RNCS Installation and Upgrade Instructions

For SR 2.7/3.7 or SR 4.2

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**.

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 Cisco 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

This guide provides Cisco field service engineers with instructions for upgrading the RNCS component of an existing DBDS currently supporting System Release (SR) 2.7/3.7 or SR 4.2.

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.

UNIX and System Expertise Requirements

System operators who follow the procedures covered in this guide need the following skills:

- Advanced knowledge of UNIX.
  - Experience with the UNIX vi editor. Several times throughout the system upgrade process, system files are edited using the UNIX vi editor. The UNIX vi editor is not intuitive. The instructions provided in this guide are no substitute for an advanced working knowledge of vi.
  - The ability to review and edit cron files.
- 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.

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 29).

Document Version

This is the first release of this document.

1

Initial Installation of RNCS Software

Introduction

This chapter describes the Sun Fire V240 server, 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 instead to ***Upgrade of RNCS Software*** (on page 29).

In This Chapter

Introducing the Sun Fire V240 Server and the ALOM Port

The Sun Fire V240 Server

Cisco has chosen the Sun Fire V240 server for the platform in the RNCS. The Sun Fire V240 server uses Sun's existing SPARC and Solaris architecture, and is designed to easily mount within a standard computer equipment rack. This highly available server is configured with the following components:

- Two UltraSPARC III processors
- Four GB of memory
- Two hard drives (36 or 73 GB)
- Four Gigabit Ethernet ports
- Serial management port
- Network management port
- Three PCI slots
- Two redundant power supplies
- A system configuration card

The ALOM Port

Taken as a whole, the serial management port and the network management port of the Sun Fire V240 server constitute the Sun Advanced Lights Out Manager (ALOM) port. The ALOM port is a system controller that allows the Sun Fire V240 server to be managed and administered from a remote location. Through the ALOM port, an engineer can monitor and control the server through a serial connection (using the SERIAL MGT port) or an Ethernet connection (using the NET MGT port).

Logging on to the Sun Fire V240 Server

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

Complete the following steps to log on to the Sun Fire V240 server.

1. Connect a laptop computer to the serial network management port of the Sun Fire V240 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 Sun Fire V240 server.
4. Type **#.** and then 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 then press **Enter**.
   b. Type the admin password and then press **Enter**. The **sc>** prompt appears.
7. Type **break** and then press **Enter**. The system interrupts the boot process of the Sun Fire V240 server.
8. Type **console -f** and then 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 Sun Fire V240 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

Configuring the ALOM Port of the Sun Fire V240 Server

Now that you have successfully connected the laptop computer to the Sun Fire V240 server and logged on, complete the following steps to configure the ALOM port.

1 At the **sc>** prompt, type **setsc if_network true** and then 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 Sun Fire V240 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 then press **Enter**. The **Re-enter new password** prompt appears.

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

c Type **setsc if_network true** and then press **Enter**. The network management port of the Sun Fire V240 server becomes functional.

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

5 Type **setsc netsc_ipaddr [IP address]** and then 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 Sun Fire V240 server for [IP address].
- The network administrator can help you determine the IP address.

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

Notes:

- Substitute the netmask of the network management port of the Sun Fire V240 server for [netmask].
- The network administrator can help you determine the netmask.

7 Type **setsc netsc_ipgateway [IP address of gateway or router]** and then 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 Sun Fire V240 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 then press **Enter**. This command sets the sc_powerstatememory variable to true.

9 Type **showsc** and then 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 and then repeat this procedure from step 8.

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

12 Type **y** and then 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 then press **Enter**.

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

16 Type **shownetwork** and then 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 then 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 Sun Fire V240 server (rather than the ALOM port).
- The **ok** prompt appears.

Choices Regarding Installation

The Sun Fire V240 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 V240 Server*** (on page 8).

  Note: Cisco recommends that you select this option in order 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 9).

Connecting to the Console of the V240 Server

After configuring the ALOM port of the V240 server, you are ready to connect to the console. Complete the following steps to connect to the console of the V240 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 then 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 then press **Enter**. A prompt for the password appears.

   c Type the password for the admin user and then 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 then press **Enter**.

Results:

- A message appears that instructs the user on how to return to the ALOM port.
- Control of the V240 is returned to the console, rather than the ALOM port.

3 Go to *Install the RNCS Software* (on page 9).

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.

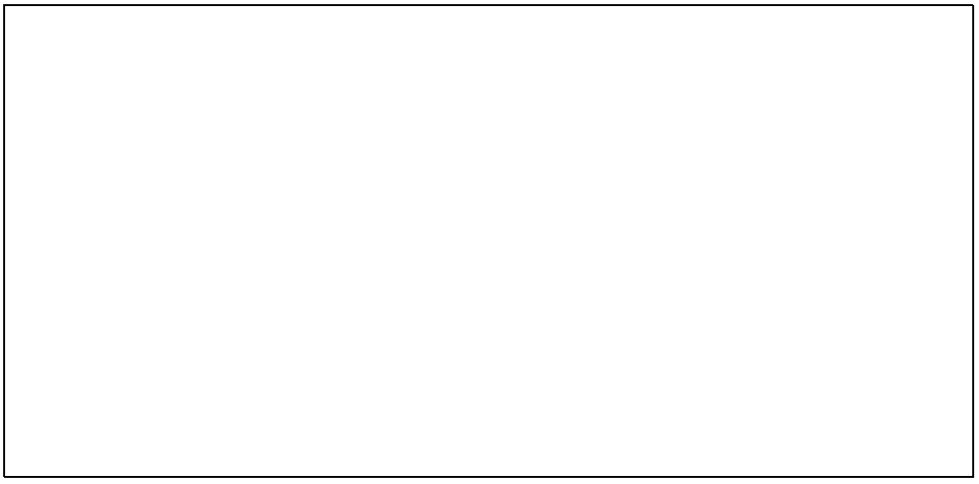
Note: In the series of screens that follow, you will often have to select a configuration parameter from a list of parameters. Use the arrow keys to navigate through your choices, and make your selection by pressing the **Spacebar**. The system usually places an **X** beside the selected parameter.

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.

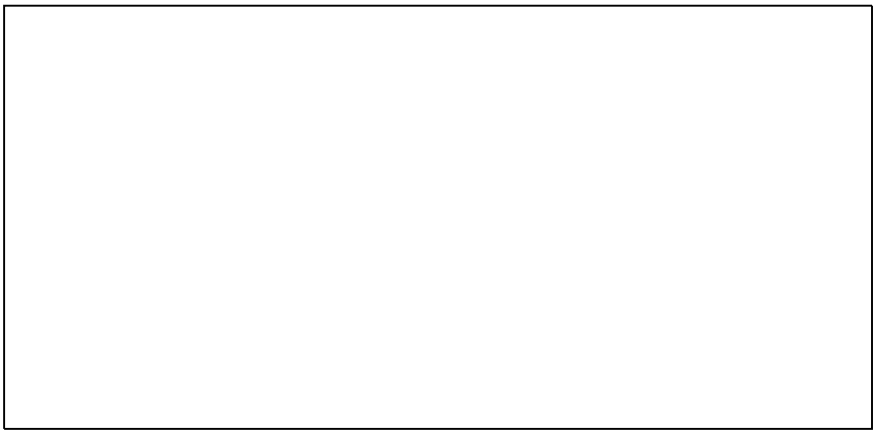
2 Type **boot cdrom – install** and then press **Enter**.

