RNCS Installation and Upgrade Instructions

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. To view a list of cisco trademarks, go to this URL: **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 the IPTV Service Delivery System (ISDS). The RNCS is a needed component in a Regional Control System (RCS) that uses the ISDS 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 ISDS that has a remote connection to the RNCS.

Appendix A of this guide, ***The siteCmd Program*** (on page 67), contains instructions and examples for running various commands that are useful in managing a remote headend.

Audience

This guide provides field service engineers with instructions for installing or upgrading the RNCS component of an existing ISDS.

Read Me

Please read this entire guide before beginning the upgrade. If you are uncomfortable with any of the procedures, contact Cisco® Services at 1-800-283-2636 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 ISDS system expertise.
  - The ability to identify keyfiles that are unique to the site being upgraded.
  - The ability to add and remove user accounts.

Supported Hardware Platforms

Platform	Hard Drives	Memory
Sun Fire V245	2 X 73 GB	2 GB minimum
Netra T5220	2 X 146 GB	4 GB minimum

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 45).

Document Version

This is the third formal release of this document. In addition to minor text and graphic changes, the following table provides the technical changes to this document.

Description	See Topic
Added procedures to back up and restore SNMP configuration data to Chapter 2.	■ See ***Back Up SNMP Configuration Data*** (on page 46). ■ See ***Restore the SNMP Configuration Data*** (on page 60).

1

Initial Installation of RNCS Software

Introduction

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 45).

In This Chapter

Introducing the ALOM and ILOM Ports

The Sun Advanced Lights Out Manager (ALOM) and Integrated Lights Out Manager (ILOM) ports are system controllers that allow the servers to be managed and administered from a remote location. Through the ALOM and ILOM ports, you can monitor and control the servers through a serial connection (using the SERIAL MGT port) or an Ethernet connection (using the NET MGT port).

Logging on to the RNCS Servers

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

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

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

   Note: The HyperTerminal application allows one computer to communicate with another computer.
3. If necessary, power on the RNCS server.
4. Choose one of the following options:
   - If you are logging on to the Sun Fire V245 server, go to ***Configuring the ALOM Port of the Sun Fire V245 Server*** (on page 3).
   - If you are logging on to the Sun Netra T5220 server, ***Configuring the ILOM Port of the Sun Netra T5220 Server*** (on page 6).

Configuring the ALOM Port of the Sun Fire V245 Server

1. Type **#.** and then press **Enter**. One of the following results occurs:
   - The **Login** prompt appears.
   - The **sc>** prompt appears.
2. Did the **Login** prompt appear after you completed step 1?
   - If **yes**, go to step 3.
   - If **no** (the **sc>** prompt appeared), go to step 4.
3. If the **Login** prompt appeared after completing step 1, complete the following steps.
   a. Type **admin** and then press **Enter**.
   b. Type the password (**changeme**) and then press **Enter**. The **sc>** prompt appears.
4. Type **break** and then press **Enter**. The system interrupts the boot process of the RNCS server.

5 Type **console -f** and then press **Enter**. A message appears that instructs you to type **#.** to return to the ALOM port.

6 Press **Enter** again.

Results:

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

7 After completing step 6, did the **ok** prompt appear, as described?

- If **yes**, go to step 8.
- If **no**, repeat steps 4 through 6.

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

Results:

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

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

Result: One of the following results occurs:

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

10 Did the system display the "setting password" message described in the first bullet of step 9?

- If **yes**, go to step 11.
- If **no**, go to step 12.

11 Complete the following steps if the "setting password" message, described in the first bullet of step 9, appeared after completing step 9.

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

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

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

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

Notes:

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

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

Notes:

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

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

Notes:

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

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

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

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

- If **yes**, type **q** to exit from the showsc display.
- If **no**, type **q** to exit from the showsc display. Repeat this procedure from step 16.

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

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

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

22 Did the **Login** prompt appear after you completed step 21?

- If **yes**, go to step 23.
- If **no** (the **sc>** prompt appeared), go to step 24.

23 If the **Login** prompt appeared after you completed step 21, follow these instructions.

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

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

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

25 Review the settings you established in steps 9 through 24 and choose one of the following options:

- If the settings are correct, go to step 26.
- If a setting is incorrect, re-run the appropriate command and then go to step 26.

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

27 Press **Enter** again.

Results:

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

28 Go to ***Choices Regarding Installation*** (on page 8).

Configuring the ILOM Port of the Sun Netra T5220 Server

1 Type **#.** and then press **Enter**. One of the following results occurs:

- The **Login** prompt appears.
- The **->** prompt appears.

2 Did the **Login** prompt appear after you completed step 1?

- If **yes**, go to step 3.
- If **no** (the **->** prompt appeared), go to step 4.

3 From the login prompt on the terminal, log on using **root** as the username and **changeme** as the password.

4 If you want to change the ILOM root password, type **set /SP/users/root password** and then press **Enter**.

Note: Enter and re-enter the new password when prompted.

5 Complete the following steps to configure the serial management port of the server.

a To disable DHCP for the port, type **set /SP/network pendingipdiscovery=static** and then press **Enter**.

b To set the IP address of the port, type **set /SP/network pendingipaddress=<xxx.xxx.xxx>** and then press **Enter**.

Note: Replace <xxx.xxx.xxx> with the IP address for the serial management port.

c To set the Default Gateway for the port, type **set /SP/network pendingipgateway=<xxx.xxx.xxx>** and then press **Enter**.

Note: Replace <xxx.xxx.xxx> with the IP address for the Default Gateway.

d To set the Network Mask for the port, type
set /SP/network pendingipnetmask=<xxx.xxx.xxx.x> and then press **Enter**.

Note: Replace <xxx.xxx.xxx.x> with the Network Mask for the serial management port.

e To configure the port to use SSH, type
set /SP/services/ssh state=enabled and then press **Enter**.

f To enable the port, type
set /SP/network state=enabled and then press **Enter**.

g To display the current port settings, type
show /SP/network and then press **Enter**.

h If any of the settings are not correct, retype the necessary command to set the parameter to the proper value, and then repeat step 5g.

i To commit and implement the new port settings, type
set /SP/network commitpending=true and then press **Enter**.

j To display the current port settings, and to verify that the settings are implemented, type
show /SP/network and then press **Enter**.

Example: Output should look similar to the following example:

commitpending = (Cannot show property)
dhcp_server_ip = none
ipaddress = 10.90.177.23
ipdiscovery = static
ipgateway = 10.90.177.1
ipnetmask = 255.255.255.0
macaddress = 00:14:4F:EB:4C:E1
pendingipaddress = 10.90.177.23
pendingipdiscovery = static
pendingipgateway = 10.90.177.1
pendingipnetmask = 255.255.255.0
state = enabled

k To enable the HOST_LAST_POWER_STATE parameter of the port, type
set /SP/policy HOST_LAST_POWER_STATE=enabled and then press **Enter**.

l Type **show /SP/policy HOST_LAST_POWER_STATE** and then press **Enter** to confirm that the HOST_LAST_POWER_STATE parameter was set correctly.

Note: The system should display **HOST_LAST_POWER_STATE = enabled**.

6 Connect an Ethernet cable from the network management port on the back of the Sun Netra T5220 server to the appropriate network hub, switch, or router.

7 Verify that the port is functional by opening an SSH session to the IP address of the port. The ILOM login prompt should appear.

8 Log on using **root** as the username and the appropriate password.

9 Type **exit** and then press **Enter** to log out from the serial management port.

Choices Regarding Installation

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

- Connect to the just-configured ALOM/ILOM port by following the instructions in the next procedure, ***Connecting to the Console of the RNCS Server*** (on page 9).

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

- Use the laptop to install the RNCS software by following the instructions in ***Install the RNCS Software*** (on page 11).

Connecting to the Console of the RNCS Server

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

1 Choose one of the following options:

- If you are connecting to the ALOM port of the Sun Fire V445 server, go to step 2.
- If you are connecting to the ILOM port of the Netra T5220 server, go to step 3.

2 Complete the following steps to remotely log on to the ALOM port of the Sun Fire V445 server.

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

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

Example: telnet 10.201.0.2

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

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

d Go to step 4.

3 Complete the following steps to remotely log on to the ILOM port of the Netra T5220 server.

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

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

Example: ssh 10.201.0.2

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

c Type the password for the admin user and press **Enter**. The **->** prompt appears as the system establishes a secure shell connection between the ISDS and the ILOM port.

d Go to step 5.

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

Results:

- A message appears that instructs the user on how to return to the ALOM port.
- Control of the server is returned to the console, rather than the ALOM port.
- The **ok** prompt appears
- Go to ***Install the RNCS Software*** (on page 11).

5 Type **start /SP/console** and then press **Enter**.

Results:

- A message appears that instructs the user on how to return to the ILOM port.
- Control of the server is returned to the console, rather than the ILOM port.
- The **ok** prompt appears.
- Go to ***Install the RNCS Software*** (on page 11).

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.

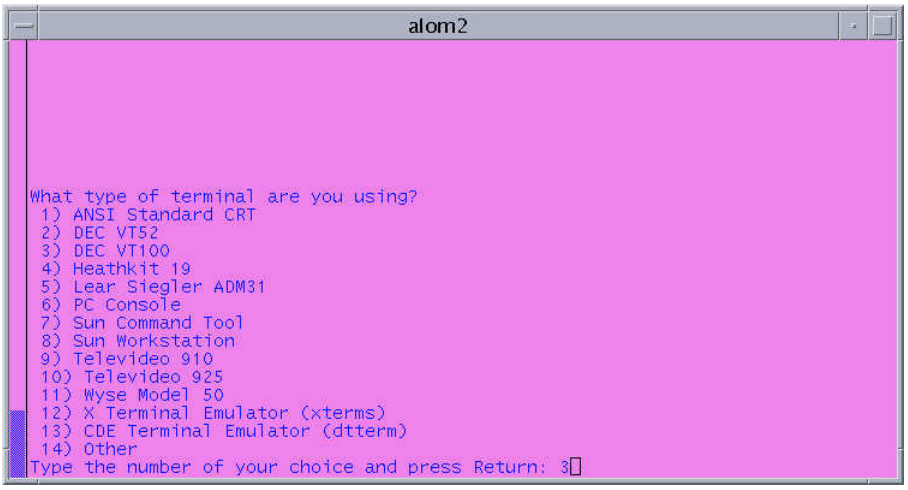
1. If necessary, ask the on-site technician at the RNCS server to insert the DVD, labeled similarly to **RNCS Install DVD,** into the DVD drive of the RNCS server.
2. At the ok prompt, type **boot cdrom – install** and then press **Enter**.

   Results:

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

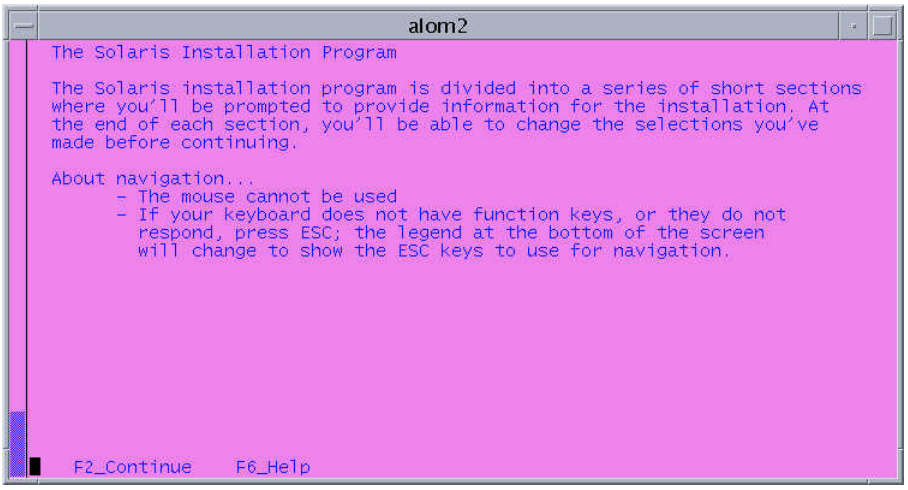
3 Type a number that corresponds to your desired language and then press **Enter**.

Result: 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**.

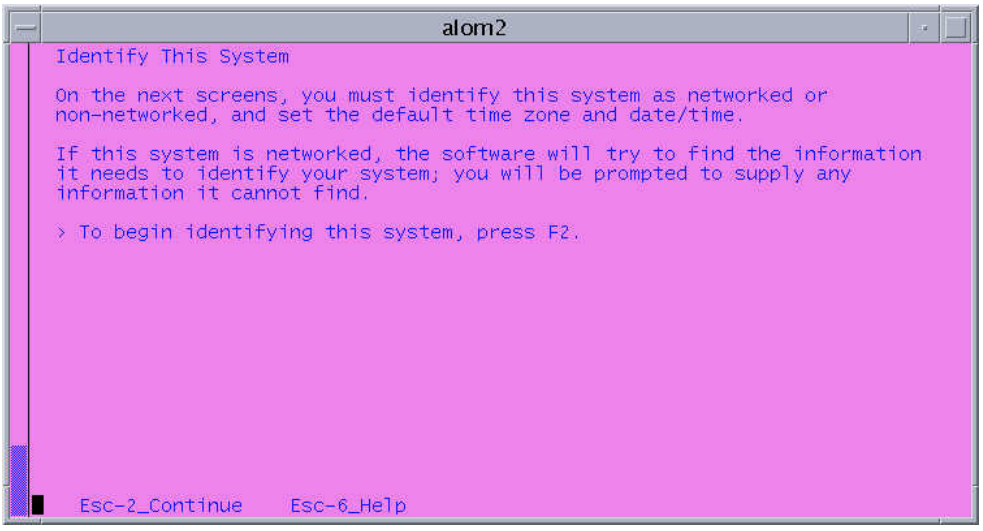
Result: The window updates to display a brief message about the installation process.



5 Read through the message displayed in step 4 and then press the **F2** key.

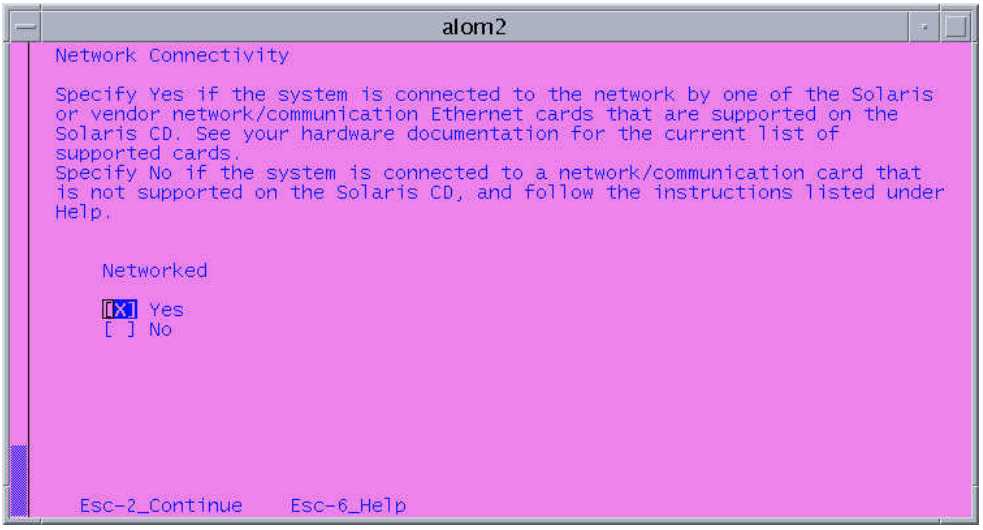
Note: On some systems, the window may also prompt you to press the **Esc** and **2** keys simultaneously in order to continue. Either method (**Esc** and **2** keys, or **F2** key) will work.

