System Release 2.7/3.7/4.2
Service Pack 4
Release Note and Installation Instructions

Please Read

Important

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

Notices

Trademark Acknowledgments

- Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.
- Rovi is a trademark of Rovi Corporation.
- OpenCable and DOCSIS are trademarks of Cable Television Laboratories, Inc.
- Other third party trademarks mentioned are the property of their respective owners.
- The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

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

Copyright

Contents

About This Guide

Introduction

This guide provides release note information and step-by-step instructions for upgrading our Digital Broadband Delivery System (DBDS) to System Release (SR) 2.7/3.7/4.2 Service Pack 4 (SP4). Sites that use this guide to upgrade must currently support SR 4.2 SP3.

Upgrade software installed through this guide is provided in the form of CDs. This is not a UniPack upgrade guide.

Scope

This release note and installation instructions pertain to sites that support either the SA Resident Application (SARA) or another resident application.

Audience

This release note and installation instructions are written for system operators of our DBDS, as well as for engineers who install the SR 2.7/3.7/4.2 SP4 software onto the Digital Network Control System (DNCS) and the Application Server.

Document Version

This is the first formal release of this document.

1

Introducing 2.7/3.7/4.2 SP4

Introduction

This chapter lists the major improvements and operational changes for the DBDS as a result of installing this updated service pack to the existing system release. In addition, this chapter provides important system information about this service pack.

Upgrade Path

Sites that want to upgrade to this service pack must support System Release 4.2 Service Pack 3 or later. This guide provides instructions for upgrading to SR 2.7/3.7/4.2 SP4.

Time to Complete the Upgrade

The upgrade to SR 2.7/3.7/4.2 SP4 must be completed within a maintenance window. Our engineers have determined that a typical site can be upgraded in approximately 6 hours.

In This Chapter

Major Improvements to SR 2.7/3.7/4.2 SP4

Introduction

SR 2.7/3.7/4.2 SP4 features several major operational improvements. Some of these improvements are described in the following section on EMM enhancements.

EMM Enhancements

This service pack provides the following EMM enhancements:

- Reduces the one-second artificial delay within the EMM distributor process to a value that allows for up to 800,000 DTA 170 devices in the system.
- Enables the DNCS to support up to 800,000 one-way PowerKEY devices and up to 700,000 two-way PowerKEY devices, with total active devices not to exceed 1.5 million.

What Are the Site Requirements?

Introduction

This section provides the following information:

- Identifies the CDs that are needed to install the service pack software
- Lists the software components tested and released as part of this service pack
- Provides the antecedents and prerequisites required before installing this service pack

Antecedents

This release succeeds and carries forward all of the enhancements, features, and improvements of previous releases and related service packs.

Prerequisites

The DBDS must meet the following prerequisites before you install this service pack:

- **SR 2.7/3.7/4.2-SP3** or later is currently installed on your system.
- **SAIpatch 4.2.1.10** (Solaris) or later is currently installed on your system.
- **SAItools 4.2.0.13p5** is currently installed on your system.
- You have the CD labeled **SR 2.7/3.7/4.2-SP4**.
- You have the CD labeled **DBDS Maintenance CD 4.3** (or later) in order to complete the required backups of the database and the file system.

  Note: DBDS Maintenance CD 4.3 is the minimum version that is certified for SR 2.7/3.7/4.2.
- **DBDS Utilities Version 6.1.x** is installed on your system.

System Release Compatibility

The following software applications and patches have been tested and are being released as part of this service pack:

- DNCS Application 4.2.0.50p11
- DNCS GUI/WUI 4.2.0.50p11

This service pack can be applied to DBDS networks operating at SR 2.7/3.7/4.2 SP3.

For a list of all available patches to date for SR 2.7, 3.7, or 4.2 and a complete configuration listing for SR 2.7/3.7/4.2 SP4, please contact Cisco Services at 1-866-787-3866.

Server Platforms

The following DNCS and Application Server hardware platforms are supported by this software release.

DNCS

Platform	Hard Drives	Memory
Sun Fire V890	■ 6 X 146 GB ■ 12 X 146 GB	■ 4 GB minimum ■ 16 GB minimum
Sun Fire V880	■ 6 X 73 GB ■ 12 X 73 GB	■ 4 GB minimum ■ 8 GB minimum
Sun Fire V445	■ 4 X 73 GB ■ 8 X 73 GB	■ 1 GB minimum ■ 2 GB minimum

Application Server

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

Note: The Sun V240 and V245 hard drives and memory configurations make them acceptable application servers for the RNCS.

What Are the Known Issues?

Open Issues

This section provides a list of open CDETS defect IDs that were identified during testing of SR 2.7/3.7/4.2 SP4. Defects are indexed by ID number in ascending order. Resolutions to these defects are currently under investigation or in development.

This list is not intended to be comprehensive. If you have questions about a particular defect, contact your account representative.

Defect ID	Headline
CSCtz94691	MMMServer core dumps sporadically after lame dumps core **Impact**: Causes MMMServer to alter core dump when trying to remove the audio file.

What's Fixed?

Introduction

This section lists the issues that were found while testing this software product. Efforts to address these issues are ongoing in the Cisco laboratories.

Resolved Issues

This section provides a list of CDETS defect IDs found in previous releases that have been corrected in SR 2.7/3.7/4.2 SP4.

Notes:

- Defects are identified by a case tracking number (Defect ID) and a headline that briefly identifies the case.
- The headlines in this section are presented exactly as they appear in the issue tracking system.

Defect ID	Headline
109380-01	Eventmanager causes session to go out in the clear if Netcrypt is rebooted
118027-03	drm has issues with sessions on table-based qams
120123-08	qamManager issues a "cancelAll" in rpc to qam
122745-01	qpskManager fails to cancel packet from MFMC CMTS bridge
82584-04	EAS Config GUI indicates save failed but really is successful
89001-06	PKE Manager opens RPC sessions to PCG for successive session deletes
109540-01	OcdlManager memory leak in XmlDb class
111540-08	qamManager needs to quarantine QAMs when it times out on messages
122624	Add setOnconfig.sh script to SR4.2SP4 DNCS package and execute during install
91850-08	Reduce camEx PowerKEY entitlement EID spec value range matching clients
108466-11	tellDhct doesn't work with mac addresses that don't start with other than 00
111332-06	The IIH utility does not deregister with portmapper when terminating
CSCtr83575	emmDistributor remove noise level debug from 'DE' level
CSCtw44672/ CSCtu24943	siManager stops reinserting c3 packet when qpskManager is bounced
CSCtx45938	EAT processing in mmmRemote caused it to send extra malformed EAN msg at the end

Defect ID	Headline
CSCtx21779	emmDistributor core dumps on systems with less than 36000 set-tops
CSCtr83594	emmDistributor enhancement to support DTA 170s
CSCtr98482	DSM core dump due to memory usage triggered by SIP timeouts

2

DNCS Pre-Upgrade Procedures

This chapter contains procedures that must be completed before you begin the actual upgrade process. These pre-upgrade procedures consist mainly of system checks and backups of the DNCS.

The first several procedures of this chapter can be completed before the maintenance window begins, while the actual upgrade of DNCS software must be completed during a maintenance window. See ***When to Complete These Procedures*** (on page 11) for a list of those procedures that can be completed before the start of the maintenance window.

In This Chapter

When to Complete These Procedures

Upgrade Process

As you are planning the upgrade, be sure to contact your billing vendor to make arrangements to suspend the billing interface on the night of the upgrade. This is an important step. Your system must not try to access the database during the upgrade process. In addition, contact the provider(s) of any third-party applications that your system supports. Follow their guidance in determining whether these third-party interfaces should be stopped and if the application needs to be updated during the upgrade.

Complete These Procedures

Pre-Maintenance Window

To save valuable time, complete the pre-maintenance window procedures in this chapter prior to the beginning of the maintenance window. Depending upon the size of the system you are upgrading, it should take about 3 or 4 hours to complete the following procedures:

- ***Plan Which Optional Features Will Be Supported*** (on page 15)
- ***Verify the Integrity of the CDs*** (on page 16)
- ***Verify the Integrity of the Maintenance CD*** (on page 18)
- ***Upgrade the RNCS (Optional)*** (on page 19)
- ***Check Available Disk Space*** (on page 20)
- ***Run the Doctor Report*** (on page 21)
- ***Examine Mirrored Devices*** (on page 23)
- ***Verify that the Boot Device is Correctly Configured*** (on page 24)
- ***Verify that the Dump Device is Correctly Configured*** (on page 25)
- ***Verify SAItools Version*** *(on page 26)*
- ***Back Up Various Data Files*** (on page 28)
- ***Check the EAS Configuration—Pre-Upgrade*** (on page 29)
- ***Obtain DNCS System Configuration*** (on page 30)
- ***Collect Network Information*** (on page 31)
- ***Check and Record Sessions*** (on page 33)

- ***Back Up the DNCS and Application Server File Systems*** (on page 35)
- ***Stop the dhctStatus, signonCount, and cmd2000 Utilities*** (on page 36)
- ***Back Up and Delete the copyControlParams File*** (on page 39)
- ***Verify DBDS Stability*** (on page 40)
- ***Back Up the Informix Database*** (on page 41)

During the Maintenance Window

At the beginning of the maintenance window, you should start with ***Suspend Billing and Third-Party Interfaces*** (on page 42) and complete all of the remaining procedures in Chapter 2. You should also complete the procedures in Chapter 3 during the same maintenance window.

Enabled Features

The following list contains some of the optional features that can be enabled by engineers at Cisco Services without a special license. Not all of these features necessarily pertain to the software you are installing in this guide. Check with your North American marketing representative or Cisco Services if you are unsure about which optional features this software supports.

- Conditional Access Mode — Indicates whether the DNCS provides PowerKEY conditional access or non-SA conditional access, such as NDS
- DBDS Network Overlay — Enables DNCS support for "Overlay" of a third-party system within an SA system
- SI Type to Use — Specifies the type of system/service information (SI) that the given system will use
- PID Mapping Mode — Specifies whether the transport stream ID (TSID) the system will use is "Dynamic Unique" or "Static non-Unique"
- PreAllocated Session Management — Support for the pre-allocation of sessions by the shared resource manager (SRM) process of the DNCS
- Direct ASI — Enables the system to eliminate the need for the Broadband Integrated Gateway (BIG) to transmit Broadcast File System (BFS) data to modulators
- Third-Party Source — Support for third-party SI sources

  Note: For additional information, refer to the technical bulletin *Program and System Information Protocol Configuration for System Releases 2.5, 2.7, 3.5, 3.7, 4.0, 4.2, and CV 3.4* (part number 4011319).
- Split Channels — Support for split channels in defined channel maps
- Netcrypt Bulk Encryptor — Support for Netcrypt provisioning
- Multiflow Multicast — Support for the Multiflow Multicast feature to work with the DOCSIS Set-Top Gateway (DSG) in the DBDS
- SSP 2.4 Compliant — Support for a Server Interactive Session Request and a Server Interactive Session Release
- OOB Staging Bridge — Support for the use of a subset of the out-of-band (OOB) bridge population within the DBDS to be dedicated to the staging of DHCTs
- Switched Digital Video — Support for the Switched Digital Video (SDV) feature
- Trusted Domain — Support for the MSO Trusted Domain feature, which includes "Home Account" support

- Fixed Key Encryption — Support for the use of the "Fixed Key" algorithm to be used in encryption tasks
- DNO Encrypted VOD — Support for encrypted VOD in an Overlay environment
- OpenCAS PowerKEY Interface — Support for an OpenCAS interface for applying PowerKEY encryption to an established "in the clear" session
- Overlay Netcrypt Bulk Encryptor — Support for the Netcrypt Bulk Encryptor feature
- OpenCable™ MP3 Audio Support — Support for the encoding of EAS audio messages to MP3 format for distribution over the TS Broadcaster
- Non SAM_EAS Force Tune — Support for force-tuning EAS for sites running the DNCS without SAM channel map services

Plan Which Optional Features Will Be Supported

Optional Features

This software includes several optional features that system operators can elect to enable on their systems. Some of these features require that the system operator obtain a license for the feature to be activated; others can simply be activated by engineers at Cisco Services without a license.

Important: Any features that are currently enabled or licensed do not have to be re-enabled.

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

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

Licensed Features

The following licensed features can be enabled with this software:

- EAS Filtering—Enables system operators to filter Emergency Alert System (EAS) messages by hub
- Enhanced Interactive Session Performance—Improves the efficiency with which the DNCS processes video-on-demand (VOD) sessions
- Session-Based Encryption—Activates encryption for session-based VOD
- Distributed DNCS—Allows the DNCS to manage several remote headends

Verify the Integrity of the CDs

Complete the following steps for each CD, except the DBDS Maintenance CD, contained in the software binder.

Note: You will verify the DBDS Maintenance CD in a separate procedure.

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 Insert a CD into the CD drive on the DNCS.

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

4 Type **cd /cdrom/cdrom0** and then press **Enter**. The /cdrom/cdrom0 directory becomes the working directory.

5 Type **ls -la** and then press **Enter**. The system lists the contents of the CD.

6 Did the system list the contents of the CD?

   - If **yes**, skip the next step and go to step 8.
   - If **no**, the CD might be defective. Go to step 7.

7 The vold process manages the auto-mount functions for the CDROM drive. Check to see if the vold process is running by typing **ps -ef | grep vold** and press **Enter**.

   a If vold is running, type the following commands:

      – **/etc/init.d/volmgt stop** and press **Enter**

      – **/etc/init.d/volmgt start** and press **Enter**

   b If vold is not running, type the following commands:

      – **/usr/sbin/vold&** and press **Enter**

      – **ps -ef | grep vold** and press **Enter**

   Note: After performing these checks, if you still cannot see the contents of the CD, contact Cisco Services for assistance.

