RNCS Installation and Upgrade Instructions

Please Read This Entire Guide

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 Acknowledgments

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. (1110R)

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 perform 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.

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.

Related Publication

You may find the following publication useful as you install or upgrade the RNCS software:

RCS Network Configuration Guide (part number 4006381, expected publish date: fall 2005)

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 procedures in Chapter 1, **Initial Installation of RNCS Software**.
- If you are upgrading existing RNCS software, follow the procedures in Chapter 2, **Upgrade RNCS Software**.

Document Version

This is the second release of these instructions.

Chapter 1
Initial Installation of RNCS Software

Overview

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 Chapter 2, **Upgrade of RNCS Software**.

In This Chapter

This chapter contains the following topics.

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 Regional Network Control System (RNCS). The Sun Fire V240 server uses Sun's existing SPARC and Solaris architecture. 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 server is designed to easily mount within a standard computer equipment rack.

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).

Log on to the Sun Fire V240 Server

Introduction

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

Logging on to the Sun Fire V240 Server

Follow these instructions 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.

  Result: A HyperTerminal window opens.
- ❑ 3. If necessary, power-on the Sun Fire V240 server.
- ❑ 4. Type **#.** and then press **Enter**.

  Result: 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**, follow these instructions.
    a) Type **admin** and then press **Enter**.
    b) Type the admin password and then press **Enter**.

    Result: The **sc>** prompt appears.
  - If **no** (the **sc>** prompt appeared), go to step 6.

❑ 6. Type **break** and then press **Enter**.

Result: The system interrupts the boot process of the Sun Fire V240 server.

❑ 7. Type **console -f** and then press **Enter**.

Result: A message appears that instructs you to type **#.** to return to the ALOM port.

❑ 8. 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.

❑ 9. After completing step 8, did the **ok** prompt appear, as described?

- If **yes**, go to step 10.
- If **no**, repeat steps 6 through 8.

❑ 10. 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, follow these instructions 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**, follow these instructions.
  a) Type the new admin password and then press **Enter**.
  Result: 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**.
  Result: The network management port of the Sun Fire V240 server becomes functional.
- If **no**, go to step 3.

❑ 3. Type **setsc netsc_dhcp false** and then press **Enter**.

Result: This command prevents the Dynamic Host Configuration Protocol (DHCP) from obtaining the network configuration.

❑ 4. Type **setsc netsc_ipaddr [IP address]** and then press **Enter**.

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.

Result: This command establishes the unique IP address of the network management port.

❑ 5. Type **setsc netsc_ipnetmask [netmask]** and then press **Enter**.

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.

Result: This command establishes the netmask of the network management port.

❑ 6. Type **setsc netsc_ipgateway [IP address of gateway or router]** and then press **Enter**.

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.

Result: This command establishes the IP address of the gateway or router of the network management port.

❑ 7. Type **setsc sc_powerstatememory true** and then press **Enter**.

Result: This command sets the sc_powerstatememory variable to true.

❑ 8. Type **showsc** and then press **Enter**.

Result: The system displays the value of variables associated with the ALOM port.

❑ 9. 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 7.

❑ 10. Type **resetsc** and then press **Enter**.

Result: A confirmation message appears.

❑ 11. Type **y** and then press **Enter**.

Result: After a few messages, the system prompts you to type **#.** to return to the ALOM port.

❑ 12. Type **#.** (Do *not* press **Enter**.).

Result: The **Login** prompt appears.

❑ 13. Did the **Login** prompt appear after you completed step 12?

- If **yes**, follow these instructions.
  a) Type **admin** and then press **Enter**.
  b) Type the admin password and then press **Enter**.
  Result: The **sc>** prompt appears.
- If **no** (the **sc>** prompt appeared), go to step 14.

❑ 14. Type **shownetwork** and then press **Enter**.

Result: The system displays the configuration settings you just established.

❑ 15. Review the settings you established in steps 1 through 14 and choose one of the following options:

- If the settings are correct, go to step 16.
- If a setting is incorrect, re-run the appropriate command and then go to step 16.

❑ 16. Type **console -f** and then press **Enter**.

Result: A message appears that instructs you how to return to the ALOM port, if needed.

❑ 17. 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 the next procedure, **Connect to the Console of the V240 Server**.

  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**, later in this chapter.

Connect to the Console of the V240 Server

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. Follow these instructions to connect to the console of the V240 server.

❑ 1. Follow these instructions to remotely log on to the ALOM port of the RNCS server.

a) Type **telnet [IP address of ALOM port]** and then press **Enter**.

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

Example: telnet 10.201.0.2

Result: A prompt for the user ID appears.

b) Type the admin user ID and then press **Enter**.

Result: A prompt for the password appears.

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

Result: 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**, next in this chapter.

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.

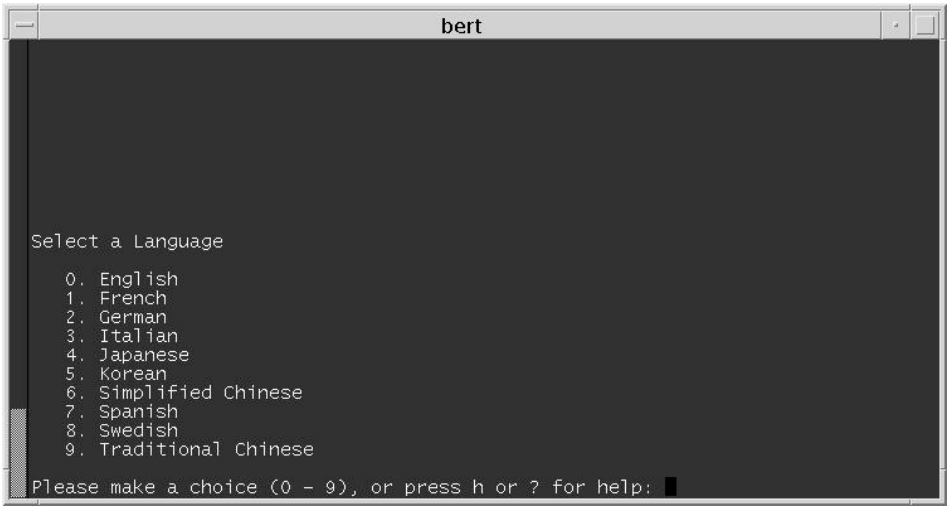
Installing the RNCS Software For the First Time

Now that you have established the correct environment for the RNCS server, you can install the software. Follow these instructions to install the software.

