System Release 2.7/3.7/4.2 Service Pack 2

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

Appendix C Direct ASI Installation and Configuration Procedures133

Appendix D Direct ASI Rollback Procedures 169

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 2 (SP2). 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 SP2 software onto the Digital Network Control System (DNCS) and the SA Application Server.

Related Publications

You may find the following publications useful as resources when you implement the procedures in this document.

- *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455)
- *Configuring Variable Length Subnet Masks in System Release 2.1 or 3.0 Upgrades* (part number 4000375)
- *CoolTools Utilities User's Guide* (part number 749640)
- *DBDS Alarm Manager 1.0 Installation Instructions* (part number 745262)
- *DBDS Backup and Restore Procedures For SR 2.2 Through 4.2* (part number 4013779 Revision A)
- *DBDS Utilities Version 6.1 Installation Instructions and DNCS Utilities User Guide* (part number 4020695)
- *Daylight Saving Time Configuration Guide* (part number 749233)
- *DHCT Status Reporting and signonCount Utilities User's Guide* (part number 738186)

- *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375)
- *GQAM Modulator Software Version 4.0.11 Release Notes and Installation Instructions* (part number 4020626)
- *Installing the SAI Tools Patch* (part number 4018566)
- *MQAM Modulator Software Version 2.6.15 Release Notes and Installation Instructions* (part number 4020085)
- *Preparing for the Extension of Daylight Saving Time* (part number 4006384)
- *QAM Modulator Software Version 2.5.3 Release Notes and Installation Instructions* (part number 4011439)
- *QPSK (Release E14) Release Notes and Installation Instructions* (part number 4013491)
- *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377)
- *Recommended Patch for All DBDS Platforms Using Solaris 10* (part number 4015090)
- *Setting Session-Based QAM TSID Ranges* (part number 4004192)

Document Version

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

Description	See Topic
Expanded section on checking TSID values	***Checking Transport Stream ID Values*** (on page 82)
Corrected prequisites in all places to say SR 2.7/3.7/4.2-SP0.2	***Prerequisites*** (on page 19)
Removed 'Bouncing the DRM' step from Setting the atm_addr Environmental Variable	***Setting the atm_addr Environmental Variable*** (on page 82)

1

Introducing System Release 2.7/3.7/4.2 Service Pack 2

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. This guide provides instructions for upgrading to SR 2.7/3.7/4.2 SP2.

Time to Complete the Upgrade

The upgrade to SR 2.7/3.7/4.2 SP2 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 SP2

Introduction

SR 2.7/3.7/4.2 SP2 features several major operational improvements. Some of these improvements are described in the following list:

- DNCS support for MP3 encoded EAS audio files on a third-party OCAP™ object carousel
- CVT host population download enhancement
- Support for OpenCable™ device IDs in the DNCS
- Switched Digital Video (SDV) Service Group scalability
- Adding BFS sources if you are utilizing Distributed BFS on an SDV system
- BOSS query support for package transactions
- Netcrypt™ Bulk Encryptor Bandwidth Savings
- Populating Host Record IDs After SP2 Upgrade

Support for MP3 EAS Audio Files

Currently, an EAS receiver receives the EAS alert from the appropriate government agency and sends the message to the DNCS. The DNCS then generates two messages: the SA proprietary EAS message encapsulated in a Multi-Media Message (MMM) and the SCTE 18 message. The audio file is then converted to AIFF format and is loaded onto the OOB BFS.

SR 2.7/3.7/4.2 SP2 includes a new configuration interface for support of third-party Object Carousel MP3 audio files. In addition to converting the file to AIFF audio format and placing it on the OOB BFS, the DNCS will also convert the file to MP3 audio format and push the file to the OCAP OOB Object Carousel. When playout of the audio file is complete, the DNCS will remove the MP3 audio file from the Object Carousel.

For additional information, refer to the technical bulletin *Configure the DNCS for OCAP EAS* (part number 4019780).

Installation

No additional DNCS installation procedures are required for this feature. The AddFeatures script now supports this new feature, called "Open Cable MP3 Audio Support" in the script.

Important: Because processes must be restarted (bounced) before this feature can be enabled, we recommend that you enable this feature after you upgrade your software (while your DNCS system is down). See ***Enable Optional and Licensed Features*** (on page 79).

Notes:

- The DNCS EAS processes and UIs check the OpenCable EAS Audio feature flag on startup.
- Configuration of the third-party Object Carousel parameters occurs after enabling the MPEG audio file feature.
- The system operator will configure the MP3 audio file parameters after enabling the MP3 EAS audio file feature.

CVT Host Population Download Enhancement

SR 2.7/3.7/4.2 SP2 allows system operators to save SA host serial numbers, MAC addresses, and HCT type information in the DNCS database so that operators can set up CVT downloads to hosts by Type and by Groups.

Support OpenCable Device IDs

SR 2.7/3.7/4.2 SP2 includes a new database table that contains the MAC address and the new host ID associated with the CableCARD modules.

SDV Service Group Scalability

For each SDV-enabled service group, a mini-carousel discovery file is created. Each BFS carousel is limited to 475 individual files; and therefore, in earlier system releases, the number of SDV-enabled service groups available on the DNCS was limited to 475.

Important: The number of 475 SDV-enabled service groups available is based on a block size of 4,000 bytes. Decreasing the block size on your system will decrease the number of available service groups that an inband source can support. We recommend a block size of 4,000 bytes for these sources. This section assumes a block size of 4,000 bytes.

Starting with this system release, the DNCS, by default, creates four additional BFS sources to deliver the mini-carousel discovery files. This enhancement provides for a default total of five carousels, or up to 2,375 SDV-enabled service groups.

The following table shows the default source IDs and the corresponding names for each source ID.

Source ID	Source ID Name
24 (the original)	SGM IB
26	SGM IB1
28	SGM IB2
30	SGM IB3
32	SGM IB4

Notes:

- After upgrading to SR 2.7/3.7/4.2 SP2, Source IDs 26, 28, 30, and 32 are created, but are disabled by default.

  Important: If a BFS source is enabled *prior to* the upgrade, the source will remain enabled *after* the upgrade.

- The data rate for each source (including source ID 24) should be set to 0.50 Mbps and the block size should be 4,000 bytes.
- Additional carousels (more than 4) may always be manually configured for a system.
- When you exceed 475 SDV service groups, refer to the *SDV Operator's Guide For System Releases 2.7/3.7 or SR 4.2 Service Pack 2* (part number 4019781) for specific instructions on how to expand SDV service groups.

BOSS Query Support for Package Transactions

The Business Operations Support System (BOSS) package transactions are required to successfully use SSC DHCTs in your DBDS. BOSS transactions have been enhanced to allow for provisioning of M-Card modules for network operation and conditional access.

Netcrypt Bulk Encryptor Bandwidth Savings

In SRs earlier than 2.7/3.7/4.2 SP2, if a site utilized a Netcrypt Bulk Encryptor, all exclusive sessions were routed through the Netcrypt Bulk Encryptor, *regardless* of whether or not they were clear or encrypted sessions.

An enhancement to SR 2.7/3.7/4.2 SP2 streamlines the session setup process by not requiring that clear sessions be routed through the Netcrypt Bulk Encryptor.

Note: If your site uses a Network Bulk Encryptor, make sure that your routing device contains paths for both encrypted and clear sessions.

Populating Host Record IDs After SP2 Upgrade

After you upgrade your system to SR 2.7/3.7/4.2 SP2, if you have separable security set-tops at your site, you must reload your old EMM files to populate the Host Record IDs in the DNCS.

If you batch load EMM files, you must make sure that you do not enable Digital Interactive Services (DIS) or any other options on the Set Up DHCT screen, Secure Services tab. If you do enable these options, you will provision the DHCTs when you bulk load the EMMs, which prevents combo binding from working correctly.

Important: When you load the EMM files, make sure that you do not provision any DHCTs. Enabling any options on the Secure Services tab in the Set Up DHCT screen causes the DNCS to provision the DHCTs.

If you do provision DHCTs when you load EMMs, combo binding will not work correctly.

1 Are you loading EMM data from a CD?

- If **yes**, make sure that the EMM CD is placed in the CD ROM drive of the DNCS.

  Note: The DNCS GUI might launch when the system mounts the CD.

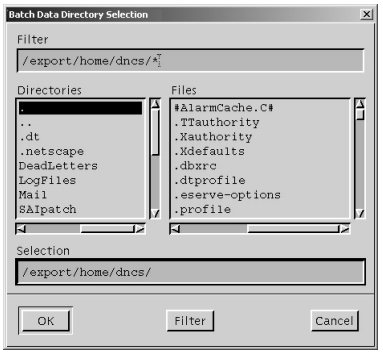
- If **no**, go to step 2.

2 On the DNCS Administrative Console, select the **DNCS** tab and then select the **Home Element Provisioning** tab.

3 Click **DHCT** to open the DHCT Provisioning window.

4 Select **New** and choose **Batch Install**.

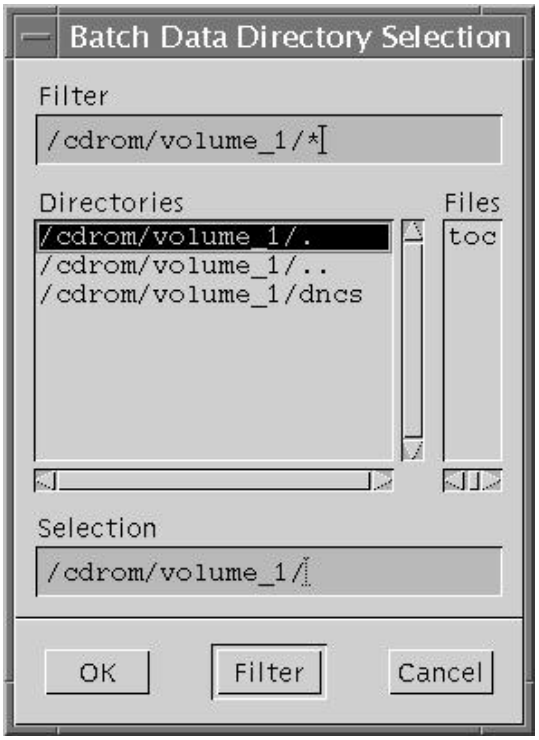
5 Click **Select**. The Batch Data Directory Selection window opens.



6 Search for the TOC file by replacing the existing **export/home/dncs** filter in the Filter field with one the following options:

- If you are loading EMMs from a CD, replace the export/home/dncs filter with **/cdrom/cdrom0/*** and press **Enter**.
- If you obtained EMMs through FTP, replace the export/home/dncs filter with the path you recorded when you extracted the EMM files. Refer to *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) for more information.

7 In the Directories panel, double-click **volume_1**. The Batch Data Directory Selection window refreshes and lists the **TOC** file.

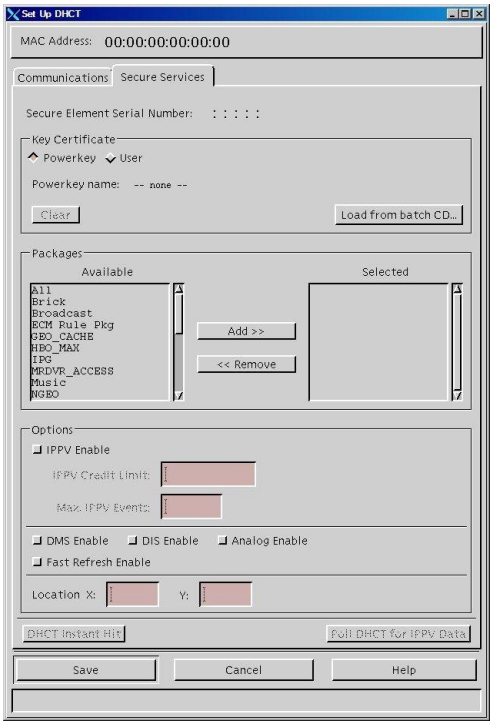


Note: The volume_1 directory may contain additional characters.

Example: volume_1#3

8 Locate the **TOC** file, verify that **TOC** is *not* highlighted, and then click **OK**. The DHCT Provisioning window opens.

9 Click the **Secure Services** tab on the DHCT Provisioning window.



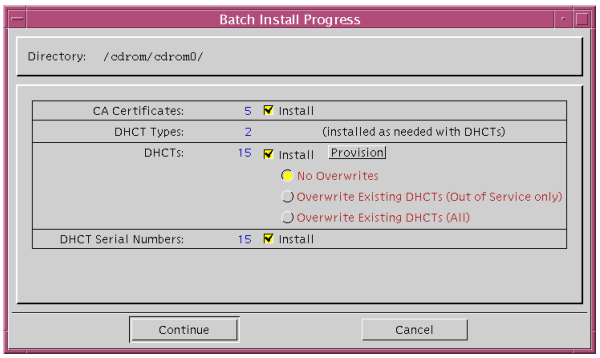
10 Is **DIS Enable** selected?

