are installed on dedicated servers. The UCM Common Services 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. 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 UCM Common Services 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 UCM Common Services Security Domain

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

1. Linux-based EM has not been installed and is not being installed now. The UCM Common Services Primary Security Service is being installed on the Linux-based Primary NRS server and the UCM Common Services 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 UCM Common Services Primary Security Service is being installed on the EM server and the UCM Common Services 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 UCM Common Services Primary and Backup Security servers.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 UCM Common Services Primary Security Service is being installed on the Linux-based Primary NRS server and the UCM Common Services 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 the VxWorks-based procedure in *Network Routing Service Installation and Commissioning (NN43001-564)*.
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. (See the VxWorks-based procedures in *Network Routing Service Installation and Commissioning (NN43001-564)*.)
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 the VxWorks-based procedure in *Network Routing Service Installation and Commissioning (NN43001-564)*.
5. **Gracefully disable the VxWorks-based Primary NRS server** forcing all endpoints to register with the VxWorks-based Alternate NRS. (See the VxWorks-based procedure in *Network Routing Service Installation and Commissioning (NN43001-564)*.)
6. **Log in to VxWorks-based Alternate NRS.**

   Verify that the SIP gateways, H.323 gateways and user endpoints have registered with the VxWorks-based Alternate NRS. (See the VxWorks-based procedures in *Network Routing Service Installation and Commissioning (NN43001-564)*.)
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),

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

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 UCM Common Services Primary Security Service. When you install the NRS application, configure the MySQL database server as Hotstandby primary MySQL server.

The Nortel Linux platform uses Centralized Deployment Manager to remotely deploy Nortel application software from the UCM Common Services Primary Security server to other Linux servers in the same security domain.

The UCM Common Services base application resides on the Linux base installation media and is installed automatically the first time the system starts after base installation. The success or failure of the base applications installation appears in an on-screen message. If the base application installation fails, you must reinstall the Linux base.

For information about installing the Linux operating system, the UCM Common Services , the NRS and the UCM Common Services Primary Security Service, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Copyright © 2010 Nortel Networks. All Rights Reserved.

9. **Create user accounts and assign roles and permissions** for access to the Primary and Secondary NRS servers from the UCM Common Services.

   For information about creating user accounts, and assigning roles and permissions for access to the NRS servers from the UCM Common Services, see *Unified Communications Management* (NN43001-116).

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

    See Procedure 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

11. **Configure the Linux-based Primary server settings**. See Procedure 7 “Configuring the Primary and Secondary NRS Server Settings for IPv4 and IPv6” (page 166).

    — 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 45 "Edit Server Configuration web page" (page 167).

    — If the IP network NRS zone contains H.323 endpoints, configure H.323 Gatekeeper settings.

    — Configure SIP Server settings.

    — Configure Network Connection Server settings.

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

    In the **NRS Manager Navigator** select **System > NRS Server**. The **NRS Server** web page opens. 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.

13. **Restore the VxWorks-based NRS database** backed up in step 4. See the procedures in “Restore the NRS database” (page 296) to restore an NRS Release 5.5, 5.0, 4.5 or 4.0 database. See “GK/NRS Data Upgrade” (page 304) 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 45 "Edit Server Configuration web page" (page 167)) and saving them in the new restored database. Ensure the Primary and Secondary server IP addresses are correct. Always restart the application services if there is an IP address or any other server configuration change.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 4, review the restored database.

    Follow the Linux-based procedures:

    Procedure 28 “Viewing the Gateway Endpoints” (page 222)

    Procedure 42 “Viewing the Routing Entries” (page 248)

    Procedure 23 “Viewing a Collaborative Server” (page 209)

    Procedure 37 “Viewing the User Endpoints” (page 239)

15. **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 28 “Viewing the Gateway Endpoints” (page 222).

    Procedure 37 “Viewing the User Endpoints” (page 239)

    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.

16. **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

Copyright © 2010 Nortel Networks. All Rights Reserved.

- 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.

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

    a. 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 UCM Common Services Backup Security Service. When you install the NRS application, configure the MySQL database server as **Hotstandby secondary MySQL server.**

    The Nortel Linux platform uses Centralized Deployment Manager to remotely deploy Nortel application software from the UCM Common Services Primary Security server to other Linux servers in the same security domain.

    The UCM Common Services base application resides on the Linux base installation media and is installed automatically the first time the system starts after base installation. The success or failure of the base applications installation appears in an on-screen message. If the base application installation fails, you must reinstall the Linux base.

    For information about installing the Linux operating system, the UCM Common Services framework, the NRS and the UCM Common Services Primary Security Service, see *Linux Platform Base and Applications Installation and Commissioning* ((NN43001-315).

18. **Log in to NRS Manager for the Secondary NRS server.** See Procedure 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

Copyright © 2010 Nortel Networks. All Rights Reserved.

19. **Configure the Linux-based Secondary server settings**. See Procedure 7 “Configuring the Primary and Secondary NRS Server Settings for IPv4 and IPv6” (page 166).

    — 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 45 "Edit Server Configuration web page" (page 167).

    — If the IP network NRS zone contains H.323 endpoints, configure H.323 Gatekeeper settings.

    — Configure SIP Server settings.

    — Configure Network Connection Server settings.

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

    In the **NRS Manager Navigator**, select **System > NRS Server**. The **NRS Server** web page opens. 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 MySQL database synchronization link should be established between the Primary and Secondary NRS servers. The MySQL databases on the Primary and Secondary servers should synchronize automatically.

21. **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 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

    — View the Gateway Endpoints on the Active Database. See Procedure 28 “Viewing the Gateway Endpoints” (page 222).

    — Note the number of Gateway Endpoints.

    — View the User Endpoints on the Active Database. See Procedure 37 “Viewing the User Endpoints” (page 239).

    — Note the number of User Endpoints

    — Log onto the Secondary NRS Manager. See Procedure 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

    — View the Gateway Endpoints on the Active Database. See Procedure 28 “Viewing the Gateway Endpoints” (page 222).

    — Note the number of Gateway Endpoints

Copyright © 2010 Nortel Networks. All Rights Reserved.

— View the User Endpoints on the Active Database. See Procedure 37 “Viewing the User Endpoints” (page 239).

— 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 UCM Common Services 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 UCM Common Services Primary Security Service is being installed on the EM server and the UCM Common Services 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 UCM Common Services Primary and Backup Security servers.

   Install and configure the Linux-based EM server

   a. 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 UCM Common Services Primary Security Service.

      The Nortel Linux platform uses Centralized Deployment Manager to remotely deploy Nortel application software from the UCM Common Services Primary Security server to other Linux servers in the same security domain.

      The UCM Common Services base application resides on the Linux base installation media and is installed automatically the first time the system starts after base installation. The success or failure of the base applications installation appears in an on-screen message. If the base application installation fails, you must reinstall the Linux base.

Copyright © 2010 Nortel Networks. All Rights Reserved.

For more information about installing the Linux operating system, the UCM Common Services , the NRS and the UCM Common Services Primary Security Service*Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

2. **Create user accounts and assign roles and permissions** for access to the Primary and Secondary NRS servers from the UCM Common Services.

   For information about creating user accounts, and assigning roles and permissions for access to the NRS servers from the UCM Common Services, see *Unified Communications Management* (NN43001-116).

3. **Log on to VxWorks-based Primary NRS**. See VxWorks-based procedure in *Network Routing Service Installation and Commissioning (NN43001-564)*.

4. **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. (See VxWorks-based procedures in *Network Routing Service Installation and Commissioning* (NN43001-564).

5. 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.

6. **Backup the VxWorks-based NRS database**. See VxWorks-based procedure in *Network Routing Service Installation and Commissioning* (NN43001-564).

7. **Gracefully disable the VxWorks-based Primary NRS server** forcing all endpoints to register with the VxWorks-based Alternate NRS. (See VxWorks-based procedure in *Network Routing Service Installation and Commissioning* (NN43001-564).

8. **Log in to VxWorks-based Alternate NRS.**

   Verify that the SIP gateways, H.323 gateways and user endpoints have registered with the VxWorks-based Alternate NRS. (See VxWorks-based procedures in *Network Routing Service Installation and Commissioning* (NN43001-564).

9. **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),

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

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

    a. 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 UCM Common Services Backup Security Service. When you install the NRS application, configure the MySQL database server as **Hotstandby primary MySQL server**.

       The Nortel Linux platform uses Centralized Deployment Manager to remotely deploy Nortel application software from the UCM Common Services Primary Security server to other Linux servers in the same security domain.

       The UCM Common Services base application resides on the Linux base installation media and is installed automatically the first time the system starts after base installation. The success or failure of the base applications installation appears in an on-screen message. If the base application installation fails, you must reinstall the Linux base.

       For more information about installing the Linux operating system, the UCM Common Services, the NRS and the UCM Common Services Backup Security Service, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

See Procedure 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

12. **Configure the Linux-based Primary server settings**. See Procedure 7 “Configuring the Primary and Secondary NRS Server Settings for IPv4 and IPv6” (page 166).

    — 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 45 "Edit Server Configuration web page" (page 167).

    — If the IP network NRS zone contains H.323 endpoints, configure H.323 Gatekeeper settings.

    — Configure SIP Server settings.

    — Configure Network Connection Server settings.

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

    In the **NRS Manager Navigator** select **System > NRS Server**. The **NRS Server** web page opens. 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.

14. **Restore the VxWorks-based NRS database** backed up in step 7. See the procedures in “Restore the NRS database” (page 296) to restore an NRS Release 5.5, 5.0, 4.5 or 4.0 database. See “GK/NRS Data Upgrade” (page 304) 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 45 "Edit Server Configuration web page" (page 167)) and saving them in the new restored database. Ensure the Primary and Secondary server IP addresses are correct. Always restart the application services if there is an IP address or any other server configuration change.

15. 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:

    Procedure 28 “Viewing the Gateway Endpoints” (page 222)

    Procedure 42 “Viewing the Routing Entries” (page 248)

    Procedure 23 “Viewing a Collaborative Server” (page 209)

    Procedure 37 “Viewing the User Endpoints” (page 239)

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 28 “Viewing the Gateway Endpoints” (page 222).

    Procedure 37 “Viewing the User Endpoints” (page 239)

    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.

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 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

    a. 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 a UCM Common Services Security Domain member; that is, without the UCM Common Services Primary or Backup Security service. The Secondary NRS is a security client of the UCM Common Services Primary and Backup Security servers. When you install the NRS application, configure the MySQL database server as Hotstandby secondary MySQL server.

    The Nortel Linux platform uses Centralized Deployment Manager to remotely deploy Nortel application, software from the UCM Common Services Primary Security server to other Linux servers in the same security domain.

    The UCM Common Services base application resides on the Linux base installation media and is installed automatically the first time the system starts after base installation. The success or failure of the base applications installation appears in an on-screen message. If the base application installation fails, you must reinstall the Linux base must be reinstalled.

    For more information about installing the Linux operating system, the UCM Common Services and the NRS, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

19. **Log in to NRS Manager for the Secondary NRS server.** See Procedure 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

20. **Configure the Linux-based Secondary server settings**. See Procedure 7 “Configuring the Primary and Secondary NRS Server Settings for IPv4 and IPv6” (page 166).

    — 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 45 "Edit Server Configuration web page" (page 167).

    — If the IP network NRS zone contains H.323 endpoints, configure H.323 Gatekeeper settings.

    — Configure SIP Server settings.

    — Configure Network Connection Server settings.

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

In the **NRS Manager Navigator** select **System > NRS Server**. The **NRS Server** web page opens. 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 MySQL database synchronization link should be established between the Primary and Secondary NRS servers. The MySQL 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 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

    — View the Gateway Endpoints on the Active Database. See Procedure 28 “Viewing the Gateway Endpoints” (page 222).

    — Note the number of Gateway Endpoints.

    — View the User Endpoints on the Active Database. See Procedure 37 “Viewing the User Endpoints” (page 239).

    — Note the number of User Endpoints.

    — Log onto the Secondary NRS Manager. See Procedure 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

    — View the Gateway Endpoints on the Active Database. See Procedure 28 “Viewing the Gateway Endpoints” (page 222).

    — Note the number of Gateway Endpoints.

    — View the User Endpoints on the Active Database. See Procedure 37 “Viewing the User Endpoints” (page 239).

    — 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, 5.0 or 5.5) or H.323 Gatekeeper database. (See VxWorks-based procedures

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

2. Install and configure the Linux-based NRS Primary and Secondary servers with the new IP addresses. See "Introduction" (page 119) and "Installation of Linux operating system, UCM Common Services and NRS application" (page 120).

   This step has four substeps:

   a. Install the Linux operating system. 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 UCM Common Services.

   d. Create user accounts and assign roles and permissions for access to the Primary and Secondary NRS servers from the UCM Common Services.

   For information about installing the Linux operating system, the UCM Common Services and the NRS, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

   For information about adding a managed element to the UCM Common Services, creating user accounts, and assigning roles and permissions for access to the NRS servers from the UCM Common Services, see *Unified Communications Management* (NN43001-116).

3. **Log in to NRS Manager.** See Procedure 5 "Logging in to UCM Common Services and Accessing NRS Manager" (page 151).

4. **Assign the new IP addresses to the Primary and Secondary NRS servers.** See Procedure 7 "Configuring the Primary and Secondary NRS Server Settings for IPv4 and IPv6" (page 166).

   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 5 "Logging in to UCM Common Services and Accessing NRS Manager" (page 151).

5. Restore the VxWorks-based NRS database backed up in "step 1" (page 146) . If a Succession 3.0 H.323 Gatekeeper database is being restored see "GK/NRS Data Upgrade" (page 304). If an NRS Release 4.0, 4.5, 5.0 or 5.5 database is being restored follow the procedures in "Restore the NRS database" (page 296).

Copyright © 2010 Nortel Networks. All Rights Reserved.

> **ATTENTION**
> Restoring the previous release database should always be followed by cross checking changes in the Primary and Secondary NRS Server settings (see Figure 45 "Edit Server Configuration web page" (page 167)) 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. 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 129) 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 24 "Editing a Collaborative Server" (page 210) 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**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

— See Procedure 67 “Downloading the latest backup log file” (page 296).

— See Procedure 66 “Downloading the latest backup file” (page 293).

2. **Restore NRS database.**

— See “Restore the NRS database” (page 296).

Operation and maintenance commands

For information about operation and maintenance commands, see *Software Input/Output Reference - Maintenance* (NN43001-711).

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).

Note: In Internet Explorer version 8 and later, the text box to input file name is disabled due to security reasons. The file name path needs to be specified using the Browse button.

Configure the browser and display settings

Before you can use NRS Manager, the following tasks must be completed:

- Enable pop-ups 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 pop-ups

If you are using a browser search utility (such as the Google™ search engine or the Yahoo!™ search engine), ensure that pop-ups are enabled. Enabling pop-up windows is usually done at the search utility’s toolbar.

Copyright © 2010 Nortel Networks. All Rights Reserved.

ATTENTION
Do not block pop-up windows if you are using a search utility (such as Google™ or Yahoo!™ search engines) in your browser.

Configure the browser settings

See Procedure 3 “Configuring the Internet Explorer browser settings” (page 150) to configure the following Internet Explorer browser settings:

- Browser retrieve page information.
- Empty session information.
- Deselect the AutoComplete options.

Procedure 3
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)

Copyright © 2010 Nortel Networks. All Rights Reserved.

Click **OK** (to close the **Internet Options** window)

--End--

Configure the Windows Display settings

See Procedure 4 “Configuring the Windows Display settings” (page 151) to configure the Windows display settings.

Procedure 4
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 UCM Common Services and Access NRS Manager

Access NRS Manager through the UCM Common Services . See Procedure 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

Two types of access privileges are supported:

- Administrator 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 5
Logging in to UCM Common Services and Accessing NRS Manager

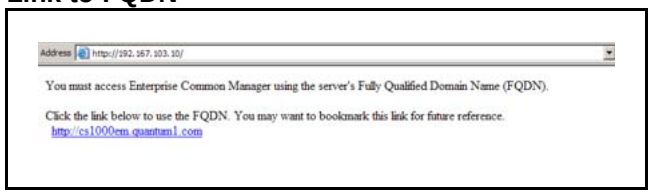
Step	Action
1	Open a Web browser.
2	In the Address bar of the Web browser enter the Fully Qualified Domain Name (FQDN) of a UCM Common Services server that

Copyright © 2010 Nortel Networks. All Rights Reserved.

is a member of the Security Domain that the NRS server is a member of.

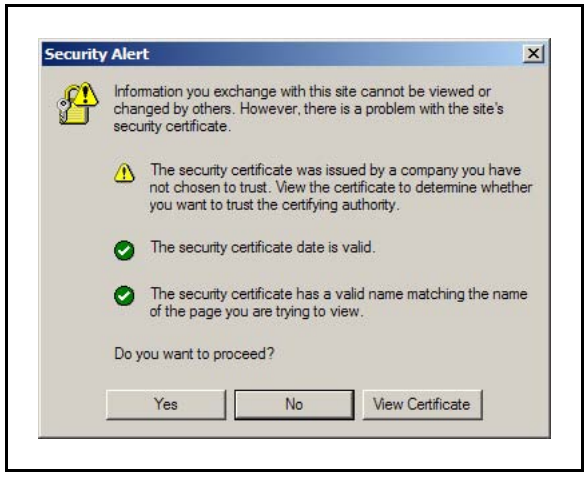
> ***Note:*** The link to the FQDN of the UCM Common Services server can be bookmarked in the Internet Explorer Favorites list. See Figure 33 "Link to FQDN" (page 152).

Figure 33
Link to FQDN



The Security Alert web page opens. See Figure 34 "Security Alert web page" (page 152). Click the **Yes** button.

Figure 34
Security Alert web page



3 The UCM Common Services log in web page opens. See Figure 35 "UCM Common Services log in web page" (page 152).

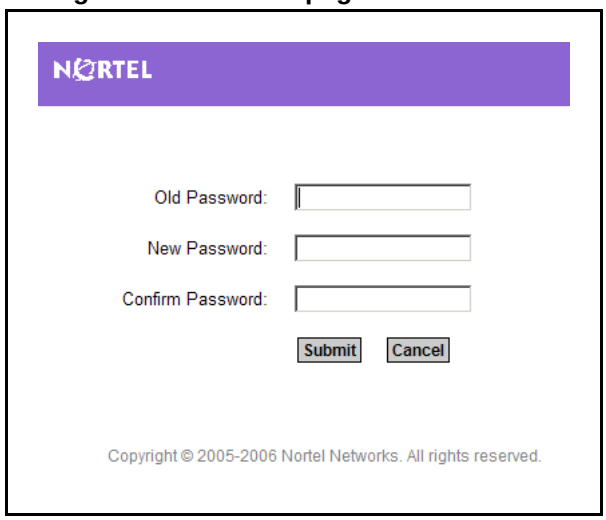
Figure 35
UCM Common Services log in web page

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

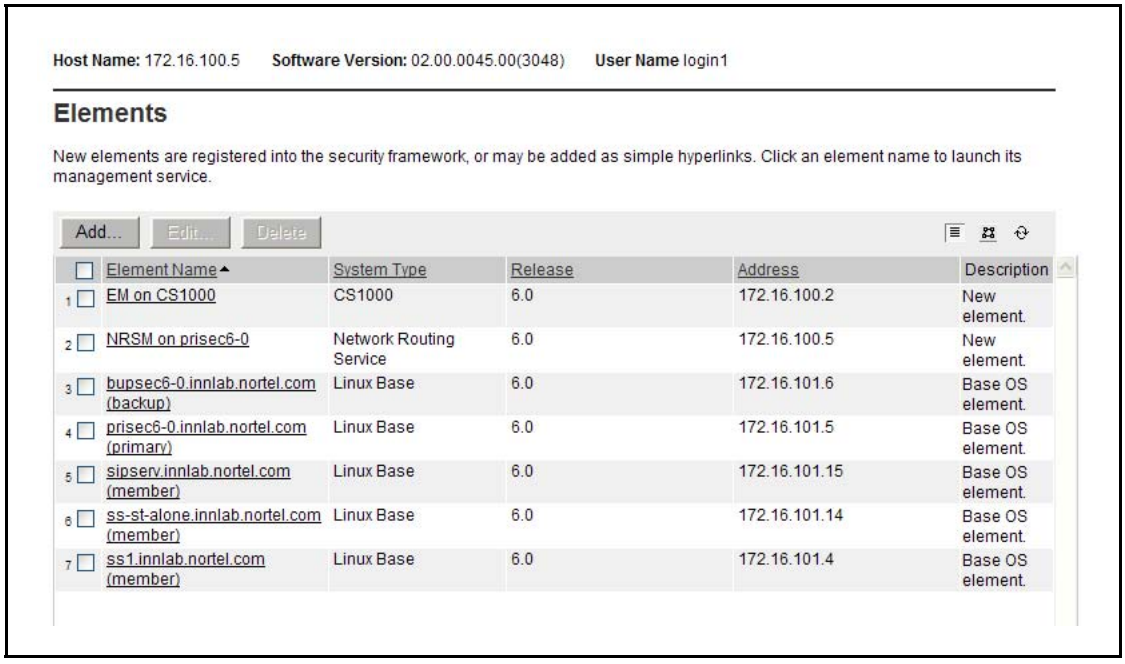
If this is your first time logging in, you will prompted to change your password. See Figure 36 "Change Password web page" (page 153).

Figure 36
Change Password web page



4 The UCM Common Services Elements web page opens. See Figure 37 "UCM Common Services Elements web page" (page 153). Click the link to the NRS Manager in the **Element Name** column.

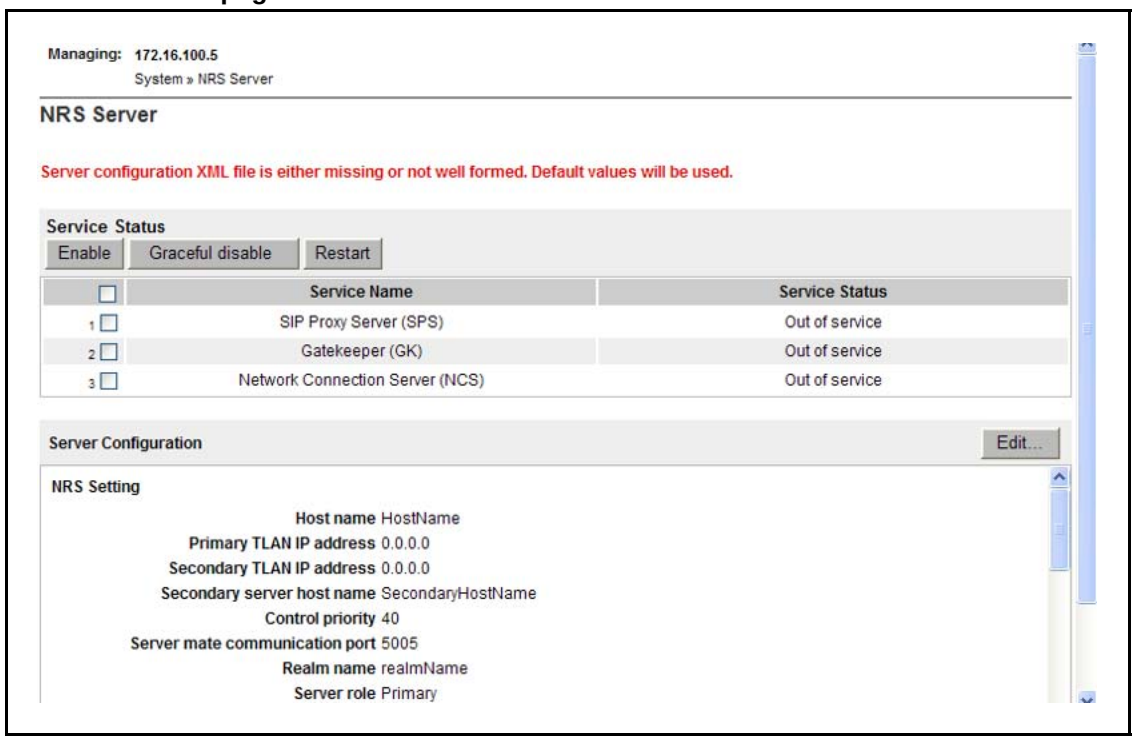
Figure 37
UCM Common Services Elements web page



Copyright © 2010 Nortel Networks. All Rights Reserved.

The NRS server Web page appears as shown in Figure 38 "NRS Server web page" (page 154).

Figure 38
NRS Server web page



--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 UCM Common Services web page. The **NRS Manager Navigator** is comprised of three main branches: **System**, **Numbering Plans**, and **Tools**.

The **System** branch contains links to

- NRS Server
- Database
- System Wide Settings

The **Numbering Plans** branch contains links to

Copyright © 2010 Nortel Networks. All Rights Reserved.

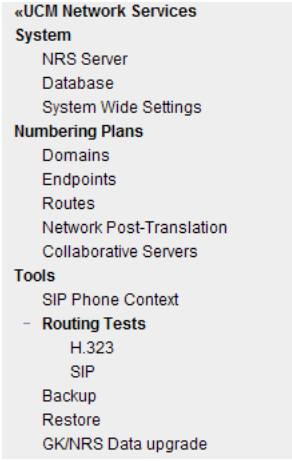
- Domains (Service, L1 and L0 Domains)
- Endpoints (Gateway and User Endpoints)
- Routes
- Network Post-Translation
- Collaborative Servers

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 39 "NRS Manager Navigator" (page 155), the NRS Manager Navigator is expanded to display all available links.

Figure 39
NRS Manager Navigator



Navigation of NRS Manager web pages

There are three navigation areas in NRS Manager web pages:

1. **NRS Manager Navigator**

   The NRS Manager navigation tree, shown in Figure 39 "NRS Manager Navigator" (page 155), is located on the left side of NRS Manager

Copyright © 2010 Nortel Networks. All Rights Reserved.

web pages. It contains links to other web pages. The web pages are opened by clicking a branch of the NRS Manager navigation tree.

2. **Navigation Path**.

   The navigation path is located at the top of NRS Manager web pages. For example, to add an L0 Domain open the **Add L0 Domain** web page shown in Figure 68 "Add L0 Domain web page" (page 196). 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 40 "Numbering Plans web page" (page 156), contains links to Domain, Endpoints, Routes, Network Post-Translation and Collaborative Servers web pages. Click on a link to open a web page.

Figure 40
Numbering Plans web page

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 51 "Service Domains pane" (page 180), 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.**

Copyright © 2010 Nortel Networks. All Rights Reserved.

Or

b. Click on **Domains** in the **Numbering Plans >> Domains >> L0 Domain** navigation path at the top of Figure 68 "Add L0 Domain web page" (page 196).

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** tab.

   e. Click the **Add....** button.

   Or

3. Add a Gateway endpoint from

   — **Service Domains** web page shown in Figure 51 "Service Domains pane" (page 180).

   or

   — **L1 Domains** web page shown in Figure 59 "L1 Domains (UDP) pane" (page 187).

   or

   — **L0 Domains** web page shown in Figure 67 "L0 Domain (CDP) pane" (page 195).

   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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

— 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 41 "Descending Alphabetical sort order" (page 158) are sorted in descending alphabetical order.

Figure 41
Descending Alphabetical sort order

	ID	Description	# of L0 Domains	# of Gateway Endpoints	# of Routing Entries	Context
1	udp		1	1	2	quantum1.com
2	mvUdpDomain		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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 42 "Pagination" (page 159).

Figure 42
Pagination

5. The following functionality has been added to the NRS Manager User Interface in CS 1000 Release 5.5

   — The NRS Manager Navigator can be expanded to the lowest leaf level of each node by clicking on the root node.

   — A **Hide** and **Show** link is introduced into the Endpoints and Routes web pages. Clicking on the **Hide** link removes the search criteria panel from the web pages, providing a larger panel for the display of the Routing Entries and Endpoints.

Mandatory fields on NRS Manager web pages

Mandatory fields on NRS Manager web pages are denoted by an asterisk (*). All other fields on NRS Manager web pages are optional.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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"Hierarchical model of the Network Routing Service" (page 38) 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 43 "Help and Logout Links" (page 161).

Figure 43
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 UCM Common Services session. See Procedure 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151).

UCM Network Services link

Select the **UCM Network Services** link on the **NRS Manager Navigator** to return to the UCM Common Services web page without terminating the current UCM Common Services session. See “NRS Manager interface” (page 154).

Configuring IPv6 in NRSM

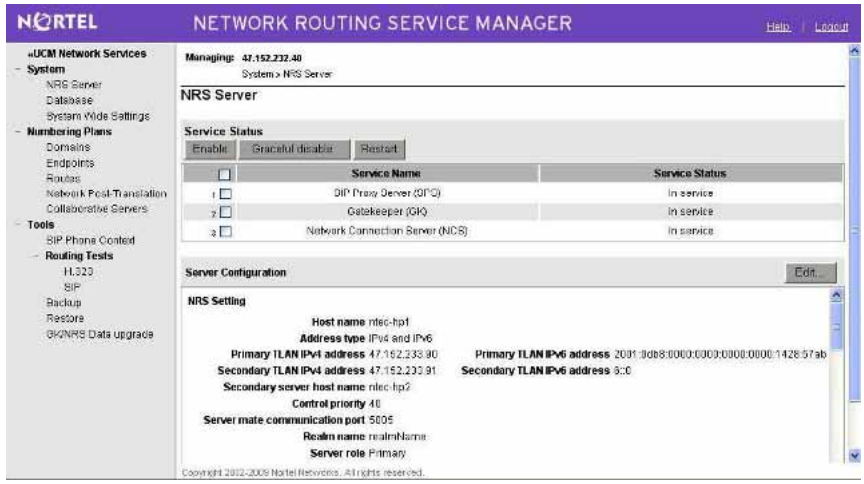
Configure IPv6 in NRSM.

Step	Action
1	In the **NRS Manager Navigator** select **System, NRS Server**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The **NRS Server** Web page appears.

2 To configure the **NRS Server Settings**, click **Edit** in the **Server Configuration** pane of the **NRS Server** Web page. The **Edit Server Configuration** Web page appears.



3 In the **Address type** field, select **IPv4 and IPv6** to enable IPv6 for NRSM.

--End--

IPv6 limitations

Following are the limitations of the IPv6:

- Global unicast IPv6 addressing is the only supported IPv6 address type.
- ELAN cannot be configured using IPv6.
- UNISTIM phones and H.323 trunks does not support IPv6, therefore, the calls established for these should have IPv4 addresses.
- IPv6 does not support the Media Security.
- SIP Lines Gateway does not support (Transport Layer Security (TLS) protocol over the IPv6.
- You can configure the primary proxy IP of SIP Signalling Gateway with either IPv4 or IPv6 address but not both.
- There may be call failures in the following situations:
  - — Endpoint does not respond back with "420 Bad Extension" for INVITE with "Require: sdp-anat"
  - — Endpoints does not respond back for INVITE having headers with IPv6 addresses

Copyright © 2010 Nortel Networks. All Rights Reserved.

Log out of UCM Common Services

See Procedure 6 “Logging out of UCM Common Services ” (page 163) to log out of the UCM Common Services . Logging out of the UCM Common Services terminates the current session.

Procedure 6
Logging out of UCM Common Services

Step	Action
1	Click the **Logout** link on the right side of the NRS Manager web page header. The **Logout successful** web page opens. **Figure 44** **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
You individually must configure primary and secondary NRS servers. You must log on to the specific (either primary or secondary) server to configure it. See Step 4 of Procedure 5 “Logging in to UCM Common Services and Accessing NRS Manager” (page 151). You must configure the **NRS services** in Deployment View before installing the server.

The attributes configured in **NRS Server settings** page should match with the attributes of the server configured in **NRS services** in Deployment Manager. If the data does not match, error messages will appear on the **NRS Server Settings** page. However, you can modify all the fields or attributes without any restriction.

Copyright © 2010 Nortel Networks. All Rights Reserved.

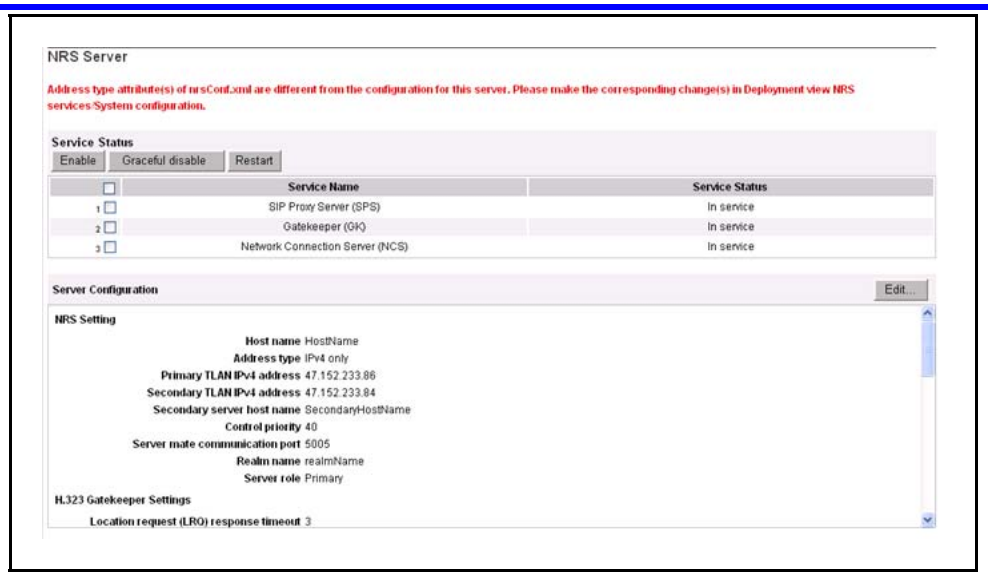
Check the following fields in **NRS Server settings** page for consistency:

- **Primary TLAN IPv4 address**: The Primary TLAN IPv4 address configured in the **NRS Server Settings** page should be the same as TLAN IPv4 address of the server configured as Primary in **NRS services**.
- **Secondary TLAN IPv4 address**: The Secondary TLAN IPv4 address configured in the **NRS Server Settings** page should be the same as TLAN IPv4 address of the server configured as Secondary in **NRS services**.
- **Primary TLAN IPv6 address**: The Primary TLAN IPv6 address configured in the **NRS Server Settings** page should be the same as TLAN IPv6 address of the server configured as Primary in **NRS services**.
- **Secondary TLAN IPv6 address**: The Secondary TLAN IPv6 address configured in the **NRS Server Settings** page should be the same as TLAN IPv6 address of the server configured as Secondary in **NRS services**.
- **Address type**: The Address type configured in the **NRS Server Settings** page should match with the Address type of the server(s) configured in **NRS services**.
  For example, if the server(s) do not have IPv6 configured or enabled in their Linux base but the Address type is selected as IPv4 and IPv6, an error message is displayed.
- **Server role:** The Server role configured in the **NRS Server Settings** page should be Primary or Secondary corresponding to the servers configured as Primary or Secondary servers in **NRS services**.

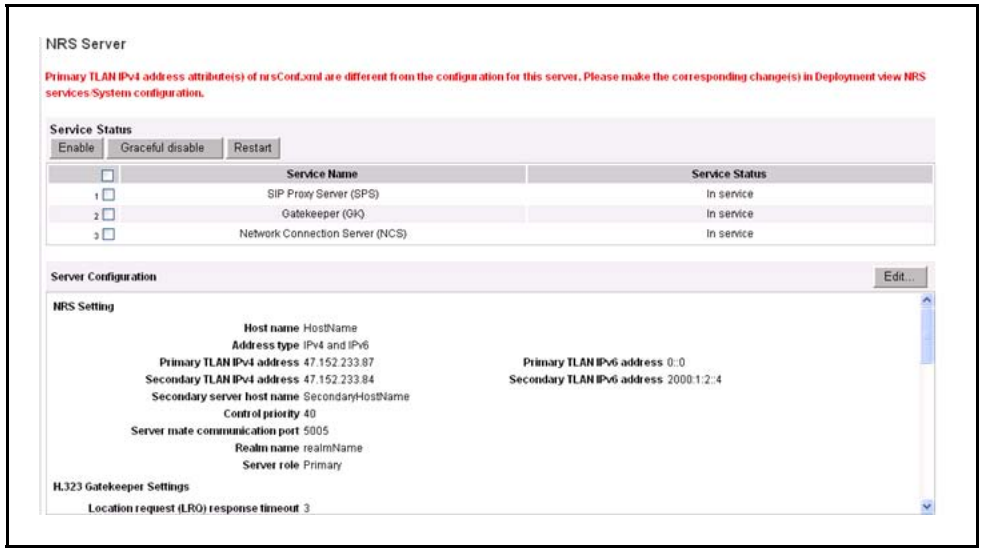
Following are the various error messages that appears on the **NRS server setting** page:

- Address type: When Address types configured in Linux base is different following error message is displayed:

Copyright © 2010 Nortel Networks. All Rights Reserved.

