DVD Upgrade Installation Instructions

for System Release i4.2.2

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**.

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

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Publication Disclaimer

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

Copyright

Contents

About This Guide

Purpose

This guide provides step-by-step instructions for upgrading a Digital Broadband Delivery System (DBDS) to System Release (SR) i4.2.2.

SR i4.2.2 Features Live Upgrade

The upgrade to SR i4.2.2 features the Solaris Live Upgrade. Through use of the Live Upgrade, engineers can upgrade the system to SR i4.2.2 without having to shut down the system processes until activation of the new system software.

Upgrade Path

Sites that upgrade to SR i4.2.2 must currently support SR i4.2.1 or SR i4.2.

How Long to Complete the Upgrade?

The upgrade to SR i4.2.2 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 stop system components in 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 i4.2.2.

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 1-866-787-3866 for assistance.

Important: Complete all of the procedures in this guide in the order in which they are presented. Failure to follow all of the instructions may lead to undesirable

results.

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 vi.
  - The ability to review and edit cron files
- Extensive DBDS system expertise
  - The ability to identify keyfiles that are unique to the site being upgraded
  - The ability to add and remove user accounts

Requirements

Before beginning the upgrade to SR i4.2.2, be sure that the site you are upgrading meets these requirements:

- You have the DVD labeled SR i4.2.2 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 i4.2.2 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 i4.2.2 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 Blade 150	■ 1 X 40 GB ■ 1 X 80 GB	512 MB minimum
Sun Fire V245	2 X 73 GB	256 MB minimum
Sun Ultra 5	1 X 20 GB	256 MB minimum

Document Version

This is the first formal release of this document.

1

SR i4.2.2 DVD Pre-Upgrade Procedures

Introduction

This chapter contains procedures that you will follow to prepare the system you are upgrading for the SR i4.2.2 upgrade.

Important Points About the Upgrade

Note these important points about the upgrade to SR i4.2.2:

- Systems that upgrade to SR i4.2.2 using the DVD method must currently support one of the following system releases:
  - SR i4.2.1
  - SR i4.2
- 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 i4.2.2 upgrade requirements. Refer to *DBDS Utilities Version 6.3 Installation Instructions and User Guide* (part number 4031374) for instructions on installing and executing the DNCS Utilities.

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.

Important Note About Third-Party Applications

Note these important points about third-party applications:

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

Plan What Optional Features Will be Supported

Optional Features

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

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

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

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

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. Are you backing up a Sun Fire V880 or V890 server?
   - If **yes**, check the dncs and root user e-mail accounts on the servers for the presence of metadevice errors.

     Note: Correct any metadevice errors before proceeding with the backup. Call Cisco Services if you need help in correcting metadevice errors.
   - If **no**, go to step 2.
2. If necessary, open an xterm window on the DNCS or Application Server, whichever server you are backing up.
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. Insert the SR i4.2.2 DVD into the DVD drive of the DNCS or the Application Server, whichever server you are backing up.
5. 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.
6. 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. Allot 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: **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -v** and then press **Enter**.
- To back up the file system on a DNCS or Application Server that does not have a local tape drive, type: **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -v -r [hostname or IP address]:[tape device]** and then press **Enter**.

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.

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.

Follow these instructions to help you run the Doctor Report.

1 From an xterm window on the DNCS, type **pkginfo -l SAIdbdsutils** and then press **Enter**.

2 Did the system reveal that this package is installed?

- If **yes**, go to **Run /dvs/dncs/Utilities/doctor**.
- If **no**, go to **Run /export/home/dncs/doctor**.

Run /dvs/dncs/Utilities/doctor

1 Type **cd /dvs/dncs/Utilities/doctor** and then press **Enter**.

2 Type **doctor -av** and then press **Enter**.

Run /export/home/dncs/doctor

1 Type **cd /export/home/dncs/doctor** and then press **Enter**.

2 Type **doctor -av** and then press **Enter**.

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.

Also analyze the output of the Doctor report to verify that the inband SI_INSERT_RATE is not greater than 0 (zero). If the inband SI_INSERT_RATE is greater than 0 (zero), refer to *Recommendation for Setting System Information to Out-of-Band* (part number 738143), and follow the procedures provided to disable inband SI.

Note: If the inband SI is disabled, then the SI_INSERT_RATE is 0.

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 prior to the SR i4.2.2 upgrade. All the disk mirroring functions must be working normally before proceeding with the upgrade.

CAUTION:

If the disk mirroring functions of the DNCS 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. This procedure should take only a few minutes to complete.

1. If necessary, open two xterm windows on the DNCS.
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.

   Example: You should see output similar to the following example, that assumes you have 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
```

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
```

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 **eeprom boot-device** and then press **Enter**.

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 **eeprom boot-device=disk:a** and then press **Enter** to reset the boot device to the original disk.

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 **clearDbSessions** and then press **Enter**. The system removes all completed session, resource, and network graph records more than 1 hour old from the database.
2. Type **clearDbSessions -c** and then press **Enter**. The system removes all completed session, resource, and network graph records from the database.
3. Type **clearDbSessions -o** and then press **Enter**. The system removes orphaned records from the database.

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 off 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.

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

Back Up Various Data Files

Our engineers recommend that you back up to tape the data in the signonCount.out and signonCount.fixrpt files, as well as the data in the dhctStatus2 directory. You can then use this data as a reference and troubleshooting tool in the event that there are problems with the system after the upgrade. The instructions in this section guide you through the steps of backing up these files.

Backing Up Various Data Directories

Follow these instructions to back up the signonCount.out and signonCount.fixrpt files, as well as the data in the dhctStatus2 directory.

1. Label a tape with the date and the following title:
   signonCount / dhctStatus2 Backups
2. Insert the tape into the tape drive of the DNCS.
3. From an xterm window on the DNCS, type
   tar cvf [device name] /dvs/dncs/tmp/signonCount.out /dvs/dncs/tmp/signonCount.fixrpt /dvs/dncs/tmp/dhctStatus2 and then press **Enter**. The system backs up the specified files.

   Note: Substitute the device name of the DNCS tape drive for [device name].

   Example: tar cvf /dev/rmt/0h /dvs/dncs/tmp/signonCount.out /dvs/dncs/tmp/signonCount.fixrpt /dvs/dncs/tmp/dhctStatus2
4. When the backup is complete, eject the tape and store it in a safe place.

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:
   - The Asynchronous Transfer Mode (ATM) switch (if one exists)
   - 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. Complete these steps to perform a slow and fast boot on a test DHCT and Combo-Box (if available) with a working return path (2-way mode):
   a. Boot a DHCT.

      Note: Do not press the power button.
   b. Access the Power On Self Test and Boot Status Diagnostic Screen on the DHCT and verify that all parameters, except UNcfg, display **Ready**.

      Note: UNcfg displays Broadcast.
   c. Wait 5 minutes.
   d. Press the power button on the DHCT. The power to the DHCT is turned on.
   e. Access the Power On Self Test and Boot Status Diagnostic Screen on the DHCT and verify that all parameters, including UNcfg, display **Ready**.
7. Verify that you can ping the DHCT.
8. Verify that the Electronic Program Guide (EPG) displays 7 days of accurate and valid data.

9 For all sites, verify that you can define, purchase, and view an IPPV and VOD event.

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.