8 Type **pkgchk -d . SAI*** and then press **Enter**.-

   Important:- Be sure to type the dot between the **-d** and **SAI***.

   Results:

   - The system checks each package on the CD that starts with SAI.
   - The system performs a checksum on each package and ensures that the checksum matches what is contained on the package map.
   - The system lists the results of a package check.

   Note: The system may list some warnings, which are normal and can be ignored. The system clearly lists any errors found during the package check.

9 Did the package check reveal any errors?

- If **yes**, contact Cisco Services for assistance.

  Important: Do *not* proceed with the upgrade if the CD contains errors.

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

  a Type **cd /** and then press **Enter**.
  b Type **eject cdrom** and then press **Enter**.

10 Repeat steps 2 through 8 for each CD received in the software binder.

11 Go to ***Verify the Integrity of the Maintenance CD*** (on page 18).

Verify the Integrity of the Maintenance CD

Complete the following steps to verify the integrity of the DBDS Maintenance CD.

1 Insert the DBDS Maintenance CD into the CD drive of the DNCS.

Note: If a File Manager window opens after you insert the CD, close the window.

2 Type **cd /cdrom/cdrom0** and then press **Enter**. The /cdrom/cdrom0 directory becomes the working directory.

3 Type **ls –lia** and then press **Enter**.

Result: The system displays the contents of the CD, which should be similar to the following example.

Example:

```
$ ls -lia
total 22
     58555 drwxr-xr-x   8 root     nobody       512 Nov  9 17:11 .
      4063 drwxr-xr-x   3 root     nobody       512 Nov  9 17:11 ..
     58822 dr-xr-xr-x   2 root     sys         4096 Mar 13  2007 s0
     58821 drwxr-xr-x  21 root     root        1024 Aug 29  2007 s1
     58771 drwxr-xr-x   2 root     root         512 Jun  9  2006 s2
     58770 drwxr-xr-x   5 root     root         512 Aug 29  2007 s3
     58769 drwxr-xr-x   2 root     root         512 Jun  9  2006 s4
     58665 drwxr-xr-x   2 root     root         512 Jun  9  2006 s5
```

4 Were the results from step 3 similar to the example?

- If **yes**, complete the following steps.
  - **a** Type **cd /** and then press **Enter**.
  - **b** Type **eject cdrom** and then press **Enter**.
  - **c** Type **exit** and then press **Enter** to log out the root user.
- If **no**, call Cisco Services.

5 If you have any RNCS servers, see ***Upgrade the RNCS (Optional)*** (on page 19); otherwise, go to ***Check Available Disk Space*** (on page 20).

Upgrade the RNCS (Optional)

If you are currently utilizing RNCS, you must upgrade your RNCS servers as part of the pre-upgrade process. If you are not utilizing RNCS, there is no need to upgrade RNCS servers, and you can skip the procedure to upgrade RNCS servers.

To upgrade your RNCS servers, refer to **Upgrade the RNCS Software** in Chapter 2 of the *RNCS Installation and Upgrade Instructions For SR 2.7/3.7 or SR 4.2* (part number 4012763).

Note: You can perform the RNCS upgrade process any time before the DNCS software upgrade, as the RNCS upgrade does not impact subscribers.

Go to ***Check Available Disk Space*** (on page 20).

Check Available Disk Space

We recommend that you have at least 700 MB of free space on the /disk1 filesystem to install the upgrade. This procedure provides instructions to check available disk space on your DNCS.

Checking Available Disk Space

1 From an xterm window on the DNCS, type **df -h** and then press **Enter**. The system displays, in the **avail** column, the amount of used and available space on the /disk1 filesystem.

```
# df -h
Filesystem             size   used  avail capacity  Mounted on
/dev/md/dsk/d500       7.9G   2.5G   5.3G    33%    /
/devices                 0K     0K     0K     0%    /devices
ctfs                     0K     0K     0K     0%    /system/contract
proc                     0K     0K     0K     0%    /proc
mnttab                   0K     0K     0K     0%    /etc/mnttab
swap                    10G   1.2M    10G     1%    /etc/svc/volatile
objfs                    0K     0K     0K     0%    /system/object
sharefs                  0K     0K     0K     0%    /etc/dfs/sharetab
fd                       0K     0K     0K     0%    /dev/fd
/dev/md/dsk/d503       7.9G   4.7G   3.1G    61%    /var
swap                    10G   2.5M    10G     1%    /tmp
swap                    10G    32K    10G     1%    /var/run
/dev/md/dsk/d510        59G   6.6G    52G    12%    /disk1
/dev/md/dsk/d507       7.9G   5.7G   2.1G    74%    /export/home
/vol/dev/dsk/c0t6d0/sr_4.2_sp4c11
                       371M   371M     0K   100%    /cdrom/sr_4.2_sp4c11
```

2 Does the Available column show that at least 700M are available for the upgrade?

- If **yes**, go to ***Run the Doctor Report*** (on page 21). You have sufficient space in which to perform the upgrade.
- If **no**, call Cisco Services. Engineers at Cisco Services can advise you regarding disk clean-up procedures.

Run the Doctor Report

Introduction

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

Notes:

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

Use the following procedure to run the Doctor Report on the DNCS.

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

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

3. Type the following command and press **Enter**. The system generates a list of parameters that you can use to run the Doctor Report.

   ```
   ./doctor
   ```

   Note: Each parameter causes the Doctor Report to generate output with specific configuration information.

4 To generate a complete Doctor Report, type the following command and press **Enter**.

```
./doctor -av
```

Results:

- The system generates the Doctor Report listing all system configuration information and directs the output of the report to the screen.
- The system also saves the output of the Doctor Report to a file in the current directory on the DNCS.

Example: The system saves the report with a name similar to `report.061026_0921.doc`

Notes:

- Depending upon the size of your system, it may take a few minutes for the report to generate.
- The final line of the report generated to the screen lists the file to which the output was saved.
- The report is a plain text file. You can view the report in a text editor of your choice.

Analyze the Doctor Report

Use the instructions provided in *DBDS Utilities Version 6.1 Installation Instructions and DNCS Utilities User Guide* (part number 4020695) to 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 Mirrored Devices

Before you disable the disk mirroring functions in preparation of an upgrade, you should examine the status of the mirrored drives on your system. 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 the Mirrored Devices

Complete the following steps to examine the status of the mirrored drives on your DNCS.

1. If necessary, open an xterm window on the DNCS.
2. 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. Check the conditions of the following *two* items and then answer the question in step 4.
   - Verify each metadevice and submirrors show the **State** as **Okay**.
   - If the system is an **E450**, verify that all **Hot Spares** indicate a status of **Available**.
4. Are the conditions listed in step 3 "true"?
   - If the system is an **E450** and both conditions listed in step 3 are true, go to ***Verify that the Boot Device is Correctly Configured*** (on page 24).
   - If the system is a V880 or V890 and the state of each metadevice and submirror is **Okay**, go to ***Verify that the Boot Device is Correctly Configured*** (on page 24).

     Note: If **both** conditions are not true for an **E450**, or if the State on the V880 or V890 is *not* **Okay**, call Cisco Services for help in resolving these issues with the metadevices.

Verify that the Boot Device is Correctly Configured

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

1. If necessary, open an xterm window on the DNCS.
2. Type **eeprom boot-device** and then press **Enter**.
3. Did you see disk:a listed as the **first** boot device?

   Example: `bootdevice=disk:a`

   - If **yes**, then you have completed this procedure.
   - If **no**, continue with the next step in this procedure.
4. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
   c. Type **eeprom boot-device=disk:a** and press **Enter** to reset the default boot device to the original disk.
   d. Type **eeprom boot-device** and press **Enter** to verify the boot device is set to **disk:a**.

Verify that the Dump Device is Correctly Configured

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

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

2 Type **su -** and press **Enter** to log on as **root** user.

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

4 Type **dumpadm** and then press **Enter**.

Result: The following output should be displayed:

```
# dumpadm
      Dump content: kernel pages
       Dump device: /dev/md/dsk/d501 (swap)
Savecore directory: /var/crash/dncs
  Savecore enabled: yes
```

5 Did the dump device show the same result as shown in step 2 above?

- If **yes**, then your dump device is configured correctly. Go to ***Verify SAItools Version*** (on page 26).
- If **no**, continue with step 4 to set the dump device correctly.

6 Type **dumpadm -d /dev/md/dsk/d501** and then press **Enter**.

7 Type **dumpadm** and then press **Enter**. The dump device should now show the same result as shown in step 2 above.

Verify SAItools Version

In many cases, sites have previously received Solaris Patch CD 4.2.1.10 and installed the contents on the DNCS. You can verify that Solaris Patch 4.2.1.10 has been installed by checking for the presence of SAIpatch 4.2.1.10 and SAItools 4.2.0.13p5 on the DNCS.

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

2 Type **pkginfo –l SAIpatch** and press **Enter**. The package information for SAIpatch will appear.

Example:

```
$ pkginfo -l SAIpatch
   PKGINST:  SAIpatch
      NAME:  Solaris 10 Patches 10-22-09
  CATEGORY:  system
      ARCH:  SunOS_sparc
   VERSION:  4.2.1.10
   BASEDIR:  /
      DESC:  Solaris 10 Patches 10-22-09
    PSTAMP:  aurora20091022134949
  INSTDATE:  Feb 24 2010 10:06
    STATUS:  completely installed
     FILES:        1 installed pathnames
                   1 executables
                  12 blocks used (approx)
```

3 Type **pkginfo –l SAItools** and press **Enter**. The package information for SAItools will appear.

Example:

```
$ pkginfo -l SAItools
   PKGINST:  SAItools
      NAME:  DNCS/AppServer Tools 05-22-09
  CATEGORY:  application
      ARCH:  sparc
   VERSION:  4.2.0.13p5
   BASEDIR:  /dvs
    VENDOR:  Scientific Atlanta
      DESC:  DNCS/AppServer Tools 05-22-09
    PSTAMP:  aurora20090522073708
  INSTDATE:  Feb 24 2010 10:57
    STATUS:  completely installed
     FILES:     2855 installed pathnames
                  12 shared pathnames
                 371 directories
                 380 executables
                   5 setuid/setgid executables
              415113 blocks used (approx)
```

4 Does SAI tools show 4.2.0.13p5 and SAIpatch is 4.2.1.10?

a If **yes**, the correct versions of SAItools and SAIpatch are installed. Go to ***Back Up Various Data Files*** (on page 28).

b If **no**, stop and install SAIpatch 4.2.1.10 and SAItools 4.2.0.13p5 before continuing with this upgrade.

Important: If SAI tools does not show 4.2.0.13p5 and SAIpatch does not show 4.2.1.10, you must stop this procedure and install SAIpatch 4.2.1.10 and SAItools 4.2.0.13p5 before continuing with this upgrade.

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 the following command and press **Enter**. The system backs up the specified files.

   ```
   tar cvf [device name] /dvs/dncs/tmp/signonCount.out
   /dvs/dncs/tmp/signonCount.fixrpt /dvs/dncs/tmp/dhctStatus2
   ```

   Note: Substitute the device name of the DNCS tape drive for [device name] ***How to Determine the Tape Drive Device Name*** (on page 87).

   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.

Backing Up Modulator Configuration Files

In the event that you ever need to access the pre-upgrade configuration files of the QAM-family and QPSK modulators, follow these instructions to make a backup copy.

1. From a root xterm window, type **mkdir /tftpboot/backup_4.2_preSP4** and then press **Enter**.
2. Type **cp –p /tftpboot/*.config /tftpboot/backup_4.2_preSP4** and then press **Enter**. The system copies all .conf files to the /tftpboot/backup directory.

Check the EAS Configuration—Pre-Upgrade

Before installing the software, verify that your EAS equipment is working correctly by testing the system's ability to transmit EAS messages. Complete all of the procedures in the **Conduct EAS Tests** chapter of *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455).

Note: You will check the EAS configuration after the upgrade to ensure there are no issues.

Obtain DNCS System Configuration

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

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

```
more /etc/hosts
```

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

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

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

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

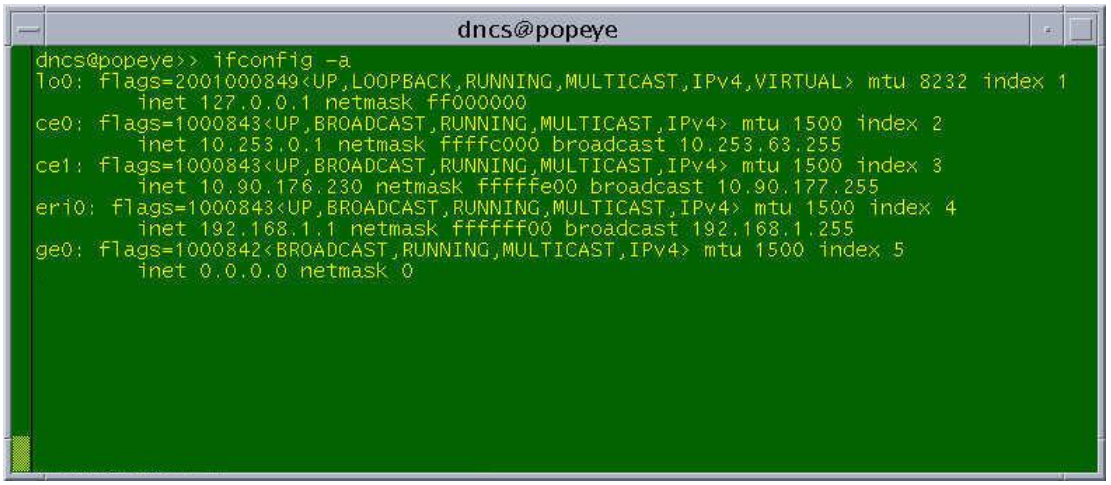
```
uname  -n
```

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

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

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

```
ifconfig -a
```



Collect Network Information

In this section, you are collecting network information required to reconstruct the system should the upgrade fail.

