Avaya Network Routing 2.0

Installation and Configuration

Document ID 585-810-101
Issue 2.0
April 2004
Compas ID 100004

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer

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

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites and does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

http://www.avaya.com/support

Preventing toll fraud

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

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Providing telecommunications security

Telecommunications security (of voice, data, and video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or person working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Use (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including, but not limited to, human and data privacy, intellectual property, material assets, financial resources, labor costs, and legal costs).

Your responsibility for your company's telecommunications security

The final responsibility for securing both this system and its networked equipment rests with you, an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources, including, but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

Trademarks

Avaya and MultiVantage are trademarks of Avaya Inc.

DEFINITY is a registered trademark of Avaya, Inc.

All non-Avaya trademarks are the property of their respective owners.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1-800-344-9670 in the United States. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Avaya Network Routing 2.0
Installation and Configuration

Contents

Preface 7

Audience 7
Reasons for reissue 7
Organization 8
Related documents 9
Support 10
Frequently asked questions (FAQs) 10
Customer support for the United States 10
Technician support for the United States 10
Customer and technician support outside the United States 10

Installing the Network Routing servers 11

NRS requirements 12
Site requirements 13
Installing the server 14
Unpacking the server 14
Installing an interface card 15
Installing a T1-SS7 interface card 15
Installing an X.25 interface card 16
Verifying the disk configuration 16
Installing the server and connecting power 16
Connecting to the network 17
Prerequisites 17
Cabling diagram 17
Connecting a monitor, keyboard, and mouse 18

Setting up the Network Routing servers 19

Prerequisites 20
Setting up the basic configuration and installing the application software 21
Logging on, starting the Linux desktop, and changing the root password 21
Setting up the network configuration 22
Setting up the MCI NIC configuration 24
Services setup 25
Installing the MCI encryption key file 26
Verifying that the configuration is complete 26
Rebooting the server 27
Verifying that you can access the server remotely 27

Assigning the administrator password 28
Setting up database synchronization 29
Preparing the system for database synchronization 29
Configuring database synchronization 32

Connecting and configuring the interface cards 35

Connecting and configuring the T1 MPAC for AT&T 36
Connecting the T1 card 36
T1 MPAC status LEDs 37
Configuring the AT&T SS7 point codes 38
Connecting the dual NIC for MCI 41
Connecting and configuring the X.25 card for Sprint 42
Connecting the X.25 card 42
Configuring the Sprint X.25 card 43

Accessing the system and administering users 45

Prerequisites 45
Administrator requirements 46
Logging in 46
Administering users 49
Adding a user 49
Resetting a user password 50
Changing user access permissions 50
Changing a user password aging interval 51
Deleting a user 51
Changing your password 52
Logging out 52

Configuring links to a Network Gateway 53

Network Gateway link options for AT&T 54
Network Gateway link options for MCI 55
Network Gateway link options for Sprint 56
Adding a Network Gateway link 57
Changing a Network Gateway link 58
Removing a Network Gateway link 59

Configuring CC links, IP trunks, and vectors 61

Prerequisite CC administration 62
Software load 62
Customer options 63
Configuring a CC link on the NRS 64
CC link options 64
Adding a CC link 65
Changing a CC link 66
Removing a CC link 66

Administering node names and IP addresses 67
Administering IP trunks from each CC to the NRS 69
Administering status polling vectors and VDNs on each CC 76
Saving translations 78

Configuring polling groups and network applications 79

Configuring polling groups 80
Polling group options 80
Adding a polling group 81
Changing a polling group 82
Removing a polling group 82
Configuring network applications 83
Network application options 83
Adding network applications 86
Changing network applications 87
Removing network applications 88
Configuring ANI groups 89
ANI group options 89
Adding an ANI group 90
Changing an ANI group 90
Removing an ANI group 91
Configuring CED groups 92
CED group options 92
Adding a CED group 93
Changing a CED group 93
Removing a CED group 94
Completing the initial configuration 95
Manually synchronizing the NRSs 95
Backing up the configuration 96
Providing TCP/IP ports to the customer 96

Monitoring system status 97

General monitoring strategy 98
Status tab pages 99
Overall system status 100
General status 101
Route and CC status 101
CC and Network Gateway status 102
System alarms and events 103
CC performance 104
Call log 106
General alarms and events 108
Interface alarms 111
Hardware diagram 115
Setting the refresh rate for the System Status and Hardware Diagram tabs 117
Changing the date format 117

Generating historical reports 118
Report graph characteristics 118
Request number reports 119
Destination label reports 120
CC reports 121
Network application reports 122
Polling group reports 123
Printing reports 124
Configuring e-mail alerts 125
E-mail alert options 125
Adding recipients to the e-mail alert database 126
Changing e-mail alert user parameters 126
Deleting recipients from the e-mail alert database 127

Ongoing configuration, maintenance, and troubleshooting 129

Updating the configuration 130
Adding CCs 130
Adding VDNs and vectors 130
Adding network applications 131
Adding destinations 131
Manually synchronizing the NRSs 131
Scheduling configuration updates 132
Setting a one-time update 132
Setting a frequent update 132
Setting a weekly update 133
Setting a monthly update 133
Updating an event 134
Deleting an event 134
Backing up the NRS 135
Restoring the NRS 135
Stopping and restarting the Distribution Manager application on an NRS 136
Stopping and restarting the Informix application on an NRS 137
Rebooting an NRS 138
Shutting down an NRS 139
Upgrading the application software 140
Troubleshooting 141
Viewing log files 141
Monitoring the Alarm Interface tab 141
Problem scenarios 142
Application out of service 142
Timeouts 142

Glossary 143

Index 147

Preface

This document describes how to install, access, configure, and maintain the Distribution Manager call routing database and Network Gateway applications of the Avaya Network Routing feature. This document also describes how to administer Best Service Routing (BSR) polling on Avaya Contact Centers (CCs).

Audience

This document is written for Avaya Implementation Services Organization (ISO) personnel and customer administrators who install, configure, monitor, and maintain the Network Routing feature.

Reasons for reissue

This is Issue 2.0 of this document. The following changes were made for Issue 2.0:

- Since this document contains a variety of hardware and software installation and configuration procedures, the title has been changed to read *Avaya Network Routing 2.0 Installation and Configuration*.
- Other changes will be listed.

Organization

This document consists of the following sections:

- Installing the Network Routing servers on page 11 describes how to install the network routing servers (NRSs), including installation of the hardware and the software applications.
- Setting up the Network Routing servers on page 19 describes how to initially configure the NRSs.
- Connecting and configuring the interface cards on page 35 describes how to install, connect, and configure the interface cards.
- Accessing the system and administering users on page 45 describes how to access the NRS, log in to the application, administer users, change passwords, and log out of the application.
- Configuring links to a Network Gateway on page 53 describes how to configure the link from the NRS to the Network Gateway server.
- Configuring CC links, IP trunks, and vectors on page 61 describes how to configure the links from the NRS to the CCs, trunks between the CCs in the configuration and the NSR, and vectors.
- Configuring polling groups and network applications on page 79 describes how to configure polling groups and network applications.
- Monitoring system status on page 97 describes how to monitor system performance and run reports.
- Ongoing configuration, maintenance, and troubleshooting on page 129 describes how to make configuration updates, back up configuration data, and troubleshoot problems.
- Glossary on page 143

Related documents

See the following documents for more information about Network Routing and related features:

Title	Number
Avaya Network Routing 2.0 Documentation Library	585-810-601
Avaya Network Routing 2.0 Overview	585-810-001
Avaya Network Routing 2.0 Installation and Configuration	585-810-101
Avaya MultiVantage Call Center Software Call Vectoring and Expert Agent Selection (EAS) Guide	555-230-714
Avaya MultiVantage Call Center Software Guide to ACD Call Centers	555-230-716
Avaya Communication Manager Call Center Call Vectoring and Expert Agent Selection (EAS) Guide	555-245-783
Avaya Communication Manager Guide to ACD Call Centers	555-245-784

Support

If you need assistance with a problem, use the support information and help lines presented below.

Frequently asked questions (FAQs)

For solutions to common problems, customers and Avaya technicians can access technical support FAQs at:

http://www.avaya.com

Select **Support > Call Center/CRM** and select the product for which you need support. Please check this information before you call in a trouble ticket. Doing so could save you time and money.

Customer support for the United States

Customers can report problems and generate trouble tickets by calling:

1-800-344-9670

The customer is prompted to identify the type of problem (that is, Automatic Call Distribution, hardware, or Avaya CMS) and is then connected to the appropriate service organization.

Technician support for the United States

Avaya technicians can receive help by calling:

1-800-248-1234

Customer and technician support outside the United States

For customer and technician support outside the United States, see the Avaya Web site:

http://www.avaya.com

Select **Support > Escalation Lists US and International**. For escalation telephone numbers outside the United States, select **Global Escalation List**.

Installing the Network Routing servers

This section describes how to install the NRSs. For all configurations, there are two servers to install. The procedures for installing each server are the same.

The information in this chapter includes the following:

- NRS requirements on page 12
- Site requirements on page 13
- Installing the server on page 14
- Connecting to the network on page 17
- Connecting a monitor, keyboard, and mouse on page 18

NRS requirements

The NRS has the following characteristics:

- IBM 345 computer (or approved equivalent), dual 2.0 GHz Xeon CPUs (minimum), 768 MB RAM (minimum)
- Redundant disk drives (18 GB minimum) set up as RAID 1
- Redundant power supplies
- Interface cards:
  - T1-SS7 Multiple Protocol Access Card (MPAC) for AT&T (installed on-site and requires a full-length PCI slot)
  - Dual Network Interface Card (NIC) for MCI (preinstalled at the factory)
  - X.25 interface card for Sprint (installed on-site)
- Red Hat Linux Professional - Version 8.0 (minimum) operating system, the Apache Httpd daemon, and Java support (preinstalled at the factory)
- IBM Informix Dynamic Server - Workgroup Edition, Version 9.40 (preinstalled at the factory)
- Distribution Manager and Network Gateway applications, which provide the Web-based Java interface for administration, configuration, and maintenance (preinstalled at the factory)

Note:

A monitor, keyboard, and mouse required. These must be provided by the customer. The monitor, keyboard, and mouse can be shared with other servers using a KVM switch.

Site requirements

Follow these site requirements when installing the NRSs:

- The servers must be installed in a secure area equipped to support computer equipment. The equipment rack or cabinet must be in place before installing the NRS.

  SECURITY ALERT:
  Equipment not installed in a secure area is subject to unauthorized access. Avaya recommends that you install the servers in a secure location.

- The IBM 345 servers have a 2U form factor for rack installations (H 3.36" x W 17.5" x D 27.5"; H 8.6cm x W 44.9cm x D 70.5cm). If you use a different server, verify that you have room for proper installation.
- The servers must be able to connect to the customer LAN so that the servers can communicate with the CCs. Verify that the customer network was analyzed to support the Network Routing traffic before installing any servers.
- The customer must supply all required TCP/IP addresses, gateways, domain name servers (DNS), desired machine names, domains, and routing information before you begin the installation.
- The customer LAN must support 100Base-T network hubs or switches. The cabling must support category 5 (100 Mbps).
- The servers must be able to connect to the service provider equipment (T1 for AT&T, NIC for MCI, X.25 for Sprint).
- Each IBM 345 server requires two 110 V AC, nonswitched power outlets. Avaya recommends that you provide uninterruptible power for each server and *all related equipment* (for example, using a UPS). Connect the power cords from the NRS to different UPS units whenever possible for proper redundancy. If you use a different server, verify that you have enough power outlets to support the server.
- You must have a monitor that supports 1024 x 768 pixels, a standard U.S. keyboard, and a PS2 mouse (3-button preferred, but not required).
- Avaya recommends that you have redundant router and UPS configurations.

Installing the server

This section describes how to unpack the server, install an interface card (AT&T or Sprint), install the server, and connect power. The procedures in this section must be done for both servers.

This section includes the following topics:

- Unpacking the server on page 14
- Installing an interface card on page 15
- Verifying the disk configuration on page 16
- Installing the server and connecting power on page 16

Unpacking the server

To unpack the server:

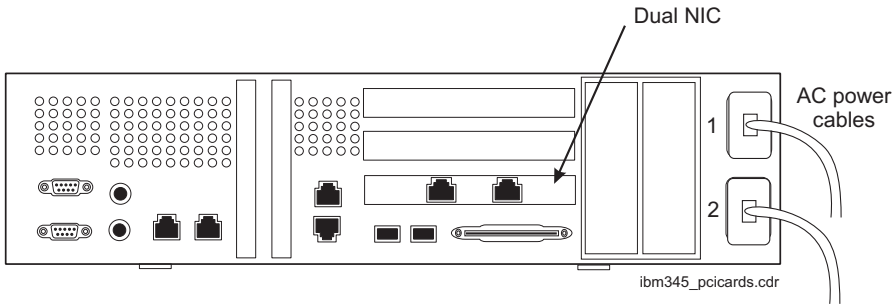
Note:

This procedure is based on using the IBM 345 server. If you are using a different server, follow the installation instructions for your server, using these instructions as general guidelines.

1. Unpack the server.
2. Verify that you received all required parts.
3. Confirm that the equipment room is adequate to support the installation (see Site requirements on page 13).

Installing an interface card

The server comes from the factory with a dual NIC installed in the bottom horizontal PCI slot. See the following figure:



The dual NIC is used for the MCI interface. If you are using the MCI interface, you can continue with Installing the server and connecting power on page 16.

If you are using the AT&T interface or Sprint interface, you must install a special interface card as described in the following topics:

- Installing a T1-SS7 interface card on page 15
- Installing an X.25 interface card on page 16

Important:
If your server came from the factory with the AT&T or Sprint interface card already installed, you may only have to configure the card.

Installing a T1-SS7 interface card

To install a T1-SS7 interface card:

1. Attach one end of an ESD antistatic wrist strap to the chassis of the server and attach the other end to your wrist.
2. Remove the cover on the server.
3. On the T1-SS7 card, locate the rotary switch used to configure the card ID. Set the card ID to 0.
4. Select an empty, full-length PCI slot. Use one of the two available horizontal PCI slots.
5. Install the T1-SS7 card in the empty slot.
6. Replace the cover on the server.
7. Remove the ESD wrist strap.

Installing an X.25 interface card

To install an X.25 interface card:

1. Attach one end of an ESD antistatic wrist strap to the chassis of the server and attach the other end to your wrist.
2. Remove the cover on the server.
3. Select an empty PCI slot. Use one of the two available horizontal PCI slots. You do not need to use a full-length PCI slot.
4. Install the X.25 card in the empty slot.
5. Replace the cover on the server.
6. Remove the ESD wrist strap.

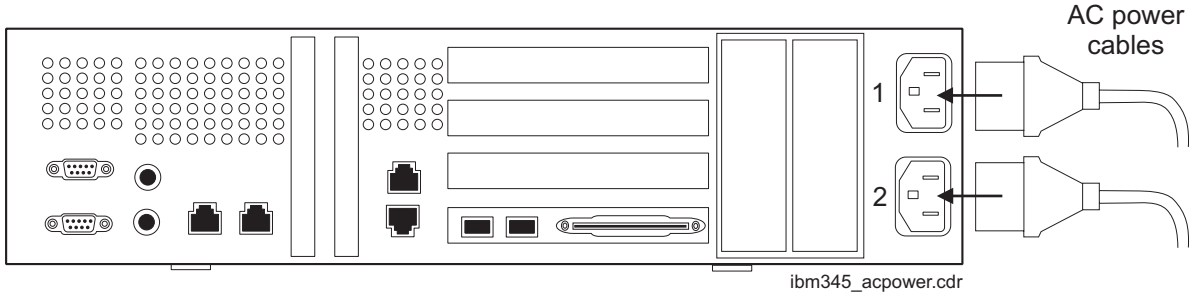
Verifying the disk configuration

When the server comes from the factory, the server should have disks installed in the first two slots in the front of the server. Verify that only two disks are installed in the server. If a third disk is installed, remove that disk before you power-up the server. Save this third disk to create a backup of the system and data files.

Installing the server and connecting power

To install the server and connect power:

1. Install the server in an equipment rack. If not using a rack, install the server in an appropriate location.
2. Connect two AC power cords from each server to separate, dedicated, nonswitched 110V AC power outlets on separate UPS units. See the following figure.



Connecting to the network

This section describes how to connect the NRSs to the customer network.

This section includes the following topics:

- Prerequisites on page 17
- Cabling diagram on page 17

Prerequisites

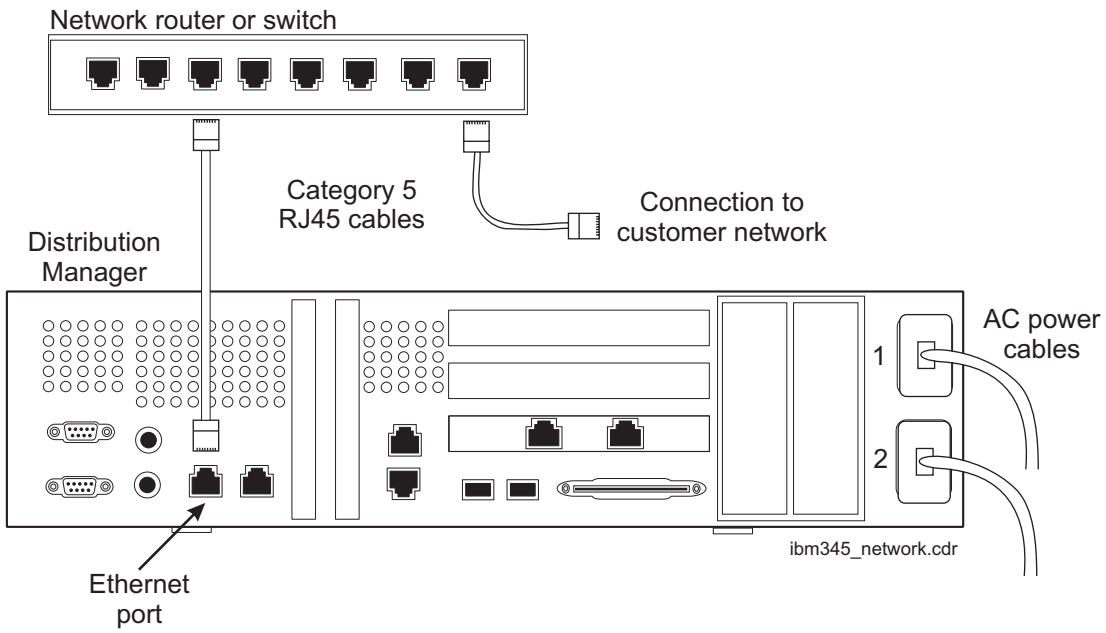
Verify that the CCs that are part of the Network Routing configuration are connected and administered as part of the customer network.

Cabling diagram

Use the following diagram when connecting the NRSs to the customer network. Avaya recommends that you use a different router or switch with each NRS for redundancy. This will help avoid a single point of failure.

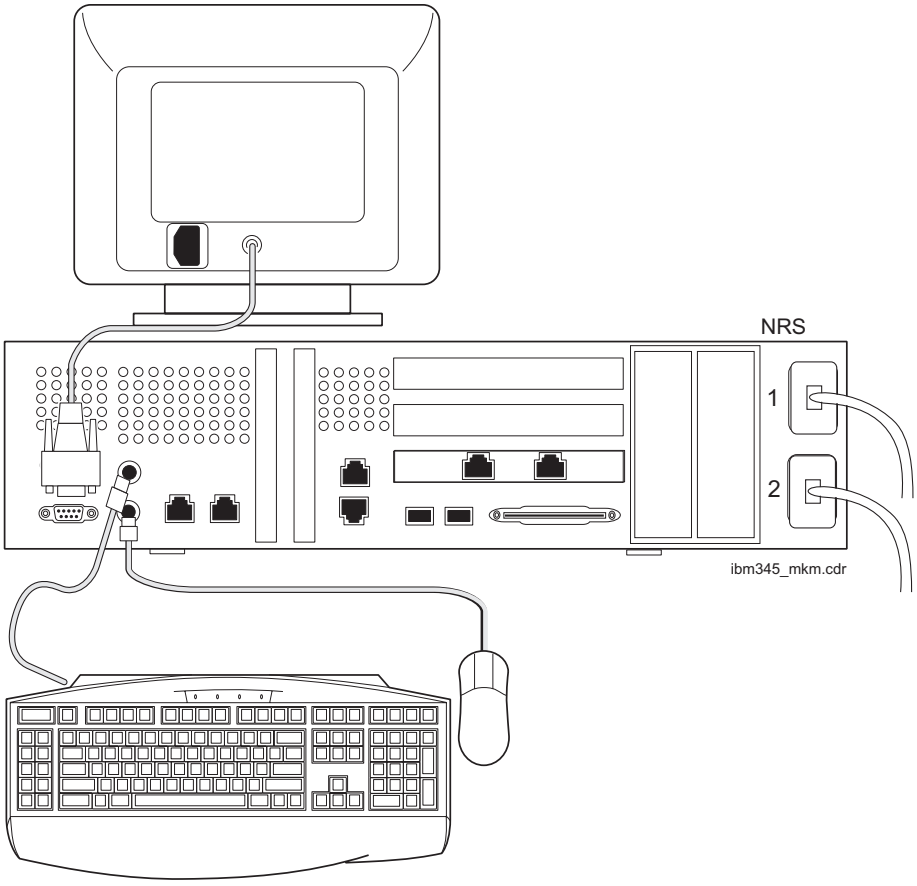
Note:

The network routers, switches, and cables are provided by the customer.



Connecting a monitor, keyboard, and mouse

Using equipment provided by the customer, connect a monitor, keyboard, and mouse to each NRS. A single monitor, keyboard, and mouse can be shared with each NRS using a KVM switch. See the following figure.



Setting up the Network Routing servers

This section describes how to set up the NRSs. The Linux operating system provides a graphical user interface (GUI) for system setup. This method requires that you connect a monitor, keyboard, and mouse to the NRS.

Important:
You must do all of the procedures in this chapter on both NRSs.