- If **yes**, click the **DIS Enable** option to disable the DIS Enable option.
- If **no**, the DIS Enable option is already off.

11 Are any other options enabled on this screen?

- If **yes**, click the option to disable the option, then click **Save**.
- If **no**, click **Save** to return to the Batch Install Progress window.

12 Click **Continue** to open the Batch Install Progress window.



13 Select **No Overwrites**.

14 On the Batch Install Progress window, click **Continue**. A window displays the status of the install process.

15 After the **Batch Install is Complete** message appears, click **Close** on the Batch Install Progress window.

16 From the Solaris toolbar, open the text editor to check the hctBatch.log and complete the following steps:

a Right-click the background area of the DNCS screen to open the **Workspace Menu** window.

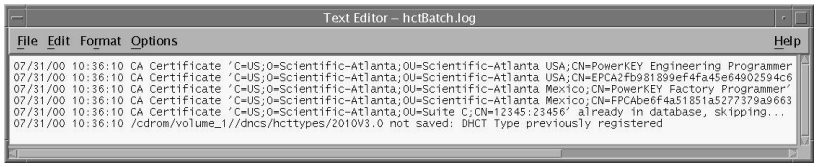
b Click the **Programs** option from the Workspace Menu window.

c From the Personal Applications menu, select the **Text Editor** option.

d From the **File** menu of the text editor, choose **Open**.

e On the text editor – Open a File window, type **/dvs/dncs/tmp/** in the Enter a Path or Folder Name field, and press **Enter**.

f Scroll through the file list that appears in the Files panel, highlight the **hctBatch.log** file, and click **OK**. The Text Editor displays the contents of the **hctBatch.log** file.



Notes:

- If the DHCT type already exists in the database, the **HctType record with version <type revision> and model <modeltype> already existed in cache** message appears.
- If a DHCT type is not added to the database for any reason, the **HctType record with version <type revision> and model <modeltype> could not be inserted into the database** message appears.

17 Select **Copy to File** from the File menu. The Text Editor – Copy to File window opens.

18 Type a unique log file name for each EMM CD in the **Enter file name** field. The naming convention of the file name is typically as follows:

/dvs/dncs/tmp/emmcdlogs/<deliverynumber>.log

Example: Type **/dvs/dncs/tmp/emmcdlogs/OL00251237-5618.log** for the file name. **OL00251237-5618** is the delivery number of the EMM CD.

Note: You might want to use the following alternate naming convention on your system:

/dvs/dncs/tmp/emmcdlogs/<deliverynumber>_date_time.log

19 Click **OK**. The system saves the log file with the new name.

20 From the **File** menu of the Text Editor window, select **Close**.

21 Are you loading EMM data from a CD?

- If **yes**, open an xterm window, type **eject**, and press **Enter** to eject the CD (or, if the GUI is open, you can eject the CD from the GUI).
- If **no**, go to step 22.

22 Repeat this procedure from step 1 for each additional EMM CD.

What CRs Are Included in This Service Pack?

Implemented Change Requests

This list highlights some of the major improvements to the DNCS that are included in this service pack. Contact your account representative for additional details on any of these change requests (CRs).

CR 59784: Upgrade JDK to Most Current Software Version

The latest Java SE Development Kit (JDK) is being shipped with the DNCS software.

CR 60891: Create New Solaris 10 Patches

Solaris 10 patches have been incorporated into this release.

CR 62557: DRM Memory Leaks

The DRM process exhibits minor memory leaks while running VOD.

CR 62980: DNCS Must Bypass Netcrypt Bulk Encryptor for Clear VOD Sessions

The DNCS bypasses the Netcrypt Bulk Encryptor for clear VOD sessions.

CR 63737: CableCARD WUI Does Not Indicate Duplicate Host ID

Users now receive a warning message if they enter a duplicate Host ID in the CableCARD WUI **Add New CRL Item** option.

CR 64335: Session List Hyperlinks Do Not Sort

Users can now sort session data using the hyperlinks at the top the Session List UI.

CR 64455: The camEx and camPsm Process Operate Correctly After Setting Up VOD with A Netcrypt Device

The camEx and camPsm process remain running after rebooting a Netcrypt device set up for VOD.

CR 64658: Encrypted Netcrypt Sessions may not Appear on Set-Tops

Netcrypt sessions are now visible on the set-top after the sessions are modified to an encrypted state.

CR 64735: The siManager Process Intermittently Core Dumps

The siManager process intermittently core dumps. If the core dump occurs the process automatically restarts.

CR 65110: Shared-Key Sessions Transmit in the Clear

Shared-key (encrypted) sessions are no longer transmitted in the clear when the DRM process is bounced (restarted) and the Netcrypt Bulk Encryptor is rebooted.

CR 65382: pkeMgr Callback Results in camPsm Core

The camPsm process no longer generates core files when the pkeMgr process performs a callback.

CR 65514: DNCS Does Not Save Dual SPF GQAM IP Address Parameters

The DNCS GUI now saves the dual SPF GQAM parameters when the same IP address is used for the GbE ports.

CR 65573: DNCS Does Not Provide Enhanced Channel Map Information for M-Cards

The DNCS now provides enhanced channel map information for Multi-Stream CableCARD modules (M-Cards).

CR 65889: qamManager Cores When a New GQAM is Added to the DNCS

The qamManager process no longer cores when new GQAM devices are added to the DNCS.

CR 66215: While Testing CableCARD Functionality, bossServer Memory Core Dumps

The bossServer memory no longer core dumps when CableCARD functionality is being tested.

CR 66217: dsm Process Cores During Clean Up of Expired Transactions

The dsm process no longer creates a core file when a system operator is cleaning up stale/expired transactions.

CR 66267: ResetDhct BOSS Transation Does Not Work Properly

Because the ResetDhct BOSS transaction now returns the correct response, system operators can reset the factory defaults on set-tops.

CR 66784: Incorrect DNCS Date Calculations

DNCS date calculations are now correct.

CR 66862: Corrupted SI Packets May Send Set-Tops into Brick Mode

The qpskManager process was corrected to prevent corrupt SI packets from sending set-tops into Brick mode.

CR 66989: sgManager Does Not Build SDV Files Over Multiple Carousels

The sgManager process now allows SDV files to be distributed over multiple carousels.

CR 67026: camPsm Cannot Always Detect when qamManager is in Service

The camPsm process now can detect when the qamManager is in service. This fix prevents streams for PPV services going in the clear.

CR 67052: Split Channels Display Correctly During DST

PowerKEY CableCARD modules now display split channels correctly during the time change to DST.

CR 67063: BFS dataPump Resets the ASI Card

The ASI card no longer resets when the dataPump (carousel) sends bad packets to the card.

CR 67225: bfsServer Does Not Reject Source Requests when BFS Source is Full

The bfsServer now rejects create link requests on a source when the BFS source is full.

CR 67256: Incorrect FIPS Codes in OpenCable EAS Message

The OpenCable EAS message now displays the correct Federal Information Processing Standard (FIPS) codes.

CR 67346: dataPump Memory Core

The dataPump no longer experiences a memory core issue during a pay-per-view (PPV) file update.

CR 67457: Solaris 10 Telnet Security Vulnerability

Software patch 4.2.0.5p1 resolves a security vulnerability in the Telnet daemon of the Solaris 10 operating system. This vulnerability could potentially enable an unauthorized user to use the Telnet protocol to gain root access to the system without using the root password.

CR 68089: Set-Tops Unable to Sign-on Due to RPC Issues with QPSKs

The hctmMac process no longer hangs up when the QPSK loses RPC connectivity with the DNCS.

CR 68394: Unable to Set Up Sessions Due to drm Core

The drm process no longer cores if bandwidth is not available when calling the DsmPartialEncryptionCombo process.

CR 68468: DNCS WUI Installation Fails on Apache Start/Restart

The DNCSwebui installation package script now stops Apache. As a result, the post installation package can now restart Apache successfully.

CR 68511: DRM Does Not Update QAM-Cached Information on Table-Based QAMs

The drm now updates QAM-cached information without a drm reboot when table-based QAMs are updated.

CR 68584: OSM OOB CVT Interval Now Configurable in Seconds

The RF CVT out-of-band (OOB) CVT interval is now configurable in seconds.

CR 68627: Memory Leak Issues with sgManager Process

The sgManager memory no longer increases when RF ports are added or modified for new or existing service groups.

CR 68877: Table-Based QAMs List Does Not Show QAMs if Data for RF and Session is Changed

The Table-Based QAMs List now displays the list of QAMs when changes are made to the QAM session data or RF parameters.

CR 68934: Issues with Format of CableCARD and Host ID Addresses in CableCARD WUI

The CableCARD and Host MAC addresses are now correctly formatted.

CR 68936: Batch Installed CableCARDs Cannot be Entered into CableCARD WUI

Batch installed CableCARDs can now be entered into the CableCARD WUI.

CR 68944: thirdparty_enc_mod Field is not Added to the Netcrypt Bulk Encryptor Table

The thirdparty_enc_mod field is now added to the Netcrypt Bulk Encryptor table.

CR 68945: SR 4.2SP1 WUIs Unavailable

The SAItools process must be installed before the SAIwebui process, otherwise the SR 4.2SP1 WUIs will not be available.

CR 68950: Wrong Node Set Shown in QPSK Demodulator GUI

The QPSK demodulator GUI shows the wrong Node Set for existing demodulators when hub_id=0 exists.

CR 68962: Improvements to File System Performance

Improvements were made to Linux file system performance.

CR 68976: QAM Changes Result in Timestamp Change to servicegroupmap.dat File

The timestamp on the servicegroupmap.dat file is no longer changed whenever a change is made to any system QAM.

CR 69035: CableCARD Authorization/Deauthorization Times Not Accurate on DST Transition Days

The CableCARD authorization and deauthorization times on Daylight Saving Time (DST) transition days are now accurate.

CR 69052: DHCTs may be Assigned to More Than One Group

The DHCT default and download groups no longer can receive the same CVT image ID.

CR 69163: S-Card Modules Do Not Load During DNCS Upgrade

Single-stream CableCARD modules (S-Cards) are now populated into the opencable_id table during a DNCS upgrade.

CR 69190: Users Cannot Autobind Combo Set-Tops

Autobinding is now allowed for combo set-tops.

CR 69248: Host ID Format Error in the Maintain CRL WUI Screen

The CableCARD host ID format issues were corrected in the CRL list field of the Maintain CRL WUI screen.

CR 69558: Slow SGManager Recovery if More than 1000 Service Groups Exist

The SGManager recovery process no longer slows down when more than 1000 service groups exist.

CR 69559: Service Groups WUI is Slow to Open when more than 1000 Service Groups Exist

The Service Group WUI is no longer slow to open when the number of service groups is greater than 1000.

CR 69582: MAC Addresses with New OUIs are not Updated After System Upgrade

After a system upgrade, MAC addresses that contain new OUIs are now upgraded in the opencable_id table.

CR 69587: Cannot Create Sessions on Newly Installed GQAMs

The DNCS no longer returns a resource allocation failure on a session attached to a newly installed GQAM.

CR 69694: Verification of null_device ID Values

Null device_id values are automatically verified before they are inserted into the opencable_id table.

CR 69718: DNCS Does Not Check the Netcrypt Port's Maximum Bandwidth Limit

The DNCS only allows a 1 GB bandwidth limit for a single Netcrypt port.

CR 69746: Incorrect UDP Port Value Assigned to VOD Sessions Routed through Netcrypt

The Digital Resource Manager (DRM) no longer allows the incorrect UDP port value to be assigned to VOD sessions that are routed through a Netcrypt.

CR 69835: siManager Memory Leak

A memory leak no longer occurs in the siManager process when reading DST rules from the database.

CR 69845: Issues with Unencrypted VOD

Unencrypted VOD now works on a table-based QAM.

CR 69869: DRM Does Not Distribute Exclusive Sessions on the Netcrypt

The DRM now distributes sessions across Netcrypt and multiple ports when the ports are included in the Gigabit Ethernet (GbE) transport connectivity to a table-based QAM.

CR 69908: Cancelling Packets and Updating Multicast Parameters Results in qpskManager Memory Leaks

The qpskManager no longer experiences memory leaks when cancelling packets and updating multicast parameters.

CR 69922: DNCS Database Fails to Upgrade

The DNCS database no longer fails to upgrade when installing the dncs package due to an issue with the hard disk writing the same message to the /dvs/dncs/tmp/upgrade.log file.

CR 69991: DSM Memory Leak

The DSM process no longer causes a memory leak that results in a loss of service and/or video at a site.

CR 70040: SIManager Cores When CF Session is Deleted

The SIManager no longer cores after a Continuous Feed (CF) session is deleted via the UI.

CR 70109: sgManager Publishes SDV Files on Different BFS Sources

The sgManager process now publishes SDV files to the same BFS source until the source limit becomes full. When that source limit is full, the sgManager correctly publishes to another BFS source.

