System Release 2.7/3.7/4.2 Service Pack 3

Release Notes 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**.

CableCARD, OCAP, and OpenCable 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 step-by-step instructions for upgrading our Digital Broadband Delivery System (DBDS) to System Release (SR) 2.7/3.7/4.2 Service Pack 3 (SP3). Sites that use this guide to upgrade must currently support SR 4.2.

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

Scope

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

Audience

These release notes 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 SP3 software onto the Digital Network Control System (DNCS) and the SA Application Server.

Document Version

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

Description	See Topic
Corrected the directory called out in Step 4.	***Verify the Integrity of the CDs*** (on page 20)
Corrected the directory called out in Step 2 and the output captured in the example for Step 3.	***Verify the Integrity of the Maintenance CD*** (on page 22)
Corrected the Savecore directory contents captured in the example for Step 2.	***Verify that the Dump Device is Correctly Configured*** (on page 28)
Added a step to verify the package information for the SAIpatch.	***Verify SAItools Version*** (on page 29)
Added three notes for DBDS networks with disaster recovery enabled in several places.	***A Note About Disaster Recovery Enabled DBDS Networks*** (on pages 38, 48, and 65)
Changed the command that reboots the TED.	***Reboot the TED*** (on page 56)

Description	See Topic
Added a note about stopping cron jobs on the DNCS if they should start before the service pack is completely installed.	***Install the Service Pack*** (on page 60)
Added notes to Step 3 that describes which Maintenance CD to use in the event of a rollback.	***Rolling Back the DNCS*** (on page 104)

1

Introducing System Release 2.7/3.7/4.2 Service Pack 3

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 0.2 or later. This guide provides instructions for upgrading to SR 2.7/3.7/4.2 SP3.

Time to Complete the Upgrade

The upgrade to SR 2.7/3.7/4.2 SP3 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 SP3

Introduction

SR 2.7/3.7/4.2 SP3 features several major operational improvements. Some of these improvements are described in the following list:

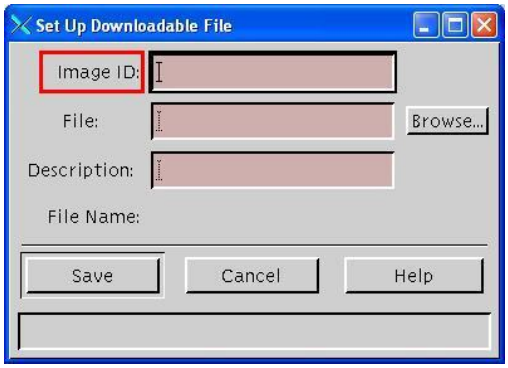
- Support for assignable Image IDs
- Special EID handling to support Common Download (CDL) 2.0
- EAS force tune support without SAM enabled

Assignable Image ID Field

This system release now allows you to specify an Image ID for device image files, instead of allowing the DNCS to assign an ID automatically. This feature allows you to use the same name for an image file across multiple headends.

If you want to specify an image ID, type the ID in the Image ID field on the Set Up Downloadable File window. If you do not want to specify an image ID, leave the Image ID field blank. Refer to the online help for more information.

Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > Downloadable Files tab > File > New



Utility Package Added for EID Handling

Some service providers use subscription packages to send authorizations to allow devices to download different versions of code. This can be a problem for the following reasons:

- Doing this uses EID values from the limited subscription package range and reduces the number of packages available for broadcast content.
- Doing this also allows the package authorizations to be deleted by the billing system during the periodic billing system audits.

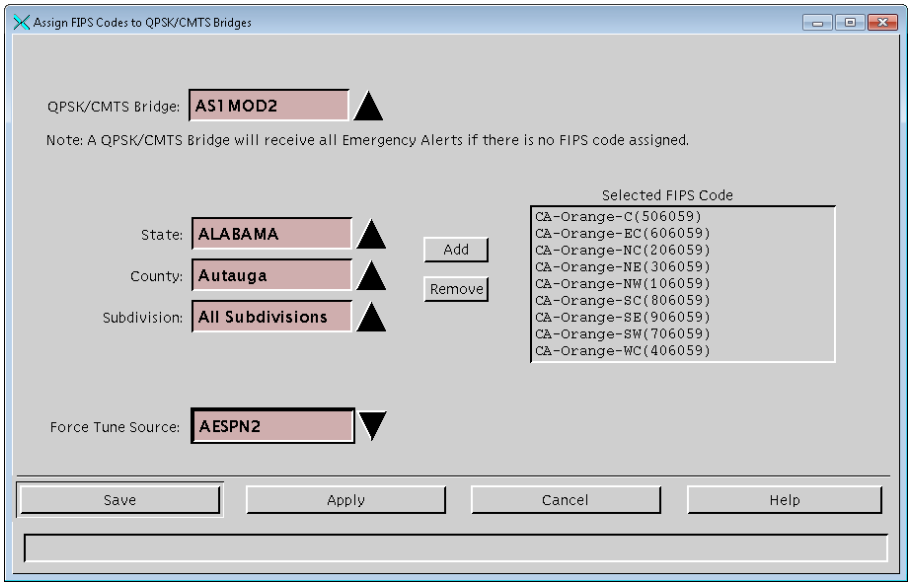
As a solution, we have added the utility package to the DNCS. The solution includes the following:

- The conditional access (CA) system was modified to reserve a range of EID values from the pay-per-view (PPV) range to allow for authorizations.
- The PPV EID range has a greater number of EIDs available than the subscription package range, thus freeing EIDs in the subscription package range of EIDs for use with broadcast content.
- Since the PPV range is not affected by the billing system audit (periodic billing refreshes), these EIDs are unchanged until acted upon by service provider personnel.
- This range of EIDs can be used for several types of non-content authorizations.

EAS Force Tune Service Change for Systems without SAM Channel Map Services

The EAS Force Tune Source option has been added to the Assign FIPS Codes to QPSK/CMTS Bridges window. When enabled, the default label, "Force Tune Service" is replaced by "Force Tune Source" and the options in the drop down menu change from SAM Services to Source IDs.

The new option provides EAS force tune support for DNCS systems that run without SAM channel map publishing services.



Note: The EAS Force Tune Source option must be enabled by Cisco engineers. Contact Cisco Services for assistance.

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-SP0.2 or later is currently installed on your system.
- You have the CD labeled **SR 2.7/3.7/4.2-SP3**.
- You have the CD labeled **DBDS Maintenance CD 3.0.14** (or later) in order to complete the required backups of the database and the filesystem.

  Note: DBDS Maintenance CD 3.0.14 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 4.2.0.50p3
- DNCS GUI/WUI 4.2.0.50
- MQAM 2.6.19
- QAM Application 2.5.7
- GQAM 4.2.2

  Note: If you are using a GQAM version later than 4.2.2, please reinstall GQAM version 4.2.2 for this service pack upgrade.

- QPSK G09

This service pack can be applied to DBDS networks operating at SR 2.7/3.7/4.2 SP0.2.

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 SP2, please contact Cisco Services at 1-866-787-3866.

Application Platform Release Dependencies

The following table shows the application platform release dependencies for this software.

Important: You must have these versions of application platform software *or later* installed on your system prior to beginning the upgrade process. If you do not install the correct application platform software *before* you upgrade your network, subscribers may see video freezing and black screens when using VOD or *anything*-On-Demand (xOD) applications.

Set-Top Platform	Operating System (OS)	SARA	PowerKEY Conditional Access Version
Explorer 4250HDC Exp 2.0.0 (0701) or later	OS 6.20.28.1	1.61.5a100	4.0.1.1
Explorer 8300HDC DVR 1.5.3 (0801) or later	OS 6.20.28.1	1.90.5a101	3.9.7.13
Explorer 8300 DVR v. 1.4.3a10 (or later) v. 1.5.2	 OS 6.14.74.1 OS 6.14.79.1	 1.88.22.1 1.89.16.2	 3.9 3.9
Explorer 8000/8010 DVR v. 1.4.3a10 (or later) v. 1.5.2	 OS 6.12.74.1 OS 6.12.79.1	 1.88.22.1 1.89.16.2	 3.7.5 3.7.5
Explorer 3250HD HD 1.6.0 (or later)	OS 3.24.5.2	1.59.18.1	3.9
Explorer 2xxx, 31xx, 3200, 3100HD	OS 3.13.6.1	1.60.6.2	1.0.6.20 (Explorer 2000s) 1.0.7 (all others)

Important: If you are not using SARA, contact your resident application provider to verify that you have the most recent version of your resident application.

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 X 1.5 GHz minimum ■ 2 X 1.5 GHz minimum
Sun Fire V880	■ 6 X 73 GB ■ 12 X 73 GB	1 GB minimum **Note:** The Sun Fire V880 server ships with 8 GB of memory.
Sun Fire V445	■ 4 X 73 GB ■ 8 X 73 GB	■ 1 GB minimum ■ 2 GB minimum
Sun Enterprise 450	■ 7 X 9 GB ■ 7 X 18 GB ■ 10 X 9 GB ■ 10 X 18 GB	1 GB minimum

Application Server

Platform	Hard Drives	Memory
Sun V240	2 X 36 GB	512 MB minimum
Sun Blade 150	1 X 40 GB	512 MB minimum
Sun Ultra 5	■ 1 X 9 GB ■ 1 X 20 GB	256 MB minimum

Note: The Sun V240 hard drive and memory configurations make an acceptable application server for RNCS.

What Are the Known Issues?

Distributed BFS on an SDV System

If you are currently utilizing Distributed BFS and you are upgrading your system to support SDV, you need to know that you will be adding a number of BFS sources (24, 26, 28, 30, 32) to your BFS source list. These additional sources must also be added to all of your secondary BFS QAMs.

Important: We recommend that this activity be performed during a maintenance window.

What CRs Are Included in This Service Pack?

Introduction

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

Implemented CRs

This section provides a list of CRs found in previous releases that have been implemented in software for SR 2.7/3.7/4.2 SP3. CRs are indexed by ID number in ascending order.

CR ID	Title
65327-06	CVT download association fails intermittently and generates a core
67137-02	In 4.2 serial numbers now required in DB for all DHCT's
69645-02	emmDistributor does not close DB connections when closing a thread
69674-02	modDhctCfg currently limits at 300 packages
70661-04	sdvManager not provisioning sdv server
70750-03	CableCARD™ WEB UI is sluggish. (WEB UI performance & scalability)
71781-02	pkeManager core dumping on 4.2.1.17
72069-01	OpenCable™ EAS repeat descriptor tag (number_of_repeats descriptor)
73260-01	Drm should not use Transport Stream Route bandwidth to calc remaining bandwidth
73483-01	Drm should try to allocate BW on parent svc grp if failing on child svcgrp
73582-01	DRM fails to properly allocate and release UDP port numbers for NetCrypt
73906-01	table space configuration needed for table opencable_id
74050-01	DRM generating UDP port value of "0" for input value sent to Netcrypt
74255-01	DRM deletes VOD exclusive session through Netcrypt/TBQAM
74395-01	XAIT stops transmitting after qpskManager is bounced
74593-01	DRM not releasing bandwidth on failed encrypted session - 218 errors

CR ID	Title
76001-01	DRM unable to recover sessions when cache read fails
77165-01	QamToSvcGroup.dat requres shared QAM ports for Concurrent
77390-01	DRM cored due to error tracking qam callbacks for sessions on DIS disabled HCTs
77539-01	qamManager crashes at TW Albany due to threads in cache

77666-01	DRM error 218 when taking QAM offline error "No destinations..."
78333-01	DSM2DRM default window setting of 20 needs to be changed
78520-02	DSM should drop the SDV requests when queue is full
78799-01	DRM is unable to load balance Netcrypts when used with multiple transport clouds
79077-04	sdvManager monitors incorrect OID for SDV Server State
79405-03	It is possible for qamManager to have two different qam IDs for one active QAM
79982-01	Message truncated intermittently when sent from dsm to sdvServer
80024-06	Netcrypt UI can display Ethernet ports in wrong order
80274-01	CCCM_SRC doesn't work on SDV Channels
80792-03	Encrypted sessions are staying "Clear" because ECMs aren't delivered
80848-02	sdvManager won't provision SDV servers with large number of switched programs
81113-01	DNCS SDV Server List UI state is out of sync
81406-01	AlarmCollector "Blocking" when responding to QAM call
81526-01	ocdlManager doesn't support multi hardware vendor CDVTs
81914-06	Make pkeBandwidth checks in drm more efficient
83264-01	QamManager crashes during quarantine list update
85689-01	DRM does not recover GQAM multicast sessions properly
86246-01	DNCS QPSK UI: Max Contention Access Message Length Default Value
86350-07	Deletion of SMDG accesses SMDG list form 2 threads
87288-06	qamManager main thread pauses when there is a RPC timeout communicating with QAM
90689-01	dbUIServer memory leak
91822-01	Primary SDV server doesn't recover (transition) from backup after a failover
92960	qpskManager not sending SI data
93004-01	Stranded Sessions in qamManager after high qamManager activity
93110-03	qamManager should perform Audit-based deletions first, then creates

CR ID	**Title**
93645-04	qamManager can nest session audits on incoming session with dup MPEG
94098-01	Setup failed while provisioning new muliticast source definition
94297	Batch package authorization WUI does not work properly
94319	Batch package authorization UI not working properly

94463	Batch Authorization UI working incorrectly with flat file
94608	Batch authorization WUI takes over 2 minutes to update
94738	TSB OC EAS Playout is not created/updated by DNCS
94890-05	qamManager provisioning not complete, RF parameters and Gige IP not updating
96216-01	DNCS package UI incorrectly display the start time for a PPV during DST
97088-01	Encrypted sessions appear in the clear after hardware change (GQAM)
99561-01	OCAP™ CVT WEBUI does not consistently update POD_Data
102315-02	MMMServer order of mp3 file posting and removal on TSBroadcaster impacts OOB OC
109380-02	eventManager causes session to go out in the clear if Netcypt is rebooted
111332	The IIH utility does not deregister with portmapper when terminating
111540-06	qamManager needs to quarantine QAMs when it times out on messages

Open CRs

This section provides a list of open CRs that were identified during testing of SR 2.7/3.7/4.2 SP3. CRs are indexed by ID number in ascending order. Resolutions to these CRs are currently under investigation or in development.

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

CR ID	Title/Description
94415	camPsm cored over weekend Impact: camPsm recovers on its own.
94605	UI should not create SMDGs on RF ports with no associated TSID Impact: If an operator creates an SMDG mapped to an RF port that doesn't have a TSID associated with it, he won't be able to delete the SMDG object from the database. Workaround: There is no workaround.
94939	_mmmui core dumps when sending an EAS audio file Impact: Generating an EAS message with an unsupported audio file causes the MMMUI to core dump and the message to fail.

CR ID	Title/Description
95134	Sort by TSID does not work correctly on table-based QAMs Impact: Operators cannot sort table-based QAM lists by TSID.
95451-01	Batch Authorization Device Type field is smaller than value stored in the DB

	Impact: The DHCT Type field length is 80 characters. The field width for Device Types in the Batch Package Add/Remove is 31 characters. The additional characters will not display for Device Types with more than 31 characters.
95812-01	dsm memory leak with failed VOD session setup Impact: When many VOD sessions fail, dsm develops a memory leak that could cause it to exceed the maximum size allowed (4 GB) for processes. Under such circumstances, dsm will core. Workaround: Dsm should recover on its own. If it does not, then bounce the process.
98778-01	SAM service Short Description allows 10 characters, but DB only allows 5 Impact: The save fails. Workaround: Reenter the SAM service with five or fewer characters in the Short Description field.
100287-02	EAS SCTE18 messages audio_file_timeout value not set to zero when fails The audio_file_timeout value for EAS SCTE18 messages is not set to zero when an mp3 file posting to the TSBroadcaster fails. Impact: Set-tops will wait to display the EAS message for a period of time equal to the audio_file_timeout value. This value is set on the Set Up MMM Configuration window. Workaround: Operators should check the communication between the DNCS and the TSBroadcaster.
103825-01	pkeManager core dumps when restarting large number of Netcrypts Impact: This causes the session recovery process to start, which will stop all VOD traffic until it has completed. Workaround: The process will core once and recover.
106034	ocdlManager Carousel directory contains duplicate images When associating an existing image with different vendor/hardware ID combinations, the image is duplicated in the /dvs/dvsFiles/OCAP_CD/CAROUSEL directory and in the /dvs/dvsFiles/OCAP_CD/CONFIG/ocap_image.xml file. Impact: If the DNCS is used to stream CDL images (hardmux solution), image files may be duplicated. Workaround: There is no workaround.