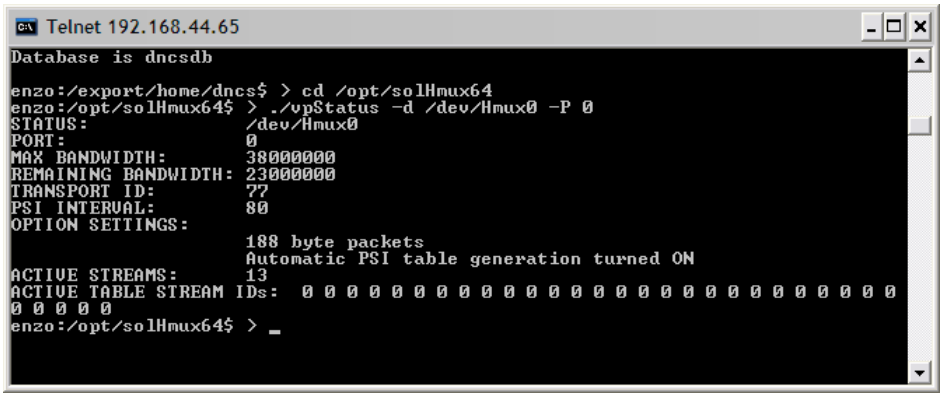
1 Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.

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 **/opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0** and then press **Enter**.

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



- If **no**, go to *Obtain System Configuration* (on page 22).

4 Do the number of **Active Streams** match the number of sessions built on the BFS QAM?

- If **yes**, go to *Obtain System Configuration* (on page 22).
- If **no**, call Cisco Services and inform them about the discrepancy.

Obtain 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
   ```

6 From an xterm window on the Application Server, type the following command and press **Enter**. A list of IP addresses and hostnames appears.

```
more  /etc/hosts
```

7 Write down the IP addresses and hostnames for the following hosts:

- dncsatm _____
- appservatm (if appservatm is not 10.253.0.10) _____

8 At the Application Server, type the following command and press **Enter**. The hostname for the Application Server appears.

```
uname  -n
```

9 Write down the hostname for the Application Server, as displayed in step 8:

_____

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.

Check the Time to Live Parameter

The number of "hops" refers to the number of routers a single packet of data traverses on its way to its destination. In the case of router failure or network misconfiguration, a packet of data can theoretically exist in an endless loop, never reaching its destination and never being discarded by the system.

To prevent data from existing in an endless loop, IP packets of data contain a Time to Live (TTL) parameter that decrements by 1 each time that packet of data navigates a router. This protocol is designed to discard the packet whenever the TTL parameter reaches 0.

We use a default TTL parameter of 10 for IP multicast packets that are generated by the DNCS; there are no known DBDS systems that are configured to require more than 10 hops for a packet of data to reach its destination.

In this procedure, you will "probe" each Cable Modem Termination System (CMTS) on the network and analyze the number of hops required for a packet of data to reach the CMTS. To do this, you will query the database to obtain the IP address of each CMTS. Then, you will run the **traceroute** command against every CMTS and count the number of hops. If the traceroute command reveals that data requires 8 or more hops to reach any CMTS, you will then modify the TTL parameter in the /export/home/dncs/.profile file on the DNCS.

Obtaining the CMTS IP Addresses

Follow these instructions to query the database regarding the IP address of each CMTS.

Note: To be certain that the IP address of each CMTS has been properly entered into the database, you may want to cross-reference any IP addresses returned from the database against the documentation that accompanied the CMTS.

1. From an xterm window on the DNCS, type **dbaccess dncsdb -** and then press **Enter**. The system opens the DNCS database.
2. Type **select * from cmts;** and then press **Enter**. The system displays the rows in the cmts table.