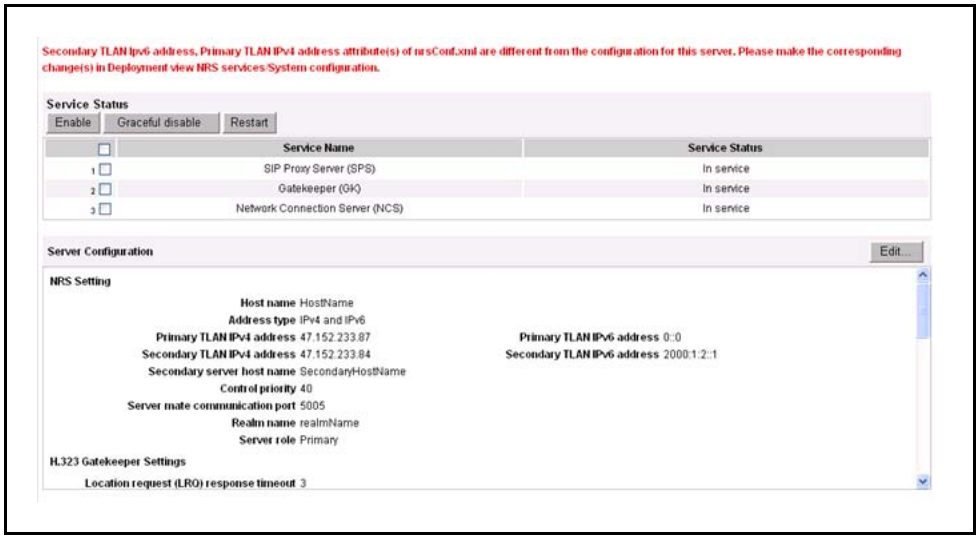


- Primary Tlan IPv4 address: When Primary Tlan IPv4 address is different in **NRS service** configured in Deployment view and in **NRS server setting** page following error message is displayed.



- Primary Tlan IPv4 and Secondary Tlan IPv6 addresses: When Primary Tlan IPv4 and Secondary Tlan IPv6 addresses are different in **NRS server setting** page and the **NRS services** view in Deployment manager following error is displayed.

Copyright © 2010 Nortel Networks. All Rights Reserved.

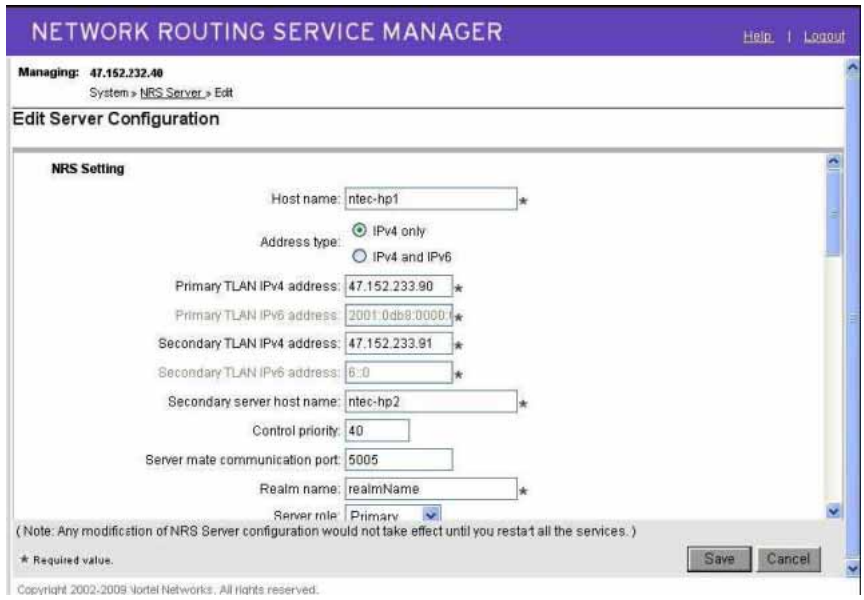


Procedure 7
Configuring the Primary and Secondary NRS Server Settings for IPv4 and IPv6

Step	Action
1	In the **NRS Manager Navigator** select **System, NRS Server**. The **NRS Server** Web page appears.
2	To configure the **NRS Server Settings**, click **Edit** in the **Server Configuration** pane of the **NRS Server** Web page. The **Edit Server Configuration** Web page appears , as shown in Figure 45 "Edit Server Configuration web page" (page 167).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 45
Edit Server Configuration web page



3 Configure the **NRS Server Settings**:

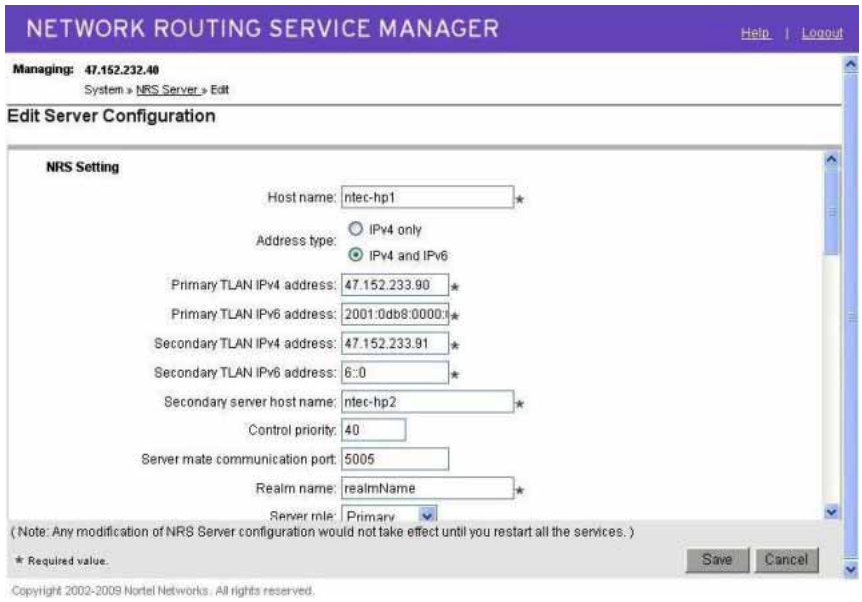
a **Host name:** Enter the Primary server host name in the text box. The host name must be alphanumeric and can be up to 20 characters in length.

b **Address type:** Choose **IPv4 only** to enable IPv4 configuration for NRS settings.

OR

Choose **IPv4 and IPv6** to enable both IPv4 and IPv6 configuration as shown in the figure.

Copyright © 2010 Nortel Networks. All Rights Reserved.



c **Primary TLAN IPv4 address:** Enter the IP address of the Primary NRS (that is, the TLAN network interface IPv4 address). The default is 0.0.0.0.

d **Primary TLAN IPv6 address:** Enter the IP address of the Primary NRS (that is, the TLAN network interface IPv6 address). The default is 0.0.0.0.

e **Secondary TLAN IPv4 address:** Enter the IP address of the Secondary NRS (that is, the TLAN network interface IPv4 address). The default is 0.0.0.0.

f **Secondary TLAN IPv6 address:** Enter the IP address of the Secondary NRS (that is, the TLAN network interface IPv6 address). The default is 0.0.0.0.

g **Secondary server host name:** Enter the Secondary server host name.

h **Control priority:** Enter a value for the control priority. 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.

i **Server mate communication port:** Enter a value for the Server mate communication port. 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 5005.

j **Realm name:** Enter a value for the Realm name. The Realm name is alphanumeric and can be up to 20 characters in length.

k **Server role:** Choose **Primary** or **Secondary** from the list.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 45 "Edit Server Configuration web page" (page 167).

a 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.

5 To configure **SIP Server Settings** scroll down to the SIP Server Settings section of the Edit Server Configuration web page. See Figure 45 "Edit Server Configuration web page" (page 167).

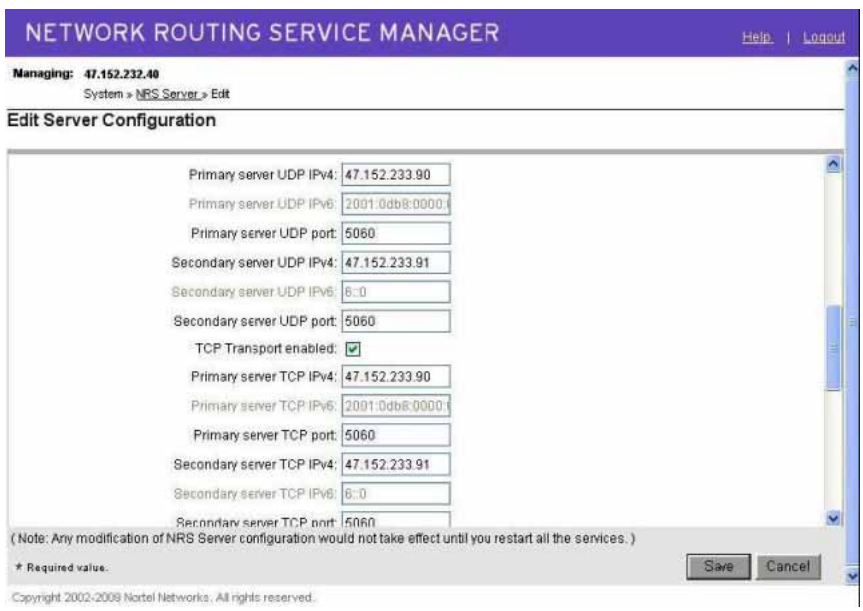
a Enter the **Public name for non-trusted networks**.

b Enter the **Public number for non-trusted networks**.

c Select the transport protocol.

ATTENTION
If a CS 1000 Release 5.0 or later Linux-based NRS is installed in a network with 4.x CS1000 gateways, the UDP transport protocol has to be enabled. It is recommended that the UDP transport protocol be enabled on a CS 1000 Release 5.0 or later Linux-based NRS, because UDP is the default protocol. To enable the other transport protocols the UDP transport protocol should be enabled.

To enable UDP IPv4:

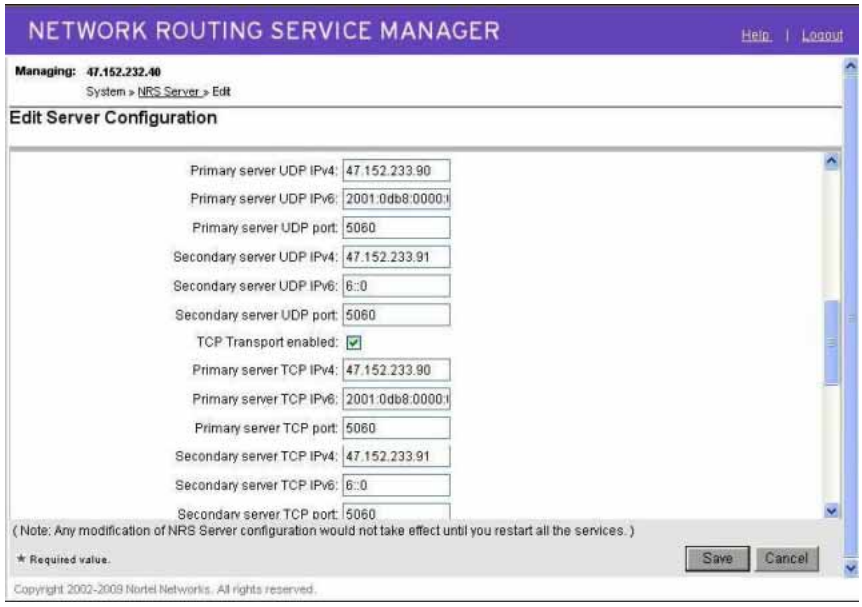


1. Select the **UDP transport enabled** check box.
2. Enter the **Primary server UDP IPv4**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

3. Enter the **Primary server UDP port**. 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 IPv4**.
5. Enter the **Secondary server UDP port**. 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.

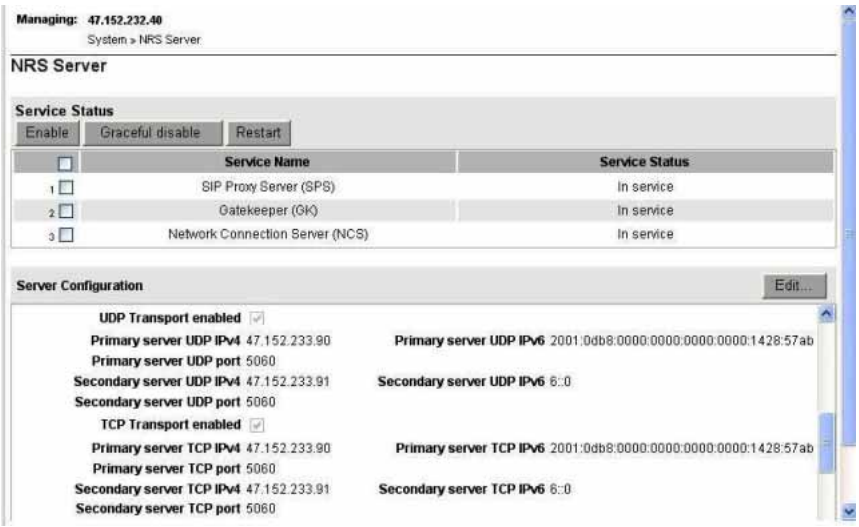
Perform the following steps to enable UDP IPv6.



1. Select the **UDP transport enabled** check box.
2. Enter the **Primary server UDP IPv6**.
3. Enter the **Primary server UDP port**. 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 IPv6**.
5. Enter the **Secondary server UDP port**. 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.

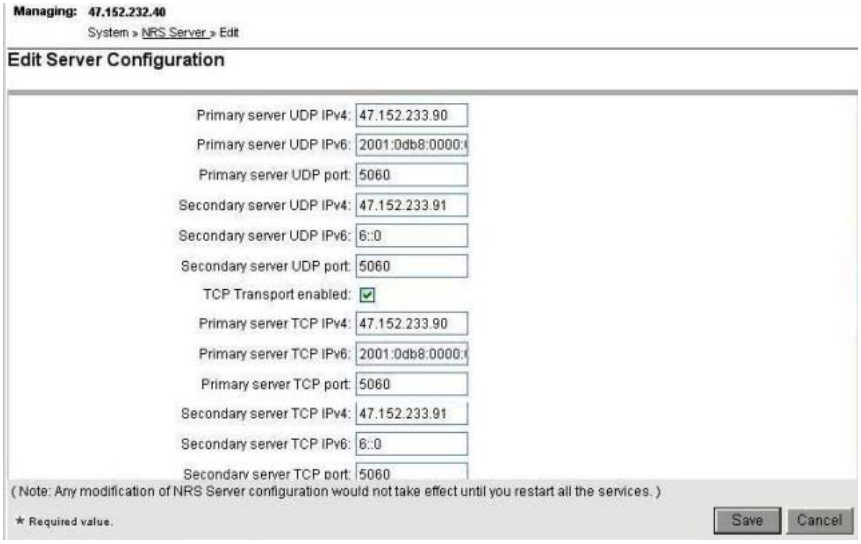
Perform the following steps to enable TCP IPv4:

Copyright © 2010 Nortel Networks. All Rights Reserved.



1. Select the **TCP transmission enabled** check box.
2. Enter the **Primary server TCP IPv4**.
3. Enter the **Primary server TCP port**. 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 IPv4**.
5. Enter the **Secondary server TCP port**. 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.

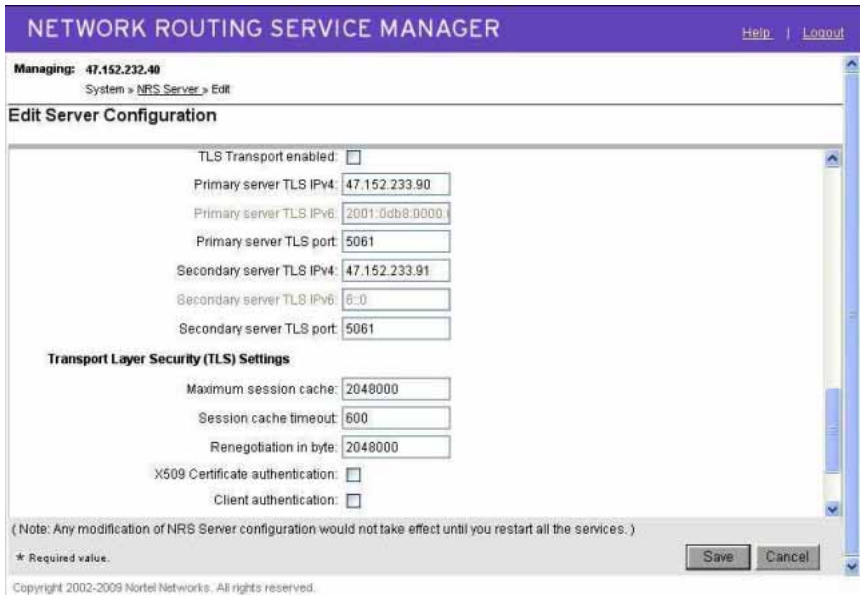
Perform the following steps to enable TCP IPv6:



Copyright © 2010 Nortel Networks. All Rights Reserved.

1. Select the **TCP transmission enabled** check box.
2. Enter the **Primary server TCP IPv4**.
3. Enter the **Primary server TCP IPv6**.
4. Enter the **Primary server TCP port**. 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.
5. Enter the **Secondary server TCP IPv4**.
6. Enter the **Secondary server TCP IPv6**.
7. Enter the **Secondary server TCP port**. 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.

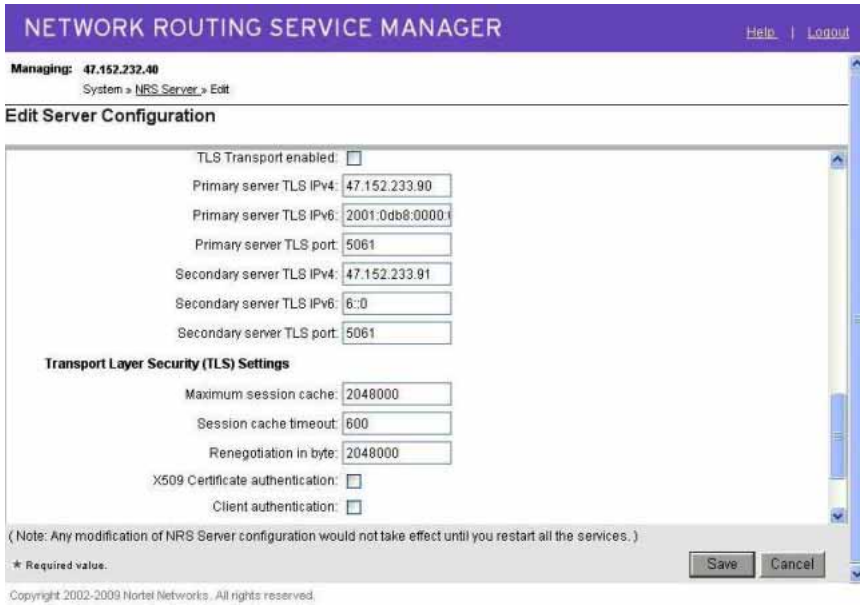
Perform the following steps to enable TLS IPv4:



1. Select the **TLS transmission enabled** check box.
2. Enter the **Primary server TLS IPv4** address.
3. Enter the **Primary server TLS port**. 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 IPv4** address.
5. Enter the **Secondary server TLS port**. 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Perform the following steps to enable TLS IPv6:



1. Select the **TLS transmission enabled** check box.
2. Enter the **Primary server TLS IPv6** address. Global unicast IPv6 addressing is the only supported IPv6 address type.
3. Enter the **Primary server TLS port**. 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 IPv6** address. Global unicast IPv6 addressing is the only supported IPv6 address type.
5. Enter the **Secondary server TLS port**. 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 To configure **Transport Layer Security (TLS) Settings** scroll to the Transport Layer Security (TLS) Settings section of the Edit Server Configuration Web page. See Figure 46 "Transport Layer Security (TLS) Settings and Network Connection Server (NCS) settings" (page 174).

a Enter **Maximum session cache** in text box. The default value is 2048000.

b Enter **Session cache timeout** in text box. The default value is 600.

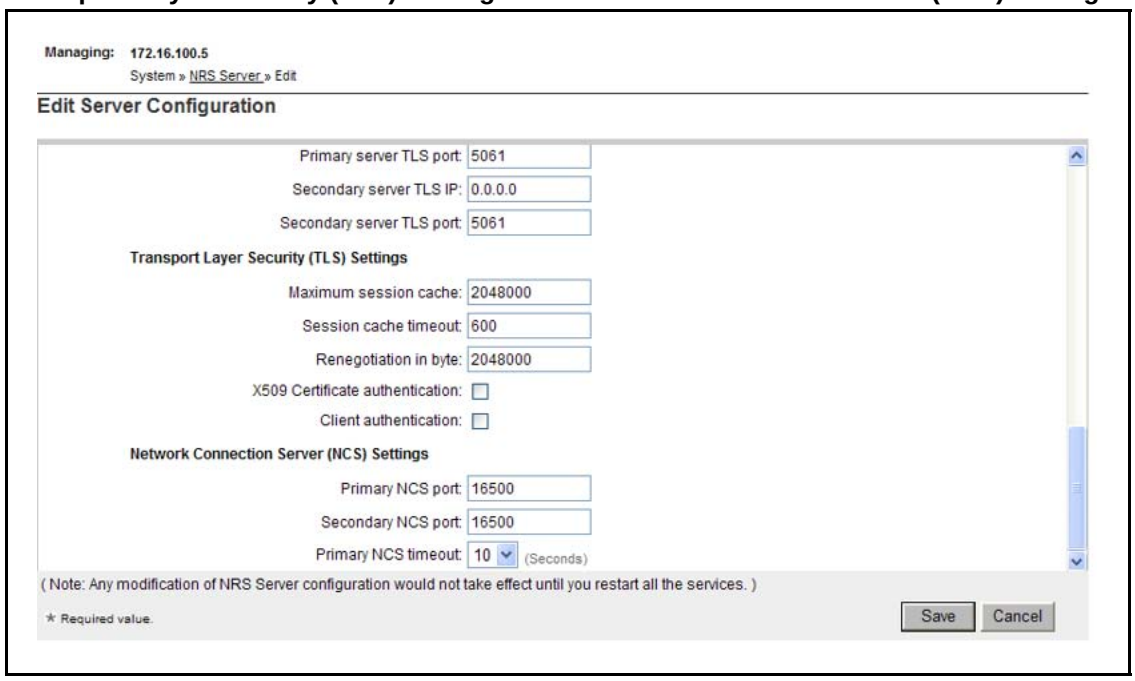
Copyright © 2010 Nortel Networks. All Rights Reserved.

c Enter **Renegotiation in byte** in text box. The default value is 2048000.

d Select the **X509 Certificate authority** check box.

e Select the **Client authority** check box.

Figure 46
Transport Layer Security (TLS) Settings and Network Connection Server (NCS) settings



7 To configure **Network Connection Server (NCS) Settings** scroll to the Network Connection Server (NCS) Settings section of the Edit Server Configuration Web page. See Figure 46 "Transport Layer Security (TLS) Settings and Network Connection Server (NCS) settings" (page 174)

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

8 Click **Save**.

9 The NRS Server Web page appears. Select at least one element on the **Service Status** pane of the **NRS Server** Web page and click **Restart**.

--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.

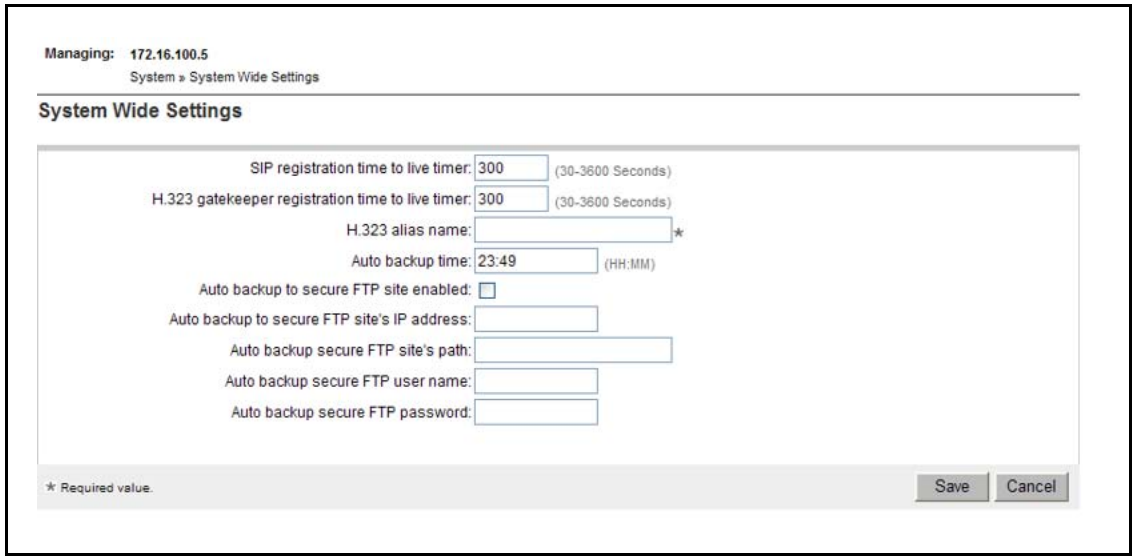
See Procedure 8 “Configuring system-wide settings” (page 175) to configure system-wide settings.

Procedure 8
Configuring system-wide settings

Step	Action
1	In the **NRS Manager Navigator** select **System, System Wide Settings**. The **System Wide Settings** Web page appears. See Figure 47 "System Wide Settings web page" (page 176).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 47
System Wide Settings web page



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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 **Save**.

--End--

Configure the NRS database

Both the SIP Proxy/Redirect Server and the H.323 Gatekeeper use the NRS (MySQL) database. For more information on the NRS database, see "Database component" (page 35).

Task summary list

Perform the procedures in this section to configure the NRS database.

- Procedure 9 "Switching between the Active and Standby databases" (page 178)
- Procedure 10 "Adding a Service Domain" (page 180)
- Procedure 14 "Adding an L1 Domain" (page 186)
- Procedure 18 "Adding an L0 Domain (CDP)" (page 195)
- Procedure 26 "Adding a Gateway Endpoint" (page 213)

  Note: Service Domain, Layer 1 Domain, Layer 0 Domain and Gateway names are case-insensitive. For example, the Service Domain names nortel.com and Nortel.com are considered the same. Similarly, the Layer 1 Domain names UDP and udp are considered the same. If an administrator attempts to configure the same string, even with different case sensitivity, for any of these parameters, the NRS Manager web page displays an error message.

- Procedure 41 "Adding a Routing Entry" (page 246)
- Procedure 22 "Adding a Collaborative Server" (page 204)
- Procedure 60 "Cutting over the database" (page 288)
- Procedure 63 "Committing the database" (page 290)

  Note 1: To add a SIP Phone as a User Endpoint, see Procedure 35 "Adding a User Endpoint" (page 233).

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 and operation component" (page 44).

- The Active database is used for runtime location queries by SIP Proxy, Gatekeeper and NCS.
- The Standby database is used for administrator modifications.

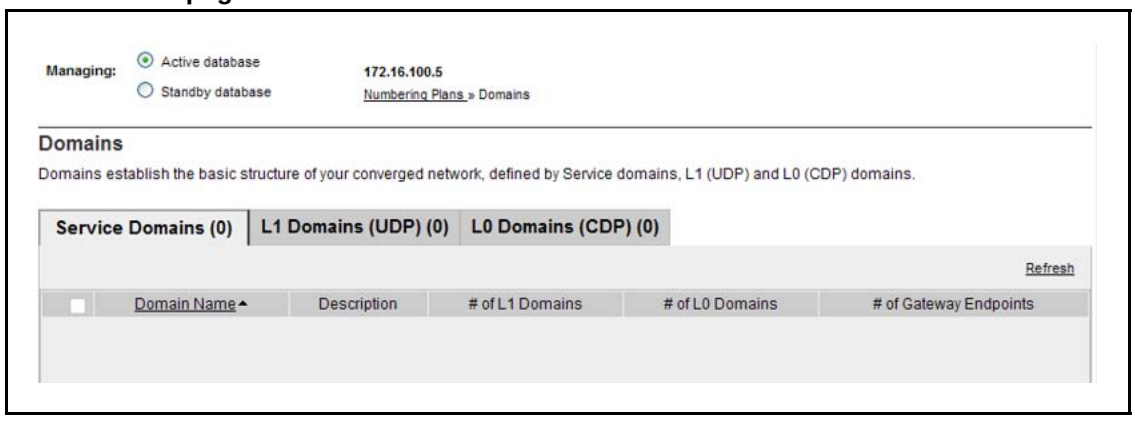
Note: By default, the database is in Active database view when the **Domains** web page is first opened. To modify the database it must be in Standby database view. Only users with administrative authority can modify the database.

Below the NRS Manager header in the Numbering Plans branch of the NRS Manager navigator is an area for switching between the Active and Standby databases. See Procedure 9 "Switching between the Active and Standby databases" (page 178)to switch between the Active and Standby database.

Procedure 9
Switching between the Active and Standby databases

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178).

Figure 48
Domains web page



Copyright © 2010 Nortel Networks. All Rights Reserved.

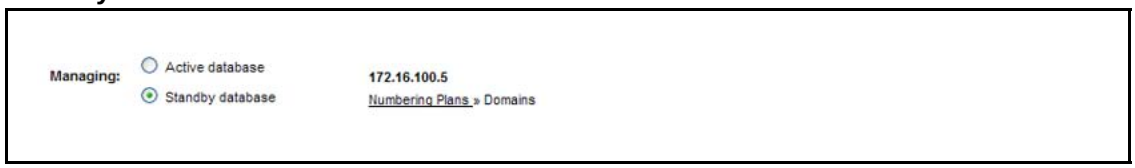
2 Click **Standby database** to switch to the Standby database. See Figure 49 "Active database selected" (page 179). The Standby database is used for database modifications.

Figure 49
Active database selected

or

3 Click **Active database** to switch to the Active database. See Figure 50 "Standby database selected" (page 179). The Active database is used for database queries.

Figure 50
Standby database selected



--End--

Note: Procedure 10 “Adding a Service Domain” (page 180) to Procedure 41 “Adding a Routing Entry” (page 246) 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 41)). For more information on Service Domains see Figure 4 "Hierarchy of the NRS database components" (page 37).

NRS Manager accepts the Primary NRS Server TLAN IP address as a Service Domain name. Use the Primary NRS Server TLAN IP Address only to interwork with third-party gateways that do not support a Service Domain name. Nortel recommends that you do not use third-party gateways for typical CS 1000 deployments. If the Primary NRS Server

Copyright © 2010 Nortel Networks. All Rights Reserved.

TLAN IP Address is used as a Service Domain name, support is not available for the collaborative server functionality because the two systems (original NRS and collaborative NRS) have different Service Domains.

Note: The NRS Manager supports both IPv4 and IPv6 addresses as a Service Domain Name.

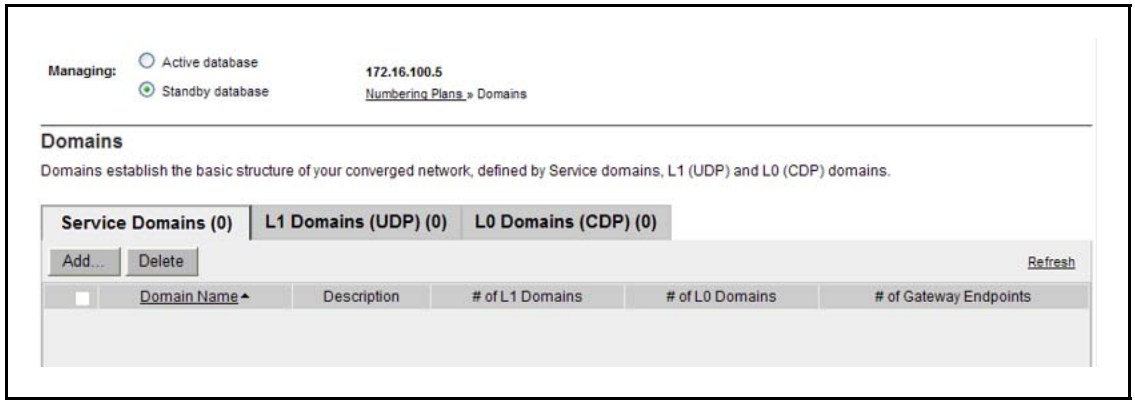
Add a Service Domain

Use the following procedure to add a service domain.

Procedure 10
Adding a Service Domain

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 51 "Service Domains pane" (page 180).

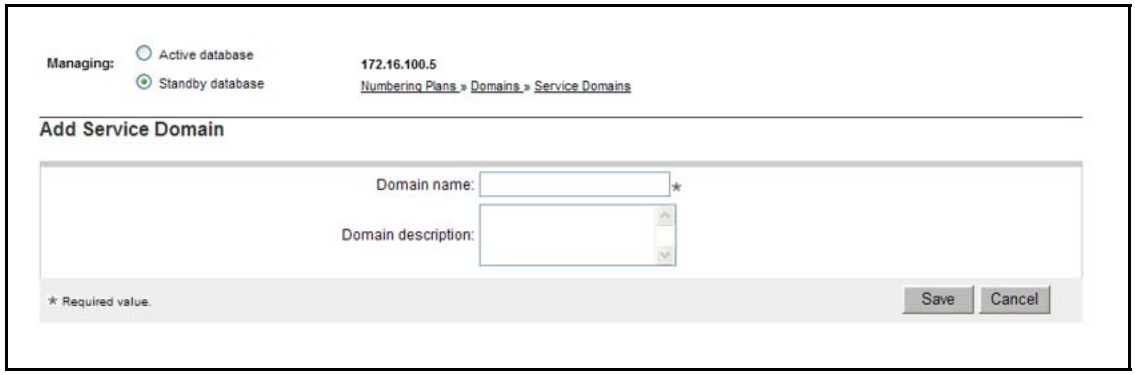
Figure 51
Service Domains pane



3	Click the **Add...** button. The **Add Service Domain** Web page appears as shown in Figure 52 "Add Service Domain web page" (page 181).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 52
Add Service Domain web page



4 Enter a **Domain name** for the Service Domain in the text box.

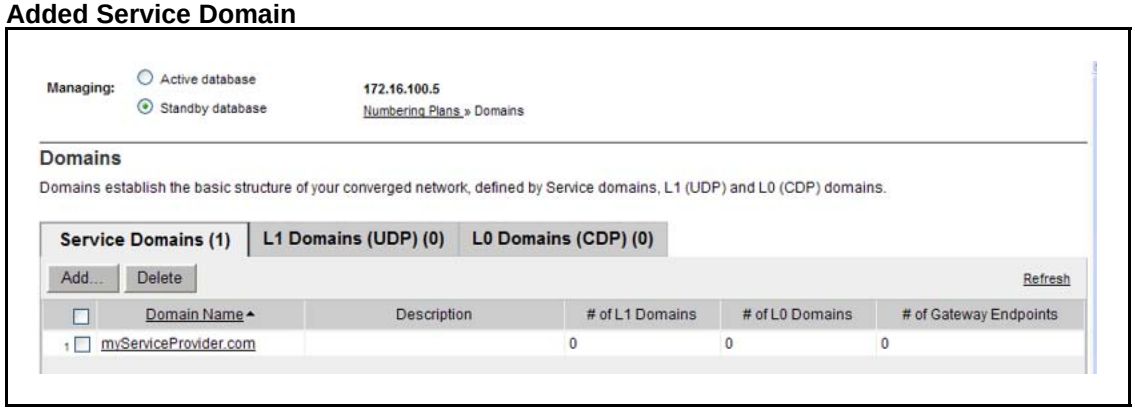
For example, enter myServiceProvider.com.

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 appears showing the newly added myServiceProvider.com Service Domain. See Figure 53 "Added Service Domain" (page 181).

Figure 53
Added Service Domain



7 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

8 Test the configuration changes.

9 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

View the Service Domain

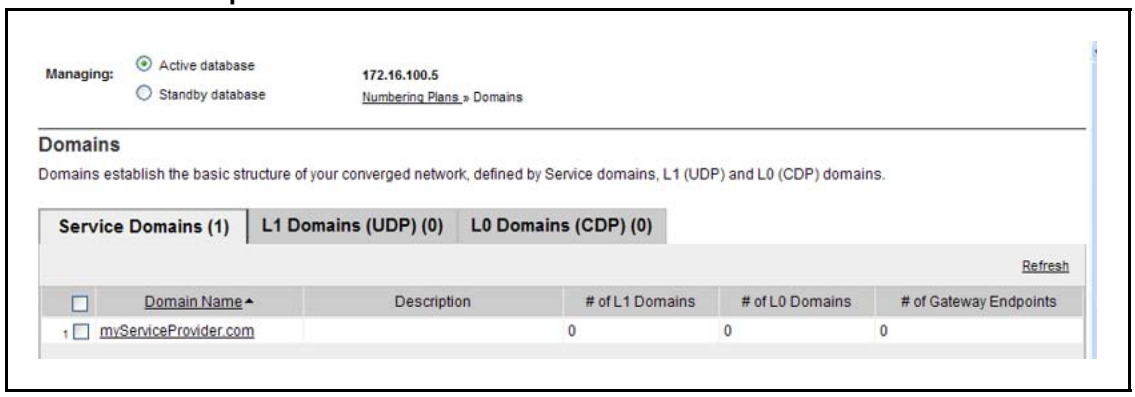
Use the following procedure to view the service domains.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 11
Viewing the Service Domains

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178). The Service Domains can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .
2	Select the **Active** or **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page 178). 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 54 "Service Domains pane Active Database" (page 182).