CR ID	Title/Description
106491-03	ocdlManager image import vendor ID and hardware ID values are not verified cdlManager image import process should either prohibit operators from deviating from the expected input format, or ocdlManager should accept

	any value entered and format the values as required. Impact: Operators must follow vendor and hardware ID format as shown in the ocdlManager image import UI, or CDVT will not be properly generated. Additionally, when this CR is fixed, operators must remove and re-add all existing cdl1.0 image entries to avoid the condition addressed by this CR.
106691-02	mechanism needed to provision the range of MpegProg numbers used by DRM Impact: Some MSO applications have a problem with numbers greater than 32K. For MSO applications that are unable to tune to program numbers greater than 32K, the program is not viewable.
108810	SR4.2 SP3 upgrade hangs in SAIdncs postinstall of installTed.sh Impact: The SR4.2 SP3 installation intermittently hangs in the SAIdncs postinstall when attempting to run the installTed.sh scripts. This script attempts to kill devtedInit and devted processes. If it fails, the script should exit. Workaround: 1. kill the install_SP processes 2. reboot the TED 3. run install_SP -i
111638	alarmCollector taking up 33% CPU Impact: alarmCollector occasionally takes up excessive CPU-time causing the system to slow. Workaround: Restart alarmCollector to resolve issue.
111768	DHCT "Batch Install" does not allow "Selected" packages to be saved after provisioning Impact: This issue only occurs during batch installation of new boxes. Workaround: There is no workaround.
114804	nested audit fix (CR 93645-04) did not cover other QAM types Impact: Audit failures can consume significant CPU time resulting in intermittent video service interruptions. Workaround: Bounce the affected QAM, which will, unfortunately, interrupt service on the device.

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 15) 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 21)
- ***Verify the Integrity of the CDs*** (on page 22)
- ***Verify the Integrity of the Maintenance CD*** (on page 24)
- ***Upgrade the RNCS (Optional)*** (on page 25)
- ***Check Available Disk Space*** (on page 26)
- ***Run the Doctor Report*** (on page 27)
- ***Examine Mirrored Devices*** (on page 28)
- ***Verify that the Boot Device is Correctly Configured*** (on page 29)
- ***Verify that the Dump Device is Correctly Configured*** (on page 30)
- ***Back Up Various Data Files*** (on page 33)
- ***Check the EAS Configuration—Pre-Upgrade*** (on page 34)
- ***Obtain DNCS System Configuration*** (on page 35)
- ***Collect Network Information*** (on page36)
- ***Check and Record Sessions*** (on page 38)
- ***Back Up the DNCS and Application Server File Systems*** (on page 40)

- ***Stop the dhctStatus, signonCount, and cmd2000 Utilities*** (on page 39)
- ***Back Up and Delete the copyControlParams File*** (on page 42)
- ***Verify DBDS Stability*** (on page 43)
- ***Back Up the Informix Database*** (on page 44)

During the Maintenance Window

At the beginning of the maintenance window, you should start with ***Suspend Billing and Third-Party Interfaces*** (on page 45) 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-Cisco 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 Settop 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
- Open Cable 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 as expected?

   - 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 24).

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 25); otherwise, go to ***Check Available Disk Space*** (on page 26).

Upgrade the RNCS (Optional)

If you are currently utilizing RNCS, you must upgrade your RNCS servers as part of the pre-upgrade process.

To upgrade your RNCS servers, perform steps 1 through 24 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 26).

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_sp3c11
                       371M   371M     0K   100%    /cdrom/sr_4.2_sp3c11
```

2 Does the Available column show that at least 310M are available for the upgrade?

- If **yes**, go to ***Run the Doctor Report*** (on page 27). 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 using the instructions provided in the *DBDS Utilities Version 6.1 Installation Instructions and DNCS Utilities User Guide* (part number 4020695). The Doctor report provides key system configuration data that might be useful before you begin the upgrade process.

Notes:

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

Analyze the Doctor Report

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

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.
   - The designation **Okay** appears in the **State** column next to each metadevice.
   - 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 29).
   - If the system is a **V880** or **V890**, is the state of each metadevice **Okay**?
   - 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. 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. Did you see disk:a listed as the **first** boot device?

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

   - If **yes**, then you have completed this procedure.
   - If **no**, type **eeprom boot-device=disk:a** and then press **Enter** to reset the default boot device to the original disk.

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 **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
```

3. 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 ***Back Up Various Data Files*** (on page 33).
   - If **no**, continue with step 4 to set the dump device correctly.
4. Type **dumpadm -d /dev/md/dsk/d501** and then press **Enter**.
5. 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:  Cisco
      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. If the SAItools version is 4.2.0.13p5 and the SAIpatch is 4.2.1.10, then you have previously installed the Solaris Patch 4.2.1.10 CD.

Note: SR 2.7/3.7/4.2 SP3 comes with SAItools 4.2.0.13p3, which is incompatible with with SAIpatch 4.2.1.10. Please, locate the Solaris Patch CD now so you can reinstall SAItools 4.2.0.13p5 after the upgrade (see ***Reinstall SAItools 4.2.0.13p5*** (on page 63)).

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 109).

   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** and then press **Enter**.
2. Type **cp -p /tftpboot/*.conf* /tftpboot/backup** 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.

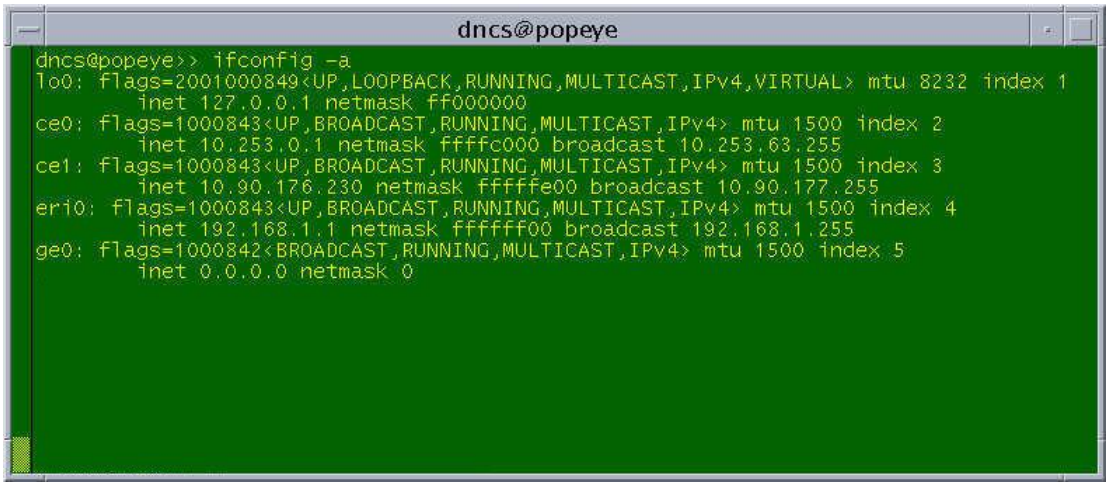
```
uname  -n
```

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

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

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

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

13 Back up DNCS files.

- **a** Type **cd /dvs/dncs/bin** and press **Enter**.
- **b** Type **cp -p tsbroadcasterclientapi.jar tsbroadcasterclientapi.jar.SP3** and press **Enter**.
- **c** Type **cp -p TSBroadcasterClient.jar TSBroadcasterClient.jar.SP3** and press **Enter**.
- **d** Type **cd /export/home/informix/etc** and press **Enter**.
- **e** Type **cp -p onconfig onconfig.preSP3** and press **Enter**.

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 BFS QAM and/or GQAM.

   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 167).*

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 **no**, go to ***Back Up and Delete the copyControlParams File*** (on page 44).
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 44).

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 SA 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 though 6.

   Note: Call Cisco Services for assistance if necessary.

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--Disaster Recovery Upgrade*** (on page 168), ***Perform a Disaster Recovery Full Sync*** (on page 172), and ***Place Disaster Recovery Jobs on Hold*** (on page 175).

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

Remove the NMI Software

1 Are you already root user in an xterm window on the DNCS?

- If **yes**, go to step 3.
- If **no**, go to step 2.

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 **pkginfo -l | grep SAInmi** and then press **Enter**. The system lists the SAInmi package if it is installed.

4 Is SAInmi installed?

- If **yes**, go to step 5.
- If **no**, you do not have NMI loaded onto your system. Skip the rest of this procedure, and go to ***Stop System Components*** (on page 50).

5 Close any user interfaces that may be open on the DNCS.

Note: If the DNCS has any open user interfaces, you cannot remove the NMI software.

6 Type **ps -ef | grep ui** and then press **Enter**. The system displays a list of user interface processes that may still be running.

7 On a sheet of paper, write down the process IDs (PIDs) of any user interface process that is still running.

8 Type **kill -9 [PID]** and then press **Enter** for any user interface process that is still running. The system stops the user interface processes.

9 Type **pkgrm SAInmi** and then press **Enter**. The system deletes the NMI software.

Stop System Components

Introduction

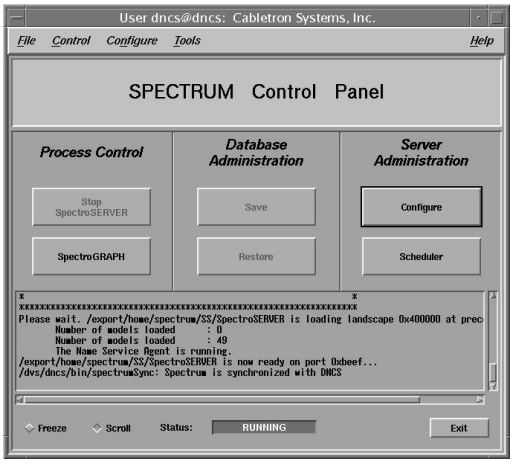
Before continuing with the installation process, follow the instructions in this section to stop system components.

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 or to send BOSS transactions. 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

If the RNCS licensed feature is enabled on your service control platform, complete the following steps to stop the RNCS processes.

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*** (on page 53).
3. Type **siteCmd <RNCS hostname> lionnStop** and then press **Enter** to stop the RNCS processes.
4. Type **siteCmd <RNCS hostname> lionnKill** and then press **Enter**.
5. Type **siteCmd <RNCS hostname> pgrep –fl dvs** and then press **Enter** to confirm that all RNCS processes are stopped.
6. Are the processes on the RNCS stopped?
   - If **yes**, go to ***Stopping the Application Server*** (on page 53).
   - 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

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

Stopping the Application Server at SARA Sites

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

   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 appears.
3. Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**. The system displays all Application Server processes.

   Note: The system updates the display periodically, or you can press **Enter** to force an update.

4 When the **Curr Stt** (Current State) field of the Applications Control window indicates that all of the Application Server processes have stopped, follow the on-screen instructions to close the Applications Control window.

5 Type **appKill** and then press **Enter**. The appInitd process stops.

Stopping the Time Warner Mystro Application Server

If the site you are upgrading uses the Time Warner Mystro Application Server (MDN), refer to the documents provided by Mystro to shut down the Mystro Application Server.

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.

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 again **/dvs/dncs/bin/stopSOAPServers** 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 SP3 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 **rsh dncsted** to connect to the TED.

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 **rsh dncsted** to verify that you can connect to the TED and that TED has rebooted.

Detach the Disk Mirrors

Introduction

In this procedure, you will detach the disk mirrors of the Enterprise E450 or Sun Fire V880 DNCS. If you fail to detach the disk mirrors, you must restore from a tape backup. Detaching the mirrors allows you the option of recovering quickly in the event of a failed upgrade by booting from the standby drives.

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

Detaching the Disk Mirrors

Complete the following steps to detach the disk mirrors before the upgrade to SR 2.7/3.7/4.2 SP3.

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

   Note: If a File Manager window opens on the DNCS, close the window.

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

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

3. Type **/cdrom/cdrom0/s3/backup_restore/mirrState -d** and then press **Enter**. The system displays the following message:

   WARNING!!
   Proceeding beyond this point will DETACH all d7xx submirrors.
   Are you certain you want to proceed?

4. Type **y** and then press **Enter**. The system disables the disk mirroring functions on the DNCS.

   Note: You may see a message similar to **Warning: d5xx metadevice is setup as a one way mirror**. This message is normal.

5 Type **metastat -p** and then press **Enter**. The system displays output similar to the following example of a V880 or 6x72 disk configuration.

Note: This is only an example of output from the metastat command. The output will differ depending on your system configuration.

```
$ metastat -p
d367             p  2.0GB d520
d366             p  2.0GB d520
d365             p  2.0GB d520
d364             p  2.0GB d520
d363             p  2.0GB d520
d362             p  2.0GB d520
d361             p  2.0GB d520
d360             p  2.0GB d520
d359             p  2.0GB d520
d358             p  2.0GB d520
d357             p  2.0GB d520
d356             p  2.0GB d520
d355             p  2.0GB d520
d354             p  2.0GB d520
d353             p  2.0GB d520
d352             p  2.0GB d520
d351             p  2.0GB d520
d350             p  1.0GB d520
  d520           m   59GB d420
    d420         s   59GB c1t2d0s0
d501             m  8.0GB d401
  d401           s  8.0GB c1t0d0s1
d503             m  8.0GB d403
  d403           s  8.0GB c1t0d0s3
d500             m  8.0GB d400
  d400           s  8.0GB c1t0d0s0
d507             m  8.0GB d407
  d407           s  8.0GB c1t0d0s5
d510             m   59GB d410
  d410           s   59GB c1t1d0s0
d720             s   59GB c2t5d0s0
d710             s   59GB c2t4d0s0
d707             s  8.0GB c2t3d0s5
d700             s  8.0GB c2t3d0s0
d703             s  8.0GB c2t3d0s3
d701             s  8.0GB c2t3d0s1
```

6 Verify that the d5xx metadevices contain only one submirror (d4xx).

Example: d500 -m d400 1

Note: If the d5xx metadevice contained two submirrors, the line containing the d5xx metadevice would look similar to **d500 -m d400 d700 1**.

7 Do the d5xx metadevices contain only one submirror?

- If **yes**, type **eject cdrom** and then press **Enter**.
- If **no**, repeat this procedure, or call Cisco Services for assistance.

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 **Important:** Be sure to include **-i** (lower case letter "i") in the following command.

Type **/cdrom/cdrom0/install_SP -i** and then press **Enter**. A list of packages displays.

Note: In the following example, the error shown in the output is only output to the screen. This error is not logged to the /dvs/install_SP.log file. All that is logged is the package name.

Example - Sample Packages List:

```
Checking the system, please wait...
Checking for running processes...
**************************************************************************
This script will install the following packages on:
DNCS Server (conanv880)
-------------------------
SAItools            DNCS/AppServer Tools 03-13-2007
                    4.2.0.13p2

SAIdncs             DNCS 12-01-09
                    4.2.0.50p3

SAIgui              DNCS GUI 12-01-09
                    4.2.0.50

SAIwebui            DNCS WEBUI 12-01-09
                    4.2.0.50

SAIqam              QAM Modulator
                    V2.5.7

SAImqam             MQAM Modulator
                    V2.6.19

SAIgqam             GQAM Modulator
                    V4.2.2
```

```
SAIgoqam            GOQAM Modulator
                    V1.1.4


SAIncrypt           Netcrypt
                    V1.2.12
pkgparam: ERROR: unable to locate parameter information for "SAIqpsk"
pkgparam: ERROR: unable to locate parameter information for "SAIqpsk"
SAIqpsk
******************************************************************************
Are you SURE you want to continue?  [y,n,?,q]
```

Note: The SAIqpsk package is not being installed. The above ERROR for SAIqpsk can be ignored.

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

Note: When the interactive mode is enabled, the system displays a message similar to the following example.

```
****************************************************************
      Copyright (c) 1998-2007 Cisco.
                    All Rights Reserved

This product is protected by copyright and distributed under
licenses restricting copying, distribution and decompilation.
****************************************************************
Hit <CR> to continue...
```

6 Press **Enter** to continue. The system displays a message that asks whether you have backed up the DNCS host and the DNCS database.