```
id name    ipaddr ipaddr2
2 vod4CiscoCMTS          192.168.201.201

1 row(s) retrieved.
```

Note: This system shows only one CMTS; your system may show more.

3 Does the output from step 2 reveal that there are CMTSs on the system?
   - If **yes**, continue with step 4.
   - If **no**, go to the next procedure in this chapter.
4 Write the IP address of each CMTS on a sheet of paper so that you can refer to it later.
5 Type the **Ctrl** and **c** keys simultaneously to close the database.
6 Go to ***Determining the Number of Hops*** (on page 28).

Determining the Number of Hops

In this procedure, you will run the UNIX **traceroute** command against each CMTS IP address that you found in a previous procedure, **Obtaining the CMTS IP Addresses**. The results of the traceroute command will indicate the number of hops required for data to reach each CMTS.

Note: If the traceroute command times out, the most likely cause is that you have supplied an inaccurate IP address to the traceroute command.

1 Type **traceroute < IP Address >** and then press **Enter**.

   Note: Substitute the IP address of a CMTS for < IP Address >.

   Example: traceroute 192.168.201.201

   Result: The system shows the number of hops; this example shows that two hops are required.

   $ traceroute 192.168.201.201

   traceroute: Warning: Multiple interfaces found; using 10.252.0.1 @ ce0

   traceroute to 192.168.201.201 (192.168.201.201), 30 hops max, 40 byte packets

   1 router (10.252.0.254) 0.541 ms 0.343 ms 0.290 ms

   2 cmts (192.168.201.201) 0.773 ms * 0.738 ms
2 On the sheet of paper that you used in step 4 of the previous procedure, write the number of hops required for data to reach each CMTS.
3 Repeat steps 1 and 2 for each CMTS that you recorded in the previous procedure, Obtaining the CMTS IP Addresses.
4 Do any of the CMTSs require 8 or more hops?
   - If **yes**, go to ***Editing the .profile File*** (on page 25).
   - If **no**, go to the next procedure in this chapter; you do not have to modify the .profile file.

Editing the .profile File

You need to edit the .profile file only if the traceroute command (previous procedure, **Determining the Number of Hops**) reveals that a packet of data requires 8 or more hops to reach a CMTS.

Follow these instructions to edit the .profile file.

1. In the space provided, write down the greatest number of hops revealed by the traceroute command in the previous procedure. _____
2. Add 3 to your number from step 1 and write the result in the space provided.

   _____

   Example: If your number in step 1 is 8, adding 3 to 8 yields 11.
3. Use a text editor to open the /export/home/dncs/.profile file.
4. Append the following lines to the .profile file:

   #Time To Live seconds/hops (default=10)
   export COMM_MULTICAST_TTL=<Number from step 2>

   #BFS Time To Live seconds/hops (default=10)
   export BFS_MULTICAST_TTL=<Number from step 2>

   #HCTM Time To Live seconds/hops (default=10)
   export HCTM_MULTICAST_TTL=<Number from step 2>

   Note: Substitute the number you recorded in step 2 for < Number from step 2 >.
5. Save the .profile file and close the text editor.

   Note: Your changes will take effect after you stop and restart the DNCS, later during this upgrade procedure.

Stop the dhctStatus, signonCount and cmd2000 Processes

When sites are being upgraded, the dhctStatus utility may occasionally be in the process of polling DHCTs. Additionally, the signonCount utility may be active in system memory. Our engineers have discovered that upgrades proceed more smoothly when the dhctStatus utility is not actively polling DHCTs and when the signonCount utility is not active in system memory. The instructions in this section guide you through the steps to terminate polling associated with the dhctStatus utility and to remove the signonCount utility from system memory.

Terminating the dhctStatus Polling Operation

Follow these instructions to determine whether the dhctStatus utility is actively polling DHCTs, and then to terminate the polling operation, if necessary.

1. From a root xterm window, type **ps -ef | grep dhctStatus** and then press **Enter**. The system reveals whether there are any instances of the dhctStatus process running.
2. Did your results from step 1 show that the dhctStatus process was running?
   - If **yes**, go to step 3 to shut down the polling operations.
   - If **no**, skip the rest of this procedure and go to ***Removing the signonCount Utility from System Memory*** (on page 27).
3. Type **dhctStatus** and press **Enter** to display the dhctStatus menu.
4. To terminate the polling operation, follow these instructions.
   a. Type **p** and then press **Enter**. The system displays a polling menu.
   b. Type **t** and then press **Enter**. The system terminates the polling operation.
   c. Press **Enter** to return to the main menu.
   d. Type **q** and then press **Enter** to exit the menu.
5. Type **ps -ef | grep dhctStatus** and then press **Enter** to determine whether all of the processes have been terminated.
6. Type **kill -9 [process ID]** and then press **Enter** for any process ID displayed in the results from step 5.

   Note: The process ID(s) to kill is/are located starting with the second column of the output from step 5.
7. Repeat steps 5 and 6 for any process that continues to remain active.

Removing the signonCount Utility from System Memory

1. Type **ps -ef | grep signonCount** and then press **Enter**. A list of DNCS processes and process IDs display on the screen.
2. Do the results from step 1 show that the signonCount utility is running?
   - If **yes**, continue with step 3.
   - If **no**, you can skip the rest of this procedure.
3. From a dncs xterm window, type **signonCount uninstall** and press **Enter**.

   Note: The utility is not permanently uninstalled; it is placed back into system memory the next time you run the signonCount utility.
4. Type **ps -ef | grep signonCount** and then press **Enter**. A list of DNCS processes and process IDs display on the screen.
5. Type **kill -9 [processid]** and then press **Enter** for each process ID displayed in step 4.

   Note: The process ID(s) to kill is/are located starting with the second column of the output from step 4.
6. Type **ps -ef | grep signonCount** and then press **Enter** to ensure all the processes are terminated.
7. Repeat steps 5 and 6 for any process that continues to display active. The system should only display the grep process.

Terminating the cmd2000 Processes

1. Type **ps -ef | grep cmd2000** and then press **Enter**. The system displays a list of cmd2000 processes and process IDs.
2. Are any cmd2000 processes running?
   - If **yes**, type **kill -9 < process ID >** and then press **Enter** for each running cmd2000 process; then, go to step 3.
   - If **no**, go to step 4.
3. Type **ps -ef | grep cmd2000** and then press **Enter** to verify that all cmd2000 processes have been terminated.

   Note: Repeat steps 2 and 3 for any cmd2000 processes that remain active.

2

SR i4.2.2 DVD Upgrade Procedures

Introduction

Use the procedures in this chapter to upgrade a site to SR i4.2.2.

In This Chapter

Upgrade the SR i4.2.2 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 i4.2.2 Software

Complete the following steps to upgrade the i4.2.2 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 i4.2.2 DVD into the DVD drive of the DNCS.
4. Wait one minute and then type **df -n** and press **Enter**. A list of the mounted filesystems appears.
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. Type **/etc/init.d/volmgt stop** and then press **Enter**. The volume manager utility stops.
7. After completing step 6, did the DVD user interface appear?
   - If **yes**, go to step 9
   - If **no**, type **/etc/init.d/volmgt start** and then press **Enter**. The volume manager utility starts.
8. Repeat steps 4 through 7. Call Cisco Services if the system still does not recognize the DVD.
9. Type **metastat | more** and then press **Enter**. The system displays the status of all of the metadevices on the DNCS.

   Note: Press the **Spacebar**, if necessary, to page through all of the output.
10. Are the following two conditions true?
    - The designation **ok** appears in the **State** column next to each metadevice.
    - No **Hot Spare** indicates **In Use**.
    - If **yes** (to both conditions), go to step 11.

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

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

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

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

Live Upgrade of jeckle started at: Friday, August 22, 2008 12:33:04 PM EDT
Checking the system, please wait...

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

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

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

15 Type **y** and then press **Enter**. A message similar to the following appears:

Running systemcheck.pl to determine system type
System type: V445_8x146
INFO: d700 1 1 c1t4d0s0 is an active submirror
INFO: d701 1 1 c1t4d0s1 is an active submirror
INFO: d703 1 1 c1t4d0s3 is an active submirror
INFO: d707 1 1 c1t4d0s7 is an active submirror
INFO: d710 1 1 c1t4d0s5 is an active submirror
INFO: d720 1 3 c1t5d0s0 c1t6d0s0 c1t7d0s0 -i 32b is an active submirror

All mirrors must be detached before proceeding.

Do you want to detach all 7xx mirrors now? [y,n,?]

16 Type **y** and then press **Enter** to detach the mirrors. The system displays a **Do you want to back up the key files?** message.

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

Results:

- The system lists the key files and directories that will be backed up and then later restored.
- The system displays a **Do you want to add to the above list?** message.

18 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 16).
  - **c** When you are finished adding key files, type **n** and then press **Enter**.

    Result: 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**.

19 During the Live Upgrade, the following message appears:

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

- open another terminal window

- check for the presence of /tmp/install_log file

