DVD Upgrade Installation Instructions

for System Release i4.4

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 provides step-by-step instructions for upgrading a Digital Broadband Delivery System (DBDS) to System Release (SR) i4.4.

SR i4.4 Features Live Upgrade

The upgrade to SR i4.4 features the Solaris Live Upgrade. Through use of the Live Upgrade, engineers can upgrade the system to SR i4.4 without having to shut down the system processes until activation of the new system software.

Upgrade Path

Sites that upgrade to SR i4.4 must currently support SR i4.2.1, SR i4.2.2, or SR i4.3.

How Long to Complete the Upgrade?

The upgrade to SR i4.4 is to be completed from within a maintenance window that usually begins at midnight. Upgrade engineers have determined that a typical site can be upgraded within one maintenance window. The maintenance window should begin when you use the doLiveUpgrade script to upgrade the Digital Network Control System (DNCS) at the beginning of Chapter 2.

System Performance Impact

Interactive services will not be available during the maintenance window.

Audience

This guide is written for field service engineers and system operators who are responsible for upgrading an existing DBDS to SR i4.4.

Read the Entire Guide

Please review this entire guide before beginning the installation. If you are uncomfortable with any of the procedures, contact Cisco® Services at +91 9840717688 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.

Required Skills and Expertise

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

- Advanced knowledge of UNIX
  - Experience with the UNIX vi editor. Several times throughout the system upgrade process, system files are edited using the UNIX vi editor. The UNIX vi editor is not intuitive. The instructions provided in this guide are no substitute for an advanced working knowledge of the UNIX vi editor.
  - The ability to review and edit cron files
- Extensive DBDS system expertise
  - The ability to identify key files that are unique to the site being upgraded
  - The ability to add and remove user accounts

Requirements

Before beginning the upgrade to SR i4.4, be sure that the site you are upgrading meets these requirements:

- You have the DVD labeled SR i4.4 DVD in order to complete the required backups of the database and the filesystem.
- The latest version of DBDS Utilities is installed on your system.

Non-SA Application Server and/or Third-Party Application

If the site you are upgrading supports a non-SA Application Server, contact the vendor of that Application Server in order to obtain upgrade requirements, as well as upgrade and rollback procedures.

If the site you are upgrading runs a third-party software application, contact the supplier of that application in order to obtain any upgrade requirements.

Important: Be certain that all third-party vendors are aware that the SR i4.4 upgrade is built upon a Solaris 10 software platform.

Supported Server Platforms

The following DNCS server and Application Server hardware platforms are supported by the SR i4.4 release:

DNCS Server

Platform	Hard Drives	Memory
Sun Fire V445	■ 4 X 73 GB ■ 8 X 73 GB	■ 4 GB w/2 CPUs ■ 8 GB w/4 CPUs
Sun Fire V880	■ 6 X 73 GB ■ 12 X 73 GB	■ 4 GB minimum ■ 8 GB minimum
Sun Fire V890	■ 6 X 146 GB ■ 12 X 146 GB	■ 8 GB minimum ■ 16 GB minimum

Application Server

Platform	Hard Drives	Memory
Sun Fire V240	2 X 36 GB	512 MB minimum
Sun Fire V245	2 X 73 GB	256 MB minimum

Document Version

This is the first formal release of this document.

1

SR i4.4 DVD Pre-Upgrade Procedures

Introduction

This chapter contains procedures that you will follow to prepare the system you are upgrading for the SR i4.4 upgrade.

Important Points About the Upgrade

Note these important points about the upgrade to SR i4.4:

- Systems that upgrade to SR i4.4 using the DVD method must currently support one of the following system releases:
  - SR i4.2.1
  - SR i4.2.2
  - SR i4.3
- Our field service engineers or the system operator must have already installed the DNCS Utilities software onto the DNCS and should have already run the pre-upgrade checks to ensure system compatibility with SR i4.4 upgrade requirements.

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

Performance Impact

Interactive services will not be available while you are within the maintenance window, after DNCS processes are stopped.

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.

Back Up the File Systems

The upgrade scripts do not back up the DNCS or Application Server 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 Application Server and the DNCS.

Important: Repeat these procedures two times: once for the Application Server and then again for the DNCS.

Preparing for the File System Backup

Follow this procedure to prepare for the DNCS or Application Server file system backup.

1. If necessary, open an xterm window on the DNCS or Application Server, whichever server you are backing up.
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 SR i4.4 DVD into the DVD drive of the DNCS or the Application Server, whichever server you are backing up.
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. Did the DVD mount successfully?
   - If **yes**, skip to step 7.
   - If **no**, continue with step 6.
6. Follow these instructions to mount the DVD manually.
   a. Type the following command and press **Enter** to stop the volmgt process.
   ```
   /etc/init.d/volmgt stop
   ```

b Type the following command and press **Enter** to determine the CD-ROM path.

```
rmformat -l
```

Example: Output should be similar to the following:

```
Looking for devices...
Volmgt Node: /vol/dev/aliases/cdrom0
sLogical Node: /dev/rdsk/c0t0d0s2
Physical Node: /pci@8,700000/ide@1/sd@0,0
Connected Device: TSSTcorp CD/DVDW TS-H652D SI00
Device Type: DVD Reader/Writer
```

c Type the following command and press **Enter** to manually mount the DVD.

```
mount -F hsfs /dev/dsk/c0t0d0s0 /cdrom
```

d Type the following command and press **Enter** to start the volmgt process.

```
/etc/init.d/volmgt start
```

7 Label a blank tape with the following information:

[DNCS or Application Server] File System Backup [Date]

[Site Name]

[Software Version]

DBDS Maintenance DVD x.x.x

Note: Customize the date, site name, and software version for the site you are backing up.

Backing Up the File System of the DNCS or Application Server

Follow these instructions if you are backing up the file system of the DNCS to a tape in the DNCS or to a remote server.

Notes:

- If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.
- Depending upon the amount of data to be backed up, backups can take up to several hours to complete. Allow enough time to complete these backups based upon how long it usually takes you to back up your system.

1 Insert the blank tape into the tape drive of the DNCS or Application Server, whichever server you are backing up, and wait for the green light to stop flashing.

2 Choose one of the following options to back up the file system:

Note: If you are using an external DVD drive, substitute *cdrom1* for **cdrom0**.

- To back up the file system on a local tape drive, type the following command and press **Enter**.
  /cdrom/cdrom/sai/backup_restore/backupFileSystems -v
- To back up the file system on a DNCS or Application Server that does not have a local tape drive, type the following command and press **Enter**.
  /cdrom/cdrom/sai/backup_restore/backupFileSystems -v -r [hostname or IP address]:[tape device]

Result: The system backs up the DNCS or Application Server file system, ejects the tape, and displays a message when the backup is complete.

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

Back Up the Database

Follow these instructions to back up the DNCS database to a tape in the DNCS or to a remote server.

Notes:

- You should currently be logged on as **root** user in an xterm window.
- The backup can take several hours to complete, based upon the size of the database. Be certain to allow for enough time for the backup to complete.

1. Insert a blank tape into the tape drive of the DNCS or the remote server and wait for the green light to stop flashing.
2. Select one of the following options:
   - If you are backing up the DNCS database to a tape drive in the DNCS, type the following command and press **Enter**.

     ```
     /cdrom/cdrom/sai/backup_restore/backupDatabase -v
     ```

   - If you are backing up the DNCS database to a tape drive on a remote server, type the following command and press **Enter**.

     ```
     /cdrom/cdrom/sai/backup_restore/backupDatabase  -v -r
     [hostname or IP address]:[tape device]
     ```

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

Run the Doctor Report

Before upgrading the system, run the Doctor Report using the instructions provided in the appropriate DBDS Utilities guide. The Doctor report provides key system configuration data that might be useful before you begin the upgrade process.

Important: You must be **dncs** user to run the Doctor Report.

Follow these instructions to help you run the Doctor Report.

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

```
pkginfo  -l  SAIdbdsutils
```

2 Did the system reveal that this package is installed?

- If **yes**, go to **Run /dvs/dncs/Utilities/doctor**.
- If **no**, contact Cisco Services to obtain the SAIdbdsutils package.

Run /dvs/dncs/Utilities/doctor

1 Type the following command and then press **Enter**.

```
cd  /dvs/dncs/Utilities/doctor
```

2 Type the following command and then press **Enter**.

```
doctor  -av
```

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.

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

Examine Disks and Mirrored Devices

Examine the status of the mirrored disk drives on the Sun Fire V445, V880, or V890 DNCS, as well as the Sun Fire V245 or V240 Application Server prior to the SR i4.4 upgrade. All the disk mirroring functions must be working normally before proceeding with the upgrade.

CAUTION:

If the disk mirroring functions of the DNCS or Application Server are not working properly before the upgrade, you may not be able to easily recover from a failed upgrade.

Examining Disks and Mirrored Devices

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

1 If necessary, open two xterm windows, one on the DNCS and the other on the Application Server.

2 In one of the windows, type **metastat | more** and then press **Enter**. The system displays the status of all of the metadevices on the DNCS.

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

3 Do all metadevices display a state of **OK**?

- If **yes**, go to step 4.
- If **no**, call Cisco Services for help in resolving these issues with the metadevices.

4 Follow these instructions to log on to one of the xterm windows as root user.

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

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

5 In the root xterm window, type **format </dev/null** and then press **Enter** to confirm that all disks are present and readable.

Examples:

- The following sample output shows results from a 6-disk, Sun Fire V880:

```
AVAILABLE DISK SELECTIONS:
       0. c1t0d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@8,600000/SUNW,qlc@2/fp@0,0/ssd@w500000e0108977d1,0
1.     c1t1d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
.
..
11. c2t5d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
/pci@9,600000/pci@1/SUNW,qlc@4/fp@0,0/ssd@w2200000c5056c543,0
```

- The following sample output shows results from a 4-disk, Sun Fire V445

```
AVAILABLE DISK SELECTIONS:
       0. c0t0d0 <FUJITSU-MBD2300RC-3701 cyl 46873 alt 2 hd 20 sec
625>
          /pci@0,600000/pci@0/pci@0/scsi@0/sd@0,0
       1. c0t1d0 <FUJITSU-MBD2300RC-3701 cyl 46873 alt 2 hd 20 sec
625>
          /pci@0,600000/pci@0/pci@0/scsi@0/sd@1,0
       2. c0t2d0 <FUJITSU-MBD2300RC-3701 cyl 46873 alt 2 hd 20 sec
625>
          /pci@0,600000/pci@0/pci@0/scsi@0/sd@2,0
       3. c0t3d0 <FUJITSU-MBD2300RC-3701 cyl 46873 alt 2 hd 20 sec
625>
          /pci@0,600000/pci@0/pci@0/scsi@0/sd@3,0
```

- The following sample output shows results from a 2-disk, Sun Fire V445:

```
AVAILABLE DISK SELECTIONS:
       0. c1t0d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1e,600000/pci@0/pci@a/pci@0/pci@8/scsi@1/sd@0,0
       1. c1t1d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@1e,600000/pci@0/pci@a/pci@0/pci@8/scsi@1/sd@1,0
```

6 Is your DNCS platform a Sun Fire V880 or V890?

- If **yes**, type (as root user) **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 (OK)           500000e0108977d0
1     On (OK)           20000004cf2bf3f1
2     On (OK)           500000e010897d30
3     On (OK)           500000e010898090
4     On (OK)           500000e010894d90
5     On (OK)           2000000c5056c543
6     Not Installed
7     Not Installed
8     Not Installed
9     Not Installed
10    Not Installed
11    Not Installed
```

- If **no**, go to the next procedure in this chapter.

7 Did the output from step 6 reveal a **Disk Status** of **OK** for all disks?

- If **yes**, continue with step 8.
- If **no**, call Cisco Services for assistance.

8 Type **metastat -c** and then press **Enter**. Results similar to the following appear:

Example:

- The following example shows a Sun Fire V880 with a 12 X 73 disk configuration. All devices in this example are in good working order. And problems with a device would be noted by "**( )**" next to the example.

```
$ metastat -c
d382              p  2.0GB d520
d381              p  2.0GB d520
d380              p  2.0GB d520
d379              p  2.0GB d520
d378              p  2.0GB d520
d377              p  2.0GB d520
d376              p  2.0GB d520
d375              p  2.0GB d520
d374              p  2.0GB d520
d373              p  2.0GB d520
d372              p  2.0GB d520
d371              p  2.0GB d520
d370              p  2.0GB d520
d369              p  2.0GB d520
d368              p  2.0GB d520
d367              p  2.0GB d520
d366              p  2.0GB d520
d365              p  2.0GB d520
d364              p  2.0GB d520
d363              p  2.0GB d520
d362              p  2.0GB d520
d361              p  2.0GB d520
d360              p  2.0GB d520
d359              p  2.0GB d520
d358              p  2.0GB d520
d357              p  2.0GB d520
d356              p  2.0GB d520
d355              p  2.0GB d520
d354              p  2.0GB d520
d353              p  2.0GB d520
d352              p  2.0GB d520
```

```
d351             p  2.0GB d520
d350             p  1.0GB d520
    d520         m  238GB d720 d420
        d720     s  238GB c2t10d0s0 c2t11d0s0 c2t12d0s0
c2t13d0s0
        d420     s  238GB c1t2d0s0 c2t3d0s0 c2t4d0s0
c2t5d0s0
d507             m  8.0GB d707 d407
    d707         s  8.0GB c2t8d0s5
    d407         s  8.0GB c1t0d0s5
d503             m  8.0GB d403
    d403         s  8.0GB c1t0d0s3
d501             m  8.0GB d701 d401
    d701         s  8.0GB c2t8d0s1
    d401         s  8.0GB c1t0d0s1
d500             m  8.0GB d400
    d400         s  8.0GB c1t0d0s0
d510             m   59GB d710 d410
    d710         s   59GB c2t9d0s0
    d410         s   59GB c1t1d0s0
d703             s  8.0GB c2t8d0s3
d700             s  8.0GB c2t8d0s0
```

- The following sample output shows results from a Sun Fire V445 with a 4 X 73 disk configuration. All devices in this example are in good working order.