This section includes the following topics:

- Prerequisites on page 20
- Setting up the basic configuration and installing the application software on page 21
- Assigning the administrator password on page 28
- Setting up database synchronization on page 29

Prerequisites

Before you set up the NRSs, collect the following information:

- A valid static IP address for each NRS, provided by the customer. This should be a valid external static network address, not an internal or Network Address Translation (NAT) address.
- A subnet mask for each NRS, provided by the customer.
- A default gateway address for each NRS, provided by the customer.
- The machine names for the NRSs, provided by the customer.
- For AT&T, the point code setup.
- For MCI, the decrypted **`SessionKeys.dat`** file that is unique for each customer, the MCI NIA IP address, gateway address, and network mask for each NRS, the subnet route parameters for MCI RDG subnet isolation, and the MCI RDG TCP/IP addresses and port numbers.
- For Sprint, the slot number and bus number will need to be determined after installation of the X.25 board.
- The Avaya Secure Network Access feature.

Setting up the basic configuration and installing the application software

The Linux operating system provides a GUI for system setup. This method requires that you connect a monitor, keyboard, and mouse to the NRS.

This section includes the following topics:

- Logging on, starting the Linux desktop, and changing the root password on page 21
- Setting up the network configuration on page 22
- Setting up the MCI NIC configuration on page 24
- Services setup on page 25
- Installing the MCI encryption key file on page 26
- Verifying that the configuration is complete on page 26
- Rebooting the server on page 27
- Verifying that you can access the server remotely on page 27

Logging on, starting the Linux desktop, and changing the root password

Before you set up the NRS, you must log in as root, start the Linux desktop, and change the root password.

SECURITY ALERT:
You *must* change the default root password immediately after logging in the first time.

To log in as root and change the root password when a monitor, keyboard, and mouse is connected to the server:

1. Turn on power to the NRS and the monitor.
2. At the login prompt, enter:

   `root`
3. At the password prompt, enter:

   `avaya`

   A warning message about logging in as root is displayed.

4. Click **OK**.

   The Linux desktop is displayed.

5. In the lower left corner of the window, click the terminal emulation program icon.

   A Linux terminal window is opened.

6. In the terminal window, enter:

   passwd

   You are prompted to enter a new password.

7. Enter a new password.

   SECURITY ALERT:
   Passwords must be from 5 to 20 characters long and should be a combination of letters and numbers. It is critical that you secure the password for the root login ID.

   You are prompted to reenter the new password.

8. Reenter the new password.

   If you reentered the new password correctly, the password is changed. If you mistyped the new password, you must repeat this procedure.

9. Check the current date and time on the server. If it is not correct, set the correct date and time.

10. Continue with Setting up the network configuration on page 22.

Setting up the network configuration

You must configure the ethernet port, IP address, and host name on the NRS so it can be accessed over the customer's network. These are often configured at the factory. Check the current network settings and update only as needed.

SECURITY ALERT:
When setting up IP access to the server, Avaya recommends that you use security products such as VPNs and firewalls to limit access to the servers to authorized personnel.

To set up the network configuration:

1. Click the Red Hat icon.
2. Move the cursor to the **System Settings > Network** selection.
3. Click the **Network** selection.

   The **Network Configuration** dialog box is displayed.

4. Select the **Devices** tab.
5. Highlight the eth0 device and click **Edit**.

   The **Ethernet Device** dialog box is displayed.
6. Select the **General** tab.
7. Select **Activate device when computer starts**.
8. Select **Statically set IP addresses**.
9. In the **Manual IP Address Settings** group box, enter the IP address, subnet mask, and default gateway address for the server.
10. Click **OK**.

    The **Network Configuration** dialog box is displayed.
11. Select the **Hosts** tab.
12. Click Add.

    The **Add/Edit Hosts entry** dialog box is displayed.
13. In the **Address** field, enter the IP address of the server.
14. In the **Hostname** field, enter a host name for the server. Select a meaningful name.
15. Click **OK**.

    The **Network Configuration** dialog box is displayed.
16. Click **Apply**.
17. Click **Close**.

    The **System Settings** window is displayed.
18. Do one of the following:
    - If you are using the MCI Network Gateway, continue with Setting up the MCI NIC configuration on page 24.
    - If you are using the AT&T or Sprint interfaces, continue with Services setup on page 25.

Setting up the MCI NIC configuration

You must configure the PCI NIC for the MCI network interface.

SECURITY ALERT:
When setting up IP access to the server, Avaya recommends that you use security products such as VPNs and firewalls to limit access to the servers to authorized personnel.

To configure the NIC for the MCI network interface:

1. Click the Red Hat icon.
2. Move the cursor to the **System Settings > Network** selection.
3. Click the **Network** selection.

   The **Network Configuration** dialog box is displayed.
4. Select the **Devices** tab.
5. Highlight an available ethernet device and click **Edit**. This can be any unused ethernet device on the PCI ethernet NIC.

   The **Ethernet Device** dialog box is displayed.
6. Select the **General** tab.
7. Select **Activate device when computer starts**.
8. Select **Statically set IP addresses**.
9. In the **Manual IP Address Settings** group box, enter the IP address, subnet mask, and default gateway address for the MCI network interface.
10. Click **OK**.

    The **Network Configuration** dialog box is displayed.
11. Select the **Route** tab.
12. Click the **Add** button to add the **Static Network Route** for the MCI interface. You will need to enter the Destination Network, Netmask, and the Gateway for the Destination Network.
13. Select the **Hosts** tab.
14. Click **Add**.

    The **Add/Edit Hosts entry** dialog box is displayed.
15. In the **Address** field, enter the static IP address for the MCI network interface.
16. In the **Hostname** field, enter a host name for the MCI network interface. This name will be provided by MCI.

17. Click **OK**.

    The **Network Configuration** dialog box is displayed.

18. Click **Apply**.

19. Click **Close**.

    The **System Settings** window is displayed.

20. Continue with Services setup on page 25.

Services setup

To verify that the HTTP service is operating and that Sendmail has been disabled:

1. Open a terminal window.
2. Enter:

   `ps -ef | grep http`

   Messages similar to the following are displayed:

```
root       684     1  0  2003 ?        00:02:04 /usr/sbin/httpd
apache   14693   684  0 Feb29 ?        00:00:00 /usr/sbin/httpd
apache   14694   684  0 Feb29 ?        00:00:00 /usr/sbin/httpd
apache   14695   684  0 Feb29 ?        00:00:00 /usr/sbin/httpd
apache   14696   684  0 Feb29 ?        00:00:00 /usr/sbin/httpd
apache   14697   684  0 Feb29 ?        00:00:00 /usr/sbin/httpd
apache   14698   684  0 Feb29 ?        00:00:00 /usr/sbin/httpd
apache   14699   684  0 Feb29 ?        00:00:00 /usr/sbin/httpd
apache   14700   684  0 Feb29 ?        00:00:00 /usr/sbin/httpd
root     25281 25244  0 21:42 pts/0    00:00:00 grep http
```

3. If the HTTP service is not operating:

   a. Click the **Control Panel** icon.

      The **System Settings** window is displayed.

   b. Select **Services**. Verify that httpd has been checked (enabled) for run levels 3 and 5. If not, then click to enable httpd.

   c. Verify that Sendmail has been disabled (unchecked) for run levels 3 and 5. If not, uncheck it for run levels 3 and 5.

   d. Select **OK** to save the settings.

4. Do one of the following:

   - If you are using the MCI Network Gateway, continue with Installing the MCI encryption key file on page 26.

- If you are using the AT&T or Sprint interfaces, continue with Verifying that the configuration is complete on page 26.

Installing the MCI encryption key file

To generate the **SessionKeys.dat** file, MCI will deliver two files to the customer and/or Avaya. The two files delivered by MCI are:

- the encrypted session keys file
- the Master Key file, which is required in order to decrypt the session keys file

These two files are delivered to the Avaya implementation team who will then decrypt them and create the **SessionKeys.dat** file. The SessionKeys.dat file must be installed under the **/export/dm** directory of each NRS.

Verifying that the configuration is complete

To verify that the configuration is complete, verify that the application software has been installed at the factory. Check for the following directories:

- **/export/dm** - common components directory
- **/export/att** - AT&T interface directory. If this is an AT&T deployment, there will be files and three other subdirectories (**etc**, **bin**, **run**) shown under this directory.
- **/export/mci** - MCI interface directory. If this is an MCI deployment, there will be files shown under this directory.
- **/export/sprint** - Sprint interface directory. If this is a Sprint deployment, there will be files shown under this directory.

If these files are not installed, escalate to Avaya technical support. If these files are installed, continue with Rebooting the server on page 27.

Rebooting the server

After setting up the network and Internet configuration, you must reboot the server.

Note:

During reboot, the system may display a screen and message that says hardware has been removed or new hardware detected. This is caused by variations in keyboards, mice, and monitors. Normally, Red Hat Linux detects these changes correctly and you only have to verify or acknowledge the changes. This message should be acknowledged. Otherwise, each time the server is rebooted, it will delay or wait for a response to the detected changes.

To reboot the server:

1. Change focus to the terminal emulation window.
2. Enter:

   `reboot`

   The server reboots.
3. Continue with Verifying that you can access the server remotely on page 27.

Verifying that you can access the server remotely

After the server reboots, you must verify that the Secure Network Access Service has been installed and is operating so that Avaya can access the server remotely for ongoing maintenance.

Verify that the following services are available to both NRSs:

- telnet
- FTP
- VNC
- Web browser access, which can only be verified after all configuration parameters have been set and checked.

Note:

When accessing the server locally from the console, you can log in as either **`informix`** or **`root`**. For security reasons, the **`root`** user ID is not enabled for **`telnet`** or **`ftp`** access. When using **`telnet`**, you must log in first with the **`informix`** user ID and password, then use **`su - root`** to "superuse" as the root user ID, and enter the root password when prompted. For **`ftp`**, root access is not allowed.

Assigning the administrator password

After setting up the NRS, use the following procedure to assign the administrator password. This password must be given to the customer.

To assign the administrator password:

1. Connect a laptop computer to the LAN hub or switch that is connected to the NRS using a standard Category 5 LAN cable or use a PC that is connected to the customer's network.
2. Open a Web browser.

   You must use Microsoft Internet Explorer 5 or later or Netscape Navigator 6.2 or later and Java plug-in 1.4.0 or later.
3. In the address box, enter:

   `http://`*`IP_address`*`/`

   where ***`IP_address`*** is the IP address assigned to the NRS.

   Note:

   When you access the NRS for the first time, a Java plug-in may be downloaded to your PC. This is normal operation if your Web browser does not already have the plug-in.

   The **DM login** dialog box is displayed.
4. Enter the user name **`init`** and the password **`init`**.
5. Click **Log in**.

   A dialog box is displayed noting that an administrator user account must be created.
6. Click **Close**.

   The **Enter administrator password** dialog box is displayed.
7. Enter a password for the **admin** login ID.

   SECURITY ALERT:

   Passwords must be from 5 to 20 characters long and should be a combination of letters and numbers. Only a person using the **admin** login ID can add and remove users, so it is critical that you secure the password for this login ID.
8. Confirm the password by entering it a second time.
9. Select a password expiration interval. The administrator login defaults to no password expiration, but you can change it to expire in 30, 60, or 90 days.

10. Click **Submit**.

    A dialog box is displayed noting that an administrator account has been created.

11. Click **Close**.

Setting up database synchronization

Database synchronization is used to keep the common database configuration tables on both NRSs identical, regardless where configuration changes are being made. When database synchronization is configured and enabled, configuration changes made to one server are automatically copied to the other server.

There are two steps required to set up database synchronization:

- Preparing the system for database synchronization on page 29
- Configuring database synchronization on page 32

Preparing the system for database synchronization

Before you configure database synchronization, you must verify that the base setup for database synchronization has been done on both NRSs. Follow these procedures, editing any files that need editing, and adding any files that are missing.

During setup, the following files will be created or changed:

```
/etc/hosts
/etc/hosts.equiv
/opt/informix/etc/onconfig.avaya
```

Note:

In these instructions, the variables ***NRS1*** and ***NRS2*** represent the machine names for the local and remote NRSs, respectively. The variable ***IP_Address*** represents the IP address for the server.

To set up the NRSs for database synchronization on the local NRS:

1. Log in as `root` on the local NRS.
2. Enter:

   ```
   vi /etc/hosts
   ```

3. Verify that there are entries for both the local (***NRS1***) and remote (***NRS2***) machines. If they do no exist, add them. The entries must have the following format:

   ```
   IP_Address    NRS1
   IP_Address    NRS2
   ```

4. Press **Esc**.
5. Enter:

   :wq!

   This writes and quits the file.
6. Enter:

   vi /etc/hosts.equiv
7. Verify that there is an entry for remote NRS (***NRS2***). If it does not exist, add it. The entry must have the following format:

   ```
   NRS2
   ```

8. Press **Esc**.
9. Enter:

   :wq!

   This writes and quits the file.
10. Enter:

    vi /opt/informix/etc/sqlhosts
11. Verify that there are entries for both the local (***NRS1***) and remote (***NRS2***) machines. If they do no exist, add them. The entries must have the following format:

    ```
    dm1    onsoctcp    NRS1     5001
    dm2    onsoctcp    NRS2     5001
    ```

12. Press **Esc**.
13. Enter:

    :wq!

    This writes and quits the file.
14. Enter:

    vi /opt/informix/etc/onconfig.avaya
15. Find the line with DBSERVERALIASES.
16. Verify that dm1 is on the DBSERVERALIASES line separated by commas without any spaces. If they do no exist, add them. The entries must have the following format:

    ```
    DBSERVERALIASES    psa,dm1
    ```

17. Press **Esc**.
18. Enter:

    :wq!

    This writes and quits the file.
19. Stop and restart Informix and the database using the procedure described in Stopping and restarting the Informix application on an NRS on page 137.

To set up the NRSs for database synchronization on the remote NRS:

1. Log in as **root** on the remote NRS.
2. Enter:

    vi /etc/hosts
3. Verify that there are entries for both the local (***NRS1***) and remote (***NRS2***) machines. If they do no exist, add them. The entries must have the following format:

    IP_Address ***NRS2***
    IP_Address ***NRS1***
4. Press **Esc**.
5. Enter:

    :wq!

    This writes and quits the file.
6. Enter:

    vi /etc/hosts.equiv
7. Verify that there is an entry for local NRS (***NRS1***). If it does not exist, add it. The entry must have the following format:

    NRS1
8. Press **Esc**.
9. Enter:

    :wq!

    This writes and quits the file.
10. Enter:

    vi /opt/informix/etc/sqlhosts
11. Verify that there are entries for both the local (***NRS1***) and remote (***NRS2***) machines. If they do no exist, add them. The entries must have the following format:

    dm1 onsoctcp ***NRS1*** 5001
    dm2 onsoctcp ***NRS2*** 5001

12. Press **Esc**.
13. Enter:

    :wq!

    This writes and quits the file.
14. Enter:

    vi /opt/informix/etc/onconfig.avaya
15. Find the line with DBSERVERALIASES.
16. Verify that dm2 is on the DBSERVERALIASES line separated by commas without any spaces. If they do no exist, add them. The entries must have the following format:

    ```
    DBSERVERALIASES    psa,dm2
    ```
17. Press **Esc**.
18. Enter:

    :wq!

    This writes and quits the file.
19. Stop and restart Informix and the database using the procedure described in Stopping and restarting the Informix application on an NRS on page 137.

Configuring database synchronization

To configure database synchronization:

1. Log in with the **admin** login ID.
2. Click **File > DM Name and IP Address**.

   The **DM Name and IP Address** dialog box is displayed.
3. Populate the dialog box with values as described in the following table.

Option	Parameters	Notes
DM Name	Server name	Enter the name of the local NRS.
DM IP Address	Valid IP address	Enter the IP address of the local NRS.
DM Domain	Valid domain name	Enter the domain name where the NRS is located.
SMTP Mail Server	Valid domain name	Enter the name of the SMTP mail server on the customer's domain.

4. Click **Submit**.
5. Click **File > Remote DM Name and IP Address**.

   The **Remote DM Name and IP Address** dialog box is displayed.
6. Populate the dialog box with values as described in the following table.

Option	Parameters	Notes
Remote DM Name	Server name	Enter the name of the remote NRS.
Remote IP Address	Valid IP address	Enter the IP address of the remote NRS.
Synchronization	Active Inactive	Specifies whether database synchronization is currently active for this NRS. Avaya recommends that you designate one server as the local server and do all synchronization from the local server to the remote server.

7. Click **Submit**.

   The database synchronization parameters are set.
8. Log out and log back in. Verify that the remote NRS is in service. If the database synchronization is not working, escalate to Avaya technical support.

Connecting and configuring the interface cards

This section describes how to connect and configure the following interface cards used in the NRS:

- Connecting and configuring the T1 MPAC for AT&T on page 36
- Connecting the dual NIC for MCI on page 41
- Connecting and configuring the X.25 card for Sprint on page 42

Connecting and configuring the T1 MPAC for AT&T

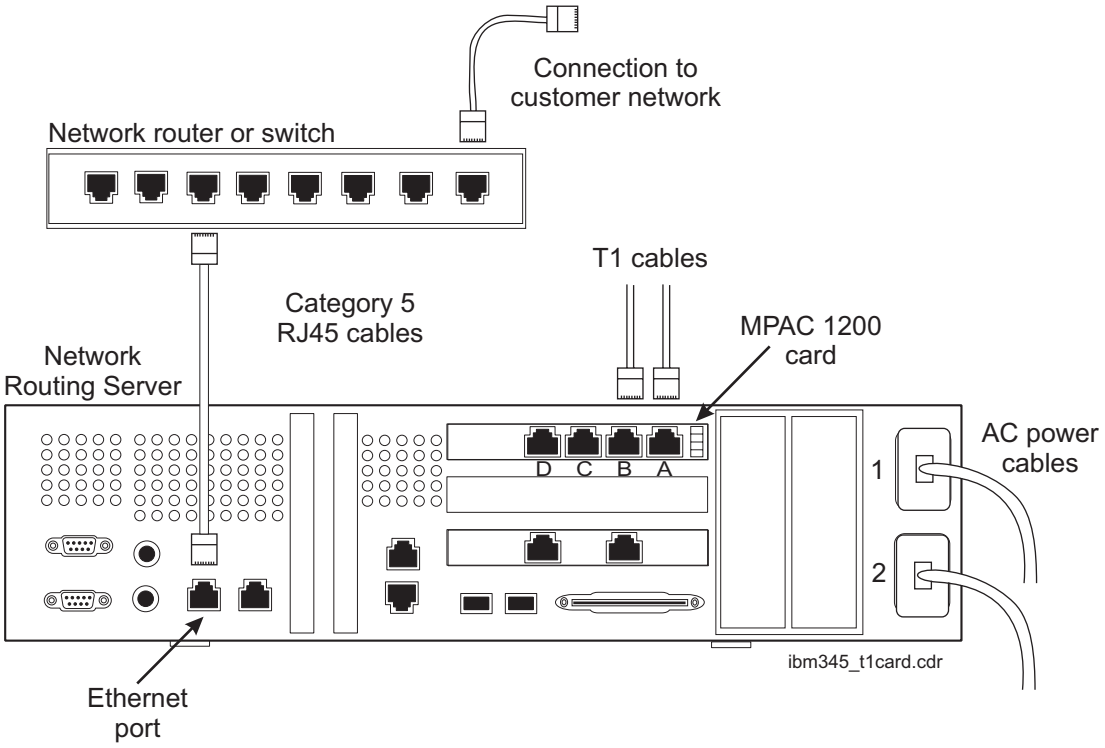
When interfacing the NRS to an AT&T network, you must connect and configure the T1 MPAC interface card.

This section includes the following topics:

- Connecting the T1 card on page 36
- T1 MPAC status LEDs on page 37
- Configuring the AT&T SS7 point codes on page 38

Connecting the T1 card

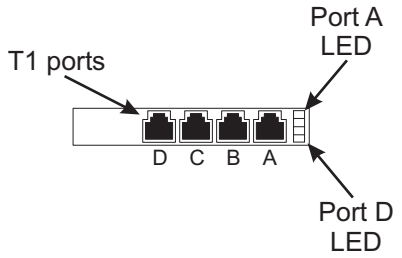
Use the following diagram when connecting the T1 cables to each NRS. In this example, you are connecting two T1 cables to ports A and B on the MPAC. The circuits for this connection can be AT&T 56 KB DDS circuits or AT&T Accunet 1.5 service.



T1 MPAC status LEDs

When configuring and connecting the T1 ports, the LEDs on the MPAC display the status of each port. Each status LED can display the colors green, yellow, and red in a variety of combinations.

The following figure shows the layout of the MPAC.



Before the T1 ports have been initialized, the status LEDs indicate the following:

LED status	Description
All LEDs off	The protocol software has not been downloaded to the card.
Slow chase sequence across all LEDs	The protocol software has been downloaded to the card.

Once the T1 ports have been initialized, the status LEDs indicate the following:

Dominant color[1]	Flashing color[1]	Description
Green	None	Aligned and operating normally.
Green	Yellow	The port is periodically losing alignment with the remote end. This usually indicates a timing problem in the system. Note that the flashing of the LED to yellow occurs in response to timing slips and may be irregular.
Green	Red	Synchronization has been achieved. However, there are framing errors.
Yellow	None	Receiving remote alarm signal from the remote end.
None	Yellow	Receiving remote alarm signal from the remote end and cyclic redundancy check is failing.

Dominant color[1]	Flashing color[1]	Description
Red	Green	Synchronization has been lost.
Red	None	The port is initialized but no signal is being received.
Blank	Red	Receiving Alarm Indicator Signal (AIS) from the remote end.

1. The "dominant" color is the main color that is shown most of the time. The "flashing" color is the color that occasionally flashes.

Configuring the AT&T SS7 point codes

After the server has been configured for the customer network, you must configure the point codes for the SS7 connections to support the AT&T ICP service. For the AT&T interface, the point code assignments must be requested from AT&T. This is done during the implementation planning meetings involving the customer, AT&T, and the appropriate Avaya associates.

