Initial Installation and Upgrade Instructions for the ISDS

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 Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

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

Copyright

Contents

About This Guide

Purpose

This guide serves the following two purposes:

- Provides step-by-step instructions for installing the IPTV Service Delivery System (ISDS) software onto a server for the first time.
- Provides step-by-step instructions for upgrading an existing system of ISDS software.

Audience

This guide is written for field service engineers and system operators who are responsible for the installation or upgrade of the ISDS software.

Read the Entire Guide

Please review this entire guide before beginning the installation or upgrade. If you are uncomfortable with any of the procedures, contact Cisco® Services at 1-866-787-3866 for assistance.

Important: Complete 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.

Review *ISDP 2.7 Release Notes* (part number 4022474) for additional details related to the installation or the upgrade that might not be covered in this guide.

What Procedures to Follow

If you are installing the ISDS software for the first time, go to Chapter 1, ***Initial Installation and Service Provisioning Instructions for ISDS*** (on page 1).

If you are upgrading the ISDS software, go directly to Chapter 2, ***Pre-Upgrade Procedures for the ISDS*** (on page 101).

Required Skills and Expertise

System operators or engineers who install or upgrade ISDS software need the following skills:

- Advanced knowledge of UNIX
  - Experience with the UNIX vi editor. Several times throughout this installation 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 add and remove user accounts

Supported Hardware Platforms

Platform	Hard Drives	Memory
Sun Fire V445	■ 4 X 73 GB ■ 8 X 73 GB	■ 4 GB minimum
Sun Fire V890	■ 6 X 146 GB ■ 12 X 146 GB	■ 8 GB minimum ■ 16 GB minimum
Sun Netra T5440	■ 2 X 146 GB	■ 4 GB minimum

Monitor Resolution

The minimum resolution required for monitors connected to the ISDS is 1280 X 1024.

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
The **Before You Begin** section was added to Chapter 1.	See ***Before You Begin*** (on page 4).

Description	See Topic
The **Configure or Restore the BOSS Interface** procedure was added to the set of post-upgrade procedures.	See *Configure or Restore the BOSS Interface* (on page 195).

1

Initial Installation and Service Provisioning Instructions for ISDS

Introduction

This chapter describes how to install ISDS software onto a system for the first time, and then how to configure the server and the software.

Important: If you are upgrading a system rather than installing the software for the first time, go to Chapter 2.

Important Points About the Installation

Many security enhancements have been implemented in ISDS software, beginning with ISDS 2.3 f2.0.0.3. Review *ISDS Security Enhancements Instructions* (part number 4027701) if you are unfamiliar with the changes implemented as a result of the security enhancements. There are fundamental changes you must be aware of to perform some of the most basic functions on the ISDS.

In This Chapter

Before You Begin

Before you begin the installation, be certain that you collect the following information or have the following items:

- How many headends, hubs, and localizations to be built on the system
- The approved network design drawing
- The IP address of the local EAS server
- Hub, cluster, and BFS Multicast flow addresses
- Customer CAA CD, Factory Root Certificate Authorization Key CD, and CAA pass phrase for the TED
- IPG account information and channel short descriptions
- Channel line-up and packages
- Billing vendor information
- STB EMMs for supported DHCTs

Supported Platforms and Physical Connections

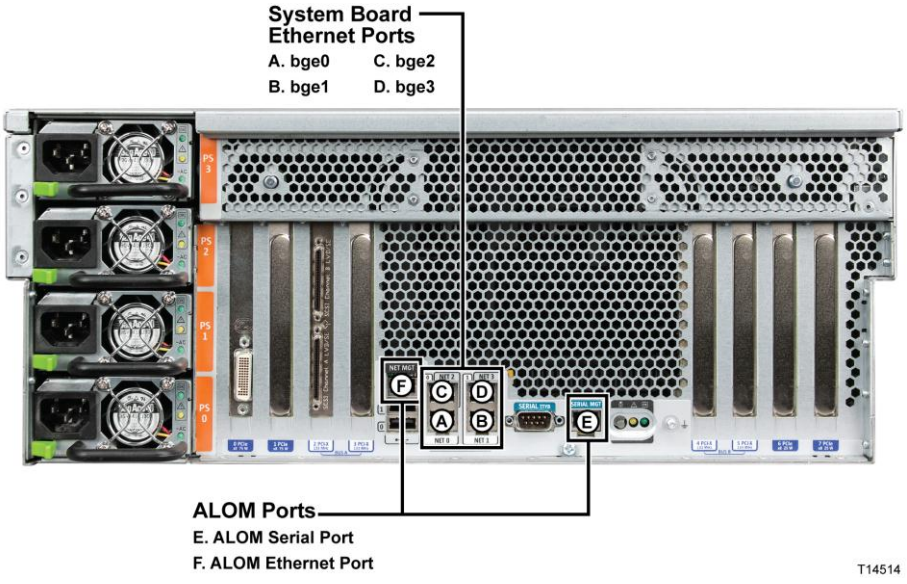
Go to one of the following sections, depending upon the server you are using:

- ***Sun Fire V445 ALOM and Network Connections*** (on page 5)
- ***Sun Fire V890 ALOM and Network Connections*** (on page 6)
- ***Sun Netra T5440 ILOM and Network Connections*** (on page 8)

Sun Fire V445 ALOM and Network Connections

The Sun Fire V445 ALOM and network connections are located on the back panel of the chassis. The mapping of the network interface name to the physical Ethernet port is provided in this section.

The Sun Fire V445 back panel ALOM and network connectors are shown in this illustration.



The following table describes the back panel ALOM and network connectors:

Component	Description
ALOM	Advance Lights Out Management SERIAL MGT = Serial Management Port NET MGT = Network Management Port
System Board Ethernet Ports	Network Connections: ■ NET 0 = bge0 ■ NET 1 = bge1 ■ NET 2 = bge2 ■ NET 3 = bge3

Note: Refer to ***ISDS Interface Chart*** (on page 10) for additional detail about network connections.

Check the Drive Placement for the Sun Fire V445

Important: Skip this section if you are installing ISDS software onto a Sun Fire V890 server. This section pertains only to the Sun Fire V445 server.

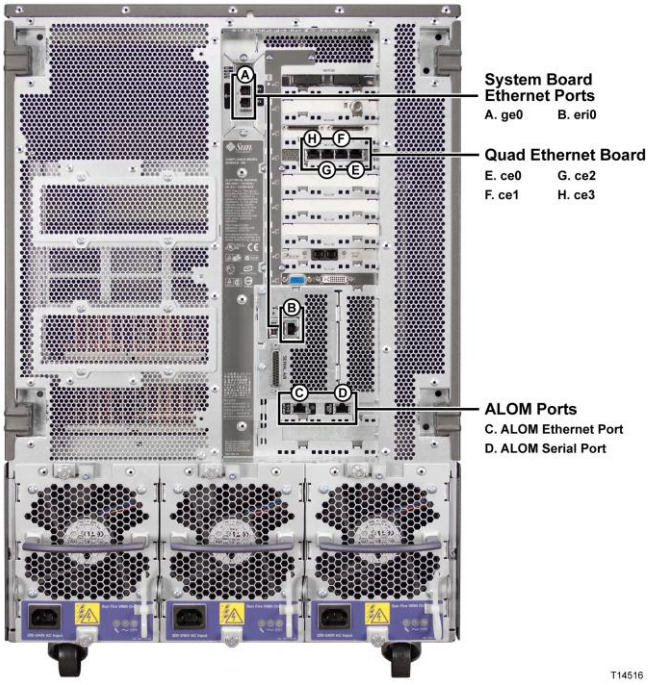
We support two configurations of the Sun Fire V445 — 4 disks and 8 disks. The disk drives for the Sun Fire V445 server need to be in specific slots. In the 4-disk configuration, the disks must be in slots 0, 1, 4, and 5. In the 8-disk configuration, the disks must be in all of the slots.

Examine the Sun Fire V445 server and confirm that the disk drives are in the correct slots. If the disk drives are not in the correct slots, correct that situation now.

Sun Fire V890 ALOM and Network Connections

The Sun Fire V890 ALOM and network connections are located on the back panel of the chassis. The mapping of the network interface name to the physical Ethernet port is provided in this section.

The Sun Fire V890 back panel ALOM and network connectors are shown in the following illustration:



The following table describes the back panel ALOM and the network connectors.

Component	Description
ALOM	Advance Lights Out Management SERIAL MGT = Serial Management Port NET MGT = Network Management Port
System Board Ethernet Ports	Network Connections: ■ SC Fiber Gigabit = ge0 ■ TPE Copper Fast Ethernet = eri0

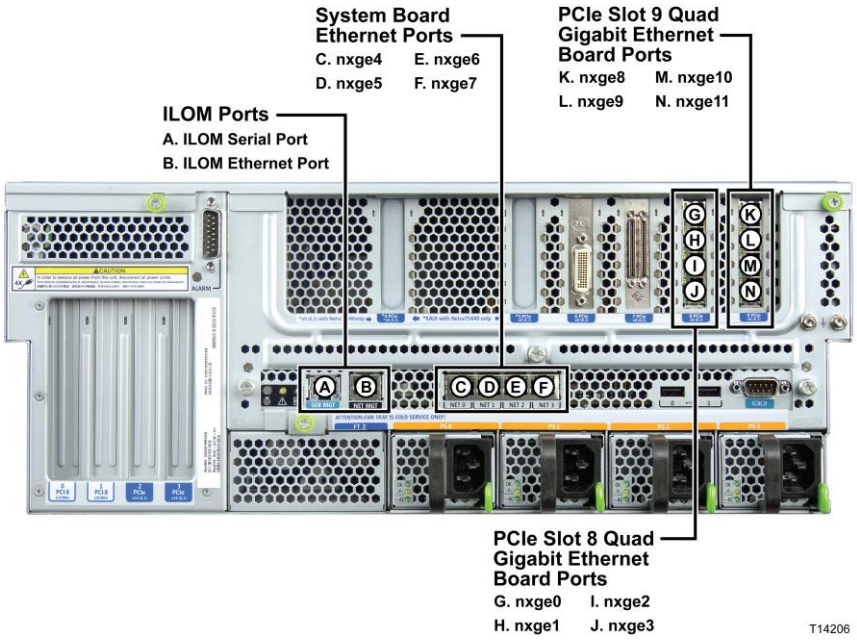
PCI Slot 5 Quad Ethernet Board	Network Connections: ■ Left = ce3 ■ 2nd = ce2 ■ 3rd = ce1 ■ Right = ce0

Note: Refer to ***ISDS Interface Chart*** (on page 10) for additional detail about network connections.

Sun Netra T5440 ILOM and Network Connections

The Netra T5440 ILOM and network connections are located on the back panel of the chassis. The mapping of the network interface name to the physical Ethernet port is provided in this section.

The Netra T5440 back panel ILOM and network connectors are shown in this illustration:



The following table describes the back panel ILOM and network connectors:

Component	Description
ILOM	■ Integrated Lights Out Management ■ SER MGT = Serial Management Port ■ NET MGT = Ethernet Management Port
System Board Ethernet Ports	Network Connections: ■ NET 0 = nxge4 ■ NET 1 = nxge5 ■ NET 2 = nxge6 ■ NET 3 = nxge7
PCIe Slot 8 Quad Gigabit Ethernet Board	Network Connections: ■ Top = nxge0 ■ 2nd = nxge1 ■ 3rd = nxge2 ■ Bottom = nxge3
PCIe Slot 9 Quad Gigabit Ethernet Board	Network Connections: ■ Top = nxge8 ■ 2nd = nxge9 ■ 3rd = nxge10 ■ Bottom = nxge11

Note: Refer to ***ISDS Interface Chart*** (on page 10) for additional detail about network connections.

ISDS Interface Chart

The ISDS software installation scripts automatically configure the host names, IP addresses, and subnet masks for the STB network interface and the TED interface. The ISDS network interface to the site's operations, administration, maintenance, and provisioning (OAM&P) functions are not configured by default. This interface will be manually configured in the following steps. The following chart provides an overview of the default configuration:

System Type	Port	Host Name	IP Address	Subnet Mask	Purpose
V890	ge0	dncsatm appservatm	10.253.0.1	255.255.192.0	ISDS Interface to the STB Network
V890	eri0	dncs	192.168.1.1	255.255.255.0	TED Interface
V890	ce0	N/A	N/A	N/A	Site OAM&P Interface
V445	bge1	dncsatm appservatm	10.253.0.1	255.255.192.0	ISDS Interface to the STB Network
V445	bge0	dncs	192.168.1.1	255.255.255.0	TED Interface
V445	bge2	N/A	N/A	N/A	Site's OAM&P Interface
T5440	nxge0	dncs	192.168.1.1	255.255.255.0	TED Interface
T5440	nxge1	dncsatm appservatm	10.253.0.1	255.255.192.0	ISDS Interface to the STB Network
T5440	nxge2	N/A	N/A	N/A	Site OAM&P Interface

Note: If you require a change to the host name, dncsatm, appservatm, or to another interface configuration, contact Cisco Services. Additional system changes may also be required, which may not be covered in this guide.

Install ISDS Software Onto the ISDS Server

Choose one of the following options:

- To set the operating environment for the Sun Fire V445 or V890 ISDS server, go to ***Setting Operating Environment for the Sun Fire V445 or V890 Server*** (on page 11).
- To set the operating environment for the Sun Netra T5440, go to ***Setting Operating Environment for the Sun Netra T5440 Server*** (on page 17).

Setting Operating Environment for the Sun Fire V445 or V890 Server

Taken as a whole, the serial management port and the network management port of the Sun Fire V445 or V890 server constitutes the Sun Advanced Lights Out Manager (ALOM) port. The ALOM port is a system controller that allows the servers to be managed and administered from a remote location. Through the ALOM port, you can monitor and control the servers through a serial connection (using the serial management port) or an Ethernet connection (using the network management port).

Complete the following steps to set the operating environment for the Sun Fire V445 or V890 ISDS server.

1. Connect power cables to the ISDS server.
2. Connect a laptop computer to the serial management port of the server.
3. 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.
4. Type **# .** and then press **Enter**. The login prompt appears.
5. Type the appropriate user ID and password.
6. At the sc> prompt, type **setsc netsc_dhcp false** and then press **Enter**. The system prepares to disable Dynamic Host Configuration Protocol on the server.
7. Type **resetsc** and then press **Enter**. A message appears that seeks confirmation of your intent to reset the configuration.

8 Type **y** and then press **Enter**. The system applies configuration changes to the server.

9 Choose one of the following options:

- If the Network Management port is *not* required for this ISDS server, skip to step 28.
- If the Network Management port is required for remote IP connection to the ISDS ALOM port, then continue with step 10.

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

Result: One of the following results occurs:

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

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

- If **yes**, continue with step 12.
- If **no**, go to step 13.

12 Complete the following steps if the "setting password" message, described in the first bullet of step 10, appeared after completing step 10.

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

Note: Some installation engineers set this password to *Cisco*, which can be changed later.

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

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

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

Notes:

- Refer to the approved network design drawing for IP-addressing information.
- Substitute the IP address of the network management port of the ISDS server for [IP address].

- The network administrator can help you determine the IP address.

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

Notes:

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

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

Notes:

- Substitute the IP address of the gateway or router of the network management port of the ISDS 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 then press **Enter**. This command sets the sc_powerstatememory variable to true.

17 Type **showsc** and then 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 and then repeat this procedure from step 16.

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

20 Type **y** and then 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**, continue with 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 then press **Enter**.

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

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

25 Review the settings you established in steps 10 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 then 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 ISDS server (rather than the ALOM port).
- The **ok** prompt appears.

28 If you have not already done so, connect the keyboard, monitor, and mouse (KVM) to the server now.

Note: If any of these components do not function properly after you have connected them, follow the short procedure in ***Troubleshooting the Keyboard, Monitor, and Mouse*** (on page 207).

29 Go to ***Installing ISDS Software Onto the Sun Fire V445 or V890 Server*** (on page 23).

Setting Operating Environment for the Sun Netra T5440 Server

The Integrated Lights Out Manager (ILOM) is a dedicated system of hardware and supporting software that allows a system administrator to manage the Sun Netra T5440 independently of the Solaris operating system. The ILOM includes a Serial Management port for directly connecting a computer or terminal server, as well as a Network Management port for connecting remotely over Ethernet.

Complete the following steps to set the operating environment for the Sun Netra T5440 ISDS server.

1 Connect a laptop computer to the serial management port of the 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 From the login prompt on the terminal, log on using **root** as the username and **changme** 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 add a user with an ALOM compatibility shell, if desired by the headend operator.

Note: The ILOM supports adding a user that uses an ALOM compatibility shell, if the headend operator prefers to use commands that resemble ALOM commands.

a Type **create /SP/users/[username] role=Administrator cli_mode=alom** and press **Enter** to create a new alom user.

Note: Replace [username] with the desired username.

Example: admin

b Enter and re-enter a new password for the new user, when prompted.

6 Complete the following steps to set the **HOST_LAST_POWER_STATE** parameter to **enabled**.

Notes:

- This ensures that the Sun operating system sets the parameter to its original state (*powered on* or *powered off*) in the event of a power failure or a restart of the Sun Netra T5440 server.
- These commands are not supported in ILOM 2.0 on the Sun Netra T5440 server.

a Type **set /SP/policy HOST_LAST_POWER_STATE=enabled** and then press **Enter**.

b Type **show /SP/policy** and then press **Enter**. Output should include the following:
HOST_LAST_POWER_STATE = enabled

7 Choose one of the following options:

- If the Network Management port is *not* required for this ISDS server, skip to step 14.
- If the Network Management port is required for remote IP connection to the ISDS ALOM port, then continue with step 8.

8 Complete the following steps to configure the Network Management port.

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

b To set the IP address of the Network Management port, type **set /SP/network pendingipaddress=[xxx.xxx.xxx]** and then press **Enter**.

Notes:

– Replace [xxx.xxx.xxx] with the IP address for the Network Management port.

– Refer to the approved network design drawing for IP-addressing

information.

c To set the Default Gateway for the Network Management 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 or router.

d To set the Network Mask for the Network Management 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 Network Management port.

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

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

g To display the current Network Management 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 8g.

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

j To display the current Network Management 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

9 Connect an Ethernet cable from the Network Management port on the back of the Sun Netra T5440 to the appropriate network hub, switch, or router.

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

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

12 Type **exit** and then press **Enter** to log out from the Network Management port.

Note: The Network Management port is not used to install the ISDS software.

13 Go to ***Installing ISDS Software Onto the Sun Netra T5440 Server*** (on page 24).

14 Complete the following steps if you do not plan to use the Network Management port.

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

   b To disable the Network Management port, type **set /SP/network state=disabled** and then press **Enter**.

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

15 Go to *Installing ISDS Software Onto the Sun Netra T5440 Server* (on page 24).

Installing ISDS Software Onto the Sun Fire V445 or V890 Server

Complete the following steps to install the ISDS software onto the Sun Fire V445 or V890 server.

Important:

- Be certain that there are no network cables installed or connected to the ISDS at this time.
- Be sure that the keyboard, mouse, and monitor are connected to the ISDS.

1 Choose one of the following options to power up the server:

   - To power up the Sun Fire V890 server, follow these instructions.
     a If necessary, turn the key switch to **|**.
     b Press the power button on the front of the server.
   - To power up the Sun Fire V445 server, press the power button just to the right of the **OK** light.

2 When the system displays **Boot device**, go to step 3.

   Note: It may take as long as 5 minutes for the system to display **Boot device**.

3 Press the **Stop** and **A** keys simultaneously. The ok prompt appears.

4 Insert the system release DVD into the DVD drive of the ISDS server.

   Note: Ignore any Solaris prompts that might appear when you first boot the system.

   Important: The system release DVD defines the system configuration information automatically (e.g., standard IP interface, time zone, default root password, etc.). Do *not* respond to the system information questions that automatically appear.

5 At the ok prompt, type **boot cdrom - install** and then press **Enter**.

Results:

- The server boots from the ISDS system release DVD.
- The Solaris Jump Start window opens.
- The ISDS software installs.

  Notes:

  – The installation process can take up to 2 hours for the Sun Fire V445 server, and up to 4 hours for the Sun Fire V890 server.

  – A console window may appear during the installation. You can ignore it.

  Important: Refer to ISDS Initial Installation Disk Formatting Issue if the **Unable to read Disk geometry** error message appears.
- The CDE Login window appears when the software has finished installing.

  Important: The DNCS login prompt may also appear, but do not log in until the CDE Login window appears.

6 Examine your appropriate set of release notes to determine whether you need to install any ISDS patches now. If you have no patches to install, go to ***Configure the ISDS Server*** (on page 30).

Installing ISDS Software Onto the Sun Netra T5440 Server

Complete the following steps to install the ISDS software onto the Sun Netra T5440 server.

Important: Be certain that the monitor, keyboard and mouse are NOT connected to the server and ensure there are no network cables installed or connected, except for the TED, to the ISDS server at this time. The network cable between the TED and the ISDS must be connected prior to the software installation to ensure any necessary TED software updates are installed.

1 At this point you should be connected to the ISDS ILOM serial management port with the HyperTerminal application and at the ILOM prompt, "**->**".

2 Type **stop /SYS** and then press **Enter** to ensure that the system is not running. A confirmation message appears.

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

4 Wait 2 minute and then type **show /SYS power_state** and the press **Enter**. The system returns the status of the system.

Note: The show /SYS result at times does not include all of the data. Repeat this step if power_state is not returned in the output.

5 Is the status of the power_state set to Off?

- If **yes**, continue with step 6.
- If **no**, wait 2 minutes and repeat steps 2 through 5.

6 Disconnect the monitor, keyboard and mouse if they are still connected to the ISDS.

7 Disconnect any network cables from the ISDS, if necessary.
Note: The ILOM network cable can remain connected.

8 Type **set /SYS keyswitch_state=diag** and then press **Enter**. This command sets the virtual key switch to diagnostic mode in order to help verify that there are no hardware or system faults during system startup.

9 To start the system, type **start /SYS** and then press **Enter**. A confirmation message appears.

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

11 Type **start /SP/console** and then press **Enter** to switch to the system console to monitor the Power On Self Test (POST) output. A confirmation message appears.

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

13 Monitor the POST output and verify that no errors are reported during the system startup. Wait for the **Select a Language** prompt or the **ok** prompt to appear.

Note: Contact Cisco Services if errors are reported during system startup.

14 Type **# .** to switch back to the ILOM. The ILOM prompt appears.

Note: Do not press Enter after typing **# .**.

15 Type **set /SYS keyswitch_state=normal** and then press **Enter** to set the virtual key switch to normal.

16 Type **start /SP/console** and then press **Enter** to switch to the system console. The **Are you sure you want to start SP/console?** message appears.

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

18 Press **Enter** again. The **ok** prompt appears.

19 Has the **ok** prompt appeared?

- If **yes**, go to step 21.
- If **no**, continue with step 20.

20 Complete the following steps to access the **ok** prompt.

a Send a *break* to the console by pressing the **Ctrl** and **Break** keys simultaneously for the HyperTerminal, or the **Ctrl** and **b** keys simultaneously for most other terminal emulators.

Note: You may also have to press Enter once in order to see the continue,

sync, reboot, and halt options.

b Type **r** and press **Enter**. The system reboots.

c Wait until the **Ethernet address … Host ID: …** message appears and then repeat step 20a in order to send another break to the console. The **ok** prompt appears.

21 Follow these instructions to set the input and output device to keyboard and monitor respectively.

a Type **setenv input-device keyboard** and then press **Enter**.

b Type **setenv output-device screen** and then press **Enter**.

22 Connect the keyboard, monitor, and mouse (KVM) to the server.

23 Insert appropriate ISDS System Release DVD into the DVD drive of the server.

24 At the ok prompt, type **boot cdrom - install** and then press **Enter** to begin the software installation process.

25 Did the server accept the ISDS System Release DVD?

- If **yes**, go to step 26.
- If **no**, follow these instructions.

a Type **reset-all** and then press **Enter** to restart the OpenBoot environment. The console switches to the keyboard and monitor.

b Press the **Stop** and **a** keys simultaneously. The **ok** prompt appears.

c Insert appropriate ISDS System Release DVD into the DVD drive of the server.

d Type **boot cdrom - install** and then press **Enter** to begin the software installation process.

Note: The OpenBoot environment may display a message that it cannot open the boot device. You can ignore this message.

26 Monitor the software installation process.

Results: The following events should occur:

- The server boots from the ISDS System Release DVD.
- The system will return the following prompt.

```
- The Solaris Installation Program ----
  The Solaris installation program is divided into a
series of short sections where you'll be prompted to
provide information for the installation. At the end of
each section, you'll be able to change the selections
you've made before continuing.
----------------------------------------
    F2_Continue    F6_Help
```

Note: The system will prompt you for the function keys if you are using the

KVM connected to the ISDS, or will prompt for Esc plus a number if you are using a terminal connection. The following steps and examples will use the Esc plus number method for entering responses.

27 Type **Esc 2** to continue. The system returns the Identify This System screen.

Example:

```
- Identify This System -----------------
  On the next screens, you must identify this system as
networked or non-networked, and set the default time zone
and date/time.
  If this system is networked, the software will try to
find the information it needs to identify your system; you
will be prompted to supply any information it cannot find.

  > To begin identifying this system, press F2.
----------------------------------------
    Esc-2_Continue    Esc-6_Help
```

28 Type **Esc 2** to continue. The system returns the Name Service screen.

Example:

```
- Name Service --------------------------------
  On this screen you must provide name service information.
Select the name service that will be used by this system,
or None if your system will either not use a name service
at all, or if it will use a name service not listed here.
  > To make a selection, use the arrow keys to highlight
the option and press Return to mark it [X].
      Name service
      ------------
      [X] NIS+
      [ ] NIS
      [ ] DNS
      [ ] LDAP
      [ ] None
----------------------------------------
Esc-2_Continue    Esc-6_Help
```

29 Arrow down to "None" and press the spacebar. None is selected for the Name service.

30 Press **Esc 2** to continue. The Name service confirmation screen is returned.

Example:

```
- Confirm Information -------------
  > Confirm the following information.  If it is correct,
press F2; o change any information, press F4.
    Name service: None
-----------------------------------
Esc-2_Continue    Esc-4_Change    Esc-6_Help
```

31 Press **Esc 2** to continue. The system returns the Subnet screen.

Example:

```
- Subnet ---------------------------
  On this screen you must specify whether this system is
part of a subnet. If you specify incorrectly, the system
will have problems communicating on the network after you
reboot.
  > To make a selection, use the arrow keys to highlight
the option and press Return to mark it [X].
      System part of a subnet
      ----------------------
      [X] Yes
      [ ] No
---------------------------------
Esc-2_Continue    Esc-6_Help
```

32 Arrow down to "No" and press Esc 2 to continue. The Subnet confirmation screen is returned.

Note: The network configuration will be defined for ISDS later in this guide.

Example:

```
- Confirm Information -------------
  > Confirm the following information.  If it is correct,
press F2; to change any information, press F4.
    System part of a subnet: No
---------------------------------
Esc-2_Continue    Esc-4_Change    Esc-6_Help
```

33 Press **Esc 2** to continue. The Software installation continues.

34 Monitor the completion of the software installation.

- The ISDS software installs.

  Note: The installation process may take more than two hours and a console window may open during installation. You can ignore the console window.

  Important: Refer to ***ISDS Initial Installation Disk Formatting Issue*** (on page 269) if the Unable to read Disk geometry error message appears.

- The CDE Login window appears on the monitor when the software has finished installing.

  Important: The dncs login prompt may also appear. Do not log on until the CDE Login window appears.

35 Examine your appropriate set of release notes to determine whether you need to install any ISDS patches now. If you have no patches to install, go to ***Configure the ISDS Server*** (on page 30).

Configure the ISDS Server

Complete the following steps to configure the IP interfaces of the ISDS server.

Note: The CDE Login window should be displaying on the server.

1 Obtain the necessary network configuration information from the network administrator for the site's OAM&P network interface.

Example: Obtain the following information:

Interface hostname: _____

IP address: _____

Network Mask: _____

Gateway Address: _____

2 Log on to the ISDS server as **root** user.

Results:

- The desktop environment starts.

  Note: After you log on, the screen and the monitor may no longer be synchronized. If this is the case, press the **Menu** button on the right side of the monitor. Then, click **Position** and **Auto-Adjust** to correct the alignment.

- A File Manager window opens because the system release DVD is still in the DVD drive.

3 Close the File Manager window.

4 Open an xterm window on the ISDS server.

5 Type **tail -20 /var/sadm/system/logs/dncs_S99appservInstall.log** and then press **Enter**. The system displays the last 20 lines of the dncs_S99appservInstall.log file.

6 Does the log file display the **appdb database missing appDbVersion in mc_config. Aborting ...** message?

- If **yes**, follow these instructions.

  a Type **su - dncs** and then press **Enter**.
  b Type **dbaccess appdb /dvs/appserv/sqlfiles/appserv/dbVersion.sql** and then press **Enter**.
  c Type (as root user) **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**.
  d After the ISDS server reboots, repeat step 5 and ensure that the installation was successful.

- If **no**, continue with step 7.

7 If necessary, open an xterm window on the ISDS.

8 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**.

9 Choose one of the following options, based upon the type of ISDS server:

- If you are installing ISDS software on the Sun Fire V445 server, go to step 10.
- If you are installing ISDS software on the Sun Fire V890 server, go to step 11.
- If you are installing ISDS software on the Sun Netra T5440 server, go to step 12.

10 Follow these instructions for the Sun Fire V445 server.

a Type **cat /etc/hostname.bge0** and then press **Enter** to verify that the hostname.bge0 entry is **dncs**.

b Type **cat /etc/hostname.bge1** and then press **Enter** to verify that the hostname.bge1 entry is **dncsatm**.

c Type **echo [hostname] > /etc/hostname.bge2** and then press **Enter** to name the ISDS OAM&P network interface.

Note: Replace [hostname] with the OAM&P interface hostname.

Example: dncseth

d Type **ifconfig bge2 plumb** and then press **Enter** to connect to the site's OAM&P network.

e Go to step 13.

11 Follow these instructions for the Sun Fire V890 server.

a Type **cat /etc/hostname.eri0** and then press **Enter** to verify that the hostname.eri0 contains **dncs**.

Note: Edit the /etc/hostname.eri0 file only if necessary.

b Type **cat /etc/hostname.ge0** and then press **Enter** to verify that the hostname.ge0 file contains dncsatm.

Note: Edit the /etc/hostname.ge0 file only if necessary.

c Type **echo [hostname] > /etc/hostname.ce0** and then press **Enter** to name the ISDS OAM&P network interface.

Note: Replace [hostname] with the OAM&P interface hostname.

Example: dncseth

d Type **ifconfig ce0 plumb** and then press **Enter** to connect to the site's OAM&P network.

e Go to step 13.

12 Follow these instructions for the Sun Netra T5440 server.

a Type **cat /etc/hostname.nxge0** and then press **Enter** to verify that the hostname.bge0 entry is dncs.

b Type **cat /etc/hostname.nxge1** and then press **Enter** to verify that the hostname.bge1 entry is dncsatm.

c Type **echo [hostname] > /etc/hostname.nxge2** and then press **Enter** to name the ISDS OAM&P network interface.

Note: Replace [hostname] with the OAM&P interface hostname.

Example: dncseth

d Type **ifconfig bge2 plumb** and then press **Enter** to connect to the site's OAM&P network.

13 Open the **/etc/hosts** file in a text editor.

14 Add to the /etc/hosts file the following entries:

a Add the following line for the OAM&P network interface:
[IP Address] [hostname]

Note: Replace [IP Address] and [hostname] with the IP address and hostname of the OAM&P network interface.

b Add any other entries as necessary for this specific system. For example, add the IP address and hostname for any PCG that will be configured on this ISDS.

Note: Save and close the /etc/hosts file when you are finished.

15 Type **echo [gateway_IP_address] > /etc/defaultrouter** and then press **Enter** to add the default gateway IP address to the /etc/defaultrouter file.

Note: Replace [gateway_IP_address] with the IP address of the STB network router to which the ISDS is connected.

16 Open the /etc/inet/netmasks file in a text editor.

17 Modify the default subnet mask values only if necessary for this specific system. Add an entry for the OAM&P network interface. Add any other entries as necessary for this specific system.

Examples:

192.168.1.0 255.255.255.0

10.253.0.0 255.255.192.0

[OAM&P network] [OAM&P subnet mask]

Note: Be sure to save the file when you are finished.

18 Reconnect all network cables to the ISDS.

19 Type **shutdown -g0 -y -i6** and press **Enter** to reboot the ISDS and implement the IP changes. The ISDS reboots and the CDE login prompt appears.

20 Log on as **root** user and open an xterm window.

21 Type **ifconfig -a** and press **Enter**. From the output, verify that all IP interfaces were created properly.

22 Complete the following steps to create the persistent static routes on the ISDS.

a Type **/usr/sbin/route -p add net [destination] [gateway]** and press **Enter** for each IP destination required for this ISDS.

Note: We recommend that all of these routes be added to a text file and retained for future reference. One option is to list all of the "route add" commands in a text file, add a note next to each explaining what it does, and then execute the file as a shell script to add all of the routes.

Example: /usr/sbin/route -p add net 192.168.64.0/24 172.40.90.254 # NMS

b Type **cat /etc/inet/static_routes** and press **Enter**.

c Verify that all of the static routes are listed properly in the output and correct any route entries if necessary.

d Add the persistent static routes to the **/etc/rc2.d/S85SAspecial** file, as well.

23 Ping all appropriate network elements to verify connectivity.

Modifying the Solaris System Information

The ISDS software installation scripts automatically configure the Solaris system information. Complete the following steps to update the Solaris system information as necessary.

1 Type **grep TZ /etc/default/init** and then press **Enter**. The system displays what timezone is currently set.

Example: TZ=US/Eastern

2 Is the timezone set accurately?

- If **yes**, go to the next procedure in this chapter.
- If **no**, follow these instructions:

a Type **cd /usr/share/lib/zoneinfo** and then press **Enter**.

b Type **ls -ltr** and then press **Enter** to display the contents of the directory.

c Look for your appropriate region and then use the cd command to change directories into that region.

Example: cd US

d Type **ls -ltr** and then press **Enter** to display the contents of the directory.

Example:

```
$ ls -ltr
total 30
-rw-r--r--   3 root     bin          125 Jan 21  2005
Samoa
-rw-r--r--   2 root     bin          130 Jan 21  2005
Hawaii
-rw-r--r--   2 root     bin          130 Jan 21  2005
```

```
Arizona
-rw-r--r--   3 root     bin         1017 Nov 17  2008
Pacific-New
-rw-r--r--   3 root     bin         1017 Nov 17  2008
Pacific
-rw-r--r--   4 root     bin          877 Nov 17  2008
Mountain
-rw-r--r--   2 root     bin          811 Nov 17  2008
Michigan
-rw-r--r--   3 root     bin          869 Nov 17  2008
Indiana-Starke
-rw-r--r--   2 root     bin         1267 Nov 17  2008
Eastern
-rw-r--r--   4 root     bin          606 Nov 17  2008
East-Indiana
-rw-r--r--   2 root     bin         1279 Nov 17  2008
```

```
Central
-rw-r--r--   3 root     bin          858 Nov 17  2008
Aleutian
-rw-r--r--   2 root     bin          861 Nov 17  2008
Alaska
```

e Open the /etc/default/init file with a text editor.

f Edit the **TZ** value so that it contains the appropriate timezone.

g Save and close the file.