```
d399             p   29GB d520
d372             p   13GB d520
d371             p   18GB d520
d370             p   18GB d520
d318             p  5.1GB d520
d317             p   18GB d520
d316             p   18GB d520
d315             p   18GB d520
d314             p   18GB d520
d313             p   18GB d520
d312             p   18GB d520
d311             p   18GB d520
d310             p   18GB d520
d304             p  6.0GB d520
d303             p  6.0GB d520
d302             p   12GB d520
```

```
d301                p  6.0GB d520
d300                p  3.0GB d520
    d520            m  262GB d420
        d420        s  262GB c0t1d0s0
d505                m  220GB d405
    d405            s  220GB c0t0d0s5
d504                m  8.0GB d404
    d404            s  8.0GB c0t0d0s4
d503                m   18GB d403
    d403            s   18GB c0t0d0s3
d501                m  8.0GB d401
    d401            s  8.0GB c0t0d0s1
d500                m  8.0GB d400
    d400            s  8.0GB c0t0d0s0
```

9 Examine each device and submirror. Is each device in good working order?

- If **yes**, you have completed this procedure. Go to the next procedure in this chapter.
- If **no**, call Cisco Services for assistance.

Verify That the Boot Device is Properly Configured

Before upgrading the DNCS, use the following procedure to verify that the boot device is properly configured.

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

```
eeprom  boot-device
```

Example:
```
boot-
device=/pci@1e,600000/pci@0/pci@2/scsi@01/d3k@0,0:a disk net
```

2 Do the results from step 1 show that disk:a is listed as a boot device?

Note: The disk:a boot device should be listed first in the output from the command executed in step 1.

- If **yes**, the boot device is properly configured.
- If **no**, type the following command and press **Enter** to reset the boot device to the original disk.

```
eeprom  boot-device=disk:a
```

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 DNCS, type the following command and then press **Enter**. The system removes all completed session, resource, and network graph records more than 1 hour old from the database.

```
clearDbSessions
```

2 Type the following command and then press **Enter**. The system removes all completed session, resource, and network graph records from the database.

```
clearDbSessions -c
```

3 Type the following command and then press **Enter**. The system removes orphaned records from the database.

```
clearDbSessions -o
```

Examine Key Files

The scripts used during the upgrade are designed to back up the key files most likely to be found on the DNCS. 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.

- 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.

- Review all entries in the /etc/vfstab file and record any unique entries that you want to retain after the upgrade.

  Note: You can also create a backup of the /etc/vfstab file and save it as a key file. After the system is upgraded, you can place unique entries into the /etc/vfstab file.

- Include all directories where set-top image files and EMM files are stored.

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

Verify System Communications

Use this procedure to verify that an active communication link exists between the DNCS and the various system components. The DNCS 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 DNCS, use the UNIX **cd** command to change to the directory that contains the Doctor Report.
2. Examine the log file created earlier in this chapter and verify that the system was able to ping the Transaction Encryption Device (TED).
3. Verify that you can manually ping the following hardware components:
   - All router interfaces in the system
   - The PCG
4. 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.
5. Verify that you can successfully stage a DHCT.
6. Follow these general instructions to verify DHCT provisioning.
   a. From the DHCT Provisioning window, supply the MAC address or serial number of an existing DHCT.
   b. Click **Continue**.
   c. Add and remove packages to/from the DHCT and verify that the ECM and EMM counts increase on the DHCT diagnostics window.

Check the Number of BFS Sessions

The number of BFS sessions post-upgrade needs to equal the number of pre-upgrade sessions. Use this procedure to determine and record the number of pre-upgrade BFS sessions. Then, after the upgrade, you will determine the number of post-upgrade BFS sessions.

Follow this procedure to check and record the number of pre-upgrade BFS sessions.

1 Press the **Options** button on the front panel of the QAM until the **Session Count** total appears.

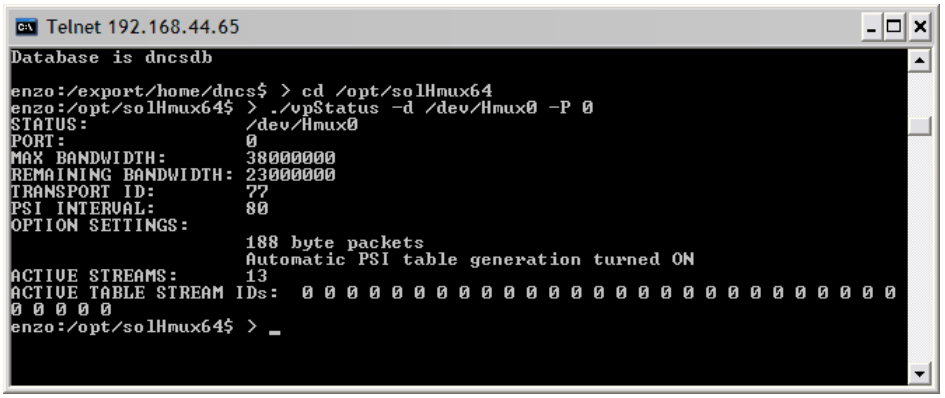
2 Record the **Session Count** total in the space provided. _____

3 Does the system you are upgrading use the ASI card?

- If **yes**, from an xterm window on the DNCS, type the following command and press **Enter**.

  `/opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0`

  Example: Output from the command should look similar to the following:



- If **no**, go to the next procedure in this chapter.

4 Note the number of **Active Streams**, as you may need this information later when you perform post-upgrade procedures.

_____

Obtain DNCS System Configuration

Complete the following steps to obtain basic system configuration data for *both* the DNCS and the Application Server. You may need some of this information later during the upgrade.

1 From an xterm window on the DNCS, type the following command and press **Enter**. A list of IP (Internet Protocol) addresses and hostnames appears.

```
more /etc/hosts
```

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:

- appservatm _____
- dncsatm _____
- dncseth _____
- dncsted _____

3 Type the following command and press **Enter**. The hostname for the DNCS appears.

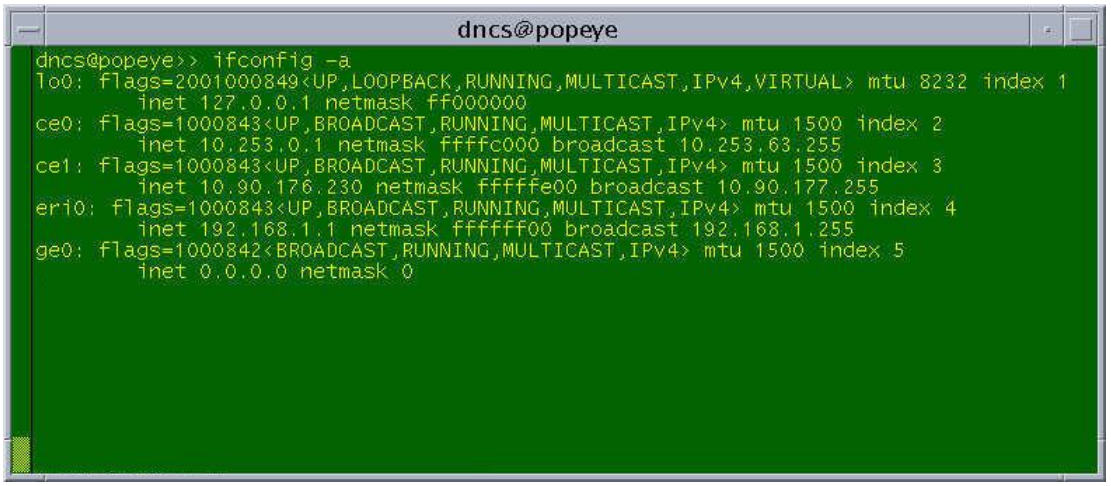
```
uname  -n
```

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 DNCS, as displayed in step 3: _____

5 Type the following command and press **Enter** to verify that the network interfaces have been plumbed and configured correctly. Output should look similar to the following example:

```
ifconfig -a
```



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.

1 From a root xterm window, type **cd /export/home/dncs** and then press **Enter**. The /export/home/dncs directory becomes the working directory.

2 Type **mkdir network** and then press **Enter**. The system creates a directory called network.

3 Type **cd network** and then press **Enter**. The /export/home/dncs/network directory becomes the working directory.

4 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/S71atminit .**

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

k **cp -p /etc/rc2.d/S85SAspecial .**

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

l **cp -p /etc/inet/ipnodes .**

m **netstat -nrv > netstat.out**

n **ifconfig -a > ifconfig.out**

o **df -k > df.out**

p **eeprom nvramrc > nvramrc.out**

5 As root user, type **cp -rp /var/spool/cron/crontabs /var/spool/cron/crontabs.previous** and then press **Enter**.

6 Type **cd /var/spool/cron** and then press **Enter**.

7 Type **tar cvf crontabs.previous.< date >.tar crontabs.previous** and then press **Enter**.

Note: Replace < date > with the current date.

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

8 Type **cp -rp crontabs.previous.< date >.tar /export/home/dncs/network** and then press **Enter**.

9 Type **cd /export/home/dncs/network** and then press **Enter**.

10 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.

11 Repeat steps 2 through 10 for the Application Server.

Stop the Replicated Database

Complete this procedure only if the site you are upgrading supports the replicated database.

Note: You should still be logged on to an xterm window on the DNCS (the primary server) as **root** user.

1. If necessary, open an xterm window on the secondary server.
2. On the secondary server, follow these instructions to log on to the xterm window as **root** user.
   a. Type **su -** and then press **Enter**.
   b. Type the **root** password and then press **Enter**.
3. Type the following command and press **Enter**, first on the primary server and then on the secondary server to disable database replication.

   ```
   /opt/SAIrepdb/RepDb -p primhost -s sechost -d
   ```
4. Wait about 10 minutes.
5. On the *secondary* server, type the following command and press **Enter**.

   ```
   onstat -
   ```

   Result: The secondary server should show a status of *online*.
6. Complete the following steps on the *primary* server to stop remote file copying.
   a. Type the following command and press **Enter**.

      ```
      export EDITOR=vi
      ```
   b. Type the following command and press **Enter** to open the crontab file for editing.

      ```
      crontab -e
      ```
   c. Insert the comment symbol (#) before the following line:

      ```
      00 * * * *    /opt/SAIrepdb/syncKeyFiles -l primhost -r
      sechost -q
      ```
   d. Save and close the file.

2

SR i4.4 DVD Upgrade Procedures

Introduction

Use the procedures in this chapter to upgrade a site to SR i4.4.

In This Chapter

Upgrade the SR i4.4 Software

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

Upgrading the i4.4 Software

Complete the following steps to upgrade the SR i4.4 software.

1. Open an xterm window on the DNCS.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Insert the SR i4.4 DVD into the DVD drive of the DNCS.
4. Wait one minute and then type the following command and press **Enter**. A list of the mounted filesystems appears.

   ```
   df -n
   ```
5. Does the output from step 4 show that the system mounted the DVD?
   - If **yes**, go to step 9.
   - If **no**, go to step 6.
6. Follow these instructions to mount the DVD manually.
   a. Type the following command and press **Enter** to stop the volmgt process.

      ```
      /etc/init.d/volmgt stop
      ```
   b. Type the following command and press **Enter** to determine the CD-ROM path.

      ```
      rmformat -l
      ```

      Example: Output should be similar to the following:

      ```
      Looking for devices...
      Volmgt Node: /vol/dev/aliases/cdrom0
      sLogical Node: /dev/rdsk/c0t0d0s2
      Physical Node: /pci@8,700000/ide@1/sd@0,0
      Connected Device: TSSTcorp CD/DVDW TS-H652D SI00
      Device Type: DVD Reader/Writer
      ```
   c. Type the following command and press **Enter** to manually mount the DVD.

      ```
      mount -F hsfs /dev/dsk/c0t0d0s0 /cdrom
      ```

7 After completing step 6, did the DVD user interface appear?

- If **yes**, go to step 9.
- If **no**, type the following command and press **Enter**. The volume manager utility starts.

  ```
  /etc/init.d/volmgt  start
  ```

8 Repeat steps 4 through 7. Call Cisco Services if the system still does not recognize the DVD.

9 Type the following command and press **Enter**. The system displays the status of all of the metadevices on the DNCS.

```
metastat | more
```

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

```
which onstat
```

12 Is the path to the onstat command /export/home/informix/bin, 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 is still not /export/home/informix/bin.

13 Type the following command and press **Enter**.

```
cd /cdrom/sai/scripts
```

14 Type the following command and press **Enter**.