The supported AT&T configuration is a mated pair with two NRSs. This provides link redundancy to each of the NRSs. Each NRS will have distinct point codes, which are identified by AT&T as CRPA (the "local" NRS) and CRPB (the "remote" NRS).

These point codes are delivered to the customer as ANSI 3 octets. You must convert these values to ITU-T 14 Bit format before you add them to the configuration file. There are three different point codes that must be set on each NRS. Within the **`milborne.cfg`** file, they are referenced as:

- Milborne Pointcode - This is the point code assigned to the MPAC card within the NRS (the customer/Avaya side of the network).
- STP 1 - The point code assigned to the primary linkset for this NRS.
- STP 2 - The point code assigned to the secondary linkset for this NRS.

To convert an ANSI 3 octet into ITU-T 14 Bit format, for example, E70A03:

1. Open the Windows scientific calculator and select the **Hex** radio button.
2. Enter the value E70A03.
3. Click the **Dec** radio button.

   The ITU-T 14 Bit format, 15141379, is displayed.

To edit the configuration file and insert the point codes:

1. Log on as **root**.
2. Enter the following commands:

   cd /export/att/run/milborne

   cp milborne.cfg milborne-cfg.orig
3. Open the **milborne.cfg** file on the "local" NRS.
4. Look for entries marked *Make Change Here*.
5. Replace the *Make Change Here* entry with the converted ITU-T 14 Bit format number.

   The following is an example of a configuration file with the *Make Change Here* entries highlighted in bold:

```
* ISUP and SCCP Call Control Configuration
*
* TCP/IP links configuration
*
* The entries in this file allow connection via 4 signalling
* links on card 0 PCM A, PCM B, PCM C, PCM D. This configuration
* uses 2 LinkSets each of which has 1 Routes.
* Primary and Secondary routing is used to 2 Destinations
   .
   .
*Milborne    Pointcode
*231-010-003 ANSI pointcode
#SS7Mtp Pc 0 *Make Change Here*
#SS7Mtp Ni 0 2
   .
   .
*Linkset For STP 1
*254-152-000 ANSI pointcode
#SS7Linkset Total 0 2
#SS7Linkset Pc 0 *Make Change Here*
#SS7Linkset Ni 0 2
#SS7Linkset Combined 0 1
#SS7Linkset Combinedid 0 1
#SS7Linkset Status 0 Ins

*Linkset For STP 2
*254-153-000 ANSI pointcode
#SS7Linkset Total 1 2
#SS7Linkset Pc 1 *Make Change Here*
#SS7Linkset Ni 1 2
#SS7Linkset Combined 1 1
#SS7Linkset Combinedid 1 0
#SS7Linkset Status 1 Ins
   .
   .
```

The following is an example of a configuration file with the inserted point codes highlighted in bold:

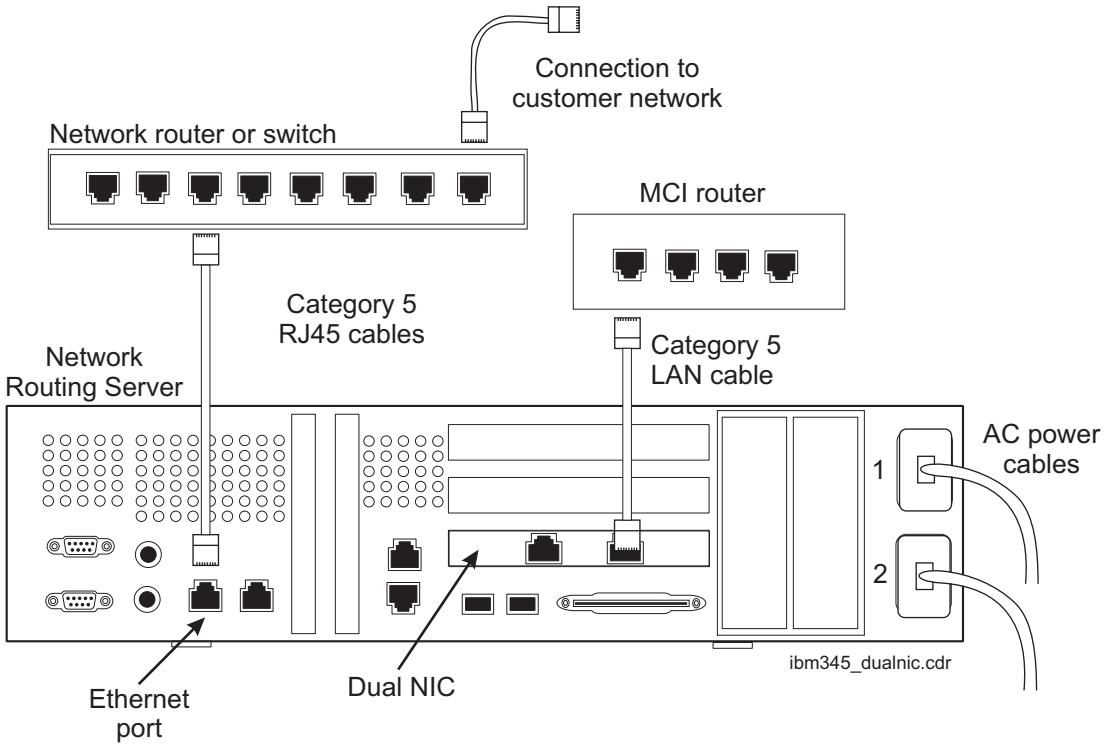
```
* ISUP and SCCP Call Control Configuration
*
* TCP/IP links configuration
*
* The entries in this file allow connection via 4 signalling
* links on card 0 PCM A, PCM B, PCM C, PCM D. This configuration
* uses 2 LinkSets each of which has 1 Routes.
* Primary and Secondary routing is used to 2 Destinations
   .
   .
*Milborne    Pointcode
*231-010-003 ANSI pointcode
#SS7Mtp Pc 0 15141379
#SS7Mtp Ni 0 2
    .
    .
*Linkset For STP 1
*254-152-000 ANSI pointcode
#SS7Linkset Total 0 2
#SS7Linkset Pc 0 16685056
#SS7Linkset Ni 0 2
#SS7Linkset Combined 0 1
#SS7Linkset Combinedid 0 1
#SS7Linkset Status 0 Ins

*Linkset For STP 2
*254-153-000 ANSI pointcode
#SS7Linkset Total 1 2
#SS7Linkset Pc 1 16685312
#SS7Linkset Ni 1 2
#SS7Linkset Combined 1 1
#SS7Linkset Combinedid 1 0
#SS7Linkset Status 1 Ins
   .
   .
```

6. Save and close the configuration file.
7. Repeat this procedure for the **milborne.cfg** file on the "remote" NRS. You will have different point code values that you must convert and insert to the configuration file for the "remote" NRS.
8. Continue with Accessing the system and administering users on page 45.

Connecting the dual NIC for MCI

When interfacing the NRS to the MCI network, you must connect and configure the NIC interface card. The dual NIC is used to interface to the MCI network. The following diagram shows a typical configuration of how to connect from the dual NIC to equipment on the router used for the MCI network.



After these connections have been done, continue with Accessing the system and administering users on page 45.

Connecting and configuring the X.25 card for Sprint

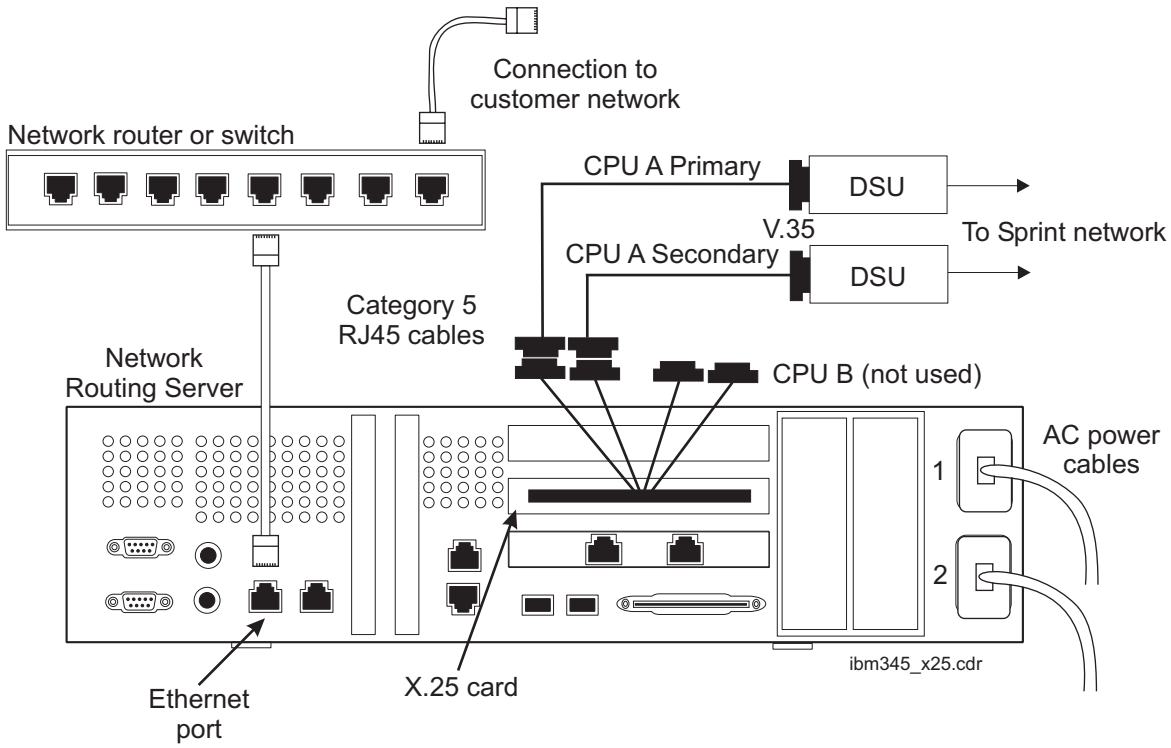
When interfacing the NRS to the Sprint network, you must connect and configure the X.25 interface card. The X.25 interface card is used to interface to the Sprint network.

This section includes the following topics:

- Connecting the X.25 card on page 42
- Configuring the Sprint X.25 card on page 43

Connecting the X.25 card

The following diagram shows how to connect the DB25 pigtail connectors from the X.25 interface card, to the V.35 interface cables, and then the DSUs on the Sprint network.



Configuring the Sprint X.25 card

Do this procedure to check and modify the configuration of the X.25 card, based on the results of the output.

To check and modify the configuration of the X.25 card:

1. Log on as **root**.
2. Enter:

   wanrouter hwprobe

   Messages similar to the following are displayed:

```
------------------------------
| Wanpipe Hardware Probe Info |
------------------------------
1. S514-2-PCI : SLOT=5 : BUS=2 : IRQ=24 : CPU=A : PORT=PRI
2. S514-2-PCI : SLOT=5 : BUS=2 : IRQ=24 : CPU=A : PORT=SEC
3. S514-2-PCI : SLOT=5 : BUS=2 : IRQ=24 : CPU=B : PORT=PRI
4. S514-2-PCI : SLOT=5 : BUS=2 : IRQ=24 : CPU=B : PORT=SEC
```

   Each of the above lines corresponds to a wanpipe configuration file.

3. Edit each of the **wanpipe?.conf** files in **/etc/wanpipe** and change the PCISLOT and PCIBUS entries to correspond to the SLOT and BUS values shown using the **wanrouter hwprobe** command.

   Note:
   The wanpipe configuration was carried out initially using the **wancfg** utility.

4. Continue with Accessing the system and administering users on page 45.

Accessing the system and administering users

This section describes how to log in to the NRS, administer users, change passwords, and log out.

This section includes the following topics:

- Prerequisites on page 45
- Administrator requirements on page 46
- Logging in on page 46
- Administering users on page 49
- Changing your password on page 52
- Logging out on page 52

Prerequisites

Before you log in to use the NRS, you must:

- Have access to a Java-enabled Web browser. The supported versions are Microsoft Internet Explorer 5 or later and Netscape Navigator 6.2 or later and must have Java plug-in 1.4.0 or later.
- Know the URL for the NRS (usually the IP address).
- Know the password for your login ID. Contact the system administrator for your initial password.

SECURITY ALERT:
After you log in for the first time, use the instructions in Changing your password on page 52 and change your password. Do not share your login ID and password with other users.

Administrator requirements

Administrators of the NRS should consider the following:

- Administrators and users that make configuration changes to the NRS database should work primarily on the server that is designated as the local server. Unless the local server is out of service, Avaya recommends that you *do not* make changes to the database on the remote server.
- As administrators and users make changes to configurations on the local NRS, database synchronization automatically copies those changes to the remote server. Administrators must confirm that database synchronization is configured properly on both NRSs. See Setting up database synchronization on page 29 for information about configuring database synchronization.
- Administrators must secure their password and all other user passwords, and instruct all other users to secure their passwords.

Logging in

To log in to the NRS:

1. Open a Web browser.
2. In the address box, enter:

   `http://`*`IP_address`*`/`

   where ***`IP_address`*** is the IP address assigned to the NRS.

   Note:

   When you access the NRS for the first time, the system may download a Java plug-in to your PC. This is normal operation if your Web browser does not already have the plug-in.

   The Distribution Manager login dialog box is displayed.
3. Enter your user name and password.
4. If **Synchronization Active** is checked, the database on this NRS will be copied to its remote server when you log in.

Important:

You can clear this option if you do not want database synchronization to occur when you log in, which may be useful when logging in to a NRS where the configuration is not up to date and you do not want the configuration copied to any other server.

5. Click **Log in**.

   The first time you log in, you are prompted to create a new password. To create a new password, continue with Step 6. If this is not the first time you have logged in, continue with Step 12.

6. Click **Close**.

   The **Change Password** dialog box is displayed.

7. Enter your old password and enter a new password.

   SECURITY ALERT:

   Passwords must be from 5 to 20 characters long and should be a combination of letters and numbers. Do not share your login ID password with any other users.

8. Confirm your new password by entering it a second time.

9. Click **Submit** to make the change, or click **Cancel** to cancel the request.

   A dialog box is displayed confirming that the user password has been changed. If the two password entries do not match, an error message is displayed, and you must reenter and confirm the new password.

10. Click **Close**.

11. The new password takes effect the next time you log in.

    Note:

    If your login ID has been assigned a password expiration interval, you will be warned when you log in that your password is about to expire or has already expired. To change your password at that time, click **Yes**. The **Change Password** dialog box is displayed and you continue with Step 7 above.

12. After the system validates the login ID and password, a dialog box is displayed noting the last time you logged into the system. This dialog box does not display the first time you log on.

SECURITY ALERT:

Do not share your login ID password with other users. If you suspect that your login ID has been used by someone else, use the instructions in Changing your password on page 52 and change your password. Contact your system administrator if you suspect that other users have been using your login ID.

13. Click **Close**.

    The main user interface window is displayed.

14. The first time you access the NRS, change the focus back to the browser window and add the address of the server to your favorites or bookmark list.

CAUTION:

Do not use this browser window for any other purpose while you are logged in to the NRS. If you use this browser window to open another address, your session will be stopped and you will be logged off. Minimize this browser window and open separate browser windows for any other purposes.

Administering users

Only the **admin** login ID can administer users.

This section includes the following topics:

- Adding a user on page 49
- Resetting a user password on page 50
- Changing user access permissions on page 50
- Changing a user password aging interval on page 51
- Deleting a user on page 51

Adding a user

To add a user to the system:

1. Click **File > User Administration**.

   The **User Administration** dialog box is displayed.

2. Click **Add User**.

   The **Edit User** dialog box is displayed.

3. In the **Edit User** dialog box:

   a. Enter a user name.

   b. Enter an initial password.

   SECURITY ALERT:
   Remind the user to change the password the next time he or she logs in to the system.

   c. Set the **Access Rights** to **Read-Only** or **Read-Write**. **Read-Write** users can make configuration changes to the system and monitor the system, but **Read-Only** users can only monitor the system.

   SECURITY ALERT:
   Give **Read-Write** access only to users that must make configuration changes. All other users must have **Read-Only** access.

   d. Select a password expiration interval (30, 60, or 90 days, or never). The default expiration interval is 30 days.

4. Click **Submit** to add the user, or click **Cancel** to cancel the request.

5. Click **Close**.

Resetting a user password

To reset a user password:

1. Click **File > User Administration**.

   The **User Administration** dialog box is displayed.

2. Double-click the user name for which you want to reset the password.

   The **Edit User** dialog box is displayed.

3. In the **Edit User** dialog box, enter a new password.
4. Click **Submit** to make the change, or click **Cancel** to cancel the request.

   SECURITY ALERT:
   Notify the user of the new password. Remind the user to change the password the next time he or she logs in to the system.

5. Click **Close**.

Changing user access permissions

To change user access permissions:

1. Click **File > User Administration**.

   The **User Administration** dialog box is displayed.

2. Double-click the user name for which you want to reset the user permissions.

   The **Edit User** dialog box is displayed.

3. In the **Edit User** dialog box, change the access permissions. **Read-Write** users can make configuration changes to the system and monitor the system, but **Read-Only** users can only monitor the system.

   SECURITY ALERT:
   Give **Read-Write** access only to users that must make configuration changes. All other users must have **Read-Only** access.

4. Click **Submit** to make the change, or click **Cancel** to cancel the request.
5. Click **Close**.

Changing a user password aging interval

To change the password aging interval:

1. Click **File > User Administration**.

   The **User Administration** dialog box is displayed.

2. Double-click the user name for which you want to change the password aging interval.

   The **Edit User** dialog box is displayed.

3. In the **Edit User** dialog box, select a password aging interval (30, 60, or 90 days, or never).

4. Click **Submit** to make the change, or click **Cancel** to cancel the request.

5. Click **Close**.

Deleting a user

To delete a user:

1. Click **File > User Administration**.

   The **User Administration** dialog box is displayed.

2. Click the user name that you want to delete.

3. Click **Delete User**.

   A warning dialog box is displayed asking if you really want to delete the user.

4. Click **Yes** to delete the user, or click **No** to cancel the request.

   The **User Administration** dialog box redisplays showing that the user has been deleted.

5. Click **Close**.

Changing your password

To change your password:

1. Click **File > Change Password**.

   The **Change Password** dialog box is displayed.

2. Enter your old password and enter a new password.

   SECURITY ALERT:
   Passwords must be from 5 to 20 characters long and should be a combination of letters and numbers. Do not share your login ID password with other users.

3. Confirm your new password by entering it a second time.

4. Click **Submit** to make the change, or click **Cancel** to cancel the request.

   A dialog box is displayed confirming that the user password has been changed. If the two password entries do not match, an error message is displayed and you must reenter and confirm the new password.

5. Click **Close**.

6. The new password takes effect the next time you log in.

   Note:
   If your login ID has been assigned a password expiration interval, you will be warned when you log in that your password is about to expire or has already expired. To change your password at that time, click **Yes**. The **Change Password** dialog box is displayed and you continue with Step 2 above.

Logging out

SECURITY ALERT:
It is important to log out of the NRS when not making changes or monitoring the system. Logging out prevents unauthorized users from making changes to the NRS using your login ID.

To log out of the NRS, click **File > Exit**.

The NRS closes. To log in again, refresh the browser window.

Configuring links to a Network Gateway

This section contains information about configuring links from the Distribution Manager application to the Network Gateway application. These procedures can be used when the Network Gateway application is coresident on the NRS server or when the Network Gateway application is on a dedicated server.

This section includes the following topics:

- Network Gateway link options for AT&T on page 54
- Network Gateway link options for MCI on page 55
- Network Gateway link options for Sprint on page 56
- Adding a Network Gateway link on page 57
- Changing a Network Gateway link on page 58
- Removing a Network Gateway link on page 59

Network Gateway link options for AT&T

With the AT&T interface, you will assign one Network Gateway link. The following table describes the Network Gateway link options for AT&T:

Option	Parameters	Notes
Name	Alphanumeric string up to 20 characters	Include the name of the AT&T point of presence as part of the name.
Type	AT&T MCI Sprint	Use AT&T. Do not select any other gateway type from the list. You cannot use two different Network Gateway types in one configuration.
IP Address	Valid IPv4 address	Enter the IP address of the NRS. With AT&T, the same IP address is used for the Distribution Manager and Network Gateway applications.
Port Number	1024-65535	Enter the TCP listen port of the XML application on the Network Gateway.
Service Key Value	0-255	Identifies the application being requested of the service provider network. For AT&T, enter `0`.
Validate Interval	1000-60000 ms	Avaya recommends a value of 5000.
Validate Timeout	500-10000 ms	Avaya recommends a value of 1000.
Max Timeouts	1-10	Avaya recommends a value of 3.
Address Indicator	Point Code/SSN Global Title	If **DM Point Code/SSN** is selected, you must enter a value in the **DM Point Code** and **Network Routing SSN** fields. If **Global Title** is selected, you must enter a value in the **Global Title** field.
Point Code	Three numbers, 0-255, separated by hyphens (-)	Enter the signaling point within the SS7 network. Obtain the correct setting from the service provider. This number must match the originating point code administered during the Network Gateway setup described in Configuring the AT&T SS7 point codes on page 38.
Network Routing SSN	0-255	Enter the subsystem used on the AT&T network, usually `254`.
Global Title		Enter the global title of the Network Gateway.

Network Gateway link options for MCI

With MCI, you always assign three Network Gateway links using the XML Port Numbers 4011, 4012, and 4013. The following table describes the Network Gateway link options for MCI:

Option	Parameters	Notes
Name	Alphanumeric string up to 20 characters	Enter a name for the MCI Network Gateway.
Type	AT&T MCI Sprint	Select MCI. Do not select any other gateway type from the list. You cannot use two different Network Gateway types in one configuration.
IP Address	Valid IPv4 address	Enter the IP address of the NRS. With MCI, the same IP address is used for the Distribution Manager and Network Gateway applications.
XML Port Number	1024-65535	Enter the TCP listen port of the XML application on the Network Gateway. For MCI, you will use port numbers 4011, 4012, and 4013 at all installations.
Service Key Value	0-255	Identifies the application being requested of the service provider network. For MCI, enter 1.