- ❑ 1. If necessary, have the technician who is on-site at the RNCS server 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**.

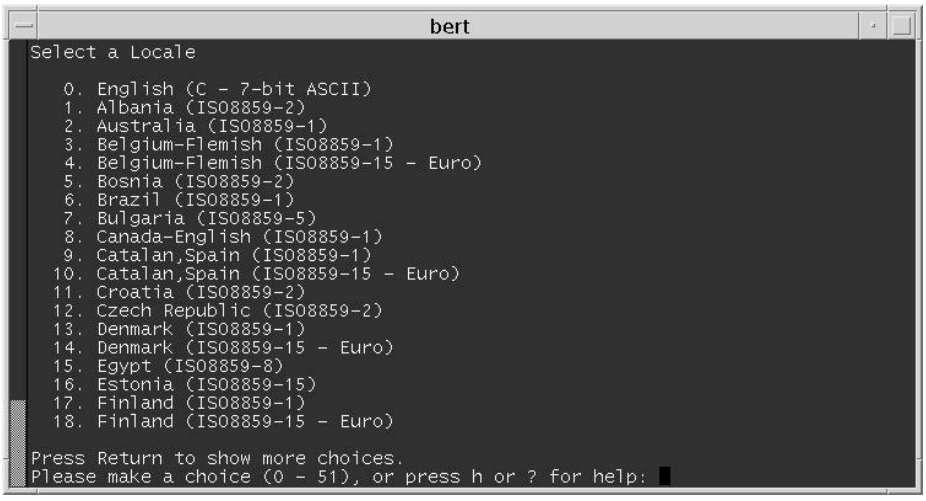
  Results:

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



❑ 3. Type the number that corresponds with **English** and then press **Enter**.

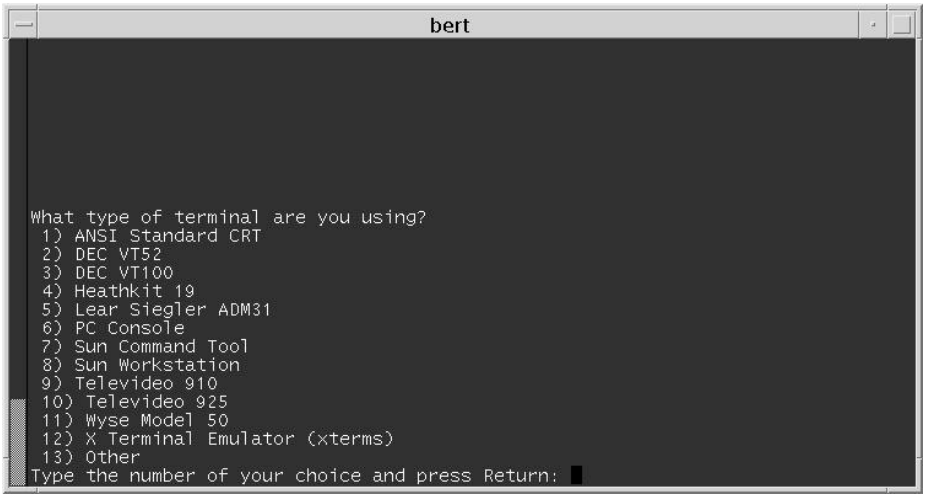
Result: The Select a Locale window appears.



❑ 4. Type the number associated with where the RNCS server is geographically located — probably **USA (en-US. ISO 8859-1)**, and then press **Enter**.

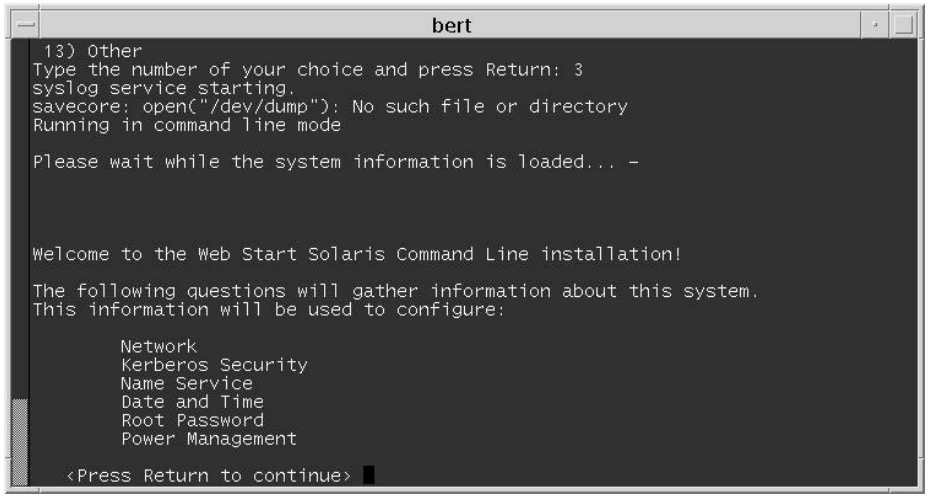
Note: That selection is typically number **49**.

Result: The **What type of terminal are you using** message appears.



❑ 5. Type **3** (for DEC VT100) and then press **Enter**.

Result: A series of messages appears, as well as a prompt to **Press Return to continue**.



❑ 6. Press **Enter**.

Result: The **Is this machine networked** question appears.

❑ 7. Type **y** (for yes) and then press **Enter**.