Note: This change will not take effect until the system is rebooted, later in this chapter.

Changing Default User Passwords and Password Expiration Settings

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

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 and the ISDS, respectively.

The root, dncsftp, 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 ISDS. The informix, dncsSSH, pcgrequest, and pcgscp users do not have password-aging, by default.

CAUTION:

The ISDS, or components within the ISDS, will become unstable if the password expires for any of the default users (root, dncs, dncsSSH, informix, dncsftp, easftp, pcgrequest, and pcgscp). The ISDS system administrator MUST ensure that these passwords do NOT expire. It is imperative that password-aging be disabled unless the ISDS system administrator ensures these account passwords do not expire.

1 If necessary, open an xterm window on the ISDS 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 9. No numbers should appear. If numbers appear after any account name, repeat steps 8 and 9 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.

Creating a New DNCS Administrator Account

For security purposes, the root user should not be used for day-to-day CDE access to the ISDS. A user other than the Solaris system administrator should be used for the vast majority of ISDS activities. The ISDS software package includes a command line script for creating new Solaris accounts on the ISDS. The dncs role must be used for executing the vast majority of ISDS commands. You cannot access the ISDS directly using the dncs role. You must first log on to the system using a DNCS Administrator account and then switch to the dncs role. Only DNCS Administrator accounts and root have the right to switch to the DNCS role. See *ISDS Security Enhancements Instructions* (part number 4027701) for more information on ISDS accounts and account management.

Follow these instructions to create a new DNCS Administrator account on the ISDS.

1 From an xterm window on the ISDS, type the following command and press **Enter**.

```
/dvs/dncs/etc/create_users
```

2 Type **3** (for Add Administrator) and then press **Enter**.

3 Type the name of the new DNCS Administrator user and then press **Enter**.

Notes:

- The user name must be between 6 and 8 characters.
- The user name can contain alpha and numeric characters, but must not contain any special characters.

4 Type **y** and then press **Enter** at the **Do you wish to continue adding this user (Y/N)** message.

5 When prompted, type a password for the new user and then press **Enter**.

Note: The password is supplied in the deployment document.

6 When prompted, re-type the password for the new user and then press **Enter**.

Important Notes About the New DNCS Administrator Account

The standard .profile generated by the create_users script is very generic. The following are suggested changes to new .profile file generated by the create_users script. You can add these lines to the /export/home/<newuser>/.profile file using a text editor. Replace <newuser> with the DNCS Administrator username created in the previous procedure.

```
export PATH=$PATH:/dvs/dncs/bin:/dvs/dncs/Utilities
export PS1='$LOGNAME'@`hostname`:'$PWD>'
set -o vi
```

Notes:

- These lines serve the following purposes:
  - Allow you to execute files that exist in the /dvs/dncs/bin/ and /dvs/dncs/Utilities/ directories without having to fully qualify the path of the file
  - Provide you with the logon name and hostname of the system you are on, as well as the path you are in on the command line
  - Enable vi commands for the command line
- Installation engineers may also want to add the following line to the .profile file of the dncs user:

```
export DODSP=y
```

Copying the Backup and Restore Scripts From the SR DVD to the ISDS

Complete the following steps to copy the entire ISDS backup and restore scripts directory from the latest installation DVD to the ISDS file system.

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

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
cp -R /cdrom/cdrom0/s3/backup_restore /usr/local and press **Enter** to copy the /cdrom/cdrom0/backup_restore directory to the /usr/local/backup_restore directory.

   Note: The command prompt returns after a few moments.

Using the Middle Mouse Button

Important: The middle mouse button on CDE provides a menu of options to execute such activities as opening the Administrative Console, starting and stopping the ISDS, and opening an xterm window. You will be prompted for the dncs role password in a console window if you select any of these options as a DNCS Administrator. The root user will not be prompted for a password. You will be denied the ability to execute any of the options if you select them as a DNCS Operator or Regular Solaris user.

Leave any console window open, that is automatically opened, if you select Administrative Console, DNCS Monitor, or App Serv Monitor until after you close the Administrative Console, DNCS Monitor, or App Serv Monitor UI, respectively. Closing this console window will result in closing the UI that was opened. The console window that is automatically opened if you select Start/Stop DNCS or Start/Stop App Serv can be closed after the selected activity is complete.

Set Up the Network Time Protocol on Sun Solaris Servers and Clients

Configuring NTP on the ISDS Server

By default, the ISDS is configured to use the internal clock for timing. Follow these instructions to configure the ISDS to obtain timing from an external NTP server, if desired. Obtain the primary and any secondary NTP source IP addresses from the system operator.

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 **vi /etc/inet/ntp.conf** and then press **Enter**.

4 Replace the contents of the ntp.conf file with the following:

   server [Primary Time Source IP Address] prefer
   server [Secondary Time Source IP Address]
   server 127.127.1.0
   driftfile /etc/ntp.drift

5 Save and close the ntp.conf file.

6 Type **vi /etc/ntp.drift** and then press **Enter**.

7 Replace the contents of the ntp.drift file with: **0.0**

8 Save and close the ntp.drift file.

9 Follow these directions to stop and restart the NTP service.

   a Type **svcadm disable ntp** and press **Enter**. The ntp service stops.

   b Type **svcadm refresh ntp** and press **Enter**. The ntp service loads the configuration.

   c Type **svcadm enable ntp** and press **Enter**. The ntp service starts.

10 Type **ntpq -p** and then press **Enter** to check the status of the NTP.

   Result: You should see output similar to the following:

```
# ntpq -p
remote           refid          st t when poll reach   delay   offset  disp
==============================================================================
*PrimNTPSvr     192.133.225.12   3 u   53   64   37    0.37   -2.320  438.31
 LOCAL(0)        LOCAL(0)        5 l   49   64   37    0.00    0.000  438.35
```

Note: It takes the NTP daemon a few minutes to decide which server will be the primary server after the ntp server is restarted. An asterisk appears next to the source that is being referenced.

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

Prepare the /dvs/resapp Directory

In this procedure, you will create a directory on the ISDS server in which to store image files. Then, you will copy image files from a CD to this newly created directory.

Creating the /dvs/resapp Directory

Complete the following steps to create the /dvs/resapp directory on the ISDS server.

1. If necessary, open an xterm window on the ISDS server.
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 the following command and press **Enter**. The system creates the /dvs/resapp directory.
   ```
   mkdir /dvs/resapp
   ```
4. Type the following command and press **Enter**.
   ```
   mkdir /dvs/resapp/EMMs
   ```
   Note: Some installation engineers recommend that this directory be created for storage and easy reference for EMMs.
5. Type the following command and press **Enter**. The system establishes the proper directory permissions.
   ```
   chown dncs:dncs /dvs/resapp
   ```
6. Type the following command and press **Enter** to set the desired access mode of the file.
   ```
   chmod g+w /dvs/resapp
   ```
7. Type **exit** and then press **Enter** to log out the root user.

Copying Resident Application Images to the /dvs/resapp Directory

In this procedure, you will copy the DHCT resident application images from a CD to the newly created /dvs/resapp directory.

Important:

- Be sure the files that you copy have the required ownership permissions values. The ISDS expects these files to have dncs:dncs ownership and read/write permissions.
- Verify that you have the most current version of the resident application images by referencing the IPTV Wiki. The address is http://wikicentral.cisco.com/confluence/display/PROJECT/ISDS+Labs+-+Trials

1. Insert the CD that contains the resident application images into the CD drive of the ISDS server.
2. Type **df -n** and then press **Enter**. A list of the mounted file systems appears.

   Note: The presence of /cdrom in the output confirms that the system correctly mounted the CD.
3. Copy the xsettopip.v##### file, as well as the settop image files, from the CD to the /dvs/resapp directory on the ISDS server.

   Note: The file extension (v#####) pertains to the version number of the file.

Enable Optional and Licensed Features

Contact Cisco Services and ask them to enable the necessary optional and licensed features for you.

Initialize the TED

Complete the following steps in *Transaction Encryption Device 3.0 Installation and Operation Guide* (part number 4031371) to complete the installation of the Transaction Encryption Device (TED) if PowerKEY will be implemented on this ISDS. Verify that you have the Customer CAA CD, Factory Root Certificate Authorization Key CD, and your CAA pass phrase prior to starting these steps. Contact your appropriate account representative if you do not have these items.

Important: Be aware that a Cisco representative must be available to enter the Cisco portion of the CAA pass phrase.

1. Complete the steps in Chapter 2, **Getting Started**, and Chapter 3, **Installing the TED Server**, if the TED hardware has not been physically installed. Skip these chapters if the hardware has already been installed.
2. Complete the **Initialize the PowerKEY CA System** procedures in Chapter 4, **Initializing the TED Server**.

   Important: If any of the steps fail or generate failure messages during this process, attempt the step again. If the error or failure message is persistent, contact Cisco Services.

Enable the TFTP and bootp Services

For security purposes, the TFTP and bootp services are disabled by default. There is a secure and an unsecure method available for installing the PCG application software onto the PCG from the ISDS. The unsecure method requires TFTP. Follow these instructions to enable the TFTP and bootp services, only if required.

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.
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. 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
4. From the root xterm window, if the "#" character was removed, 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. Type **cd /dvs/dncs/etc** and then press **Enter**.
   b. Type **chmod 4550 bootpd** and then press **Enter**.
   c. Type **su - dncs** and then press **Enter**.
   d. Type **dncsControl -start bootpd** and then press **Enter**.
   e. Type **exit** and then press **Enter** to log out of the dncs role.
8. Type **exit** and then press **Enter** to log out the root user.

Enable the FTP Service

For security purposes, the FTP service is disabled by default. FTP is required for EAS, and may be required for certain billing systems. Follow these instructions to enable the FTP service.

Note: Complete this procedure *only* if FTP is required on this system.

1 Is the FTP service required on this system?

- If **yes**, continue with step 2.
- If **no**, you do not need to complete this procedure.

2 If necessary, open an xterm window on the ISDS.

3 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**.

4 Type **inetadm -e svc:/network/ftp:default** and then press **Enter**.

5 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

6 Use a text editor and add the following lines to the /export/home/dncs/.profile file:

 # Source the Local EAS Server IP Address

LOCAL_EAS_IP=<EAS Server IP>; export LOCAL_EAS_IP

Note: Replace <EAS Server IP> with the IP address of the local EAS server.

7 Save and close the file.

8 Type **usermod –d /export/home/easftp –s /bin/sh –c "EAS FTP Account" easftp** and then press **Enter**. The default shell changes to /bin/sh (Bourne shell) for the easftp user.

9 After running step 8, did the system display a message that indicated that the easftp user did not exist?

- If **yes** (the easftp user does not exist), follow these instructions.

a Type **useradd -m -c "EAS FTP Account" -d /export/home/easftp -u 800 -g dncs -s /bin/sh easftp** and then press **Enter**.

b Type **chmod 770 /export/home/easftp** and then press **Enter**.

c Type **passwd easftp** and then press **Enter** to set the password.

Important: The password for the easftp user should never expire. See

Manage User Passwords and Password Expiration Settings (on page 192) for instructions on setting the password accordingly.

- If **no** (the easftp user exists), continue with step 10.

10 Type **grep easftp /etc/passwd** and then press **Enter**.

11 Confirm that the last item in the output string from step 10 is **/bin/sh**.

12 Type **usermod -d /dvs/ftp -s /bin/sh -c "DNCS FTP Account" dncsftp** and then press **Enter**. The default shell changes to /bin/sh (Bourne shell) for the dncsftp user.

13 After running step 8, did the system display a message that indicated that the easftp user did not exist?

- If **yes** (the dncsftp user does not exist), follow these instructions.
  - **a** Type **useradd -m -c "DNCS FTP Account" -d /dvs/ftp -u 900 -g dncs -s /bin/sh dncsftp** and then press **Enter**.
  - **b** Type **chmod 770 /dvs/ftp** and then press **Enter**.
  - **c** Type **passwd dncsftp** and then press **Enter** to set the password.
- If **no** (the easftp user exists), continue with step 14.

14 Type **grep dncsftp /etc/passwd** and then press **Enter**.

15 Confirm that the last item in the output string from step 14 is **/bin/sh**.

Configure SSL/TLS for the BOSS Interface

Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) for the Billing and Order Support System (BOSS) interface is introduced in ISDS 2.3 f2.0.0.8. The BOSS interface is not functional until the necessary TLS/SSL configuration is implemented, or an exception is defined for the IP address of the billing system to allow HyperText Transfer Protocol (HTTP).

Refer to ***TLS/SSL for the BOSS Interface*** (on page 209) for detailed instructions on configuring the BOSS for plain HTTP or for implementing TLS/SSL.

Northbound SNMP V3 User and Pass Phrase Management

To add additional network security, the Northbound SNMP interface on the ISDS supports only SNMP version 3. User names and phrases are used to limit access to the Northbound SNMP interface on the ISDS.

The ISDS is delivered with a user name, an authentication pass phrase, and a privileged pass phrase. Please contact your appropriate account representative for these values.

Install Service Packs or Patches

Use this time to install any service packs or patches that may also need to be installed as part of the ISDS software installation. Refer to the readme file loaded onto the DVD that contains the patch or service pack software for installation instructions.

Check Installed Version Numbers on the ISDS

Follow these instructions to check the installed software versions on the ISDS.

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. If necessary, insert the system release DVD into the DVD drive of the ISDS.
4. From an xterm window on the ISDS, as a dncs administrator user, type the following command and press **Enter**.
   `/cdrom/cdrom0/s3/sai/scripts/utils/listpkgs -i`
   Notes:
   - Or, some engineers prefer to run the following command:
     `pkginfo -l SAI*`
   - It may take a few minutes for either of these commands to run.

   Result: The system displays a listing of installed packages.
5. Record the version number in the **Actual Results** column of the accompanying table for each package name (**Pkg Name**) listed.

Component	Pkg Name	Expected Results	Actual Results
ISDS Application	SAIisds	f2.2.1.1	
ISDS/App Tools	SAItools	4.2.1.30	
ISDS GUI	SAIgui	f2.2.1.1	
ISDS WUI	SAIwebui	f2.2.1.1	
Solaris Patches	SAIpatch	4.5.0.3	
ISDS Online Help	SAIisdshelp	1.3.1.0	
ISDS Report Writer	SAIrptwrt	r1.0.0.3	
Command 2000	SAIcmd2k	1.0.0.3	
Common platform	SAIcomplat	2.0.0.12	
DBDS Utilities	SAIdbdsutils	6.3.0.12	
PowerKEY CAS Gateway	SAIpcg	v2.1.0.8	
TED	SAIted	3.1.0.3	

6 Do the first two digits of the **Actual Results** match the first two digits of the **Expected Results** for each component in the table in step 5?

Important: The third or fourth number may differ.

- If **yes**, type **eject cdrom** and then press **Enter**.
- If **no**, call Cisco Services and inform them of the discrepancy.

Note: The **Actual Results** may not match the **Expected Results** if you have installed any patches before reaching this procedure.

Start the System Processes

In this procedure, you will start the user interface of the ISDS server, as well as the system processes.

1 In an xterm window, type **dncsStart** and then press **Enter**.

2 Follow these instructions to monitor the restart of the ISDS processes.

   a Type **dncsControl** and then press **Enter**. The Dncs Control window opens.

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

   c Wait until all of the processes display a Current State of **running**.

   Note: You can press **Enter** on the dncsControl utility window a few times to refresh the screen.

   d Follow the onscreen instructions to close the dncsControl window.

3 Verify that all of the processes in the ISDS Control window are in a green state.

4 Did the mgrUIServer process remain in the yellow or red state?

- If **yes**, complete the following steps to restart the http service.

  a Open an xterm window on the ISDS as **root** user.

  b Type **svcadm -v disable -st http** and then press **Enter** to stop the http service.

  c Type **svcadm refresh http** and then press **Enter** to refresh the http service.

  d Type **svcadm -v enable http** and then press **Enter** to restart the http service.

  Note: If the mgrUIServer process does not start within 2 minutes, contact Cisco Services.

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

- If **no**, continue with step 5.

5 Type **cd /dvs/appserv/bin** and then press **Enter**.

6 Type **./appStart** and then press **Enter**.

Note: In rare instances, executing the appStart command will not be successful. If the ./appStart command does not start the processes, use the **snmx appStart.s** command instead.

7 Follow these instructions to monitor the restart of the Application Server processes.

   a Type **. appservSetup** and then press **Enter** to establish the Application Server environment.

   b Type **appControl** and then press **Enter**. The appControl utility window opens.

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

d Wait until all of the processes display a Current State of **running**.

e Follow the onscreen directions to close the appControl utility window.

8 Click **Control**, next to AppServer on the Console Status window. The AppServer Control window opens.

Note: The AppServer Control window should display green indicators.

9 Click **Control** next to ISDS on the Console Status window. The ISDS Control window opens.

10 Monitor the process status until all indicators display green.

Notes:

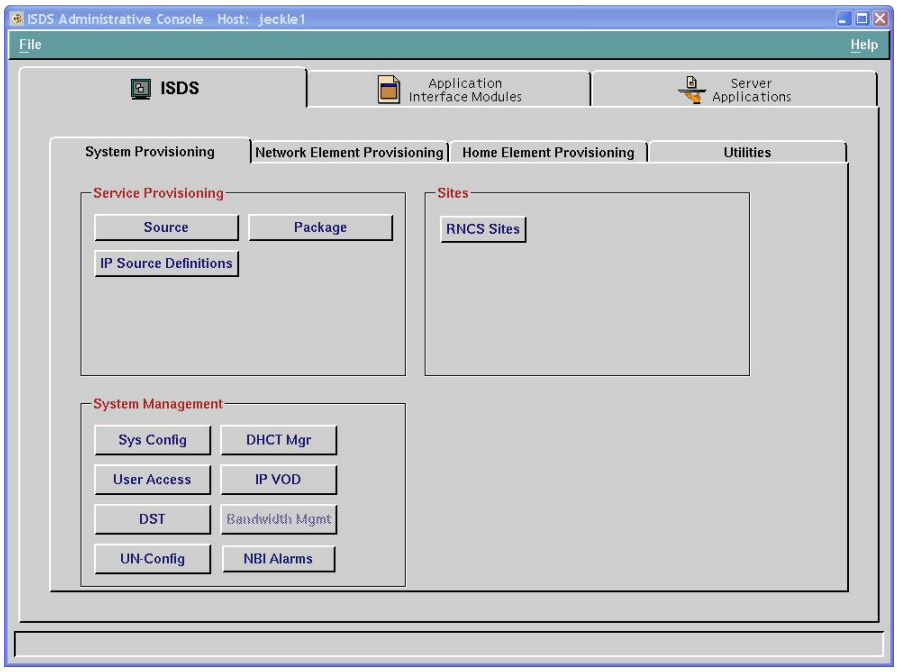
- This may take as long as 10 minutes.
- Contact Cisco Services if any process remains in a yellow or red state.

11 Type **exit** and then press **Enter** to log out of the dncs role.

Configure the dncs Role for Full System Access

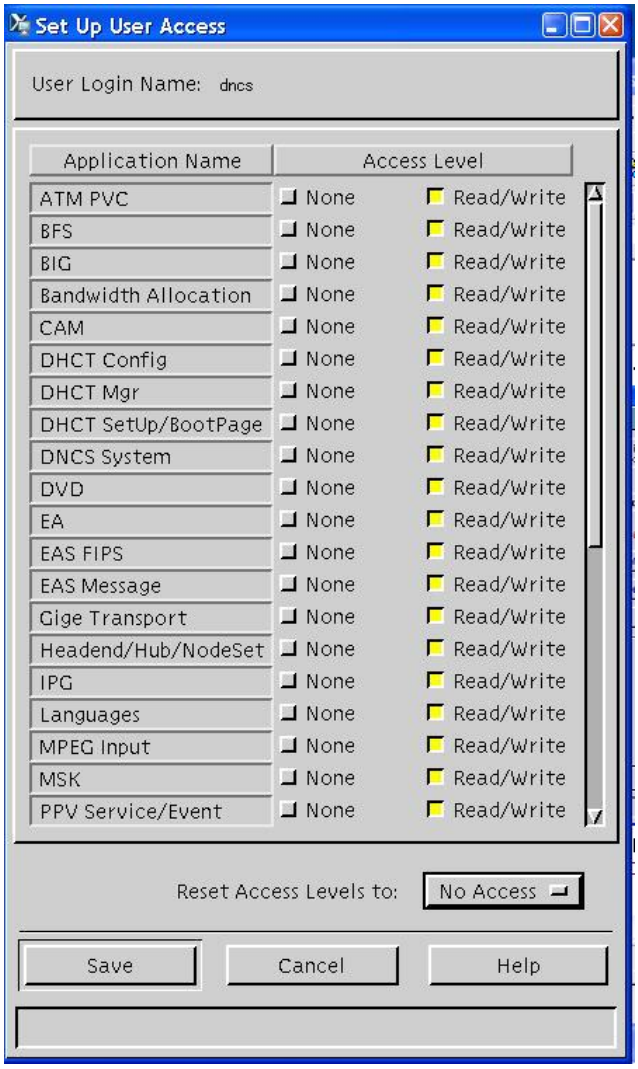
In this procedure, you will configure the dncs user and grant the user full system access.

1 From the ISDS Administrative Console, click the **System Provisioning** tab.



2 Click **User Access** (in the System Management section). The User Access List window opens.

3 Highlight the **dncs** user; then click **File** and select **Open**. The Set Up User Access window opens.



4 Click **No Access** and then select **Full Access** from the drop-down menu to configure the dncs user.

5 Click **Save** and then close the Set Up User Access and the User Access List windows.

Note: You may need to close and then reopen the ISDS Administrative Console in order to see all of these changes.

Check the DNCS Site (Optional)

Complete the procedures in this section only if the Distributed DNCS feature is enabled on the system. Otherwise, skip this procedure and go to the next procedure in this chapter.

Complete the following procedure to verify the IP Address of the DNCS Site. The IP address for the DNCS Site should be the dncsatm interface IP address, which is 10.253.0.1 by default. The DNCS Site entry can be viewed in the RNCS Sites window if the Distributed DNCS feature is enabled on the system. The DNCS Site entry is only accessible through the DNCS database if the Distributed DNCS feature is disabled on the system.

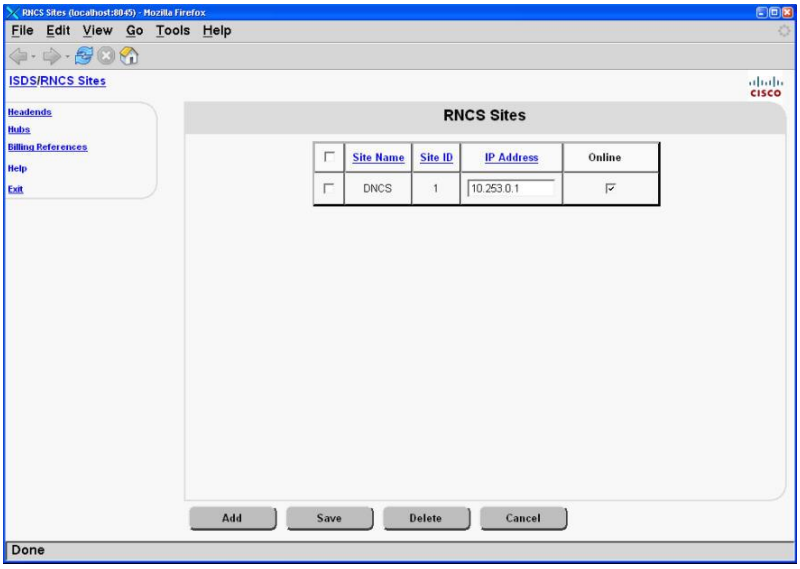
1 From an xterm window on the ISDS, type **grep dncsatm /etc/hosts** and press **Enter**. The IP address and associated hostnames of the dncsatm interface are displayed.

2 Is the Distributed DNCS feature enabled on this system?

- If **yes**, then complete the following steps to check the DNCS Site IP Address using the RNCS Sites window.

  a From the ISDS Administrative Console, click **System Provisioning** tab.

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



  c Does the DNCS Site IP address match the dncsatm IP address?

  - If **yes**, skip to step d.
  - If **no**, change the IP Address for the DNCS Site to match the dncsatm interface IP address and click **Save**. The DNCS Site IP Address is updated.

d Click **Exit**. The RNCS Sites window closes.

- If **no**, then complete the following steps to check the DNCS Site IP address using database commands.
  - **a** Open an xterm window on the ISDS as the dncs role.
  - **b** Type **echo 'select site_ip_address from site_info where site_name="DNCS";' | dbaccess dncsdb** and press **Enter**. The DNCS Site IP address appears.
  - **c** Does the DNCS Site IP address match the dncsatm IP address?
    - If **yes**, skip to step d.
    - If **no**, then type
      echo 'update site_info set site_ip_address="[IP Address]" where site_name="DNCS" ;' | dbaccess dncsdb and press **Enter**. The system returns **1 row(s) updated** to indicate a successful update of the IP address.
      Note: Replace [IP Address] with the IP Address of the dncsatm interface.
  - **d** Type **exit** to log out of the dncs role.

Rebuild VASP Entries (If the dncsatm or appservatm Interfaces Were Modified)

If the ISDS and integrated Application Server are NOT using the default IP scheme for the ISDS dncsatm and appservatm interface (10.253.0.1), you need to delete and rebuild all of the VASP entries. To do this, follow these instructions.

Note: If RNCS is enabled on this site, the VASP entries for the Application Server may need to be updated to reflect the correct Site ID of 1.

1. Are the ISDS and integrated Application Server using the default IP scheme for the ISDS dncsatm and appservatm interface (10.253.0.1)?
   - If **yes**, skip the rest of this procedure and go to ***Create the Headend*** (on page 64).
   - If **no**, continue with step 2.
2. From the **Network Element Provisioning** tab, click **VASP**. The VASP List window opens.
3. Follow these instructions for each entry on the VASP List window.
   - **a** Double click an entry on the VASP List window. The entry opens.
   - **b** On a sheet of paper, record the **VASP Name** and **ID** for the entry.
   - **c** Click **Cancel** to close the entry.
   - **d** Click to highlight the entry.
   - **e** Click **File** and then select **Delete**. A confirmation message appears.

f Click **OK** to delete the entry

g Repeat steps 3a through 3g for each entry on the VASP List.

Note: The appendix ***Default VASP Values for the ISDS*** (on page 277) contains a listing of default VASP values and may be useful as you access the entries on the VASP List.

4 Follow these instructions to rebuild the VASP entries.

a On the VASP List window, click **File** and then select **New**. The Set Up VASP window opens.

b Using your sheet of paper as a reference, recreate each entry with the same **VASP Name** and **ID**, but use the desired IP address.

c Click **Save**.

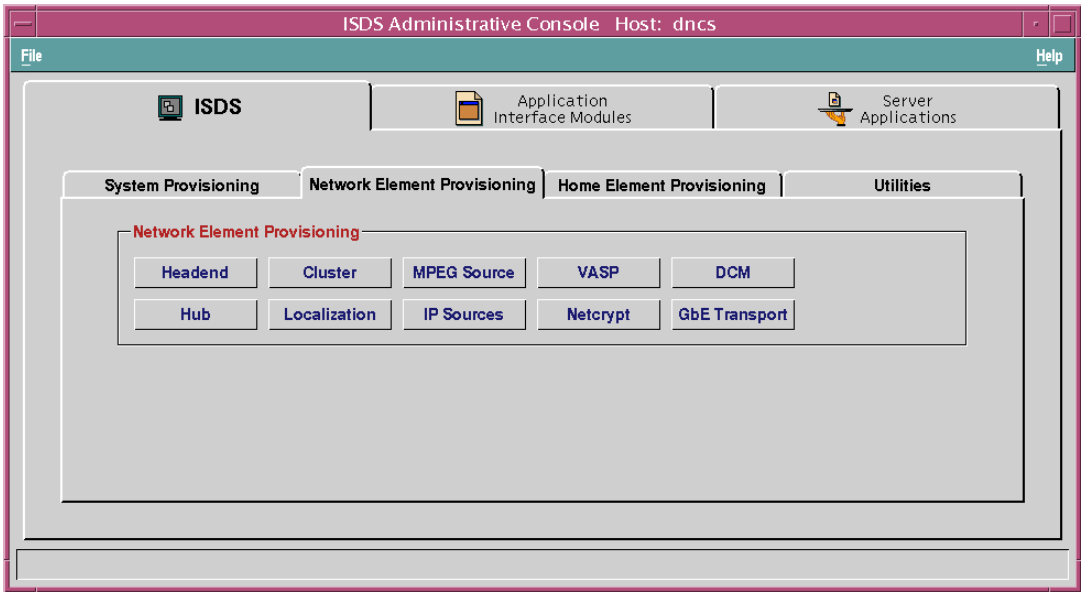
d Repeat steps 4a through 4c to recreate each entry that you wrote on your sheet of paper.

Create the Headend

Complete the following steps to create the headend entry for the ISDS.

Note: It is not necessary to create headends for the RNCS sites at this time. When you do create headends for the RNCS sites, however, refer to *RNCS Installation and Upgrade Instructions* (part number 4021167) for instructions.

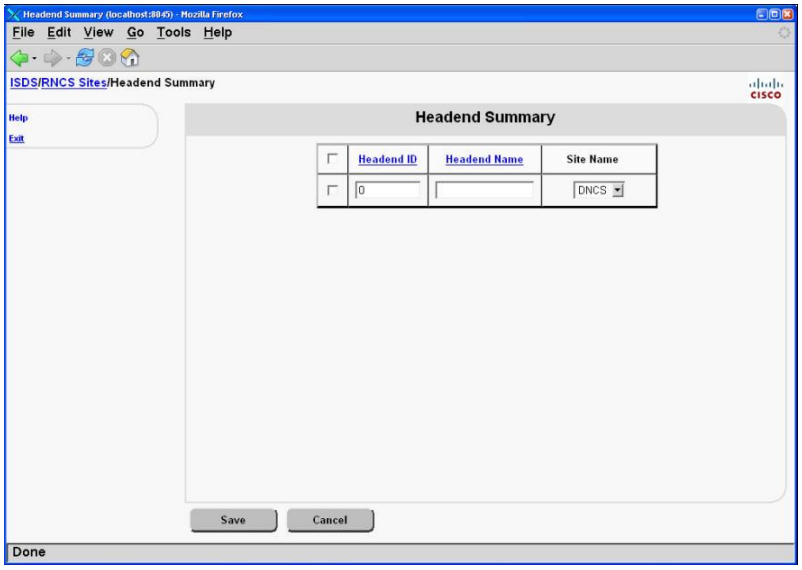
1 From the ISDS Administrative Console, click the **Network Element Provisioning** tab.



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

Note: The Headend Summary window may appear differently for an ISDS that does not have the Distributed DNCS feature enabled.

3 Click **Add**. The Headend Summary window updates to allow for the addition of a new headend.

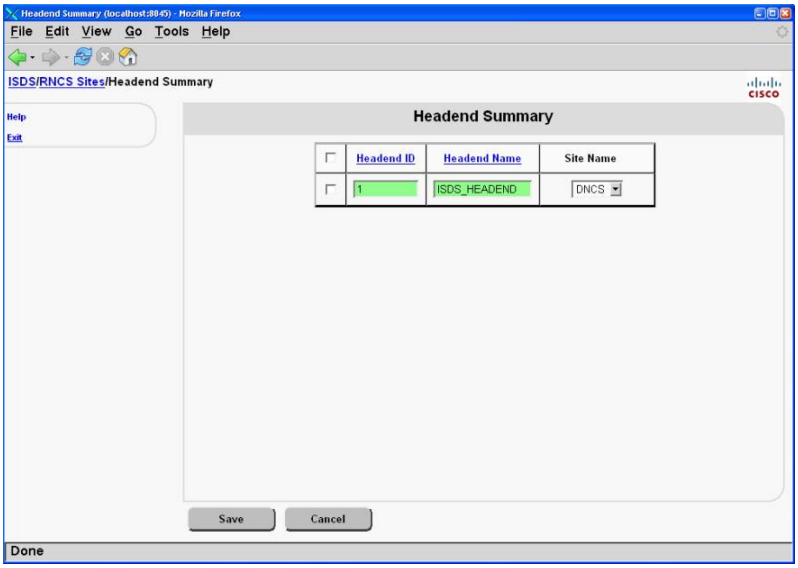


4 Type the **Headend Name** and the **Headend ID**.

Notes:

- The Headend ID must be an integer greater than 0.

- Leave the **Site Name** as **DNCS** for the ISDS headend.



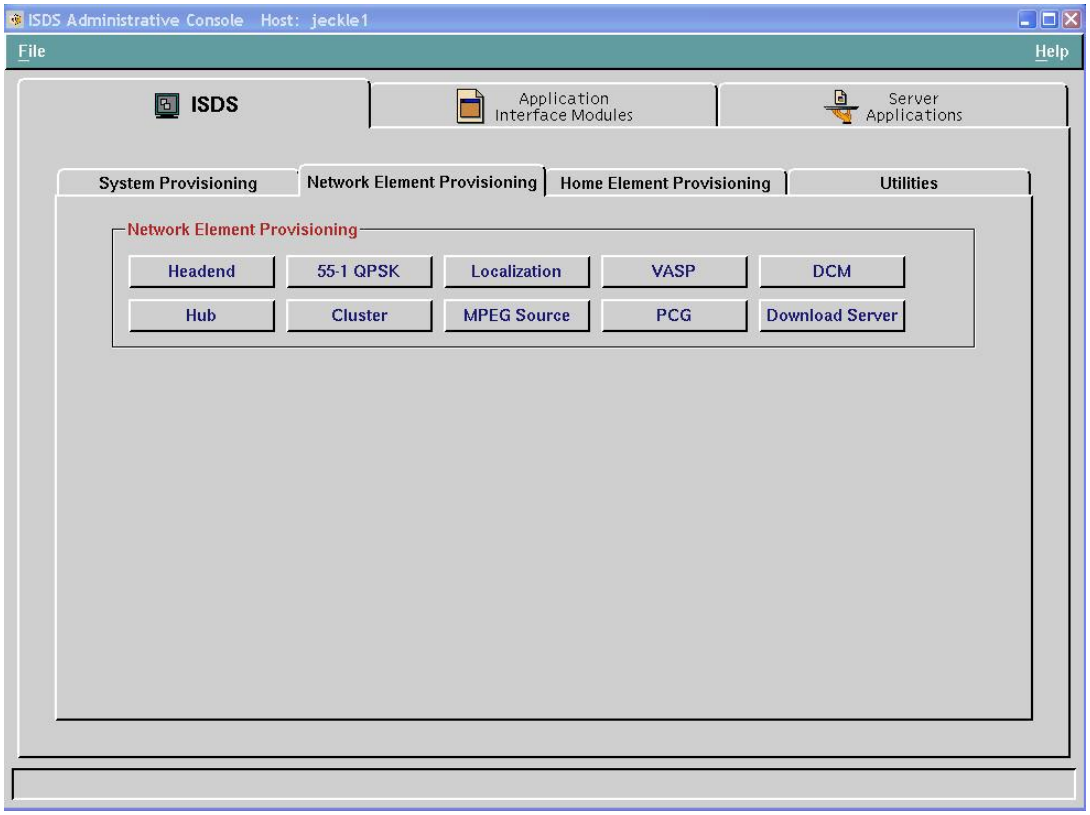
5 Click **Save** and then close the Headend Summary window.