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

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

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

6 Type the following commands to copy the necessary files to this newly created directory.

   Important:

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

   a **cp -p /etc/hosts .**

   b **cp -p /etc/hostname.* .**

   c **cp -p /etc/inet/hosts inet.hosts**

   d **cp -p /etc/netmasks .**

   e **cp -p /etc/defaultrouter .**

      Note: If this file is not present, you will receive the **cp: cannot access /etc/defaultrouter** message. In this case, continue with the next command.

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

      Note: If this file is not present, you will receive the **cp: cannot access /etc/defaultrouter** message. In this case, continue with the next command.

   g **cp -p /etc/vfstab .**

   h **cp -p /etc/nsswitch.conf .**

   i **cp -p /etc/rc2.d/S82atminit .**

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

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

   l **netstat -nrv > netstat.out**

   m **ifconfig -a > ifconfig.out**

n **df -k > df.out**

o **eeprom nvramrc > nvramrc.out**

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

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

Note: Replace < date > with the current date.

Example: tar cvf crontabs.020107.tar crontabs

9 Type **mv crontabs.< date >.tar /export/home/dncs/network** and then press **Enter**.

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

11 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: The "l" in **ls** and **-ltr** is a lowercase letter L.

12 Back up DNCS files.

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

b Type **cp -p tsbroadcasterclientapi.jar tsbroadcasterclientapi.jar.preSP4** and press **Enter**.

c Type **cp -p TSBroadcasterClient.jar TSBroadcasterClient.jar.preSP4** and press **Enter**.

d Type **cd /export/home/informix/etc** and press **Enter**.

e Type **cp -p onconfig onconfig.preSP4** and press **Enter**.

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

Check and Record Sessions

Introduction

After you obtain your system configuration, your next step is to check the BFS QAM for the number of sessions and to remove any completed or orphaned sessions. This check enables you to compare the number of sessions before and after the installation process is complete, and indicates a successful upgrade if an equal number of sessions are built after the upgrade process is complete.

Checking the BFS Sessions on the BFS QAM or GQAM

Complete the following steps to check and record the number of pre-upgrade BFS sessions.

1 Follow these instructions to check the number of active sessions on the Cisco BFS QAM and/or GQAM.

Note: If your system does not use a Cisco BFS QAM or GQAM, skip to the next step.

a Press the **Options** button on the front panel of the modulator until the **Session Count** total appears. Record the **Session Count** here. _____

b Press the **Options** button again and record the **Program Count** here. _____

Note: If all sessions are encrypted, the **Session Count** and **Program Count** should be equal.

Important: *If the Program Count is 40 or more (i.e., you have 40 or more encrypted sessions) and the device is a CA-QAM, it may be necessary to replace your CA-QAM with an M-QAM* **before** *you upgrade. Contact Cisco Services for assistance.*

2 In an xterm window on the DNCS, type the following command and press **Enter**:

```
auditQam -query [BFS QAM IP address] [output port number]
```

3 Record the output from step 2 here: _____

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

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

5 Record the **Active Streams Count** here. _____

6 Do the results of steps 1, 2, and 4 all show the same number of sessions?

- If **yes**, continue with the next procedure in this chapter.
- If **no**, contact Cisco Services for help in resolving this issue.

Removing Completed or Orphaned Sessions

Complete the following steps to remove completed or orphaned sessions by running the clearDbSessions utility.

Note: The clearDbSessions utility takes several minutes to complete and can run in the background as you complete the remaining procedures in this chapter.

1. If necessary, open an xterm window on the DNCS.
2. 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.
3. Type **clearDbSessions -c** and then press **Enter**. The system removes all completed session, resource, and network graph records from the database.
4. Type **clearDbSessions -o** and then press **Enter**. The system removes orphaned records from the database.

Back Up the DNCS and Application Server File Systems

Perform a complete backup of the DNCS and Application Server file system now. Procedures for backing up the file system are contained in *DBDS Backup and Restore Procedures For SR 2.2 Through 4.3 User Guide* (part number 4013779). The backup procedures have been modified so that you no longer have to shut down the DNCS or the Application Server to complete the backup. If necessary, call Cisco Services to obtain a copy of these backup and restore procedures.

Notes:

- Procedures for backing up the file system are found in the **Backing Up and Restoring the DNCS and Application Server** chapter of the *DBDS Backup and Restore Procedures For SR 2.2 Through 4.3 User Guide* (part number 4013779).
- It may take up to 2 hours to back up a DNCS file system; you can usually back up an Application Server file system in about 30 minutes.

A Note About Disaster Recovery Enabled DBDS Networks

If your DBDS is enabled for Disaster Recovery, you must perform the tasks in ***Appendix E Perform a DNCS Upgrade in a Disaster Recovery Enabled Network*** (on page 91).

Note: If your DBDS is *not* enabled for Disaster Recovery, continue to the next section in this chapter.

Stop the dhctStatus, signonCount, and cmd2000 Utilities

Introduction

When sites are being upgraded, the dhctStatus utility may occasionally be actively polling DHCTs, and the signonCount and cmd2000 utilities may be active in system memory. Upgrades proceed more smoothly when the dhctStatus utility is not actively polling DHCTs and when the signonCount and cmd2000 utilities are not in system memory. The procedures in this section guide you through the steps required to terminate the polling activity of the dhctStatus utility, as well as to remove the signonCount and cmd2000 utilities from system memory.

Terminating the dhctStatus Utility Polling Operation

Complete the following steps to determine whether the dhctStatus utility is actively polling DHCTs, and then terminate the polling operation, if necessary.

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

2 Type the following command and press **Enter** to determine if the dhctStatus utility is running.

```
ps -ef | grep dhctStatus
```

Example: (if it is running)

```
dncs 12514 12449 0 13:50:27 pts/3 0:00 /bin/ksh
/dvs/dncs/bin/dhctStatus
dncs 12556 12514 0 13:50:28 pts/3 0:01 /usr/local/bin/perl
/dvs/dncs/bin/DhctStatus/dhctStatus.pl
dncs 12681 12632 0 13:50:54 pts/10 0:00 grep dhct
```

3 Do the results from step 2 show that the dhctStatus utility is running?

- If **yes**, type **dhctStatus** and press **Enter** to display the dhctStatus menu.
- If **no**, skip the rest of this procedure.

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 Press **q** and then press **Enter** to exit the menu.

5 Type the following command and press **Enter** to determine if all of the processes are terminated.

```
ps -ef | grep dhctStatus
```

Example:

```
dncs 12514 12449 0 13:50:27 pts/3 0:00 /bin/ksh
/dvs/dncs/bin/dhctStatus
dncs 12556 12514 0 13:50:28 pts/3 0:01 /usr/local/bin/perl
/dvs/dncs/bin/DhctStatus/dhctStatus.pl
dncs 12681 12632 0 13:50:54 pts/10 0:00 grep dhct
```

6 To kill any remaining processes, type the following command and press **Enter.**

```
pkill dhctStatus
```

Removing the signonCount Utility from System Memory

1 Type the following command and press **Enter**. A list of DNCS processes and process IDs display on the screen.

```
ps -ef | grep signonCount
```

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 the following command and press **Enter**.

```
signonCount uninstall
```

Note: The utility is not permanently uninstalled; it is placed back into system memory the next time you run the signonCount utility.

4 Type the following command and press **Enter**. A list of DNCS processes and process IDs display on the screen.

```
ps -ef | grep signonCount
```

5 To kill any remaining processes, type the following command and press **Enter**.

```
pkill signonCount
```

6 Type the following command and press **Enter** to ensure all the processes are terminated.

```
ps -ef | grep signonCount
```

7 Repeat steps 5 and 6 for any process that continues to be displayed. The system should only display the grep process.

Terminating the cmd2000 Utility

Complete the following steps to determine if any cmd2000 processes are running and then to terminate them, if necessary.

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

2 Type **ps -ef | grep cmd2000** and press **Enter**. The system displays a list of cmd2000 processes.

3 Do the results from step 2 show any active cmd2000 processes?

- If **yes**, choose one of the following options:
  - If you have a SA Application Server, type **kill -9 <processID>** and then press **Enter** for any cmd2000 processes that may be running.
  - If you have an Aptiv Application Server, type **/pdt/bin/StopCmd2000Logging** and then press **Enter**.
  - If you have a MAS server, refer to the documents supplied by Mystro to stop the active cmd2000 processes on the MAS server.
- If **no**, go to ***Back Up and Delete the copyControlParams File*** (on page 39).

4 Type **ps -ef | grep cmd2000** again and then press **Enter** to confirm that all cmd2000 processes are stopped.

5 Do the results from step 4 show that there are cmd2000 processes that are still running?

- If **yes**, type **kill -9 <processID>** and then press **Enter** for any cmd2000 processes that may be running; then, repeat steps 4 and 5.
- If **no**, go to ***Back Up and Delete the copyControlParams File*** (on page 39).

Back Up and Delete the copyControlParams File

Complete these steps to back up and delete the copyControlParams.inf file from the DNCS. During the upgrade, the system recreates the copyControlParams.inf file with appropriate default values. You can add customized entries back to the file after the upgrade.

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

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

3. Does the copyControlParams.inf file have any customized entries?
   - If **yes**, type the following command and press **Enter**. The system makes a backup copy of the copyControlParams.inf file.

     ```
     cp copyControlParams.inf  copyControlParams.inf.bak
     ```

   - If **no**, go to step 4.
4. Type the following command and press **Enter**. The system deletes the copyControlParams.inf file.

   ```
   rm copyControlParams.inf
   ```

   Note: When you restart the DNCS after the upgrade, the system will note the absence of the copyControlParams.inf file and will create a new one.

   Important: After the upgrade, use the backup copy of the copyControlParams.inf file, as a reference, to add any customized entries to the new file.

Verify DBDS Stability

1. Complete the following 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**. UNcfg displays **Broadcast**.

      Note: The fields on this screen may take up to 2 minutes to completely populate with data.

   c. Press the **Power** button on the DHCT to turn on the power and establish a two-way network connection.

   d. Access the Power On Self Test and Boot Status diagnostic screen on the DHCT and verify that all parameters, including UNcfg, display **Ready**.
2. Verify that you can ping the test DHCT.
3. Stage at least one new DHCT. After staging the DHCT, verify the following:
   - The DHCT loaded the current client release software.
   - The DHCT received at least 33 EMMs (Entitlement Management Messages).
   - The DHCT successfully received its Entitlement Agent.
4. Verify that the Interactive Program Guide (IPG) displays 7 days of valid and accurate data.
5. Verify the pay-per-view (PPV) barkers appear on the PPV channels correctly.
6. Verify that all third-party applications have loaded and operate properly.
7. Verify that you can purchase a VOD and/or xOD program.
8. Verify that SDV channels are available.

Back Up the Informix Database

Perform a complete backup of the Informix database just before the beginning of the maintenance window. This ensures that you have the latest copy of the database before the start of the upgrade. For example, if this process typically takes 45 minutes to complete, then begin this process 45 minutes before the maintenance window begins.

Procedures for backing up the database are contained in *DBDS Backup and Restore Procedures For SR 2.2 Through 4.3 User Guide* (part number 4013779). If necessary, call Cisco Services to obtain a copy of these backup and restore procedures.

Suspend Billing and Third-Party Interfaces

Important Note About the Maintenance Window

CAUTION:

Be sure that you are within a maintenance window as you begin this procedure. You will remain in the maintenance window as you continue to complete the installation process. The post-upgrade procedures can be completed the day after the installation is complete.

Suspending Billing and Third-Party Interfaces

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

Stop the cron Jobs

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

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

Stop the cron Jobs on the DNCS

1. In the xterm window, type **cd** and then press **Enter**. The home directory on the DNCS becomes the working directory.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type **pgrep -fl cron** and press **Enter**. The DNCS displays the cron process ID (PID).
4. Did the results from step 3 only include /usr/sbin/cron?
   - If **yes**, type **svcadm -v disable -s cron** and press **Enter**.
   - If **no**, (results from step 3 show multiple cron processes), perform the following steps:
     – Use the cron PID from step 3, and type **ptree <PID>** and press **Enter**. The DNCS displays the process tree of all cron processes.
     – Type **kill -9 <PIDs>** and press **Enter**.

       Important: List the PIDs in reverse order.

       Example: kill -9 14652 14651 209
   - If the results from step 3 did not show /usr/sbin/cron, then the cron jobs are already stopped.
5. Confirm that the cron jobs have stopped by typing **pgrep -fl cron** and press **Enter**. The command prompt should be the only item displayed; no processes should be displayed.

   Note: The "l" in "fl" is a lowercase L.
6. If the results from step 5 show that the cron process is still running, repeat steps 4 and 5.

   Note: Call Cisco Services for assistance if necessary.

Stop the cron Jobs on the Application Server or MAS

This section provides procedures for stopping cron jobs on either a Cisco Application Server or a MAS.

Stop the cron Jobs on the Cisco Application Server

1 In the xterm window, type **cd** and then press **Enter**. The home directory on the DNCS becomes the working directory.

Note: Alternatively, you can complete this procedure from a remote shell on the Application Server:

a In a DNCS xterm window, type **rsh appserver** and press **Enter**. This will open a remote shell on the Application Server.

b Proceed to step 2 and run the commands from the remote shell.

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

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

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

3 Type **pgrep -fl cron** and press **Enter**. The Application Server displays the cron process ID (PID).

4 Use the cron PID from step 3, and type **ptree <PID>** and press **Enter**. The Application Server displays the process tree of all cron processes.

5 Did the results from step 4 only include /usr/sbin/cron?

- If **yes**, type **svcadm -v disable -s cron** and press **Enter**.
- If **no**, (results from step 2 show multiple cron processes), **type kill -9 <PIDs>** and press **Enter**.