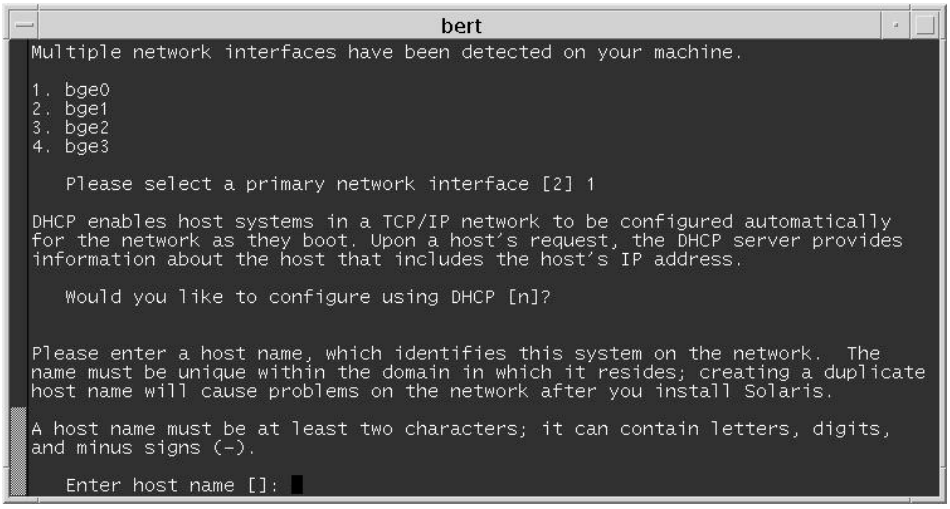
Result: The window updates to acknowledge that multiple networks have been detected and prompts you to select a primary network interface.

❑ 8. Type **1** (for bge0) and then press **Enter**.

Result: The window updates to display a message that describes Dynamic Host Configuration Protocol (DHCP) and then asks if you want to configure your system using DHCP.

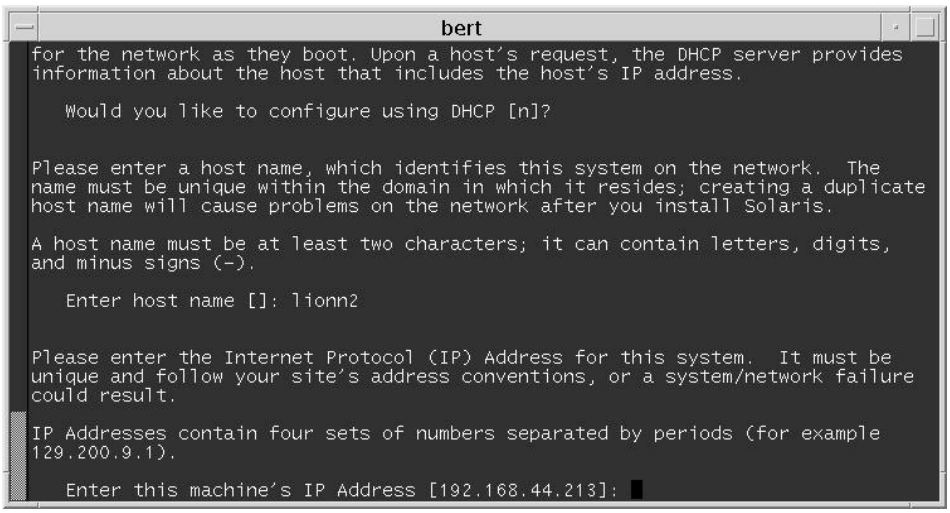
❑ 9. Type **n** (for no) and then press **Enter**.

Result: The window updates to prompt you to enter a host name.



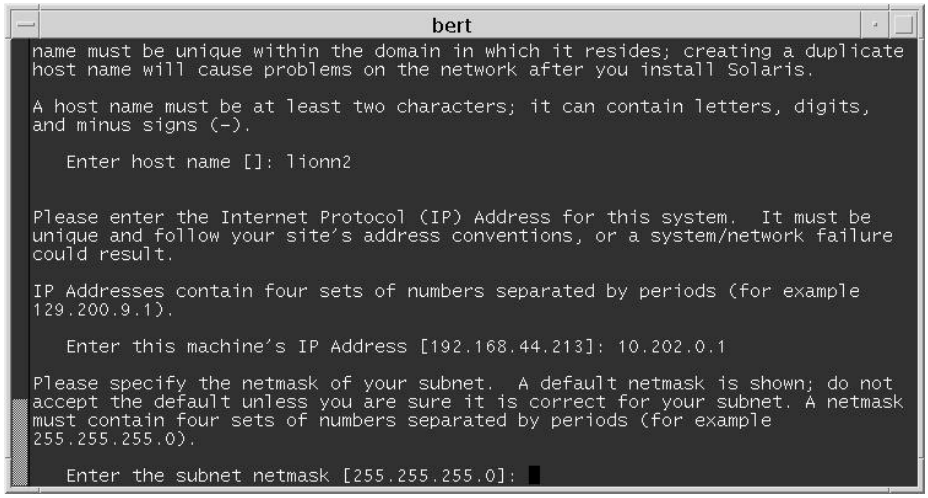
❑ 10. Type the host name of the RNCS server and then press **Enter**.

Result: The window updates to prompt you to enter an IP address.



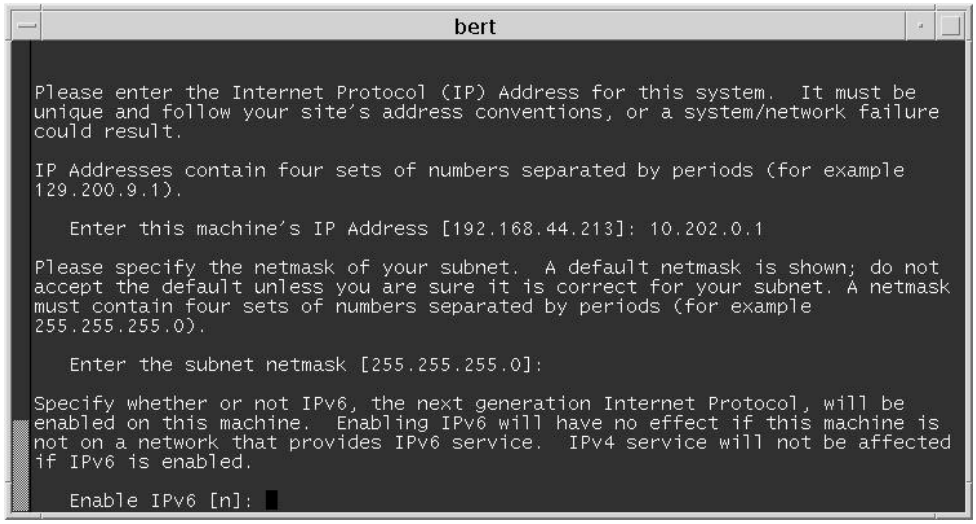
❑ 11. Type the IP address of the RNCS server and then press **Enter**.