CR 70307: OSM Links Not Created After Upgrading to SR 4.2

The bfsServer now creates OSM links after an SR 4.0 to SR 4.2 upgrade.

CR 70455: dbUIServer Process Cores when CableCARD WUI is Opened

The dbUIServer process no longer cores when the CableCARD WUI is opened.

CR 70460: User Cannot View or Edit Group Definitions

Users can now view and edit Group Definitions entries that begin with "NOT."

CR 70467: DNCS snmp Process Cores

The DNCS snmp process no longer cores with unassigned (zombie) threads.

CR 70471: Adding MC Disc File Fails to Update sgManager Log Entry

The update to the sgManager log entry no longer fails when adding a MC Disc file.

CR 70580: MPEG Source ID UI Core Dumps if Connectivity Tab Information Cannot be Found

The MPEG Source UI no longer core dumps when the UI cannot find the data needed for the Connectivity tab.

CR 70621: camEx Memory Leak with Netcrypt in VOD Session Path

The camEx process no longer experiences memory leaks when the Netcrypt is in the VOD session path.

CR 70647: SDV-enabled Sessions Cannot be Encrypted

The siManager now has the ability to encrypt existing SDV-enabled sessions.

CR 70656: Session List UI Does Not Display VOD Sessions for Table-based QAMs

VOD sessions are now displayed in the Session List UI screen when the sessions are configured on a table-based QAM without going through a Netcrypt.

CR 70750: Users Unable to Access CableCARD Data in a Timely Fashion

Improvements were made to CableCARD WUI performance issues.

CR 70788: Multicast Session WUI Displays Incorrect SDV Session Status

The Multicast Session WUI now displays the correct SDV Session status.

CR 70889: DRM Uses Unique UDP Port for VOD Through a Netcrypt Bulk Encryptor

When VOD sessions are routed through a Netcrypt Bulk Encryptor, the DRM can no longer use the same UDP port for two (or more) different VOD sessions.

CR 70997: Need to Allow SMDGs to be set up with Active Sessions

The SMDG WUI now allows SMDGs to be set up with active sessions.

CR 71073: SgManager Cores when Create Link File to BfsServer Times Out

The sgManager process no longer cores when the create link file to the bfsServer process times out.

CR 71080: SMDG WUI Does Not Notify User if GQAM Rejects SMDG

The SMDG WUI now warns the user if the GQAM rejects a session.

CR 71084: Source Definitions for BFS Sources 26 to 32 are Pending with Active Session Status

The source definitions for BFS sources 26 to 32 no longer display as pending with active session status.

CR 71381: drm Process Allocates Wrong Source UDP Port

The drm process no longer allocates the incorrect source UDP port on Netcrypt overlay sessions/routes when the operator specifies the source UDP port.

CR 71452: Table-Based QAM Session Data Script Causes Mozilla to Run Slowly

An update to the table-based QAM session script resolves Mozilla performance issues.

CR 71886: Incorrect camPsm Behavior when pkeMgr Process Is Not Licensed

The camPsm process now checks to see if the Netcrypt feature is enabled before trying to query for the pkeManager operating state.

CR 71915: DNCS Session List Does Not Show NOBE Sessions

Netcrypt Overlay Bulk Encryptor (NOBE) sessions now appear in the DNCS Session List.

CR 72041: Free-Memory-Write Error May Cause Unpredictable Behavior in drm

A Free-Memory-Write error no longer causes unpredictable behavior in drm, including intermittent core dumps, when the DNCS_DRM_INCLUDE_HE_RSR_VOD variable is set to 1.

CR 72069: User Cannot Use number_of_repeats Descriptor Tag when Sending EAS Messages

Customers can now use the "number_of_repeats" descriptor tag when sending EAS messages.

CR 72786: Delay in Posting of TSBroadcaster Files

There is no longer a delay when OCAP EAS files are posted to the TSBroadcaster object carousel.

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. See ***Configuring Secondary BFS QAMs on an SDV System (Optional)*** (on page 96) for more information.

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

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 system 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 is currently installed on your system.
- You have the CD labeled **SR 2.7/3.7/4.2-SP2**.
- 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.
- You have two CDs labeled similarly to **Solaris Patches**.
- Sites that are using the RNCS component of the DBDS need the DVD labeled similarly to **RNCS Install DVD 2.0.0.13.**

  Note: Note that this is a DVD and not a CD.
- DBDS Utilities Version 6.1.x or later 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 4.2.0.31
- DNCS GUI/WUI 4.2.0.31

- DNCS/Application Server Platform 4.2.0.13p2
- Solaris Patches 4.2.1.6
- MQAM 2.6.15
- QAM Application 2.5.3
- GQAM 4.0.11
- QPSK E14/A62
- RNCS 2.0.0.17

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.

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	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	1 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?

Open Change Requests

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

CR 56086: Convert bfsServer to Use Dynamic Logging

The operator may have issues with setting up sources when the bfsServer tracing is set to Level 2. Tracing should not be set at Level 2 under normal conditions, as this may impact system performance.

System operators should also avoid leaving the extended logging function on, due to potential system performance issues.

CR 65475: QAM Report Error in Report Writer

The QAM report in Report Writer is not working correctly.

When a user runs a QAM report, the following error message is displayed:

```
Running

QAMs Report

You Have Report Generation Errors.
Errors Are Displayed Below.

Unable to Prepare Query:Column
```

CR 67137: Set-Tops Must Contain Serial Numbers in DNCS Database

The hctmConfig process rejects sign-on requests for set-tops that do not have serial number entries in the pdsernummap table. (This issue impacts legacy set-top models.)

If this issue is not resolved, some set-top models will be unable to sign on in 2-way mode. This condition impacts other applications, such as VOD, due to the amount of activity generated by the constant hctmConfig failing condition.

Workaround: Software patch 4.2.sp2p2EP3 resolves this open issue. Contact the representative who handles your account or Cisco Services for information about obtaining the software patch.

CR 68586: Memory Issues with VOD Session Setup

A condition exists where the DRM fails VOD session setup. This condition results in the TB_QAM UDP port being allocated before releasing UDP port resources.

CR 70490: Underscore Character in Host Names Not Processed by SOAP Servers

We are aware that Service Oriented Architecture Protocol (SOAP) servers are not designed to process underscores in host names. The mgrUIServer process on the DNCS uses vod1_890 as a host name, causing a communication error with the tomcat SOAP server.

Workaround

A workaround was developed for this issue. Provide an alias to the vod1_890 server in the /etc/hosts file, and then reference that alias in the SOAPServerConfiguration.xml file. Refer to the following example for guidance:

/etc/host

The /etc/hosts file should contain an entry similar to **192.168.47.26 vod1_890 loghost**

/usr/local/tomcat/webapps/.webdb/SOAPServerConfiguration.xml

Then, open the /usr/local/tomcat/webapps/.webdb/SOAPServerConfiguration.xml file using a text editor. Replace the original reference to **vod1_890** with **loghost**.

Call Cisco Services if you need help implementing this workaround.

CR 70620: DRM Memory Leaks with Netcrypt in VOD Session Path

The DRM is experiencing memory leaks when the Netcrypt is in the VOD session path.

Workaround: The DRM process will eventually need to be bounced (restarted).

CR 70724: Table-based QAMs Cannot Load Third-party QAM Files

Customers cannot load files for third-party QAMs.

CR 70854: Issues with qamManager GQAM Reports

The qamManager process enters an infinite loop if AuditQAM returns a duplicate part number for a GQAM.

CR 70867: DRM Does Not Consistently Find the VOD Downstream Port

The DRM does not consistently find the VOD downstream port, causing intermittent errors.

CR 70871: DNCS Sends OOB Data to Incorrect Multicast IP Address

The DNCS is sending out-of-band (OOB) data to the incorrect multicast IP address. As a result, the MFMC function is not working.

CR 71153: DRM Exception Prevents VOD Streaming

The DRM is initiating an unknown error exception for VOD. As a result, customers cannot stream VOD programming.

CR 71781: pkeManager Cannot Recover after dncsStop and dncsStart

The pkeManager process cores and is unable to recover after a user performs the dncsStop and dncsStart commands.

CR 71806: DRM Generates Core when Netcrypt is Disabled

The DRM process generates a memory core when the Netcrypt feature is disabled.

CR 72146: "Omit" Line Option Not Supported in CP MMI Configuration Screen

The "omit" line option (line number = 0) is currently not supported in the CP MMI Configuration Screen of the CableCARD WUI.

The CableCARD module will not process a CPDefinition.tbl file that contains a line number equal to zero; therefore, when the omit line option is used in the CP MMI Configuration Screen, the updated information will not be presented to the user.

CR 72175: WUIs Do Not Appear After Upgrading to Software Version 4.2.0.30

After performing a software upgrade to version 4.2.0.30, the web user interfaces (WUIs) fail to open.

Workaround: Restart the Tomcat and Apache servers to resolve this issue.

CR 72304: DRM Memory Leak on Database Cache Refresh

Customers may have to restart the DRM process when updating multiple QAMs. This is due to a DRM memory leak on the database cache refresh.

CR 72398: Intermittent drm Memory Cores

Memory of the drm process may sometimes become corrupted if the process is not stopped and restarted when any of the following seven processes are stopped and restarted: qamManager, bigManager, camEX, camPsm, sgManager, pkeManager, and dsm.

CR 72411: DRM Memory Leak on SDV Sessions

A DRM memory leak can occur on Switched Digital Video (SDV) sessions that fail to set up due to not having a network path (for example, no connectivity; no bandwidth).

These types of memory leaks, over time, can cause a process to core dump or require down time for process restarts.

CR 72703: pkeManager Cores if Netcrypt Bulk Encryptor Cannot be Reached

The pkeManager process cores upon recovery when a Netcrypt Bulk Encryptor cannot be reached.

CR 72823: Enhance CableCARD UI Performance

The performance of the CableCARD WUI needs enhancement. Currently, the CableCARD WUI tends to be extremely slow when users try to navigate the WUI.

CR 72859: Configuring RF Session Data on QAMs Causes the Creation of Bogus Service Groups

When configuring RF Session Data for a QAM device, additional service groups are mistakenly added. This action results in reduced performance of the Service Groups GUI screen.

Workaround: System operators must manually delete the additional service groups each time that RF Session Data is added on a QAM device.

CR 72963: Error with Save Button in Modify CableCARD WUI Screen

The Save button in the Modify CableCARD WUI screen does not work correctly. The WUI screen allows users to make modifications to the CableCARD ID, MAC, and Host MAC items, yet the Save button only supports the modifications made to the Host ID.

CR 72972: Unexpected Growth of MAC Addresses in DHCT Group ID List

The user is required to define the DHCT Group ID when creating a new DHCT Group, yet a list of existing Group IDs is not provided. When a DHCT Group is saved with an existing Group ID, the save fails according to the UI, yet a PassThru message is sent out to all MAC addresses in this new group that failed to save, causing those MAC addresses to be assigned to the Group. This causes an unexpected growth of MAC addresses in an existing group.

CR 73260: drm Process Underallocates Bandwidth on Netcrypt Bulk Encryptor when TSRs Present

The drm process includes the Transport Stream Route (TSR) bandwidth amount when determining available bandwidth for sessions on a Netcrypt Bulk Encryptor.

CR 73510: Service Group UI Allows Operator to Configure Different SDV Servers for Child/Parent Service Group

The present Service Group UI allows the system operator to configure different SDV servers for the children/parent service groups.

CR 73906: High Number of Extents Could Cause Poor System Performance

Excessive extents occur on the opencable_id as more CableCARD modules and set-tops with CableCARD modules are added to the system.

Workaround: Software patch 4.2.0.31p2EP2 resolves this open issue. Contact your North American marketing manager or Cisco Services for information about obtaining the software patch.

CR 74395: XAIT Stops Transmitting when qpskManager Restarts

If the qpskManager is bounced (restarted), the XAIT stops transmitting. If this issue occurs, set-tops will not receive SI data.

Workaround: Software patch 4.2.0.31p2EP1 resolves this open issue. Contact your North American marketing manager or Cisco Services for information about obtaining the software patch.

CR 76001: drm Unable to Recover Sessions when Cache Read Fails

The drm process does not send any session recovery messages to the QamManager, therefore the QamManager has no knowledge of any sessions. After recovery, the QamManager enforces session recovery on the QAMs, which indicates no sessions on any QAMs.

CR 76170: pkeManager Process Cores upon Receipt of an OverlayTSRoute Query

The pkeManager incorrectly parses the receipt of an OverlayTSRoute Query response from the Netcrypt Bulk Encryptor. This issue causes the pkeManager process to core.

Additional Known Issues

DNCS Does Not Send XAIT Data when SI or qpskManager is Rebooted

If the qpskManager is bounced (restarted), the XAIT stops transmitting. If this issue occurs, set-tops will not receive SI data.

Workaround: Software patch 4.2.0.31p2EP1 resolves this open issue. Contact your North American marketing manager or Cisco Services for information about obtaining the software patch.