Figure 54
Service Domains pane Active Database



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 55 "Edit Service Domains web page Active Database" (page 183).

Note: See Procedure 12 “Editing a Service Domain” (page 183) to Edit the Service Domain.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 55
Edit Service Domains web page Active Database

--End--

Edit a Service Domain

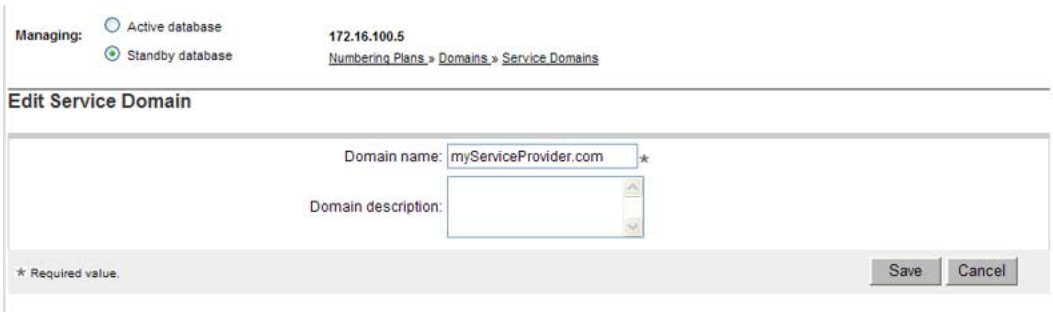
Use the following procedure to edit a service domain.

Procedure 12
Editing a Service Domain

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178). The Service Domains can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 51 "Service Domains pane" (page 180).
3	Click a link in the **ID** column of the **Service Domains** pane. The **Edit Service Domain** Web page appears as shown in Figure 56 "Edit Service Domain web page" (page 184).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 56
Edit Service Domain web page



4 Modify the **Domain name** or the **Domain description** .

5 Click the **Save** button. The standby database is updated.

The **Service Domains** Web page appears as shown in Figure 51 "Service Domains pane" (page 180).

6 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

7 Test the configuration changes.

8 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Delete a Service Domain

Use the following procedure to delete a service domain.

Procedure 13
Deleting a Service Domain

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178). The Service Domains can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 51 "Service Domains pane" (page 180).

Copyright © 2010 Nortel Networks. All Rights Reserved.

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**.

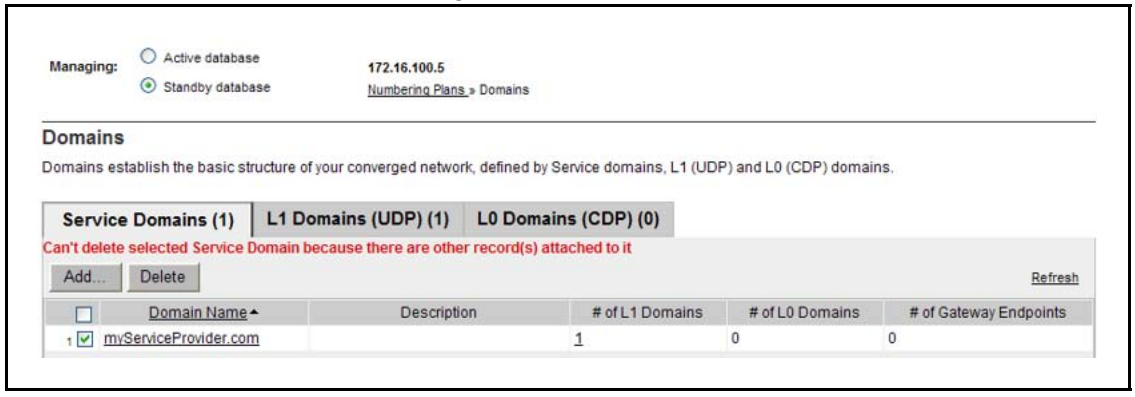
Figure 57
Confirmation Box

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 51 "Service Domains pane" (page 180).

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 58
Delete Service domain error message



The associated **L1 Domain** or **Collaborative Server** must be deleted before the **Service Domain** can be deleted.

See Procedure 17 “Deleting an L1 Domain (UDP)” (page 193) to delete the associated **L1 Domain**.

See Procedure 25 “Deleting a Collaborative Server” (page 212) to delete the associated **Collaborative Server**.

6 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state.

Copyright © 2010 Nortel Networks. All Rights Reserved.

7	See Procedure 63 “Committing the database” (page 290) 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 41). For more information on L1 Domains, see Figure 4 "Hierarchy of the NRS database components" (page 37).

Add an L1 Domain (UDP)

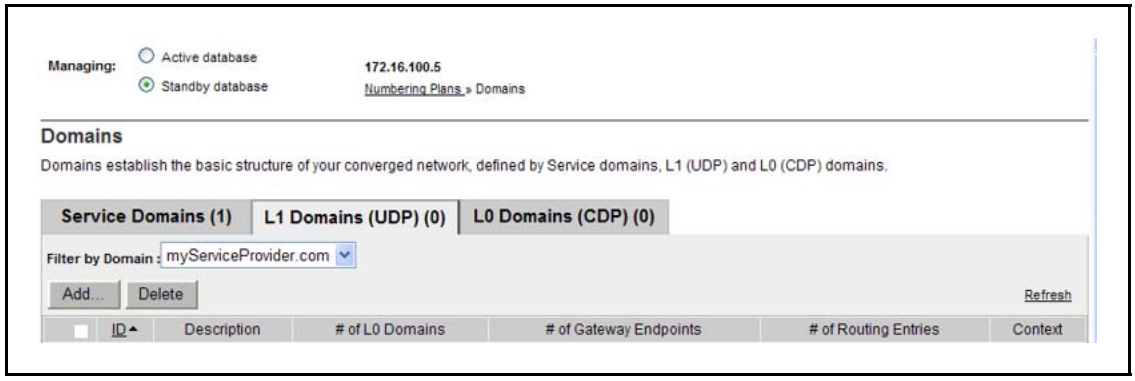
Use the following procedure to add an L1 Domain (UDP).

Procedure 14
Adding an L1 Domain

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 51 "Service Domains pane" (page 180).
3	Click **L1 Domains (UDP)** tab. The **Domains** web page refreshes displaying the **L1 Domains (UDP)** pane, as shown in Figure 59 "L1 Domains (UDP) pane" (page 187). The L1 Domains can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 59
L1 Domains (UDP) pane

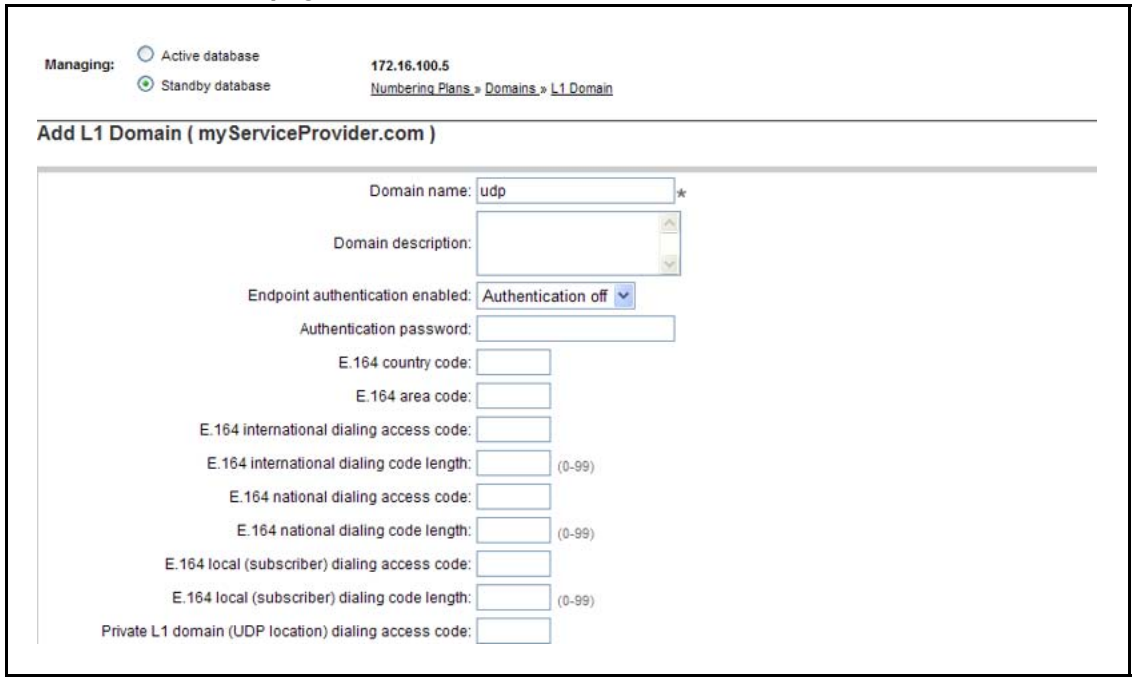


4 The **Filter by Domain:** drop-down list contains configured Service Domains. Select the **Service Domain**, where the new L1 subdomain will be added, from the drop-down list.

5 Click the **Add...** button.

The **Add L1 Domain** Web page appears as shown in Figure 60 "Add L1 Domain web page" (page 187).

Figure 60
Add L1 Domain web page



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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 160).

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

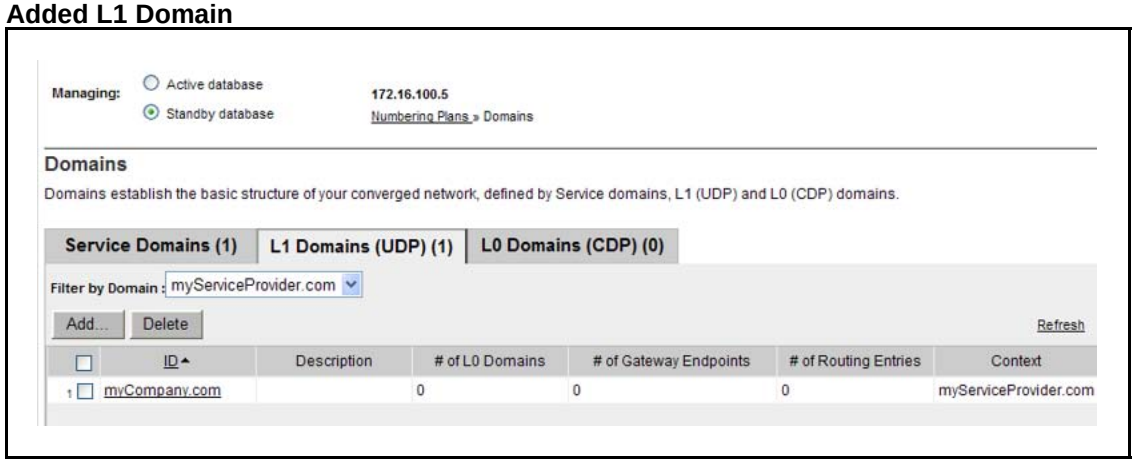
22 Enter the **Emergency service access prefix** in the text box. The number must be numeric and can be up to 30 digits in length.

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 displays the newly added myCompany.com L1 domain in the myServiceProvider.com Service Domain. See Figure 61 "Added L1 Domain" (page 189).

Figure 61
Added L1 Domain



25 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

26 Test the configuration changes.

27 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

View an L1 Domain (UDP)

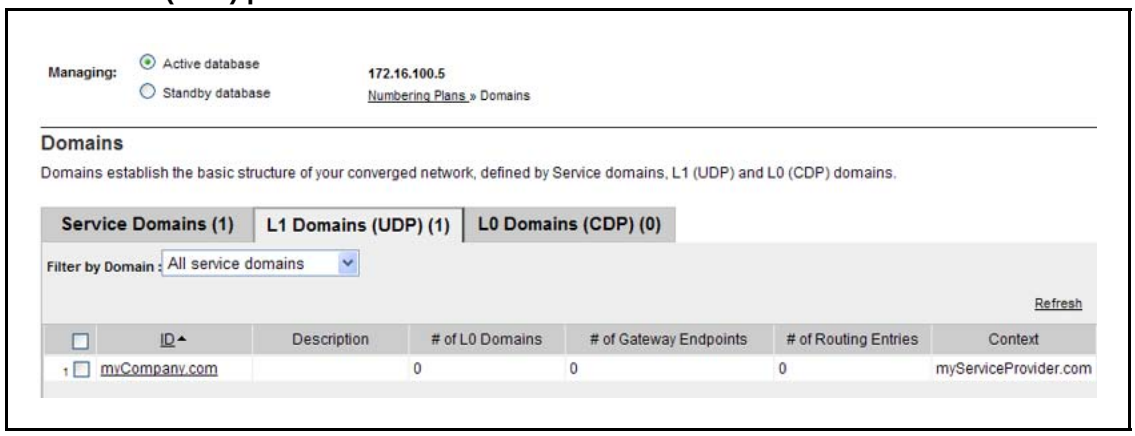
Use the following procedure to view an L1 Domain (UDP).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 15
Viewing an L1 Domain (UDP)

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178).
2	Select the **Active** or **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page 178). 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 54 "Service Domains pane Active Database" (page 182).
3	Click **L1 Domains (UDP)** tab. The **Domains** web page refreshes displaying the **L1 Domains (UDP)** pane, as shown in Figure 62 "L1 Domains (UDP) pane Active database" (page 190). The L1 Domains can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

Figure 62
L1 Domains (UDP) pane Active database



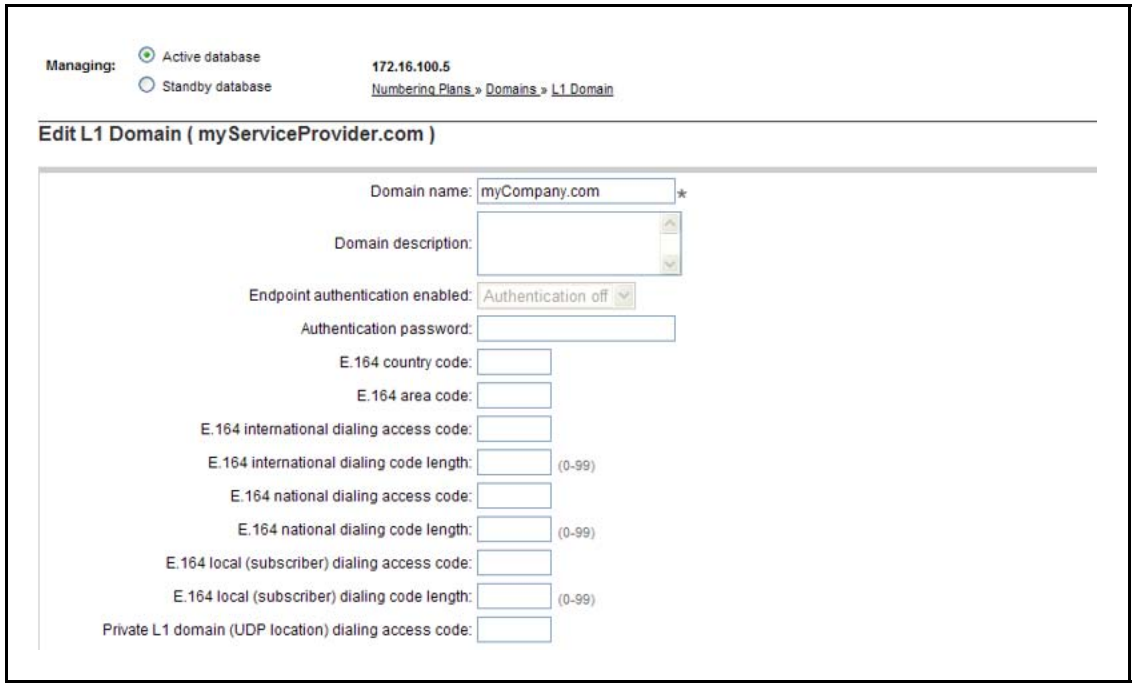
4	The **Filter by Domain:** drop-down list contains configured Service Domains. Select the **Service Domain**, that the L1 domain is a subdomain of, from the drop-down list. The **Domains** web page refreshes.
5	Click a **link** in the **ID** column of the L1 domains (UDP) web page. The **Edit L1 Domain** web page opens and displays the configured data for the selected L1 Domain, as shown in Figure

Copyright © 2010 Nortel Networks. All Rights Reserved.

63 "Edit L1 Domain (UDP) web page Active database" (page 191).

Note: See Procedure 16 “Editing an L1 Domain (UDP)” (page 191) to Edit the L1 Domain.

Figure 63
Edit L1 Domain (UDP) web page Active database



--End--

Edit an L1 Domain (UDP)

Use the following procedure to edit an L1 Domain (UDP).

Procedure 16
Editing an L1 Domain (UDP)

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).

Copyright © 2010 Nortel Networks. All Rights Reserved.

The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 51 "Service Domains pane" (page 180).

3 Click **L1 Domains (UDP)** tab.

The **Domains** web page refreshes displaying the **L1 Domains (UDP)** pane, as shown in Figure 59 "L1 Domains (UDP) pane" (page 187).

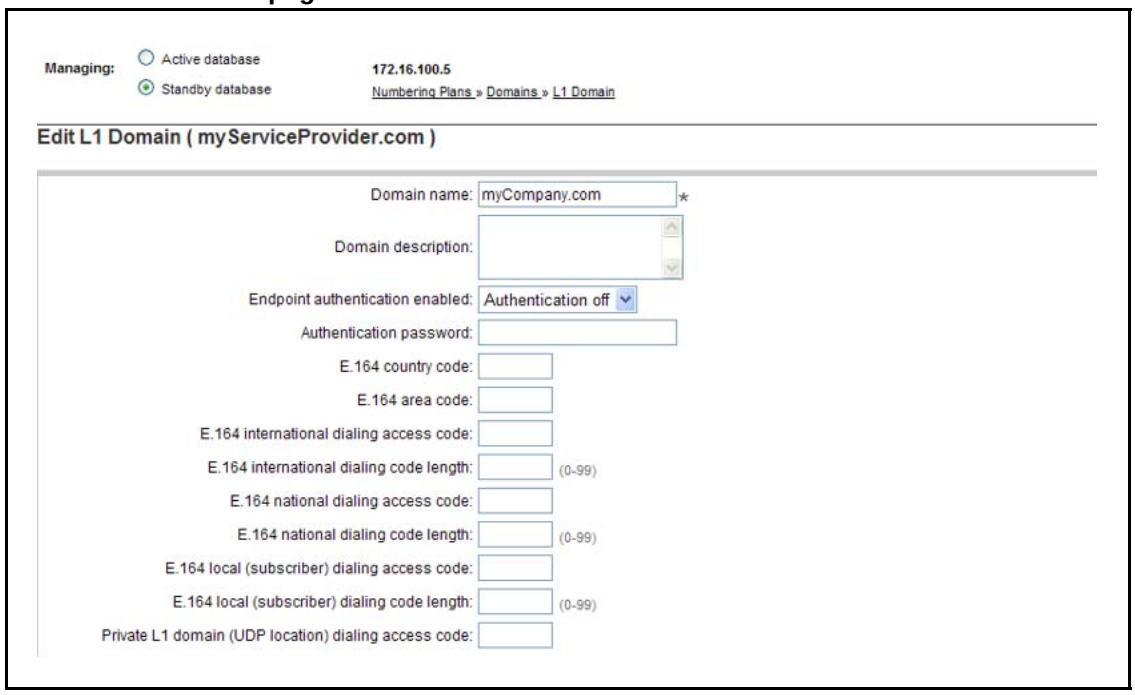
The L1 Domains can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

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 appears as shown in Figure 64 "Edit L1 Domain web page" (page 192).

Figure 64
Edit L1 Domain web page



6 Modify the fields of the **Edit L1 Domain** web page as appropriate. See “Manage a Level 1 Domain (UDP)” (page 186).

Note: An L1 Domain can inherit configuration parameters from its parent Service Domain. See “Numbering Plans inherited fields” (page 160).

7 Click the **Save** button.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The standby database is updated. The **Domains** web page opens displaying the **L1 Domains (UDP)** pane, as shown in Figure 59 "L1 Domains (UDP) pane" (page 187).

8 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

9 Test the configuration changes.

10 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Delete an L1 Domain (UDP)

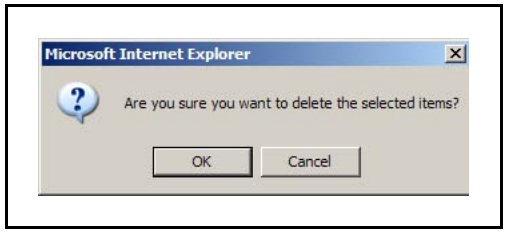
Use the following procedure to delete an L1 Domain (UDP).

Procedure 17
Deleting an L1 Domain (UDP)

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 51 "Service Domains pane" (page 180).
3	Click **L1 Domains (UDP)** tab. The **Domains** web page refreshes displaying the **L1 Domains (UDP)** pane, as shown in Figure 59 "L1 Domains (UDP) pane" (page 187). The L1 Domains can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .
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**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 65
Confirmation Box

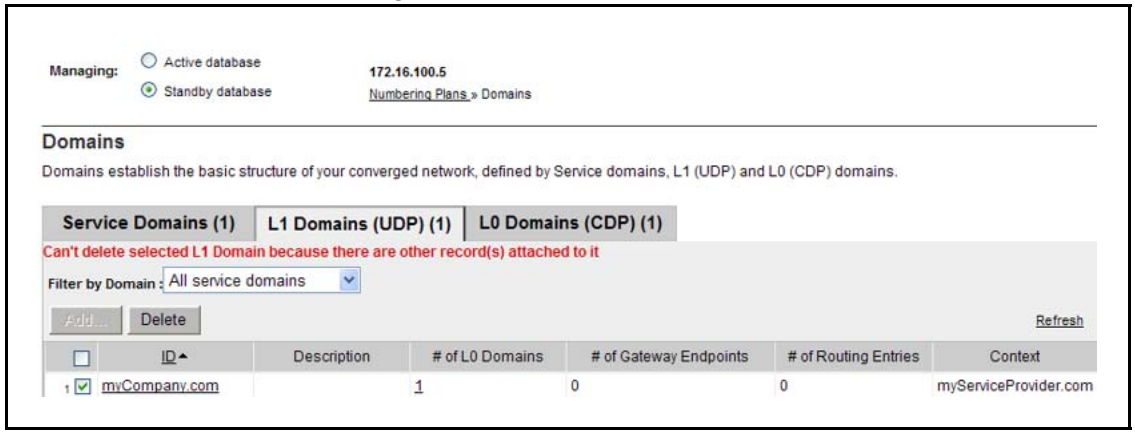


7 Click **OK**.

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 59 "L1 Domains (UDP) pane" (page 187).

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 66 "Delete L1 Domain error message" (page 194).

Figure 66
Delete L1 Domain error message



The associated **L0 Domain** or **Collaborative Server** must be deleted before the **L1 Domain** can be deleted.

See Procedure 21 “Deleting an L0 Domain (CDP)” (page 202) to delete the associated **L0 Domain**.

See Procedure 25 “Deleting a Collaborative Server” (page 212) to delete the associated **Collaborative Server**.

8 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state.

9 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 41). For more information on L0 Domains, see Figure 4 "Hierarchy of the NRS database components" (page 37).

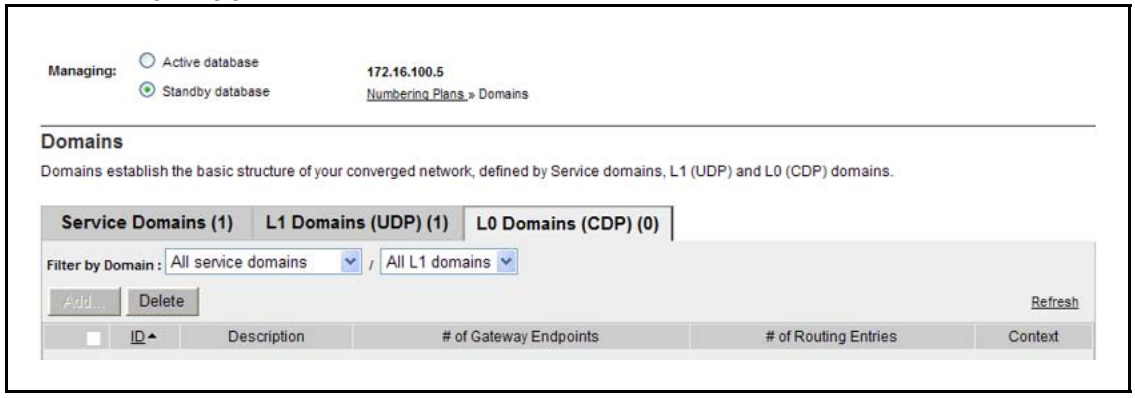
Add an L0 Domain (CDP)

Use the following procedure to add an L0 Domain (CDP).

Procedure 18
Adding an L0 Domain (CDP)

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178).
2	Ensure **Standby database** is selected. See Procedure 9 "Switching between the Active and Standby databases" (page 178). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 51 "Service Domains pane" (page 180).
3	Click **L0 Domains (CDP)** tab. The **Domains** web page refreshes displaying the **L0 Domains (CDP)** pane, as shown in Figure 67 "L0 Domain (CDP) pane" (page 195).

Figure 67
L0 Domain (CDP) pane

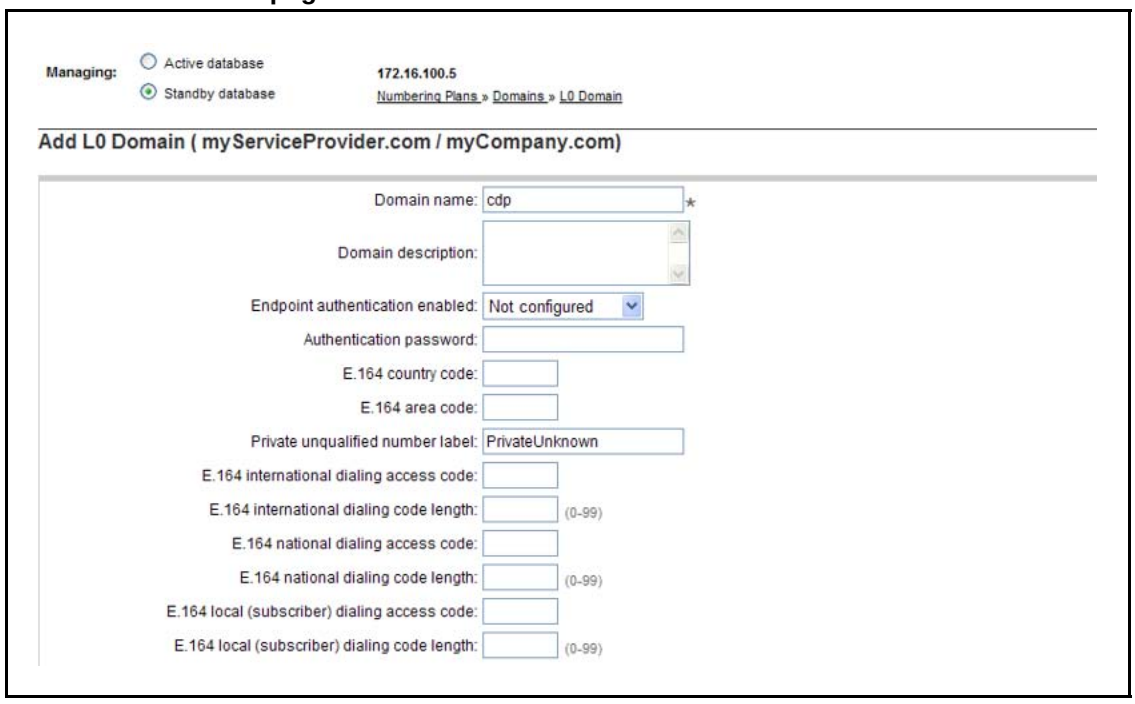


4	The **Filter by Domain:** drop-down lists contain configured Service Domains and L1 Domains. Select the Service Domain and the L1 Domain, where the new L0 subdomain will be added, from the respective drop-down lists.
5	Click the **Add...** button.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The **Add L0 Domain** Web page appears as shown in Figure 68 "Add L0 Domain web page" (page 196).

Figure 68
Add L0 Domain web page



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 160).

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

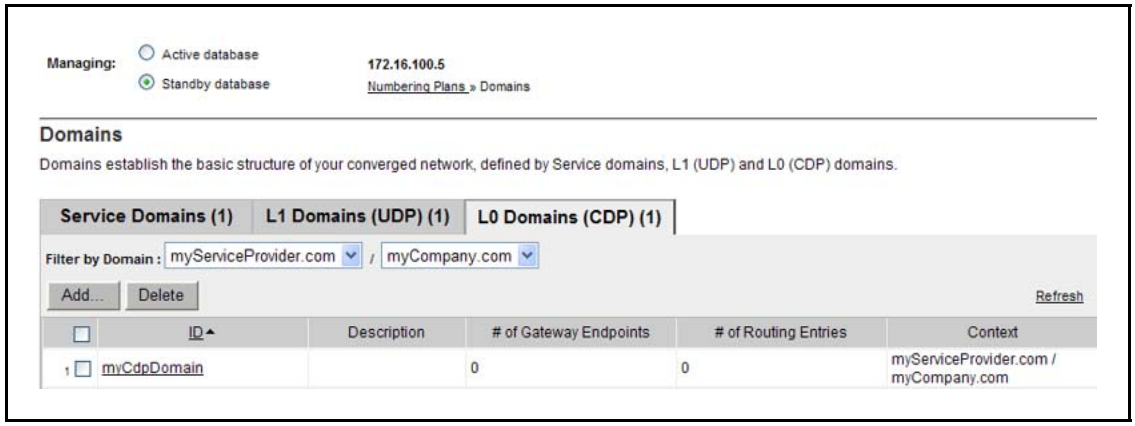
23 Enter the **Emergency services access prefix** in the text box. The number must be numeric and can be up to 30 digits in length.

24 Click the **Save** button. The standby database is updated.

The **Domains** Web page displays the newly added myCdpDomain L0 domain. See Figure 69 "Added L0 Domain" (page 198).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 69
Added L0 Domain



25 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

26 Test the configuration changes.

27 See Procedure 63 “Committing the database” (page 290) 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 19
Viewing an L0 Domain (CDP)

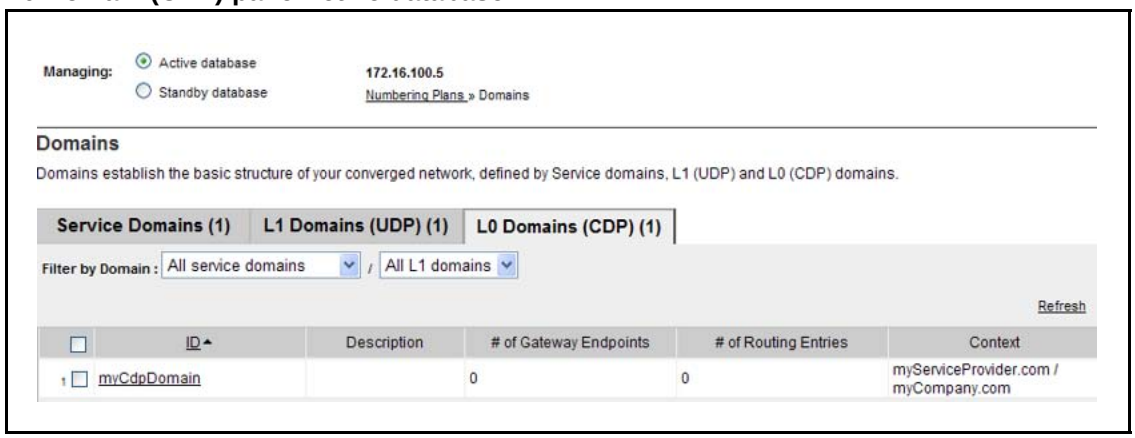
Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178).
2	Select the **Active** or **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page 178). 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 54 "Service Domains pane Active Database" (page 182).
3	Click **L0 Domains (CDP)** tab.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The **Domains** web page refreshes displaying the **L0 Domains (CDP)** pane, as shown in Figure 70 "L0 Domain (CDP) pane Active database" (page 199).

The L0 Domains can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

Figure 70
L0 Domain (CDP) pane Active database



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.

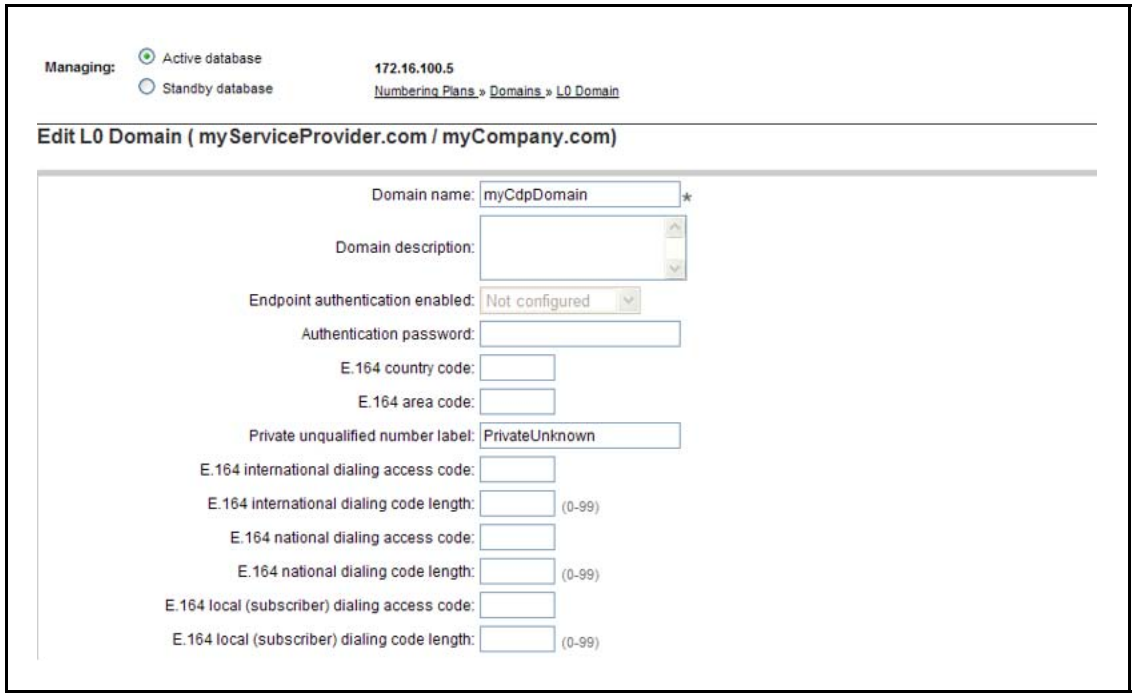
The **Edit L0 Domain** web page opens and displays the configured data for the selected L0 Domain.

See Figure 71 "Edit L0 Domain (CDP) web page Active database" (page 200).

Note: See Procedure 20 “Editing an L0 Domain (CDP)” (page 200) to Edit the L0 Domain.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 71
Edit L0 Domain (CDP) web page Active database



--End--

Edit an L0 Domain (CDP)

Use the following procedure to edit an L0 Domain (CDP).

Procedure 20
Editing an L0 Domain (CDP)

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 51 "Service Domains pane" (page 180).
3	Click **L0 Domains (CDP)** tab. The **Domains** web page refreshes displaying the **L0 Domains (CDP)** pane, as shown in Figure 67 "L0 Domain (CDP) pane" (page 195).

Copyright © 2010 Nortel Networks. All Rights Reserved.