7 Have you backed up the DNCS file systems and database?

- If **yes**, type **y** and then press **Enter**.
- If **no**, type **n** and then press **Enter**.

  Note: If you type n, the installation will terminate. Back up the file systems and database and then repeat this procedure from step 4.

8 Choose one of the following options to configure dbOptimizer:

- Enter the number of days passed, or type **d** (lower-case D) for the default value of 90 days
- Press **Enter** to accept the default value

Note: You can determine the current setting by using the cat command to examine the /dvs/dncs/bin/CED.in file.

9 Follow these instructions regarding the configuration parameters that are displayed on the screen.

Example - Sample Installation Configuration Screen:

```
********************** Installation Configuration **********************
**                                                                    **
**     0)  INFORMIXSERVER        =                      dncsDbServer    **
**     1)  DNCS_HOST             =                              dncs    **
**     2)  BFS_HOST              =                              dncs    **
**     3)  DNCSATM_IP            =                       10.253.0.1     **
**     4)  APPSERVATM_IP         =                      10.253.0.10     **
**     5)  DNCSTED_IP            =                      192.168.1.2     **
**                                                                    **
************************************************************************
Number to change ("0", "1", ...,"5"), "c" to continue, or "q" to quit:
```

a Examine the configuration parameters and follow onscreen instructions to change any parameter that needs to be changed.

b Type **c** and then press **Enter** when you are finished. The installation continues.

10 Cron jobs will start up on the DNCS during the install, but they must be stopped for the install to complete. To resolve the issue, follow theses instructions:

a When the system begins installing the postinstall script, begin watching the console for the text in the output example below. The text indicates that cron jobs have started.

Example:

```
Beginning build/update of database dncsdb
Output is saved in file /dvs/dncs/convert.out
dataspace1 is properly configured.
```

Note: You can also view the same output by checking /dvs/dncs/convert.out. Open a separate xterm window, then type **tail -f /dvs/dncs/convert.out** and press **Enter**. Do this at regular intervals after the postinstall script starts until you see the text in the example above.

b When you see the text, return to ***Stop the cron Jobs on the DNCS*** (on page 46) and, in a separate xterm window, issue the commands to stop the DNCS cron jobs.

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

12 Check the log file for errors.

Notes:

- The installation log file is in the /dvs directory of the DNCS. The name of the log file is **install_SP.log**.
- Call Cisco Services for assistance if the log file reveals errors.

Reinstall SAItools 4.2.0.13p5

Introduction

When Solaris Patch 4.2.1.10 is installed, it installs SAItools 4.2.0.13p5 to support some of the Solaris patches. Service Pack 3 (SP3) installs SAItools 4.2.0.13p2.

If you have not yet installed Solaris Patch 4.2.1.10, go to ***Check the Installed Software Version*** (on page 68). If you installed Solaris Patch 4.2.1.10 prior to installing SP3, you must re-install Solaris Patch 4.2.1.10.

Complete the following steps to reinstall the SAItools package.

Important: This procedure will have you edit the /etc/system file first on the DNCS and then on the SARA Application Server.

1. Insert the CD labeled **Solaris Patch 4.2.1.10**.
2. Type **/cdrom/cdrom0/tools/install_patch** and press **Enter**.
3. Type **y** and then press **Enter**. The package is installed on the DNCS.
4. Did the "Installation of <SAItools> successful" message appear?
   - If **yes**, go to step 5.
   - If **no**, contact Cisco Services for assistance.
5. Type **cd /var/sadm/system/logs** and then press **Enter**.
6. Open the SAItools log file and look for any errors, warnings, or failures.
7. Are any errors, warnings, or failures present?
   - If **yes**, contact Cisco Services for assistance.
   - If **no**, go to step 8.

8 Type **pkginfo -l SAItools** and press **Enter** to verify that the SAItools package is completely installed. The result should resemble the following output.

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:  Cisco
     DESC:  DNCS/AppServer Tools 05-22-09
   PSTAMP:  aurora20090522073708
 INSTDATE:  Nov 05 2009 07:24
   STATUS:  completely installed
    FILES:     2855 installed pathnames
                 12 shared pathnames
                371 directories
                380 executables
                  5 setuid/setgid executables
             415113 blocks used (approx)
```

Note: If the STATUS is anything other than "completely installed", call Cisco Services for assistance.

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 68).

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 176) for instructions.

Note: If your DBDS is *not* enabled for Disaster Recovery, continue to the next section in this 1chapter.

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/s3/sai/scripts/utils** and then press **Enter**. The working directory is now /cdrom/cdrom0/s3/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 Service Pack	SAISP	SR_4.2_C11	
DNCS Application	SAIdncs	4.2.0.50p3	
DNCS/App Tools	SAItools	4.2.0.13p5	
DNCS GUI	SAIgui	4.2.0.50	
DNCS WUI	SAIwebui	4.2.0.50	
DNCS Online Help	SAIhelp	4.2.0.3	
QAM	SAIqam	2.5.7	
MQAM	SAImqam	2.6.19	
GQAM	SAIgqam	4.2.2	
GoQAM	SAIgoqam	1.1.4	
Netcrypt	SAIncrypt	1.2.12	

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 70) 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.SP3** and press **Enter**.
   c. Type **cp -p TSBroadcasterClient.jar TSBroadcasterClient.jar.SP3** and press **Enter**.
2. Put the preSP3 files back in place.
   a. Type **cp -p tsbroadcasterclientapi.jar.preSP3 tsbroadcasterclientapi.jar** and press **Enter**.
   b. Type **cp -p TSBroadcasterClient.jar.preSP3 TSBroadcasterClient.jar** and press **Enter**.
3. Compare /export/home/informix/etc/onconfig to /export/home/informix/etc/onconfig.preSP3 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.SP3** and press **Enter**.
   b. Type **cp -p /export/home/informix/etc/onconfig.preSP3 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.

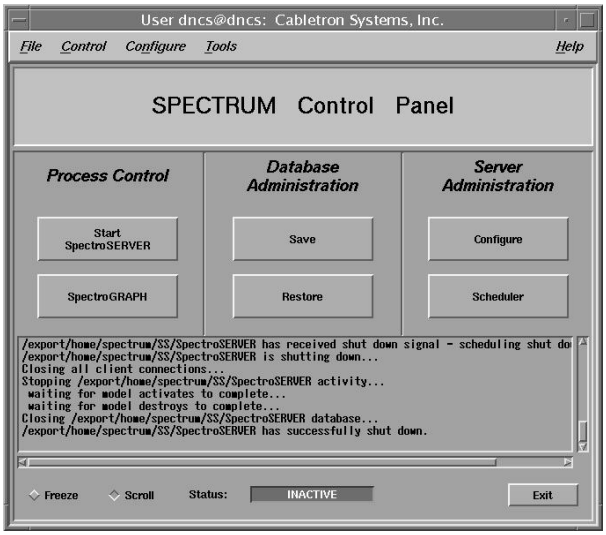
Important: If a patch was provided, be sure you have installed the patch and completed the instructions that accompanied it. Then go to ***Check the Installed Software Version*** (on page 66) and complete the instructions there before restarting the system components.

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.

Restarting the DNCS

1. From an xterm window on the DNCS, type **dncsStart** and press **Enter**. The Informix database, the SOAPServers, and DNCS processes start.
2. Click the middle mouse button on the DNCS and select **Administrative Console**. The DNCS Administrative Console opens.
3. From the DNCS Administrative Console Status window, click **DNCS Control**.

   Results:

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

   Notes:

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

Restarting the RNCS Processes

If the Distributed DNCS licensed feature is enabled on your system, complete the following steps to restart the RNCS processes.

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

This section provides procedures for restarting either a SARA Server or a 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.

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 72).
- You should be logged on to the DNCS as **dncs** user.

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.

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.

Check the Transport Stream ID Values

Checking Transport Stream ID Values

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

Follow this procedure to verify that the session-based QAM reserved range for your facility matches the TSIDs that you actually use.

Before you begin:

Does your site use table-based QAM modulators?

- If **yes**, or if you are not sure, go to ***Download getTSID*** (on page 75), then ***Run getTSID*** (on page 76), and then ***Check TSID Values*** (on page 76).
- If **no**, go to ***Check TSID Values*** (on page 76).

Download getTSID

1 Log on to the FTP server.

- The address of the server is **ftp.sciatl.com** or **192.133.243.133**.

Note: The address for the FTP server is subject to change. If you are unable to reach the FTP server, please contact Cisco Services for the latest address.

- The username is **anonymous**.
- The password is the e-mail address of the person logging in.

2 Choose one of the following options to navigate to the directory in which the file is located:

- If you are *outside* of our firewall, type **cd /pub/scicare/TOOLS.**
- If you are *inside* of our firewall, type **cd /scicare/TOOLS.**

3 Configure FTP:

Command	Description
Type **ascii** and press **Enter**.	Sets the transfer mode to ascii.
Type **hash** and press **Enter**.	Displays hash marks that show file-transfer progress.
Type **prompt** and press **Enter**.	Sets interactive mode to off.

4 Type **mget getTSID** and press **Enter**. The system begins copying the file (or files) from the FTP site to the current directory on your DNCS.

5 Type **bye** and press **Enter** to log out of the FTP server.

Run getTSID

1. Copy getTSID to the /export/home/dncs/scripts directory of the DNCS.
2. Type **chmod 755 getTSID** and press **Enter** to change the permissions for getTSID.
3. Type **getTSID** and press **Enter**. The DNCS displays the range of TSIDs that your facility uses.

   Example:

```
$./getTSID
database access in progress. Please wait ...
database access in progress. Please wait ...