  Important: List the PIDs in reverse order.

  Example: kill -9 14652 14651 209
- If the results from step 4 did not show /usr/sbin/cron, then the cron jobs are already stopped.

6 Confirm that the cron jobs have stopped by typing **pgrep -fl cron** and press **Enter**. The command prompt should be the only item displayed; no processes should be displayed.

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

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

Note: Call Cisco Services for assistance if necessary.

Stop the cron Jobs on the Time Warner Mystro Application Server

If necessary, refer to the documents supplied by Mystro to stop the cron job on the MAS.

Stop Basic Backup or Auto Backup Servers

If the site you are upgrading uses the Auto Backup or Basic Backup server and if this server is configured to start a backup during the maintenance window, disable that backup or reschedule the backup for after the maintenance window.

A Note About Disaster Recovery Enabled DBDS Networks

If your DBDS is enabled for Disaster Recovery, you must perform all of the tasks in ***Process Overview*** (on page 92), ***Perform a Disaster Recovery Full Sync*** (on page 96), and ***Place Disaster Recovery Jobs on Hold*** (on page 99).

Note: If your DBDS is *not* enabled for Disaster Recovery, continue to the next section in this chapter.

Stop System Components

Introduction

CAUTION:

Do not continue with the procedures in this section unless you are within a maintenance window. Performing these procedures outside of a maintenance window may disrupt services.

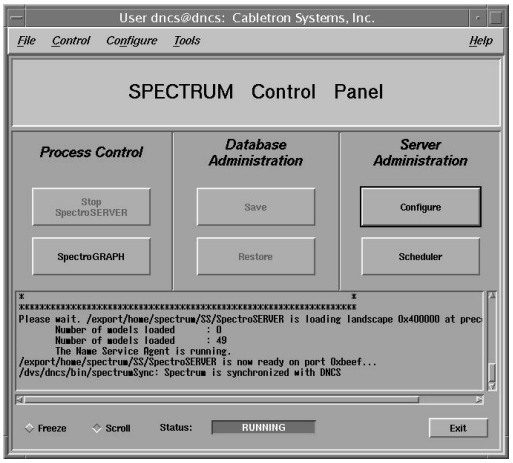
Before continuing with the installation process, follow the instructions in this section to stop system components.

Stop Third-Party Servers

Some sites use devices that mount drives on the DNCS or the Application Server. These devices are usually used to register files with the BFS. Be sure to stop these devices. Also, be sure to stop any third-party applications.

Stopping Spectrum

1. From the DNCS Administrative Console Status window, click **Control** in the NMS section of the window. The Select Host to run on window appears.
2. Select the appropriate **Host Machine** and then click **OK**. The Spectrum Control Panel appears.



3. Click **Stop SpectroSERVER**. A confirmation message appears.
4. Click **OK** at the confirmation message. The Status message on the Spectrum Control Panel shows **Inactive.**
5. Click **Exit** on the Spectrum Control Panel. A confirmation message appears.
6. Click **OK** at the confirmation message. The Spectrum Control Panel closes.

Stopping the RNCS Processes

Complete this procedure only if **Distributed DNCS** is licensed and you have active RNCS systems. Complete this procedure for each active RNCS.

1. From an xterm window on the DNCS, type **siteCmd <RNCS hostname> pgrep -fl dvs** and then press **Enter**.
2. Are the RNCS processes currently running?
   - If **yes**, go to step 3.
   - If **no**, go to *Stopping the Application Server, MAS, or Third-Party Server* (on page 47).
3. Type **siteCmd <RNCS hostname> lionnStop** and then press **Enter** to stop the RNCS processes.
4. Type **pgrep –fl dvs** and press **Enter**. The only remaining process should be **lionnInitd**.
5. Type **siteCmd <RNCS hostname> lionnKill** and then press **Enter**.
6. Type **siteCmd <RNCS hostname> pgrep –fl dvs** and then press **Enter** to confirm that all RNCS processes are stopped.
7. Are the processes on the RNCS stopped?
   - If **yes**, go ***to Stopping the Application Server, MAS, or Third-Party Server*** (on page 47).
   - If **no**, repeat steps 4 through 6. If the processes still do not stop, call the Cisco Services Video Technical Assistance Center (VTAC) for assistance.

Stopping the Application Server, MAS, or Third-Party Server

This section provides procedures for stopping either a Cisco Server, MAS, or third-party server. Choose the procedure that pertains to your system.

Stopping the Cisco Application Server

1. Press the middle mouse button on the Application Server and select **App Serv Stop**.

   Note: Alternatively, you can complete this procedure from the DNCS using a remote shell to the Application Server:

   a. In an xterm window on the DNCS, type **rsh appservatm** and press **Enter** to open a remote shell on the Application Server.

   b. Type **appStop** and press **Enter** to stop Application Server processes. It may take a few minutes for all processes to stop.

   c. Type **pgrep –fl dvs** and press **Enter**. The only Application Server processes still running should be appInitd.
2. Type **appKill** and then press **Enter**. The appInitd process stops.

Stopping the MAS

If necessary, refer to the documents supplied by Mystro to stop the MAS.

Preparing the Rovi Application Server

Refer to **Aptiv Technical Note Number 41**. Complete steps 1 through 3 to prepare the Rovi® Application Server for the service pack upgrade.

Note: Contact the Rovi Corporation for the latest copy of the technical note.

Stopping the DNCS

1. At the DNCS, press the middle mouse button and then select **DNCS Stop**. A confirmation message appears.
2. Click **Yes**.
3. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The Dncs Control utility window opens.
4. Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**. The system displays all DNCS processes.

   Note: The system updates the display periodically, or you can press **Enter** to force an update.
5. When the **Curr Stt** (Current State) field of the utility window indicates that all of the DNCS processes have stopped, follow the on-screen instructions to close the Dncs Control window.
6. Type **pgrep –fl dvs** and press **Enter**. Information similar to the following appears:

   ```
   633 /usr/sbin/dtrace -qws /dvs/dncs/etc/app_crash/app_crash_global.d
   919 -ksh -c /dvs/dncs/bin/dncsResMon
   23823 /dvs/dncs/bin/dncsInitd
   ```

   Note: There is no need to stop the dtrace, dncsResMon, or dncsInitd processes.

Ensure No Active Database Sessions on the DNCS

1. Close all windows and GUIs that are open except for the xterm window in which you are working.
2. Are you already logged on as root user in the xterm window on the DNCS?
   - If **yes**, go to step 4.
   - If **no**, go to step 3.
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 **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the correct user environment.

   Important:
   - Be sure to type the dot followed by a space prior to typing /dvs.
   - If **-0 bad options** message displays, ignore the message and go to step 5.
5. Type **/usr/ucb/ps -auxww | grep tomcat** and then press **Enter**. The system lists running processes that use the tomcat server.

   Sample Output - tomcat server (running):

```
$ /usr/ucb/ps -auxww | grep tomcat
dncs       247  0.1  3.2227576131184 ?        S   Dec 21 46:07
/usr/java/bin/java -Djava.util.logging.manager=org.apache.juli.ClassL
oaderLogManager -
Djava.util.logging.config.file=/usr/local/tomcat/conf/logging.properties -
Djava.endorsed.dirs=/usr/local/tomcat/com
mon/endorsed -classpath
:/usr/local/tomcat/bin/bootstrap.jar:/usr/local/tomcat/bin/commons-logging-
api.jar -Dcatalina.base=/usr/loca
l/tomcat -Dcatalina.home=/usr/local/tomcat -
Djava.io.tmpdir=/usr/local/tomcat/temp org.apache.catalina.startup.Bootstrap
start
dncs     14929  0.0  0.1 1312 1104 pts/4    S 08:02:16  0:00 grep tomcat
```

6. Is the tomcat server running?
   - If **yes**, type **/etc/rc2.d/S98tomcat stop** and then press **Enter**.
   - If **no**, go to step 7.
7. Type **/usr/ucb/ps -auxww | grep tomcat** and then press **Enter** to confirm that the tomcat server has stopped.

   Note: If the tomcat server is still running, repeat step 5.
8. Type **ps -ef | grep -i ui** and then press **Enter**. The system lists running UI processes.

9 Are any UI processes running (such as dbUIServer or podUIServer)?

- If **yes**, type **/dvs/dncs/bin/stopSOAPServers** and then press **Enter**.
- If **no**, go to step 13.

10 Type **ps -ef | grep -i ui** and then press **Enter** to confirm that all UI processes have stopped.

Note: If any UI processes are still running, type **/dvs/dncs/bin/stopSOAPServers** again and then press **Enter**.

11 Type **ps -ef | grep -i ui** and then press **Enter** to confirm that UI process have stopped.

12 Are any UI processes still running?

- If **yes**, type **kill -9 [PID]** and then press **Enter** for any UI process that is still running.

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

- If **no**, go to step 13.

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

Result: One of the following messages appears:

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

14 Did the message in step 13 indicate that there are active database sessions?

- If **yes**, complete these steps:
  - **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 database sessions?
    - If **yes**, call Cisco Services.
    - If **no**, go to step 15.
- If **no**, go to step 15.

15 Type **dncsKill** and then press **Enter**. The system terminates if the dncsInitd process is still running.

16 Wait a few moments, and then type **ps -ef | grep dncsInitd** and press **Enter**. The system reports whether the dncsInitd process is still running.

17 Is the dncsInitd process still running?

- If **yes**, then repeat this procedure from step 15 until the process stops running, then go to the installation procedures.
- If **no**, go to the installation procedures.

3

SR 2.7/3.7/4.2 SP4 Installation Procedures

Introduction

In this chapter, you will install the new software for the DNCS and the graphical and Web user interfaces (GUI and WUI) for the DNCS.

Note: If you followed the procedures in Chapter 2 correctly, all of the system components have been stopped. Additionally, you should still be logged on to an xterm window on the DNCS as root user.

Important: Do not attempt to perform the procedures in this chapter more than once. If you encounter any problems while upgrading the DNCS, contact Cisco Services at 1-866-787-3866.

In This Chapter

Reboot the TED

Note: If you have correctly followed all instructions to this point, you should still be logged on as root user in an xterm window on the DNCS.

1 Type one of the following commands to connect to the TED:

- For a TEDFX, type **rsh dncsted**.
- For a TED III, type **ssh dncsted**.

Result:

```
Last login: Tue Nov 24 11:26:53 from dncsted-x
You have new mail.
[root@dncsted /root]#
```

2 Type **shutdown -r now** at the [root@dncsted /root]# sign to reboot the TED.

3 Wait 5 minutes for the TED to reboot.

4 Type one of the following commands to verify that you can connect to the TED and that the TED has rebooted:

- For a TEDFX, type **rsh dncsted**.
- For a TED III, type **ssh dncsted**.

Install the Service Pack

Note: If you have correctly followed all instructions to this point, you should still be logged on as root user in an xterm window on the DNCS.

1 Insert the DBDS Service Pack CD into the CD drive of the DNCS. The system automatically mounts the CD within 30 seconds.

2 Is the File Manager window open?

- If **yes**, select **File** and choose **Close**, then go to step 3.
- If **no**, go to step 3.

3 Type **df -n** and then press **Enter**. A list of the mounted file systems appears.

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

4 Type **cd /cdrom/cdrom0** and press **Enter**. The /cdrom/cdrom0 becomes the working directory.

5 Type **./install_patch** and press **Enter**. A list of packages displays.

Example:

```
# ./install_patch


Checking the system, please wait...
*********************************************************************
This script will install the following packages on:
DNCS Server (vod2)
------------------------
SAIdncs             DNCS 08-25-11
                    4.2.0.50p11


SAIgui              DNCS GUI 08-25-11
                    4.2.0.50p11
*********************************************************************
Are you SURE you want to continue?  [y,n,?,q] y
```

6 Type **y** and press **Enter**. The software begins to install on the DNCS.

7 Type **cd** and press **Enter** to make the root directory the working directory.

8 Type **eject cdrom** and then press **Enter** when the installation is complete.

9 Check the log file for errors.

Notes:

- The installation log files are in the **/var/sadm/system/logs** directory on the DNCS. Each package will have its own log file.

  Example:

  – SAIdncs_4.2.0.50p11_install.log

  – SAIgui_4.2.0.50p11_install.log

- Call Cisco Services for assistance if the log file reveals errors.

Install Additional Software

We may have provided you with additional software, such as a patch, to install after you have finished installing all of the software components. If this is the case, install the additional software now using the instructions provided with the software. These instructions may be either a written document or bundled with the software as a readme file. These instructions provide step-by-step procedures to install the additional software.

After installing any additional software, go to ***Check the Installed Software Version*** (on page 56).

A Note About Disaster Recovery Enabled DBDS Networks

If your DBDS is enabled for Disaster Recovery, you must install all Disaster Recovery triggers, stored procedures, and tables. See ***Install Disaster Recovery Triggers, Stored Procedures, and Tables*** (on page 100) for instructions.

Note: If your DBDS is *not* enabled for Disaster Recovery, continue to the next section in this chapter.

Check the Installed Software Version

Introduction

Use *pkginfo*, a Solaris software management tool, to verify installed software versions on the DNCS and the Application Server. Use the **Version** field and the **Status** field of the output produced by *pkginfo* to obtain the information you need. If the Status field indicates that the software is not completely installed, contact Cisco Services at 1-866-787-3866 for assistance.

Note: Running the Doctor report with the *–g* option also displays installed software versions.

Verifying DNCS Versions

Complete the following steps to verify the installed software versions on the DNCS.

1 Insert the Maintenance CD.

2 Type **cd /cdrom/cdrom0/sai/scripts/utils** and then press **Enter**. The working directory is now /cdrom/cdrom0/sai/scripts/utils.

3 From an xterm window on the DNCS, type **./listpkgs -i** and then press **Enter**. The system displays the package and version installed for each package.