Note: This issue is also addressed in **CR 74395**. See ***What Are the Known Issues?*** (on page 22).

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 31) 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 33)
- ***Verify the Integrity of the CDs*** (on page 34)
- ***Verify the Integrity of the DBDS Maintenance CD*** (on page 36)
- ***Upgrade the RNCS*** (see "Upgrade the RNCS (Optional)" on page 37)
- ***Check Available Disk Space*** (on page 38)
- ***Run the Doctor Report*** (on page 40)
- ***Examine Mirrored Devices*** (on page 41)
- ***Verify and Back Up the Current Modulator Software*** (on page 43)
- ***Check the EAS Configuration—Pre-Upgrade*** (on page 44)
- ***Obtain System Configuration*** (on page 45)
- ***Collect Network Information*** (on page 46)
- ***Check and Remove Sessions*** (on page 48)
- ***Back Up the DNCS and Application Server File Systems*** (on page 50)
- ***Stop the dhctStatus, signonCount, and cmd2000 Utilities*** (on page 51)
- ***Back Up and Delete the copyControlParams File*** (on page 53)

- *Verify DBDS Stability* (on page 54)
- *Back Up the Informix Database* (on page 55)

During the Maintenance Window

At the beginning of the maintenance window, you should start with ***Suspend Billing and Third-Party Interfaces*** (on page 56) and complete all of the remaining procedures in Chapter 2. You should also complete the procedures in Chapter 3 during the same maintenance window.

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

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

11 Go to ***Verify the Integrity of the DBDS Maintenance CD*** (on page 36).

Verify the Integrity of the DBDS 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 –l** and then press **Enter**.

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

```
total 18
32060 drwxr-xr-x   8 root     nobody       512 Mar 22 10:46 .
32960 drwxr-xr-x   4 root     other        512 Mar 22 10:46 ..
32992 dr-xr-xr-x   2 root     sys         2048 Sep 30  2005 s0
32984 drwxr-xr-x  20 root     other       1024 Nov  3 09:55 s1
32983 drwxr-xr-x   2 root     root         512 Jul 14  2005 s2
32982 drwxr-xr-x   5 root     root         512 Nov  3 09:55 s3
32981 drwxr-xr-x   2 root     root         512 Jul 14  2005 s4
32966 drwxr-xr-x   2 root     root         512 Jul 14  2005 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 37); otherwise, go to ***Check Available Disk Space*** (on page 38).

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 2.7/3.7/4.2 and SR 2.7.1/3.7.1/4.2.1* (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 38).

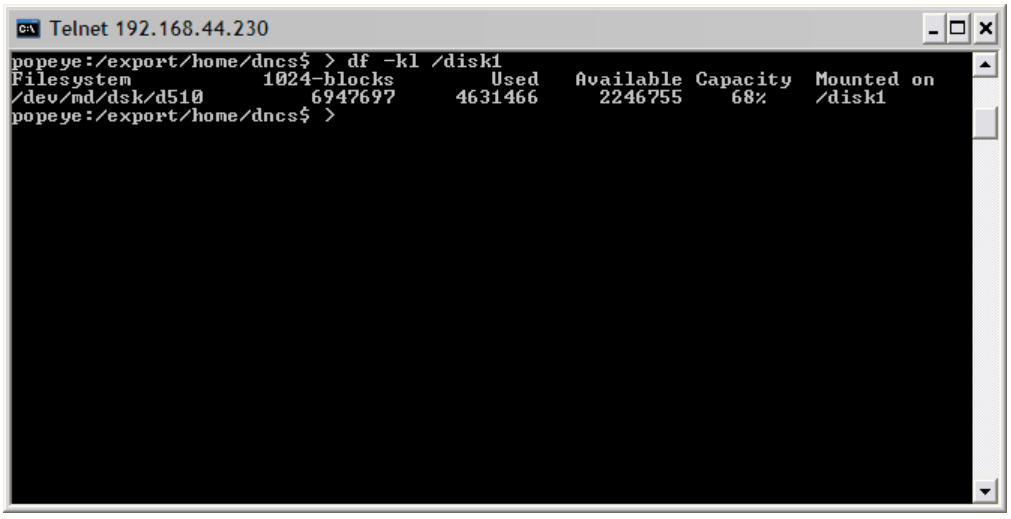
Check Available Disk Space

Introduction

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 -kl /disk1** and then press **Enter**. The system displays, in the **Available** column, the amount of used and available space on the /disk1 filesystem.



2 Does the Available column show that at least 700,000 blocks are available for the upgrade?

- If **yes**, go to ***Run the Doctor Report*** (on page 40). 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.

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—Specifies whether the SA (PowerKEY®) encryption method or a non-SA encryption method is used for DHCTs in the network
- DBDS Network Overlay—Allows SA DHCTs to be used on a Motorola system
- SI Type to Use—Specifies the type of System Information (SI) to use on the system (ATSC or DVB). ATSC is the standard SI type for North American cable systems. DVB is frequently used in Europe and other areas of the world
- Dynamic PID Mapping Mode—Allows for the use of non-unique transport stream IDs (TSIDs) throughout the system
- Preallocated Session Management—Permits the set up of sessions on SA Multiple Quadrature Amplitude modulators (MQAMs) for use by an external session resource manager process for VOD
- Direct ASI—Permits the use of the Asynchronous Serial Interface (ASI) card in the DNCS for transmitting inband data directly to a QAM without the need for a Broadband Integrated Gateway (BIG)

  Note: Refer to Appendix C for detailed instructions to install and configure the Direct ASI feature.
- Third-Party Source—Allows tuning tables to be built for clear digital sources generated by QAMs not managed by the DNCS, and it eliminates the need to use a mirror QAM for Program and System Information Protocol (PSIP) services

  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).
- Enhanced Split Channels—Enables two different content streams and multiple channel schedules at different times of the day
- Netcrypt Bulk Encryptor—Supports encrypted digital broadcast and narrowcast transport streams across multiple headends, as well as up to three distinct conditional access systems

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

Introduction

Before you disable the disk mirroring functions of the Enterprise 450 or the Sun Fire V445, V880, or V890 DNCS 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 **ok** appears in the **State** column next to each metadevice.
   - No **Hot Spare** indicates **In Use**.
4. Are both of the conditions listed in step 3 "true"?
   - If **yes** (to both conditions listed in step 3), go to ***Verify and Back Up the Current Modulator Software*** (on page 43).
   - If **no** (to either or both conditions listed in step 3), call Cisco Services for help in resolving these issues with the metadevices.

Verify that Boot Device is Correctly Configured

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

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

Before beginning the upgrade process, verify the current software version of the QPSK, QAM, MQAM, and GQAM software. This provides the operator an understanding of what software is currently being used in the network. At this time in the pre-upgrade process, you also need to back up this software to ensure you can roll back to your previous network configuration.

Refer to the **Verify the Current Software Version on the DNCS** and **Back Up the Current Configuration Files** sections in each of the following installation guides for complete instructions:

- *System Release 2.7/3.7/4.2 Service Pack 0.2 Release Notes and Installation Instructions* (part number 4019303)
- *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)
- *QPSK (Release E14) Release Notes and Installation Instructions* (part number 4013491)

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 System Configuration

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

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

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

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

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

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

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

4 Write down the hostname for the Application Server, as displayed in step 3:

_____

5 From an xterm window on the Application Server, type **more /etc/hosts** and then press **Enter**. A list of IP addresses and hostnames appears.

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

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

7 At the Application Server, type **uname -n** and then press **Enter**. The hostname for the Application Server appears.

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

_____

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

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

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

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

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

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

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

   k **netstat -nrv > netstat.out**

   l **ifconfig -a > ifconfig.out**

   m **df -k > df.out**

   n **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 Go to ***Check and Remove Sessions*** (on page 48).

Check and Remove 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 BFS GQAM

Complete the following steps to check and record the number of pre-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 numbers for a GQAM range from 1 to 16.

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

3 Go to Tearing Down and Restarting Session 199.

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 4.2* (part number 4013779 Revision A). 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 4.2* (part number 4013779 Revision A).
- 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.

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 **dhctStatus** and press **Enter** to display the dhctStatus menu.
3. 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.
4. Type **ps -ef | grep dhctStatus** and then press **Enter** to determine if all of the processes are terminated.

   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
5. Type **kill -9 <processid>** and then press **Enter** for any process ID displayed in step 4.

   Example: kill -9 12449

Removing the signonCount Utility from System Memory

1. Type **signonCount uninstall** and press **Enter**.

   Note: The utility is not permanently uninstalled; it is placed back into system memory the next time you run the signonCount utility.
2. Type **ps -ef | grep signonCount** and then press **Enter**. A list of DNCS processes and process IDs display on the screen.
3. Type **kill -9 <processid>** and then press **Enter** for each process ID displayed in step 2.
4. Type **ps -ef | grep signonCount** and then press **Enter** to ensure all the processes are terminated.
5. Repeat steps 3 and 4 for any process that continues to display active. 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 53).
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 53).

Back Up and Delete the copyControlParams File

Complete these steps to back up and delete the copyControlParams.inf file from the DNCS.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /export/home/dncs** and then press **Enter**. The /export/home/dncs directory becomes the working directory.
3. Does the copyControlParams.inf file have any customized entries?
   - If **yes**, type **cp copyControlParams.inf copyControlParams.inf.bak** and then press **Enter**. The system makes a backup copy of the copyControlParams.inf file.
   - If **no**, go to step 4.
4. Type **rm copyControlParams.inf** and then press **Enter**. The system deletes the copyControlParams.inf file.

   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.

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 4.2* (part number 4013779 Revision A). 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 the third-party application provider's instructions you received before the maintenance window began to stop applications during the installation process.

Stop the cron Jobs

Introduction

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. Use the cron PID from step 3, and type **ptree <PID>** and press **Enter**. The DNCS 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 4 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 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.
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 Cisco Basic Backup or Auto Backup Servers

If the site you are upgrading uses the Cisco 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.

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.
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 the Application Server and the DNCS.

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 the RNCS Processes on the DNCS

If the RNCS licensed feature is enabled on your service control platform, then refer to *RNCS Installation and Upgrade Instructions For SR 2.7/3.7/4.2 and SR 2.7.1/3.7.1/4.2.1* (part number 4012763) to stop the RNCS processes.

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**.
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 Aptiv Application Server for the Service Pack

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

Note: Contact Aptiv Digital 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.
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 the dncsInitd process if it 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

System Release 2.7/3.7/4.2 SP2 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.

In This Chapter

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 SP2.

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 DNCS E450.

Note: This is only an example of output from the metastat command.

```
$ metastat -p
d500 -m d400 1
d400 1 1 c0t0d0s0 -h hsp120
d501 -m d401 1
d401 1 1 c0t0d0s1 -h hsp121
d503 -m d403 1
d403 1 1 c0t0d0s3 -h hsp123
d507 -m d407 1
d407 1 1 c0t0d0s7 -h hsp127
d510 -m d410 1
d410 1 1 c0t1d0s0 -h hsp220
d513 -m d413 1
d413 1 1 c0t1d0s3 -h hsp223
d514 -m d414 1
d414 1 1 c0t1d0s4 -h hsp224
d515 -m d415 1
d415 1 1 c0t1d0s5 -h hsp225
d516 -m d416 1
d416 1 1 c0t1d0s6 -h hsp226
d517 -m d417 1
d417 1 1 c0t1d0s7 -h hsp227
d700 1 1 c2t0d0s0 -h hsp120
d701 1 1 c2t0d0s1 -h hsp121
d703 1 1 c2t0d0s3 -h hsp123
d707 1 1 c2t0d0s7 -h hsp127
d710 1 1 c2t1d0s0 -h hsp220
d713 1 1 c2t1d0s3 -h hsp223
d714 1 1 c2t1d0s4 -h hsp224
d715 1 1 c2t1d0s5 -h hsp225
d716 1 1 c2t1d0s6 -h hsp226
d717 1 1 c2t1d0s7 -h hsp227
hsp120 c4t0d0s0
hsp121 c4t0d0s1
hsp123 c4t0d0s3
hsp124 c4t0d0s4
hsp127 c4t0d0s7
hsp220 c4t1d0s0
hsp221 c4t1d0s1
hsp223 c4t1d0s3
hsp224 c4t1d0s4
hsp225 c4t1d0s5
hsp226 c4t1d0s6
hsp227 c4t1d0s7
```

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.

Example - Sample Packages List:

```
Checking the system, please wait...
Checking for running processes...
*************************************************************************
This script will install the following packages on:
DNCS Server (dncs)
------------------------
SAItools            DNCS/AppServer Tools 03-13-2007
                    4.2.0.13p2
SAIdncs             DNCS 07-09-2007
                    4.2.0.31
SAIgui              DNCS GUI 07-09-2007
                    4.2.0.31
SAIwebui            DNCS WEBUI 07-09-2007
                    4.2.0.31
SAIqam              QAM Modulator
                    V2.5.3
SAImqam             MQAM Modulator
                    V2.6.15
SAIgqam             GQAM Modulator
                    V4.0.11
SAIgoqam            GOQAM Modulator
                    V1.1.3
SAIncrypt           Netcrypt
                    V1.1.3
*************************************************************************
Are you SURE you want to continue?  [y,n,?,q]
```

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 Systems, Inc..
                    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**. The system displays a message to configure the CED.in file. Continue to step 8.
- 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 Type **eject cdrom** and then press **Enter** when the installation is complete.

11 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.

Edit the /etc/system File

Introduction

In this procedure, you will modify the /etc/system file to re-enable TCP Fusion. Because of issues documented in Sun Alert document #102576, TCP Fusion may have been disabled on your system during a previous upgrade. You need to complete this procedure on any system on which Solaris patches have been installed.

Editing the /etc/system File

Complete the following steps to edit the /etc/system file to re-enable TCP Fusion.

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

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 /etc** and then press **Enter**. The /etc directory becomes the working directory.
4. Type **cp -p system system.< date >** and then press **Enter**. The system makes a copy of the /etc/system file.

   Note: Substitute today's date, in yyyymmdd format, for < date >.

   Example: cp -p system system.2006.1121
5. Type **vi system** and then press **Enter**. The system file opens for editing using the UNIX vi text editor.
6. Type **/do_tcp_fusion** and then press **Enter**. The cursor advances to the line that contains the entry that disabled TCP Fusion.

   Note: That line should look like **set ip:do_tcp_fusion=0x0**.
7. Did the cursor advance to the line described in step 6?
   - If **yes**, go to step 8.
   - If **no** (the message **Pattern not found**, or an asterisk precedes the line), TCP Fusion is not disabled on your system. Type **:q!** to close the file and exit from the vi text editor.
8. Type **0** (zero). The cursor moves to the beginning of the current line.

9 Complete the following steps to turn the current line into a comment.

   a Type **i***

   b Press the **Spacebar**.

   c Press **Esc**.

   Result: Your line should now look like * **set ip:do_tcp_fusion=0x0**.

10 Type **:wq!** to save the file and to close the vi editor.

11 Repeat this procedure on the Application Server, as well.

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 75).

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 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_SP2	
DNCS Application	SAIdncs	4.2.0.31	
DNCS/App Tools	SAItools	4.2.0.13p2	
DNCS GUI	SAIgui	4.2.0.31	
DNCS WUI	SAIwebui	4.2.0.31	
DNCS Online Help	SAIhelp	4.2.0.3	
QAM	SAIqam	2.5.3	
MQAM	SAImqam	2.6.15	
GQAM	SAIgqam	4.0.11	
GoQAM	SAIgoqam	1.1.3	
QPSK	SAIqpsk	E14	
Netcrypt	SAIncrypt	1.1.3	

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 79) for Aptiv sites or ***Add an EAS Variable to the .profile File*** (on page 77) 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.

Add an EAS Variable to the .profile File

Introduction

In order to make the EAS work properly, you need to add the LOCAL_EAS_IP variable to the .profile file. This procedure describes how to add the LOCAL_EAS_IP variable.

Adding an EAS Variable to the .profile File

Complete the following steps to add the LOCAL_EAS_IP variable to the .profile file.

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

2 Type **grep -i LOCAL_EAS_IP /export/home/dncs/.profile** and then press **Enter**. The system searches for LOCAL_EAS_IP in the /export/home/dncs/.profile file.

Note: Be sure to type a space between grep –i LOCAL_EAS_IP and /export/home/dncs/.profile.

3 Do the results from step 2 reveal that there is already an entry for LOCAL_EAS_IP in the /export/home/dncs/.profile?

- If **yes**, go to ***Enable Optional and Licensed Features*** (on page 79).
- If **no**, go to step 4.

4 Type **cat /etc/hosts | grep dncseth** and then press **Enter**. The system displays the value of the dncseth variable in the /etc/hosts file.

5 Type **cat /etc/hosts | grep eac** and then press **Enter**. The system displays the value of the eac variable in the /etc/hosts file.

6 Evaluate the results from steps 4 and 5 to determine whether the eac is on the same network as the DNCS or if it is on a different network. Refer to the following example for guidance in making this determination:

Same Network	**Different Network**
dncseth=192.168.2.1	dncseth=192.168.2.1
eac=192.168.1.5	eac=192.168.4.5

Note: When the DNCS and the eac are on the same network, the first three octets of the IP address are identical. They are on different networks when the first three octets of the IP address are different.

7 Are the DNCS and the eac on the same network?

- If **yes**, go to step 8.
- If **no** (they are on different networks), go to step 10.

8 Using a text editor, append the following line to the .profile file:

export LOCAL_EAS_IP=[Ethernet address of the DNCS]

Note: Substitute the Ethernet address of the DNCS for [Ethernet address of the DNCS], displayed in step 4.
Example: LOCAL_EAS_IP=192.168.2.1

9 Go to ***Enable Optional and Licensed Features*** (on page 79).

10 Type **ifconfig -a** and then press **Enter**. Examine the output and find the IP address of the DNCS that is on the same network as the eac.

Note: In this example, the IP address of the eac (from step 6) is 192.168.4.5; the IP address of the DNCS that is on the same network as the eac is 192.168.4.1.

Example:
hme0: flags=1000843< UP,BROADCAST,RUNNING,MULTICAST,IPv4 > mtu 1500 index 2
inet 192.168.2.1 netmask ffffff00 broadcast 192.168.2.255

ci0: flags=1000842< BROADCAST,RUNNING,MULTICAST,IPv4 > mtu 9180 index 5
inet 192.168.4.1 netmask ffffff00 broadcast 192.168.40.255

11 Using a text editor, append the following line to the /export/home/dncs/.profile file
export LOCAL_EAS_IP=[Ethernet address of the DNCS]
Note: Substitute the Ethernet address of the DNCS for [Ethernet address of the DNCS], displayed in step 10.
Example: LOCAL_EAS_IP=192.168.4.1

12 Go to ***Enable Optional and Licensed Features*** (on page 79).

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.

Edit the .profile File

Introduction

After the upgrade to SR 2.7/3.7/4.2, some of the logging and debug settings that were managed through the .profile file will be managed through the DNCS user interface.

In this section, you will edit to the .profile file on the DNCS to help facilitate the upgrade. You may need to edit the debug and logging settings in the .profile file and for SSP 2.3 compliance, you may need to add or modify the LOCAL_EAS_IP variable in the .profile file.

Editing Debug and Logging Settings in the .profile File

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

2 To set the export/home/dncs directory as the working directory, type **cd /export/home/dncs** and then press **Enter.**

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

export EMCDEBUG=BbKkQ9SD

Select one of the following options:

- If the EMCDEBUG variable is not present in the file or is commented out (with a # character in front of the EMCDEBUG= line), go to ***Setting the atm_addr Environmental Variable*** (on page 82).
- If the EMCDEBUG variable is present go to step 4.