Network Gateway link options for Sprint

The following table describes the Network Gateway link options for Sprint:

Option	Parameters	Notes
Name	Alphanumeric string up to 20 characters	Enter a name for the Sprint Network Gateway.
Type	AT&T MCI Sprint	Select Sprint. Do not select any other gateway type from the list. You cannot use two different Network Gateway types in one configuration.
IP Address	Valid IPv4 address	Enter the IP address of the NRS. With Sprint, the same IP address is used for the Distribution Manager and Network Gateway applications.
XML Port Number	1024-65535	Enter the TCP listen port of the XML application on the Network Gateway. For Sprint, use ports 9541 for CPU A Primary and 9542 for CPU A Secondary. Ports 9543 and 9544 are used for CPU B, but CPU B is not normally used.
Service Key Value	0-255	Identifies the application being requested of the service provider network. For Sprint, enter 1.

Adding a Network Gateway link

To add a Network Gateway link:

1. Click **Configure > Network Gateway > Add**.

   The **Add Network Gateway** dialog box is displayed.

2. Populate the dialog box with values as described in one of the following:

   - Network Gateway link options for AT&T on page 54
   - Network Gateway link options for MCI on page 55
   - Network Gateway link options for Sprint on page 56

3. Click **Submit**.

   The link to the Network Gateway is added.

4. Log out of the Distribution Manager application.
5. Open a telnet session to the NRS.
6. Enter the following commands to stop and restart the Network Gateway interface:

   ```
   cd /export/dm
   ./stop-all
   ./go-psa
   ```

7. Repeat this procedure for the other NRS in the configuration.

Changing a Network Gateway link

To change a Network Gateway link:

1. Click **Configure > Network Gateway > Edit**.

   The **Select Network Gateway** dialog box is displayed.

2. Double-click the Network Gateway you want to edit.

   The **Edit Network Gateway** dialog box is displayed.

3. Populate the dialog box with values as described in one of the following:

   - Network Gateway link options for AT&T on page 54
   - Network Gateway link options for MCI on page 55
   - Network Gateway link options for Sprint on page 56

4. Click **Submit**.

   The link to the Network Gateway is changed and the **Select Network Gateway** dialog box is displayed.

5. Click **Close**.
6. Log out of the Distribution Manager application.
7. Open a telnet session to the NRS.
8. Enter the following commands to stop the Network Gateway interface:

   ```
   cd /export/dm
   ./stop-all
   ./go-psa
   ```

9. Repeat this procedure for the other NRS in the configuration.

Removing a Network Gateway link

To remove a Network Gateway link:

1. Click **Configure > Network Gateway > Remove**.

   The **Remove Network Gateway** dialog box is displayed.

2. Double-click the Network Gateway you want to remove.

   A **Warning** dialog box is displayed asking if you really want to remove the link.

3. Click **Yes** to remove the Network Gateway link, or click **No** to cancel the request.

   The **Remove Network Gateway** dialog box redisplays showing that the Network Gateway has been deleted.

4. Click **Close**.

Configuring CC links, IP trunks, and vectors

This section describes how to configure IP trunks from the NRS to the CCs, vectors, and network applications.

This section includes the following topics:

- Prerequisite CC administration on page 62
- Configuring a CC link on the NRS on page 64
- Administering node names and IP addresses on page 67
- Administering IP trunks from each CC to the NRS on page 69
- Administering status polling vectors and VDNs on each CC on page 76
- Saving translations on page 78

You must have access to both NRSs and to all CCs in the customer's Network Routing configuration because you must do the procedures in the order shown in this section.

For example, you can use a PC with a Web browser to access the NRSs, and you can use the same PC with Avaya Site Administration to access the CCs. It is critical to have access to all systems while configuring the links and vectors.

Prerequisite CC administration

Before you begin the network application administration required for Network Routing, you must first verify that certain prerequisite administration has been done on all CCs within the configuration.

This section includes the following topics:

- Software load on page 62
- Customer options on page 63

Software load

Network Routing is available on CCs with the following software:

- Avaya MultiVantage Software 1.3.1, load 533 or later (V11 or R011)
- Avaya Communication Manager 2.0, load 218.6 or later (V12 or R012)

If any of the CCs do not meet this requirement, the CCs cannot be part of the Network Routing configuration.

To verify the software load:

1. Enter:

   display system-parameters customer-options

   Verify that the G3 Version field is **V11** or **v12**.

2. Enter:

   list config software

   Verify that the SOFTWARE VERSION is one of the following:

   - **R011**, load 533 or later
   - **R012**, load 218.6 or later

Customer options

To set up the polling between the NRS and the CCs in the Network Routing configuration, certain features must be enabled on each CC. If any of these features are not enabled, the customer must purchase these features and a new license file must be applied to the CC.

To verify that the customer options are enabled:

1. Enter:

   display system-parameters customer-options

   The OPTIONAL FEATURES form is displayed.

2. Under IP PORT CAPACITIES (Page 1 or 2, depending on CC software), verify that there are at least 4 IP trunks available in the `Maximum Administered IP Trunks` field.

3. On Page 3 or 4 (depending on CC software), verify that the `IP Trunks` option is enabled.

4. Under CALL CENTER OPTIONAL FEATURES, verify that `Lookahead Interflow (LAI)` and `Vectoring (Best Service Routing)` are enabled.

5. Under QSIG OPTIONAL FEATURES, verify that QSIG `Basic Call Setup` and `Basic Supplementary Services` are enabled.

Configuring a CC link on the NRS

This section contains information about configuring links from the NRS to each CC. You can assign a link to 16 different CCs. You must configure a link from both NRSs to each CC.

This section includes the following topics:

- CC link options on page 64
- Adding a CC link on page 65
- Changing a CC link on page 66
- Removing a CC link on page 66

Note:

If there is a sample CC link administered the first time you use the Distribution Manager, delete the sample link after you administer the working links.

CC link options

The following table describes the CC link options:

Option	Parameters	Notes
Name	Alphanumeric string up to 20 characters	Enter the location and model as part of the name.
Type	CM or IC	Select **CM**. The **IC** option is for a future development.
IP Address	Valid IPv4 address	Enter the IP address of the CLAN circuit pack that is being used to route IP trunks to the NRS.
TCP Port Number	1024-65535	Enter the TCP listen port of the ethernet port on the CC. This must match the `Far-end Listen Port` field administered on the IP trunk Signaling Group form on the CC. The port number defaults to 1720.
Maximum Number of Retries	0-10	Enter the maximum number of times the NRS should retry polling, in case there is a polling timeout, before putting the link out of service. Avaya recommends a value of 3.

Option	Parameters	Notes
Polling Timeout	0-15 seconds	Enter the length of time to wait for a reply from the CC before stopping a poll. Avaya recommends a value of 3 seconds. **Important:** If you are consistently seeing timeouts in the **CC Performance** status display, increase this timeout as needed. See CC performance on page 104 for more information.
Out of Service Retry Interval	0-300 seconds	Enter the length of time to wait before retrying an out of service H.323 link. Avaya recommends a value of 30 seconds.

Adding a CC link

To add a CC link:

1. Click **Configure > CC Link > Add**.

   The **Add CC** dialog box is displayed.

2. Populate the dialog box with values as described in CC link options on page 64.

3. Click **Submit**.

   The CC link is added.

Note:

If you want to schedule the addition for a later date or time, click **Schedule** (see Scheduling configuration updates on page 132).

Changing a CC link

To change a CC link:

1. Click **Configure > CC Link > Edit**.

   The **Select CC** dialog box is displayed.

2. Double-click the CC you want to edit.

   The **Edit CC** dialog box is displayed.

3. Populate the dialog box with values as described in CC link options on page 64.

4. Click **Submit**.

   The CC link is changed and the **Select CC** dialog box is displayed.

   Note:

   If you want to schedule the change for a later date or time, click **Schedule** (see Scheduling configuration updates on page 132).

5. Click **Close**.

Removing a CC link

To remove a CC link:

1. Click **Configure > CC Link > Remove**.

   The **Remove CC** dialog box is displayed.

2. Double-click the CC link you want to remove.

   A **Warning** dialog box is displayed asking if you really want to remove the link.

3. Click **Yes** to remove the CC link, or click **No** to cancel the request.

   The **Remove CC** dialog box redisplays showing that the CC link has been deleted.

4. Click **Close**.

Administering node names and IP addresses

Node names and IP addresses must be administered for the following:

- The local NRS
- The remote NRS

Important:
You must administer node names and IP addresses on every CC that is being polled by the NRS.

To administer node names and IP addresses:

1. Obtain the IP addresses for the NRSs. These were assigned in Setting up the Network Routing servers on page 19.
2. Enter:

   `list config all`

   Note the board number of all CLAN circuit packs. Verify that the circuit packs are at least version D.
3. Enter one of the following:

   `display ip-interfaces` (MultiVantage 1.3)

   `display ip-interfaces <board_location>` (Communication Manager 2.0)

   The IP INTERFACES form is displayed.
4. Note the node name of the circuit pack.
5. Enter:

   `change node-names ip`

   The IP NODE NAMES form is displayed.
6. Enter a name for the local NRS.
7. Enter the IP address for the local NRS.
8. Enter a name for the remote NRS.
9. Enter the IP address for the remote NRS.
10. Submit the change.

The following is a typical example of an administered IP NODE NAMES form. In most cases, there will be more IP node names administered than is shown in this example.

```
change node-names ip                                          Page   1 of   1
                                IP NODE NAMES
    Name                 IP Address           Name               IP Address
NRservA               156.34 .76 .105                            .   .   .
NRservB               156.34 .76 .111                            .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
                         .   .   .                               .   .   .
( 3  of 3  administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Administering IP trunks from each CC to the NRS

From each CC in the Network Routing configuration, you must administer an IP trunk to each NRS, which means that you must administer two trunks per CC. You must also administer the QSIG TSC Extension.

Important:
You must administer IP trunks on every CC that is being polled by the NRS.

To administer an IP trunk to the NRS:

1. Enter:

   display dialplan analysis

   The DIAL PLAN ANALYSIS TABLE form is displayed.

2. Verify that **dac** is an administered `Call Type`. Note the `Dialed String` and the `Total Length`.

3. Enter:

   list trunk-group

   The TRUNK GROUPS form is displayed.

4. Use **Page Down** to see all pages of administered trunk groups. Select an unused range of trunk groups to use for the Network Routing configuration.

5. Enter:

   list signaling-group

   The SIGNALING GROUPS form is displayed.

6. Use **Page Down** to see all pages of administered signaling groups. Select an unused range of signaling groups to use for the Network Routing configuration.

   Note:
   Avaya recommends that you use corresponding trunk group numbers, signaling group numbers, and routing patterns. For example, if you use trunk groups 1 through 10, try to use signaling groups 1 through 10 and route patterns 1 through 10.

7. Enter:

   add trunk-group *XX*

   where ***XX*** is the trunk group number. The TRUNK GROUP form is displayed.

8. On Page 1, set the fields as shown in the following table. Leave fields not shown in the table set to the default value.

Field	Value
Group Type	isdn
Group Name	Enter a name that describes the link to the NRS. Avaya recommends that you use the "A" designator for the local server and "B" for the remote server (for example, **NRA** and **NRB**)
COR	Select a class of restriction (COR) that can be used for all Network Routing administration (trunks, VDNs, and so on). Avaya recommends that you use the most restrictive COR available.
TAC	Enter a trunk access code (TAC) as defined by the dial plan.
Carrier Medium	IP
Service Type	tie (for the local NRS) cbc (for the remote NRS)
Supplementary Service Protocol	b

The following is an example of Page 1.

```
add trunk-group 22                                          Page   1 of  22
                              TRUNK GROUP

Group Number: 22                    Group Type: isdn          CDR Reports: y
  Group Name: IP NR trunk act              COR: 1        TN: 1        TAC: #122
   Direction: two-way        Outgoing Display? n         Carrier Medium: IP
 Dial Access? n                Busy Threshold: 255       Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n            TestCall ITC: rest
                        Far End Test Line No:
TestCall BCC: 4
TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6
       Max Message Size to Send: 260   Charge Advice: none
  Supplementary Service Protocol: b     Digit Handling (in/out): enbloc/enbloc

            Trunk Hunt: descend
                                                   Digital Loss Group: 13
Calling Number - Delete:     Insert:                 Numbering Format:
             Bit Rate: 1200         Synchronization: async    Duplex: full
 Disconnect Supervision - In? y  Out? y
 Answer Supervision Timeout: 0
```

9. Go to Page 2 of the form.
10. On Page 2, set the fields as shown in the following table. Leave fields not shown in the table set to the default value.

Field	Value
NCA-TSC Trunk Member	1
UUI IE Treatment	shared
Maximum Size of UUI IE Contents	32
Send UCID	n
Send Codeset 6/ 7 LAI IE	n

The following is an example of Page 2.

```
add trunk-group 22                                          Page   2 of  23
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                 Internal Alert? n        Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member: 1
                                      Send Name: n      Send Calling Number: n
            Used for DCS? n
   Suppress # Outpulsing? n
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: shared
                                           Maximum Size of UUI IE Contents: 32
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                                      Send Connected Number: n
Network Call Redirection: none
              Send UUI IE? y
                Send UCID? n                BSR Reply-best DISC Cause Value: 31
 Send Codeset 6/7 LAI IE? n



                            Network (Japan) Needs Connect Before Disconnect? n
```

11. Submit the change.

Note:

No trunk ports are added at this time. You do this after you administer the signaling group.

12. Enter:

    `add signaling-group XX`

    where ***XX*** is the signaling group number. The SIGNALING GROUP form is displayed.

    Tip:

    Avaya recommends that the signaling group number matches the trunk group number.

13. On Page 1, set the fields as shown in the following table. Leave fields not shown in the table set to the default value.

Field	Value
Group Type	h.323
Max number of NCA TSC	10
Trunk Group for NCA TSC	Enter the trunk group number you added with Step 7.
Trunk Group for Channel Selection	Enter the trunk group number you added with Step 7.
Supplementary Service Protocol	b
Near-end Node Name	Enter the node name of the CC. Use the **`display node-names ip`** command to display node names.
Near-end Listen Port	Enter the listen port administered on the NRS. This is usually 1720.
Far-end Node Name	Enter the node name of the NRS as assigned in Administering node names and IP addresses on page 67.
Far-end Listen Port	Enter the listen port administered on the NRS. This is usually 1720.
Calls Share IP Signaling Connection	y

The following is an example of Page 1.

```
add signaling-group 22                                        Page   1 of   5
                              SIGNALING GROUP

 Group Number: 22              Group Type: h.323
                            Remote Office? n          Max number of NCA TSC: 10
                                                        Max number of CA TSC: 0
                                                    Trunk Group for NCA TSC: 22
      Trunk Group for Channel Selection: 22
         Supplementary Service Protocol: b          Network Call Transfer? n


       Near-end Node Name: chcago            Far-end Node Name: NRservACT
     Near-end Listen Port: 1720            Far-end Listen Port: 1720
                                        Far-end Network Region:
             LRQ Required? n             Calls Share IP Signaling Connection? y
             RRQ Required? n
                                            Bypass If IP Threshold Exceeded? n

                                             Direct IP-IP Audio Connections? y
                                                       IP Audio Hairpinning? y
                                            Interworking Message: PROGress
```

14. Submit the change.
15. Enter:

    change trunk-group *XX*

    where ***XX*** is the trunk group number added in Step 7. The TRUNK GROUP form is displayed.
16. Go to Page 7 of the form.

17. On Page 7, add one IP trunk and set it to the signaling group number added in Step 12.

    The following is an example of Page 7.

```
change trunk-group 22                                        Page   7 of  23
                                  TRUNK GROUP
                                       Administered Members (min/max):   1/25
GROUP MEMBER ASSIGNMENTS                   Total Administered Members:  25

       Port    Code Sfx Name        Night            Sig Grp
  1: IP                                              22
  2:
  3:
  4:
  5:
  6:
  7:
  8:
  9:
 10:
 11:
 12:
 13:
 14:
 15:
```

18. Submit the change.

    Note:

    The next time you display the trunk members, the `Port` field will display specific IP trunk port members (for example, `T00145`).

19. Enter:

    `status trunk-group XX`

    where ***XX*** is the trunk group number added in Step 7. Verify that all trunk members are in the `in-service/idle` state.

20. Enter:

    `change system-parameters features`

    The FEATURE-RELATED SYSTEM PARAMETERS form is displayed.

21. Go to Page 7 of the form.

22. On Page 7, enter an unassigned extension number in the `QSIG TSC Extension` field.

    The following is an example of Page 7.

```
change system-parameters features                              Page   7 of  12
                        FEATURE-RELATED SYSTEM PARAMETERS

ISDN PARAMETERS

 Send Non-ISDN Trunk Group Name as Connected Name? y
 Display Connected Name/Number for ISDN DCS Calls? y
       Send ISDN Trunk Group Name on Tandem Calls? y


                                 QSIG TSC Extension: 6220
 MWI - Number of Digits Per Voice Mail Subscriber: 5

                               National CPN Prefix:
                          International CPN Prefix:
                         Pass Prefixed CPN to ASAI? n
    Unknown Numbers Considered Internal for AUDIX? n
              USNI Calling Name for Outgoing Calls? n
                Path Replacement with Measurements? y
                   QSIG Path Replacement Extension:
             Path Replace While in Queue/Vectoring? n
```

23. Submit the change.
24. Repeat this procedure for the remote NRS.

Administering status polling vectors and VDNs on each CC

Vectors and VDNs are used to obtain status on all of the CCs in the Network Routing configuration.

To administer a status polling vector and VDN:

1. Enter:

   `list hunt-group`

   A list of hunt groups is displayed. Use **Page Down** and **Page Up** to see all pages of administered hunt groups.

2. Enter:

   `display hunt-group` ***`XXX`***

   where ***`XXX`*** is the number of a hunt group. These forms show you more information about the hunt group to help you decide which hunt group to select for polling.

   Note:
   The hunt group number is the same as the split/skill number.

3. Determine which vector and VDN you are going to add. These must be vectors and VDNs that are not already administered.

4. Enter:

   `change vector` ***`XX`***

   where ***`XX`*** is the vector number. The CALL VECTOR form is displayed.

5. Enter a meaningful name for the vector (for example, **`NR statpoll 1`**).

6. In vector step 1, enter a **`consider`** step that checks the split/skill selected by the customer as being the split/skill that best represents the status of the CC.

7. In vector step 2, enter:

   reply-best

   The following is an example vector for status polling. The customer can use more detailed vectors to determine the best available split/skill, but this example shows the minimum required.

```
change vector 6                                              Page   1 of   3
                                CALL VECTOR

    Number: 6                 Name: NR statpoll 1
                   Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y

01 consider     skill    46  pri h adjust-by 0
02 reply-best
03
04
05
06
07
08
09
10
11
```

8. Submit the change.
9. Enter:

   add vdn *XXXXXX*

   where ***XXXXXX*** is the VDN.

10. On Page 1, set the fields as shown in the following table. Leave fields not shown in the table set to the default value.

Field	Value
Name	Enter the same name as assigned to the vector.
Vector Number	Enter the vector number added in Step 4.
COR	Select a class of restriction (COR) that can be used for all Network Routing administration (trunks, VDNs, and so on). Avaya recommends that you use the most restrictive COR available.

The following is an example of Page 1.