SA TSID Range
=====================================
Min: 101
Max: 10111

NON SA TSID Range
=====================================
Min: 50010
Max: 50010
```

   Important: Be sure that the session-based (SA) range and the table-based (non-Cisco) range do *not* overlap. If these ranges overlap, then you must re-map your TSIDs.

Check TSID Values

1. From the DNCS Administrative Console, select the **DNCS** tab and then the **System Provisioning** tab.
2. Click **DNCS System**. The DNCS System Configuration window opens.
3. Click the **Advanced Parameters** tab.
4. Verify that the **Start Transport Stream ID** and **End Transport Stream ID** values encompass the session-based TSID Range that you found using getTSID.
   - If your site uses only session-based QAM modulators, these values should be 0 and 65535, respectively.
   - If your site uses table-based QAM modulators, make sure that the TSID ranges for the table-based QAM modulators do not fall within the range of SA reserved TSIDs.
   - If your site uses switched digital video (SDV), the DNCS will not allow you to save a TSID range unless you have also defined a range of MPEG program numbers for SDV. Click on the SDV Parameters tab to define starting and ending MPEG program numbers.
5. Click **Save** and close the DNCS System Configuration window.

6 If you made any changes to the **Start Transport Stream ID** or **End Transport Stream ID** values, remember to stop and restart the DNCS and the Application Server to ensure that the new settings take effect for each configuration change.

7 For more information, see *Setting Session-Based QAM TSID Ranges* (part number 4004192).

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 78).
   - 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 SA 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.

Check cron Jobs

After restarting the billing and third-party interfaces, examine the root and dncs crontab entries for any cron jobs that may not have run, such as the IPG Collector, during the maintenance window while cron jobs were stopped. If necessary, run these cron jobs manually.

Follow these instructions to check the crontab files.

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

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

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

   ```
   tar xvf crontabs.tar
   ```

3. Type **cd crontabs** and press **Enter**.
4. Follow these instructions to compare the dncs crontab file to the actual post-upgrade entries.
   a. Type **less dncs** and press **Enter**.
   b. Type `crontab -l dncs` and press **Enter**.
   c. Compare the output from steps a and b. Verify that customer-specific cron entries in step a are included in step b.
   d. Add any missing entries from step a to the dncs crontab file.
5. Repeat step 4 for the root crontab file.

4

Post-Upgrade Procedures

Introduction

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

In This Chapter

Remove Object Carousel EAS Playout

This procedure removes incompatible playouts on the TS Broadcaster and is required for both TS Broadcaster version 1.x and 2.x. software. You must perform this procedure because the original OCEAS application and playout create a conflict with 2.7/3.7/4.2 SP3—the mechanism that constructs the OCEAS playout and application was changed in this release.

Note: This procedure should be performed now and immediately followed by an EAS system test. For instructions, see ***Check the EAS Configuration—Post Upgrade*** (on page 83).

1 Open a browser and log into your TS Broadcaster.

2 Delete the OCEAS playout.

TSB 1.x Systems:

a Click **Playouts,** select the stream name from the pull-down menu and click **Select**.

b Click **Delete Playout** and select the OCEAS playout (if present) from the pull-down menu.

c Click **Delete**.

TSB 2.x Systems:

d Click **Live Applications** and change **Playout Type:** to **OOB OC Playouts.**

e Delete the OCEAS playout, if present.

3 Delete the OCEAS application.

TSB 1.x Systems:

a Click **Application Sets** and click **Delete Application Set**.

b Select the OCEAS application set name (if present) from the pull-down menu.

c Click **Delete**.

TSB 2.x Systems:

d Click **OCAP Applications** and change **View** to **Unscheduled.**

e Delete the OCEAS application, if present.

The next time EAS occurs, the OCEAS playout and application will be automatically created by the DNCS. The OCEAS playout and application will also be removed at the successful completion of each EAS test.

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 85).

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**.

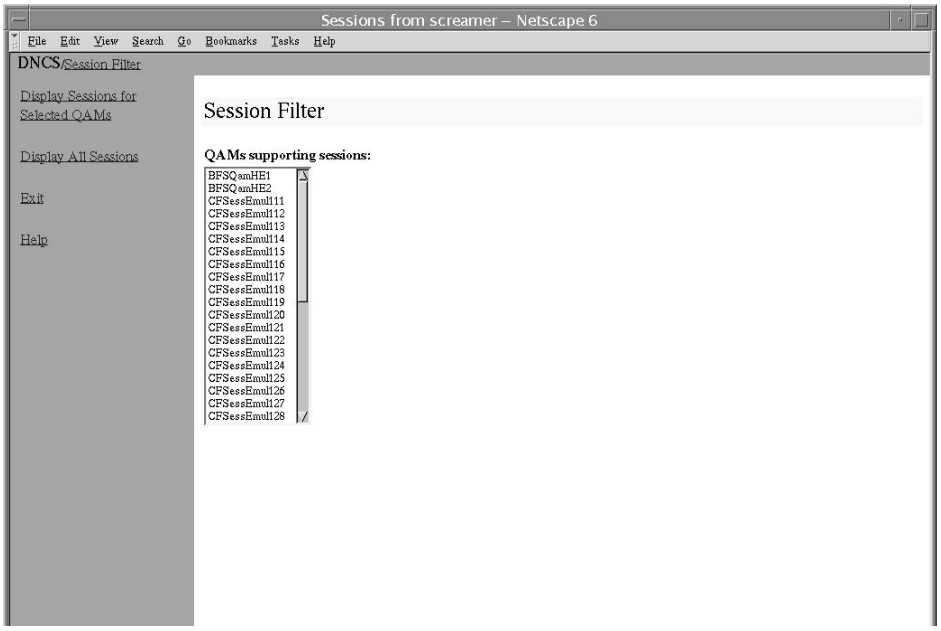
5 Verify that the Active Stream total equals the number of streams you recorded in Checking the BFS Sessions on the BFS QAM or GQAM.

6 If the pre-upgrade stream total matches the post-upgrade stream total, *skip the next section* and go to ***Authorize the BRF as a BFS Server (Optional)*** (on page 89).

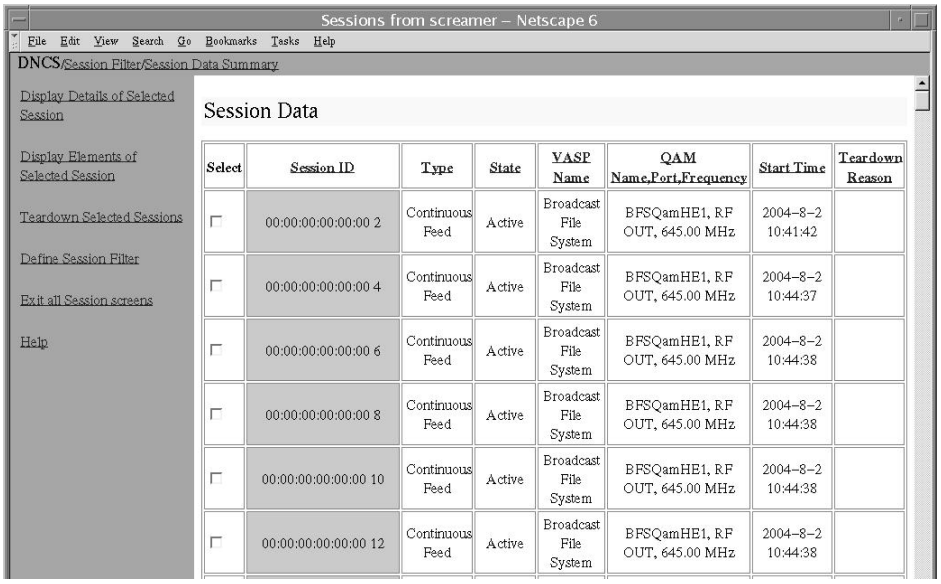
Tearing Down the BFS and OSM Sessions

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.



Select	Session ID	Type	State	VASP Name	QAM Name,Port,Frequency	Start Time	Teardown Reason
☐	00:00:00:00:00:00 2	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004-8-2 10:41:42	
☐	00:00:00:00:00:00 4	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004-8-2 10:44:37	
☐	00:00:00:00:00:00 6	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004-8-2 10:44:38	
☐	00:00:00:00:00:00 8	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004-8-2 10:44:38	
☐	00:00:00:00:00:00 10	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004-8-2 10:44:38	
☐	00:00:00:00:00:00 12	Continuous Feed	Active	Broadcast File System	BFSQamHE1, RF OUT, 645.00 MHz	2004-8-2 10:44:38	

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 87). 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.

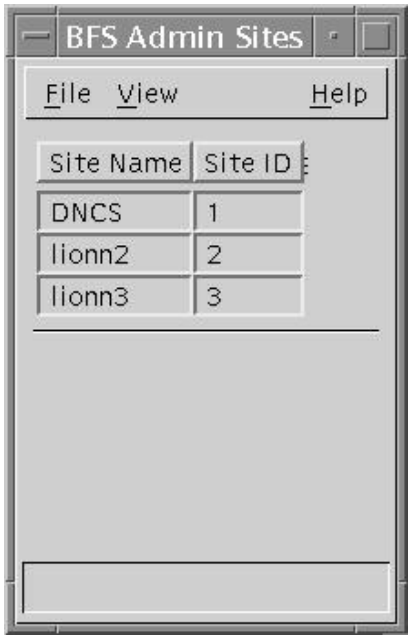
Authorizing the BRF

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)?

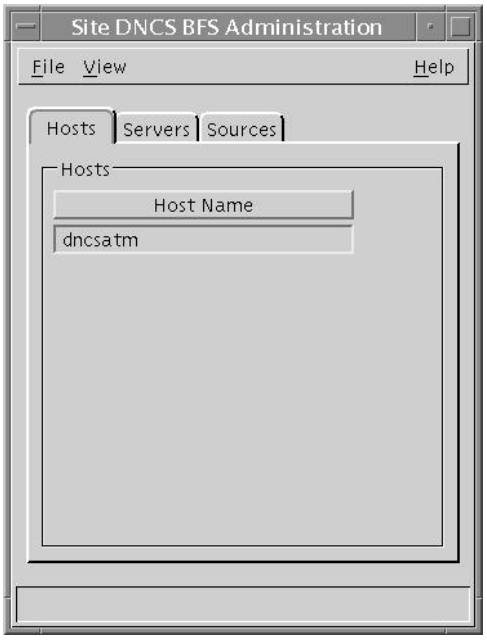
a If **yes**, click **BFS Admin**. The BFS Admin Sites window opens.



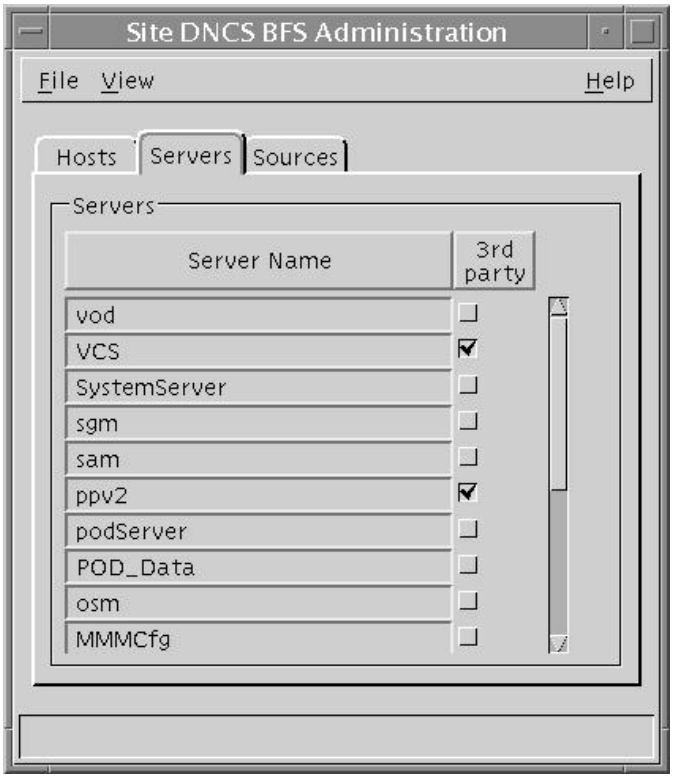
b If **no**, go to step 3.

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 ***Reset the Modulators*** (on page 92).

  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.

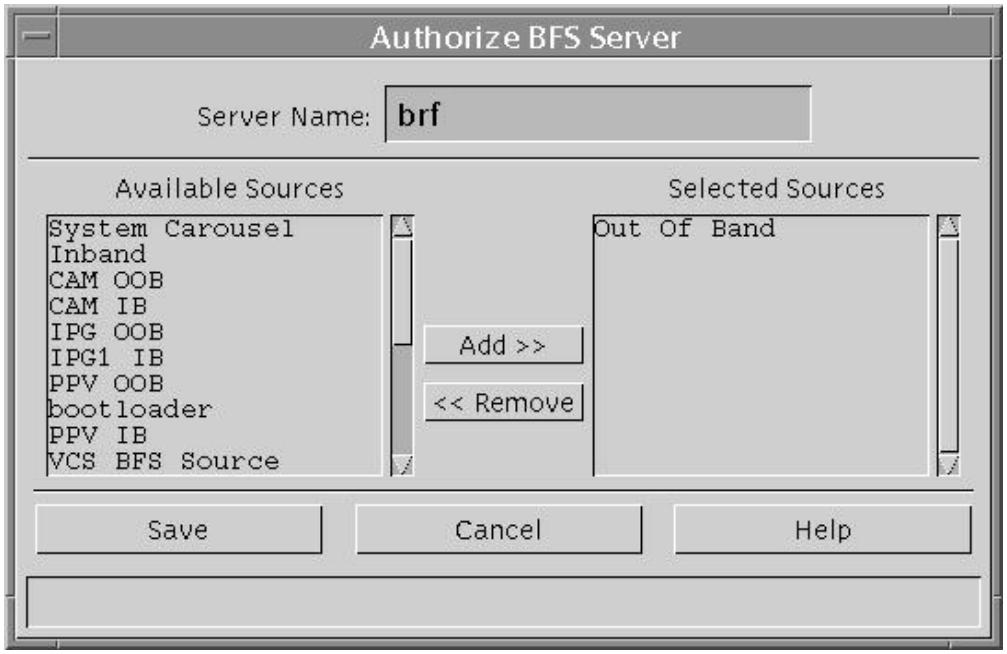
6 Click **File** and then select **New**. The Authorize BFS Server window appears.

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 ***Reset the Modulators*** (on page 92).

Reset the Modulators

After completing the upgrade process, it is now time to reset the modulators in your network. Go to the **Establish a Download Sequence** and **Download Software to the Modulators** sections in the following installation guides:

- *System Release 2.7/3.7/4.2 Service Pack 0.2 Release Notes and Installation Instructions* (part number 4019303)
- *GQAM Modulator Software Version 4.2.2 Release Notes* (part number 4031376)
- *MQAM Software Version 2.6.2 Release Notes and Installation Instructions* (part number 4013674)
- *QAM Modulator Software Version 2.5.1 Release Notes and Installation Instructions* (part number 740242)

For QPSK modulators, go to the **Download Software to the QPSK Modulators** and **Continue to Monitor the DHCT Sign-On Traffic** sections in the *QPSK (Release E14) Release Notes and Installation Instructions* (part number 4013491).

Final System Validation Tests

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.

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 *Reinstall the NMI Software (Optional)* (on page 97).

   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.

Reinstall the NMI Software (Optional)

If you are using NMI software and removed it as part of the upgrade, you need to reinstall the NMI software now. Complete the following steps to reinstall the NMI software.

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 **pkginfo -l | grep SAInmi** and then press **Enter**. The system lists the SAInmi package if it is installed.
4. Is SAInmi installed?
   - If **yes**, go to step 5.
   - If **no**, you do not have NMI loaded onto your system. Skip the rest of this procedure.
5. Close any user interfaces that may be open on the DNCS.

   Note: If the DNCS has any open user interfaces, you will be unable to remove the NMI software.
6. Type **ps -ef | grep ui** and then press **Enter**. The system displays a list of user interface processes that may still be running.
7. On a sheet of paper, write down the process IDs (PIDs) of any user interface process that is still running.
8. Type **kill -9 [PID]** and then press **Enter** for any user interface process that is still running. The system stops the user interface processes.
9. To reinstall the NMI software, refer to *DBDS Alarm Manager 1.0 Installation Instructions* (part number 745262) and follow the **Install the NMI Software Directly Onto the DNCS** procedure.

Reattach the Disk Mirrors

Introduction

In this procedure, you will reattach the disk mirrors of the Enterprise 450 or Sun Fire V880 DNCS.

Do not perform this procedure unless you are certain that the upgrade has been successful. After the mirrors are reattached, you cannot easily roll back to the previous system release; instead, you will have to restore your system using your latest file system and database backup tapes.

Reattaching the Disk Mirrors

Complete the following steps to reattach the disk mirrors of the DNCS.

1. Insert the **DBDS Maintenance CD** into the CD drive of the DNCS.
2. Type **df -n** and then press **Enter**. A list of the mounted file systems appears.

   Note: The presence of /cdrom in the output confirms that the system correctly mounted the CD.
3. 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 **/cdrom/cdrom0/s3/backup_restore/mirrState -a** and then press **Enter**. The system begins to reattach the disk mirrors.
5. Type **y** and press **Enter** at prompt. The mirrState displays the **Are you sure that you want to proceed** message.
6. After the disk mirroring process is complete, type **metastat | more** and then press **Enter**. The system displays the status of all the metadevices on the DNCS.

   Note: Press the **Spacebar**, if necessary, to scroll through all of the output.
7. Verify that the following two conditions are true:
   - The designation **ok** appears in the **State** column next to each metadevice.
   - No **Hot Spare** indicates **In Use**.
8. Are both conditions (listed in step 7) true?
   - If **yes** (to both conditions), the upgrade is complete.
   - If **no** (to either or both conditions), call Cisco Services for help in resolving these issues with the metadevices.

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 38)
- For the Informix database - see ***Back Up the Informix Database*** (on page 44)

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 450 or Sun Fire V880 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 In ***Stop System Components*** (on page 50), use these procedures, if necessary.
   a ***Stopping the Application Server*** (on page 51)