Results:

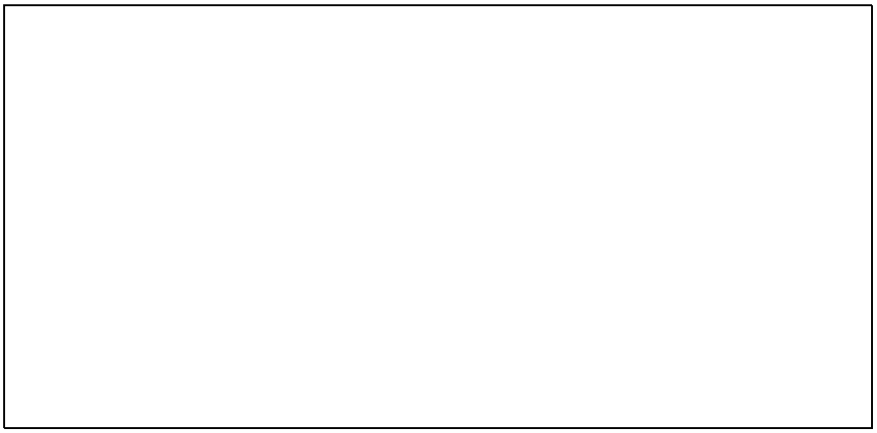
- The RNCS server reboots as the installation script begins.
- The Select a Language window appears.



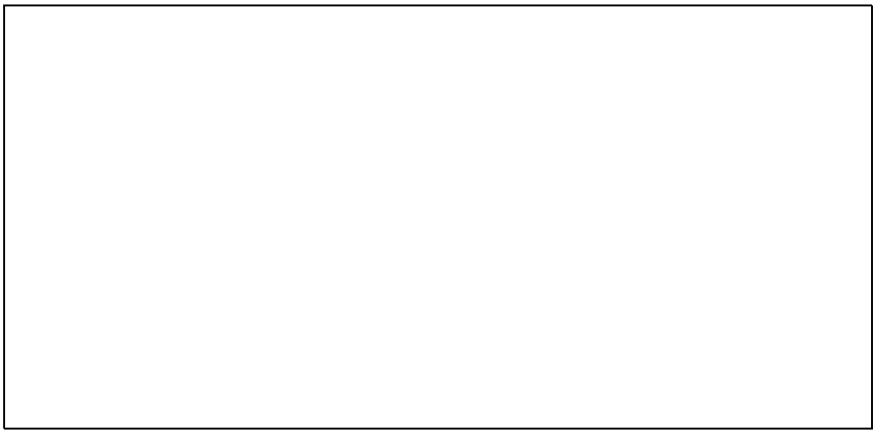
3 Type a number that corresponds to your desired language and then press **Enter**. The window updates to prompt you to identify the type of terminal you are using.



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



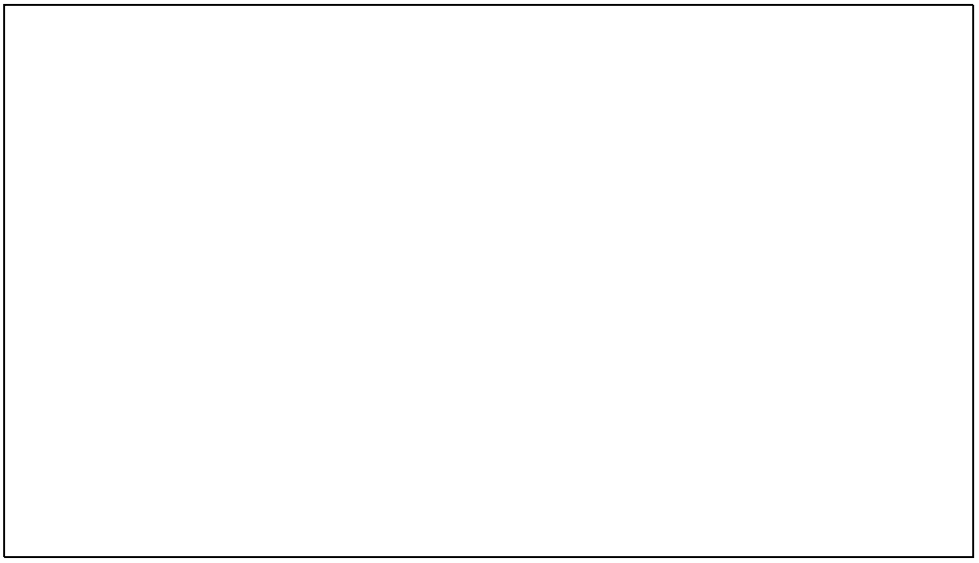
5 Read through the message displayed in step 4 and then press the **F2** key. The window updates to display another brief informational message.



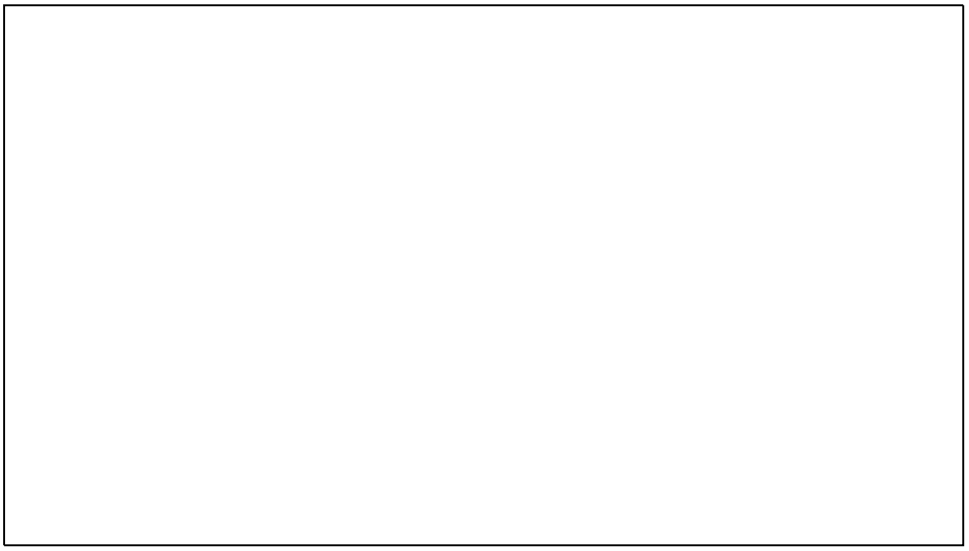
Note: On some systems, the window may also prompt you to press the **Esc** and **2** keys simultaneously in order to continue. Either method (**Esc** and **2** keys, or **F2** key) will work.

6 Press the **Esc** and **2** keys simultaneously. The window updates to prompt you to select the network interface that you want to configure.

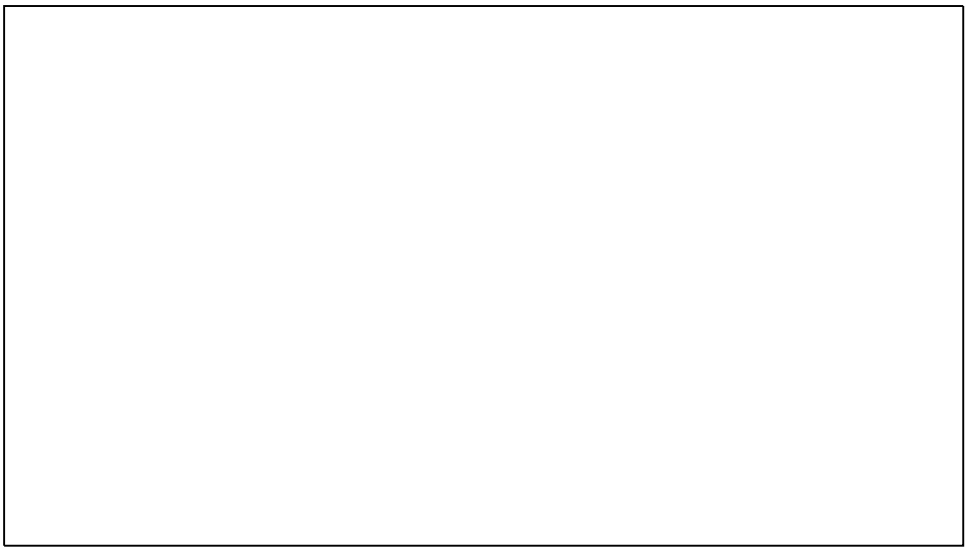
Note: Alternatively, you can press the **F2** key.