The L0 Domains can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

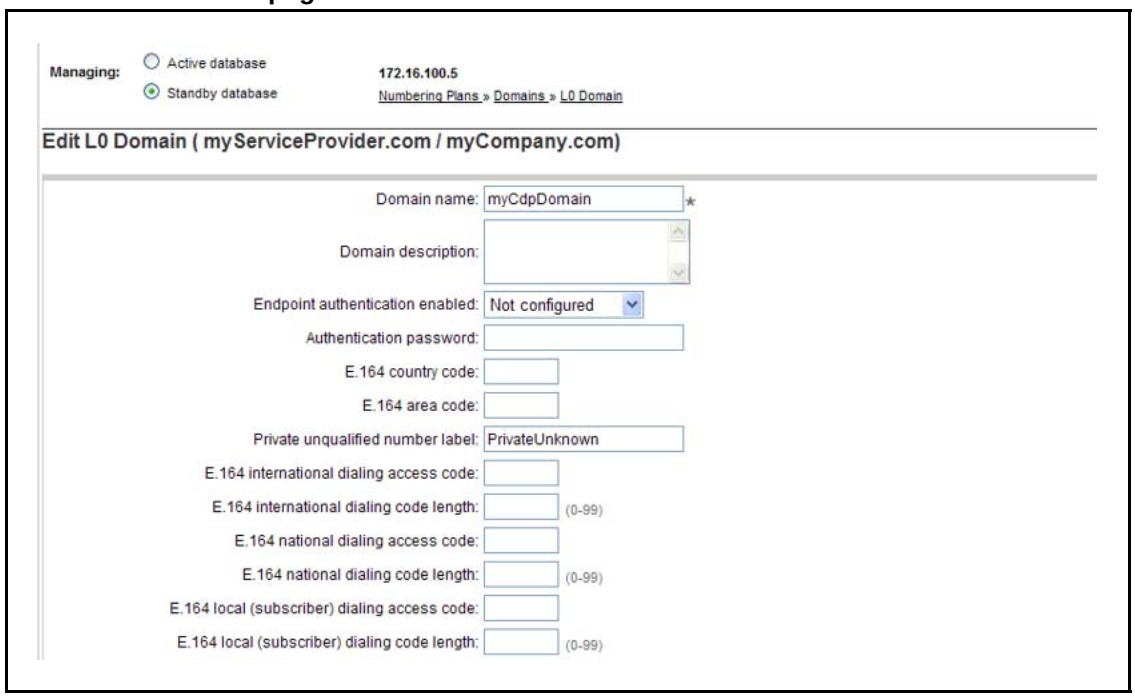
4 The **Filter by Domain:** drop-down lists contain configured Service Domains and L1 Domains. Select a Service Domain and L1 Domain from the drop-down lists.

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 appears as shown in Figure 72 "Edit L0 Domain web page" (page 201).

Figure 72
Edit L0 Domain web page



6 Modify the fields of the **Edit L0 Domain** web page as appropriate. See Procedure 18 “Adding an L0 Domain (CDP)” (page 195).

> ***Note:*** An L1 Domain can inherit configuration parameters from its parent L0 Domain. See “Numbering Plans inherited fields” (page 160)

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 67 "L0 Domain (CDP) pane" (page 195).

Copyright © 2010 Nortel Networks. All Rights Reserved.

8	See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.
9	Test the configuration changes.
10	See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Delete an L0 Domain (CDP)

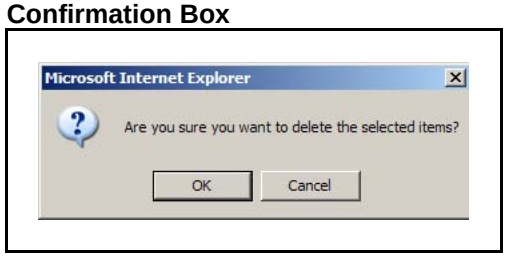
Use the following procedure to delete an L0 Domain (CDP).

Procedure 21
Deleting an L0 Domain (CDP)

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Domains.** The **Domains** Web page appears as shown in Figure 48 "Domains web page" (page 178).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178). The **Domains** web page refreshes displaying the **Service Domains** pane, as shown in Figure 51 "Service Domains pane" (page 180).
3	Click **L0 Domains (CDP)** tab. The **Domains** web page refreshes displaying the **L0 Domains (UDP)** pane, as shown in Figure 67 "L0 Domain (CDP) pane" (page 195). The L0 Domains can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .
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**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 73
Confirmation Box

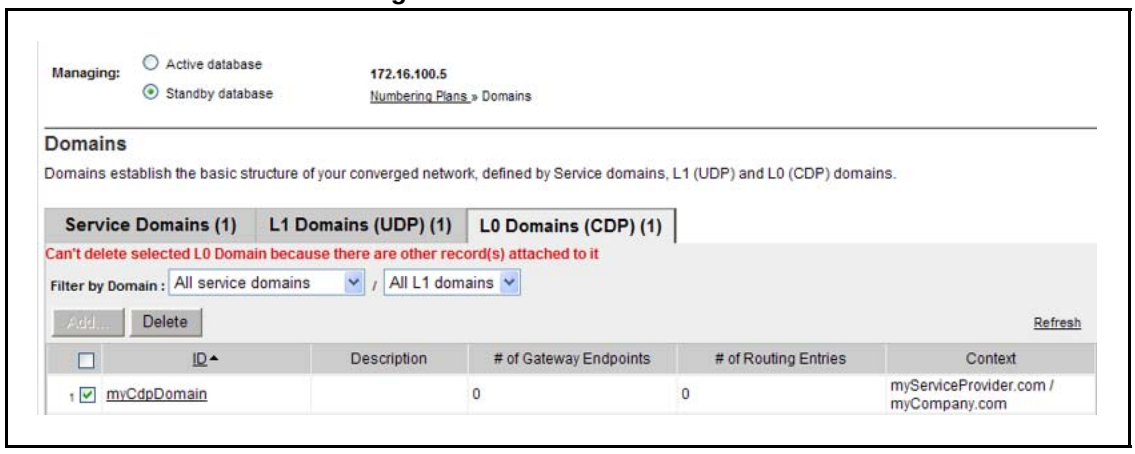


7 Click **OK**.

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 67 "L0 Domain (CDP) pane" (page 195).

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 74 "Delete L0 Domain error message" (page 203).

Figure 74
Delete L0 Domain error message



The associated **Collaborative Server** must be deleted before the **L0 Domain** can be deleted.

See Procedure 25 “Deleting a Collaborative Server” (page 212)to delete the associated **Collaborative Server**.

> ***Note:*** An error message is displayed if there is a Gateway Endpoint or a routing entry configured in the L0 Domain. The Gateway Endpoint or routing entry must be deleted before the L0 domain can be deleted. See Procedure 30 “Deleting the Gateway Endpoints” (page 226) to delete a Gateway Endpoint. See Procedure 44 “Deleting a Routing Entry” (page 252) to delete a routing entry.

8 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state.

Copyright © 2010 Nortel Networks. All Rights Reserved.

9	See Procedure 63 “Committing the database” (page 290) 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.

Earlier to Release 7.0, calls through the collaborative servers could only be made in the same domain. Calls failed if a mismatch was found in the keys formed between the first SPS and the second SPS.

In Release 7.0, support for IPv6 related calls through IPv4 or IPv6 collaborative servers is achieved by building two x-nt-trusted (x-nt-trusted and x-nt-trusted-v6) headers for IPv4 and IPv6 respectively.

Add a Collaborative Server

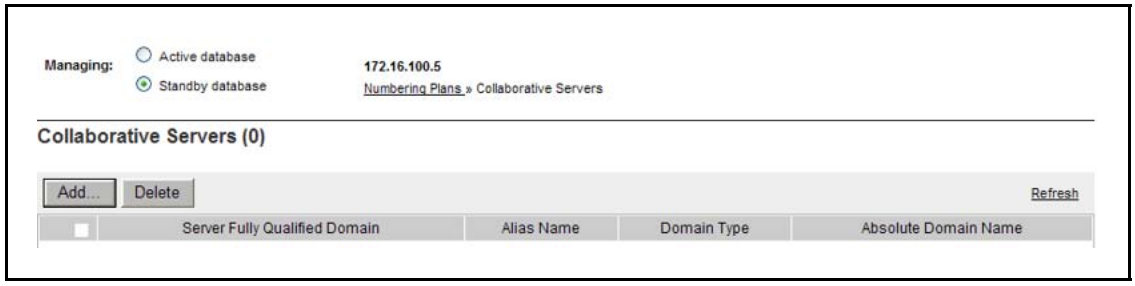
Use the following procedure to add a Collaborative Server.

Procedure 22
Adding a Collaborative Server

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Collaborative Servers.** The **Collaborative Servers** Web page appears as shown in Figure 75 "Collaborative Servers web page" (page 205).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 75
Collaborative Servers web page

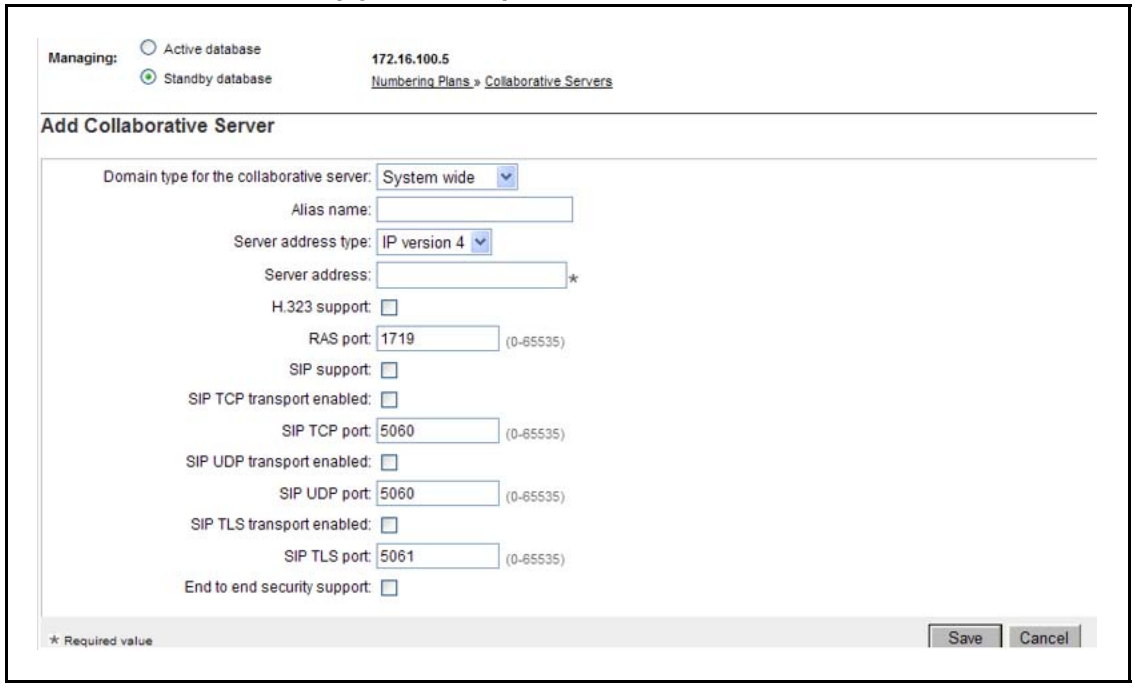


2 Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178)

3 Click the **Add....** button.

The **Add Collaborative Server** Web page appears as shown in Figure 76 "Add Collaborative Server (System wide)" (page 205).

Figure 76
Add Collaborative Server (System wide)



4 Select the **Domain type for Collaborative Server** from the drop-down list.

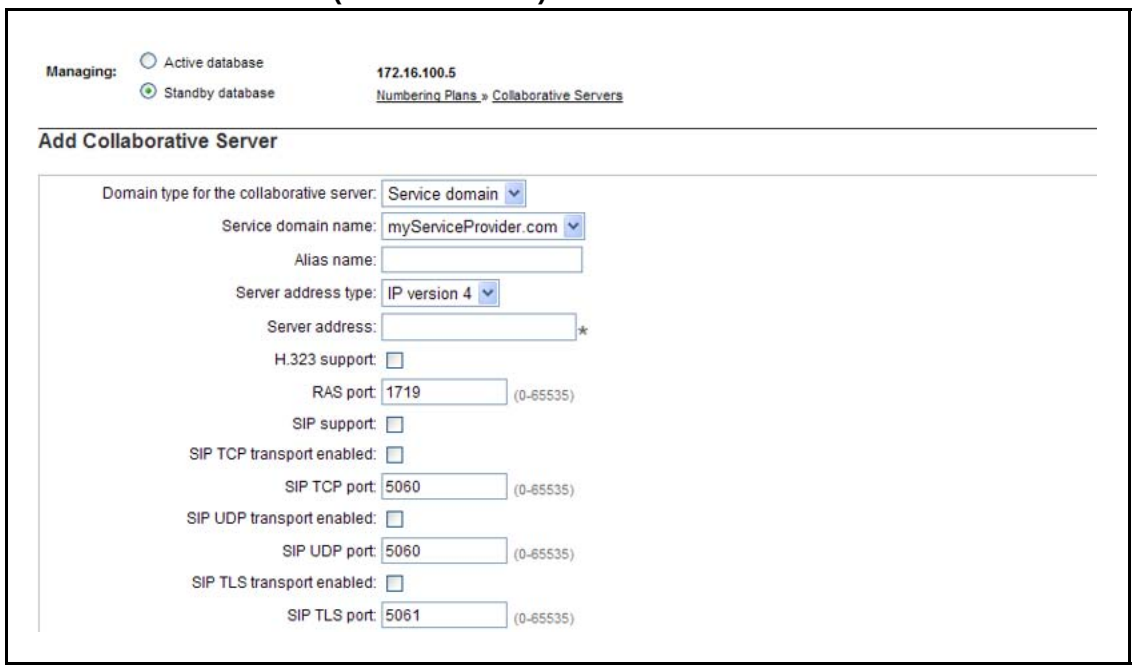
- Select **System wide** if the Collaborative Server is to be a system-wide server. See Figure 76 "Add Collaborative Server (System wide)" (page 205).
- Select **Service domain** if the Collaborative Server is to be a Service Domain server.

Copyright © 2010 Nortel Networks. All Rights Reserved.

An additional field **Service domain name** is displayed, as shown in Figure 77 "Add Collaborative Server (Service domain)" (page 206). 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 78 "Add Collaborative Server (L1 Domain)" (page 207). 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 79 "Add Collaborative Server (L0 Domain)" (page 207). Select the Service Domain name, the L1 Domain name and the L0 Domain name from the drop-down lists.

Figure 77
Add Collaborative Server (Service domain)



Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 78
Add Collaborative Server (L1 Domain)

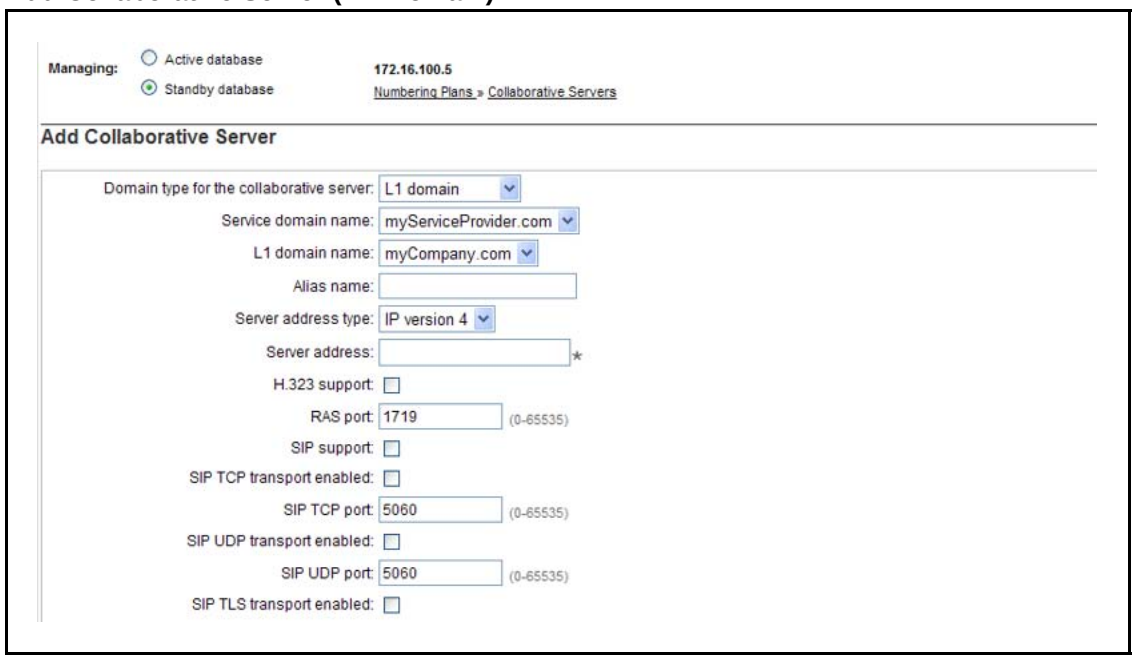
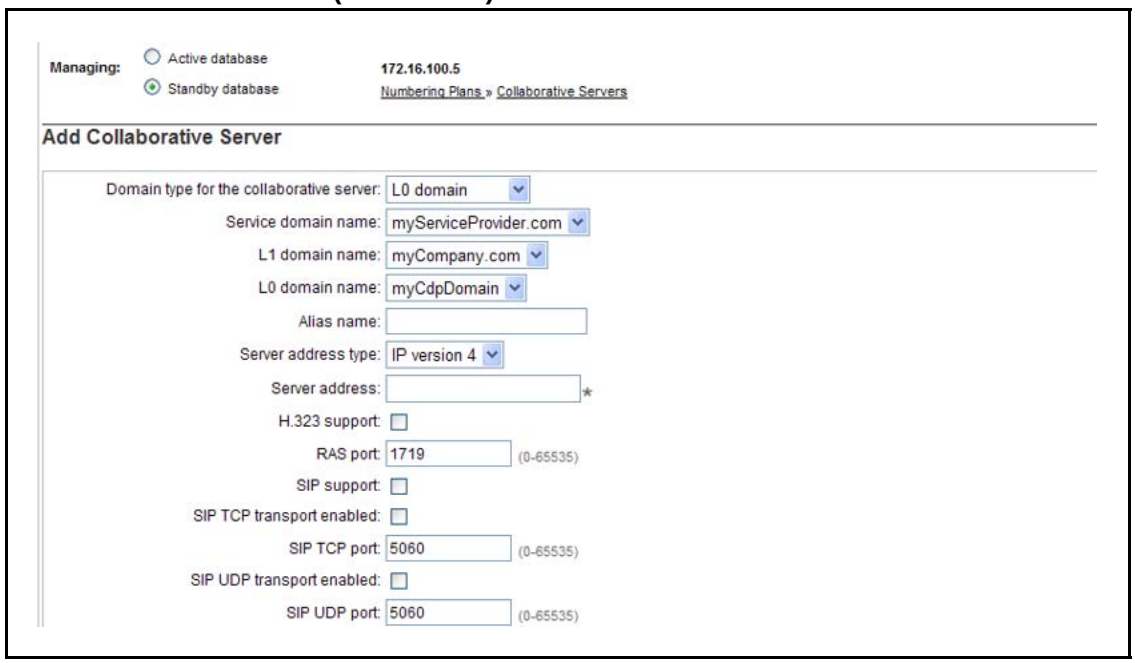


Figure 79
Add Collaborative Server (L0 Domain)



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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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:
  a. Select the **H.323 support** check box.
  b. 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:
  a. Select the **SIP support** check box.
  b. 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.

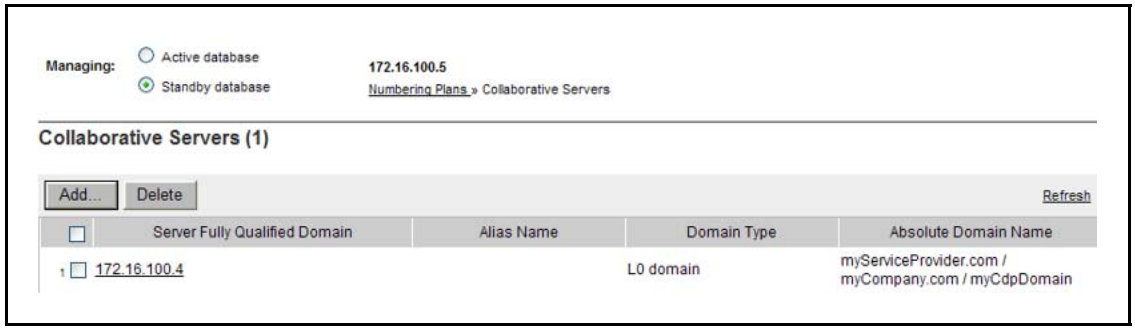
     If SIP TLS is supported:
     – Select the **SIP TLS transport enabled** check box.
     – Enter the **SIP TLS port** number in the text box. The port number must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port value is 5061.
- If **End to end security** is 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 80 "Added Collaborative Server" (page 209).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 80
Added Collaborative Server



10 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

11 Test the configuration changes.

12 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

View a Collaborative Server

Use the following procedure to view a Collaborative Server.

Procedure 23
Viewing a Collaborative Server

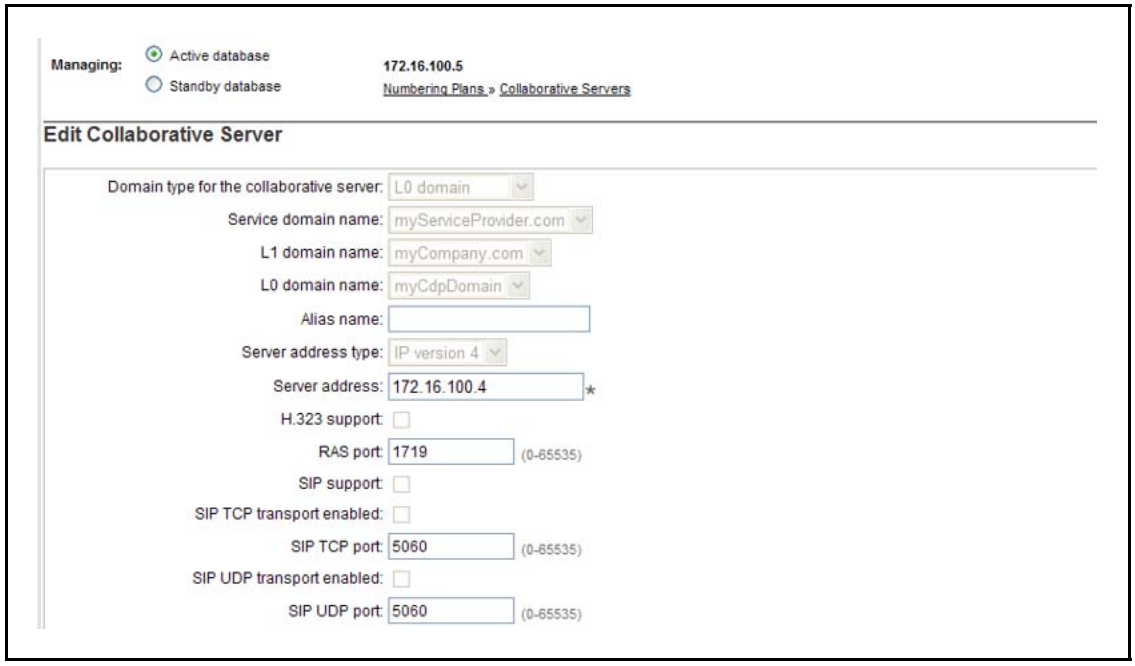
Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Collaborative Servers.** The **Collaborative Servers** Web page displays a list of configured Collaborative Servers as shown in Figure 75 "Collaborative Servers web page" (page 205). The Collaborative Servers can be sorted in ascending or descending alphabetical order. See "Sort web page by Server Fully Qualified Domain " (page 158) .
2	Select the **Active** or **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page 178). 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

See Figure 81 "Edit Collaborative Server web page Active database" (page 210).

Note: See Procedure 24 “Editing a Collaborative Server” (page 210) to Edit the Collaborative Server.

Figure 81
Edit Collaborative Server web page Active database



--End--

Edit a Collaborative Server

Use the following procedure to edit a Collaborative Server.

Procedure 24
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 75 "Collaborative Servers web page" (page 205). The Collaborative Servers can be sorted in ascending or descending alphabetical order. See "Sort web page by Server Fully Qualified Domain " (page 158) .

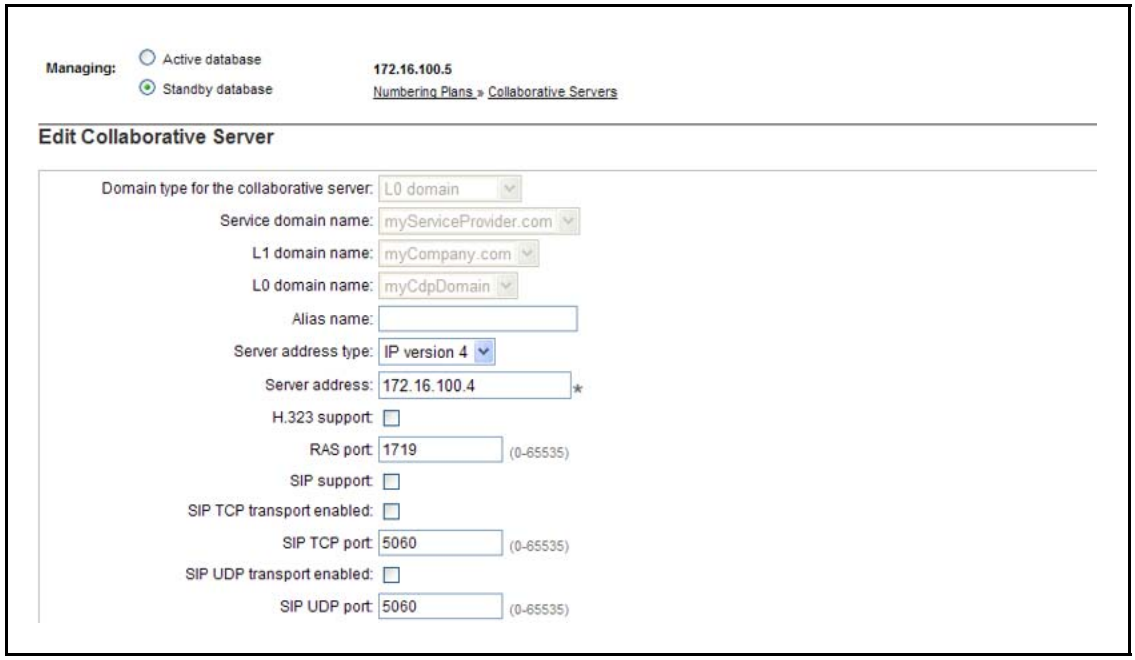
Copyright © 2010 Nortel Networks. All Rights Reserved.

2 Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178)

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 82 "Edit Collaborative Server web page" (page 211).

Figure 82
Edit Collaborative Server web page



4 Modify the fields of the **Edit Collaborative Server** web page as appropriate. See Procedure 22 “Adding a Collaborative Server” (page 204).

5 Click **Save**. The standby database is updated.

The **Collaborative Servers** Web page appears as shown in Figure 75 "Collaborative Servers web page" (page 205).

6 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

7 Test the configuration changes.

8 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

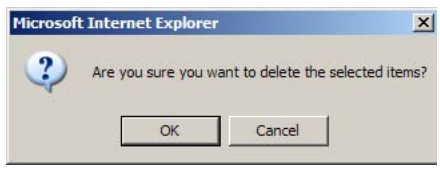
--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Delete a Collaborative Server

Use the following procedure to delete a Collaborative Server.

Procedure 25
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 75 "Collaborative Servers web page" (page 205). The Collaborative Servers can be sorted in ascending or descending alphabetical order. See "Sort web page by Server Fully Qualified Domain " (page 158) .
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178)
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 83** **Confirmation Box** 
5	Click **OK**. The standby database is updated. The **Collaborative Servers** web refreshes displaying a list of configured collaborative servers, as shown in Figure 75 "Collaborative Servers web page" (page 205).
6	See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state.
7	See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Manage a Gateway Endpoint

Release 7.0 supports 5 000 Gateway Endpoints and User Endpoints.

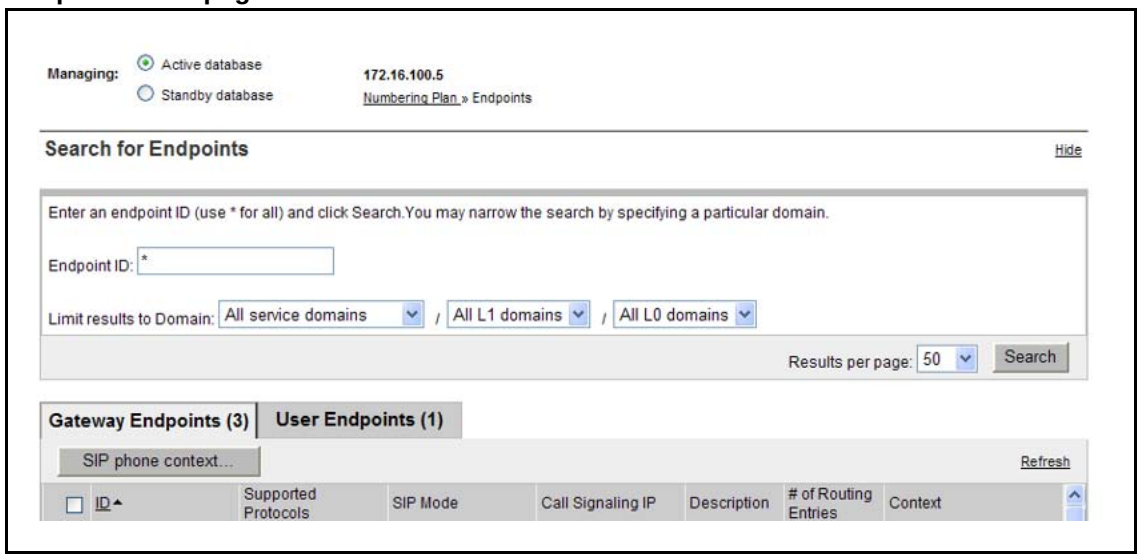
Add a Gateway Endpoint

Perform the following procedure to add a Gateway Endpoint.

Procedure 26
Adding a Gateway Endpoint

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** Web page appears, as shown in Figure 84 "Endpoints web page" (page 213).

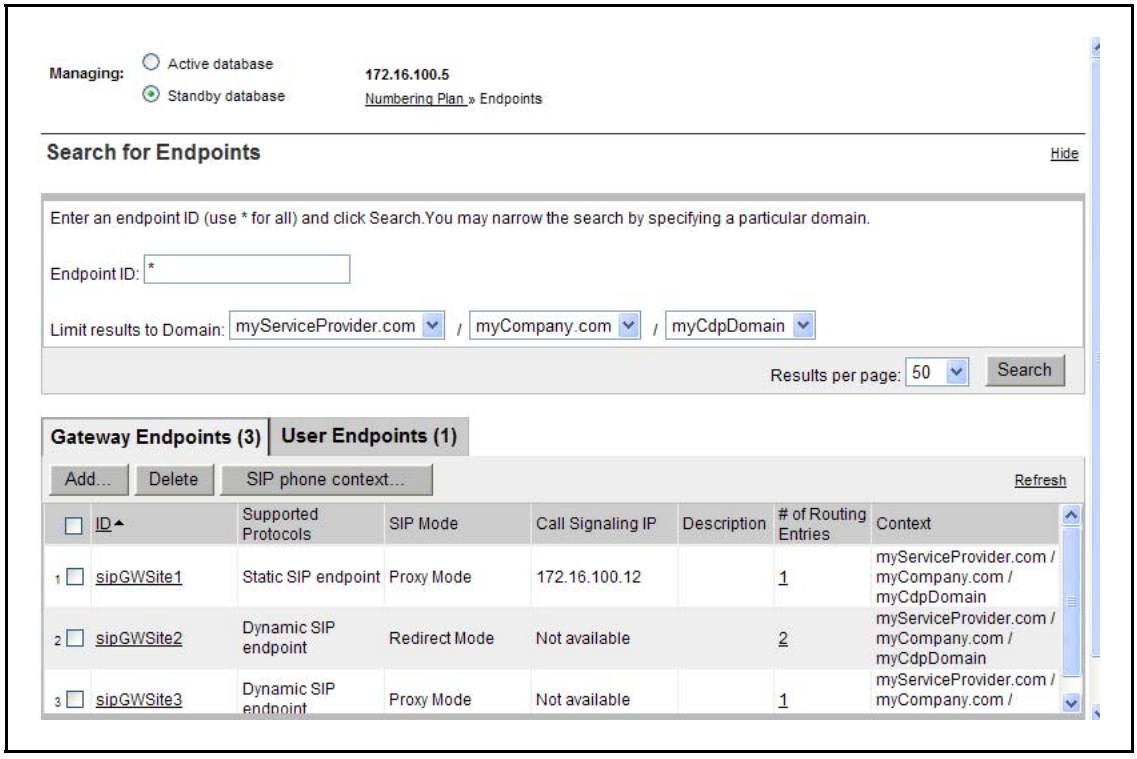
Figure 84
Endpoints web page



2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
3	The **Limit results to Domain:** lists contain configured Service Domains, Layer 1 Domains and Layer 0 Domains. Select a Service Domain, a Layer 1 Domain and a Layer 0 Domain from the respective drop-down lists.
4	Click the **Gateway Endpoints** tab. The **Endpoints** Web page refreshes displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 85 "Gateway Endpoints pane" (page 214). You can sort the Gateway Endpoints in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 85
Gateway Endpoints pane



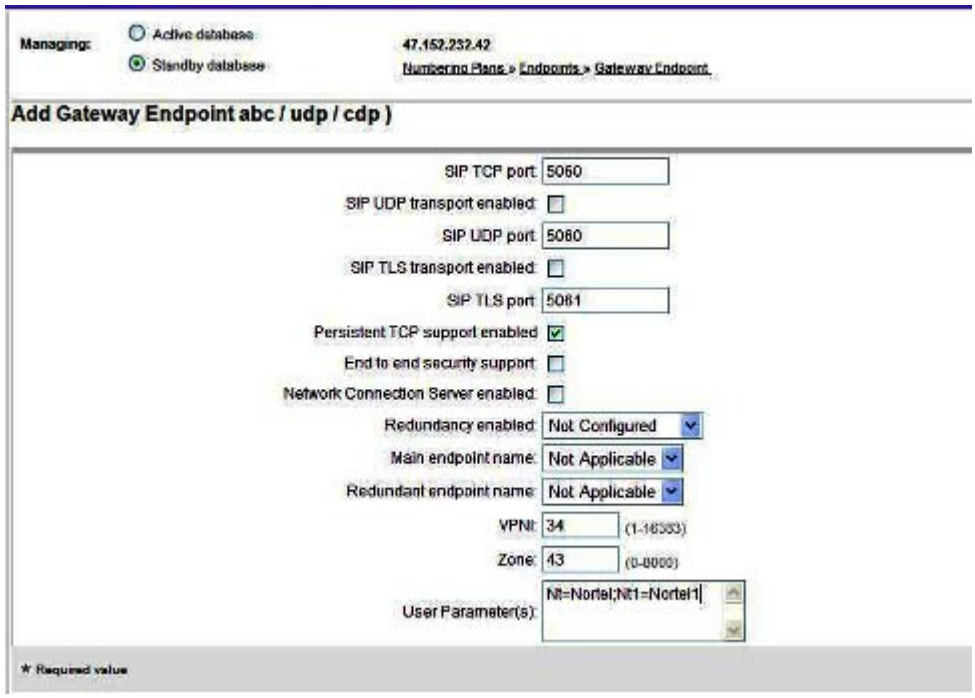
5 Optional: Click **Search** to display a list of configured Gateway Endpoints associated with the selected Service Domain, Layer 1 domain, and Layer 0 Domain.

6 Click **Add**.

The **Add Gateway Endpoint** Web page appears, as shown in Figure 86 "Add Gateway Endpoint Web page" (page 215).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 86
Add Gateway Endpoint Web page



7 Enter the **Endpoint name** of the gateway. The name must be alphanumeric and can be up to 30 characters in length.

For example, enter sipGWSite1.

8 Enter an endpoint description in the **Description** box. The description must be alphanumeric and can be up to 120 characters in length.

9 Check the **Trust Node:** check box.

10 Select the **Tandem gateway endpoint name** from the list, if required to indicate whether the endpoint is used for 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 Layer 0 Domain in which it exists. See "Numbering Plans inherited fields" (page 160).

11 Select an option from the **Endpoint authentication enabled** list:

- **Not configured**: If you select this option, then the gateway endpoint uses the L1 or L0 Authentication (if L1 or L0 authentication is enabled).
- **Authentication on**: If you select this option, then authentication is on for this gateway endpoint and the

Copyright © 2010 Nortel Networks. All Rights Reserved.

authentication overrides the L1 or L0 authentication (if it is enabled).

- **Authentication off**: If you select this option, then authentication is off for this gateway endpoint even if Layer 1 or Layer 0 authentication is enabled.

12 If you selected **Authentication on**, enter the **Authentication password**. The password must be alphanumeric and can be up to 24 characters in length.

13 Enter the **E.164 country code**. The code must be numeric and can be up to eight digits in length.

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

15 Enter the **E.164 international dialing access code**. The code must be numeric and can be up to eight digits in length.