```
add vdn 350                                                    Page   1 of   2
                            VECTOR DIRECTORY NUMBER

                              Extension: 350
                                   Name: NR statpoll 1
                          Vector Number: 6
                    Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                    TN: 1
                              Measured: none

               Service Objective (sec): 20
          VDN of Origin Annc. Extension:
                              1st Skill:
                              2nd Skill:
                              3rd Skill:
```

11. Submit the change.
12. Repeat this procedure on this CC to create a status-polling vector and VDN to every other CC in the configuration. You must then repeat this procedure for every CC in the configuration.

Saving translations

After making translation changes on each CC, use the **`save translation`** command to save the changes you have made.

Configuring polling groups and network applications

This section describes how to configure polling groups, network applications, and related parameters. This section also includes procedures for completing the initial configuration.

This section includes the following topics:

- Configuring polling groups on page 80
- Configuring network applications on page 83
- Configuring ANI groups on page 89
- Configuring CED groups on page 92
- Completing the initial configuration on page 95

CAUTION:

Submitting changes to polling groups, network applications, ANI groups, and CED groups will cause an interruption to call routing responses. During this interruption, calls are routed using the network failsafe. Submit changes or schedule changes during low- or no-traffic periods.

Configuring polling groups

Polling groups are used to poll the CCs to see if multiple network applications are needed. Since these groups of agents may handle calls from numerous TFN, ANI, and CED combinations, these same polling groups are used in multiple network applications. Members of the polling groups are defined by the CC where they reside and a Queue label The CC and Queue label pair are unique in the database. Each polling group has an associated failsafe percent distribution that is used for all network applications in case communication is lost to all CCs.

CAUTION:

Submitting changes to polling groups will cause an interruption to call routing responses. During this interruption, calls are routed using the network failsafe. Submit changes or schedule changes during low- or no-traffic periods.

This section includes the following topics:

- Polling group options on page 80
- Adding a polling group on page 81
- Changing a polling group on page 82
- Removing a polling group on page 82

Polling group options

The following table describes the polling group options:

Option	Parameters	Notes
Polling Group name	Alphanumeric string up to 20 characters	Enter a descriptive name for the polling group.
CC Name	Alphanumeric string up to 20 characters	Select a CC from the drop-down list.

Option	Parameters	Notes
Queue label	Valid VDN	For MultiVantage or Communication Manager, enter the status polling VDN for the split or skill.
Failsafe % distribution	0-100	Enter a value for each CC Name/Queue label pair to determine the percentage of calls that will use this pair in case access to a CC is lost. If the selected percentages do not add up to 100%, a warning message is displayed when you submit the change. You can either let the system automatically equalize the percentages, or you can manually calculate the values so it will add up to 100%.

Adding a polling group

To add a polling group:

1. Click **Configure > Polling Group > Add**.

   The **Add Polling Group** dialog box is displayed.

2. Populate the dialog box with values as described in Polling group options on page 80.

3. Click **Submit**.

   The polling group is added.

Note:

If you want to schedule the addition for a later date or time, click **Schedule** (see Scheduling configuration updates on page 132).

Changing a polling group

To change a polling group:

1. Click **Configure > Polling Group > Edit**.

   The **Edit Polling Group** dialog box is displayed.

2. Double-click the polling group you want to edit.

   The **Edit Polling Group** dialog box is displayed.

3. Populate the dialog box with values as described in Polling group options on page 80.

4. Click **Submit**.

   The polling group is changed and the **Edit Polling Group** dialog box is displayed.

   Note:

   If you want to schedule the change for a later date or time, click **Schedule** (see Scheduling configuration updates on page 132).

5. Click **Close**.

Removing a polling group

To remove a polling group:

1. Click **Configure > Polling Group > Remove**.

   The **Remove Polling Group** dialog box is displayed.

2. Double-click the polling group you want to remove.

   A **Warning** dialog box is displayed asking if you really want to remove the polling group. You may also see a warning noting the sequence number and VDN being removed when you remove this polling group.

3. Click **Yes** to remove the polling group, or click **No** to cancel the request.

   The **Remove Polling Group** dialog box is displayed.

4. Click **Close**.

Configuring network applications

Use network applications to determine the best route or a failsafe route for a call. This is done by polling all CCs in the configuration.

CAUTION:
Submitting changes to network applications will cause an interruption to call routing responses. During this interruption, calls are routed using the network failsafe. Submit changes or schedule changes during low- or no-traffic periods.

This section includes the following topics:

- Network application options on page 83
- Adding network applications on page 86
- Changing network applications on page 87
- Removing network applications on page 88

Network application options

The following tables describe each portion the network application options dialog box:

NA Name and Default NA - This portion of the dialog box defines basic network application options.

Option	Parameters	Notes
NA Name	Alphanumeric string up to 20 characters	Select the function or purpose associated with the department where the network application number terminates (for example, customer service, billing, maintenance).
Default NA	Checked Unchecked	If checked, this network application is used when no other network application criteria matches criteria for the incoming route request. This is equivalent to having the wild card character + optioned for both the **Request Number** and **ANI** in the **Trigger Criteria**. There can be only one default network application. The first network application assigned to the server remains the default network application until another channel is selected as default. If you delete the default network application, you must select another network application as the default.

Incoming Network Application Definition Criteria - This defines the criteria that must be met to process an incoming route request using this network application. When the **Request Number** is dialed by someone calling from the defined **ANI** (automatic number identifier) area using the defined **CED** (caller-entered data), the associated network application will be used to route the call. You can assign up to 50 Request Number/ANI/CED combinations.

For example, if you want all calls from area code 865 that call number 877-345-2424 and use the CEDs 4545 to be processed using this network application, enter 8773452424 in the **Request Number** field, enter 865+ in the **ANI** field, and enter 4545 in the **CED** field.

The matching algorithm always gives higher priority to the network application with the best matching Request Number rather than the best matching ANI. For example, if two network applications are configured as follows:

- Network Application 1 - Request Number = 01483+, ANI = 0196286+
- Network Application 2 - Request Number = 01483123+, ANI = 01962+

an incoming route request that has Request Number 01483123456 and ANI 019628612234 uses Network Application 2.

Option	Parameters	Notes
Request Number	+, partial or complete telephone numbers, up to 30 digits	The Request Number is populated with telephone numbers used to call a business. The numbers are usually toll-free telephone numbers. If + is assigned, calls from any ANI numbers will use this network application. If a partial telephone number followed by + is assigned (for example, 877345+), all calls to telephone numbers that start with those digits use this network application.

Option	Parameters	Notes
ANI	+, partial or complete telephone numbers, up to 30 digits, or predefined ANI group	The ANI is populated with incoming calling line telephone numbers. You can either enter digits here or use a predefined ANI group (see Configuring ANI groups on page 89 for more information). *This field cannot be left blank.* If + is assigned, calls to any Request Numbers use this network application. If an area code followed by + is assigned (for example, 865+), all calls from that area code use this network application.
CED	+, any combination of 16 digits, or predefined CED group	The CED is populated with digits that callers may enter and collected by the service provider. You can either enter digits here or use a predefined CED group (see Configuring CED groups on page 92 for more information). *This field cannot be left blank.* If + is assigned, any CEDs will use this network application. If a set of digits followed by + is assigned (for example, 4545+), all calls that have 4545 plus any other digits will use this network application.

Outgoing Call Distribution - This determines the destination where calls will be routed.

Option	Parameters	Notes
Polling Group	An assigned polling group	The polling groups are assigned in Configuring polling groups on page 80.
CC Name	Display only	The CC names associated with the polling group are displayed, but cannot be changed.
Queue	Display only	The Queue labels associated with the polling group are displayed, but cannot be changed.
Failsafe %	Display only	The Failsafe % for each Queue label is displayed, but cannot be changed.

Option	Parameters	Notes
Destination 1	Alphanumeric characters	The destinations are supplied by the service provider. For AT&T, it will be a series of numeric characters without any spaces. For MCI and Sprint, it will be a series of alphanumeric characters without any spaces. For example, if you have two incoming trunk groups for the CC, the service provider may supply two destinations. The NRS will alternate between the two destinations.
Destination 2 (optional)	Alphanumeric characters	See Destination 1 above. Destination 2 is used as a backup, but if both are configured, the call routing is distributed evenly across both destinations.

Adding network applications

The option values for network applications are described in Network application options on page 83.

To add network applications:

1. Click **Configure > Network Application > Add**.

   The **Add Network Application** dialog box is displayed.

2. Enter a name for the network application.
3. Click the **Default Application** check box if this network application will be used as the default network application.
4. For the **Incoming Network Application Definition Application**:
   a. Enter a Request Number.
   b. Enter or select an ANI.
   c. Enter or select a CED.
   d. Click **Add**.
5. For the **Routing Designation**:
   a. Select a Polling Group.

      The CCs, Queue label and Failsafe % are displayed based on how the Polling Group was configured (see Configuring polling groups on page 80).

   b. Double-clicking the field, enter a Destination 1 label and, if needed, a Destination 2 label.

Important:

After entering values in any of the data fields, remember to press **Enter** or move the cursor to another data field.

6. Click **Submit**.

   The network application is added.

Note:

If you want to schedule the addition for a later date or time, click **Schedule** (see Scheduling configuration updates on page 132).

Changing network applications

To change network applications:

1. Click **Configure > Network Application > Edit**.

   The **Select Network Application** dialog box is displayed.

2. Double-click the network application you want to edit.

   The **Edit Network Application** dialog box is displayed.

3. Change the data for the network application. You can edit existing assignments, remove assignments, or add new assignments. The option values are described in Network application options on page 83.

   Important:

   After entering values in any of the data fields, remember to press **Enter** or move the cursor to another data field.

4. Click **Submit**.

   The network application is changed and the **Select Network Application** dialog box is displayed.

Note:

If you want to schedule the change for a later date or time, click **Schedule** (see Scheduling configuration updates on page 132).

5. Click **Close**.

Removing network applications

To remove network applications:

1. Click **Configure > Network Application > Remove**.

   The **Remove Network Application** dialog box is displayed.

2. Double-click the network application you want to remove.

   A **Warning** dialog box is displayed asking if you want to remove the network application. If the network application being deleted is the default network application, a special message is displayed.

3. Click **Yes** to remove the network application, or click **No** to cancel the request.

   The **Remove Network Application** dialog box is displayed.

4. Click **Close**.

Configuring ANI groups

ANI groups are used to create special groups of regular callers so as to better identify groups of customers so that they receive special treatment.

CAUTION:
Submitting changes to ANI groups will cause an interruption to call routing responses. During this interruption, calls are routed using the network failsafe. Submit changes or schedule changes during low- or no-traffic periods.

This section includes the following topics:

- ANI group options on page 89
- Adding an ANI group on page 90
- Changing an ANI group on page 90
- Removing an ANI group on page 91

ANI group options

The following table describes the ANI group options:

Option	Parameters	Notes
ANI Group name	Alphanumeric string up to 20 characters	Select a descriptive name for the ANI group.
ANI number	Valid telephone number	Enter the telephone number of an incoming caller.
Identifier	Alphanumeric string up to 20 characters	Enter a distinctive name for the caller that uses the ANI number.

Adding an ANI group

To add an ANI group:

1. Click **Configure > ANI Group > Add**.

   The **Add ANI Group** dialog box is displayed.

2. Populate the dialog box with values as described in ANI group options on page 89.

3. Click **Submit**.

   The ANI group is added.

   Note:

   If you want to schedule the addition for a later date or time, click **Schedule** (see Scheduling configuration updates on page 132).

Changing an ANI group

To change an ANI group:

1. Click **Configure > ANI Group > Edit**.

   The **Edit ANI Group** dialog box is displayed.

2. Double-click the ANI group you want to edit.

   The **Edit ANI Group** dialog box is displayed.

3. Enter an ANI number or partial ANI number in the field and click the **Get ANIs** button. You can then edit or remove the ANI numbers that are assigned.

4. Click **Submit**.

   The ANI group is changed and the **Edit ANI Group** dialog box is displayed.

   Note:

   If you want to schedule the change for a later date or time, click **Schedule** (see Scheduling configuration updates on page 132).

5. Click **Close**.

Removing an ANI group

To remove an ANI group:

1. Click **Configure > ANI Group > Remove**.

   The **Remove ANI Group** dialog box is displayed.

2. Double-click the ANI group you want to remove.

   A **Warning** dialog box is displayed asking if you really want to remove the ANI group.

3. Click **Yes** to remove the ANI group, or click **No** to cancel the request.

   The **Remove ANI Group** dialog box is displayed.

4. Click **Close**.

Configuring CED groups

CED groups are used to create special groups of CED collected by a service provider. CEDs are used to better identify groups of customers so that the customers receive special treatment. The CEDs could be customer account numbers, personal ID numbers, and so on.

CAUTION:

Submitting changes to CED groups will cause an interruption to call routing responses. During this interruption, calls are routed using the network failsafe. Submit changes or schedule changes during low- or no-traffic periods.

This section includes the following topics:

- CED group options on page 92
- Adding a CED group on page 93
- Changing a CED group on page 93
- Removing a CED group on page 94

CED group options

The following table describes the CED group options:

Option	Parameters	Notes
CED Group name	Alphanumeric string up to 20 characters	Select a descriptive name for the CED group.
CED number	Numeric string up to 16 digits	Enter a string of digits regularly entered by an incoming caller.
Identifier	Alphanumeric string up to 20 characters	Enter a distinctive name for the caller that uses the CED string.

Adding a CED group

To add a CED group:

1. Click **Configure > CED Group > Add**.

   The **Add CED Group** dialog box is displayed.

2. Populate the dialog box with values as described in CED group options on page 92.

3. Click **Submit**.

   The CED group is added.

   Note:

   If you want to schedule the addition for a later date or time, click **Schedule** (see Scheduling configuration updates on page 132).

Changing a CED group

To change a CED group:

1. Click **Configure > CED Group > Edit**.

   The **Edit CED Group** dialog box is displayed.

2. Double-click the CED group you want to edit.

   The **Edit CED Group** dialog box is displayed.

3. Enter a CED string or partial CED string in the field and click the **Get CEDs** button. You can then edit or remove the CED strings that are assigned.

4. Click **Submit**.

   The CED group is changed and the **Edit CED Group** dialog box is displayed.

   Note:

   If you want to schedule the change for a later date or time, click **Schedule** (see Scheduling configuration updates on page 132).

5. Click **Close**.

Removing a CED group

To remove a CED group:

1. Click **Configure > CED Group > Remove**.

   The **Remove CED Group** dialog box is displayed.

2. Double-click the CED group you want to remove.

   A **Warning** dialog box is displayed asking if you really want to remove the CED group.

3. Click **Yes** to remove the CED group, or click **No** to cancel the request.

   The **Remove CED Group** dialog box is displayed.

4. Click **Close**.

Completing the initial configuration

This section includes the following topics:

- Manually synchronizing the NRSs on page 95
- Backing up the configuration on page 96
- Providing TCP/IP ports to the customer on page 96

Manually synchronizing the NRSs

After you complete the initial configuration, you should manually synchronize the databases between the two servers.

CAUTION:

Do not run manual synchronization while other users are make changes on the NRS.

To manually synchronize the databases:

1. Confirm that you have set up database synchronization. See Setting up database synchronization on page 29 for more information.
2. Do one of the following:
   - If you are on the NRS that has the latest changes, click **File > Sync To Remote DB**.
   - If you are on the NRS that does not have the latest changes, click **File > Sync From Remote DB**.

   A warning dialog box is displayed asking if you want to overwrite the database.
3. Click **Yes** if you want to begin the synchronization, or click **No** to cancel the request.

   The database synchronization begins.

Backing up the configuration

After you complete the initial configuration, you must back up the configuration.

To back up the configuration:

1. Log out of your administrative session so that no changes will be written to disk.
2. On the front of the server, locate the two disk drives. Verify that the green light on the second disk drive is not lit.
3. Remove the second disk drive. This disk drive will be your backup disk drive. Store this disk drive in a secure location away from the server. Be sure to note to which NRS, the disk drive belongs.
4. Install your third disk drive into the second disk drive slot.

   The disk drive is automatically synchronized with the first disk drive.
5. Repeat this procedure for the other NRS.

Providing TCP/IP ports to the customer

For security purposes, customers often block unused TCP/IP ports on their networks. Because of this, you should provide the customer a list of the TCP/IP ports used with the NRS configurations.

To find the TCP/IP ports currently in use, use the following commands:

- Go to **Configure > Network Gateway > Edit** and note the **XML Port Number** for each Network Gateway.
- Go to **Configure > CC Link > Edit** and view the **TCP Port Number** for each CC.

Repeat this procedure for each NRS.

Monitoring system status

This section describes the monitoring features of the NRS and includes the following topics:

- General monitoring strategy on page 98
- Status tab pages on page 99
- Setting the refresh rate for the System Status and Hardware Diagram tabs on page 117
- Changing the date format on page 117
- Generating historical reports on page 118
- Configuring e-mail alerts on page 125

General monitoring strategy

Using the tools described in this section, use the following strategy when monitoring Network Routing:

Monitor both NRSs - Since the NRSs can alternate control of the polling results between the two servers, you should always log in to both NRSs when monitoring the system. Testing has found that IXC carriers sometimes switch control between facilities (specifically, MCI on Wednesdays), so the NRS will react to this and switch "control" between the two servers. The IXC can control which server is currently active and which is on standby. The IXCs currently operate their links as follows:

- Only AT&T uses a true active/standby mode.
- MCI, which uses three RDG links, operates in a manner where you have two links active on one NRS and the other active on the other NRS.
- Sprint has two sites in the United States, which translates to having two links to each NRS. All sites are active and all could be making requests to the NRSs.

Since the NRS links to the Avaya CCs may take different paths, Avaya recommends that you should monitor both NRSs all of the time. The status lights are on the right side of the screen on the status panel, so you can display one behind the other enough to see the status of both NRSs.

Check the general status - On the System Status tab (see Overall system status on page 100), check the CC and Gateway status to confirm there aren't any failures (red indicates a faulty connection).

Check for timeouts - Under the **CC Performance** tab (see CC performance on page 104), see if any CCs are reporting regular timeouts. This may indicate that the networking to that CC is not operating properly or that the default timeout level may need to be adjusted (see Configuring a CC link on the NRS on page 64).

Check the call log - On the **Call Log** tab (see Call log on page 106), check that the calls are being processed with reasonable route response times.

Check for alarms - On the **System Status** tab, there is a list of the latest alarms. Use the **Alarms** tab (see General alarms and events on page 108) and the **Interface Alarms** tab (Interface alarms on page 111).

Status tab pages

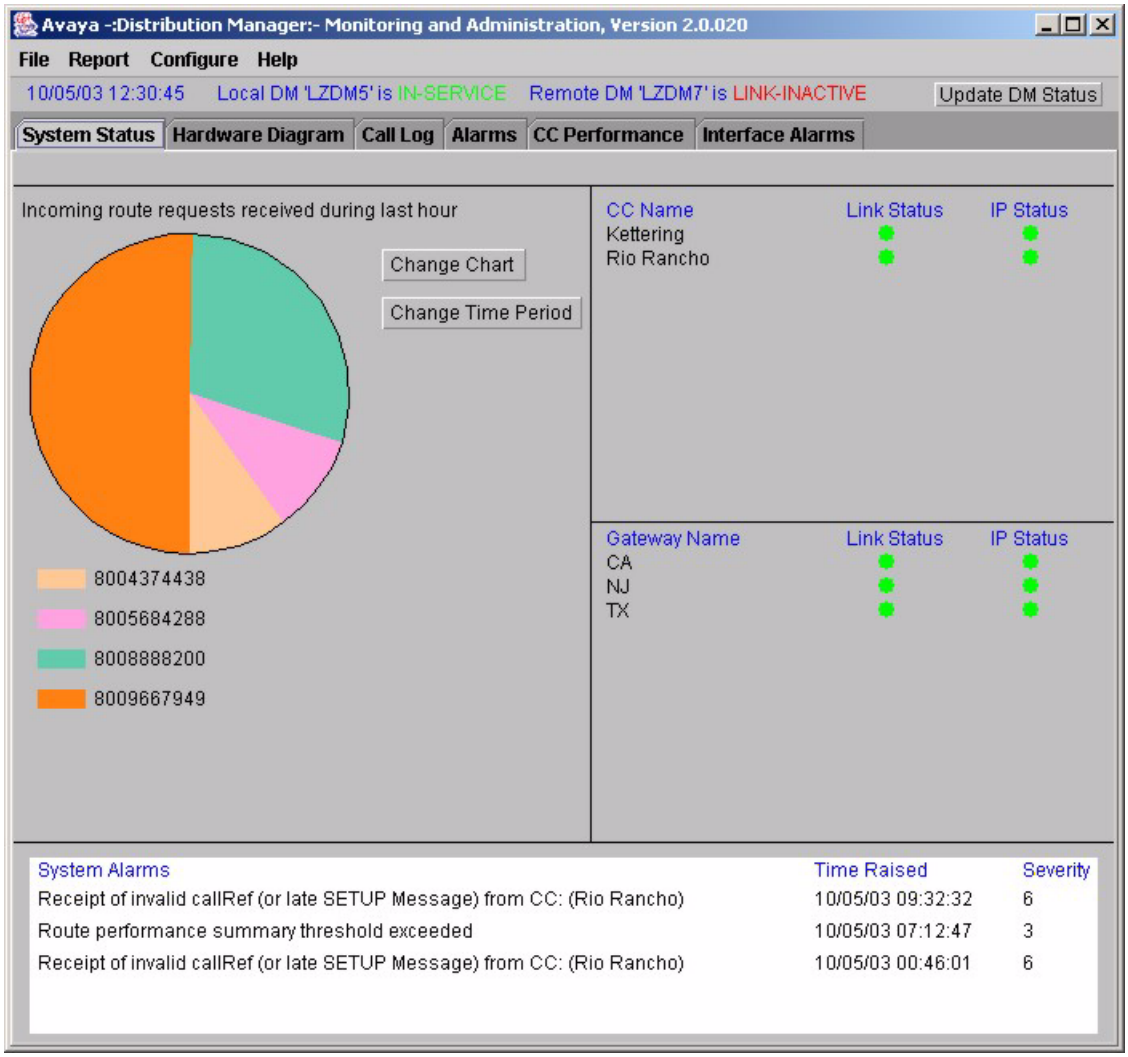
The status tab pages display the current status of the NRS:

- Overall system status on page 100
- CC performance on page 104
- Call log on page 106
- General alarms and events on page 108
- Interface alarms on page 111
- Hardware diagram on page 115

Overall system status

System Status displays overall system status for the NRS.

The following figure shows an example of **System Status**:



System Status is divided into the following areas of information:

- General status on page 101
- Route and CC status on page 101
- CC and Network Gateway status on page 102
- System alarms and events on page 103

General status

Across the top of the tab, the following information is displayed:

- The local time of the NRS