Result: The window updates to prompt you to enter the netmask of the RNCS server.



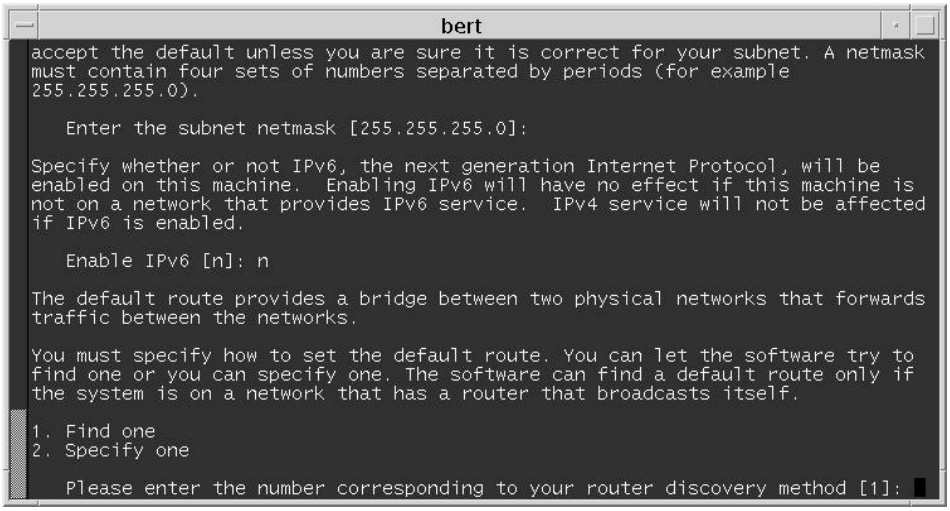
❑ 12. Press **Enter** to accept the default value of 255.255.255.0.

Result: The window updates to prompt you to specify whether you want to enable IPv6, an Internet protocol.



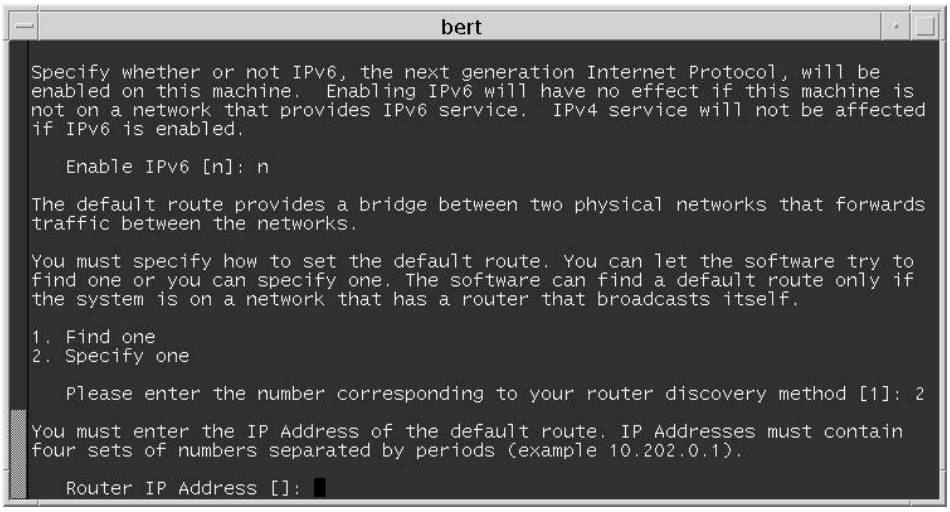
❑ 13. Press **Enter** to accept the default value of no.

Result: The window updates to prompt you to specify how you want to set the default route.



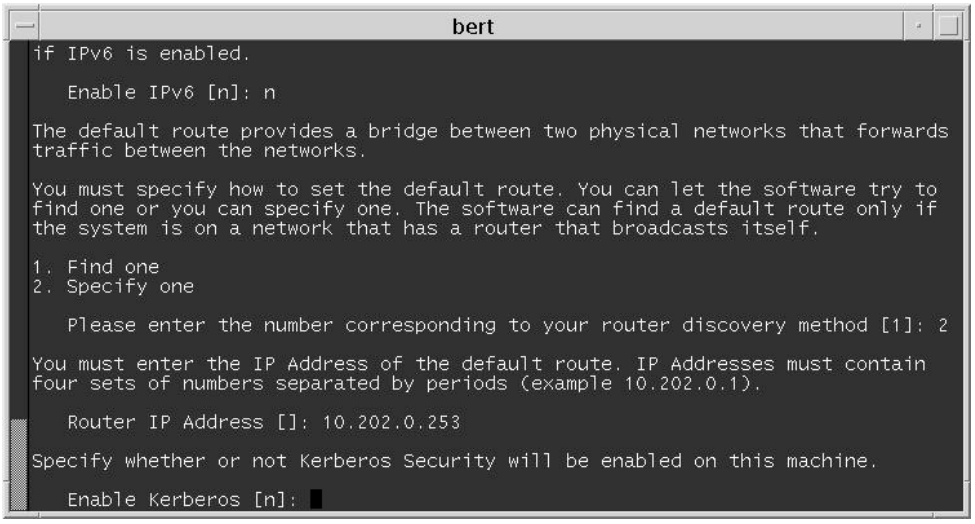
❑ 14. Type **2** (for Specify one) and then press **Enter**.

Result: The window updates to prompt you to enter the IP address of the default route.