4 Record the version number in the Actual Results column of the accompanying table for each Package Name you check.

Component	Pkg Name	Expected Results	Actual Results
DNCS Application	SAIdncs	4.2.0.50p11	
DNCS GUI	SAIgui	4.2.0.50p11	
Service Pack	SAISP	SR_4.2_SP3C11*	

*__Note__: The SAISP package version was not changed in this release because it was treated as a patch. For this reason, SAISP will be displayed as **SR_4.2_SP3C11** even after the upgrade.

5 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 4?

- If **yes**, go to ***Enable Optional and Licensed Features*** (on page 57) for Aptiv sites or Add an EAS Variable to the .profile File for SARA sites.
- If **no**, call Cisco Services and inform them of the discrepancy.

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

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.

Enable the RNCS (Optional)

If you have an RNCS and have followed these instructions fully, complete the RNCS upgrade process now. Complete steps 25 through 35 in Chapter 2 of the *RNCS Installation and Upgrade Instructions For SR 2.7/3.7 or SR 4.2* (part number 4012763).

After the RNCS Upgrade

After the RNCS upgrade, complete the following tasks:

1. Back up RNCS files.
   - **a** Type **cd /dvs/dncs/bin** and press **Enter**.
   - **b** Type **cp -p tsbroadcasterclientapi.jar tsbroadcasterclientapi.jar.SP4** and press **Enter**.
   - **c** Type **cp -p TSBroadcasterClient.jar TSBroadcasterClient.jar.SP4** and press **Enter**.
2. Put the preSP4 files back in place.
   - **a** Type **cp -p tsbroadcasterclientapi.jar.preSP4 tsbroadcasterclientapi.jar** and press **Enter**.
   - **b** Type **cp -p TSBroadcasterClient.jar.preSP4 TSBroadcasterClient.jar** and press **Enter**.
3. Compare /export/home/informix/etc/onconfig to /export/home/informix/etc/onconfig.preSP4 to ensure that nothing has changed. If something has changed, enter the following commands:
   - **a** Type **cp -p /export/home/informix/etc/onconfig /export/home/informix/etc/onconfig.SP4** and press **Enter**.
   - **b** Type **cp -p /export/home/informix/etc/onconfig.preSP4 cp /export/home/informix/etc/onconfig** and press **Enter**.

Restart the System Components

Introduction

After installing this software, follow these instructions to restart the system components.

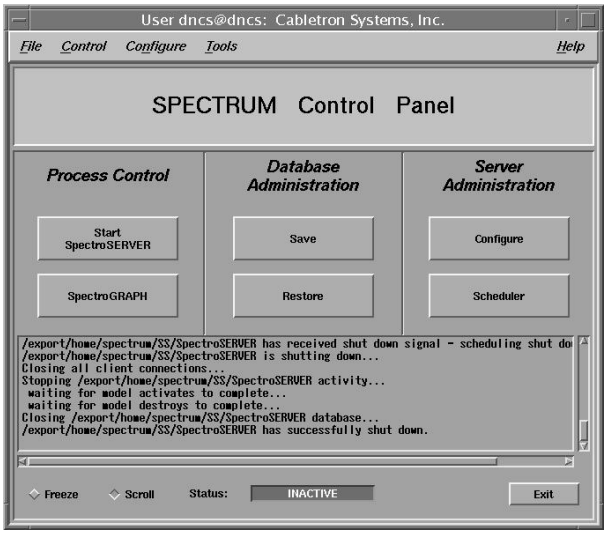
Important: If a patch was provided, be sure you have installed the patch and completed the instructions that accompanied it. Then go to ***Check the Installed Software Version*** (on page 56) and complete the instructions there before restarting the system components.

Restarting Spectrum

Important: Skip this procedure if you are using DBDS Alarm Manager instead of Spectrum.

1 From the DNCS Administrative Console Status window, click **Control** in the NMS section of the window. The Select Host to run on window opens.

2 Select the appropriate **Host Machine**, and then click **OK**. The Spectrum Control Panel window opens.



3 On the Spectrum Control Panel window, click **Start SpectroSERVER**. The Spectrum Network Management System starts.

4 On the Spectrum Control Panel window, click **Exit**. A confirmation message appears.

5 Click **OK** on the confirmation message. The Spectrum Control Panel window closes.

Disable the SAM Process on Rovi and MDN/ODN Systems

If the site you are upgrading uses the Aptiv or MDN/ODN application server, you need to disable the SAM process before you restart the system components. Complete the following steps to disable the SAM process.

Notes:

- If the site you are upgrading does not use the Aptiv or MDN/ODN application server, skip this procedure and go to ***Restart the System Components*** (on page 59).
- You should be logged on to the DNCS as **dncs** user.

Prerequisites

Before disabling the SAM process, make sure that the following have been completed:

- You should be logged on to the DNCS as **dncs** user.
- The SaManager process is stopped and not running.

Disable the SAM Process on Aptive Systems

1. In the DNCS section of the DNCS Administrative Console Status window, click **Control**. The DNCS Monitor window opens.
2. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The DNCS Control window opens.
3. Type **4** (for Define/Update Grouped Elements) and then press **Enter**. The window updates to list a series of element groups.
4. Type **14** (for saManager) and then press **Enter**. The window updates to list the elements in the group.
5. Type **1** (for /dvs/dncs/bin/saManager) and then press **Enter**. The first in a series of confirmation messages appears.
6. Press **Enter** at each confirmation message to accept the default setting until a message about **cpElmtExecCtrlStatus** appears. In total, you should see about six confirmation messages.
7. At the cpElmtExecCtrlStatus message, type **2** (for Disabled) and then press **Enter**. A confirmation message appears.
8. Type **y** (for yes) and then press **Enter**. The message **Element Definition was Modified** appears.
9. Follow the on-screen instructions to exit from the DNCS Control window.

If the site you are upgrading uses the Aptiv or MDN/ODN application server, you need to disable the SAM process before you restart the system components. Complete the following steps to disable the SAM process.

Note: If the site you are upgrading does not use the Aptiv or MDN/ODN application server, skip this procedure and go to *Restart the System Components* (on page 59).

Restarting the DNCS

1. From an xterm window on the DNCS, type **exit** and then press **Enter** to log out the root user.
2. Type **dncsStart** and press **Enter**. The Informix database, the SOAPServers, and DNCS processes start.
3. Click the middle mouse button on the DNCS and select **Administrative Console**. The DNCS Administrative Console opens.
4. 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.
5. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The DNCS Control utility window opens.
6. 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.
7. Wait for the DNCS Control window to list the current status (Curr Stt) of all the processes and servers as **running**.

   Notes:

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

Restarting the RNCS Processes

Complete this procedure only if **Distributed DNCS** is licensed and you have active RNCS systems. Complete this procedure for each active RNCS.

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

   ```
   siteCmd <RNCS hostname> lionnStart
   ```

   Note: Replace <RNCS hostname> with the hostname of the RNCS.
2. Wait a few moments and then type the following command and press **Enter** to verify that all of the RNCS processes have started.

   ```
   siteCmd <RNCS hostname> pgrep -fl dvs
   ```

Restarting the Application Server or MAS Server

This section provides procedures for restarting either a Cisco Application Server, MAS, or third-party server. Choose the procedure that pertains to your system.

Restarting the Application Server at SARA Sites

1. Press the middle mouse button on the Application Server and select **App Serv Start**.

   Note: Alternatively, you can complete this procedure from a remote shell on the Application Server:

   a. In a DNCS xterm window, type **rsh appserver** and press **Enter**. This will open a remote shell on the Application Server.

   b. Proceed to step 2 and run the commands from the remote shell.

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.

Preparing the Aptiv Application Server for the Service Pack

Refer to **Aptiv Technical Note Number 41**. Complete steps 6 through 14 to restart the Aptiv Application Server after the upgrade is complete.

Note: Contact Aptiv Digital for the latest copy of the technical note.

Restarting the Time Warner Mystro Application Server

If necessary, refer to the documents supplied by Mystro to restart the MDN.

Restart the Billing and Third-Party Interfaces

Contact your billing vendor to restart the billing interface. If you stopped any third-party interfaces during the pre-upgrade process, restart those interfaces now. Additionally, examine the dncs and root crontab files for any third-party interfaces that were scheduled to start during the installation process while the system components were stopped. Restart these interfaces, as well.

Restart the cron Jobs

Restart the cron Jobs on the DNCS

1. If necessary, open an xterm window on the DNCS.
2. Confirm that the cron jobs are not running by typing **ps -ef | grep cron** and press **Enter**.
3. Have the cron jobs restarted on their own?
   - If **yes**, skip the rest of this procedure and go to ***Restart the cron Jobs on the Application Server*** (on page 64).
   - If **no**, go to step 4.
4. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
5. Type **svcadm -v enable -rs cron** and press **Enter**. The system restarts all cron jobs.
6. Confirm that the cron jobs have restarted by typing **ps -ef | grep cron** and press **Enter**. The system should list **/usr/sbin/cron**.

Restart the cron Jobs on the Application Server

Important: This procedure pertains to the Cisco Application Server only. If the site you are upgrading supports the Aptiv Digital Application Server, contact Aptiv Digital for the appropriate procedure.

1. If necessary, open an xterm window on the Application Server.
2. Confirm that the cron jobs are not running by typing **ps -ef | grep cron** and press **Enter**.

   Note: If you see the cron jobs running, then the cron jobs may have restarted on their own when you booted the Application Server.
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 **svcadm -v enable -rs cron** and press **Enter**. The system restarts all cron jobs.
5. Confirm that the cron jobs have restarted by typing **ps -ef | grep cron** and press **Enter**. The system should list /usr/sbin/cron.
6. Type **exit** and press **Enter** to log out as root user.

Restart the cron Jobs on the MAS Server

If necessary, refer to the documents supplied by Mystro to restart the cron jobs on the MAS server.

4

Post-Upgrade Procedures

Introduction

Follow the procedures in this chapter to complete the upgrade process.

In This Chapter

Check the EAS Configuration—Post Upgrade

You now need to verify that your EAS equipment is working correctly by testing the system's ability to transmit EAS messages. Complete all of the procedures in the **Conduct EAS Tests** chapter of *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455). After completing the procedures in that chapter, verify an EAS message is generated from the Emergency Alert Controller (EAC).

Check BFS QAM Sessions

Introduction

After you obtain your system configuration, your next step is to check the BFS QAM for the number of sessions and to remove any completed or orphaned sessions. This check enables you to compare the number of sessions before and after the installation process is complete, and indicates a successful upgrade if an equal number of sessions are built after the upgrade process is complete.

Verifying the Number of Recovered BFS Sessions

Complete the following steps to check the number of post-upgrade BFS sessions.

1 Choose one of the following options to check the number of BFS sessions:

- Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.
- Type **/dvs/dncs/bin/auditQam -query <IPAddr> <output port number>** and press **Enter**.

  Example: /dvs/dncs/bin/auditQam -query 172.16.1.101 3

  Notes:

  – <IPAddr> is the IP address of the data QAM or GQAM.
  – The output port number for a QAM is 2.
  – The output port number for a GQAM is 1-16.

2 Does the **Session Count** total equal the value you recorded in Checking the BFS Sessions on the BFS QAM or GQAM?

- If **yes**, go to step 3.
- If **no**, go to ***Tearing Down the BFS and OSM Sessions*** (on page 70).

3 Does the **Program Count** total equal the value you recorded in Checking the BFS Sessions on the BFS QAM or GQAM?

- If yes, go to step 4.
- If no, then some sessions may be in the clear that should be encrypted. Contact Cisco Services for assistance.

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

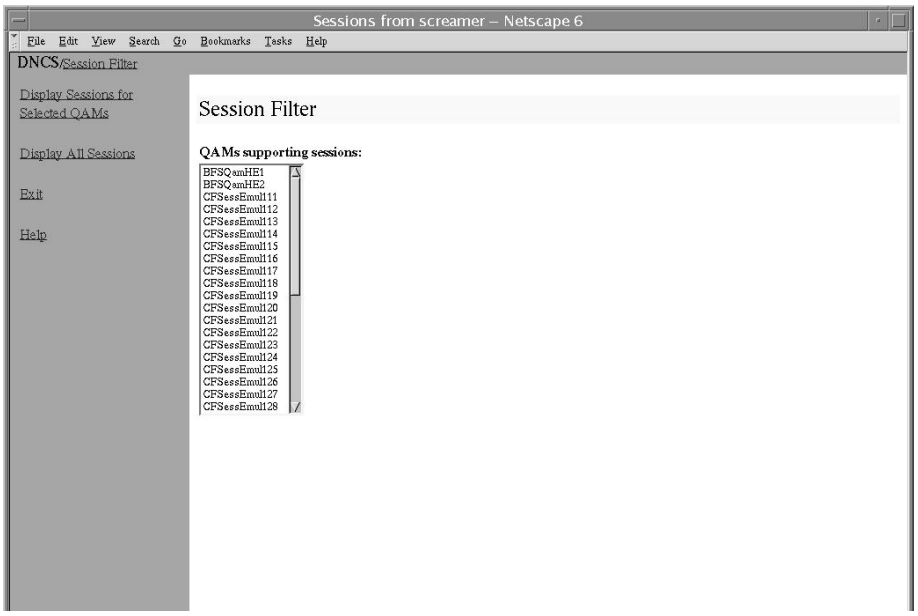
5 Verify that the Active Stream total equals the number of streams you recorded in Checking the BFS Sessions on the BFS QAM or GQAM.

6 If the pre-upgrade stream total matches the post-upgrade stream total, *skip the next section* and go to ***Verifying a Successful Installation*** (on page 72).