Result: The window updates to display another brief informational message.



6 Press the **Esc** and **2** keys simultaneously.

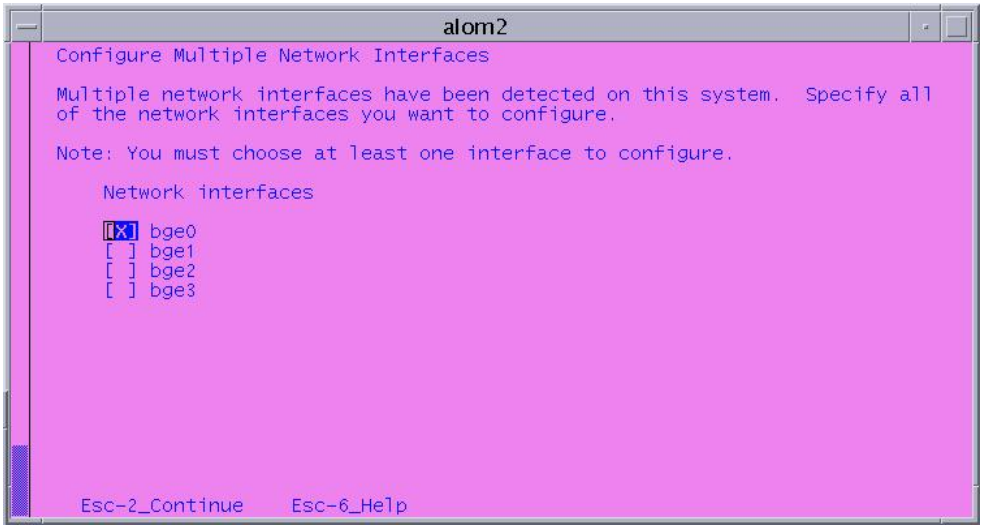
Result: The window updates to ask whether the system is connected to the network through a Solaris-compatible Ethernet card.



7 Select **Yes** and then press the **Esc** and **2** keys simultaneously.

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

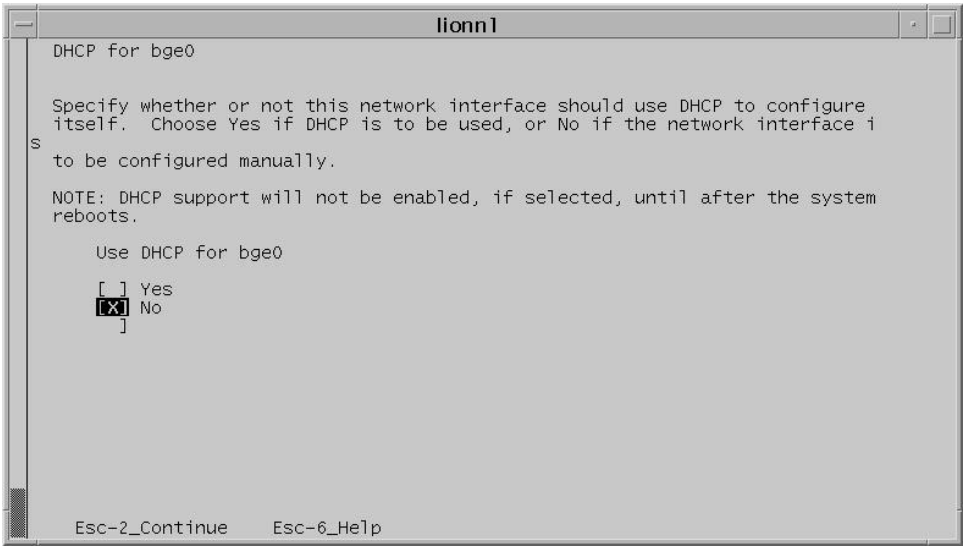
Result: The window updates to prompt you to select the network interface that you want to configure.



8 Select **bge0** and then press the **Esc** and **2** keys simultaneously.

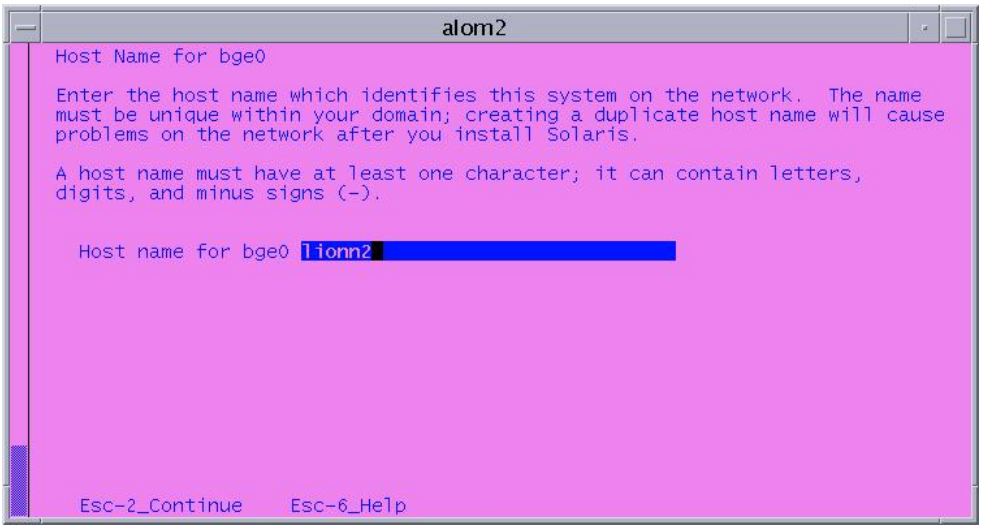
Note: If your site uses the Netra T5220 server, select the e1000g0 interface, instead.

Result: The window updates to prompt you to specify whether the Dynamic Host Configuration Protocol (DHCP) is to be used to configure the bge0 interface.



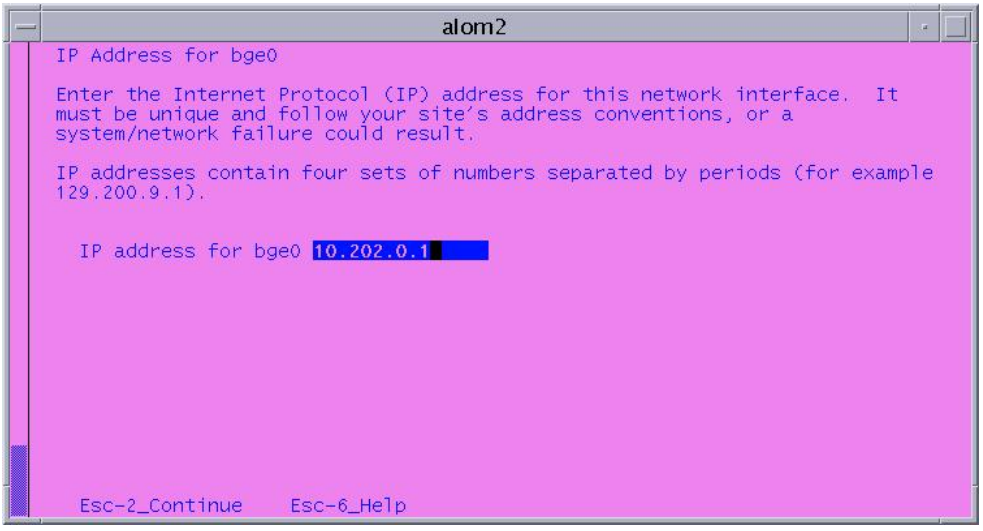
9 Select **No** and then press the **Esc** and **2** keys simultaneously.

Result: The window updates to prompt you to enter the host name that identifies this system on the network.



10 Type the host name (example, lionn2) and then press the **Esc** and **2** keys simultaneously.

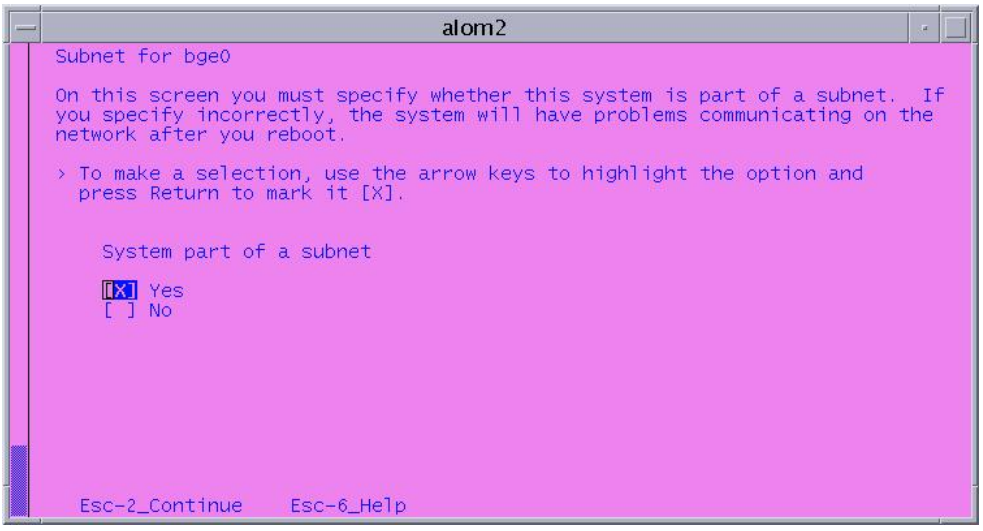
Result: The window updates to prompt you to enter the IP address for the bge0 interface.



11 Type the IP address and then press the **Esc** and **2** keys simultaneously.

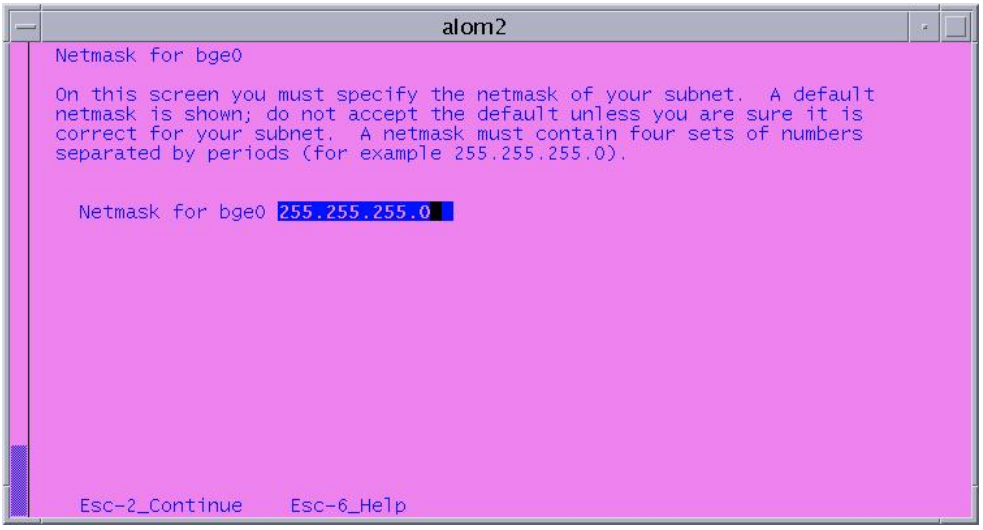
Note: If your site uses the Netra T5220 server, enter the IP address for the e1000g0 interface.

Result: The window updates to prompt you to specify whether your system is part of a subnet.



12 Select **Yes** and then press the **Esc** and **2** keys simultaneously.

Result: The window updates to prompt you to specify the netmask for the bge0 interface.



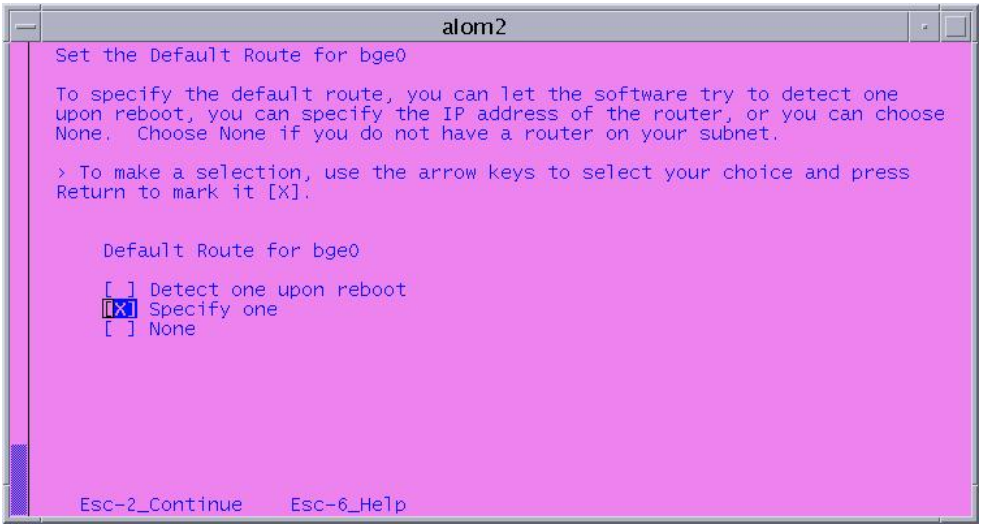
13 Type the appropriate netmask (for example, 255.255.255.0) and then press the **Esc** and **2** keys simultaneously.

Note: If your site uses the Netra T5220 server, specify the netmask of the e1000g0 interface.

Result: The window updates to prompt you to specify whether you want to enable the IPv6 Internet protocol on the interface.