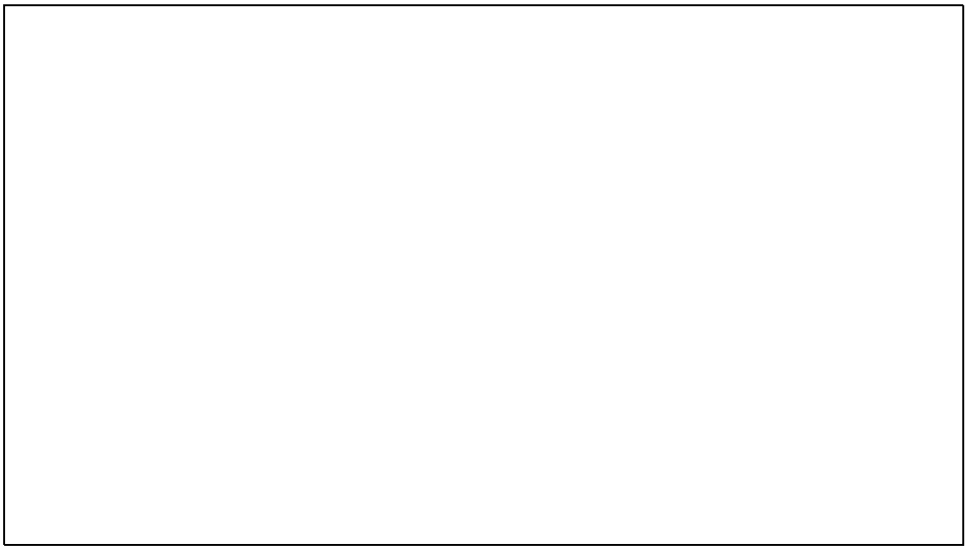
7 Select **bge0** and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify whether the Dynamic Host Configuration Protocol (DHCP) is to be used to configure the bge0 interface.



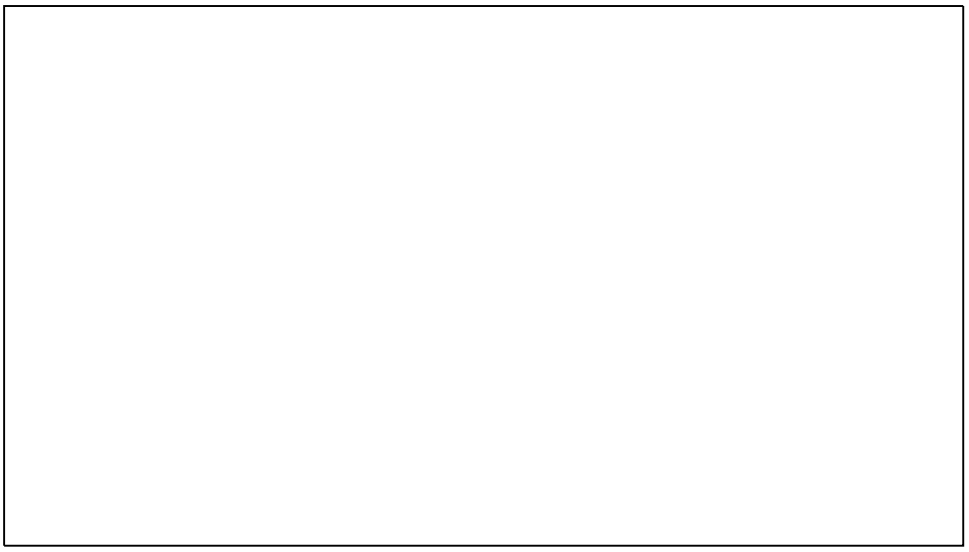
8 Select **No** and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to enter the host name that identifies this system on the network.



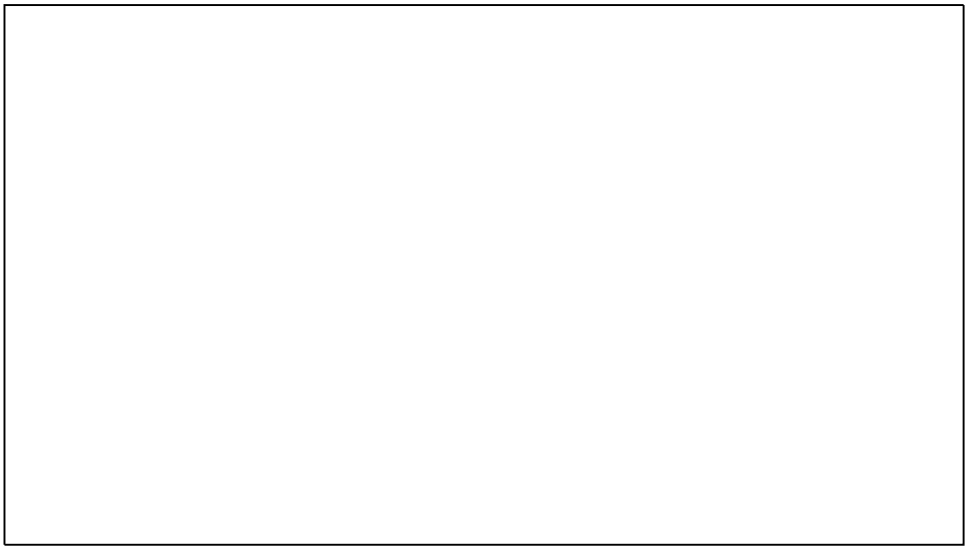
9 Type the host name (example, lionn1) and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to enter the IP address for the bge0 interface.



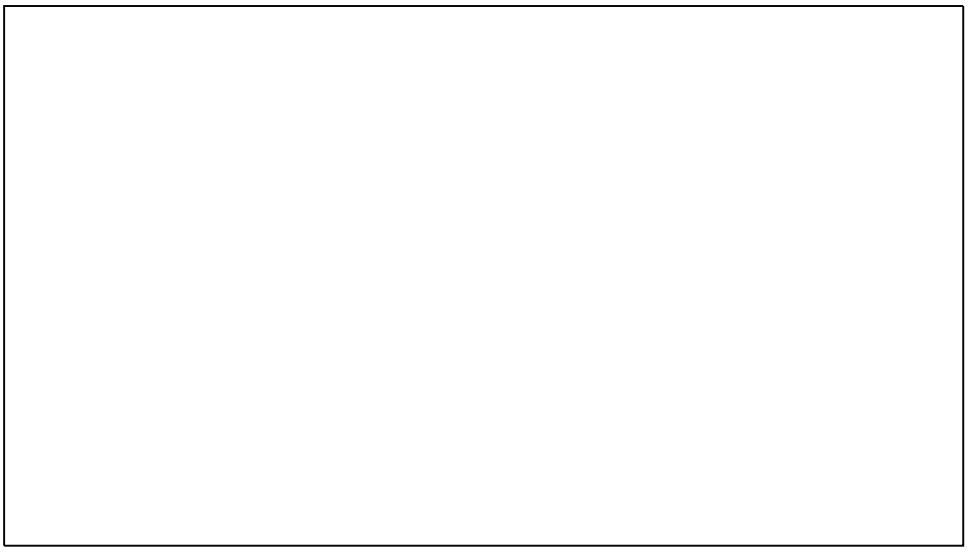
10 Type the IP address and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify whether your system is part of a subnet.