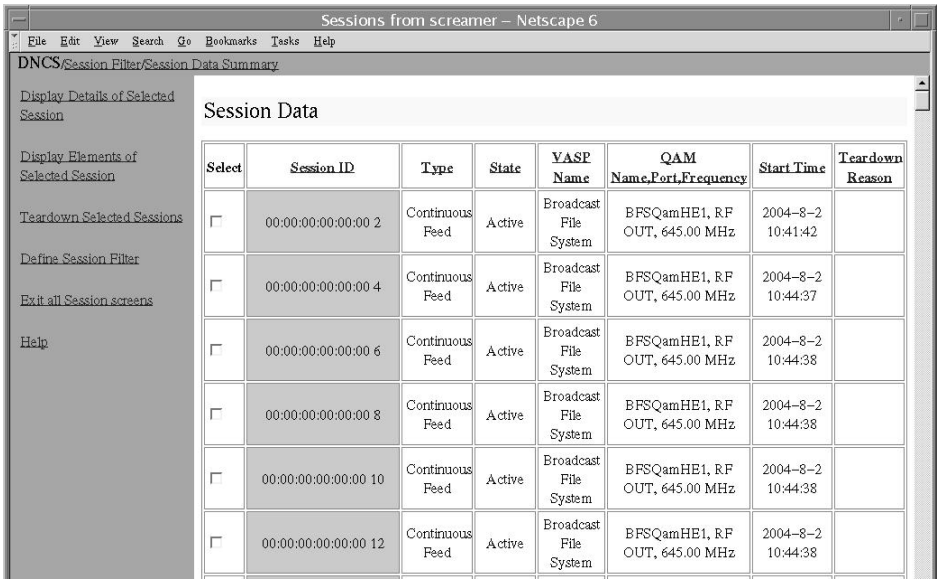
Tearing Down the BFS and OSM Sessions

Complete the following steps to tear down the BFS and OSM sessions in order to return the BFS session count to the expected number of sessions.

1. On the DNCS Control window, highlight the **osm** process**.**
2. Click **Process** and then select **Stop Process**. In a few minutes, the indicator for the osm process changes from green to red.
3. Highlight the **bfsServer** process.
4. Click **Process** and then select **Stop Process**. In a few minutes, the indicator for the bfsServer process changes from green to red.
5. On the DNCS Administrative Console, select the **DNCS** tab and go to **Utilities**.
6. Click **Session List**. The Session Filter window opens.



7. Select the BFS QAM from the Session Filter list and then click **Display Sessions for Selected QAMs**. The Session Data window opens.



8 In the **Select** column, check the box associated with each BFS/OSM session.

9 Click **Teardown Selected Sessions**. The system tears down the BFS and OSM sessions.

10 On the DNCS Control window, highlight the **bfsServer** process.

11 Click **Process** and then select **Start Process**. In a few minutes, the indicator for the bfsServer process changes from red to green.

12 After the indicator for the bfsServer process has turned green, highlight the **osm** process.

13 Click **Process** and then select **Start Process**. In a few minutes, the indicator for the osm process changes from red to green.

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

15 Wait about 10 minutes for the system to rebuild the sessions.

16 Does the **Session Count** total now equal the number of sessions you recorded in the Checking the BFS Sessions on the BFS QAM or GQAM procedure?

- If **yes**, go to ***Verifying a Successful Installation*** (on page 72). The system has recovered all of the BFS sessions.
- If **no**, call Cisco Services for assistance.

Verifying a Successful Installation

1. Complete the following steps to perform a slow boot and a fast boot on a 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. Power to the DHCT is turned on.

   e. Access the Power On Self Test and Boot Status diagnostic screen on the DHCT.

   f. Do all of the parameters, including UNcfg, display **Ready**?

      – If **yes,** go to step 2.

      – If **no**, contact Cisco Services.
2. Ping a test DHCT.
3. Did the DHCT receive the ping?
   - If **yes**, go to step 4.
   - If **no**, call Cisco Services.
4. Stage at least one new DHCT to the system operator's specifications.
5. After staging, did the DHCT successfully load the current client release software?
   - If **yes**, go to step 6.
   - If **no**, call Cisco Services for assistance.
6. Did the DHCT receive at least 33 EMMs (Entitlement Management Messages) and successfully receive its Entitlement Agent?
   - If **yes**, go to step 7.
   - If **no**, call Cisco Services for assistance.
7. Does the IPG display 7 days of valid and accurate data?
   - If **yes**, go to step 8.
   - If **no**, call Cisco Services for assistance.
8. Do the PPV barkers appear on the PPV channels correctly?
   - If **yes**, go to step 9.
   - If **no**, call Cisco Services for assistance.

9 Do third-party applications load and run properly?

- If **yes**, go to step 10.
- If **no**, call Cisco Services for assistance.

10 Can test DHCTs buy a VOD and/or an xOD program?

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

11 Boot a DHCT and look at Statuses and Network Parameter Diagnostic Screen. Is the Hub ID number displayed?

- If **yes**, go to step 12.
- If **no**, call Cisco Services for assistance.

12 If applicable, are the SDV channels available?

- If **yes**, the BRF is successfully authorized and you have completed the upgrade.
- If **no**, call Cisco Services for assistance.

Authorize the BRF as a BFS Server (Optional)

Introduction

In systems that use a DOCSIS® return path for DHCT communications, there is no support in the cable modem termination system (CMTS) for the downstream channel descriptor (DCD). These systems need a Bridge Resolution File (BRF) to use as a BFS server in order to enable DHCTs to discover their hub ID and MAC layer multicast address. After an upgrade, the system does not automatically authorize the creation of the BRF as a BFS server; you must authorize the file creation manually. Follow these instructions to inspect the BFS GUIs for the presence of the BRF and then to authorize the file, if necessary.

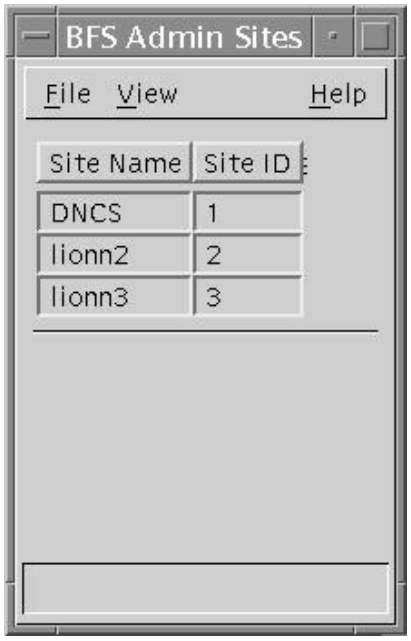
Authorizing the BRF

Complete the following steps to check for the BRF and then to authorize the file, if necessary.

1 From the DNCS Administrative Console, select the **Application Interface Modules** tab.

2 Is your site running Regional Network Control System (RNCS)?

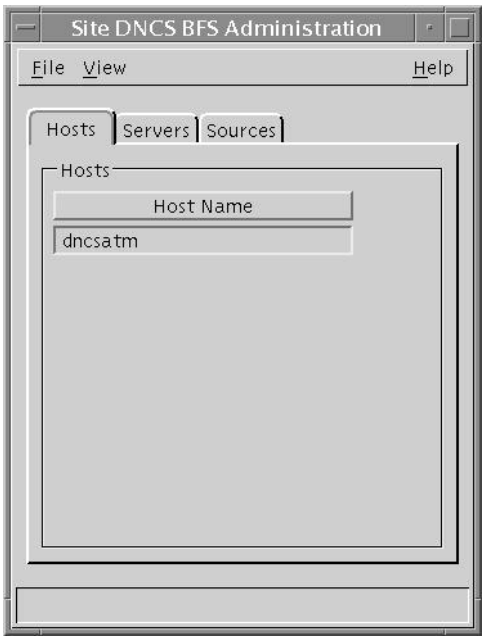
a If **yes**, click **BFS Admin**. The BFS Admin Sites window opens.



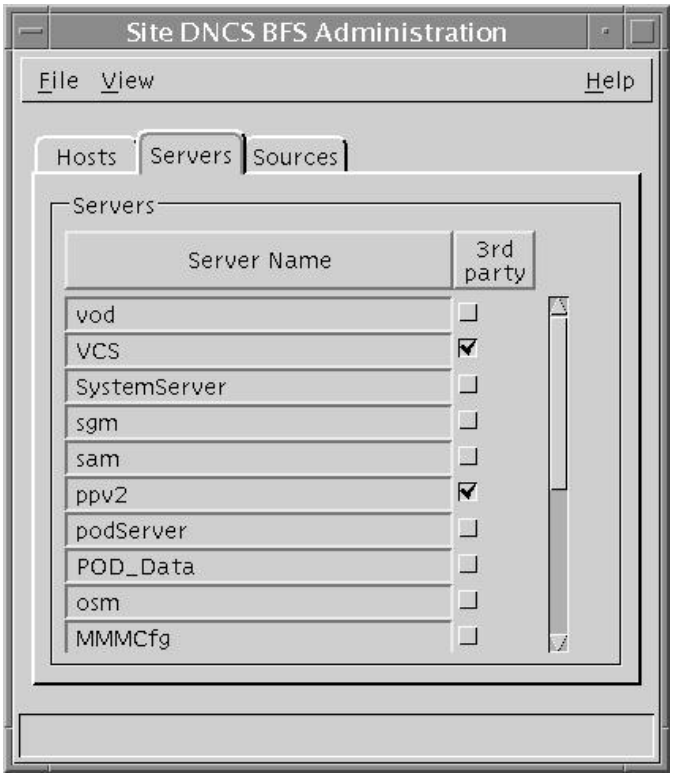
b If **no**, go to step 3.

3 Double-click **DNCS**.

Note: This procedure does not apply to remote sites. The Site DNCS BFS Administration window appears.



4 Click the **Servers** tab. A list of servers appears.



5 Does **brf** appear in the **Server Name** column?

- If **yes**, click **File** and then select **Close** to close the Site DNCS BFS Administration window. You have completed this procedure; go to Final System Validation Tests.

  Note: The BRF is already authorized as a BFS server.

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

Note: Use the scroll bar to see the entire list.

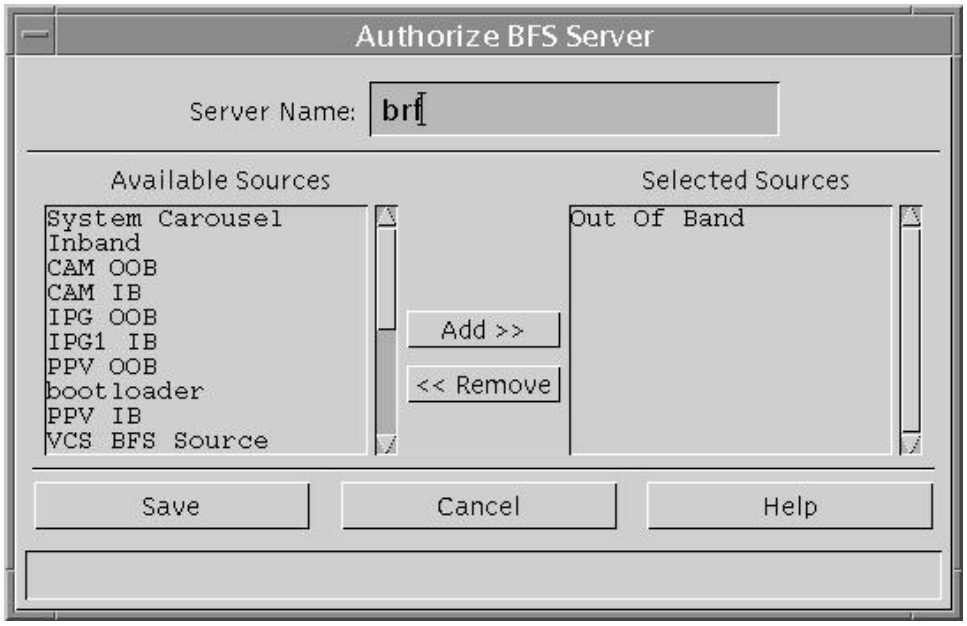
6 Click **File** and then select **New**. The Authorize BFS Server window appears.

7 Complete the following steps to configure the Authorize BFS Server window.

a Type **brf** in the **Server Name** text box.

b In the **Available Sources** column, highlight **Out of Band** and then click **Add**. The Out of Band source moves to the **Selected Sources** column.

Example: The Authorize BFS Server window should look similar to the following example when you are finished.



8 Click **Save**. The system saves the newly authorized BRF.

9 Click **File** and then select **Close** to close the Authorize BFS Server window.

10 Go to Final System Validation Tests.

Remove Scripts That Bounce the Pass-Through Process

In order to correct some issues associated with the Pass-Through process on the DNCS, some sites have been regularly bouncing this process through scripts that reside in the crontab file. This software corrects issues associated with the Pass-Through process. Therefore, after the upgrade, you should remove any entries in the crontab file that reference scripts that bounce the Pass-Through process. The instructions in this section guide you through the process of removing these references.

Notes:

- Bouncing a process refers to stopping and then restarting that process.
- The scripts that were written to bounce the Pass-Through process are called **elop** and **bouncePassThru**.

Removing Scripts That Bounce the Pass-Through Process

Complete the following steps to remove entries from the crontab file that reference scripts that bounce the Pass-Through process.

1. If necessary, open an xterm window on the DNCS.
2. Follow these instructions to check on the presence of scripts in the crontab file that bounce the Pass-Through process.
   a. Type **crontab -l | grep -i elop** and then press **Enter**. The system lists the line(s) within the crontab file that contain elop scripts.
   b. Type **crontab -l | grep -i bouncePassThru** and then press **Enter**. The system lists the line(s) within the crontab file that contain bouncePassThru scripts.
3. Did the output of step 2 contain any references to the elop or the bouncePassThru scripts?
   - If **yes**, go to step 4 to remove those references.
   - If **no**, go to ***Back Up The System Components*** (on page 79).