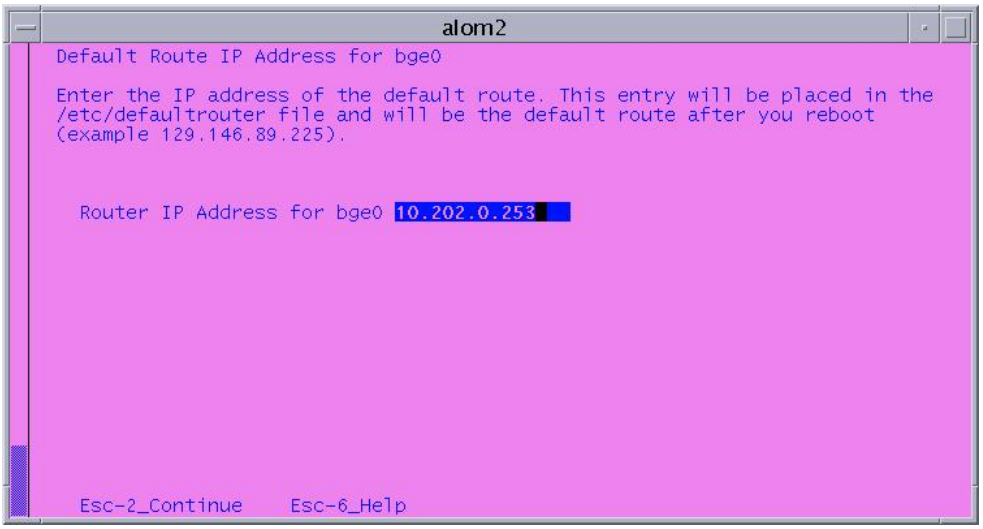
14 Select **No** and then press the **Esc** and **2** keys simultaneously.

Result: The window updates and prompts you to set the default route for the interface.



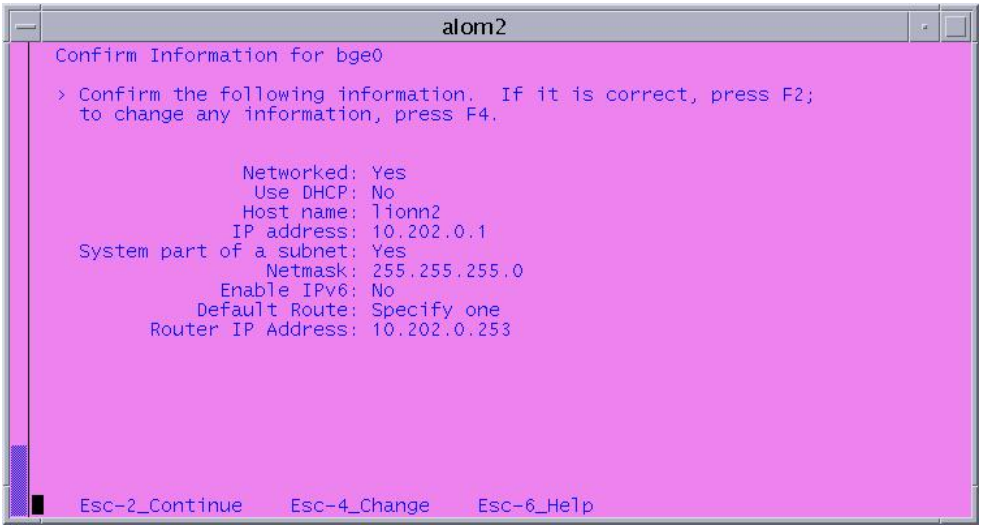
15 Select **Specify one** and then press the **Esc** and **2** keys simultaneously.

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



16 Type the Router IP Address for the interface and then press the **Esc** and **2** keys simultaneously.

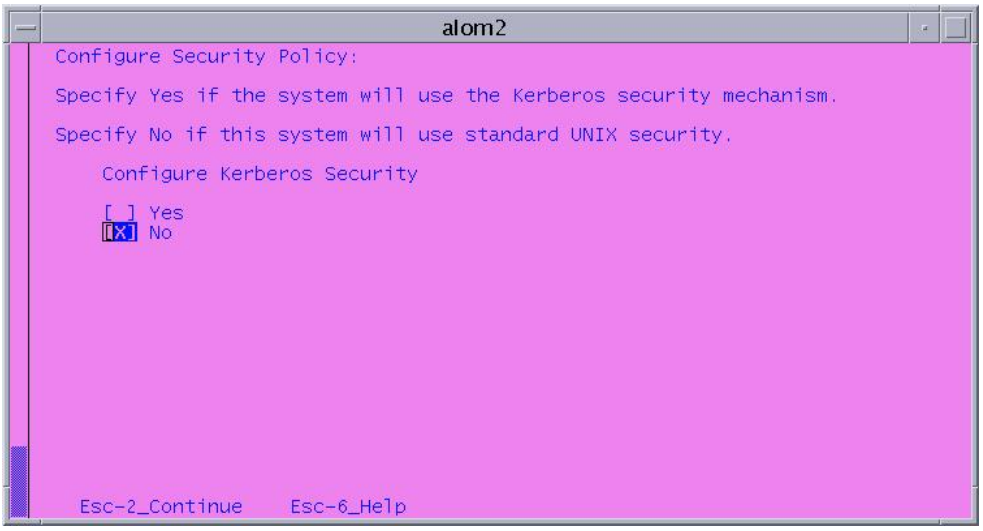
Result: The window updates and asks that you confirm the network configuration.



17 Review the configuration and then press the **Esc** and **2** keys simultaneously.

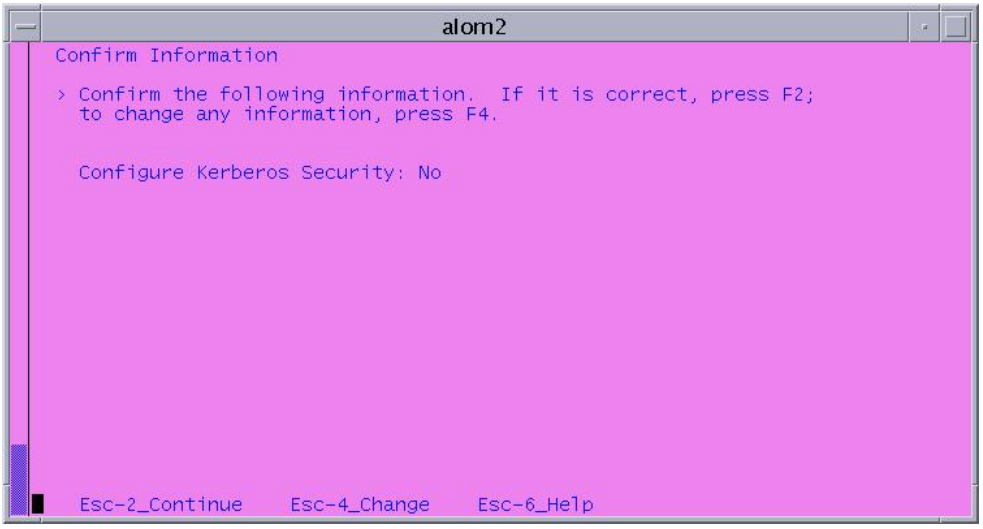
Result: The window updates to prompt you to specify whether your system will use the Kerberos security.

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



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

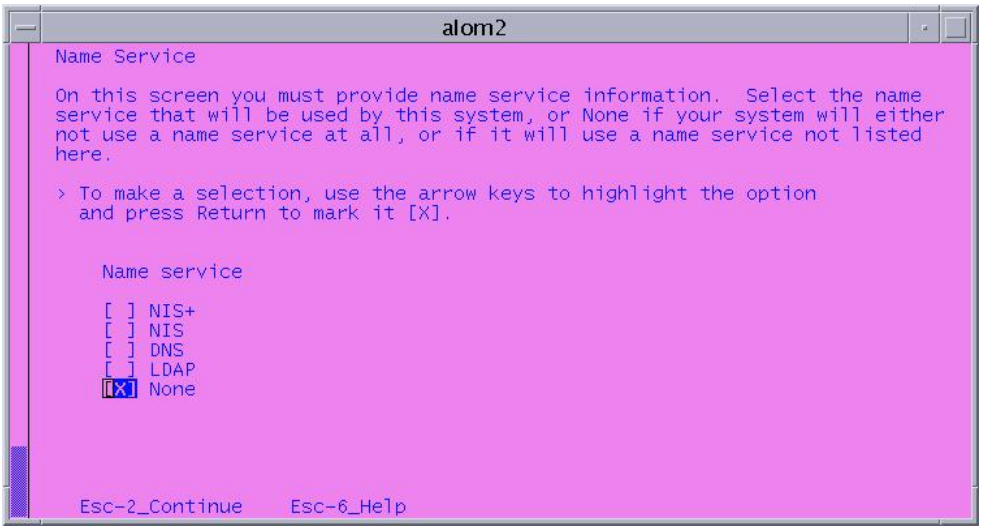
Result: The window updates to ask you to confirm that you made the correct selection regarding Kerberos network security.



19 Review the Kerberos configuration and then press the **Esc** and **2** keys simultaneously.

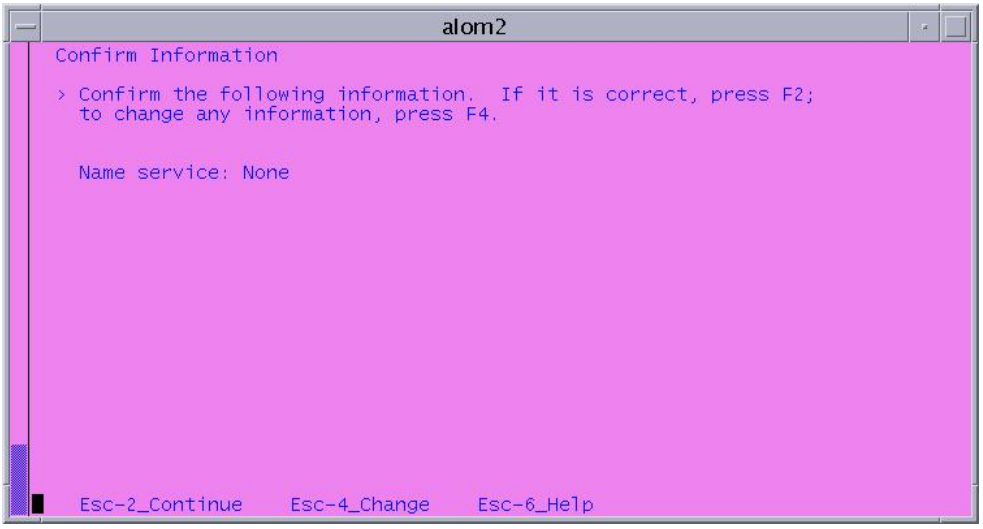
Note: If you need to change the Kerberos configuration, press the **Esc** and **4** keys simultaneously, and then follow the on-screen instructions to make the change.

Result: The window updates to prompt you to select the **Name service** for your system.



20 Select **None** and then press the **Esc** and **2** keys simultaneously.

Result: The window updates to prompt you to confirm that you made the correct decision regarding the Name service.

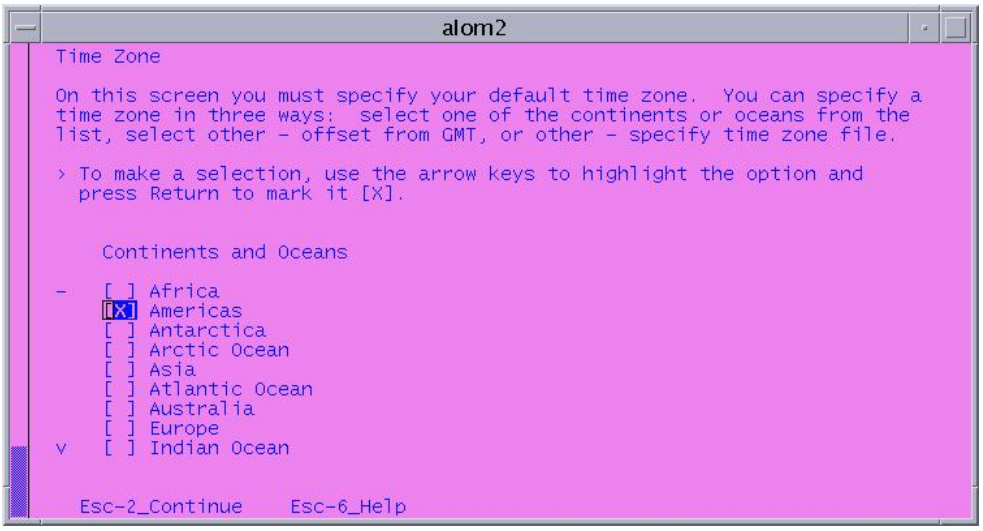


21 Review the Name service configuration and then press the **Esc** and **2** keys simultaneously. The window updates to prompt you to specify the NFSv4 Domain Configuration.

22 Select **Use the NFSv4 domain derived by the system** and press the **Esc** and **2** keys simultaneously.

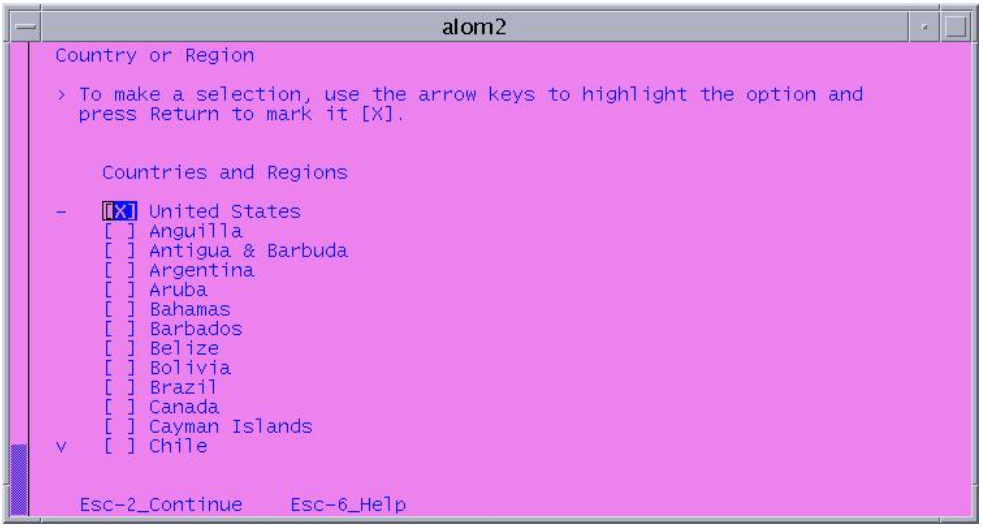
Note: If you need to change the Name service configuration, press the **Esc** and **4** keys simultaneously, and then follow the on-screen instructions to make the change.

