RNCS Installation and Upgrade Instructions

For SR 2.8/3.8/4.3

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgements

- Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.
- CableCARD is a trademark of Cable Television Laboratories, Inc.
- Other third party trademarks mentioned are the property of their respective owners.
- The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

Cisco® Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

About This Guide

Introduction

This guide provides step-by-step instructions for installing and configuring the Remote Network Control Server (RNCS) component of a Digital Broadband Delivery System (DBDS). The RNCS is a needed component in a Regional Control System (RCS) that uses the Digital Network Control System (DNCS) to manage several remote headends.

The RNCS software is contained on a DVD. A technician is needed to insert the RNCS DVD into the RNCS. Installation engineers then complete the software installation from the DNCS that has a remote connection to the RNCS.

Appendix A of this guide, **The siteCmd Program**, contains instructions and examples for running various commands that are useful in managing a remote headend.

Audience

These instructions are written for headend technicians using the DNCS.

These instructions are also written for Cisco® Services engineers and other qualified service provider personnel with the following skills required to complete the installation or upgrade process successfully:

- Advanced knowledge of UNIX
  - Experience with a UNIX text editor. The instructions provided in this guide are no substitute for an advanced working knowledge of a UNIX text editor
  - The ability to review and edit cron files
  - Backing up file systems and databases
  - Working knowledge of Sun hardware
  - Working knowledge of Solaris
  - Working knowledge of script languages
- Extensive DBDS system expertise
  - The ability to identify keyfiles that are unique to the site being upgraded
  - The ability to add and remove user accounts
  - Troubleshooting for basic system errors
  - Stopping and starting system components

Read Me

Please read this entire guide before beginning the upgrade. If you are uncomfortable with any of the procedures, contact Cisco Services for assistance.

Important: Perform all of the procedures in this guide in the order in which they are presented. Failure to follow all of the instructions may lead to undesirable results.

Two Installation Procedures

Choose one of the following options when installing RNCS software:

- If you are installing the RNCS software for the first time, follow the instructions in ***Initial Installation of RNCS Software*** (on page 1).
- If you are upgrading existing RNCS software, follow the instructions in ***Upgrade of RNCS Software*** (on page 59).

Document Version

This is the second formal release of this document.

1

Initial Installation of RNCS Software

Introduction

This chapter describes the Sun Fire V240 and V245 servers, on which you will install the RNCS software. In addition, this chapter contains procedures for installing RNCS software for the first time on a system.

Note: If you are upgrading RNCS software at a site that already supports the RCS feature, go to ***Upgrade of RNCS Software*** (on page 59).

In This Chapter

Before You Begin

There are several things to consider before you install remote sites:

- The Distributed DNCS feature on the DNCS must be licensed before you can set up an RCS. Contact Cisco Services for licensing information.
- Default BFS sources (those having source IDs of 200 or less) are automatically re-created by the RNCS installation; however, you must manually start these sources after starting the newly installed RNCS. See ***Starting the RNCS*** (on page 56) for more information.
- Non-default BFS sources (such as multiple bootloaders or VCS sources) that existed on the DNCS before licensing the Distributed DNCS feature must be manually re-created in the All Sites window for them to be available to the DNCS and the RNCS BFS. You should record the parameters of these sources before starting the installation. See ***Re-Creating the All Sites Sources*** (on page 57) for more information.

Installation Overview

The following table lists the steps required for the RNCS software initial installation, where the section for each step begins in this document, and the information required for each procedure.

Step	Procedure	Reference	Parameters Required
1	Record all the information required for non-default BFS sources (such as multiple bootloader or VCS sources) You will re-create these sources on the RNCS later	***Before You Begin*** (on page 2)	■ Source Name ■ Source ID ■ Source Type ■ Transport Type ■ Data Rate ■ Block Size ■ Indication Interval ■ Data Pump ■ Available Hosts
2	Log onto the RNCS servers	***Logging on to the RNCS Servers*** (on page 11)	N/A
3	Configure the ALOM port	***Configure the ALOM Port*** (on page 13)	■ Password for admin ■ Unique IP address for network management port ■ Netmask of the network management port ■ IP address for gateway or router of the network management port
4	Connect to the Console of the RNCS server	***Connecting to the Console of the RNCS Server*** (on page 16)	■ IP address of the ALOM port ■ Admin user ID ■ Admin user password
5	Install the RNCS software	***Install the RNCS Software*** (on page 17)	■ Host name of the new RNCS ■ IP address of the new RNCS ■ Netmask of the new RNCS ■ Router IP address for bge0 interface ■ Your current time zone and region ■ Root password for the new RNCS
	■ Run the create_sysidcfg Script	***Running the create_sysidcfg Script*** (on page 30)	■ IP address of the dncsatm

Step	Procedure	Reference	Parameters Required
6	Attach mirrors	***Attach Mirrors*** (on page 31)	N/A
7	Configure the network		*See below*
	■ Edit the RNCS hosts file	***Editing the RNCS /etc/hosts File*** (on page 32)	■ RNCS IP address ■ RNCS hostname ■ DNCS IP address
	■ Edit the DNCS hosts file	***Editing the DNCS /etc/hosts File*** (on page 32)	■ RNCS IP address ■ RNCS ALOM interface IP address
	■ Edit the nodename file	***Editing the /etc/nodename File*** (on page 33)	■ RNCS hostname
	■ Edit the hostname.bg0 file	***Editing the /etc/hostname.bge0 File*** (on page 33)	■ RNCS hostname
	■ Edit the defaultrouter file	***Editing the /etc/defaultrouter File*** (on page 34)	■ RNCS hostname
	■ Edit the sqlhosts file	***Editing the /export/home/informix/etc/sqlhosts File*** (on page 34)	■ RNCS hostname
	■ Enable FTP service	***Enabling the FTP Service on the RNCS*** (on page 35)	■ EAS interface IP address
	■ Reboot the RNCS	***Reboot the RNCS*** (on page 35)	N/A
	■ Check NTP activation	***Checking NTP Activation*** (on page 36)	N/A
8	Add and configure the RNCS	***Add and Configure the RNCS*** (on page 37)	*See below*
	■ License the distributed DNCS	***License the Distributed DNCS*** (on page 37)	■ Root password

Step	Procedure	Reference	Parameters Required
	■ Add the RNCS site	***Adding the RNCS Site*** (on page 37)	■ Site name ■ Site ID ■ RNCS IP address ■ RNCS MAC address ■ RNCS BFS MAC address (this is also the Session ID MAC address) ■ Online
	■ Create the RNCS BFS host	***Creating the RNCS BFS Host*** (on page 38)	■ BFS in-band mode ■ Inband device name ■ RNCS host name ■ RNCS BFS QAM Input port TSID ■ PSI interval (80) ■ Port (0) ■ Bandwidth (38.80)
	■ Set up the remote site	***Setting Up the Remote Site*** (on page 39)	■ RNCS host name ■ RNCS IP address
	■ Create RNCS headend components	***Create RNCS Headend Components*** (on page 40)	*See below*
	– Add headend	***Adding the Headend*** (on page 40)	■ Headend name ■ Headend ID ■ RNCS site name associated with this headend
	– Add hub	***Adding a New Hub Entry*** (on page 41)	■ Hub name ■ Hub ID ■ Headend associated with this hub ■ Time zone associated with this hub ■ DST zone ID associated with this hub
	– Add node set	***Adding a Node Set*** (on page 42)	■ Node set name ■ Hub associated with this node set
	– Add billing reference	***Adding a Billing Reference to an RCS Site*** (on page 43)	■ Billing ID ■ RNCS site associated with this billing reference

Step	Procedure	Reference	Parameters Required
	– Create BFS MPEG sources	***Creating BFS MPEG Sources*** (on page 44)	■ Headend associated with the ASI card ■ MPEG source name ■ Device name (ASI) ■ ASI card IP address ■ ASI card MAC address
	– Create video MPEG sources	***Creating Video MPEG Sources*** (on page 44)	■ Headend associated with the source ■ MPEG source name ■ Device type ■ MPEG source IP address ■ MPEG source MAC address
	– Add a BFS QAM	***Adding a BFS QAM*** (on page 45)	■ Headend name where this BFS QAM resides ■ QAM name ■ QAM IP address ■ Modulation type this QAM uses ■ QAM MAC address ■ QAM subnet mask ■ Default gateway IP address (if used) ■ Allow SI ■ Input port ■ Input transport stream ■ QAM modulation type ■ QAM output transport stream ID ■ Channel center frequency (in MHz) ■ Hubs associated with this BFS QAM

Step	Procedure	Reference	Parameters Required
	– Connect BFS MPEG source to RNCS BFS QAM	***Connecting the BFS MPEG Source to the RNCS BFS QAM*** (on page 47)	■ MPEG source output port number ■ MPEG source transport stream ID ■ MPEG source transport protocol ■ MPEG source output card MAC address ■ MPEG source output card IP address ■ MPEG source output card subnet mask ■ Headend name where this BFS QAM resides ■ Device type (QAM) ■ Port number on BFS QAM that connects to MPEG source
	– Add a QPSK	***Adding a QPSK*** (on page 48)	*See below*
	▪ Add a QPSK modulator	***Add a QPSK Modulator*** (on page 48)	■ Hub name associated with this QPSK ■ QPSK name ■ QPSK IP address ■ QPSK MAC address ■ QPSK subnet mask ■ Default router ■ DHCT base IP address in the domain of this QPSK ■ DHCT subnet mask ■ QPSK frequency ■ DCM ■ ADSG options
	▪ Add a QPSK demodulator	***Add a QPSK Demodulator*** (on page 50)	■ Port number that receives data on the demodulator ■ Node set name associated with the demodulator ■ Frequency of the demodulator

Step	Procedure	Reference	Parameters Required
	– Add video QAMs	***Adding Video QAMs*** (on page 52)	■ Headend name associated with the QAM ■ QAM name ■ QAM MAC address ■ QAM IP address ■ QAM subnet mask ■ QAM modulation type ■ Default gateway (if used) ■ QAM administrative state (online or offline) ■ Allow SI ■ QAM input port (type) ■ Modulation type ■ Output TSID ■ QAM center channel frequency (in MHz) ■ Hubs associated with this QAM
	– Connect RNCS video sources to RNCS video QAMs	***Connecting RNCS Video MPEG Sources to the RNCS Video QAMs*** (on page 53)	■ MPEG source output port number ■ MPEG source transport stream ID ■ MPEG source transport protocol ■ MPEG source output card MAC address ■ MPEG source output card IP address ■ MPEG source output card subnet mask ■ Headend name where this QAM resides ■ Device type (QAM) ■ Port number on QAM that connects to MPEG source
	– Create BFS source definitions	***Creating BFS Source Definitions*** (on page 55)	■ First part of the session ID: Use the RNCS MAC address ■ Second part of the session ID: Use the original source ID
	– Start RNCS sources	***Starting the RNCS Sources*** (on page 55)	N/A
9	Start the RNCS	***Starting the RNCS*** (on page 56)	N/A

Step	Procedure	Reference	Parameters Required
10	Re-create the all sites sources	***Re-Creating the All Sites Sources*** (on page 57)	■ Source Name ■ Source ID ■ Source Type ■ Transport Type ■ Data Rate ■ Block Size ■ Indication Interval ■ Data Pump ■ Available Hosts

Introducing the RNCS Servers and the ALOM Port

The RNCS Servers

We have chosen the Sun Fire V240 and V245 servers for the platform of the RNCS. These servers use Sun's existing SPARC and Solaris architecture, and are designed to easily mount within a standard computer rack. These servers are configured with the following components:

Sun Fire V240	Sun Fire V245
Two UltraSPARC III processors	Two UltraSPARC III processors
Four GB of memory	One GB of memory
■ 2 x 36 GB hard drives ■ 2 x 73 GB hard drives	■ 2 x 73 GB hard drives ■ 4 x 74 GB hard drives
Four Gigabit Ethernet ports	Four Gigabit Ethernet ports
Serial management port	Serial management port
Network management port	Network management port
Three PCI slots	■ Two PCI slots ■ Two PCI-x slots
Two redundant power supplies	Two redundant power supplies
A system configuration card	A system configuration card

Taken as a whole, the serial management port and the network management port of the RNCS server constitutes the Sun Advanced Lights Out Manager (ALOM) port. The ALOM port is a system controller that allows the servers to be managed and administered from a remote location. Through the ALOM port, you can monitor and control the servers through a serial connection (using the SERIAL MGT port) or an Ethernet connection (using the NET MGT port).

Logging on to the RNCS Servers

These instructions are to be completed at the remote location and assume that the Sun Fire V240 and V245 servers have not yet been configured to serve as a remote server in the RNCS design.

Complete the following steps to log on to an RNCS server.

1. Connect a laptop computer to the serial network management port of the RNCS server.
2. Start the HyperTerminal application on the laptop and configure the application with the following parameters:
   - Baud rate—9600
   - Data bits—8
   - Parity—none
   - Stop bit—1
   - Flow control—no

   Note: The HyperTerminal application allows one computer to communicate with another computer.
3. If necessary, power on the RNCS server.
4. Type **#.** and press **Enter**. One of the following results occurs:
   - The **Login** prompt appears.
   - The **sc>** prompt appears.
5. Did the **Login** prompt appear after you completed step 4?
   - If **yes**, go to step 6.
   - If **no** (the **sc>** prompt appeared), go to step 7.
6. If the **Login** prompt appeared after completing step 4, complete the following steps.
   a. Type **admin** and press **Enter**.
   b. Type the password (**changeme**) and press **Enter**. The **sc>** prompt appears.
7. Type **break** and press **Enter**. The system interrupts the boot process of the RNCS server.
8. Type **console -f** and press **Enter**. A message appears that instructs you to type **#.** to return to the ALOM port.
9. Press **Enter** again.

   Results:
   - Control transfers to the console of the RNCS server (rather than the ALOM port).
   - The **ok** prompt should appear.

10 After completing step 9, did the **ok** prompt appear, as described?

- If **yes**, go to step 11.
- If **no**, repeat steps 7 through 9.

11 Type **#.** (the **#** key followed by a period).

Results:

- Control returns to the ALOM port.
- The **sc>** prompt appears.

Configure the ALOM Port

Now that you have successfully connected the laptop computer to the server and logged on, complete the following steps to configure the ALOM port.

1 At the **sc>** prompt, type **setsc if_network true** and press **Enter**.

Result: One of the following results occurs:

- If you have never before set the admin password for this server, the system responds with a message similar to the following:
  Warning: the setsc command is being ignored because the password for admin has not been set.
  Setting password for admin.
  New password:
- If the system detects that the admin password for this server has previously been set, then the network management port of the server becomes functional.

2 Did the system display the "setting password" message described in the first bullet of step 1?

- If **yes**, go to step 3.
- If **no**, go to step 4.

3 Complete the following steps if the "setting password" message, described in the first bullet of step 1, appeared after completing step 1.

a Type the new admin password and press **Enter**. The **Re-enter new password** prompt appears.

b Retype the new admin password and press **Enter**.

c Type **setsc if_network true** and press **Enter**. The network management port of the server becomes functional.

4 Type **setsc netsc_dhcp false** and press **Enter**. This command prevents the Dynamic Host Configuration Protocol (DHCP) from obtaining the network configuration.

5 Type **setsc netsc_ipaddr [IP address]** and press **Enter**. This command establishes the unique IP address of the network management port.

Notes:

- Substitute the IP address of the network management port of the RNCS server for [IP address].
- The network administrator can help you determine the IP address.

6 Type **setsc netsc_ipnetmask [netmask]** and press **Enter**. This command establishes the netmask of the network management port.

Notes:

- Substitute the netmask of the network management port of the RNCS server for [netmask].
- The network administrator can help you determine the netmask.

7 Type **setsc netsc_ipgateway [IP address of gateway or router]** and press **Enter**. This command establishes the IP address of the gateway or router of the network management port.

Notes:

- Substitute the IP address of the gateway or router of the network management port of the RNCS server for [IP address of gateway or router].
- The network administrator can help you determine the IP address.

8 Type **setsc sc_powerstatememory true** and press **Enter**. This command sets the sc_powerstatememory variable to true.

9 Type **showsc** and press **Enter**. The system displays the value of variables associated with the ALOM port.

10 Is the **sc_powerstatememory** variable set to *true*?

- If **yes**, type **q** to exit from the showsc display.
- If **no**, type **q** to exit from the showsc display. Repeat this procedure from step 8.

11 Type **resetsc** and press **Enter**. A confirmation message appears.

12 Type **y** and press **Enter**. After a few messages, the system prompts you to type **#.** to return to the ALOM port.

13 Type **#.** (Do *not* press Enter.). The Login prompt appears.

14 Did the **Login** prompt appear after you completed step 13?

- If **yes**, go to step 15.
- If **no** (the **sc>** prompt appeared), go to step 16.

15 If the **Login** prompt appeared after you completed step 13, follow these instructions.

a Type **admin** and press **Enter**.

b Type the admin password and press **Enter**. The **sc>** prompt appears.

16 Type **shownetwork** and press **Enter**. The system displays the configuration settings you just established.

17 Review the settings you established in steps 1 through 16 and choose one of the following options:

- If the settings are correct, go to step 18.
- If a setting is incorrect, re-run the appropriate command and then go to step 18.

18 Type **console -f** and press **Enter**. A message appears that instructs you how to return to the ALOM port, if needed.

19 Press **Enter** again.

Results:

- Control transfers to the console of the RNCS server (rather than the ALOM port).
- The **ok** prompt appears.

Choices Regarding Installation

The server is now ready for the installation of RNCS software. You have the following two options:

- Telnet from the DNCS to the just-configured ALOM port by following the instructions in ***Connecting to the Console of the RNCS Server*** (on page 16).

  Note: We recommend that you select this option to test the just-configured ALOM port.

- Use the laptop to install the RNCS software by following the instructions in ***Install the RNCS Software*** (on page 17).

Connecting to the Console of the RNCS Server

After configuring the ALOM port of the RNCS server, you are ready to complete the following steps to connect to the console of the server.

1 Complete the following steps to remotely log on to the ALOM port of the RNCS server.

   a Type **telnet [IP address of ALOM port]** and press **Enter**. A prompt for the user ID appears.

   Note: Substitute the IP address of the ALOM port for [IP address of ALOM port].

   Example: telnet 10.201.0.2

   b Type the admin user ID and press **Enter**. A prompt for the password appears.

   c Type the password for the admin user and press **Enter**. The **sc >** prompt appears as the system establishes a telnet session between the DNCS and the ALOM port.

2 Type **console -f** and press **Enter**.

Results:

- A message appears that instructs the user on how to return to the ALOM port.
- Control of the server is returned to the console, rather than the ALOM port.

3 Go to ***Install the RNCS Software*** (on page 17).

Install the RNCS Software

Notice to Installation Engineers

Be sure that you are using the procedures in this section to install the RNCS software for the first time. If you are upgrading RNCS software at a site that already supports the RCS feature, use the installation procedures in Chapter 2, instead.

Installing the RNCS Software for the First Time

Now that you have established the correct environment for the RNCS server, you can install the software. Complete the following steps to install the software.

Note: In the series of screens that follow, you will often have to select a configuration parameter from a list of parameters. Use the arrow keys to navigate through your choices, and make your selection by pressing the **spacebar**. The system usually places an **X** beside the selected parameter.