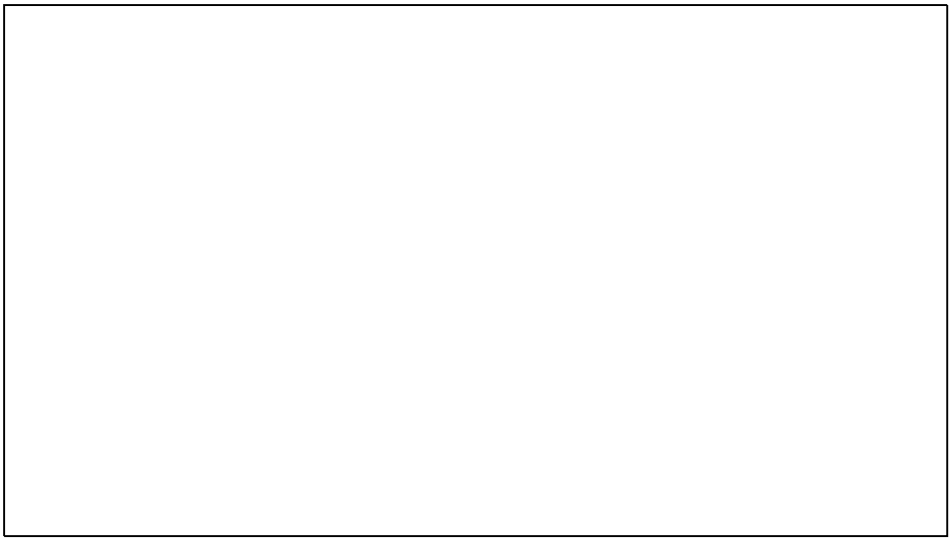
11 Select **Yes** and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify the netmask for the bge0 interface.



12 Type a netmask of **255.255.255.0** and then 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.

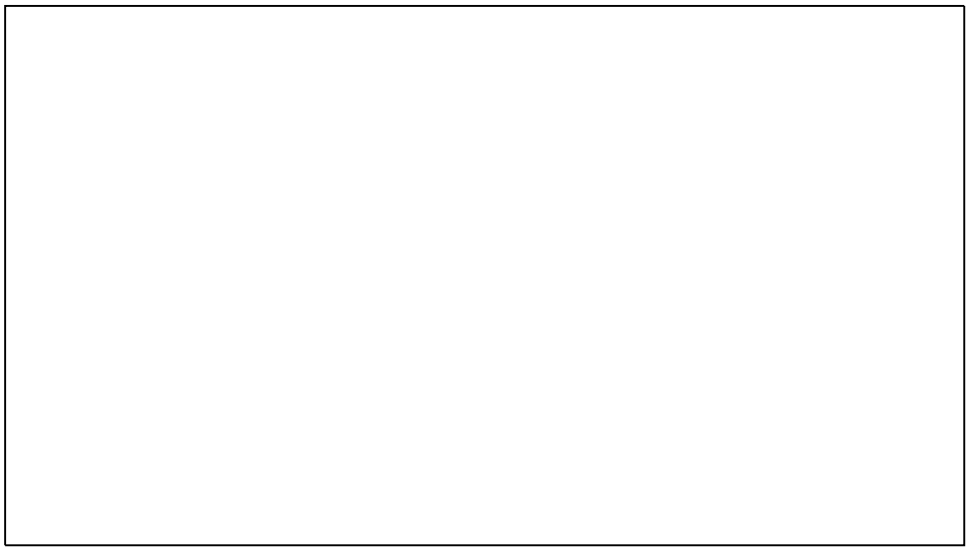


13 Select **No** and then press the **Esc** and **2** keys simultaneously. The window updates and prompts you to set the default route for the interface.

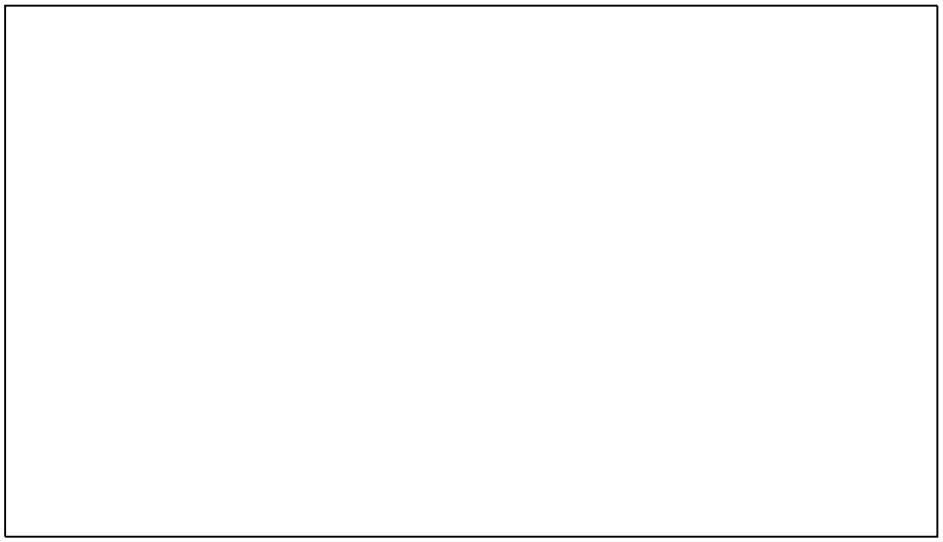


14 Choose one of the following options:

- To select no default route, select **None** and then press the **Esc** and **2** keys simultaneously. The window updates and asks you to confirm the network configuration.



- To select a default route, select **Specify one** and then press the **Esc** and **2** keys simultaneously. The window updates and prompts you to enter the IP address of the default route.

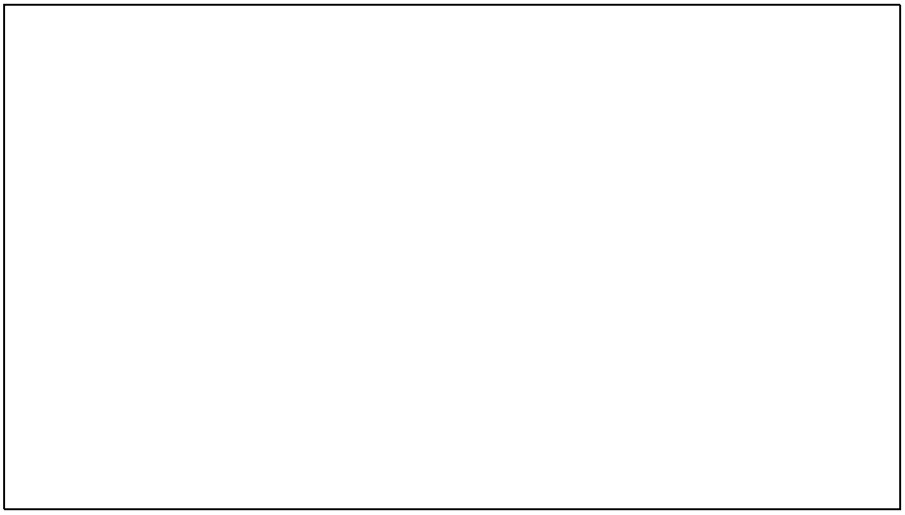


15 Did you specify a default route in step 14?

- If **yes**, type the IP address for the bge0 interface; then press the **Esc** and **2** keys simultaneously.
- If **no**, go to step 16.

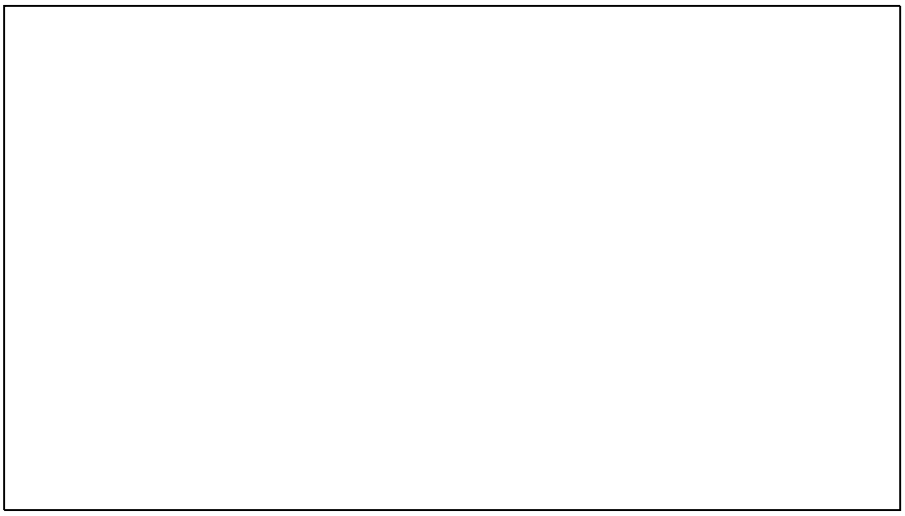
16 Review the configuration and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify whether your system will use the Kerberos security.