3 In order to remove the debug flags for the bossServer (Bb), qamManager (Q9), and dsm (S), **delete** the following three flags from the entry described above: **Bb, Q9,** and **S**

Note: In the above example, export EMCDEBUG=BbKkQ9SD becomes export EMCDEBUG=KkD after you delete **Bb Q9 S**

4 Do any other debug or logging flags remain with the EMCDEBUG variable after having completed step 4?

- If **yes,** call Cisco Services to see if these flags are still needed.
- If **no,** delete the entire export EMCDEBUG= line or comment it out by adding the # character in front of the EMCDEBUG= variable setting as shown in the following example:

  #export EMCDEBUG=BbKkQ9SD

5 Save the changes to the .profile file.

6 After making these changes, bounce the DRM as shown in ***Bouncing the DRM Process*** (on page 81).

Setting SSP 2.3 Compliance

1. If necessary, open an xterm window on the DNCS.
2. To set the export/home/dncs directory as the working directory, type **cd /export/home/dncs** and then press **Enter.**
3. Open the .profile file using the text editor of your choice. Look for an entry in the .profile file similar to the following example:

   export DNCS_DRM_INCLUDE_HE_RSR_VOD=1
4. Is the DNCS_DRM_INCLUDE_HE_RSR_VOD variable present in your .profile file?
   a. If **yes,** continue to step 6.
   b. If **no,** continue to step 5.
5. Do you need SSP 2.3 compliance to be *enabled*?
   a. If **yes,** continue to step 7.
   b. If **no,** continue to step 9.
6. The DNCS_DRM_INCLUDE_HE_RSR_VOD variable can be set to *enabled* or *disabled.*
   - If export DNCS_DRM_INCLUDE_HE_RSR_VOD=0 then SSP 2.3 is *enabled.*
   - If export DNCS_DRM_INCLUDE_HE_RSR_VOD=1 then SSP 2.3 is *disabled.*

   Is the DNCS_DRM_INCLUDE_HE_RSR_VOD variable set to the correct value?
   a. If **yes,** continue to step 7.
   b. If **no,** continue to step 8.
7. You are finished. Exit the text editor.
8. Add the # character in front of the DNCS_DRM_INCLUDE_HE_RSR_VOD variable setting as in the following example:

   #export DNCS_DRM_INCLUDE_HE_RSR_VOD=1
9. Set the SSP 2.3 compliance:
   a. If you need to *disable* SSP 2.3 compliance type

      export DNCS_DRM_INCLUDE_HE_RSR_VOD=1
   b. If you need to *enable* SSP 2.3 compliance typ

      export DNCS_DRM_INCLUDE_HE_RSR_VOD=0
10. Save the changes to the .profile file.
11. After making these changes, bounce (stop and restart) the DRM as shown in ***Bouncing the DRM Process*** (on page 81).

Bouncing the DRM Process

Follow these instructions to bounce (stop and restart) the DRM process.

1. If the DNCS Control window is not already open, click the **Control** button in the DNCS area of the **DNCS Administrative Console Status** window.
2. From the list of processes, select **DRM**
3. Click the **Process** menu and then select **Stop Process**.
4. When a confirmation message appears, click **Yes** to stop the DRM process. This causes the indicator next to DRM to turn red.
5. From the list of processes, select **DRM**
6. From the **Process** menu, click **Start Process**. The indicator next to DRM turns green when the process has successfully restarted.

Setting the atm_addr Environmental Variable

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

   Example: export atm_addr=dncseth
2. Does the .profile file contain an entry as described in step 1?

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

   • If **yes,** insert the "#" character at the beginning of the line that contains atm_addr so that the line becomes a comment.

   • If **no,** go to step 3.
3. **Save** and close the .profile file.

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.

If you are using SR 2.5/3.5/4.0 or later, 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 83), then ***Run getTSID*** (on page 83), and then ***Check TSID Values*** (on page 84).
- If **no**, go to ***Check TSID Values*** (on page 84).

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 /external_pub/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-SA) 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.

   Note: Beginning with SR 2.7.1/3.7.1/4.2.1, this button is labeled **Sys Config**.
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).

Enable the RNCS (Optional)

To complete the RNCS upgrade process, perform steps 25 through 35 in Chapter 2 of the *RNCS Installation and Upgrade Instructions For SR 2.7/3.7/4.2 and SR 2.7.1/3.7.1/4.2.1* (part number 4012763).

Shut Down the SA Application Server

Complete the following steps to shut down the SA Application Server.

1. If necessary, open an xterm window on the Application Server.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. From the xterm window on the Application Server, type **/usr/sbin/shutdown -g0 -y -i0** and then press **Enter**. The Application Server shuts down.
4. Go to *Shut Down the DNCS* (on page 87).

Shut Down the DNCS

Complete the following steps to shutdown the DNCS server.

Note: You should still be root user in an xterm window on the DNCS.

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

2 Go to ***Install the Solaris Patches on the DNCS*** (on page 88).

Install the Solaris Patches on the DNCS

Restarting the DNCS in Single-User Mode

Before you can install the Solaris patches, you need to restart the DNCS in single-user mode. Complete the following steps to restart the DNCS in single-user mode.

1. At the **OK** prompt on the DNCS, type **boot -s** and then press **Enter**. The DNCS boots into single-user mode and the **password** prompt appears.
2. Type the root password and then press **Enter**. The console prompt (**#**) appears.
3. Insert the CD labeled similarly to **Solaris Patches** into the CD drive of the DNCS.
4. At the console prompt, type **TERM=vt100; export TERM** and then press **Enter**. The terminal environment for the DNCS console is set to vt100.
5. At the console prompt, type **stty erase** and then a space. Press the **Backspace** key, then press **Enter**. The system sets the Backspace key to erase.
6. Choose one of the following options based upon the type of DNCS server you are upgrading:
   - If you are upgrading a Sun Fire V880 DNCS, type **mount -F hsfs /dev/dsk/c0t6d0s0 /mnt** and then press **Enter**.
   - If you are upgrading a Sun Fire V890 DNCS, type **mount -F hsfs /dev/dsk/c0t0d0s0 /mnt** and then press **Enter**.
   - If you are upgrading an Enterprise 450 DNCS, type **mount -F hsfs /dev/dsk/c1t6d0s0 /mnt** and then press **Enter**.

   Result: The system mounts the Solaris patch CD to /mnt.

   Note: While the DNCS is installing Solaris patches, you can install Solaris patches on the Application Server at the same time by following these steps: ***Installing the Solaris Patches on the Application Server*** (on page 90).

Installing the Solaris Patches on the DNCS

Complete the following steps to install the Solaris patches on the DNCS.

Notes:

- You should still be logged on to the console of the DNCS as root user.
- Installation of the Solaris patches should take no longer than 45 minutes.
- Some patches will fail to install if they have already been installed, a newer version of the patch is already installed, or if the required package is not present. Ignore returned error codes of *2*, *8*, and *35*.

1 Type **/mnt/install_patches** and then press **Enter**.

Results:

- The system installs the Solaris patches.
- The system displays error codes if some patches fail to install.

2 Type **umount /mnt** and then press **Enter**. The system unmounts the Solaris patches CD.

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

Note: Ignore any **auditd** messages.

4 At the **ok** prompt, type **boot** and then press **Enter**. The DNCS reboots.

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

6 Are you upgrading a SA Application Server?

- If **yes**, go to ***Install the Solaris Patches on the Application Server*** (on page 90).
- If **no**, go to ***Initialize the DBDS System*** (on page 92).

Install the Solaris Patches on the Application Server

Restarting the Application Server in Single-User Mode

Before you can install the Solaris patches, you need to restart the Application Server in single-user mode. Complete the following steps to restart the Application Server in single-user mode.