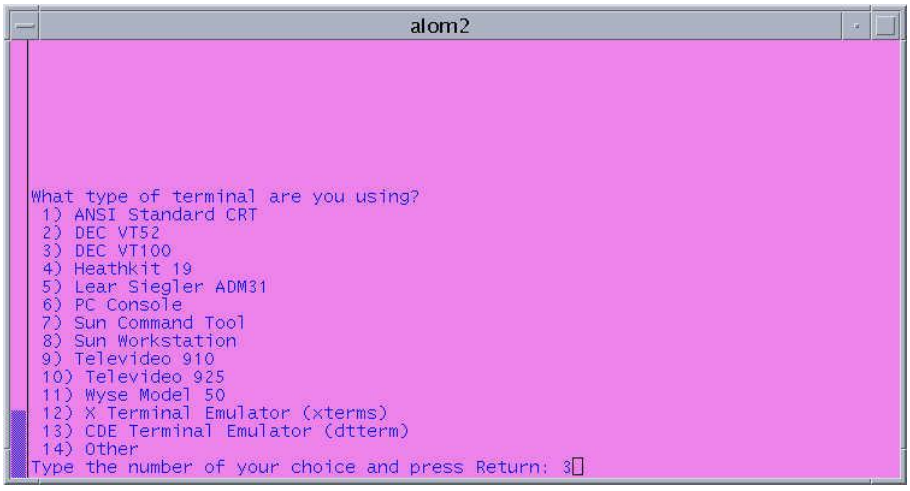
1 If necessary, ask the on-site technician at the RNCS server to insert the DVD, labeled similarly to **RNCS Install DVD,** into the DVD drive of the RNCS server.

2 Type **boot cdrom – install** and press **Enter**.

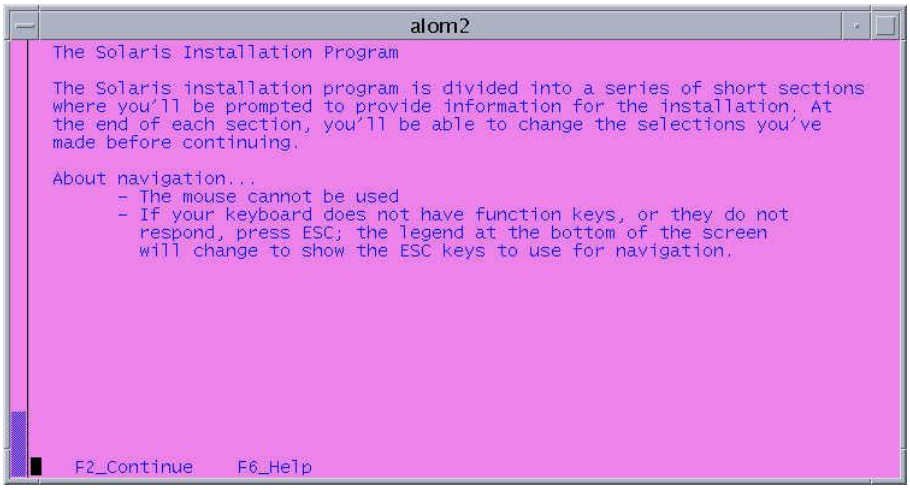
Results:

- The RNCS server reboots as the installation script begins.
- The Select a Language window appears.

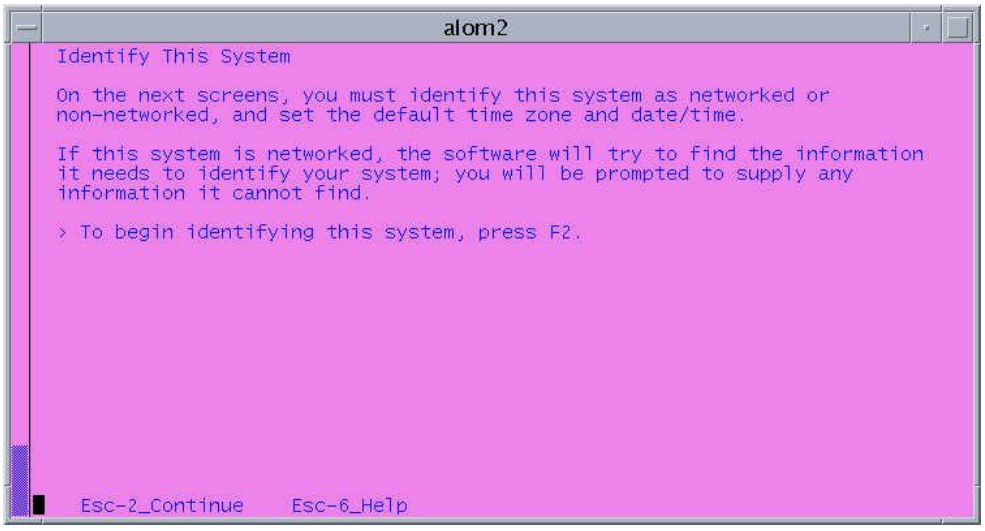
3 Type a number that corresponds to your desired language and press **Enter**. The window updates to prompt you to identify the type of terminal you are using.



4 Type the number that corresponds to **DEC VT100** and press **Enter**. The window updates to display a brief message about the installation process.

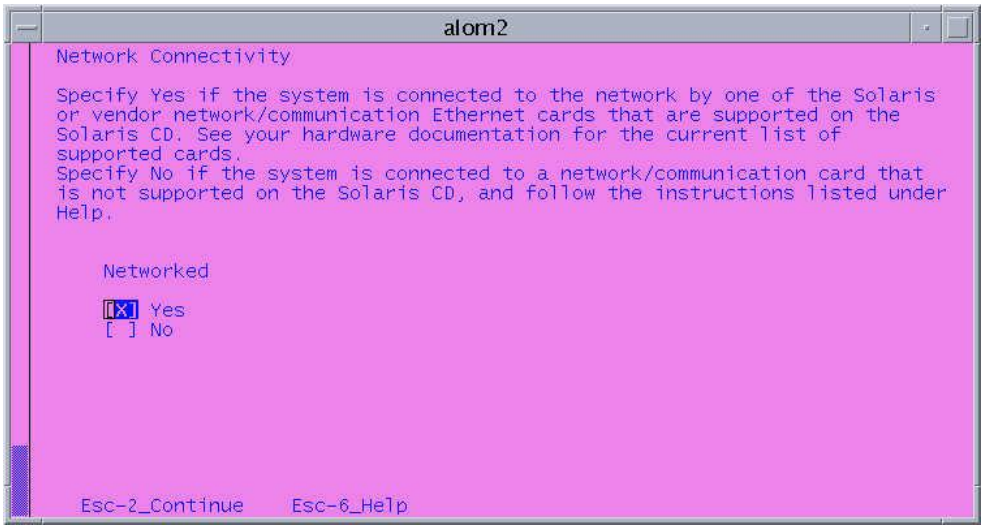


5 Read through the message displayed in step 4 and press the **F2** key. The window updates to display another brief informational message.



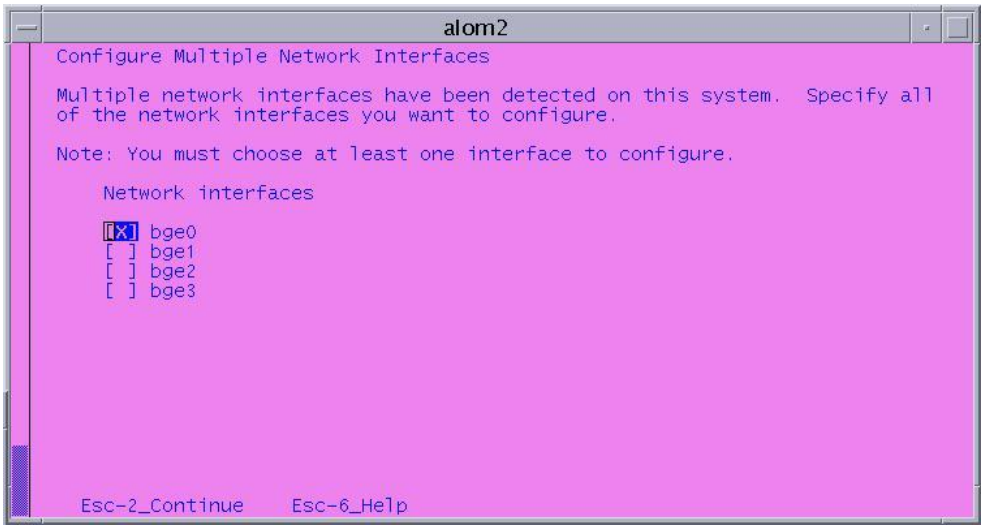
Note: On some systems, the window may also prompt you to press the **Esc** and **2** keys simultaneously to continue. Either method (**Esc** and **2** keys, or **F2** key) will work.

6 Press the **Esc** and **2** keys simultaneously. The window updates to ask whether the system is connected to the network through a Solaris-compatible Ethernet card.

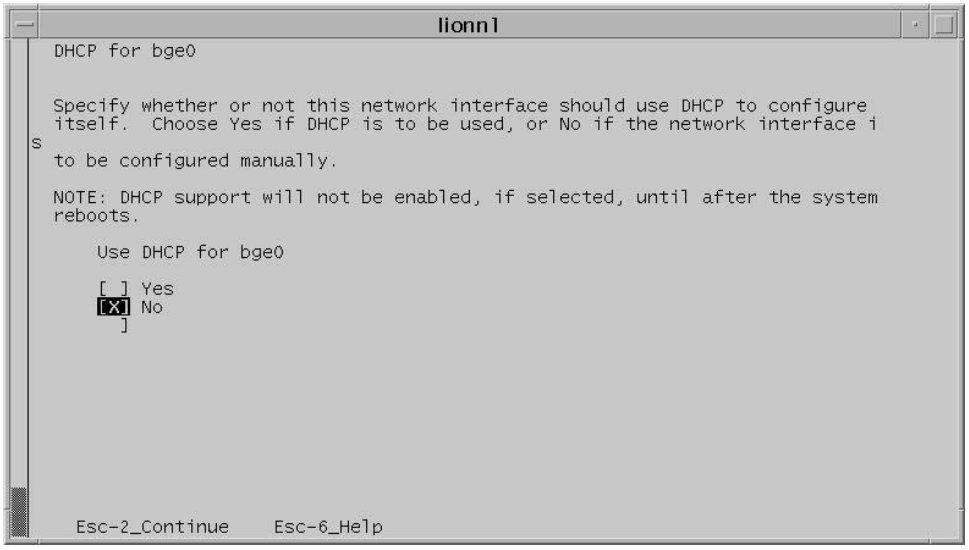


7 Select **Yes** and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to select the network interface that you want to configure.

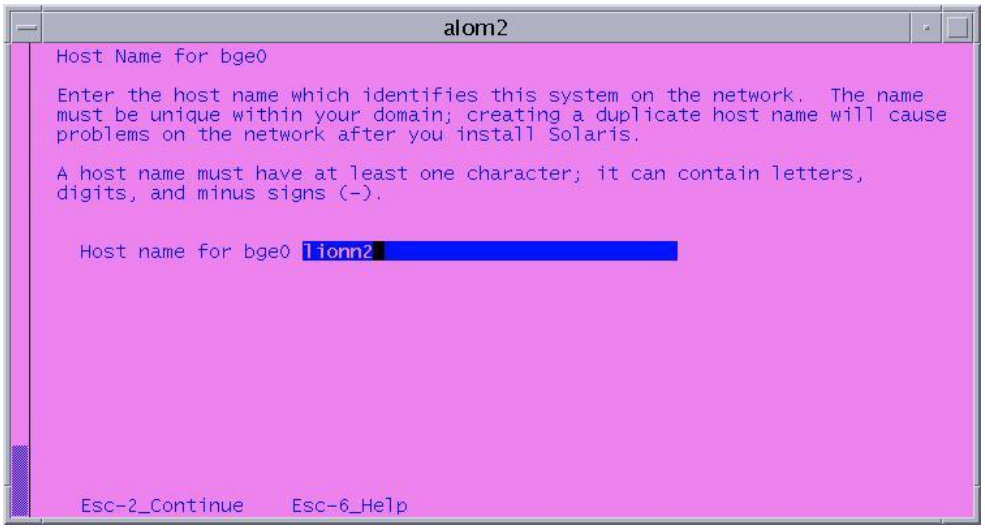
Note: Alternately, you can press the **F2** key.



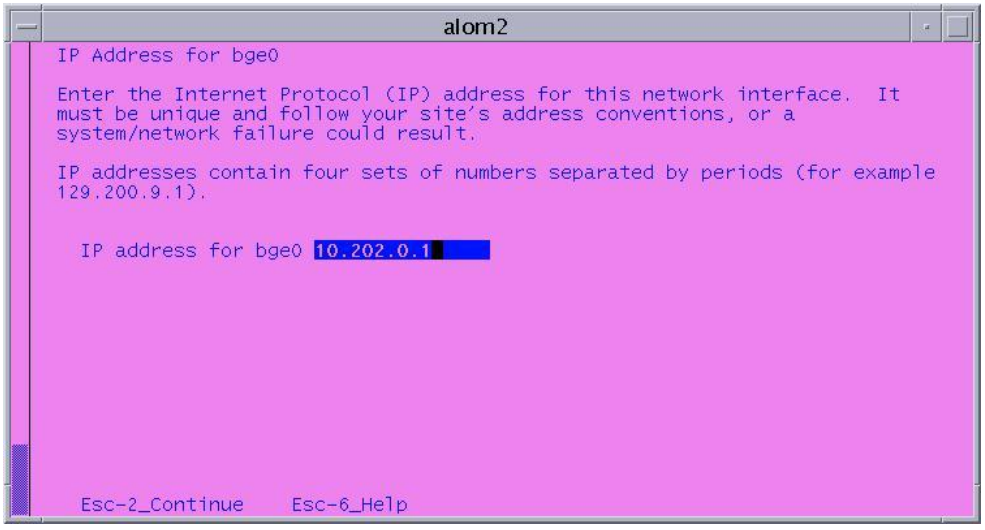
8 Select **bge0** and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify whether the Dynamic Host Configuration Protocol (DHCP) is to be used to configure the bge0 interface.



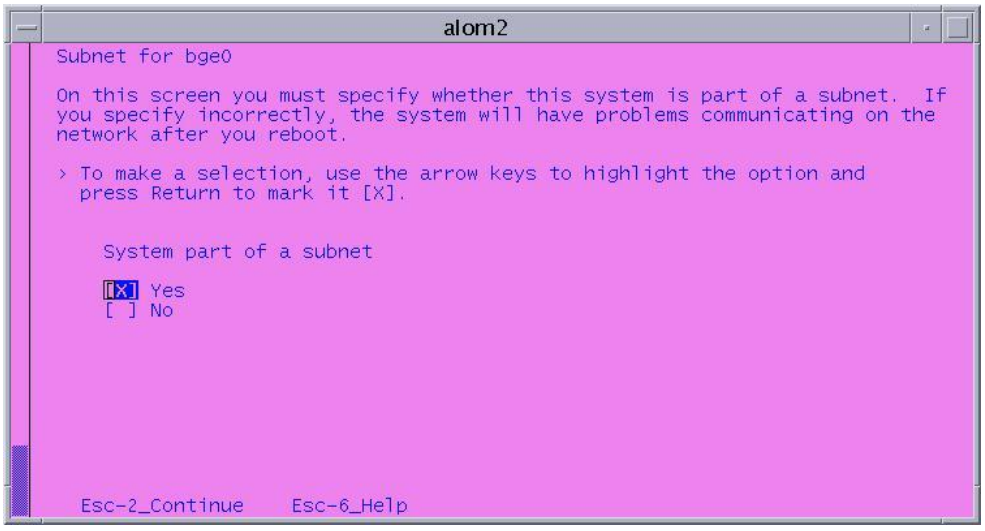
9 Select **No** and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to enter the host name that identifies this system on the network.



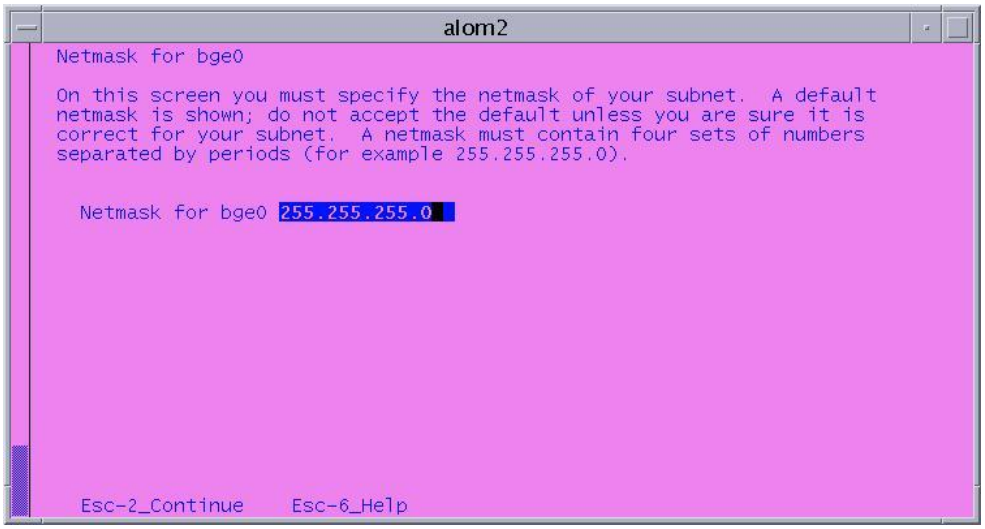
10 Type the host name (example, lionn2) and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to enter the IP address for the bge0 interface.



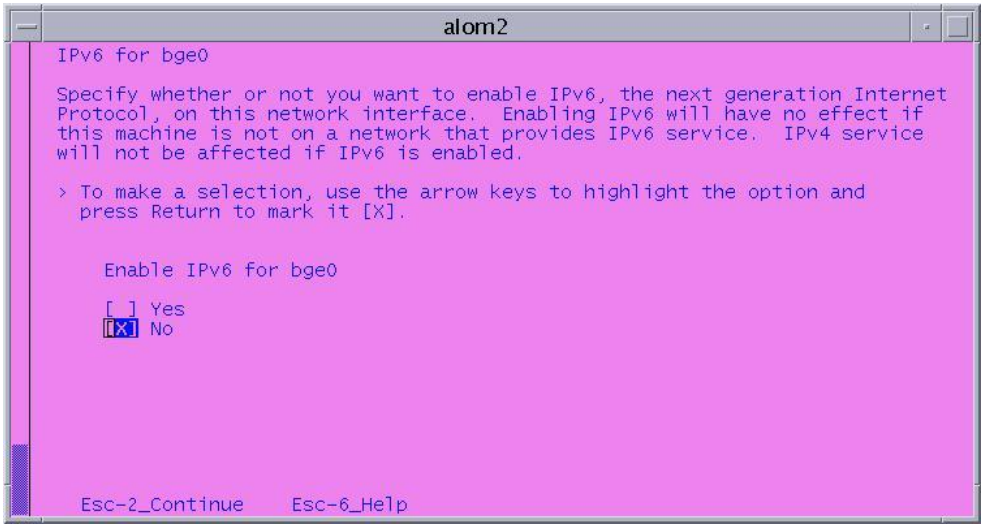
11 Type the IP address and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify whether your system is part of a subnet.