- do tail -f /tmp/install_log

- type Control + C to exit the tail

----

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

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

Important: Ignore this command for now.

21 Type the tail command (**tail -f /tmp/install_log**) to inspect the log file.

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

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

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

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

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 **./appStop** and then press **Enter**.

f 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.

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

h Close the AppControl utility user interface.

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

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

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

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 **dncsStop** and then press **Enter**.

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

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 24.

– If **no** (there are other processes still running), follow these instructions.

a Type **dncsKill** and then press **Enter**.
b Type **appKill** and then press **Enter**.

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

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 24.
- 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.

24 Close the dncsControl utility user interface.

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

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

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

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

- If **yes**, go to step 28.
- If **no**, follow these instructions.

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

28 As root user again, type **/var/tmp/doLiveDbUpgrade** and then press **Enter**. A **Do you want to continue?** message appears.

29 Type **y** and then press **Enter**. A message similar to the following appears:

You're now ready to:

*** Check the status of the Live Upgrade (LU) using:**

 # lustatus

*** Activate the ABE by doing:**

 # luactivate XXX

*** Reboot the machine using:**

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

Important: Do NOT execute any of these commands yet.

30 Type **lustatus** and then press **Enter**. Output similar to the following should appear:

Boot Environment Name	Is Complete	Active Now	Active On Reboot	Can Delete	Copy Status
SAIdncs XXX	yes	yes	yes	no	-
XXX	yes	no	no	yes	-

31 Type **luactivate DNCSXXX** and then press **Enter**. Output similar to the following should appear:

****

In case of a failure while booting to the target BE, the following process needs to be followed to fallback to the currently working boot environment:

1. Enter the PROM monitor (ok prompt).

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

setenv boot-device

/pci@1f,700000/pci@0/pci@2/pci@0/pci@8/LSILogic,sas@1/disk@0,0:a

3. Boot to the original boot environment by typing:

boot

****

Activation of boot environment <XXX> successful.

32 Type **lustatus** and then press **Enter**. Output similar to the following should appear:

Boot Environment Name	Is Complete	Active Now	Active On Reboot	Can Delete	Copy Status
SAIdncs_XXX	yes	yes	no	no	-
XXX	yes	no	yes	no	-

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

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

34 Type **/usr/sbin/shutdown -g0 -i6 -y** and then press **Enter** to reboot the system.

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.

35 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 **svcadm -v disable -st cron** and then press **Enter**. The system stops the cron jobs on the server.
4. Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.

   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 **bldDncsDb** and then press **Enter**. The system converts the DNCS database.

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

Run the APP_postinstall Script

The APP_postinstall script configures the Application Server portion of the DNCS server and builds the appdb database.

Note: You should already be logged on to an xterm window as root user and you should already have run the dncsSetup script.

1. From the xterm window on the DNCS, type **cd /dvs/appserv/bin** and then press **Enter**. The /dvs/appserv/bin directory becomes the working directory.
2. Type **./APP_postinstall** and then press **Enter**. The system runs the APP_postinstall script.

   Important: Be sure to type the period before typing /APP_postinstall.

   Note: Call Cisco Services if execution of the script results in an error.

Start the DNCS Processes and Check Log Files

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

Starting the DNCS Processes

Complete the following steps to start the DNCS processes.

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

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

Checking the DNCS Log Files

In this procedure, you will inspect the DNCS log files for errors.

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

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

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
  - sprite_LiveUpgrade.log
  - sprite_S74restoreKeyFiles.log
  - sprite_S74sethosts.log
  - sprite_update_TED.log
  - sprite_S75create_ssh_host_keys.log
  - sprite_setup_sds.log
  - sprite_S90SetOnconfig.log
  - sprite_S90setInformixPerms.log
  - sprite_S98add_headend_pkgs.log
  - sprite_APP_postinstall.log

Attach Mirrors

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

Attaching Mirrors

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

1. Log on to the DNCS server as **root** user.
2. Type **cd /cdrom/cdrom0/s3/sai/scripts** and then press **Enter**. The /cdrom/cdrom0/s3/sai/scripts directory becomes the working directory.
3. Type **./attach_mirrors** and then press **Enter**. A confirmation message appears.
4. Type **y** (for yes) and then press **Enter**. The system runs a script that enables the disk-mirroring function of the DNCS server.
5. When the mirrors have been enabled, type **exit** and then press **Enter**. The root user logs out of the server.

3

SR i4.2.2 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

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.
   - 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. If necessary, insert the SR i4.2.2 DVD into the DVD drive of the DNCS.
2. From an xterm window on the DNCS, type one of the following commands:
   - If your DNCS has an *internal* DVD drive, type **/cdrom/cdrom0/s3/sai/scripts/utils/listpkgs -i** and then press **Enter**.
   - If your DNCS has an *external* DVD drive, type **/cdrom/cdrom1/s3/sai/scripts/utils/listpkgs -i** and then press **Enter**.

   Note: It may take a few minutes for this command to run.

   Result: The system displays a listing of installed packages.
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	i4.2.2.3p3	
DNCS/App Tools	SAItools	4.2.1.12	
DNCS GUI	SAIgui	i4.2.2.3	
DNCS WUI	SAIwebui	i4.2.2.3p3	
Solaris Patches	SAIpatch	4.3.0.1	
DNCS Online Help	SAIhelp	i4.2.1.1	
DNCS Report Writer	SAIrptwrt	4.3.0.9	
MQAM	SAImqam	V3.2.0	
ORCA	SAIorca	4.2.0.0	
PCG	SAIpcg	V1.0.17	
DBDS Utils	SAIdbsutils	6.2.0.5	

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?

   Important: The build number (the fourth digit of the version number) may differ.
   - If **yes**, go to step 5.
   - If **no**, call Cisco Services and inform them of the discrepancy.
5. Type **eject cdrom** and then press **Enter**.

Edit the .profile File

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

Editing Debug and Logging Settings in the .profile File

After the upgrade to SR i4.2.2, 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 **cd /export/home/dncs** and then press **Enter**.
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**, continue with the next procedure in this section.
5. Save the changes to the .profile file and then close the text editor.

   Note: Keep the .profile file open for additional changes.

Adding a DRM Variable to the .profile File

In order for VOD to work correctly on systems that are not SSP2.3-compliant, you need to add the DNCS_DRM_INCLUDE_HE_RSR_VOD variable to the .profile file. This procedure describes how to add the variable.

1. Is the site you are upgrading SSP2.3-compliant?

   Note: Contact Cisco Services if you are not sure.
   - If **yes**, you do not have to complete this procedure. Go to ***Editing the .profile File for the atm_addr Environmental Variable*** (on page 52).
   - If **no**, continue with step 2.

2 Append the following two lines to the .profile file:

 # VOD variable for systems that are not SSP2.3-compliant

DNCS_DRM_INCLUDE_HE_RSR_VOD=1

export DNCS_DRM_INCLUDE_HE_RSR_VOD

Note: Put the uncommented line that contains the actual variable on one line.

3 Save the .profile file.

Editing the .profile File for the atm_addr Environmental Variable

After the upgrade, the .profile file must no longer contain a reference to the atm_addr environment variable. If the reference is there, you must either transform that line into a comment or delete the line.

1 Examine the .profile file and look for an entry that contains atm_addr.

Example: export atm_addr=dncseth

2 Does the .profile file contain an entry as described in step 1?

Important: If the entry is "commented out," you should answer no.

- If **yes**, insert the "**#**" character at the beginning of the line that contains atm_addr. The line becomes a comment.
- If **no**, go to step 3.

3 Save and close the .profile file.

Activating the Changes to the .profile File

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

1 Click **Exit.**

2 When the confirmation message appears, Click **OK.**

3 When The CDE log-in window appears, log on to the system as **dncs** user.

Enable rdate on the DNCS

In this procedure, you will enable rdate on your system. By enabling rdate, remote hosts can set their local time from the DNCS.

From a root xterm window, type the following command and then press **Enter**. The system enables the time daemon on the DNCS.