- The status of the local NRS:
  - IN-SERVICE - the NRS is operational
  - OUT-OF-SERVICE - the NRS is out of service
- The status of the remote NRS:
  - IN-SERVICE - the NRS is operational
  - OUT-OF-SERVICE - the NRS is out of service
  - LINK_INACTIVE - the link to the remote NRS is not configured or is out of service.

While viewing **System Status**, you can click **Update DM Status** to get an immediate update of the system status.

Route and CC status

The route and CC status area display pie charts that give the status of how calls have been distributed and how the CCs have been performing over a recent time period. The **Change Chart** and **Change Time Period** buttons control the status displayed in this area.

Note:

If there is no data for the selected status request, a pie chart is not displayed.

By clicking **Change Chart**, you can request status information for the following:

- **Incoming Route Request Numbers** - Displays all requested telephone numbers.
- **Outgoing Route Response Destination ACDs** - Displays the destination ACD (communications server) used to process most incoming calls.
- **CC Reliability (retries)** - Displays the number of polling retries that occurred on each CC.
- **CC Polls** - Displays the number of polls received on each CC.

By clicking **Change Time Period**, you can select the time period from which the status will display. You can select from the following time periods:

- the last *XX* minutes (the value *XX* is based on the short call log flush interval administered with **Configure > Archiving**, multiplied by 3)
- the last hour
- the last 4 hours
- the last 12 hours

- the last 24 hours
- since a specific date and time

The pie charts are color-coded to represent the active request numbers, destination ACDs, and CCs. Under the pie chart is a key that displays numerical values for the representations in the pie chart. You can click and hold the mouse pointer on the color bars to display the actual counts as reported by the NRS. For example, when you display the CC Polls, click one of the resulting color bars. The value shown is the actual number of CC Polls for the selected CC.

CC and Network Gateway status

The right-side area of **System Status** displays the link and IP status of the connections from the NRS to the CCs and Network Gateways. Scroll arrows are displayed if there are more than 12 links.

The status indicators are defined as follows:

Link Status	TCP/IP Status	Description
Green	Green	Both the logical link and IP connections are operating normally.
Green	Red	This status is not likely because when the IP connection is lost, the link connection is also lost. If you do see this condition, check network connectivity.

Link Status	TCP/IP Status	Description
Red	Green	When this status occurs on a Network Gateway link, the physical connection is operating, but a link connection cannot be established. Verify that the software on the Network Gateway is operating normally. When this status occurs on a CC link, the physical connection is operating, but the CC failed to respond to polls from the NRS. Check for timeout errors to the CC. If there are timeout errors, check the IP trunk administration to verify that the interflow number is routing back over the same IP trunk group. Also check the following: ● On the NRS, use the **`/export/dm/status`** command to display the critical processes. There should be three processes running. ● Check the software status on the Network Gateway and on the CCs. ● Network connectivity.
Red	Red	When this status occurs, neither the logical link nor the IP connections are operating properly. To correct this problem, do the following: ● Check the physical link connection. ● Check the IP administration on the NRS, the Network Gateway, and the CCs. ● On the NRS, use the **`/export/dm/status`** command to display the critical processes. There should be three processes running. ● Use the **`ping`** command to verify that you have IP connectivity. ● Check network connectivity.

System alarms and events

The bottom area of **System Status** displays the most recent system alarms and events. There is a brief description of the alarm or event, the time the alarm or event occurred, and the severity of the alarm (1=most severe, 7=least severe).

Note:

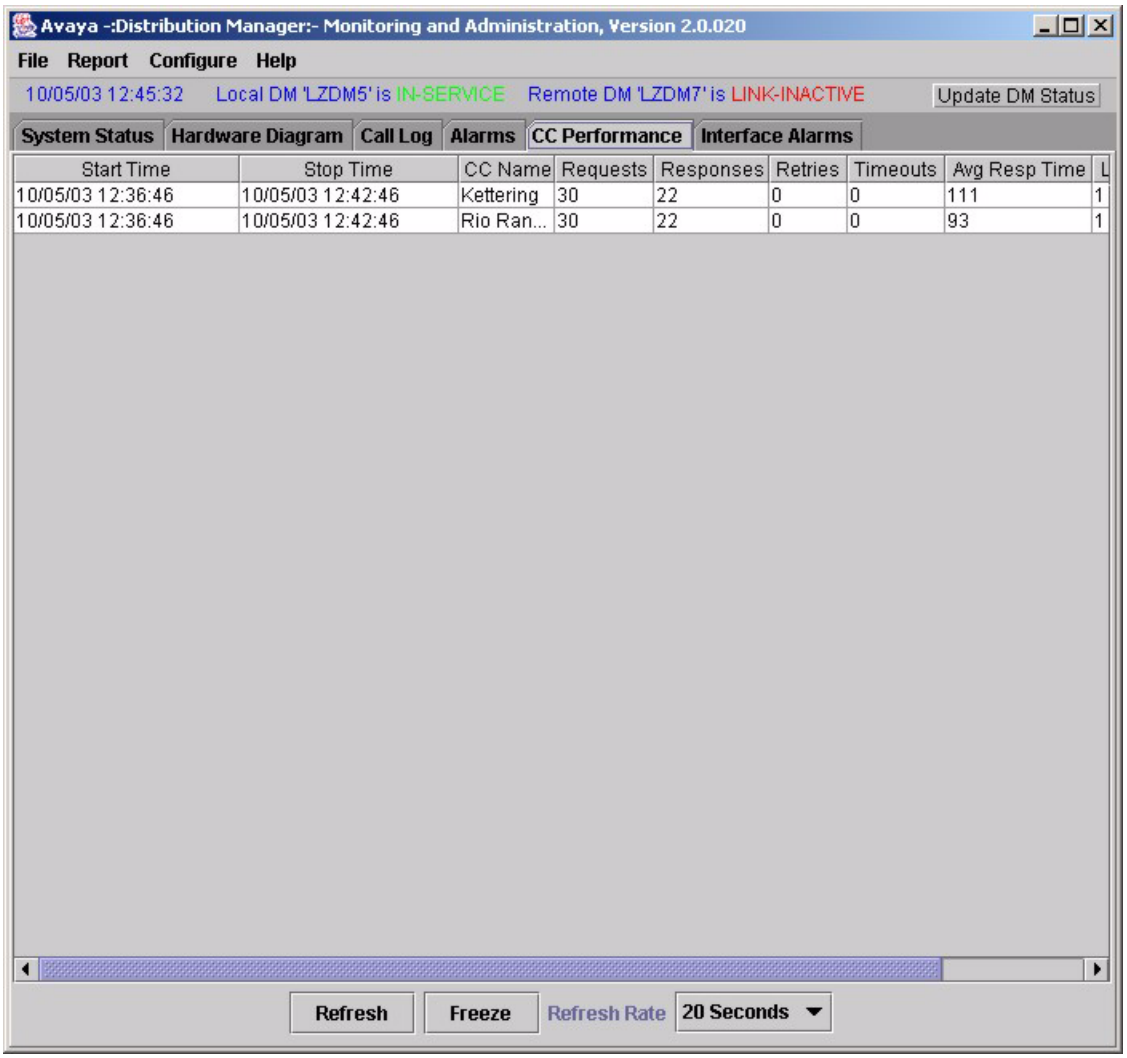
Events do not have a severity level.

For more information about alarms and events, see General alarms and events on page 108.

CC performance

CC Performance displays the most recent status for each CC. The information is logged here before being saved in memory and used for reports (see Generating historical reports on page 118).

The following figure shows an example of **CC Performance**:



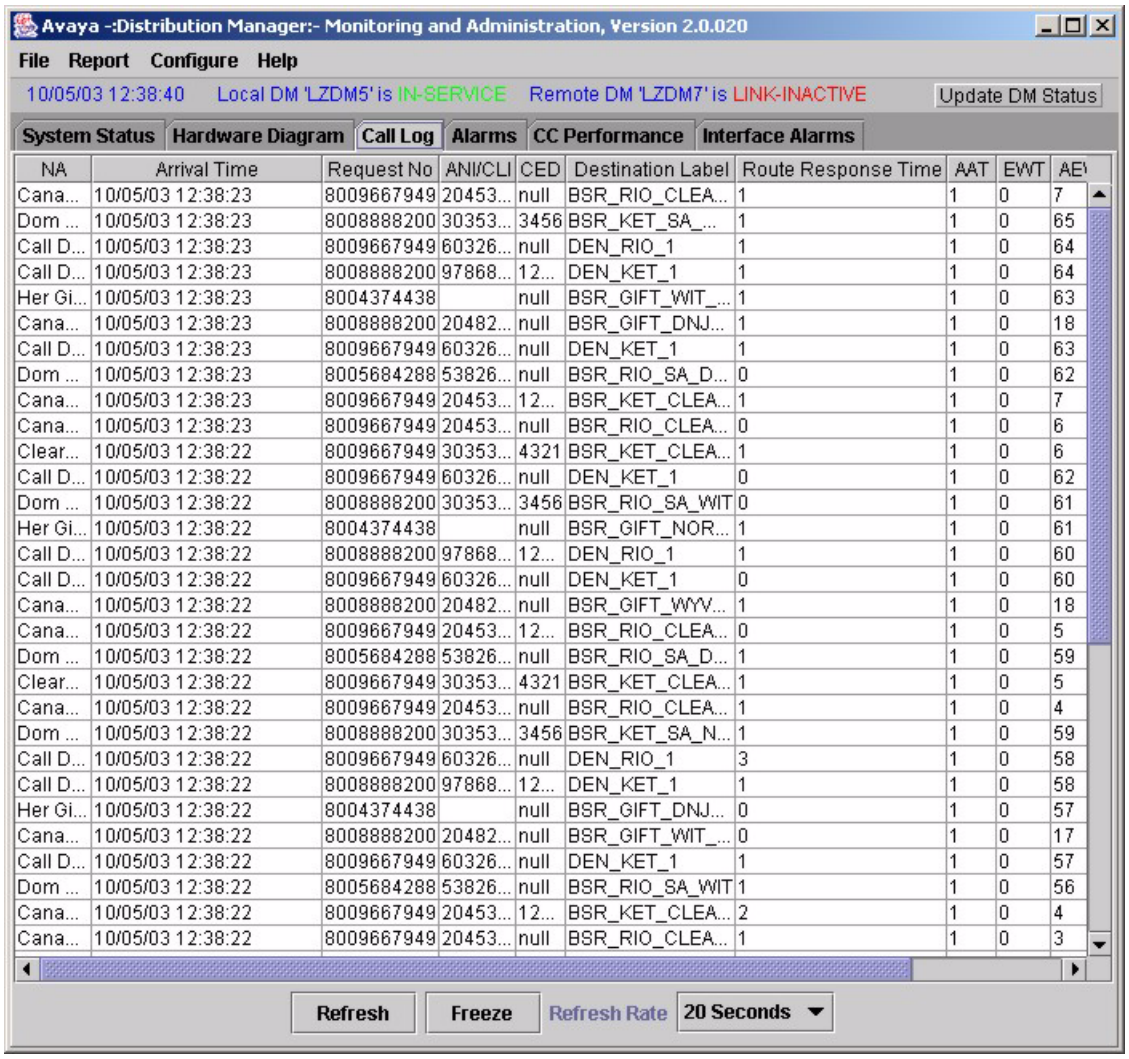
The following table describes the data displayed in the **CC Performance** tab.

Heading	Definition
Start Time/Stop Time	The time interval during which the data for this record has been gathered.
CC Name	The name of the CC.
Requests	The number of poll requests sent to this CC during the interval defined by the Start Time and Stop Time.
Responses	The number of poll responses received from this CC during the interval defined by the Start Time and Stop Time. If there are fewer responses than requests, check the network administration on the NRS and the CCs.
Retries	The number of polling retries.
Timeouts	The number of polling timeouts. **Important:** If you are consistently seeing timeouts, increase the Polling Timeout as needed. See Configuring a CC link on the NRS on page 64 for more information.
Avg Resp Time	The average amount of time (in milliseconds) it takes the CC to respond to a polling request.
Link Avail.	The percentage of time the link to the CC is available for polling.
IP Avail.	The percentage of time the IP connection to the CC is available for polling.

While viewing **CC Performance**, you can click **Refresh** to get an immediate update of the information, click **Freeze** to stop any updates while you view the information, or change the refresh rate for the information.

Call log

The following figure shows an example of **Call Log**:



NA	Arrival Time	Request No	ANI/CLI	CED	Destination Label	Route Response Time	AAT	EWT	AE
Cana...	10/05/03 12:38:23	8009667949	20453...	null	BSR_RIO_CLEA...	1	1	0	7
Dom ...	10/05/03 12:38:23	8008888200	30353...	3456	BSR_KET_SA_...	1	1	0	65
Call D...	10/05/03 12:38:23	8009667949	60326...	null	DEN_RIO_1	1	1	0	64
Call D...	10/05/03 12:38:23	8008888200	97868...	12...	DEN_KET_1	1	1	0	64
Her Gi...	10/05/03 12:38:23	8004374438		null	BSR_GIFT_WIT_...	1	1	0	63
Cana...	10/05/03 12:38:23	8008888200	20482...	null	BSR_GIFT_DNJ...	1	1	0	18
Call D...	10/05/03 12:38:23	8009667949	60326...	null	DEN_KET_1	1	1	0	63
Dom ...	10/05/03 12:38:23	8005684288	53826...	null	BSR_RIO_SA_D...	0	1	0	62
Cana...	10/05/03 12:38:23	8009667949	20453...	12...	BSR_KET_CLEA...	1	1	0	7
Cana...	10/05/03 12:38:23	8009667949	20453...	null	BSR_RIO_CLEA...	0	1	0	6
Clear...	10/05/03 12:38:22	8009667949	30353...	4321	BSR_KET_CLEA...	1	1	0	6
Call D...	10/05/03 12:38:22	8009667949	60326...	null	DEN_KET_1	0	1	0	62
Dom ...	10/05/03 12:38:22	8008888200	30353...	3456	BSR_RIO_SA_WIT	0	1	0	61
Her Gi...	10/05/03 12:38:22	8004374438		null	BSR_GIFT_NOR...	1	1	0	61
Call D...	10/05/03 12:38:22	8008888200	97868...	12...	DEN_RIO_1	1	1	0	60
Call D...	10/05/03 12:38:22	8009667949	60326...	null	DEN_KET_1	0	1	0	60
Cana...	10/05/03 12:38:22	8008888200	20482...	null	BSR_GIFT_WYV...	1	1	0	18
Cana...	10/05/03 12:38:22	8009667949	20453...	12...	BSR_RIO_CLEA...	0	1	0	5
Dom ...	10/05/03 12:38:22	8005684288	53826...	null	BSR_RIO_SA_D...	1	1	0	59
Clear...	10/05/03 12:38:22	8009667949	30353...	4321	BSR_KET_CLEA...	1	1	0	5
Cana...	10/05/03 12:38:22	8009667949	20453...	null	BSR_RIO_CLEA...	1	1	0	4
Dom ...	10/05/03 12:38:22	8008888200	30353...	3456	BSR_KET_SA_N...	1	1	0	59
Call D...	10/05/03 12:38:22	8009667949	60326...	null	DEN_RIO_1	3	1	0	58
Call D...	10/05/03 12:38:22	8008888200	97868...	12...	DEN_KET_1	1	1	0	58
Her Gi...	10/05/03 12:38:22	8004374438		null	BSR_GIFT_DNJ...	0	1	0	57
Cana...	10/05/03 12:38:22	8008888200	20482...	null	BSR_GIFT_WIT_...	0	1	0	17
Call D...	10/05/03 12:38:22	8009667949	60326...	null	DEN_KET_1	1	1	0	57
Dom ...	10/05/03 12:38:22	8005684288	53826...	null	BSR_RIO_SA_WIT	1	1	0	56
Cana...	10/05/03 12:38:22	8009667949	20453...	12...	BSR_KET_CLEA...	2	1	0	4
Cana...	10/05/03 12:38:22	8009667949	20453...	null	BSR_RIO_CLEA...	1	1	0	3

Call Log displays the most recent contents of the short term call log on the NRS. The calls are logged in the call log before being summarized for viewing in the reports (see Generating historical reports on page 118).

Note:

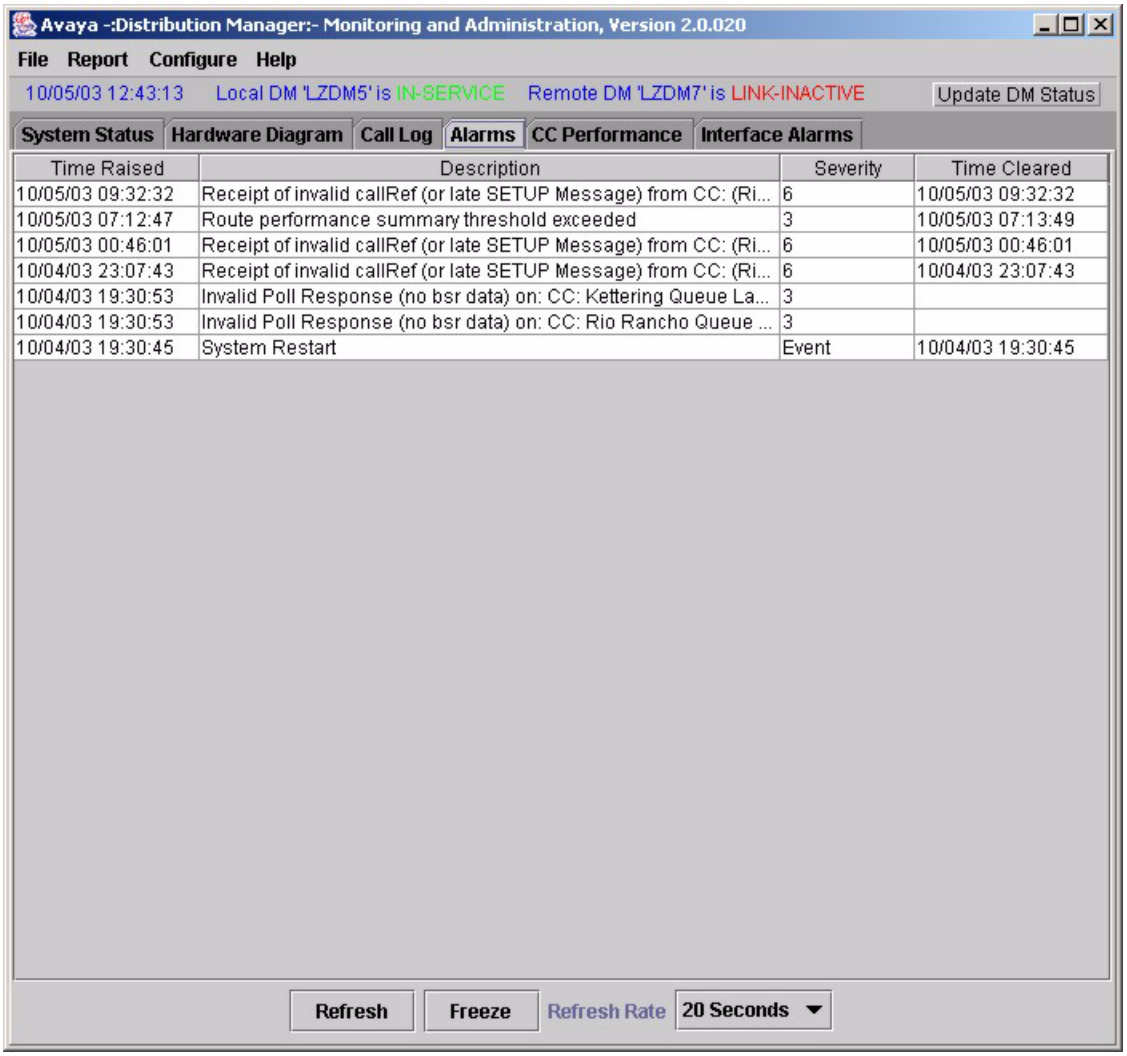
When the NRS is processing a large number of calls, some calls may not appear in the call log, but will be included in report generation.

Heading	Definition
Network Applications	The name of the network application used for the call.
Arrival Time	The date and time the route request was received from the Network Gateway.
Request No.	The route request number received from the Network Gateway.
ANI/CLI	The calling party number included in the route request.
CED	The caller entered digits included in the route request.
Destination Label	The route destination label sent to the Network Gateway.
Route Response Time	The amount of time (in milliseconds) it took to respond to a route request with a route response. When the route response time is over 500 ms, a route response will be sent to the service provider, but the network failsafe route will be used for this call request.
AAT	The Average Advance Time (AAT), in seconds, received from the CC.
EWT	The Expected Wait Time (EWT), in seconds, received from the CC.
AEWT	The local Adjusted EWT (AEWT), in seconds.
Response Type	The response used for the call. For failsafe calls, asynchronous polling is used.

While viewing **Call Log**, you can click **Refresh** to get an immediate update of the log, click **Freeze** to stop any updates while you view the log, or change the refresh rate for the log.

General alarms and events

The following figure shows an example of **Alarms**:



Alarms displays the alarms and events that occur on the NRS. The system will display the 100 most recent alarms and events.

The following table defines the **Alarms** display:

Heading	Definition
Time Raised	The time when the alarm or event occurred
Description	A brief description of the alarm or event
Severity	The severity of the alarm (1=most severe, 7=least severe); events do not have a severity
Time Cleared	The time when the alarm was cleared; events are not cleared

While viewing alarms and events, you can click **Refresh** to get an immediate update of the listing. Click **Freeze** to stop any updates while you view the alarms and events, or change the refresh rate for the alarms and events.

The following table defines each of the alarm and event messages:

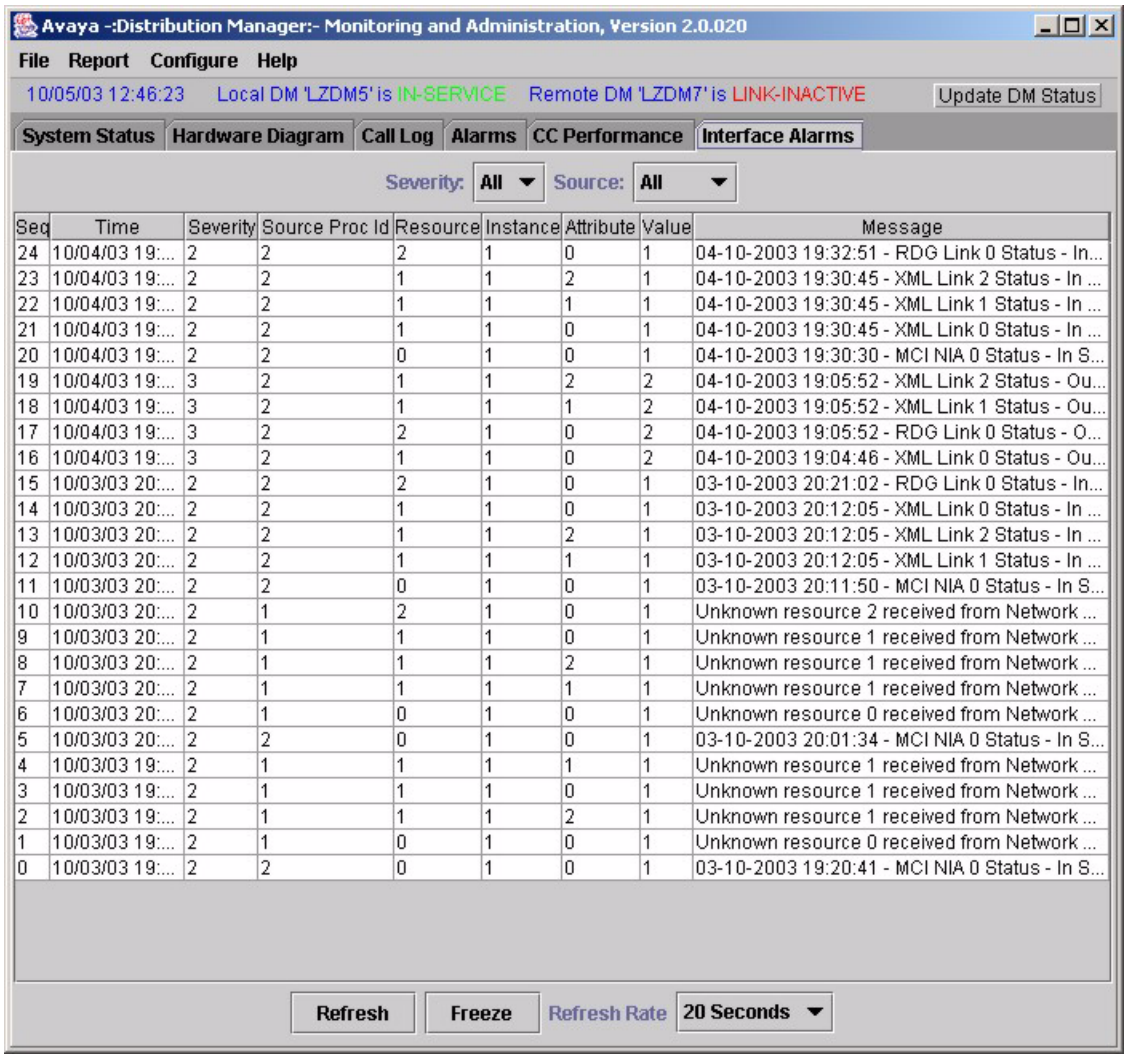
Message	Definition and solution
CC (*CC_Name*) out of service	The NRS has stopped polling to this CC because it did not receive poll responses after the Maximum Number of Retries as configured in CC link options on page 64. The NRS retries polling to this CC at the frequency specified in the Out Of Service Retry Interval as configured in CC link options on page 64. Check the following: • The physical link connection • The IP connection (use the ping command) • IP trunk administration on the CC
CC Link failure for CC: (*CC_Name*)	The link to the CC failed. Check the cabling from the NRS to the CC.
Failsafe Routeing Started for NA: (*Network_Application*)	All CCs used by the network application are out of service (see *CC out of service* message above). Calls using this network application respond with the failsafe destination labels defined for this channel (see Network application options on page 83). Check the following: • The physical link connection • The IP connection (use the ping command) • IP trunk administration on the CC
Invalid Poll Response (no bsr data) on: CC (*CC_Name*) Queue Label: *XXXXX*	A response was received from the CC, but the data was no valid. The VDN or vector were not valid, or the vector was not written correctly.
Link failure to NG: (*NG_Name*)	Either the Link Status or TCP/IP Status has gone to red. See CC and Network Gateway status on page 102 for possible solutions.

Message	Definition and solution
Link to CC process down	The physical connection between the NRS and the CC is operating, but the CC failed to respond to polls from the NRS. Check for timeout errors to the CC. If there are timeout errors, check the IP trunk administration to verify that the interflow number is routing back over the same IP trunk group.
Link to XML process down	The XML link has failed. Check for the following: • Network problems • Hardware failures If there are no network or hardware problems, do the following: • Stop and restart the NRS software. • Stop and restart the Network Gateway software.
System Restart	This indicates that the server rebooted. There is nothing to do except to keep track of frequent reboots, which should not be happening except when rebooted by maintenance personnel. If this is happening without user intervention, escalate the problem using the normal channels.

You can also set up electronic mail alerts when alarms occur (see Configuring e-mail alerts on page 125).

Interface alarms

The following figure shows an example of **Interface Alarms** (in this example, MCI interface alarms):



Seq	Time	Severity	Source Proc Id	Resource	Instance	Attribute	Value	Message
24	10/04/03 19:...	2	2	2	1	0	1	04-10-2003 19:32:51 - RDG Link 0 Status - In...
23	10/04/03 19:...	2	2	1	1	2	1	04-10-2003 19:30:45 - XML Link 2 Status - In ...
22	10/04/03 19:...	2	2	1	1	1	1	04-10-2003 19:30:45 - XML Link 1 Status - In ...
21	10/04/03 19:...	2	2	1	1	0	1	04-10-2003 19:30:45 - XML Link 0 Status - In ...
20	10/04/03 19:...	2	2	0	1	0	1	04-10-2003 19:30:30 - MCI NIA 0 Status - In S...
19	10/04/03 19:...	3	2	1	1	2	2	04-10-2003 19:05:52 - XML Link 2 Status - Ou...
18	10/04/03 19:...	3	2	1	1	1	2	04-10-2003 19:05:52 - XML Link 1 Status - Ou...
17	10/04/03 19:...	3	2	2	1	0	2	04-10-2003 19:05:52 - RDG Link 0 Status - O...
16	10/04/03 19:...	3	2	1	1	0	2	04-10-2003 19:04:46 - XML Link 0 Status - Ou...
15	10/03/03 20:...	2	2	2	1	0	1	03-10-2003 20:21:02 - RDG Link 0 Status - In...
14	10/03/03 20:...	2	2	1	1	0	1	03-10-2003 20:12:05 - XML Link 0 Status - In ...
13	10/03/03 20:...	2	2	1	1	2	1	03-10-2003 20:12:05 - XML Link 2 Status - In ...
12	10/03/03 20:...	2	2	1	1	1	1	03-10-2003 20:12:05 - XML Link 1 Status - In ...
11	10/03/03 20:...	2	2	0	1	0	1	03-10-2003 20:11:50 - MCI NIA 0 Status - In S...
10	10/03/03 20:...	2	1	2	1	0	1	Unknown resource 2 received from Network ...
9	10/03/03 20:...	2	1	1	1	0	1	Unknown resource 1 received from Network ...
8	10/03/03 20:...	2	1	1	1	2	1	Unknown resource 1 received from Network ...
7	10/03/03 20:...	2	1	1	1	1	1	Unknown resource 1 received from Network ...
6	10/03/03 20:...	2	1	0	1	0	1	Unknown resource 0 received from Network ...
5	10/03/03 20:...	2	2	0	1	0	1	03-10-2003 20:01:34 - MCI NIA 0 Status - In S...
4	10/03/03 19:...	2	1	1	1	1	1	Unknown resource 1 received from Network ...
3	10/03/03 19:...	2	1	1	1	0	1	Unknown resource 1 received from Network ...
2	10/03/03 19:...	2	1	1	1	2	1	Unknown resource 1 received from Network ...
1	10/03/03 19:...	2	1	0	1	0	1	Unknown resource 0 received from Network ...
0	10/03/03 19:...	2	2	0	1	0	1	03-10-2003 19:20:41 - MCI NIA 0 Status - In S...

Interface Alarms displays the 100 most recent alarms for the service provider interface cards. Using the **Severity** and **Source** drop-down menus, you can select any one severity level (or all), or you can select any one interface source (or all).

The following table defines the Interface **Alarms** display:

Heading	Definition
Seq	The sequence of the alarm message
Time	The time when the alarm occurred
Severity	The severity of the alarm (1=most severe, 7=least severe)
Source Proc ID	Not meaningful in this release
Resource	Not meaningful in this release
Instance	Not meaningful in this release
Attribute	Not meaningful in this release
Value	Not meaningful in this release
Message	The interface alarm message

While viewing **Interface Alarms**, you can click **Refresh** to get an immediate update of the information, click **Freeze** to stop any updates while you view the information, or change the refresh rate for the information.

The following table defines each of the interface alarm messages:

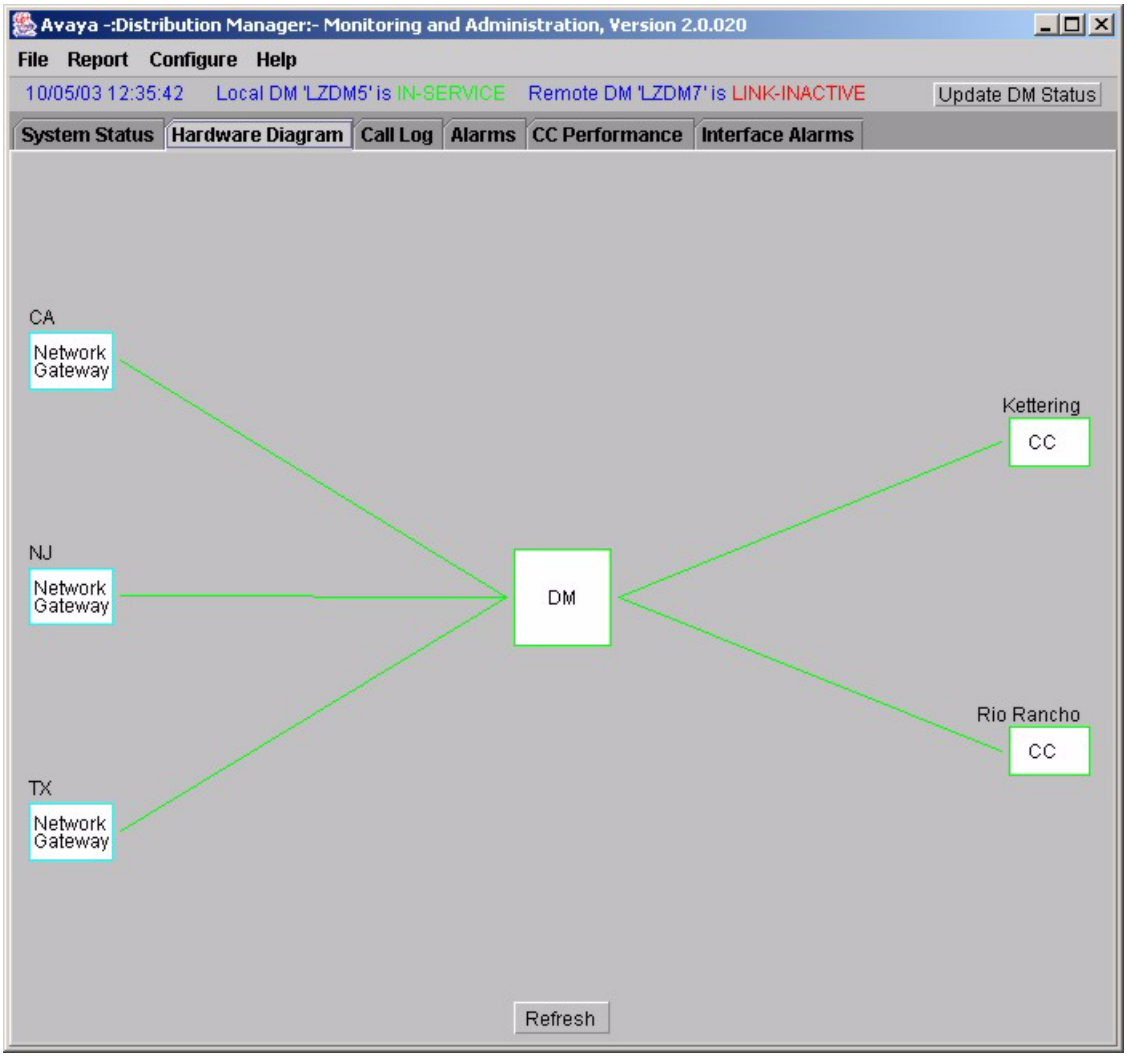
Message	Definition and solution
Application - In Service	The application is in service.
Application - Out Of Service	The application is out of service.
C7 Circuit - Out Of Service	This alarm will have no affect on the system if received.
C7 Circuit Local Block - Out Of Service	This alarm will have no affect on the system if received.
C7 Circuit Remote Block - Out Of Service	This alarm will have no affect on the system if received.
C7 Node - Out Of Service	This alarm will have no affect on the system if received.
C7 Node - In Service	If these alarm are seen, the **`milborne.cfg`** configuration file option `:!SuppressNodes` should be set to 1.
C7 Mpac Card - In Service	The MPAC card is working properly.

Message	Definition and solution
C7 Mpac Card - Out Of Service	Very severe. All signalling links to the AT&T network on this card are lost.
C7 Pcm Cable - In Service	The physical cable is working properly.
C7 Pcm Cable - Out Of Service	Severe. The physical cable is bad and the signalling link associated with this cable is lost too.
C7 Routeset - In Service	This means that all the routes on that routeset to the AT&T network are working properly.
C7 Routeset - Out Of Service	Severe. This means that all the routes on that routeset to the AT&T network will be lost.
C7 Signalling Link *X* Status - In Service	This means that a signalling link to the AT&T network is working properly.
C7 Signalling Link *X* Status - Out Of Service	Severe. This means that a signalling link to the AT&T network will be lost.
Destination *X* Status - In Service	This means that access to the AT&T network has returned.
Destination *X* Status - Out Of Service	Severe. This means that access to the AT&T network has been lost.
Link to Network Operator - In Service	The link to the network operator (RDG for MCI or SCP for Sprint) is in service.
Link to Network Operator - Out Of Service	The link to the network operator (RDG for MCI or SCP for Sprint) is out of service.
Mau Link - Out Of Service	This alarm will have no affect on the system if received.
MCI NIA *X* Status - In Service	MCI NIA is the MCI adaptor process that talks to the MCI links and the XML server.
MCI NIA *X* Status - Out Of Service	The MCI link is out of service.
Mtp Link	Very severe. This means that an internal TCP/IP connection has been lost between the MTP and TCAP processes. All messages inbound and outbound from the AT&T NIA will be lost.
RDG Link *X* Status - In Service	The link to one of the MCI RDG sites has come back into service. The three RDG links are only in service on one NRS at a time if they are configured Active/ Standby. If configured in shared mode, then all the links are up to both NRSs.

Message	Definition and solution
RDG Link *X* Status - Out Of Service	The link to one of the MCI RDG sites has gone out of service. During weekly testing by MCI, the links can go Out Of Service for a minute. This is usually done in the early hours of Wednesday morning. Contact MCI if this occurs.
Sms Link - Out Of Service	This alarm will have no affect on the system if received.
Tcap Link	Very severe. This means that an internal TCP/IP connection has been lost between the TCAP and ICP processes. All messages inbound and outbound from the AT&T NIA will be lost.
Trap Link	Lowest severity. This is the Alarm Adaptor link resource. An alarm will be sent on this link to indicate that the link is In Service but obviously not when it has gone Out Of Service.
Unknown resource *X* received from Network	An unknown request has been received from the network.
XML Link *X* Status - In Service	The XML links are in service if the XML server is up and the translations are correct. XML Link is the link from the PSA process to the XML server within the NRS.
XML Link *X* Status - Out Of Service	The XML links are down or the translations are incorrect.

Hardware diagram

The following figure shows an example of **Hardware Diagram**:



Hardware Diagram shows a basic configuration diagram of each Network Routing component connected to the NRS. The lines between each device are green when the link is operating and red when the link is not operating. Scroll arrows are displayed if there are more than 12 links.

You can configure different components of the configuration by right-clicking on certain areas of the diagram:

Right-click	To configure	See
Background	Network Gateway link	Adding a Network Gateway link on page 57
	CC link	Adding a CC link on page 65
Network Gateway	Network Gateway link	Changing a Network Gateway link on page 58 Removing a Network Gateway link on page 59
	Network Gateway setup and monitoring	Connecting and configuring the interface cards on page 35
DM	Network applications	Configuring network applications on page 83
	Scheduled updates	Deleting an event on page 134
CC	CC link	Changing a CC link on page 66 Removing a CC link on page 66

While viewing **Hardware Diagram**, you can click **Refresh** to get an immediate update of the diagram.

Setting the refresh rate for the System Status and Hardware Diagram tabs

You can set the refresh rate for the **System Status** and **Hardware Diagram** tabs to 1 or 6 minutes, or have no refresh rate. If you turn off the refresh rate, you must manually refresh the **System Status** by clicking the **Update DM Status** button and the **Hardware Diagram** by clicking the **Refresh** button.

Note:

The **CC Performance**, **GP Performance**, **Call Log**, **General Alarms**, and **Interface Alarms** tabs have individual refresh rates that you can set on each tab.

To set the refresh rate for the status tabs:

1. Click **File > Change Refresh Rate**.

   The **Select Refresh Rate** dialog box is displayed.

2. Double-click the refresh rate you want.

   The **Select Refresh Rate** dialog box is closed.

Note:

The new refresh rate will take effect after the next scheduled refresh or after a manual refresh.

Changing the date format

The date format on the status tab pages and reports can be either month/day/year (default) or day/month/year. Once you have changed the date format, the selected date format is used every time you log in to the NRS.

To change the date format:

1. Click **File > Change Date Format**.
2. Select either **Month/Day/Year** or **Day/Month/Year**.

   All status tab pages and reports now show the selected date format.

Generating historical reports

To troubleshoot problems with the Network Routing configuration, run regular reports to check for long response times (over 500 ms) and large numbers of retries and timeouts.

This section includes the following topics:

- Request number reports on page 119
- Destination label reports on page 120
- CC reports on page 121
- Network application reports on page 122
- Polling group reports on page 123
- Printing reports on page 124

Report graph characteristics

Each report graph has the following characteristics:

- The reports are displayed as statistical graphs in a new window. This allows you to display any number of reports at the same time.
- The local date and time when you requested the report is displayed on the graph.
- Shared reports add the data from both NRSs. These shared reports will only be accurate if the clocks on the NRSs are within 3 minutes of each other.
- The horizontal axis displays the selected time period for the report. The vertical axis displays the statistical value range of the selected report.
- Multiple report statistics are shown in different colors.
- Each graph displays a key that shows the following:
  - The colors used for each type of report
  - The total or average count, depending on the type of report
- You can click and hold the mouse button within the graph area to display a precise value for that location in the graph.
- You can print the report graphs (see Printing reports on page 124).

Note:

None of the Network Routing report data can be compared with reports generated by Avaya Call Management System (CMS) or Avaya BCMS.

Request number reports

Call routing reports provide historical information on one or more route request numbers.