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.



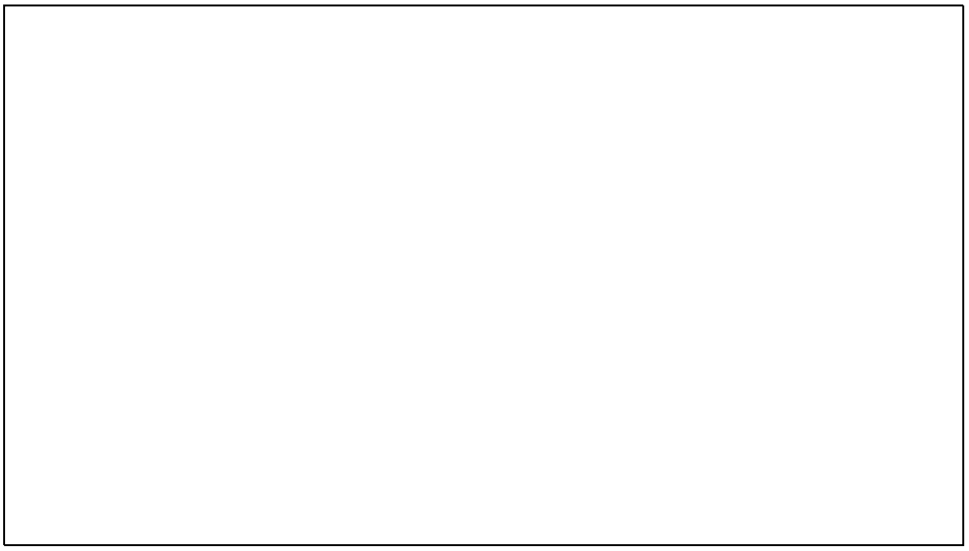
17 Select **No** and then press the **Esc** and **2** keys simultaneously.

Result: The window updates to ask you to confirm that you made the correct selection regarding Kerberos network security.

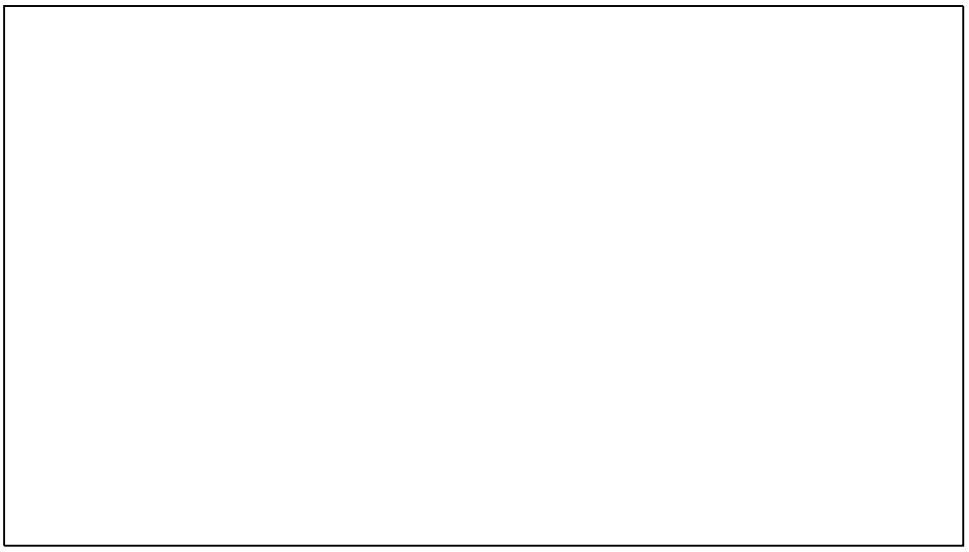


18 Review the Kerberos configuration and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to select the **Name service** for your system.

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.

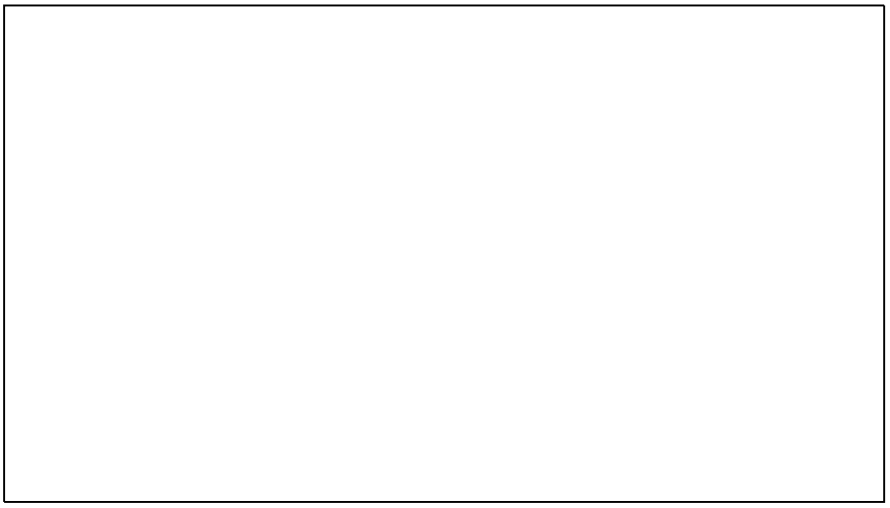


19 Select **None** and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to confirm that you made the correct decision regarding the Name service.

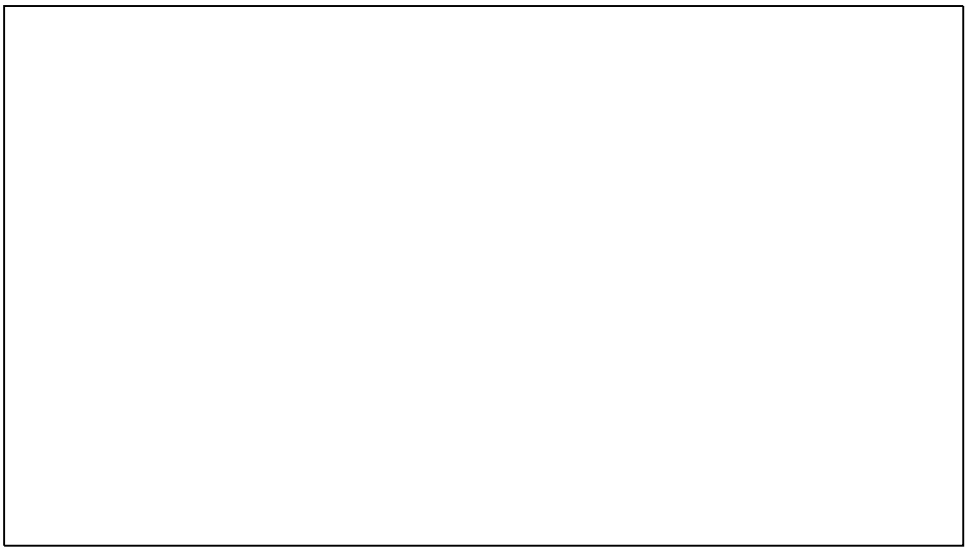


20 Review the Name service configuration and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to select your default time zone.

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.