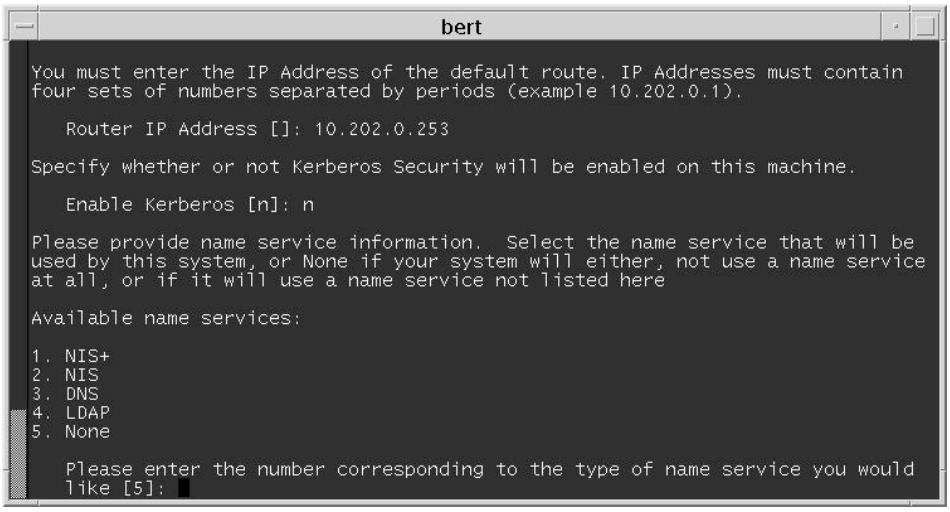
❑ 15. Type the IP address of the default route and then press **Enter**.

Result: The window updates to prompt you to specify whether Kerberos Security is to be enabled on the computer.



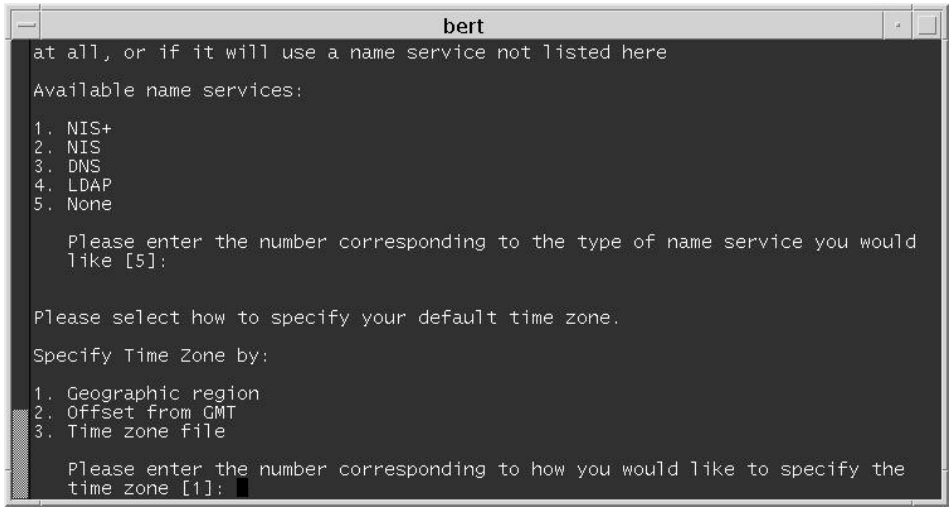
❑ 16. Type **n** (for no) and then press **Enter**.

Result: The window updates to prompt you to select the name service that will be used by the system.



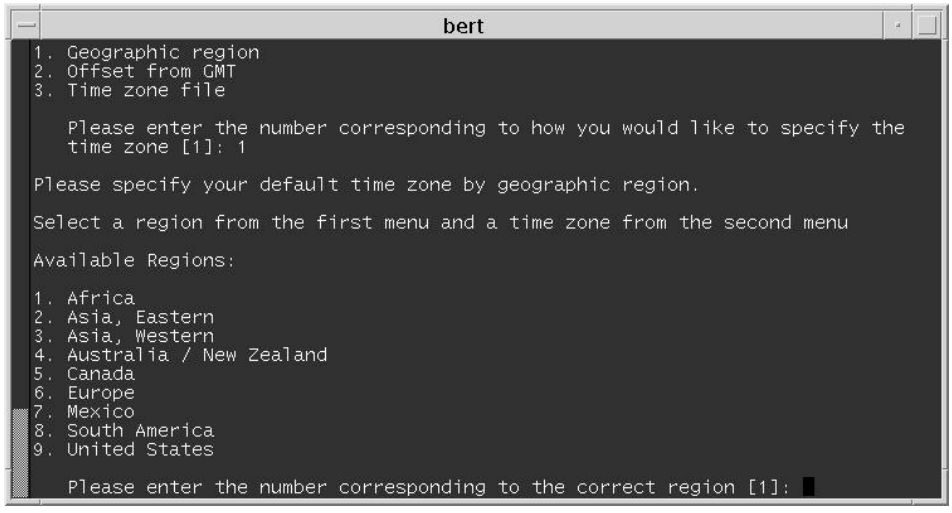
❑ 17. Type **5** (for none) and then press **Enter**.

Result: The window updates to prompt you to select your default time zone.



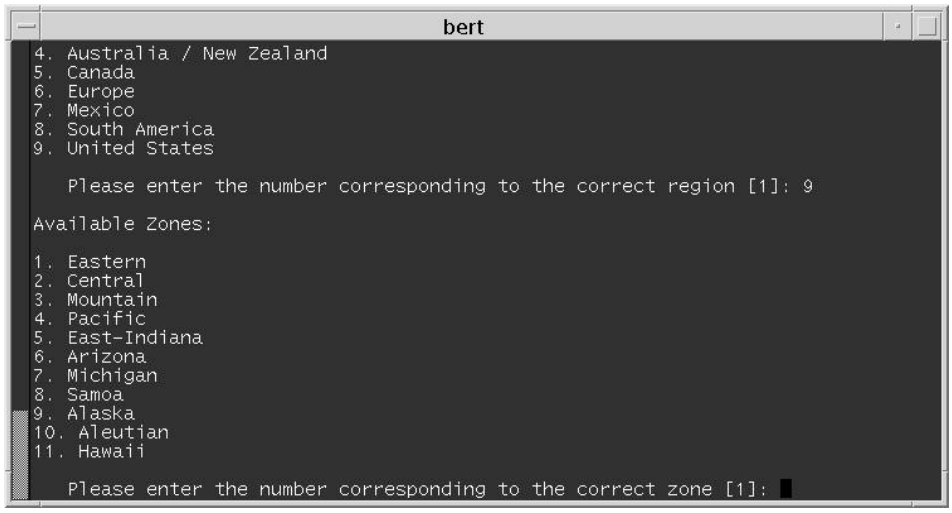
❑ 18. Type **1** (for Geographic region) and then press **Enter**.