Create a Hub

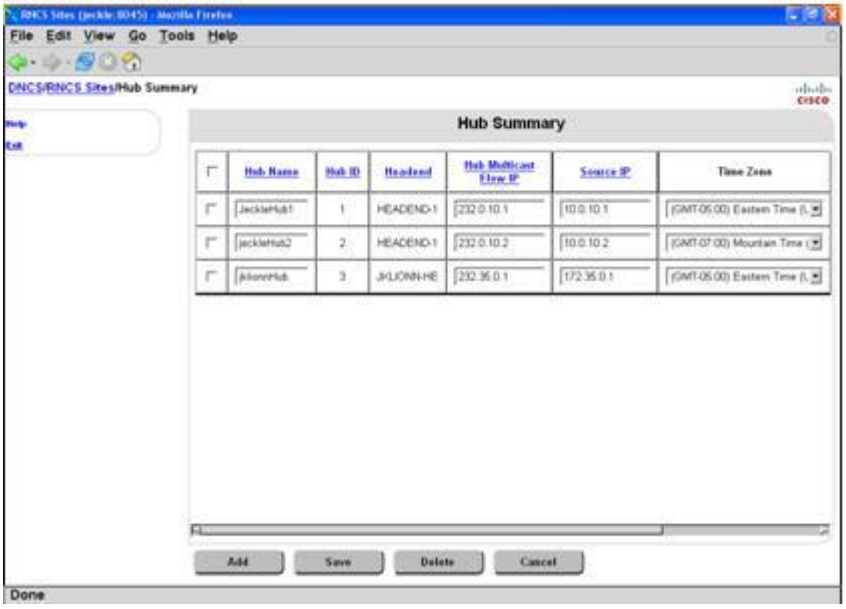
Adding a New Hub Entry

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

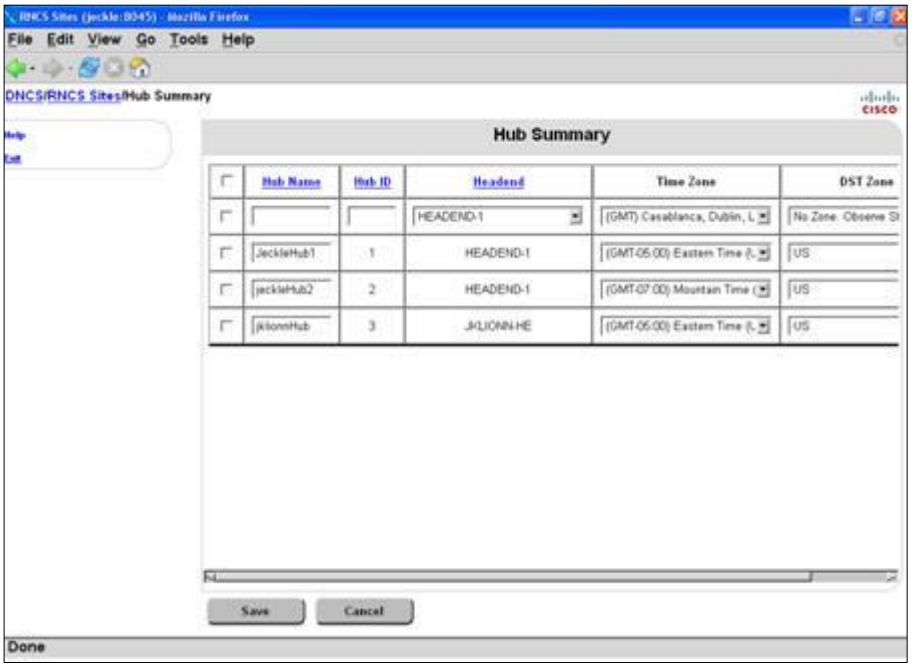
1 From the Application Server Administrative Console, select the **Network Element Provisioning** tab.



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. You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map.
- **Hub ID**—The number you will use to identify this hub. Be sure to use an ID number that is consistent with the numbering scheme used on your network map.

  Example: You might type **11** as a numerical representation for Headend 1, Hub 1.

  Important: You will not be able to modify this field later.
- **Headend**—The headend associated with this hub.
- **Time Zone**—The time zone where this hub is located.
- **DST Zone ID**—The DST Zone ID associated with this hub.

  Note: Refer to *Daylight Saving Time Configuration Guide for an IP Network* (part number 4018286) for complete instructions on using the DST rules feature in a network.

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

6 Click **OK**. The system saves the hub information in the ISDS database and the Hub Summary window updates to include the new hub.

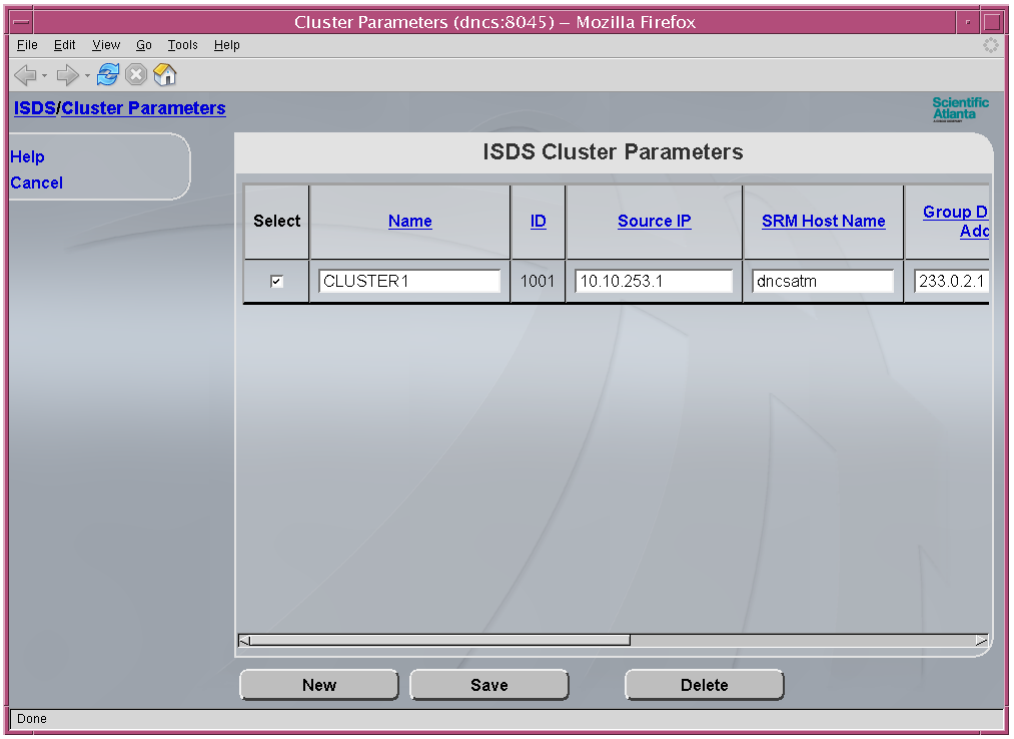
7 If necessary, repeat this procedure from step 3 to add another hub.

Create a Cluster

Note: Complete this procedure only if you are running an IP-only configuration.

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

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



3 Click **New**. A new row opens on the ISDS Cluster Parameters window.

4 Type the new cluster **Name**.

5 Type the dncsatm IP address in the **Source IP** field.

6 Type **dncsatm** in the **SRM Host Name** field.

7 Type the cluster multicast address in the **Group Destination Address** field.

8 Select the hub to which you want to assign this cluster.

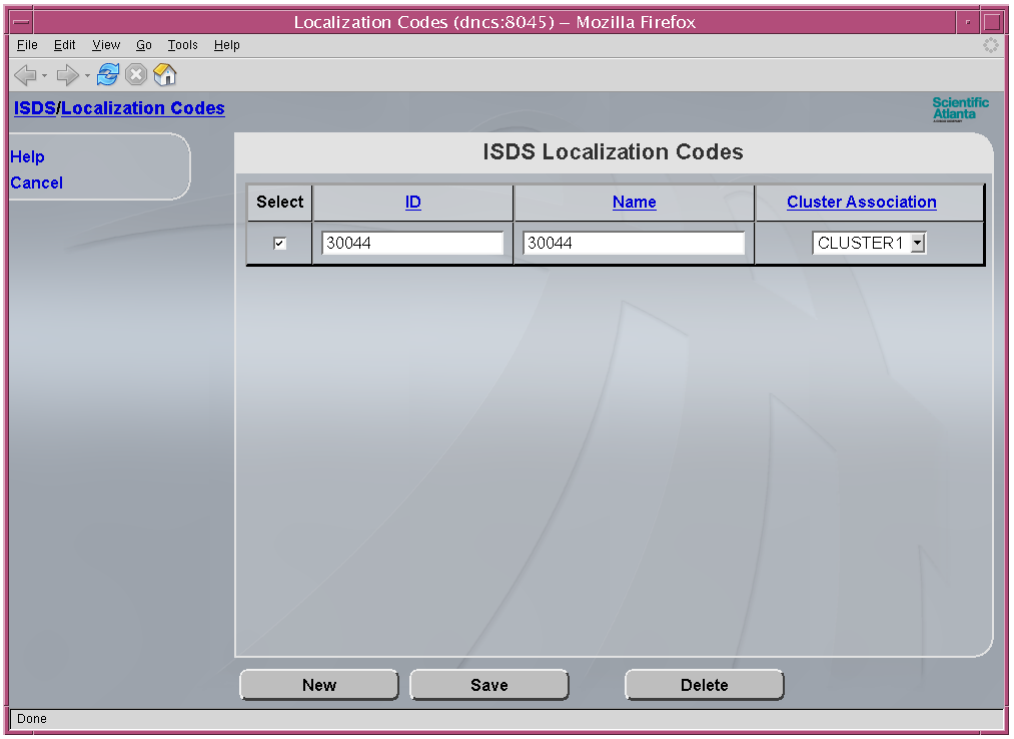
9 Click **Save** and then close the ISDS Cluster Parameters window.

Create Localization

Complete the following steps to configure localization for the ISDS. Without localization, DHCTs will be unable to transmit UNConfig data.

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

2 Click **Localization**. The ISDS Localization Codes window opens.



3 Click **New**. A new row opens up on the ISDS Localization Codes window.

4 Type the Localization ID code into the **ID** field.

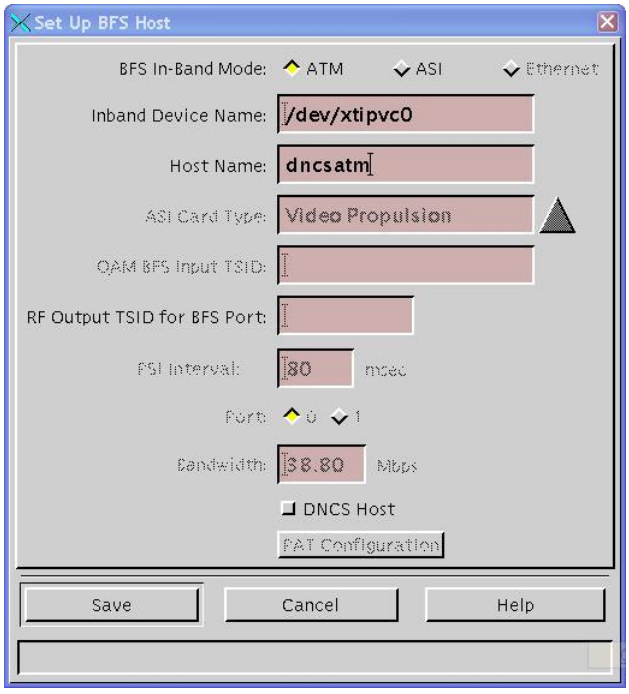
5 Type the Localization name into the **Name** field.

6 Select the appropriate cluster from the **Cluster Association** field.

7 Click **Save** and then close the ISDS Localization Codes window.

Add the BFS Host

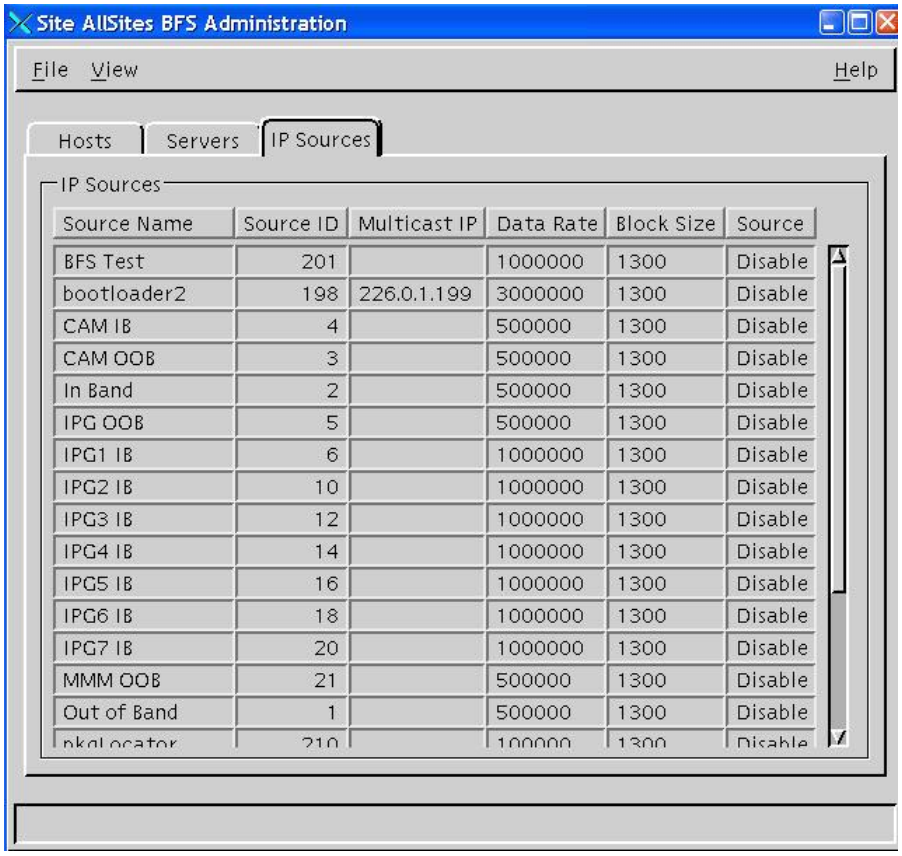
1. From the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Admin**. The BFS Administration window opens.
3. Double-click the **DNCS** site. The Site DNCS BFS Administration window opens.
4. Click **File** and then select **New**. The Set Up BFS Host window opens.



5. Click **ATM** in the **BFS In-Band Mode** field.
6. Type **dncsatm** in the **Host Name** field.
7. Click **Save** and then close the Set Up BFS Host window and the BFS Administration window.

Build BFS Sources

1. From the **Application Interface Modules** tab on the ISDS Administrative Console, click **BFS Admin**. The BFS Admin Sites window opens.
2. Click **File** and then select **All Sites**. The Site AllSites BFS Administration window opens.
3. Click **IP Sources**. The window updates with default IP source information.



Note: If the sources do not build automatically, close and then reopen the window.

4. Double-click a source. The Set Up BFS Source window opens.
5. Configure the **Transport Type**, **Data Rate**, **Block Size**, **Indication Interval**, **Multicast IP Address**, and **Source** (enable or disable) fields. Some of the data can be obtained from ***Data Carousel Rate Settings*** (on page 206).
6. Click **Save**.
7. Repeat steps 4 through 6 for all of the remaining BFS sources.
8. Close the BFS Administration window.

Set Up the PCG

At this time, you should configure the PCGs on the ISDS, if required. The PCGs need to be configured before you set up video sources. Refer to *PowerKEY CAS Gateway (PCG) for DBDS and ISDP Networks Installation, Upgrade, and Operation Guide* (part number 4017672) for information on setting up PCGs.

Note: The PCG is only needed to set up secure services. If you just want to set up clear video for the time being, you can set up the PCG later.

Manual Setup of Sources

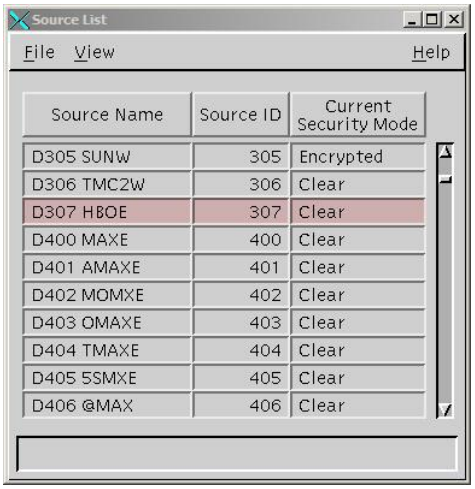
Creating Video Sources

Note: Before beginning this procedure, you may want to consult with the billing vendor to determine what kind of bundling of services will be done.

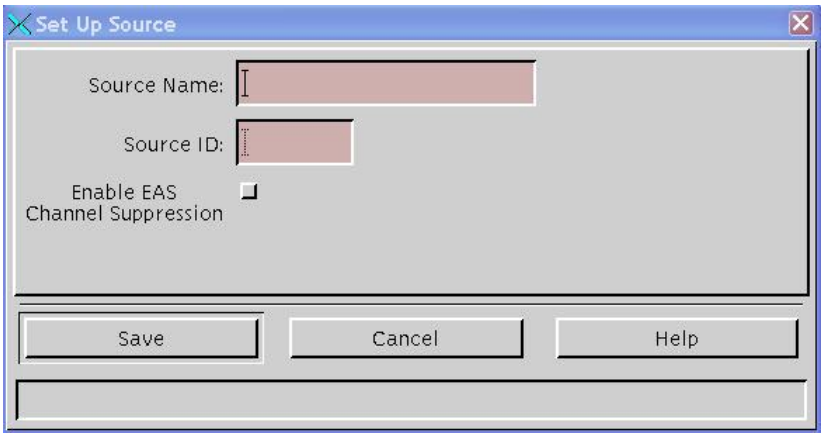
Complete the following steps to set up video sources.

1 From the ISDS Administrative Console, click the **System Provisioning** tab.

2 Click **Source**. The Source List window opens.



3 Click **File** and then select **New**. The Set Up Source window opens.



4 Type the **Source Name**.

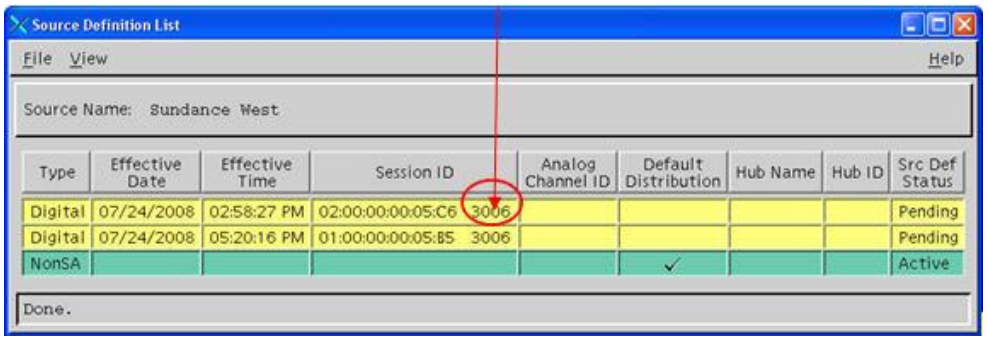
Note: The Source Name is typically the Short Description.

5 Type the **Source ID**.

Important: The Source ID must be *unique and greater than* 200. IDs 200 or less are reserved for BFS sources.

6 Click **Save** and then close the Set Up Source window.

7 From the Source List window (already open), highlight the source you just created; then click click **File** and select **Source Definitions**. The Source Definition List window opens.

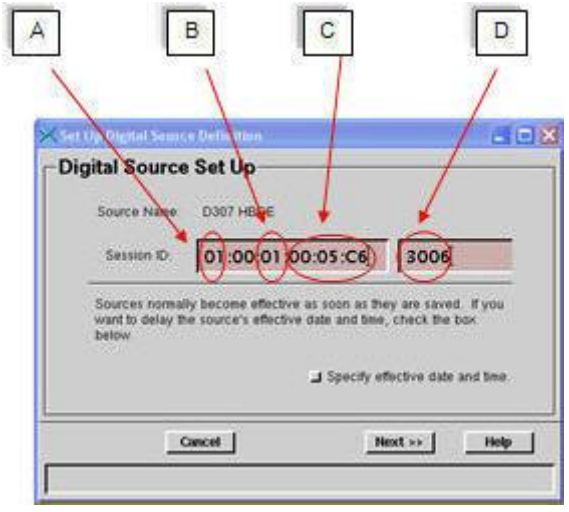


8 From the Source Definition List window, click **File** and then select **New Digital**. The Digital Source Setup window opens.

9 Configure the Digital Source Setup window according to the following guidelines:

- A = Site ID
- B = PCG Number
- C = (Not Used)
- D = Source ID

Example: Use the images associated with steps 10 and 11 to help you configure the Digital Source Setup window. The Digital Source Setup window should look similar to the following example when you are finished.



10 Click **Next**. The Digital Source Setup window updates to allow you to specify the PCG Device.

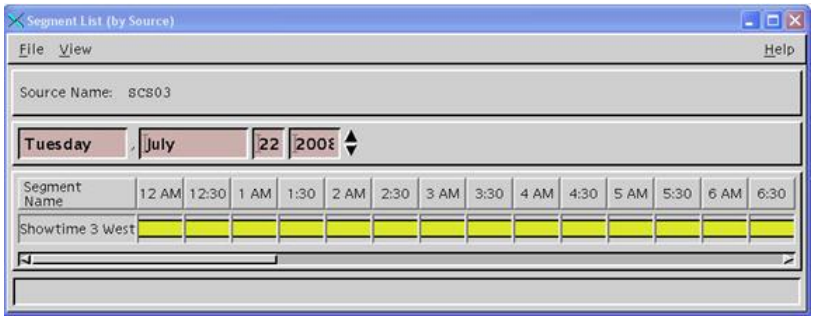
11 Select the appropriate PCG Device and then click **Next**. The window updates to allow you to set the **Scrambling Mode**.

12 Leave **Scrambling Mode** as **Default** and then click **Next**.

13 Click **Save**.

14 Set up a segment for the source by following these instructions.

- **a** In the Source List window, highlight a source, click **File** and then select **Segments**. The Segment List window opens.
- **b** Click **File** and then select **New**.
- **c** Give the segment a **Name**, click **Save**, and then close the Segment List window.

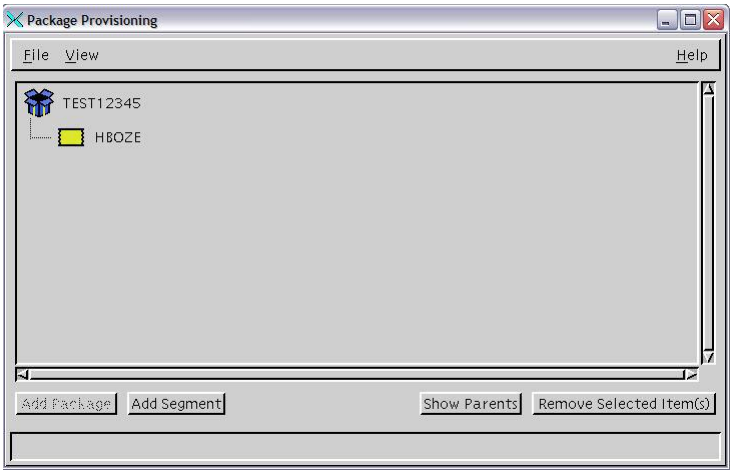


15 Follow these instructions to create a package in which the segment can be provisioned..

- **a** From the ISDS Administrative Console, click the **System Provisioning** tab, and then select **Package**.
- **b** Click **File** and then select **New**.
- **c** Name the package and then click **Save**.

16 From the ISDS Administrative Console, click **Package** and then select the

package to which you want to add the segment.



17 Click **File** and then select **Provision** and then click **Add Segment** to add the segment to the package.

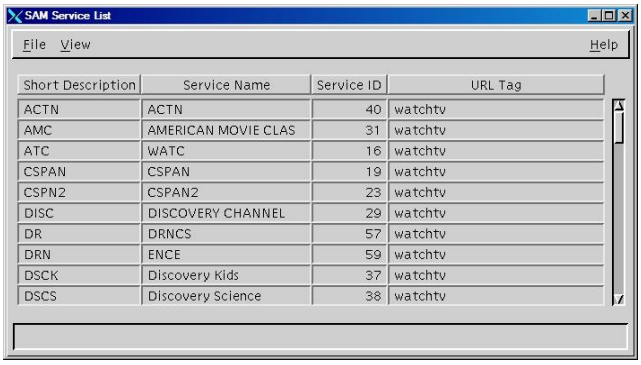
18 Repeat steps 3 through 17 for each source you create.

Create SAM Services

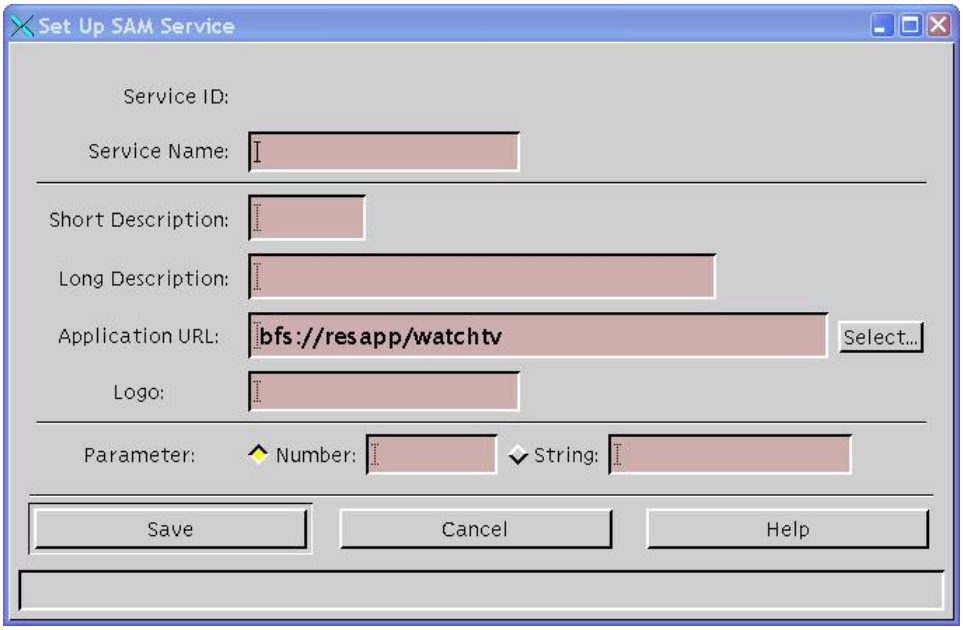
In this procedure, you will create SAM services for the newly created sources.

1 From the ISDS Administrative Console, click the **Application Interface Modules** tab.

2 Click **SAM Service**. The SAM Service List window opens.



3 Click **File** and then select **New**. The Set Up SAM Service window opens.



4 Type the name of the SAM service in the **Service Name** field.

5 Type a short description of the SAM service in the **Short Description** field.

Note: The Short Description and the Long Description (step 7) control what is displayed on the TV and must be selected carefully.

6 Type a longer description of the SAM service in the **Long Description** field.

7 Click **Select** and choose the appropriate application for the **Application URL** field.

8 Type the logo ID for the current source in the **Logo** field.

9 Select **Number** in the **Parameter** field and then type the source ID for this SAM service.

Note: The source ID that is entered must be the source ID for the service that will be displayed when this SAM service is selected on the STB.

10 Click **Save**.

Note: Make a note of the Service ID that is automatically generated. You will need this ID when you configure the IPG Collector later.

11 Repeat this procedure from step 3 to create additional SAM services.

12 Close the SAM Service List window when you are finished.

Build Services Associated with Features

This section provides instructions to provision authorization for features (downloadable applications, DVR, EPG Search, or Walled Garden) on ISDP-compatible set-tops. Once the procedures in this section are complete, the authorization package can be added to the applicable set-tops through the ISDS or the billing system.

Create a Package

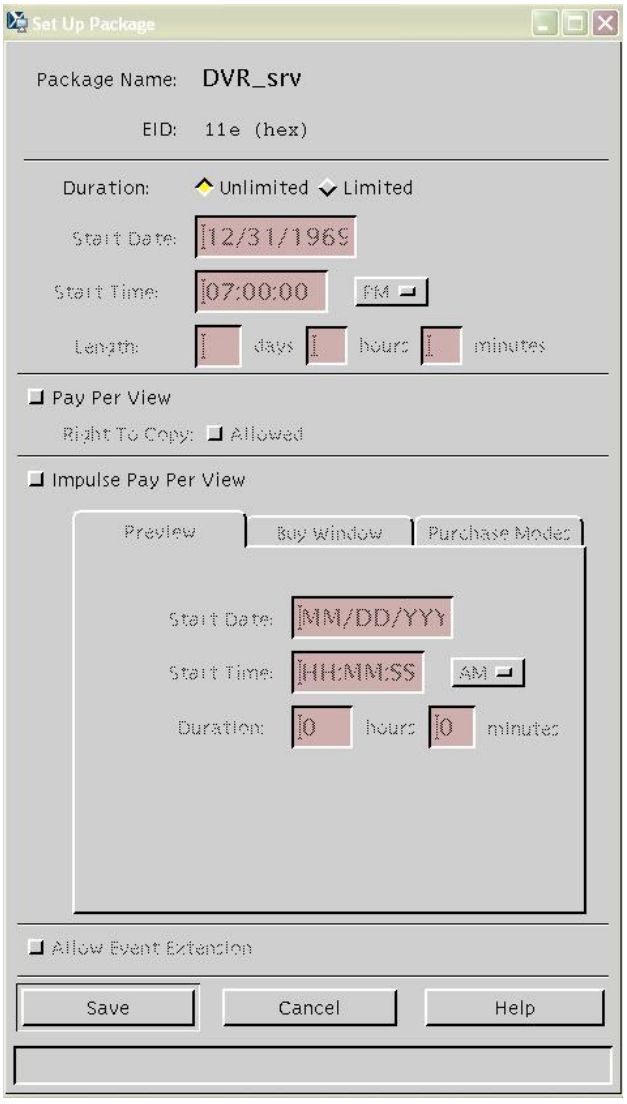
Complete the following steps to create a new package for the services or applications that you want to provision. If you have already created the package you want to use for the service, skip to the section ***Determine the EID Value*** (on page 67).

1. On the ISDS Administrative Console, click **Package** from the System Provisioning tab. The Package List window opens.
2. Select **File > New** to open the Set Up Package window.
3. Enter a unique name for the package.
4. Click **Save**. The package is created.

Determine the EID Value

Complete the steps below to determine the EID value of the service you want to authorize.

1 Open the package you will use to authorize the service and record the EID value: _____.



2 Click **Cancel** to close the Set Up Package window.

3 In the Package List window, select **File > Close** to close the window.

4 Continue with ***Create a SAM Service*** (on page 68).

Create a SAM Service

Complete the following steps to create a SAM service for the package you created.

1. From the ISDS Administrative Console, select the **Application Interface Modules** tab.
2. Click the **SAM Service** button. The SAM Service List window opens.
3. Click **File > New.** The Set Up SAM Service window opens.
4. Enter the SAM Service information per the guidelines below.

   Guidelines:

   The following variables are available to define a SAM Service:

   - **Service Name** (required) - this name is only available and shown to users of the ISDS who have access to the SAM Services List. Make this descriptive enough to understand which service is being offered. End users will not see this field.
   - **Short Description** (required) - the short description must match one of the values defined in this document; the set-top UI will use these short description values to determine if those services are being provisioned.

     The following short description names are reserved for provisioning services. Each of these Short Descriptions must only be used once per system and must be used **exactly** as shown.

SAM Short Description	Service
_SADV	DVR
_MRDV	MR-DVR
_VOD	VOD
_EPGS	EPG Search
_WG00	Walled Garden 0
_WG01	Walled Garden 1
_WG02	Walled Garden 2
_WG03	Walled Garden 3
_WG04	Walled Garden 4
_WG05	Walled Garden 5
_WG06	Walled Garden 6

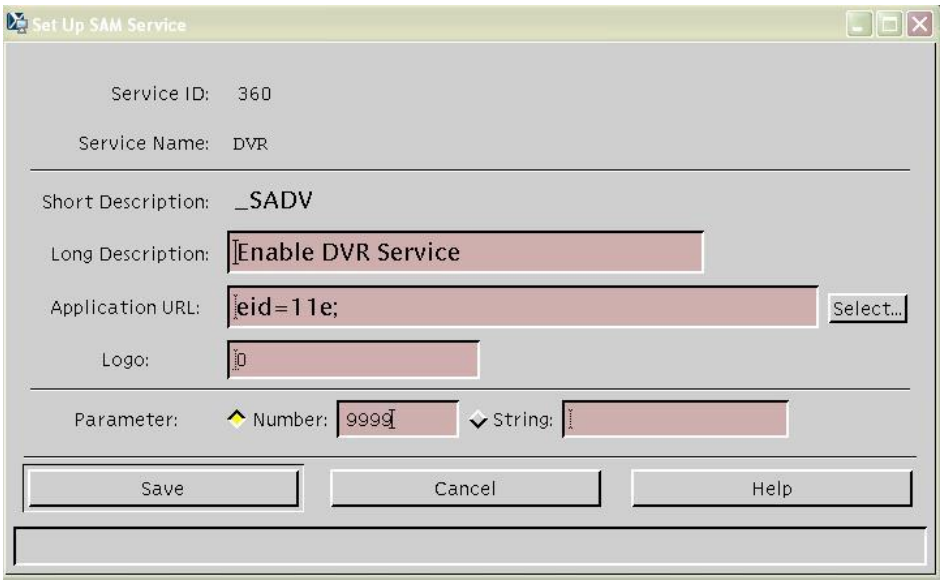
_WG07	Walled Garden 7
_WG08	Walled Garden 8
_WG09	Walled Garden 9
_WGMA	Walled Garden for "My Account"
_WGAP	Walled Garden for "App Store"

- **Long Description** - The long description will be used for meaningful display to the user. The Long Description will appear in the Menu and/or in the grid cell of the electronic programming guide (EPG), as indicated by the options in the "Application URL", described below.
- **Application URL** - The application URL provides additional information for how the service can be accessed.
  Are you creating a service for a Walled Garden?
  - If **yes**, enter the following:
    wgarden://wgarden;inEPG=0;inMenu=1;eid=[xx];url=http://[server]/[location].html

    Notes:
    - Replace “xx” with the EID value associated with the Walled Garden package and “server” with the name or IP address of the server.
    - Replace [server] with the name or IP address of the server
    - Replace [location] with the location of the web page or application
  - If **no**, enter **eid=<EID value>;** using the the EID information you recorded in step x of the ***Determine the EID Value*** (on page 67) procedure.
    Note: One package can support multiple services by reusing the EID information for each associated service.
- **Logo** - Are you creating a service for a Walled Garden?
  - If **yes**, enter the logo ID.
  - If **no**, leave blank; a default logo will be displayed.