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



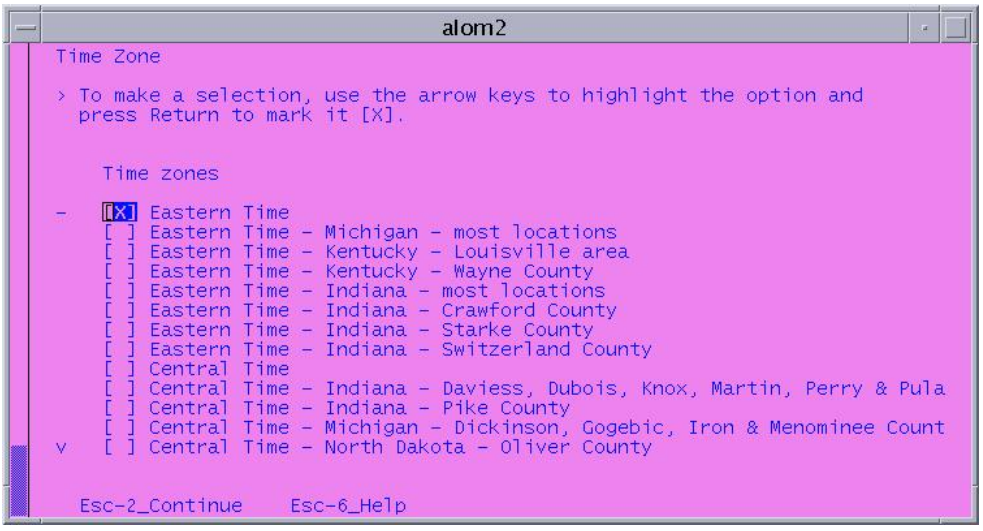
23 Select **Americas** and then press the **Esc** and **2** keys simultaneously.

Result: The window updates to prompt you to specify the appropriate country or region.



24 Select the appropriate country or region and then press the **Esc** and **2** keys simultaneously.

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

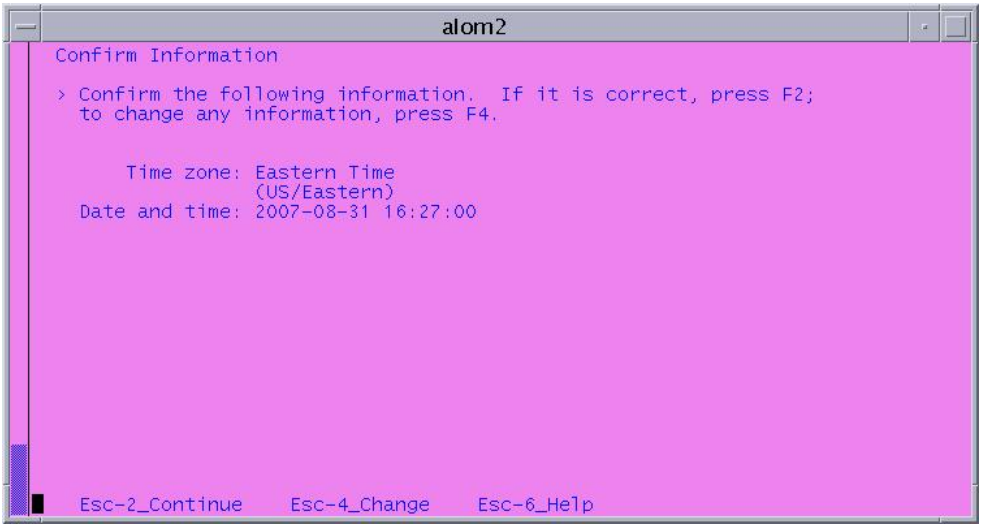


25 Select the appropriate time zone and then press the **Esc** and **2** keys simultaneously.

Result: The window updates to prompt you to select the appropriate time and date.

26 Select the default value, if it is correct, or type in the correct values and then press the **Esc** and **2** keys simultaneously.

Result: The window updates to prompt you to confirm the date and time information.

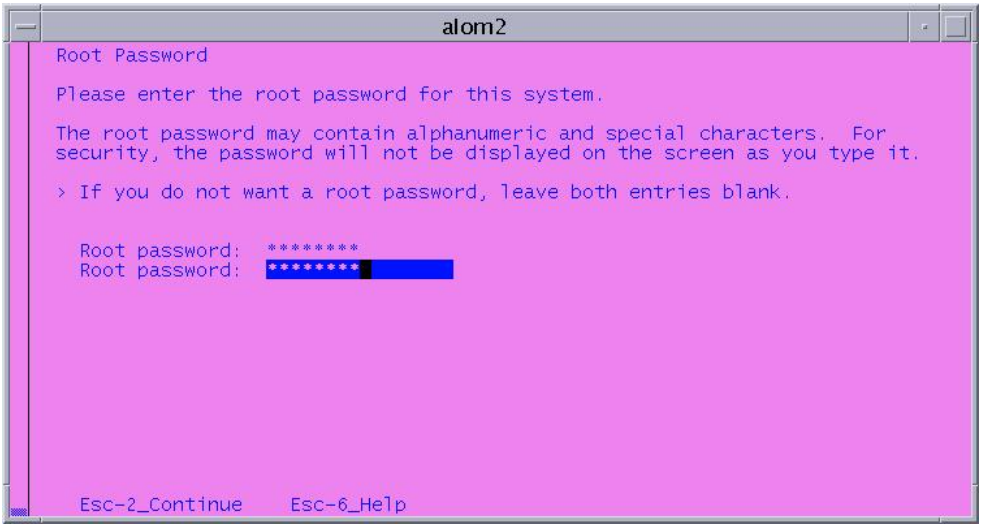


27 Review the date and time information and then press the **Esc** and **2** keys simultaneously.

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.

Result: The window updates and asks you to provide the root password for the system.

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



29 Type the **root** password a second time and then press the **Esc** and **2** keys simultaneously.

Result: The installation process continues and the console login prompt appears when the installation process has ended.

30 Log on to the RNCS through the console port as **root** user.

31 Go to *Running the create_sysidcfg Script* (on page 24).

Running the create_sysidcfg Script

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

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

2 Is the default IP address correct?

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

Result: The following message appears:

Restarting ntp
Sysidcfg information written successfully to nvramrc

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

Attach Mirrors

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

Attaching Mirrors

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

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

Suggestion Regarding the RNCS Software DVD

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

Network Configuration

Editing the RNCS /etc/hosts File

Complete the following steps to update the /etc/hosts file.

1. Log on to the RNCS as **root** user.
2. Open the **/etc/hosts** file with a text editor.
3. Verify that the RNCS Headend Control Network entry is accurate. The entry must be the following:

   <IPAddress> <hostname> <hostname>. loghost

   Note: The **<IPAddress>** field contains the Headend Control Network IP Address and the **<Hostname>** field contains the RNCS Hostname.

   Example:

   ```
   172.35.0.1      lionn2 lionn2.        loghost
   ```
4. Update the RNCS Headend Control Network if the values are not correct.
5. On the ISDS, type **grep dncsatm /etc/hosts** and press **Enter**. The IP address of the ISDS dncsatm IP network interface is returned.
6. In the RNCS /etc/hosts file, verify that the ISDS Network Element Control (dncsatm) entry is accurate. The entry must be the following:

   <IPAddress> dncsatm dncs_host isds_host

   Note: The **<IPAddress>** field contains the ISDS Network Element Control (dncsatm) IP Address.

   Example:

   ```
   10.253.0.1     dncsatm dncs_host       isds_host
   ```
7. Update the ISDS Network Element Control (dncsatm) IP Address if the value does not match the value found in step 5.
8. Add the following line to the end of the file for the OOB (OM2000) network interface.

   <OOB IP Address> <OOB Hostname>

   Notes:

   - Replace **<OOB IP Address>** and **<OOB Hostname>** with the IP Address and Hostname of the OOB (OM2000) network interface.
   - This step (step 8) is required only for IPTV system releases (ISR).
9. Save and close the file.
10. Type **cat /etc/hosts** and press **Enter**.

11 The /etc/hosts file should look similar to the following example:

```
#
# Internet host table
#
::1     localhost
127.0.0.1       localhost
172.35.0.1      lionn2 lionn2.        loghost
10.253.0.1      dncsatm dncs_host       isds_host
192.168.64.1    lionn2OM
```

Editing the /etc/nodename File

1 If necessary, log on to the RNCS as **root** user.

2 Type **cat /etc/nodename** and press **Enter**. The /etc/nodename file opens for inspection.

3 Does the file already contain the hostname of the RNCS?

- If **yes**, go to ***Editing the /etc/hostname.bge0 File*** (on page 27).
- If **no**, open the **/etc/nodename** file in a text editor.

4 Change or add the RNCS hostname to the file.

Note: The hostname should be the same hostname that you entered in step 10 of ***Install the RNCS Software*** (on page 11).

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

```
lionn2
```

5 Save and close the file.

Editing the /etc/hostname.bge0 File

1 If necessary, log on to the RNCS as **root** user.

2 Type **cat /etc/hostname.bge0** and press **Enter**. The /etc/hostname.bge0 file opens for inspection.

Note: For sites that use the Netra T5220 server, the file is */etc/hostname.e1000g0*.

3 Does the file already contain the hostname of the RNCS?

- If **yes**, go to ***Editing the /etc/defaultrouter File*** (on page 28).
- If **no**, open the **/etc/hostname.bge0** file in a text editor.

  Note: For sites that use the Netra T5220 server, the file is */etc/hostname.e1000g0*.

4 Change or add the RNCS hostname to the file.

Note: The hostname should be the same hostname that you entered in step 10 of ***Install the RNCS Software*** (on page 11).

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

```
lionn2
```

5 Save and close the file.

Editing the /etc/defaultrouter File

Complete the following steps to update the /etc/defaultrouter File.

1 If necessary, log on to the RNCS as **root** user.

2 Type **cat /etc/defaultrouter** and press **Enter**. The /etc/defaultrouter file opens for inspection.

3 Does an entry already exist that contains the correct IP address of the Headend Control Network Router?

- If **yes**, go to ***Editing the /export/home/informix/etc/sqlhosts File*** (on page 28).
- If **no**, open the **/etc/defaultrouter** file in a text editor.

4 Add or change the entry so that it contains the correct IP address of the Headend Control Network Router.

Example: Your entry should look similar to the following example:

```
10.253.0.254
```

5 Save and close the file.

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

1 If necessary, log on to the RNCS as **root** user.

2 Type **cat /export/home/informix/etc/sqlhosts** and press **Enter**. The /export/home/informix/etc/sqlhosts opens for examination.

3 Does the file contain the hostname of the RNCS?

- If **yes**, go to ***Enabling the FTP Service on the RNCS*** (on page 29).
- If **no**, open the **/export/home/informix/etc/sqlhosts** file in a text editor.

4 Change or add the RNCS hostname to the file that contains the name of the RNCS. If other entries exist, separate this new entry from the other entries by using the **Tab** key.

Note: The hostname should be the same hostname that you entered in step 10 of ***Install the RNCS Software*** (on page 11).

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

```
demo_on onipcshm        on_hostname     on_servername
demo_se seipcpip        se_hostname     sqlexec
lionnDbServer           setlitcp        lionn2    informixSE
```

5 Save and close the file.

Enabling the FTP Service on the RNCS

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

1 Is the FTP service required on this system?

- If **yes**, continue with step 2.
- If **no**, go to ***Enabling TFTP and bootp Services*** (on page 30).

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

inetadm –e svc:/network/ftp:default

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

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

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

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

 # Source the Local EAS Interface IP address

LOCAL_EAS_IP=[EAS Interface IP]; export LOCAL_EAS_IP

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

5 Save and close the file.

Enabling TFTP and bootp Services

Note: Do not execute this procedure if TFTP and bootp are not required or desired on this system.

1. If necessary, open an xterm window on the RNCS as root user.
2. Use a text editor to uncomment (delete the "#" character, if present, at the beginning of the line) the following line in the **/etc/inet/inetd.conf** file.

   tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
3. Save and close the file.
4. If the "#" character was removed in the file, type **inetconv** and then press **Enter**. The system configures the TFTP service.
5. Type **svcadm enable svc:/network/tftp/udp6** and then press **Enter** to enable the TFTP service.
6. Type **svcs svc:/network/tftp/udp6** and then press **Enter** to verify that the TFTP service is running.

   Example: You should see output similar to the following:

   STATE STIME FMRI

   online 15:15:14 svc:/network/tftp/udp6:default
7. Follow these instructions to enable the bootp service.
   a. As root user, type **cd /dvs/lionn/etc** and then press **Enter**.
   b. Type **chmod 4550 bootpd** and then press **Enter**.

Reboot the RNCS

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

1. Type **shutdown -y -g0 -i6** and press **Enter**.
2. Log on to the RNCS as **root** user.

Checking NTP Activation

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

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

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

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

2 Does an asterisk precede dncsatm?

- If **yes**, NTP is properly configured on the RNCS; go to ***Verifying the Distributed DNCS License*** (on page 32).
- If **no**, continue with step 3.

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

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

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

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

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

Important: If you are running Solaris 8 (instead of Solaris 10), type **/etc/rc2.d.S99xntpd stop** and press **Enter** to stop NTP.

7 Type **ntpdate dncsatm** and press **Enter**. Output similar to the following should appear:

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

Note: Ignore any **No Server Suitable for Synchronization** message.

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

Note: If you are running Solaris 8 (instead of Solaris 10), type **./s99xntpd start** instead.

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

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

Verifying the Distributed DNCS License

Complete the following steps to verify the Distributed DNCS license.

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

Add and Configure the RNCS

Adding the RNCS Site

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

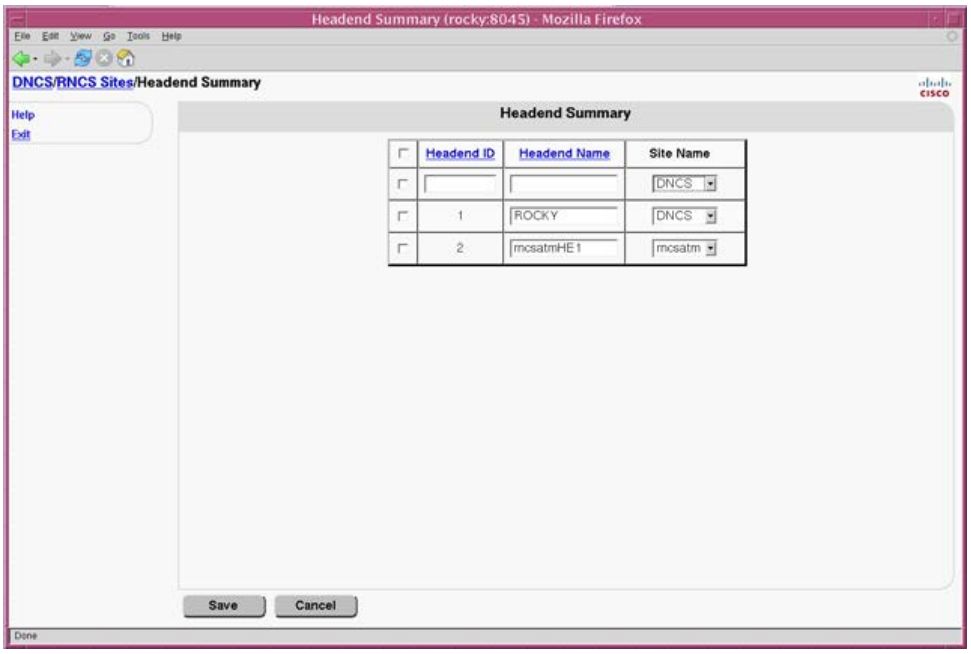
1. On the ISDS, open, if necessary, the ISDS Administrative Console.
2. Select the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Add**. The Site Summary window updates to reveal a new, empty row.
5. Enter the following information:
   - **Site Name**—A unique name for the site

     Note: Our engineers recommend that the site name should be the same as the hostname that you entered in step 10 of ***Install the RNCS Software*** (on page 11).
   - **Site ID**—A unique number identifying the site
   - **IP Address**—The IP address of the site
   - **Online**—Select this option (so that a checkmark appears in the box) to activate the site.
6. Click **Save**. A Confirmation message appears.
7. Click **OK**.
8. Click **Exit**.