```
inetadm  -e  svc:/network/time:stream
```

Run the configureASI.pl Script

Complete this procedure only if the system you are upgrading already has the ASI card installed. This procedure ensures that the ASI card is configured correctly.

1 As root user, type **/dvs/dncs/bin/configureASI.pl** and then press **Enter**.

Result: The script checks for the presence of the ASI card and detects any problems with how the card is configured. The script displays a message that indicates the card is correctly configured, or it seeks confirmation regarding correcting any problems the script finds.

2 Did the script reveal any problems with how the ASI card is configured?

- If **yes**, go to step 3.
- If **no**, follow these instructions.
  - **a** Type **shutdown -y -g0 -i6** and then press **Enter**. The system reboots.
  - **b** After the system reboots, go to ***Check the Status of the ASI Card*** (on page 58).

3 Type **y** (if you want the script to correct configuration problems with the ASI card) and then press **Enter**. The script modifies the configuration of the ASI card and prompts you to reboot the DNCS.

4 Type **shutdown -y -g0 -i6** and then press **Enter**. The system reboots.

5 Go to ***Configure/Verify the ASI Card*** (on page 57).

Install the ASI Card

In this procedure, you will install the ASI card into the DNCS. The DNCS should be completely turned off.

1. Turn off power to the DNCS.
2. Remove the cover to the DNCS and install the ASI card into one of the following slots:
   - Slot 7 if you have a Sun Fire V880, or V890 DNCS
   - Slot PCI 5 if you have a Sun Fire V445 DNCS

   Note: If the site you are upgrading also supports the Common Download feature, you can install the Common Download card at this time. Install the Common Download card into one of the following slots:
   - Slot 2 if you have a Sun Fire V880 or V890 DNCS
   - Slot PCI 3 if you have a Sun Fire V445 DNCS
3. Put the cover back on the DNCS.

Boot the DNCS

In this procedure, you will restore power to the DNCS, boot the DNCS, and log in as dncs user.

1 Turn on power to the DNCS.

2 When the message **Boot device: <full path of boot device>** disk file and args appears on the screen of the DNCS, press the **Stop** and **a** keys simultaneously. An **ok** prompt appears.

3 Type **boot -r** and then press **Enter**.

Results:

- A series of messages scroll across the screen as the DNCS boots.
- The CDE window opens.

4 Log into the CDE of the DNCS as **dncs** user.

5 Ensure that the DNCS application is still stopped.

Notes:

- In rare cases, the DNCS application may have restarted.
- If the DNCS application restarted, follow the ***Stopping the DNCS*** (on page 112) procedure.

Configure/Verify the ASI Card

In this procedure, you will ensure that the ASI card is configured correctly.

1 Type **/dvs/dncs/bin/configureASI.pl** and then press **Enter**.

Result: The script checks for the presence of the ASI card and detects any problems with how the card is configured. The script displays a message that says the card is configured correctly, or seeks confirmation to correct any problems that are found.

2 Did the script uncover any problems with how the ASI card is configured?

- If **yes**, go to step 3.
- If **no**, go to step 8.

3 Type **y** (if you want the script to correct the problem) and then press **Enter**. The system modifies the configuration of the Direct ASI card and prompts you to reboot the computer.

4 Type **/usr/sbin/shutdown -g0 -i6 -y** and then press **Enter** to reboot the DNCS.

5 Log in to the DNCS as **dncs** user.

6 Log on to an xterm window on the DNCS as **root** user.

7 Repeat steps 1 through 6.

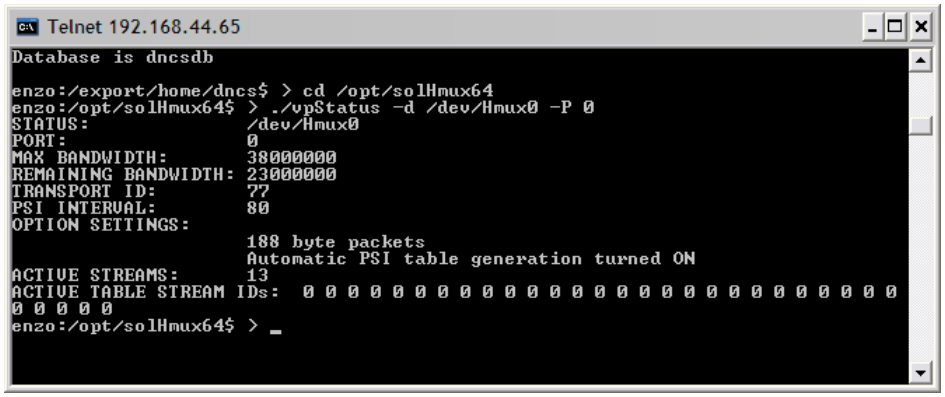
8 Is the ASI card configured correctly?

- If **yes**, follow these instructions.
  - **a** Type **/usr/sbin/shutdown -g0 -i6 -y** and then press **Enter** to reboot the DNCS.
  - **b** Log on to the DNCS as **dncs** user.
- If **no**, call Cisco Services.

Check the Status of the ASI Card

1 As dncs user on the DNCS, type **/opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0** and press **Enter**. After a few minutes, the system displays the status of the ASI card.

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 **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**.

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

4 Type **/opt/solHmux64 -d /dev/Hmux0 -P 0** and then press **Enter**.

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.

Stop the cron Jobs on the DNCS

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.
   - 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.

Upgrade the Application Server Software

Use the instructions in this section to upgrade the Application Server by completing the procedures in one of the following sections:

- ***Upgrading the Sun Blade 150 or Sun Ultra 5 Application Server*** (on page 60)
- ***Completing the Sun Fire V240 or V245 Application Server Upgrade*** (on page 57)

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

Upgrading the Sun Blade 150 or Sun Ultra 5 Application Server

If you have followed the procedures of these upgrade instructions in order, all system components have been shut down and the Application Server is displaying the CDE window.

Complete the following procedure to install the Solaris OS and Application Server software on to the Sun Blade 150 or Ultra 5 server.

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

1. At the **ok** prompt on the Application Server, type **boot -r** and press **Enter**. 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 i4.2.2 DVD into the DVD drive of the Application Server.

   Note: If the File Manager window opens, you can close it.
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 Type one of the following commands:

- If the Application Server has an *internal* DVD drive, type **/cdrom/cdrom0/s3/sai/scripts/doAppUpgrade** and then press **Enter**.
- If the Application Server has an *external* DVD drive, type **/cdrom/cdrom1/s3/sai/scripts/doAppUpgrade** and then press **Enter**.

Results:

- The system displays a doAppUpgrade message.
- The script performs a system check.

  Note: It should take only 5 minutes to complete the system check.

  Important: If the script that checks system configuration takes longer than 5 minutes to execute, something may have gone wrong. Call Cisco Services for assistance in troubleshooting the system check.
- A **Do you want to continue message?** appears.

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

Results:

- The system lists the key files and directories that will be backed up and then later restored.
- The system displays a **Do you wish to add to the above list** message.

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

- If you want to add to the list of key files and directories to be backed up, follow these instructions.

  a Type **y** and then press **Enter**.
  b Follow the on-screen instructions to add to the list of files or directories.
- If you do not want to add to the list of key files and directories to be backed up, type **n** and then press **Enter**.

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

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

9 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.

10 Did the doAppUpgrade script execute without error?

- If **yes**, call Cisco Services.
- If **no**, go to step 11.

11 Are you upgrading a Sun Blade 150?

- If **yes**, go to step 18.
- If **no**, go to 12.

12 Type **shutdown -y -g0 -i0** and press **Enter**.

13 At the OK prompt, type **printenv auto-boot?** and then press **Enter**.

14 Is *auto-boot* set to true?

- If **yes**, type **setenv auto-boot? false**, press **Enter**, and go to step 15.
- If **no**, go step 16.

15 Type **reset-all** and press **Enter**.