   b ***Stopping the DNCS*** (on page 52)
2 From an xterm window on the Application Server, type **shutdown -g0 -y -i0** and then press **Enter**. The system halts all processes on the Application Server and an **ok** prompt appears.
3 Place the **DBDS Maintenance CD** in the DNCS CD drive.

   Notes:

   - If SAIpatch 4.2.1.10 is installed, use Maintenance CD 4.3 with Backup_Restore 6.0.25p1.
   - If SAIpatch 4.2.1.6 is installed, use Maintenance CD 3.0.14 with Backup_Restore 6.0.11.

4 Log in to the DNCS as **root** user.
5 Open an xterm window on the DNCS.

   Note: You will have root permissions in the xterm window.

6 Type **/cdrom/cdrom0/s3/backup_restore/make_d700_bootable** and then press **Enter**. A message appears that seeks confirmation to make bootable the disk device that contains the old software.

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

8 Type **y** and then press **Enter**. The DNCS reboots.

9 Log in to the DNCS as **root** user.

10 Open an xterm window on the DNCS.

Note: You have root permissions in the xterm window.

11 Type **pkginfo -l SAIdncs** and then press **Enter**. The system displays the version of software now running on the DNCS.

12 Is the version of software running on the DNCS version 4.2.0.x?

- If **yes**, continue the rollback by going to step 13; the DNCS successfully rebooted with the old software in place.
- If **no**, call Cisco Services for help in determining why the DNCS failed to reboot with the old software in place.

13 Type **/cdrom/cdrom0/s3/backup_restore/make_d500_bootable** and then press **Enter**. A message appears that seeks confirmation to make bootable the disk device that contains the old software.

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

Results:

- The make_d500_bootable script reconfigures the mirrored disks on the DNCS.
- A message appears that seeks permission to reboot the server

15 Type **y** and then press **Enter**. The DNCS reboots.

16 Log in to the DNCS as **root** user.

17 Open an xterm window on the DNCS.

18 Type **shutdown -y -g0 -i6** and then press **Enter** to reboot the system.

19 Log into the DNCS as **dncs** user.

20 Open an xterm window on the DNCS.

21 Change to root user by typing **su-** and entering the **root** password.

Note: You will have root permissions in the xterm window.

22 Type **/cdrom/cdrom0/s3/backup_restore/mirrState -a** and then press **Enter**. The system displays the following message:

WARNING!
Proceeding beyond this point will ATTACH all d7xx submirrors.
Are you certain you want to proceed?

23 Type **y** and then press **Enter**. The system enables the disk mirroring functions on the DNCS.

Notes:

- Depending upon your system configuration, it may take up to an hour for all of the data to become mirrored.
- To monitor the mirroring process, open another xterm window on the DNCS, type **syncwait.ksh**, and then press **Enter**.

  Note: Continue with step 24. You do *not* have to wait for disk mirroring to complete before continuing.

24 At the ok prompt on the Application Server, type **boot** and then press **Enter**. The Application Server reboots.

25 While the Application Server is rebooting, go to an xterm window on the DNCS and type **dncsStart** and then press **Enter**. The DNCS processes start.

26 When the Application Server completes the boot process, log on as **dncs** user.

27 Open an xterm window on the Application Server and type **appStart** and then press **Enter**. The Application Server processes start.

28 When the disk mirroring has completed, type **eject cdrom** and then press **Enter**. The system ejects the CD.

29 When all DNCS and Application Server processes are started, go to ***Reinstall the NMI Software (Optional)*** (on page 107).

Reinstall the NMI Software (Optional)

If you are using NMI software and removed it as part of the upgrade, you need to reinstall the NMI software now. Complete the following steps to reinstall the NMI software.

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 **pkginfo -l | grep SAInmi** and then press **Enter**. The system lists the SAInmi package if it is installed.
4. Is SAInmi installed?
   - If **yes**, go to step 5.
   - If **no**, you do not have NMI loaded onto your system. Skip the rest of this procedure.
5. Close any user interfaces that may be open on the DNCS.

   Note: If the DNCS has any open user interfaces, you will be unable to remove the NMI software.
6. Type **ps -ef | grep ui** and then press **Enter**. The system displays a list of user interface processes that may still be running.
7. On a sheet of paper, write down the process IDs (PIDs) of any user interface process that is still running.
8. Type **kill -9 [PID]** and then press **Enter** for any user interface process that is still running. The system stops the user interface processes.
9. To reinstall the NMI software, refer to *DBDS Alarm Manager 1.0 Installation Instructions* (part number 745262) and follow the **Install the NMI Software Directly Onto the DNCS** procedure.

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:

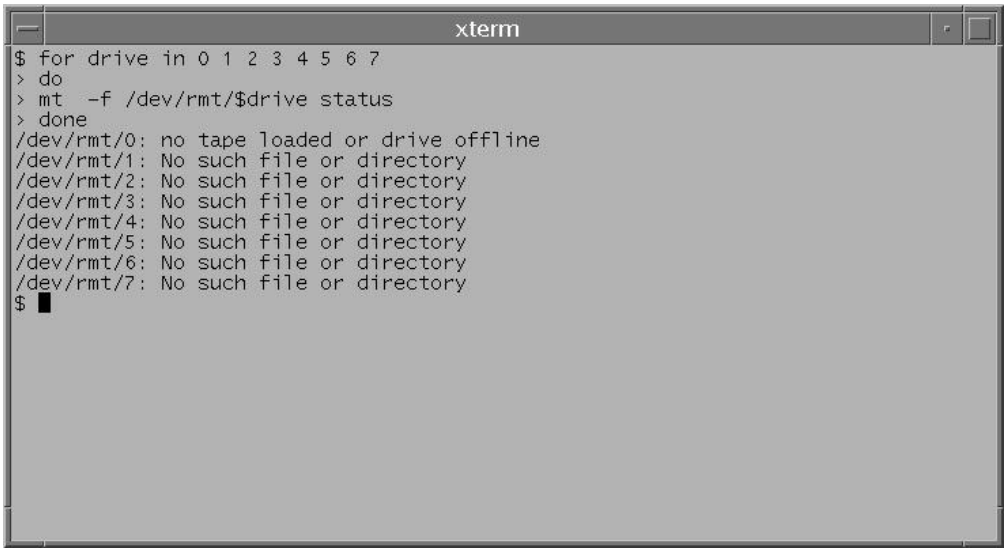
- You will only have to complete this procedure once. The device name of your tape drive will not change unless you specifically change the tape drive configuration.
- Do not have a tape in the tape drive when you complete this procedure.

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

Direct ASI Installation and Configuration Procedures

Introduction

To reduce network infrastructure complexity, we have removed the requirement for a Broadband Integrated Gateway (BIG) to transmit Broadcast File System (BFS) data to QAMs. The BFS now produces a full transport stream, and no longer feeds an MPEG stream to the BIG for further processing and multiplexing.

The DNCS is now configurable so that inband data can be transmitted through the current asynchronous transfer mode (ATM) interface or through a new asynchronous serial interface (ASI). This appendix provides instructions for installing and configuring the ASI.

In This Appendix

Check for the Existence of the ASI Package

Before installing the ASI card, determine whether the ASI package currently exists on the DNCS. If it currently exists on the DNCS, you will have to remove it because a new ASI package cannot successfully install over an existing ASI package. Follow these instructions to check for the ASI package and then to remove it, if necessary.

Notes:

- Be sure that you have the CD containing the old ASI package before deleting the package from the DNCS. You may need the old software should you ever have to roll back from an unsuccessful upgrade.
- Normally, systems without an ASI card should not have an ASI package.

1. If necessary, open an xterm window on the DNCS.
2. Type **pkginfo -l SAIasi** and then press **Enter**. The system displays information about the ASI package, if it exists.
3. After completing step 2, did the ASI package exist on the DNCS?
   - If **yes**, go to step 4 to begin removing the package.
   - If **no**, go to ***Enable the ASI Feature*** (on page 116).
4. Follow these instructions to log on to the xterm window as root user.
   a. Type **su -** and then press **Enter**. The password prompt appears.
   b. Type the root password and then press **Enter**.
5. Type **pkgrm SAIasi** and then press **Enter**. The system removes the ASI package from the DNCS.
6. Go to ***Enable the ASI Feature*** (on page 116).

Enable the ASI Feature

After removing the ASI package from the DNCS, contact Cisco Services. Engineers at Cisco Services will enable the Direct ASI feature.

Stop the System Components

Introduction

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

Stopping the Application Server

Choose one of the following procedures based upon the resident application that runs on your system:

- For sites that support the SA Resident Application, follow the instructions in **Stopping the Application Server at SARA Sites**.
- For sites that support the Aptiv resident application, follow the instructions in **Stopping the Application Server at Aptiv Sites**.

Stopping the Application Server at SARA Sites

Complete these steps to stop the Application Server at sites that support the SA Resident Application.

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

   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 appears.
3. Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**. The system displays all Application Server processes.

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

Shutting Down the SA Application Server

After stopping the SA Application Server, follow these steps to stop the Application Server.

1 Log on to an xterm window on the Application Server as **root** user.

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 command from the remote shell.

2 Type **/usr/sbin/shutdown -i0 -g0 -y** and then press **Enter**. The Application Server shuts down and the ok prompt appears.

Stopping the Application Server at Aptiv Sites

Complete these steps to stop the Application Server at sites that support the Aptiv resident application.

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

2 From an xterm window on the Application Server, type **CheckServices** and then press **Enter**. A list of drivers appears.

Note: Each driver is associated with an Application Server process.

3 Wait until the word **No** appears next to each driver.

4 Log in to an xterm window as **root** user.

5 Type **init 0** and then press **Enter**. The Application Server shuts down and an ok prompt appears.

6 Go to ***Stopping the DNCS*** (on page 52). Then go to ***Install the ASI Card*** (on page 119).

Install the ASI Card

The Common Download feature requires that a special card be installed in the DNCS. Sites that support both the Direct ASI feature, as well as the Common Download feature, may find it convenient to install the Common Download card at the same time that the Direct ASI card is installed. For this reason, information pertaining to the Common Download card is included in step 4.

After deleting (if necessary) the ASI package from the DNCS, follow the instructions in this section to install the ASI card.

1. Follow these instructions, if necessary, to log in to the xterm window as root user.

   Note: If you had to remove the ASI package in the previous procedure, you should already be root user.

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

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

2. Type **shutdown -y -g0 -i0** and then press **Enter**. The DNCS shuts down and the ok prompt appears.
3. Turn off power to the DNCS.
4. Remove the cover to the DNCS and install the ASI card into one of the following slots:
   - For a Enterprise 450 DNCS, Slot 5
   - For a Sun Fire V880 DNCS, Slot 7
5. Is your site you upgrading to support the common download feature?
   - If **yes**, then install the common download card in the following slot:
     - For a Sun Fire V880 DNCS, Slot 2
     - For a Enterprise 450 DNCS, Slot 4
   - If **no**, go to step 6.
6. Put the cover back on the DNCS.
7. Turn on power to the DNCS.
8. Log on to the DNCS as **root** user.