Adding the Headend

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

1. From the ISDS Administrative Console, click the **Element Provisioning** tab.
2. Click **Headend**. The Headend Summary window opens.
3. Click **Add Headend**. The Headend Summary window opens with a new, blank row.

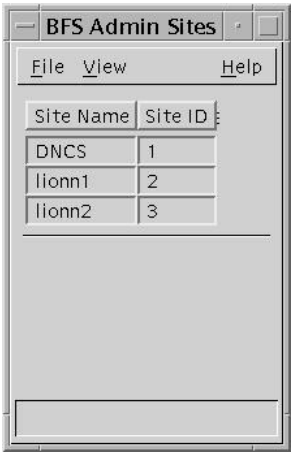


4. Enter the following information:
   - **Headend Name**—A unique name for this headend.
   - **Headend ID**—A unique number identifying this headend.
   - **Site Name**—Select the site this headend is associated with from the list.
5. Click **Save**. A confirmation message appears.
6. Click **OK** on the confirmation message.
7. Click **Exit**.
8. Add the new headend to your network map.

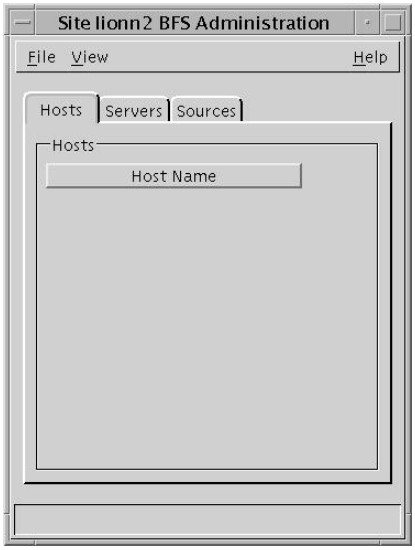
Adding a New BFS Host

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

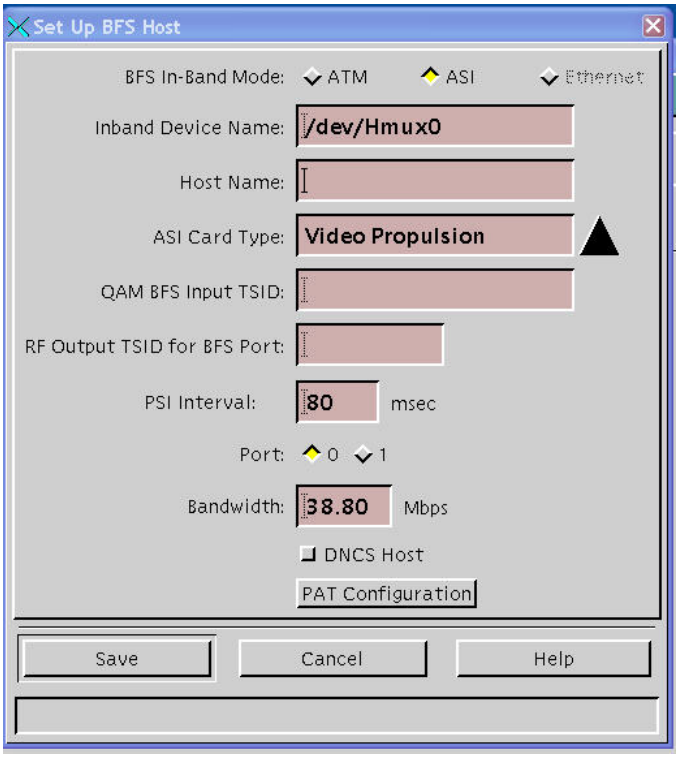
1. From the ISDS Administrative Console, select the **Application Interface Modules** tab.
2. Click **BFS Admin**. The BFS Admin Sites window opens.



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



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



6 Enter the following information:

- **BFS In-Band Mode** (ATM)
- **Inband Device Name**

  Note: You can leave this field at its default setting.
- **Host Name**

  Note: The hostname should be the same hostname that you entered in step 10 of ***Install the RNCS Software*** (on page 11).

Note: Any additional selectable parameters on the Set Up BFS Host window are not needed when ATM is selected as the BFS In-Band Mode.

7 Click **Save**.

Enabling RF or IP Sources for the New Site

Refer to ***Recommended Data Carousel Rate Settings*** (on page 85) for guidance when configuring these sources.

1 From the BFS Admin Sites window, double-click the site you just created.

2 Choose one of the following options:

- If your site uses RF sources, go to step 3.
- If your site uses IP-only sources, go to step 6.

3 Click the **RF Sources** tab.

4 Enable the following sources:

- Bootloader OOB
- CAM OOB
- Out of Band
- MMM OOB
- PkgLocator
- POD Channels
- PPV OOB
- System Carousel

5 Go to step 8.

6 If your site uses IP sources, click the **IP Sources** tab.

7 For an IP-only site, enable all inband and out-of-band sources.

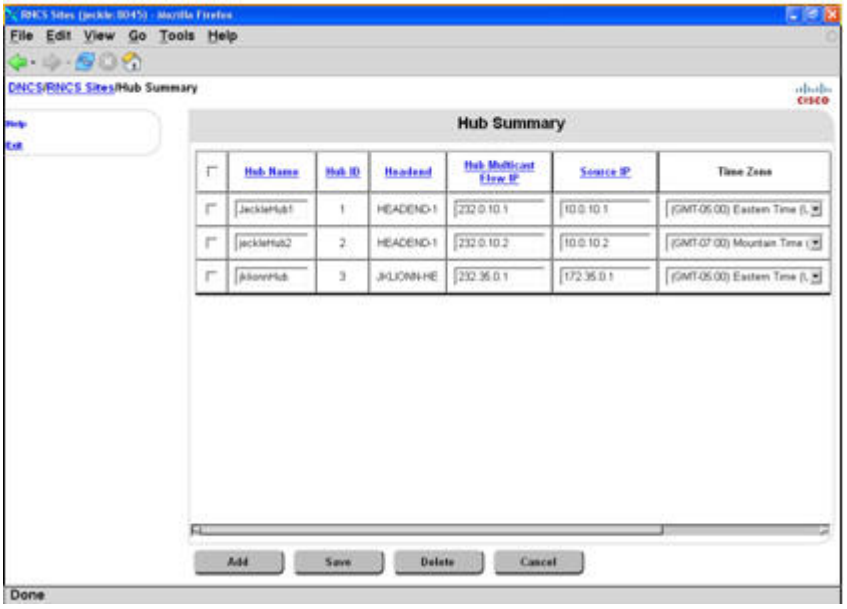
8 Click **Save**.

Adding a New Hub Entry

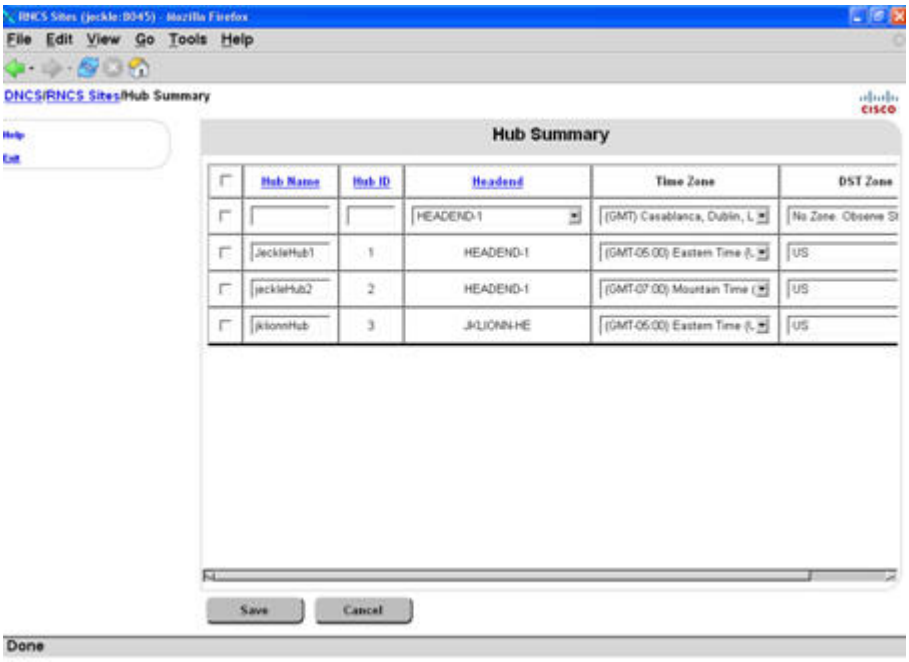
Follow these general instructions to add a new hub entry to the system.

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

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



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



4 Configure the new hub with the following information:

- **Hub Name**—The name you will use to identify this hub.
- **Hub ID**—The number you will use to identify this hub.
- **Headend**—The headend associated with this hub.
- **Time Zone**—The time zone associated with this hub.
- **DST Zone ID**—The DST Zone ID associated with this hub.

5 Click **Save**. The Hub Summary window updates.

6 If required, configure the new hub with a **Hub Multicast Flow IP Address** and a **Source IP Address**.

7 Click **Save**.

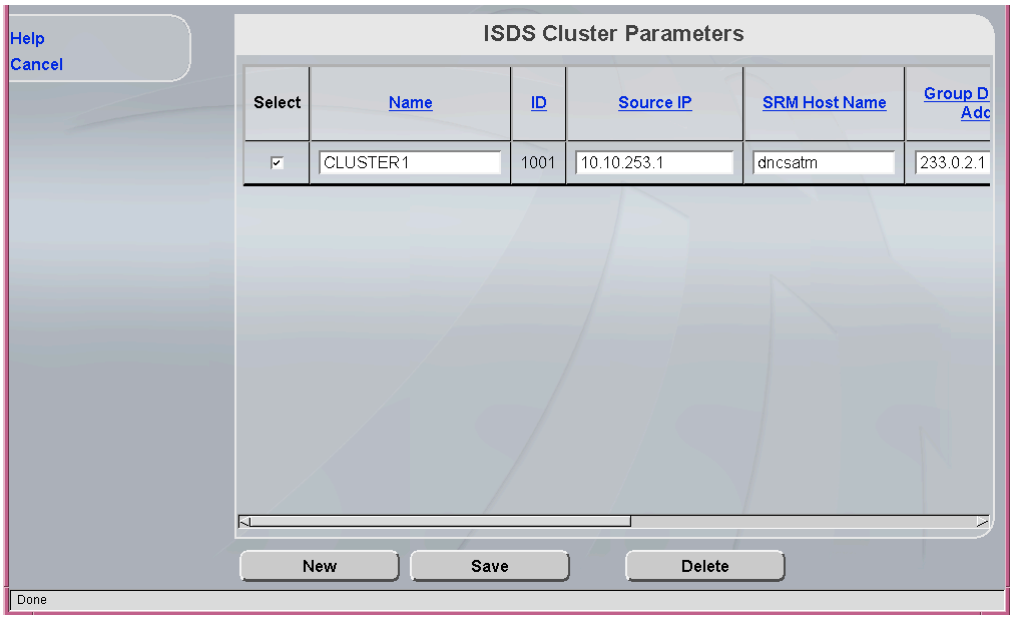
Adding a New Cluster Entry for the RNCS

Follow these instructions to add a new cluster entry for the RNCS.

Note: Skip this procedure if your site does not use clusters.

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

2 Click **Cluster**. The ISDS Cluster Parameters window opens.



3 Click **New**.

4 Configure the new cluster with the following information:

- **Name** — the name you will use to identify this cluster
- **Source IP** — The IP address of the ISDS (dncsatm) associated with this cluster
- **SRM Host Name** — The name or IP address of the Session Resource Manager
- **Group Destination Address** — The Multicast IP address associated with the cluster
- **Hub Association** — The hub associated with the cluster

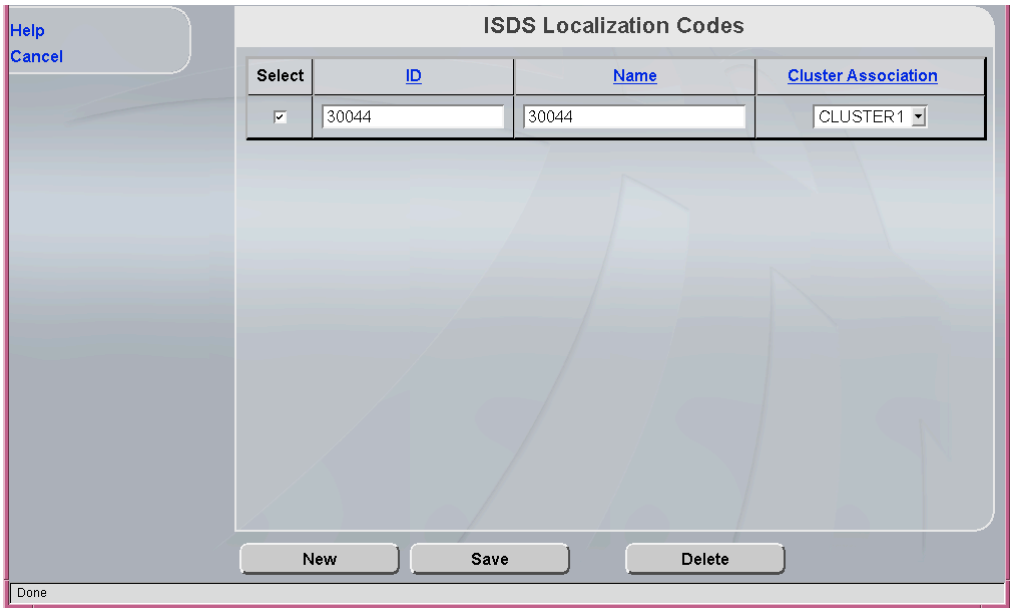
5 Click **Save**.