```
./doLiveUpgrade
```

Result: A message similar to the following appears.

Note: The message portion **A Live Upgrade is not allowed. A Migration is required** will not appear if the Informix version of the upgrade is the same as the Informix version before the upgrade.

```
bash-3.00# ./doLiveUpgrade
Checking for LU patches...
Applying LiveUpgrade patches...
Installing program: p7zip
Determined current system type is: DNCS
The installation set is: /cdrom/sai/INSTALL/dncs_iset
WARNING:
WARNING: The database soft partitions on the new system
WARNING: do not match the partitions on the current system.
A Live Upgrade is not allowed.
A Migration is required.
Would you like to do a migration?  [y,n,?,q] y
*************************************************************
 Attention!          Attention!          Attention!          Attention!

This script will Upgrade the other side of the mirror using Live Upgrade
Process.
The database will be migrated to the newly installed system.
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 then press **Enter** to detach the mirrors. A message similar to the following appears:

```
Live Upgrade log of dncs started at: Monday, February 21, 2011  5:16:10
PM EST


Detaching any non-database mirrors...
d510: submirror d710 is detached
d710: Concat/Stripe is cleared
d507: submirror d707 is detached
d707: Concat/Stripe is cleared
d503: submirror d703 is detached
d703: Concat/Stripe is cleared
d500: submirror d700 is detached
d700: Concat/Stripe is cleared
d501: submirror d701 is detached
d701: Concat/Stripe is cleared


Current boot-device in eeprom:
```

```
disk:a /pci@1e,600000/pci@0/pci@2/scsi@0/disk@4,0:a

Will be replaced temporarily with:
/pci@1e,600000/pci@0/pci@2/scsi@0/disk@0,0:a disk:a
/pci@1e,600000/pci@0/pci@2/scsi@0/disk@4,0:a
Setting your Alternate Boot Env Name to DNCS.i4.4.0.7....
Setting your Current Boot Env Name to DNCS.pre_lu....
Adding / entry to /var/sadm/system/logs/lu.dncs.mnts file.
Creating a new file system (2) on /dev/dsk/c1t4d0s0...
Adding swap entry to /var/sadm/system/logs/lu.dncs.mnts file.
Adding /var entry to /var/sadm/system/logs/lu.dncs.mnts file.
Creating a new file system (2) on /dev/dsk/c1t4d0s3...
Adding /export/home entry to /var/sadm/system/logs/lu.dncs.mnts file.
Creating a new file system (2) on /dev/dsk/c1t4d0s4...
Adding /disk1 entry to /var/sadm/system/logs/lu.dncs.mnts file.
Creating a new file system (2) on /dev/dsk/c1t4d0s5...

WARNING: /etc/vfstab was modified.

Backup file /etc/vfstab.preLiveUpgrade will be restored upon a rollback.

  If you decide to cancel this upgrade at any OTHER
  time, restore the file with the following command.

  cp -p /etc/vfstab.preLiveUpgrade /etc/vfstab
  Press <ENTER> to continue.
```

16 Press **Enter** to save the vfstab file and to continue with the Live Upgrade.

17 Read through the following message which then shortly appears:

```
Analyzing system configuration.
No name for current boot environment.
Current boot environment is named <DNCS.pre_lu>.
Creating initial configuration for primary boot environment
<DNCS.pre_lu>.
WARNING: The device </dev/md/dsk/d500> for the root file system mount
point </> is not a physical device.
WARNING: The system boot prom identifies the physical device
</dev/dsk/c1t0d0s0> as the system boot device.
INFORMATION: Assuming the boot device </dev/dsk/c1t0d0s0> obtained from
the system boot prom is
the physical boot device for logical device </dev/md/dsk/d500>.
The device </dev/dsk/c1t0d0s0> is not a root device for any boot
environment; cannot get BE ID.
PBE configuration successful: PBE name <DNCS.pre_lu> PBE Boot Device
</dev/dsk/c1t0d0s0>.
Updating boot environment description database on all BEs.
Searching /dev for possible boot environment filesystem devices
```

```
Updating system configuration files.
The device </dev/dsk/c1t4d0s0> is not a root device for any boot
environment; cannot get BE ID.
Creating <ufs> file system for </> in zone <global> on
</dev/dsk/c1t4d0s0>.
Creating <ufs> file system for </disk1> in zone <global> on
</dev/dsk/c1t4d0s5>.
Creating <ufs> file system for </export/home> in zone <global> on
</dev/dsk/c1t4d0s4>.
Creating <ufs> file system for </var> in zone <global> on
</dev/dsk/c1t4d0s3>.
Creation of boot environment <DNCS.i4.4.0.7> successful.
Removing "/etc/openwin/server/etc/OWconfig" entry from lu_transfer_list.
------------------------------------------------------------
   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
------------------------------------------------------------
44845 blocks
miniroot filesystem is <lofs>
Mounting miniroot at </cdrom/Solaris_10/Tools/Boot>
Validating the contents of the media </cdrom>.
The media is a standard Solaris media.
Validating the contents of the miniroot </cdrom/Solaris_10/Tools/Boot>.
Locating the flash install program.
Checking for existence of previously scheduled Live Upgrade requests.
Constructing flash profile to use.
Creating flash profile for BE <DNCS.i4.4.0.7>.
Performing the operating system flash install of the BE <DNCS.i4.4.0.7>.
CAUTION: Interrupting this process may leave the boot environment
unstable or unbootable.
Extracting Flash Archive: 5% completed (of   81.00 megabytes)
```

18 As directed in the message displayed in the previous step, type the following command and then press **Enter** to inspect the log file.

```
tail -f /tmp/install_log
```

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

19 At the **Do you want to add to the above list?** message, 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, as well as any special files you identified in ***Identify Special Files to be Backed Up*** (on page 17).
    - Be certain that set-top image files and EMM directories are included.
  - **c** When you are finished adding key files, type **n** and then press **Enter**. The system displays a **Do you want to continue?** message.
  - **d** 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**.

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

```
Copying /etc/lutab and /etc/lu/ICF.1 to DNCS.i4.4.0.7...
Copying sysidcfg file...
Copying SAI installation set...
Copying scripts...

Reseting boot-device in eeprom...
Boot Environment           Is       Active Active    Can    Copy
Name                       Complete Now    On Reboot Delete Status
-------------------------- -------- ------ --------- ------ ----------
DNCS.pre_lu                yes      yes    yes       no     -
DNCS.i4.4.0.7              yes      no     no        yes    -

Live Upgrade Procedure completed. Check the logs for any errors.
Continuing from here should be done during a MAINTENANCE WINDOW
All DNCS processes must be brought down in order to proceed.

*** INSTRUCTIONS FOR COMPLETING THE LIVE UPGRADE ***
When you are ready to continue, run the script /var/tmp/lu_continue
Run /var/tmp/lu_continue when you are ready to ASCII export your
database.
```

Important: Ignore this command for now.

21 Log on to the Application Server as **dncs** user and then follow these steps to stop the Application Server process.

a Open an xterm window on the Application Server.

b Type the following command and press **Enter**.

```
cd /dvs/appserv/bin
```

c Type the following command and press **Enter**. The AppControl utility appears.

```
./appControl
```

d Type **2** and then press **Enter**.

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

f Type the following command and press **Enter**.

```
./appStop
```

g Wait a few minutes, press **Enter** on the AppControl user interface, 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 If, after waiting several minutes, there are Application Server processes still running, type the following command and press **Enter**.

```
./appKill
```

i Close the AppControl utility user interface.

22 As dncs user, follow these steps to stop the DNCS.

a Type the following command and press **Enter**.

```
cd /dvs/dncs/bin
```

b Type the following command and press **Enter**. The dncsControl utility appears.

```
dncsControl
```

c Type **2** and then press **Enter**.

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 Type the following command and press **Enter**.

```
dncsStop
```

f Wait a few minutes, press **Enter** on the dncsControl user interface, 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 Type the following command and press **Enter** to verify that the DNCS processes have stopped.

```
ps -ef | grep dvs
```

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

- If **yes**, go to step 23.
- If **no** (there are other processes still running), follow these instructions.

a Type **dncsKill** *on the DNCS* and then press **Enter**.
b Type **appKill** *on the Application Server* and then press **Enter**.

i Type the following command and press **Enter** to verify that the processes have stopped.

```
ps -ef | grep dvs
```

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

- If **yes**, go to step 23.
- If **no** (there are other processes still running), type (as root user) **kill -9 < PID >** for all processes that have not stopped, where PID is the Process ID.

23 Close the dncsControl utility user interface.

24 As **root** user, type the following command and press **Enter** to set the correct operating environment.

```
. /dvs/dncs/bin/dncsSetup
```

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

25 Type the following command and press **Enter**.

```
showActiveSessions
```

26 Did the results from step 25 include the message **INFORMIXSERVER is idle**?

- If **yes**, go to step 27.
- If **no**, follow these instructions.

a Type the following command and press **Enter**.

```
killActiveSessions
```

b Type the following command and press **Enter**. The message **INFORMIXSERVER is idle** should appear.

```
showActiveSessions
```

27 As **root** user again, type the following command and press **Enter**. A **Do you want to continue?** message appears.

```
/var/tmp/lu_continue
```

28 Type **y** and then press **Enter**. Messages similar to the following appear:

```
You're now ready to:
  * Reboot the machine using:
  # /usr/sbin/shutdown -g0 -i6 -y
```

Important: Do NOT execute the reboot command yet.

```
bash-3.00# /var/tmp/lu_continue


Do you want to continue with the upgrade?  [y,n,?,q] y

The live upgrade will now continue...

************************************************************************
*                          WARNING!!!                                  *
************************************************************************

Proceeding beyond this point will detach ALL d7xx submirrors!
All un-attached mirrors will be cleared.

Are you certain you want to proceed?  [y,n,?,q] y
d520: submirror d720 is detached
d720: Concat/Stripe is cleared
Data disks will be: c1t5d0s0
```

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

Modifying boot archive service
Activation of boot environment <DNCS.i4.4.0.7> successful.
Boot Environment           Is       Active Active    Can    Copy
Name                       Complete Now    On Reboot Delete Status
-------------------------- -------- ------ --------- ------ ----------
DNCS.pre_lu                yes      yes    no        no     -
DNCS.i4.4.0.7              yes      no     yes       no     -

################################################################################
################################################################################

The next step is to reboot the system to the new installation.
When you are ready, reboot with the following commands:

init 6

################################################################################
################################################################################
```

29 Examine the previous output and verify that the new software version displays **yes** for **Active on Reboot** for the new system release.

Note: Call Cisco Services if this is not the case.

30 Type the following command and press **Enter** to reboot the system.

```
/usr/sbin/shutdown -g0 -i6 -y
```

Important:

- The reboot process will take about an hour to complete and the system will actually reboot several times.
- Do NOT log on to the system until the CDE Login window appears. Several non-CDE log-on opportunities will appear. Ignore these.

31 When the CDE Login window appears, log onto the system as **root** user.

Build the DNCS Database

Note: If you have properly followed the instructions up to this point, the system components are stopped.

1. If necessary, open an xterm window on the DNCS.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type the following command and then press **Enter**. The system stops the cron jobs on the server.

   ```
   svcadm  -v  disable  -st  cron
   ```

4. Type the following command and then press **Enter**. The system establishes the root user environment.

   ```
   . /dvs/dncs/bin/dncsSetup
   ```

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

   Important: At some sites, a message similar to the following may appear:

   ```
   Failed to get SITE_ID __ database up?
   No LOCAL_SITE_ID available for site hostname=<hostname>.
   ```

   You can ignore this message.
5. Type the following command and then press **Enter**. The system converts the DNCS database.

   ```
   bldDncsDb
   ```

   Note: Depending upon the size of the database, this script may take over 30 minutes to complete.

Run the setupAS Script on the DNCS

In this procedure, you will run the setupAS script to establish the Application Server settings for the DNCS.

Note: If the system you are upgrading has no Application Server, skip this procedure and go to the next procedure in this chapter.

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

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

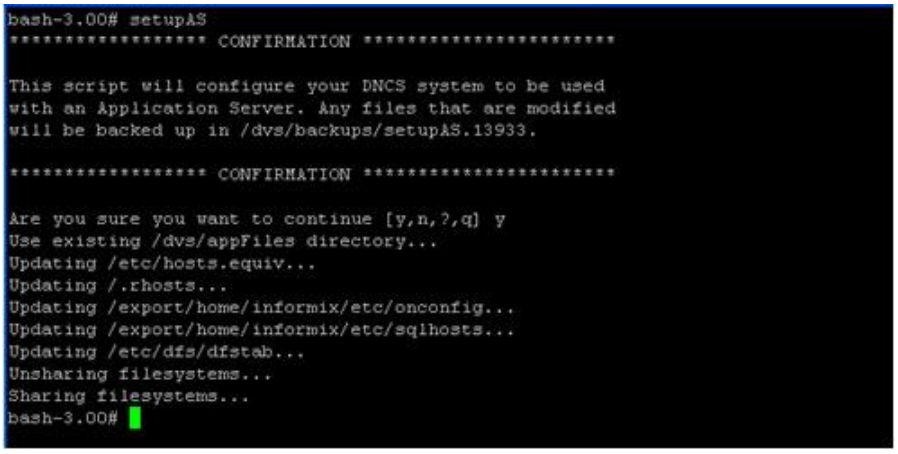
   a Type **su -** and press **Enter**. The password prompt appears.

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

3 Type the following command and press **Enter** to run the setupAS script. The **Are you SURE you want to continue** message appears.

   `setupAS`

4 Type **y** and press **Enter**. The script establishes the Application Server settings for the DNCS.



5 Complete the following steps on the DNCS to stop and restart the Informix engine.

   a Type the following command and press **Enter**.

   `/etc/init.d/informix stop`

   b Type the following command and press **Enter**.

   `/etc/init.d/informix start`

Check Log Files

In this procedure, you will inspect the log files associated with the upgrade of the DNCS software and confirm that there are no errors.

1 From an xterm window on the DNCS, type the following command and then press **Enter**. The /var/sadm/system/logs directory becomes the working directory.