16 Type **probe-scsi-all** and press **Enter**. The system lists the path to all devices that are connected to the Ultra 5 Application Server.

17 Write down the following information that pertains to the path for the external DVD device:

path = _____

Target = _____ = X

Unit = _____ = Y

18 Depending on the Application Server you are upgrading, complete one of the following boot commands:

- If you are upgrading a Sun Blade 150, type **reboot -- "cdrom - install"** and press **Enter**.

  Important: Be certain that you type two dashes after "reboot" and that "cdrom - install" is enclosed in double quotes.

- If you are upgrading an Ultra 5, type **boot [path]/sd@X,Y:f - install** and press **Enter**.

  Important: If this command does not execute, re-run the command but substitute **disk** for **sd** in the boot path.

  Example: OK> boot /pci@1f,0/pci@1/scsi@8/sd@0,0:f - install

Results:

- The Application Server boots from the DVD.
- The Solaris OS installs.

  Note: An Application Server with only 256 MB of memory will not boot into the OpenWindows desktop environment. Instead, the server will boot into a text-based installation mode, and the installation will still complete successfully.

- All Application Server software packages install.

- The Application Server key files restore.

  Note: If a "glob failed" message appears, it may be because your system does not have NIS configuration files. You can ignore this message.

- The CDE window appears.

Notes:

- The installation process may take more than 2 hours. Do not interrupt the installation process.
- In some cases, a system identification window opens after booting.
- In some cases, a Solaris Registration Wizard window opens.

19 Did a system identification window open, as described in step 18?

- If **yes**, the window will ask you a series of questions. The following steps detail what your answers to those questions should be.

  a Press **F2** to continue.
  b Press **F2** to continue.
  c Select **None** for the Name Service.
  d Press **F2** to continue.
  e Confirm and press **F2** to continue.
  f Select **Yes** for Part of a Subnet.
  g Press **F2** to continue.
  h Type the Netmask of **255.255.255.0**.
  i Press **F2** to continue.
  j Confirm and press **F2** to continue.
  k Go to step 20.

- If **no**, go to step 20.

20 Did a Solaris Registration Wizard open, as described in step 18?

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

  a Select **Run the Solaris Software without Registering**.
  b Click **Next** in the lower part of the window.
  c Select **Never Register**.
  d Go to step 21.

- If **no**, go to step 21.

21 Log in to the CDE of the Application Server as **root** user.

22 Did you upgrade an Ultra 5 Application Server?

- If **yes**, go to step 23.
- If **no**, go to ***Check Installed Version Numbers on the Application Server*** (on page 66).

23 Type **shutdown -y -g0 -i0** and press **Enter**.

24 At the OK prompt, type **printenv auto-boot?** and press **Enter**. The auto-boot value displays.

25 Is **auto-boot** set to **true**?

- If **yes**, type boot, press **Enter**, and login as **dncs** user.
- If **no**, go to step 26.

26 Type **setenv auto-boot? true** and press **Enter**.

27 Type **printenv auto-boot?** to verify that auto-boot is now set to true.

28 Type **boot -r** and press **Enter**.

29 Login as **dncs** user.

Completing the Sun Fire V240 or V245 Application Server Upgrade

1 At the **OK** prompt, type **boot -r** and press **Enter**.

Results:

- The Application Server reboots several times. On the first reboot, the system builds the disk mirrors and reboots.
- The system then restores the key files and reboots.
- The system begins to build the new file system.
- After the final reboot, the new boot environment contains SR i4.2.2.

2 Log on to the CDE window of the V240 or V245 Application Server as **dncs** user.

Check Installed Version Numbers on the Application Server

Before you eject the DVD from the Application Server, confirm that the installed software versions match the requirements for SR i4.2.2.

1 If necessary, insert the SR 4.4 DVD into the DVD drive of the Application Server.

2 From a root xterm window on the Application Server, type one of the following commands:

- If your Application Server has an *internal* DVD drive, type **/cdrom/cdrom0/s3/sai/scripts/utils/listpkgs -i** and then press **Enter**.
- If your Application Server has an *external* DVD drive, type **/cdrom/cdrom1/s3/sai/scripts/utils/listpkgs -i** and then press **Enter**.

Note: It may take a few minutes for this command to run.

Result: The system displays a listing of installed packages.

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	i3.4.0.3	
DNCS/App Tools	SAItools	4.2.1.12	
Solaris Patches	SAIpatch	4.3.0.1	
Platform	SAIdnapp	4.3.0.3	

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?

Important: The build number (the fourth digit of the version number) may differ.

- If **yes**, go to step 5.
- If **no**, call Cisco Services and inform them of the discrepancy.

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

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. ASI feature requires extensive system configuration. If the system you are upgrading is 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 **Cisco**

mc_param_name **DIRECT_ASI**

mc_param_data **0**

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

Restart the System Components

Refer to Appendix B, ***Restarting System Components*** (on page 113), to 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.
- If the EARS process does not start, follow these instructions.
  a Open an xterm window on the DNCS.
  b Type **cd /dvs/dvsFiles/EARS** and then press **Enter**.
  c Type **mv IPs IPs.orig** and then press **Enter**. The EARS process should start and the indicator should turn green.

  Note: If the EARS process still does not start, stop and restart the EARS process manually.

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 71).
   - 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 71).

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 **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 ***SR i4.2.2 Post Upgrade Procedures*** (on page 73).
   - If **no**, continue with step 3.
3. From a root xterm window on the Application Server, 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 press **Enter**. The system should list /usr/sbin/cron.

4

SR i4.2.2 Post Upgrade Procedures

Introduction

After upgrading your system by following the procedures described earlier in these upgrade instructions, 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 1-866-787-3866.

In This Chapter

Check Transport Stream ID Values

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 **Sys Config**. 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 **/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 51) 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.

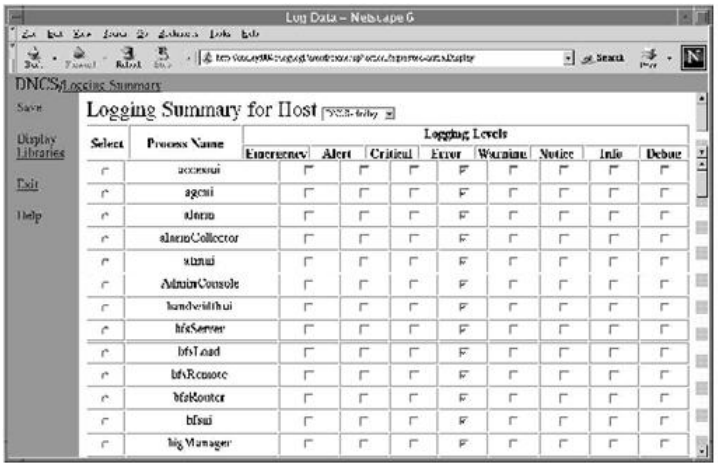
Example: For the example in step 2, *BbKkSDQLGOo*, the following Debug logs should be enabled:

- 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 Local BFS QAMs** 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. Highlight **BFSqam** and then click **Display** at the bottom of the window. The window updates to display session data for the BFS QAM.
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 i4.2.2, 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 Site Name. The Site [site name] 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.

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 BIG PAT Setup window appears.

4. On the BIG 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**.

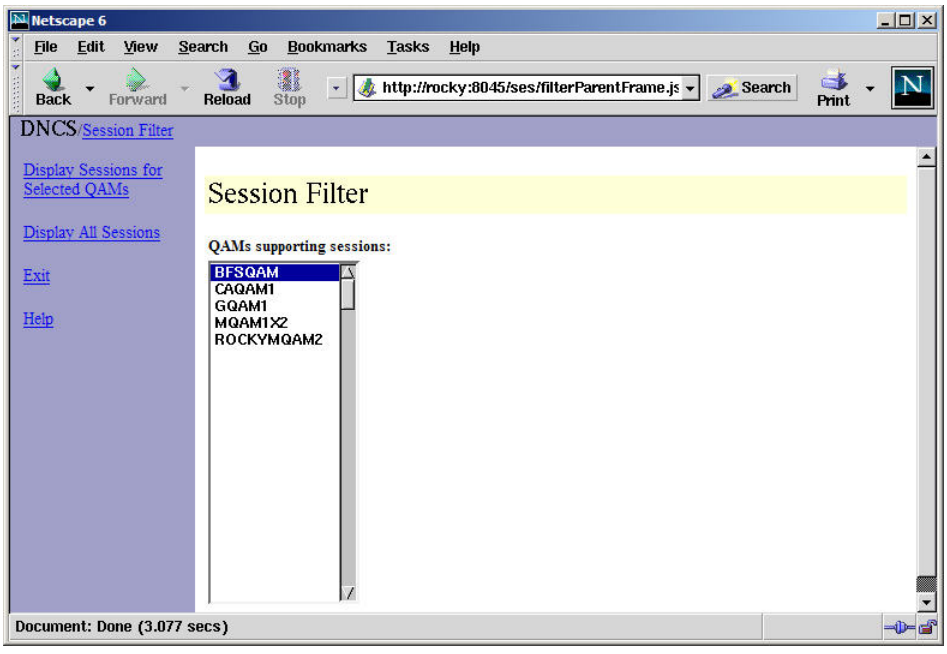
3 Click **Process** and then select **Stop Process**. A confirmation message opens.