16 Enter the **E.164 international dialing code length**. The code length must be numeric and must exceed the E.164 international dialing access code length.

17 Enter the **E.164 national dialing access code**. The code must be numeric and can be up to seven characters in length.

18 Enter the **E.164 national dialing code length**. The code length must be numeric and must exceed the E.164 national dialing access code length.

19 Enter the **E.164 local (subscriber) dialing access code**. The code must be numeric and can be up to eight digits in length.

20 Enter the **E.164 local (subscriber) dialing code length**. The code length must be numeric and has to exceed the E.164 local (subscriber) dialing access code length.

21 Enter the **Private L1 domain (UDP location) dialing access code**. The code must be numeric and can be up to eight digits in length.

22 Enter the **Private L1 domain (UDP location) dialing code length**. The code length must be numeric and has to exceed the Private L1 domain (UDP location) dialing access code length.

23 Enter the **Private special number 1**. The number must be numeric and can be up to 30 digits in length.

24 Enter the **Private special number 1 dialing code length**. The code length must be numeric and equal to the Private special number 1 length.

25 Enter the **Private special number 2**. The number must be numeric and can be up to 30 digits in length

Copyright © 2010 Nortel Networks. All Rights Reserved.

26 Enter the **Private special number 2 dialing code length**. The code length must be numeric and equal to the Private special number 2 length.

> ***Note:*** Avoid information conflict when you configure the access codes. This is to support unqualified DN-based URIs by pretranslating to find the appropriate phone context.

27 Select **IP Version 4** from the **Static endpoint address type** list **OR** select **IP Version 6** from the **Static endpoint address type** list for IPv6 settings.

28 Enter the **Static endpoint address**.

This is the Node IP address of the Signaling Server. If you use a third-party gateway, then use the IP address of the gateway.

29 Select the H.323 support setting from the **H.323 Support** list:

- H.323 not supported
- RAS H.323 endpoint
- Not RAS H.323 endpoint.

> ***Note 1:*** If you configure an H.323 Gateway Endpoint 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 appears 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 27 “Viewing Gateway Endpoint Dynamic Registration Information” (page 220).

30 Configure SIP support.

1. Select an option from the **SIP Support** list. The three options are SIP not supported, Static SIP endpoint, and Dynamic SIP endpoint.
2. If SIP support is enabled, select the **SIP Mode**. The two options are Proxy Mode and Redirect Mode.
3. If SIP support is enabled, select the transport protocol:

   — If SIP TCP is supported, perform the following steps:

Copyright © 2010 Nortel Networks. All Rights Reserved.

– Select the **SIP TCP transport enabled** check box.

– Enter the **SIP TCP 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 5060.

— If SIP UDP is supported, perform the following steps:

– Select the **SIP UDP transport enabled** check box.

– Enter the **SIP UDP 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 5060.

— If SIP TLS is supported, perform the following steps:

– Select the **SIP TLS transport enabled** check box.

– Enter the **SIP TLS 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 5061.

Note: If you configure a SIP Trunk Gateway Endpoint 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 appears only when NRS Manager is in Active DB view. The detailed dynamic registration information also appears only inside the Gateway Endpoint Web page. See Procedure 27 “Viewing Gateway Endpoint Dynamic Registration Information” (page 220).

31 Check the **Persistent TCP support enabled** check box.

32 If support is available for end to end security, select the**End to end security** check box.

33 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.

34 Select the Redundancy setting from the **Redundancy enabled** list:

- Not configured
- Main Office
- Redundant Office

Copyright © 2010 Nortel Networks. All Rights Reserved.

You can link geographic redundant gateways (Main Office and Redundant office endpoints).

To set the main endpoint

- Select **Main Office** from the **Redundancy enabled** list.
- Select the desired endpoint name in the **Redundant endpoint name** list.

To set the redundant endpoint

- Select **Redundant Office** from the **Redundancy enabled** list.
- Select the desired endpoint name in the **Main endpoint name** field.

If two endpoints are linked (configured properly), NRS Manager prompts you to configure routes for the redundant endpoint when you add routes to the main endpoint. This configuration provides two routes (one for the main office endpoint and one for the redundant office endpoint) at the same time with approximately configured values.

35 The **Main endpoint name** is dynamically generated based on the Gateway Endpoint configuration. The default selection is **Not configured**.

36 The **Redundant endpoint name** is dynamically generated based on the Gateway Endpoint configuration. The default selection is **Not configured**.

37 Select the SIP support type from the options **Static SIP Endpoint and Dynamic SIP Endpoint**.

The fields **VPNI, Zone,** and **User Parameter(s)** are enabled. The fields are not mandatory and are used to form the URI parameters.

38 Enter valid values for **VPNI, Zone,** and **User Parameter(s)**.

39 Click **Save**. The Endpoints Web page appears.

In the database, URI Parameters are constructed from the user defined parameters.

> **ATTENTION**
> If you enter an invalid VPNI, Zone, or User Parameter, an error appears asking you to re-enter valid values, or click the Cancel button. No error occurs if the values are NULL.

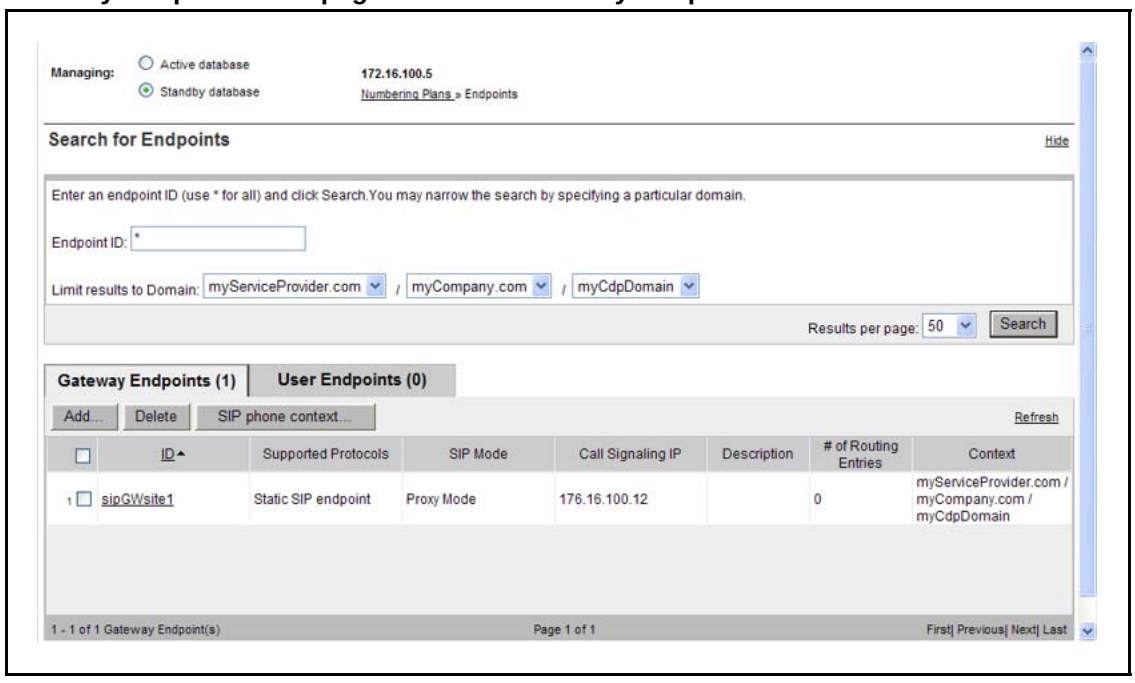
40 Click **Save**.

The standby database is updated.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The **Gateway Endpoints** Web page appears, showing the newly added sipGWSite1 endpoint. See Figure 87 "Gateway Endpoints web page for added Gateway Endpoint" (page 220).

Figure 87
Gateway Endpoints web page for added Gateway Endpoint



41 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state.

42 Test the configuration changes.

43 See Procedure 63 “Committing the database” (page 290) 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 27
Viewing Gateway Endpoint Dynamic Registration Information

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213).

Copyright © 2010 Nortel Networks. All Rights Reserved.

2 Ensure **Active database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).

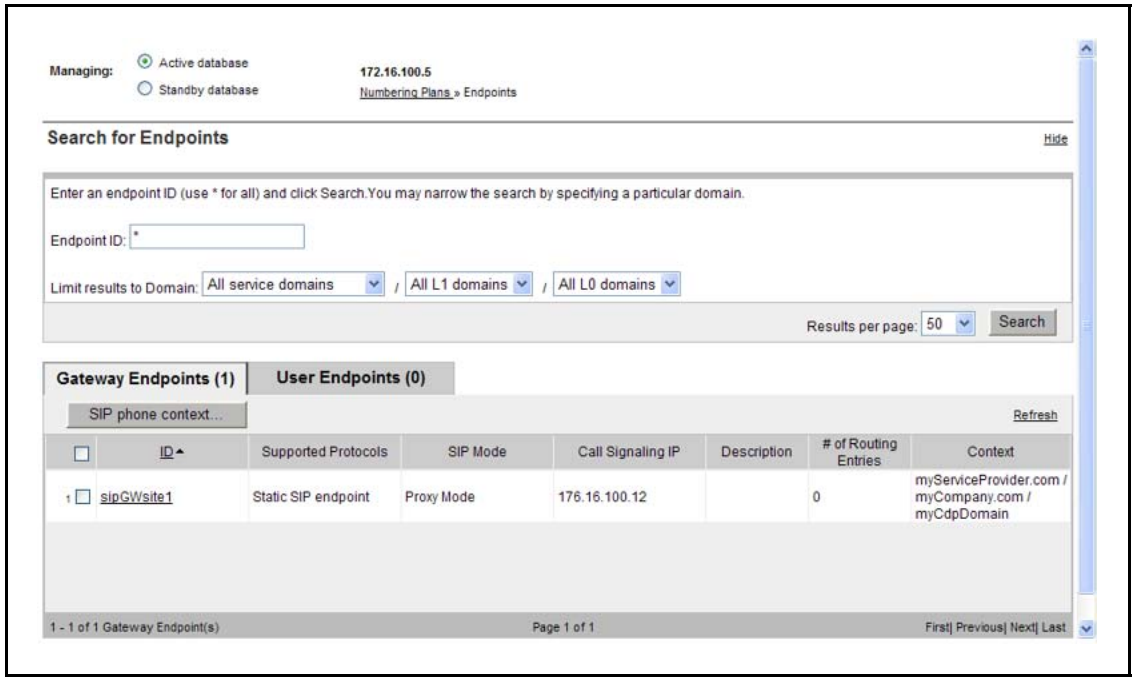
3 The **Limit results to Domain:** drop-down lists contain configured Service Domains, L1 Domains and L0 Domains. Select a Service Domain, a L1 Domain and a L0 Domain from the respective drop-down lists.

4 Click the **Gateway Endpoint** tab.

The **Endpoints** web page refreshes displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 88 "Gateway Endpoints Summary web page" (page 221).

The Gateway Endpoints can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

Figure 88
Gateway Endpoints Summary web page



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 90 "Edit Gateway Endpoint web page Active database" (page 223).

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:

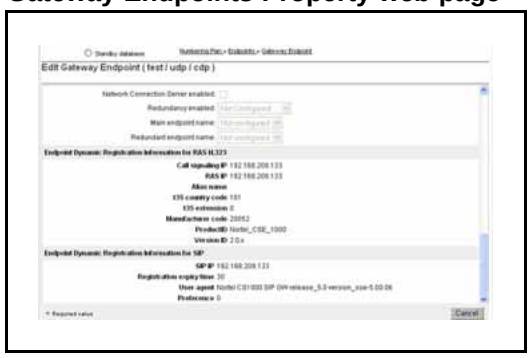
Copyright © 2010 Nortel Networks. All Rights Reserved.

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 89 "Gateway Endpoints Property web page" (page 222).

Figure 89
Gateway Endpoints Property web page



--End--

View the Gateway Endpoints

Use the following procedure to view the Gateway Endpoints.

Procedure 28
Viewing the Gateway Endpoints

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213).
2	Select the **Active** or **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page 178). 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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** tab. The **Endpoints** web page refreshes displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 85 "Gateway Endpoints pane" (page 214).

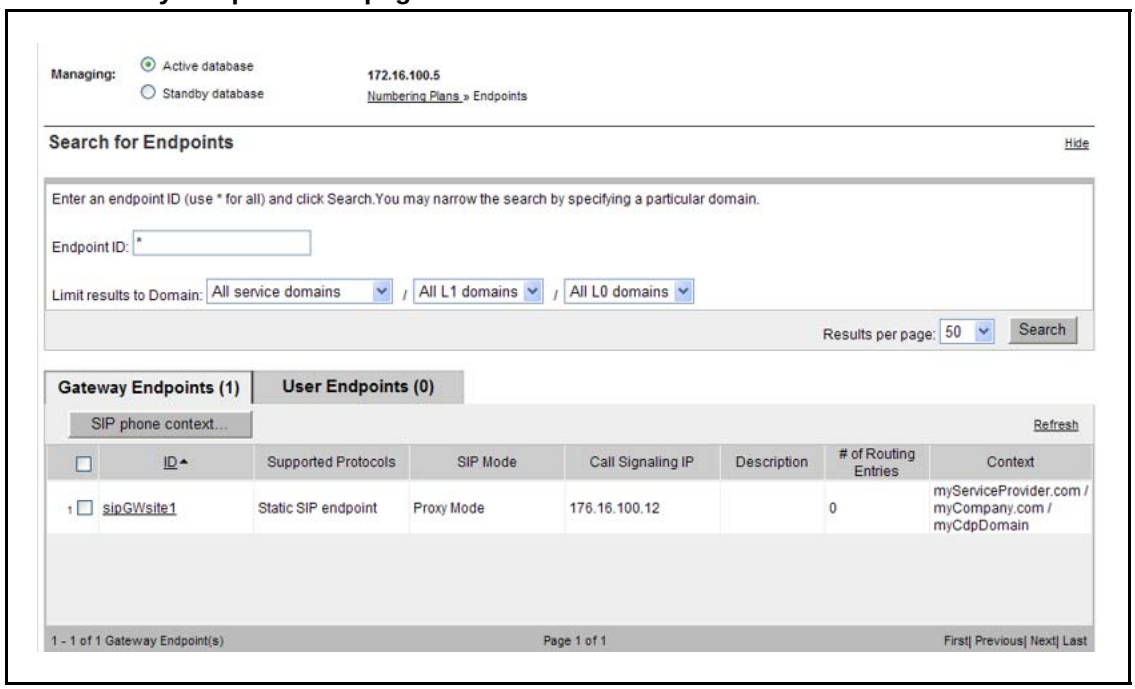
The Gateway Endpoints can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

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 90 "Edit Gateway Endpoint web page Active database" (page 223).

Note: See Procedure 29 “Editing the Gateway Endpoints” (page 224) to Edit the Gateway Endpoint.

Figure 90
Edit Gateway Endpoint web page Active database



--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Edit the Gateway Endpoints

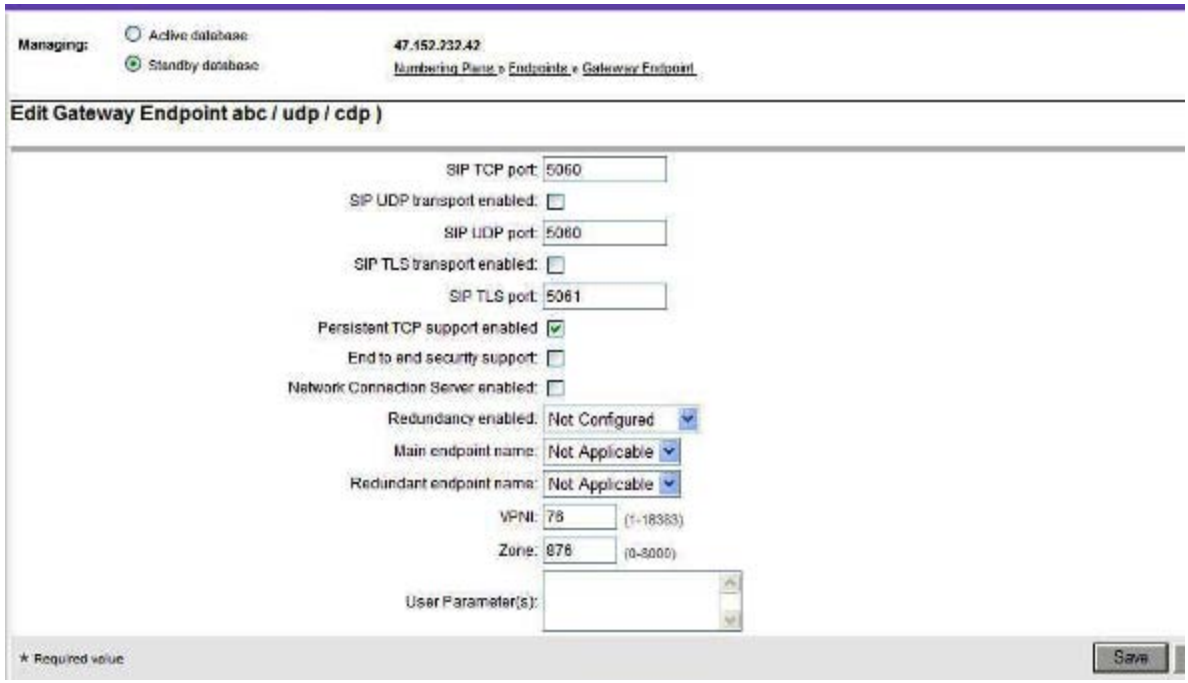
Edit the Gateway Endpoints.

Procedure 29
Editing the Gateway Endpoints

Step	Action
1	In the **NRS Manager Navigator,** select **Numbering Plans > Endpoints.** The **Endpoints** Web page appears, as shown in Figure 84 "Endpoints web page" (page 213).
2	Ensure you select **Standby database**. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
3	The **Limit results to Domain:** lists contain configured Service Domains, Layer 1 Domains and Layer 0 Domains. Select a Service Domain, a Layer 1 Domain and a Layer 0 Domain from the respective lists.
4	Click the **Gateway Endpoint** tab. The **Endpoints** Web page displays a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 85 "Gateway Endpoints pane" (page 214). You can sort the Gateway Endpoints in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .
5	Click a **link** in the **ID** column of the Endpoints pane. The **Edit Gateway Endpoint** Web page displays the configured values for the selected Gateway Endpoint, as shown in Figure 91 "Edit Gateway Endpoint web page" (page 225).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 91
Edit Gateway Endpoint web page



Note: A Gateway Endpoint can inherit configuration parameters from the Layer 0 Domain in which it exists. See "Numbering Plans inherited fields" (page 160).

6 Modify the fields of the **Edit Gateway Endpoint** Web page as appropriate. See Procedure 26 "Adding a Gateway Endpoint" (page 213).

7 Click **Save** .

The standby database is updated. The **Endpoints** Web page displays a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 85 "Gateway Endpoints pane" (page 214).

8 See Procedure 60 "Cutting over the database" (page 288) to place the database in a Switched Over state.

9 Test the configuration changes.

10 See Procedure 63 "Committing the database" (page 290) to update the database with the configuration changes.

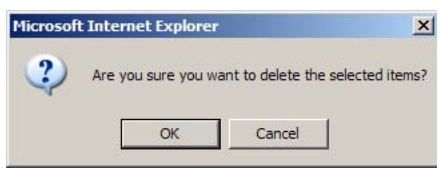
--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Delete the Gateway Endpoints

Use the following procedure to delete the Gateway Endpoints.

Procedure 30
Deleting the Gateway Endpoints

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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** tab. The **Endpoints** web page opens displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 85 "Gateway Endpoints pane" (page 214). The Gateway Endpoints can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .
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 92 "Confirmation Box" (page 226). **Figure 92** **Confirmation Box** 
7	Click **OK**. The standby database is updated. The **Endpoints** web page refreshes displaying a list of configured Gateway

Copyright © 2010 Nortel Networks. All Rights Reserved.

Endpoints in the Endpoints pane, as shown in Figure 85 "Gateway Endpoints pane" (page 214).

> ***Note:*** The standby database is updated only for Gateway Endpoints that do not have routing entries or default routes. If a Gateway Endpoint has routing entries or default routes they have to be deleted before the Gateway Endpoint can be deleted.

8 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state.

9 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Manage Post-routing SIP URI Modification

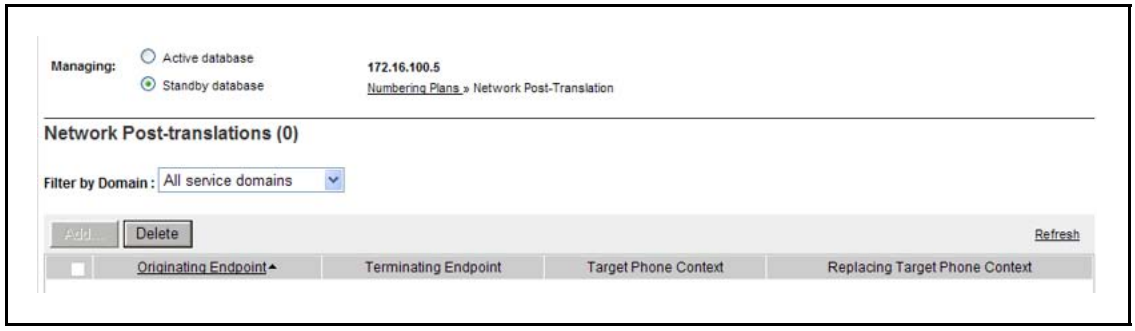
Add Post-routing SIP URI Modification

Use the following procedure to add Post-routing SIP URI Modification.

Procedure 31
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 appears as shown in Figure 93 "Network Post-translations web page" (page 227).

Figure 93
Network Post-translations web page



2 Ensure you select **Standby database**. See Procedure 9 “Switching between the Active and Standby databases” (page 178).

3 Select a **Service domain** from the **Filter by Domain:** list.

4 Click **Add**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The **Add Network Post Translations** Web page appears as shown in Figure 94 "Add Network Post Translations web page" (page 228).

Figure 94
Add Network Post Translations web page

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 remove by** in the text box. The parameter must be numeric and ***can not*** exceed the value of the **Originating routing string length**.

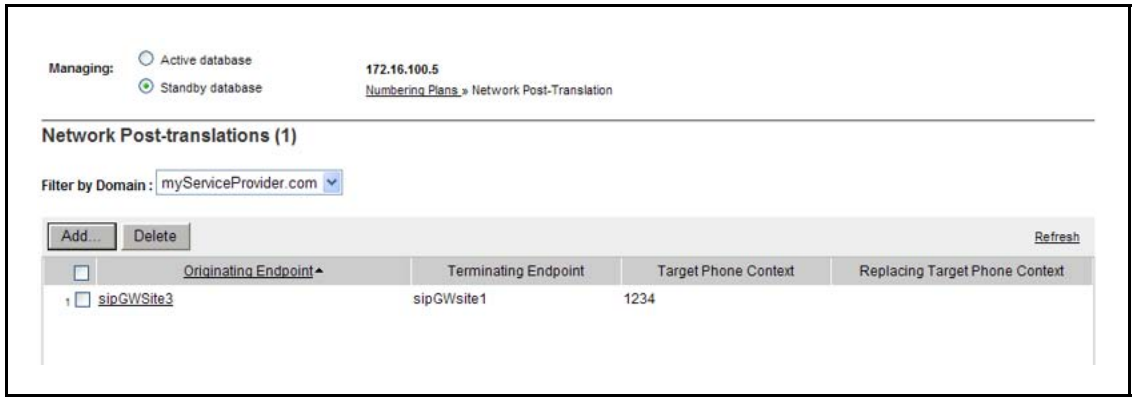
12 Enter a **Adding prefix to the routing digits with** in the text box. The parameter must be numeric and can be up to 64 digits in length. The parameter ***can not*** contain a leading + character.

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 95 "Added Network Post-translations web page" (page 229).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 95
Added Network Post-translations web page



14 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

15 Test the configuration changes.

16 See Procedure 63 “Committing the database” (page 290) 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 32
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 appears as shown in Figure 93 "Network Post-translations web page" (page 227).
2	Select the **Active** or **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page 178). 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 93 "Network Post-translations web page" (page 227).
3	Select a **Service domain** from the **Filter by Domain:** drop-down list.
4	Click the **Refresh** link.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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" (page 158) .

5 Click a **link** in the **Originating Endpoint** column of the **Network Post-translations** web page.

The **Edit Network Post Translations** Web page appears as shown in Figure 96 "Edit Network Post Translations web page" (page 231), 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 33
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 appears as shown in Figure 93 "Network Post-translations web page" (page 227).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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" (page 158) .
5	Click a **link** in the **Originating Endpoint** column of the *Network Post-translations* web page. The **Edit Network Post Translations** Web page appears as shown in Figure 96 "Edit Network Post Translations web page" (page 231), and displays the configured data for the selected Network Post Translation.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 96
Edit Network Post Translations web page

6 Modify the fields of the**Edit Network Post Translations** web page as appropriate. See Procedure 31 “Adding Post-routing SIP URI Modification” (page 227).

7 Click the **Save** button. The standby database is updated.

The **Network Post-translations** Web page appears as shown in Figure 93 "Network Post-translations web page" (page 227).

8 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

9 Test the configuration changes.

10 See Procedure 63 “Committing the database” (page 290) 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 34
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 appears as shown in Figure 93 "Network Post-translations web page" (page 227).

Copyright © 2010 Nortel Networks. All Rights Reserved.

2 Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).

3 Select a **Service domain** from the **Filter by Domain:** drop-down list.

4 Click the Refresh link.

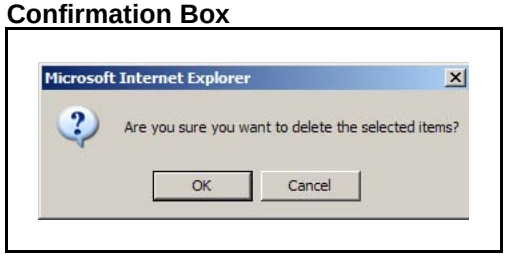
The **Network Post-translations** web page refreshes displaying a list of **Originating Endpoints**.

The Originating Endpoints can be sorted in ascending or descending alphabetical order. See "Sort web page by Originating Endpoint" (page 158) .

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 97 "Confirmation Box" (page 232), requesting confirmation before deleting the selected **Network Post Translation**.

Figure 97
Confirmation Box



7 Click **OK**. The standby database is updated.

The **Network Post-translations** Web page appears as shown in Figure 93 "Network Post-translations web page" (page 227).

8 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

9 Test the configuration changes.

10 See Procedure 63 “Committing the database” (page 290) 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. In Release 7.0, 5000 Gateway Endpoints / User Endpoints will be supported.

Copyright © 2010 Nortel Networks. All Rights Reserved.

To add a User Endpoint, see Procedure 35 “Adding a User Endpoint” (page 233).

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 10 “Adding a Service Domain” (page 180)
- Procedure 14 “Adding an L1 Domain” (page 186)
- Procedure 18 “Adding an L0 Domain (CDP)” (page 195)

Add a User Endpoint (SIP Phone)

Use the following procedure to add a User Endpoint.

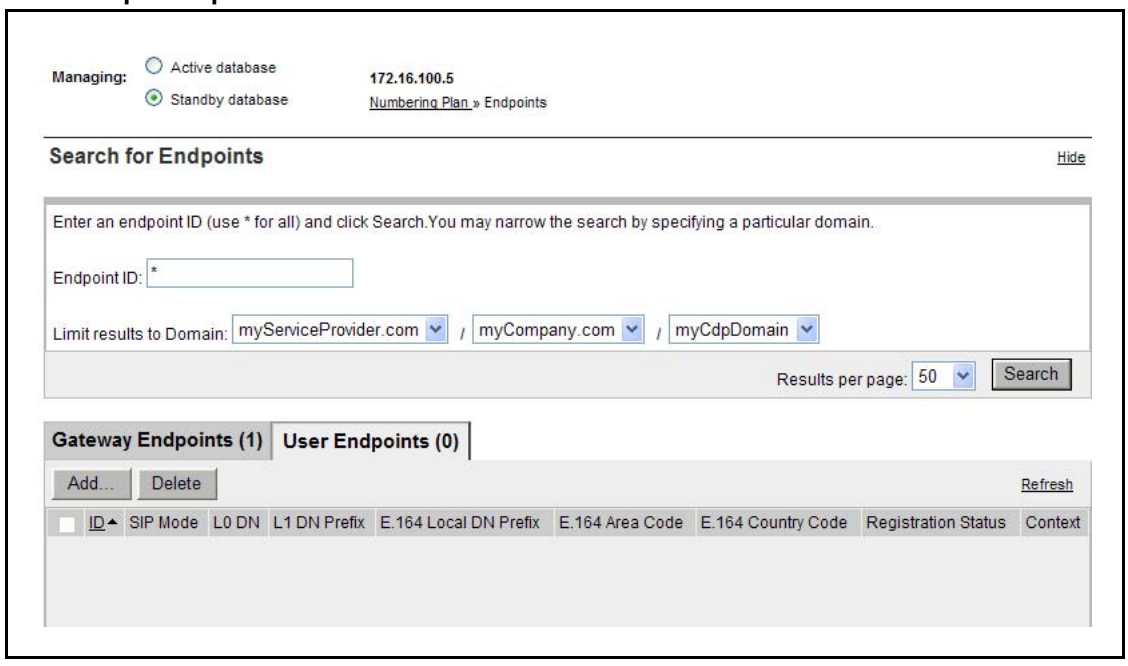
Procedure 35
Adding a User Endpoint

Step	Action
1	In the **NRS Manager Navigator,** select **Numbering Plans > Endpoints.** The **Endpoints** Web page appears, as shown in Figure 84 "Endpoints web page" (page 213).
2	Ensure you select **Standby database**. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
3	The **Limit results to Domain:** lists contain configured Service Domains, Layer 1 Domains and Layer 0 Domains. Select a Service Domain, a Layer 1 Domain and a Layer 0 Domain from the respective lists.

Copyright © 2010 Nortel Networks. All Rights Reserved.

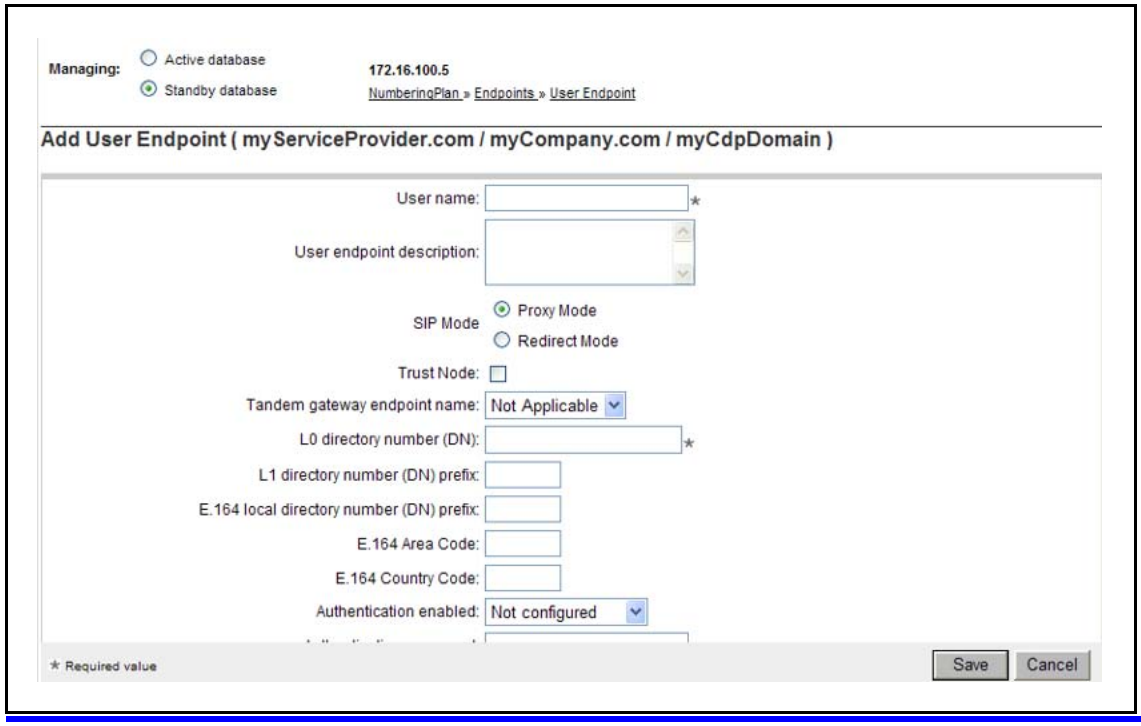
4 Click the **User Endpoints** tab. The **Endpoints** Web page displays a list of configured User Endpoints in the Endpoints pane, as shown in Figure 98 "User Endpoints pane" (page 234).

Figure 98
User Endpoints pane



5 Click **Add**. The **Add User Endpoint** Web page appears, as shown in Figure 99 "Add User Endpoint web page" (page 234).

Figure 99
Add User Endpoint web page



Copyright © 2010 Nortel Networks. All Rights Reserved.

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 Select the **SIP Mode**. The two options are Proxy Mode and Redirect Mode.

9 Check the **Trust Node** check box.

10 Choose a **Tandem gateway endpoint name** from the drop-down list.

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.

11 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.

12 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

13 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

14 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

15 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

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

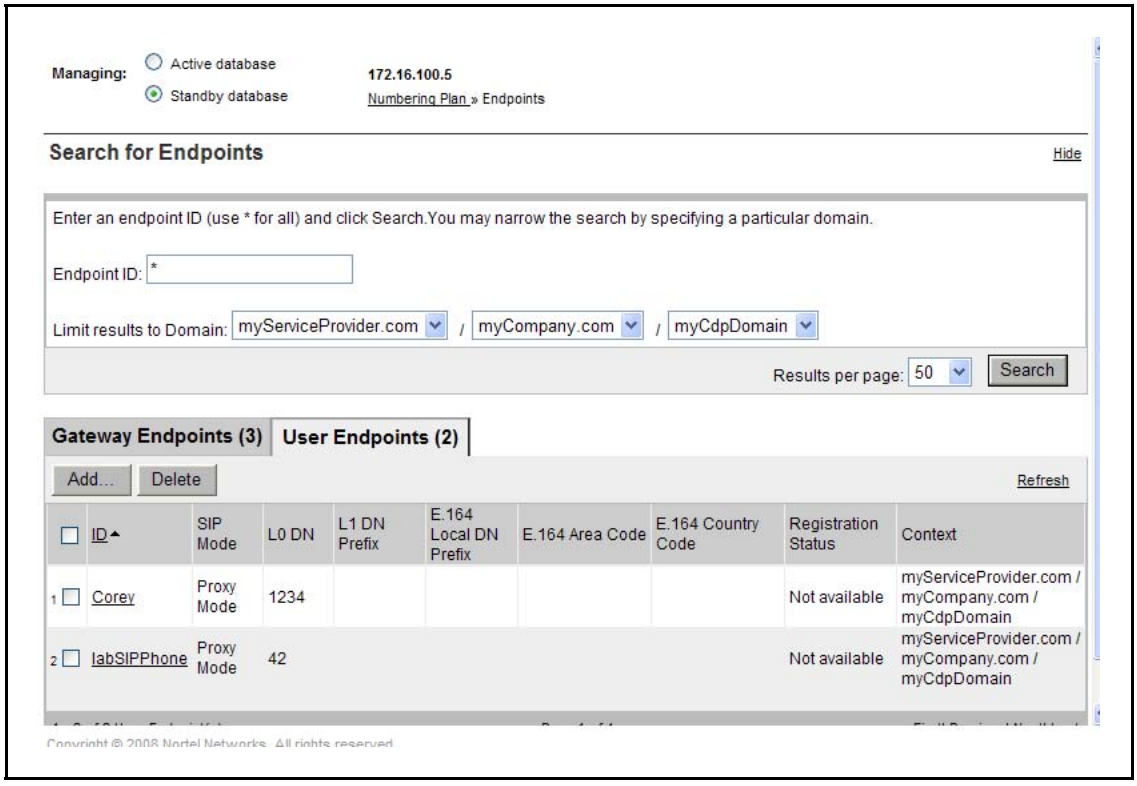
17 If authentication is enabled in , then enter the **Authentication password**. The password must be alphanumeric and can be up to 24 characters in length.

18 Click the **Save** button. The standby database is updated.

The **Endpoints** Web page displays the newly added User Endpoint in the **User Endpoints** pane. See Figure 100 "Added User Endpoints" (page 237).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 100
Added User Endpoints



19 If required, click **Add...** to add additional User Endpoints.

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 36 “Viewing User Endpoint Dynamic Registration Information” (page 238).

20 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

21 Test the configuration changes.

Copyright © 2010 Nortel Networks. All Rights Reserved.