```
cd /var/sadm/system/logs
```

2 Type the following command and then press **Enter**. The log file opens for review using the UNIX *more* utility.

```
more [log file]
```

Notes:

- Substitute the name of the log file for [log file].
- The log files associated with the upgrade of DNCS software are:
  - sysidtool.log
  - install_log
  - dncs_LiveUpgrade.log
  - dncs_restoreKeyFiles.log
  - dncs_S74update_TED.log
  - dncs_setupsds.log

Create the Custom User on the DNCS

In this procedure, you will create a custom user in order to provide access through remote services like the secure shell (SSH) or virtual network computing (VNC).

In conventional UNIX systems, the root user (also referred to as the superuser) is all-powerful, with the ability to read and write to any file, run all programs, and send kill signals to any process. In practical terms, this means that anyone who can become superuser has the power to modify configuration, or even bring down the entire network.

Role-based access control (RBAC) is an alternative to the all-or-nothing superuser model. RBAC is in keeping with the security principle of least privilege, which states that no user should be given more privilege than necessary for performing that user's job.

Notes:

- Console access is restricted to the root user.
- There is a default role in the system called the dncs user.

1 Type the following command and press **Enter** to add a new user, called dncsop (for DNCS operator) on the DNCS and the Application Server.

```
useradd -g dncs -c customuser -d /export/home/dncsop -m dncsop
```

2 Type the following command and press **Enter** to assign this role to the custom user.

```
usermod -R dncs dncsop
```

3 To switch to the dncs role over the network using SSH or VNC, type the following command and press **Enter**.

```
suxterm - dncs
```

Notes:

- You can add many user accounts in this manner to the DNCS system, such as smsoperator, remoteoperator, and vpnoperator. All of these users can access the DNCS remotely using SSH.
- The system operator needs X Windowing software, such as Xmanager or Exceed, running on a laptop in order to have remote GUI access to the DNCS or Application Server.

3

SR i4.4 Common Upgrade Procedures

Introduction

Now that you have finished upgrading the DNCS, you will upgrade the Application Server and complete additional upgrade procedures.

In This Chapter

Stop the cron Jobs on the DNCS

In this procedure, you will stop any cron jobs running on the DNCS and then kill any active sessions that might still be running.

1 From a root xterm window on the DNCS, type **pgrep -fl cron** and press **Enter**.

2 Is the cron process running?

- If **yes**, type **svcadm -v disable -s cron** and then press **Enter**. The system stops all cron jobs on the DNCS.

  Note: Go to step 3 when you are finished.

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

3 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.

4 Wait a few moments and then type **showActiveSessions** and press **Enter**.

  Result: One of the following messages appears:

- A message indicating that the **INFORMIXSERVER is idle**
- A message listing active sessions

5 Did the message in step 4 indicate that there are active sessions?

- If **yes**, follow these instructions:
  - **a** Type **killActiveSessions** and then press **Enter**. The system removes all active sessions from the database.
  - **b** Type **showActiveSessions** again and then press **Enter**.
  - **c** Did a message appear indicating that there are active sessions?
    - If **yes**, wait a few minutes and then repeat step b.
    - If **no**, the cron jobs are stopped.
- If **no**, the cron jobs are stopped.

Check Installed Version Numbers on the DNCS

1. From an xterm window on the DNCS, type the following command and press **Enter** to obtain a list of packages that are installed on the DNCS.

   ```
   pkginfo | grep SAI
   ```

2. Type the following command and press **Enter** to record the versions of the packages, one by one.

   ```
   pkginfo –l SAI[Package Name]
   ```

3. 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
DNCS Application	SAIdncs	i4.4.0.7	
DNCS/App Tools	SAItools	4.2.1.22	
DNCS Application Patch	SAIpatch	i4.4.0.7p3	
DNCS Platform	SAIcomplat	3.0.6	
DNCS GUI	SAIgui	i4.4.0.7	
DNCS WUI	SAIwebui	i4.4.0.7	
Solaris Patches	SAIpatch	10.20090928.0	
DNCS Online Help	SAIhelp	i4.2.2.1	
DNCS Report Writer	SAIrptwrt	R2.0.0.5	
MQAM	SAImqam	3.2.0	
PCG	SAIpcg	2.1.0.18	

4. 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 3?
   - If **yes**, go to the next procedure in this chapter.
   - If **no**, call Cisco Services and inform them of the discrepancy.

Edit the .profile File

In this section, you will make several edits to the .profile file on the DNCS that help facilitate the upgrade.

Note About Presence of Application Server at the Headend

In the following procedure, you will open and possibly edit the .profile file on the DNCS. In the event that the site you are upgrading does not use an Application Server, the **PKDVB_APPSERV_NOT_PRESENT** variable needs to be set accordingly. Follow these guidelines after you open the .profile file in the following procedure.

- If an Application Server is in use at the headend, be sure that the **PKDVB_APPSERV_NOT_PRESENT** variable is set to **0**.
- If an Application Server is NOT in use at the headend, be sure that the **PKDVB_APPSERV_NOT_PRESENT** variable is set to **1**.

Editing Debug and Logging Settings in the .profile File

After the upgrade to SR i4.4, some of the logging and debug settings that were managed through the .profile file will be managed through the DNCS user interface. Edit the .profile to remove these logging and debug settings.

Note: You will implement these logging and debug settings through the DNCS user interface later in the upgrade.

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

   ```
   cd  /export/home/dncs
   ```

2. Open the .profile file using the text editor of your choice.
3. Look for an entry in the .profile file similar to the following example:

   ```
   export  EMCDEBUG=BbKkQ9SD
   ```

4. Is the entry indicated in step 3 present in the .profile file?
   - If **yes**, record that entry here: _____; then, transform the entry into a comment.
   - If **no**, close the .profile file and continue with the next procedure in this section.
5. Save the changes to the .profile file and then close the text editor.

Activating the Changes to the .profile File

Follow this procedure to activate any changes that were made to the .profile file.

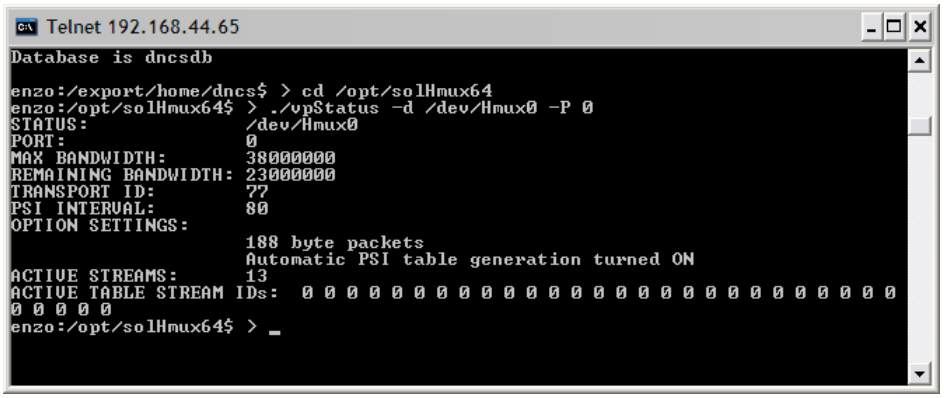
1. Click **Exit** (at the bottom of the screen).
2. When the confirmation message appears, Click **OK.**
3. When The CDE log-in window appears, log on to the system as **dncs** user.

Check the Status of the ASI Card

1 As **dncs** user on the DNCS, type the following command and press **Enter**. After a few minutes, the system displays the status of the ASI card.

```
/opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0
```

Example: Your results should look similar to, but not exactly like, the following example.



Note: An improperly installed ASI card will yield either no results or results that clearly show an error.

2 Do the results from step 1 look similar to the image displayed in step 1?

- If **yes**, go to the next procedure in this chapter.
- If **no**, type the following command and then press **Enter**.

  ```
  /usr/sbin/shutdown -y -g0 -i6
  ```

3 Log on to the DNCS as **dncs** user and open an xterm window.

4 Type the following command and then press **Enter**.

```
/opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0
```

5 Is the dncs user able to open the ASI card?

- If **yes**, go to the next procedure in this chapter.
- If **no**, call Cisco Services for assistance.

Upgrade the Application Server Software

Completing the Sun Fire V240 or V245 Application Server Upgrade

Use the instructions in this section to upgrade the Application Server.

Important: If you are upgrading a non-Cisco DVB Navigator server, follow the upgrade instructions that you obtained from the vendor of that server.

If you have followed all of the procedures of this document in order, all system components are shut down and the Application Server displays the CDE window.

Complete the following procedure to install the Solaris OS and Application Server software on to the Application Server.

Note: If you are using an external DVD drive, substitute *cdrom1* for *cdrom0*.

1 At the **ok** prompt on the Application Server, type the following command and press **Enter**.

```
boot -r
```

Result: The system boots into the Application Server and the CDE window appears.

2 Log on to the CDE of the Application Server as **root** user.

3 Insert the SR i4.4 DVD into the DVD drive of the Application Server.

Note: If the File Manager window opens, you can close it.

4 Type the following command and press **Enter**. A list of the mounted filesystems appears.

```
df -n
```

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

5 Does the output from step 4 show that the system mounted the DVD?

- If **yes**, go to step 7.
- If **no**, continue with step 6.

6 Follow these instructions to mount the DVD manually.

a Type the following command and press **Enter** to stop the volmgt process.

```
/etc/init.d/volmgt stop
```

b Type the following command and press **Enter** to determine the CD-ROM path.

```
rmformat -l
```

Example: Output should be similar to the following:

```
Looking for devices...
Volmgt Node: /vol/dev/aliases/cdrom0
sLogical Node: /dev/rdsk/c0t0d0s2
Physical Node: /pci@8,700000/ide@1/sd@0,0
Connected Device: TSSTcorp CD/DVDW TS-H652D SI00
Device Type: DVD Reader/Writer
```

c Type the following command and press **Enter** to manually mount the DVD.

```
mount -F hsfs /dev/dsk/c0t0d0s0 /cdrom
```

7 Type the following command and press **Enter**. The system displays the status of all of the metadevices on the DNCS.

```
metastat | more
```

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

8 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 9.
- If **no** (to either or both conditions), call Cisco Services for help in resolving these issues with the metadevices.

9 Type the following command and press **Enter**.

```
cd /cdrom/sai/scripts
```

10 Type the following command and press **Enter**. A confirmation message appears.

```
./doLiveUpgrade
```

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

Result: During the Live Upgrade of the Application Server, 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
-----------------------------------------------------
```

12 Type the following command and press **Enter** to inspect the log file.

```
tail -f /tmp/install_log
```

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

13 At the **Do you want to add to the above list?** message, 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 press **Enter**.
  - **b** Follow the on-screen directions to add to the list of files or directories.

    Important: Remember to include the /export/home/dncs/network directory, as well as any special files you identified in ***Identify Special Files to be Backed Up*** (on page 17).
  - **c** When you are finished adding key files, type **n** and then press **Enter**. The system displays a **Do you want to continue?** message.
  - **d** Type **y** and 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**.

Result: The system displays a **Do you wish to delete from the above list?** message.

14 Type **n** and then press **Enter**. The system displays a **Do you want to continue?** message.

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

Results:

- The system backs up the Application Server key files.
- The system generates the system identification (sysidcfg) file for the Solaris OS installation.

16 Wait for the following message to appear.

```
Run /var/tmp/lu_continue when you are ready to ASCII export
your database.
```

17 As **root** user, type the following command and press **Enter**. A **Do you want to continue?** message appears.

```
/var/tmp/lu_continue
```

18 Type **y** and press **Enter**. The following message appears.

```
You're now ready to reboot the machine.
```

19 Type the following command and press **Enter**.

```
/usr/sbin/shutdown -y -i6 -g0
```

Results:

- The Application Server reboots several times over a period of about an hour.
- Do NOT log on to the system until the CDE Login window appears. Several non-CDE log-on opportunities will appear. Ignore these.

20 Log on to the CDE window of the Application Server as **root** user.

Check Installed Version Numbers on the Application Server

1. From an xterm window on the DNCS, type the following command and press **Enter** to obtain a list of packages that are installed on the DNCS.

   ```
   pkginfo | grep SAI
   ```

2. Type the following command and press **Enter** to record the versions of the packages, one by one.

   ```
   pkginfo -l SAI[Package Name]
   ```

3. 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
Application Server	SAIapsrv	i3.4.0.8	
DNCS/App Tools	SAItools	4.2.1.22	
Solaris Patches	SAIpatch	10.20090928.0	
Platform	SAIcomplat	3.0.6	

4. 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 3?
   - If **yes**, go to the next procedure in this chapter.
   - If **no**, call Cisco Services and inform them of the discrepancy.