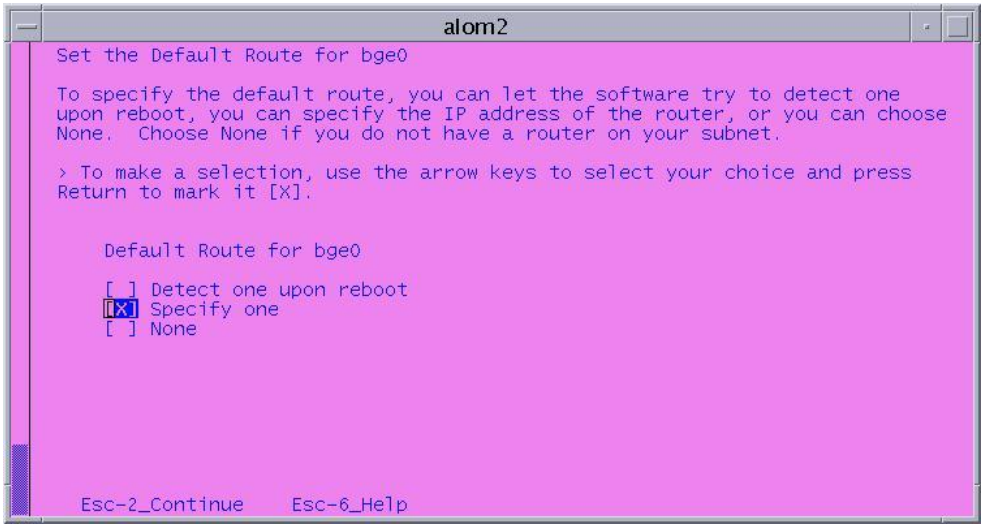
12 Select **Yes** and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify the netmask for the bge0 interface.



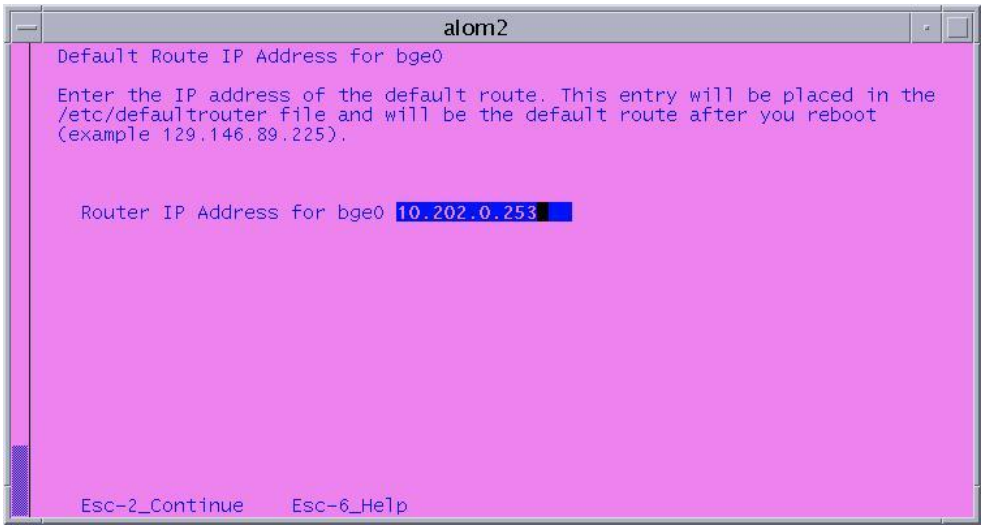
13 Type a netmask of **255.255.255.0** and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify whether you want to enable the IPv6 Internet protocol on the bge0 interface.



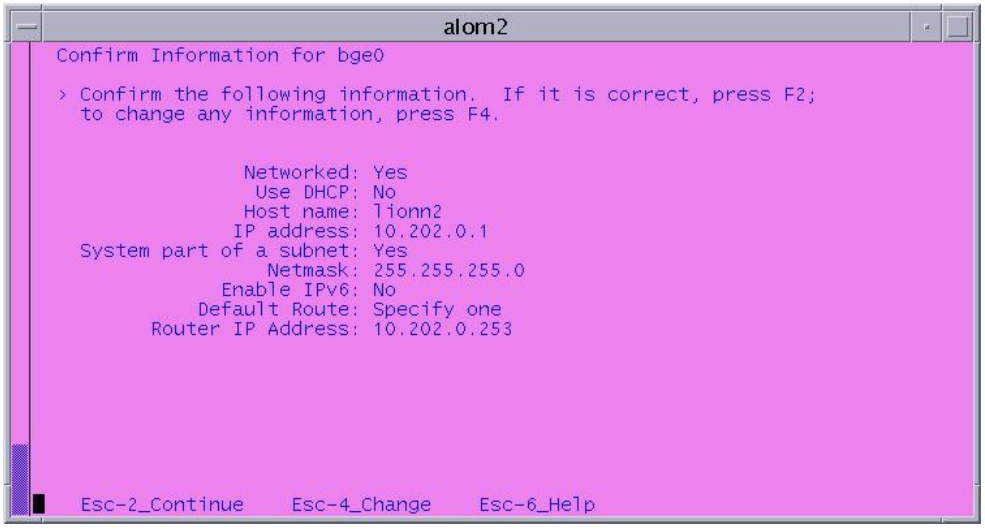
14 Select **No** and press the **Esc** and **2** keys simultaneously. The window updates and prompts you to set the default route for the interface.



15 Select **Specify one** and press the **Esc** and **2** keys simultaneously. The window updates and prompts you to enter the IP address of the default route.

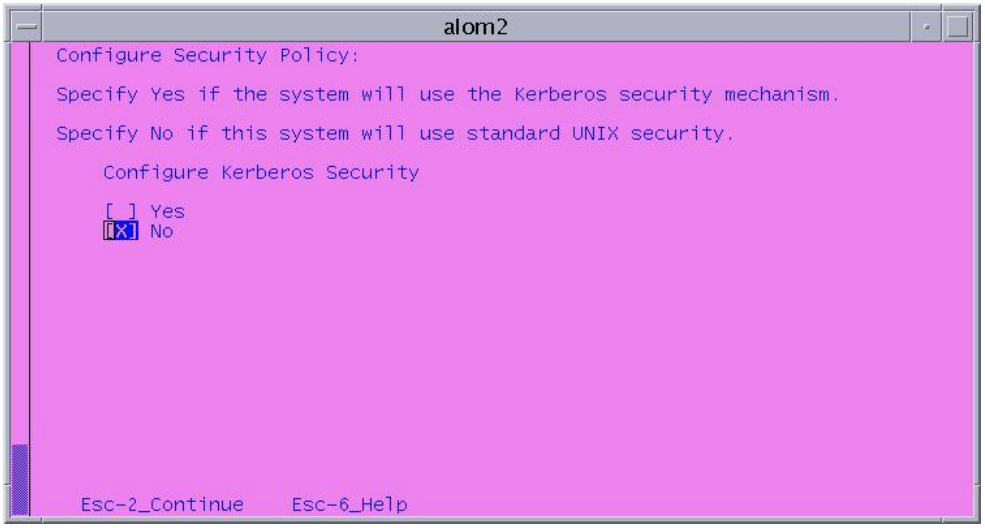


16 Type the Router IP Address for the interface and press the **Esc** and **2** keys simultaneously. The window updates and asks that you confirm the network configuration.

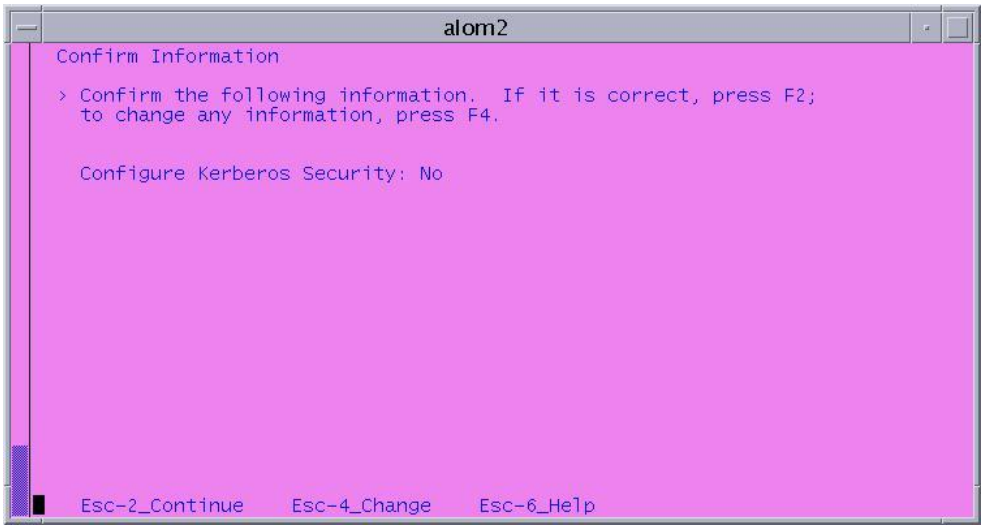


17 Review the configuration and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify whether your system will use the Kerberos security.

Note: If you need to change any configuration parameters, press the **Esc** and **4** keys simultaneously, and then follow on-screen instructions to make any changes.

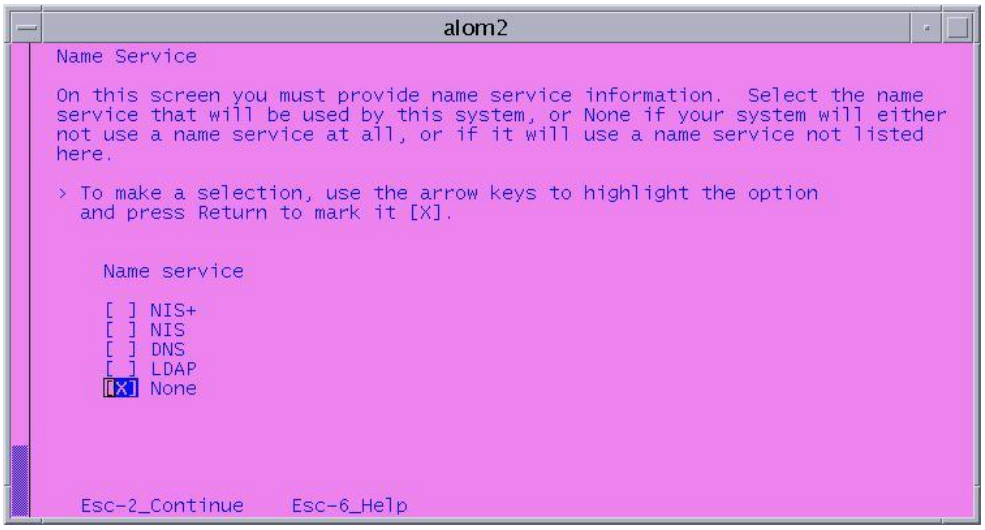


18 Select **No** and press the **Esc** and **2** keys simultaneously. The window updates to ask you to confirm that you made the correct selection regarding Kerberos network security.

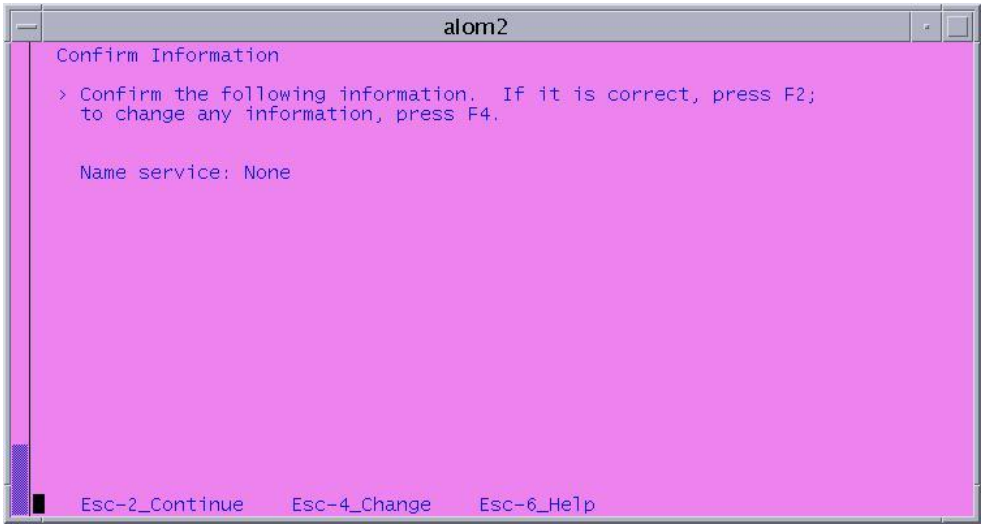


19 Review the Kerberos configuration and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to select the **Name service** for your system.

Note: If you need to change the Kerberos configuration, press the **Esc** and **4** keys simultaneously, and then follow on-screen instructions to make the change.

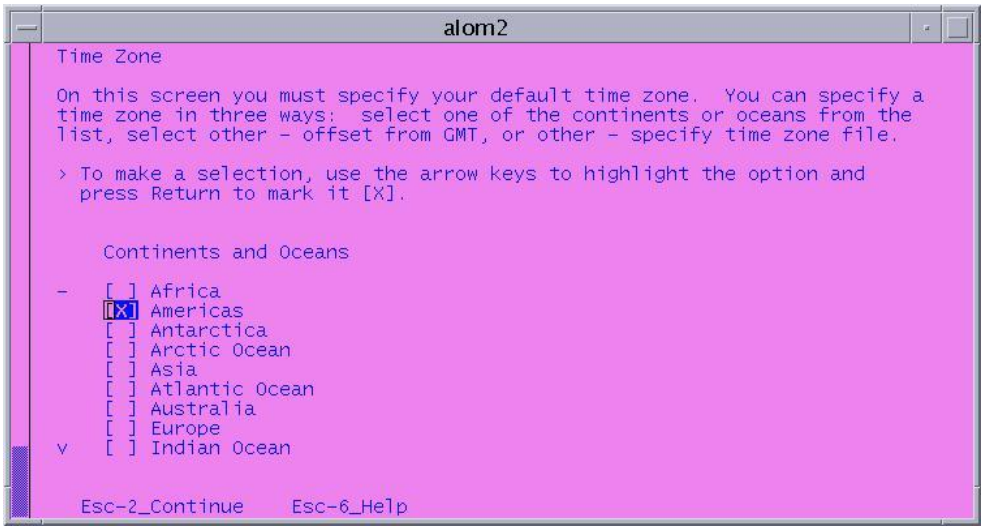


20 Select **None** and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to confirm that you made the correct decision regarding the Name service.

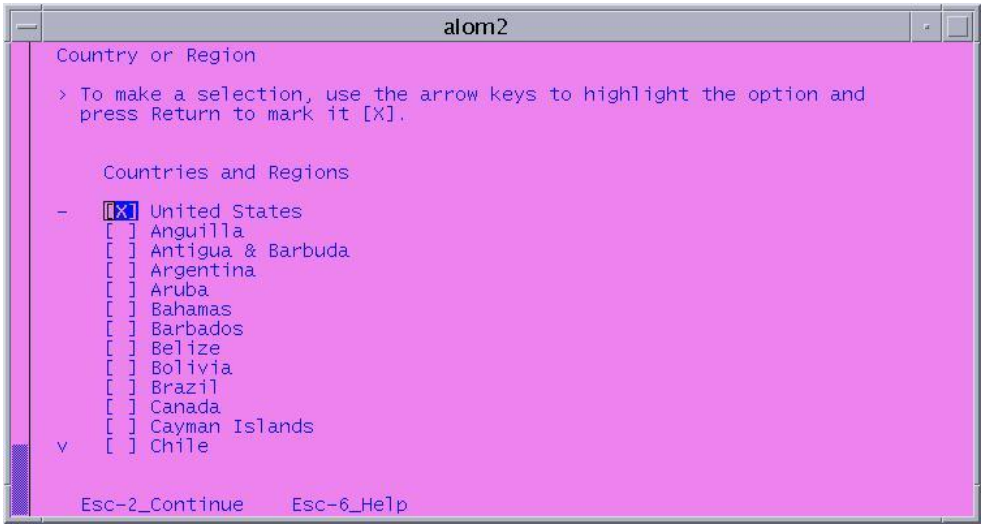


21 Review the Name service configuration and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to select your default time zone.

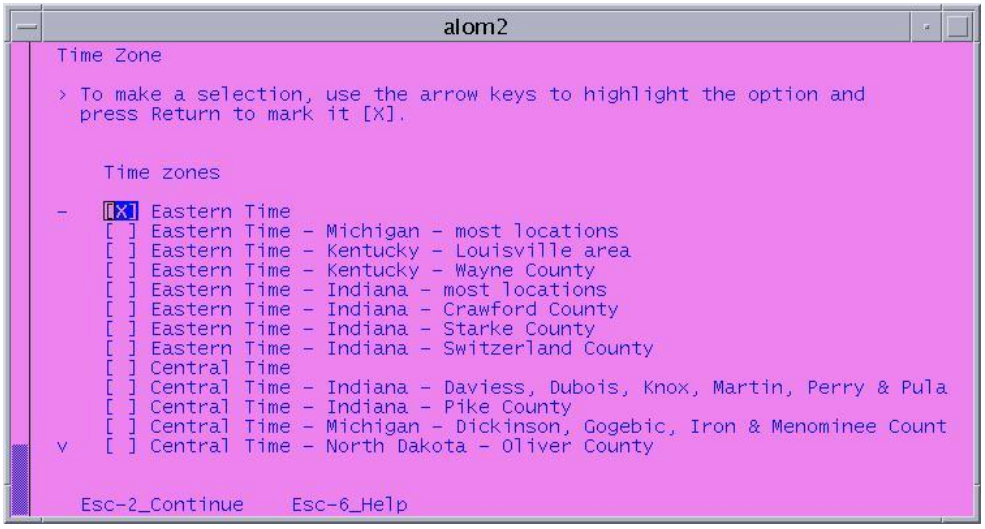
Note: If you need to change the Name service configuration, press the **Esc** and **4** keys simultaneously, and then follow on-screen instructions to make the change.



22 Select **Americas** and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify the appropriate country or region.

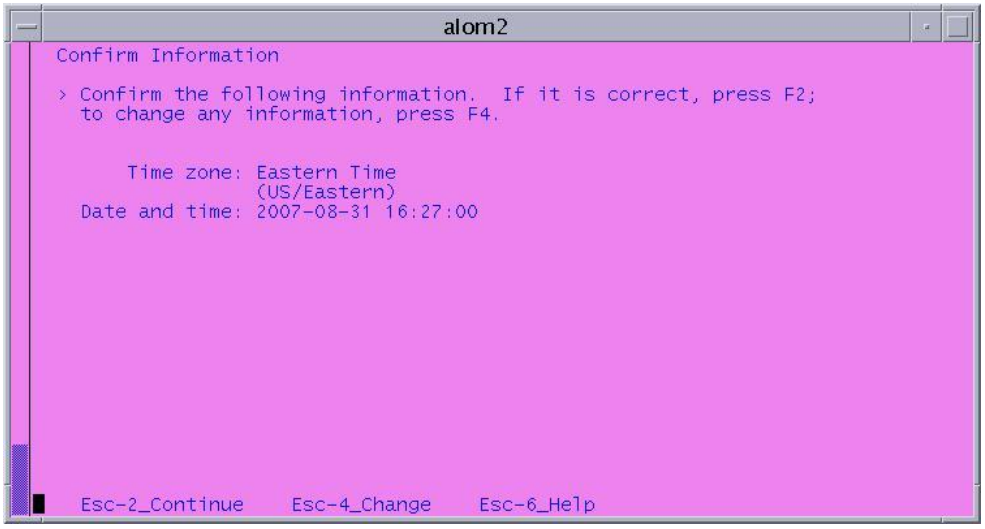


23 Select the appropriate country or region and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to select the appropriate time zone.