22 See Procedure 63 “Committing the database” (page 290) 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 36
Viewing User Endpoint Dynamic Registration Information

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints**. The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213).
2	Ensure **Active database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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** tab. The **Endpoints** web page refreshes displaying a list of configured User Endpoints in the Endpoints pane, as shown in . The User Endpoints can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

Figure 101
User Endpoints Summary web page

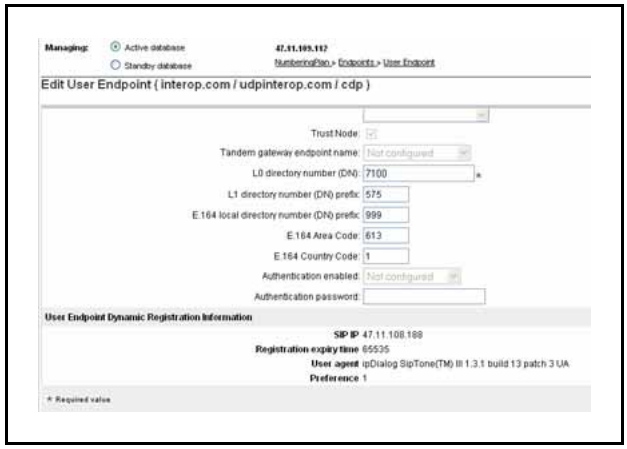
5 Click a **link** in the **ID** column of the **Endpoints** pane.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The **Edit User Endpoint** web page opens and displays the configured data for the selected User Endpoint, as shown in Figure 102 "User Endpoints Property web page" (page 239).

> ***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 102
User Endpoints Property web page



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 37
Viewing the User Endpoints

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints**. The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213).
2	Select the **Active** or **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page 178). 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

between Active and Standby database views at any time. The **Endpoints** web page refreshes.

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** tab. The **Endpoints** web page refreshes displaying a list of configured User Endpoints in the Endpoints pane, as shown in Figure 98 "User Endpoints pane" (page 234). The User Endpoints can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

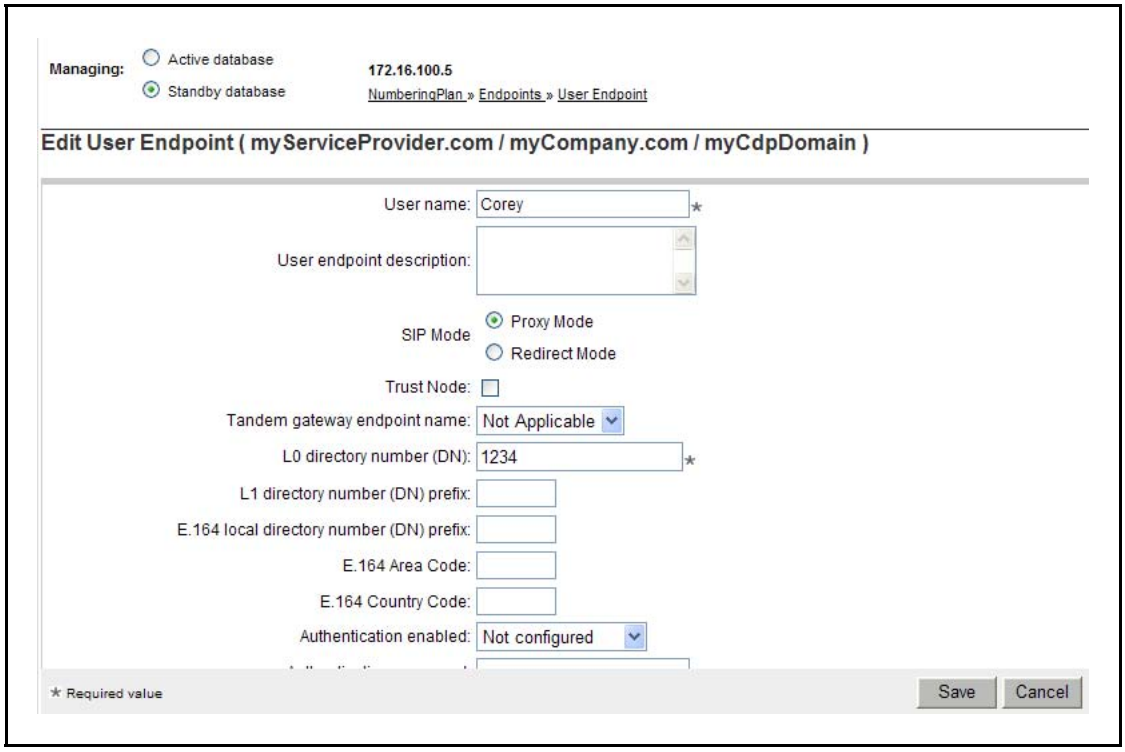
5 Click a **link** in the **ID** column of the **Endpoints** pane.

The **Edit User Endpoint** web page opens and displays the configured data for the selected User Endpoint, as shown in Figure 103 "Edit User Endpoint Web page Active database" (page 241).

Note: See Procedure 38 “Editing a User Endpoint” (page 241) to Edit the User Endpoint.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 103
Edit User Endpoint Web page Active database



--End--

Edit a User Endpoint

Use the following procedure to edit a User Endpoint.

Procedure 38
Editing a User Endpoint

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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.

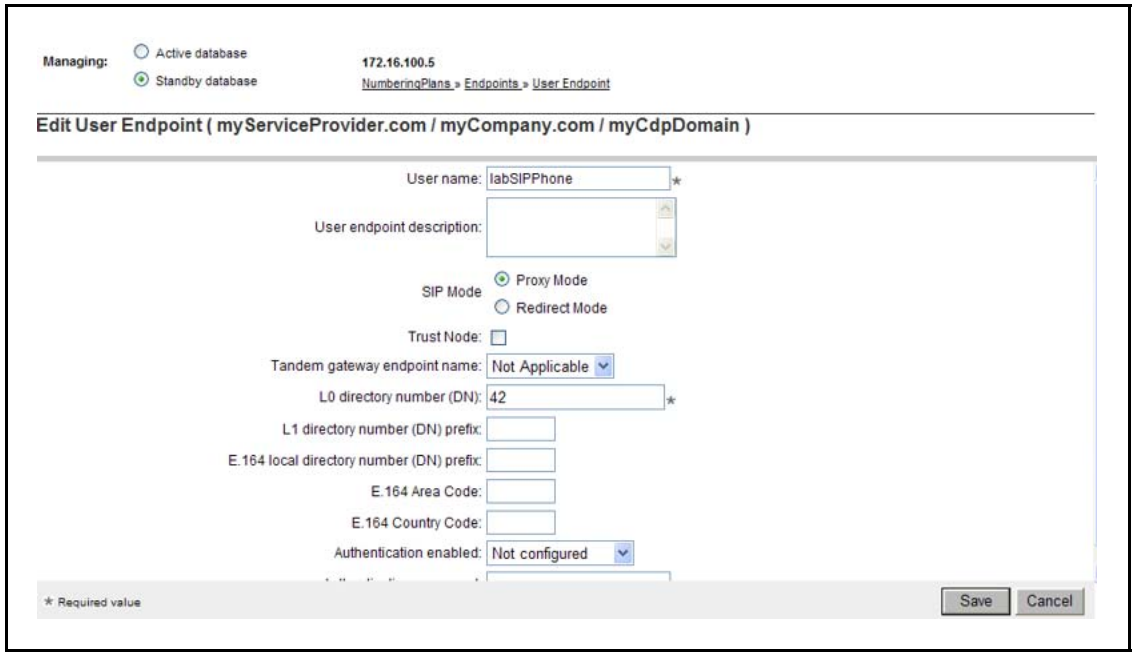
Copyright © 2010 Nortel Networks. All Rights Reserved.

4 Click the **User Endpoints** tab. The **Endpoints** web page opens displaying a list of configured User Endpoints in the Endpoints pane, as shown in Figure 98 "User Endpoints pane" (page 234).

The User Endpoints can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .

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 104 "Edit User Endpoint web page" (page 242).

Figure 104
Edit User Endpoint web page



6 Modify the fields of the **Edit User Endpoint** web page as appropriate. See Procedure 35 “Adding a User Endpoint” (page 233).

7 Click the **Save** button. The standby database is updated. The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213)

8 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

9 Test the configuration changes.

10 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

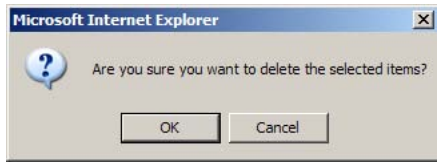
--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Delete a User Endpoint

Use the following procedure to delete a User Endpoint.

Procedure 39
Deleting a User Endpoint

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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** tab. The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213) The User Endpoints can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .
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 105 "Confirmation Box" (page 243), requesting confirmation before deleting the selected **User Endpoint**. **Figure 105** **Confirmation Box** 
7	Click **OK**. The standby database is updated. The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213).
8	See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state.
9	See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

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. To open the SIP Phone Context web page select **Tools > SIP Phone Context** in the NRS Manager Navigator, or follow the steps in Procedure 40 “Mapping the SIP Phone Context” (page 244).

Procedure 40
Mapping the SIP Phone Context

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Endpoints.** The **Endpoints** Web page appears as shown in Figure 84 "Endpoints web page" (page 213).
2	Select **Standby database** or **Active database**. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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** tab. The **Endpoints** web page refreshes displaying a list of configured Gateway Endpoints in the Endpoints pane, as shown in Figure 85 "Gateway Endpoints pane" (page 214). The Gateway Endpoints can be sorted in ascending or descending alphabetical order. See "Sort web page by ID" (page 157) .
5	Select a check box beside a **link** in the **ID** column of the Endpoints pane.
6	Click the **SIP phone context** tab. The **SIP Phone Context** Web page appears as shown in Figure 106 "SIP Phone Context web page" (page 245).

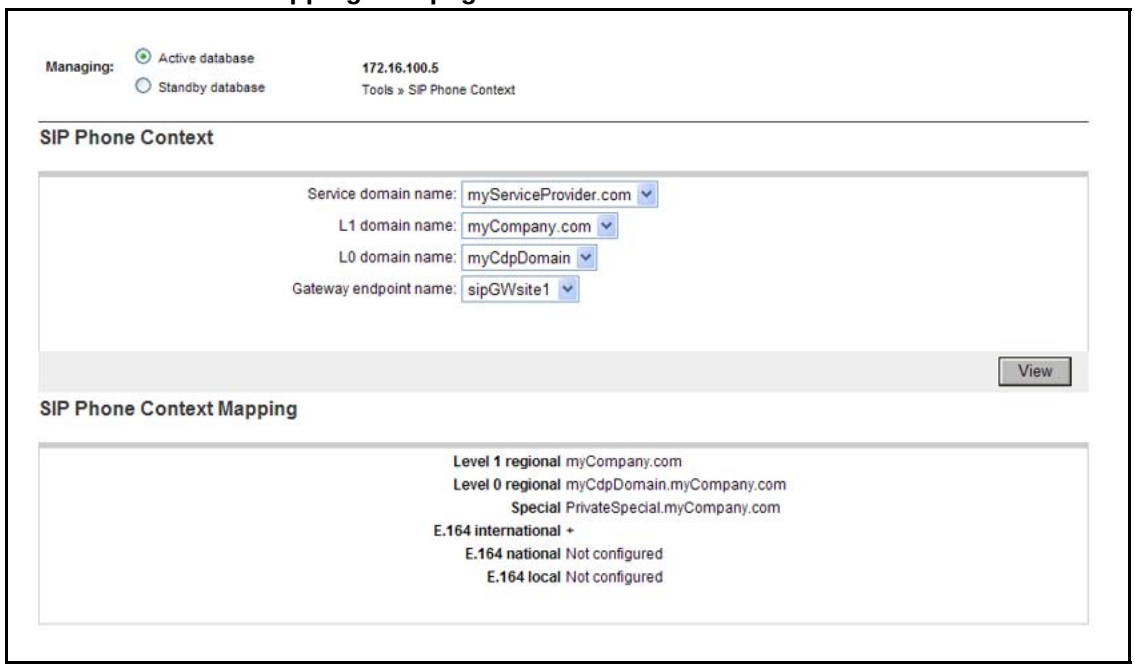
Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 106
SIP Phone Context web page

7 Click the **View** tab.

The SIP Phone Context web page expands to display the **SIP Phone Context Mapping** pane, as shown in Figure 107 "SIP Phone Context Mapping web page" (page 245).

Figure 107
SIP Phone Context Mapping web page



--End--

Manage a Routing Entry

Add a Routing Entry

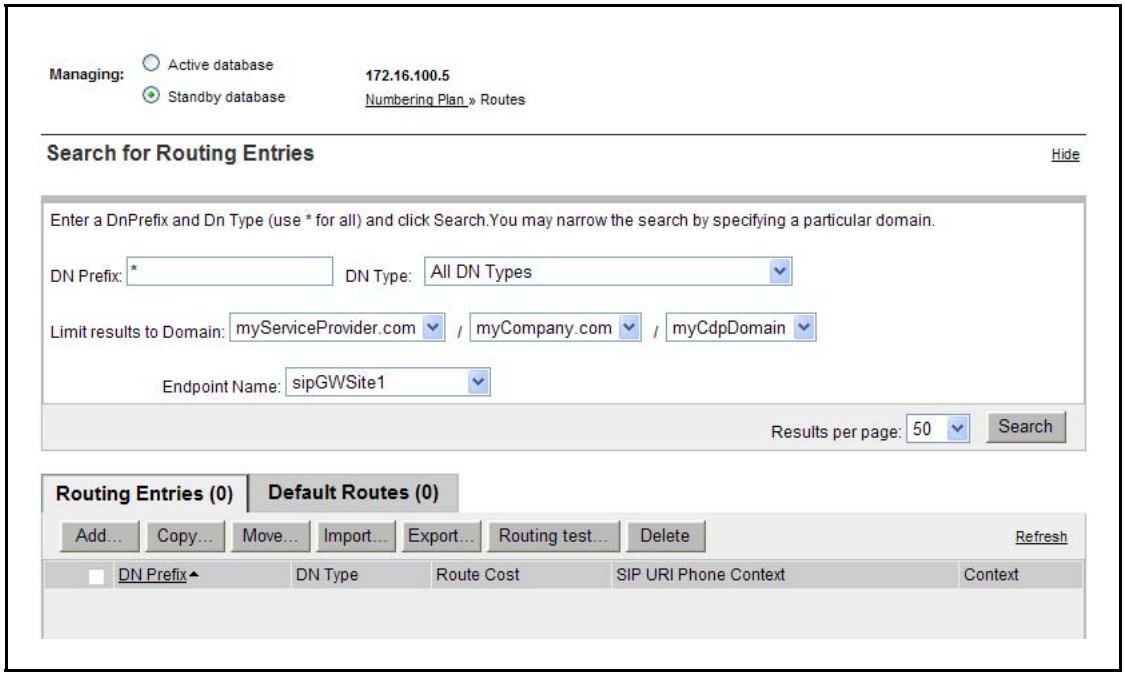
Use the following procedure to add a Routing Entry.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 41
Adding a Routing Entry

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).

Figure 108
Routes web page



2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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** tab.
6	Click the **Add** button. The **Add Routing Entry** Web page appears as shown in Figure 109 "Add Routing Entry web page" (page 247).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 109
Add Routing Entry web page

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 1-100 for a route under H323 or SIP Endpoints if it need to be considered for Call routing . Route cost in the range 1-255 is considered for Geographical Redundancy.

You can configure a maximum of eight Gateway Endpoints configured with the same DN type, DN prefix, and route cost.

The Route Cost is used to define least-cost routing. Higher numbers indicate higher costs.

The error message "**Duplicate Entries within the same Gateway Endpoint are not allowed**" is displayed if a new routing entry is added which has the same DN Type and DN Prefix as another routing entry that is already present under the same Gateway Endpoint.

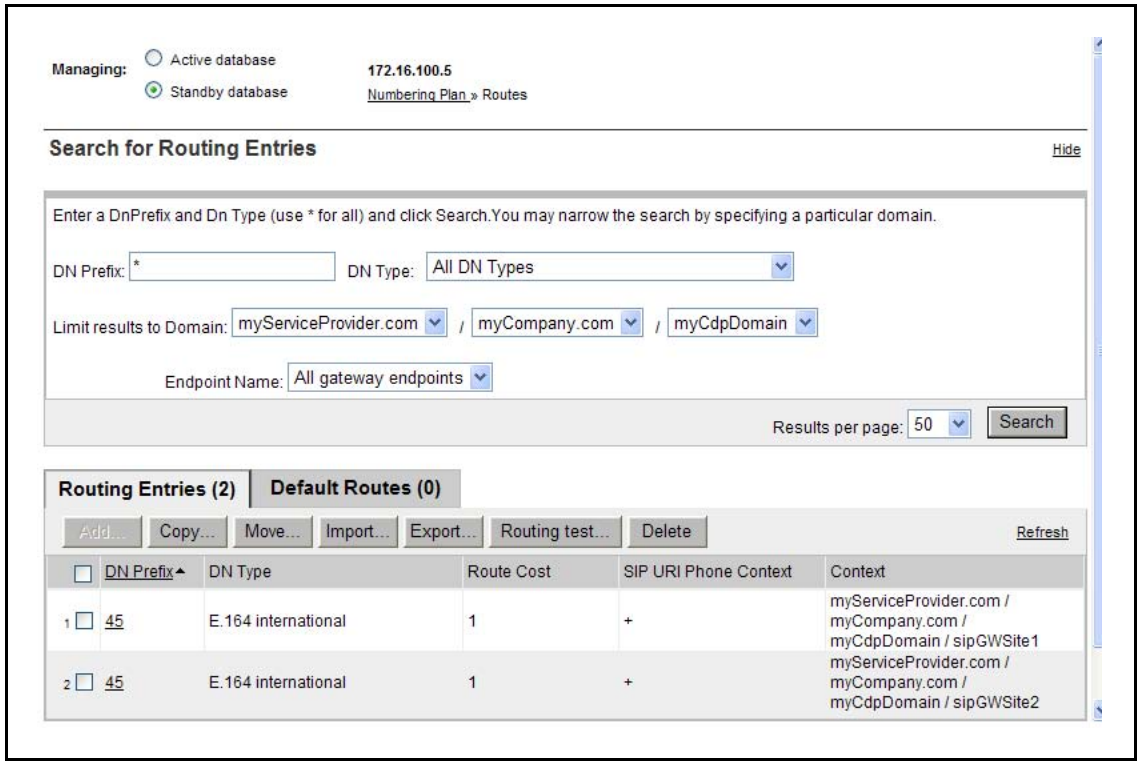
10 Click **Save**.

The standby database is updated.

The **Routes** Web page displays the newly added routing entry in the Routing Entries pane, as shown in Figure 110 "Added Routing Entry" (page 248).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 110
Added Routing Entry



11 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

12 Test the configuration changes.

13 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

View the Routing Entries

Use the following procedure to view the Routing Entries.

Procedure 42
Viewing the Routing Entries

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Select the **Active** or **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page

Copyright © 2010 Nortel Networks. All Rights Reserved.

178). 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** tab.

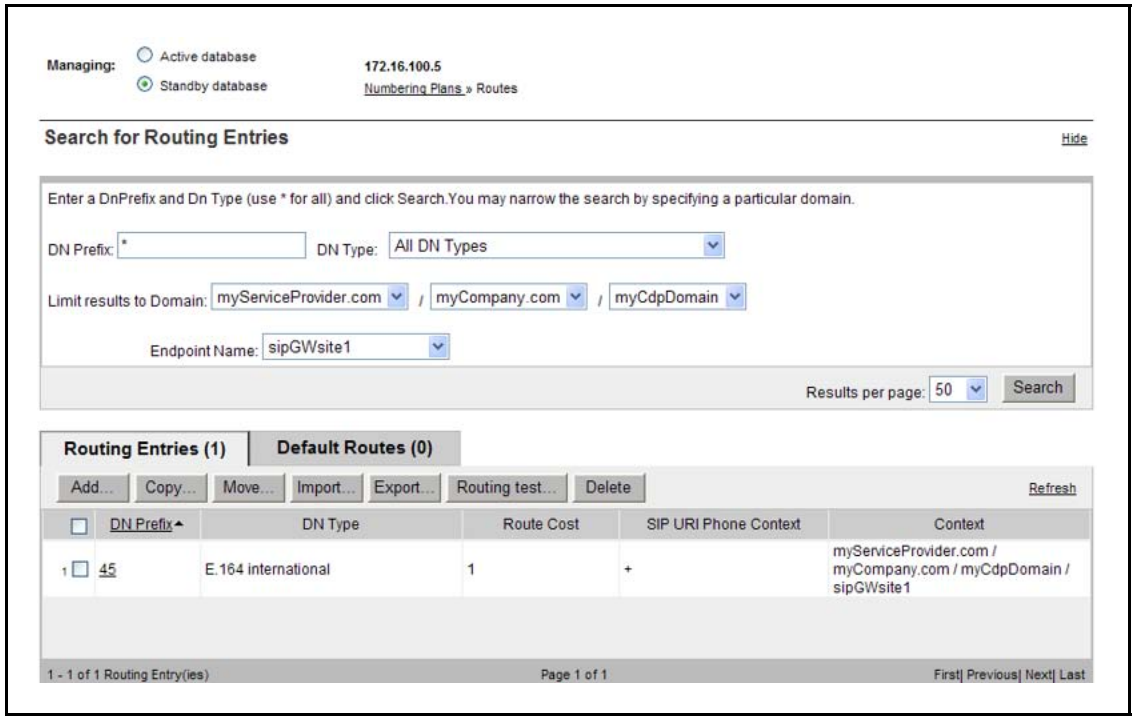
8 Click **Search**.

The web page refreshes to display a list of configured Routing Entries, as shown in Figure 111 "Search for Routing Entries web page" (page 250).

The Routing Entries can be sorted in ascending or descending numerical order. See "Sort web page by DN Prefix" (page 157) .

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 111
Search for Routing Entries web page



--End--

Edit a Routing Entry

Use the following procedure to edit a Routing Entry.

Procedure 43
Editing a Routing Entry

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

5 Click the **Routing Entries** tab.

6 Click **Search**.

The web page refreshes to display a list of configured Routing Entries, as shown in Figure 111 "Search for Routing Entries web page" (page 250).

The Routing Entries can be sorted in ascending or descending numerical order. See "Sort web page by DN Prefix" (page 157) .

7 Click a **link** in the **DN Prefix** column of the Routing Entries pane.

The **Edit Routing Entry** Web page appears as shown in Figure 112 "Edit Routing Entry web page" (page 251).

Figure 112
Edit Routing Entry web page

8 Modify the **DN Type**, **DN Prefix** or **Route Cost**.

9 Click the **Save** button. The standby database is updated. The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).

10 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

11 Test the configuration changes.

12 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Delete a Routing Entry

Use the following procedure to delete a Routing Entry.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 44
Deleting a Routing Entry

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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** tab.
6	Click **Search**. The web page refreshes to display a list of configured Routing Entries, as shown in Figure 111 "Search for Routing Entries web page" (page 250). The Routing Entries can be sorted in ascending or descending numerical order. See "Sort web page by DN Prefix" (page 157) .
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 113 "Confirmation Box" (page 252), requesting confirmation before deleting the selected **Routing Entry**. **Figure 113** **Confirmation Box**
9	Click **OK**. The standby database is updated. The **Routes** web page refreshes, as shown in Figure 108 "Routes web page" (page 246).
10	See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state.

Copyright © 2010 Nortel Networks. All Rights Reserved.

11	See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Copy a Routing Entry

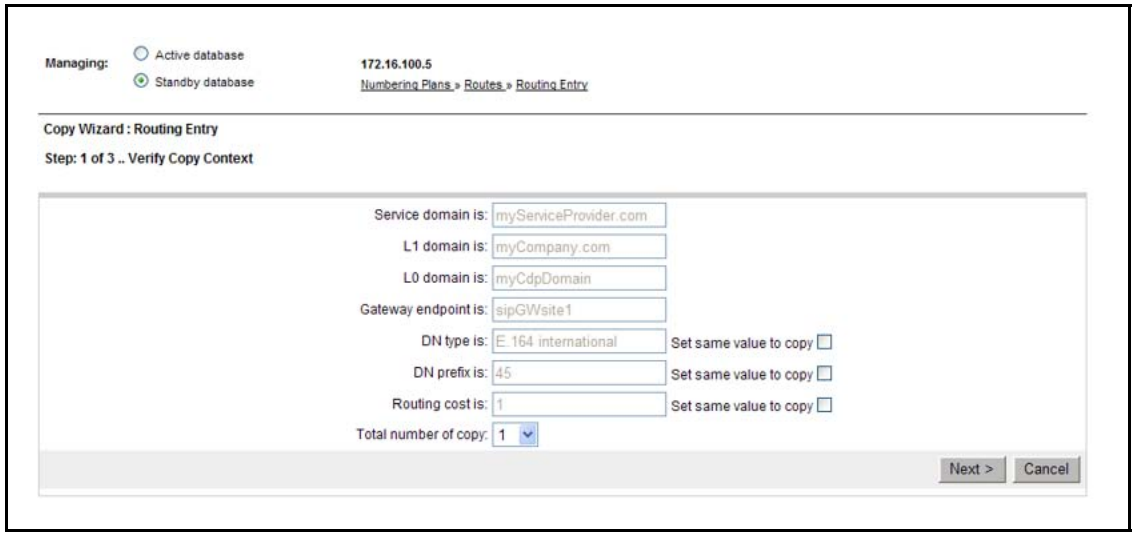
Use the following procedure to copy a Routing Entry.

Procedure 45
Copying a Routing Entry

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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** tab.
6	Click **Search**. The web page refreshes to display a list of configured Routing Entries, as shown in Figure 111 "Search for Routing Entries web page" (page 250). The Routing Entries can be sorted in ascending or descending numerical order. See "Sort web page by DN Prefix" (page 157) .
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 appears as shown in Figure 114 "Copy Wizard: Routing Entry Verify Copy Context web page" (page 254).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 114
Copy Wizard: Routing Entry Verify Copy Context web page

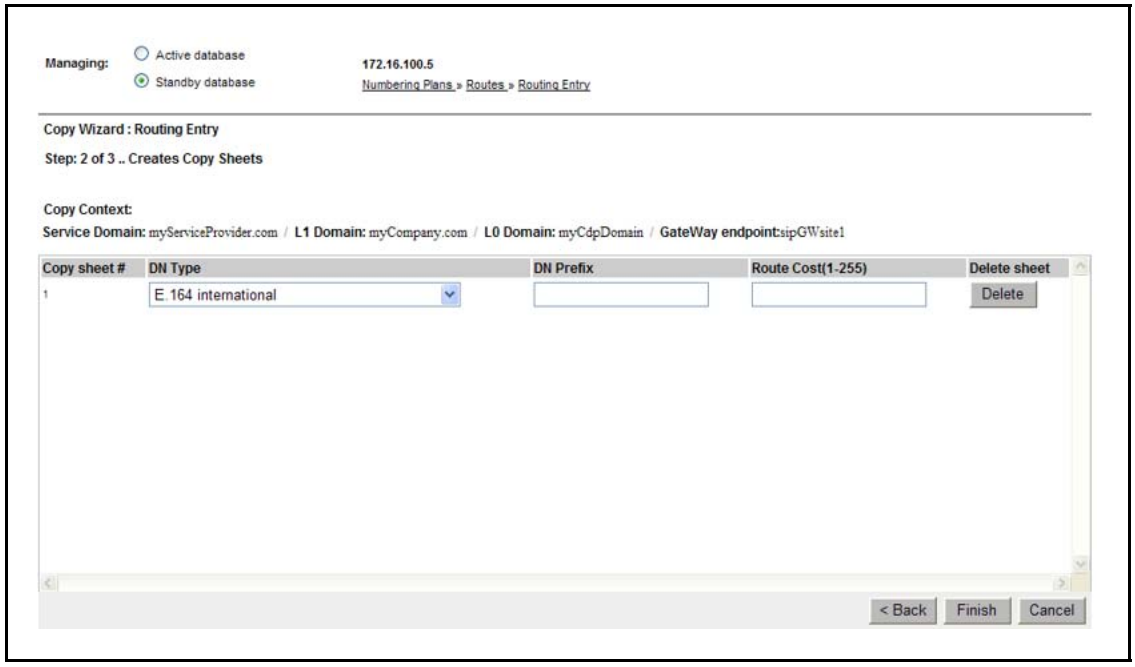


9 Select **Total number of copy** from the drop down list.

10 Click **Next**.

The **Copy Wizard: Routing Entry Creates Copy Sheets** Web page appears as shown in Figure 115 "Copy Wizard: Routing Entry Creates Copy Sheets web page" (page 254).

Figure 115
Copy Wizard: Routing Entry Creates Copy Sheets web page



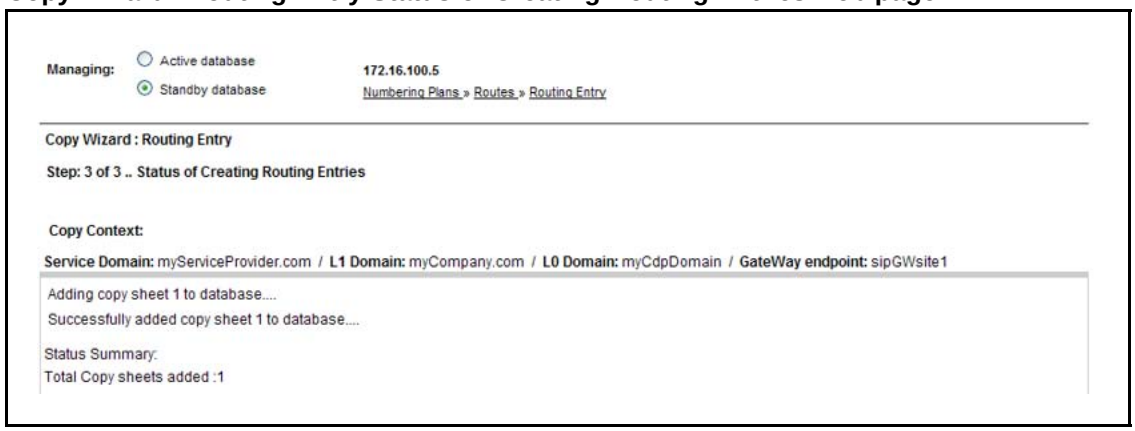
11 Modify the copy sheet(s).

12 Click **Finish**. The standby database is updated.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The **Copy Wizard: Routing Entry Status of Creating Routing Entries** Web page appears as shown in Figure 116 "Copy Wizard: Routing Entry Status of Creating Routing Entries web page" (page 255).

Figure 116
Copy Wizard: Routing Entry Status of Creating Routing Entries web page



13 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

14 Test the configuration changes.

15 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Move Routing Entries

Use the following procedure to move a Routing Entries.

Procedure 46
Moving Routing Entries

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

4 Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.

5 Click the **Routing Entries** tab.

6 Click **Search**.

The web page refreshes to display a list of configured Routing Entries, as shown in Figure 111 "Search for Routing Entries web page" (page 250).

The Routing Entries can be sorted in ascending or descending numerical order. See "Sort web page by DN Prefix" (page 157) .

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 appears as shown in Figure 117 "Moving Wizard: Routing Entry Verify Moving Context web page" (page 256).

Figure 117
Moving Wizard: Routing Entry Verify Moving Context web page

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 appears as shown in Figure 118 "Moving Wizard: Routing Entry Creates Moving Sheets web page" (page 257).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 118
Moving Wizard: Routing Entry Creates Moving Sheets web page

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 appears as shown in Figure 119 "Moving Wizard: Routing Entry Status of Moving Routing Entries web page" (page 257).

Figure 119
Moving Wizard: Routing Entry Status of Moving Routing Entries web page

13 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

14 Test the configuration changes.

Copyright © 2010 Nortel Networks. All Rights Reserved.

15	See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Search Routing Entries

Use the following procedure to search Routing Entries by DN Prefix.

Procedure 47
Searching Routing Entries

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Select **Standby database** or **Active database**. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
3	Select the **Routing Entries** tab.
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 111 "Search for Routing Entries web page" (page 250). The Routing Entries can be sorted in ascending or descending numerical order. See "Sort web page by DN Prefix" (page 157) .

--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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Add a Default Route

Use the following procedure to add a Default Route.

Procedure 48
Adding a Default Route

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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** tab. The **Routes** web page refreshes to display a list of configured default routes,
6	Click the **Add** button. The **Add Default Route** Web page appears as shown in Figure 120 "Add Default route web page" (page 259).

Figure 120
Add Default route web page

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

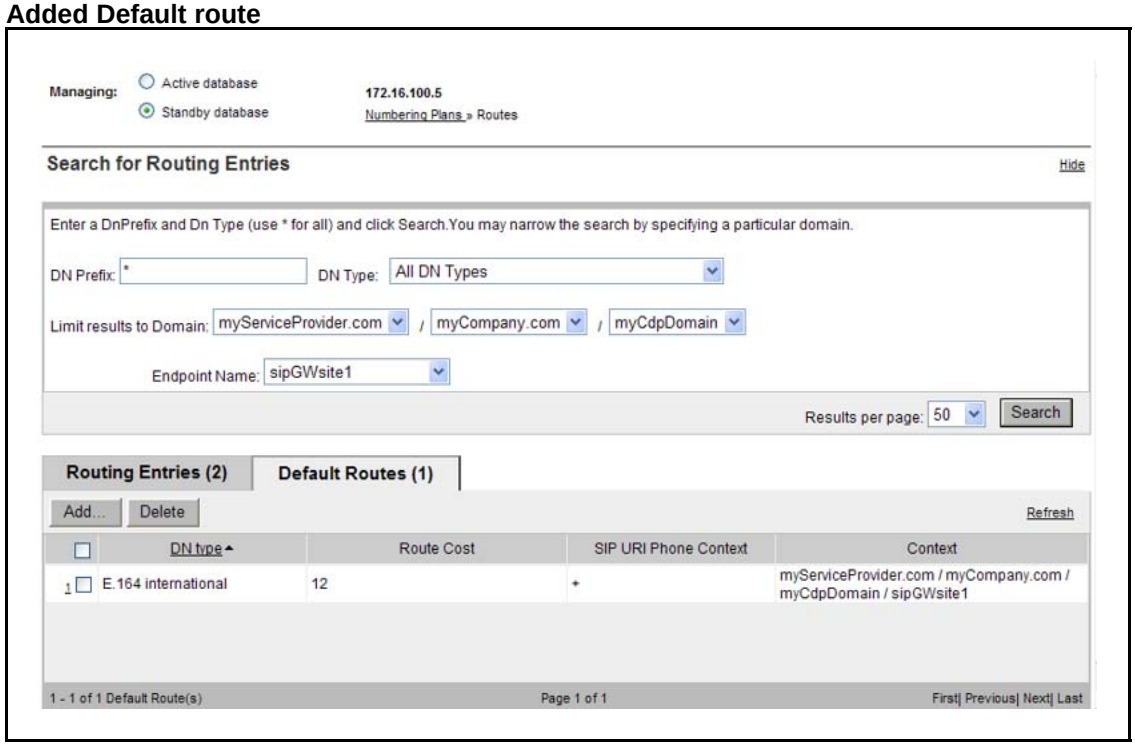
The DN type attribute determines how the phone context value, that is used to qualify the DN prefix, is built from the building blocks configured for the routing entry parents.

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 121 "Added Default route" (page 260).

Figure 121
Added Default route



10 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

11 Test the configuration changes.

12 See Procedure 63 “Committing the database” (page 290)to update the database with the configuration changes.

--End--

View Default Routes

Use the following procedure to view Default Routes.