Create the Custom User on the Application Server

In this procedure, you will create a custom user in order to provide access through remote services like the secure shell (SSH) or virtual network computing (VNC).

In conventional UNIX systems, the root user (also referred to as the superuser) is all-powerful, with the ability to read and write to any file, run all programs, and send kill signals to any process. In practical terms, this means that anyone who can become superuser has the power to modify configuration, or even bring down the entire network.

Role-based access control (RBAC) is an alternative to the all-or-nothing superuser model. RBAC is in keeping with the security principle of least privilege, which states that no user should be given more privilege than necessary for performing that user's job.

Notes:

- Console access is restricted to the root user.
- There is a default role in the system called the dncs user.

1 Type the following command and press **Enter** to add a new user, called dncsop (for DNCS operator) on the DNCS and the Application Server.

```
useradd -g dncs -c customuser -d /export/home/dncsop -m dncsop
```

2 Type the following command and press **Enter** to assign this role to the custom user.

```
usermod -R dncs dncsop
```

3 To switch to the dncs role over the network using SSH or VNC, type the following command and press **Enter**.

```
suxterm - dncs
```

Notes:

- You can add many user accounts in this manner to the DNCS system, such as smsoperator, remoteoperator, and vpnoperator. All of these users can access the DNCS remotely using SSH.
- The system operator needs X Windowing software, such as Xmanager or Exceed, running on a laptop in order to have remote GUI access to the DNCS or Application Server.

Run the siteCmd Program

In this procedure, you will run the siteCmd program to create a "trusting relationship" between DNCS and Application Server.

Note: You need the hostname and IP address of the Application Server in order to run this program.

1 Open an xterm window on the DNCS.

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

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

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

3 Type the following command and press **Enter**.

```
siteCmd -S
```

4 At the **Enter the hostname of the site you are adding** prompt, type the hostname of the Application Server and press **Enter**.

5 At the **Enter the IP address of the site you are adding** prompt, type the IP address of the Application Server and press **Enter**. The **Do you want to continue** message appears.

   Example:

```
bash-3.00# siteCmd -S
Enter the host name of the site you are adding: appservatm
Enter the IP address of the site you are adding: 10.253.0.10
  The following line will be added to /etc/hosts:
  10.253.0.10     appservatm
Do you want to continue?  [y,n,?,q]
```

6 Type **y** and press **Enter**. The script checks Application Server connectivity, displays a warning message, and asks for confirmation to continue.

```
A backup of /etc/hosts is being placed in
/dvs/backups/setupSite.8238.
Checking site connectivity...
WARNING: Unable to access this site with the "generic" key.
This script will
attempt to repair this problem, but you will need the root
password for this
site ("appservatm") in order to continue. If you chose to
continue you
will be prompted for the root password.
Do you want to continue?  [y,n,?,q]
```

7 Type **y** and press **Enter**. The system prompts for the remote system (Application Server) root user password.

```
------------------------------------------------------------------
This system is for the use of authorized users only.
To protect the system from unauthorized use and to ensure the
system is functioning properly, activities on this system are
monitored and recorded.

Anyone using this system expressly consents to such monitoring
and recording.  If such monitoring reveals possible
evidence of criminal activity, system personnel may provide the
evidence of such monitoring to law enforcement officials and
it could lead to criminal and civil penalties.

Please note that "dncs" user is now a Role and you can't login
as "dncs" user.  Please contact your sysadmin for a login id.
------------------------------------------------------------------
Password:
```

8 Type the **root** password of the Application Server and press **Enter**.

Results:

- The script copies the public and RSA keys to both systems.
- The script enables the "trusting relationship" between DNCS and Application Server.
- The message **done** appears when the script has finished running.

Install DNCS or Application Server Patches

If you have any patch software for the DNCS or the Application Server, install them now. Instructions for installing the patch software should have accompanied the DVD that contains the software.

Enable Optional and Licensed Features

If you have properly followed the instructions in this chapter, the system processes should currently be stopped. Now is the time to enable the optional features you have chosen as part of this upgrade, except for Direct ASI. The ASI feature requires extensive system configuration. If the system you are upgrading has planned to support this feature, contact Cisco Services to have the licensed or optional features enabled on your network.

Confirm That Direct ASI is Enabled (Optional)

If you have enabled Direct ASI as part of this upgrade, complete this procedure to ensure that an entry has been made for Direct ASI in the database.

1 From an xterm window on the DNCS, type **dbaccess dncsdb -** and then press **Enter**.

2 Type **select * from mc_config where mc_param_name = "DIRECT_ASI";** and then press **Enter**. You should see output similar to the following:

mc_name **Scientific-Atlanta**

mc_param_name **DIRECT_ASI**

mc_param_data **0**

Note: Call Cisco Services if the results from step 2 do not show DIRECT_ASI.

3 Press the **Ctrl** and **c** keys simultaneously to exit from the dbaccess utility.

Restart the System Components

Important: Note these important points:

- Do not overlook this procedure. This procedure restarts system processes. You must restart the system processes at this time. If you fail to restart the system processes, you will delay completion of the upgrade.
- Be certain that you are logged on to the DNCS as dncs user. Do not start the processes as root user.
- Be certain to start the DNCS processes and the Application Server processes.
- Be certain that the set-top image and EMM files have been reloaded before starting the processes. Failure to load the set-top image files will result in code download failing, as the set-top image files cannot be loaded onto the carousel.

Restarting the DNCS

Stop the dncs Process

1 As **dncs** user, follow these steps to stop the DNCS.

a Type the following command in a console window and press **Enter**.

```
cd /dvs/dncs/bin
```

b Type the following command and press **Enter**. The dncsControl utility window opens.

```
dncsControl
```

c Type **2** and then press **Enter**.

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 Type the following command in the console window from step a, and then press **Enter**.

```
dncsStop
```

f Wait a few minutes and then press **Enter** on the dncsControl user interface. 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 Type the following command and press **Enter** to verify that the DNCS processes have stopped.

```
ps -ef | grep dvs
```

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

- If **yes**, go to step 2.
- If **no**, (there are other processes still running) follow these instructions, type **dncsKill** on the DNCS and then press **Enter**.

i Type the following command and press **Enter** to verify that the processes have stopped.

```
ps -ef | grep dvs
```

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

- If **yes**, go to step 2.
- If **no**, (there are other processes still running), type (as **root** user) **kill -9 [PID]** for all processes that have not stopped, and then press **Enter**.

  Note: Substitute the process ID for [PID].

2 Close the dncsControl utility user interface.

Start the dncs Process

Note: You need to be dncs user to start the dncs process.

1 Type the following command and press **Enter**.

```
cd /dvs/dncs/bin
```

2 Type the following command and press **Enter**.

```
dncsStart
```

3 Type the following command and press **Enter** to open the Administrative Console.

```
admincon
```

Results:

- The DNCS Control window opens.
- Green indicators replace red indicators on the DNCS Control window.

4 From an xterm window on the DNCS, type the following command and press **Enter**. The Dncs Control window updates to list the status of all of the processes and servers running on the DNCS.

```
dncsControl
```

5 Wait for the Dncs Control window to list the current status (**Curr Stt**) of all the processes and servers as **running**.

Notes:

- The Dncs Control window updates automatically every few seconds, or you can press **Enter** to force an update.
- The indicators on the DNCS Control window all become green when the processes and servers have restarted.

Restarting the Application Server

Stop the Application Server Process

Note: You need to be dncs user in an xterm window on the Application Server to stop the Application Server process.

1. If necessary, open an xterm window, as **dncs** user, on the Application Server.
2. Type the following command and press **Enter**.

   ```
   cd /dvs/appserv/bin
   ```

3. Type the following command and press **Enter**. The AppControl utility window opens.

   ```
   ./appControl
   ```

4. Type **2** and then press **Enter**.
5. Make a note of the processes that are running so that you can compare these processes with those that are running after the upgrade.
6. Type the following command and press **Enter**.

   ```
   ./appStop
   ```

7. Wait a few minutes, press **Enter** on the AppControl user interface, 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.

8. If, after waiting several minutes, there are Application Server processes still running, type the following command and press **Enter**.

   ```
   ./appKill
   ```

9. Close the AppControl utility window.

Start the Application Server Process

Log on to the Application server as **dncs** user and follow these steps to start the Application Server process.

1. Open an xterm window on the Application 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** to confirm that all the cross-mounted folders are mounted properly.

```
df -h
```

Example: Output should be similar to the following example:

```
dncs_host:/disk1/dvs/dvs_doc
              217G   726M   214G     1%    /disk1/dvs/dvs_doc
dncs_host:/disk1/dvs/appFiles
              217G   726M   214G     1%    /disk1/dvs/appFiles
dncs_host:/export/home/informix
               7.9G   3.0G   4.8G    38%
/export/home/informix
```

4 Did the cross-mounted folders mount properly?

- If **yes**, skip to step 7.
- If **no**, continue with step 5.

5 Type the following command and press **Enter**.

```
mountall
```

6 Type the following command and press **Enter** to log out as the **root** user.

```
exit
```

7 As **dncs** user, type the following command and press **Enter**.

```
cd /dvs/appserv/bin
```

8 Type the following command and press **Enter**. The AppControl utility window opens.

```
./appControl
```

9 Type **2** and then press **Enter**.

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

11 Type the following command and press **Enter**.

```
./appStart
```

12 Wait a few minutes, press **Enter** on the AppControl user interface, and verify that all of the processes have started.

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

13 Close the AppControl utility window.

Restart the cron Jobs

Restarting the cron Jobs on the DNCS

1. From a dncs xterm window on the DNCS, type **pgrep -fl cron** and then press **Enter**.
2. Have the cron jobs restarted on their own?
   - If **yes,** skip the rest of this procedure and go to ***Restarting the cron Jobs on the Application Server*** (on page 60).
   - If **no**, continue with step 3.
3. From a root xterm window, type **svcadm -v enable -rs cron** and then press **Enter**. The system restarts all cron jobs.
4. Confirm that the cron jobs have restarted by typing **pgrep -fl cron** and then pressing **Enter**.
5. Go to ***Restarting the cron Jobs on the Application Server*** (on page 60).

Restarting the cron Jobs on the Application Server

Follow these instructions to restart the cron jobs, if necessary, on the Application Server.

Note: The cron jobs on the Application Server may have restarted on their own when you booted the application Server, earlier in this chapter.

1. From a dncs xterm window on the Application Server, type the following command and then press **Enter**.

   ```
   pgrep -fl cron
   ```

2. Have the cron jobs restarted on their own?
   - If **yes**, skip the rest of this procedure and go to SR i4.4 Post Upgrade Procedures.
   - If **no**, continue with step 3.
3. From a root xterm window on the Application Server, type the following command and then press **Enter**. The system restarts all cron jobs.

   ```
   svcadm -v enable -rs cron
   ```

4. Confirm that the cron jobs have restarted by typing the following command and then pressing **Enter**. The system should list /usr/sbin/cron.

   ```
   pgrep -fl cron
   ```

4

SR i4.4 Post Upgrade Procedures

Introduction

Complete 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 +91 9840717688 for assistance.

In This Chapter

Check Transport Stream ID Values

Important: Complete this procedure only in the event that the system you are upgrading supports the QAM-family of modulators. If your system does not utilize any of the QAM-family of modulators, skip this procedure and go to the next procedure in this chapter.

In this procedure, confirm that both the **Start Transport Stream ID** and **End Transport Stream ID** values are not both set to 0 (zero). If both values are set to 0, the system operator will be unable to save a QAM configuration or a VOD stream.

1. From the DNCS Administrative Console, select the DNCS tab and then the System Provisioning tab.
2. Click **DNCS System**. The DNCS System Configuration window opens.
3. Click the **Advanced Parameters** tab.
4. Are both the **Start Transport Stream ID** and **End Transport Stream ID** values set to 0 (zero)?
   - If **yes**, go to step 5 and follow the guidelines for setting the transport stream values ID (TSID).
   - If **no**, leave them at their current values and exit from the DNCS System Configuration window by clicking **Cancel**.

   Note: Only change the values if *both* fields are set to 0.
5. You were directed to step 5 because both the **Start Transport Stream ID** and **End Transport Stream ID** values were set to 0. Consult with the system operator and determine what TSIDs were in use on the system prior to the upgrade, and set the TSIDs accordingly.

   In general, follow these guidelines when setting the values:
   - If the site you are upgrading uses only our QAM modulators, set the **Start Transport Stream ID** and **End Transport Stream ID** values to **0** and **65535**, respectively.
   - If the site you are upgrading uses third-party QAM modulators, in addition to our QAM modulators, select a range for those third-party modulators. For example, select **0** and **39999** as the range for our modulators, and **40000** and **65535** as the range for the third-party modulators.
6. If you made an edit in step 5, click **Save** and close the DNCS System Configuration window.

Set Debug Flags

Follow this procedure to reset the debug flags through the user interface of the DNCS.