Result: The window updates to prompt you to select a geographic region.



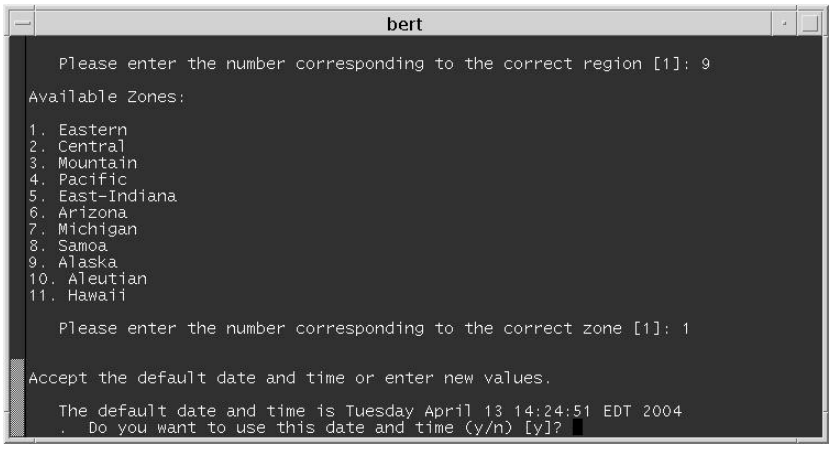
❑ 19. Type **9** (for United States) and then press **Enter**.

Result: The window updates to prompt you to select a time zone.



❑ 20. Type the number that corresponds to the time zone in which the RNCS server is located and then press **Enter**.

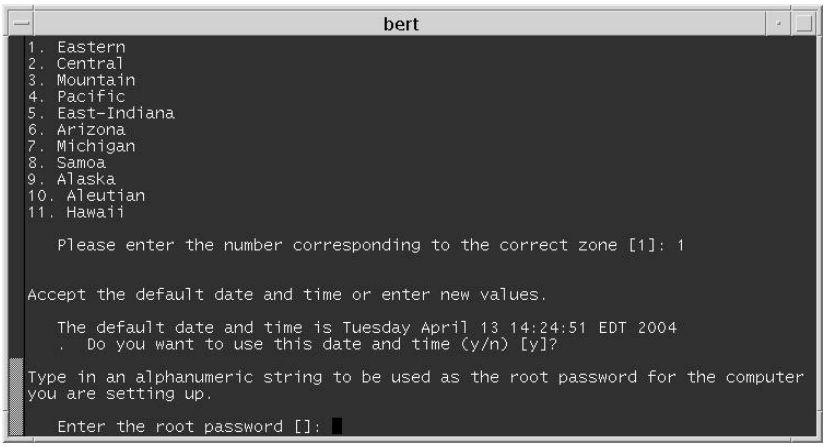
Result: The window updates by displaying the current date and time and asks that you confirm the display.



❑ 21. Are the current date and time accurately displayed?

- If **yes**, type **y** (for yes) and then press **Enter**.

  Result: The window updates to prompt you to enter the root password.



- If **no**, follow these instructions.

  a) Type **n** (for no) and then press **Enter**.

  Result: The window returns to the display shown in step 18.

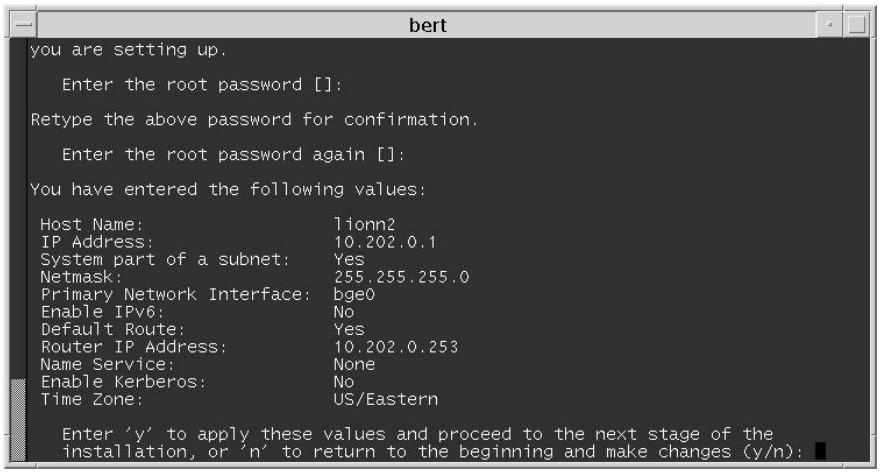
  b) Repeat these instructions from step 18.

❑ 22. Type the root password and then press **Enter**.

Result: The window updates by prompting you to re-enter the root password.

❑ 23. Retype the root password and then press **Enter**.

Result: The window updates to display a list of the configuration parameters you have just set and asks that you confirm their accuracy.



❑ 24. Are the parameters correct?

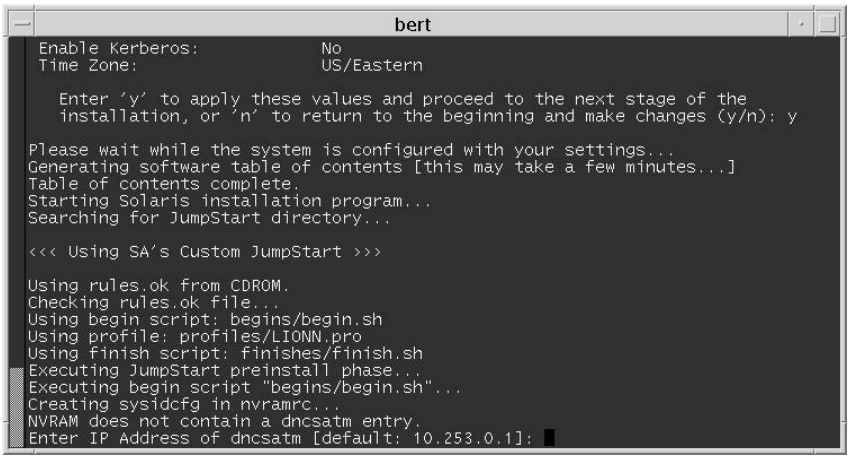
- If **yes**, type **y** (for yes) and then press **Enter**.