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 Select the **BFS QAM** and click **Display Sessions for Selected QAM**. The session data for the BFS QAM appears.

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**. 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

After rebooting the BIG and the BIG QAM, you can 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, and that it contains no entry for camEmmDeleter. 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*** (on page 85).
- 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*** (on page 87).

- 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 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 system 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 i4.2.2

Verifying the System Upgrade

Complete these steps to verify a successful upgrade to SR i4.2.2.

1 Examine the dncsLog file in the /var/log directory to see if there are VASP entry errors.

- If **yes**, complete these steps to rebuild the VASP entries.
  - **a** Open the DNCS Administrative Console, select the **System Provisioning** tab, and then click **ATM PVC**. The ATM PVC Map List window appears.
  - **b** Record all of the information from the ATM PVC Map List window on a piece of paper.
  - **c** Delete all of the entries from the ATM PVC Map List window.
  - **d** Re-enter each entry from the recorded information.
- If **no**, go to step 2.

2 Type **cd /dvs/dncs/Utilities/doctor** and press **Enter**.

3 Type **doctor -vn** and press **Enter**. This command runs the Doctor Report generates. Review the Doctor Report to ensure that communications exists between all DBDS elements.

Important: It is normal for Rovi Corporation sites to report errors on Application Server checks.

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.

Important: If any disk partition lists a capacity greater than 85 percent, contact Cisco Services at 1-866-787-3866 before proceeding.

5 Complete these steps to perform a slow and fast boot on a test DHCT with a working return path (2-way mode):

- **a** Boot a DHCT.

  Note: Do not press the power button.
- **b** Access the Power On Self Test and Boot Status Diagnostic Screen on the DHCT and verify that all parameters, except UNcfg, display **Ready**.

  Note: UNcfg displays **Broadcast**.
- **c** Wait 5 minutes.
- **d** Press the power button on the DHCT. The power to the DHCT is turned on.
- **e** Access the Power On Self Test and Boot Status Diagnostic Screen on the DHCT and verify that all parameters, including UNcfg, display **Ready**.

6 If the DHCT is configured for two-way communication, verify that you can ping the DHCT.

7 Tune each available channel on a DHCT to confirm that a full channel lineup is present.

Note: Write down any anomalies you notice while verifying the lineup.

8 Verify that you can purchase and view an IPPV event.

9 Verify that you can purchase and view VOD events.

10 Did you have a point-to-point protocol (PPP) link prior to the upgrade?

- If **yes**, follow these steps.
  - **a** As root user, type **/etc/ppp/pppup-sa.sh** and then press **Enter**. The system establishes a PPP session and assigns a dynamic IP address.
  - **b** Type **ping 192.168.41.209** and then press **Enter**.
  - **c** Verify that the returned data shows that the PPP link is functional.
- If **no**, go to step 11.

11 Stage at least one new DHCT to the system operator's specifications. After staging the DHCT, verify the following:

- The DHCT receives 33 or 34 EMMs (Entitlement Management Messages).
- The DHCT successfully receives its Entitlement Agent.

Set Staging Options

After upgrading SR i4.2.2, 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 **cd /dvs/dncs/bin** and then press **Enter**. The /dvs/dncs/bin directory becomes the working directory.
3. Type **more dncsSetup** and then press **Enter**. The dncsSetup opens for viewing using the UNIX *more* utility.
4. Examine the dncsSetup file and look for the following entry:
   atm_addr=dncsatm
5. Does the dncsSetup file contain the entry as described in step 4?
   - If **yes**, follow these instructions.
     a. Press the **Ctrl** and **c** keys simultaneously to exit the *more* utility.
     b. Go to the next procedure in this chapter.
   - If **no**, follow these instructions.
     a. Press the **Ctrl** and **c** keys simultaneously to exit the *more* utility.
     b. If necessary, open an xterm window on the DNCS.
     c. Type **su - dncs** and then press **Enter**. The **password** prompt appears.
     d. Type the dncs password and then press **Enter**.
     e. Type **vi dncsSetup** and then press **Enter**. The dncsSetup file opens using the UNIX vi text editor.
     f. Edit the dncsSetup file so that it contains an **atm_addr=dncsatm** entry.
     Note: The file may contain an atm_addr=dncseth entry. If so, change it so that it reads **atm_addr=dncsatm**. You must not have an atm_addr=dncseth entry in the dncsSetup file after the upgrade to SR 2.1 or later.
     g. Save and close the dncsSetup file.
     h. Type **exit** and then press **Enter** to log out of the dncs role.
     i. Go to the next procedure in this chapter.

Set the Clock on the TED (Optional)

Complete these steps to set the clock on the TED.

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 the root user.

Install the NMI Software

If you supported the Alarm Manager product prior to the upgrade, or plan to support Alarm Manager after the upgrade, you need to install or re-install the Network Management Interface (NMI) software now.

Note: The upgrade to SR i4.2.2 overwrote the NMI software at sites that supported the Alarm Manager product prior to the upgrade.

Refer to Chapter 2 of the *DBDS Alarm Manager 1.0 Installation Instructions* (part number 745262) for instructions on installing the NMI software.

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

Contact Cisco Services to enable the Distributed DNCS feature on your system.

Register RNCS With the DNCS

After the Distributed DNCS feature is licensed 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

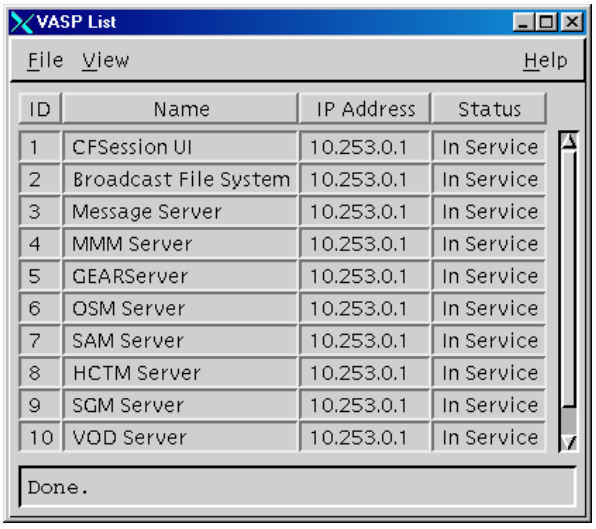
After using the siteCmd program to register the RNCS with the DNCS, use the online help of the DNCS to provision the RNCS.

Note: Provisioning the RNCS refers to adding components, such as QAMs and QPSKs, 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 i4.2.2.

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 **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.
3. From an xterm window where you are logged on as root user, type **/cdrom/cdrom0/s3/sai/scripts/attach_mirrors** and then press **Enter**. A confirmation message appears.
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 **eject cdrom** and then press **Enter**.
6. Repeat steps 1 through 5 if you need to attach the mirrors on a second server.

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 i4.2.2, 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

Reference Back Up Procedures

The backup procedures for sites that run SR i4.2.2 system software are found in *DBDS Backup and Restore Procedures For SR 2.2 Through 4.3 User Guide* (part number 4013779). To back up the Informix database, the DNCS file system, and the Application Server file system, reference the following chapters:

- Chapter 3, **Back Up Procedures**
- Chapter 4, **Restoration Procedures**

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

In This Appendix

Introduction

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

Stop System Components

Stopping the Application Server

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

1. Press the middle mouse button on the Application Server and select **App Serv Stop**.
2. From an xterm window on the Application Server, type **appControl** and then press **Enter**. The Applications Control window appears.
3. Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**. The system displays all Application Server processes.