24 Select the appropriate time zone. and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to select the appropriate time and date.

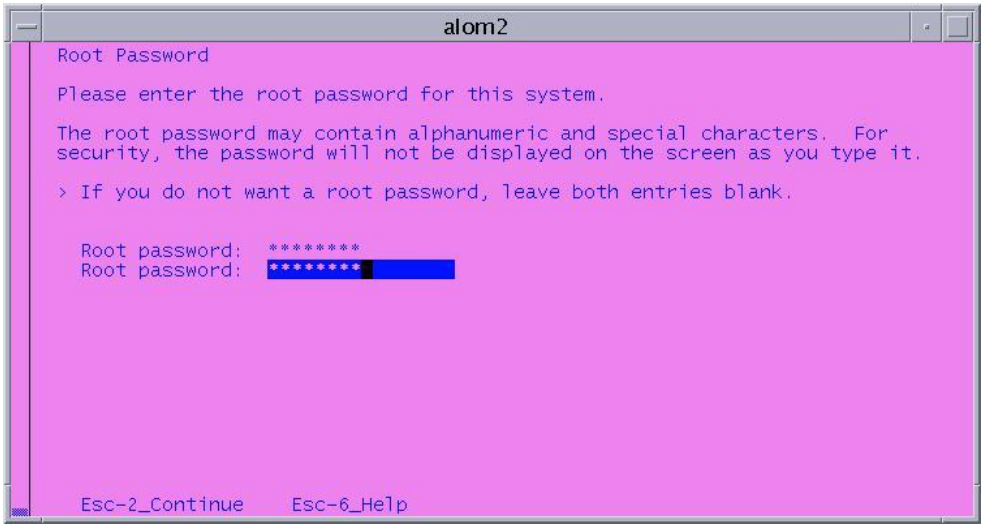
25 Select the default value, if it is correct, or type in the correct values and press the **Esc** and **2** keys simultaneously. The window updates to prompt you to confirm the date and time information.



26 Review the date and time information and press the **Esc** and **2** keys simultaneously. The window updates and asks you to provide the root password for the system.

Note: If you need to change the date and time information, press the **Esc** and **4** keys simultaneously, and then follow on-screen instructions to make the change.

27 Type the **root** password and press **Enter**. The system asks you to type the root password again.



28 Type the **root** password a second time and press the **Esc** and **2** keys simultaneously. The installation process continues and the console login prompt appears when the installation process has ended.

29 Go to ***Running the create_sysidcfg Script*** (on page 30).

Running the create_sysidcfg Script

The create_sysidcfg script creates a sysidcfg file in a specified directory and writes system identification configuration information to the nvramrc file. Complete the following steps to run the create_sysidcfg script.

1 Type **/cdrom/cdrom0/s0/sai/scripts/create_sysidcfg /var/tmp** and then press **Enter**. The system displays the **Enter IP Address of dncsatm [default: 10.253.0.1]** message.

2 Is the default IP address correct?

- If **yes**, press **Enter**.
- If **no**, type the correct IP address for dncsatm and then press **Enter**.

Result: The following message appears:

Restarting ntp
Sysidcfg information written successfully to nvramrc

Note: Disregard any **not found** message.

Attach Mirrors

In this procedure, you will enable the disk-mirroring function of the server. Complete the following steps to log on to the RNCS server and then to attach the server's mirrors.

Attaching Mirrors

Note: It may take up to 20 minutes to complete this process.

1. Log on to the RNCS server as **root** user, if necessary.
2. Type **cd /cdrom/cdrom0/s0/sai/scripts** and press **Enter**. The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.
3. Type **./LIONN_attach_mirrors** and press **Enter**. A confirmation message appears.
4. Type **y** (for yes) and press **Enter**. The system runs a script that enables the disk-mirroring function of the RNCS server.
5. When the mirrors have been enabled, type **exit** and press **Enter**. The root user logs out of the RNCS server.

Suggestion Regarding the RNCS Software DVD

Leave the RNCS software DVD in the DVD drive of the RNCS server. You need the DVD in place in case you ever have to re-install the software.

Network Configuration

Editing the RNCS /etc/hosts File

1. Log on to the RNCS as **root** user.
2. Type **cat /etc/hosts** and press **Enter**. The /etc/hosts file opens for inspection.
3. Inspect the /etc/hosts file for the following entries:
   - An entry for the RNCS (for example, lionn1), similar to **172.30.0.1 LIONN1 loghost**
   - An entry for dncsatm, similar to **10.253.0.1 dncsatm**

   Note: These IP addresses are examples only, the IP addresses you will use here will be different.
4. Do *all* entries already exist in the /etc/hosts file?
   - If **yes**, go to ***Editing the DNCS /etc/hosts File*** (on page 32).
   - If **no**, open the **/etc/hosts file** in a text editor.
5. Add the required entry or entries to the /etc/hosts file; then save and close the file.

Editing the DNCS /etc/hosts File

1. Log on to the DNCS as **root** user.
2. Type **cat /etc/hosts** and press **Enter**. The /etc/hosts file opens for inspection.
3. Inspect the /etc/hosts file for the following entries:
   - An entry for the RNCS (for example, lionn1), similar to **172.30.0.25 LIONN1 #DNCS network access to RNCS**
   - An entry for the RNCS ALOM interface, similar to **172.38.4.13 alomlionn #RNCS alom access**

   Note: These IP addresses are examples only, the IP addresses you will use here will be different.
4. Do *both* entries already exist in the /etc/hosts file?
   - If **yes**, go to ***Editing the /etc/nodename File*** (on page 33).
   - If **no**, open the **/etc/hosts file** in a text editor.
5. Add the required entry or entries to the /etc/hosts file; then save and close the file.

Editing the /etc/nodename File

1. If necessary, log on to the RNCS as **root** user.
2. Type **cat /etc/nodename** and press **Enter**. The /etc/nodename file opens for inspection.
3. Does the file already contain the hostname of the RNCS?
   - If **yes**, go to ***Editing the /etc/hostname.bge0 File*** (on page 33).
   - If **no**, open the **/etc/nodename** file in a text editor.
4. Change or add the RNCS hostname to the file.

   Example: If your RNCS hostname is lionn2, you should add the following to this file:

   ```
   lionn2
   ```
5. Save and close the file.

Editing the /etc/hostname.bge0 File

1. If necessary, log on to the RNCS as **root** user.
2. Type **cat /etc/hostname.bge0** and press **Enter**. The /etc/hostname.bge0 file opens for inspection.

   Note: For sites that use the Netra T5220 server, the file is /etc/hostname.e1000g0.
3. Does the file already contain the hostname of the RNCS?
   - If **yes**, go to ***Editing the /etc/defaultrouter File*** (on page 34).
   - If **no**, open the **/etc/hostname.bge0** file in a text editor.

     Note: For sites that use the Netra T5220 server, the file is /etc/hostname.e1000g0.
4. Change or add the RNCS hostname to the file.

   Example: If your RNCS hostname is lionn2, you should add the following to this file:

   ```
   lionn2
   ```
5. Save and close the file.

Editing the /etc/defaultrouter File

1. If necessary, log on to the RNCS as **root** user.
2. Type **cat /etc/defaultrouter** and press **Enter**. The /etc/defaultrouter file opens for inspection.
3. Does the file contain the hostname or the IP address of the default router?
   - If **yes**, close the file and go to ***Editing the /export/home/informix/etc/sqlhosts File*** (on page 34).
   - If **no**, close the file and open the **/etc/defaultrouter** file in a text editor.
4. Change or add the correct default router hostname (as defined in the /etc/hosts file) or router IP address to the file.

   Example: If the RNCS route to the DNCS is 172.30.0.30, add the following to this file:

   ```
   172.30.0.30
   ```
5. Save and close the file.

Editing the /export/home/informix/etc/sqlhosts File

1. If necessary, log on to the RNCS as **root** user.
2. Type **cat /export/home/informix/etc/sqlhosts** and press **Enter**. The /export/home/informix/etc/sqlhosts opens for examination.
3. Does the file contain the hostname of the RNCS?
   - If **yes**, go to ***Enabling the FTP Service on the RNCS*** (on page 35).
   - If **no**, open the **/export/home/informix/etc/sqlhosts** file in a text editor.
4. Change or add the RNCS hostname to the file that contains the name of the RNCS. If other entries exist, separate this new entry from the other entries by using the **Tab** key.

   Example: If your RNCS hostname is lionn2, the file entry may look similar to this example when you are finished:

   ```
   demo_on onipcshm        on_hostname     on_servername
   demo_se seipcpip        se_hostname     sqlexec
   lionnDbServer           setlitcp        lionn2    informixSE
   ```
5. Save and close the file.

Enabling the FTP Service on the RNCS

For security purposes, the FTP service is disabled after the installation. EAS equipment typically uses the FTP method to place files on the RNCS. Follow these instructions to determine whether you need to enable the FTP service on the RNCS.

1 Is the FTP service required on this system?

- If **yes**, continue with step 2.
- If **no**, go to Enabling TFTP and bootp Services.

2 As root user in an xterm window on the RNCS, type the following and press **Enter**:

inetadm –e svc:/network/ftp:default

3 Type **svcs ftp** and press **Enter** to verify that the ftp service is running.

Example: If the ftp service is running, you should see output similar to the following:

```
STATE      STIME         FMRI
online     15:08:44      svc:/network/ftp:default
```

4 Using a text editor add the following lines to the /export/home/dncs/.profile file:

 # Source the Local EAS Interface IP address

LOCAL_EAS_IP=[EAS Interface IP]; export LOCAL_EAS_IP

Note: Replace [EAS Interface IP] with the IP address of the local interface on the RNCS that will receive EAS messages. Do not type the brackets **[ ]** in the command.

5 Save and close the file.

Reboot the RNCS

To activate these network configuration changes, you need to reboot the RNCS. Follow these instructions to reboot the RNCS.

1 Type **shutdown -y -g0 -i6** and press **Enter**.

2 Log on to the RNCS as **root** user.

Checking NTP Activation

Your next step is to see if the Network Time Protocol (NTP) is activated on the RNCS. These steps guide you through the process.

1 Type **ntpq -p** and press **Enter**. The system displays output which reveals whether the RNCS is synchronized with the DNCS.

```
     remote           refid      st t when poll reach   delay   offset  disp
==============================================================================
*dncsatm        192.133.225.100  5 u   51   64   77    0.34    3.219  377.32
```

Note: The asterisk signifies that the RNCS is synchronized with the DNCS.

2 Does an asterisk precede dncsatm?

- If **yes**, NTP is properly configured on the RNCS; go to ***Add and Configure the RNCS*** (on page 37).
- If **no**, continue with step 3.

3 As root user, type **cd /etc/inet** and press **Enter**.

4 Open the **ntp.conf file** in a text editor.

5 Confirm that the ntp.conf file contains these two entries:

```
server  dncsatm
driftfile  /etc/ntp.drift
```

6 Type **svcadm disable svc:/network/ntp** and press **Enter** to stop NTP.

7 Type **ntpdate dncsatm** and press **Enter**.

Note: Ignore any "Not suitable for synchronization" message that may (or may not) appear.

Output similar to the following should appear:

```
28 Aug  12:00:32  ntpdate[18558]: step time server 10.253.1.1  offset
15.640575 sec
```

8 Type **svcadm enable svc:/network/ntp** and press **Enter** to start NTP.

9 Type **ntpq -p** and press **Enter** to verify that NTP is properly configured.

Note: You may have to repeat this command a time or two, until the asterisk appears next to dncsatm.

Add and Configure the RNCS

License the Distributed DNCS

To license the distributed DNCS, you need to complete the following procedures.

1. License the distributed DNCS. Contact Cisco Services for more information on licensing the distributed DNCS.
2. Bounce (stop and restart) the DNCS and Application Server processes. Contact Cisco Services for more information on bouncing the DNCS and Application Server processes.
3. Verify the distributed DNCS license.

Verifying the Distributed DNCS License

Complete the following steps to verify the Distributed DNCS license.

1. In the DNCS xterm window where you are logged in as root, type **licenseAud** and press **Enter**.
2. Type the number corresponding to **Display all features** and press **Enter**. A list of all available features on the DNCS displays.
3. Does **Distributed DNCS** display as **licensed**?
   - If **yes**, press **Enter**, type the number corresponding to **Quit** and press **Enter**. You are finished with this procedure.
   - If **no**, contact Cisco Services.

Adding the RNCS Site

Complete the following steps to add the RNCS to the DNCS configuration.

1. On the DNCS, open, if necessary, the DNCS Administrative Console.
2. Select the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Add**. The Site Summary window updates to reveal a new, empty row.
5. Enter the following information:
   - **Site Name**—A unique name for the site.
   - **Site ID**—A unique number identifying the site.
   - **IP Address**—The IP address of the site.
   - **MAC Address**—The MAC address must be the same as the BFS MAC address. It cannot be the same MAC address as the DNCS MAC address.

- **BFS MAC Address**—The unique MAC address of the BFS this site will use to distribute information. Use this BFS MAC Address as the Session ID MAC Addr when you define the BFS Inband Sources for this site. This BFS MAC address is also the same as the previous MAC address.
- **Online**—Select this option (so that a checkmark appears in the box) to activate the site.

6 Click **Save**. A Confirmation message appears.

7 Click **OK**.

8 Click **Exit**.

Creating the RNCS BFS Host

Complete the following steps to add the RNCS BFS host.

1 On the DNCS, click the **Application Interface Modules ta**b.

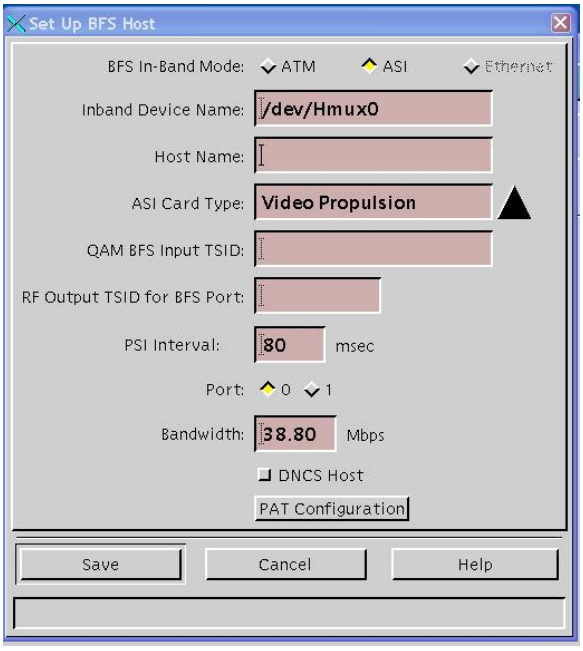
2 Click **BFS Admin**. The BFS Admin Sites window opens.

3 Select the new RNCS you added earlier.

4 Click **File > Select**. The Site BFS Administration window opens.

5 Click the **Hosts** tab.

6 Click **File > New**. The Set Up BFS Host window opens.



7 Enter the following information:

- **BFS In-Band Mode**—Select either **ATM** or **ASI**.
- **Inband Device Name**—If you are using ASI, enter **/dev/Hmux0**.
- **Host Name**—Enter the host name of the RNCS.
- **QAM BFS Input TSID**—Enter the input TSID of the RNCS BFS QAM.

- **RF Output TSID for BFS Port**—Enter the RNCS BFS QAM output port.
- **PSI Interval**—Enter **80**.
- **Port**—Select **0**.
- **Bandwidth**—Enter **38.80**.

8 Click **Save**.

Setting Up the Remote Site

Complete the following steps for each RNCS site that your DNCS will manage.

1 If necessary, open an xterm window on the DNCS.

2 Complete the following steps to log on to the xterm window as **root** user.

a Type **su -** and press **Enter**. The password prompt appears.

b Type the root password and press **Enter**.

3 Type **siteCmd -S** and press **Enter**. The following message appears:

```
Enter the host name of the site you are adding.
```

4 Type the host name of the remote site you are registering and press **Enter**.

Example: site1

Result: The following message appears:

```
Enter the IP address of the site you are adding.
```

5 Type the IP address of the remote site you are registering and press **Enter**.

Example: 192.168.100.4

Result: The following message appears:

```
The following line will be added to /etc/hosts:
[IP address]  [host name]
Do you want to continue? [y,n,?,q]
```

6 Type **y** (for yes) and press **Enter**.

Results:

- The system performs a connectivity check between the RNCS and the DNCS.
- The system sets up the RNCS with the required configuration so that a Secure Shell can be used for communications between the DNCS and the RNCS.
- The system creates a synchronization directory for the RNCS in the DNCS (/dvs/distFiles/[host name]).

Example: In the example used in this procedure, the siteCmd program creates the following directory on the DNCS: **/dvs/distFiles/site1**.

7 Verify that a secure connection exists by typing **siteCmd [hostname] ls -l** and press **Enter**. The system should display the hostname and site ID of the remote site, as well as a listing of the files in the directory of the remote site.

Note: Substitute the hostname of the remote site for [hostname].

8 Did the system display the results described in step 7?

- If **yes**, type **exit** and press **Enter** to log out the root user.
- If **no**, contact Cisco Services.

Note: For more information on the siteCmd program, see ***Options for the siteCmd Program*** (on page 73).

Create RNCS Headend Components

This section contains the procedures you need to add the required headend components to the RNCS. If you have added more than one RNCS, you will need to complete these procedures for each.

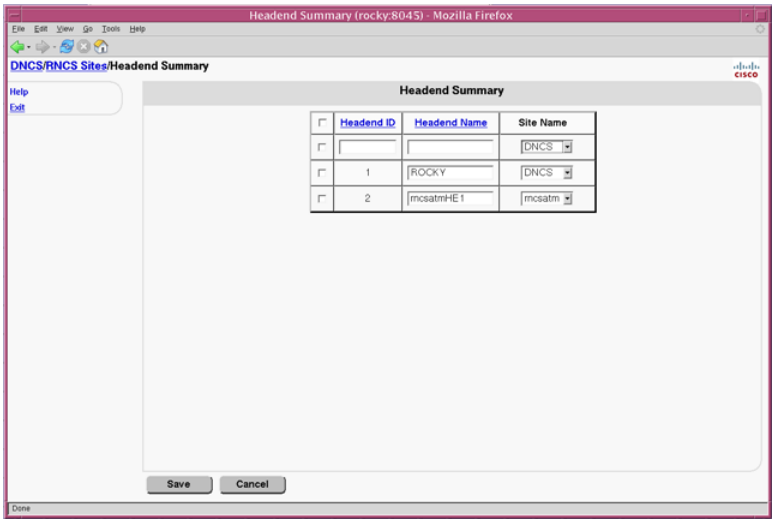
Adding the Headend

Now that you have added the RNCS to the DNCS, complete the following steps to configure the headend on the RNCS.

1 From the DNCS Administrative Console, click the **Element Provisioning** tab.

2 Click **Headend**. The Headend Summary window opens.

3 Click **Add Headend**. The Headend Summary window opens with a new, blank row.



4 Enter the following information:

- **Headend Name**—A unique name for this headend.
- **Headend ID**—A unique number identifying this headend.
- **Site Name**—Select the site this headend is associated with from the list.