Adding a New Localization Code

Complete these instructions to add a new localization code.

Note: Skip this procedure if your site does not use localization codes.

1. From the ISDS Site Administrative Console, select the **Network Element Provisioning** tab.
2. Click **Localization**. The ISDS Localization Codes window opens.



3. Click **New**.
4. Configure the new localization code with the following information:
   - **ID —** A unique numerical identifier you will use to identify this localization code
   - **Name —** The name you will use to identify this localization code
   - **Cluster Association —** The cluster associated with this localization code
5. Click **Save**.

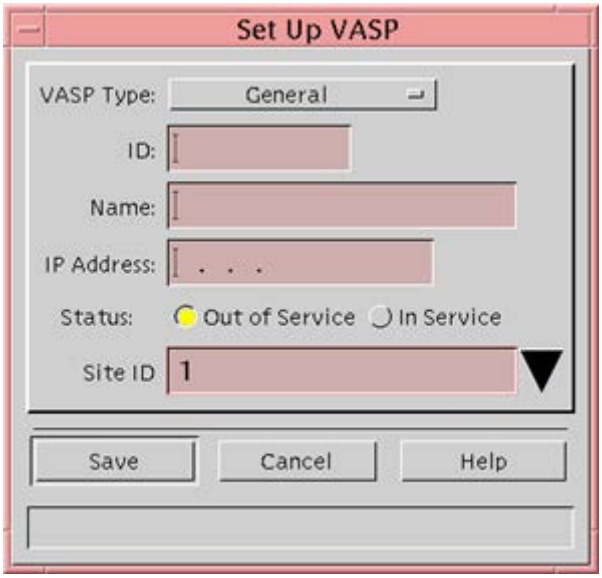
Adding a VASP

Complete these steps to add a new Value-added service provider (VASP).

1 From the ISDS Administrative Console, select the **ISDS** tab and then the **Network Provisioning** tab.

2 Click **VASP**. The VASP List opens.

3 Click **File > New**. The Set Up VASP window opens.



4 Configure the new VASP with the following information:

- Select **General** as the **VASP Type**.
- Type a unique VASP **ID**.
- Type the VASP **Name**.
- Type the **IP Address** of the RNCS.
- Select **In Service** in the **Status** field.
- Select the RNCS **Site ID**.

5 Click **Save**.

6 Will your RNCS receive EAS messages?

- If yes, go to step 7.
- If no, go to ***Set Up the Remote Site*** (on page 42).

7 Repeat steps 3 through 5, except for the **VASP Type**, select **mmmServer**.

Set Up the Remote Site

Your next step is to initialize the RNCS using the siteCmd program. Follow the instructions in ***Set Up the Remote Site*** (on page 69). Then, return to this page and continue with ***Adding QPSK Modulators to the RNCS*** (on page 42).

CAUTION:

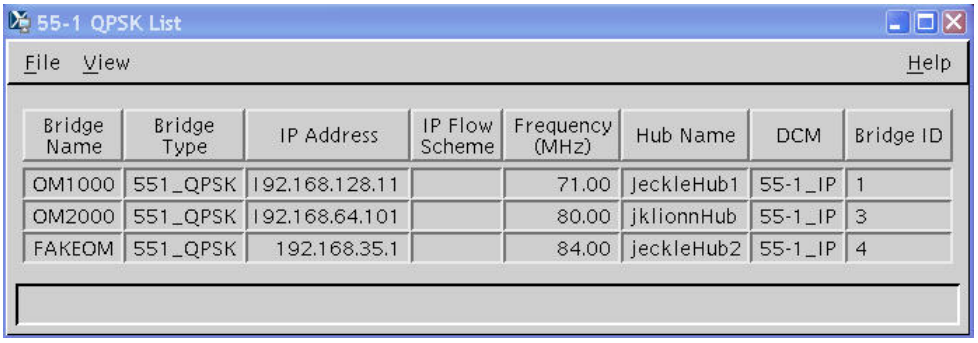
The installation of RNCS software will not be successful if you do not set up the remote site.

Adding QPSK Modulators to the RNCS

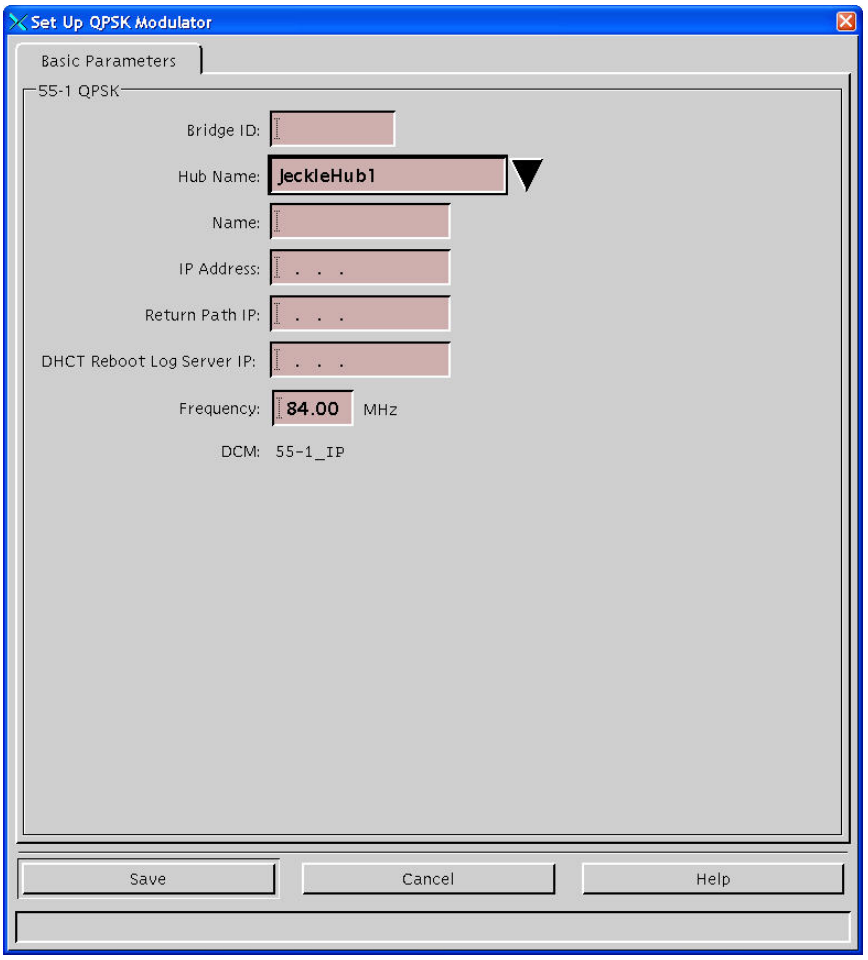
Note: Skip this procedure if your site does not use QPSK modulators.

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

2 Click **55-1 QPSK**. The 55-1 QPSK List window opens.



3 Click **File**, select **New**, and then select **551-QPSK**. The Set Up QPSK Modulator window opens.



4 Follow these instructions to configure the Set Up QPSK Modulator window.

a Enter the **Bridge ID**.

b Enter the **Hub Name** of the hub associated with this QPSK.

c Enter the **Name** of the QPSK.

d Enter the **IP Address** of the QPSK.

e Enter the **Return Path IP** address of the QPSK.

f Enter the **DHCT Reboot Log Server IP** address of the QPSK.

g Enter the **Frequency** of the QPSK.

Note: You may have to consult with the system operator to determine the frequency.

5 Click **Save**.

6 Close the Set Up QPSK Modulator window and the 55-1 QPSK List window.

Starting the RNCS

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

1. Open an xterm window on the ISDS.
2. Type **siteCmd < hostname > lionnStart** and press **Enter**.

   Note: Substitute the hostname of the RNCS for < hostname >.
3. In the xterm window on the ISDS, type **siteCmd < hostname > lionnControl** and press **Enter**. The lionnControl utility window opens.
4. Select **2** and press **Enter** to view all process elements.
5. Select **x** and press **Enter** to return to the main menu of the lionnControl utility window.
6. Select **1** and press **Enter** to stop all processes.

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

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

2

Upgrade of RNCS Software

Introduction

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

In This Chapter

Back Up SNMP Configuration Data

Custom SNMP configurations in the snmpd.conf file are not automatically backed up and restored. The following procedure helps you identify custom SNMP configurations that should be added back to the system after the upgrade.

1. Log on to the RNCS as **root** user.
2. Type **grep rocommunity /etc/sma/snmp/snmpd.conf** and press **Enter**.
3. In the space provided, record any lines that are not comments.

   Note: It is possible that all of the lines are comments.

   _____

   _____

   _____

   _____

   Important: These lines must be added back to the/etc/sma/snmp/snmpd.conf file after the upgrade.
4. Type **grep trapsess /etc/sma/snmp/snmpd.conf** and press **Enter**.
5. In the space provided, record any lines that appear in the output from step 4.

   Note: It is possible that no lines will appear in the output.

   _____

   _____

   _____

   _____

   Important: These lines must be added back to the /etc/sma/snmp/snmpd.conf file after the upgrade.

Upgrade the RNCS Software

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

Important: If you are installing RNCS software on a Sun Fire server for the first time, go to ***Initial Installation of RNCS Software*** (on page 1).

RNCS Server Connection Options

There are two options for connecting to the RNCS for software upgrades:

- Connect directly to the serial management port on the RNCS server with a laptop computer
- Remotely connect to the ALOM/ILOM network management port on the RNCS server

Both options are covered in detail in the following sections.

Connect Directly to the Serial Management Port on the RNCS Server with a Laptop Computer

1. Connect a laptop computer to the serial management port of the RNCS server.
2. Start the HyperTerminal application on the laptop and configure the application with the following parameters:

   Note: The HyperTerminal application allows one computer to communicate with another computer.

   - **Baud rate — 9600**
   - **Data bits — 8**
   - **Parity — none**
   - **Stop bit — 1**
   - **Flow control — no**
3. Choose one of the following options:
   - If you are connecting to a Sun Fire V245 server, press **Enter** and go to step 4.
   - If you are connecting to a Netra T5220 server, press **Enter** and go to step 7.

4 Did the system display the ALOM login prompt after you pressed Enter?

Example: Sun(tm) Advanced Lights Out Manager 1.6.4 (SanJose-LIONN)

Please login:

- If **yes**, follow these instructions.
  - **a** Type the admin user ID and press **Enter**. A prompt for the password appears.
  - **b** Type the password for the admin user and press **Enter**. The **sc >** prompt appears as the system establishes a login session to the ALOM port of the RNCS.
  - **c** Type **console -f** and press **Enter**. The system displays **Enter #. to return to ALOM**.
  - **d** Press **Enter** once. The console login prompt appears.
  - **e** Type **root** and press **Enter**. The password prompt appears.
  - **f** Type the RNCS root password and press **Enter**. The console command line appears.
  - **g** Go to ***Upgrading the RNCS Software*** (on page 51).
- If **no**, continue with step 5.

5 Does the system display the **sc>** command line prompt?

- If **yes**, complete these steps to log on to the console.
  - **a** Type **console -f** and press **Enter**. The system displays **Enter #. to return to ALOM**.
  - **b** Press **Enter** once. The console login prompt appears.
  - **c** Type **root** and press **Enter**. The password prompt appears.
  - **d** Type the RNCS root password and press **Enter**. The console command line appears.
  - **e** Go to ***Upgrading the RNCS Software*** (on page 51).
- If **no**, continue with step 6.

6 Does the system display the console login prompt?

Example: console login:

- If **yes**, complete these steps to log on to the console.
  - **a** Type **root** and press **Enter**. The password prompt appears.
  - **b** Type the RNCS root password and press **Enter**. The console command line appears.
  - **c** Go to ***Upgrading the RNCS Software*** (on page 51).
- If **no**, then the console command line should be displaying. Go to ***Upgrading the RNCS Software*** (on page 51).

7 Does the system display the ILOM login prompt?

Example: SUNSP002128100EDD login:

- If **yes**, complete the following steps to log on to the ILOM port and then to access the console.
  - **a** Type the administrator user ID (the default is **root**) and press **Enter**. A prompt for the password appears.
  - **b** Type the password for the administrator user (the default is **changeme**) and press **Enter**. The **->** prompt appears as the system establishes a login session to the ILOM port of the RNCS.
  - **c** Type **start /SP/console** and press **Enter**. The system displays a **Are you sure you want to start /SP/console (y/n)?** prompt.
  - **d** Type **y** and press **Enter**. The system displays a **Serial console started. To stop, type #.** message.
  - **e** Press **Enter** once. The console login prompt appears.
  - **f** Type **root** and press **Enter**. The password prompt appears.
  - **g** Type the RNCS root password and press **Enter**. The console command line appears.
  - **h** Go to ***Upgrading the RNCS Software*** (on page 51).
- If **no**, continue with step 8.

8 Does the system return the **->** command line prompt?

- If **yes**, complete the following steps to access the console.
  - **a** Type **start /SP/console** and press **Enter**. The system displays a **Are you sure you want to start /SP/console (y/n)?** prompt.
  - **b** Type **y** and press **Enter**. The system displays a **Serial console started. To stop, type #.** message.
  - **c** Press **Enter** once. The console login prompt appears.
  - **d** Type **root** and press **Enter**. The password prompt appears.
  - **e** Type the RNCS root password and press **Enter**. The console command line appears.
  - **f** Go to ***Upgrading the RNCS Software*** (on page 51).
- If **no**, continue with step 9.

9 Does the system return the console login prompt?

- If **yes**, complete the following steps to log on to the console.
  - **a** Type **root** and press **Enter**. The password prompt appears.
  - **b** Type the RNCS root password and press **Enter**. The console command line appears.
  - **c** Go to ***Upgrading the RNCS Software*** (on page 51).
- If **no**, then the console command line should be displaying. Go to ***Upgrading the RNCS Software*** (on page 51).

Connect Remotely to the ALOM/ILOM Network Management Port on the RNCS Server

1. Choose one of the following options:
   - If you are connecting to the ALOM port of the Sun Fire V245 server, go to step 2.
   - If you are connecting to the ILOM port of the Netra T5220 server, go to step 3.
2. Complete the following steps to remotely log on to the ALOM port of the Sun Fire V245 server.
   a. Type **telnet [IP address of ALOM port]** and press **Enter**. A prompt for the user ID appears.

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

      Example: telnet 10.201.0.2

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

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

   d. Type **console -f** and then press **Enter**. The following message appears:

      Warning: User <auto> currently has write permission to this console and forcibly removing them will terminate any current write actions and all work will be lost. Would you like to continue? [y/n]

   e. Type **y** and press **Enter**. The system displays the **Enter #. to return to ALOM** prompt.

   f. Press **Enter** once. The console login prompt appears.

   g. Type **root** and press **Enter**. The password prompt appears.

   h. Type the RNCS root password and press **Enter**. The console command line appears.

   i. Go to ***Upgrading the RNCS Software*** (on page 51).