1. From a **dncs** xterm window, type **more /export/home/dncs/.profile** and press **Enter**. The contents of the .profile file appear.
2. Locate the **export EMCDEBUG** entry that you remarked out in ***Editing Debug and Logging Settings in the .profile File*** (on page 42) and record it here:

   _____

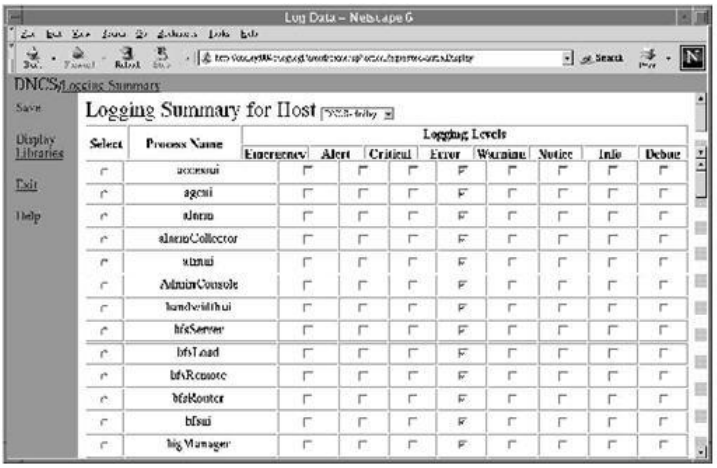
   Example: export EMCDEBUG=BbKkSDQLGOo
3. Using the export EMCDEBUG value, record the logs in which you want to enable the Debug log on the DNCS user interface UI.

   Note: If you need assistance, contact Cisco Services.

   Example: For the example in step 2, *BbKkSDQLGOo*, the following Debug logs should be enabled:

   - bossServer
   - camAm
   - camAuditor
   - camEx
   - camFastrefrsh
   - camparamui-deprecate
   - camPsm
   - camTedChecker
   - siManager
   - MMMServer
   - saManager
4. On the DNCS Administrative Console, click the **DNCS** tab.
5. Click the **Utilities** tab.

6 Click **Logging**. The Logging Summary window opens.



7 Click the checkbox in the **Debug** column for each process that you recorded in step 3, as well as the following processes if they were not included in your list:

- bossServer
- dsm
- qamManager

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

9 Click **Exit**.

10 Close the Logging Summary window.

Examine and Re-Order the pddataqampat Table

In some system releases, session ID 199 had to be the last entry in the **Session Number** column of the pddataqampat table. With the current release, this is no longer a requirement, and in fact, session ID 199 must now appear in numerical order along with all the other BFS sessions. Session ID 199 should now appear immediately after session ID 22.

First, you need to ensure that BFS session 199 is enabled. If the system you are upgrading has the Distributed DNCS licensed, consult with the system operator to determine which distributed site(s) should have session 199 (bootloader) enabled.

Verify that BFS Session 199 is Enabled

Make sure that BFS session 199 is enabled. If the system you are upgrading has the Distributed DNCS licensed, consult with the system operator to determine which distributed site(s) should have session 199 (bootloader) enabled.

1. From the DNCS Administrative Console, select the **Application Interface Modules** tab.
2. Select **BFS Admin**. The Site DNCS BFS Administration window opens.
3. Does your system support the Distributed DNCS feature?
   - If **yes**, the result from step 2 shows multiple site names; go to step 4.
   - If **no**, the result from step 2 shows that **dncsatm** and maybe **appservatm** are displayed; go to step 5.
4. Double-click the DNCS entry, typically Site ID 1. The Site DNCS BFS Administration window opens.
5. Click **Sources**. The Source List window opens.
6. Double-click Source ID 199. The Set Up BFS Source window opens.
7. Is the **Run** button (next to **Datapump**) selected?
   - If **yes**, click **Cancel** and go to step 10.
   - If **no**, select **Run**, click **Save**, and then go to step 8.
8. Select a **QAM** from the **Available** list and then select a port from the **Output Ports** list.
9. Click **Save**.
10. Repeat steps 4 through 9 for each applicable distributed site.
11. Close any open BFS-related windows.

Tear Down Session ID 199

Begin the process of re-ordering the pddataqampat table by tearing down session ID 199. Follow these instructions to tear down session ID 199.

Note: From an xterm window on the DNCS where you are logged on as dncs user, you can run the *clearDbSessions*, *clearDbSessions -c*, and *clearDbSessions -o* commands to remove expired sessions from the BFS. This will clean up the Session List UI and allow you to see only those sessions that have been rebuilt.

1. From the DNCS tab on the DNCS Administrative Console, select **Utilities** and then click **Session List**. The Sessions Filters window appears.
2. Choose one of the following options:
   - If your system uses QAM modulators, click **Display QAM Sessions**.
   - If your system uses PCGs, click **Display PCG Sessions**.

   Result: The window updates to display session data for the selected hardware item.
3. Does the data show that session ID 199 *directly* follows session ID 22, and that session ID 199 has a session MAC address of 00:00:00:00:00:00?
   - If **yes** (to both conditions), close all session-related windows and skip this entire section; go to the next procedure in this chapter.
   - If **no** (to at least one condition), continue with step 4.
4. Click the checkbox associated with session ID 199.

   Note: Session ID 199 is likely to be at the bottom of the window.
5. Click **Teardown**. The system tears down the selected session.
6. Wait a few minutes for the BFS sessions to rebuild.
7. Confirm that the rebuilt BFS session ID 199 now has a session MAC address of 00:00:00:00:00:00 and that it follows session ID 22.

Checking the pddataqampat Table-ASI

After upgrading to SR i4.4, follow these instructions to inspect the contents of the pddataqampat table and then to re-order the table, if necessary.

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

   Note: If the RCS feature is not enabled on the system, the Site DNCS BFS Administration window appears instead.
2. Double-click the appropriate hostname. The Site [hostname] BFS Administration window opens.

   Note: You will probably want to examine the pddataqampat table on the DNCS first, before you examine any remote sites.
3. Double-click the appropriate Host Name. The Set Up BFS Host window opens.

4 Click **PAT Configuration**. The Inband Data PAT window opens.

5 Go to Recording and Re-Creating Out-of-Order Entries.

Recording and Re-Creating Out-of-Order Entries

In this procedure, you will delete session IDs greater than 22, and then recreate them such that session ID 199 comes right after session ID 24.

Important: Pay special attention to step 4 of this procedure. Step 4 provides special instructions regarding session ID 199.

1 On a sheet of paper, write down every entry in the Inband Data PAT window with a **Session Number** greater than 22.

Important: Be sure to record each field: **Session MAC Address**, **Session Number**, **Program Number**, and **PMT PID**.

2 Follow these instructions to delete each entry with a **Session Number** greater than 22.

a Highlight an out-of-order entry and click **Delete Entry**. A confirmation message appears.

b Click **OK** (to confirm the intention to delete). The system deletes the out-of-order entry.

Note: Ignore any BFS restart messages that may appear. You will stop and restart the BFS processes later in this section.

3 Click **New Entry** on the Inband Data PAT window. The PAT Setup window appears.

4 On the PAT Setup window, type in **Session MAC Address 00:00:00::00:00:00** and **Session Number 199**.

Note: The **Program Number** and **PMT PID** fields are already filled in. Use the default data for these entries.

Important: For session ID 199, do *not* enter 77:77:77:77:77:77 as the Session MAC Address. Instead, enter the session MAC address for the site, similar to what you would do for any other session.

5 Click **Save**. The system saves the just-added entry in proper ascending order.

6 Repeat steps 3 through 5 for each out-of-order entry that you recorded on the sheet of paper from step 1.

Note: When you have completed this procedure, all Program Numbers and PMT PIDs will be in ascending order.

Stopping the bfsServer Process

Complete the following steps to stop the bfsServer process that is running on the DNCS.

1 If the DNCS Control window is not already open, click the **Control** button in the DNCS area of the DNCS Administrative Console Status.

Result: The DNCS Control window opens.

2 Select **bfsServer**.

3 Click **Process** and then select **Stop Process**. A confirmation message opens.

4 Click **Yes** to stop the bfsServer process. The indicator next to bfsServer turns red.

Tearing Down the BFS Sessions

After stopping the BFS Server processes, tear down the BFS sessions. Follow these instructions to tear down the BFS sessions.

1 From the **DNCS** tab, click the **Utilities** tab, and then click **Session List**. The Session Filter window opens.

2 Choose one of the following options:

- If your system uses QAM modulators, click **Display QAM Sessions**.
- If your system uses PCGs, click **Display PCG Sessions**.

Result: The window updates to display session data for the selected hardware item.

3 Click the **Select** box adjacent to the lowest numbered session. A checkmark appears in the Select box to the left of that session.

4 Click **Teardown Selected Sessions**. The BFS will tear down all sessions and will then rebuild each session.

Note: It may take a few minutes for all of the sessions to rebuild.

5 When all sessions have been rebuilt (the session IDs are green in color), click **Exit all Session** screens.

Restarting the bfsServer Process

Use the dncsControl utility to restart the BFS Server processes on the DNCS. Follow these instructions to restart the BFS Server processes.

1. If the DNCS Control window is not already open, open this window by clicking the **Control** button in the DNCS area of the DNCS Administrative Console Status. The DNCS Control window opens.
2. From the list of processes, select **bfsServer**.
3. On the Process menu, click **Start Process**.
4. Wait for the indicator next to bfsServer to turn green. A green indicator next to bfsServer means the process has restarted.

Verify the crontab Entries

After upgrading the DNCS, inspect the crontab file to verify that it contains an entry for dbOptimizer. Follow these instructions to inspect the crontab file.

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

2 Type **cd** and then press **Enter**. The home directory of /export/home/dncs becomes the working directory.

3 Type **crontab -l** and then press **Enter**. The system lists the entries in the crontab file.

Note: The 'l' is a lowercase L.

4 Does the crontab file include an entry for **dbOptimizer**?

- If **yes**, go to Examining the CED.in Entry.
- If **no**, call Cisco Services for assistance.

Examining the CED.in Entry

Our engineers developed the dbOptimizer program to delete EMMs that are no longer needed by DHCTs. Most EMMs are assigned to DHCTs during the staging process when DHCTs are prepared for deployment in the homes of subscribers. These EMMs are also stored in the database of the DNCS. When a DHCT has been successfully staged, those EMMs associated with the staging process are no longer needed and should be removed from the DNCS database. The dbOptimizer program is configured to run by default each Saturday at 4 AM.

The /dvs/dncs/bin/CED.in file in the DNCS contains a value that represents a number of *days*. The dbOptimizer program is designed to delete unneeded EMMs that are older than the number of days specified in the CED.in file.

In this procedure, you will examine and change, if necessary, the number of days specified in the CED.in file.

Note: Our engineers recommend the default value of 90 days.

1 From an xterm window on the DNCS, type **cat /dvs/dncs/bin/CED.in** and then press **Enter**. The system displays the number of days that EMMs will be retained. EMMs that are older than this number of days will be deleted by the dbOptimizer program when it runs each Saturday.

2 Are you satisfied by the number of days specified by the CED.in file?

- If **yes**, go to Adding Custom crontab Entries.
- If **no**, go to step 3 to edit the CED.in file.

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 **echo <new # of days> > /dvs/dncs/bin/CED.in** and then press **Enter**. The system changes the value stored in the CED.in file.

Example: To set the value to our recommended default value of 90 days, type **echo 90 >/dvs/dncs/bin/CED.in** and then press **Enter**.

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

Adding Custom crontab Entries

We preserve old crontab entries in the /var/spool/cron/crontabs.previous directory on the DNCS and the Application Server. Examine these old crontab entries for each user on the DBDS system (dncs, root, informix). Then consult with the system operator to determine whether any of these old entries should be retained. If necessary, add the required crontab entries to the current crontab file.

1 Open two xterm windows and log on to each as **root** user.

2 Follow these instructions in one xterm window.

Note: This xterm window will contain the pre-upgrade crontab entries for each user.

a Type **cd /var/spool/cron/crontabs.previous** and then press **Enter**.

b Type **less root** and then press **Enter**.

Result: The system displays the contents of the pre-upgrade root crontab file.

3 In the second xterm window, type **crontab -l root** and then press **Enter**. The system displays the contents of the current root crontab file.

4 Compare the pre-upgrade and post-upgrade crontab entries. If the pre-upgrade crontab file contains site-specific, unique entries, consult with the system operator regarding whether those entries are still needed.

5 Are there unique crontab entries that need to be retained?

- If **yes**, follow these instructions.
  - **a** Type **crontab -l > /tmp/root.cron** and then press **Enter**. The systems copies the root crontab file to /tmp/root.cron.
  - **b** Type **vi /tmp/root.cron** and then press **Enter**.
  - **c** Add any unique entries to the /tmp/root.cron file and then save the file.
  - **d** Type **crontab /tmp/root.cron** and then press **Enter**. The edited /tmp/root.cron file becomes the new root crontab file.
  - **e** Type **crontab -l root** and then press **Enter** to verify that the crontab file properly contains the unique entries.
- If **no**, go to step 6.

6 Type **su - informix** and then press **Enter**.

7 Repeat steps 2 through 5 for the informix user.

8 Type **exit** and then press **Enter** in both xterm windows.

9 Repeat steps 2 through 5 for the dncs user.

Change the DNCS Data Pump Rates

See Recommendations for Data Carousel Rate Management

Refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377) and make any changes to the system's data carousel rates that may be required.

CAUTION:

Do not make any changes to the data rates without first receiving permission from the system operator to make those changes.

Verify SR i4.4

Verifying the System Upgrade

Complete these steps to verify a successful upgrade to SR i4.4.