5 Click **Save**. A confirmation message appears.

6 Click **OK** on the confirmation message.

7 Click **Exit**.

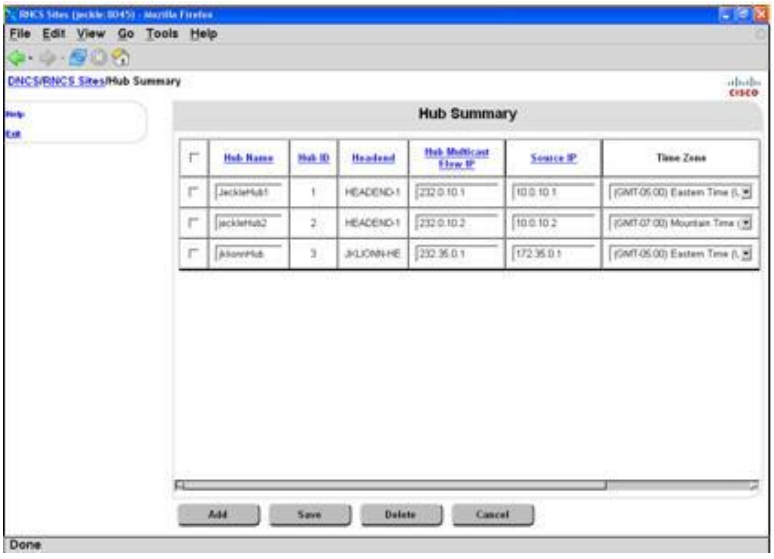
8 Add the new headend to your network map.

Adding a New Hub Entry

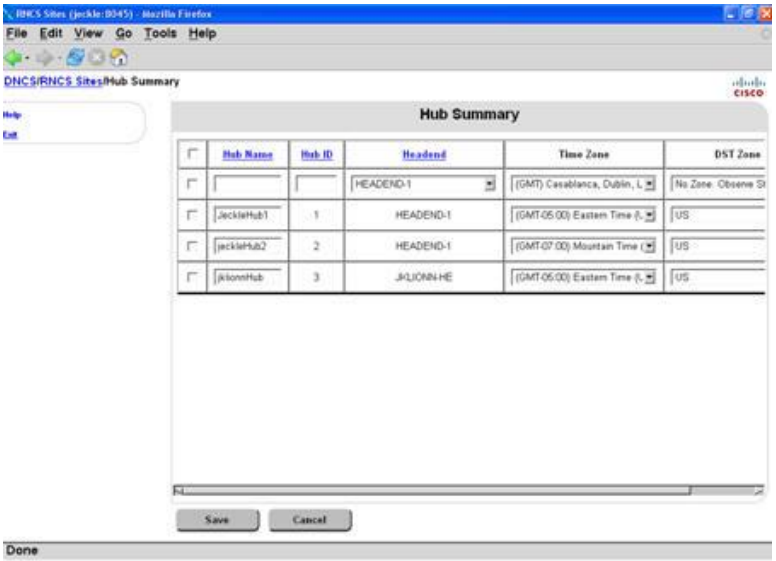
Follow these general instructions to add a new hub entry to the system.

1 From the DNCS Administrative Console, select the **Network Element Provisioning** tab.

2 Click **Hub**. The Hub Summary window opens.



3 Click **Add**. The Hub Summary window is modified to allow you to configure a new hub.



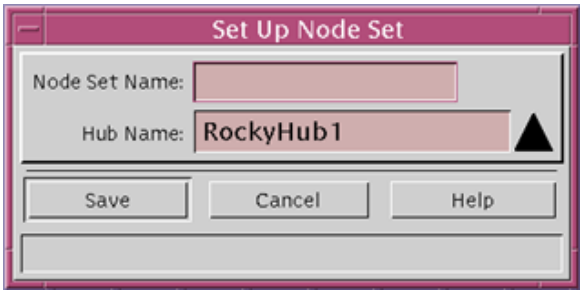
4 Configure the new hub with the following information:
   - **Hub Name** – The name you will use to identify this hub.
   - **Hub ID** – The number you will use to identify this hub.
   - **Headend** – The headend associated with this hub.
   - **Time Zone** – The time zone associated with this hub.
   - **DST Zone ID** – The DST Zone ID associated with this hub.
5 Click **Save**.
6 Add the new hub to your network map.

Adding a Node Set

Complete these steps to add a node set to the hub.

Note: We recommend that you create one node set for each QPSK demodulator you will use in this network.

1 On the DNCS Administrative Console, click the **DNCS** tab.
2 Click the **Network Element Provisioning** tab.
3 Click **Node Set**. The Node Set List window opens.
4 Click **File > New**. The Set Up Node Set window opens.



5 Type the **Node Set Name** that you will use to identify this node set. You can use up to 20 alphanumeric characters. Be sure to use a name that contains no spaces and that is consistent with the naming scheme used on your network map.
6 Select the **Hub Name** that is associated with this node set from the list.
7 Click **Save**. The system saves the node set information in the DNCS database and closes the Set Up Node Set window. The Node Set List window updates to include the new node set.
8 Add the new node set to your network map.

Adding a Billing Reference to an RCS Site

Follow these steps to add a billing reference to an RNCS site.

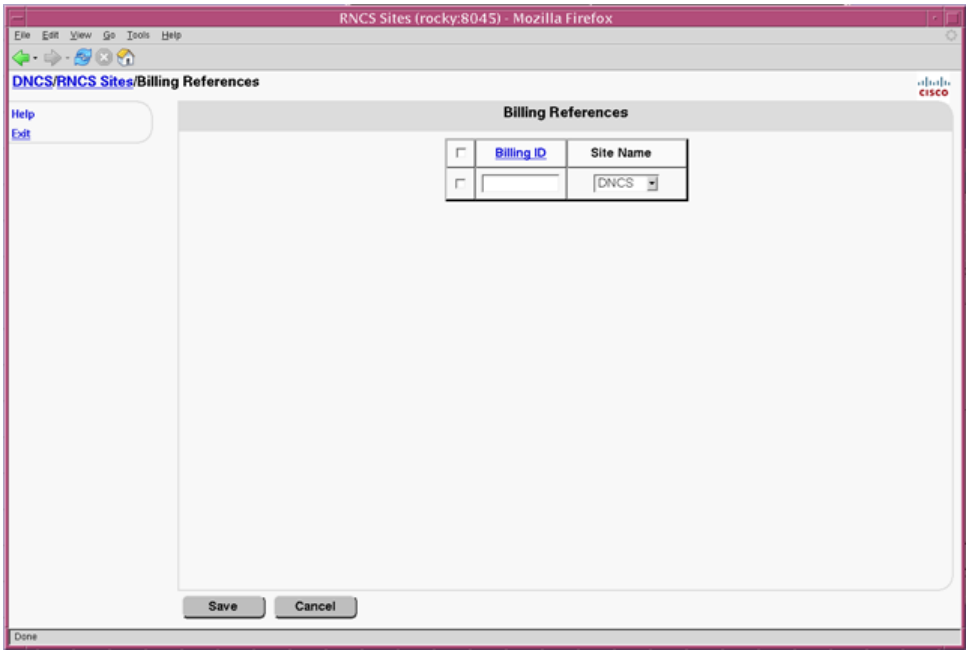
1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **System Provisioning** tab.

3 Click **RNCS Sites**. The Site Summary window opens.

4 Click **Billing References**. The Billing Reference Summary opens and lists any billing IDs have been assigned to a site.

5 Click **Add**. A new row appears in the Billing Reference Summary window.



Note: Be careful when entering information in these fields. After a billing reference is created, you cannot modify these fields unless you delete the billing reference and add it again using new information.

6 Click in the **Billing ID** field and type any number (2 or greater) that you will use to identify the billing system for each site.

Important: Ensure that each billing ID is unique. In addition, be sure to use a number that is consistent with the numbering scheme used on your network map.

Example: You might have the billing ID match the Site ID.

7 Click the **Site Name** arrow and select the site you will associate with this billing ID.

8 Click **Save**. The system displays the message "Billing update completed."

Tip: If the system does not accept the save and displays a message in an Alert box (for example, if you have inadvertently entered a number that is already used), click **OK** to close the message. Then click **Go > Back**. The system displays the information you entered earlier in step 6. You can now modify this information and click **Save** again.

Creating BFS MPEG Sources

The MPEG BFS source represents the ASI card installed in the RNCS. You will need to add an MPEG BFS source for each RNCS in your network.

Follow these steps to create a BFS MPEG source to your RNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **MPEG Source**. The MPEG Source List window opens.
4. Click **File > New**. The Set Up MPEG Source window opens with the Basic Parameters tab in the forefront.
5. Complete the following:
   - **Headend Name**—Select the headend associated with the ASI card.
   - **MPEG Source Name**—Enter the name of this MPEG source.

     Example: RNCS1_ASI

     You can use up to 20 alphanumeric characters.
   - **Device Type**—Select **ASI** as the type of MPEG source you are adding.

     Note: If ASI does not appear in the list of device types, click in the Device Type field and type ASI.
   - **IP Address**—Enter the IP address for the ASI card.
   - **Physical Address**—Enter the MAC address of the ASI card.
6. Click **Apply**. The system saves the basic parameters for this MPEG source in the database. The previously disabled Connectivity tab becomes available.
7. You will connect the BFS MPEG source to the RNCS BFS QAM after you create the other video MPEG sources and add the BFS QAM.

Creating Video MPEG Sources

Complete the following steps to add an MPEG Source for the RNCS. You must create an MPEG source for each carousel and for each audio and video stream.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **MPEG Source**. The MPEG Source List window opens.
4. Click **File > New**. The Set Up MPEG Source window opens with the Basic Parameters tab in the forefront.
5. Complete the following:
   - **Headend Name**—Select the headend associated with this source.
   - **MPEG Source Name**—Enter the name of this source. You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map.

- **Device Type**—Select the device type associated with this MPEG source. If the source will provide VOD data, select the Service Group Object option.
- **IP Address**—Enter the IP address for this MPEG source.
- **Physical Address**—Enter the MAC address for the MPEG source.

6 Click **Apply**. The system saves the basic parameters for this MPEG source in the DNCS database. The previously disabled Connectivity tab becomes available.

7 Click **Apply**. The system saves the MPEG source information in the DNCS database and updates the Connectivity illustration to include the new port information.

8 Click **Save**. The system saves the MPEG source information in the DNCS database and closes the Set Up MPEG Source window. The MPEG Source List window updates to include the new MPEG source.

9 Repeat this procedure from step 4 for additional MPEG sources you need to create.

10 You will connect the MPEG source to an RNCS QAM after you create the other video MPEG sources and add the QAM.

Adding a BFS QAM

Complete these steps to add a BFS QAM modulator for the RNCS.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Network Network Element Provisioning** tab.

3 Click **QAM**. The QAM List window opens.

4 Click **File > New > QAM**. The Set Up QAM window opens with the Basic Parameters tab in the forefront.

5 Complete the following:

- **Headend Name**—Select the headend in which this BFS QAM modulator resides.
- **QAM Name**—Enter the name you will use to identify this BFS QAM modulator. You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map.
- **IP Address**—Enter the IP address for this QAM modulator.
- **Modulation Type**—Select the type of modulation standard this modulator uses.
- **MAC Address**—Enter the MAC address for this QAM modulator.
- **Subnet Mask**—Enter the subnet mask where this QAM modulator resides.
- **Default Gateway**—If your system uses a default gateway, enter the IP address of the default gateway. Using a default gateway speeds up the reconnection process that occurs after a BFS QAM modulator is rebooted.

- **Allow SI—**Determines whether the QAM carries SI (system information), which defines it as a Distinguished QAM). Since this BFS QAM modulator is being used in an RNCS, set this option to **no (unselected)**. SI information is carried by QPSK modulators in an RNCS.
- **Input Port—**Defines the interface that connects to this QAM modulator. Since this BFS QAM modulator is being used in an RNCS, select the **ASI** option.
- **INPUT Transport Stream—**The system sets this value automatically when the corresponding transport stream ID is set up in the ASI card and the connection is established on the Connectivity tab.
- **RF OUT Fields**
  - **Modulation—**Select the type of modulation this QAM modulator uses. For example, if this modulator uses 256 QAM, you would select **256 QAM**.
  - **Transport Stream ID—**Enter a unique number that identifies the transport stream going from this QAM modulator to the set-tops on your system. You can use up to 5 numeric characters.
  - **Channel Center Frequency (MHz)—**Enter the channel frequency that will send system information to set-tops. We recommend that you enter a value in 6 MHz increments from 91 to 867 MHz.
  - **Continuous Wave Mode—**Enable this option to produce an unmodulated RF carrier. This is useful when performing testing.
  - **Mute RF Output—**Enable this option to turn off the RF output for a port. This is helpful when installing the modulator.
  - **Disabled—**Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.) This may be helpful when performing plant maintenance or in the rare event that a port fails.
  - **Interleaver Depth—**Select the depth of interleaving that the modulator uses. Available only if you are using Overlay technology.
  - **Port to Hubs—C**lick to view the hubs that are available to receive content data from this QAM.

6 Click **Apply**. The system saves the QAM modulator information you have entered thus far into the DNCS database and enables the Port To Hubs button.

7 Click **Port to Hubs**. The RF Output Port window opens. The Basic Parameters area of this window shows the data that you entered for key RF output fields. The Associated Hubs area shows the hubs that are available to receive content data from this QAM modulator.

8 Make sure the **Selected Hubs** field shows no hub names so that this QAM modulator sends BFS data (DNCS BFS QAM only) to all hubs in the headend.

Note: To remove a hub name from the Selected Hubs field, select the hub name, and click **Remove**. The hub name moves to the Available Hubs field.

9 Click **Save**. The system saves this information into the DNCS database and closes the RF Output Port window.

Important: Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use.

10 Add the BFS QAM to your network map.

Connecting the BFS MPEG Source to the RNCS BFS QAM

Follow these steps to connect the BFS MPEG source to the RNCS BFS QAM.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Network Element Provisioning** tab.

3 Click **MPEG Source**. The MPEG Source List window opens.

4 Select the BFS MPEG source that you created in ***Creating BFS MPEG Sources*** (on page 44).

5 Click **File > Open**.

6 On the Set Up MPEG source window, click the **Connectivity** tab. The Connectivity window opens with an illustration of any devices already connected to this MPEG source.

7 Click **Create Port**. The Port Number Prompt window opens.

8 Complete the following:

- **Port Number—**Enter the number that identifies the output port on this MPEG source that is physically connected to the input port on the BFS QAM modulator.
- **Transport Stream ID—**Enter the number that identifies the transport stream going from this MPEG source to the BFS QAM modulator.
- **Transport Protocol—**Select the type of output card that is installed in this MPEG source: ASI, DHEI, SWIF, or Ethernet.

  Note: If you select Ethernet, complete the Physical Address, IP Address, and the Subnet Mask fields.
- **Physical Address—**Enter the MAC address of the output card installed in this MPEG source. Only displays if you select Ethernet as the Transport Protocol.
- **IP Address—**Enter the IP address of the output card installed in this MPEG source. Only displays if you select Ethernet as the Transport Protocol.
- **Subnet Mask—**Enter the subnet mask of the output card that is installed in this MPEG source. Only displays if you select Ethernet as the Transport Protocol.

9 In the Connect To section, complete the following:

- **Headend Name**—Select the headend in which the BFS QAM resides.
- **Device Type**—Select **QAM**.
- **Device Name**—Select the name of the BFS QAM.
- **Port Number**—Select the port number on the BFS QAM modulator that is connected to the ASI card.

10 Click **Apply**. The system saves the MPEG source information in the DNCS database and updates the Connectivity illustration to include the new port information.

11 Add the connection to your network map.

Adding a QPSK

Add a QPSK Modulator

A QPSK modulator processes data going downstream from the RNCS to DAVIC set-tops, as well as data going upstream from the set-tops to the RNCS.

Note: We offer a software product that enables the DNCS to also transport DOCSIS-compliant CMTS data to DHCTs. For more information about this software product, contact the representative who handles your account.

Adding a QPSK Modulator

Follow these steps to add a QPSK modulator to the RNCS.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Network Element Provisioning** tab.

3 Click **QPSK/CMTS**. The QPSK/CMTS List window opens.

4 Click **File > New > QPSK**. The Set Up QPSK Modulator window opens with the Basic Parameters tab in the forefront.

5 Complete the following:

- **Hub Name**—Select the hub associated with this QPSK.
- **Name**—Enter the name of this QPSK. You can use up to 15 alphanumeric characters.
- **IP Address**—Enter the IP address for this QPSK.
- **Physical Address**—Enter the MAC address for the QPSK.
- **Subnet Mask**—Enter the subnet mask where this QPSK modulator resides.
- **Default Router**—Enter the IP address for the router associated with this modulator.
- **DHCT Base IP Address**—Enter the base IP address for all DHCTs (set-tops) within the domain of this modulator.

- **DHCT Subnet Mask**—Enter the subnet mask for all DHCTs within the domain of this modulator.
- **Frequency**—Enter the RF output frequency assigned to this modulator. This value can be from 70 to 130 MHz in increments of 0.25 MHz.
- **DCM (DHCT Communications Mode)**—Select the appropriate DCM from one of the following choices:
  - **DAVIC**—Select if DHCTs receive all communications (out-of-band and unicast data) on a DAVIC channel.
  - **Mixed DOCSIS/DAVIC**—Select if DHCTs receive out-of-band data on a DAVIC channel, and unicast communications on a DOCSIS channel.
  - **DOCSIS**—Select if DHCTs receive out-of-band data and unicast data on a DOCSIS channel. (The DAVIC channel may be used for out-of-band data if the DOCSIS channel is impaired.)
- **ADSG Options**—Options for creating ADSG bridges for CableCARD® module communications. Refer to *Advanced DOCSIS Set-Top Gateway Application Guide For System Release 3.8/4.3* (part number 4022455) for more information.
- **Basic Options**
  - **Continuous Wave Mode**—Determines whether the QPSK produces an unmodulated RF carrier. This is useful when performing testing.
  - **Mute RF Output**—Determines whether the QPSK's RF output port is muted. This is helpful when installing the QPSK.
  - **Broadcast Only Mode**—Determines whether the QPSK sends priority broadcast transmissions.
  - **Database Persistence**—Determines whether the QPSK stores the IP addresses of DHCTs in RAM.

6 Click the **Advanced Parameters** tab.

7 In general, the system sets up the QPSK modulator advanced parameters automatically, and you should not change them. However, if you need to change any of these parameters, use these descriptions as guidelines:

- Configuration File Name—Do not change this parameter without first consulting Cisco Services.
- Service Channel Frequency—Enter a value from 8 to 26.5 MHz based on your plant design. This parameter establishes the frequency that the DHCTs use to broadcast to the demodulators on this hub.

- Backup Service Channel Frequency—If you are NOT using a backup service channel, enter the same value in this field that you entered for the Service Channel Frequency parameter on the basic parameters tab. Otherwise, enter a value from 8 to 26.5 MHz based on your plant design.

  Important: We recommend that you **not** use a backup service channel. The backup service channel is used when the service channel fails. All reverse channel messaging is sent over the channel on which the DHCT achieves initial sign-on. If a backup service channel is in use, the DHCT may not be able to achieve initial sign-on.

- Tuner Input Attenuator—The DHCT calibration setting based on the design targets of your RF plant and the combining networks. If you need assistance, contact Cisco Services. The system will not connect to any levels that are in the fail range.

8 Click **Save**. The system saves the advanced parameters for this modulator in the DNCS database and closes the Set Up QPSK Modulator window. The QPSK List window updates to include the new QPSK modulator.