3 Complete the following steps to remotely log on to the ILOM port of the Netra T5220 server.

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

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

   Example: ssh 10.201.0.2

   b Type the administrator user ID (the default is root) and press **Enter**. A prompt for the password appears.

   c Type the password for the administrator user (the default is **changeme**) and press **Enter**. The **->** prompt appears as the system establishes a secure shell connection to the ILOM port.

   d Type **start /SP/console** and press **Enter**. The system displays a **Are you sure you want to start /SP/console (y/n)?** prompt.

   e Type **y** and press **Enter**. The system displays a **Serial console started. To stop, type #.** message.

   f Press **Enter** once. The console login prompt appears.

   g Type **root** and press **Enter**. The password prompt appears.

   h Type the RNCS root password and press **Enter**. The console command line appears.

   i Go to ***Upgrading the RNCS Software*** (on page 51).

Upgrading the RNCS Software

Complete the following steps to upgrade the RNCS software.

1 In an xterm window on the ISDS, type **ssh root@[RNCS]** and press **Enter**. The RNCS server returns a password prompt.

   Note: Replace [RNCS] with the IP address or hostname of the RNCS server.

2 Type the RNCS root password and press **Enter**. The ssh root login session on the RNCS starts.

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

4 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.

5 Follow these instructions to confirm that the system correctly mounted the DVD.

a Wait about a minute after having inserted the RNCS installation DVD; then type **df -n** and press **Enter**. A list of mounted file systems appears.

Note: The presence of /cdrom in the output confirms that the system correctly mounted the DVD

b Did the system correctly mount the DVD?

– If **yes**, go to step 6.

– If **no**, continue with steps c) and d); then, repeat step a).

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

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

6 As root user in an xterm window on the ISDS, type **siteCmd [hostname] ps -ef | grep dvs** and then press **Enter**.

Example: siteCmd lionn2 ps -ef | grep dvs

7 Does the output from step 6 reveal that lionn processes are running?

- If **yes**, go to step 8.
- If **no**, troubleshoot the issue to the best of your abilities.

Note: Call Cisco Services if you need assistance.

8 Type **metastat | more** and then press **Enter**. The system displays the status of all of the metadevices on the RNCS.

Note: Press the **Spacebar**, if necessary, to page through all of the output.

9 Are the following two conditions true?

— The designation **Okay** appears in the **State** column next to each metadevice.

— No Hot Spare indicates **In Use**.

- If **yes** (to both conditions), go to step 10.
- If **no** (to either or both conditions), call Cisco Services for help in resolving the issue.

10 Type **metastat –c** and press **Enter**. The system displays a list of metadevices on the system.

11 Does the output from step 10 show that there are two attached submirrors for each device?

Note: There should be a d4xx and d7xx submirror listed under each d5xx metadevice, as illustrated in the following example. If there is only one d7xx or d4xx submirror listed under each d5xx metadevice, then the mirrors are not attached.

Example:

d506 m 8.0GB d406 d706

d406 s 8.0GB c1t0d0s6

d706 s 8.0GB c1t1d0s6

- If **yes**, go to step 12.
- If **no**, follow these instructions using the console to attach the mirrors.
  - **a** Type **cd /cdrom/cdrom0/s0/sai/scripts** and press **Enter**. The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.
  - **b** Type **./LIONN_attach_mirrors** and press **Enter**. A confirmation message appears.
  - **c** Type **y** (for yes) and press **Enter**. The system runs a script that enables the disk-mirroring function of the server.

    Note: This script may take 20 minutes or longer to complete.
  - **d** When the synchronization of the mirrors is complete, type **metastat | more** and press **Enter** to verify that submirrors d4xx and d7xx are in an **ok** state.

12 From the console on the RNCS, type **cd /cdrom/cdrom0/s0/sai/scripts** and then press **Enter**. The /cdrom/cdrom0/s0/sai/scripts directory becomes the working directory.

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

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

15 Type **metastat -c** and then press **Enter** to verify that the **d7xx** mirrors are no longer shown.

Example: You should see output similar to the following.

```
d506          m  8.0GB d406
  d406        s  8.0GB c1t0d0s6
d505          m   40GB d405
  d405        s   40GB c1t0d0s5
d503          m  8.0GB d403
  d403        s  8.0GB c1t0d0s3
d501          m  4.0GB d401
  d401        s  4.0GB c1t0d0s1
d500          m  8.0GB d400
  d400        s  8.0GB c1t0d0s0
```

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

16 From the console on the RNCS, type **./LU_LIONN** and then press **Enter**. A confirmation message appears.

17 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.

18 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.

19 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 and displays a **Live Upgrade procedure finished. Please check logs for any Errors** message when the upgrade has completed.

20 Examine the log file for errors.

Note: The log file is /tmp/install_log.

21 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	Is Complete	Active Now	Active On Reboot	Can Delete	Copy Status
f12.0.0.7p7	**yes**	**yes**	**yes**	**no**	**—**
LIONN_V3.1.0.x	**yes**	**no**	**no**	**yes**	**—**

Notes:

- The version of LIONN software associated with the *f12.0.0.7p7* 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_3.1.0.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.

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

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

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

```
**********************************************************************

The target boot environment has been activated. It will be used when you
reboot.
NOTE: You must use either init or shutdown when you reboot.  If you do
not use one of these commands,

the system will not boot using the target BE.

**********************************************************************

In case of a failure while booting to the target BE, the following
process

needs to be followed to fallback to the currently working boot
environment:

1. Enter the PROM monitor (ok prompt).

2. Change the boot device back to the original boot environment by
typing:

   setenv boot-device disk:a

3. Boot to the original boot environment by typing:
   boot

**********************************************************************

Activation of boot environment <LIONN_3.1.0.x> successful.
```

23 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	Is Complete	Active Now	Active On Reboot	Can Delete	Copy Status
fl2.0.0.7p7	**yes**	**yes**	**no**	**no**	**—**
LIONN_V3.1.0.x	**yes**	**no**	**yes**	**no**	**—**

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

24 From an xterm window on the ISDS (as root user), type **siteCmd [hostname of Sun Fire server] lionnStop** and then press **Enter**. A confirmation message about stopping the lionn appears.

Example: siteCmd lionn2 lionnStop

25 Type **y** and then press **Enter**. The lionn processes stop.

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

27 Do the results from step 26 show only the **lionnInitd** and **Informix** processes?

- If **yes**, go to step 28.
- 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 27 b still show lionn processes that are running.

28 From the console on the RNCS, 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 ISDS.
- Do not use the *reboot* or *halt* commands to reboot the server.
- After the first reboot, the engineer *may* be prompted to supply answers to some questions that appear in ***Install the RNCS Software*** (on page 11).

29 From the console on the RNCS, open the /etc/ssh/sshd_config file with a text editor.

30 Un-comment the **PermitRootLogin yes** line by removing the **#** from the beginning of the line to allow remote SSH login for root user

31 Save and close the /etc/ssh/sshd_config file.

32 Type **svcadm refresh ssh** and press **Enter**. The SSH service is restarted and the SSH login for root is enabled.

33 From an xterm window on the ISDS, use the **ssh** command to access the RNCS server as **root** user. You should see screen output similar to the following example:

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

34 Does the output from step 33 reveal that Sun OS version 5.10 installed?

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

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

```
PKGINST:  SAIlionn
     NAME:  LIONN 05-08-09
 CATEGORY:  application
     ARCH:  sparc
  VERSION:  fl2.2.0.0
  BASEDIR:  /dvs
   VENDOR:  Cisco
     DESC:  LIONN 05-08-09
   PSTAMP:  bumblebee20090508222059
 INSTDATE:  Jun 09 2009 15:50
   STATUS:  completely installed
    FILES:      168 installed pathnames
                 14 shared pathnames
                 21 directories
                114 executables
                  2 setuid/setgid executables
               205544 blocks used (approx)
```

36 Does the output from step 35 indicate that the correct version was successfully installed?

- If **yes**, go to step 37.
- If **no**, call Cisco Services for assistance.

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

38 Complete the following steps to enable ftp, if required, on this system.

Important: The ftp service is required for EAS support on the RNCS. The ftp service can be enabled if it is preferred over sftp or scp for file transfer to and from the RNCS.

Note: Enabling the ftp service degrades the security enhancements implemented on the RNCS. We recommend that you do not enable the ftp service unless required.

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

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

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

STATE STIME FMRI

online 15:08:44 svc:/network/ftp:default

39 Complete the following steps verify the status of the tftp and bootp services, if required, on this system.

Important: The tftp and bootp services are required for Cisco QAMs and QPSKs and may be used for PCGs.

Note: Enabling the tftp and bootp services degrades the security enhancements implemented on the RNCS. We recommend that you do not enable the tftp and bootp services unless required.

a As root user in an xterm window on the RNCS, type **svcs svc:/network/tftp/udp6** and then press **Enter** to determine whether the TFTP services are running.

Note: If a message similar to Pattern 'svc:/network/tftp/udp6' doesn't match any instances appears, the tftp service is not running. Go to ***Enable the TFTP and bootp Services*** (on page **Error! Bookmark not defined.**) to enable the tftp services.

b As root user in an xterm window in the ISDS, type **siteCmd [SITE_NAME] lionnControl** and then press **Enter**. The lionnControl menu appears.

c Select option **2**.

Note: If output similar to **[5] Bootp Daemon run(2) inval(7) 0 0** appears, the bootp service is not running. Go to ***Enable the TFTP and bootp Services*** (on page **Error! Bookmark not defined.**) to enable the bootp services.

40 Complete the following steps to verify the EAS configuration on the RNCS, if EAS messages are handled by this system.

a As root user in an xterm window on the RNCS, open the /export/home/dncs/.profile with a text editor.

b Verify that the following lines are present in the .profile file:

Source the Local EAS Server IP address

LOCAL_EAS_IP=<EAS Server IP>; export LOCAL_EAS_IP

c Replace <EAS Server IP> with the IP address of the local interface that will receive EAS messages, if that value does not already exist in the file.

d Save and close the file.

41 From an xterm window on the ISDS as root user, type **siteCmd [hostname of lionn] lionnStart** and then press **Enter**. The lionn processes start.

Example: siteCmd lionn2 lionnStart

42 From an xterm window on the ISDS as root user, type **siteCmd [hostname of lionn] lionnControl** and then press **Enter**. Examine the output to verify that the lionn startup processes are running.

43 From the console on the RNCS, type **exit** and press **Enter**. The console session closes.

44 Choose one of the following options to log out of the console:

- If the RNCS is a Sun Fire V240, follow these instructions to log out of the ALOM port:
  a Type **#** and then type the period key (**#.**). The **sc>** prompt appears.
  b Type **logout** and press **Enter**. The ALOM log in session closes.
- If the RNCS is a Sun Netra T5220, follow these instructions to log out of the ILOM port:
  a Type **#** and then type the period key (**#.**). The **->** prompt appears.
  b Type **exit** and press **Enter**. The ILOM log in session closes.

Restore the SNMP Configuration Data

If the SNMP interfaces had custom configurations prior to the upgrade, then complete the following steps to restore the configuration.

Note: You recorded the custom SNMP configuration data in ***Back Up SNMP Configuration Data*** (on page 46).

1. Log on to the RNCS as **root** user.
2. Did you find any un-commented lines that contain *rocommunity* in the /etc/sma/snmp/snmpd.conf file prior to the upgrade?
   - If **yes**, follow these instructions.
     a. Type **cd /etc/sma/snmp/** and press **Enter**.
     b. Type **cp snmpd.conf snmpd.conf.bkup1** and press **Enter** to create a backup copy of the SMA snmpd.conf file.
     c. Open the snmpd.conf file with a text editor.
     d. Add to the snmpd.conf the *rocommunity* lines you recorded prior to the upgrade.
        Note: Add them right after the **#rocommunity public** line.
     e. Save and close the snmpd.conf file.
   - If **no**, continue with step 3.
3. Did you find any lines in the /etc/sma/snmp/snmpd.conf file that contain *trapsess* prior to the upgrade?
   - If **yes**, follow these instructions.
     a. Type **cp snmpd.conf snmpd.conf.bkup2** and press **Enter** to create a backup copy of the SMA snmpd.conf file.
     b. Open the snmpd.conf file with a text editor.
     c. Add to the end of the snmpd.conf file those lines that you recorded prior to the upgrade.
     d. Did any of the original trap destinations include -v 3 which indicates the trap destination is SNMPv3?
        - If **yes**, go to step 4.
        - If **no**, save and close the snmpd.conf file; then go to step 5.

4 Follow these instructions to update the engine ID.

a As root user in another xterm window on the RNCS, type **grep usmUser /var/sma_snmp/snmpd.conf** and press **Enter**. SNMP configuration data, including the hexadecimal engine ID, appears.

Note: The first hexadecimal number after usmUser 1 3 in the second entry returned in the results from the previous set is the SNMPv3 engine ID.

Example: 0x800007e580744f551d000000004aae8371

b Update the engine ID in the snmpd.conf SNMPv3 trap destination with the engine ID found in step 4 a.

Example: trapsess -e 0x800007e580744f551d000000004aae8371 -v 3 -u snmpUser -a MD5 -A "I Can Read" -l authNoPriv 172.40.90.1:162

c Save and close the snmpd.conf file; then go to step 5.

5 Did you make any modifications to the /etc/sma/snmp/snmpd.conf file?

- If **yes**, follow these instructions.
  - **a** Type **svcadm -v disable -st sma** and press **Enter** to stop the SMA service.
  - **b** Type **svcadm -v enable -s sma** and press **Enter** to restart the SMA service.
  - **c** Type **svcs -x sma** and press **Enter** to verify that the SMA service started.

    Example: You should see output similar to the following example:

```
svc:/application/management/sma:default (net-snmp SNMP daemon)
 State: online since Fri Sep 18 16:53:03 2009
   See: snmpd(1M)
   See: /var/svc/log/application-management-sma:default.log
Impact: None
```

  - **d** Type **svcadm -v disable fmd** and press **Enter** to stop the Fault Management daemon.
  - **e** Type **svcadm -v enable -s fmd** and press **Enter** to restart the Fault Management daemon. The system displays the following message; then the command prompt appears once the Fault Management service has started.

    svc:/system/fmd:default enabled

    Note: It may take more than 30 seconds for the service to start.
  - **f** Type **svcs -xv fmd** and press **Enter** to verify that the Fault Management service started successfully.

    Example: You should see output similar to the following example:

```
svc:/system/fmd:default (Solaris Fault Manager)
 State: online since Fri Sep 18 16:46:29 2009
   See: man -M /usr/share/man -s 1M fmd
   See: /var/svc/log/system-fmd:default.log
Impact: None
```

- If **no**, go to step 6.