1 Type the following command and press **Enter**.

```
cd /dvs/dncs/Utilities/doctor
```

2 Type the following command and press **Enter**. This command runs the Doctor Report. Review the Doctor Report to ensure that communications exists between all DBDS elements.

```
doctor -vn
```

3 Type the following command and then press **Enter** to verify that you are using no more than 85 percent of the partition capacity of each disk.

```
df -k
```

Important: If any disk partition lists a capacity greater than 85 percent, contact Cisco Services at +91 9840717688 before proceeding.

Set Staging Options

After upgrading SR i4.4, remember to set the DHCT staging options. Complete these steps to set the default staging options for the DHCTs.

Note: The staging options may have been set in a previous upgrade.

Important: Consult with the system operator before you make any changes. Each site uses different staging options.

1. From the DNCS Administrative Console, click the **Server Applications** tab.
2. Click **DHCT Config**. The DHCT Configure Prompt window appears.
3. Click **Staging Defaults** on the DHCT Configure Prompt window. The Set Up Staging Defaults window appears.
4. Set your DHCT staging options and click **Save** when complete.

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 DNCS for the presence of the atm_addr variable, and to add the variable, if necessary.

1. If necessary, open an xterm window on the DNCS.
2. Type the following command and then press **Enter**. The /dvs/dncs/bin directory becomes the working directory.

   ```
   cd  /dvs/dncs/bin
   ```

3. Type the following command and press **Enter**.

   ```
   grep atm_addr dncsSetup
   ```

   Example: Output should be similar to the following example:

   ```
   atm_addr=dncsatm; export atm_addr
   ```

4. Does the dncsSetup file contain the entry as described in step 3?
   - If **yes**, go to the next procedure in this chapter.
   - If **no**, follow these instructions.
     a. If necessary, open an xterm window on the DNCS.
     b. Type the following command and then press **Enter**. The **password** prompt appears.

        ```
        su - dncs
        ```

     c. Type the dncs password and then press **Enter**.
     d. Type the following command and then press **Enter**. The dncsSetup file opens using the UNIX vi text editor.

        ```
        vi  dncsSetup
        ```

     e. 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.

     f. Save and close the dncsSetup file.
     g. Type **exit** and then press **Enter** to log out of the dncs role.
     h. Go to the next procedure in this chapter.

Set the Clock on the TED (Optional)

Complete these steps to set the clock on the TED.

Note: In Ted 2.x, the rsh program is enabled. In Ted 3.x, rsh is not enabled and you may have to use the SSH protocol. Contact Cisco Services for assistance, if needed.

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

   Note: The "l" is a lowercase L.
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 as the root user.

Upgrade the PCG

An upgrade of the PCG is required for the SR i4.4 system upgrade. To upgrade the PCG, refer to *PowerKEY CAS Gateway (PCG) for DBDS and ISDP Networks Installation, Upgrade, and Operation Guide* (part number 4017672).

Important: Note these important points about the PCG upgrade.

- Sites that upgrade from version 1.x of the PCG to version 2.x need the PCG boot install CD.
- Sites that upgrade from version 2.0 of the PCG to version 2.1 do not need the boot install CD.

Upgrade the TED

An upgrade to version 3.1.0.7 of the TED is required for SR i4.4. To upgrade the TED, refer to *Upgrading the TED to Release 3.1.0.6 Technical Bulletin* (part number 4038947).

Note: After the system has been upgraded to SR i4.4, the TED needs to be reinitialized. The system operator needs to have all the necessary keys available in order to reinitialize the TED. Reinitializing instructions are contained in the aforementioned document.

Set Up the RNCS

If the site you are upgrading is licensed to support the Regional Network Control System (RNCS), then follow the directions in this section.

Enable the RNCS Feature

Run the licenseGen software in order to enable the RNCS feature of the DBDS. Refer to the technical bulletin *Proprietary: Procedures for Enabling Optional Features on the DBDS -- INTERNAL ONLY* (part number 4000631), for instructions on how to enable the RNCS feature.

Note: The interface of the licenseGen software refers to the RNCS as the Distributed DNCS.

Register RNCS With the DNCS

After using the licenseGen software to enable the Distributed DNCS feature on the DNCS, your next step is to register each RNCS with the DNCS. Refer to Appendix A, **The siteCmd Program**, in *RNCS Installation and Upgrade Instructions For SR 2.7/3.7 or SR 4.2* (part number 4012763), for an overview of the siteCmd program and for specific instructions on registering the RNCS.

Provision the RNCS

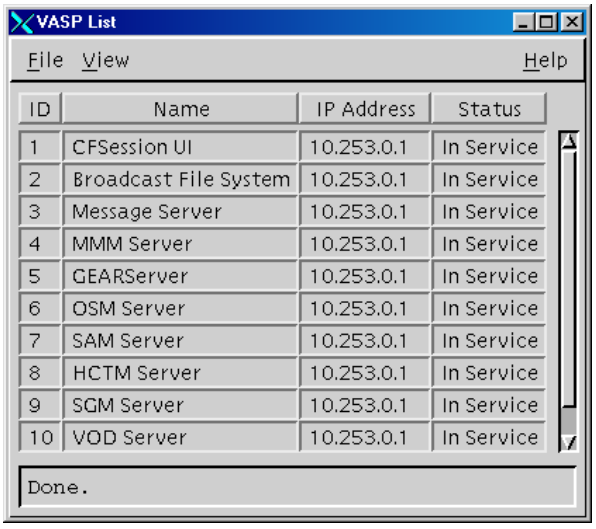
After using the siteCmd program to register the RNCS with the DNCS, use the online help of the DNCS to provision the RNCS.

Note: Provisioning the RNCS refers to adding components, such as QAMs and PCGs, as well as configuring the parameters on the BFS Administration GUI.

Create a VASP Entry on the DNCS

After provisioning each remote site that your system supports, you need to create a VASP entry on the DNCS for each of those sites. Follow these instructions to create the VASP entry.

1 From the DNCS Administrative Console, select the **Network Element Provisioning** tab and then click **VASP**. The VASP List window appears.



2 Click **File** and then select **New**. The Set Up VASP window appears.

3 Follow these directions to configure the Set Up VASP window.

- **a** For the **VASP Type** field, select **MMM Server**.
- **b** In the **ID** field, type a unique ID number.
- **c** In the **Name** field, type a meaningful name that you can use when referring to the remote site.
- **d** In the **IP Address** field, type the IP address of the remote site.
- **e** In the **Status** field, click **In Service**.
- **f** In the **Site ID** field, select the number that you have used to identify this site.

4 Repeat these instructions for each remote site that the system supports.

5

Enable Disk Mirroring

Introduction

Follow the procedure in this chapter only if you have upgraded a Sun Fire V880 or V890 DNCS or a a Sun Fire V240 or V245 Application Server during the upgrade to SR i4.4.

Important: Be sure that you complete this procedure during the current maintenance window on the night of the server upgrade. If you wait until the following night to complete this procedure, the server will operate an entire day without its disk-mirroring functions in place.

Important Note to Consider

You should follow the procedure in this chapter only under one of the following circumstances:

- You are satisfied with the upgrade and want to commit the system changes

  Note: Rolling back an upgrade after completing the procedure in this chapter is time consuming and takes more effort.

- You have rolled back from an unsuccessful upgrade and want to synchronize the mirrors

In This Chapter

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.

Attaching Mirrors

Follow this procedure to run a script that attaches submirrors to their respective mirrors and creates all necessary hot spare disks.

Important: Follow this procedure only if you have upgraded a Sun Fire V445, V880 or V890 DNCS server or a Sun Fire V240 or V245 Application Server.

Note: If you are using an external DVD drive, substitute *cdrom1* for *cdrom0*.

1. Insert the system upgrade DVD into the DVD drive of the DNCS or Application Server.
2. Type the following command and press **Enter**. A list of the mounted filesystems appears.

   ```
   df  -n
   ```

   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the DVD.
3. From an xterm window where you are logged on as root user, type the following command and press **Enter**. A confirmation message appears.

   ```
   /cdrom/cdrom/sai/scripts/attach_mirrors
   ```
4. 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.
5. Type the following command and press **Enter**.

   ```
   eject cdrom
   ```
6. Repeat steps 1 through 5 if you need to attach the mirrors on a second server, such as the standalone Application Server.

Set the Boot Device on the V445 Hardware Platform

After the DNCS upgrade to SR i4.4, if your hardware platform is a Sun Fire V445, you need to set the boot device. Use this procedure to set the boot device.

1 As **root** user in an xterm window on the DNCS, type the following command and press **Enter**.

Note: This command is lengthy; it needs to be entered on one line (before pressing **Enter**).

```
eeprom boot-
device=/pci@1e,600000/pci@0/pci@2/scsi@0/disk@0,0:a
/pci@1e,600000/pci@0/pci@2/scsi@0/disk@4,0:a
```

2 Type the following command and press **Enter** to verify the boot device.

```
eeprom boot-device
```

6

Back Up the System Components

Introduction

This chapter directs the upgrade engineer to reference the latest version of the backup procedures that pertain to SR i4.4, in order to back up the database, the DNCS file system, and the Application Server file system.

Notes:

- The backup procedures that pertain to the Application Server refer to the SA Application Server. Consult with the vendor of any third-party Application Server you may be using for the relevant procedures.
- We recommend that the system operator be present when performing these backups.

In This Chapter

Back Up the System Components

Follow these procedures in Chapter 1 of this guide to back up the file systems and the database:

- ***Back Up the File Systems*** (on page 5)
- ***Back Up the Database*** (on page 8)

7

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

Stopping System Components

Introduction

Use the procedures in this appendix to stop the Application Server and the DNCS.

In This Appendix

Stop System Components

Stopping the Application Server

This section provides procedures for stopping the Cisco DVB Navigator Server.

You need to be **dncs** user in an xterm window on the Application Server to stop the Application Server process.

1. If necessary, open an xterm window, as **dncs** user, on the Application Server.
2. Type the following command and press **Enter**.

   ```
   cd /dvs/appserv/bin
   ```

3. Type the following command and press **Enter**. The AppControl utility window opens.

   ```
   ./appControl
   ```

4. Select option **2** and then press **Enter**.
5. Make a note of the processes that are running so that you can compare these processes with those that are running after the upgrade.
6. Type the following command and press **Enter**.

   ```
   ./appStop
   ```

7. Wait a few minutes, press **Enter** on the AppControl user interface, 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.

8. If, after waiting several minutes, there are Application Server processes still running, type the following command and press **Enter**.

   ```
   ./appKill
   ```

9. Close the AppControl utility window.

Stopping the DNCS

1. As **dncs** user in an xterm window on the DNCS, type the following command and press **Enter**.

   ```
   cd /dvs/dncs/bin
   ```

2. Type the following command and press **Enter**. The dncsControl utility window opens.

   ```
   dncsControl
   ```

3. Select option **2** and then press **Enter**.
4. Make a note of the processes that are running so that you can compare these processes with those that are running after the upgrade.

5 Type the following command and press **Enter**.

```
dncsStop
```

6 Wait a few minutes and then press **Enter** on the dncsControl user interface. 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.

7 Type the following command and press **Enter** to verify that the DNCS processes have stopped.

```
ps -ef | grep dvs
```

8 Do the results from step 7 show that dncsInitd, dncsResMon, and appInitd are the only three processes still running?

- If **yes**, go to step 11.
- If **no** (there are other processes still running), follow these instructions.
  - **a** Type **dncsKill** on the DNCS and then press **Enter**.
  - **b** Type **appKill** on the Application Server and then press **Enter**.

9 Type the following command and press **Enter** to verify that the processes have stopped.

```
ps -ef | grep dvs
```

10 Do the results from step 9 show that dncsInitd, dncsResMon, and appInitd are the only three processes still running?

- If **yes**, go to step 11.
- If **no** (there are other processes still running), type (as **root** user) the following command for all processes that have not stopped, and then press **Enter**.

  ```
  kill -9 [PID]
  ```

  Note: Substitute the process ID of the running process for [PID].

11 Close the dncsControl utility user interface.

B

Restarting System Components

Introduction

Use the procedures in this appendix to restart the system components.

In This Appendix

Restart System Components

Restarting the DNCS

You need to be **dncs** user to start the DNCS processes.

1 As **dncs** user in an xterm window on the DNCS, type the following command and press **Enter**.

```
cd /dvs/dncs/bin
```

2 Type the following command and press **Enter**.

```
dncsStart
```

3 Type the following command and press **Enter** to open the Administrative Console.

```
admincon
```

Results:

- The DNCS Control window opens.
- Green indicators replace red indicators on the DNCS Control window.

4 Type the following command and press **Enter**. The Dncs Control window updates to list the status of all of the processes and servers running on the DNCS.

```
dncsControl
```

5 Wait for the Dncs Control window to list the current status (**Curr Stt**) of all the processes and servers as **running**.

Notes:

- The Dncs Control window updates automatically every few seconds, or you can press **Enter** to force an update.
- The indicators on the DNCS Control window all become green when the processes and servers have restarted.

Restarting the Application Server

You need to be **dncs** user on the Application Server to restart the Application Server processes.