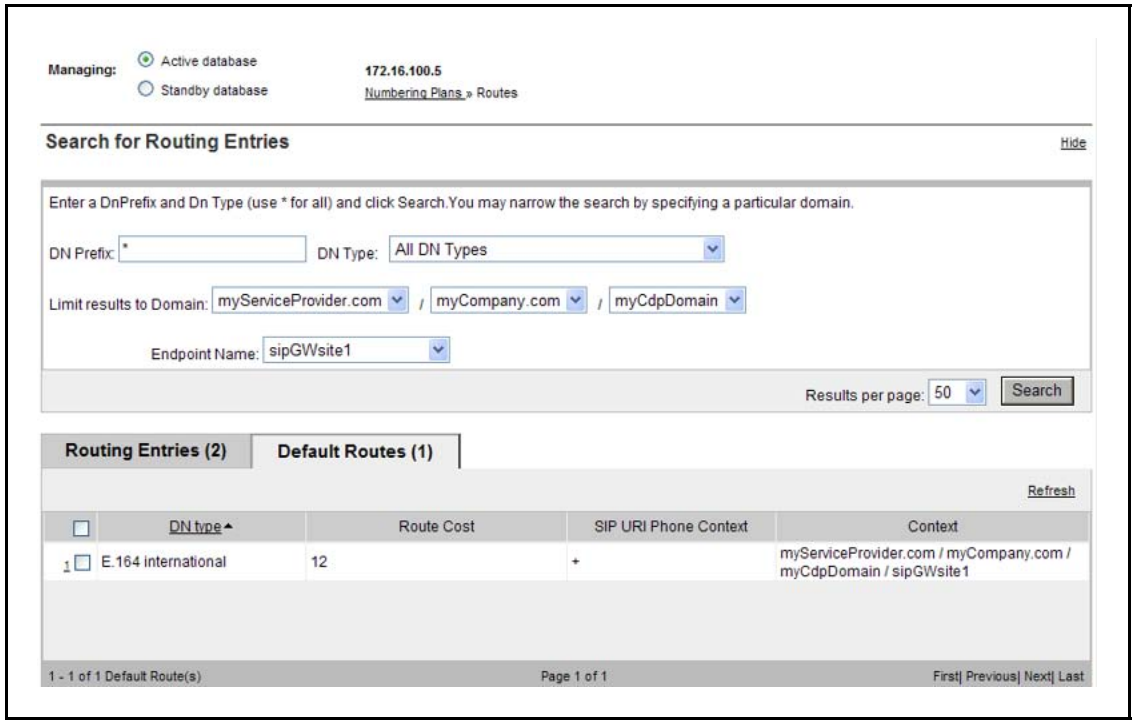
Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 49
Viewing Default Routes

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Select the **Active** or **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page 178). 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	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** tab.
6	Click **Search**. The web page expands to display a list of configured Default Route(s), as shown in Figure 122 "Search for Default Routes web page" (page 262). The Default Routes can be sorted in ascending or descending alphabetical order. See "Sort web page by DN type" (page 158) .

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 122
Search for Default Routes web page



--End--

Edit a Default Route

Use the following procedure to edit a Default Route.

Procedure 50
Editing a Default Route

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
3	Select the **DN Type** from the **DN Type:** drop-down list.
4	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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

5 Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.

6 Click the **Default Routes** tab

7 Click **Search**.

The web page expands to display a list of configured Default Route(s), as shown in Figure 122 "Search for Default Routes web page" (page 262).

The Default Routes can be sorted in ascending or descending alphabetical order. See "Sort web page by DN type" (page 158) .

8 Click a **link** in the **DN Type** column of the Default Routes pane.

The **Edit Default Route** web page opens.

9 Modify the **DN Type** or **Route Cost**.

10 Click the **Save** button. The standby database is updated. The **Routes** web page opens displaying the modified default route, as shown in Figure 108 "Routes web page" (page 246)

11 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state. The configuration changes can now be tested.

12 Test the configuration changes.

13 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Delete a Default Route

Use the following procedure to delete a Default Route.

Procedure 51
Deleting a Default Route

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.**The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Ensure **Standby database** is selected. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

4 Select a **Gateway Endpoint** from the **Endpoint Name** drop-down list in the **Search for Routing Entries** pane.

5 Click the **Default Routes** tab.

6 Click **Search**.

The web page expands to display a list of configured Default Route(s), as shown in Figure 122 "Search for Default Routes web page" (page 262).

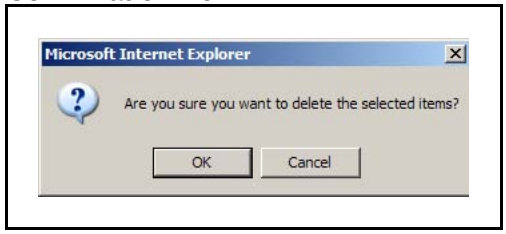
The Default Routes can be sorted in ascending or descending alphabetical order. See "Sort web page by DN type" (page 158) .

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 123 "Confirmation Box" (page 264), requesting confirmation before deleting the selected **Default Route**.

Figure 123
Confirmation Box



9 Click **OK**. The standby database is updated. The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).

10 See Procedure 60 “Cutting over the database” (page 288) to place the database in a Switched Over state.

11 See Procedure 63 “Committing the database” (page 290) to update the database with the configuration changes.

--End--

Manage bulk export of routing entries

The NRS supports up to 5 0000 routing entries and default routes. A Comma Separated Value (CSV) file is used to create routing entries in the Standby database. The routing entries in the Standby or Active database can be exported into a CSV file.

Nortel recommends that you do not perform bulk export database operations while traffic runs on a server that has NRS hosted co-resident with Signaling Server applications. The operation can take a large amount of time, depending on the amount of information and the traffic rate.

Copyright © 2010 Nortel Networks. All Rights Reserved.

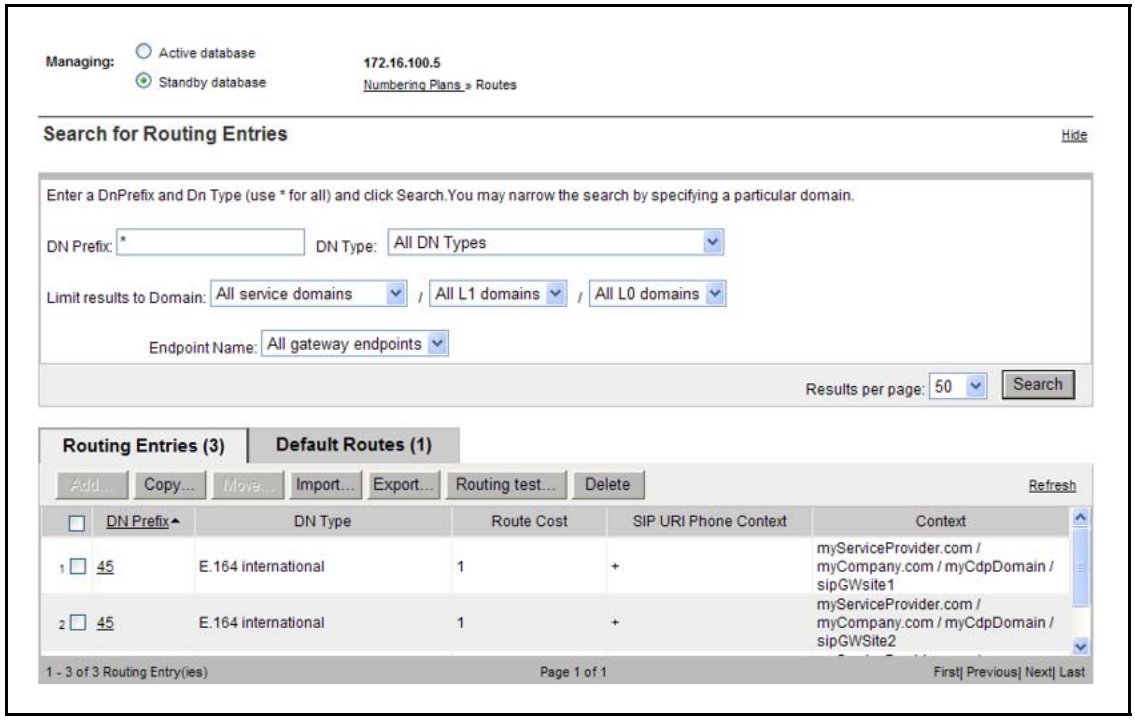
Bulk export of routing entries

Use the following procedure for bulk export of routing entries.

Procedure 52
Bulk export of routing entries

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 124 "Routes web page" (page 265).

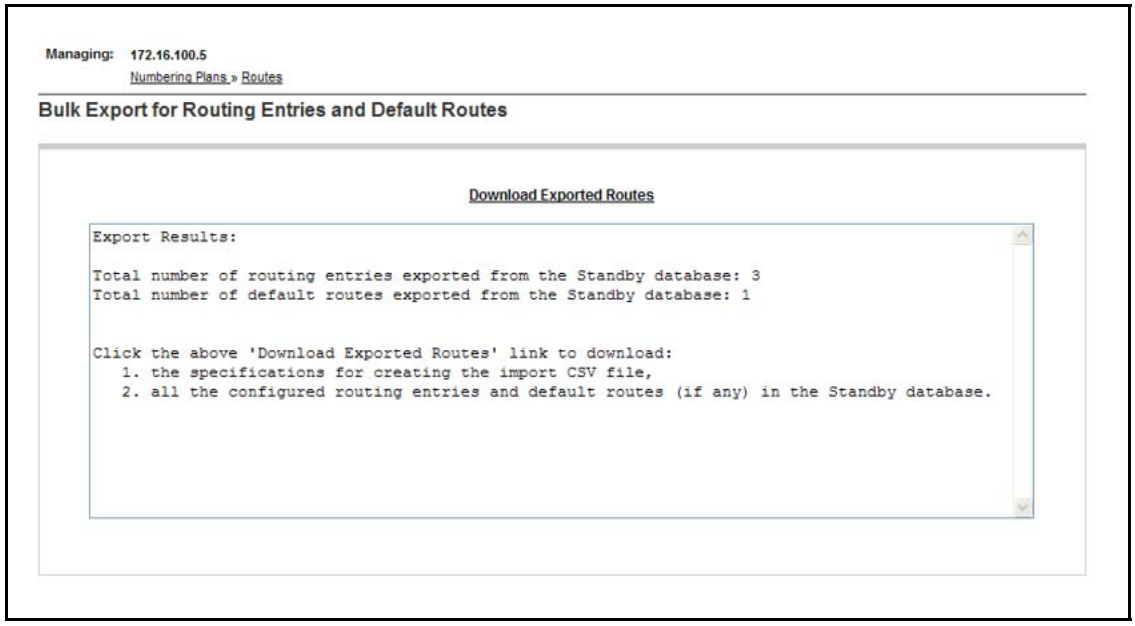
Figure 124
Routes web page



2	Select the **Active** or **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
3	Click the **Export** button. The **Bulk Export for Routing Entries and Default Routes** Web page appears as shown in Figure 125 "Bulk Export for Routing Entries and Default Routes web page" (page 266), summarizing the number of routing entries exported.

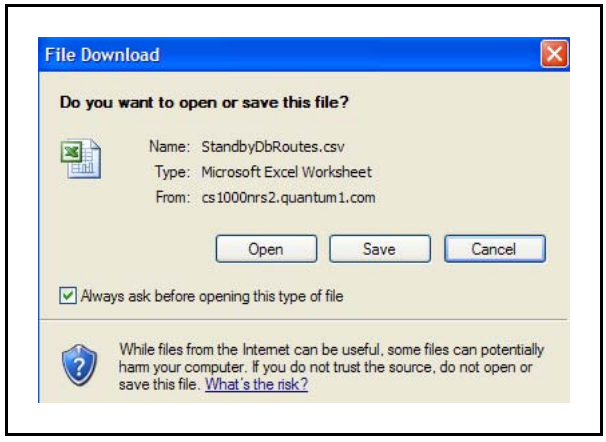
Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 125
Bulk Export for Routing Entries and Default Routes web page



4 Click the **Download Exported Routes** link to download and save the CSV file. The **File Download** Web page appears as shown in Figure 126 "File Download web page" (page 266).

Figure 126
File Download web page

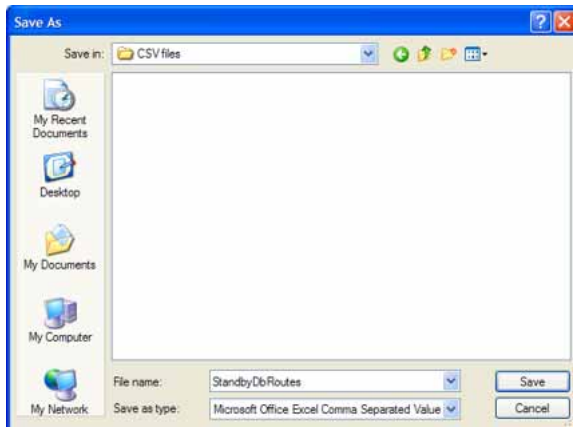


Note: Even if there are no routing entries or default routes configured in the selected database, the **Download Exported Routes** link will still be displayed. The exported file can be used as the specification for the import CSV file.

5 Click the **Save** button. The **Save As** Web page appears as shown in Figure 127 "Save As web page" (page 267).

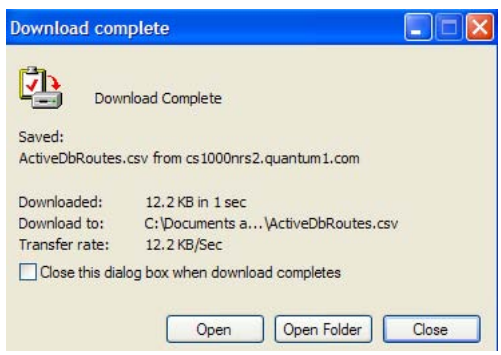
Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 127
Save As web page



6 Select a folder from the **Save in:** drop down list and click the **Save** button. The **Download Complete** Web page appears as shown in Figure 128 "Download complete web page" (page 267).

Figure 128
Download complete web page



7 Click the **Close** button.

--End--

Manage bulk import of routing entries

Recommendations

ATTENTION
The existing routing entries and default routes in the Standby database will be deleted completely during a bulk import operation, even if the import operation fails.

Nortel recommends that

Copyright © 2010 Nortel Networks. All Rights Reserved.

- a CSV file containing configured routing entries and default routes in the Active and Standby databases be saved before a bulk import operation.
- the Active database is manually backed up before a bulk import operation. To manually backup the Active database see Procedure 65 “Backing up the database manually” (page 292).
- bulk export and import operations be performed during maintenance windows.
- necessary routing tests to validate the configuration be performed before committing the imported routing entries to the Active database.
- not performing bulk import database operations while traffic runs on a server that has NRS hosted co-resident with Signaling Server applications. The operation can take a large amount of time, depending on the amount of information and the traffic rate.

Bulk import of routing entries

The bulk import operation imports routing entries into the Standby database. Routing entries can not be imported directly into the Active database. To import routing entries into the Active database

- import routing entries into the Standby database
- perform a database **Cut over**. See Procedure 60 “Cutting over the database” (page 288).
- perform a database **Commit**. See Procedure 63 “Committing the database” (page 290).

The import CSV file should contain the Service Domain, L1 Domain, L0 Domain and Endpoints which are present in the database. If the respective Service Domain, L1 Domain, L0 Domain and Endpoints are not present, then the routes will be skipped.

When importing data from that CSV file, the concept of NRS bulk import/export helps to capture more information when downloading such that the import process supports the creation of service domains, L1 domains, L0 domains, and endpoints automatically if not present in the NRS database.

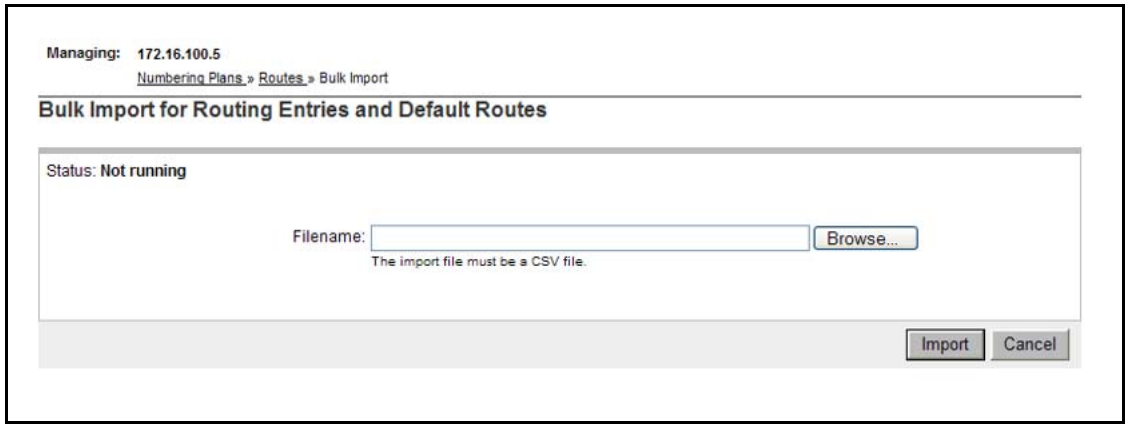
Use the following procedure for bulk import of routing entries into the Standby database.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 53
Bulk import of routing entries

Step	Action
1	In the **NRS Manager Navigator** select **Numbering Plans > Routes.** The **Routes** Web page appears as shown in Figure 108 "Routes web page" (page 246).
2	Select the **Standby** database. See Procedure 9 “Switching between the Active and Standby databases” (page 178).
3	Click the **Import** button. The **Bulk Import for Routing Entries and Default Routes** Web page appears as shown in Figure 129 "Bulk Import for Routing Entries and Default Routes web page" (page 269).

Figure 129
Bulk Import for Routing Entries and Default Routes web page



Note: The **Import** button will be enabled only if the **Standby** database is selected.

4 Click the **Browse** button to choose the CSV file to be imported, or type the file name in the **Specify the import CSV file name** text box.

Note: In Internet Explorer version 8 and later, the text box to input file name is disabled due to security reasons. The path needs to be specified using the Browse button.

5 Click the **Import** button.

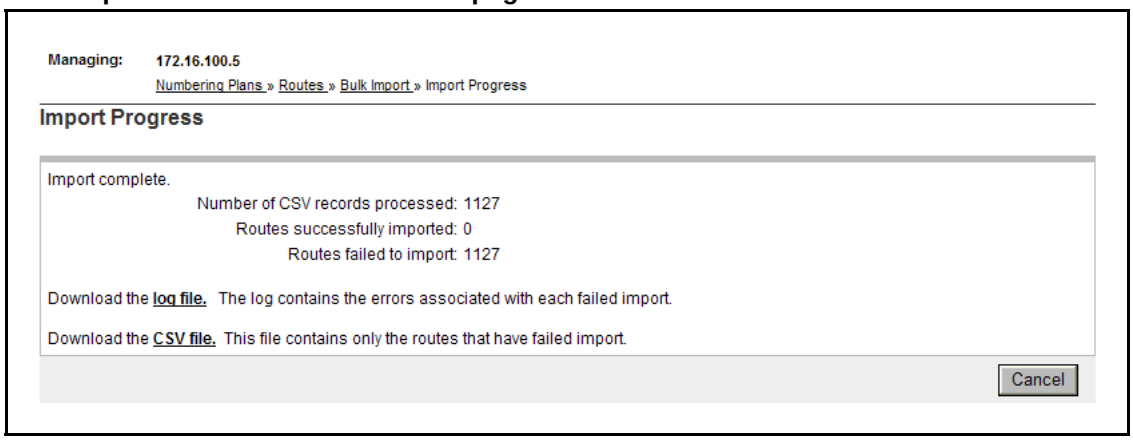
When the Import operation is started the user is redirected to the Import Progress web page showing the status of the Import operation. The progress of the Import operation is available for viewing at any time. While the routing entries are being imported the user can navigate to any page in NRS Manager and return to the Import Progress page to view the status of the Import operation.

Copyright © 2010 Nortel Networks. All Rights Reserved.

6 The results of the **Import** operation are shown in the Import Progress web page.

If there are errors, edit the import CSV file and repeat the import operation. The import operation is stopped if there are more than 20 errors. There is no restriction on the editors that can be used to edit the import CSV file. The CSV file must follow the specifications summarized in "Import CSV file specifications" (page 271). See Figure 130 "Bulk Import Results with errors web page" (page 270) for an example of a **Bulk Import Results with errors web page**.

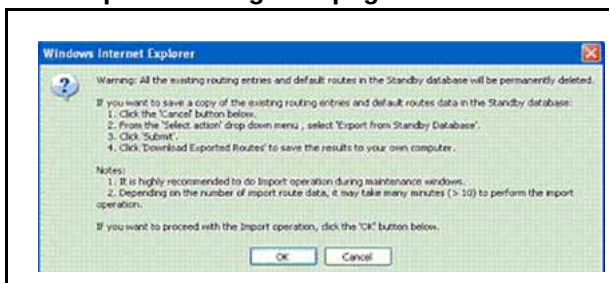
Figure 130
Bulk Import Results with errors web page



ATTENTION
The existing routing entries and default routes in the Standby database will be deleted completely during a bulk import operation, even if the import operation fails.

If there are no Import Results errors the warning page shown in Figure 131 "Bulk Import warning web page" (page 270) opens.

Figure 131
Bulk Import warning web page



7 Click the **OK** button to confirm the import operation, or click the **Cancel** button to abort the import operation.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Import CSV file specifications

1. Comments are indicated by # at the beginning of the line.
2. The order of the eight mandatory data fields in each record is as follows:
   a. serviceDomain
   b. l1Domain
   c. l0Domain
   d. gatewayEndpoint
   e. dnType
   f. defaultRouteFlag
   g. dnPrefix
   h. routeCost

   Note: All of the above 8 data fields are mandatory except dnPrefix when defaultRouteFlag is 1 (default route).
3. Each field has to be separated by a comma.
4. NRSM is restricting singlequote, comma, and new line character in the description field of service domain, L1 domain, L0 domain, Gateway Endpoint, and user Endpoint. If any of these values are entered, an error message is thrown in the UI stating that its an invalid input character for the description field.
5. Each record takes up one row.
6. Fields serviceDomain/l1Domain/l0Domain/gatewayEndpoint are text fields. Domain names are case sensitive.
7. Field dnType is numeric:
   — 1: E.164 international
   — 11:E.164 national
   — 21:E.164 local (subscriber)
   — 2: Private level 1 regional (UDP location code)
   — 3: Private special
   — 4: Private level 0 regional (CDP steering code)
8. Field defaultRouteFlag is numeric:
   — 0: routing entry
   — 1: default route
9. Field dnPrefix is a text field and can have only the following characters:

Copyright © 2010 Nortel Networks. All Rights Reserved.

— 0-9

— - (dash: for specifying a range. It can not be the first character of this field.)

— # (pound sign. It can not be the first character of this field.)

— ? (question mark. It can not be the first character of this field.)

Note: The dnPrefix field should be left blank for default route records. The input will be ignored if it is not left blank.

10. Field routeCost is numeric (range 1-255).
11. Any invalid input in a Web UI routes data entry is also invalid in an import CSV file.
12. Data entered in the nineth column (field) and beyond is ignored.
13. There is not a limit to the size of the CSV file, but a maximum of 50000 entries can be imported.

For further details on the data fields in the CSV file, see Table 25 "Specification of data fields in the CSV file" (page 272).

Table 25
Specification of data fields in the CSV file

Order of fie lds in each record	Field Type	Type	Valid characters	Mandatory	Remarks
1	serviceDomain	text field	0-9 a-z should begin with a letter or a number .(dot sign) -(dash: for specifying a range. It can not be the first character of this field) 0-29 : maximum number of characters allowed	yes	

Copyright © 2010 Nortel Networks. All Rights Reserved.

2	l1Domain	text field	0-9 a-z should begin with a letter or a number .(dot sign) -(dash: for specifying a range. It can not be the first character of this field) 0-29 : maximum number of characters allowed	yes	
3	l0Domain	text field	0-9 a-z should begin with a letter or a number .(dot sign) -(dash: for specifying a range. It can not be the first character of this field) 0-29 : maximum number of characters allowed	yes	
4	gatewayEndpoint	text field	0-9 a-z should begin with a letter or a number .(dot sign) -(dash: for specifying a range. It can not be the first character of this field) 0-29 : maximum number of characters allowed	yes	
5	description	text field	0-120 : maximum number of characters allowed can contain all alphanumeric characters except single quote ’(single quote: It cannot be used)	no	

Copyright © 2010 Nortel Networks. All Rights Reserved.

6	trustNodeEnabled	boolean	should be true or false default value will be 'true'	no	
7	tandemEndpointId	numeric		no	contains the gatewayEndpoint ids default value will be 'Not configured'
8	authEnabled	numeric	0: Not configured 1: Authentication on 2: Authentication off	no	
9	password	text field	0-24 : maximum number of characters allowed _(underscore: is allowed and also can begin with this symbol) other special characters are not allowed	no: When the field 'authEnabled' is 0: Not configured or 2: Authentication off yes: When the field 'authEnabled' is 1: Authentication on	
10	e164CountryCode	numeric	0-8 : maximum number of digits allowed 0-9 digits allowed special characters and alphabets are not allowed	no	
11	e164AreaCode	numeric	0-8 : maximum number of digits allowed 0-9 digits allowed special characters and alphabets are not allowed	no	
12	intDialingAccessCode	numeric	0-8 : maximum number of digits allowed 0-9 digits allowed special characters and alphabets are not allowed	no	

Copyright © 2010 Nortel Networks. All Rights Reserved.

13	intDialingLen	numeric	0-99 : numbers in this range is only allowed special characters and alphabets are not allowed should exceed the length of intDialingAccessCode	no	
14	natDialingAccessCode	numeric	0-8 : maximum number of digits allowed 0-9 digits allowed special characters and alphabets are not allowed	no	
15	natDialingLen	numeric	0-8 : maximum number of digits allowed 0-9 digits allowed special characters and alphabets are not allowed	no	
16	localDialingAccessCode	numeric	0-8 : maximum number of digits allowed 0-9 digits allowed special characters and alphabets are not allowed	no	
17	localDialingLen	numeric	0-99 : numbers in this range is only allowed special characters and alphabets are not allowed should exceed the length of localDialingAccessCode	no	
18	privateL1DialingAccessCode	numeric	0-8 : maximum number of digits allowed 0-9 digits allowed special characters and alphabets are not allowed	no	

Copyright © 2010 Nortel Networks. All Rights Reserved.

19	privateL1DialingLen	numeric	0-99 : numbers in this range is only allowed special characters and alphabets are not allowed should exceed the length of privateL1DialingAccessCode	no	
20	privateSpecialNumber1	numeric	0-8 : maximum number of digits allowed 0-9 digits allowed special characters and alphabets are not allowed	no	
21	privateSpeNumLen1	numeric	0-99 : numbers in this range is only allowed special characters and alphabets are not allowed should exceed the length of privateSpecialNumber1	no	
22	privateSpecialNumber2	numeric	0-8 : maximum number of digits allowed 0-9 digits allowed special characters and alphabets are not allowed	no	
23	privateSpeNumLen2	numeric	0-99 : numbers in this range is only allowed special characters and alphabets are not allowed should exceed the length of privateSpecialNumber2	no	
24	addressType	numeric	0 : always contains this default value		value cannot be altered
25	address	numeric	should be in ip address format 00.00.00.00 0-255: range		

Copyright © 2010 Nortel Networks. All Rights Reserved.

26	h323SupportType	numeric	0: H.323 not supported 1: RAS H.323 endpoint 2: Not RAS H.323 endpoint	if 2: Not RAS H.323 endpoint is selected the 'address' field should be filled with valid ip address	
27	sipSupportType	numeric	0: SIP not supported 1: Static SIP endpoint 2: Dynamic SIP endpoint	if 1: Static SIP endpoint is selected the 'address' field should be filled with valid ip address if 2: Dynamic SIP endpoint is selected any one of the fields 'sipTcpTransportEnabled' or 'sipUdpTransportEnabled' or 'sipTlsTransportEnabled' should contain the value true	
28	sipTcpTransportEnabled	boolean	should be 'true' or 'false' default value will be 'false'		
29	sipTcpPort	numeric	0-65535 : numbers in this range is only allowed 0-5 : maximum number of digits allowed special characters and alphabets are not allowed		

Copyright © 2010 Nortel Networks. All Rights Reserved.

30	sipUdpTransportEnabled	boolean	should be 'true' or 'false' default value will be 'false'		
31	sipUdpPort	numeric	0-65535 : numbers in this range is only allowed 0-5 : maximum number of digits allowed special characters and alphabets are not allowed		
32	sipTlsTransportEnabled	boolean	should be 'true' or 'false' default value will be 'false'		
33	sipTlsPort	numeric	0-65535 : numbers in this range is only allowed 0-5 : maximum number of digits allowed special characters and alphabets are not allowed		
34	persistentTcpSupportEnabled	boolean	should be 'true' or 'false' default value will be 'false'		
35	sipsSupportEnabled	boolean	should be 'true' or 'false' default value will be 'false'		
36	ncsEnabled	boolean	should be 'true' or 'false' default value will be 'false'		
37	redundancyEnabled	numeric	0: Not Configured 1: Main Office 2: Redundant Office		
38	mainEndpointId	numeric	contains the gatewayEndpoint ids default value will be 'Not configured'		

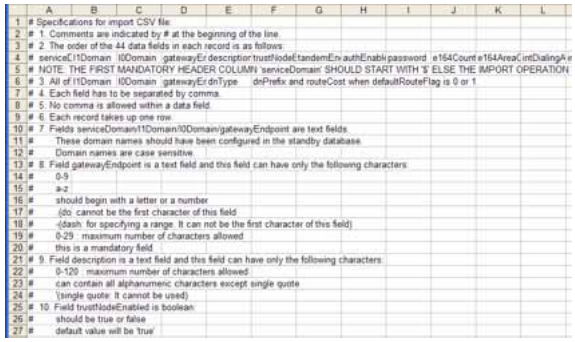
Copyright © 2010 Nortel Networks. All Rights Reserved.

39	redundantEndpointId	numeric	contains the gatewayEndpoint ids default value will be 'Not configured'		
40	dnType	numeric	1: E.164 internationa l 11: E.164 national 21: E.164 local (subscriber) 2: Private level 1 regional (UDP location code) 3: Private special 4: Private level 0 regional (CDP steering code)	yes	
41	defaultRouteFlag	numeric	0: routing entry 1: default route	yes	
42	dnPrefix	text field	0-9 - (dash: for specifying a range. It can not be the first character of this field.) # (pound sign. It can not be the first character of this field.) ? (question mark. It can not be the first character of this field.)	yes	dnPrefix should be left blank for default route records. The input will be ignored if it is not left blank.
43	routeCost	numeric	range is 1 - 255	yes	
44	SIP Mode	numeric	range is 0 - 2 0: SIP Mode (Not Applicable) for H323 Endpoints 1: SIP Mode (proxy) for SIP Endpoints 2: SIP Mode (Redirect) for SIP Endpoints		
45	Data entered in this field and beyond is ignored. These columns can be used for comments.				

See Figure 132 "Example of a CSV file" (page 280) for an example of a **CSV file**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 132
Example of a CSV file



	A	B	C	D	E	F	G	H	I	J	K	L
1	# Specifications for import CSV file:											
2	# 1. Comments are indicated by # at the beginning of the line.											
3	# 2. The order of the 44 data fields in each record is as follows:											
4	# serviceD1Domain l0Domain gatewayEr description trustNodeE tandemEn authEnabl password e164Count e164AreaC intDialingA											
5	# NOTE: THE FIRST MANDATORY HEADER COLUMN 'serviceDomain' SHOULD START WITH '#' ELSE THE IMPORT OPERATION											
6	# 3. All of l1Domain l0Domain gatewayEr dnType dnPrefix and routeCost when defaultRouteF lag is 0 or 1.											
7	# 4. Each field has to be separated by comma.											
8	# 5. No comma is allowed within a data field.											
9	# 6. Each record takes up one row.											
10	# 7. Fields serviceDomain/l1Domain/l0Domain/gatewayEndpoint are text fields.											
11	# These domain names should have been configured in the standby database.											
12	# Domain names are case sensitive.											
13	# 8. Field gatewayEndpoint is a text field and this field can have only the following characters:											
14	# 0-9											
15	# a-z											
16	# should begin with a letter or a number											
17	# .(do cannot be the first character of this field											
18	# -(dash for specifying a range. It can not be the first character of this field)											
19	# 0-29 maximum number of characters allowed											
20	# this is a mandatory field											
21	# 9. Field description is a text field and this field can have only the following characters:											
22	# 0-120 maximum number of characters allowed											
23	# can contain all alphanumeric characters except single quote											
24	# '(single quote. It cannot be used)											
25	# 10. Field trustNodeEnabled is boolean:											
26	# should be true or false											
27	# default value will be 'true'											

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 54
Verifying the numbering plan

Step	Action
1	Perform a database **Cut over**. Cutting over places the database on the network. See Procedure 60 “Cutting over the database” (page 288).
2	Perform the routing tests. • See Procedure 55 “Performing an H.323 Routing Test” (page 281). • See Procedure 56 “Performing a SIP Routing Test” (page 282).
3	If the routing tests succeed, perform a database **Commit**. See Procedure 63 “Committing the database” (page 290).
4	If there are problems with the network testing, use the database **Revert** command to undo the **Cut over.** See Procedure 61 “Reverting the database changes” (page 289) 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 62 “Rolling back changes to the database” (page 290)

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

H.323 and SIP Routing Tests

To ascertain if a numbering plan entry exists in the active or standby database:

- See Procedure 55 “Performing an H.323 Routing Test” (page 281) to perform an H.323 Routing Test.
- See Procedure 56 “Performing a SIP Routing Test” (page 282) to perform a SIP Routing Test.

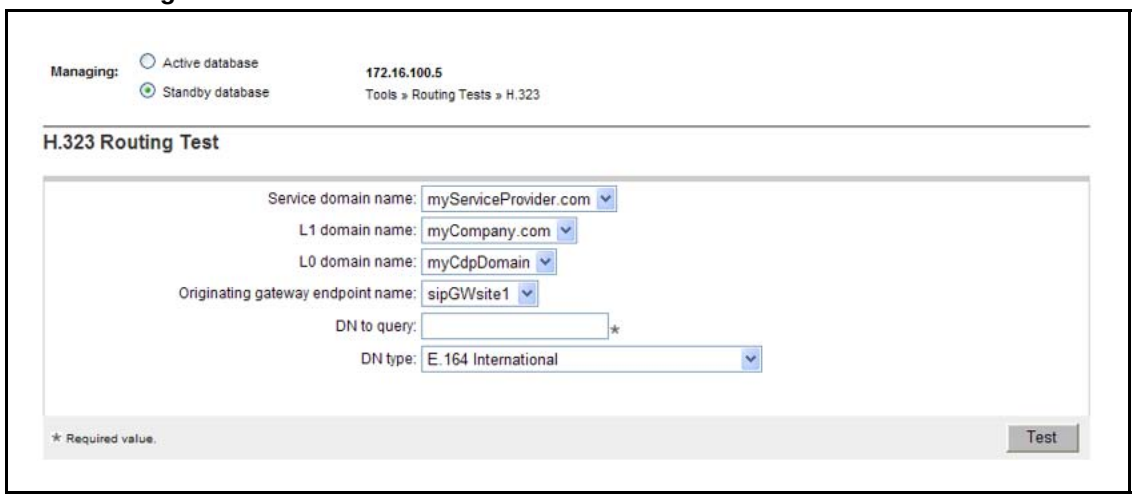
Perform an H.323 Routing Test

Use the following procedure to perform an H.323 Routing Test.

Procedure 55
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 appears as shown in Figure 133 "H.323 routing Test" (page 281).

Figure 133
H.323 routing Test



2	Select **Active database** or **Standby database**. See Procedure 9 “Switching between the Active and Standby databases” (page 178)
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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

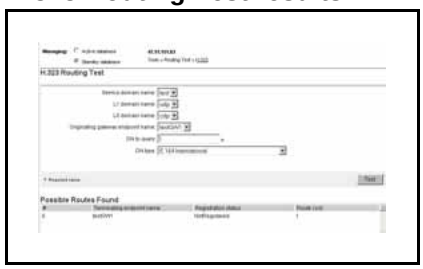
7 Enter a numbering plan entry you want to check in the **DN to query** text box.

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 282).

Figure 134
H.323 Routing Test results



--End--

Perform a SIP Routing Test

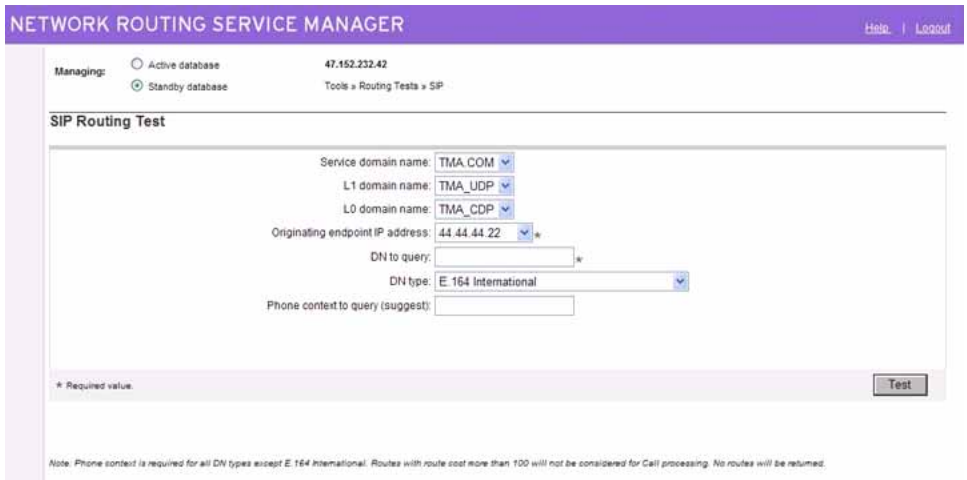
Perform a SIP Routing Test.