     Note: You do not have to remove any references to the scripts from the crontab file.
4. Type **crontab -l > /tmp/dncs.crontab** and then press **Enter**. The system redirects the contents of the crontab into dncs.crontab.

   Note: While you can edit the crontab directly, we recommend that you first redirect the contents of the crontab to dncs.crontab so you can recover the original crontab if necessary.

5 Type **vi /tmp/dncs.crontab** and then press **Enter**. The dncs.crontab file opens for editing using the vi text editor.

6 Remove all lines from the dncs.crontab file that reference the elop or bouncePassThru scripts.

7 Save the dncs.crontab file and close the vi text editor.

8 Type **crontab /tmp/dncs.crontab** and then press **Enter**. The just-edited dncs.crontab file becomes the crontab file.

Back Up the System Components

Reference Backup Procedures

After a successful system upgrade, it is important to perform an additional system backup to ensure that your site has a solid backup of the new SR.

Reference the following sections of this document for information about backup procedures:

- For the DNCS and Application Server File Systems - see ***Back Up the DNCS and Application Server File Systems*** (on page 35)
- For the Informix database - see ***Back Up the Informix Database*** (on page 41)

5

Customer Information

If You Have Questions

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

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

A

System Release Rollback Procedures

Introduction

This appendix contains the procedures for rolling back the Enterprise 450 or Sun Fire V880 DNCS.

Prior to executing these rollback procedures, contact Cisco Services at 1-866-787-3866.

In This Appendix

Roll Back the Enterprise 445/450 or Sun Fire V880/V890 DNCS

Introduction

If your upgrade is unsuccessful, you may need to use the procedures in this section to restore your system to its condition prior to the upgrade and then to reattach disk mirroring on the DNCS.

Important: Be sure to notify Cisco Services before concluding that an upgrade has failed and before following any of the procedures in this section. In many cases, Cisco Services can help you easily resolve the problems related to the failed upgrade. In addition, the procedures in this section apply only if you have not yet completed the Re-Enable the Disk Mirroring Function. If you have already enabled disk-mirroring on the DNCS, you will have to restore your system using your latest file system and database backup tapes.

Rolling Back the DNCS

Follow these instructions to roll back the DNCS from an unsuccessful upgrade to your previous DNCS release.

Note: You need to be at the CDE Login window to begin this procedure. If you are unable to get to the CDE Login window, call Cisco Services for assistance.

1. If necessary, open an xterm window on the DNCS.
2. In ***Stop System Components*** (on page 46), use these procedures, if necessary.
   a. Stopping the Application Server
   b. Stopping the DNCS
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 SR4.2 SP4 CD in the drive on the DNCS.

   Note: If the File Manager window opens, you can close it.
5. Type **cd /cdrom/cdrom0** and press **Enter**. The /cdrom/cdrom0 directory becomes the working directory.
6. Type **ls -la** and press **Enter**. The system lists the contents of the CD.
7. Did the system list the contents of the CD as expected?
   a. If **yes**, skip the next step and go to step 9.
   b. If **no**, the CD might be defective. Go to step 8.

8 Type **y** and then press **Enter**. A message appears that seeks permission to reboot the server.

9 Type **./backout_patch SAIgui SAIdncs** and press **Enter**. A list showing the packages that will be backed out is displayed.

Example:

```
# ./backout_patch SAIgui SAIdncs
Checking the system, please wait...
Checking for existing packages and saved data...
************************************************************************
This script will backout the following packages on:
DNCS Server (vod2)
-------------------------
SAIgui              DNCS GUI 08-25-11
                    4.2.0.50p11


SAIdncs             DNCS 08-25-11
                    4.2.0.50p11
************************************************************************
Are you SURE you want to continue?  [y,n,?,q] y
```

Results: Both SAIgui and SAIdncs packages are backed out.

10 Type **pkginfo -l SAIdncs** and press **Enter**. The system displays the version of the software now installed on the DNCS. Verify the pre-upgrade versions are installed.

11 Backout logs are in **/var/sadm/system/logs**. Review the backout logs for SAIdncs and SAIgui for any errors.

12 Re-start the DNCS, Application Server and RNCS processes.

- **a** Type **dncsStart** and press **Enter** in an xterm on the DNCS. The DNCS processes start.
- **b** If your system uses a Cisco Application server, type **appStart** and press **Enter** in an xterm on the Application Server. The Application Server processes start. Otherwise, refer to the documents supplied by the vendor of your Application server to stop Application Server processes.
- **c** If you have Distributed DNCS licensed and active RNCS systems, type **siteCmd <lionn hostname> lionnStart** and press **Enter** in a DNCS xterm.

13 Verify system functionality.

B

How to Determine the Tape Drive Device Name

Introduction

Chapter 2 of this guide requires that you back up the DNCS file system and database before upgrading the system. The procedure to back up these files requires that you know the device name of the tape drive of the DNCS.

If you are unsure of the device name of the tape drive in the DNCS or simply wish to confirm the device name, the procedure in this appendix will help you determine the device name.

In This Appendix

Determine the Tape Drive Device Name

Use this procedure if you need to determine the device name of the tape drive used by your DNCS.

Notes:

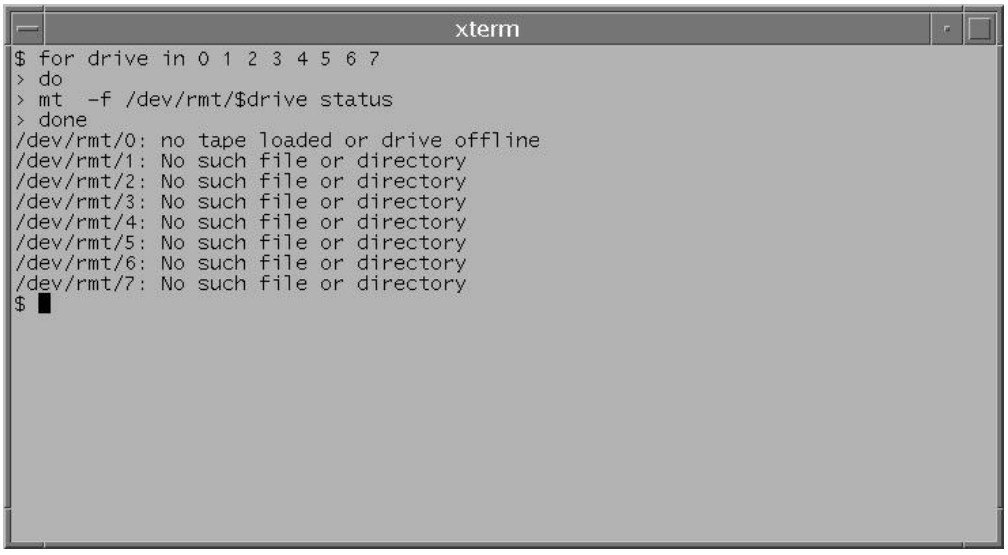
- You will only have to complete this procedure once. The device name of your tape drive will not change unless you specifically change the tape drive configuration.
- Do not have a tape in the tape drive when you complete this procedure.

1. If necessary, open an xterm window on the DNCS.
2. Ensure that no tape is currently in your tape drive.
3. Type the following UNIX routine. The system checks the status of eight possible tape drive configurations and displays the results.

   Important: Type the routine just as shown by pressing **Enter** at the end of each line.

   ```
   For drive in 0 1 2 3 4 5 6 7
   do
   mt  -f  /dev/rmt/$drive status
   done
   ```

   Note: Your system will display results similar to the following example.



4 Examine your results and use the following observations, based upon the example used in step 3, to determine the device name of your tape drive:

- In the example in step 3, no tape drives are detected in /dev/rmt/1 through /dev/rmt/7 (as indicated by **No such file or directory**). Therefore, you can conclude that /dev/rmt/1 through /dev/rmt/7 are not valid device names for tape drives on the system queried in step 3.
- In the example in step 3, a tape drive is detected in /dev/rmt/0 and the system accurately notes that no tape is loaded. Therefore, you can conclude that the device name of the tape drive on the system queried in step 3 is /dev/rmt/0.
- If /dev/rmt/1 is the device name of your tape drive, then **no tape loaded or drive offline** would appear next to /dev/rmt/1.

5 Write the device name of your tape drive in the space provided.

_____

C

Perform a DNCS Upgrade in a Disaster Recovery Enabled Network

Introduction

Use the procedures in this appendix to perform a DNCS upgrade on Disaster Recovery enabled DBDS networks.

Note: If your DBDS is *not* enabled for Disaster Recovery, disregard the procedures in this appendix.

In This Appendix

Process Overview

The following provides an overview of the tasks completed as part of the Disaster Recovery upgrade process.

1. Perform a Disaster Recovery Full Sync. See ***Perform a Disaster Recovery Full Sync*** (on page 96).
2. Place all Disaster Recovery jobs on hold. See ***Place Disaster Recovery Jobs on Hold*** (on page 99).
3. Upgrade the Standby DNCS.
4. Re-install the Disaster Recovery triggers and tables. See ***Install Disaster Recovery Triggers, Stored Procedures, and Tables*** (on page 100).

   Note: This step can be completed immediately following the DNCS database conversion step, bldDncsDb, of the DNCS upgrade process.
5. Log in to the Active monitoring computer (MC) on the Disaster Recovery platform via command-line.
6. On the Active MC, type:

   a **cd /export/home/dradmin/dr/app/ui/webroot/reg/engine**

   b **./test_buildRoutes.php**

   Note: This step sets up all of the necessary network routes on the Standby DNCS. The routes are configured to send the DNCS-generated network traffic for the emulated QAM modulators and Netcrypts to the Standby MC, the local BFS Data QAM, Test QPSK modulator, and Test DHCT network traffic to the local standby DBDS isolation network switch, and the production QPSK modulators and DHCT network traffic to the Disaster Recovery bit-bucket (the default bit-bucket address is defined as 192.168.1.4).
7. Run a DNCS Doctor report and analyze it for issues/anomalies. The production QPSK modulators and their respective RF subnets will not be reachable and will be logged as failures in the Doctor PING report due to the re-direction of the QPSK mod and DHCT traffic into the Disaster Recovery bit-bucket.
8. Verify via the Standby DBDS System Test Hub that a DHCT can boot and can receive advanced services (VOD, IPG, xOD, SDV, etc.). You will want to boot and verify SARA, Aptive/Pioneer, and MDN/ODN DHCTs if you have them. This is the time to troubleshoot any issues discovered on the Standby DBDS system.

9 Take all of the Disaster Recovery jobs off of hold. See ***Take Disaster Recovery Jobs Off Hold*** (on page 102).

Note: Verify that Disaster Recovery Near Real Time Syncs and Periodic Syncs are successful. These two syncs will keep the data between the Primary DNCS and Standby DNCS synchronized until the maintenance window opens and the Disaster Recovery Switch-Over is performed. It is strongly recommended that the customer not modify any of the DBDS elements (QAMs, QPSKs, Netcrypts, etc.) as well as no modification of the logical DBDS entities (channel maps, sources, services etc.). The Disaster Recovery Near Real Time Sync and Periodic Sync processes will only keep DHCT-related data/configs and Impulse Pay-Per-View events and purchase data synchronized between the Primary DNCS and Standby DNCS.

10 Customer needs to make Go/No-Go decision regarding whether to proceed with the Switch-Over to the Standby DNCS during the next maintenance window.

11 Perform a Disaster Recovery Switch-Over. This process makes the Standby DNCS the Active DNCS and the Primary DNCS the Inactive DNCS.

12 Verify that the Switch-Over was successful by:

a Verifying that the correct network switch ports on the Primary DBDS isolation network switch are down and that the correct network switch ports on the Standby DBDS isolation network switch are up.

b Verifying that the Disaster Recovery "bit-bucket" and "QAM emulation gateway" are no longer present in the Standby DNCS routing table. The bit-bucket IP address is 192.168.1.4 and the "QAM emulation gateway" address is the Standby MC IP address.

- netstat -rvn |grep 192.168.1.4

Note: You should not see any occurrence of 192.168.1.4 in the routing table. If you do, you will want to flush the routing table and then setup the correct routes by executing the /etc/rc2.d/S82atminit file.

- route -f

- netstat -rvn |grep <Standby MC IP Address>

Note: You should not see any occurrence of the Standby MC IP address in the routing table. If you do, you will want to flush the routing table and then setup the correct routes by executing the /etc/rc2.d/S82atminit file.

13 On the Standby DBDS System, verify that a DHCT can boot and can receive advanced services (VOD, IPG, xOD, SDV, etc.). You will want to boot and verify SARA, Aptive/Pioneer, and MDN/ODN DHCTs if you have them. You will also want to verify billing server connectivity. Troubleshoot any issues before proceeding.

14 Customer needs to make Go/No-Go decision regarding whether to proceed or Switch-Back to the Primary DNCS.

15 Enable the collection of Disaster Recovery Near Real Time Sync DHCT data on Standby DNCS:

   a Type **dbaccess dncsdb -q**

   b UPDATE track_mod_chk SET run_flag="Y", last_run = CURRENT;

16 Upgrade the Primary DNCS.

17 Re-install the Disaster Recovery triggers and tables onto the Primary DNCS. See ***Install Disaster Recovery Triggers, Stored Procedures, and Tables*** (on page 100).

   Note: This step can be completed immediately following the DNCS database conversion step, bldDncsDb, of the DNCS upgrade process.

18 Log in to the Active MC and type:

   a **cd /export/home/dradmin/dr/app/ui/webroot/reg/engine**

   b **./test_buildRoutes.php**

   Note: This step sets up all of the necessary network routes on the Primary DNCS. The routes are configured to send the DNCS-generated network traffic for the emulated QAM modulators and Netcrypts to the Standby MC, the local BFS Data QAM, Test QPSK modulator, and Test DHCT network traffic to the local standby DBDS isolation network switch, and the production QPSK modulators and DHCT network traffic to the Disaster Recovery bit-bucket (the default bit-bucket address is defined as 192.168.1.4).