   Note: The system updates the display periodically, or you can press **Enter** to force an update.
4. When the **Curr Stt** (Current State) field of the Applications Control window indicates that all of the Application Server processes have stopped, follow the on-screen instructions to close the Applications Control window.

Stopping the DNCS

Complete these steps to stop the DNCS.

1. At the DNCS, press the middle mouse button and then select **DNCS Stop**.

   Note: If a confirmation message appears, click **OK**.
2. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**.

   Result: The Dncs Control window appears.
3. Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**.

   Result: The system displays all DNCS processes.

   Note: The system updates the display periodically, or you can press Enter to force an update.
4. When the **Curr Stt** (Current State) field of the Dncs Control window indicates that all of the DNCS processes have stopped, follow the on-screen instructions to close the Dncs Control window.

B

Restarting System Components

In This Appendix

Introduction

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

Restart System Components

Restarting the DNCS

1. Click the middle mouse button on the DNCS and select **DNCS Start**. The DNCS processes start.
2. Click the middle mouse button on the DNCS and select **Administrative Console**. The DNCS Administrative Console opens.
3. From the DNCS Administrative Console Status window, click **DNCS Control**.

   Results:

   - The DNCS Control window opens.
   - Green indicators begin to replace red indicators on the DNCS Control window.
4. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The Dncs Control utility window opens.
5. Type **2** (for Startup / Shutdown Single Element Group) and then press **Enter**. The Dncs Control window updates to list the status of all of the processes and servers running on the DNCS.
6. 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.

   Important: If the EARS process does not start, go to step 7.
7. From an xterm window on the DNCS, type **cd /dvs/dvsFiles/EARS** and then press **Enter**.
8. Type **cp -p IPs IPs.old** and then press **Enter**.
9. Type **rm IPs** and then press **Enter**. The EARS process should start.

   Note: If the EARS process still does not start, stop and restart all DNCS processes.

Restarting the Application Server

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

Restarting the Application Server

1. Press the middle mouse button on the Application Server and select **App Serv Start**.
2. From an xterm window on the Application Server, type **appControl** and then press **Enter**. The Applications Control window opens.
3. Select option **2** on the Applications Control window. The system displays a list of Application Server processes and their current status.

   Note: The system updates the display periodically, or you can press **Enter** to force an update.
4. When the Application Control window indicates that the current state (**Curr Stt**) of each process is running, follow the on-screen instructions to close the Applications Control 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 i4.2.2 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 every day.

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 i4.2.2 Rollback Procedures for the DVD Upgrade

In This Appendix

Introduction

The SR i4.2.2 rollback procedures are intended for field service engineers who encounter problems while upgrading an existing digital system to SR i4.2.2. Prior to executing the SR i4.2.2 rollback procedures, contact Cisco Services at 1-866-787-3866.

Which Rollback Procedure to Run

Two rollback procedures exist for rolling back from SR i4.2.2. 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 105), then use the procedure under ***Activate the Old System Release*** (on page 123) to roll back from SR i4.2.2.

  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 105), 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 i4.2.2.

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

_____

2 If necessary, follow the procedures in Appendix A, Stopping System Components, to stop the system components.

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

4 Type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The system reboots and activates the old software.

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

5 Did the DNCS reboot without error?

- If **yes**, skip to step 9.
- If **no**, go to 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 **df -k** and then press **Enter**. The system displays the mounted filesystems.

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 10.

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 7.

   a Type **mount /var** and then press **Enter**. The system mounts the /var filesystem.

   b Type **df -k** and then press **Enter**. The system displays the /var filesystem in the output.

   c **Note:** If the /var filesystem is still not present in the output, call Cisco Services for assistance.

   d 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 45) procedure.

Note: Go to ***Updating the TED Files*** (on page 124) after you have completed the **Attach Mirrors** 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 **ping dncsted** and then press **Enter**. The system responds with a **dncsted is alive** message.

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

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

4 Type **./loadTedFiles.sh** and then press **Enter**.

Important: Be sure to type the period before typing /loadTedFiles.sh.

Results:

- The system copies the appropriate files to the TED.
- The system initializes the TED.
- After a brief pause, the system displays the contents of the TED logfile (devtedLog.000) to the screen.

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 Sun Blade 150 or Ultra 5 Application Server*** (on page 127).

Roll Back the Sun Blade 150 or Ultra 5 Application Server

Preparing to Restore the Application Server File System From Tape

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 i4.2.2 DVD into the DVD drive of the Application Server.
4. If necessary, type **shutdown -g0 -y -i0** and then press **Enter**. The system halts all processes on the Application Server and an **ok** prompt appears.

   Note: The Application Server may already be shut down.
5. At the **ok** prompt, type **boot cdrom - SAshell** and then press **Enter**.

   Results:

   - The Application Server boots from the CD.
   - An xterm window opens.
6. Insert your most recent Application Server file system backup tape into the tape drive of the DNCS.

Restoring the Application Server File System

Follow these instructions to restore the Application Server file system from a tape in the tape drive of the DNCS.

1. Type **/tmp/cdrom/backup_restore/restoreFileSystems -r [hostname or IP address]:[tape device]** and then press **Enter**.

   Notes:

   - Substitute the hostname or IP address of the DNCS for [hostname or IP address].
   - Type the command on one line.

   Example:

   /tmp/cdrom/backup_restore/restoreFileSystems -r 192.168.44.71:/dev/rmt/0h

   Result: The system restores the Application Server file system and displays a message when the restoration is complete.
2. When the restoration is complete, eject the tape and store it in a safe place.

3 Type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The Application Server reboots and the Common Desktop Environment (CDE) login window appears.

4 Log on to the CDE as **dncs** user.

5 Follow the procedures in Appendix B, ***Restarting System Components*** (on page 113), to restart the system components.

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

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

August 2012 Printed in USA Part Number 4036631 Rev B