  Results:

  – The system saves the parameters.

  – The RNCS software begins to install.

  – The system prompts you for the IP address of dncsatm.



- If **no**, type **n** (for no) and then press **Enter**.

  Result: The system provides you with another opportunity to supply configuration parameters beginning with step 2.

❑ 25. Type the IP address of dncsatm and then press **Enter**.

Result: The RNCS software continues to install.

Note: The console login prompt appears when the installation process has ended.

❑ 26. Go to **Attaching Mirrors**, next in this section.

Attaching Mirrors

In this procedure, you will log in to the Sun Fire V240 server and enable the disk-mirroring function of the server. Follow this procedure to log on to the Sun Fire V240 server and then to attach the server's mirrors.

❑ 1. Log on to the Sun Fire V240 server as **root** user.

❑ 2. Type **cd /cdrom/cdrom0/s0/sai/scripts** and then press **Enter**.

Result: The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.

- ❑ 3. Type **./V240_attach_mirrors** and then press **Enter**.

  Result: A confirmation message appears.

- ❑ 4. Type **y** (for yes) and then press **Enter**.

  Result: 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**.

  Result: 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.

Start the RNCS

Starting the RNCS

After installing the RNCS software, you are now ready to start the server. Follow these instructions to start the server.

- ❑ 1. Log in to the Sun Fire V240 server as **dncs** user.
- ❑ 2. Type **lionnStart** and then press **Enter**.

Chapter 2
Upgrade of RNCS Software

Overview

Introduction

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

In This Chapter

This chapter contains the following topics.

Upgrade the RNCS Software

Introduction

The Sun Fire V240 server is to be upgraded 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**

Upgrading the RNCS Software

Follow these instructions to upgrade the RNCS software.

❑ 1. Follow these instructions 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**.

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

Example: telnet 10.201.0.2

Result: A prompt for the user ID appears.

b) Type the admin user ID and then press **Enter**.

Result: A prompt for the password appears.

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

Result: 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**.

  Result: 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. Log on to the Sun Fire V240 server as **root** user.

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

- ❑ 6. Have the technician who is on-site at the RNCS server insert the DVD labeled similarly to **RNCS Install DVD**, into the DVD drive of the RNCS server.

- ❑ 7. 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**.

- ❑ 8. Type **cd /dvs/lionn/bin** and then press **Enter**.

  Result: The /dvs/lionn/bin directory becomes the working directory.

- ❑ 9. Type **snmx lionnAppExec.s** and then press **Enter**.

  Result: The Lionn Control menu of the Lionn Control window appears.

- ❑ 10. Type **2** (for Startup/Shutdown Single Element Group) and then press **Enter**.

  Result: The system displays all lionn processes.

  Note: The system updates the display periodically or you can press **Enter** to force an update.

❑ 11. Does the **Curr Stt** (Current State) field of the Lionn Control window indicate that all Lionn processes are **running**? (All processes should be running.)

- If **yes**, follow the on-screen instructions to close the Lionn Control window.
- If **no**, troubleshoot to the best of your abilities any processes that are not running.

Note: Contact 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**.

Result: The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.

❑ 14. Type **./V240_detach_mirrors** and then press **Enter**.

Result: 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**.

Result: A confirmation message appears.

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

Results:

- The Live Upgrade of the RNCS server begins.
- The message **Do you want to back up the key files** 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, follow these instructions.
  a) Type **y** and then press **Enter**.
  b) 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**.

Result: 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**.

Result: 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 **siteControl <host name of LIONN>** and then press **Enter**.

Example: siteControl lionn1

Result: A menu displays to stop the DNCS processes.

❑ 26. Type **1** (Startup/Shutdown All Element Groups) and then press **Enter**.

❑ 27. To stop the processes, type **1** and then press **Enter**.

❑ 28. To confirm the shutdown process, type **y** and then press **Enter**.

❑ 29. To exit the menu, type **x** and then press **Enter**.

❑ 30. From the xterm window that you used *prior* to step 19, type **shutdown -g0 -y -i6** and then press **Enter**.

Important: Note these important points:

- Do not use an xterm window on the DNCS.
- Do not use the *reboot* or *halt* command to reboot the server.

Result: The system reboots with the new software in place.

❑ 31. Log on to the Sun Fire V240 server as **root** user.

❑ 32. Type **lustatus** and then press **Enter**.