19 Run a DNCS Doctor report on the Primary DNCS and analyze it for issues/anomalies. The production QPSK modulators and their respective RF subnets will not be reachable and will be logged as failures in the Doctor PING report due to the re-direction of the QPSK mod and DHCT traffic into the Disaster Recovery bit-bucket.

20 Verify via the Primary DBDS System Test Hub that a DHCT can boot and can receive advanced services (VOD, IPG, xOD, SDV, etc.). You will want to boot and verify SARA, Aptive/Pioneer, and MDN/ODN DHCTs if you have them. This is the time to troubleshoot any issues discovered on the Primary DBDS system.

21 Take all of the Disaster Recovery jobs off of hold. See ***Take Disaster Recovery Jobs Off Hold*** (on page 102).

   Note: Verify that Disaster Recovery Near Real Time Syncs and Periodic Syncs are successful. These two syncs will keep the data between the Standby DNCS and Primary DNCS synchronized until the maintenance window opens and the Disaster Recovery Switch-Over is performed. It is strongly recommended that the customer not modify any of the DBDS elements (QAMs, QPSKs, Netcrypts, etc.) as well as no modification of the logical DBDS entities (channel maps, sources, services etc.). The Disaster Recovery Near Real Time Sync and Periodic Sync processes will only keep DHCT-related data/configs and Impulse Pay-Per-View events and purchase data synchronized between the Standby DNCS and Primary DNCS.

22 Customer needs to make Go/No-Go decision regarding whether to proceed with the Switch-Back to the Primary DNCS during the next maintenance window.

23 Perform a Disaster Recovery Switch-Back. This process makes the Primary DNCS the Active DNCS and the Standby DNCS the Inactive DNCS.

24 Verify that the Switch-Over was successful by:

a Verifying that the correct network switch ports on the Primary DBDS isolation network switch are up and that the correct network switch ports on the Standby DBDS isolation network switch are down.

b Verifying that the Disaster Recovery "bit-bucket" and "QAM emulation gateway" are no longer present in the Primary DNCS routing table. The bit-bucket IP address is 192.168.1.4 and the "QAM emulation gateway" address is the Primary MC IP address.

- netstat -rvn |grep 192.168.1.4

Note: You should not see any occurrence of 192.168.1.4 in the routing table. If you do, you will want to flush the routing table and then setup the correct routes by executing the /etc/rc2.d/S82atminit file.

- route -f

- netstat -rvn |grep <Primary MC IP Address>

Note: You should not see any occurrence of the Primary MC IP address in the routing table. If you do, you will want to flush the routing table and then setup the correct routes by executing the /etc/rc2.d/S82atminit file.

25 Run a DNCS Doctor report on the Primary DNCS and analyze it for issues/anomalies.

26 On the Primary DBDS (Active DBDS) System, verify that a DHCT can boot and can receive advanced services (VOD, IPG, xOD, SDV, etc.). You will want to boot and verify SARA, Aptive/Pioneer, and MDN/ODN DHCTs if you have them. Troubleshoot any issues before proceeding.

27 Customer needs to make Go/No-Go decision regarding whether to proceed or Switch-Back to the Standby DNCS.

Perform a Disaster Recovery Full Sync

Complete the following steps to perform a Disaster Recovery full synchronization.

1. Log in to the Disaster Recovery system via the Disaster Recovery GUI to display the System Status page.
2. On the left navigation panel of the System Status page, under the Configuration header, select **QAM**. The QAMs page is displayed.
3. Under the Primary Headend field, select **IP Address** to sort and order the list of QAMs by their IP address.
4. Review the list of QAMs and apply the following rules regarding emulation:
   - All QAMs belonging to a particular IP subnet should all have the same emulation status configured. That is to say, that all of the QAMs for a particular subnet should have the same value of either 'Y' or 'N', i.e., yes or no, in their respective "Emulated?" column/field. Use the Subnet Mask column/field to aid in determining IP subnets and IP subnet boundaries.
   - Each of the systems, i.e., Primary and Standby, BFS Data QAMs *should not* be emulated. Subsequently, the only time you should set the "Emulated?" column/field of a QAM is if the QAM exists on the Primary DBDS system but does not exist on the Standby DBDS system.

   Important: Correct any discrepancies for the QAM emulation states based on the above QAM emulation rules before proceeding!
5. From the System Status page, select **Synchronize** in the Synchronization Status window to display the Sync Confirmation page.
6. Enter the user name as **dradmin** and enter the appropriate password.
7. Select **Synchronize** below the Username and Password fields. The Full Sync will be queued to execute almost immediately.
8. On the left navigation panel, select **DBDS Status** to display the System Status page.
9. Select the "refresh" hyperlink in the upper right-hand corner of the page. In the Synchronization Status window, the Full Sync Status should display "In Progress".
10. Select the **Full Sync** hyperlink to monitor the Full Sync progress in the Disaster Recovery GUI.
11. The Job Status - Full Sync page should be displayed. The page should automatically refresh once a minute.
12. The first major Full Sync task is to back up the Active DNCS database and key files. (This is represented as the "abBackup" step in the Child Jobs listing of the Full Sync steps.)

13 On the Active DNCS, log in to monitor the backup log file, abServer.log, as follows:

cd /dvs/dncs/tmp

tail -f abServer.log

Note: The log file should indicate that the Full Sync is performing a tar of all of the system and DBDS Key files. It will then proceed to backing up the Active DNCS database.

14 The next major Full Sync task is to restore the DNCS database and key files that were backed up in the preceding steps to the Inactive DNCS. (This is represented as the "abRestore" step in the Child Jobs listing of the Full Sync steps.) The DNCS processes on the Inactive DNCS will be stopped.

15 On the Inactive DNCS, log in to monitor the restore log file, abServer.log, as follows:

cd /dvs/dncs/tmp

tail -f abServer.log

Note: The log file should indicate that the Full Sync is extracting the key files to the Inactive DNCS. It will then proceed to restoring the DNCS database that was backed up in the preceding steps to the Inactive DNCS.

16 The next major Full Sync task is the restart of the Inactive DNCS and App Server processes. (This is represented as the "restartDNCS" and "restartAPPS" steps, respectively, in the Child Jobs listing of the Full Sync steps.) You will want to monitor the restart of the DNCS and App Server processes to ensure that all necessary processes are restarted on both Inactive servers.

17 The next major Full Sync task is the configuration of the QAM and Netcrypt Emulators. (This is represented as the "configQamEmulator" step in the Child Jobs listing of the Full Sync steps.) This step determines what the routing table on the Inactive DNCS should look like and then sets up the configuration files for the QAMs and Netcrypts that are to be emulated.

Note: You can estimate the time it will take for the configQamEmulator step to complete as follows:

Total number of emulated QAMs divided by 200. Use the whole number value, i.e., the value preceding the decimal point and this is the estimated amount of time in minutes. If the configQamEmulator step does not complete within a minute or two of this estimate, it may be stalled/hung-up. If it is indeed stalled, you will need to kill the Full Sync process manually as follows:

On an Active MC, open a terminal/XTERM window and enter:

<PID value> = ps -ef | grep sync_dhct | awk '{print $2}'

kill -9 <PID value>

18 If the Full Sync completes successfully, you will want to check the Active MC for the emulated QAM configurations for both the bge3 sub-interfaces and the unique instances of the QAM Emulator as follows:

Open a terminal/XTERM window and enter:

NUMBER INTERFACES = ifconfig -a | grep bge3 | wc -l

NUMBER INSTANCES = ps -ef | grep Qam | wc -l

Note: The NUMBER INTERFACES and NUMBER INSTANCES should be equal to each other.

Place Disaster Recovery Jobs on Hold

Complete the following steps to place Disaster Recovery jobs on hold.

1. Log in to the Active MC's Disaster Recovery GUI with the following credentials
   - Username = **dradmin**
   - Password = **dradmin**
2. In the Synchronization Status block, select **Near Real-Time Sync**.
3. Under the Action column on the extreme right side of the GUI, select **Hold**.
4. On the left navigation panel, select **DBDS Status**.
5. In the Synchronization Status block, select **Periodic Sync**.
6. Under the Action column on the extreme right side of the GUI, select **Hold**.
7. On the left navigation panel, select **DBDS Status**.
8. In the Maintenance Status block, select **Audit**.
9. Under the Action column on the extreme right side of the GUI, select **Hold**.
10. On the left navigation panel, select **DBDS Status**.
11. In the Maintenance Status block, select **Backup Primary DNCS**.
12. Under the Action column on the extreme right side of the GUI, select **Hold**.
13. On the left navigation panel, select **DBDS Status**.
14. In the Maintenance Status block, select **Backup Standby DNCS**.
15. Under the Action column on the extreme right side of the GUI, select **Hold**.

Install Disaster Recovery Triggers, Stored Procedures, and Tables

Important: This procedure must be performed during a maintenance window if the DNCS is in production and live.

Complete the following steps to install the Disaster Recovery triggers, stored procedures, and track_mods table onto the DNCS.

1. On either MC, type **cd /export/home/dradmin/dr/dncs**.
2. FTP the load_triggers.sh script to the DNCS.
3. Log in to the DNCS as **root** user.
4. Change directory (cd) to the location where you transferred the script in step 2.
5. Type **chmod +x load_triggers.sh**.
6. Source DNCS environment variables: **. /dvs/dncs/bin/dncsSetup**
7. Stop the DNCS, App Server, 3rd-party Application Servers, and 3rd-party/custom scripts, tools, and utilities.
8. Execute the **showLocks** command.

   Note: If there are database connection sessions still running, execute the killActiveSessions command.
9. Run the load_triggers.sh script: **./load_triggers.sh**
10. On the DNCS, verify that the track_mods and track_mod_chk tables exist as well as the triggers.

    Note: Use the spacebar and **Enter** key to navigate.

    - Type **dbaccess dncsdb -q**
    - Scroll over to INFO and select **INFO** and scroll to the track_mod_chk and track_mods tables and verify that the tables exist.
    - Scroll over to New and enter **select * from track_mod_chk**, then select **escape** to exit back out. Scroll over to RUN and press **Enter**.
    - Verify that the run_flag = **N**
    - Scroll back over to INFO. Select **INFO**, then select the **hct_profile** table and scroll over to **triggers**. There should be a track_mods_trig1 and a track_mods_trig3 listed. Choose a trigger and select **exit** to back out.
    - Scroll back over to INFO. Select **INFO**, then select the **sm_pkg_auth** table and scroll over to **triggers**. There should be a track_mods_trig4 and a track_mods_trig5 listed. Choose a trigger and select **exit** to back out.
    - Scroll back over to INFO. Select **INFO**, then select the **sm_auth_profile** table and scroll over to **triggers**. There should be a track_mods_trig2 listed. Choose a trigger and select **exit** to back out.

11 Verify that all of the Disaster Recovery stored procedures were installed:

- Type **dbschema -d dncsdb -f ins_track_mods | grep 'No procedure' | wc -l**

  Note: If a value of 0 (zero) is returned, it indicates that the stored procedure is installed. Otherwise, a value of 1 indicates that the stored procedure is not installed.

- Type **dbschema -d dncsdb -f dpkg_track_mods |grep 'No procedure' | wc -l**

  Note: If a value of 0 (zero) is returned, it indicates that the stored procedure is installed. Otherwise, a value of 1 indicates that the stored procedure is not installed.

- Type **dbschema -d dncsdb -f ipkg_track_mods | grep 'No procedure' | wc -l**

  Note: If a value of 0 (zero) is returned, it indicates that the stored procedure is installed. Otherwise, a value of 1 indicates that the stored procedure is not installed.

- Type **dbschema -d dncsdb -f upd_track_mods | grep 'No procedure' | wc -l**

  Note: If a value of 0 (zero) is returned, it indicates that the stored procedure is installed. Otherwise, a value of 1 indicates that the stored procedure is not installed.

- Type **dbschema -d dncsdb -f chk_track_mods | grep 'No procedure' | wc -l**

  Note: If a value of 0 (zero) is returned, it indicates that the stored procedure is installed. Otherwise, a value of 1 indicates that the stored procedure is not installed.

- Type **dbschema -d dncsdb -f spkg_track_mods | grep 'No procedure' | wc -l**

  Note: If a value of 0 (zero) is returned, it indicates that the stored procedure is installed. Otherwise, a value of 1 indicates that the stored procedure is not installed.

12 Return to ***Check the Installed Software Version*** (on page 56) and then continue with ***Take Disaster Recovery Jobs Off Hold*** (on page 102).

Take Disaster Recovery Jobs Off Hold

Complete the following steps to take Disaster Recovery jobs off Hold.

1. Log in to the Active MC's Disaster Recovery GUI with the following credentials
   - Username = **dradmin**
   - Password = **dradmin**
2. In the Synchronization Status block, select **Near Real-Time Sync**.
3. Under the Action column on the extreme right side of the GUI, select **Restart**.
4. On the left navigation panel, select **DBDS Status**.
5. In the Synchronization Status block, select **Periodic Sync**.
6. Under the Action column on the extreme right side of the GUI, select **Restart**.
7. On the left navigation panel, select **DBDS Status**.
8. In the Maintenance Status block, select **Audit**.
9. Under the Action column on the extreme right side of the GUI, select **Restart**.
10. On the left navigation panel, select **DBDS Status**.
11. In the Maintenance Status block, select **Backup Primary DNCS**.
12. Under the Action column on the extreme right side of the GUI, select **Restart**.
13. On the left navigation panel, select **DBDS Status**.
14. In the Maintenance Status block, select **Backup Standby DNCS**.
15. Under the Action column on the extreme right side of the GUI, select **Restart**.

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

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

May 2012 Printed in United States of America

Part Number 4042389 Rev A