To generate a request number report:

1. Do one of the following:
   - Click **Report > Call Routeing > Request Number**.
   - Click **Report > Shared DM Reports > Call Routeing > Request Number**.

   The **Select data for report** dialog box is displayed.
2. Click the request number, the report statistic you want, and the time period for the report.

   Note:

   To generate a number of reports, you can select more than one request number or more than one report statistic. Press and hold the **Ctrl** key to select each item with the mouse, or press and hold the **Shift** key to select a range of items with the mouse. You cannot select multiple numbers *and* multiple report statistics.

   The request number report statistics include the following:

Statistic	Description
Number of Calls	Reports the number of calls for the selected request number.
Average Response Time (ms)	Reports the average response time for route responses completed for the selected request number.
No. Failsafe Calls	Reports the number of times a failsafe destination label was used for the selected request number.

3. Click **OK**.

   A report window is displayed, showing a graph of the requested information. If you select several report statistics, you may get more than one report window.

Destination label reports

Destination label reports provide historical information on one or more destination labels.

To generate a destination label report:

1. Do one of the following:
   - Click **Report > Call Routeing > Destination Label**.
   - Click **Report > Shared DM Reports > Call Routeing > Destination Label**.

   The **Select data for report** dialog box is displayed.
2. Click the destination label, the report statistic you want, and the time period for the report.

   Note:

   To generate a number of reports, you can select more than one destination label or more than one report statistic. Press and hold the **Ctrl** key to select each item with the mouse, or press and hold the **Shift** key to select a range of items with the mouse. You cannot select multiple numbers *and* multiple report statistics.

   The destination label report statistics include the following:

Statistic	Description
Number of Calls	Reports the number of calls for the selected destination label.
Average Response Time (ms)	Reports the average response time for route responses completed for the selected destination label.

3. Click **OK**.

   A report window is displayed, showing a graph of the requested information. If you select several report statistics, you may get more than one report window.

CC reports

CC reports provide historical information on the performance of one or more CCs.

To generate a CC report:

1. Click **Report > CC**.

   The **Select data for report** dialog box is displayed.

2. Click the CC name, the report statistic you want, and the time period for the report.

   Note:

   To generate a number of reports, you can select more than one CC or more than one report statistic. Press and hold the **Ctrl** key to select each item with the mouse, or press and hold the **Shift** key to select a range of items with the mouse. You cannot select multiple CCs *and* multiple report statistics.

   The CC report statistics include the following:

Statistic	Description
No. Requests Received	Reports the number of route requests received for the selected CC.
No. Responses Sent	Reports the number of route responses sent by the selected CC.
No. of Retries	Reports the number of route request retries for the selected CC.
No. of Timeouts	Reports the number of timeouts that occurred on the selected CC. When a timeout occurs, the route request uses a failsafe route administered at the IXC routing database.
Average Response Time (ms)	Reports the average response time for route responses completed for the selected CC. Ideally, the route response time should be under 500 ms. If the route response time is consistently over 500 ms, the network should be analyzed for potential improvements.
Link Availability (%)	Reports the percentage of time the link is available from the CC to the NRS.

3. Click **OK**.

   A report window is displayed, showing a graph of the requested information. If you select several report statistics, you may get more than one report window.

Network application reports

Network application reports provide historical information on one or more network applications. The report data for network applications is gathered from both NRSs when the links are active and you select the shared reports.

To generate a network application report:

1. Do one of the following:
   - Click **Report > Network Application**.
   - Click **Report > Shared DM Reports > Network Application**.

   The **Select data for report** dialog box is displayed.
2. Click the network application, the report statistic you want, and the time period for the report.

   Note:

   To generate a number of reports, you can select more than one network application or more than one report statistic. Press and hold the **Ctrl** key to select each item with the mouse, or press and hold the **Shift** key to select a range of items with the mouse. You cannot select multiple numbers *and* multiple report statistics.

   The network application report statistics include the following:

Statistic	Description
Number of Calls	Reports the number of calls for the selected network application.

3. Click **OK**.

   A report window is displayed, showing a graph of the requested information. If you select several report statistics, you may get more than one report window.

Polling group reports

Polling group reports provide historical information on one or more polling groups. The report data for polling groups is gathered from both NRSs when the links are active.

To generate a polling group report:

1. Click **Report > Network Application**.

   The **Select data for report** dialog box is displayed.

2. Click the polling group, the report statistic you want, and the time period for the report.

   Note:

   To generate a number of reports, you can select more than one polling group or more than one report statistic. Press and hold the **Ctrl** key to select each item with the mouse, or press and hold the **Shift** key to select a range of items with the mouse. You cannot select multiple numbers *and* multiple report statistics.

   The polling group report statistics include the following:

Statistic	Description
Number of Calls	Reports the number of calls for the selected polling group.

3. Click **OK**.

   A report window is displayed, showing a graph of the requested information. If you select several report statistics, you may get more than one report window.

Printing reports

To print a report:

1. Right-click anywhere in the graph window.

   A **Print** pop-up is displayed.

2. Click **Print**.

   A warning message is displayed asking if you want to print the report.

3. Click **Yes**.

   The Windows **Print** dialog box is displayed.

4. Modify the print properties as required.

5. Click **OK**.

   The graph is sent to the selected printer.

Configuring e-mail alerts

You can configure the NRS to send electronic mail to notify users of DM alarms and interface alarms on the server. For the DM alarms, any alarms that are resolved within two minutes of occurring are not emailed.

This section includes the following topics:

- E-mail alert options on page 125
- Adding recipients to the e-mail alert database on page 126
- Changing e-mail alert user parameters on page 126
- Deleting recipients from the e-mail alert database on page 127

Important:
You must coordinate e-mail alert with the customer to operate within the customer's corporate e-mail and firewall setup.

E-mail alert options

The following table describes the e-mail alert options:

Option	Parameters	Notes
User Name	Any valid name	Enter the name of the person receiving the e-mail alerts.
Email Address	Any valid e-mail address	Enter the e-mail address for the person receiving the e-mail alerts.
Severity Threshold	1-7 (default=7)	Defines which severity of alarms will generate an e-mail alert. The user will receive all alarms up to the selected threshold. For example, if you select severity threshold 4, the user will receive alerts for thresholds 1 through 4 (more severe alarms), but not 5 through 7 (less severe alarms).

Adding recipients to the e-mail alert database

To add a recipient to the e-mail alert database:

1. Click **File > Email Alarms**.

   The **Email Alarm Configuration** dialog box is displayed.

2. Click **Add**.

   The **User Details** dialog box is displayed.

3. Populate the dialog box with values as described in E-mail alert options on page 125.

4. Click **Submit**.

   A new recipient is added to the e-mail alert database. The **Email Alarm Configuration** dialog box is displayed showing the new user.

5. Click **Close**.

Changing e-mail alert user parameters

To change the attributes for a recipient receiving e-mail alerts:

1. Click **File > Email Alarms**.

   The **Email Alarm Configuration** dialog box is displayed.

2. Double-click the user you want to change.

   The **User Details** dialog box is displayed.

3. Change the dialog box with values as described in E-mail alert options on page 125.

4. Click **Submit**.

   The e-mail alert database is updated. The **Email Alarm Configuration** dialog box is displayed showing the change.

5. Click **Close**.

Deleting recipients from the e-mail alert database

To delete a recipient from the e-mail alert database:

1. Click **File > Email Alarms**.

   The **Email Alarm Configuration** dialog box is displayed.

2. Click the recipient you want to delete.
3. Click **Delete**.

   A **Warning** dialog box is displayed asking if you want to delete this recipient.

4. Click **Yes**.

   The recipient is removed from the e-mail alert database. The **Email Alarm Configuration** dialog box is displayed showing that the user has been removed.

5. Click **Close**.

Ongoing configuration, maintenance, and troubleshooting

There are several procedures you can do to maintain and troubleshoot the databases, configurations, and hardware on the NRS.

This section includes the following topics:

- Updating the configuration on page 130
- Scheduling configuration updates on page 132
- Backing up the NRS on page 135
- Restoring the NRS on page 135
- Stopping and restarting the Distribution Manager application on an NRS on page 136
- Stopping and restarting the Informix application on an NRS on page 137
- Rebooting an NRS on page 138
- Shutting down an NRS on page 139
- Upgrading the application software on page 140
- Troubleshooting on page 141

Contact Avaya for support with any hardware failures on an NRS, the operating system, or Informix.

Updating the configuration

After you have done the initial configuration at installation, you will occasionally need to update your existing Network Routing configuration. This section describes typical scenarios that will require changes and lists which procedures to use to make those changes.

This section includes the following topics:

- Adding CCs on page 130
- Adding VDNs and vectors on page 130
- Adding network applications on page 131
- Adding destinations on page 131
- Manually synchronizing the NRSs on page 131

Adding CCs

When you add a new CC, you must do the procedures in the following sections:

- Configuring CC links, IP trunks, and vectors on page 61 to create your links from the CC to the NRSs and to set up the VDNs and vectors
- Configuring polling groups and network applications on page 79 to create the polling groups and network applications

Adding VDNs and vectors

When you have new VDNs and vectors, you must do the procedures in the following sections:

- Administering status polling vectors and VDNs on each CC on page 76 to create the VDNs and vectors used for polling
- Configuring polling groups and network applications on page 79 to create the polling groups and network applications

Adding network applications

When you add new network applications, you must do the procedures in the following sections:

- Configuring polling groups on page 80 to create a polling group to be used with the network application
- Configuring network applications on page 83 to associate a polling group to a network application

Adding destinations

When you add new destinations, you must do the procedures in the following sections:

- Configuring network applications on page 83 to add new destinations to existing network applications or create new network applications for the new destinations

Manually synchronizing the NRSs

After you complete the configuration changes, you should manually synchronize the databases between the two servers.

CAUTION:
Do not run manual synchronization while other users are make changes on the NRS.

To manually synchronize the databases:

1. Confirm that you have set up database synchronization. See Setting up database synchronization on page 29 for more information.
2. Do one of the following:
   - If you are on the NRS that has the latest changes, click **File > Sync To Remote DB**.
   - If you are on the NRS that does not have the latest changes, click **File > Sync From Remote DB**.

   A warning dialog box is displayed asking if you want to overwrite the database.
3. Click **Yes** if you want to begin the synchronization, or click **No** to cancel the request.

   The database synchronization begins.

Scheduling configuration updates

When making changes to a configuration, you can schedule a configuration change to occur once, on a frequent basis, on a weekly basis, or on a monthly basis. You can schedule updates to occur during low-traffic periods or before a special event such as a holiday or sale.

This section contains the following information about scheduling configuration updates:

- Setting a one-time update on page 132
- Setting a frequent update on page 132
- Setting a weekly update on page 133
- Setting a monthly update on page 133
- Updating an event on page 134
- Deleting an event on page 134

Setting a one-time update

To schedule a configuration update to occur once:

1. After entering data into a configuration dialog box, click **Schedule**.

   The **Events Scheduling** dialog box is displayed.

2. Enter a name for the event. This should be a meaningful name that you can remember if you must later delete the event.
3. Enter the date and time you want the event to occur.
4. Click **OK**.

Setting a frequent update

To schedule a configuration update to occur on a recurring basis:

1. After entering data into a configuration dialog box, click **Schedule**.

   The **Events Scheduling** dialog box is displayed.

2. Enter a name for the event. This should be a meaningful name that you can remember if you must later delete the event.
3. Enter the date and time you want the event to occur first.

4. Select the **Frequent** recurrence pattern.
5. Set the frequency of the event. For example, if you select 00 hours and 30 minutes, the event will occur every 30 minutes.
6. Click **OK**.

Setting a weekly update

To schedule a configuration update to occur at the same time every week:

1. After entering data into a configuration dialog box, click **Schedule**.

   The **Events Scheduling** dialog box is displayed.
2. Enter a name for the event. This should be a meaningful name that you can remember if you must later delete the event.
3. Select the date when you want this weekly event to start occurring. The default date is today.
4. Enter the time of day you want the event to occur.
5. Select the **Weekly** recurrence pattern.
6. Select the day (or days) of the week you want the event to occur.
7. Click **OK**.

Setting a monthly update

To schedule a configuration update to occur at the same time every month:

1. After entering data into a configuration dialog box, click **Schedule**.

   The **Events Scheduling** dialog box is displayed.
2. Enter a name for the event. This should be a meaningful name that you can remember if you must later delete the event.
3. Enter the time of day you want the event to occur. Do not set the date.
4. Select the **Monthly** recurrence pattern.
5. Select the day of the month you want the event to occur.

   Note:

   If you select days 29, 30, or 31, and the month has fewer days than the day selected, the event will run on the last day of the month.
6. Click **OK**.

Updating an event

To update a scheduled event:

1. Delete the event as described in Deleting an event on page 134.
2. Reschedule the event as described in Scheduling configuration updates on page 132.

Deleting an event

To delete a scheduled event:

1. Click **Configure > Scheduled Configuration Updates**.

   The **Scheduled Events** dialog box is displayed.
2. Click the event you want to delete.

   The event is highlighted.
3. Click **Delete**.

   A **Warning** dialog box is displayed.
4. Click **Yes**.

   The **Scheduled Events** dialog box is displayed, showing that the event was deleted.
5. Click **Close**.

Backing up the NRS

This section shows you how to back up the NRS. Avaya recommends that you back up the NRS immediately after initial installation and configuration, and then every week after installation or after you make significant configuration changes.

To back up the NRS:

1. Log out of your administrative session so that no changes will be written to disk.
2. On the front of the server, locate the two disk drives. Verify that the green light on the second disk drive is not lit.
3. Remove the second disk drive. This disk drive will be your backup disk drive. Store this disk drive in a secure location away from the server. Be sure to note to which NRS, the disk drive belongs.
4. Install your third disk drive (your previous backup disk drive) into the second disk drive slot.

   The disk drive is automatically synchronized with the first disk drive.
5. Repeat this procedure for the other NRS.

Restoring the NRS

Restoring an NRS after catastrophic failure is not a procedure that should be done without assistance from Avaya. Contact Avaya for assistance.

Stopping and restarting the Distribution Manager application on an NRS

To stop and restart the Distribution Manager application on an NRS:

1. From a telnet interface window on a PC or server, enter:

   telnet *IP_address*

   where ***IP_address*** is the IP address assigned to the NRS.
2. Log on to the server as **informix**.
3. Enter:

   su - root
4. Enter the **root** password when prompted.
5. Enter the following commands to stop and restart the Distribution Manager application:

   cd /export/dm

   ./stop-all

   ./go-psa

Stopping and restarting the Informix application on an NRS

To stop and restart the Informix application on an NRS:

1. From a telnet interface window on a PC or server, enter:

   telnet *IP_address*

   where ***IP_address*** is the IP address assigned to the NRS.
2. Log on to the server as **informix**.
3. Enter:

   su - root
4. Enter the **root** password when prompted.
5. Enter:

   cd /export/dm
6. Enter:

   ./stop-all

   This stops the Distribution Manager application, which is required before stopping Informix.
7. Enter:

   exit

   This changes the user login back to **informix** from **root**.
8. Enter:

   onmode -ky
9. After waiting 10 seconds for the Informix database to come down and stabilize, enter:

   oninit
10. Enter:

    su - root
11. Enter the **root** password when prompted.
12. After waiting 30 seconds for the Informix database to settle, enter:

    ./go-psa

    This restarts the Distribution Manager application.

Rebooting an NRS

Should the server temporarily lose power or become disconnected from the network, you might not be able to access the server over the network. With this condition, you must reboot the server.

Note:

During reboot, the system may display a screen and message that says hardware has been removed or new hardware detected. This is caused by variations in keyboards, mice, and monitors. Normally, Red Hat Linux detects these changes correctly and you only have to verify or acknowledge the changes. This message should be acknowledged. Otherwise, each time the server is rebooted, it will delay or wait for a response to the detected changes.

To reboot the server:

1. Verify that the server is connected to power, that the power is on, and that the server is connected to the customer network.
2. From a telnet interface window on a PC or server, enter:

   `telnet` ***`IP_address`***

   where ***`IP_address`*** is the IP address assigned to the NRS.
3. Log on to the server as **`informix`**.
4. Enter:

   `su - root`
5. Enter the **`root`** password when prompted.
6. Enter:

   `reboot`

   The server reboots. This will interrupt your telnet session.
7. Verify that the server can be accessed over the network. If the server still cannot be accessed over the network, escalate using the normal procedure.

Shutting down an NRS

To shut down and power off an NRS:

1. From a telnet interface window on a PC or server, enter:

   telnet *IP_address*

   where ***IP_address*** is the IP address assigned to the NRS.
2. Log on to the server as root.
3. Enter:

   shutdown

   The server shuts down. This will interrupt your telnet session.
4. Turn off power to the NRS.

Upgrading the application software

To upgrade the application software:

1. Save your old configuration files. The files you must save include:
   - **`/export/dm/PsaProperties`**
   - **`/etc/profile`**
   - **`/var/www/html`**
   - **`/export/att/adapter.xml`** (AT&T configuration only)
   - **`/export/mci/adapter.xml`** (MCI configuration only)
   - **`/etc/wanpipe/*.conf`** (Sprint configuration only - there will be 2 to 4 configuration files)

   Save these files with the format of ***`filename.mo-da-yr`***, where ***`filename`*** is the name of the configuration file, ***`mo`*** is the two-digit month, ***`da`*** is the two-digit day of the month, and ***`yr`*** is the last two digits of the year. Determine the proper date extension by using the **`ls -la`** ***`filename`*** command, where ***`filename`*** is the name of the configuration file(s) to be backed up. This should be done either in the directory where the files are located or by using the full path name to the file. If the year is not explicitly shown, it is from the current year.
2. Run the **`rpm`** commands as described in the upgrade software you receive from Avaya technical support. This will be in the form of one or more RPM packages or may be a single executable to be upgraded.
3. Reapply your old configurations. This will depend on the extent of the upgrade. The details of the configuration(s) to be reapplied will be included with the patch/upgrade details.

Troubleshooting

Use the information in this section to help resolve problems with Network Routing. This section includes the following topics:

- Viewing log files on page 141
- Monitoring the Alarm Interface tab on page 141
- Problem scenarios on page 142

Viewing log files

When troubleshooting problems, look for errors in log files at the following locations:

- For Informix, see **/opt/informix/online.log**
- For AT&T, see **/export/dm** and **/export/att/run/mpac**
- For MCI, see **/export/dm**
- For Sprint, see **/export/sprint**

The following log files are provided:

- **psaDebug.log** - Logs Distribution Manager errors, both debug and information errors. The log level can be changed in **SysLogs.lcf** as well as the number of files and the size of files. The log files are automatically deleted, and the level may be changed without restarting the Distribution Manager application.
- **h225Stack0.log** -Logs information from the H.323 stack. The level is set by using the "-d" option of the appropriate "go-psa" start-up script, or by using **telnet 127.0.0.1 7799** and the **debug** command. New log files are created by using the **newlog** command.
- **xmlsrv.log** - Logs XML server information. The level is set by using the "-d" option of the appropriate "go-psa" start-up script.

Monitoring the Alarm Interface tab

Monitor the Alarm Interface tab as described in Interface alarms on page 111. Follow any suggested solutions to the alarms. If the alarms persist, escalate to Avaya technical support.

Problem scenarios

This section describes problems you may see on the NRS and procedures you can use to correct the problem.

This section includes the following topics:

- Application out of service on page 142
- Timeouts on page 142

Application out of service

If you see the alarm message:

```
Application Out of Service
```

The Distribution Manager is not running. Stop and restart the application and Informix as described in Stopping and restarting the Distribution Manager application on an NRS on page 136.

Timeouts

If, when monitoring the **CC Performance** status tab, you are consistently seeing timeouts, increase the Polling Timeout as needed. See Configuring a CC link on the NRS on page 64 for more information.

Glossary

AIS	Alarm Indicator Signal
ANI	Automatic Number Identifier
API	Application Programming Interface
Asynchronous polling	Polls continually, based on an administered polling interval.
BSR	Best Service Routing
CC	Contact Center. This is an overarching term that represents the communication server equipment used in a customer's Network Routing configuration. The communication servers in a Network Routing configuration report polling status back to the NRS.
CED	Caller-entered digits
COR	Class of Restriction
communication server	A communication server is an Avaya switch in the Network Routing configuration that is polled by other switches in the configuration, but does not report status back to the NRS directly.
DAC	Dial Access Code
Distribution Manager	The Distribution Manager is a Web-based application that stores configuration and performance data to determine the best site available to route a call. It responds to call routing requests from the carrier network through the Network Gateway.
DPC	Destination Point Code
failsafe response	The default response number if a specific number cannot be determined for the route request.
GUI	Graphical User Interface

ICP	Intelligent Call Processing A service of the AT&T network that provides the capability to temporarily suspend a toll-free call being processed in the AT&T NCP database and query a customer database (for the Avaya implementation, the Distribution Manager database) to get routing information before resuming call processing.
ISO	Implementation Services Organization. The ISO is the provisioning group of Avaya.
IXC	Inter eXchange Carrier
Local NRS	The NRS to which the administrator is currently logged in and making changes. The roles of local and remote servers can be exchanged as required.
MPAC	Multiple Protocol Access Card
MTP	Message Transfer Part
NCP	Network Control Point
Network Gateway	The Network Gateway interfaces between the IXC with SS7 protocol and the Distribution Manager with an XML API to help determine the best available destination to route a call.
Network application	Network applications are used for two reasons: • To determine which set of CCs/skills or failsafe routes should be used to process incoming route requests • To group the resources necessary to process the route requests
Network routing server	The server where coresident Network Gateway and Distribution Manager applications reside. For some service providers, there will be a dedicated Network Gateway server.
NRS	Network routing server
OCP	Origination Point Code

RAID-1	A method of disk backup management. RAID-1 is also known as disk mirroring and consists of at least two drives that duplicate the storage of data. There is no striping. Read performance is improved since either disk can be read at the same time. Write performance is the same as for single disk storage. RAID-1 provides the best performance and the best fault-tolerance in a multi-user system.
Rate based polling	Polls DPNs based on how often route requests are received from the network. As more calls are received from the network, polling occurs more often. As fewer calls are received from the network, polling occurs less often. This method can help balance the polling load on the DPNs.
Remote NRS	For duplicated NRSs, the NRS where changes are not being made, but is receiving automatic updates over the network. The roles of local and remote servers can be exchanged as required.
Request number	The toll-free telephone numbers used for incoming calls.
SS7	Signaling System Seven A common channel signaling system whereby signaling links, separate from the voice path, are used to transfer messages between switches or other nodes to set up trunks or access databases (such as the NRS database).
STP	Signal Transfer Point
Synchronous polling	Does not poll until a route request is received. The poll starts immediately, unless there is a Poll Suppression Interval administered.
T1 drops	Fractional connections to a T1 line.
TFN	Toll-free number
VDN	Vector Directory Number
XML	Extensible Markup Language

Index

A

accessing the user interface 28
adding
  DPN link 65, 81, 90, 93
  e-mail alerts 126
  network applications 86
  Network Gateway link 57
  user 49
alarms 103, 108
application out of service 142
audience 7

B

backup 135

C

cabling diagram
  NRS 17
call log 106
changing
  configuration 130
  date format 117
  DPN link 66, 82, 90, 93
  e-mail alerts 126
  network applications 87
  Network Gateway link 58
  password 52
  user access permissions 50
changing the root password 21
communication server 143
configuration
  ongoing changes 130
configuring
  e-mail alerts 125
  httpd parameters 25
  link to a DPN 64
  links to the Network Gateway 53
  network applications 83
  T1 connections 38
connecting
  T1 cables 35
  to the network
    NRS 17
customer options 63
customer support 10

D

database synchronization 46
deleting
  e-mail alerts 127
  scheduled event 134
  user 51
destination label reports 120
DPN
  link options 64, 80, 89, 92
  performance 104, 111
  reports 121
  status 102

E

e-mail alerts 125

G

general status 101
generating reports 118

H

hardware diagram 115
httpd parameters 25

I

installing
  NRS 11
IP addresses 67
IP trunks to the NRS 69

L

Linux desktop 21
logging in 21, 46
logging out 52

M

monitoring
  Network Gateway server 141

N

network connections

NRS . . . 17
Network Gateway
link options . . . 54, 55, 56
status . . . 102
network setup . . . 22, 24
node names . . . 67

O

options
DPN link . . . 64, 80, 89, 92
e-mail alerts . . . 125
Network Gateway link . . . 54, 55, 56
organization . . . 8

P

password aging . . . 51
passwords . . . 45, 50
permissions . . . 50
preface . . . 7
prerequisite administration . . . 62
prerequisites . . . 45
printing reports . . . 124

R

reasons for reissue . . . 7
rebooting the server
NRS . . . 27, 138
recent system alarms . . . 103
refresh . . . 117
related documents . . . 9
removing
DPN link . . . 66, 82, 91, 94
network applications . . . 88
Network Gateway link . . . 59
report graph characteristics . . . 118
reports
destination label . . . 120
generating . . . 118
printing . . . 124
request number . . . 119
request number reports . . . 119
resetting a user password . . . 50, 51
restore . . . 135

S

scheduling configuration updates . . . 132
security . . . 45
access controls . . . 49, 50
equipment installation . . . 13
firewalls . . . 22, 24
logging off . . . 52
passwords . . . 21, 22, 28, 47, 48, 49, 50, 52
server characteristics . . . 12
setting
frequent update . . . 132
monthly update . . . 133
one-time update . . . 132
refresh rate . . . 117
weekly update . . . 133
setting up
Linux desktop . . . 21
NRS . . . 19
site requirements . . . 13
software load . . . 62
status LEDs . . . 37
status polling VDNs . . . 76
status polling vectors . . . 76
status tab pages . . . 99
synchronizing the database . . . 46
system status . . . 100

T

T1 cables . . . 35
T1 connections . . . 38
T1 MPAC card status LEDs . . . 37
technician support . . . 10
timeouts . . . 142
troubleshooting
application out of service . . . 142
timeouts . . . 142

U

user administration . . . 49
user interface access . . . 28
user permissions . . . 50