1. At the **ok** prompt on the Application Server, type **boot -s** and then press **Enter**. The Application Server boots into single-user mode and the **password** prompt appears.
2. Type the root password and then press **Enter**. The console prompt (**#**) appears.
3. Insert the CD labeled similarly to **Solaris Patches** into the CD drive of the Application Server.
4. At the console prompt, type **TERM=vt100; export TERM** and then press **Enter**. The terminal environment for the Application Server console is set to vt100.
5. At the console prompt, type **stty erase** and then a space. Press the **Backspace** key, then press **Enter**. The system sets the Backspace key to erase.
6. Choose one of the following options based upon the type of Application Server you are upgrading:
   - If you are upgrading a Sun Blade 150 server, type **mount -F hsfs /dev/dsk/c0t1d0s0 /mnt** and then press **Enter**.
   - If you are upgrading a Sun Ultra 5 server, type **mount -F hsfs /dev/dsk/c0t2d0s0 /mnt** and then press **Enter**.
   - If you are upgrading a Sun V240 server, type **mount -F hsfs /dev/dsk/c0t0d0s0 /mnt** and then press **Enter**.

   Result: The system mounts the Solaris patch CD to /mnt.

Installing the Solaris Patches on the Application Server

Complete the following steps to install the Solaris patches on the Application Server.

Notes:

- You should still be logged on to the console of the Application Server as root user.
- Installation of the Solaris patches should take no longer than 45 minutes.

1 Type **/mnt/install_patches** and then press **Enter**.

Results:

- The system installs the Solaris patches.
- The system displays error codes if some patches fail to install.

Note: Some patches will fail to install if they have already been installed, a newer version of the patch is already installed, or if the required package is not present. Ignore returned error codes of *2*, *8*, and *35*.

2 Type **umount /mnt** and then press **Enter**. The system unmounts the Solaris patches CD.

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

Note: Ignore any **auditd** messages.

4 At the **OK** prompt, type **boot** and then press **Enter**. The Application Server reboots.

5 Log on to the Application Server as **dncs** user.

Initialize the DBDS System

After installing the Solaris patches, choose one of the following options to initialize the DBDS system:

- If you are using a SA Application Server, go to ***Restart the System Components*** (on page 94).
- If you are using an Aptiv Application Server, go to ***Disable the SAM Process on Aptiv Systems*** (on page 93).

Disable the SAM Process on Aptiv Systems

If the site you are upgrading uses the Aptiv 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 application server, skip this procedure and go to ***Restart the System Components*** (on page 94).
- 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 System Components

Introduction

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

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 on the DNCS

If your DNCS is licensed for the RNCS feature, then refer to the *RNCS Installation and Upgrade Instructions* (part number 4003191) to restart the RNCS processes.

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**.
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.

Configuring Secondary BFS QAMs on an SDV System (Optional)

Introduction

If you are currently utilizing Distributed BFS and you are upgrading your system to support SDV, the system automatically adds sources 24 through 32 and automatically disables any newly created sources. Any existing sources will be disabled. These additional sources will need to be added to all of your secondary BFS QAMs.

Note: If your site does not support the SDV option, you may skip the procedures in this section.

This section provides procedures for sites using either a BFS BIG or a Direct ASI model. Choose the procedure that pertains to your system.

Adding BFS Sources - Sites Using a BFS BIG

Complete the following procedure if your DNCS uses a BFS BIG to distribute the BFS carousel data.

1 Open the Set Up BIG window by following the quick path:
DNCS Administrative Console > Network Element Provisioning tab > BIG > File > Open

2 Click **PAT Configuration** to open the BIG PAT window.

3 Verify the BIG PAT Session Number and Program Number data, making sure that your Program Numbers are sequentially in order and in line with the Session Numbers.

Note: Your DNCS sessions 2 through 22 should not change; however, DNCS sessions greater than 22 must be deleted and reentered with the correct sequential Program Number.

Example: BIG PAT Session Number and Program Number Data (Program Numbers in Sequential Order and in line with Session Numbers)

Session Number	Program Number
2	128
4	129
6	130
8	131
10	132
12	133

Session Number	Program Number
14	134
16	135
18	136
20	137
22	138
24	139
26	140
28	141
30	142
32	143
199	144

4 Once the PAT Configuration Table has been modified, update any secondary BFS QAMs by tearing down any session greater than 22 and rebuilding the session with the correct Program Number.

Adding BFS Sources - Sites Using Direct ASI

Complete the following procedure if your DNCS uses the Direct ASI option to distribute BFS data.

Note: A benefit of using the Direct ASI option is that you only need to build sessions *as you need them* on your primary and secondary BFS QAMs. There is no need to tear down any DNCS sessions greater than 22 as you would do within a BFS QAM system.

1 As BFS sources are built, the DNCS automatically retrieves the next available program number from the source list. As a result, there is no need to update the PAT Configuration Table by hand.

In the following example, note that Session 22 is Program Number 138, while Session 199 is Program Number 139, and Session 24 is Program Number 140.

When Session 24 was built, it took the next available Program Number, which was 140. With the Direct ASI model, you can have Program Numbers out of sequence in the PAT Configuration table.

Example:

Session Number	Program Number
2	128
4	129
6	130
8	131

Session Number	Program Number
10	132
12	133
14	134
16	135
18	136
20	137
22	138
24	140
26	141
28	142
30	143
32	144
199	139

2 After adding the BFS sources, update any secondary BFS QAMs by adding the same sessions to the secondary BFS QAMs.

Example: If you added sessions 24 and 26 to the primary BFS QAM, you must add the same sessions to all secondary BFS QAMs as Continuous Feed sessions.

Restart the Billing and Third-Party Interfaces

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

Restart the cron Jobs

Restart the cron Jobs on the DNCS

1. If necessary, open an xterm window on the DNCS.
2. Confirm that the cron jobs are not running by typing **ps -ef | grep cron** and press **Enter**.
3. Have the cron jobs restarted on their own?
   - If **yes**, skip the rest of this procedure and go to ***Restart the cron Jobs on the Application Server*** (on page 100).
   - 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.

4

Post-Upgrade Procedures

Introduction

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

In This Chapter

Configure SAM Timers

Introduction

After you complete the installation process, the **Update Timer** and **Schedule Timer** fields on the SAM Configuration window need to be set at specific values. These values ensure that channel maps and the database have sufficient time to update. The instructions in this section guide you through the necessary steps.

Important: Skip this procedure if your site does not support SARA.

Configuring the SAM Timers

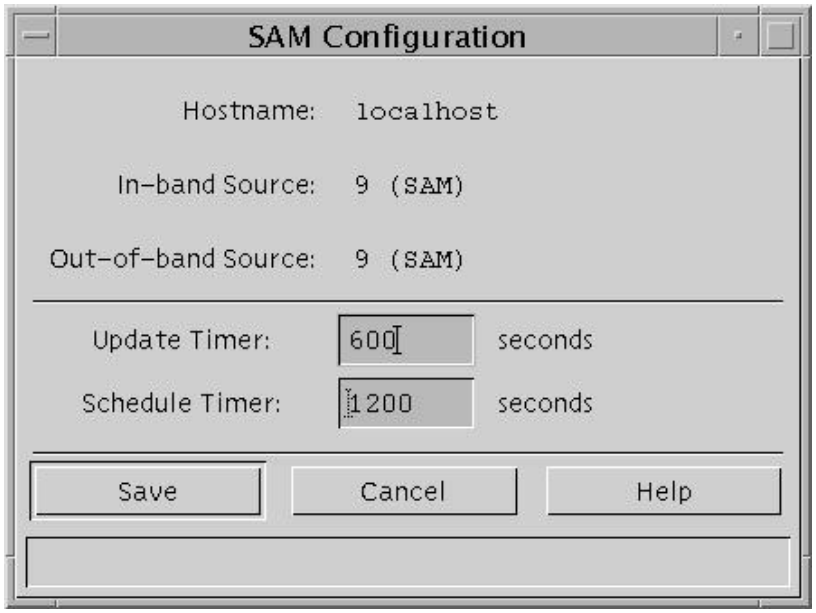
Follow these instructions to set the Update Timer and Schedule Timer fields on the SAM Configuration window.

1 From the DNCS Administrative Console, select the **Application Interface Modules** tab and then click **SAM Config**. The SAM Configuration window opens.

2 Follow these instructions to configure the SAM Configuration window.

   a In the **Update Timer** field, type **600**.

   b In the **Schedule Timer** field, type **1200**.



3 Click **Save**.

Configure the CableCARD Server

Introduction