1 Open an xterm window on the Application 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** to confirm that all the cross-mounted folders are mounted properly.

```
df –h
```

Example: Output should be similar to the following example:

```
dncs_host:/disk1/dvs/dvs_doc
217G 726M 214G 1% /disk1/dvs/dvs_doc
dncs_host:/disk1/dvs/appFiles
217G 726M 214G 1% /disk1/dvs/appFiles
dncs_host:/export/home/informix
7.9G 3.0G 4.8G 38% /export/home/informix
```

4 Did the cross-mounted folders mount properly?

- If **yes**, skip to step 7.
- If **no**, continue with step 5.

5 Type the following command and press **Enter**.

```
mountall
```

6 Type the following command and press **Enter** to log out the root user.

```
exit
```

7 As **dncs** user, type the following command and press **Enter**.

```
cd /dvs/appserv/bin
```

8 Type the following command and press **Enter**. The AppControl utility window opens.

```
./appControl
```

9 Select option **2** and press **Enter**.

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

11 Type the following command and press **Enter**.

```
./appStart
```

12 Wait a few minutes, press **Enter** on the AppControl user interface, and verify that all of the processes have started.

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

13 Close the AppControl utility window.

C

Setting Up an Automated Database Backup

Introduction

You can perform an automatic nightly backup of the database by using the cron script, backupDatabase.

Note: A cron script is an automated process that operates at predefined time intervals. You may sometimes hear a cron script referred to as a cron job.

System operators can later check messages that pertain to the execution of the backupDatabase script by examining the /var/log/backupDatabaselog file.

To configure your system to execute the backupDatabase script, add an entry to the crontab file on the DNCS. Use the instructions in this appendix to configure your system to execute the backupDatabase script.

In This Appendix

Configure the DNCS for an Automatic Database Backup

Copying the Backup/Restore Scripts to the DNCS

The system operator should follow these instructions to copy the backup and restore scripts from the CD or DVD to the DNCS.

1. Insert the SR i4.4 DVD into the DVD drive of the DNCS.
2. Type **cp -pr /cdrom/cdrom0/s3/backup_restore /usr/local** and then press **Enter**.

Editing the crontab

Follow these instructions to configure your nightly backup of the Informix database on the DNCS.

1. From an xterm window on the DNCS, log in as **root** user.
2. Type **crontab -l > /tmp/root.crontab** and then press **Enter**. The system redirects the contents of the crontab into root.crontab.

   Important: The 'l' in crontab -l is a lower case L.

   Note: While you can edit the crontab directly, our engineers recommend that you first redirect the contents of the crontab to root.crontab so you can recover the original crontab if necessary.
3. Type **vi /tmp/root.crontab** and then press **Enter**. The system opens root.crontab for editing using the UNIX vi editor.
4. Add the following lines to the end of root.crontab, depending upon your tape drive configuration:

   - If you have a standard tape drive configuration, add the following to the end of the root.crontab file:

     #cron to automatically back up the database

     0 2 * * * (. /dvs/dncs/bin/dncsSetup;

     /usr/local/backup_restore/backupDatabase -n

   - If you have a custom tape drive configuration, add the following to the end of the root.crontab file:

     #cron to automatically back up the database

     0 2 * * * (. /dvs/dncs/bin/dncsSetup;

     /usr/local/backup_restore/backupDatabase -n -b [blocksize] -s [tapesize]

   Note: This command will back up the DNCS database at 2 am everyday. To learn more about the various fields in the command you just entered, type **man crontab** and then press **Enter** at an xterm window on the DNCS.

5 Save the file and exit the vi editor.

6 Type **crontab /tmp/root.crontab** and then press **Enter**. The system automatically backs up your DNCS database everyday.

Important Notes to the System Operator

The system will eject the tape after each backup. Remember to insert a blank tape into the tape drive of the DNCS each day. Store your daily tapes offsite to protect against loss or damage.

D

SR i4.4 Rollback Procedures for the DVD Upgrade

Introduction

The SR i4.4 rollback procedures are intended for field service engineers who encounter problems while upgrading an existing digital system to SR i4.4. Prior to executing the SR i4.4 rollback procedures, contact Cisco Services at +91 9840717688.

In This Appendix

Which Rollback Procedure to Run

Two rollback procedures exist for rolling back from SR i4.4. Identify the rollback procedure you should use based upon your hardware platform and whether you have already enabled disk mirroring.

Sun Fire V880 or V890 DNCS and Sun Fire V240 or V245 Application Server

Two rollback procedures exist for these servers:

- Sun Fire V445, V880, or V890 DNCS
- Sun Fire V240 or V245 Application Server

Read the following choices to help you decide which to use.

- If you have not already run the procedure under ***Enable Disk Mirroring*** (on page 83), then use the procedure under ***Activate the Old System Release*** (on page 105) to roll back from SR i4.4.

  Notes:

  - It should take you about 10 minutes to roll back the Sun Fire V445, V880 or V890 DNCS, as well as the Sun Fire V240 or V245 Application Server using the **Activate the Old System Release** procedure.
  - It should take you about 1 hour to roll back the Sun Blade 150 Application Server using the **Activate the Old System Release** procedure.

- If you have already run the procedure under ***Enable Disk Mirroring*** (on page 83), then use the procedures to restore the DNCS and Application Server file systems and the Informix database in *DBDS Backup and Restore Procedures For SR 2.2 Through 4.3 User Guide* (part number 4013779).

  Notes:

  - It may take as long as 4 hours to roll back the Sun Fire V445, V880 or V890 DNCS.
  - It should take you about 1 hour to roll back the Sun Blade 150 Application Server, or the Sun Fire V240 or V245 Application Server.

Activate the Old System Release

Restoring the Old System Release

Follow this procedure to restore the system software that was in place prior to the unsuccessful upgrade to SR i4.4.

1 Write down the version of the system release you are trying to restore.

_____

2 If necessary, follow the procedures in Appendix A, ***Stopping System Components*** (on page 91), to stop all system components.

3 From a root xterm window, type the following command and then press **Enter**. The system resets the default boot device to the original disk.

```
eeprom  boot-device=disk:a
```

4 Type the following command on the DNCS and then press **Enter**. The system reboots and activates the old software.

```
shutdown -y -g0 -i6
```

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

5 Did the DNCS reboot without error?

- If **yes**, skip to step 9.
- If **no**, continue with step 6.

6 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 the following command and then press **Enter**. The system displays the mounted filesystems.

```
df  -k
```

7 Is the /var filesystem present in the output from step 6?

- If **yes**, go to step 8.
- If **no** (the /var filesystem is not present), go to step 9

8 Follow these instructions if the /var filesystem was present in the output from step 6.

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.

9 Follow these instructions if the /var filesystem was *not* present in the output from step 6.

   a Type the following command and press **Enter**.

   ```
   mount  /var
   ```

   b Type the following command and press **Enter**.

   ```
   dk -k
   ```

   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.

10 Log on to the CDE of the DNCS as **dncs** user.

11 Log on to an xterm window as **root** user.

12 Follow the ***Attach Mirrors*** (on page 84) procedure.

Updating the TED Files

Complete the rollback of the DNCS by following these instructions to update the TED files.

1 If necessary, log on to an xterm window on the DNCS as **root** user.

2 Type the following command and then press **Enter**. The system responds with a **dncsted is alive** message.

   ```
   ping  dncsted
   ```

   Note: If you cannot ping the TED, call Cisco Services for help.

3 Type the following command and then press **Enter**. The /dvs/dncs/TED directory becomes the working directory.

   ```
   cd  /dvs/dncs/TED
   ```

4 Type the following command and then press **Enter**.

   ```
   ./loadTedFiles.sh
   ```

   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) on the screen.

Notes:

- If the operating system on the TED is Linux version 4.0, the system copies files with the 2.0.27 file extension.
- If the operating system on the TED is Linux version 6.0, the system copies files with the 2.2.5-15 file extension. (You may sometimes hear this version of TED referred to as TED FX.)

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.

6 If necessary, go to ***Roll Back the Application Server*** (on page 108).

Roll Back the Application Server

1. If necessary, open an xterm window on the Application 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. Insert the SR i4.4 DVD into the DVD drive of the Application Server.
4. Type the following command ad press Enter. The system resets the default boot device to the original disk.

   ```
   eeprom  boot-device=disk:a
   ```

5. Type the following command on the DNCS and then press **Enter**. The system reboots and activates the old software.

   ```
   shutdown -y -g0 -i6
   ```

   Important: Do not use the *reboot* or *halt* command to reboot the server.
6. Did the DNCS reboot without error?
   - If **yes**, skip to step 10.
   - If **no**, continue with 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 the following command and then press **Enter**. The system displays the mounted filesystems.

      ```
      df  -k
      ```
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 the following command and press **Enter**.

```
mount  /var
```

b Type the following command and press **Enter**.

```
dk -k
```

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 DNCS as **dncs** user.

12 Log on to an xterm window as **root** user.

13 Follow the ***Attach Mirrors*** (on page 84) procedure.

E

New Installation of SR i4.4 Software

Introduction

Use the procedures in this appendix for an initial installation (rather than an upgrade) of SR i4.4 software.

In This Appendix

Configure the New DNCS

Complete the following steps to configure the new DNCS.

Important: Note these important points:

- If you are configuring a new Sun Fire V445 DNCS, be sure that the disks are inserted into slots 0, 1, 4, and 5.
- Be sure that the new DNCS is not yet connected to the network and that the power is turned off.

1. Turn on power to the new DNCS.
2. While the new DNCS is booting, press the **Stop** and **A** keys simultaneously. The **ok** prompt appears.
3. At the **ok** prompt, insert the CD containing the new version of software into the DVD drive of the new DNCS.
4. Type the following command and press **Enter**. The new DNCS boots from the DVD into the OpenWindows environment.

   ```
   boot  cdrom - install
   ```

   Result: In the OpenWindows environment, a terminal window opens and prompts you to identify the type of terminal you are using.
5. Type the number that corresponds to **DEC VT100** and then press **Enter**. The window updates to display a brief message about the installation process.
6. Read through the message displayed in step 5 and then press the **F2** key. The window prompts you to select the installation type.

   ```
   Starting remote procedure call (RPC) services: done.
   System identification complete.
   Starting Solaris installation program...
   Searching for JumpStart directory...
   Using rules.ok from Cisco SRDVD.
   Checking rules.ok file...
   Using begin script: sparc/begin.sh
   Using profile: sparc/profiles/profile
   Using finish script: sparc/finish.sh
   Executing JumpStart preinstall phase...
   Executing begin script "sparc/begin.sh"...
   <*> Executing begin.sh script for JumpStart via CD installation
   Please Choose Installation Type.
   1.              DNCS Server
   Choice:
   ```

7 Select option **1** and press **Enter**. The window prompts you to specify the network configuration of the server.

```
Network Configuration:

1. Local interface for "dncs".
        IP = 192.168.1.1
        Netmask = 255.255.255.0
2. Local interface for "dncsatm".
        IP = 10.253.0.1
        Netmask = 255.255.192.0
3. Remote IP address for "appservatm appserv_host ppv_manager_host vc_server_hos
t config_manager_host" = 10.253.0.10
4. Remote IP address for "dncsted" = 192.168.1.2
5. Hostname = dncs
6. Default Gateway = 10.253.0.254

Enter the line number to change or 'c' to continue: _
```

Note: If you need to change any configuration parameters, type the line number and provide the corresponding value.

8 Select **c** (to continue) and press **Enter**.

Results:

- The new DNCS install and boots from the DVD.
- The operating system and packages install.

Important:

- The reboot process will take about an hour to complete and the system will reboot several times.
- Do not log on to the system until the CDE Login window appears. Several non-CDE log-on opportunities will appear. Ignore these.

9 When the CDE Login window appears, log onto the system as **root** user.

10 Log on to the new DNCS as **root** user.

11 Open an xterm window on the new DNCS.

12 Type the following command and then press **Enter**. A confirmation message appears.

```
/cdrom/cdrom0/sai/scripts/Media/attach_mirrors
```

13 Type **y** and then press **Enter**. The system configures the disk-mirroring function on the new DNCS.

Notes:

- It could take an hour to configure the disk-mirroring function.
- The **#** prompt appears when the disk-mirroring function is configured.

14 From an xterm window on the new DNCS, type the following command and press **Enter** to eject the DVD.

```
eject cdrom
```

Convert the DNCS Database

In this procedure, you will convert the DNCS database to SR i4.4 standards.

Note: The system components should be stopped.

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

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

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

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

3 Type the following command and then press Enter. The system stops the cron jobs on the DNCS.

```
svcadm -v disable -st cron
```

4 Type the following command and press **Enter**. The system establishes the root user environment.

```
. /dvs/dncs/bin/dncsSetup
```

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

Important: At some sites, a message similar to the following may appear: **Failed to get SITE_ID __ database up? No LOCAL_SITE_ID available for site hostname=<hostname>.**

You can ignore this message.

5 Type the following command and then press **Enter**. The system converts the DNCS database.

```
bldDncsDb
```

Note: Depending upon the size of the database, this script may take over 30 minutes to complete.

Examine and Re-Order the pddataqampat Table

Complete the ***Examine and Re-Order the pddataqampat Table*** (on page 65) procedure. Keep these points in mind as you complete the procedure:

- Delete the 199 entry.
- Create a new entry with a Session ID of 199, a Program Number of 139, and a PMT value of 288.

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

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

August 2011 Printed in USA

Part Number 4038829 Rev A