  Note: The logo will also function in the EPG in the same way current channel logos function.
- **Parameter** - Select the bullet next to **Number** and type **0** in the field.

Example: Set Up SAM Service Window



5 Click **Save**.

Create Channel Map

In this procedure, you will add your newly created SAM services to the channel map.

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

2 Click **Channel Maps**. The Display Channel Map List window opens.

3 Follow these instructions to create a new channel map.

   a Click **File** and then select **New**. The Set Up Channel Map window opens.

   b Give the new channel map a **Name**.

   c Select the hub from **Available Hubs** to which you want the channel map to apply.

   d Click **Continue**. The Set Up Display Channel Map window opens.

4 Highlight a newly created SAM service (in the Available Services column) and then select the appropriate channel in the **Channel Slot** column.

5 Click **Add**. The selected service moves from the **Available Services** column into the **Channel Slot** column.

6 Repeat this procedure from step 4 for any additional channels that you want to add to the map.

7 Click **Save**.

8 Close the Set Up Display Channel Map window and the Display Channel Map List window.

Load DHCTs from a CD or from Files Obtained from Cisco FTP Site

Complete the steps in Chapter 4 of *ISDP Set-Top Staging Guide* (part number 4021173) to add DHCTs, to add additional DHCT types (if necessary), and to load DHCT Entitlement Management Messages (EMMs) using a CD or files obtained from the Cisco FTP site.

The following sections cover the manual process for adding DHCTs to the ISDS if loading from a CD or our FTP site is not available or is not desired:

- ***Manually Create DHCT Types*** (on page 90)
- ***Manually Add Two-Way DHCTs*** (on page 92)

Manually Create DHCT Types

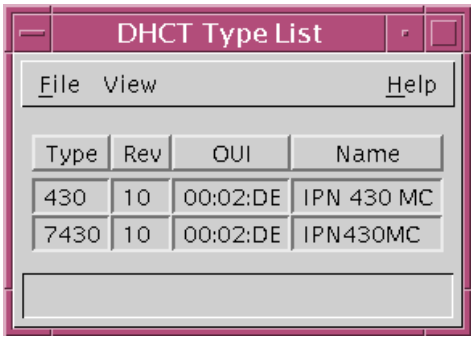
Note: Skip this section if you are loading DHCTs from an inventory CD or from an EMM.tar file.

1 Obtain the DHCT Type Number, Revision, Org. Unit ID, and Vendor information prior to starting this procedure. Contact your appropriate account representative if you do not have this information.

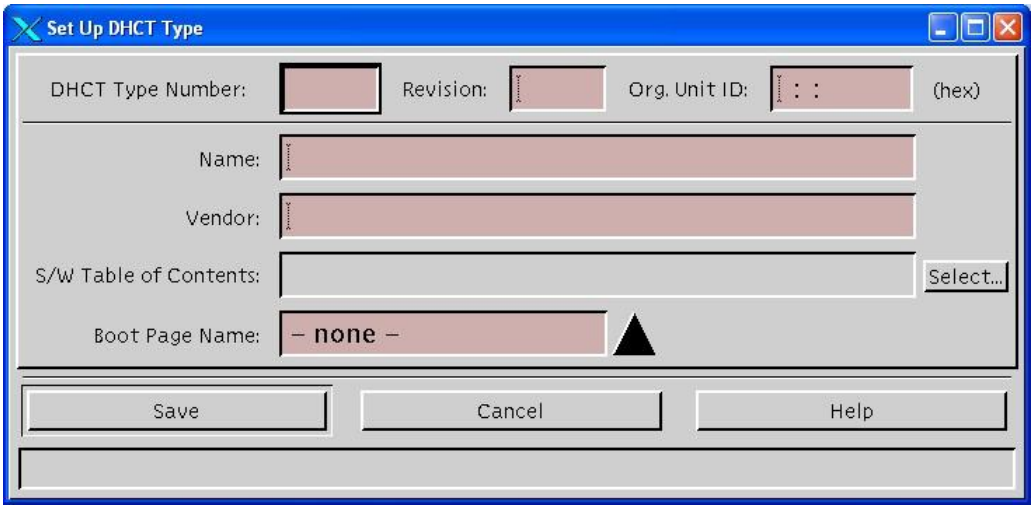
2 On the ISDS Administrative Console, click the **ISDS** tab.

3 Click the **Home Element Provisioning** tab.

4 Click **Type**. The DHCT Type List window opens.



5 Click **File** and then select **New**. The Set Up DHCT Type window opens.



6 Complete the following steps to add DHCT types to the Set Up DHCT Type window.

a Type the **DHCT Type Number**.

b Type the **Revision** number.

c Type the **Org. Unit ID**.

d Type the model **Name**.

e Type the **Vendor** name.

f Click **Save** and then close the Set Up DHCT Type window and the DHCT Type List window.

Manually Add Two-Way DHCTs

Note: Skip this procedure if you are loading DHCTs from an inventory CD or from an EMM.tar file.

These steps are for DHCTs that communicate in two-way mode. System operators normally add DHCTs to the database by means of CDs that accompany the DHCTs or by means of an EMM tar file. However, if there are no CDs or tar file available, use this procedure to add DHCTs to the database.

1. From the ISDS Administrative Console, select the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. In the **Select Option** field, click **New**.
5. Click **By MAC Address** and then type the MAC address of the DHCT you want to add.
6. Click **Continue**. The Set Up DHCT window opens.
7. In the **Admin Status** field, select **In Service Two Way**.
8. In the **DHCT Type** field, select the DHCT type that corresponds to the type of DHCT you are adding.
9. In the **DHCT Serial Number** field, type the serial number of the DHCT you are adding.
10. Follow these instructions to load the EMMs for the DHCTs from a file.
    a. Click the **Secure Services** tab on the Set Up DHCT window.
    b. Click **Load from batch CD**.
    c. Navigate to the directory that contains the "toc" file.
    d. Click **OK**.
11. Click **DMS Enable** and **DIS Enable**.
12. Click **Save**. A message appears at the bottom of the screen that displays the status of the localization record.
13. Follow these instructions to re-open the record of the DHCT you just added.
    a. From the ISDS Administrative Console, select the **ISDS** tab.
    b. Click the **Home Element Provisioning** tab.
    c. Click **DHCT**. The DHCT Provisioning window opens.
    d. In the **Select Option** field, click **Open**.
    e. Click **By MAC Address** and then type the MAC address of the DHCT you just added.
    f. Click **Continue**. The Set Up DHCT window opens.

14 On the Set Up DHCT window, click the **Secure Services** tab.

15 Select the package which authorizes the DHCT, as well as the package which provides service authorization.

16 Click **IPPV Enable** if the DHCT will have IPPV-capabilities, and then enter the **IPPV Credit Limit** and the **Max. IPPV Events** value.

17 Click **Save**.

18 Close the Set Up DHCT window and the DHCT Provisioning window.

19 Turn on power to the DHCT you just added.

Configure the DHCT Image File

Refer to *Downloading Client Application Software to ISDP Set-Tops Installation Instructions* (part number 4021172) to configure the DHCT image file. Set up default downloads for the STBs you will be testing. Do not set up test groups because test groups are not viable until they have code loaded.

Note: Complete only the following steps from this guide. The other steps are not necessary for an initial installation.

- From Chapter 2: **Phase One - Perform Pre-Upgrade Checks**
  - **Phase One Checklist** — steps 6, 8, and 9
  - **Verify the Download Directory**
  - **Obtain Software**
  - **Install the Client Application Software Release onto the ISDS**
  - **Install the Set-Top Resource File**
- Chapter 3: **Phase Two - Test New Software** (Complete all of Chapter 3)
- Chapter 4: **Phase Three - Install New Software** (Complete all of Chapter 4)
- Chapter 5: **Phase Four - Verification** (Complete all of Chapter 5)

Confirm That the System Is Transmitting BFS Transactions

Complete the following steps to confirm that the BFS is transmitting transactions.

Note: This procedure is executed as the part of the initial installation of an RNCS. You do not need to complete this procedure unless it is necessary to verify that an RNCS is transmitting BFS transactions.

1. Log on to the appropriate RNCS as root user.
2. Open the /etc/hosts file with a text editor and note the IP address associated with the hostname of the RNCS.
3. Type **ifconfig -a** and then press **Enter** to find the physical interface associated with the IP address you identified in step 2.

4 Type **snoop -V -d [interface] -x0 port 13821** and press **Enter**.

Note: Replace [interface] with the physical interface you identified in step 3.

Result: A significant amount of data is returned, similar to the following:

```
SanJose-LIONN -> 232.0.2.110  ETHER Type=0800 (IP), size = 1360 bytes
SanJose-LIONN -> 232.0.2.110  IP  D=232.0.2.110 S=172.30.0.1 LEN=1346,
ID=27296, TOS=0x80, TTL=10
SanJose-LIONN -> 232.0.2.110  UDP D=13821 S=63577 LEN=1326
0: 0100 5e00 026e 0014 4fa2 8582 0800 4580    ..^..n..O¢....E.
16: 0542 6aa0 0000 0a11 0000 ac1e 0001 e800    .Bj
32: 026e f859 35fd 052e 0000 1103 1003 0000    .n.Y5
48: 000a ff00 051a 7d3d 00ff 001a 9596 0156    ......}=.......V
64: 4b00 0000 0242 0b06 7795 06c6 4300 0000    K....B..w...C...
80: 03f8 0b10 3b00 0c04 4300 0000 03fa 0b19    ....;...C.......
96: 7790 0100 4000 0000 03fc 0b1f 1d00 1a00    w...@...........
112: 4000 0000 03fe 0b23 3b00 0705 4000 0000    @......#;...@...
128: 0400 0b2b 7796 0646 4b00 0000 0402 0b32    ...+w..FK......2
144: 9796 08f9 4b00 0000 0404 0b3b 9500 1d00    ....K......;....
160: 4000 0000 0407 0b3e 1d00 0100 4000 0000    @......>....@...
176: 0409 0b42 5995 06d9 4b00 0000 040b 0b49    ...BY...K......I
192: 5990 0800 4b00 0000 040d 0b4f 1d00 1a00    Y...K......O....
208: 4000 0000 03d2 0b54 1d00 0604 5100 0000    @......T....Q...
224: 040f 0b59 7295 06c9 4b00 0000 0411 0b60    ...Yr...K......`
240: 6393 0dd9 4300 0000 0413 0b67 7790 07c7    c...C......gw...
256: 4200 0000 0322 082b 1300 0805 4100 0000    B....".+....A...
272: 0417 0b6d 2200 0402 4300 0000 0030 0b6f    ...m"...C....0.o
288: 5992 0186 4b00 0000 041a 0b76 7790 0805    Y...K......vw...
304: 4100 0000 00ef 0b7c 1d00 1a00 4000 0000    A......|....@...
320: 041d 0b80 7794 11d9 4b00 0000 041f 0b88    ....w...K.......
336: 9898 0859 4b00 0000 0194 0b91 3b00 0e04    ...YK.......;...
352: 4300 0000 0421 0b97 1d00 1a00 4000 0000    C....!......@...
368: 0424 0b9b 3b00 0707 4000 0000 00c2 07da    .$.;...@.......
384: 3b00 1300 4000 0000 03d0 0ba1 3b00 1300    ;...@.......;...
400: 4100 0000 03d2 0ba8 1d00 0604 5100 0000    A.......¨....Q...
416: 0427 0bad 7296 08f8 4100 0000 0429 0bb5    .'..r...A....)..
432: 6d94 08e9 4b00 0000 042c 0bbc 6894 06e9    m...K....,..h...
448: 4200 0000 01d2 0bc4 6395 08d6 4b00 0000    B.......c...K...
464: 042e 0bcc 6392 0695 4b00 0000 042f 0bd3    ....c...K..../..
480: 6395 18d6 4b00 0000 0431 0bdb 5996 0707    c...K....1..Y...
496: 4200 0000 03d2 0be3 1d00 0604 5100 0000    B...........Q...
```

5 Press the **Ctrl** and **c** keys simultaneously to stop the snoop command.

Set Up the PKES

Refer to ***PowerKEY Server for Encrypted VOD in an ISDP Network Installation, Upgrade and Operation Guide*** (part number 4034718) and follow the instructions to set up the PowerKEY Server for Encrypted VOD (PKES).

Attach Mirrors

Before starting this procedure, inform the system operator that completing this procedure commits the install or the upgrade. Any attempt to roll back after the mirrors are attached will take up to 4 hours to complete. Additionally, the rollback procedure cannot be performed during the current night and will have to be performed during a maintenance window tomorrow.

Complete this procedure once you have determined that the installed software is functioning properly. This procedure runs a script that attaches submirrors to their respective mirrors and creates all necessary hot spare disks.

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. Insert the system release DVD into the DVD drive of the ISDS.
4. Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.
   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
5. Type **/cdrom/cdrom0/s3/sai/scripts/attach_mirrors** and then press **Enter**. A confirmation message appears.
6. Type **y** and then press **Enter**. The system executes a script that attaches submirrors to their respective mirrors and creates all necessary hot spare disks.
   Note: It may take several hours to execute the attach_mirrors script.
7. Type **eject cdrom** and then press **Enter**.
8. Type **exit** and then press **Enter** to log out the root user.

2

Pre-Upgrade Procedures for the ISDS

Introduction

This chapter contains procedures that you will follow to prepare the system for the upgrade. To upgrade a system, follow the procedures in Chapters 2, 3, and 4.

Note: If you are installing ISDS software onto a system for the first time, follow instead the procedures in Chapter 1.

Upgrade Path

Sites that upgrade to ISDS 2.3 need to be at version f2.2.0.2p6 or later.

Important Point About the Upgrade

Many security enhancements have been implemented starting with ISDS 2.3 f2.0.0.3. Please read *ISDS Security Enhancements Instructions* (part number 4027701) if you are upgrading from a release prior to ISDS 2.3 or are unfamiliar with the changes implemented as a result of the security enhancements. There are fundamental changes that you must be aware of to perform some of the most basic functions on the ISDS.

Notice to Installers

To ensure a successful system upgrade, it is important that you follow the instructions described in this chapter in the order given.

In This Chapter

Important Points About the Upgrade

Estimated Time to Complete the Upgrade

Our engineers have designed the upgrade so that it can be completed while you are within one maintenance window. Expect to spend the following amount of time completing the following upgrade procedures:

- Upgrading the ISDS software (doLiveUpgrade command) — about 45 to 60 minutes, depending on the number of key files that must be backed up
- Detach Database Mirrors (detach_DBmirrors command) — about 15 minutes
- Reboot of ISDS after the upgrade — about 1 hour

Important Note About Third-Party Applications

Note these important points about third-party applications:

- Identify all third-party applications currently loaded onto the ISDS.
- Contact all third-party vendors before you upgrade. Inform the vendor that you are upgrading and determine whether you need to complete any steps related to the third-party application before or after the upgrade.

Plan What Optional Features Will be Supported

Optional Features

An upgrade can contain additional optional features that system operators can elect to enable on their systems. Some of these features require that the system operator obtain a special license for the feature to be activated; others can simply be activated by our engineers without a special license.

Important: Any features that have been previously enabled or licensed as part of an earlier upgrade do not have to be re-enabled.

Determine what optional features (licensed or unlicensed) need to be enabled as a result of this upgrade. You will activate these optional features later during the upgrade, while the system processes are down.

If any licensed features are to be enabled as a result of this upgrade, contact Cisco Services to purchase the required license.

Examine Disks and Mirrored Devices

Examine the status of the mirrored disk drives on the Sun Fire V445, V890, or Sun Netra T5440 servers prior to the upgrade. All the disk mirroring functions must be working normally before proceeding with the upgrade.

> **CAUTION:**
> If the disk mirroring functions of the ISDS are not working properly before the upgrade, you may not be able to easily recover from a failed upgrade.

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. Insert the DVD into the DVD drive of the ISDS.
4. Type **df -n** and press **Enter**. A list of mounted filesystems appears.

   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the DVD.
5. After waiting at least 1 minute, did /cdrom appear in the output of the command executed in step 4.
   - If **yes**, go to the next procedure in this chapter.
   - If **no**, follow these instructions.
     a. Type **/etc/init.d/volmgt stop** and press **Enter**.
     b. Type **/etc/init.d volmgt start** and press **Enter**.
     c. Repeat steps 4 and 5.

Examining Disks and Mirrored Devices

Follow these instructions to examine the status of the mirrored drives on your ISDS. This procedure should take only a few minutes to complete.

1. If necessary, open an xterm window on the ISDS.
2. Type **metastat | more** and then press **Enter**. The system displays the status of all of the metadevices on the ISDS.

   Note: Press the **Spacebar**, if necessary, to page through all of the output.
3. 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 4.
- If **no** (to either or both conditions), call Cisco Services for help in resolving these issues with the metadevices.

4 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**.

5 Type **metastat -c** and then press **Enter**.

6 Does the output from step 5 show that there are two attached submirrors for each metadevice?

   Note: There should be a d7xx and d4xx 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: The mirrors are properly attached in the following example:

```
d520          m  511GB d420 d720
        d420      s  511GB c1t2d0s0 c1t3d0s0 c1t4d0s0
c1t5d0s0
        d720      s  511GB c2t10d0s0 c2t11d0s0 c2t12d0s0
c2t13d0s0
d510              m  128GB d410 d710
    d410          s  128GB c1t1d0s0
    d710          s  128GB c2t9d0s0
d507              m   76GB d407 d707
    d407          s   76GB c1t0d0s5
    d707          s   76GB c2t8d0s5
d503              m   36GB d403 d703
    d403          s   36GB c1t0d0s3
    d703          s   36GB c2t8d0s3
d501              m  8.0GB d401 d701
    d401          s  8.0GB c1t0d0s1
    d701          s  8.0GB c2t8d0s1
d500              m  8.0GB d400 d700
    d400          s  8.0GB c1t0d0s0
    d700          s  8.0GB c2t8d0s0
```

   - If **yes**, go to step 7.
   - If **no**, follow these instructions to attach the mirrors.

     a Type **cd /cdrom/cdrom0/s3/sai/scripts** and then press **Enter**.

     b Type **attach_mirrors** and then press **Enter**. The system executes a script that attaches submirrors to their respective mirrors and creates all necessary hot spare disks.

Note: It may take several hours to execute the attach_mirrors script.

7 Type **format** and then press **Enter** to confirm that all disks are present and readable.

Example: You should see output similar to the following example, that assumes you have a 12-disk, Sun Netra T5440:

```
AVAILABLE DISK SELECTIONS:
       0. c1t0d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@0,0
       1. c1t1d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@1,0
       2. c1t2d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@2,0
       3. c1t3d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@3,0
       4. c1t4d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@4,0
       5. c1t5d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@5,0
       6. c1t6d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@6,0
       7. c1t7d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@7,0
       8. c1t8d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@8,0
       9. c1t9d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@9,0
      10. c1t10d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@a,0
      11. c1t11d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@400/pci@0/pci@8/scsi@0/sd@b,0
```

Note: Exit from the format command by pressing the **Ctrl** and **c**, or the **Ctrl** and **d** keys simultaneously.

8 Is your DNCS platform a Sun Fire V890?

- If **yes**, type **luxadm display FCloop** and then press **Enter** to verify that all slots with disks have a Disk Status of **OK**.

  Example:

```
SUNWGS INT FCBPL
                    DISK STATUS
SLOT    DISKS               (Node WWN)
0       On (O.K.)           20000014c3203cd4
1       On (O.K.)           20000014c3202a8a
2       On (O.K.)           20000014c31b8ac6
3       On (O.K.)           20000014c3203a66
4       On (O.K.)           500000e010a2d420
5       On (O.K.)           500000e010a32660
6       On (O.K.)           500000e010a32700
7       On (O.K.)           500000e010a2d490
8       On (O.K.)           500000e010a2fcf0
9       On (O.K.)           500000e010a44370
10      On (O.K.)           20000011c6d48a12
11      On (O.K.)           20000014c38a2809
```

- If **no**, go to step 9.

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

Back Up the File Systems

The upgrade scripts do not back up the ISDS file systems. Prior to beginning the upgrade, back up the file systems manually. The following procedures provide instructions on backing up the file systems of the ISDS.

Note: The file system backup may require more than one tape.

Preparing for the File System Backup

Follow this procedure to prepare for the ISDS file system backup.

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. Insert the system release DVD into the DVD drive of the ISDS.
4. Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.
   Note: The presence of /cdrom in the output confirms that the system correctly mounted the DVD.
5. After waiting at least 1 minute, did **/cdrom** appear in the output of the command executed in step 4?
   - If **yes**, go to step 6.
   - If **no**, follow these instructions to stop and restart the vold process, which manages the auto-mount functions for the DVD drive.
     a. Type **/etc/init.d/volmgt stop** and then press **Enter**.
     b. Type **/etc/init.d/volmgt start** and then press **Enter**.
     c. Repeat step 4.
6. Label a blank tape with the following information:
   ISDS File System Backup [Date]
   [Site Name]
   [Software Version]
   System Release x.x.x DVD
   Notes:
   - Customize the date, site name, and software version for the site you are backing up.
   - The file system backup may require more than one tape.

Backing Up the File System of the ISDS

Follow these instructions to back up the file system of the ISDS.

Notes:

- If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.
- Expect to spend about an hour backing up the ISDS.

1 Insert the blank tape into the tape drive of the ISDS.

2 Type **./dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.

3 Type **/cdrom/cdrom0/s3/backup_restore/backupFileSystems** and then press **Enter** to back up the file system to the local tape drive.

Results:

- The system backs up the ISDS file system.
- The system prompts you for the next tape if the backup requires more than one tape. Insert a new tape and continue the backup.

  Note: If more than one tape is required, be sure to include the tape number on the label. Label the first tape generated by the backup with the number 1.
- The system displays a message when the backup is complete.

4 When the backup is complete, remove the tape and store it in a safe place.

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

Back Up the Database

In this procedure, you will back up the Informix database. The system release DVD should still be in the DVD drive of the ISDS.

Backing Up the ISDS Database

Use this procedure to back up the ISDS database.

Notes:

- The ISDS can be running while you back up the Informix database.
- It may take up to 30 minutes to back up a typical database with approximately 100,000 set-top boxes.

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 **df -n** and then press **Enter**. A list of the mounted filesystems appears.

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

4 After waiting at least 1 minute, did **/cdrom/cdrom** appear in the output of the command executed in step 3?

   - If **yes**, go to step 5.
   - If **no**, follow these instructions.

     a Type **/etc/init.d/volmgt stop** and then press **Enter**.
     b Type **/etc/init.d/volmgt start** and then press **Enter**.
     c Repeat step 3.

5 Label your backup tape with the following information:

   ISDS Database Backup [Day of the Week]

   [Site Name]

   [Software Version]

   System Release DVD x.x.x

   [Tape #]

   Notes:

   - Customize the label with the day of the week, site name, and software version for the site you are backing up.
   - If your database backup requires more than one tape, be sure to note the tape

number on the label.

6 Insert the tape into the tape drive of the ISDS.

7 Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.

Important: Be sure to type the dot, followed by a space, prior to typing /dvs.

8 Type **/cdrom/cdrom0/s3/backup_restore/backupDatabase** and then press **Enter**. The system displays the following message:

Please mount tape 1 on /dev/rmt/0h and then press Return to continue.

9 Press **Enter**. The system backs up your Informix database.

Notes:

- The system will prompt you to insert additional tapes if your backup requires more than one tape.
- The message **Successfully completed the database backup** appears when the backup has completed successfully.
- If the database backup was not successful, the system displays an error message. Call Cisco Services at 1-866-787-3866 for assistance in resolving the error message.

10 Type **eject cdrom** and then press **Enter**.

11 Remove the DVD and tape(s) and store them in a safe place.

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

Verify Database Integrity

Complete the following steps to check the database integrity before the upgrade. Resolve any database corruption issues, if they exist, before proceeding.

Important: Note these important items:

- On systems with a large number of set-tops, this step can take more than one hour to complete. Furthermore, the *oncheck* command used in this procedure requires a lot of database resources. On live systems, run this procedure only during a maintenance window.
- VOD performance is likely to be degraded while the *oncheck* command runs.
- If a standby ISDS server is deployed at this site as part of the Replicated Database feature, complete steps 1 through 8 *only* on the standby server.

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 **./dvs/dncs/bin/dncsSetup** and press **Enter**.
   Note: Be sure to type the period, followed by a space, before typing /dvs.
4. Type **oncheck -cIDn dncsdb >> /tmp/dncsDbChk.out** and press **Enter**.
   Note: This command may take more than an hour to complete.
5. After the oncheck command has finished running, open the /tmp/dncsDbChk.out file with a text editor and verify that no issues with dncsdb are reported in the output.
   Note: You can ignore **Table fragment partition** messages.
6. Type **./dvs/appserv/bin/appservSetup** and press **Enter**.
   Note: Be sure to type the period, followed by a space, before typing /dvs.
7. Type **oncheck -cIDn appdb >> /tmp/appDbChk.out** and press **Enter**.
   Note: This command usually completes in a few minutes.
8. Open the /tmp/appDbChk.out file with a text editor and verify that no issues with appdb are reported in the output.
   Note: You can ignore **Table fragment partition** messages.
9. Were any database errors found in either the dncsdb or appdb output files?
   - If **yes**, go to ***Resolve Database Issues*** (on page 94).
   - If **no**, go to ***Run the Doctor Report*** (on page 124).

Resolve Database Issues

Complete the following procedure to resolve database integrity problems *only* if you found database issues in ***Verify Database Integrity*** (on page 117).

Important:

- The ISDS and Application Server processes must be stopped as part of this procedure. Therefore, this procedure must be executed during the maintenance window.
- Contact Cisco Services before beginning this procedure.

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

2 Type **su - dncs** and press **Enter** to assume the dncs role.

3 As dncs user, follow these steps to stop the integrated Application Server.

   a Type **cd /dvs/appserv/bin** and then press **Enter**.

   b Type **./appControl** and then press **Enter**. The AppControl utility window appears.

   c Type **2** and then press **Enter** in the AppControl utility window.

   d In the xterm window, type **./appStop** and then press **Enter**.

   e Wait a few minutes, press **Enter** on the AppControl utility window, and verify that all of the processes have stopped.

   Note: This may take a few minutes and you may have to press **Enter** a few times.

   f If, after waiting several minutes, there are Application Server processes still running, type **./appKill** and then press **Enter**.

   g Close the AppControl utility user interface.

4 As dncs role, follow these steps to stop the ISDS.

   a Type **cd /dvs/dncs/bin** and then press **Enter**.

   b Type **dncsControl** and then press **Enter**. The dncsControl utility window appears.

   c Type **2** and then press **Enter** in the dncsControl utility window.

   d In the xterm window, type **dncsStop** and then press **Enter**.

   Result: A window opens and displays the **Are you sure you want to shut down the DNCS?**

   e Click **yes**. The window closes.

   f Wait a few minutes, press **Enter** on the dncsControl utility window, and verify that all of the processes have stopped.

   Note: This may take a few minutes and you may have to press **Enter** a few

times.

g From the xterm window, type **ps -ef | grep dvs** and then press **Enter** to verify that the ISDS processes have stopped.

h Do the results from step g show that dncsInitd, dncsResMon, appInitd, and app_crash_global.d are the only processes still running?

- If **yes**, go to step 5.
- If **no** (there are other processes still running), follow these instructions.
  a. Type **dncsKill** and then press **Enter**.
  b. Type **/dvs/appserv/bin/appKill** and then press **Enter**.
  c. Type **exit** and press **Enter** to return to the root user.

i Type **ps -ef | grep dvs** and then press **Enter** to verify that the ISDS processes have stopped.

j Do the results from step i show that dncsInitd, dncsResMon, appInitd, and app_crash_global.d are the only processes still running?

- If **yes**, go to step k.
- If **no** (there are other processes still running), type **kill -9 < PID >** for all processes that have not stopped, where PID is the Process ID.

k Close the dncsControl utility user interface.

5 As root user, type **./dvs/dncs/bin/dncsSetup** and then press **Enter** to set the correct operating environment.

Important: Make sure there is a space between the . and the /.

6 Type **showActiveSessions** and then press **Enter**.

7 Did the results from step 6 include the message **INFORMIXSERVER is idle**?

- If **yes**, go to step 8.
- If **no**, follow these instructions.

  a Type **killActiveSessions** and then press **Enter**.
  b Type **showActiveSessions** and then press **Enter**. The message **INFORMIXSERVER is idle** should appear.

8 If a dncsdb database problem was identified in the dncsDbChk.out file then continue with step 9; otherwise, skip to step 12.

9 Type **oncheck -cIDy dncsdb** and press **Enter** to correct dncsdb errors.

10 Type **oncheck -cID dncsdb >> /tmp/dncsDbFixChk.out** and press **Enter**.

11 Open the /tmp/dncsDbFixChk.out file and verify that there are no issues with dncsdb in the output.

Note: Contact Cisco Services if there are database errors.

12 If an appDb database problem was identified in the appDbChk.out file then continue with step 13; otherwise, skip to step 17.

13 Type **./dvs/appserv/bin/appservSetup** and then press **Enter**.

Important: Make sure there is a space between the . and the /.

14 Type **oncheck -cIDy appdb** and press **Enter** to correct appdb errors.

15 Type **oncheck -cID appdb >> /tmp/appDbFixChk.out** and press **Enter**.

16 Open the /tmp/appDbFixChk.out file and verify that there are no issues with appdb in the output.

Note: Contact Cisco Services if there are database errors.

17 Back up the database again by following the procedures in ***Back Up the Database*** (on page 114).

18 Restart the system components.

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

Run the Doctor Report

Before upgrading the system, run the Doctor Report. The Doctor Report provides key system configuration data that might be useful before you begin the upgrade process.

Notes:

- On a typical system, the Doctor Report takes about 10 minutes to run.
- Call Cisco Services if the Doctor Report indicates that the database requires additional data space or temporary space.

Analyze the Doctor Report

When you analyze the output of the Doctor Report, be certain that no disk partition is at over 85 percent capacity. Call Cisco Services if the Doctor report reveals that a disk partition is over 85 percent capacity.

When you analyze the output of the Doctor Report, verify the accuracy of the Timezone and Daylight Saving Time values for the hubs on this system. The values prior to the upgrade should be compared against the values post-upgrade to ensure that the configuration was migrated successfully.

Important: Do not go to the next procedure until you have completed running and analyzing the Doctor Report and correcting any problems it reports.

Run the clearDbSessions Utility

Run the clearDbSessions utility to remove orphaned and completed sessions from the database. Follow these instructions to run the clearDbSessions utility.

Note: The system components can be running while you run the clearDbSessions utility.

1. From an xterm window on the ISDS, type **su - dncs** and then press **Enter**.
2. Type the dncs password and then press **Enter**.
3. Type **clearDbSessions** and then press **Enter**. The system removes all completed session, resource, and network graph records more than 1 hour old from the database.
4. Type **clearDbSessions -c** and then press **Enter**. The system removes all completed session, resource, and network graph records from the database.
5. Type **clearDbSessions -o** and then press **Enter**. The system removes orphaned records from the database.
6. Type **exit** and then press **Enter** to log out as dncs user.

Examine Key Files

The scripts used during the upgrade are designed to back up the key files most likely to be found on the ISDS. Some sites, however, include special key files that are unique to that site, only. As part of the backup, the upgrade scripts ask if you have any special files that you want to add to the list of files to be backed up. When you answer **yes**, the system offers you an opportunity to type in the directory path and name of any special files you want to back up.

Important: You can save a lot of time if you spend a few minutes identifying those special files now. Work with the system operator to determine if there are any special files or scripts that need to be backed up.

Identify Special Files to be Backed Up

On a sheet of paper, create a list of special key files that you will back up. Use the following guidelines when you create the list:

- Write down the home directories of all user accounts.
  Note: These directories are typically found in the /export/home directory. The upgrade scripts do not automatically back up or restore user-configured accounts. All user-configured home directories must be specified as a key file to be backed up in order to be properly restored after the upgrade.
  Important:
  - Be sure that you include the home directories of all users that have been created.
  - Be sure to include the /export/home/dncs/SiteFiles directory, which contains site-specific logo and configuration files.
- Make a list of all custom scripts that your system uses.
- Review all system cron files and write down any special cron files that you want to retain after the upgrade.
  Notes:
  - Some of your special cron files may reference custom scripts. Be certain to include those custom scripts on any list of special cron files you want backed up.
  - Call Cisco Services if you are unsure of what cron files you need to back up separately.

Do Not Include These Files

When you create your list of special files to be backed up, avoid including the following types of files:

- Do not include any binary files from the /usr/local/bin directory or binary files from any other directory. These binary files may not function after the upgrade and may actually harm the upgrade.
- Do not include any library files from the /usr/lib or the /usr/local/lib directories. These library files may not function after the upgrade and may actually harm the upgrade.
- Do not include any files in the /dvs/dncs/bin directories. When these files are restored (after the upgrade), they will overwrite the new binary files associated with the upgrade.
  Note: You should not have a need to back up any files in the /dvs/dncs/bin directories. However, if you have placed a utility in this directory and decide to back it up, our engineers recommend that you move the utility to /export/home/dncs/scripts after the upgrade.
- Do not include any Solaris Operating System binary or library files.
- Do not include any Informix software binary or library files.
- Do not include any of the following home directories:
  - /export/home/dncs
  - /export/home/dncsSSH
  - /export/home/dncsftp
  - /export/home/easftp
  - /export/home/dbreader
  - /export/home/secure
  - /export/home/sysadmin
  - /export/home/informix
  - /export/home/headend
  - /export/home/secure
  - /export/home/lost+found
- Do not include any of the following files:
  - /etc/apache2/httpd.conf
  - /etc/apache2/ssl.conf

- /etc/sma/snmp/snmpd.conf

Note: Any unique configuration within these files must be identified prior to the upgrade and added back to the system after the upgrade.

Verify System Communications

Use this procedure to verify that an active communication link exists between the ISDS and the various system components. The ISDS must be able to communicate with other system components to ensure a successful system upgrade.