Result: 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       no          no              -
LIONN_V1.0.0.x            yes       yes         yes             -
```

Note: The example shows that the new RNCS version is active.

❑ 33. Type **/dvs/lionn/bin/fixSiteConfigs** and then press **Enter**.

Result: The system makes necessary modifications to the headend configuration file in the /tftpboot directory.

❑ 34. From an xterm window on the DNCS, type **siteControl <host name of LIONN>** and then press **Enter**.

Example: siteControl lionn1

Result: A menu displays to start the RNCS processes.

❑ 35. Type **1** (Startup/Shutdown All Element Groups) and then press **Enter**.

❑ 36. To start the processes, type **2** and then press **Enter**.

❑ 37. To confirm the startup process, type **y** and then press **Enter**.

❑ 38. To exit the menu, type **x** and then press **Enter**.

❑ 39. Is the system stable after upgrading the RNCS software?

- If **yes**, go to step 40.
- If **no**, go to Appendix B, **RNCS Rollback Procedure**, to restore your system to its pre-upgrade condition.

  Important: Call Cisco Services before deciding to roll back.

❑ 40. Go to **Attaching Mirrors**, next in this section.

Important: Once you attach the mirrors, then you are committed to the upgrade. Be certain that your system is stable before attaching the mirrors.

Attaching Mirrors

After upgrading the RNCS software, follow this procedure to attach the server's mirrors.

Important: 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.

- ❑ 1. Type **cd /cdrom/cdrom0/s0/sai/scripts** and then press **Enter**.

  Result: The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.

- ❑ 2. Type **./V240_attach_mirrors** and then press **Enter**.

  Result: A confirmation message appears.

- ❑ 3. Type **y** (for yes) and then press **Enter**.

  Result: 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**.

  Result: 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.

Chapter 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.

Appendix A
The siteCmd Program

Overview

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

This appendix contains the following topic.

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

Repeat this procedure for each RNCS site that your DNCS will manage.

- ❑ 1. If necessary, open an xterm window on the DNCS.
- ❑ 2. Follow these instructions to log onto the xterm window as **root** user.
  a) Type **su -** and then press **Enter**.

  Result: The **password** prompt appears.
  b) Type the root password and then press **Enter**.
- ❑ 3. Type **siteCmd -S** and then press **Enter**.

  Result: 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**.

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

Result: 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.

❑ 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**, contact 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.

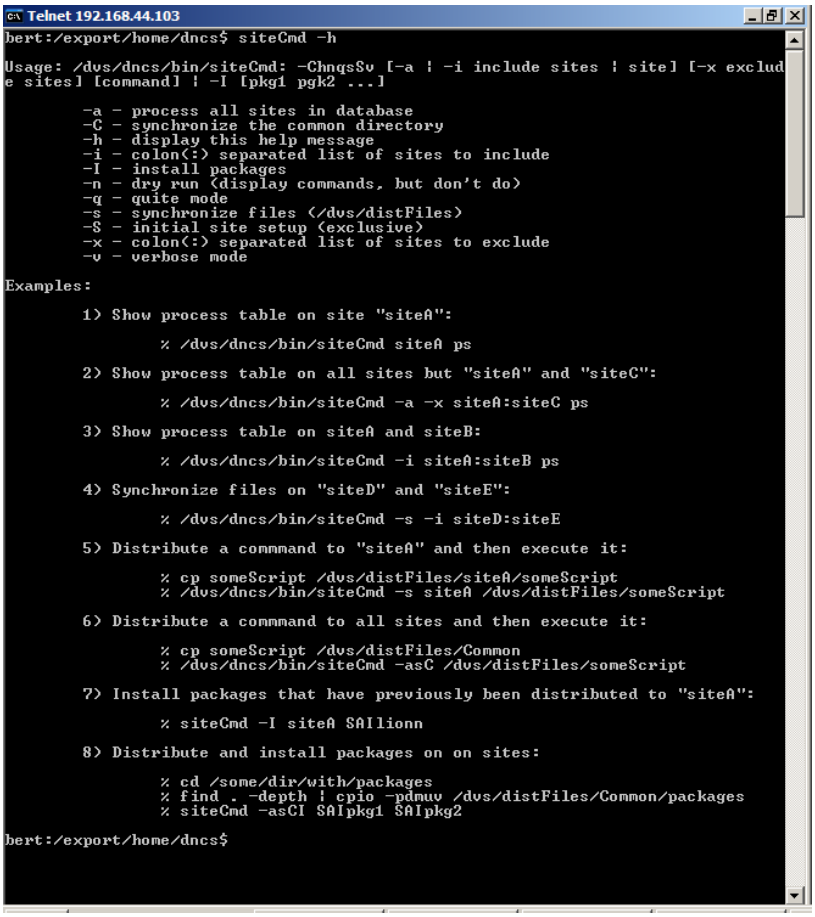
Displaying the siteCmd Help Window

Follow these directions 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**.

Result: The system displays the help window for the siteCmd program.



❑ 3. Go to **Options Available With the siteCmd Program**, next in this section.

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 form 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 will demonstrate how to use the siteCmd program to install a package on the RNCS.

Note: This example assumes that a CD containing the package to be installed (SAIlionn) 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**.

  Result: The **password** prompt appears.

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

- ❑ 2. Type **cd /cdrom/cdrom0** and then press **Enter**.

  Result: The /cdrom/cdrom0 directory of the DNCS becomes the working directory.

- ❑ 3. Type **find . –name SAIlionn | cpio -pdmuv /dvs/distFiles/Common/packages** and then press **Enter**.

  Result: The system copies the files on the CD into the common directory of the DNCS.

- ❑ 4. Type **cd /** and then press **Enter**.

  Result: The home directory becomes the working directory.

- ❑ 5. Type **eject cdrom** and then press **Enter**.

  Result: The system ejects the CD.

- ❑ 6. Choose one of the following options to install the SAIlionn package on the RNCS:

  - To install the package on *all* sites, type **siteCmd -asCi SAIlionn** and then press **Enter**.
  - To install the package on one specified site (site3, in this example) only, type **siteCmd -sCI site3 SAIlionn** and then press **Enter**.
  - To install the package on all sites *except* site1 and site2, type **siteCmd -asCIx site1:site2 SAIlionn** and then press **Enter**.

- ❑ 7. Type **exit** and then press **Enter** to log out the root user.

Appendix B
RNCS Rollback Procedure

Overview

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 Chapter

This chapter contains the following topic.

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

Follow these instructions 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 **lustatus** and then press **Enter**.

Result: 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        no       no               -
LIONN_V1.0.0.x            yes        yes      yes              -
```

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 installed and is now active.

- ❑ 2. Type l**uactivate 1.0.0.x** and then press **Enter**.

  Note: Substitute the current version of the SAIlionn package for 1.0.0.x.

  Result: The system activates the version of RNCS software that was installed on your system prior to the upgrade 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 <1.0.0.x> successful.

- ☐ 3. Type **lustatus** and then press **Enter**.

  Result: 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	no	yes	-
LIONN_V1.0.0.x	yes	yes	no	-

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

- ☐ 4. Type **shutdown -g0 -y -i6** and then press **Enter**.

  Important: Do not use the *reboot* or *halt* command to reboot the server.

  Results: The system reboots and activates the old RNCS software.

- ☐ 5. Type **lustatus** and then press **Enter**.

  Result: 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	-

  Note: The example shows that the new RNCS version is active.

- ☐ 6. Go to **Attaching Mirrors**, next in this appendix.

Attaching Mirrors

After rolling back the RNCS software, follow this procedure 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**.

  Result: The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.

- ❑ 2. Type **./V240_attach_mirrors** and then press **Enter**.

  Result: A confirmation message appears.

- ❑ 3. Type **y** (for yes) and then press **Enter**.

  Result: 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**.

  Result: 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

February 2013 Printed in USA

Part Number 78-4003191-01 Rev B