9 Cick **File > Close** to close the QPSK List window.

10 Add the new QPSK modulator to your network map.

Add a QPSK Demodulator

A QPSK demodulator performs data error correction, and then passes the data upstream to the QPSK modulator. The QPSK demodulator also monitors power levels and slot timing of incoming set-top signals. You can assign up to eight QPSK demodulators to one QPSK modulator.

Note: We offer a software product that enables the DNCS to also transport DOCSIS-compliant CMTS data. For more information about this software product, contact the representative who handles your account.

Adding a QPSK Demodulator

Important: Be very careful when you add a QPSK demodulator. Incorrectly configuring demodulators causes large numbers of DHCTs to be classified as non-responding units. In addition, the network management system will falsely log errors originating from incorrectly configured QPSK demodulators.

After you add a QPSK modulator to the RNCS, complete these steps to add all QPSK demodulators that are connected to that modulator.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Network Element Provisioning** tab.

3 Click **QPSK/CMTS**. The QPSK/CMTS List window opens.

4 Select the modulator to which you need to assign this demodulator.

5 Click **File > Demodulators**. The QPSK Modem window opens with an illustration of the modulator and its eight possible port connections.

6 Click **File > New Demod**. The Set Up QPSK Demodulator window opens.

7 Complete the following:

- **Port Number—**Select the port on the QPSK modulator from which this demodulator receives data.
- **Node Set Name—**Select the node set that you want to associate with this demodulator.

  Important: We recommend that you assign each demodulator to a unique node set.
- **Frequency—**Enter the RF input frequency assigned to this modulator. You can enter a value from 8 to 26.5 MHz, based on your plant design.

  Important:

  – Set the frequency equal to the service channel frequency of the associated QPSK modulator. (The service channel frequency of the QPSK modulator is shown in the Advanced Parameters tab of the Set Up QPSK modulator window.)

  – Set all demodulators associated with the same modulator to the same frequency.

8 Click **Save**.

- The system saves the demodulator information in the DNCS database and closes the Set Up QPSK Demodulator window.
- Then, the QPSK Modem window opens with the new demodulator appearing in the illustration.
- An information window opens.

9 Click **OK** to close the information window.

10 Add the new QPSK demodulator to your network map.

11 Repeat this procedure from step 6 to add another demodulator to this QPSK modulator, or from step 4 to add demodulators to a different QPSK modulator.

Adding Video QAMs

Complete the following steps to add a video QAM modulator to the RNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click **File> New > QAM/MQAM/GQAM** (select the appropriate option based on your installation). The Set Up QAM window opens with the Basic Parameters tab in the forefront.
5. Complete the following:
   - **Headend Name**—Select the RNCS headend associated with this QAM.
   - **QAM Name**—Enter the name of this QAM. You can use up to 20 alphanumeric characters.
   - **MAC Address**—Enter the MAC address for the QAM.
   - **IP Address**—Enter the IP address for this QAM.
   - **Subnet Mask**—Enter the subnet mask where this QAM modulator resides.
   - **Modulation Type**—Select the type of modulation this modulator uses.
   - **Default Gateway**—If your system uses a default gateway, the IP address of your default gateway. Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted.
   - **Administrative State**—Select whether this modulator is enabled.
     - Select **Online** to enable this QAM.
     - Select **Offline** to disable this QAM.
   - **Allow SI**—Since this is a content (video) QAM, do not select this option (no checkmark).
   - **Input Port**—Select the type of interface that will receive data from the QAM.
   - **INPUT Transport Stream ID**—The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab.
   - **RF OUT**
     - **Modulation**—Select the type of modulation this QAM modulator uses.
     - **Transport Stream ID**—Enter a number that identifies the transport stream going from this modulator. You can use up to 5 numeric characters.
     - **Channel Center Frequency (MHz)**—Enter the channel frequency that will send system information to set-tops. We recommend that you enter a value in 6 MHz increments from 91 to 867 MHz.
     - **Continuous Wave Mode**—Determines whether the QAM produces an unmodulated RF carrier. Enable this option to produce an unmodulated RF carrier, which is is useful when performing testing.

- **Mute RF Output—**Determines whether the QAM's RF output port is muted. Enable this option to turn off the RF output for a port. Turning off the RF output port is helpful when installing the modulator.
- **Disabled—**Determines whether you can set up additional sessions on an RF output port on the QAM. Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.) Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.

6 Click **Apply**. The system saves the information and activates the Hubs button.

7 Click **Hubs**. The RF Output Port window opens.

8 In the Available Hubs list, select the RNCS hub name that will receive data from this QAM and click **Add**. The hub name moves into the Selected Hubs list.

9 Click **Save**. The RF Output Port window closes and the Set Up QAM window is now visible.

10 Add the QAMs to your network map.

Important: Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab.

Connecting RNCS Video MPEG Sources to the RNCS Video QAMs

Follow these steps to connect the video MPEG source to the RNCS QAM.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Network Element Provisioning** tab.

3 Click **MPEG Source**. The MPEG Source List window opens.

4 Select one of the MPEG sources that you created in ***Creating Video MPEG Sources*** (on page 44).

5 Click **File > Open**. The Set Up MPEG source window opens.

6 Click the **Connectivity** tab. The Connectivity window opens with an illustration of any devices already connected to this MPEG source.

7 Click **Create Port**. The Port Number Prompt window opens.

8 Complete the following:

- **Port Number—**Enter the number that identifies the output port on this MPEG source that is physically connected to the input port on the associated content QAM, MQAM, GQAM, or GoQAM modulator. Start with the first available port number. We recommend starting with 0 (zero).
- **Transport Stream—**Enter the number that identifies the transport stream going from this MPEG source to the associated content QAM, MQAM, GQAM, or GoQAM modulator. For VOD, this number must correspond with the ASI input (usually on your network map) on the associated QAM, MQAM, GQAM, or GoQAM modulator.

  Important: You will need this number when you set up the QAM, MQAM, or GQAM.
- **Transport Protocol—**Select the type of output card that is installed in this MPEG source.

  Notes:

  – If the MPEG source is a VOD server, select **ASI**.

  – If you select **Ethernet**, complete the Physical Address, IP Address, and the Subnet Mask fields.
- **Physical Address—**Enter the MAC address of the output card installed in this MPEG source. Only displays if you select **Ethernet** as the Transport Protocol.
- **IP Address—**Enter the IP address of the output card installed in this MPEG source. Only displays if you select **Ethernet** as the Transport Protocol.
- **Subnet Mask—**Enter the subnet mask of the output card that is installed in this MPEG source. Only displays if you select **Ethernet** as the Transport Protocol.

9 In the Connect To section, complete the following:

- **Headend Name—**Select the headend in which the RNCS QAM resides.
- **Device Type—**Select **QAM**.
- **Device Name—**Select the name of the RNCS QAM.
- **Port Number—**Select the port number on the RNCS QAM modulator that is connected to this MPEG source.

10 Click **Apply**. The system saves the MPEG source information in the DNCS database and updates the Connectivity illustration to include the new port information.

11 Repeat this procedure from step 4 for each MPEG source that you need to connect to the RNCS QAM.

12 Add these connections to your network map.

Creating BFS Source Definitions

Complete these steps to create the BFS source definitions for the RNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Select the first source in the list and click **File > Source Definitions**. The Source Definition List window opens.
5. Click **File > New Digital**. The Set Up Digital Source Definition window opens.
6. In the first part of the **Session ID**, type the **RNCS MAC address**.
7. In the second part of the **Session ID,** type the original **Source ID**.
8. Click **Next**.
9. Click **Save**. The new source definition is displayed in the Source Definition List as Pending.
10. Repeat this procedure from step 4 for each BFS source in the Source List.
11. When you are finished with this procedure, close the Source Definition List window and the Source List window.

Starting the RNCS Sources

1. On the DNCS Administration Console, select the **Application Interface Modules** tab.
2. Click **BFS Admin**. The BFS Admin Sites window opens.
3. Select the RNCS you want to work with from the list, and click **File > Select**. The Site [site ID] BFS Administration window opens.
4. Click the **Sources** tab. A list of all the sources automatically created by the RNCS installation process opens.
5. Select the first source in the list and click **File > Open**. The Set Up BFS Source window for that source opens.
6. Select the **DataPump: Run** option.
7. Click **Save**. The Set UP BFS Source window closes.
8. Repeat steps 5 through 7 for each source in the RNCS with a Source ID less than or equal to 200.

Starting the RNCS

After installing and configuring the RNCS software and setting up the remote sites, you are now ready to start the server. Complete the following steps to start the server.

1. Open an xterm window on the DNCS.
2. Type **siteCmd [hostname] lionnStart** and press **Enter**.

   Note: Do not type the brackets **[ ]** in the command.
3. In the xterm window on the DNCS, type **siteCmd [hostname] lionnControl** and press **Enter**. The lionnControl utility window opens.

   Note: Do not type the brackets **[ ]** in the command.
4. Select **2** and press **Enter** to view all process elements.
5. Select **x** and press **Enter** to return to the main menu of the lionnControl utility window.
6. Select **1** and press **Enter** to stop all processes.

   Note: Wait until the **Curr Stt** (Current State) of all processes shows that they have stopped.
7. Select **2** and press **Enter** to start all processes.

   Note: Wait until the **Curr Stt** (Current State) of all processes shows that they are running.
8. Follow the on-screen instructions to exit from the lionnControl utility.

Re-Creating the All Sites Sources

After you make sure that the RNCS is running properly, you must re-create the original DNCS sources for All Sites for these sources to be available to the DNCS and the RNCS.

Follow these instructions to re-create the All Sites sources.

1. On the DNCS Administrative console, click the **Application Interface Modules** tab.
2. Click **BFS Admin**. The BFS Admin Sites window opens.
3. Select the entry that corresponds to All Sites and click **File > Select**. The Site BFS Administration window opens.

   Note: The All Sites entry could be named All Sites, DNCS, or some other name. Check your network map or with your network administrator if you are not sure which site represents All Sites.
4. Click the **Sources** tab.
5. Click **File > New**.
6. Enter the following information based on the information you recorded before you installed the RNCS.
   - Source Name
   - Source ID
   - Source Type
   - Transport Type
   - Data Rate
   - Block Size
   - Indication Interval
   - Data Pump
   - Available Hosts
7. Click **Add.** The dncsatm host moves to the Selected Hosts column.
8. Click **Save.**

2

Upgrade of RNCS Software

Introduction

Use the procedures in this chapter for upgrading a site that already supports RNCS software.

In This Chapter

Upgrade Overview

The following table lists the steps required for the RNCS software upgrade, where the section for each step begins in this document, and the information required for each procedure.

Step	Procedure	Reference	Parameters Required
1	Upgrade the RNCS software	***Upgrade the RNCS Software*** (on page 61)	■ IP address of ALOM port ■ RNCS admin user ID ■ RNCS admin user password ■ RNCS host name or IP address ■ RNCS root user password ■ EAS server IP address
2	Attach mirrors to the RNCS	***Attach Mirrors*** (on page 67)	N/A

Upgrade the RNCS Software

Upgrade the server with RNCS software using Solaris' Live Upgrade. Live Upgrade is a Solaris facility that allows operating system or application upgrades in an inactive boot environment while the active boot environment continues to run without interruption. Therefore, do *not* shut down the DNCS, RNCS, or Application Server processes unless you are instructed to do so.

Important: If you are installing RNCS software on a Sun Fire server for the first time, go to Initial Installation of RNCS Software.

Upgrading the RNCS Software

Complete the following steps to upgrade the RNCS software.

1 Complete the following steps to remotely log on to the ALOM port of the RNCS server.

   a From the DNCS, type **telnet [IP address of ALOM port]** and press **Enter**. A prompt for the user ID appears.

   Note: Substitute the IP address of the ALOM port for [IP address of ALOM port]. Do not type the brackets **[ ]** in the command.

   b Type the admin user ID and press **Enter**. A prompt for the password appears.

   c Type the password for the admin user and press **Enter**. The SC > prompt appears as the system establishes a telnet session between the DNCS and the ALOM port.

2 Type **console -f** and press **Enter**. The following message appears:
Warning: Usr <> currently has write permissions to this console and forcibly removing them will terminate any current write actions and all work will be lost. Would you like to continue?

3 Type **y** and press **Enter**.

Results:

- A confirmation message appears that instructs the user on how to return to the ALOM port.
- Control of the server is returned to the console, rather than the ALOM port.

4 On the DNCS, open another xterm window.

5 From this xterm window, telnet into the server.

Example: telnet lionn1 or **telnet [IP address of Sun Fire server]**.

6 Log on to the server as **root** user.

7 In the event that there is an existing CD or DVD in the drive of the server, type **eject cdrom** and press **Enter**.

8 Ask the on-site technician at the RNCS server to insert the DVD, labeled similarly to **RNCS Install DVD**, into the DVD drive of the RNCS server.

9 Follow these instructions to stop and restart the vold process, which manages the auto-mount functions for the CDROM drive.

a Type **/etc/init.d/volmgt stop** and press **Enter**.

b Type **/etc/init.d/volmgt start** and press **Enter**.

c Wait about a minute and type **df -k** and press **Enter** to verify that the system mounted the DVD.

10 From an xterm window on the DNCS, type **siteCmd [hostname] ps -ef | grep dvs** and press **Enter**.

Example: siteCmd lionn1 ps -ef | grep dvs

11 Does the output from step 10 reveal that lionn processes are running?

- If **yes**, go to step 12.
- If **no**, troubleshoot the issue to the best of your abilities.

Note: Call Cisco Services if you need assistance.

12 Type **metastat** and press **Enter** to verify that all metadevices have a state of **ok**.

Notes:

- Verify that all d7xx submirrors are attached.
- If any device displays a needs maintenance message, correct the issue before proceeding. Contact Cisco Services if you need assistance.

13 Type **cd /cdrom/cdrom0/s0/sai/scripts** and press **Enter**. The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.

14 Type **./LIONN_detach_mirrors** and press **Enter**. A confirmation message appears.

15 Type **y** and press **Enter**.

16 Type **metastat** and press **Enter** to verify that the **d7xx** mirrors are no longer shown.

Note: Contact Cisco Services if the d7xx mirrors are still displayed.

17 Type **./LU_LIONN** and press **Enter**. A confirmation message appears.

18 Type **y** and press **Enter**.

Results:

- The Live Upgrade of the RNCS server begins.
- The **Do you want to back up the key files** message appears.

19 Type **y** and press **Enter**.

Results:

- The system lists the key files and directories that will be backed up and later restored.
- The system displays a **Do you wish to add to the above list** message.

20 Examine the list of key files and directories that will be backed up and choose one of the following options.

- If you want to add to the list of key files and directories to be backed up, type **y** and press **Enter**. Then, follow the on-screen instructions to add to the list of files or directories.
- If you do not want to add to the list of key files and directories to be backed up, type **n** and press **Enter**.

Result: The Live Upgrade of the RNCS server continues.

21 Examine the log file for errors.

Note: The log file is /tmp/install_log.

22 Type **lustatus** and press **Enter**. The system displays the status of the LiveUpgrade boot environment.

Example: You should see results similar to this example:

```
BE_name          Complete      Active ActiveOnReboot      CopyStatus
-------------------------------------------------------------------------
1.0.0.x        yes             yes          yes                -
LIONN_V1.0.0.x   yes           no           no                 -
```

Notes:

- The version of LIONN software associated with the *1.0.0.x* designation refers to the version of the SAIlionn package currently installed on the RNCS server.
- The version of LIONN software associated with the upgrade (LIONN_V1.0.0.x) is the same as what is listed on the LIONN DVD.
- This example shows that the new version of RNCS software is not yet active.

23 Type **luactivate LIONN_<version number>** and press **Enter**.

Note: <version number> refers to the version of the RNCS DVD.

Result: The system activates the new version of RNCS software and displays the following message:

```
**************************************************************************
The target boot environment has been activated. It will be used when you
reboot.
NOTE: You must use either init or shutdown when you reboot.  If you do
not use one of these commands,
the system will not boot using the target BE.
**************************************************************************
In case of a failure while booting to the target BE, the following
process
needs to be followed to fallback to the currently working boot
environment:
1. Enter the PROM monitor (ok prompt).
2. Change the boot device back to the original boot environment by
typing:
   setenv boot-device disk:a
3. Boot to the original boot environment by typing:
   boot
**************************************************************************
Activation of boot environment <LIONN_V1.0.0.x> successful.
```

24 Type **lustatus** and press **Enter**. The system displays the status of the LiveUpgrade boot environment.

Example: You should see results similar to this example:

```
BE_name          Complete     Active ActiveOnReboot      CopyStatus
-------------------------------------------------------------------------
2.0.0.8          yes          yes          no                   -
LIONN_V1.0.0.x   yes          no           yes                  -
```

Note: The example shows that the new RNCS environment will become active after the next reboot.

25 From an xterm window on the DNCS, type **siteCmd [hostname of Sun Fire server] lionnStop** and press **Enter**. A confirmation message about stopping the lionn appears.

Example: siteCmd lionn1 lionnStop

26 Type **y** and press **Enter**. The lionn processes stop.

27 Verify that the lionn processes have stopped by typing **siteCmd [hostname of lionn] ps -ef | grep dvs** and press **Enter**.

28 Do the results from step 27 show only the **lionnInitd** and **Informix** processes?

- If **yes**, go to step 29.
- If **no** (you see other processes), complete the following steps.
  - **a** Type **siteCmd [hostname of lionn] lionnkill** and press **Enter**.
  - **b** Type **siteCmd [hostname of lionn] ps -ef | grep dvs** and press **Enter**.

    Note: Contact Cisco Services if the results from step 28 b) still show lionn processes that are running.

29 From the xterm window that you opened in step 4, type **shutdown -g0 -y -i6** and press **Enter**. The system reboots with the new software in place.

Important: Note these important points:

- Do not use an xterm window on the DNCS.
- Do not use the *reboot* or *halt* commands to reboot the server.
- After the first reboot, the engineer *may* be prompted to supply answers to some questions that appear in Installing the RNCS Software for the First Time.

30 From an xterm window on the DNCS, use the **ssh** command to access the Sun Fire server as **root** user. You should see screen output similar to the following example:

```
Last login:  < date of last login >
Sun Microsystems Inc.  Sun OS 5.10  Generic Patch  December 2002
Working directory is /dvs/lionn
Database is lionndb
Site ID= IP Addr=
```

31 Does the output from step 30 reveal that Sun OS version 5.10 installed?

- If **yes**, the upgrade is progressing successfully.
- If **no**, call Cisco Services for assistance.

32 Type **pkginfo -l SAIlionn** and press **Enter**. Your output should be similar to the following example:

```
Working directory is /dvs/lionn
Database is lionndb
Site ID=2 IPAddr=172.35.0.1
# pkginfo -l SAIlionn
   PKGINST:  SAIlionn
      NAME:  LIONN 10-10-08
  CATEGORY:  application
      ARCH:  sparc
   VERSION:  fl2.0.0.8
   BASEDIR:  /dvs
    VENDOR:  Cisco
      DESC:  LIONN 10-10-08
    PSTAMP:  bumblebee20081010083808
  INSTDATE:  Oct 12 2008 16:20
    STATUS:  completely installed
```

```
FILES:      135 installed pathnames
              8 shared pathnames
             14 directories
            101 executables
              2 setuid/setgid executables
         190458 blocks used (approx)
```

33 Does the output from step 32 indicate that version fl2.0.0.x installed successfully?

- If **yes**, go to step 34.
- If **no**, call Cisco Services for assistance.

34 Type **/dvs/lionn/bin/fixSiteConfigs** and press **Enter**. The system makes necessary modifications to the headend configuration file in the /tftpboot directory.