Important: If any of the following tests fail, troubleshoot the system to the best of your ability. If you are unable to resolve the failure, contact Cisco Services for assistance.

1. From an xterm window on the ISDS, type **su - dncs** and then press **Enter**.
2. Type the dncs password and then press **Enter**.
3. Use the UNIX **cd** command to change to the directory that contains the Doctor Report.

   Note: The directory where the Doctor Report is usually stored is /dvs/dncs/Utilities/doctor.
4. Examine the log file created in ***Run the Doctor Report*** (on page 124), and verify that the system was able to ping the following hardware components:
   - All PowerKEY CAS Gateways (PCGs) in the system
   - All Regional Network Control Systems (RNCS) in the system
   - The Transaction Encryption Device (TED)
   - The PowerKEY Server for Encrypted VOD (PKES)
5. Verify that you can manually ping all router interfaces in the system.
6. Type **df -k** and then press **Enter** to verify that you are using no more than 85 percent of the partition capacity of each disk.

   Note: If any disk partition lists a capacity of greater than 85 percent, contact Cisco Services before proceeding.
7. Verify that you can successfully stage a set-top.
8. Complete these steps to perform a fast boot on a test set-top:
   a. Boot a set-top.

      Note: Do not press the power button.

   b. Wait 5 minutes.
9. Verify that the Interactive Program Guide (IPG) displays 7 days of accurate and valid data.
10. Tune to each available channel on a set-top to confirm that a full channel lineup is present.

    Note: Record any anomalies you notice while verifying the channel lineup.

11 Verify that you can define, purchase, and view an IPPV and VOD event, if these services are offered.

12 Type **exit** and then press **Enter** to log out of the dncs role.

Check the EAS Configuration—Pre-Upgrade

Checking the EAS Configuration

Before installing the ISDS software, verify that your EAS equipment is working correctly by testing the system's ability to transmit EAS messages by referencing chapters 5 and 6 in *Configuring and Troubleshooting the Digital Emergency Alert System for ISDS Networks User Guide* (part number 4024428).

Obtain System Configuration

Complete the following steps to obtain basic system configuration data. You may need some of this information later during the upgrade.

1 From an xterm window on the ISDS, type **more /etc/hosts** and then press **Enter**. A list of IP (Internet Protocol) addresses and hostnames appears.

2 On a sheet of paper, write down the IP addresses of the hosts that appear in the /etc/hosts file.

Important: At a minimum, write down the IP addresses for the following hosts:

- Headend Control (dncsatm) _____
- dncsted _____
- OAM&P (example: dncseth) _____

Note: This is the value that is most likely to be seen.

3 Type **uname -n** and then press **Enter**. The hostname for the ISDS appears.

Important: Call Cisco Services if the hostname contains a period (.). Cisco Services engineers will help you change it to a valid hostname.

4 Write down the hostname for the ISDS, as displayed in step 3: _____

5 Determine from the system operator if the ftp service is required on this system.

Note: Most EAS equipment uses ftp to transfer files to the ISDS for EAS messages. If the ftp service is required on this system, the service must be restarted after the upgrade.

Collect System Information

In this section, you will collect information required to reconstruct the system should the upgrade fail. Follow these instructions to collect the system information.

Note: The steps in this section have the upgrade engineer copy system files to another directory on the ISDS. Some upgrade engineers prefer to copy these files to a memory stick or to a remote server, instead.

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 **cd /export/home/dncs** and then press **Enter**. The /export/home/dncs directory becomes the working directory.
4. Type **mkdir network** and then press **Enter**. The system creates a directory called network.
5. Type **cd network** and then press **Enter**. The /export/home/dncs/network directory becomes the working directory.
6. Type the following commands to copy the necessary files to this newly created directory.

   Important:

   - Press **Enter** after typing each command.
   - Note that the first few commands require a space, followed by a period, after the body of the command.

   a. `cp -p /etc/hosts .`
   b. `cp -p /etc/hostname.* .`
   c. `cp -p /etc/inet/hosts inet.hosts`
   d. `cp -p /etc/netmasks .`
   e. `cp -p /etc/defaultrouter .`

      Note: This file may not be included in your network configuration.

   f. `cp -p /etc/defaultdomain .`

      Note: This file may not be included in your network configuration.

   g. `cp -p /etc/vfstab .`
   h. `cp -p /etc/nsswitch.conf .`
   i. `cp -p /etc/rc2.d/S82atminit .`

      Note: This file may not be included in your network configuration.

j `cp -p /etc/rc2.d/S85SAspecial .`

k `cp -p /etc/inet/ipnodes .`

l `cp -p /etc/apache2/httpd.conf .`

m `cp -p /etc/apache2/ssl.conf .`

n `cp -p /etc/sma/snmp/snmpd.conf .`

o `cp -p /etc/apache2/conf/SAIwebui.soap.conf .`

p `cp -p /etc/inet/static_routes .`

Note: Depending on the implementation of the network configuration, this file may not exist.

q `cp -p /etc/sma/snmp/snmpTrapHandler.cfg .`

r `cp -p /opt/SAIrepdb/KeyFiles2Sync.list .`

s `netstat -nrv > netstat.out`

t `ifconfig -a > ifconfig.out`

u `df -k > df.out`

v `eeprom nvramrc > nvramrc.out`

7 As root user, type the following command and press **Enter**:
`cp -rp /var/spool/cron/crontabs /var/spool/cron/crontabs.previous`

8 Type the following command and press **Enter**:
`cd /var/spool/cron`

9 Type the following command and press **Enter**:
`tar cvf crontabs.previous.< date >.tar crontabs.previous`

Note: Replace < date > with the current date.

Example: `tar cvf crontabs.previous.020107.tar crontabs.previous`

10 Type the following command and then press **Enter**:
`cp -rp crontabs.previous.< date >.tar /export/home/dncs/network`

11 Type the following command and press **Enter**:
`cd /export/home/dncs/network`

12 Type **ls -ltr** and then press **Enter** to verify that each file copied successfully to the /export/home/dncs/network directory and that no file has a size of 0 (zero).

Note: If any file is of 0 size, delete that file and run the appropriate copy command again.

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

Identify Custom BOSS and SNMP Configurations

Custom BOSS configurations in the httpd.conf and ssl.conf files are not automatically backed up and restored. For example, the httpd.conf file may include entries that allow HTTP billing transactions from specific IP addresses. The ssl.conf file may include configuration changes that disable Client Authentication. Custom SNMP configurations in the snmpd.conf file are not automatically backed up and restored.

The following procedure helps you identify custom BOSS and SNMP configuration files that should be added back to the system after the upgrade.

1. Open the /etc/apache2/httpd.conf file in a text editor and search for "Allow from appservatm".
2. In the space provided, record any lines that exist between "Allow from appservatm" and "ErrorDocument 403 ."

   Note: It is possible that there will be no lines.

   Example: Allow from 192.168.100.1

   _____

   _____

   _____

   _____

   Important: These lines must be added back to the /etc/apache2/httpd.conf file after the upgrade to allow HTTP billing transactions from the specified IP address.
3. Close the /etc/apache2/httpd.conf file.
4. Type **grep SSLVerifyClient /etc/apache2/ssl.conf** and press **Enter**.
5. Determine whether the line containing SSLVerifyClient is commented out. Is there a **#** symbol (which causes the line to become a comment) at the beginning of each line?

   Yes_____ **No** _____

   Important: After the upgrade, this line must be identical to how it was before the upgrade to either disable or enable BOSS client authentication.
6. Type **cat /etc/apache2/conf/SAIwebui.soap.conf** and press **Enter**. The system displays the contents of the file.

7 Examine the following lines that appeared after completing step 6:

```
<IfDefine SSL>

    SSLVerifyClient optional
    SSLVerifyDepth  10
    SSLOptions +StrictRequire
    SSLRequire ( %{REMOTE_ADDR} eq "127.0.0.1" or \
            %{SSL_CLIENT_VERIFY} eq "SUCCESS" )
</IfDefine>
<IfDefine !SSL>
    Order Allow,Deny
    Allow from localhost
</IfDefine>
```

8 Is there a **#** symbol (which causes the line to become a comment) at the beginning of each line?

Yes _____ **No** _____

Important: After the upgrade, these lines must be identical to how they were before the upgrade to either disable or enable BOSS client authentication.

9 Type **grep rocommunity /etc/sma/snmp/snmpd.conf** and press **Enter**.

10 In the space provided, record any lines that are *not* commented out.

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

_____

_____

_____

_____

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

11 Type **grep trapsess /etc/sma/snmp/snmpd.conf** and press **Enter**.

12 In the space provided, record any lines that are returned in the output from step 11.

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.

3

DVD Upgrade Procedures for ISDS

Introduction

Use the procedures in this chapter to upgrade ISDS software.

In This Chapter

Stop the cron Jobs

Stop any cron jobs that are currently running on the ISDS. This ensures that no applications or programs initialize during the installation process. Follow the instructions in this section to stop all cron jobs.

Note: Take note of what time you stop the cron jobs. You may need to manually run these applications or programs after the installation is complete.

Stopping the cron Jobs on the ISDS

Follow these instructions to stop cron jobs on the ISDS.

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 **pgrep -fl cron** and then press **Enter**. The ISDS displays the cron process ID (PID).

   Example: The following are only examples of sample output. Your output is likely to be different.

   - If the cron process is running without any child processes, you should see something similar to this example:

     pgrep -fl cron
     209 /usr/sbin/cron

   - If the cron process has spawned a child process, you should see something similar to this example:

     pgrep -fl cron
     209 /usr/sbin/cron
     14651 sh -c /export/home/dncs/test/tst 2>&1
     14652 sh -c /export/home/dncs/tst2 2>&1

     Note: The cron process may have spawned multiple child processes.
4. Use the cron PID from step 3, and type **ptree <PID>** and then press **Enter**. The ISDS displays the process tree of all cron processes.
5. Did the results from step 4 only include /usr/sbin/cron?
   - If **yes**, type **svcadm -v disable -st cron** and then press **Enter**.
   - If **no** (results from step 4 show multiple cron processes), type **kill -9 <PIDs>**

and then press **Enter**.

Important: List the PIDs in reverse order.

Example: kill -9 14652 14651 209

- If the results from step 4 did not show /usr/sbin/cron, skip the rest of this procedure. The cron jobs are already stopped.

6 Confirm that the cron jobs have stopped by typing **pgrep -fl cron** and then press **Enter**.

Note: The "l" in "fl" is a lowercase L.

Result: The command prompt should be the only item displayed; no processes should be displayed.

7 If the results from step 4 show that the cron process is still running, repeat steps 4 through 6.

Note: Call Cisco Services for assistance, if necessary.

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

Upgrade the ISDS Software

Upgrade the ISDS 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.

Upgrading the ISDS Software

Complete the following steps to upgrade the ISDS software.

Important: Complete the following procedures using the keyboard, video, and mouse connected directly to the ISDS. The system display may not restore properly after the system reboot if a KVM extender is used.

1. 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. Insert the ISDS DVD into the DVD drive of the ISDS.
4. Wait one minute and then type **df -n** and press **Enter**. A list of the mounted filesystems appears.
5. Did /cdrom/cdrom0 appear in the output from step 4, verifying that the system mounted the DVD?
   - If **yes**, go to step 9.
   - If **no**, go to step 6.
6. Type **/etc/init.d/volmgt stop** and then press **Enter**. The volume manager utility stops.
7. After completing step 6, did the DVD user interface appear?
   - If **yes**, go to step 9
   - If **no**, type **/etc/init.d/volmgt start** and then press **Enter**. The volume manager utility starts.
8. Repeat steps 4 through 7. Call Cisco Services if the system still does not recognize the DVD.
9. Type **metastat | more** and then press **Enter**. The system displays the status of all of the metadevices on the ISDS.

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

10 Are the following two conditions true?

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

— No **Hot Spare** indicates **In Use**.

- If **yes** (to both conditions), go to step 11.
- If **no** (to either or both conditions), call Cisco Services for help in resolving these issues with the metadevices.

11 Type **which onstat** and then press **Enter**. Output should reveal that the path to the onstat command is /export/home/informix/bin.

12 Does the which command return the path to the onstat command, as described in step 11?

- If **yes**, continue with step 13.
- If **no**, then the path to the environment is incorrect; follow these instructions.

  a Type **exit** and then press **Enter** to log out the root user.
  b Type **su -** and then press **Enter**.
  c Repeat steps 11 and 12.

  Note: Call Cisco Services if the path to the onstat command, /export/home/informix/bin, is still not returned.

13 Type **cd /cdrom/cdrom0/s3/sai/scripts** and then press **Enter**.

14 Type **./detach_UFSmirrors** and press **Enter** to detach the mirrored devices. A message similar to the following appears:

This script will detach all submirrors that contain UFS file system information (submirrors containing Database will not be detached), so that they can be used during a Live Upgrade (LU).

If you are not SURE what this means, please quit now.

Are you SURE you want to do this? [y,n,?,q]

15 Type **y** and press **Enter** to confirm the detach mirrors action. The system returns a **Successfully detached UFS submirrors on this machine** message once the mirrors are successfully detached.

16 Open a second xterm window on the ISDS and follow these instructions:

a Type **tail -f /tmp/install_log** and then press **Enter** to monitor the status of the upgrade.

Note: The install script must complete several pre-processing steps prior to creating the install_log file. If the /tmp/install_log file does not exist immediately after the message in step 19 (later in this procedure) appears, wait five minutes and check for the file again.

b Close the second xterm window when the following message appears:

Extraction complete

Important: Do not remove the DVD from the DVD drive, or reboot the system, until you are instructed to do so.

17 Type **./doLiveUpgrade** and then press **Enter**. A message similar to the following appears:

Checking the system, please wait...

Live Upgrade (LU) provides a mechanism to manage and upgrade on-disk Solaris Operating Environments allowing the upgrade of one environment without taking the system down.

LU can be used for imaging the detached mirrored disks without shutting down application processes.

Do you want to continue? [y,n,?]

18 Type **y** and then press **Enter**. The software upgrade process begins.

19 During the Live Upgrade, the following message appears:

To check the status of the upgrade, do the following:

- open another terminal window

- check for the presence of /tmp/install_log file

- do tail -f /tmp/install_log

- type Control + C to exit the tail

----

20 In the original xterm window, the system displays a list of key files that will be backed up by default and displays the **Do you wish to add to the above list [y,n]?** message.

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

- If you want to add to the list of key files and directories to be backed up, follow these instructions.
  - **a** Type **y** and then press **Enter**.
  - **b** Follow the on-screen instructions to add to the list of file names and directories.

    Important: Remember to include the /export/home/dncs/network directory, all user home directories, as well as any special files you identified in Identify Special Files to be Backed Up.
  - **c** When you are finished adding key files, type **n** and then press **Enter**.

    Result: The system displays a **Do you wish to delete from the above list?** message.
  - **d** Review the list one final time and type **n** if the list is complete and then press **Enter**.

    Result: The system displays a **Do you want to continue? [y,n]** message.
  - **e** Type **y** and then press **Enter**.

- 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**.

22 Wait for the following message to appear, which indicates that the upgrade script completed successfully:

Reseting boot-device in eeprom.

Stop System Components

Maintenance Window

CAUTION:

You need to be in a maintenance window to complete the remaining procedures in this chapter, as well as in the following chapter.

Suspending Billing and Third-Party Interfaces

Before installing this software, contact your billing vendor in order to suspend the billing interface. In addition, follow third-party application instructions to stop applications during the installation process which also includes any real-time monitoring tools.

Stopping System Components

1. Type **su - dncs** and press **Enter** to assume the dncs role.
2. As dncs user, follow these steps to stop the integrated Application Server.
   - **a** Type **cd /dvs/appserv/bin** and then press **Enter**.
   - **b** Type **./appControl** and then press **Enter**. The AppControl utility window appears.

     Note: If the message **xtwrm xt error cannot open display** appears, follow these instructions.

     1. Type **echo DISPLAY** and then press **Enter**.
     2. If the display is not returned, type **DISPLAY=0:0** and press **Enter**.
     3. Type **export DISPLAY** and press **Enter**.
   - **c** Type **2** and then press **Enter** in the AppControl utility window.
   - **d** Make a note of the processes that are running so that you can compare these processes with those that are running after the upgrade.
   - **e** In the xterm window, type **./appStop** and then press **Enter**.
   - **f** Wait a few minutes, press **Enter** on the AppControl utility window, and verify that all of the processes have stopped.

     Note: This may take a few minutes and you may have to press **Enter** a few times.
   - **g** If, after waiting several minutes, there are Application Server processes still running, type **./appKill** and then press **Enter**.

h Close the AppControl utility user interface.

3 As dncs role, follow these steps to stop the ISDS.

a Type **cd /dvs/dncs/bin** and then press **Enter**.

b Type **dncsControl** and then press **Enter**. The dncsControl utility window appears.

c Type **2** and then press **Enter** in the dncsControl utility window.

d Make a note of the processes that are running so that you can compare these processes with those that are running after the upgrade.

e In the xterm window, type **dncsStop** and then press **Enter**.

Result: A window opens and displays the **Are you sure you want to shut down the DNCS?**

f Click **yes**. The window closes.

g Wait a few minutes, press **Enter** on the dncsControl utility window, and verify that all of the processes have stopped.

Note: This may take a few minutes and you may have to press **Enter** a few times.

h From the xterm window, type **ps -ef | grep dvs** and then press **Enter** to verify that the ISDS processes have stopped.

i Do the results from step h show that dncsInitd, dncsResMon, appInitd, cmd2000, snmptrapd, and app_crash_global.d are the only processes still running?

– If **yes**, go to step 4.

– If **no** (there are other processes still running), follow these instructions.

a. Type **dncsKill** and then press **Enter**.

b. Type **/dvs/appserv/bin/appKill** and then press **Enter**.

c. Type **exit** and press **Enter** to return to the root user.

j Type **ps -ef | grep dvs** and then press **Enter** to verify that the ISDS processes have stopped.

k Do the results from step j show that dncsResMon, app_crash_global.d, snmptrapd, and cmd2000 are the only processes still running?

– If **yes**, go to step 4.

– If **no** (there are other processes still running), type **kill -9 < PID >** for all processes that have not stopped, where PID is the Process ID.

4 Close the dncsControl utility user interface.

Detach Database Mirrors

In this procedure, you will detach the database mirrors of the ISDS.

Notes:

- You should be logged in to the ISDS as root user.
- The system components and the cron jobs should be stopped.
- The DVD should still be in the DVD drive of the ISDS.

Important: Interactive services are unavailable at this point and will not be available until you restart system components.

1 As root user, type **./dvs/dncs/bin/dncsSetup** and then press **Enter** to set the correct operating environment.

Important: Make sure there is a space between the . and the /.

2 Type **showActiveSessions** and then press **Enter**.

3 Did the results from step 2 include the message **INFORMIXSERVER is idle**?

- If **yes**, go to step 4.
- If **no**, follow these instructions.
  - **a** Type **killActiveSessions** and then press **Enter**.
  - **b** Type **showActiveSessions** and then press **Enter**. The message **INFORMIXSERVER is idle** should appear.

4 Type **/cdrom/cdrom0/s3/sai/scripts/detach_DBmirrors** and then press **Enter.**

Result: The following message appears:

This script will detach Database submirrors so that they can be used during the Live Upgrade (LU) process.

If you are not SURE what this means, please quit now.

Are you SURE you want to do this?

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

Result: The following message appears:

After the Database submirrors are detached, the machine needs to be booted using the upgrade disks. So answer "yes" when prompted about activating the Alternate Boot Environment (ABE).

Do you want to activate the Alternate Boot Environment (ABE)?

6 Type **y** and then press **Enter**. The system detaches the database mirrors.

Note: The script takes about 10 minutes to run and returns output similar to the following when complete:

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

to be followed to fall back 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 /pci@400/pci@0/pci@8/scsi@0/disk@0,0:a

3. Boot to the original boot environment by typing:
boot
Activation of boot environment <ISDS-f2.2.0> successful.

7 Make an exact note of the setenv boot-device command from the output of the previous step. This may be required if a back out is performed.

8 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:

```
                Is       Active     Active         Copy
BE_name      Complete    Now        On Reboot      Status
-------------------------------------------------------------
SR_[old]        yes       yes          no            -
SR_[new]        yes        no          yes           -
```

Note: This example shows that the new system release environment will be active upon the next reboot.

9 Do the results from step 8 show that the new system release environment is active on reboot?

- If **yes**, continue with step 10.
- If **no**, call Cisco Services.

10 Type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The ISDS reboots several times.

Important: Do not type *reboot* at any time.

Results:

- The system restores the key files and reboots several times.
- The system builds the new database and restores the dncsdb and appdb databases. This operation can take more than 90 minutes to complete, depending on the size of the database.
- Once complete, the CDE login prompt will appear.

11 Did the ISDS reboot without error?

- If **yes**, skip to step 14.
- If **no**, go to step 12.

12 The system may have displayed an error message similar to **/var is busy**, or **The allowable number of mount points has been exceeded**. Follow these instructions.

Note: This is a known issue that occurs randomly during an upgrade.

a Log on to the system as root user.

b Type **df -k** and then press **Enter**. The system displays the mounted filesystems.

13 Is the **/var** filesystem present in the output from step 12?

- If **yes**, press the **Ctrl** and **d** keys simultaneously and go to step 14. The system boots into multi-user mode and the Login window opens.
- If **no** (the /var filesystem is not present), follow these instructions.
  - **a** Type **mount /var** and then press **Enter**. The system mounts the /var filesystem.
  - **b** Type **df -k** and then press **Enter**. The system displays the /var filesystem in the output.

    Note: If the /var filesystem is still not present in the output, call Cisco Services for assistance.
  - **c** Press the **Ctrl** and **d** keys simultaneously. The system boots into multi-user mode and the Login window opens.

14 Log into the CDE window of the ISDS as a DNCS administrator account.

Note: A warning message is likely to appear that indicates that the system disks are in a one-way status. Click OK on the message. This is the normal state of the system at this point in the upgrade.

15 Check your appropriate set of release notes for any required ISDS patches that may need to be installed now.

Check Installed Version Numbers on the ISDS

Follow these instructions to check the installed software versions on the ISDS.

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 If necessary, insert the system release DVD into the DVD drive of the ISDS.

4 From an xterm window on the ISDS, as a dncs administrator user, type **/cdrom/cdrom0/s3/sai/scripts/utils/listpkgs -i** and then press **Enter**.

   Note: It may take a few minutes for this command to run.

   Result: The system displays a listing of installed packages.

5 Record the version number in the Actual Results column of the accompanying table for each package name (Pkg Name) listed.

Component	Pkg Name	Expected Results	Actual Results
ISDS Application	SAIdncs	f2.2.0.1	
ISDS/App Tools	SAItools	4.2.1.18	
ISDS GUI	SAIgui	f2.2.0.1	
ISDS WUI	SAIwebui	f2.2.0.1	
Solaris Patches	SAIpatch	4.5.0.2	
ISDS Online Help	SAIisdshelp	isds2.3.0.6	
ISDS Report Writer	SAIrptwrt	4.3.0.10	
Command 2000	SAIcmd2k	1.0.0.3	
Common platform	SAIcomplat	2.0.0.8	
DBDS Utilities	SAIdbdsutils	6.3.0.8	
PowerKEY CAS Gateway	SAIpcg	V2.1.0.1	
TED	SAIted	v3.1.0.1	

6 Do the first three digits of the Actual Results match the first three digits of the Expected Results for each component in the table in step 5?

   Important: The build number (the fourth digit of the version number) may differ.

- If **yes**, continue with the next section in this guide.
- If **no**, call Cisco Services and inform them of the discrepancy.

Note: The **Actual Results** may not match the **Expected Results** if you have installed any patches before reaching this procedure.

Verify Successful Migration of the /etc/hosts File and Network Routes

Follow these instructions to compare the contents of the current /etc/hosts file to the backup copy of the /etc/hosts file, and to ensure that network routing information is accurate.

Note: If you have correctly followed the instructions in this chapter, you should be logged on to an xterm window as root user.

1. As root user in an xterm window on the ISDS, type **cat /etc/hosts** and then press **Enter**.
2. In another xterm window, type **cat /export/home/dncs/network/hosts** and then press **Enter**.
3. Compare the two files and modify the /etc/hosts file, if necessary.
4. Save the /etc/hosts file, if necessary and close one xterm window.
5. Type **netstat -nrv** and then press **Enter**.
6. In another xterm window, type **cat /export/home/dncs/network/netstat.out** and then press **Enter**.
7. Compare the output from the *netstat -nrv* command with the contents of the netstat.out file.

   Important: Pay close attention to the 224.0.0.0 static route.
8. If the 224.0.0.0 static route is not accurate, as **root** user, execute the following commands:
   a. Type **/usr/sbin/route -n delete -interface 224.0/4 -gateway `/usr/bin/uname -n`** and then press **Enter**.
   b. Type **/usr/sbin/route -n add -interface 224.0/4 -gateway dncsatm** and then press **Enter**.
   c. Open the /etc/rc2.d/S85SAspecial file and insert the commands from steps a and b into the file.
9. If any other site-specific routes are missing that existed prior to the upgrade, and that should exist on the system after the upgrade, complete the following steps.

   Note: As a reference, the /etc/inet/static_routes file contains a list of all previously defined static routes on the ISDS. Do not modify the contents of this file.
   a. Use the **/usr/sbin/route –p add net [destination] [gateway]** command to add

any missing routes.

b Type **netstat –nrv** and press **Enter**. A list of all active network routes is displayed.

c Verify that the output from the netstat –nrv command appropriately matches the contents of the netstat.out file.

10 Type **ls -ltr /etc/hostname.*** and then press **Enter**.

11 Type **ls -ltr /export/home/dncs/network/hostname.*** and then press **Enter**.

12 Compare the output from steps 10 and 11. Add, delete, or modify any of the /etc/hostname files that do not match the /export/home/dncs/network/hostname files.

Note: An */etc/hostname.* file and a *hostname.* entry in the /etc/hosts file may be added to the system as part of the upgrade. Do not delete this new file or remove the hostname entry in the /etc/hosts file.

13 Did you have to modify the dncsatm, appservatm or dncseth entries in the /etc/hostname file?

- If **yes**, go to step 14.
- If **no**, continue with ***Verify the Application Server IP Interface Configuration*** (on page 159).

14 Type **shutdown –i6 –g0 –y** and then press **Enter** to reboot the ISDS.

15 Log on to the ISDS as root user or as dncs Administrator.

Verify the Application Server IP Interface Configuration

The Application Server IP interface must use the same IP interface as the dncsatm interface in order for PassThru messaging to function properly. Complete the following procedure to verify that the Application Server hostnames are defined on the same IP interface as the dncsatm interface.

Note: The dncsatm and appservatm IP addresses may be different than the values provided in this procedure if the ISDS does not have a default IP address scheme.

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 **more /etc/hosts** and then press **Enter**. Take note of the line that includes *appservatm*.

   - If the Application Server hostnames exist in a line separate from the dncsatm interface, then go to step 4.

     Example: 10.253.0.10 appservatm appserv_host ppv_manager_host vc_server_host config_manager_host

   - If the Application Server hostnames exist in the same line as the dncsatm interface, then go to Verify Informix Rootsize.

     Example: 10.253.0.1 dncsatm dncs_host appservatm appserv_host ppv_manager_host vc_server_host config_manager_host

4 Open the /etc/hosts file with a text editor, such as vi.

5 Copy the hostnames listed after the Application Server IP address (10.253.0.10) to the list of hostnames associated with dncsatm IP address (10.253.0.1).

   Example: The modified line for the dncsatm IP address 10.253.0.1 should look like the following example, and should be typed on one line.

   10.253.0.1 dncsatm dncs_host appservatm appserv_host ppv_manager_host vc_server_host config_manager_host

6 Save and close the /etc/hosts file.

7 From an xterm window on the ISDS, type **rm /etc/hostname.bge1:1** and press **Enter**.

8 As root user in the xterm window, type **/usr/sbin/shutdown –g0 –i6 –y** and then press **Enter** to reboot the ISDS.

9 When the CDE login prompt appears, log on to the ISDS using an ISDS Administrator account or as root user.

Enable the TFTP and bootp Services

For security purposes, the TFTP and bootp services are disabled by default. There is a secure and an unsecure method available for installing the PCG application software onto the PCG from the ISDS. The unsecure method requires TFTP. Follow these instructions to enable the TFTP and bootp services, only if required.

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

1 Are the TFTP and bootp services required on this system.

Note: You were instructed to obtain this information from the system operator when completing the ***Obtain System Configuration*** (on page 132) procedure.

- If **yes**, continue with step 2.
- If **no**, you do not have to complete this procedure.

2 If necessary, open an xterm window on the ISDS.

3 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**.

4 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

5 From the root xterm window, if the "#" character was removed, type **inetconv** and then press **Enter**. The system configures the TFTP service.