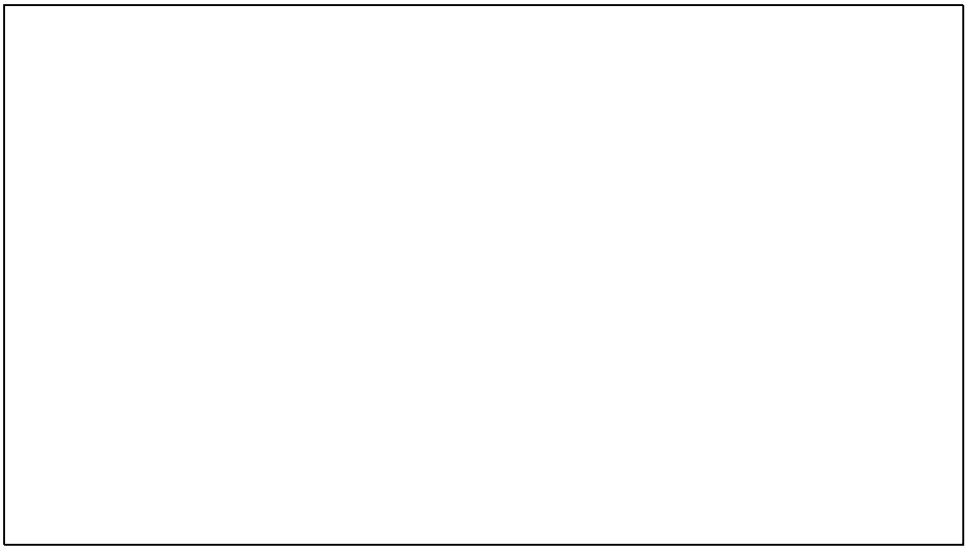


21 Select **other — specify time zone file** and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify the time zone file you want to use.

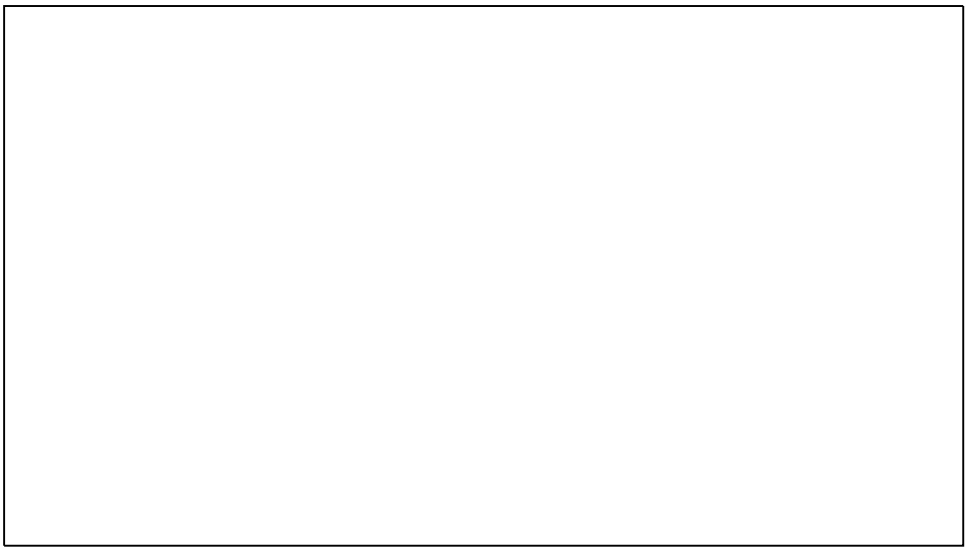


22 Type the name of the appropriate time zone file and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify the current date and time.

Note: Check the /usr/share/lib/zoneinfo directory for a list of available time zone files.



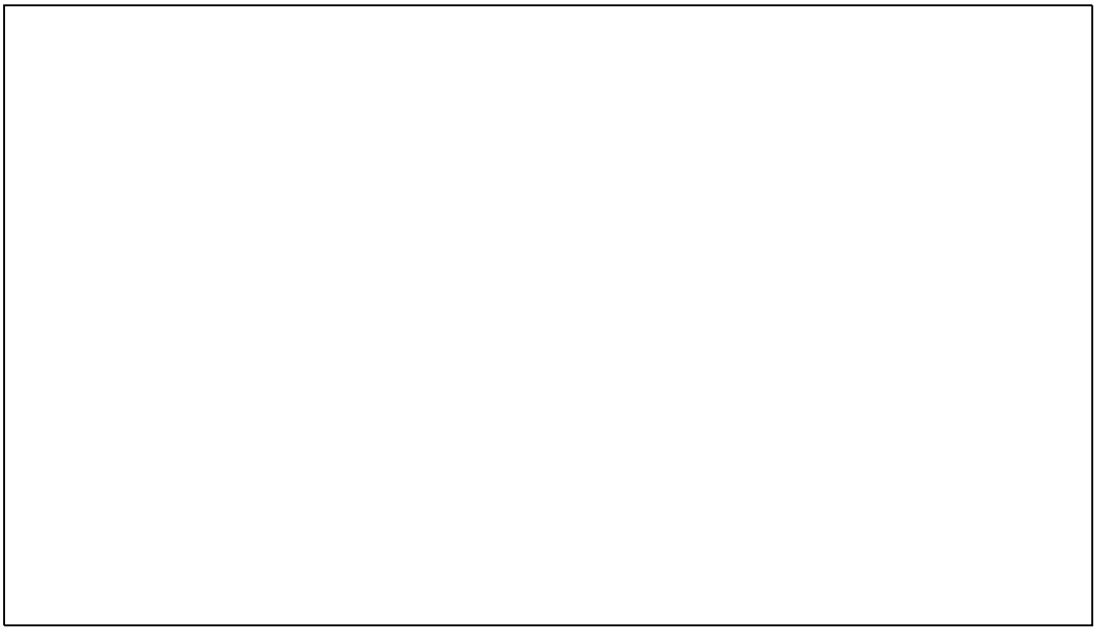
23 Select the default value, if it is correct, or type in the correct values and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to confirm the date and time information.



24 Review the date and time information and then 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.

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



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

27 Type **/cdrom/cdrom0/sai/scripts/create_sysidcfg** and then press **Enter** in order to write system ID information into memory (nvramrc).

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.

Editing the /etc/system File

Complete the following steps to edit the /etc/system file to disable TCP Fusion. TCP Fusion is a no-protocol data path for loop-back TCP connections.

Note: This procedure corrects issues documented in Sun Microsystems Alert Document (#102576).

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 **cd /etc** and then press **Enter**. The /etc directory becomes the working directory.
4. Type **cp -p system system.< date >** and then press **Enter**. The system makes a copy of the /etc/system file.

   Note: Substitute today's date, in yyyymmdd format, for < date >.

   Example: cp -p system system.2006.1121
5. Type **vi system** and then press **Enter**. The system file opens for editing using the UNIX vi text editor.
6. Press **Shift** and **g** simultaneously. The cursor advances to the last line in the file.
7. Type **o** (letter o). The system opens a new line at the end of the file.
8. Insert the following lines:
   *** Disable TCP Fusion (Sun Alert 102576)**
   set ip:do_tcp_fusion=0x0

   Important! Note these important points:
   - Be sure to type the ***** (Shift and 8 keys) at the beginning of the first line.
   - There is only one space on the second line—between **set** and **ip**. There are no other spaces on the second line.
9. Examine the lines you added in step 8 and ensure that you typed everything correctly.
10. Press **Esc**. The system exits from editing mode.
11. Type **:wq!** to save the file and to close the vi editor.
12. In the xterm window on the DNCS, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The DNCS reboots.
13. Log on to the DNCS as **dncs** user.

Attach Mirrors

In this procedure, you will log in to the Sun Fire V240 server and enable the disk-mirroring function of the server. Complete the following steps to log on to the Sun Fire V240 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 Sun Fire V240 server as **root** user.
2. Type **cd /cdrom/cdrom0/s0/sai/scripts** and then press **Enter**. The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.
3. Type **./V240_attach_mirrors** and then press **Enter**. A confirmation message appears.
4. Type **y** (for yes) and then press **Enter**. The system runs a script that enables the disk-mirroring function of the Sun Fire V240 server.
5. When the mirrors have been enabled, type **exit** and then press **Enter**. The root user logs out of the Sun Fire V240 server.