6 Type **exit** and press **Enter** to log out of the RNCS.

7 Consult with the Network Administrator at the headend to verify that SNMP is working as expected.

Attach Mirrors

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

Important: Note these important points:

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

Attaching Mirrors

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

Suggestion Regarding the RNCS Software DVD

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

3

Customer Information

If You Have Questions

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

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

A

The siteCmd Program

Introduction

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

- Register a remote site with the ISDS
- Copy files from the ISDS 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 ISDS, 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 ISDS and the remote sites managed by the ISDS. Our engineers have implemented this requirement through use of the Secure Shell.

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

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

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

Set Up the Remote Site

Before using the Secure Shell to communicate with a remote site, you need to set up that site with the ISDS. 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 ISDS will manage.

1. If necessary, open an xterm window on the ISDS.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type **siteCmd -S** and press **Enter**. The following message appears:
   ```
   Enter the host name of the site you are adding.
   ```
4. Type the host name of the remote site you are registering and press **Enter**.
   Example: lionn2
   Result: The following message appears:
   ```
   Enter the IP address of the site you are adding.
   ```
5. Type the IP address of the remote site you are registering and press **Enter**.
   Example: 10.202.0.1
   Result: The following message appears:
   ```
   The following line will be added to /etc/hosts:
   [IP address]  [host name]
   Do you want to continue? [y,n,?,q]
   ```
6. Type **y** (for yes) and press **Enter**.
   Results:
   - The system performs a connectivity check between the RNCS and the ISDS.
   - The system sets up the RNCS with the required configuration so that a Secure Shell can be used for communications between the ISDS and the RNCS.
   - The system creates a synchronization directory for the RNCS in the ISDS (/dvs/distFiles/[host name]).

   Example: In the example used in this procedure, the siteCmd program creates the following directory on the ISDS: **/dvs/distFiles/lionn2**.
7. Verify that a secure connection exists by typing **siteCmd [hostname] ls -l** and press **Enter**. The system should display the hostname and site ID of the remote site, as well as a listing of the files in the directory of the remote site.
   Note: Substitute the hostname of the remote site for [hostname].

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

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

Note: For more information on the siteCmd program, see ***Options for the siteCmd Program*** (on page 71).

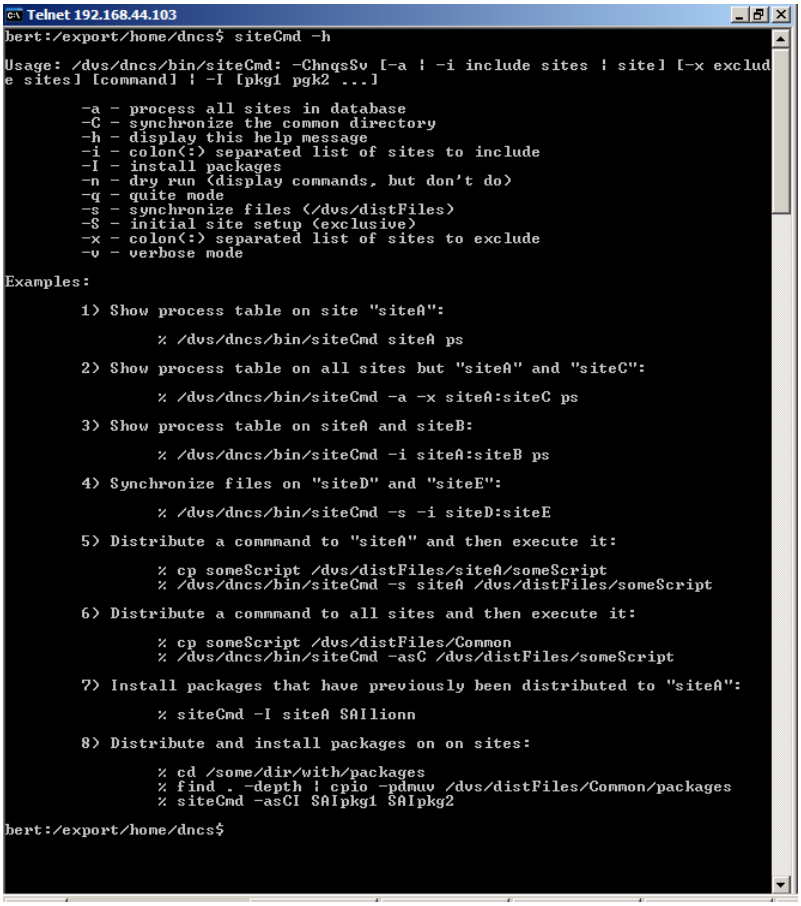
Options for the siteCmd Program

Now that you have registered each of your remote sites with the ISDS, 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 ISDS.
2. Type **siteCmd -h** and press **Enter**. The system displays the help window for the siteCmd program.



Options Available With the siteCmd Program

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

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

Include / Exclude Remote Sites

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

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

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

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

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

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

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

Copy Files from the ISDS to the RNCS

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

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

1. To copy the file **someScript** into the common directory of the ISDS, type **cp someScript /dvs/distFiles/Common** and press **Enter**.
2. To distribute the someScript file to each RNCS, type **siteCmd -asC /dvs/distFiles/someScript** and press **Enter**.

   Notes:

   - The **–a** option specifies that **all** RNCS sites are to receive the file.
   - The **s** option indicates **synchronize**. Synchronizing involves updating the RNCS with the contents of the common directory of the ISDS.
   - The **C** option specifies to the siteCmd program that the source directory of the ISDS 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 ISDS.

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

   Note: You must be root user to install packages.

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

   b Type the root password and press **Enter**.
2. Type **cd /cdrom/cdrom0** and press **Enter**. The /cdrom/cdrom0 directory of the ISDS becomes the working directory.
3. Type **find [package_name] | cpio -pudmv /dvs/distFiles/Common/packages** and press **Enter**. The system copies the files on the CD into the common directory of the ISDS.

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

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

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

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

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

Example: siteCmd -a lionnStop

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

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

Example: siteCmd -a lionnKill

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

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

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

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

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

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

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

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

13 Was the package successfully installed?

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

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

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

Example: siteCmd -a lionnStart

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

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

B

RNCS Rollback Procedure

Introduction

This appendix is intended for field service engineers who encounter problems while upgrading existing RNCS software. Prior to executing these rollback procedures, contact Cisco Services at 1-800-283-2636.

In This Appendix

Roll Back the RNCS Software

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

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

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

Rolling Back the RNCS Software

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

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

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

   Important: Do not use the reboot or halt command to reboot the server.
3. After the server reboots, log on as **dncs** user.
4. Type **pkginfo -l SAIlionn** and press **Enter**. Verify that the old software is in place.
5. Type **siteCmd [hostname of server] lionnStart** and press **Enter**. The system starts the lionn processes.
6. Go to *Attaching Mirrors* (on page 79).

Attaching Mirrors

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

Important:

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

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

C

Managing Default User Passwords and Password Expiration Settings

Introduction

The information in this appendix provides guidance in managing the passwords of the various user accounts associated with the RNCS.

In This Appendix

Change Default User Passwords and Password Expiration Settings

We recommend that, at a minimum, you change the default password for the root role and the dncs role in order to increase the level of security on the RNCS.

You should not change the informix and dncsSSH passwords as these accounts are locked by default. Additionally, changing the pcgrequest and pcgscp user passwords is not absolutely necessary because these accounts are not used directly by an operator and do not support normal login shells. Changing the easftp and dncsftp passwords should be done only in coordination with the administrator of the EAS, ISDS, and the RNCS, respectively.

The root, dncsSSH, informix, easftp, and any custom accounts, as well as the dncs role, all have password-aging set by default. These passwords will expire after 13 weeks. You can modify this expiration if the operator does not want to manage password expiration on the RNCS.

CAUTION:

The RNCS or components within the RNCS will become unstable if the default password of the user (root, dncs, dncsSSH, informix, or easftp) expire. The RNCS system administrator MUST ensure that these passwords do NOT expire. It is imperative that password-aging be disabled unless the RNCS system administrator ensures these account passwords do not expire.

1. If necessary, open an xterm window on the RNCS as root user.
2. Select one of the following options:
   - If password-aging is *not* desired on this system, go to step 3.
   - If password-aging is desired on this system, skip to step 9.
3. Open the /etc/default/passwd file with a text editor.
4. Change the **MAXWEEKS** and **WARNWEEKS** parameter values to **-1**.
5. Save and close the file.
6. Type **more /etc/default/passwd** and then press **Enter**. The MAXWEEKS and WARNWEEKS should look like the following example:

   MAXWEEKS=-1

   WARNWEEKS=-1
7. Repeat the following step for the root, dncs, dncsftp, and easftp account names to disable password expiration:

   Type **passwd -r files -x -1 [accountName]** and then press **Enter**.

   Note: Replace [accountName] with the appropriate account name — root, dncs, dncsftp, or easftp.

8 Repeat the following step for the root, dncs, dncsftp, and easftp account names to verify that password expiration has been disabled:

Type **passwd -r files -s [accountName]** and then press **Enter**.

Notes:

- Replace [accountName] with the appropriate account name — root, dncs, dncsftp, or easftp.
- Only PS should be displayed after the account name after you complete step 8. No numbers should appear. If numbers appear after any account name, repeat steps 7 and 8 for the appropriate account name.

9 Repeat the following step for the necessary account names (only root and dncs, unless otherwise required) in order to change passwords:

Type **passwd -r files [accountName]** and then press **Enter**. Enter and re-enter the new password, when prompted.

D

Recommended Data Carousel Rate Settings

Introduction

Refer to the data carousel settings in this appendix when configuring your BFS carousel.

For sites that support the RF + IP configuration, go to ***Data Carousel Rate Settings for an RF + IP Configuration*** (on page 86).

For sites that support the IP-only configuration , go to ***Data Carousel Rate Settings for an IP-Only Configuration*** (on page 87).

In This Appendix

Data Carousel Rate Settings for an RF + IP Configuration

The following table lists the suggested source data carousel rate settings for the RF + IP configuration. Reference the Site DNCS BFS Administration window to review the current settings, if necessary. Refer to *Configuring the ISDS for Verizon STB Operations User Guide* (part number 4001522) for additional information.

Note: In the following table, TT refers to Transport Type.

Source ID	Data Carousel	TT	Data Rate (Mbps)	Block Size (Bytes)	Indication Interval (ms)	Enabled
0	System Carousel	OOB	0.01	1024	200	x
1	Out-of-Band	OOB	0.01	1024	200	x
2	Inband	IB	N/A	N/A	N/A	
3	CAM OOB	OOB	0.01	1024	200	x
4	CAM IB	IB	N/A	N/A	N/A	
5	IPG OOB	OOB	N/A	N/A	N/A	
6	IPG1 IB	IB	N/A	N/A	N/A	
7	PPV OOB	OOB	0.01	1024	200	x
8	PPV IB	IB	N/A	N/A	N/A	
9	SAM	OOB	N/A	N/A	N/A	
10	IPG2 IB	IB	N/A	N/A	N/A	
11	POD_Channels	OOB	0.01	1024	200	x
12	IPG3 IB	IB	N/A	N/A	N/A	
14	IPG4 IB	IB	N/A	N/A	N/A	
16	IPG5 IB	IB	N/A	N/A	N/A	
18	IPG6 IB	IB	N/A	N/A	N/A	
20	IPG7 IB	IB	N/A	N/A	N/A	
21	MMM OOB	OOB	N/A	N/A	N/A	
22	PPV IB2	IB	N/A	N/A	N/A	
195	bootloaderOOB	OOB	1.00	1024	200	x
199	bootloader		1.00	1024	200	
197	pkgLocator		0.01	1024	200	x

Data Carousel Rate Settings for an IP-Only Configuration

The following table lists the suggested source data carousel rate settings for an IP-only configuration. Reference the Site DNCS BFS Administration window to review the current settings, if necessary. Refer to *Configuring the ISDS for Verizon STB Operations User Guide* (part number 4001522) for additional information.

Note: In the following table, TT refers to Transport Type.

Source ID	Data Carousel	TT	Data Rate (bps)	Block Size (Bytes)	Indication Interval (ms)	Enabled
0	System Carousel	OOB	500000	1300	200	x
1	Out-of-Band	OOB	500000	1300	200	x
2	Inband	IB	1000000	1300	N/A	x
3	CAM OOB	OOB	500000	1300	200	x
4	CAM IB	IB	500000	1300	N/A	x
5	IPG OOB	OOB	500000	1300	N/A	x
6	IPG1 IB	IB	1000000	1300	N/A	x
7	PPV OOB	OOB	500000	1300	200	x
9	SAM	OOB	500000	1300	N/A	x
10	IPG2 IB	IB	1000000	1300	N/A	x
11	POD_Channels	OOB	500000	1300	200	x
12	IPG3 IB	IB	1000000	1300	N/A	x
14	IPG4 IB	IB	1000000	1300	N/A	x
16	IPG5 IB	IB	1000000	1300	N/A	x
18	IPG6 IB	IB	1000000	1300	N/A	x
20	IPG7 IB	IB	1000000	1300	N/A	x
21	MMM OOB	OOB	500000	1300	N/A	x
22	PPV IB2	IB	1000000	1300	N/A	x
181	VQE		500000	1300		x
199	bootloader		3000000	1304	200	x

E

Enable the TFTP and bootp Services

Introduction

For security purposes, the TFTP and bootp services are disabled by default. Cisco QAMs and QPSKs require that the TFTP and bootp services be running on the RNCS. The TFTP and bootp services may also be used for the PCG, depending upon the implementation. Follow the instructions in this appendix to enable the TFTP and bootp services only if required.

In This Appendix

Enabling the TFTP and bootp Services

Note: Do not execute this procedure if TFTP and bootp are not required or desired on this system.

1. If necessary, open an xterm window on the ISDS as root user.
2. Use a text editor to uncomment (delete the "#" character, if present, at the beginning of the line) the following line in the **/etc/inet/inetd.conf** file.

   tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
3. From the root xterm window, if the "#" character was removed, type **inetconv** and then press **Enter**. The system configures the TFTP service.
4. Type **svcadm enable svc:/network/tftp/udp6** and then press **Enter** to enable the TFTP service.
5. Type **svcs svc:/network/tftp/udp6** and then press **Enter** to verify that the TFTP service is running.

   Example: You should see output similar to the following:

   STATE STIME FMRI

   online 15:15:14 svc:/network/tftp/udp6:default
6. Follow these instructions to enable the bootp service.
   a. As root user, type **cd /dvs/lionn/etc** and then press **Enter**.
   b. Type **chmod 4550 bootpd** and then press **Enter**.
7. Type **exit** and then press **Enter** to log out the root user.

Index

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

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

August 2012 Printed in USA

Part Number 78-4021167-01 Rev D