6 Type **svcadm enable tftp** and then press **Enter** to enable the TFTP service.

7 Type **svcs tftp** 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
```

8 Follow these instructions to enable the bootp service.

a Type **cd /dvs/dncs/etc** and then press **Enter**.

b Type **chmod 4550 bootpd** and then press **Enter**.

c Type **su - dncs** and then press **Enter**.

d Type **dncsControl -start bootpd** and then press **Enter**.

e Type **exit** and then press **Enter** to log out of the dncs role.

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

Start the System Processes

In this procedure, you will start the user interface of the ISDS server, as well as the system processes.

1 Type **dncsStart** and then press **Enter**.

2 Follow these instructions to monitor the restart of the ISDS processes.

   a Type **dncsControl** and then press **Enter**. The Dncs Control window opens.

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

   c Wait until all of the processes display a Current State of **running**.

   d Type **x** and then press **Enter** to close the dncsControl window.

3 Verify that all of the processes in the ISDS Control window are in a green state.

4 Did the mgrUIServer process remain in the yellow or red state?

- If **yes**, complete the following steps to restart the http service.

   a Open an xterm window on the ISDS as **root** user.

   b Type **svcadm -v disable -st http** and then press **Enter** to stop the http service.

   c Type **svcadm refresh http** and then press **Enter** to refresh the http service.

   d Type **svcadm -v enable http** and then press **Enter** to restart the http service.

   Note: If the mgrUIServer process does not start within 2 minutes, contact Cisco Services.

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

- If **no**, continue with step 5.

5 Type **cd /dvs/appserv/bin** and then press **Enter**.

6 Type **./appStart** and then press **Enter**.

Note: In rare instances, executing the appStart command will not be successful. If the ./appStart command does not start the processes, use the **snmx appStart.s** command instead.

7 Follow these instructions to monitor the restart of the Application Server processes.

   a Type **. appservSetup** and then press **Enter** to establish the Application Server environment.

   b Type **appControl** and then press **Enter**. The appControl utility window opens.

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

   d Wait until all of the processes display a Current State of **running**.

e Follow the onscreen directions to close the appControl utility window.

8 Click **Control**, next to AppServer on the Console Status window. The AppServer Control window opens.

Note: The AppServer Control window should display green indicators.

9 Click **Control** next to ISDS on the Console Status window. The ISDS Control window opens.

10 Monitor the process status until all indicators display green.

Notes:

- This may take as long as 10 minutes.
- Contact Cisco Services if any process remains in a yellow or red state.

11 Type **exit** and then press **Enter** to log out of the dncs role.

Restore Custom cron Entries

All default cron entries and associated files are restored after the upgrade. As part of the pre-upgrade procedures, you were instructed to make a list of any special cron files that you wanted to retain after the upgrade. Complete this section to restore custom cron entries identified in ***Examine Key Files*** (on page 126).

Note: You backed up your cron files as part of ***Collect System Information*** (on page 133). These backed-up cron files are stored at /export/home/dncs/network/crontabs.previous.<date>.tar.

1. Verify that all custom script files required for all other custom cron entries identified as key files were restored properly.
2. Add back all necessary custom cron entries.
3. Verify that all cron entries were added successfully.

Rebuild VASP Entries (if the Application Server IP Interface Was Modified)

Complete these steps ONLY if the Application Server hostnames were collapsed into the dncsatm IP address in the /etc/hosts file, in ***Verify the Application Server IP Interface Configuration*** (on page 159).

1 Did the Application Server hostnames exist in the same line as the dncsatm interface in ***Verify the Application Server IP Interface Configuration*** (on page 159)?

- If **yes**, continue with step 2.
- If **no**, skip this procedure and go to the next procedure in this chapter.

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

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

4 On the VASP List window, scroll down to the **Appserv DHCT Config**, **Appserv PPV**, and **Appserv IPG** entries.

5 Complete these steps to delete the **Appserv DHCT Config**, **Appserv PPV**, and **Appserv IPG** entries.

a Click to highlight each entry in turn.

b Click **File** and then select **Delete**.

6 Click **File** and then select **Close** to close the VASP List window.

7 From an xterm on the ISDS where you are logged on as the dncs role, complete the following steps to re-populate the VASP table with the correct Application Server entries.

a Type **cd /dvs/appserv/bin** and then press **Enter**.

b Type **createVASPEntries.ksh** and then press **Enter**. The **All registrations succeeded** message should appear.

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

9 Click **VASP**. The VASP List window opens.

10 On the VASP List window, scroll down to the **Appserv DHCT Config**, **Appserv PPV**, and **Appserv IPG** entries.

11 Verify that each of these entries was recreated successfully using the dncsatm IP address.

12 Click **File** and then select **Close** to close the VASP List window.

Enable Optional and Licensed Features

This upgrade may include several optional and/or licensed features that system operators can elect to enable on their systems. Any features that have been previously enabled or licensed as part of an earlier upgrade do not have to be re-enabled. Contact Cisco Services and ask them to enable any new optional and/or licensed features for you.

Enable the FTP Service

For security purposes, the FTP service is disabled by default. FTP is required for EAS, and may be required for certain billing systems. Follow these instructions to enable the FTP service.

Note: Complete this procedure *only* if FTP is required on this system.

1 Is the FTP service required on this system?

- If **yes**, continue with step 2.
- If **no**, you do not need to complete this procedure.

2 If necessary, open an xterm window on the ISDS.

3 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**.

4 Type **inetadm -e svc:/network/ftp:default** and then press **Enter**.

5 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

6 Use a text editor and add the following lines to the /export/home/dncs/.profile file:

 # Source the Local EAS Server IP Address

LOCAL_EAS_IP=<EAS Server IP>; export LOCAL_EAS_IP

Note: Replace <EAS Server IP> with the IP address of the local EAS server.

7 Save and close the file.

8 Type **usermod –d /export/home/easftp –s /bin/sh –c "EAS FTP Account" easftp** and then press **Enter**. The default shell changes to /bin/sh (Bourne shell) for the easftp user.

9 After running step 8, did the system display a message that indicated that the easftp user did not exist?

- If **yes** (the easftp user does not exist), follow these instructions.

a Type **useradd -m -c "EAS FTP Account" -d /export/home/easftp -u 800 -g dncs -s /bin/sh easftp** and then press **Enter**.

b Type **chmod 770 /export/home/easftp** and then press **Enter**.

c Type **passwd easftp** and then press **Enter** to set the password.

Important: The password for the easftp user should never expire. See

Manage User Passwords and Password Expiration Settings (on page 192) for instructions on setting the password accordingly.

- If **no** (the easftp user exists), continue with step 10.

10 Type **grep easftp /etc/passwd** and then press **Enter**.

11 Confirm that the last item in the output string from step 10 is **/bin/sh**.

12 Type **usermod -d /dvs/ftp -s /bin/sh -c "DNCS FTP Account" dncsftp** and then press **Enter**. The default shell changes to /bin/sh (Bourne shell) for the dncsftp user.

13 After running step 8, did the system display a message that indicated that the easftp user did not exist?

- If **yes** (the dncsftp user does not exist), follow these instructions.
  - **a** Type **useradd -m -c "DNCS FTP Account" -d /dvs/ftp -u 900 -g dncs -s /bin/sh dncsftp** and then press **Enter**.
  - **b** Type **chmod 770 /dvs/ftp** and then press **Enter**.
  - **c** Type **passwd dncsftp** and then press **Enter** to set the password.
- If **no** (the easftp user exists), continue with step 14.

14 Type **grep dncsftp /etc/passwd** and then press **Enter**.

15 Confirm that the last item in the output string from step 14 is **/bin/sh**.

4

Post Upgrade Procedures

Introduction

After upgrading your system by following the procedures set forth earlier in these upgrade installation instructions, perform the procedures in this chapter to verify that the system is fully functional and to complete the upgrade.

Important: If any of the tests in this chapter fail, troubleshoot the system to the best of your ability. If you are unable to resolve the failure, contact Cisco Services at 1-866-787-3866.

In This Chapter

Check/Verify the ISDS Data Pump Rates

Refer to ***Data Carousel Rate Settings*** (on page 206) for guidance on how to set the data carousel rates.

Verify the Upgrade

Complete these steps to verify the upgrade.

1. If necessary, open an xterm window on the ISDS.
2. Complete the following steps to log on to the xterm window as dncs user and to set the appropriate environmental variables.
   a. Type **su - dncs** and then press **Enter**. The **password** prompt appears.
   b. Type the dncs password and then press **Enter**.
3. Type **cd /dvs/dncs/Utilities/doctor** and press **Enter**.
4. Type **doctor -vn** and press **Enter**. This command runs the Doctor Report with the *ping* option. Review the Doctor Report to ensure that communications exists between all ISDS elements.
5. Type **doctor -tv** and press **Enter**. This command runs the Doctor Report with the *time* option.
6. Verify that the **Timezone** and **Daylight Saving Time** values match the values obtained in the Doctor Report when you completed the Run the Doctor Report procedure during the pre-upgrade activities.
7. Update any Timezone or Daylight Saving Time values only if necessary and in coordination with the ISDS system administrator. See *Daylight Saving Time Configuration Guide for an IP Network* (part number 4018286) for details.
8. Type **df -k** and then press **Enter** to verify that you are using no more than 85 percent of the partition capacity of each disk.

   Important: If any disk partition lists a capacity greater than 85 percent, contact Cisco Services at 1-866-787-3866 before proceeding.
9. Verify that you can successfully stage a set-top box (STB) through the CVT method.
10. Complete these steps to perform a fast boot on a test STB with a working return path (2-way mode):
    a. Boot a STB.
    b. Wait 5 minutes.
11. Verify that the IPG displays accurate and valid data.
12. Tune each available channel on a STB to confirm that a full channel lineup is present.

    Note: Write down any anomalies you notice while verifying the lineup.
13. Verify that you can purchase and view an IPPV event.
14. Verify that you can purchase and view VOD events.

15 Type **ls -ld /dvs/resapp** and then press **Enter**.

16 From the output displayed after running step 15, verify that the group has write permissions.

Example: drwxrwxr-x 2 dncs dncs 512 Dec 1 21:35 /dvs/resapp

Important: If write is not allowed for the group, type **chmod g+w /dvs/resapp** and then press **Enter**.

Important: You may want to examine the installation log files. These files are found in the /var/sadm/system/logs directory. Review of these files is not necessary unless upgrade failures have occurred.

Set the Clock on the TED (Optional)

There is no requirement that the clocks on the ISDS and the TED match exactly. The intent of this procedure is to synchronize the clocks so that log activity can be easily compared.

Complete these steps to set the clock on the TED.

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 **date** and then press **Enter**. The system date and time appears.
4. Write down the system date and time in the space provided.
   System Date: _____
   System Time: _____
5. Choose one of the following options to log on to the TED:
   - On a TED 3.0 system, type **ssh root@dncsted** and press **Enter**.
   - On a TED FX system, type **rsh -l root dncsted** and press **Enter**.
6. Type in the root password and press **Enter**. You are logged on to the TED as root user.
7. Type **date** and press **Enter**. The TED date and time appears.
8. Compare the time results from step 4 with step 7. Do the time results match the time zone where the equipment is physically located?
   - If **yes**, go to step 11.
   - If **no**, go to step 9.
9. At the prompt, type **date [mmddhhmm]** and press **Enter**.
   Example: date 07132316
   Notes:
   - The format for the date command is:
     – mm-month
     – dd-day
     – hh-hours in 24 hour format
     – mm-minutes
   - The command can be modified to include the year, the seconds, or both the year and seconds.

Examples:

- The **date 073123162001** includes the year.
- The **date 07132316.30** includes the seconds.
- The **date 071323162001.30** includes the year and seconds.

10 Type **date** again and press **Enter**. Verify that the correct time now appears.

11 Type **/sbin/clock -r** and press **Enter**. The time on the hardware clock appears.

12 Type **/sbin/clock -w** and press **Enter**. This command writes the system time to the TED hardware clock.

13 Type **/sbin/clock -r** and press **Enter**. Verify the time is synchronized between the system and the TED hardware clock.

14 Type **exit** and press **Enter** to log out of the TED.

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

Verify the Channel Map After the Upgrade

Verify that the channel map associated with various types of set-tops in the headend is accurate for each specific hub.

Verify the EAS Network Configuration

Occasionally after an upgrade, the /etc/hosts.equiv and the /etc/hosts files on the ISDS do not contain an entry for the Emergency Alert Controller (EAC) in use on the system. Follow the procedures in this section to inspect each file and to add the entries, if this system is configured to receive and distribute EAS messages.

Inspecting the /etc/hosts File on the ISDS

Follow these instructions to inspect the /etc/hosts.equiv file on the ISDS and to add the missing entry, if required.

1. If necessary, open an xterm window on the ISDS.
2. Type **cd /etc** and then press **Enter**. The /etc directory becomes the working directory.
3. Type **more hosts** and then press **Enter**. The hosts file opens for viewing using the UNIX more utility.
4. Inspect the hosts file and look for an entry that contains an IP address, followed by **eac**.

   Example: 172.18.28.173 eac
5. Does the hosts file contain an entry as described in step 4?
   - If **yes**, follow these instructions.
     a. Press the **Ctrl** and **c** keys simultaneously to exit the more utility.
     b. Go to ***Inspecting the /etc/hosts.equiv File on the ISDS*** (on page 181).
   - If **no**, follow these instructions.
     a. Press the **Ctrl** and **c** keys simultaneously to exit the more utility.
     b. Obtain the IP address for the EAC.

        Note: You can obtain the IP address for the EAC from the /export/home/dncs/network/hosts file or from the Network Administrator of the site you are upgrading.
     c. Log on to an xterm window as root user.
     d. Type **vi hosts** and then press **Enter**. The hosts file opens for editing using the UNIX vi text editor.
     e. Append the IP address and eac to the hosts file.

        Important: Use the following format:

        [IP address] eac

        Example: 172.18.28.173 eac
     f. Save and close the /etc/hosts file.
     g. Type **exit** and then press **Enter** to log out the root user.

h Go to ***Inspecting the /etc/hosts.equiv File on the ISDS*** (on page 181).

Inspecting the /etc/hosts.equiv File on the ISDS

Follow these instructions to inspect the /etc/hosts.equiv file on the ISDS and to add the missing entry, if required.

1. If necessary, open an xterm window on the ISDS.
2. Type **cd /etc** and then press **Enter**. The /etc directory becomes the working directory.
3. Type **more hosts.equiv** and then press **Enter**. The hosts.equiv file opens for viewing using the UNIX *more* utility.
4. Inspect the hosts.equiv file and look for an entry that contains **eac easftp**.
5. Does the hosts.equiv file contain an entry as described in step 4?
   - If **yes**, follow these instructions.
     a Press the **Ctrl** and **c** keys simultaneously to exit the *more* utility.
     b Go to ***Inspect the dncsSetup File for the atm_addr Environment Variable*** (on page 182).
   - If **no**, follow these instructions.
     a Press the **Ctrl** and **c** keys simultaneously to exit the *more* utility.
     b Log on to an xterm window as root user.
     c Type **vi hosts.equiv** and then press **Enter**. The hosts.equiv file opens for editing using the UNIX vi text editor.
     d Append **eac easftp** to the hosts.equiv file.
     e Save and close the /etc/hosts.equiv file.
     f Type **exit** and then press **Enter** to log out the root user.
     g Go to ***Inspect the dncsSetup File for the atm_addr Environment Variable*** (on page 182).

Inspect the dncsSetup File for the atm_addr Environment Variable

After an upgrade, the dncsSetup file must contain the following entry: **atm_addr=dncsatm**. If the atm_addr=dncseth entry exists in the dncsSetup file after an upgrade, you must edit it so that it becomes atm_addr=dncsatm.

Inspecting the dncsSetup File

Follow these instructions to inspect the dncsSetup on the ISDS for the presence of the atm_addr variable, and to add the variable, if necessary.

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

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

3 Type **more dncsSetup** and then press **Enter**. The dncsSetup opens for viewing using the UNIX *more* utility.

4 Examine the dncsSetup file and look for the following entry:

atm_addr=dncsatm

5 Does the dncsSetup file contain the entry as described in step 4?

- If **yes**, follow these instructions.
  - **a** Press the **Ctrl** and **c** keys simultaneously to exit the *more* utility.
  - **b** Go to ***Check for Stranded Audio Links*** (on page 183).
- If **no**, follow these instructions.
  - **a** Press the **Ctrl** and **c** keys simultaneously to exit the *more* utility.
  - **b** If necessary, open an xterm window on the ISDS.
  - **c** Type **su - dncs** and then press **Enter**. The **password** prompt appears.
  - **d** Type the dncs password and then press **Enter**.
  - **e** Type **vi dncsSetup** and then press **Enter**. The dncsSetup file opens using the UNIX vi text editor.
  - **f** Edit the dncsSetup file so that it contains an **atm_addr=dncsatm** entry.

    Note: The file may contain an atm_addr=dncseth entry. If so, change it so that it reads **atm_addr=dncsatm**. You must not have an atm_addr=dncseth entry in the dncsSetup file after the upgrade to SR 2.1 or later.
  - **g** Save and close the dncsSetup file.
  - **h** Type **exit** and then press **Enter** to log out of the dncs role.
  - **i** ***Go to Check for Stranded Audio Links*** (on page 183).

Check for Stranded Audio Links

Audio files used in conjunction with the EAS system are defined with an expiration time and date. Sometimes, when the MMM Server process of the ISDS is bounced before an audio file expires, a link to that audio file remains on the ISDS. This audio link is said to be "stranded." After an upgrade, engineers need to examine the dncsLog file for the presence of a stranded audio link, and then delete that link, if necessary.

Checking for Stranded Audio Links

Follow these instructions to check the ISDS for a stranded audio link and then to delete that stranded link if one is found.

1. If necessary, open an xterm window on the ISDS.
2. Type **cd /var/log** and then press **Enter**. The /var/log directory becomes the working directory.
3. Type **grep -i aiff dncsLog** and then press **Enter**. The system checks the dncsLog file for the presence of aiff.

   Note: The file extension of audio files used by the MMM Server is **aiff**.
4. Did the grep operation from step 3 return a line similar to **[Date Time] dncs bfsServer BFSDir::_checkLinkedFiles() Error, can't find file /MMMAud/a1847750.aiff, marking as inaccessible**?
   - If **yes**, go to ***Deleting the Stranded Audio Links*** (on page 183).
   - If **no**, go to ***Check the EAS Configuration — Post Upgrade*** (on page 186); you have no stranded audio links.

Deleting the Stranded Audio Links

Follow these instructions to delete the stranded audio links from the ISDS.

1. From the ISDS Administrative Console, select the **Application Interface Modules** tab.
2. Click **BFS Client**. The BFS Client Sites window opens.
3. For each of the BFS client sites, click the appropriate site, click **File**, and then **Select**. The Broadcast File Server List window opens.
4. Scroll down the window and double-click the **MMMAud** icon. The filing cabinet icon "opens" to display the individual files within.

   Note: The icon is in the form of a filing cabinet.

5 Highlight the individual file that corresponds with the stranded audio link you identified in the **Checking for Stranded Audio Links** procedure.

6 Click **File** and then select **Delete**. A confirmation message appears.

7 Click **Yes**. The system deletes the selected file.

Notes:

- In some cases, you may have to repeat steps 4 through 6 several times before the system finally deletes the file.
- If, after several attempts, the system does not delete the file, repeat steps 4 through 6, but delete the entire MMMAud filing cabinet, instead.

8 Close the Broadcast File Server List window.

9 Close the BFS Client Sites window.

Check the EAS Configuration—Post Upgrade

Checking the EAS Configuration

After installing the ISDS software, verify that your EAS equipment is working correctly by testing the system's ability to transmit EAS messages. Reference chapters 5 and 6 in *Configuring and Troubleshooting the Digital Emergency Alert System for ISDS Networks User Guide* (part number 4024428) to verify your ability to transmit EAS messages.

Configure or Restore the Northbound SNMP Interface

The ISDS includes a Northbound SNMP interface which supports *only* SNMP Version 3 by default. The ISDS is delivered with a user name, an authentication passphrase, and a privacy passphrase. Contact your appropriate account representative to obtain these values. The Northbound SNMP interface can also be modified to support SNMPv2c, as well as very limited SNMP traps.

If the SNMP Northbound interface has not been modified on this ISDS but changes are required after the upgrade, contact Cisco Services for detailed instructions.

If the SNMP Northbound interface had custom configurations prior to the upgrade, then complete the following steps to restore the configuration. You captured custom configuration data prior to the upgrade, in ***Identify Custom BOSS and SNMP Configurations*** (on page 135).

Important: A copy of the /etc/sma/snmp/snmpd.conf file was backed up to the /export/home/dncs/network directory. This file should only be used as a reference. This file should not be used to replace the new /etc/sma/snmp/snmpd.conf file.

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. Did you find any un-commented lines that contain *rocommunity* in the etc/sma/snmp/snmpd.conf file when completing steps 7 and 8 in ***Identify Custom BOSS and SNMP Configurations*** (on page 135)?
   - 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 in step 10 of **Identify Custom BOSS and SNMP Configurations**.

        Note: Add them right after the #*rocommunity public* line.

     e. Save and close the file.
   - If **no**, continue with step 4.

4 Did you find any lines that contain *trapsess* when you completed steps 11 and 12 of ***Identify Custom BOSS and SNMP Configurations*** (on page 135)?

- 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 in step 11 of **Identify Custom BOSS and SNMP Configurations**.
  - **d** Save and close the file.
- If **no**, continue with 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. You should see output similar to the following:

```
svc:/application/management/sma:default (net-snmp SNMP
daemon)
State: online since December 11, 2008 5:41:54 PM EST
See: snmpd(1M)
See: /var/svc/log/application-management-
sma:default.log
Impact: None.
```

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

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

Configure or Restore the SNMP Trap Handler

The ISDS includes an event logging function for receiving and logging SNMP traps generated by IBDS network elements. If the ISDS SNMP Trap Handler was not configured prior to the upgrade, contact Cisco Systems for help in configuring it.

If the ISDS SNMP Trap Handler was configured prior to the upgrade, then complete the following steps to restore the configuration.

Note: The /dvs/dncs/mibs/external directory was added to the ISDS in f2.1.0.4. All network element MIBs, such as the SA-PCG-MIB, must reside in this directory.

1 Verify that all of the necessary network element MIBs, e.g. SA-PCG-MIB, exist in the /dvs/dncs/mibs/external directory.

   Note: The SNMP Trap Handler sources the MIBs in this directory to decode SNMP traps received from other network elements.

2 If any MIBs were added to the /dvs/dncs/mibs/external directory, then complete the following steps to restart the SNMP Trap Daemon.

   a If necessary, open an xterm window on the ISDS as root user.

   b Type **ps –ef | grep snmptrapd** and press **Enter**. The running snmptrapd process information is displayed.

   Example:
   root 20838 1 0 12:47:36 ? 0:08 /usr/sfw/sbin/snmptrapd -n -M/etc/sma/snmp/mibs:/dvs/dncs/mibs:/dvs/dncs/mibs/

   c Type **kill -9 [PID]** and press **Enter**. The snmptrapd process is stopped.

   Note: Replace [PID] with the process ID for snmptrapd returned in the output of the previous step.

   d Type **/etc/rc2.d/S85snmptrapd** and press **Enter**. The snmptrapd process starts.

3 Compare the configuration settings in the /etc/sma/snmp/snmpTrapHandler.cfg file to the previous snmpTrapHandler.cfg file backed up in the /export/home/dncs/network directory.

   Note: The snmpTrapHandler.cfg file should have been backed up to the export/home/dncs/network/ directory as part of the steps in Collect System Information.

4 Update the /etc/sma/snmp/snmpTrapHandler.cfg file if any configuration changes are required. Pay close attention to the list of critical events.

   Note: It is not necessary to restart any process after updating the

snmpTrapHandler.cfg file. The changes are implemented dynamically when changes to the file are saved.

Restore the Password Expiration and Password Expiration Warning Parameters

Complete the following steps to restore the **MAXWEEKS** and **WARNWEEKS** values if they do not match the values prior to the upgrade.

Note: These values set the password expiration and password expiration warning interval when user passwords are created or modified. A value of -1 is used to disable password expiration and the password expiration warning.

1. Open an xterm window on the ISDS as the root user.
2. Type **grep WEEKS /etc/default/passwd** and press **Enter**. The password expiration parameters are displayed.
3. Do the MAXWEEKS and WARNWEEKS values returned in step 2 match the values you recorded in ***Obtain System Configuration*** (on page 132)?
   - If **yes**, go to the next procedure in this chapter.
   - If **no**, open the /etc/default/passwd file with a text editor, change the MAXWEEKS and WARNWEEKS values to match the pre-upgrade values, and then save and close the file.

Manage User Passwords and Password Expiration Settings

Changing Default User Passwords and Password Expiration Settings

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

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 and the ISDS, respectively.

The root, dncsftp, 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 ISDS. The informix, dncsSSH, pcgrequest, and pcgscp users do not have password-aging, by default.

CAUTION:

The ISDS, or components within the ISDS, will become unstable if the password expires for any of the default users (root, dncs, dncsSSH, informix, dncsftp, easftp, pcgrequest, and pcgscp). The ISDS system administrator MUST ensure that these passwords do NOT expire. It is imperative that password-aging be disabled unless the ISDS system administrator ensures these account passwords do not expire.

1. If necessary, open an xterm window on the ISDS 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 9. No numbers should appear. If numbers appear after any account name, repeat steps 8 and 9 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.

Copy the Backup and Restore Scripts from the SR DVD to the ISDS

Complete the following steps to copy the entire ISDS backup and restore scripts directory from the latest installation DVD to the ISDS file system.

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

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
cp -R /cdrom/cdrom0/s3/backup_restore /usr/local and press **Enter** to copy the /cdrom/cdrom0/backup_restore directory to the /usr/local/backup_restore directory.

   Note: The command prompt returns after a few moments.

Configure or Restore the BOSS Interface

Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) for the Billing and Order Support System (BOSS) interface is introduced in ISDS 2.3 f2.0.0.8. The BOSS interface is not functional until the necessary TLS/SSL configuration is implemented, or an exception is defined for the IP address of the billing system to allow HyperText Transfer Protocol (HTTP).

If the BOSS interface has not yet been configured on this ISDS, but is required after the upgrade, refer to TLS/SSL for the BOSS Interface for detailed instructions on configuring the BOSS for plain HTTP or for implementing TLS/SSL.

If the BOSS interface was functional prior to the upgrade, then complete the following steps to restore the configuration.

Important: A copy of the /etc/apache2/httpd.conf, /etc/apache2/ssl.conf, and /etc/apache2/conf/SAIwebui.soap.conf files were backed up to the /export/home/dncs/network directory. These files should only be used as a reference. These files should not be used to replace the new /etc/apache2/httpd.conf, /etc/apache2/ssl.conf and /etc/apache2/conf/SAIwebui.soap.conf files.

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. Were any "Allow from [IP addresses]" found and noted in step 2 of Identify Custom BOSS and SNMP Configurations?
   - If **yes**, continue with step 4.
   - If **no**, skip to step 8.
4. Type **cp /etc/apache2/httpd.conf /etc/apache2/httpd.conf.orig.bkup** and then press **Enter** to make a backup copy of the httpd.conf file.
5. Open the /etc/apache2/httpd.conf file with a text editor.
6. Insert any "Allow from [IP addresses]" lines that you identified prior to the upgrade into the /etc/apache2/httpd.conf file.

   Important: Insert them after the *Allow from appservatm* line, but before the *ErrorDocument 403…* line.

   Example: This section of the file should look similar to the following example:

   <Location />

Order Allow,Deny
Allow from localhost
Allow from dncs
Allow from appservatm
Allow from <billing server IP>
ErrorDocument 403 …

7 Save and close the file.

8 Type **grep SSLVerifyClient /etc/apache2/ssl.conf** and press **Enter**.

9 Determine whether the output from step 8 matches what you found when you completed step 5 of Identify Custom BOSS and SNMP Configurations.

Example: If the line containing *SSLVerifyClient* was commented out prior to the upgrade, it needs to be commented out after the upgrade. If the line containing *SSLVerifyClient* was not commented out prior to the upgrade, you should not comment it out after the upgrade.

10 Do you need to edit the /etc/apache2/ssl.conf file to make the pre-upgrade and post-upgrade versions of the SSLVerifyClient line match?

- If **yes**, follow these instructions.
  - **a** Open the /etc/apache2/ssl.conf file with a text editor.
  - **b** Comment or un-comment the line containing *SSLVerifyClient*, as apprpriate.
  - **c** Save and close the /etc/apache2/ssl.conf file.
  - **d** Type **grep SSLVerifyClient /etc/apache2/ssl.conf** and then press **Enter** to verify that you updated the file correctly.
- If **no**, continue with step 11.

11 Type **cat /etc/apache2/conf/SAIwebui.soap.conf** and press **Enter**. The system displays the contents of the file.

12 Determine whether the output from step 11 matches what you found when you completed steps 7 and 8 of Identify Custom BOSS and SNMP Configurations.

Example: If the following lines were commented out prior to the upgrade, you must comment out the lines after the upgrade. If the following lines were not commented out prior to the upgrade, you should not comment them out after the upgrade.

<IfDefine SSL>

SSLVerifyClient optional
SSLVerifyDepth 10
SSLOptions +StrictRequire
**SSLRequire (%{REMOTE_ADDR} eq "127.0.0.1" or **

```
            %{SSL_CLIENT_VERIFY} eq "SUCCESS" )
</IfDefine>
<IfDefine !SSL>
    Order Allow,Deny
    Allow from localhost
</IfDefine>
```

13 Do you need to edit the /etc/apache2/conf/SAIwebui.soap.conf file to make the pre-upgrade and post-upgrade versions match?

- If **yes**, follow these instructions.
  - **a** Open the **/etc/apache2/conf/SAIwebui.soap.conf** file with a text editor.
  - **b** Comment or un-comment all of the lines listed in the example, as appropriate.
  - **c** Save and close /etc/apache2/conf/SAIwebui.soap.conf file.
  - **d** Type **cat /etc/apache2/conf/SAIwebui.soap.conf** and press **Enter** to verify that you have updated the file correctly
- If **no**, continue with step 14.

14 Did you have to modify the /etc/apache2/httpd.conf file, the /etc/apache2/ssl.conf file, or the /etc/apache2/conf/SAIwebui.soap.conf file?

- If **yes**, follow these instructions to stop and restart the httpd process.
  - **a** Type **svcadm -v disable -s http** and then press **Enter**.
  - **b** Type **svcadm refresh http** and then press **Enter**.
  - **c** Type **svcadm -v enable -s http** and then press **Enter**.
- If **no**, go to step 15.

15 Follow these instructions to verify that the http service has started correctly.

a Type **ps -ef | grep http** and then press **Enter**. Output should look similar to the following example:

```
root  4705     1 0 23:14:12 ? 0:01 /usr/apache2/bin/httpd
-k start -DSSL
dncs  4710  4705 0 23:14:13 ? 0:00 /usr/apache2/bin/httpd
-k start -DSSL
dncs  4709  4705 0 23:14:13 ? 0:01 /usr/apache2/bin/httpd
-k start -DSSL
```

b Type **lsof -i :443** and then press **Enter**. Output should look similar to the following example:

```
httpd 4705 root 258u  IPv4 0x6001b2cdd00  0t0  TCP *:443
(LISTEN)
httpd 4709 dncs  258u  IPv4 0x6001b2cdd00  0t0  TCP *:443
(LISTEN)
httpd 4710 dncs  258u  IPv4 0x6001b2cdd00  0t0  TCP *:443
(LISTEN)
```

16 Does your output, after completing step 15, look similar to the output examples provided with step 15?

- If **yes**, you are finished with this procedure. Go to the next procedure in this chapter.
- If **no**, continue with step 17.

17 Type **/dvs/tools/bin/gen_crt** and then press **Enter** to verify the configuration and to enable HTTP-S. The gen_crt menu appears.

18 Select choice **5** and then press **Enter**. The system checks the certificates.

19 Follow these instructions to stop and restart the httpd process.

a Type **svcadm -v disable -s http** and then press **Enter**.

b Type **svcadm refresh http** and then press **Enter**.

c Type **svcadm -v enable -s http** and then press **Enter**.

20 Follow these instructions to verify that the http service has started correctly.

a Type **ps -ef | grep http** and then press **Enter**. Output should look similar to the following example:

```
root  4705     1 0 23:14:12 ? 0:01 /usr/apache2/bin/httpd
-k start -DSSL
dncs  4710  4705 0 23:14:13 ? 0:00 /usr/apache2/bin/httpd
-k start -DSSL
dncs  4709  4705 0 23:14:13 ? 0:01 /usr/apache2/bin/httpd
-k start -DSSL
```

b Type **lsof -i :443** and then press **Enter**. Output should look similar to the following example:

```
httpd 4705 root  258u  IPv4 0x6001b2cdd00  0t0  TCP *:443
(LISTEN)
httpd 4709 dncs  258u  IPv4 0x6001b2cdd00  0t0  TCP *:443
(LISTEN)
httpd 4710 dncs  258u  IPv4 0x6001b2cdd00  0t0  TCP *:443
(LISTEN)
```

21 Does your output, after completing step 20, look similar to the output examples provided with step 20?

- If **yes**, verify with the technicians at the headend that billing transactions are transmitting, as expected.
- If **no**, contact Cisco Services.

Attach Mirrors

Before starting this procedure, inform the system operator that completing this procedure commits the upgrade. Any attempt to roll back from the upgrade after the mirrors are attached will take up to 4 hours to complete. Additionally, the rollback procedure cannot be performed during the current night and will have to be performed during a maintenance window tomorrow.

Complete this procedure once you have determined that the installed software is functioning properly. This procedure runs a script that attaches submirrors to their respective mirrors and creates all necessary hot spare disks.

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. Insert the system release DVD into the DVD drive of the ISDS.
4. Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.
   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
5. Type **/cdrom/cdrom0/s3/sai/scripts/attach_mirrors** and then press **Enter**. A confirmation message appears.
6. Type **y** and then press **Enter**. The system executes a script that attaches submirrors to their respective mirrors and creates all necessary hot spare disks.
   Note: It may take several hours to execute the attach_mirrors script.
7. Type **eject cdrom** and then press **Enter**.
8. Type **exit** and then press **Enter** to log out the root user.

5

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

Recommended Data Carousel Rate Settings

In This Appendix

Introduction

Refer to the data carousel settings in this appendix when configuring the Set Up BFS Source window.

Data Carousel Rate Settings

The following table lists the suggested data carousel rate settings for the ISDS. The settings should be preserved during the upgrade. Reference the Site DNCS BFS Administration window to review the current settings, if necessary.

Note: The transport type is Multicast IP.

Source ID	Data Carousel	Data Rate (Mbps)	Block Size (Bytes)	Indication Interval (ms)
0	System Carousel	0.50	1300	100
1	Out-of-Band	0.50	1300	100
2	Inband	0.50	1300	100
3	CAM OOB	0.50	1300	100
4	CAM IB	0.50	1300	100
5	IPG OOB	0.50	1300	200
6	IPG1 IB	1.00	1300	100
7	PPV OOB	0.50	1300	200
9	SAM	0.50	1300	100
10	IPG2 IB	1.00	1300	100
11	POD_Channels	0.50	1300	100
12	IPG3 IB	1.00	1300	100
14	IPG4 IB	1.00	1300	100
16	IPG5 IB	1.00	1300	100
18	IPG6 IB	1.00	1300	100
20	IPG7 IB	1.00	1300	100
21	MMM OOB	0.50	1300	100
22	PPV IB2	1.00	1300	100
181	VQE Client	0.50	1300	100
198	bootloaderMcast	3.00	1300	100

B

Troubleshooting the Keyboard, Monitor, and Mouse

In This Appendix

Introduction

If the keyboard, the monitor, or the mouse do not function properly after you have connected them to the ISDS, complete the short procedure in this appendix to get them working properly.

Keyboard, Monitor, and Mouse Troubleshooting Procedure

By completing the following steps, your keyboard will be set to the input device and your monitor set to the output device.

1. Connect a laptop computer to the serial network management port of the 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. Type **# .** and then press **Enter**. The login prompt appears.
4. Type **# .** again and then press **Enter**. The **sc>** prompt appears.
5. Type **break -y** and then press **Enter**.
6. Type **console -f** and then press **Enter**. A warning message appears.
7. Reply **yes** to the warning message. An informational message appears.
8. Press **Enter**. The **ok>** prompt appears.
9. Type **setenv input-device keyboard** and then press **Enter**. The system configures the keyboard for receiving input.
10. Type **setenv output-device screen** and then press **Enter**. The system configures the computer monitor (the screen) for displaying output.
11. Type **reset-all** and then press **Enter**. The system reboots and applies the environmental changes.
12. Log out of the HyperTerminal application.

Note: If this procedure is not successful in troubleshooting your keyboard, mouse, and/or monitor issues, contact Cisco Services for assistance.

C

TLS/SSL for the BOSS Interface

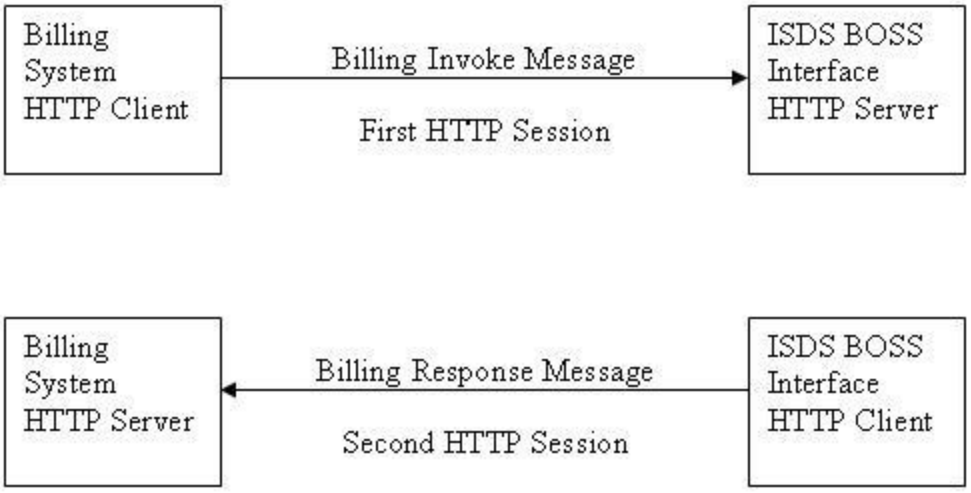
In This Appendix

Introduction

The communication protocol used between the billing system and the Billing and Order Support System (BOSS) interface of the ISDS is the HyperText Transfer Protocol (HTTP). Transport Layer Security (TLS) or the Secure Sockets Layer (SSL) can be utilized to secure the HTTP traffic between the billing system and BOSS. This appendix describes the necessary concepts and procedures.

Overview

Implementation of TLS/SSL requires that both the billing system and the BOSS support TLS/SSL. The billing interface is asynchronous, so both the billing system and the BOSS interface of the ISDS must act as an HTTP client as well as an HTTP server. That is, there are two separate HTTP sessions for each billing transaction — one session for the invoke message and a second session for the response message. Therefore, the billing system is both an HTTP client and an HTTP server. Likewise, the ISDS Boss Interface is both an HTTP server and an HTTP client. The following illustration describes this relationship:



This requires that the billing system supports TLS/SSL as both a client and a server. If the billing system does not support TLS/SSL, or if the feature is not required, it is possible to disable TLS/SSL on the ISDS.

The BOSS interface also supports Client Authentication when acting as a HyperText Transfer Protocol Secure (HTTP-S) client or HTTP-S server. That is, when acting as the HTTP-S server, the BOSS interface can be configured to request a certificate from the billing system. This functionality is also configurable on the ISDS. Additionally, when acting as the HTTP-S client, the BOSS interface supports providing a certificate if requested by the billing system. Client Authentication adds an additional step in the TLS/SSL authentication process when the HTTP server requests and validates a certificate from the HTTP client.

There are several different configuration options for the billing system-to-BOSS interface of the ISDS. A list of these options is provided in the following table:

Configuration	Billing System	ISDS BOSS Interface
1	HTTP	HTTP
2	TLS/SSL without Client Authentication	TLS/SSL without Client Authentication
3	TLS/SSL without Client Authentication	TLS/SSL with Client Authentication
4	TLS/SSL with Client Authentication	TLS/SSL without Client Authentication
5	TLS/SSL with Client Authentication	TLS/SSL with Client Authentication

Note: This appendix covers the necessary steps to configure the ISDS. Instructions to implement SSL / TLS on the billing server are beyond the scope of this appendix.

Disable TLS/SSL for the BOSS Interface

If TLS/SSL will not be implemented for the BOSS interface on this system, then execute the following commands to add an exception for the billing system and to disable client authentication. This exception allows the billing system to communicate with the BOSS interface using HTTP instead of HTTPS.

1. If necessary, open an xterm window on the ISDS.
2. Type **cp /etc/apache2/httpd.conf /etc/apache2/httpd.conf.orig.bkup** and then press **Enter** to make a backup copy of the httpd.conf file.
3. Open the /etc/apache2/httpd.conf file using a text editor.
4. Add the following line *after* the **Allow from appservatm** line and *before* the **ErrorDocument 403…** line.

   Allow from [billing server IP]

   Notes:

   - The line you add should be near the bottom of the file.
   - Replace [billing server IP] with the IP address of the billing system.

   Example: That section of the file should look similar to the following example:

   [Location /]

   Order Allow,Deny
   Allow from localhost
   Allow from dncs
   Allow from appservatm
   Allow from [billing server IP]
   ErrorDocument 403 …
5. Save and close the file.
6. Use a text editor to open the **/etc/apache2/conf/SAIwebui.soap.conf** file.
7. Comment out (by adding the **#** symbol at the beginning of each line) the following lines:

   <IfDefine SSL>
   SSLVerifyClient optional
   SSLVerifyDepth 10
   SSLOptions +StrictRequire
   **SSLRequire (%{REMOTE_ADDR} eq "127.0.0.1" or **
   %{SSL_CLIENT_VERIFY} eq "SUCCESS")
   </IfDefine>
   <IfDefine !SSL>