9. Did the DNCS processes start after you turned on the power?
   - If **yes**, go to ***Stopping the DNCS*** (on page 52). Then, go to ***Install the ASI Package*** (on page 120).
   - If **no**, go to ***Install the ASI Package*** (on page 120).

Install the ASI Package

After installing the ASI card into the DNCS, follow these instructions to install the ASI package.

Note: If you have properly followed the instructions in the previous procedure, you should be logged on as root user to the DNCS.

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

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

2 Insert the CD labeled similarly to **SAIasi** into the cdrom drive of the DNCS.

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

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

4 Type **cd /cdrom/cdrom0** and then press **Enter**.

5 Type **install_pkg** and then press **Enter**. Software installs which prepares the DNCS for Direct ASI support.

6 Type **eject cd** and then press **Enter**. The CD ejects from the DNCS.

7 Go to ***Configure the ASI Card*** (on page 121).

Configure the ASI Card

Now that you have installed the ASI package, follow these instructions to configure the ASI card.

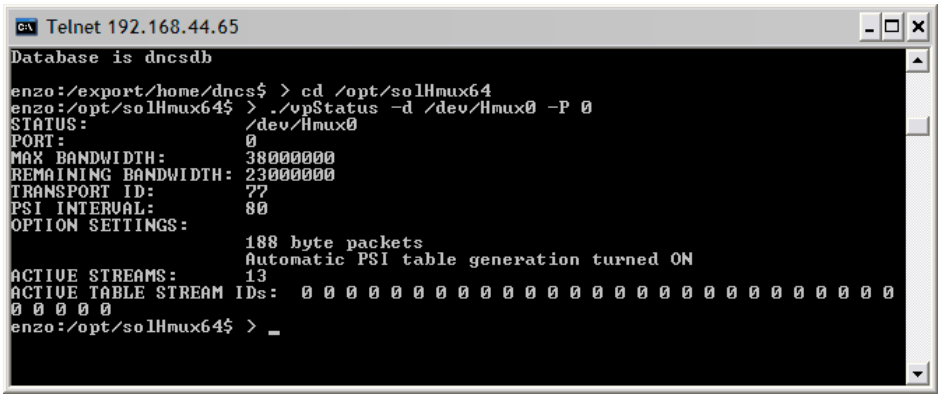
1. Type **cd /dvs/dncs/bin** and then press **Enter**. The /dvs/dncs/bin directory becomes the working directory.
2. Type **./configureASI.pl** and then press **Enter**. If the configuration script detects a problem with how the card is configured, the script displays a message seeking confirmation to correct the problem.
3. Type **y** and then press **Enter**. The system modifies the configuration of the Direct ASI card and prompts you to reboot the computer.
4. Type **/usr/sbin/shutdown -g0 -i6 -y** and then press **Enter**. The DNCS reboots.
5. Log in to the DNCS as **dncs** user.
6. At the **ok** prompt on the Application Server, type **boot**.
7. Log in to the Application Server as **dncs** user.
8. Go to ***Check the Status of the ASI Card*** (on page 122).

Check the Status of the ASI Card

After installing and configuring the ASI card and installing the ASI package, follow these instructions to test the status of the card.

1. Type **cd /opt/solHmux64** and then press **Enter**. The /opt/solHmux64 directory becomes the working directory.
2. Type **./vpStatus -d /dev/Hmux0 -P 0** and then press **Enter**. The system displays the status of the ASI card.

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



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

3. Do the results from step 2 show the ASI card to be properly installed?
   - If **yes**, go to ***Restart System Components*** (on page 123).
   - If **no**, call Cisco Services for assistance.

Restart System Components

Introduction

Use the procedures in this section to restart the DNCS and the Application Server.

Restarting the DNCS

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

   Results:

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

   Notes:

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

Restarting the Application Server

This section provides procedures for restarting either a SARA Server or a 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.

Restarting the Application Server at Rovi Corporation Sites

Complete the following steps to verify that the Passport resident application has started on the Application Server, and then to start it, if necessary.

1 Open an xterm window on the Application Server.

2 Type **CheckServices** and then press **Enter**. A list of drivers appears.

Note: Each driver is associated with an Application Server process.

3 Does the word **Yes** appear next to each driver, indicating that the process has started?

- If **yes**, you have completed this procedure.
- If **no**, go to step 4.

4 Press the middle mouse button, and then select **Passport Start**.

5 When the word **Yes** appears next to each driver, go to step 6.

6 Follow the on-screen instructions to close the window containing the list of drivers associated with the Passport resident application.

Record Configuration Data

After enabling the ASI feature on the DNCS, take a few minutes to record the BFS transport stream ID (TSID) and the QAM connection details regarding the Direct ASI card.

Note: This data may be useful for troubleshooting purposes later on.

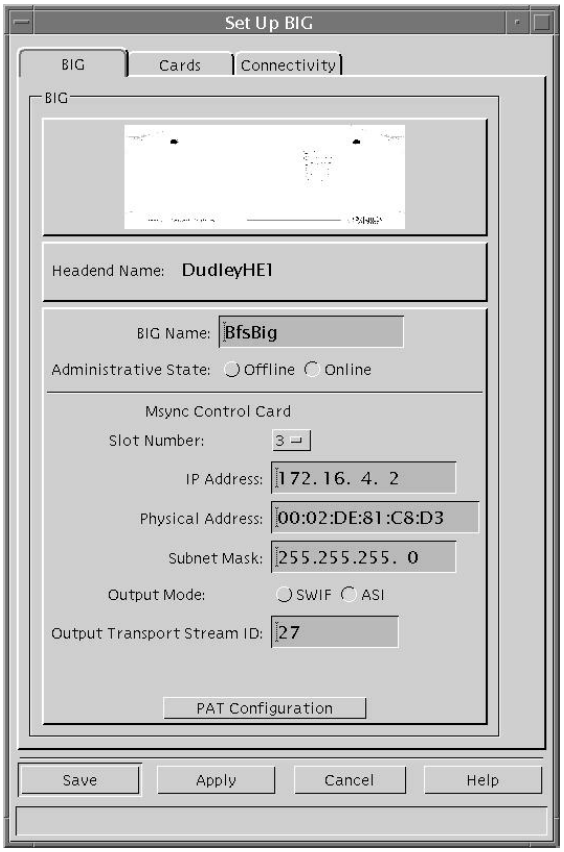
1 From the DNCS Administrative Console, select the **Element Provisioning** tab.

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

3 Double-click the **BfsBig** entry. The Set Up BIG window opens.

4 On a sheet of paper, record the **Output Transport Stream ID**.

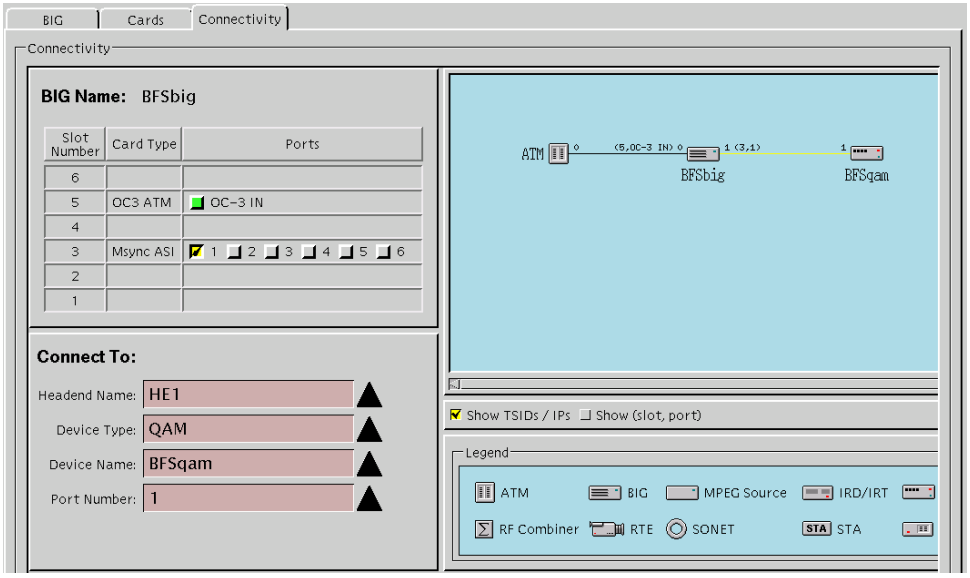
Note: In this example, the Output Transport Stream ID value is 27.



5 Click the **Connectivity** tab. The window updates to show connection data.

6 Click and drag the right border of the window to expand it.

7 Click **Show TSIDs / IPs**. The window updates to show additional connection detail.



8 Click the SWIF Transmit or Msync ASI port currently connected to the BFS QAM. In the **Connect To** area of the window, the system displays the **Headend Name**, **Device Type**, **Device Name**, and **Port Number**.

9 In the space provided, record the data displayed in step 8.

Headend Name: _____

Device Type: _____

Device Name: _____

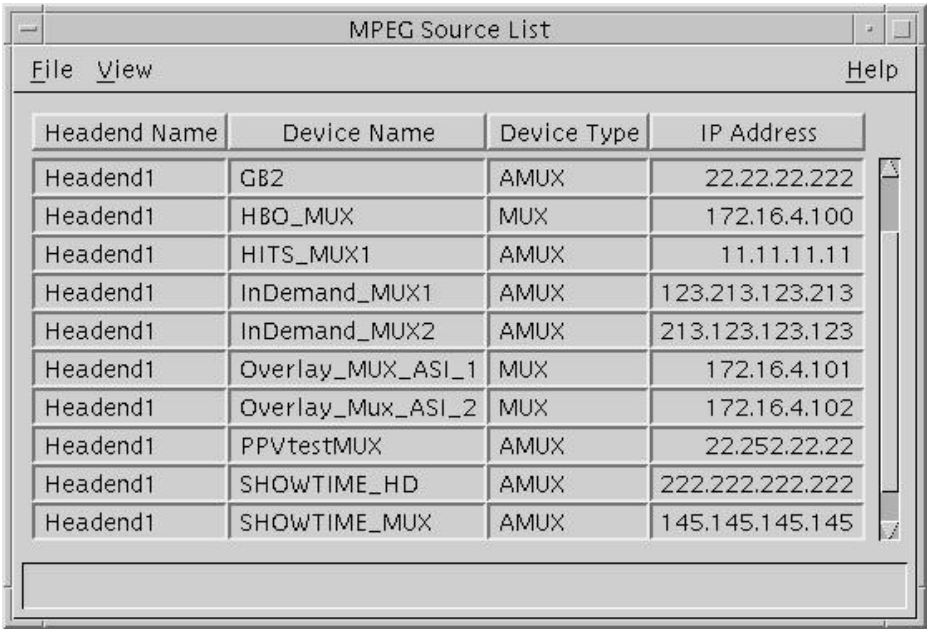
Port Number: _____

10 Click **Cancel** to close the window.

Create an MPEG Source

Your next step is to create an MPEG source. Follow these instructions to create an MPEG source.

1 From the DNCS Administrative Console, click the **Element Provisioning** tab and then select **MPEG Source**. The MPEG Source List window opens.



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

3 Follow these instructions to configure the Set Up MPEG Source window.

a Click the arrow next to the Headend Name field and choose the appropriate headend.

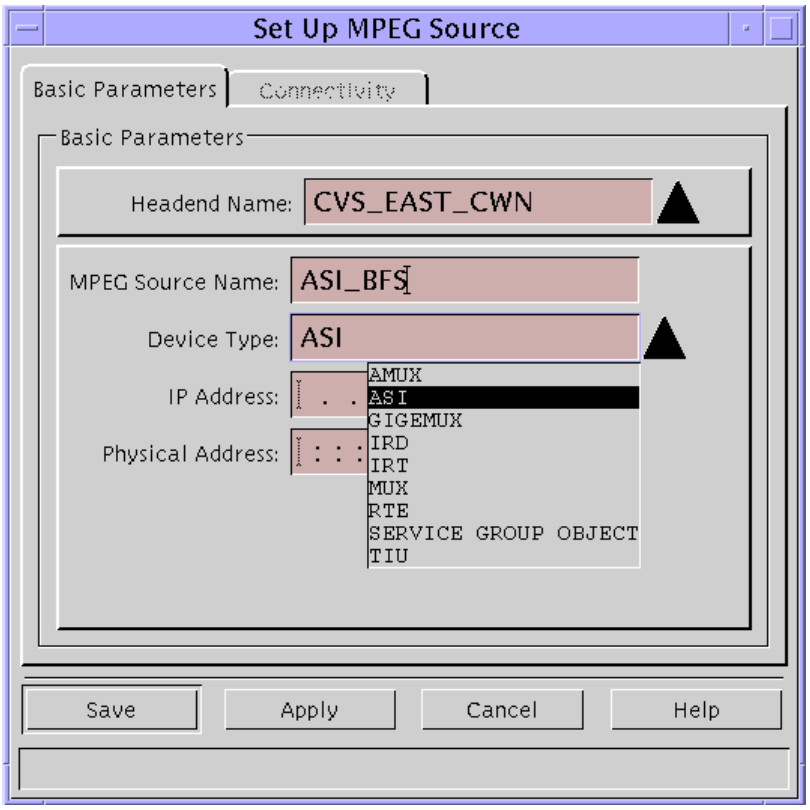
b Type ASI_BFS in the MPEG Source Name field.

c Type ASI in the Device Type field.

Note: If ASI is already configured, you can click the arrow next to the Device Type field and select **ASI**.

d Type any IP address and MAC address in the **IP Address** and **Physical Address** fields.

Note: The actual IP address and MAC address you use are not important.



e Click **Save**. The Connectivity tab becomes active.

4 Click the **Connectivity** tab on the Set Up MPEG Source window.

5 Click **Create Port**. The Port Number Prompt window opens.

6 Follow these instructions to configure the Port Number Prompt window.

   a In the **Output Port** field, type **0** (zero).

   b In the **TSID** field, type a transport stream ID (TSID) that is equal to the input TSID for the BFS QAM.

   c If the **Transport Protocol** field does not display **ASI**, click the arrow to the right of the field and select **ASI**.

   d Click **OK**. The Set Up MPEG Source window reappears and the new configuration is saved.

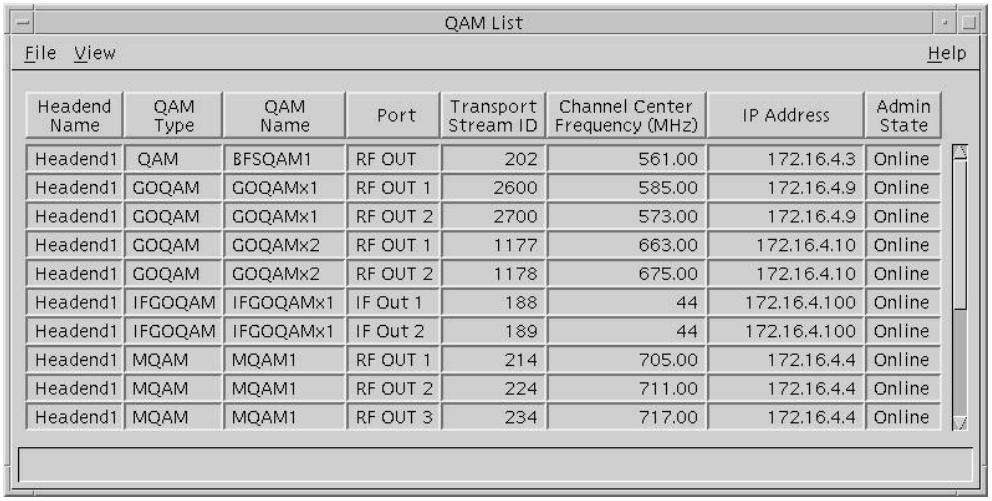
7 Click **Close**. The Set Up MPEG Source window closes.

8 Go to ***Set Up the QAM*** (on page 131).

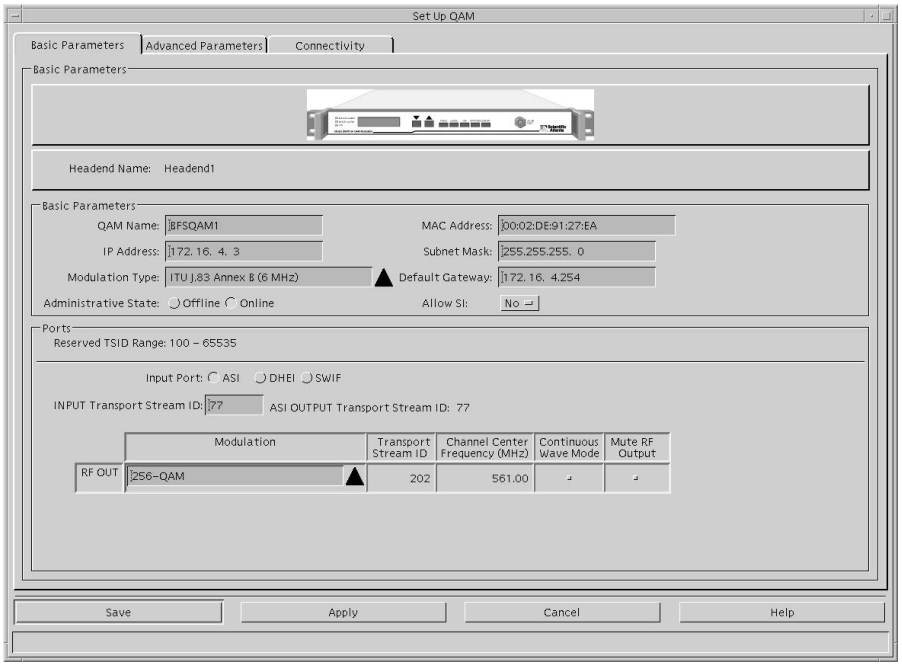
Set Up the QAM

After creating the MPEG source, follow these instructions to set up the QAM.

1 From the DNCS Administrative Console, click **Element Provisioning** and then select **QAM**. The QAM List window opens.



2 Double-click the **BFS QAM**. The Set Up QAM window opens.



3 On the Set Up QAM window, configure the **Input Port** field to **ASI**.

4 Configure the **INPUT Transport Stream ID** field with the same value that you recorded as the TSID on the Set Up MPEG Source window in a previous procedure, ***Create an MPEG Source*** (on page 128).

5 Click the **Connectivity** tab.

6 In the **Connect To** area of the window, click the arrow to the right of each of the following fields and set each field to **none**:

- **Device Type**
- **Device Name**
- **Card Type**
- **Slot Number**
- **Port Number**

Note: The system requires that you first set these fields to none before you change the configuration.

7 Click **Save**.

Important: If the **Save** button is unavailable after completing step 7, close the Set Up QAM window. Then, double-click the BFS QAM from the QAM List window to gain access again to the Set Up QAM window.

8 Now, follow these instructions to configure the remainder of the Set Up QAM window.

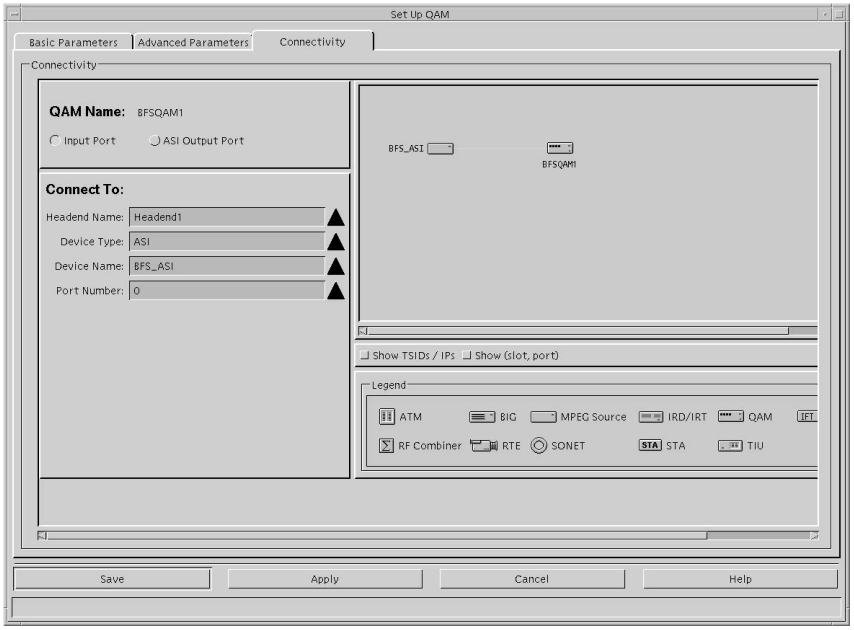
a Click the arrow to the right of the **Headend Name** field and choose the appropriate headend.

b Click the arrow to the right of the **Device Type** field and choose the appropriate device (probably **ASI**).

c Click the arrow to the right of the **Device Name** field and choose the appropriate device name.

d Click the arrow to the right of the **Port Number** field and set the port number to **0** (zero).

Example: When you are finished, the Set Up QAM window should look similar to the following example.



9 Click **Save**. The system saves the QAM configuration.

Note: A message may appear that concerns the QAM connection with Spectrum. You can ignore such a message. Click **Save** one or two more times until the QAM configuration is saved without any messages.

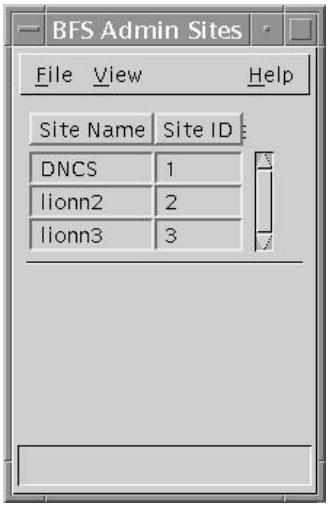
10 Close the Set Up QAM window.

11 Go to ***Set Up the BFS Host*** (on page 134).

Set Up the BFS Host

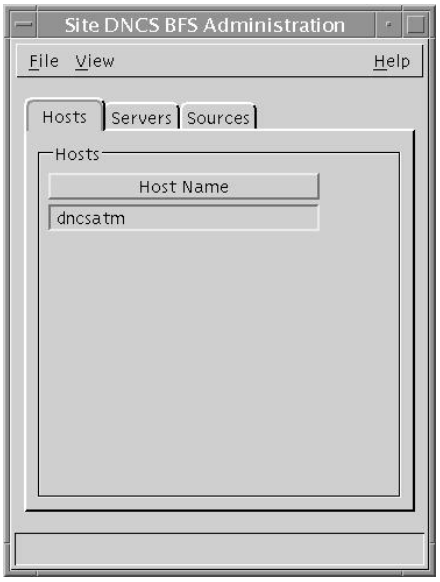
After setting up the QAM, follow these instructions to set up the BFS host.

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

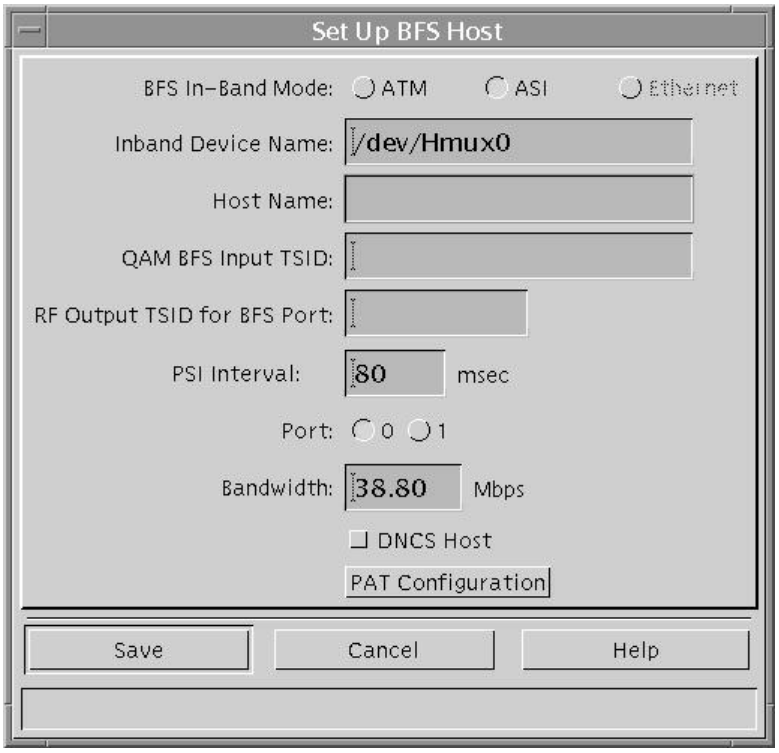


2 Double-click the site name of the system you are setting up. The Site [BFS site] BFS Administration window opens.

Note: If your site does not support RCS, this window does not appear. Instead, the window in step 3 appears.



3 Select the **Hosts** tab; then double-click on the existing DNCS host. The Set Up BFS Host window opens.



4 Follow these directions to configure the Set Up BFS Host window.

a In the **BFS In-Band Mode** field, select **ASI**.

b In the **Inband Device** Name field, type **/dev/Hmux0**.

c In the **Host Name** field, type the name of the DNCS host.

Example: dncsatm

d In the **QAM BFS Input TSID** field, type the value that represents the output TSID for the ASI_BFS MPEG source.

e In the **RF Output TSID for BFS Port** field, type the value that represents the output TSID for the BFS QAM or the BFS port on an MQAM.

f In the **PSI Interval** field, type **80**.

g In the **Port** field, select **0**.

h In the **Bandwidth** field, type **38.80**.

i Are you configuring Direct ASI on a DNCS (rather than an RNCS)?

– If **yes**, click **DNCS Host**.

– If **no**, go to step 5.

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

6 Click **Close** on the Inband Data PAT window.

7 Click **Save** on the Set Up BFS Host window. The system saves the BFS host configuration.

8 Go to *Set the BIG Offline* (on page 137).

Set the BIG Offline

After setting up the BFS source, follow these instructions to set the BIG offline.

CAUTION:

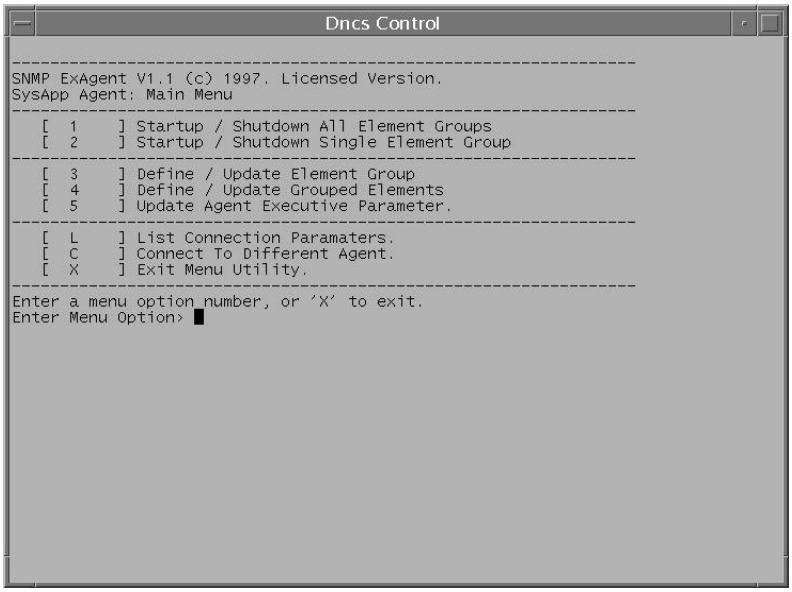