Suggestion Regarding the RNCS Software DVD

Leave the RNCS software DVD in the DVD drive of the Sun Fire V240 server. You need the DVD in place in case you ever have to reboot the server or re-install the software.

Add and Configure the RNCS

Configuring the RNCS on the DNCS

Now that you have added the RNCS to the DNCS, complete the following steps to configure 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**
   - **Headend ID**
   - **Site Name**
5. Click **Save**. A confirmation message appears.
6. Click **OK** on the confirmation message.
7. Click **Exit**.

Adding the RNCS Site

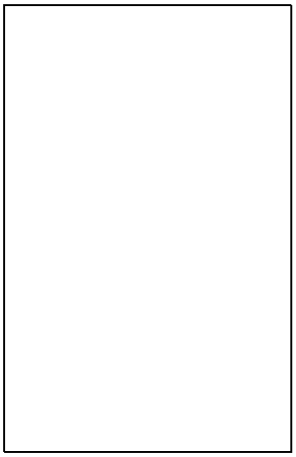
Complete the following steps to add the RNCS to the DNCS configuration.

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 Site**. The Site Summary window updates to reveal a new, empty row.
5. Enter the following information:
   - **Site Name**
   - **Site ID**
   - **Site IP Address**
   - **Site MAC Address**
   - **BFS MAC Address**
6. Click **Save**. A Confirmation message appears.
7. Click **OK**.
8. Click **Exit**.

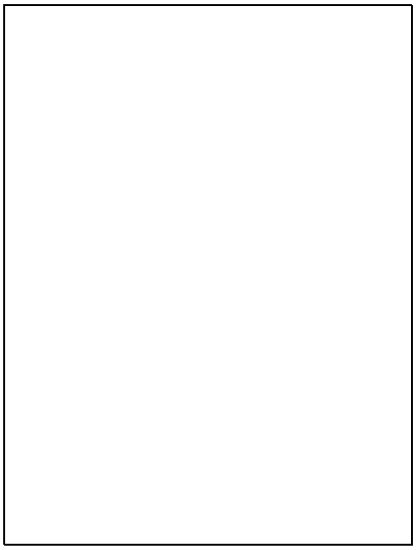
Adding a New BFS Host

After configuring the RNCS on the DNCS, complete the following steps to add a new BFS host.

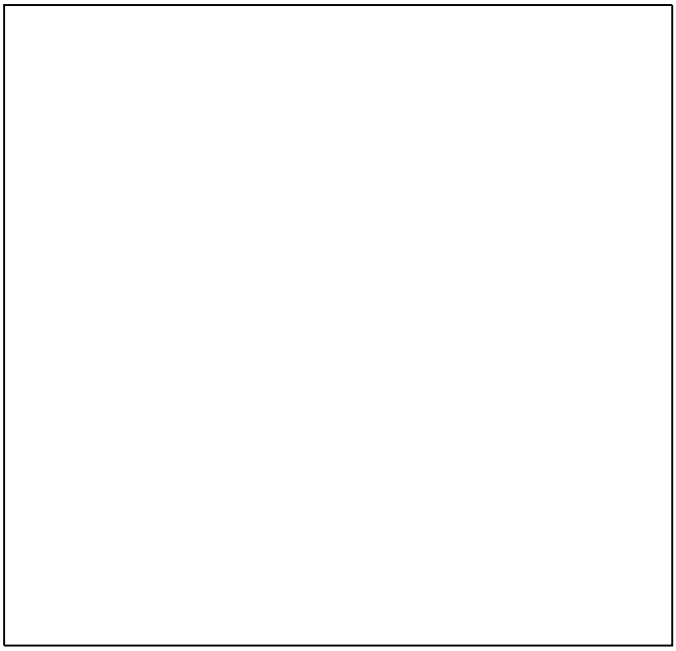
1. From the DNCS Administrative Console, select the **Application Interface Modules** tab.
2. Click **BFS Admin**. The BFS Admin Sites window opens.



3. Highlight the new RNCS site.
4. Click **File** and then click **Select**. The Site <site name> BFS Administration window opens.



5 Click **File** and the click **New**. The Set Up BFS Host window opens.



6 Enter the following information:

- **BFS In_Band Mode** (ATM or ASI)
- **Inband Device Name**
- **Host Name**
- **QAM BFS Input TSID**
- **RF Output TSID for BFS Port**
- **PSI Interval**
- **Port**
- **Bandwidth**

7 Click **Save**.

8 Click **PAT Configuration**.

9 Click **Save**.

Set Up the Remote Site

Your next step is to initialize the RNCS using the siteCmd program. Follow the ***Setting Up the Remote Site*** (on page 43) procedure in Appendix A.

Starting the RNCS

After installing and configuring the RNCS software, 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 then press **Enter**.

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 the RNCS Software

Introduction

Upgrade the Sun Fire V240 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 V240 server for the first time, go to Chapter 1, ***Initial Installation of RNCS Software*** (on page 1).

Upgrading the RNCS Software

Complete the following steps to upgrade the RNCS software.

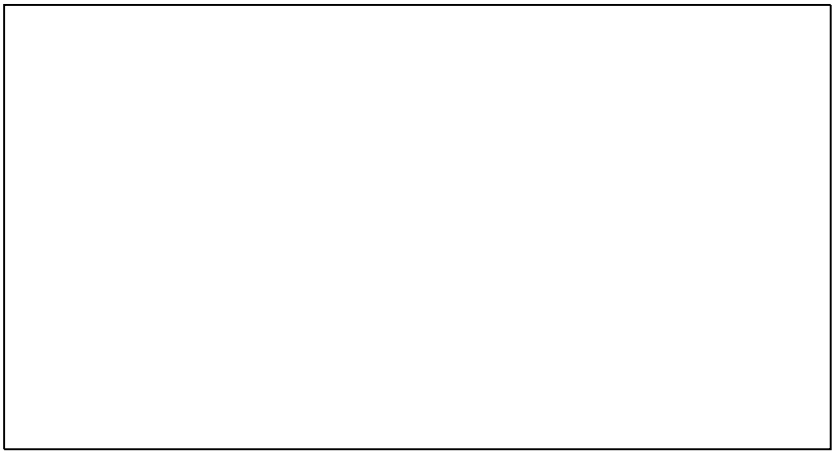
1 Complete the following steps to remotely log on to the ALOM port of the RNCS server.

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

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

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

   c Type the password for the admin user and then 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 then 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 then press **Enter**.

Results:

- A confirmation message appears that instructs the user on how to return to the ALOM port.
- Control of the V240 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 Sun Fire V240 server.

Example: **telnet lionn1** or **telnet <IP address of Sun Fire V240 server>**.

6 Log on to the Sun Fire V240 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 then 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 then press **Enter**.

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

10 From an xterm window on the DNCS, type **siteCmd <hostname> "ps -ef | grep dvs"** and then 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 then press **Enter** to verify that all metadevices have a state of **ok**.

Note: 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 then press **Enter**. The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.

14 Type **./V240_detach_mirrors** and then press **Enter**. A confirmation message appears.

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

16 Type **metastat** and then 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_V240** and then press **Enter**. A confirmation message appears.

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

Results:

- The system lists the key files and directories that will be backed up and then 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 then 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 then 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 then 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 then 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_V1.0.0.x** and then press **Enter**.

Note: V1.0.0.x 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 then 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	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 V240 server> lionnStop** and then press **Enter**. A confirmation message about stopping the lionn appears.

Example: siteCmd lionn1 lionnStop

26 Type **y** and then 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 then 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 then press **Enter**.
  - **b** Type **siteCmd <hostname of lionn> ps -ef | grep dvs** and then 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 then 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.