```
    Order Allow,Deny
    Allow from localhost
</IfDefine>
```

8 Save and close the file.

9 Follow these instructions to restart the httpd process.

   a Type **svcadm -v disable -st http** and then press **Enter**.

   b Type **svcadm refresh http** and then press **Enter**.

   c Type **svcadm -v enable -s http** and then press **Enter**.

Implement TLS/SSL on the ISDS

Certificate File Overview

For configuration options 2 through 5, from ***Overview*** (on page 210), certificates must be implemented on both the billing system and the BOSS interface of the ISDS. On the ISDS, the HTTP-S server cannot be used until the necessary certificates and other required files are created and deployed. Before the BOSS interface of the ISDS can be used, you need to deploy certificates signed by an internal CA or a commercial CA. The following is a high level overview of the files required on the HTTP-S server and client, and how they are created:

Private Key — A private key file must be created for the HTTP-S server. This file must be well guarded and should never leave the HTTP-S server. It is preferable to generate the private key file on the HTTP-S server itself. The private key file is typically identified by the .key extension.

Certificate Signing Request (CSR) — A CSR file must be created for the HTTP-S server for the certificate authority (CA) to sign. This file includes the HTTP-S server identity information and a public key. The CSR is digitally signed (encrypted) with the private key. The CSR file is sent to the CA to sign. The CSR file is typically identified by the .csr extension.

HTTP-S Server Certificate — The CA receives the CSR file and, if necessary, verifies that the originator of the CSR is genuine; that is, the sender of the CSR is who they say they are. The CA will then digitally sign the CSR with the private key of the CA. This creates the certificate file for the HTTP-S server. The certificate file is typically identified by the .crt extension.

HTTP-S Client Certificate — If Client Authentication is required by the billing server, then a client certificate must be created. The same steps outlined in the previous three items can be used to create the client certificate. Note that you can use the one certificate for both the server certificate and client certificate.

Certificate Authority Certificates — The certificate authority will have one or more self-signed certificates, the root certificates, and possibly intermediate certificates, which are CA certificates signed using a root certificate or another intermediate certificate. These certificates contain information about the CA, including the CA's website, the CA's public key, and are digitally signed with the appropriate CA private key. The CA can be you, someone in your company, or can be a commercial CA such as VeriSign.

Certificate Chain — The succession of certificates starting from the server or client certificate to the root certificate make up a certificate chain. The shortest possible certificate chain is two: the server or client certificate and a root CA certificate. This occurs when the server or client certificate is signed by the root CA private key. To decrease the risk of compromising the root CA's private key, some Certificate Authorities only use an intermediate certificate authority to sign server or client certificates. It is also possible to use an intermediate CA to sign another intermediate CA certificate, thus the certificate chain becomes longer.

CA Certificate Chain — A CA certificate chain is the succession of intermediate CA certificates to the root certificate. If a server or client certificate is signed by the root CA, then the CA certificate chain contains only the root certificate. If a server or client certificate is signed by an intermediate CA, then the CA certificate chain contains all intermediate CA certificates and the root certificate. For example if the client or server certificate was signed by intermediate CA 2 and the intermediate CA 2 certificate was signed by intermediate CA 1 which was signed by the root CA, then intermediate CA 2, intermediate CA 1, and the root certificate make up the CA certificate chain. The cachain.crt file on the ISDS must contain the entire CA certificate chain for the ISDS server certificate. The cacert.pem file on the ISDS must contain the entire CA certificate chain for the ISDS client certificate

Trusted Certificate Authorities — For an HTTP-S client to trust an HTTP-S server's certificate, the HTTP-S client must trust the server's root CA certificate. If client authentication is enabled on the HTTP-S server, the server must trust the client's root CA certificate. Web browsers, a type of HTTP-S client, typically include a set of trusted root CA certificates for companies such as VeriSign.The cacert.pem file on the ISDS must contain all of the trusted root CA certificates

Certificate Files Required on the ISDS

Two lists of certificate files for the ISDS BOSS interface follow. The first list contains the certificate files required for the billing invoke message when the ISDS BOSS interface acts as an HTTP-S server. The second list contains the certificates files required for the billing response message when the ISDS BOSS interface acts as an HTTP-S client. Note that the cacert.pem file is used for multiple purposes.

Note: All of the following files exist in the /etc/opt/certs directory on the ISDS.

- ISDS BOSS Server
  - server key — The server private key.
  - server.crt — The server signed certificate.

- cachain.crt — The server certificate CA certificate chain. This file must contain the entire CA certificate chain used to sign the server certificate.
- cacert.pem — If client authentication is implemented, then this file must contain the root CA certificate for the Billing System client certificate.

- ISDS BOSS Client
  - bossclient.key — A concatenation of the client private key and client certificate. Until CR 101109 is resolved, this file must exist even if client authentication is not required by the billing system.
    Note: It is possible to set the name of the concatenated file to a value other than bossclient.key, using the BOSS_CLIENT_SSL_KEYFILE environment variable. This environment variable is not utilized in the steps within this guide. If the environment variable is utilized, it must be defined in the /export/home/dncs/.profile file. Additionally, the file referenced by the environment variable must be readable ONLY by the dncs role.
  - cacert.pem — This file must contain the root CA certificate for the billing system server certificate. This file must contain the entire CA certificate chain used to sign the ISDS certificate.
    Note: It is possible to define a different file than the cacert.pem file using the BOSS_SSL_CACERTS environment variable. This environment variable is not utilized in the steps within this guide. If the environment variable is utilized, it must be defined in the /export/home/dncs/.profile file. Additionally, the file referenced by the environment variable must be readable by the dncs role.

Certificate Deployment Options

The Open Source toolkit (openssl) from the OpenSSL Project collaborative is included with the ISDS. This tool can be used to create the private key and the CSR file. It can also be used to create a CA on the ISDS, allowing you to sign and install your own CA certificates. For more information on the Open Source toolkit and for documentation on toolkit commands, go to: http://www.openssl.org. The ISDS also includes a custom certificate creation and signing tool called gen_crt. The provided instructions direct you to use the appropriate tool. There are several different methods for creating and signing certificates. Instructions for these methods are detailed in the following sections:

- ***Generating and Deploying Self-Signed SSL Certificates*** (on page 220)
- ***Generating and Deploying SSL Certificates Signed by a CA on an ISDS*** (on page 227)
- ***Deploying SSL Certificates Signed by an External CA*** (on page 236)

Notes:

- Use the root user to execute all commands in this section. The following commands log the user on as root user:
  1. If necessary, open an xterm window on the ISDS.
  2. Type **su -** and press **Enter**. The password prompt appears.
  3. Type the root password and then press **Enter**.
- To implement TLS/SSL for the BOSS interface on the ISDS, it is helpful to have an understanding of TLS/SSL, the certificate generation process, and HTTP message flows. The following is a list of websites that can be used as references:
  - https://www.covalent.net/resource/documentation/ers/2.2.0/HTML/ProductGuide/sslfeatures.html
  - http://www.freesoft.org/CIE/Topics/121.htm
  - http://en.wikipedia.org/wiki/Secure_Sockets_Layer
- Be sure to carefully plan for the implementation of TLS/SSL for the BOSS interface on the ISDS. Implementation of TLS/SSL should not be attempted during the upgrade maintenance window unless you have thoroughly planned for it and are well-prepared.
- Certificate expiration dates must be closely managed to ensure stability of the BOSS Interface.

Use the ISDS gen_crt SSL Configuration Utility for Generating SSL Certificates

The ISDS gen_crt SSL Configuration Utility includes options to execute several of the steps necessary to generate and deploy SSL certificates. The following is an overview of the utility options:

- Option 1: The ISDS gen_crt SSL Configuration Utility creates a self-signed SSL certificate (server.crt) and private key (server.key). This option is used as part of the ***Generating and Deploying Self-Signed SSL Certificates*** (on page 220) method.
- Option 2: The ISDS gen_crt SSL Configuration Utility generates a private key (server.key) and a Certificate Signing Request (CSR) file (server.csr) in the /etc/opt/certs directory. The CSR must be signed by a CA on an ISDS, or by an external CA.
- Option 3: Not used.
- Option 4: Not used.
- Option 5: This option allows you to check that the necessary files are available and, if so, enables HTTP-S.
  - If all needed files are available, HTTP-S is enabled.
  - If any required files are not available, this option provides detailed information about missing files.

Generating and Deploying Self-Signed SSL Certificates

This section provides step-by-step instructions for generating and deploying self-signed SSL certificates. The gen_crt utility is used to create and deploy a self-signed SSL certificate (server.crt) and private key (server.key) on the ISDS server.

To use the ISDS gen_crt SSL Configuration Utility to create and deploy self-signed SSL certificates, complete the following steps:

1 From an xterm window on the ISDS, type **/dvs/tools/bin/gen_crt** and then press **Enter**. The system displays a message similar to the following:

Prepare SSL certificate for HTTPS service. HTTPS will not be supported on this host without an SSL certificate in place. Choose from following options:

1. Generate a self-signed SSL certificate and deploy now. You will need to manually deploy the certificate to those clients connecting to this server.

2. Generate a certificate signing request for the server certificate and proceed. No SSL certificate will be deployed, you will need to sign the generated CSR

file externally and manually deploy it.

3. Skip this step now and manually deploy SSL certificate later. Refer to the system User's Guide for instructions.

4. Import a server certificate for use by openssl and apache.

5. Check dependencies and enable apache SSL.

Please enter your choice: [1|2|3|4|5]

2 Select choice **1** and then press **Enter**. The command prompts you for the X.509 attributes of the certificate.

3 Use these guidelines to answer the prompt displayed in step 2.

Note: We recommended that you provide valid input for the X.509 information. Use a period (.) to indicate blank input.

- **Country Name —** The country where your company resides. Use the two-letter country code without punctuation for country (for example, US or FR).
- **State or Province —** The state or province where your company resides. Spell out the state completely (for example, California). Do not abbreviate the state or province name.
- **Locality or City —** The city or town where your company resides (for example, Berkeley).
- **Organization Name —** Your company's name (for example, XYZ Corporation). If your company or department name has an **&**, @, or any other symbol that requires using the **Shift** key in its name, you must spell out the symbol or omit it.
- **Organizational Unit —** The organization within the company. This field is optional but can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press **Enter**.
- **Common Name —** The Common Name is the host plus the domain name (for example, www.company.com or *.company.com). For the ISDS, use the IP address of the billing interface.
- **Email Address —** E-mail address of the certificate requester.

Result: The system creates the server.crt and server.key files in the /etc/opt/certs directory.

Note: The system may generate errors concerning the missing cachain.crt file, missing cacert.pem files, as well as that apache will not start. These errors are expected.

4 Type **chmod 400 /etc/opt/certs/server.key** and then press **Enter**. The system sets the file permissions to read-only for the root user.

5 Follow these instructions to link the server.crt file to the cachain.crt file, and to ensure that the file is globally readable.

   a Type **ln -s /etc/opt/certs/server.crt /etc/opt/certs/cachain.crt** and then press **Enter**.

   b Type **chmod 444 /etc/opt/certs/server.crt** and then press **Enter**.

6 Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's HTTP-S server certificate and place it in the /etc/opt/certs directory of the ISDS.

7 Follow these instructions to copy the billing system's HTTP-S server root CA certificate to the list of trusted certificate authorities and to ensure that the file is globally readable.

   a Type **cat [billing server Root CA Crt] >> cacert.pem** and then press **Enter** to create or append the cacert.pem file.

   Note: Replace [Billing Server Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS server certificate.

   Important: Do not attempt to append the root CA certificate to the cacert.pem file using a text editor.

   b Type **chmod 444 /etc/opt/certs/cacert.pem** and then press **Enter**.

8 Select one of the following options:

- If the billing system's HTTP-S server does not utilize client authentication, then go to step 9.
- If the billing system uses the same certificate for both the server and the client, then go to step 10.
- If the billing system uses two separate root CAs (one to sign the server certificate and one to sign the client certificate), then follow these instructions:

   a Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's client certificate and place it in the /etc/opt/certs directory of the ISDS.

   b Type **cat [Billing Client Root CA Crt] >> cacert.pem** and then press **Enter** to append the CA certificate to the cacert.pem file.

   Note: Replace [Billing Client Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS-server certificate. Do not attempt to append the second CA Certificate to the cacert.pem file using a text editor.

c Go to step 10.

9 If the billing system's HTTP-S client does not support client authentication or client authentication is not required then follow these instructions to disable client authentication on the ISDS HTTP-S server.

Note: The ISDS HTTP-S server uses client authentication by default, which requires the billing system's HTTP-S client to support client authentication.

a Use a text editor to open the **/etc/apache2/ssl.conf** file.

b Comment out (add **#** to the beginning of the line) the **SSLVerifyClient require** line.

c Save and close the file.

d Type **grep SSLVerifyClient /etc/apache2/ssl.conf** and then press **Enter** to verify that the file was updated successfully.

Result: Your output should look similar to:
#SSLVerifyClient require

e Use a text editor to open the **/etc/apache2/conf/SAIwebui.soap.conf** file.

f Comment out (add **#** to the beginning of the line) the following lines:

```
<IfDefine SSL>
    SSLVerifyClient optional
    SSLVerifyDepth  10
    SSLOptions +StrictRequire
    SSLRequire ( %{REMOTE_ADDR} eq "127.0.0.1" or \
            %{SSL_CLIENT_VERIFY} eq "SUCCESS" )
</IfDefine>

<IfDefine !SSL>
    Order Allow,Deny
    Allow from localhost
</IfDefine>
```

g Save and close the file.

h Continue with step 10.

10 Complete the following steps to concatenate the ISDS client private key and client certificate into the bossclient.key file.

Notes:

- Until CR 101109 is resolved, this file must exist even if client authentication is not required by the billing system HTTP-S server.
- Unless a separate client certificate is required, the server certificate should be used. If a unique client certificate is required, then temporarily move the server.key and server.crt files to alternate names, repeat steps 1 through 3, and then move the original server.key and server.crt files back after the completion of this step. Finally, provide a copy of the client.crt file to the billing system administrator for use as the trusted root CA certificate.

a Type **cd /etc/opt/certs** and then press **Enter**.

b Type **cat server.key server.crt >> bossclient.key** and then press **Enter** to create the necessary file for the BOSS client to return a client certificate when requested by the billing server.

c Type **chown dncs:dncs bossclient.key** and then press **Enter** to set the ownership to the dncs role and dncs group.

d Type **chmod 400 bossclient.key** and then press **Enter** to set the necessary file permissions.

e Type **cat server.crt >> cacert.pem** and then press **Enter** to add the BOSS HTTP-S client CA chain to the cacert.pem file.

11 Type **/dvs/tools/bin/gen_crt** and then press **Enter** to verify the configuration and

to enable HTTP-S.

Result: The output from this command is similar to what is displayed after executing step 1.

12 Select choice **5** and then press **Enter**.

13 Follow these instructions to verify that the http service started properly.

a Type **ps -ef | grep http** and then press **Enter**. Output should look similar to the following:

```
root  4705    1   0 23:14:12 ?        0:01 /usr/apache2/bin/httpd -k start -DSSL
dncs  4710  4705   0 23:14:13 ?        0:00 /usr/apache2/bin/httpd -k start -DSSL
dncs  4709  4705   0 23:14:13 ?        0:01 /usr/apache2/bin/httpd -k start -DSSL
```

b Type **lsof -i :443** and then press **Enter**. Output should look similar to the following:

```
httpd   4705 root  258u  IPv4 0x6001b2cdd00      0t0  TCP *:443 (LISTEN)
httpd   4709 dncs  258u  IPv4 0x6001b2cdd00      0t0  TCP *:443 (LISTEN)
httpd   4710 dncs  258u  IPv4 0x6001b2cdd00      0t0  TCP *:443 (LISTEN)
```

14 Does the output match what is displayed in steps 13 a and 13 b?

- If **yes**, go to step 15.
- If **no**, follow these instructions.

a Type **svcadm -v disable -st http** and then press **Enter**.
b Type **svcadm refresh http** and then press **Enter**.
c Type **svcadm -v enable -s http** and then press **Enter**.
d Repeat steps 13 and 14.

15 Copy the /etc/opt/certs/server.crt file from the ISDS host to the appropriate location on the billing system for use as the root CA certificate. The server.crt file is used for the ISDS BOSS root CA certificate because the server certificate is self-signed. Use the appropriate command for the billing system (openssl, keytool, browser import, or another mechanism) to ensure that the billing system recognizes the ISDS BOSS self-signed certificate.

16 After the ISDS is configured, you can verify that the BOSS HTTP-S server certificates are created and deployed correctly by completing the following steps.

a To verify that ISDS BOSS HTTP-S server is accessible from a client, use a web browser to access: **https://[ip_address_of_ISDS_host]**.

Results:

– When Client Authentication is enabled on the ISDS, the web browser should prompt you to select a certificate to send back to the ISDS, similar to this example:

– When Client Authentication is disabled on the ISDS, the web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b To verify the billing system HTTP-S server is accessible from the ISDS, use Firefox on the ISDS and enter the following in the address bar: **https://[ip_address_of_Billing_System_host]**.

Generating and Deploying SSL Certificates Signed by a CA on an ISDS

This section provides step-by-step instructions for generating the ISDS BOSS interface private key and (CSR) file, creating the ISDS BOSS interface certificate by signing the CSR file using a CA on an ISDS, and deploying the signed certificate. The gen_crt utility is used to create the private key and CSR file, as well as deploying the

signed certificate (server.crt) on the ISDS BOSS HTTP-S server. The openssl tool is used to create the CA on an ISDS and sign the ISDS BOSS interface certificate. Please note that these instructions implement one certificate for the ISDS BOSS interface; that is, the same certificate is used for the ISDS BOSS HTTP-S server and HTTP-S client.

Notes:

- In these instructions, ISDS refers to the system that needs a certificate. ISDS CA refers to the ISDS that was chosen to be the CA. The ISDS and ISDS CA can be the same system.
- If a CA has not been created on the chosen ISDS, then follow the steps in ***Create Your Own Certificate Authority*** (on page 244).

To create, and deploy SSL certificates using an ISDS CA, complete the following steps.

1. From an xterm window on the ISDS, type **/dvs/tools/bin/gen_crt** and then press **Enter**. The system displays a message similar to the following:

   Prepare SSL certificate for HTTPS service. HTTPS will not be supported on this host without an SSL certificate in place. Choose from following options:

   1. Generate a self-signed SSL certificate and deploy now. You will need to manually deploy the certificate to those clients connecting to this server.

   2. Generate a certificate signing request for the server certificate and proceed. No SSL certificate will be deployed, you will need to sign the generated CSR file externally and manually deploy it.

   3. Skip this step now and manually deploy SSL certificate later. Refer to the system User's Guide for instructions.

   4. Import a server certificate for use by openssl and apache.

   5. Check dependencies and enable apache SSL.

   Please enter your choice: [1|2|3|4|5]
2. Select choice **2** and then press **Enter**. The command prompts you for the X.509 attributes of the certificate.
3. Use these guidelines to answer the prompt displayed in step 2.

   Note: We recommended that you provide valid input for the X.509 information. Use a period (.) to indicate blank input.

   - **Country Name —** The country where your company resides. Use the two-letter country code without punctuation for country (for example, US or FR).
   - **State or Province —** The state or province where your company resides. Spell out the state completely (for example, California). Do not abbreviate the state

or province name.

- **Locality or City —** The city or town where your company resides (for example, Berkeley).
- **Organization Name —** Your company's name (for example, XYZ Corporation). If your company or department name has an **&**, **@**, or any other symbol that requires using the **Shift** key in its name, you must spell out the symbol or omit it.
- **Organizational Unit —** The organization within the company. This field is optional but can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press **Enter**.
- **Common Name —** The Common Name is the host plus the domain name (for example, www.company.com or *.company.com). For the ISDS, use the IP address of the billing interface.
- **Email Address —** E-mail address of the certificate requester.
- **Challenge Password —** Type **.** and then press **Enter**.
- **Optional Company Name —** Type **.** and then press **Enter**.

Result: The ISDS creates the CSR file (server.csr) and private key file (server.key) in the /etc/opt/certs directory.

4 Type **chmod 400 /etc/opt/certs/server.key** and then press **Enter**. The system sets the file permissions to read-only for the root user.

5 Copy the **/etc/opt/certs/server.csr** file from the ISDS to the ISDS CA **/export/home/dncs/isdsCA/** directory.

6 Follow these steps to create the certificate file by signing the CSR on the ISDS CA.

a If necessary, open an xterm window on the ISDS CA.

b Type **cd /export/home/dncs/isdsCA** and press **Enter**.

c Type **/dvs/tools/openssl/bin/openssl x509 -req -days [days] -in server.csr -CA ca.crt -CAkey ca.key -set_serial [SN] -out server.crt** and then press **Enter**.

Notes:

– Replace [days] with the number of days the ISDS certificate will be valid.

– Replace [SN] with a unique serial number for this certificate. This can be a decimal number or hexadecimal value if preceded by 0x (e.g. **0xDEADFACE**).

d When prompted, enter the ca.key pass phrase that was created in ***Create Your Own Certificate Authority*** (on page 244). The openssl x509 command saves the new certificate file, server.crt, in the current working directory, /export/home/dncs/isdsCA.

e Copy the newly created /export/home/dncs/isdsCA/server.crt file from the ISDS CA to the ISDS /etc/opt/certs/ directory.

f Copy the ISDS CA certificate file, /export/home/dncs/isdsCA/ca.crt, to the ISDS /etc/opt/certs/ directory.

g Type **rm /export/home/dncs/isdsCA/server.crt** and then press **Enter** to delete the server.crt file from the ISDS CA.

h Type **exit** and then press **Enter** to exit from the ISDS CA.

7 If necessary, go back to the /etc/opt/certs directory on the ISDS by typing **cd /etc/opt/certs** and pressing **Enter** in the xterm window.

8 Type **chmod 444 server.crt** and then press **Enter** to ensure that the certificate is globally readable.

9 Follow these instructions to copy the ISDS CA certificate into the cachain.crt file and to ensure that the file is globally readable.

a Type **cp ca.crt cachain.crt** and then press **Enter**.

b Type **chmod 444 cachain.crt** and then press **Enter**.

10 Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's HTTP-S server certificate and place it in the /etc/opt/certs directory of the ISDS.

11 Follow these instructions to copy the billing system's HTTP-S server root CA certificate to the list of trusted certificate authorities and to ensure that the file is globally readable:

a Type **cat [billing server Root CA Crt] >> cacert.pem** and then press **Enter** to create or append the cacert.pem.

Note: Replace [Billing Server Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS server certificate.

Important: Do not attempt to append the root CA certificate to the cacert.pem file using a text editor.

b Type **chmod 444 /etc/opt/certs/cacert.pem** and then press **Enter**.

12 Select one of the following options:

- If the billing system HTTP-S client does not support client authentication or client authentication is not required, then go to step 13.
- If the billing system uses the same certificate for both the server and the client, then go to step 14.
- If the billing system uses two separate root CAs, one to sign the server certificate and one to sign the client certificate, then complete the following steps.

a Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's HTTP S client certificate and place it in the /etc/opt/certs directory on the ISDS.

b Type **cat [Billing Client Root CA Crt] >> cacert.pem** and then press **Enter** to append the CA Certificate to the cacert.pem file.

Note: Replace [Billing Client Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS client certificate.

Important: Do not attempt to append the root CA certificate to the cacert.pem file using a text editor.

c Go to step 14.

13 The ISDS HTTP-S server uses client authentication by default, which requires the billing system's HTTP S client to support client authentication. If the billing system's HTTP S client does not support client authentication or client authentication is not required, then complete the following steps to disable client authentication on the ISDS.

a Use a text editor to open the **/etc/apache2/ssl.conf** file.

b Comment out (add **#** to the beginning of the line) the **SSLVerifyClient require** line.

c Save and close the file.

d Type **grep SSLVerifyClient /etc/apache2/ssl.conf** and then press **Enter** to verify that the file was updated successfully. You should see output similar to the following example:

#SSLVerifyClient require

e Use a text editor to open the **/etc/apache2/conf/SAIwebui.soap.conf** file.

f Comment out (add # to the beginning of the line) the following lines:

```
<IfDefine SSL>
    SSLVerifyClient optional
    SSLVerifyDepth  10
    SSLOptions +StrictRequire
    SSLRequire ( %{REMOTE_ADDR} eq "127.0.0.1" or \
            %{SSL_CLIENT_VERIFY} eq "SUCCESS" )
</IfDefine>

<IfDefine !SSL>
    Order Allow,Deny
    Allow from localhost
</IfDefine>
```

g Save and close the file.

14 Complete the following steps to concatenate the ISDS client private key and client certificate into the bossclient.key file.

Notes:

- Until CR 101109 is resolved, this file must exist even if client authentication is not required by the billing system HTTP-S server.
- Unless a separate client certificate is required, the server certificate should be used. If a unique client certificate is required, then temporarily move the server.key, server.csr, and server.crt files to alternate names, repeat steps 1 through 7, and finally move the original server.key, server.csr, and server.crt files back after the completion of this step.

a Type **cd /etc/opt/certs** and then press **Enter**.

b Type **cat server.key server.crt >> bossclient.key** and then press **Enter** to create the necessary file for the BOSS client to return a client certificate when requested by the billing server.

c Type **chown dncs:dncs bossclient.key** and then press **Enter** to change the owner to the dncs role and group to dncs.

d Type **chmod 400 bossclient.key** and then press **Enter** to set the necessary file permissions.

e Type **cat ca.crt >> cacert.pem** and press **Enter** to add the BOSS HTTP-S client CA chain to the cacert.pem file.

15 Type **/dvs/tools/bin/gen_crt** and then press **Enter** to verify the configuration and enable HTTP-S.

Result: Your output should be identical to what was displayed after running

step 1.

16 Select choice **5** and then press **Enter**.

17 Run the following commands to verify that the http service started properly.

a Type **ps -ef | grep http** and press **Enter**. Output should be similar to the following:

```
root  4705    1   0 23:14:12 ?        0:01 /usr/apache2/bin/httpd -k start -DSSL
dncs  4710  4705   0 23:14:13 ?        0:00 /usr/apache2/bin/httpd -k start -DSSL
dncs  4709  4705   0 23:14:13 ?        0:01 /usr/apache2/bin/httpd -k start -DSSL
```

b Type **lsof -i :443** and then press **Enter**. Output should be similar to the following:

```
httpd   4705 root  258u  IPv4 0x6001b2cdd00      0t0  TCP *:443 (LISTEN)
httpd   4709 dncs  258u  IPv4 0x6001b2cdd00      0t0  TCP *:443 (LISTEN)
httpd   4710 dncs  258u  IPv4 0x6001b2cdd00      0t0  TCP *:443 (LISTEN)
```

18 Does the output match what is displayed in steps 17 a and 17 b?

- If **yes**, go to step 19.
- If **no**, follow these instructions.

a Type **svcadm -v disable -st http** and then press **Enter**.
b Type **svcadm refresh http** and then press **Enter**.
c Type **svcadm -v enable -s http** and then press **Enter**.
d Repeat steps 17 and 18.

19 Copy the /export/home/dncs/isdsCA/ca.crt file from the ISDS CA to the appropriate location on the billing system for use as the trusted root CA certificate. Use the appropriate command for the billing system (openssl, keytool, browser import, or another mechanism) to ensure that the billing system recognizes the ISDS BOSS certificate(s).

20 After the ISDS is configured you can verify that the BOSS HTTP-S server certificates are created and deployed correctly by completing the following steps:

a To verify that ISDS BOSS HTTP-S server is accessible from a client, use a web browser to access: **https://[ip_address_of_ISDS_host]**.

Results:

– When Client Authentication is enabled on the ISDS, the web browser should prompt you to select a certificate to send back to the ISDS, similar to this example:

– When Client Authentication is disabled on the ISDS, the web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b To verify the billing system HTTP-S server is accessible from the ISDS, use Firefox on the ISDS and enter the following in the address bar: **https://[ip_address_of_Billing_System_host]**.

Deploying SSL Certificates Signed by an External CA

This section provides step-by-step instructions for generating the ISDS BOSS interface private key and CSR files, and then deploying the Certificate signed by the external CA. The gen_crt utility is used to create the private key and CSR file, as well as deploying the signed certificate (server.crt) on the ISDS BOSS interface. Note that

these instructions implement one certificate for the ISDS BOSS interface; that is, the same certificate is used for the ISDS BOSS HTTP-S server and HTTP-S client.

The Certificate Authority can be someone or some group within your company or a commercial CA, such as VeriSign.

To create, and deploy SSL certificates using an External CA, complete the following steps.

1 From an xterm window on the ISDS, type **/dvs/tools/bin/gen_crt** and then press **Enter**. The system displays a message similar to the following:

Prepare SSL certificate for HTTPS service. HTTPS will not be supported on this host without an SSL certificate in place. Choose from following options:

1. Generate a self-signed SSL certificate and deploy now. You will need to manually deploy the certificate to those clients connecting to this server.

2. Generate a certificate signing request for the server certificate and proceed. No SSL certificate will be deployed, you will need to sign the generated CSR file externally and manually deploy it.

3. Skip this step now and manually deploy SSL certificate later. Refer to the system User's Guide for instructions.

4. Import a server certificate for use by openssl and apache.

5. Check dependencies and enable apache SSL.

Please enter your choice: [1|2|3|4|5]

2 Select choice **2** and then press **Enter**.

3 Use these guidelines to answer the prompt displayed in step 2.

Note: We recommended that you provide valid input for the X.509 information. Use a period (.) to indicate blank input.

- **Country Name —** The country where your company resides. Use the two-letter country code without punctuation for country (for example, US or FR).
- **State or Province —** The state or province where your company resides. Spell out the state completely (for example, California). Do not abbreviate the state or province name.
- **Locality or City —** The city or town where your company resides (for example, Berkeley).
- **Organization Name —** Your company's name (for example, XYZ Corporation). If your company or department name has an **&**, **@**, or any other symbol that requires using the **Shift** key in its name, you must spell out the symbol or omit it.
- **Organizational Unit —** The organization within the company. This field is

optional but can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press **Enter**.

- **Common Name —** The Common Name is the host plus the domain name (for example, www.company.com or *.company.com). For the ISDS, use the IP address of the billing interface.
- **Email Address —** E-mail address of the certificate requester.
- **Challenge Password —** Type **.** and then press **Enter**.
- **Optional Company Name —** Type **.** and then press **Enter**.

Result: The ISDS creates the CSR file (server.csr) and private key file (server.key) in the /etc/opt/certs directory.

4 Type **chmod 400 /etc/opt/certs/server.key** and then press **Enter**. The system sets the file permissions to read-only for the root user.

5 Send a copy of the /etc/opt/certs/server.csr file from the ISDS to the external CA for signing.

6 After the signed ISDS certificate is returned, copy the certificate into the /etc/opt/certs/ directory.

7 From an xterm window on the ISDS, type **cd /etc/opt/certs** and then press **Enter**.

8 Type **mv [certificate] server.crt** and then press **Enter**.

Note: Replace [certificate] with the name of the signed certificate file from the external CA.

9 Type **chmod 444 server.crt** and then press **Enter** to ensure that the certificate is globally readable.

10 Obtain a copy of the external CA's certificate chain, the root CA certificate, and any intermediate CA certificates, that were used to sign the ISDS BOSS HTTP-S server certificate. Then, place it in the /etc/op/certs/ directory.

11 Type **cat [caCertificateChain] >> cachain.crt** and then press **Enter** to create the cachain.crt file on the ISDS.

Note: Replace [caCertificateChain] with the name of the file that contains the external CA root and any intermediate certificates used to sign the ISDS BOSS HTTP-S server certificate.

12 Type **chmod 444 cachain.crt** and then press **Enter** to set the cachain.crt file permissions to *read* for all.

13 Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's HTTP-S server certificate and place it in the /etc/opt/certs

directory of the ISDS.

14 Follow these instructions to copy the billing system's HTTP-S server root CA certificate to the list of trusted certificate authorities and to ensure that the file is globally readable.

a Type **cat [billing server Root CA Crt] >> cacert.pem** and then press **Enter** to create or append the cacert.pem.

Note: Replace [Billing Server Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS server certificate.

Important: Do not attempt to append the root CA certificate to the cacert.pem file using a text editor.

b Type **chmod 444 /etc/opt/certs/cacert.pem** and then press **Enter**.

15 Select one of the following options:

- If the billing system HTTP-S client does not support Client Authentication or if client authentication is not required, then go to step 16.
- If the billing system uses the same certificate for both the server and the client, then go to step 17.
- If the billing system uses two separate root CAs, one to sign the server certificate and one to sign the client certificate, then complete the following steps.

a Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's HTTP S client certificate and place it in the /etc/opt/certs directory on the ISDS.

b Type **cat [Billing Client Root CA Crt] >> cacert.pem** and then press Enter to append the CA certificate to the cacert.pem file.

Note: Replace [Billing Client Root CA Crt] with the root CA certificate in the CA certificate chain used to sign the billing system's HTTPS client certificate.

Important: Do not attempt to append the CA certificate to the cacert.pem file using a text editor.

c Go to step 17.

16 The ISDS HTTP-S server uses client authentication by default, which requires the billing system's HTTP-S client to support client authentication. If the billing system's HTTP-S client does not support client authentication, or if client authentication is not required, then complete the following steps to disable client authentication on the ISDS.

a Use a text editor to open the /etc/apache2/ssl.conf file.

b Comment out (add **#** to the beginning of the line) the **SSLVerifyClient**

require line.

c Save and close the file.

d Type **grep SSLVerifyClient /etc/apache2/ssl.conf** and the press **Enter** to verify that the file was updated successfully. Output should look similar to the following example:

#SSLVerifyClient require

e Use a text editor to open the **/etc/apache2/conf/SAIwebui.soap.conf** file.

f Comment out (add **#** to the beginning of the line) the following lines:

```
<IfDefine SSL>
    SSLVerifyClient optional
    SSLVerifyDepth  10
    SSLOptions +StrictRequire
    SSLRequire ( %{REMOTE_ADDR} eq "127.0.0.1" or \
            %{SSL_CLIENT_VERIFY} eq "SUCCESS" )
</IfDefine>

<IfDefine !SSL>
    Order Allow,Deny
    Allow from localhost
</IfDefine>
```

g Save and close the file.

17 Complete the following steps to concatenate the ISDS client private key and client certificate into the bossclient.key file.

Notes:

- Until CR 101109 is resolved, this file must exist even if client authentication is not required by the billing system HTTP-S server.
- Unless a separate client certificate is required, the server certificate should be used. If a unique client certificate is required, then temporarily move the server.key, server.csr, and server.crt files to alternate names, repeat steps 1 through 7. Finally, move the original server.key, server.csr, and server.crt files back after the completion of this step.

a Type **cd /etc/opt/certs** and then press **Enter**.

b Type **cat server.key server.crt >> bossclient.key** and then press **Enter** to create the necessary file for the BOSS client to return a client certificate when requested by the billing server.

c Type **chmod 444 bossclient.key** and then press **Enter** to set the necessary file permissions.

d Obtain a copy of the external CA's certificate chain, the root CA certificate, and any intermediate CA certificates, that were used to sign the ISDS BOSS HTTP-S certificate. Then, place it in the /etc/op/certs/ directory.

e Type **cat [caCertificateChain] >> cacert.pem** and then press **Enter** to add the CA certificate chain to the cacert.pem file.

Note: Replace [caCertificateChain] with the name of the file that contains external CA's root and any intermediate certificates used to sign the ISDS BOSS HTTP-S certificate.

18 Type /**dvs/tools/bin/gen_crt** and then press **Enter** to verify the configuration and enable HTTP-S.

Result: Your output should be identical to what was displayed after running step 1.

19 Select choice **5** and then press **Enter**.

20 Run the following commands to verify that the http service started properly.

a Type **ps -ef | grep http** and press **Enter**. Output should be similar to the following:

```
root  4705    1   0 23:14:12 ?        0:01 /usr/apache2/bin/httpd -k start -DSSL
dncs  4710  4705   0 23:14:13 ?        0:00 /usr/apache2/bin/httpd -k start -DSSL
dncs  4709  4705   0 23:14:13 ?        0:01 /usr/apache2/bin/httpd -k start -DSSL
```

b Type **lsof -i :443** and then press **Enter**. Output should be similar to the following:

```
httpd   4705 root  258u  IPv4 0x6001b2cdd00      0t0  TCP *:443 (LISTEN)
httpd   4709 dncs  258u  IPv4 0x6001b2cdd00      0t0  TCP *:443 (LISTEN)
httpd   4710 dncs  258u  IPv4 0x6001b2cdd00      0t0  TCP *:443 (LISTEN)
```

21 Does the output match what is displayed in steps 20 a and 20 b?

- If **yes**, go to step 22.
- If **no**, follow these instructions.

a Type **svcadm -v disable -st http** and then press **Enter**.
b Type **svcadm refresh http** and then press **Enter**.
c Type **svcadm -v enable -s http** and then press **Enter**.
d Repeat steps 20 and 21.

22 Copy the root CA certificate file from the CA certificate chain used to sign the ISDS BOSS HTTP-S certificate(s) to the appropriate location on the billing system for use as the trusted root CA certificate. Use the appropriate command for the billing system (openssl, keytool, browser import, or another mechanism) to ensure that the billing system recognizes the ISDS BOSS HTTP-S certificate(s).

Appendix C
TLS/SSL for the BOSS Interface

23 After the ISDS is configured you can verify that the BOSS HTTP-S server certificates are created and deployed correctly by completing the following steps.

a To verify that ISDS BOSS HTTP-S server is accessible from a client, use a web browser to access: **https://[ip_address_of_ISDS_host]**.

Results:

– When Client Authentication is enabled on the ISDS, the web browser should prompt you to select a certificate to send back to the ISDS, similar to this example:

– When Client Authentication is disabled on the ISDS, the web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b To verify the billing system HTTP-S server is accessible from the ISDS, use Firefox on the ISDS and enter the following in the address bar: **https://[ip_address_of_Billing_System_host]**.

Create Your Own Certificate Authority

A Certificate Authority (CA) is an entity that signs certificate files for web servers and web clients. A CA can exist within a company or on your own computer. There are also commercial CAs, such as VeriSign, that will create certificates for a fee. This section includes instructions for creating a CA on an ISDS. We recommend that you create one CA on only one ISDS within your company. This one CA can be used to sign certificates for all other ISDS servers. This is the preferred method so that only one CA certificate is required for distribution to all other ISDS servers and billing systems. The CA key file will be used every time you sign a certificate and must NEVER leave the ISDS that is acting as the CA. The CA Certificate must be copied to all HTTP-S clients and HTTP-S servers that use Client Authentication that will receive certificates signed by this CA. In other words, the ca.crt file should be propagated to all ISDS servers and associated billing systems.

Follow these steps to create a CA key file (ca.key) and a CA certificate (ca.crt) on the selected ISDS.

1. Log on to the ISDS that will be the CA and open an xterm window.
2. Type **mkdir /export/home/dncs/isdsCA** and then press **Enter** to create a directory for all of the necessary CA files.
3. Type **cd /export/home/dncs/isdsCA** and then press **Enter** to switch to the new directory.

   Important: Ensure that you include this directory in the list of key files that must be backed up and restored for every upgrade.
4. Type **/dvs/tools/openssl/bin/openssl genrsa -des3 -out ca.key 4096** and then press **Enter**. The system prompts you to enter a ca.key pass phrase.

   Notes:

   - This pass phrase is needed every time this CA signs a certificate request.
   - Keep this pass phrase very secure. To ensure the highest level of security, never move or copy the key file to any other system.
   - The **openssl genrsa** command saves the ca.key file in your current working directory.
   - The generated key is a 4096-bit RSA key, which is encrypted using Triple-DES and stored in PEM format so that it is readable as ASCII text.
5. Type **chmod 400 ca.key** and then press **Enter** to change the ca.key file permissions to read-only, for root.

   Important: Keep this key file safely guarded. Any breach of this file will

compromise the root CA certificate trust.

6 Type **/dvs/tools/openssl/bin/openssl req -new -x509 -days [days] -key ca.key -out ca.crt** and then press **Enter** to generate the CA certificate. A prompt for a pass phrase appears.

Note: Replace [Days] with the number of days the root CA certificate is valid. We suggested that this value be as long as possible to reduce the impact of re-deploying signed certificates.

7 Enter the ca.key pass phrase that was just created and then press **Enter**. You are prompted for the following X.509 attributes of the certificate. We recommended that you provide valid input for all X.509 information. Use a period (.) to indicate blank input.

- **Country Name —** The country where your company resides. Use the two-letter country code without punctuation for country (for example, US or FR).
- **State or Province —** The state or province where your company resides. Spell out the state completely (for example, California). Do not abbreviate the state or province name.
- **Locality or City —** The city or town where your company resides (for example, Berkeley).
- **Organization Name —** Your company's name (for example, XYZ Corporation). If your company or department name has an **&**, **@**, or any other symbol that requires using the **Shift** key in its name, you must spell out the symbol or omit it.
- **Organizational Unit —** The organization within the company. This field is optional but can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press **Enter**.
- **Common Name —** The Common Name is the host plus the domain name (for example, www.company.com or *.company.com). For the ISDS, use the IP address of the billing interface.
- **Email Address —** E-mail address of the certificate requester.

8 Type **ls -l** and then press **Enter** to verify that the ca.key and ca.crt files were created successfully. Output should look similar to the following:

-rw-r----- 1 root root 2358 Oct 24 17:30 ca.crt
-r-------- 1 root root 3311 Oct 24 16:28 ca.key

Troubleshooting TLS/SSL on the ISDS

Execute the following commands to verify that the http service started properly.

1 Type **ps -ef | grep http** and press **Enter**. Output should look similar to the following:

root 4705 1 0 23:14:12 ? 0:01 /usr/apache2/bin/httpd -k start -DSSL
dncs 4710 4705 0 23:14:13 ? 0:00 /usr/apache2/bin/httpd -k start -DSSL
dncs 4709 4705 0 23:14:13 ? 0:01 /usr/apache2/bin/httpd -k start -DSSL

Note: If TLS/SSL is not enabled, either no data is displayed or the "-DSSL" will not appear at the end of each line.

2 Type **lsof -i :443** and then press **Enter**. Output should look similar to the following:

httpd 4705 root 258u IPv4 0x6001b2cdd00 0t0 TCP *:443 (LISTEN)
httpd 4709 dncs 258u IPv4 0x6001b2cdd00 0t0 TCP *:443 (LISTEN)
httpd 4710 dncs 258u IPv4 0x6001b2cdd00 0t0 TCP *:443 (LISTEN)

Note: If TLS/SSL is not enabled, either no data is displayed or the "(LISTEN)" will not appear at the end of each line.

3 If the output does not match what is displayed in the first two bullets, complete the following steps.

a Type **svcadm -v disable -st http** and then press **Enter**.

b Type **svcadm refresh http** and then press **Enter**.

c Type **svcadm -v enable -s http** and then press **Enter**.

d Repeat steps 1 through 3.

Log Files to Monitor

The following is a list of several log files that can be monitored for errors related to HTTPS sessions:

- /dvs/dncs/tmp/bossServer.x
  - Type **logLvl bossServer +DEBUG** and then press **Enter** to increase the log level for the bossServer process.
  - Type **logLvl bossServer -DEBUG** and then press **Enter** to reduce the log level for the bossServer process once troubleshooting is complete.
  - Type **logLvl bossServer.soap +DEBUG** and then press **Enter** to increase the log level for the bossServer SOAP process.
  - Type **logLvl bossServer.soap -DEBUG** and then press **Enter** to reduce the log level for the bossServer SOAP process once troubleshooting is complete.

- Files in the /var/apache2/logs directory

Files and Directory Permissions

File and directory permissions are critical for the operation of the web servers on the ISDS. The following is a sample error message from the bossServer log when permissions are incorrect for the /etc/opt/certs/cacert.pem file:

|ERROR|bossServer:BossResponseClientSoap.C(99)|SOAP FAULT: SOAP-ENV:Server SOAP-ENV:Server SSL error Can't read CA file and directory initializing context

The following is a list of the required permissions for the required files and directory:

- drwxr-xr-x 7 root sys 1024 Jul 16 19:41 /etc/opt/certs
- -r-------- 1 root root 887 Jul 16 18:43 server.key
- -r--r--r-- 1 root root 1419 Jul 16 18:43 server.crt
- -r--r--r-- 1 root root 4716 Jul 16 13:53 cachain.crt
- -r-------- 1 dncs dncs 2294 Jul 16 18:39 bossclient.key
- -r--r--r-- 1 root root 9456 Jul 16 19:43 cacert.pem

To View Certificate Files

The following command can be used to view certificate files. Viewing the contents of certificate files can be helpful if the file name is generic.

/dvs/tools/openssl/bin/openssl x509 -text -in [certificate]

Note: Replace [certificate] with the name of the certificate file that you would like to view.

Add Trusted Root CA Certificates

Complete the following procedure to add a trusted root CA certificate to the list of trusted certificate authorities.

1 Obtain a text copy of the root CA certificate and place it in the /etc/opt/certs directory on the ISDS.

Note: The text file must contain the entire certificate starting with **-----BEGIN CERTIFICATE-----** and ending with **-----END CERTIFICATE-----**.

Example:

```
-----BEGIN CERTIFICATE-----
MIICWjCCAcMCAgGlMA0GCSqGSIb3DQEBBAUAMHUxCzAJBgNVBAYTAlVTMRgwFgYD
VQQKEw9HVEUgQ29ycG9yYXRpb24xJzAlBgNVBAsTHkdURSBDeWJlclRydXN0IFNv
bHV0aW9ucywgSW5jLjEjMCEGA1UEAxMaR1RFIEN5YmVyVHJ1c3QgR2xvYmFsIFJv
b3QwHhcNOTgwODEzMDAyOTAwWhcNMTgwODEzMjM1OTAwWjB1MQswCQYDVQQGEwJV
UzEYMBYGA1UEChMPR1RFIENvcnBvcmF0aW9uMScwJQYDVQQLEx5HVEUgQ3liZXJU
cnVzdCBTb2x1dGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDeWJlclRydXN0IEds
b2JhbCBSb290MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCVD6C28FCc6HrH
iM3dFw4usJTQGz0O9pTAipTHBsiQl8i4ZBp6fmw8U+E3KHNgf7KXUwefU/ltWJTS
r41tiGeA5u2ylc9yMcqlHHK6XALnZELn+aks1joNrI1CqiQBOeacPwGFVw1Yh0X4
04Wqk2kmhXBIgD8SFcd5tB8FLztimQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAG3r
GwnpXtlR22ciYaQqPEh346B8pt5zohQDhT37qw4wxYMWM4ETCJ57NE7fQMh017l9
3PR2VX2bY1QY6fDq81yx2YtCHrnAlU66+tXifPVoYb+O7AWXX1uw16OFNMQkpw0P
lZPvy5TYnh+dXIVtx6quTx8itc2VrbqnzPmrC3p/
-----END CERTIFICATE-----
```

2 Open an xterm window on the ISDS as **root**.

3 Type **cd /etc/opt/certs** and then press **Enter**.

4 Type **cp cacert.pem cacert.pem.orig** and then press **Enter** to create a backup copy of the existing cacert.pem file.

5 Type **cat [root CA File] >> cacert.pem** and then press **Enter** to copy the contents of the root CA certificate to the cacert.pem file.

Note: Replace [root CA File] with the file name of the root CA certificate obtained in step 1.

6 Follow these instructions to stop and restart the http process.

- **a** Type **svcadm -v disable -st http** and then press **Enter** to stop the http process.
- **b** Type **svcadm refresh http** and then press **Enter** to refresh the http configuration.
- **c** Type **svcadm -v enable -s http** and then press **Enter** to start the http process.

7 Follow these instructions to stop and restart the bossServer process.

- **a** Type **dncsControl -stop bossServer** and then press **Enter** to stop the bossServer process.
- **b** Type **dncsControl -start bossServer** and then press **Enter** to start the bossServer process.

8 Follow these instructions to verify that the http service started properly.

- **a** Type **ps -ef | grep http** and press **Enter**. Output should look similar to the following:

  root 4705 1 0 23:14:12 ? 0:01 /usr/apache2/bin/httpd -k start -DSSL
  dncs 4710 4705 0 23:14:13 ? 0:00 /usr/apache2/bin/httpd -k start -DSSL
  dncs 4709 4705 0 23:14:13 ? 0:01 /usr/apache2/bin/httpd -k start -DSSL

  Note: If TLS/SSL is not enabled, either no data is displayed or the "-DSSL" will not appear at the end of each line.

- **b** Type **lsof -i :443** and then press **Enter**. Output should look similar to the following:

  httpd 4705 root 258u IPv4 0x6001b2cdd00 0t0 TCP *:443 (LISTEN)
  httpd 4709 dncs 258u IPv4 0x6001b2cdd00 0t0 TCP *:443 (LISTEN)
  httpd 4710 dncs 258u IPv4 0x6001b2cdd00 0t0 TCP *:443 (LISTEN)

  Note: If TLS/SSL is not enabled, either no data is displayed or the "(LISTEN)" will not appear at the end of each line.

9 Log out of the ISDS.

D

Stopping System Components

In This Appendix

Introduction

Use the procedures in this appendix to stop the Application Server and the ISDS application.

Notes:

- The Application Server must be shut down prior to shutting down the ISDS application.
- The Application Server and ISDS application must be shut down prior to shutting down the ISDS Sun Server.

Stop the Application Server on the ISDS

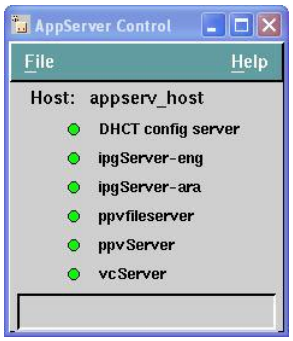
The Application Server can be stopped using the middle mouse button commands from the Keyboard Video Mouse (KVM) connected to the ISDS server or from a command line. Both methods are provided.

Stopping the Application Server Processes Using the Middle Mouse Button

1. If necessary, log on to the ISDS CDE using a dncs administrator account.

   Note: For security purposes, we do not recommend that you log on to the CDE as root user for this task.

2. If necessary, complete the following steps to open the Administrative Console.
   a. Press the middle mouse button and select **Administrative Console**. A console window appears.
   b. If prompted in the console window, type the dncs role password and press **Enter**. The Administrative Console window and Administrative Console Status window open.
3. Click the **Control** button for the AppServer in the ISDS Administrative Console Status window. The AppServer Control window opens.



4. Press the middle mouse button and select **App Serv Stop**. A console window appears.
5. If prompted, type the dncs role password and then press **Enter**. The Application Server processes stop.
6. Monitor the AppServer Control window until the status indicators for all processes turn red.
7. In the AppServer Control window, click **File** and then select **Close**. The window closes.
8. In the App Stop console window, click **File** and then select **Close**. The window closes.

Stopping the Application Server Processes Using the Command Line

1. If necessary, open a console on the ISDS as a dncs administrator or as root.

   Note: The console can be an SSH session or a terminal window on the ISDS.
2. Type **su - dncs** and press **Enter**. The password prompt appears.
3. Type the dncs role password and press **Enter**. The dncs role command line appears.
4. Type **/dvs/appserv/bin/appStop** and press **Enter**. The Application Server processes stop.
5. Wait at least 1 minute and then type **ps -ef | grep app** and press **Enter**. A list of running Application Server processes appears.
6. Do the results from step 5 show that **app_crash_global.d** and **appInitd** are the only processes running?
   - If **yes**, go to step 7.
   - If **no** (there are other processes running), follow these instructions.
     a. Type **/dvs/appserv/bin/appKill** and then press **Enter**.
     b. Repeat steps 5 and 6.
7. Type **exit** and press **Enter** to log out of the dncs role.

Stop the ISDS Application

The ISDS Application can be stopped using the middle mouse button commands from the Keyboard Video Mouse (KVM) connected to the ISDS server or from a command line. Both methods are provided.

Stopping the ISDS Application Processes Using the Middle Mouse Button

1. If necessary, log on to the ISDS CDE using a dncs administrator account.

   Note: For security purposes, we do not recommend that you log on to the CDE as root user for this task.
2. If necessary, complete the following steps to open the Administrative Console.
   a. Press the middle mouse button and select **Administrative Console**. A console window appears.
   b. If prompted in the console window, type the dncs role password and press **Enter**. The Administrative Console window and Administrative Console Status window open.
3. Click the **Control** button for the ISDS in the ISDS Administrative Console Status window. The ISDS Control window opens.
4. Press the middle mouse button and select **ISDS Stop**. A console window appears.
5. If prompted, type the dncs role password and then press **Enter**. The ISDS Application processes stop.
6. Monitor the ISDS Control window until the status indicators for all processes turn red.
7. In the ISDS Control window, click **File** and then select **Close**. The window closes.
8. In the ISDS Stop console window, click **File** and then select **Close**. The window closes.

Stopping the ISDS Application Processes Using the Command Line

1. If necessary, open a console on the ISDS as a dncs administrator or as root.

   Note: The console can be an SSH session or a terminal window on the ISDS.
2. Type **su - dncs** and press **Enter**. A password prompt appears.
3. Type the dncs role password and press **Enter**. The dncs role command line appears.
4. Type **dncsStop** and press **Enter**. The **Are you sure you want to stop the DNCS?**

message appears.

5 Type **y** and press **Enter**. The ISDS Application processes stop.

6 Type **dncsControl** and then press **Enter**. The ISDS Control window appears.

7 Type **2** (for **Startup / Shutdown Single Element Group**) and press **Enter**. The system returns a list of the ISDS processes and their current state.

8 Press **Enter** to refresh the list until the current state is **stopped** for all processes.

9 Type **x** and press **Enter**. The ISDS Control main menu appears.

10 Type **x** and press **Enter**. The ISDS Control window closes and the command line appears.

11 Type **exit** and press **Enter** to log out of the dncs role.

E

Restarting System Components

In This Appendix

Introduction

Use the procedures in this appendix to restart the ISDS application and the Application Server.

Note: The ISDS application must be running before you start the Application Server.

Start the ISDS Application

The ISDS Application can be started using the middle mouse button commands from the Keyboard Video Mouse (KVM) connected to the ISDS server or from a command line. Both methods are provided.

Starting the ISDS Application Processes Using the Middle Mouse Button

Complete the following steps to start the ISDS Application using the middle mouse button from the KVM attached to the ISDS server.

1. If necessary log on to the ISDS CDE using a dncs administrator account.

   Note: For security reasons, we do not recommend that you log on as root user for this task.
2. If necessary, complete the following steps to open the Administrative Console.
   a. Press the middle mouse button and select **Administrative Console**. A console window appears.
   b. If prompted in the console window, type the dncs role password and press **Enter**. The Administrative Console and Administrative Console Status windows open.
3. Click the **Control** button for the ISDS in the ISDS Administrative Console Status window. The ISDS Control window opens.
4. Press the middle mouse button and select **ISDS Start**. A console window opens.
5. If prompted, type the dncs role password and then press **Enter**. The ISDS Application processes start.
6. Monitor the ISDS Control window until the status indicators for all processes turn green.

   Note: This may take several minutes.
7. In the ISDS Control window, click **File** and then select **Close**. The window closes.
8. In the ISDS Stop console window, press **File** and then select **Close**. The window closes.

Starting the ISDS Application Processes Using the Command Line

Complete the following steps to start the ISDS Application using the command line.

1. If necessary open a console on the ISDS as a **dncs administrator** or **root**.

   Note: The console can be an SSH session or terminal window on the ISDS.
2. Type **su - dncs** and press **Enter**. The password prompt appears.

3 Type the dncs role password and press **Enter**. The dncs role command line appears.

4 Type **dncsStart** and press **Enter**. The ISDS Application processes start.

Note: It may take several minutes for the command line prompt to reappear.

5 Type **dncsControl** and then press **Enter**. The ISDS Control window appears.

6 Type **2** (for Startup / Shutdown Single Element Group) and press **Enter**. The system displays a list of the ISDS processes and their current state.

7 Press **Enter** to refresh the list until the Current State is **running** for all processes.

Note: Depending on the features enabled on this ISDS, some processes will stay in the stopped state.

Example: DNCS sgManager, Bootp Daemon, sdvManager and DREDD Proxy Server

8 Type **x** and press **Enter**. The ISDS Control main menu appears.

9 Type **x** and press **Enter**. The ISDS Control window closes and the command line appears.

10 Type **exit** and press **Enter** to log out of the dncs role.

Start the Application Server on the ISDS

The Application Server can be started using the middle mouse button commands from the KVM connected to the ISDS server or from a command line. Both methods are provided.

Starting the Application Server Processes Using the Middle Mouse Button

Complete the following steps to start the integrated Application Server on the ISDS using the middle mouse button from the KVM attached to the ISDS server.

1. If necessary, log on to the ISDS CDE using a dncs administrator account.

   Note: For security purposes, we do not recommend that you log on as root user for this task.

2. If necessary, complete the following steps to open the Administrative Console.
   a. Press the middle mouse button and select **Administrative Console**. A console window appears.
   b. If prompted in the console window, type the dncs role password and press **Enter**. The Administrative Console and Administrative Console Status windows open.
3. Click the **Control** button for the AppServer in the ISDS Administrative Console Status window. The AppServer Control window opens.
4. Press the middle mouse button and select **App Serv Start**. A console window appears.
5. If prompted, type the dncs role password and then press **Enter**. The Application Server processes start.
6. Monitor the AppServer Control window until the status indicators for all processes turn green.
7. In the AppServer Control window, click **File** and then select **Close**. The window closes.
8. In the App Stop console window, press **File** and then select **Close**. The window closes.

Starting the Application Server Processes Using the Command Line

Complete the following steps to start the integrated Application Server on the ISDS using the command line.

1. If necessary, open a console on the ISDS as a dncs administrator or as root.

Note: The console can be an SSH session or a terminal window on the ISDS.

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

3 Type the dncs role password and press **Enter**. The dncs role command line appears.

4 Type **./dvs/appserv/bin/appservSetup** and press **Enter**. The Application Server environment is established.

5 Type **/dvs/appserv/bin/appStart** and press **Enter**. The Application Server processes start.

6 Type **appControl** and press **Enter**. The Application Server control window appears.

7 Type **2** (for Startup / Shutdown Single Element Group) and press **Enter**. A list of the Application Server processes and their current status appears.

8 Press **Enter** to refresh the list until the Current State is **running** for all processes.

Note: The BFS process will remain in the **stopped** state.

9 Type **x** and press **Enter**. The Application Server Control main menu appears.

10 Type **x** and press **Enter**. The Application Server Control window closes and the command line appears.

11 Type **exit** and press **Enter** to log out of the dncs role.

F

ISDS Rollback Procedure

In This Appendix

Introduction

These rollback procedures are for field service engineers who encounter problems while upgrading an ISDS. Call Cisco Services, however, before concluding that you have to roll back the system release.

Which Rollback Procedure to Run

The rollback procedure you use depends upon whether or not you have already enabled disk mirroring. If you have already enabled disk mirroring, then use restoration procedures to restore the ISDS file systems and the Informix database. Refer to your online help for procedures to restore the ISDS file systems and the Informix database.

Note: It may take as long as 4 hours to roll back the Sun Fire V445, V890, or Sun Netra T5440 ISDS using this method.

For sites that have not yet enabled disk mirroring, complete the ***Roll Back the ISDS Server*** (on page 265) procedure to switch back to the system disks with the original software.

Roll Back the ISDS Server

Follow this procedure to restore the original ISDS software.

1 Write down the version of the system release are you trying to restore.

_____

2 If necessary, follow the procedures in Stop System Components to stop the system components.

3 If necessary, log on to an xterm window on the ISDS as root user.

4 Type **eeprom boot-device=disk:a** and then press **Enter**. The system resets the default boot device to the original disk.

5 Type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The system reboots and activates the old software.

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

6 Did the ISDS reboot without error?

- If **yes**, skip to step 9.
- If **no**, go to step 7.

7 The system may have displayed an error message similar to **/var is busy**, or **The allowable number of mount points has been exceeded**. Follow these instructions.

Note: This is a known issue that occurs randomly during an upgrade.

a Log on to the system as root user.

b Type **dk -k** and then press **Enter**. The system displays the mounted filesystems.

8 Is the **/var** filesystem present in the output from step 7?

- If **yes**, go to step 9.
- If **no** (the /var filesystem is not present), go to step 10.

9 Follow these instructions if the **/var** filesystem was present in the output from step 7.

a Press the **Ctrl** and **d** keys simultaneously. The system boots into multi-user mode and the Login window opens.

b Go to step 11.

10 Follow these instructions if the **/var** filesystem was *not* present in the output from step 7.

a Type **mount /var** and then press **Enter**. The system mounts the /var filesystem.

b Type **dk -k** and then press **Enter**. The system displays the /var filesystem in the output.

Note: If the /var filesystem is still not present in the output, call Cisco Services for assistance.

c Press the **Ctrl** and **d** keys simultaneously. The system boots into multi-user mode and the Login window opens.

11 Log on to the CDE of the ISDS as a **DNCS Administrator** role.

12 Log on to an xterm window as **root** user.

13 Type **pkginfo -l SAIdncs** and then press **Enter**. Verify that the system release to which you rolled back is restored on the server.

14 Complete the instructions in Attach Mirrors.

Important: Attaching the mirrors will completely remove the newly installed ISDS software. When you are ready you must re-execute the upgrade after the mirrors are attached.

15 Go to ***Update the TED Files*** (on page 267).

Update the TED Files

Complete the rollback of the ISDS by following these instructions to update the TED files.

1 If necessary, log on to an xterm window on the ISDS as root user.

2 Type **ping dncsted** and then press **Enter**. The system responds with a **dncsted is alive** message.

Note: If you cannot ping the TED, call Cisco Services for help.

3 Type **cd /dvs/dncs/TED** and then press **Enter**. The /dvs/dncs/TED directory becomes the working directory.

4 Type **./loadTedFiles.sh** and then press **Enter**.

Important: Be sure to type the period before typing /loadTedFiles.sh.

Results:

- The system copies the appropriate files to the TED.
- The system initializes the TED.
- After a brief pause, the system displays the contents of the TED logfile (devtedLog.000) to the screen.

5 Examine the output from the logfile displayed on the screen for any error messages.

Note: Call Cisco Services if you have any questions or concerns about the TED upgrade.

G

ISDS Initial Installation Disk Formatting Issue

In This Appendix

Introduction

On rare occasions, the system may return the **Unable to readk Disk geometry** error after you execute the **boot cdrom - install** command during initial installation of ISDS software. This error indicates that you must format the hard drives by following the instructions in this appendix.

Error Condition and Workaround

Error Condition

If error messages similar to the following appear after you execute the **boot cdrom - install** command, you need to format the hard drives:

prvtoc: /dev/rdsk/c1t0d0s2: Unable to readk Disk geometry errno=0X5

prvtoc: /dev/rdsk/c1t0d1s2: Unable to readk Disk geometry errno=0X5

prvtoc: /dev/rdsk/c1t0d4s2: Unable to readk Disk geometry errno=0X5

prvtoc: /dev/rdsk/c1t0d5s2: Unable to readk Disk geometry errno=0X5

prvtoc: /dev/rdsk/c1t0d0s2: Unable to readk Disk geometry errno=0X5

prvtoc: /dev/rdsk/c1t0d1s2: Unable to readk Disk geometry errno=0X5

prvtoc: /dev/rdsk/c1t0d4s2: Unable to readk Disk geometry errno=0X5

prvtoc: /dev/rdsk/c1t0d5s2: Unable to readk Disk geometry errno=0X5

Formatting the Hard Drives

Follow these instructions to format the hard drives responsible for the **Unable to readk Disk geometry** error.

1. Log on to an xterm window on the ISDS as **root** user.
2. Type **format** and then press **Enter**. The system displays a list of available disks and requests that you specify a disk number.
3. Enter the first disk number (which should be 0) and then press **Enter**.
4. Type **y** and then press **Enter** when prompted to "Label it now".
5. Repeat steps 2 through 4 for the remaining disks.
6. Return to one of the following procedures and re-enter the **boot cdrom - install** command:
   - *Installing ISDS Software Onto the Sun Fire V445 or V890 Server* (on page 23)
   - *Installing ISDS Software Onto the Sun Netra T5440 Server* (on page 24)

H

Stopping and Starting the Sun Server

In This Appendix

Introduction

The instructions in this appendix describe how to stop and start the Sun server.

Note: The Application Server and ISDS application should be stopped prior to stopping the Sun Server. Complete the steps, if necessary, in ***Stopping System Components*** (on page 251) before you stop the Sun server.

Stop the Sun Server

Complete these steps to shut down the ISDS Sun server.

Note: The Application Server and ISDS application must be stopped prior to beginning this procedure.

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. From the xterm window, type **ps -ef | grep dvs** and then press **Enter** to verify that the ISDS processes have stopped.
4. Do the results from step 3 show that dncsInitd, dncsResMon, appInitd, and app_crash_global.d are the only processes still running?
   - If **yes**, go to step 7.
   - If **no** (there are other processes still running), follow these instructions.
     a. Type **dncsKill** and then press **Enter**.
     b. Type **/dvs/appserv/bin/appKill** and then press **Enter**.
     c. Type **exit** and then press **Enter** in the xterm window to return to the root user.
5. Type **ps -ef | grep dvs** and then press **Enter** to verify that the ISDS processes have stopped.
6. Do the results from step 5 show that dncsInitd, dncsResMon, appInitd, and app_crash_global.d are the only processes still running?
   - If **yes**, go to step 7.
   - If **no** (there are other processes still running), type **kill -9 < PID >** for all processes that have not stopped, where PID is the Process ID.
7. As root user, type **./dvs/dncs/bin/dncsSetup** and then press **Enter** to set the correct operating environment.

   Important: Make sure there is a space between the . and the /.
8. Type **showActiveSessions** and then press **Enter**.
9. Did the results from step 8 include the message **INFORMIXSERVER is idle**?
   - If **yes**, go to step 10.
   - If **no**, follow these instructions.
     a. Type **killActiveSessions** and then press **Enter**.
     b. Type **showActiveSessions** and then press **Enter**. The message

INFORMIXSERVER is idle should appear.

10 Choose one of the following options:

- If you would like to reboot the ISDS Sun server, type **/usr/sbin/shutdown -g0 -i6 -y** and then press **Enter**.

  Result: The Sun server reboots and the CDE Login window appears.

  Note: The reboot process can take several minutes to complete.

- If you would like to shut down the ISDS Sun server to power off the system, type **/usr/sbin/shutdown -g0 -i5 -y** and then press **Enter**.

  Results:

  – For a Sun Fire V445 or Sun Netra T5440 server, the hard drive lights turn off and the **OK** light blinks slowly once the power-down is complete.

  – For a Sun Fire V890 server, all three top lights on the front panel turn off once the power-down is complete.

  Note: You can remove power cables, if desired, once the power-down is complete.

Restart the Sun Server

Complete these steps to restart the ISDS Sun server after completely powering down the server.

Important: Complete these steps *only* if the ISDS Sun server was completely powered-down.

1 Choose one of the following options:

- To restart a Sun Fire V890 server, go to step 2.
- To restart a Sun Fire V445 or Sun Netra T5440 server, go to step 3.

2 Follow these instructions to restart a Sun Fire V890 server.

a If necessary, turn the key switch to **|**.

b Press the power button on the front of the server. The server powers up and the CDE Login window appears.

Note: It can take several minutes for the server to power up.

3 To restart a Sun Netra T5440 or a Sun Fire V445 server, press the recessed power button which is just to the right of the **OK** light. The server powers up and the CDE Login window appears.

Note: It can take several minutes for the server to power up.

I

Default VASP Values for the ISDS

In This Appendix

Introduction

This appendix contains a listing of the default VASP entries that are used by the ISDS. Installation engineers may find this information useful when they rebuild VASP entries during the ***Rebuild VASP Entries (if the dncsatm or appservatm Interfaces Were Modified)*** (on page 61) procedure.

ISDS Default VASP Values

The information contained in the following table may be useful as engineers rebuild the system's VASP entries.

Note: The IP address assigned to each VASP entry is the IP address of the dncsatm interface and is dynamic per site.

ID	Name
1	CFSession UI
2	Broadcast File System
3	Message Server
4	MMM Server
5	OSM Server
6	SAM Server
7	HCTM Server
8	SGM Server
9	PASM Server
10	RPC UI Server
11	cmd2000
12	ippvmgr
13	dhctproxy
14	cammgr
15	simgr
110	Appserv DHCT Config
111	Appserv PPV
112	Appserv IPG

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

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

Part Number 4028676 Rev C
June 2012 Printed in USA