35 Is the FTP service required on this system?

- If **yes**, continue with step 36.
- If **no**, skip to step 40.

36 As root user in an xterm window on the RNCS, type **inetadm –e svc:/network/ftp:default** and press **Enter**.

37 Type **svcs ftp** and press **Enter** to verify that the ftp service is running.

Example: If the ftp service is running, you should see output similar to the following:

```
STATE      STIME         FMRI
online     15:08:44      svc:/network/ftp:default
```

38 Using a text editor add the following lines to the /export/home/dncs/.profile file:

 # Source the Local EAS Interface IP address

LOCAL_EAS_IP=[EAS Interface IP]; export LOCAL_EAS_IP

Note: Replace <EAS Interface IP> with the IP address of thelocal interface that will receive EAS messages. Do not type the brackets **[ ]** in the command.

39 Save and close the file.

40 From an xterm window on the DNCS, type **siteCmd [hostname of lionn] lionnStart** and press **Enter**. The lionn processes start.

Example: siteCmd lionn1 lionnStart

41 From an xterm window on the DNCS, type **siteCmd [hostname of lionn] lionnControl** and press **Enter**. Examine the output to verify that the lionn startup processes are running.

Attach Mirrors

After upgrading the RNCS software, complete the following steps to attach the server's mirrors.

Important: Note these important points:

- You need to be root user to attach the server's mirrors.
- After attaching the server's mirrors, you are committed to the upgrade. Be certain that the RNCS server is stable before committing to the upgrade.

Attaching Mirrors

1. Type **cd /cdrom/cdrom0/s0/sai/scripts** and press **Enter**. The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.
2. Type **./LIONN_attach_mirrors** and press **Enter**. A confirmation message appears.
3. Type **y** (for yes) and press **Enter**. The system runs a script that enables the disk-mirroring function of the server.
4. When the mirrors have been enabled, type **exit** and press **Enter**. The root user logs out of the server.

Suggestion Regarding the RNCS Software DVD

Leave the RNCS software DVD in the DVD drive of the RNCS server. You need the DVD in place in case you ever have to re-install the software.

3

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

A

The siteCmd Program

Introduction

The siteCmd program is useful for helping the DNCS manage remote sites. System operators typically use the siteCmd program to perform the following tasks:

- Register a remote site with the DNCS
- Copy files from the DNCS to the remote site
- Install packages onto the remote site

This appendix describes the siteCmd program, provides instructions for registering a remote site with the DNCS, and introduces (with examples) some of the options available with the siteCmd program.

In This Appendix

Introducing the siteCmd Program

The siteCmd Program and the Secure Shell

One of the requirements of the Regional Control System (RCS) is that secure communications exist between the DNCS and the remote sites managed by the DNCS. Our engineers have implemented this requirement through use of the Secure Shell.

The Secure Shell is a program that enables one computer (the host) to log on to a remote computer over a network. Through the Secure Shell, the host computer can execute commands and transfer files. The Secure Shell provides strong authentication and secure communications over unsecured channels. The Secure Shell serves as a replacement for the UNIX telnet, rlogin, rsh, and rcp utilities.

Our engineers developed the siteCmd program to serve as an interface between the user and the Secure Shell. Through use of the siteCmd program, the user can take full advantage of the functionality of the Secure Shell without having to be aware of all of the details involved in configuring the Secure Shell.

Note: The siteCmd program references the fixSiteConfigs program. The fixSiteConfigs program corrects IP addresses in the TFTP configuration files of remote sites.

Set Up the Remote Site

Before using the Secure Shell to communicate with a remote site, you need to set up that site with the DNCS. The instructions in this section describe how to use the siteCmd program to set up a remote site.

Setting Up the Remote Site

Complete the following steps for each RNCS site that your DNCS will manage.

1. If necessary, open an xterm window on the DNCS.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type **siteCmd -S** and press **Enter**. The following message appears:

   ```
   Enter the host name of the site you are adding.
   ```
4. Type the host name of the remote site you are registering and press **Enter**.

   Example: site1

   Result: The following message appears:

   ```
   Enter the IP address of the site you are adding.
   ```
5. Type the IP address of the remote site you are registering and press **Enter**.

   Example: 192.168.100.4

   Result: The following message appears:

   ```
   The following line will be added to /etc/hosts:
   [IP address]  [host name]
   Do you want to continue? [y,n,?,q]
   ```
6. Type **y** (for yes) and press **Enter**.

   Results:

   - The system performs a connectivity check between the RNCS and the DNCS.
   - The system sets up the RNCS with the required configuration so that a Secure Shell can be used for communications between the DNCS and the RNCS.
   - The system creates a synchronization directory for the RNCS in the DNCS (/dvs/distFiles/[host name]).

   Example: In the example used in this procedure, the siteCmd program creates the following directory on the DNCS: **/dvs/distFiles/site1**.

7 Verify that a secure connection exists by typing **siteCmd [hostname] ls -l** and press **Enter**. The system should display the hostname and site ID of the remote site, as well as a listing of the files in the directory of the remote site.

Note: Substitute the hostname of the remote site for [hostname].

8 Did the system display the results described in step 7?

- If **yes**, type **exit** and press **Enter** to log out the root user.
- If **no**, contact Cisco Services.

Note: For more information on the siteCmd program, see ***Options for the siteCmd Program*** (on page 73).

Options for the siteCmd Program

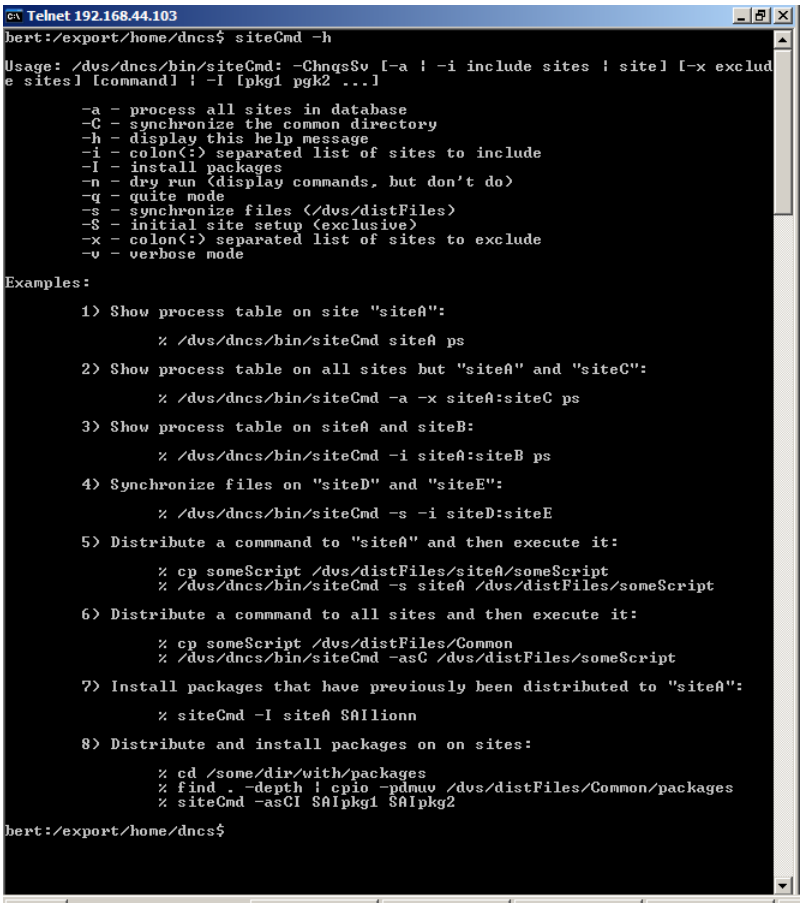
Introduction

Now that you have registered each of your remote sites with the DNCS, spend some time examining the options available with the siteCmd program. To see a list of available options, display the help window for the siteCmd program. This section describes how to display the help window of the siteCmd program and provides a few examples on the use of the various options.

Displaying the siteCmd Help Window

Complete the following steps to display the help window of the siteCmd program.

1. If necessary, open an xterm window on the DNCS.
2. Type **siteCmd -h** and press **Enter**. The system displays the help window for the siteCmd program.



Options Available With the siteCmd Program

To help you use the siteCmd program, read through the following descriptions of some of the options available for you to use with the program. The following discussion includes those relatively simple options that you are most likely to use with the siteCmd program.

Important: For more complex operations involving the Secure Shell and the siteCmd program, the user should be familiar with the use of quotation marks and other syntax rules.

Include / Exclude Remote Sites

The **–a**, **–i**, and the **–x** options allow you to specify to the siteCmd program the RNCS sites to which the commands you execute should apply.

- **–a** (all) option: Your command applies to all RNCS sites. To include only one specific site, simply name the site.
- **–i** (include) option: Include two or more specific sites.
- **–x** (exclude) option: Exclude specific sites.

Examples: The following examples are constructed using the **ps -ef** command. The **ps -ef** command lists what processes are running at the site-specific RNCS(s):

- To execute the **ps -ef** command on all RNCS sites, type **siteCmd -a ps -ef** and press **Enter**.
- To apply the **ps -ef** command to only one specific RNCS site (called site1), type **siteCmd site1 ps -ef** and press **Enter**.
- To apply the **ps -ef** command to two specific sites (called site1 and site2), type **siteCmd -i site1:site2 ps -ef** and press **Enter**.
- To exclude one specific RNCS site from the **ps -ef** command, add the **–x** option, followed by the host name of the site you want to exclude.

  Type **siteCmd -a -x site1 ps -ef** and press **Enter**.
- To exclude two specific RNCS sites from the **ps -ef** command, add the **–x** option, followed by the host names of the sites you want to exclude.

  Type **siteCmd -a -x site1:site2 ps -ef** and press **Enter**.

  Note: The **–x** (exclude) option is always used in conjunction with the **–a** (all) option.

Copy Files from the DNCS to the RNCS

The /dvs/distFiles/Common directory on the DNCS is known as the **common directory**. Files that are to be loaded onto the RNCS are usually copied into the common directory of the DNCS first. The following series of commands demonstrates how to copy a file into the common directory of the DNCS and distribute that file to each RNCS.

Note: In this example, the file someScript represents the file that needs to be distributed to each RNCS.

1 To copy the file **someScript** into the common directory of the DNCS, type **cp someScript /dvs/distFiles/Common** and press **Enter**.

2 To distribute the someScript file to each RNCS, type **siteCmd -asC /dvs/distFiles/someScript** and press **Enter**.

Notes:

- The **–a** option specifies that **all** RNCS sites are to receive the file.
- The **s** option indicates **synchronize**. Synchronizing involves updating the RNCS with the contents of the common directory of the DNCS.
- The **C** option specifies to the siteCmd program that the source directory of the DNCS is to be the common directory.
- The /dvs/distFiles/someScript portion of the command specifies the destination of the copy operation, as well as the name of the file that is to be executed once the copying has taken place.

Install a Package on the RNCS

This procedure provides instructions on using the siteCmd program to install a package on the RNCS.

Note: This procedure assumes that a CD containing the package to be installed is already inserted into the CD drive of the DNCS.

1 Follow these instructions to log onto an xterm window on the DNCS as **root** user.

Note: You must be root user to install packages.

a Type **su -** and press **Enter**. The **password** prompt appears.

b Type the root password and press **Enter**.

2 Type **cd /cdrom/cdrom0** and press **Enter**. The /cdrom/cdrom0 directory of the DNCS becomes the working directory.

3 Type **find . –name [package_name] | cpio -pudmv /dvs/distFiles/Common/packages** and press **Enter**. The system copies the files on the CD into the common directory of the DNCS.

Example:
find . -name SAImqam | cpio -pudmv /dvs/distFiles/Common/packages

4 Type **cd /** and press **Enter**. The root user home directory becomes the working directory.

5 Type **eject cdrom** and press **Enter**. The system ejects the CD.

6 Type **siteCmd [site name] lionnStop** and press **Enter**. The processes on the RNCS server are stopped.

Note: To stop processes on **all** sites, use the **-a** option.

Example: siteCmd -a lionnStop

7 Type **siteCmd [site name] lionnKill** and press **Enter**. The lionnInitd process stops.

Note: To stop the lionnInitd process on **all** sites, use the **-a** option.

Example: siteCmd -a lionnKill

8 Type **siteCmd [site name] ps -ef | grep dvs** and press **Enter** to confirm that all lionn processes are stopped.

Note: No process should contain the word **lionn** in its name. Repeat steps 6 through 8, if it does.

9 Choose one of the following options to install the SAIlionn package on the RNCS:

- To install the package on **all** sites, type **siteCmd -asCI [package_name]** and press **Enter**.
- To install the package on one specified site (site3, in this example) only, type **siteCmd -sCI site3 [package_name]** and press **Enter**.
- To install the package on multiple sites (site1 and site2, in this example), type **siteCmd -scIi site1:site2 [package_name]** and press **Enter**.
- To install the package on all sites **except** site1 and site2, type **siteCmd -asCIx site1:site2 [package_name]** and press **Enter**.

Result: The **Are you SURE you want to continue** message appears.

10 Type **y** and press **Enter**. The system processes the package and another **Are you SURE you want to continue** message appears.

11 Type **y** and press **Enter**. The system installs the package.

12 Type **siteCmd [site_name] pkginfo -l [package_name]** and press **Enter** to confirm whether the package was successfully installed.

13 Was the package successfully installed?

- If **yes**, go to step 14.
- If **no**, contact Cisco Services for assistance.

14 To restart the lionn processes, type **siteCmd [site_name] lionnStart** and press **Enter**.

Note: To start the lionn processes on **all** sites, use the **-a** option.

Example: siteCmd -a lionnStart

15 Type **siteCmd [site name] ps -ef | grep dvs** and press **Enter** to confirm that lionn processes have restarted.

16 Type **exit** and press **Enter** to log out the root user.

B

Troubleshooting

Introduction

This appendix is intended for field service engineers who encounter problems while installing or upgrading the RNCS software.

In This Appendix

Troubleshooting Steps

Follow these steps to troubleshoot your RNCS installation if it is not performing correctly.

Note: If these steps do not alleviate your problem, contact Cisco Services for assistance.

Step	Action	Notes
1.	Make sure that the Distributed DNCS feature is licensed.	Check with Cisco Services if you are not sure if this feature is licensed.
2.	Run a Doctor report on the DNCS to determine whether the DNCS is recognizing the RNCS site and that the results for the remote site (DoctorRemote) match your expectations.	See ***Run the Doctor Report*** (on page 81) for more information. Also, refer to the *DBDS Utilities Version 6.2 Installation Instructions and User Guide* (part number 4022210) for complete instructions for running the Doctor report and for information on interpreting the report results.
3.	Check the ASI Card log messages to see if the following error is reported: `ASI card in slot PCI1 (/dev/Hmux0) does not have the correct permissions` If this error is reported, verify the ASI card owner and permissions.	For more information, see one of the following sections: ■ ***ASI Card Log Messages*** (on page 85) ■ ***Verifying the ASI Card Owner and Permissions*** (on page 86)
4.	Check the BFS MAC address to make sure it is unique in your network.	For more information, see ***Check the BFS MAC Address*** (on page 88).
5.	Make sure all your BFS inband sources use the correct BFS MAC address in the Session ID MAC Address field.	For more information, see ***Check the BFS Inband Sources*** (on page 89).
6.	Check the RNCS BFSQAM to make sure that it has a connection to the RNCS ASI card using an RNCS ASI MPEG source.	For more information, see ***Check the RNCS BFSQAM*** (on page 90).
7.	Make sure that the RNCS BFS Host contains the correct BFSQAM TSIDs.	For more information, see ***Check the BFSQAM TSIDs*** (on page 91).
8.	Make sure that all the RNCS source definitions have been manually created and that their DataPumps have been manually started.	For more information, see ***Check the RNCS Source Definitions*** (on page 92).

Run the Doctor Report

The Doctor Report is one of the most important tools that system operators and support engineers can use to evaluate the configuration and operation of a DBDS. Output from the Doctor Report appears on the screen of the DNCS and is written to an output file for later analysis.

The Doctor Report generates a snapshot of system configuration. The following list contains some of the system configuration information reported by the Doctor Report:

- Installed software versions
- DNCS and Application Server disk partition utilization
- Status of DNCS and Application Server processes
- Summary of supported DHCT types
- Summary of sources, source definitions, segments, and sessions
- Summary of PPV services and events
- Data carousel/pump status and rates
- Configuration data for remote sites
- Common configuration errors that may lead to problems later

Refer to the *DBDS Utilities Version 6.2 Installation Instructions and User Guide* (part number 4022210) for complete instructions for running the Doctor report and for information on interpreting the report results.

Use the following procedure to run the Doctor Report on the DNCS.

1 If necessary, open an xterm window on the DNCS.

2 Type **cd /dvs/dncs/Utilities/doctor** and press **Enter**. The /dvs/dncs/Utilities/doctor directory becomes the working directory.

3 Type **doctor** and press **Enter**. The system generates a list of parameters that you can use to run the Doctor Report.

Note: Each parameter causes the Doctor Report to generate output with specific configuration information.

```
scooby:/dvs/dncs/Utilities/doctor$ doctor

= Doctor software version 6.2.0.2 =
= Doctor package version  =
  doctor -agestpbinghcrx [ vd ] or
  doctor [-c<number>]

        a - (almost) All options (except q and x)
        g - General Info: DNCS info, installed software info, DNCS and
            App Server disk utilization, DNCS and App Server swap space,
            database utilization, database extents, load average, DNCS
            and App Server debug flags, tracing levels, DNCS and App
            Server processes, DNCS and App Server corefiles, DNS, check
            force tune for valid service, dncs license check, large log file che
ck
            DNCS install options
        e - Element Info: DHCT state summary, DHCT type summary, active
            elements, mod slot tolerance, source, source definitions,
            segments, sessions, subscription packages, EMMs expiring soon.
        s - SI Info: SI_INSERT_RATE, system time message, distinguished
            SI QAM, SI out of band interval.
        t - Time Info: DNCS and App Server time sync, timezone, DST.
        p - PPV Info: PPV services and events, PPV and SAM service
            discrepancies, event use services, PPV files, phoneactivetime,
            EUT, GBAMs.
        b - BFS Info: BFS carousels, BFS sessions, BFS source definitions.
        i - IPG Info: IPG collector, IPG data files.
        n - Ping Elements: QPSK Ethernet, QPSK RF, QAM, NETCRYPT, BIG, TED.
        q - Check for quarantined qams and ping elements.
            This option is NOT included in all (-a).
        x - Check one-one correspondence of DHCIs and serial numbers.
            This option is NOT included in all (-a).
        v - Verbose mode: Detailed output, even if OK.
        d - Suppress screen output. Write to output file only.
        h - Generate this help text.
        c - Clean up (delete) all but the last <number> doctor reports.
            Use this switch independently of all others. Report NOT GENERATED.


        r - and one of the following options:
            hubqamList      - list what hub are associated to which QAMs
            smdgInfo        - list SMDG (StatMUX Dejitter Group) and respective
GQAM
            sdbsgInfo       - list SDB Service Group Mini Carousel Info
            genericQamInfo  - display generic QAMs and IPs
            dualGbeGqamInfo - display generic QAMs and IPs
            sdbInfo         - display SDB server info and status
            pcgInfo         - display PCGs info and status


One or more of the a, g, e, s, t, p, b, i, n, c, x or q options is required.
d and v are optional but should be used with a required option.
Option order is irrelevant.

        Note the q option must be explicitly chosen.  It can be time consuming.
        The q option automatically sets the v (verbose) option and pings and che
cks rpc bind for qams.
scooby:/dvs/dncs/Utilities/doctor$
```

4 To generate a complete Doctor Report, type **doctor -av** and press **Enter**.

Results:

- The system generates the Doctor Report listing all system configuration information and directs the output of the report to the screen.
- The system also saves the output of the Doctor Report to a file in the current directory on the DNCS.