30 From an xterm window on the DNCS, telnet into the Sun Fire V240 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=< site ID > IP Addr=< IP address >

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 then press **Enter**. Your output should be similar to the following example:

PKGINST: SAIlionn
NAME: LIONN 10-31-2006
CATEGORY: application
ARCH: sparc
VERSION: 1.2.0.24
BASEDIR: /dvs
VENDOR: Cisco
DESC: LIONN 10-31-2006
PSTAMP: nilo20061031044840
INSTDATE: Oct 31 2006 03:49
STATUS: completely installed
FILES: 132 installed pathnames
4 shared pathnames
14 directories
103 executables
2 setuid/setgid executables
104900 blocks used (approx)

33 Does the output from step 32 indicate that version 1.2.0.x installed successfully?

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

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

35 From an xterm window on the DNCS, type **siteCmd <hostname of lionn> lionnStart** and then press **Enter**. The lionn processes start.

Example: siteCmd lionn1 lionnStart

Editing the /etc/system File

Complete the following steps to edit the /etc/system file to disable TCP Fusion. TCP Fusion is a no-protocol data path for loop-back TCP connections.

Note: This procedure corrects issues documented in Sun Microsystems Alert Document (#102576).

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 **cd /etc** and then press **Enter**. The /etc directory becomes the working directory.
4. Type **cp -p system system.< date >** and then press **Enter**. The system makes a copy of the /etc/system file.

   Note: Substitute today's date, in yyyymmdd format, for < date >.

   Example: cp -p system system.2006.1121
5. Type **vi system** and then press **Enter**. The system file opens for editing using the UNIX vi text editor.
6. Press **Shift** and **g** simultaneously. The cursor advances to the last line in the file.
7. Type **o** (letter o). The system opens a new line at the end of the file.
8. Insert the following lines:
   *** Disable TCP Fusion (Sun Alert 102576)**
   set ip:do_tcp_fusion=0x0

   Important! Note these important points:
   - Be sure to type the ***** (Shift and 8 keys) at the beginning of the first line.
   - There is only one space on the second line—between **set** and **ip**. There are no other spaces on the second line.
9. Examine the lines you added in step 8 and ensure that you typed everything correctly.
10. Press **Esc**. The system exits from editing mode.
11. Type **:wq!** to save the file and to close the vi editor.
12. In the xterm window on the DNCS, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The DNCS reboots.
13. Log on to the DNCS as **dncs** user.

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 then press **Enter**. The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.
2. Type **./V240_attach_mirrors** and then press **Enter**. A confirmation message appears.
3. Type **y** (for yes) and then press **Enter**. The system runs a script that enables the disk-mirroring function of the Sun Fire V240 server.
4. When the mirrors have been enabled, type **exit** and then press **Enter**. The root user logs out of the Sun Fire V240 server.

Suggestion Regarding the RNCS Software DVD

Leave the RNCS software DVD in the DVD drive of the Sun Fire V240 server. You need the DVD in place in case you ever have to reboot the server or 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. Cisco 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.

Cisco 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

Introduction

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 then 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 then 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 then 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 then 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 then 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 then press **Enter** to log out the root user.
- If **no**, call Cisco Services for assistance.

Options for the siteCmd Program

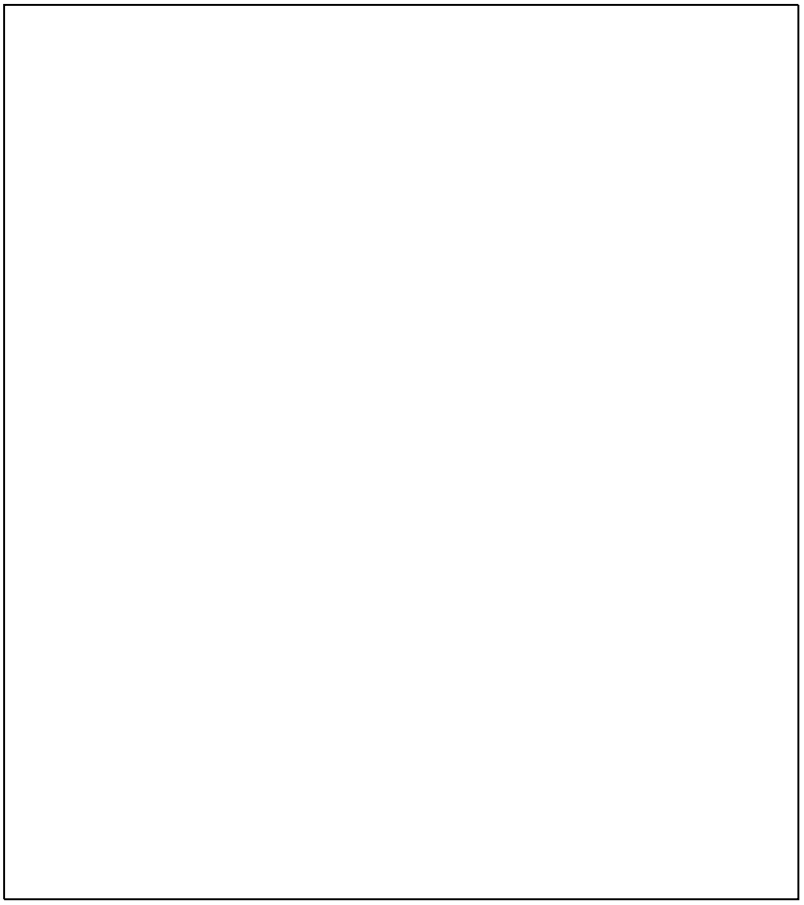
Introduction

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 then 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. To have your command apply to all RNCS sites, use the *–a* option. To include only one specific site, simply name the site. To include two or more specific sites, use the *–i* option. To exclude specific sites, use the *–x* option.

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 then press **Enter**.
- To apply the *ps -ef* command to only one specific RNCS site (called site1), type **siteCmd site1 ps -ef** and then press **Enter**.
- To apply the *ps -ef* command to two specific sites (called site1 and site2), type **siteCmd -i site1:site2 ps -ef** and then 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 then 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 then press **Enter**.

  Note: Note that the *–x* 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 then 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 then press **Enter**.

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

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

2 Type **cd /cdrom/cdrom0** and then 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 then 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 then press **Enter**. The root user home directory becomes the working directory.

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

6 Type **siteCmd <site name> lionnStop** and then 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 then 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 then 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 then press **Enter**.
- To install the package on one specified site (site3, in this example) only, type **siteCmd -sCI site3 <package_name>** and then press **Enter**.
- To install the package on multiple sites (site1 and site2, in this example), type **siteCmd -scIi site1:site2 <package_name>** and then press **Enter**.
- To install the package on all sites *except* site1 and site2, type **siteCmd -asCIx site1:site2 <package_name>** and then press **Enter**.

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

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

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

12 Type **siteCmd <site_name> pkginfo -l <package_name>** and then 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 then 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 then press **Enter** to confirm that lionn processes have restarted.

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

B

RNCS Rollback Procedure

Introduction

This appendix is intended for Cisco 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

Introduction

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 then press **Enter.** The system resets the boot device.
2. Type **shutdown -y -g0 -i6** and then 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 then press **Enter**. Verify that the old software is in place.
5. Type **siteCmd < hostname of server > lionnStart** and then press **Enter**. The system starts the lionn processes.
6. Go to *Attaching Mirrors* (on page 51).

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.

1. Type **cd /cdrom/cdrom0/s0/sai/scripts** and then press **Enter**. The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.
2. Type **./V240_attach_mirrors** and then press **Enter**. A confirmation message appears.
3. Type **y** (for yes) and then press **Enter**. The system runs a script that enables the disk-mirroring function of the Sun Fire V240 server.
4. When the mirrors have been enabled, type **exit** and then press **Enter**. The root user logs out of the Sun Fire V240 server.
5. Type **metastat** and then press **Enter** to verify that submirrors d4xx and d7xx are in an **ok** state.

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

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

March 2012 Printed in USA

Part Number 4012763 Rev B