Never delete the BIG. You need the BIG if you ever have to roll back the install of Direct ASI.

1. From the DNCS Administrative Console, select the **Element Provisioning** tab.
2. Click **BIG**. The BIG List window opens.
3. Double-click the BIG. The Set Up BIG window opens.
4. At the **Administrative Status** field, select **Offline**.
5. Click **Save**. The system saves the BIG status to be offline.
6. Go to ***Stop the BFS and OSM Processes*** (on page 138).

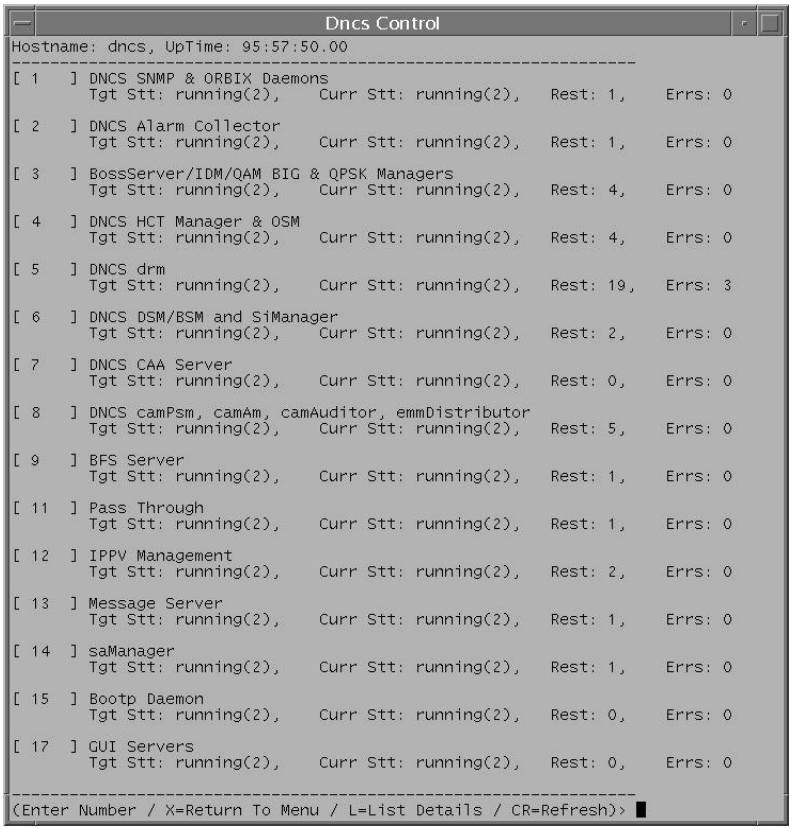
Stop the BFS and OSM Processes

After setting the BIG offline, you need to stop the BFS and OSM processes on the DNCS next. Follow these instructions to stop the processes.

1. If necessary, open an xterm window on the DNCS.
2. Type **dncsControl** and then press **Enter**. The Dncs Control window opens.



3 Type **2** (for Startup / Shutdown Single Element Group) and then press **Enter**. The Dncs Control window updates to show all the servers and processes running on the DNCS.



4 Type the number associated with **BFS Server** and then press **Enter**. The Dncs Control window updates to display a message prompting you to enter the target status for the entire element group or to type E to display the individual elements of the group.

5 Type **1** (for stopped) and then press **Enter**. A confirmation message appears.

6 Type **y** (for yes) and then press **Enter**. After a few moments, the Dncs Control window updates to display the current state (Curr Stt) of the selected group.

7 Wait until the current state of the BFS Server group is **Stopped**.

Note: The Dncs Control window updates automatically every few seconds or you can press **Enter** to force an update.

8 When the current state of the BFS Server group is **Stopped**, type the number associated with **DNCS HCT Manager & OSM** and then press **Enter**. The Dncs Control window updates to display a message prompting you to enter the target status for the entire element group or to type E to display the individual elements of the group.

9 Type **e** and then press **Enter**. The Dncs Control window updates to display the individual elements of the DNCS HCT Manager & OSM group.

10 Type the number associated with **/dvs/dncs/bin/OSM** and then press **Enter**. The Dncs Control window updates to display a message prompting you to enter the target status of the selected element.

11 Type **1** (for stopped) and then press **Enter**. A confirmation message appears.

12 Type **y** (for yes) and then press **Enter**. After a few moments, the Dncs Control window updates to display the current state (Curr Stt) of the selected element.

13 Wait until the current state of the /dvs/dncs/bin/OSM process is **Stopped**.

Note: The Dncs Control window updates automatically every few seconds or you can press **Enter** to force an update.

14 When the current state of the /dvs/dncs/bin/OSM process is **Stopped**, follow the on-screen instructions to exit from the dncsControl utility.

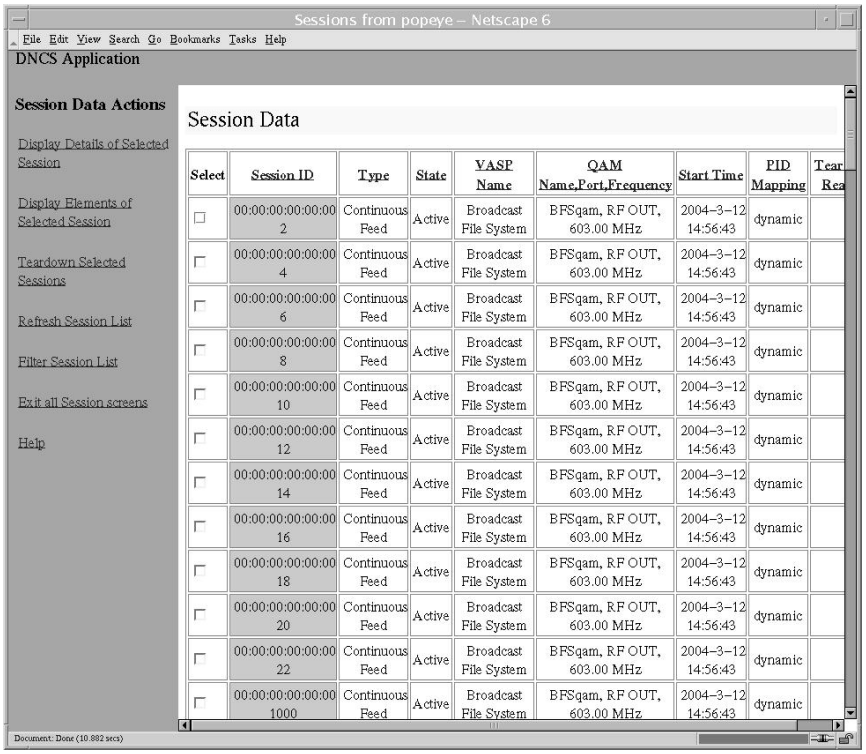
15 Go to ***Tear Down BFS Sessions*** (on page 141).

Tear Down BFS Sessions

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

1 From the DNCS Administrative Console, select the **Utilities** tab.

2 Click **Session List**. The Sessions window opens.



3 Highlight the BFS sessions and then click **Teardown Selected Sessions**. A confirmation message appears.

4 Click **OK**. The system tears down the BFS sessions.

Clear Completed, Pending, or Failed Sessions

Follow these instructions to clear completed, pending, or failed sessions.

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

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

Important: Complete this step even if the Session List window, in the previous procedure—Tear Down BFS Sessions—shows no sessions.

Enable the System for ASI

Introduction

To finally enable your system for Direct ASI, there are a few more steps you need to complete. These steps are detailed in the following sections.

Enable ASI From the DNCS GUI

Follow these instructions to configure the BFS QAM for ASI.

1. From the DNCS Administrative Console, select the **Element Provisioning** tab.
2. Click **QAM**. The QAM List opens.
3. Double-click the BFS QAM. The Set Up QAM window opens.
4. At the **Ports** field, select **ASI**.
5. Click **Save**.
6. Click **Close**. The Set Up QAM window closes.
7. Click **File** and then select **Close** on the QAM List window.

Reset the BFS QAM

Reset the BFS QAM, using one of the following methods:

- The DNCS GUI
- The front panel of the BFS QAM
- The auditQam Utility

Inspect the Front Panel of the BFS QAM

In this procedure, you will inspect the front panel of the BFS QAM to confirm that the BFS QAM is indeed configured for ASI. If the front panel reveals that the BFS QAM is not configured for ASI, you need to manually configure it. The following procedure guides you through the necessary steps.

1 Press the **Options** button on the front panel of the BFS QAM until **Input Selection** appears.

2 Does the **Input Selection** field reveal that the BFS QAM is configured for ASI?

- If **yes**, skip the remainder of this procedure and go to ***Re-Cable the System for ASI*** (on page 144).
- If **no**, continue with step 3.

3 Press the up or down arrow button until **ASI** appears in the **Input Selection** field.

4 Press **Enter** to save the newly configured BFS QAM.

Re-Cable the System for ASI

Now that the BFS QAM is configured for ASI, your next step is to configure the cabling of the BFS QAM. Follow these instructions to re-cable the system for ASI.

1 Remove the SWIF cable from the back of the BFS QAM.

2 Connect one end of the ASI cable to the back of the BFS QAM and connect the other end to the ASI connector on the back of the DNCS.

Re-Check the BFS QAM

Check the front panel of the BFS QAM periodically for an hour, or so. Make sure that the **Input Selection** field still reads **ASI**. If it no longer reads ASI, reset it to ASI.

Restart the BFS and OSM Processes

You are now ready to restart the BFS and OSM processes, which you stopped earlier in this appendix. Follow these instructions to restart the BFS and OSM processes.

Note: When you restart the BFS processes, the system rebuilds the PAT Configuration table. It may take up to 10 minutes for the PAT Configuration table to be rebuilt.

1. If necessary, open an xterm window on the DNCS.
2. Type **dncsControl** and then press **Enter**. The Dncs Control window opens.
3. Type **2** (for Startup / Shutdown Single Element Group) and then press **Enter**. The Dncs Control window updates to show all the servers and processes on the DNCS.
4. Type the number associated with **BFS Server** and then press **Enter**. The Dncs Control window updates to display a message prompting you to enter the target status for the entire element group or to type E to display the individual elements of the group.
5. Type **2** (for running) and then press **Enter**. A confirmation message appears.
6. Type **y** (for yes) and then press **Enter**. After a few moments, the Dncs Control window updates to display the current state (Curr Stt) of the selected group.
7. Wait until the current state of the BFS Server group is **Running**.

   Note: The Dncs Control window updates automatically every few seconds or you can press **Enter** to force an update.
8. When the current state of the BFS Server group is **Running**, type the number associated with **DNCS HCT Manager & OSM** and then press **Enter**. The Dncs Control window updates to display a message prompting you to enter the target status for the entire element group or to type E to display the individual elements of the group.
9. Type **e** and then press **Enter**.

   Note: The Dncs Control window updates to display the individual elements of the DNCS HCT Manager & OSM group.
10. Type the number associated with **/dvs/dncs/bin/OSM** and then press **Enter**. The Dncs Control window updates to display a message prompting you to enter the target status of the selected element.

11 Type **2** (for running) and then press **Enter**. A confirmation message appears.

12 Type **y** (for yes) and then press **Enter**. After a few moments, the Dncs Control window updates to display the current state (Curr Stt) of the selected element.

13 Wait until the current state of the /dvs/dncs/bin/OSM process is **Running**.

Note: The Dncs Control window updates automatically every few seconds or you can press Enter to force an update.

14 When the current state of the /dvs/dncs/bin/OSM process is **Running**, follow the on-screen instructions to exit from the dncsControl utility.

Powering Down the BFS BIG

Conclude your procedure for configuring your system for Direct ASI by turning off power to the BFS BIG.

Checkout Procedures for the ASI Card

Introduction

After completing the procedures in this appendix to install and configure the ASI card, complete some or all of the tests in this section to confirm that the ASI card is working as intended. These tests are in outline form, only. We assume that upgrade engineers are familiar with the detail behind each test.

Confirming the Session Count

After completing the procedures in this appendix to install and configure the ASI card, complete some or all of the tests in this section to confirm that the ASI card is working as intended. These tests are only in outline form. We assume that upgrade engineers are familiar with the detail behind each test.

1. Press the **Options** button on the front panel of the BFS QAM until the **Session Count** appears.
2. Confirm that the number of sessions on the BFS QAM is equal to the number of BFS sessions on the DNCS.
3. Re-run the procedures in ***Verify DBDS Stability*** (on page 43).

Verify DBDS Stability

Re-run the procedures in ***Verify DBDS Stability*** (on page 43).

D

Direct ASI Rollback Procedures

Introduction

Use the procedures in this appendix to roll a system back from an unsuccessful installation of Direct ASI.

Important: Never roll a system back without having first consulted with Cisco Services. In many cases, Cisco engineers can help you troubleshoot whatever problems you may have experienced with the installation of Direct ASI.

In This Appendix

Record TSID Values for BFS MPEG Source and BFS QAM

Introduction

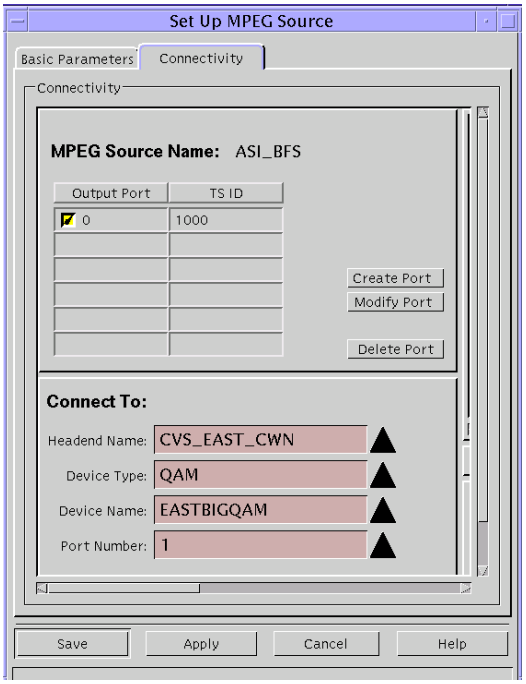
The first step in rolling back the Direct ASI installation requires that you record the current transport stream ID (TSID) values for the BFS MPEG source and the BFS QAM.

Note: If a GQAM or an MQAM is used as the BFS QAM, record the TSID for the BFS port of the GQAM or MQAM.

Recording the TSID Value for the BFS MPEG Source

Follow these instructions to record the TSID for the BFS MPEG Source.

1. From the DNCS Administrative Console, click the **Element Provisioning** tab and then select **MPEG Source**. The MPEG Source List window opens.
2. Double-click the entry for **ASI_BFS**. The Set Up MPEG Source window opens.
3. Select the **Connectivity** tab.

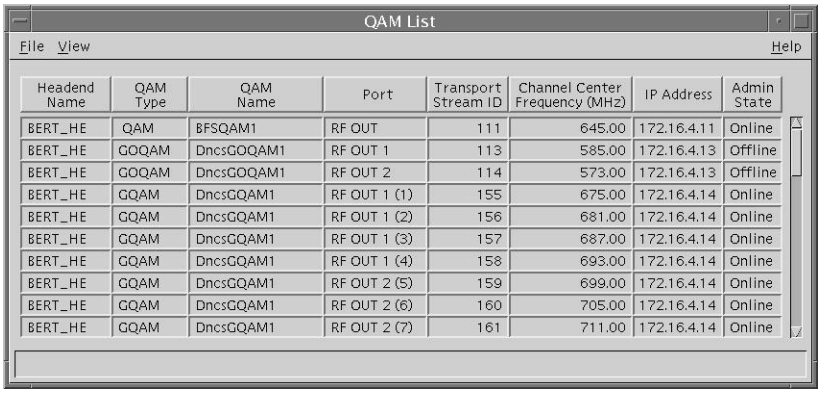


4. Record the value for **TS ID** here: _____
5. Click **Cancel** to close the Set Up MPEG Source window.
6. Click **File** and then select **Close** to close the MPEG Source List window.