Procedure 56
Performing a SIP Routing Test

Step	Action
1	In the **NRS Manager Navigator,** select **Tools, Routing Tests, SIP.** The **SIP Routing Test** Web page appears as shown in Figure 135 "SIP Routing Test" (page 283).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 135
SIP Routing Test



2 Select **Active database** or **Standby database**. See Procedure 9 “Switching between the Active and Standby databases” (page 178)

3 Select the Service Domain from the **Service domain name** list.

4 Select the L1 Domain name from the **L1 domain name** list.

5 Select the L0 Domain name from the **L0 domain name** list.

6 Select the **Originating gateway endpoint IP address** from the list.

7 Enter a numbering plan entry you want to check in the **DN to query** box.

8 Select the DN type you want to check from the **DN type** list.

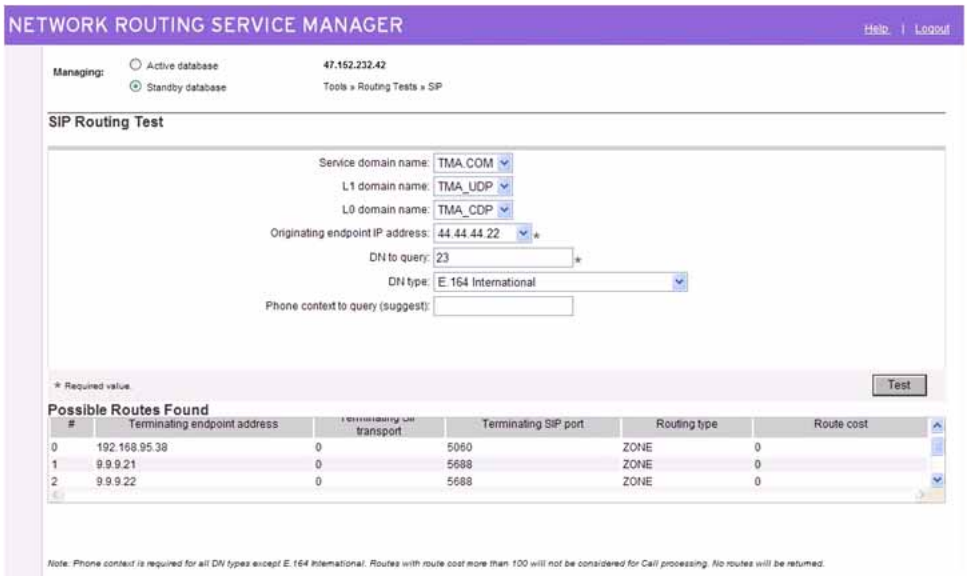
9 Enter the **Phone context to query**.

10 Click **Test**.

The results of the SIP Routing Test appears as shown in Figure 136 "SIP Routing Test results" (page 284).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 136
SIP Routing Test results



--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 57 “Disabling the NRS server” (page 285) to take the NRS out-of-service (disabling the NRS server).

See Procedure 58 “Enabling the NRS server” (page 286) to bring the NRS back in to service.

Copyright © 2010 Nortel Networks. All Rights Reserved.

See Procedure 59 “Restarting the NRS Server” (page 286) to restart the NRS.

The SIP Proxy must be started and running before you can disable or enable the application. To enable the SIP Proxy, click the **Restart** button in the **Service Status** pane of the **NRS Server** web page. See Procedure 59 “Restarting the NRS Server” (page 286).

To enable the Network Connection Service or the H.323 Gatekeeper, select **Enable** from the **Service Status** pane of the **NRS Server** web page. See Procedure 58 “Enabling the NRS server” (page 286).

Disable the NRS server

Use the following procedure to disable the NRS server.

Procedure 57
Disabling the NRS server

Step	Action
1	In the **NRS Manager Navigator** select **System > NRS Server.** The **NRS Server** web page opens.
2	Select a check box beside one or more configured services in the service name column of the **Service Status** pane of the **NRS Server** web page. See Figure 137 "Service Status pane" (page 285). **Figure 137** **Service Status pane**
3	Select **Graceful disable** from the **Service Status** pane of the **NRS Server** web page. The system disables the selected services.

--End--

Enable the NRS server

Use the following procedure to enable the NRS server.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 58
Enabling the NRS server

Step	Action
1	In the **NRS Manager Navigator** select **System > NRS Server.** The **NRS Server** web page opens
2	Select a check box beside one or more configured services in the service name column of the **Service Status** pane of the **NRS Server** web page. See Figure 137 "Service Status pane" (page 285).
3	Select **Enable** from the **Service Status** pane of the **NRS Server** web page. The system enables the selected services.

--End--

Restart the NRS Server

Use the following procedure to restart the NRS Server.

Procedure 59
Restarting the NRS Server

Step	Action
1	In the **NRS Manager Navigator** select **System > NRS Server.** The **NRS Server** web page opens.
2	Select a check box beside one or more configured services in the service name column of the **Service Status** pane of the **NRS Server** web page. See Figure 137 "Service Status pane" (page 285).
3	Click the **Restart** button in the **Service Status** pane of the **NRS Server** web page.

--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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 288). 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, “Database synchronization and operation component” (page 44).

To perform a:

Copyright © 2010 Nortel Networks. All Rights Reserved.

- database **Cut over**, see Procedure 60 “Cutting over the database” (page 288).
- database **Revert**, see Procedure 61 “Reverting the database changes” (page 289).
- database **Commit**, see Procedure 63 “Committing the database” (page 290).
- database **Roll back**, see Procedure 62 “Rolling back changes to the database” (page 290).

Perform a database Cut over

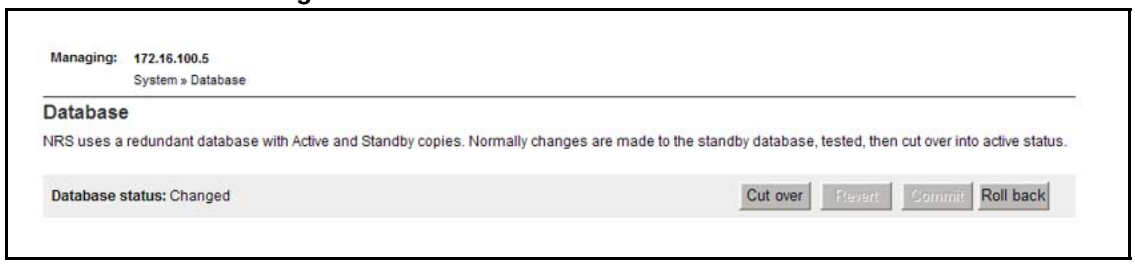
Cutting over a database switches the active and standby database access pointer. This swaps the primary and standby databases, so configuration changes take effect.

See Procedure 60 “Cutting over the database” (page 288) to perform a database cut over.

Procedure 60
Cutting over the database

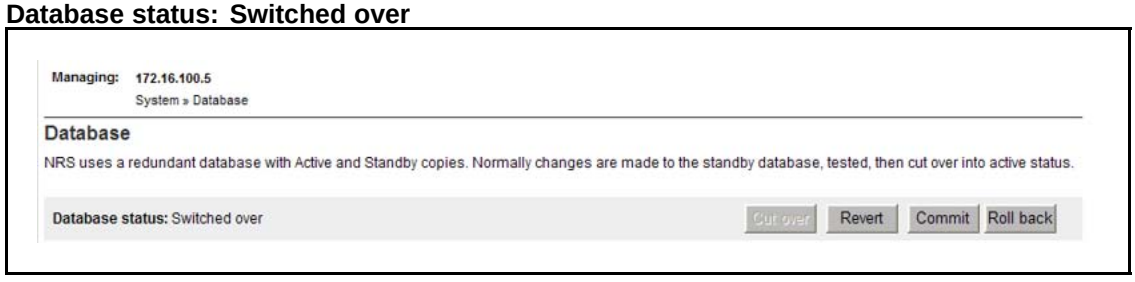
Step	Action
1	In the **NRS Manager Navigator** select **System > Database.** The **Database** Web page appears as shown in Figure 138 "Database status: Changed" (page 288).

Figure 138
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 288).

Figure 139
Database status: Switched over



Copyright © 2010 Nortel Networks. All Rights Reserved.

3	Perform a database **Commit** to save the changes after the cut over. See Procedure 63 “Committing the database” (page 290). If you do not want to save the changes to the database, perform a database Revert (see Procedure 61 “Reverting the database changes” (page 289)) or database Roll back (see Procedure 62 “Rolling back changes to the database” (page 290)).

--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 61 “Reverting the database changes” (page 289) to interchange the active and standby database access pointers .

Procedure 61
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 288).
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 288).

--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.

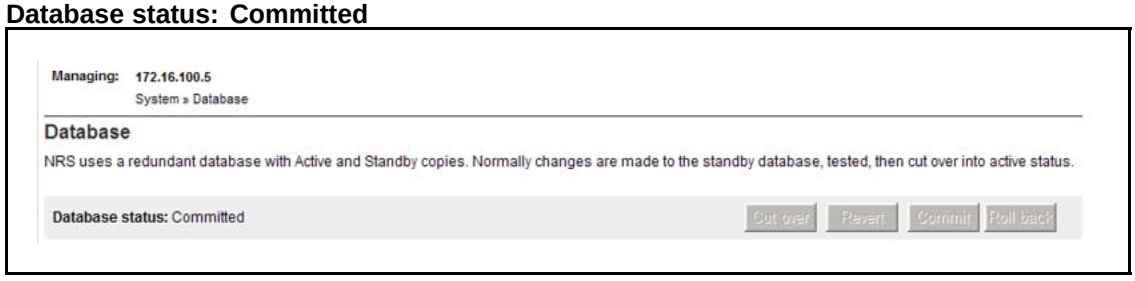
To roll back changes made to the standby database, perform Procedure 62 “Rolling back changes to the database” (page 290).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 62
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 288).
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 290)Figure 140 "Database status: Committed" (page 290).

Figure 140
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 63 “Committing the database” (page 290) to perform a database **Commit**.

Procedure 63
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 288).

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 290).

--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 8 “Configuring system-wide settings” (page 175) 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 64
Backing up the database automatically

Step	Action
1	In the **NRS Manager Navigator** select **Tools > Backup.** The **Database Backup** Web page appears as shown in Figure 141 "Database Backup web page" (page 292).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 141
Database Backup web page

2 Select **Auto backup** from the **Select backup action** drop-down list.

3 Click the **Submit** button.

The **System Wide Settings** Web page appears as shown in Figure 47 "System Wide Settings web page" (page 176).

4 Perform step 3 to step 6 of Procedure 8 “Configuring system-wide settings” (page 175).

--End--

Manually backup the database

Use the following procedure to manually backup the database.

Procedure 65
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 292).
2	Select **Manual backup** from the **Select backup action** drop-down list.
3	Click the **Submit** button.

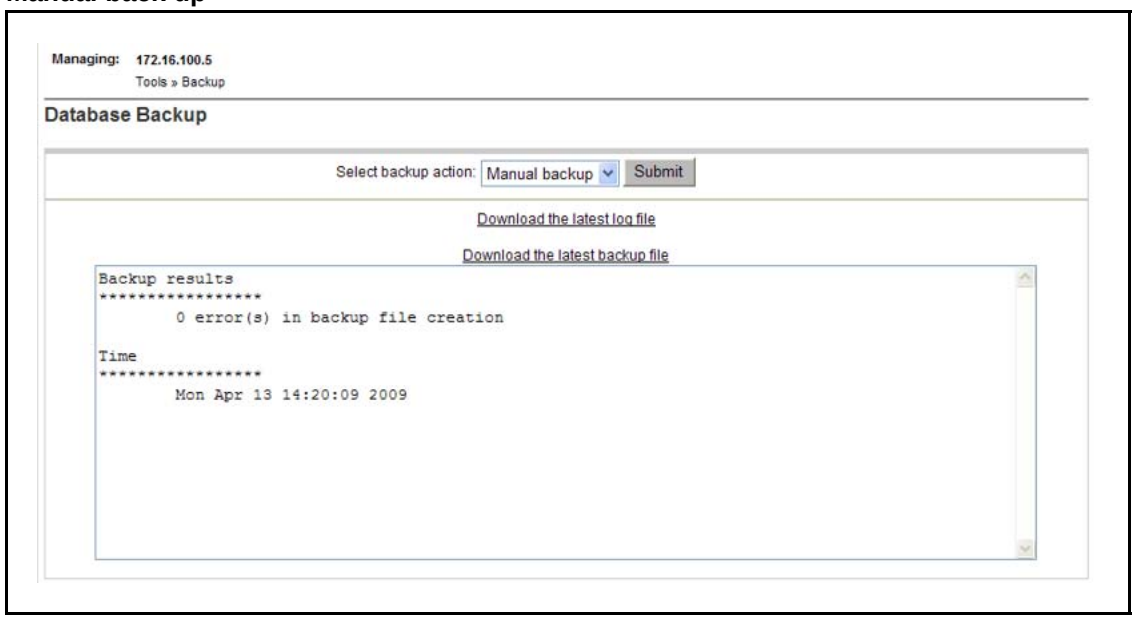
Copyright © 2010 Nortel Networks. All Rights Reserved.

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 293).

Two links appear on the screen:

- **Download the latest log file**.
  See Procedure 67 “Downloading the latest backup log file” (page 296) to download the latest backup log file.
- **Download the latest backup file**.
  See Procedure 66 “Downloading the latest backup file” (page 293) to download the latest backup file.

Figure 142
Manual back up



--End--

Download the latest backup file

Use the following procedure to download the latest backup file.

Procedure 66
Downloading the latest backup file

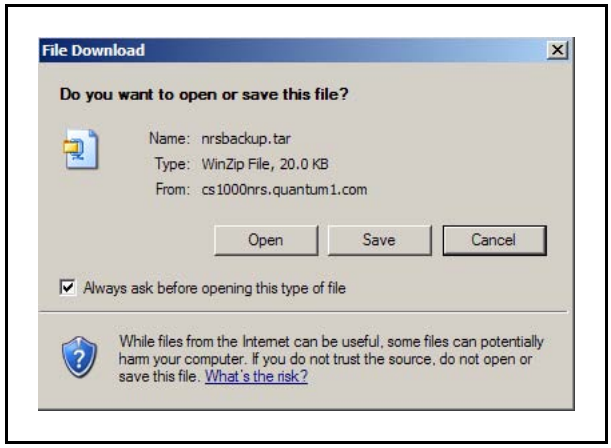
Step	Action
1	See Procedure 65 “Backing up the database manually” (page 292)

Copyright © 2010 Nortel Networks. All Rights Reserved.

2 Click the **Download the latest backup file** link on the **Database Backup** web page. See Figure 142 "Manual back up" (page 293).

The **File Download** dialog box opens.

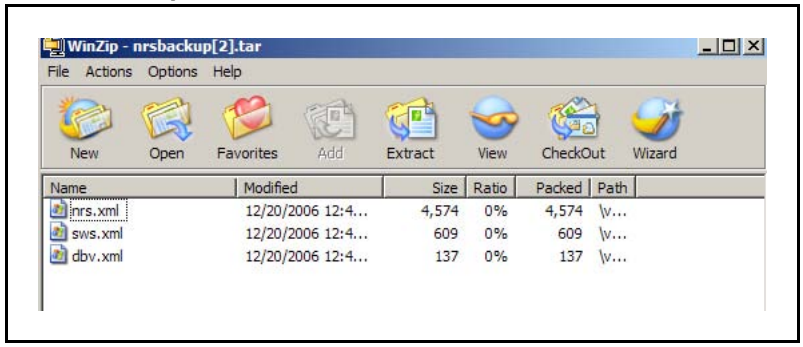
Figure 143
File Download dialog box



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



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.

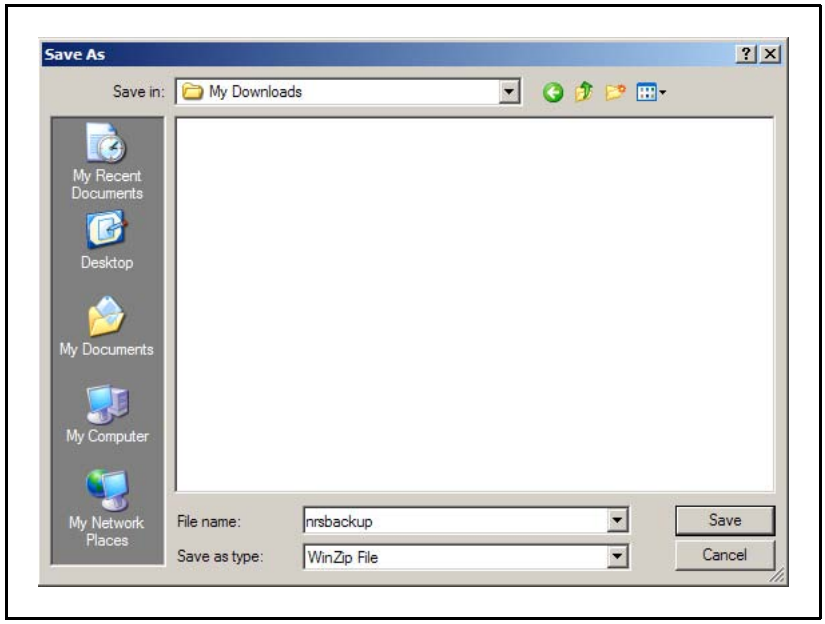
Or

4 Click **Save** to save the file to a local client.

The **Save As** dialog box opens.

Copyright © 2010 Nortel Networks. All Rights Reserved.

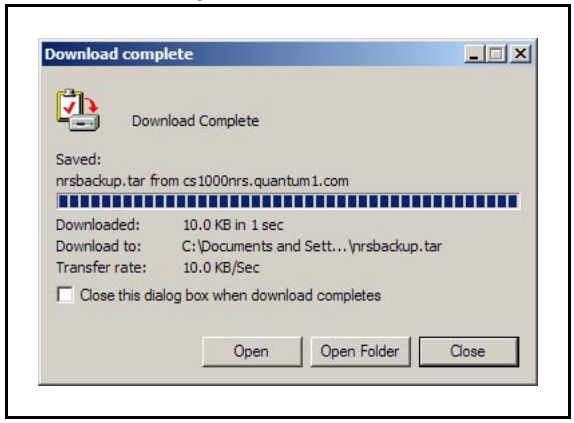
Figure 145
Save As dialog box



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



6 Click **Close**.

--End--

Download the latest backup log file

Use the following procedure to download the latest backup log file.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 67
Downloading the latest backup log file

Step	Action
1	See Procedure 65 “Backing up the database manually” (page 292)
2	Click **Download the latest log file** link on the **Database Backup** web page. See Figure 142 "Manual back up" (page 293). A window opens containing the latest backup log file, as shown in Figure 144 "Latest backup file" (page 294). 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

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

Nortel recommends that you do not restore a database while traffic runs on a server that has NRS hosted co-resident with Signaling Server applications. The operation can take a large amount of time depending on the amount of information and the traffic rate.

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 run the database restore commands.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 CS 1000 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 68
Restoring the database

Step	Action
1	In the **NRS Manager Navigator** select **Tools > Restore.** The **Database Restore** Web page appears as shown in Figure 148 "Database Restore web page" (page 298).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 148
Database Restore web page

2 The database can be restored from three source locations:

- From the **Connected Signaling Server**.
  See Procedure 69 “Restoring from the connected Signaling Server” (page 298) to restore the database from the Connected Signaling Server.
- From a secure **FTP site**.
  See Procedure 70 “Restoring from a secure FTP site” (page 301) to restore the database from a secure FTP site.
- From the **Client machine**.
  See Procedure 71 “Restoring from a client machine” (page 302) to restore the database from the Client machine.

--End--

Restore from the connected Signaling Server

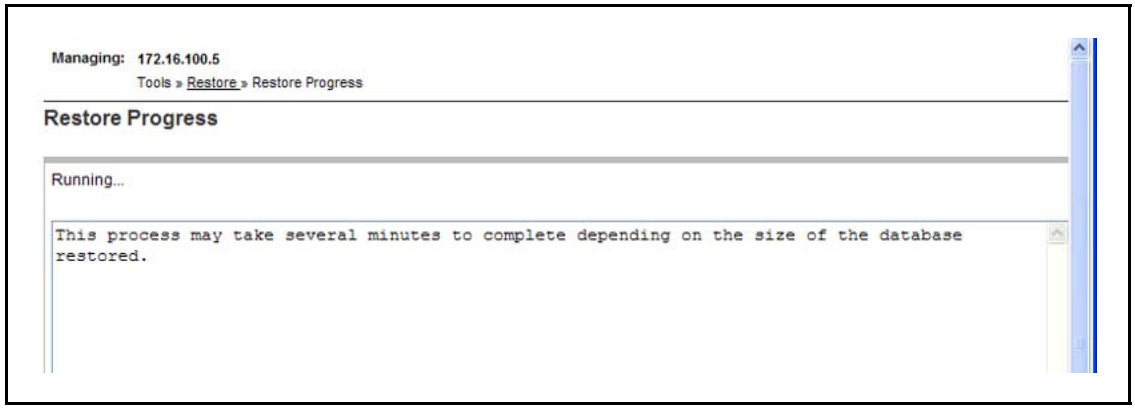
Use the following procedure to restore from the connected Signaling Server.

Procedure 69
Restoring from the connected Signaling Server

Step	Action
1	In the **NRS Manager Navigator** select **Tools > Restore.** The **Database Restore** Web page appears as shown in Figure 148 "Database Restore web page" (page 298).
2	Select **Connected Signaling Server** from the **Restore from** drop-down list. See Figure 148 "Database Restore web page" (page 298).
3	Click the **Restore** button. The **Restore Progress Running** Web page appears as shown in Figure 149 "Restore Progress Running" (page 299).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 149
Restore Progress Running



The **Database Restore** web page refreshes displaying the Database Restore status, as shown in Figure 150 "Database Restore status" (page 299).

Figure 150
Database Restore status

While the database is being restored the user can navigate to any page in NRS Manager and return to the Database Restore page to view the status of the database restore operation. To view the status of the Database Restore operation click the **View progress** hyperlink.

When the Database Restore operation completes the **Database Restore** web page refreshes, as shown in Figure 151 "Database Restore complete" (page 300).

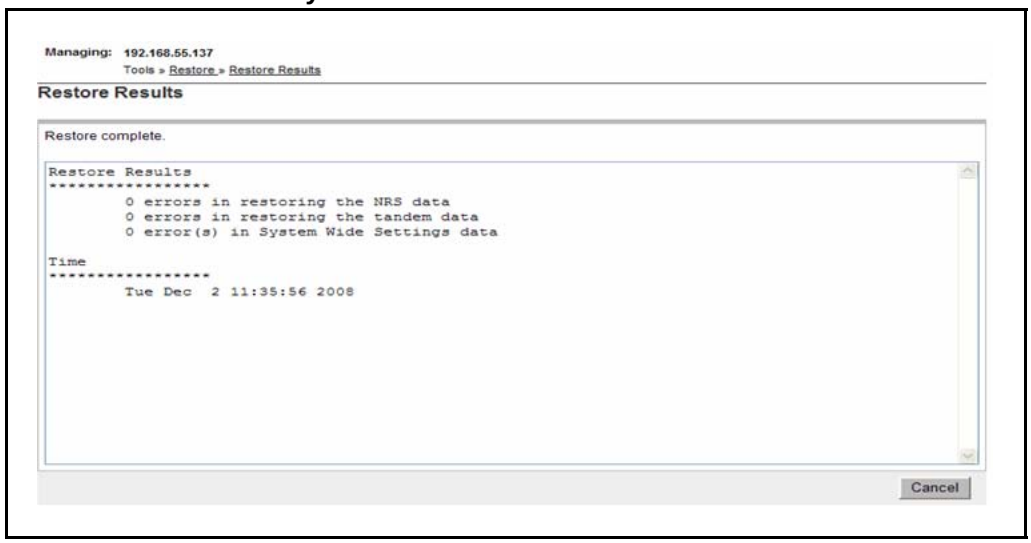
Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 151
Database Restore complete

4 Click the **View results** hyperlink.

A message displays in the text area of the **Database Restore** web page showing a summary of the database restore from the Signaling Server, as shown in Figure 152 "Restore Result summary" (page 300) .

Figure 152
Restore Result summary



--End--

Restore from a secure FTP site

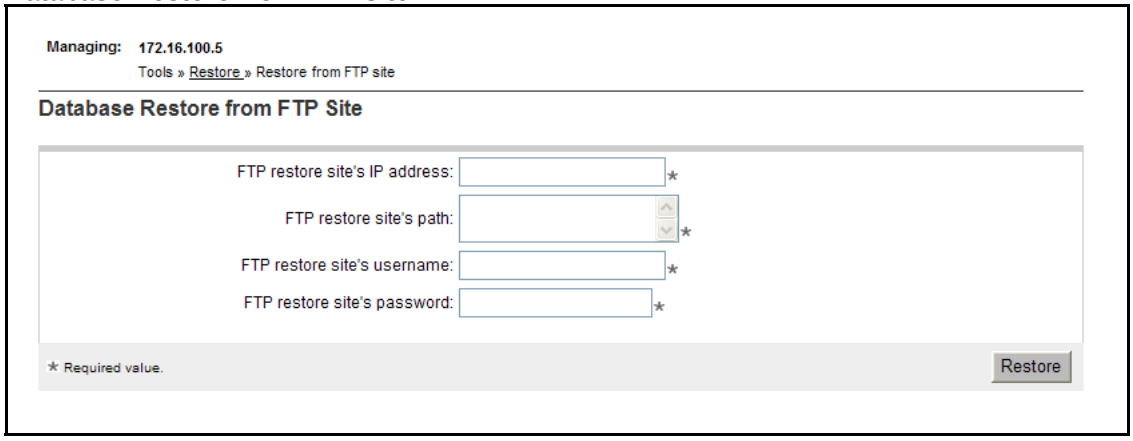
Use the following procedure to restore from a secure FTP site.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 70
Restoring from a secure FTP site

Step	Action
1	In the **NRS Manager Navigator** select **Tools > Restore.** The **Database Restore** Web page appears as shown in Figure 148 "Database Restore web page" (page 298).
2	Select **FTP site** from the **Restore from** drop-down list.
3	Click the **Restore** button. The **Database Restore from FTP Site** Web page appears as shown in Figure 153 "Database Restore from FTP site" (page 301).

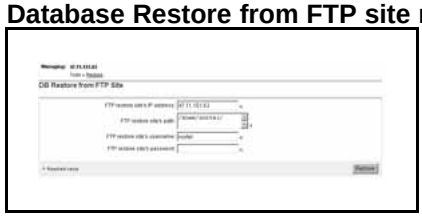
Figure 153
Database Restore from FTP site



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 154 "Database Restore from FTP site results" (page 302). The **Download the latest log file** link also appears on the web page. See Procedure 72 "Downloading the latest restore log file" (page 303) for downloading the restore log file.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 154
Database Restore from FTP site results



--End--

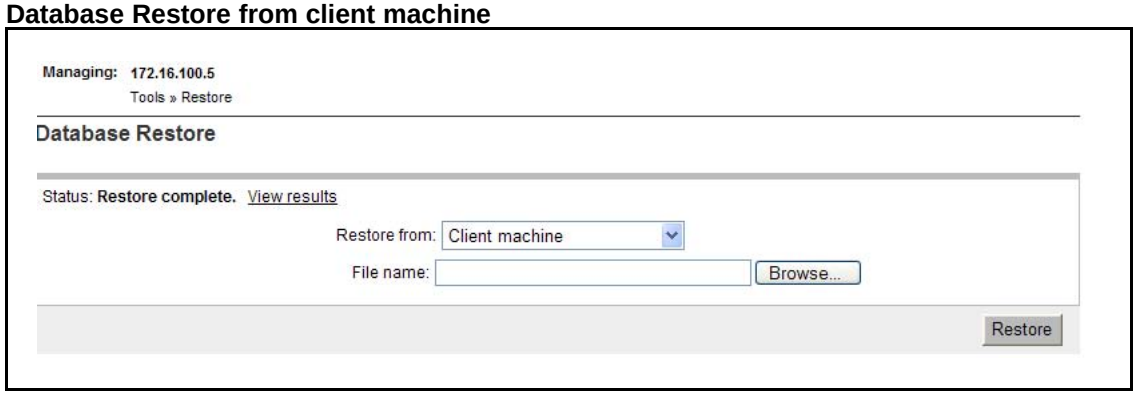
Restore from a client machine

Use the following procedure to restore from a client machine.

Procedure 71
Restoring from a client machine

Step	Action
1	In the **NRS Manager Navigator** select **Tools > Restore.** The **Database Restore** Web page appears as shown in Figure 148 "Database Restore web page" (page 298).
2	Select **Client machine** from the **Restore from** drop-down list. See Figure 148 "Database Restore web page" (page 298). The **Database Restore** Web page appears as shown in Figure 155 "Database Restore from client machine" (page 302).

Figure 155
Database Restore from client machine



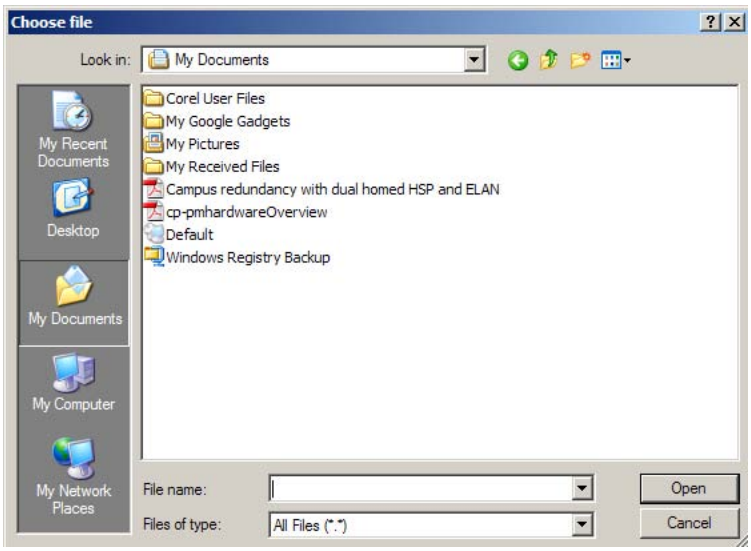
3	Click **Browse** to navigate to the folder containing the backup file.

Note: In Internet Explorer version 8 and later, the text box to input file name is disabled due to security reasons. The path needs to be specified using the Browse button.

The **Choose file** dialog window opens.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 156
Choose file dialog window



4 Select the backup file, and click **Open**.

The **File name** text box auto-fills with the path and filename of the backup file.

5 Click the **Restore** button.

--End--

Note: During a 'Restore' operation it is not allowed to do a 'reboot' of the system. In case the system goes down due to reasons such as power failure, it is recommended that the restore operation be restarted again.

Download the latest restore log file

Use the following procedure to download the latest restore log file.

Procedure 72
Downloading the latest restore log file

Step	Action
1	NRS Manager provides the option to restore the database from three source locations:

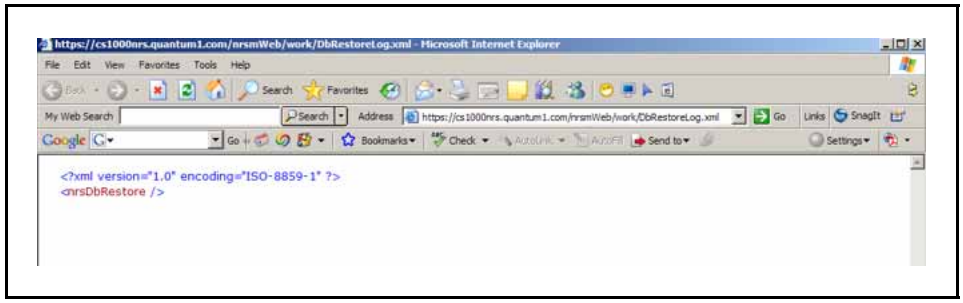
Copyright © 2010 Nortel Networks. All Rights Reserved.

- See Procedure 69 “Restoring from the connected Signaling Server” (page 298) to restore the database from the **Connected Signaling Server**.
- See Procedure 70 “Restoring from a secure FTP site” (page 301)to restore the database from a secure **FTP site**.
- See Procedure 71 “Restoring from a client machine” (page 302) 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 157 "Restore log file" (page 304). The name of the log file is DbRestoreLog.xml. The DbRestoreLog.xml file contains information about the database restore.

Figure 157
Restore log file



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, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

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 UCM Common Services Security Domain to assure a highly available authentication and authorization service for OA&M users

Copyright © 2010 Nortel Networks. All Rights Reserved.

who need to access managed systems/elements in the UCM Common Services Security Domain, as well as for auxiliary applications that rely on continuous availability of the UCM Common Services 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 119) and "Installation of Linux operating system, UCM Common Services and NRS application" (page 120).

  This step has four substeps:

  a. 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 UCM Common Services.

  d. Create user accounts and assign roles and permissions for access to the Primary and Secondary NRS servers from the UCM Common Services.

  Linux Platform Base and Applications Installation and Commissioning (NN43001-315) for detailed information on installing the Linux operating system, the UCM Common Services, the NRS and the Primary and Backup Security Services.

  For information about adding a managed element to the UCM Common Services, creating user accounts, and assigning roles and permissions for access to the NRS server from the UCM Common Services, see *Unified Communications Management* (NN43001-116).
- Adding a Service Domain and Level 1 domain using NRS Manager. (These two domains do not exist in the CS 1000 Release 3.0 Gatekeeper.) See Procedure 10 "Adding a Service Domain" (page 180) to add a Service Domain . See "Manage a Level 1 Domain (UDP)" (page 186) 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

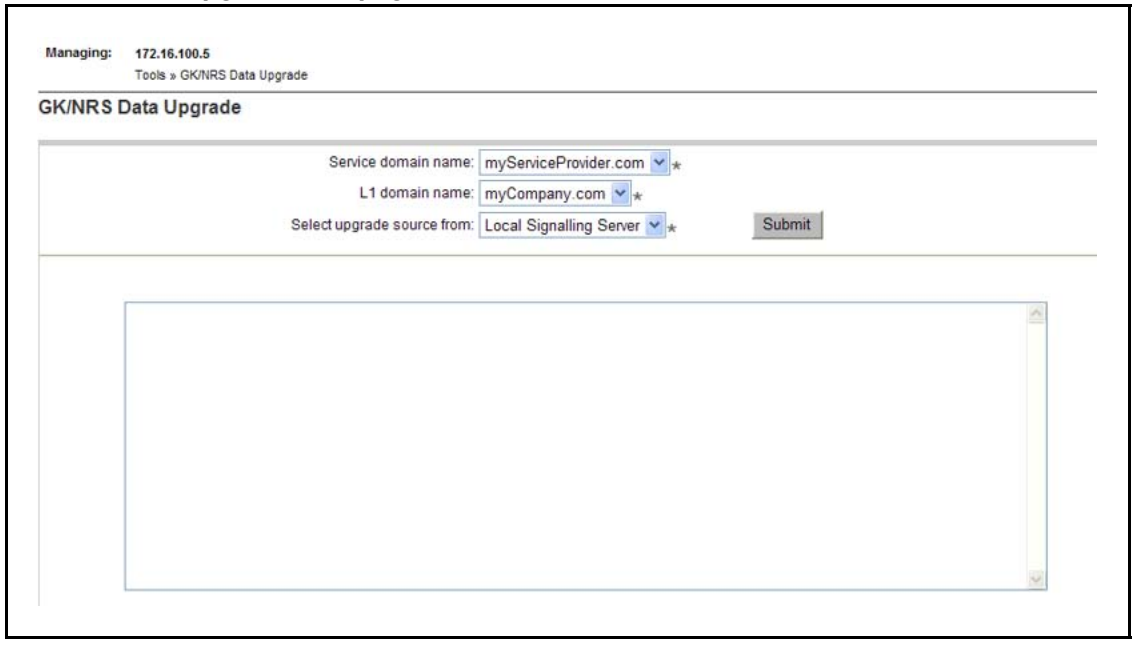
The converted H.323 Gatekeeper database is stored in the NRS standby database. Changes made to the standby database do not immediately effect call processing. Before changes made to the standby database effect call processing, database **Cut over** and **Commit** commands must be executed. See "Perform NRS database actions" (page 286).

See Procedure 60 "Cutting over the database" (page 288) to perform a database **Cut over** . See Procedure 63 "Committing the database" (page 290) to perform a database **Commit**.

Note: Only users with administrator privileges can execute Gatekeeper/NRS (GK/NRS) data conversion.

Figure 158 "GK/NRS Data Upgrade web page" (page 306) and Figure 159 "GK/NRS Data Upgrade results" (page 307) are only for illustration purposes, to show the user interface for the Gatekeeper to NRS Upgrade area in NRS Manager.

Figure 158
GK/NRS Data Upgrade web page



Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 159
GK/NRS Data Upgrade results

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

“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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Nortel Communication Server 1000

Network Routing Service Fundamentals

Release: 7.0
Publication: NN43001-130
Document revision: 02.01
Document release date: 4 June 2010

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

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

All other trademarks are the property of their respective owners.

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

www.nortel.com