Example: The system saves the report with a name similar to **report.061026_0921.doc**.

Notes:

- Depending upon the size of your system, it may take a few minutes for the report to generate.
- The final line of the report generated to the screen lists the file to which the output was saved.
- The report is a plain text file. You can view the report in a text editor of your choice.

DoctorRemote

The Doctor Report reports on the configuration of any remote site supported by the system. The information collected from remote sites is similar to the information collected from the DNCS. The following list contains the fields reported on for the remote sites:

- System Name
- All SAI Installed Package Information
- LIONN Info
- Virtual CPUs
- Physical Memory Configuration
- IO Devices
- Disk Info
- Checking the Status of the Metadevices
- LIONN Disk Partition Utilization
- LIONN Swap Space
- LIONN Basic System Performance Stats
- LIONN Database Log Check

  Note: This field appears only for remote sites. The LIONN Database Log Check field reports on the size of the /dvs/lionndb/liondb.log and /dvs/lionndb/lionnconnection.log files.
- LIONN Database Process Check

  Note: This field appears only for remote sites. The LIONN Database Process Check field reports on whether the Informix daemon processes are running.
- LIONN Load Average
- Current LIONN Debug Flags Set

- LIONN Processes
- Recent LIONN Corefiles (last 2 days)
- DNS Check
- Force Tune / Valid Service Check
- LIONN File Size Check
- Timezone and Daylight Savings Time Check
- EUT Update Check
- Ping All Active Elements

Refer to the *DBDS Utilities Version 6.2 Installation Instructions and User Guide* (part number 4022210) for complete instructions for running the Doctor report and for information on interpreting the report results.

ASI Card Log Messages

Solaris logs the ASI card error messages as part of the standard Solaris log. In Solaris 9 and later, the Solaris log is handled by the logadm tool. This tool is configured to rotate and delete log files on a regular basis. Check with your network administrator if you have questions concerning the rotation and deletion periods of the Solaris log files.

For more information on the logadm tool, access the manual (man) pages on Solaris by following these instructions.

1. Open an xterm window on the DNCS.
2. Type **man logadm** and press **Enter**. The UNIX man page for the logadm tool opens.

The Solaris log files that contain the ASI card log messages are located in the /var/adm directory.

Accessing the ASI Card Log Messages

1. Open an xterm window on the RNCS.
2. Type **cd /var/adm** and press **Enter**. The /var/adm directory becomes the working directory.
3. Use one of the following options:
   - To view all ASI card log messages, type **grep Hmux messages*** and press **Enter**. A list similar to the following opens:

```
messages:Jan  6 09:45:44 rncsatm Hmux: [ID 625728 kern.notice] NOTICE:
Hmux0 info: BOARD TYPE IS DVP-2764, mux enabled
messages:Jan  6 09:45:44 rncsatm Hmux: [ID 218146 kern.notice] NOTICE:
Hmux0: firmware 01.03.06
messages.1:Dec 22 08:09:16 rncsatm Hmux: [ID 625728 kern.notice] NOTICE:
Hmux0 info: BOARD TYPE IS DVP-2764, mux enabled
messages.1:Dec 22 08:09:16 rncsatm Hmux: [ID 218146 kern.notice] NOTICE:
Hmux0: firmware 01.03.06
messages.3:Dec 11 15:56:55 rncsatm Hmux: [ID 625728 kern.notice] NOTICE:
Hmux0 info: BOARD TYPE IS DVP-2764, mux enabled
messages.3:Dec 11 15:56:55 rncsatm Hmux: [ID 218146 kern.notice] NOTICE:
Hmux0: firmware 01.03.06
rncsatm:/var/adm>
```

- To view all ASI card log messages while ignoring the case, type **grep -i Hmux messages*** and press **Enter**. A list similar to the following opens:

```
messages:Jan 6 09:45:44 rncsatm Hmux: [ID 625728 kern.notice] NOTICE:
Hmux0 info: BOARD TYPE IS DVP-2764, mux enabled
messages:Jan 6 09:45:44 rncsatm Hmux: [ID 218146 kern.notice] NOTICE:
Hmux0: firmware 01.03.06
messages.1:Dec 22 08:09:16 rncsatm Hmux: [ID 625728 kern.notice] NOTICE:
Hmux0 info: BOARD TYPE IS DVP-2764, mux enabled
messages.1:Dec 22 08:09:16 rncsatm Hmux: [ID 218146 kern.notice] NOTICE:
Hmux0: firmware 01.03.06
messages.3:Dec 11 15:56:55 rncsatm Hmux: [ID 625728 kern.notice] NOTICE:
Hmux0 info: BOARD TYPE IS DVP-2764, mux enabled
messages.3:Dec 11 15:56:55 rncsatm Hmux: [ID 218146 kern.notice] NOTICE:
Hmux0: firmware 01.03.06
rncsatm:/var/adm>
```

Notes:

- If the ASI card is working correctly, the log file will be relatively small (few log entries).
- For more information on the grep utility, type **man grep** and press **Enter**.

4 Scan the log messages for errors.

- If you find the `ASI card in slot PCI1 (/dev/Hmux0) does not have the correct permissions` error, you need to copy the configureASI.pl script from the DNCS to the RNCS. See Copying the configureASI.pl Script to the RNCS for more information.
- If you find other recurring errors, contact Cisco Services.

Verifying the ASI Card Owner and Permissions

If you receive an error message concerning the ASI card in your RNCS when you attempt to start the RNCS services, you will need to verify the ASI card owner and the card permissions.

Note: Solaris logs the ASI card error messages as part of the standard Solaris log. To view the ASI log messages, see ***ASI Card Log Messages*** (on page 85).

1 Log into the RNCS as any user except root.

2 Open an xterm window.

3 Type **/opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0** and press **Enter**. The screen displays the ASI card status information similar to the following:

```
STATUS:              /dev/Hmux0
PORT:                0
MAX BANDWIDTH:       38800000
REMAINING BANDWIDTH: 18300000
TRANSPORT ID:        2
PSI INTERVAL:        80
OPTION SETTINGS:
                     188 byte packets
```

```
                    Automatic PSI table generation turned ON
ACTIVE STREAMS:     10
ACTIVE TABLE STREAM IDs:  0 0 0 0 0 0 0 0 0 0
```

4 Did the ASI card status display?

- If **yes**, you were able to log into the ASI card successfully. You are finished with this procedure.
- If **no**, continue with this procedure.

5 In the xterm window, log into the RNCS as root.

6 Type **ls -IL /dev/Hmux0** and press **Enter**. The screen displays the ASI card permissions information similar to the following:

```
crw -rw -rw    1 root    sys    0666,    0    Mar 01  17:37  /dev/Hmux0
```

7 Do the permissions display as shown above?

- If **yes**, go to step 10.
- If **no**, go to step 8.

8 Type **chmod 0666 /dev/Hmux0** and press **Enter**.

9 Repeat step 6 to verify that the permissions have changed.

10 Type **grep Hmux /etc/security/device_policy** and press **Enter** to verify that the Hmux entry exists in the device_policy file. You should see the following message:

```
Hmux*  read_priv_set=none  write_priv_set=none
```

11 Did the command return the message as shown above?

- If **yes**, go to step 15.
- If **no**, go to step 12.

12 Type **echo "Hmux* read_priv_set=none write_priv_set=none" >> etc/security/device_policy** and press **Enter**.

13 Repeat step 10 to verify that the Hmux entry is now in the device_policy file.

14 Type **shutdown -y -g0 -i6** and press **Enter** to reboot the system.

15 Open an xterm window and log into the RNCS as any user other than root.

16 Type **/opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0** and press **Enter**. The ASI card status should display.

17 Did the ASI card status display?

- If **yes**, you are finished with this procedure.
- If **no**, repeat this procedure from step 14.

Note: If the ASI card status does not display after rebooting the system again, contact Cisco Services.

Check the BFS MAC Address

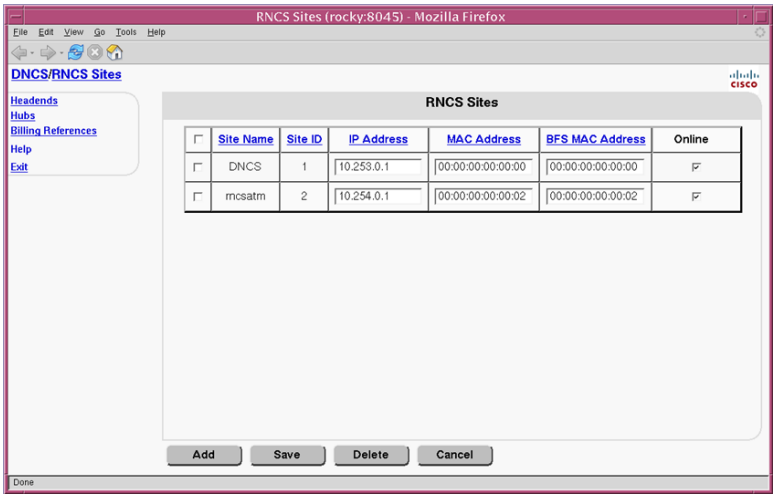
When you create an RNCS site, the BFS MAC address must be unique in your network. Follow these instructions to determine if there are any redundant BFS MAC addresses in your network.

Note: You can also consult your network map for an inventory of all the BFS QAMs in your network and their MAC addresses.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **System Provisioning** tab.

3 Click **RNCS Sites**. The RNCS Sites window opens.



4 Note the BFS MAC address of the site you are working with. You might need to refer to this MAC address in later procedures.

5 Compare this BFS MAC address to all of the other sites listed in the RNCS window.

6 If there are redundant MAC addresses, contact Cisco Services.

Check the BFS Inband Sources

The BFS inband sources in your RNCS network must use the correct BFS MAC address in the Session ID MAC Address field to work correctly.

Follow these instructions to check your BFS inband sources.

1 On the DNCS Administrative Console, click the **Application Interface Modules** tab.

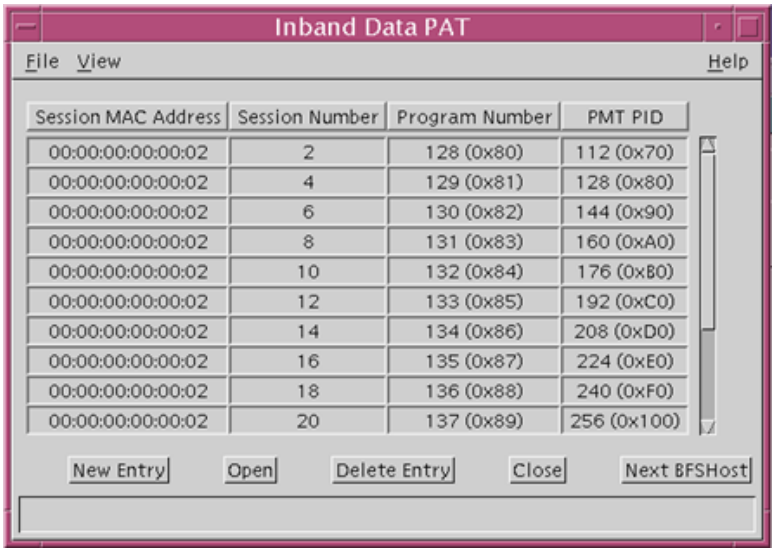
2 Click **BFS Admin**. The BFS Admin Sites window opens.

3 Select the RNCS you want to check and click **File > Select**. The Site BFS Administration window opens.

4 Click the **Hosts** tab.

5 Select the Host name in the list and click **File > Open**. The Set Up BFS Host window opens for that host.

6 Click **PAT Configuration**. The Inband Data PAT opens.



7 Look through the list of inband sources and their listed Session MAC Addresses. Do they all match the BFS MAC Address you noted in ***Check the BFS MAC Address*** (on page 88)?

- If **yes**, you are finished with this procedure. Go to ***Check the RNCS BFSQAM*** (on page 90).
- If **no**, you will need to delete the source and re-create it with the BFS MAC Address as the Session MAC Address.

Check the RNCS BFSQAM

The RNCS BFSQAM must have a connection to the RNCS ASI card using an RNCS ASI MPEG source.

Follow this procedure to check the RNCS BFSQAM connection.

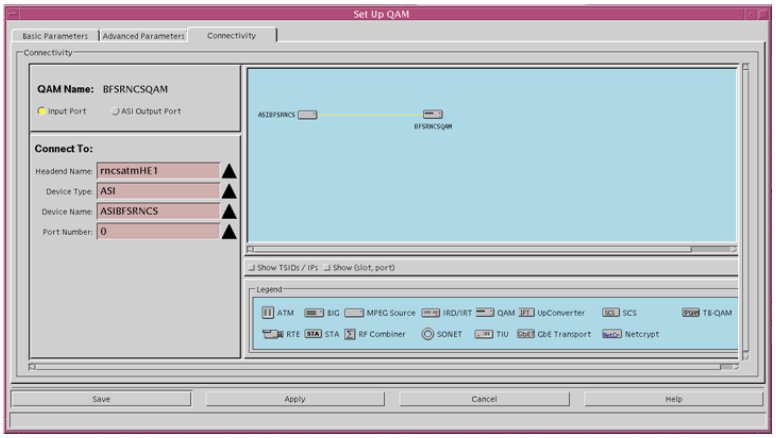
1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Network Element Provisioning** tab.

3 Click **QAM**. The QAM List window opens.

4 Select the QAM that represents the BFS QAM of the remote site and click **File > Open**. The Set Up QAM window for that QAM modulator opens.

5 Click the **Connectivity** tab. The window changes to show the connections for this QAM modulator.



6 Check the source for this QAM. Is it an MPEG source for the ASI card?

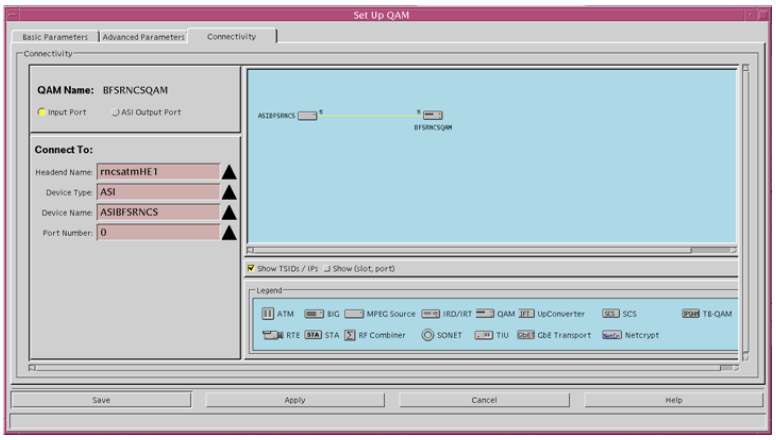
- If **yes**, you are finished with this procedure. Keep this screen open and go to to ***Check the BFSQAM TSIDs*** (on page 91).
- If **no**, correct the connection using the options in the Connect To: section of the screen.

Check the BFSQAM TSIDs

You need to make sure that the RNCS BFS Host contains the correct BFSQAM TSIDs.

Follow these steps to check the BFSQAM TSIDs.

1 On the Connectivity tab of the RNCS BFS QAM, click Show TSIDs. The window updates to show the TSIDs at both the source and at the QAM modulator.



2 Do the TSIDs at the source and at the QAM modulator match?

- If yes, you are finished with this procedure.
- If no, you need to update the TSIDs.

Check the RNCS Source Definitions

During remote site creation, the DNCS creates the standard sources (the ones with Source IDs of 200 and less). For other sources (above 200), you must sure that all the source definitions have been created and that their DataPumps have been manually started.

Follow these steps to check the RNCS source definitions.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Admin**. The BFS Admin Sites window opens.
3. Select the RNCS site you are working with and click **File > Select**. The Site BFS Admin window opens.
4. Click the **Sources** tab.
5. Click the **Source ID** column heading twice to sort the Source IDs in order from lowest to highest.
6. Leave this window open and go back to the BFS Admin Sites window.
7. Select the site that represents All Sites (for example, the DNCS site or the All Sites site) and click **File > Select**. The Site BFS Admin window opens.
8. Click the **Source ID** column heading twice to sort the Source IDs in order from lowest to highest.
9. Move the two source windows so that they are side-by-side. Are there any non-default sources (those with Source IDs higher than 200) that exist in the All Sites site that do not exist in the RNCS site?
   - If **yes**, you must create those sources in the RNCS site.
   - If **no**, go to the next step.
10. Click in the All Sites window and click **File > Close**. The All Sites window closes.
11. Click in the RNCS window.
12. Select the first non-default source in the list and click **File > Open**. The Set Up BFS Source window opens.
13. Does the **DataPump** have the **Run** option selected?
    - If **yes**, you are finished with this source. Close the Set Up BFS Source window and go to the next step.
    - If **no**, select the **Run** option (so that it is highlighted). Click **Save**. Go to the next step.
14. Repeat steps 12 and 13 for every non-default source in the list. When you are finished, close the Site BFS Admin window.

C

RNCS Rollback Procedure

Introduction

This appendix is intended for field service engineers who encounter problems while upgrading existing RNCS software. Prior to executing these rollback procedures, contact Cisco Services.

In This Appendix

Roll Back the RNCS Software

If your upgrade of RNCS software is unsuccessful, you may need to use the procedures in this appendix to restore your system to its condition prior to the upgrade.

Note: For this procedure to work, you must not yet have reattached the disk mirrors.

Important: Be sure to notify Cisco Services before concluding that an upgrade has failed and before following any of the procedures in this section. In many cases, Cisco Services can help you easily resolve the problems related to the failed upgrade.

Rolling Back the RNCS Software

Complete the following steps to roll back from an unsuccessful upgrade of RNCS software.

Note: You should still be remotely logged in to the RNCS server with root permissions.

1. Type **eeprom boot-device=disk:a** and press **Enter.** The system resets the boot device.
2. Type **shutdown -y -g0 -i6** and press **Enter**. The system reboots using the disks containing the old software.

   Important: Do not use the reboot or halt command to reboot the server.
3. After the server reboots, log on as **dncs** user.
4. Type **pkginfo -l SAIlionn** and press **Enter**. Verify that the old software is in place.
5. Type **siteCmd [hostname of server] lionnStart** and press **Enter**. The system starts the lionn processes.
6. Go to Attaching Mirrors.

Attaching Mirrors

After rolling back the RNCS software, complete the following steps to attach the server's mirrors.

Important:

- After attaching the server's mirrors, you are committed to the rollback.
- If you have already synchronized the server's mirrors, call Cisco Services for assistance before proceeding.

1. Type **cd /cdrom/cdrom0/s0/sai/scripts** and press **Enter**. The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.
2. Type **./LIONN_attach_mirrors** and press **Enter**. A confirmation message appears.
3. Type **y** (for yes) and press **Enter**. The system runs a script that enables the disk-mirroring function of the RNCS server.
4. When the mirrors have been enabled, type **exit** and press **Enter**. The root user logs out of the RNCS server.
5. Type **metastat** and press **Enter** to verify that submirrors d4xx and d7xx are in an **ok** state.

Index

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

April 2012 Printed in USA

Part Number 4022447 Rev B