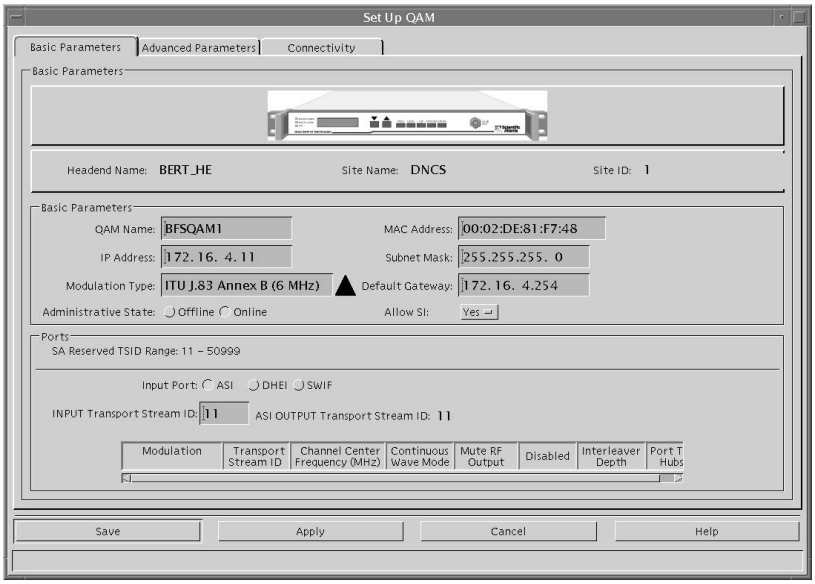
Recording the TSID Value for the BFS QAM

Follow these instructions to record the TSID for the BFS QAM.

1 From the DNCS Administrative Console, click the **Element Provisioning** tab and then select **QAM**. The QAM List window opens.



2 Double-click the entry for the BFS QAM. The Set Up QAM window opens.



3 Record the value for **Input Transport Stream ID** here: _____

4 Click **Cancel** to close the Set Up QAM window.

5 Click **File** and then select **Close** to close the QAM List window.

Turn on the BIG

Verify Power-up Sequence

Turn on the BIG and verify that the BIG goes through a power-up sequence. Various lights should illuminate. After about a minute, the BIG should settle into a steady state.

Record Configuration Data

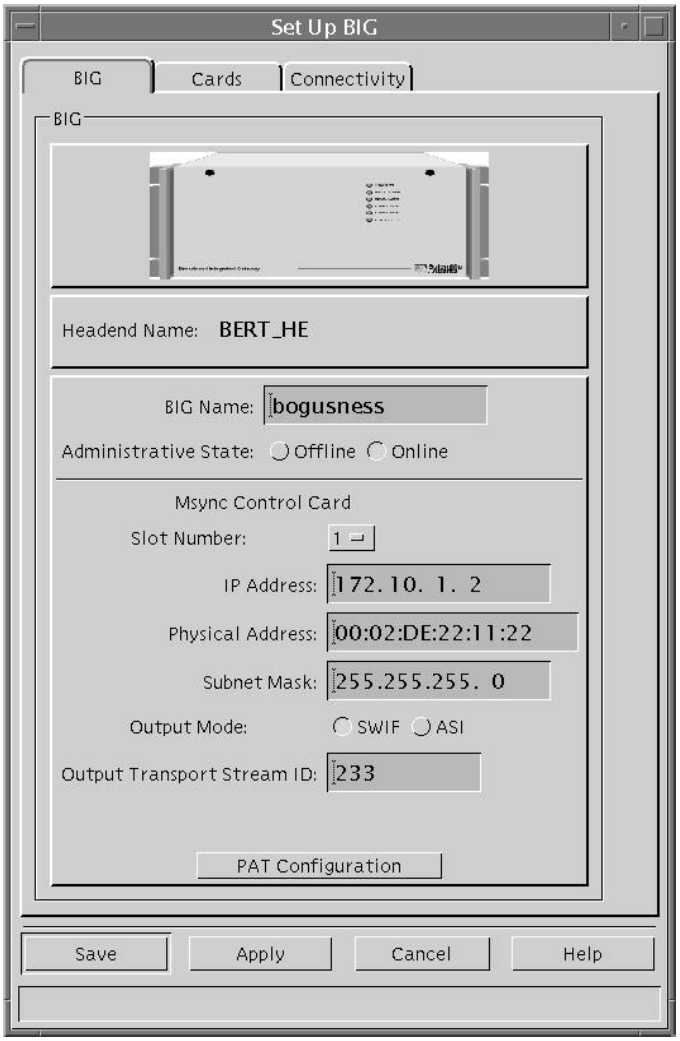
When you configured your system for Direct ASI in Appendix C, one of the procedures called for you to record the BFS TSID and the QAM connection details regarding the Direct ASI card. If you failed to complete the ***Record Configuration Data*** (on page 125) procedure when you configured your system for Direct ASI, complete that procedure now.

Set the BIG Online

Follow these instructions to set the BIG online.

1 From the DNCS Administrative Console, click the **Element Provisioning** tab and then select **BIG**. The BIG List window opens.

2 Double-click the entry for the BIG. The Set Up BIG window opens.



3 Click **Online** in the **Administrative State** field.

4 Click **Save**.

5 Click **File** and then select **Close** to close the BIG List window.

Reconfigure the QAM

Follow these instructions to reconfigure the BFS QAM to support the rollback of Direct ASI.

1. From the DNCS Administrative Console, click the **Element Provisioning** tab and then select **QAM**. The QAM List window opens.
2. Double-click the entry for the BFS QAM. The Set Up QAM window opens.
3. Select the **Connectivity** tab.
4. In the **Connect To** area of the window, click the arrow to the right of each of the following fields and set each field to **none**:
   - **Device Type**
   - **Device Name**
   - **Card Type**
   - **Slot Number**
   - **Port Number**
5. Click **Save**.
6. Select the **Basic Parameters** tab on the Set Up QAM window.
7. In the **Input Port** field, select **SWIF**.

   Exception: If your system uses ASI output from the Msync card, leave the Input Port field at **ASI**.
8. In the **Input Transport Stream ID** field, enter the value from the SWIF transmit card on the BIG.

   Note: You can find this value by clicking **Show TSIDs** from the Connectivity tab of the Set Up BIG window.
9. Click **Save**.
10. Select the **Connectivity** tab again on the Set Up QAM window.

11 Follow these instructions to configure the fields in the **Connect To** area of the window to support the BIG.

Note: Click the arrow to the right of each field to change the value of the field.

a Set the **Device Type** field to **BIG**.

b Set the **Device Name** field to match the name of the BFS BIG.

c Set the **Card Type** field to **SWIF Transmit**.

Exception: Select **Msync** if your system uses ASI output from the Msync card.

d Set the **Slot Number** field to whatever slot the SWIF transmit card is installed in the BIG.

e Set the **Port Number** field to the port used by the SWIF transmit card in the BIG.

12 Click **Save**.

13 Close the Set Up QAM window.

Reconnect the BIG

Follow these instructions to reconnect the input cable from the BFS QAM to the BIG.

1. Remove the ASI input cable from the back of the BFS QAM.
2. Reinstall the SWIF cable to the back of the BFS QAM.

Configure the Front Panel of the BFS QAM

In this procedure, you will inspect the front panel of the BFS QAM to confirm that the BFS QAM is indeed configured for SWIF. If the front panel reveals that the BFS QAM is *not* configured for SWIF, you need to manually configure it. The following procedure guides you through the necessary steps.

1 Press the **Options** button on the front panel of the BFS QAM until **Input Selection** appears.

2 Does the **Input Selection** field reveal that the BFS QAM is configured for **SWIF**?

- If **yes**, you have completed this procedure; go to ***Configure Inband Data*** (on page 159).
- If **no**, continue with step 3.

3 Press the up or down arrow button until **SWIF** appears in the **Input Selection** field.

4 Press **Enter** to save the newly configured BFS QAM.

Configure Inband Data

After reconnecting the BIG, follow these instructions to configure inband data.

1. From the DNCS Administrative Console, select the **Application Interface Modules** tab.
2. Click **Inband Data Config**. The Inband Data Configuration window opens.
3. In the **BFS In-Band Mode** field, select **ATM**.
4. Click **Save**.
5. Close the Inband Data Configuration window.

Set Up DNCS Host

Follow these instructions to configure the DNCS host.

1. From the DNCS Administrative Console, select the **Application Interface Modules** tab.
2. Click **BFS Admin**. The BFS Administration window opens.
3. Select the **Hosts** tab.
4. Double-click **dncsatm**. The Set Up BFS Host window opens

   Note: If this is a distributed site (supports the RNCS feature), double-click the DNCS site.
5. On the Set Up BFS Host window, confirm that the **Host Name** is **dncsatm** and that the other fields are empty.
6. Close the Set Up BFS Host window.
7. Select **Sources** on the BFS Administration window. The window updates to list all BFS sources.
8. Double-click Source ID **2**. The Set Up BFS Source window opens.
9. On the Set Up BFS Source window, verify that the **Transmit Type** is **In-band** and that the **Device Name** is **/dev/xtipvc0**.
10. Click **Save** to close the Set Up BFS Source window.
11. Repeat steps 8 through 10 for all inband sources, plus any customized inband sources defined by the system operator.

    Note: An inband source usually has the designation IB as part if its name.

Stop the BFS, OSM, and siManager Processes

You next need to stop the BFS, OSM, and siManager processes on the DNCS. Follow these instructions to stop the processes.

1. From the DNCS Control window, click to highlight the **bfsRemote** process.
2. Click **Process** and then select **Stop Process**. In a few minutes, the indicator for the bfsRemote process changes from green to red.

   Important: Do not go to step 3 until the indicator has changed to red.
3. From the DNCS Control window, click to 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.

   Important: Do not go to step 5 until the indicator has changed to red.
5. From the DNCS Control window, click to highlight the **osm** process.
6. Click **Process** and then select **Stop Process**. In a few minutes, the indicator for the osm process changes from green to red.

   Important: Do not go to step 7 until the indicator has changed to red.
7. From the DNCS Control window, click to highlight the **siManager** process.
8. Click **Process** and then select **Stop Process**. In a few minutes, the indicator for the siManager process changes from green to red.

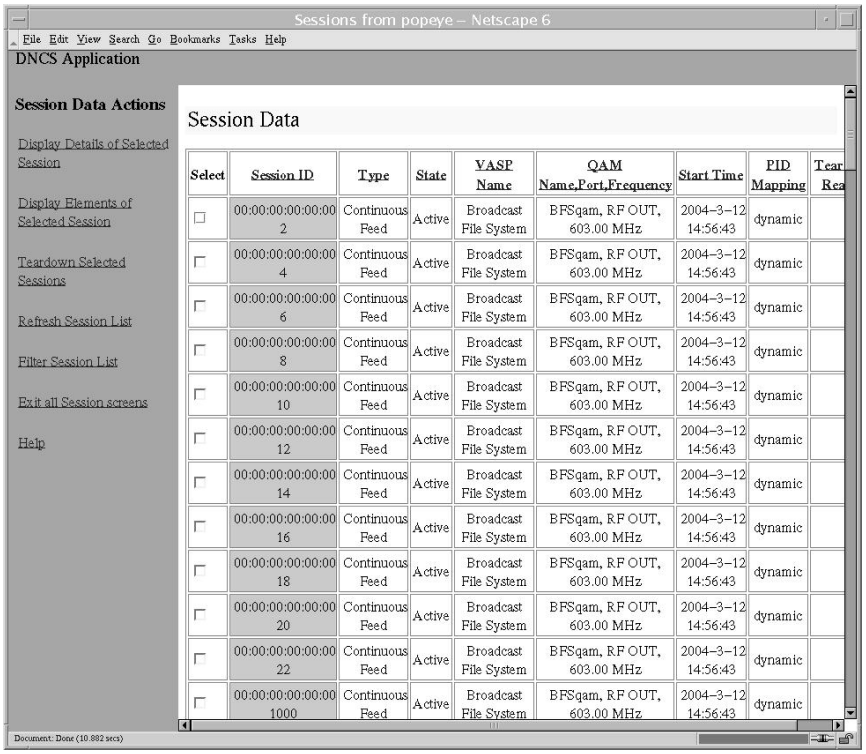
   Important: Do not go to the next procedure until the indicator has changed to red.

Tear Down BFS Sessions

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

1 From the DNCS Administrative Console, select the **Utilities** tab.

2 Click **Session List**. The Sessions window opens.



3 Highlight the BFS sessions and then click **Teardown Selected Sessions**. A confirmation message appears.

4 Click **OK**. The system tears down the BFS sessions.

Clear Completed, Pending, or Failed Sessions

Follow these instructions to clear completed, pending, or failed sessions.

1. If necessary, open an xterm window on the DNCS.
2. Type **clearDbSessions -c** and then press **Enter**.

   Important: Complete this step even if the Session List window, in the previous procedure—Tear Down BFS Sessions—shows no sessions.

Stop the BFS QAM

After running the clearDbSessions command to clear completed, pending, or failed sessions, you need to turn off the BFS QAM. Locate the power switch on the back panel of the BFS QAM and set it to the **Off** position.

Restart the BFS, OSM, and siManager Processes

Follow these instructions to restart the BFS, OSM, and siManager processes.

1. From the DNCS Control window, click to highlight the bfsRemote process.
2. Click **Process** and then select **Start Process**. In a few minutes, the indicator for the bfsRemote process changes from red to green.

   Important: Do not go to step 3 until the indicator has changed to green.
3. From the DNCS Control window, click to highlight the **bfsServer** process.
4. Click **Process** and then select **Start Process**. In a few minutes, the indicator for the bfsServer process changes from red to yellow.

   Note: The bfsServer process will not show green because the BFS QAM is currently stopped.

   Important: Do not go to step 5 until the indicator has changed to yellow.
5. From the DNCS Control window, click to highlight the **osm** process.
6. Click **Process** and then select **Start Process**. In a few minutes, the indicator for the osm process changes from red to green.

   Important: Do not go to step 7 until the indicator has changed to green.
7. From the DNCS Control window, click to highlight the **siManager** process.
8. Click **Process** and then select **Start Process**. In a few minutes, the indicator for the siManager process changes from red to green.

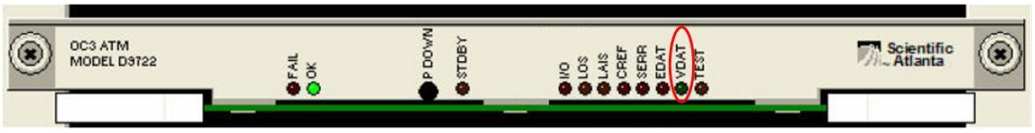
   Important: Do not go to the next procedure until the indicator has changed to green.

Restart the BFS QAM

Locate the power switch on the back panel of the BFS QAM and set it to the **On** position.

Notes:

- The BFS sessions that you tore down earlier in this appendix will rebuild in 10 to 15 minutes.
- After the BFS sessions have rebuilt, the indicator for the bfsServer process on the DNCS Control window will change from yellow to green.
- After the BFS sessions have rebuilt, the VDAT light on the BIG should illuminate.



E

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 172).
2. Place all Disaster Recovery jobs on hold. See ***Place Disaster Recovery Jobs on Hold*** (on page 175).
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 176).

   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 178).

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: 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 176).

   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 178).

   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: 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 QAM's 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 QAM's 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 be 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 a 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 transfered 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 66) and then continue with ***Take Disaster Recovery Jobs Off Hold*** (on page 178).

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

Part Number 4023737 Rev C
April 2012 Printed in USA