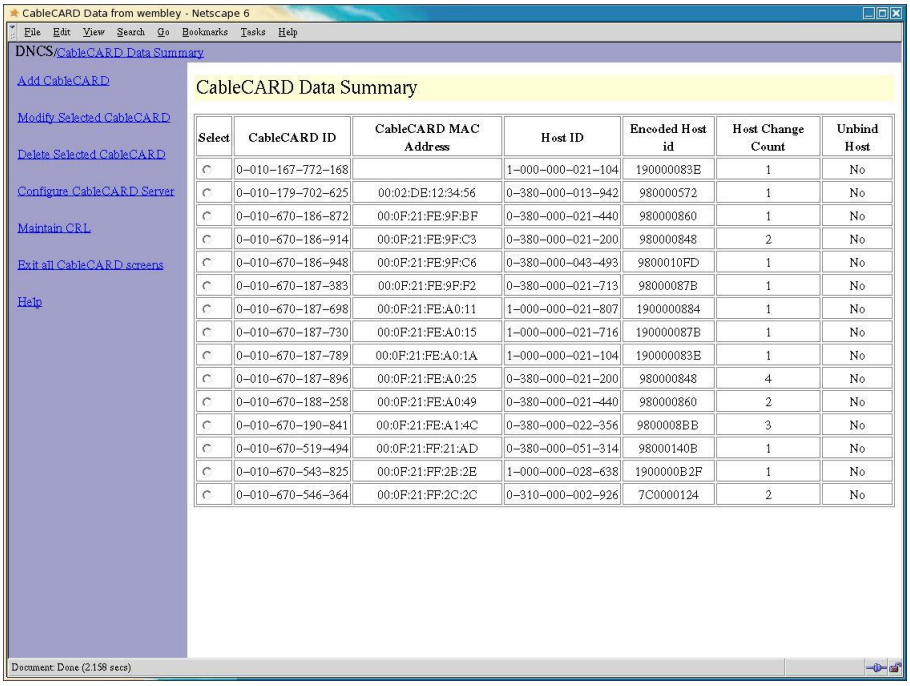
Next in the post-upgrade process, the **Set Authorization Time-out Period** and **Set DeAuthorization Time-out Period** fields on the Configure CableCARD Server window need to be set to specific values. These values instruct the CableCARD server when to stop adding authorization and deauthorization records to the BFS file, which keeps the BFS file from growing too large. The instructions in this section guide you through the necessary steps.

Configuring the CableCARD Server

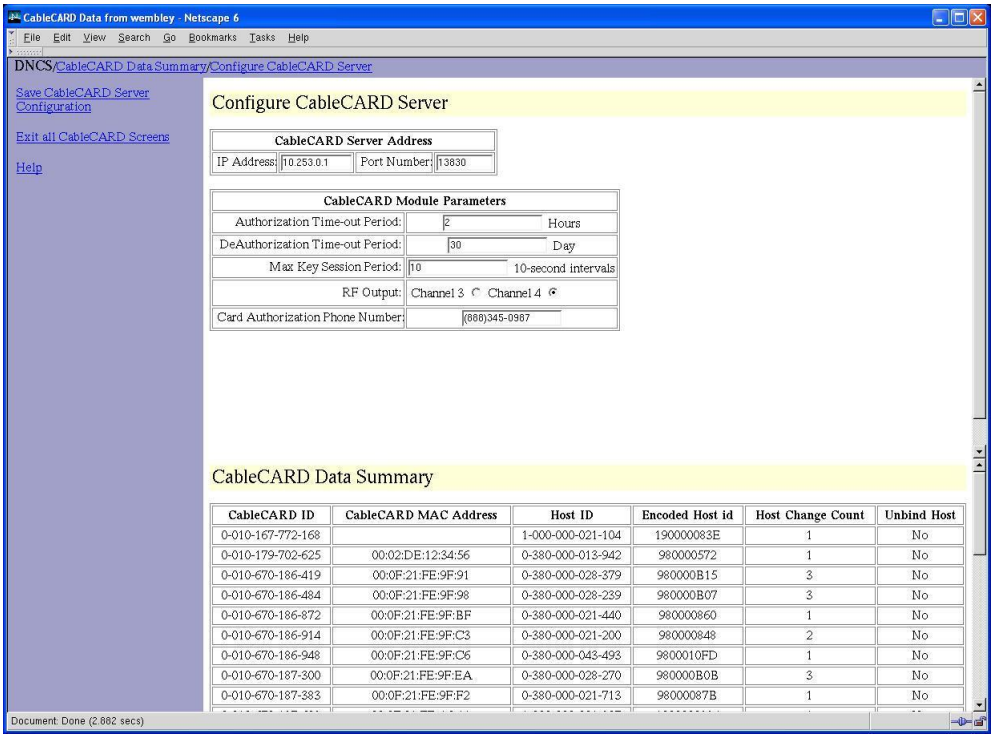
Complete the following steps to configure the minimum Set Authorization Time-out Period and Set DeAuthorization Time-out Period fields on the Configure CableCARD Server window.

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

2 Select the **Home Element Provisioning** tab and then click **CableCARD**. The CableCARD Data Summary screen opens.



3 Click **Configure CableCARD Server**. The CableCARD Data Summary screen updates to display Configure CableCARD Server portion of the screen.



4 Follow these instructions to configure the CableCARD Modules Parameters section of the screen.

a In the **Authorization Time-out Period** field, type **2**.

b In the **DeAuthorization Time-out Period** field, type **30**.

5 Click **Save CableCARD Server Config**.

6 Click **Exit all CableCARD Screens**.

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 number of sessions you recorded in the ***Checking the BFS Sessions on the BFS QAM or BFS GQAM*** (on page 48) procedure?

- If **yes**, skip the remainder of this section, and go to ***Verifying a Successful Installation*** (on page 108). The system recovered all of the BFS sessions.
- If **no**, go to ***Tearing Down the BFS and OSM Sessions*** (on page 106).

Tearing Down the BFS and OSM Sessions

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

1 On the DNCS Control window, highlight the **osm** process**.**

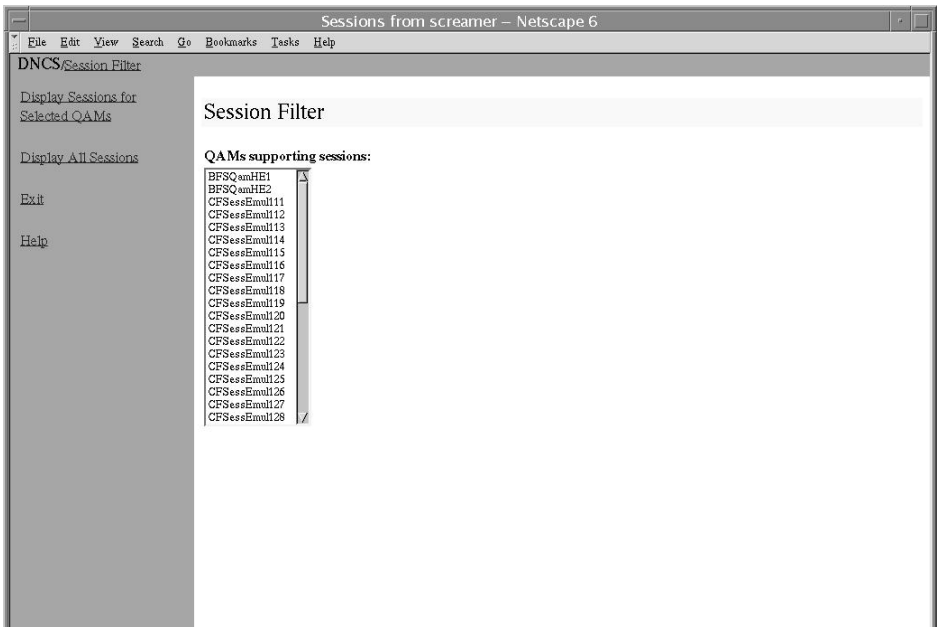
2 Click **Process** and then select **Stop Process**. In a few minutes, the indicator for the osm process changes from green to red.

3 Highlight the **bfsServer** process.

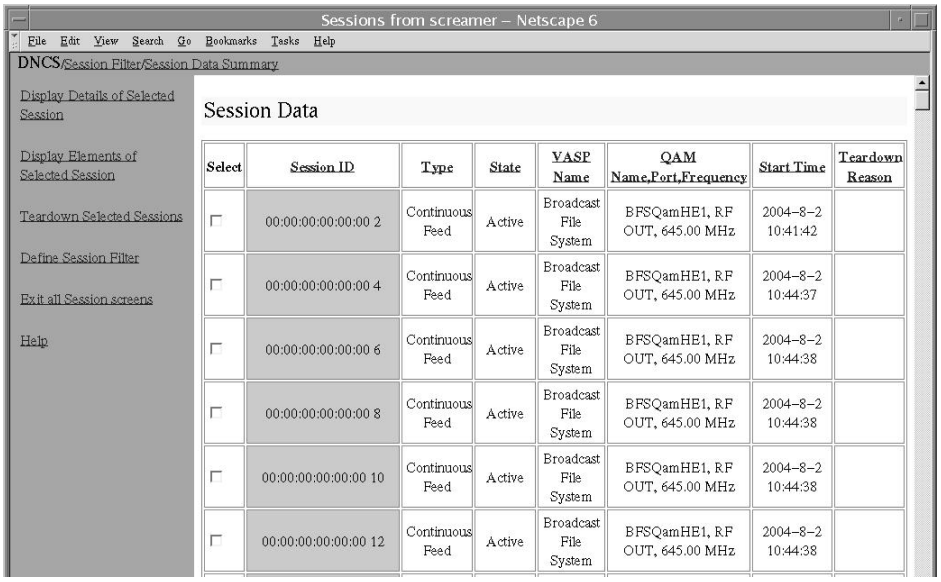
4 Click **Process** and then select **Stop Process**. In a few minutes, the indicator for the bfsServer process changes from green to red.

5 On the DNCS Administrative Console, select the **DNCS** tab and go to **Utilities**.

6 Click **Session List**. The Session Filter window opens.



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



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

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

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

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

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

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

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

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

16 Does the **Session Count** total now equal the number of sessions you recorded in the ***Checking the BFS Sessions on the BFS QAM or BFS GQAM*** (on page 48) procedure?

- If **yes**, go to ***Verifying a Successful Installation*** (on page 108). 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**, 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.

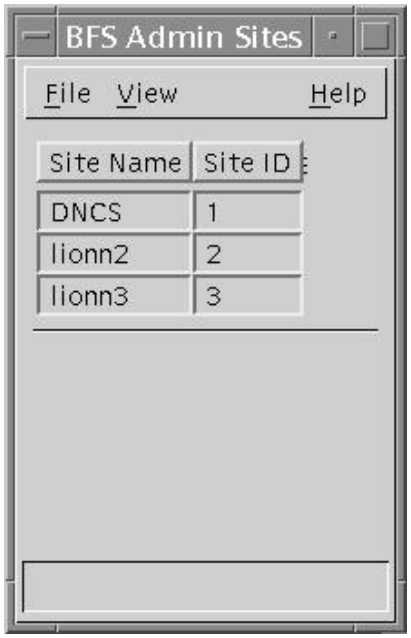
Authorizing the BRF

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)?

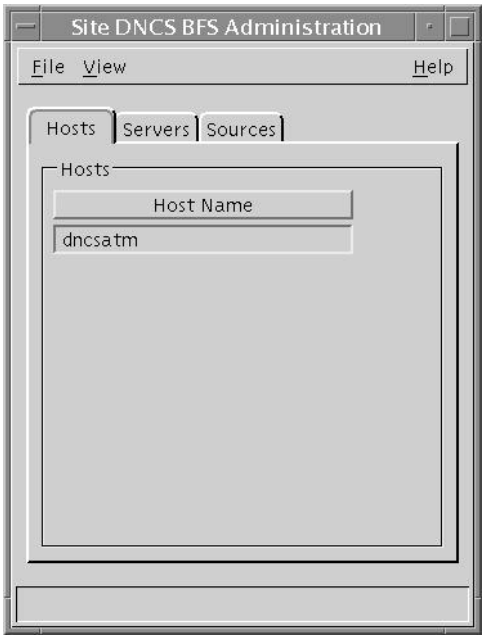
a If **yes**, click **BFS Admin**. The BFS Admin Sites window opens.



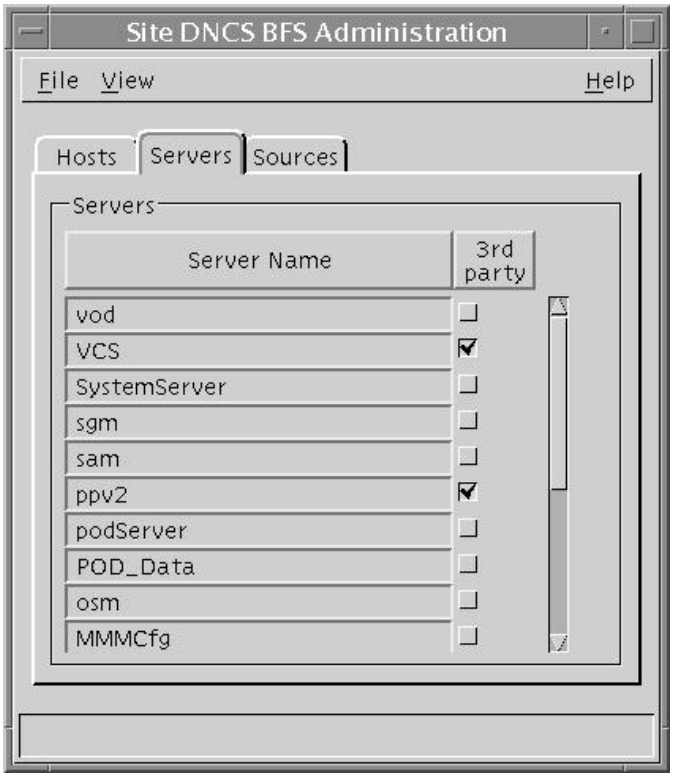
b If **no**, go to step 3.

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 113).

  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.

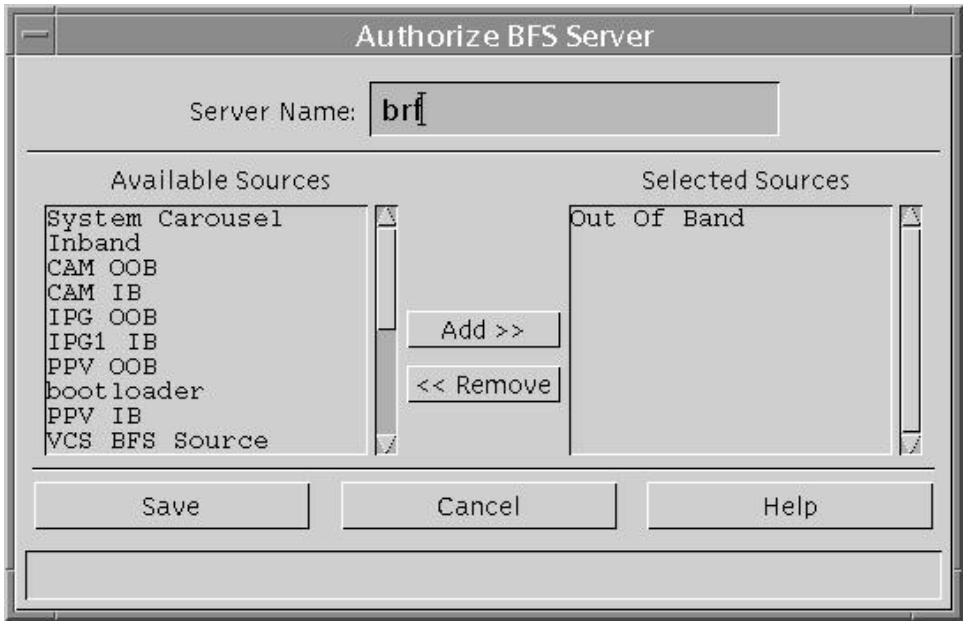
6 Click **File** and then select **New**. The Authorize BFS Server window appears.

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 113).

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)
- *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**, 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

Introduction

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 we wrote to bounce the Pass-Through process are called **elop.sh** 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.sh** and then press **Enter**. The system lists the line(s) within the crontab file that contain elop.ksh.
   b. Type **crontab -l | grep -i bouncePassThru** and then press **Enter**. The system lists the line(s) within the crontab file that contain bouncePassThru.
3. Did the output of step 2 contain any references to the elop.sh or the bouncePassThru scripts?
   - If **yes**, go to step 4 to remove those references.
   - If **no**, go to *Restart the Billing and Third-Party Interfaces* (on page 99).

     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.ksh 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

If you removed the NMI software as part of this 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 50)
- For the Informix database - see ***Back Up the Informix Database*** (on page 55)

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.

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 61), use these procedures, if necessary.
   a ***Stopping the Application Server*** (on page 61)
   b ***Stopping the DNCS*** (on page 62).
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 Insert the CD labeled **DBDS Maintenance CD** into the CD drive of the DNCS.
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.

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

18 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?

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

Note: Depending upon your system configuration, it may take up to an hour for all of the data to become mirrored.

20 Type **eject cdrom** and then press **Enter**. The system ejects the CD.

21 Type **exit** and then press **Enter**. The xterm window closes.

22 Click **EXIT** on the toolbar to log out of the DNCS.

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

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

25 Log on to the Application Server as **dncs** user.

26 Follow the procedures in the ***Restart the System Components*** (on page 94).

Reinstall the NMI Software

If you removed the NMI software as part of this 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:

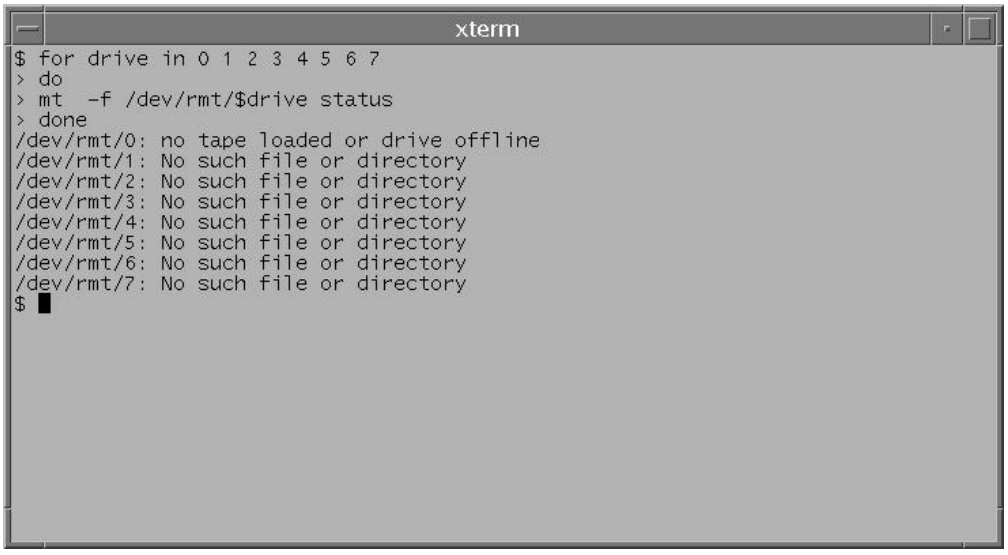
- You will only have to complete this procedure once. The device name of your tape drive will not change unless you specifically change the tape drive configuration.
- Do not have a tape in the tape drive when you complete this procedure.

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 136).
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 136).

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**.
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.
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 62).

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 142).

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 62). Then, go to ***Install the ASI Package*** (on page 139).
- If **no**, go to ***Install the ASI Package*** (on page 139).

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 143).

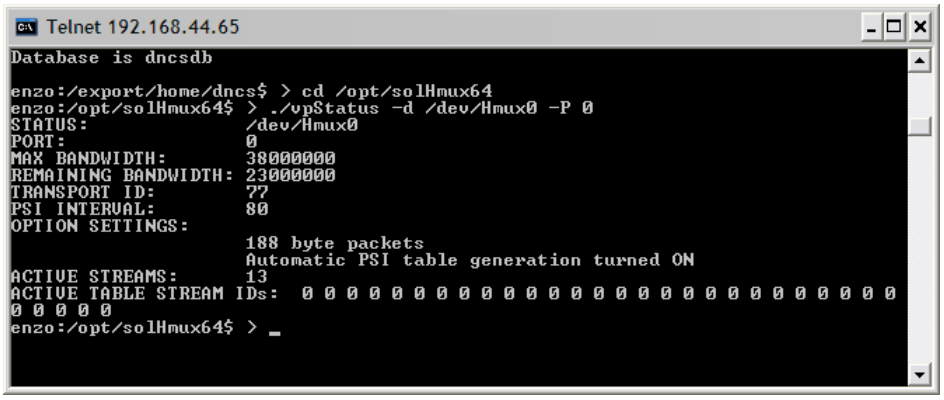
Check the Status of the ASI Card

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 144).
- 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**.
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 Aptiv 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.

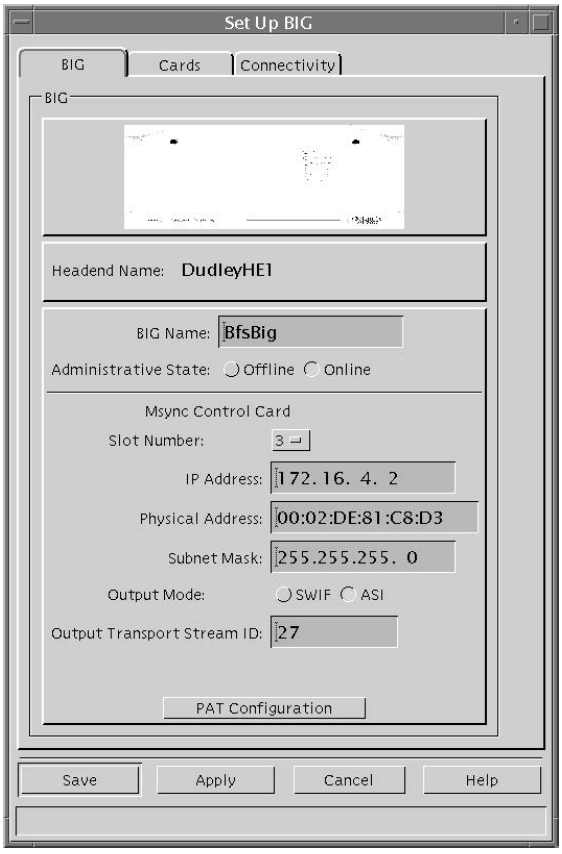
1 From the DNCS Administrative Console, select the **Element Provisioning** tab.

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**.

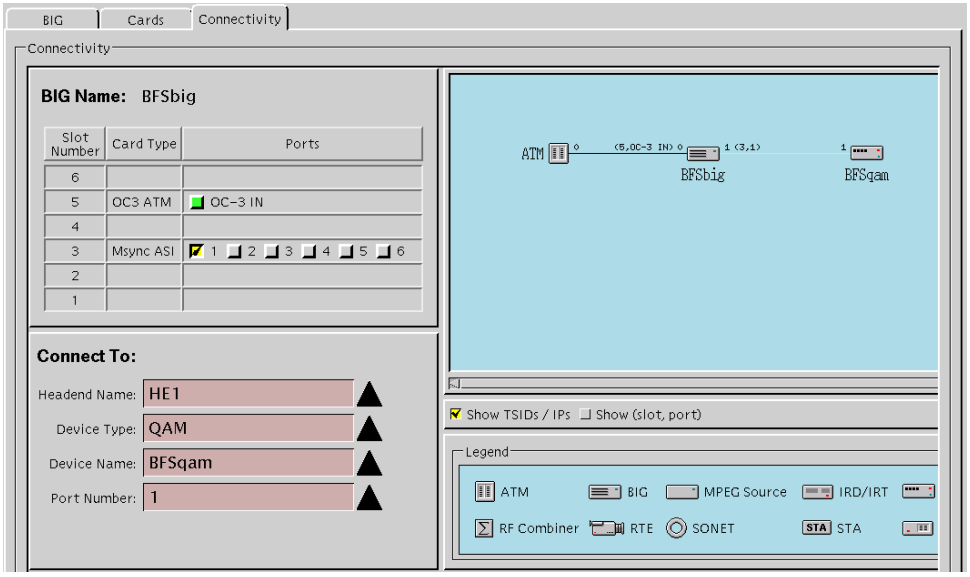
Note: In this example, the Output Transport Stream ID value is 27.



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: _____

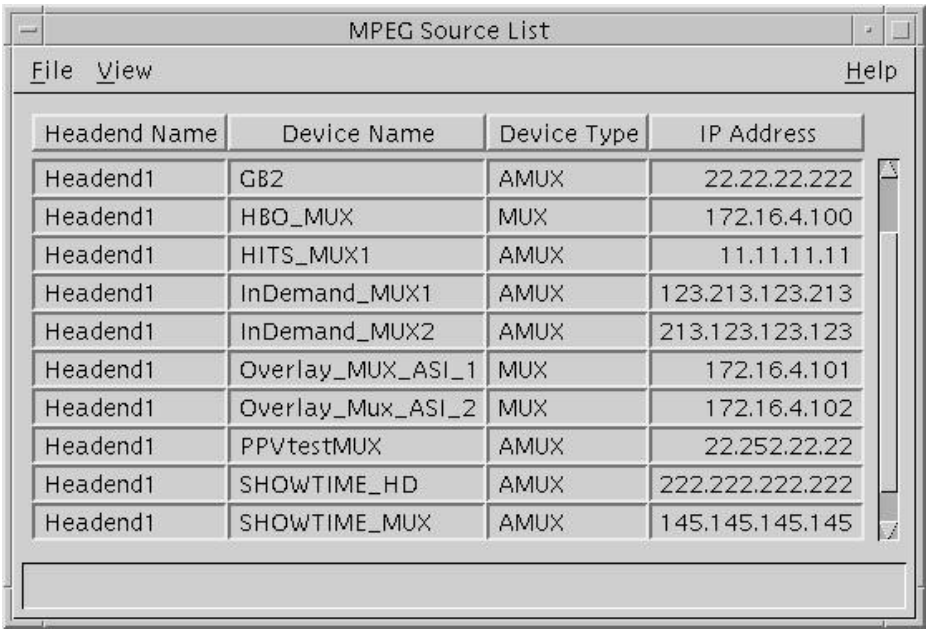
Port Number: _____

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.

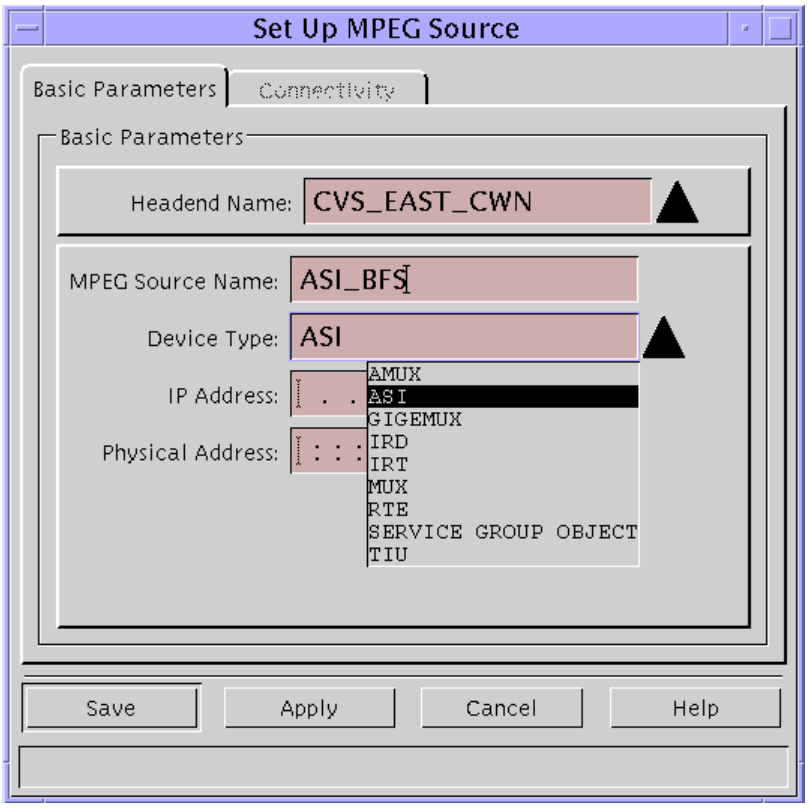
b Type ASI_BFS in the MPEG Source Name field.

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.

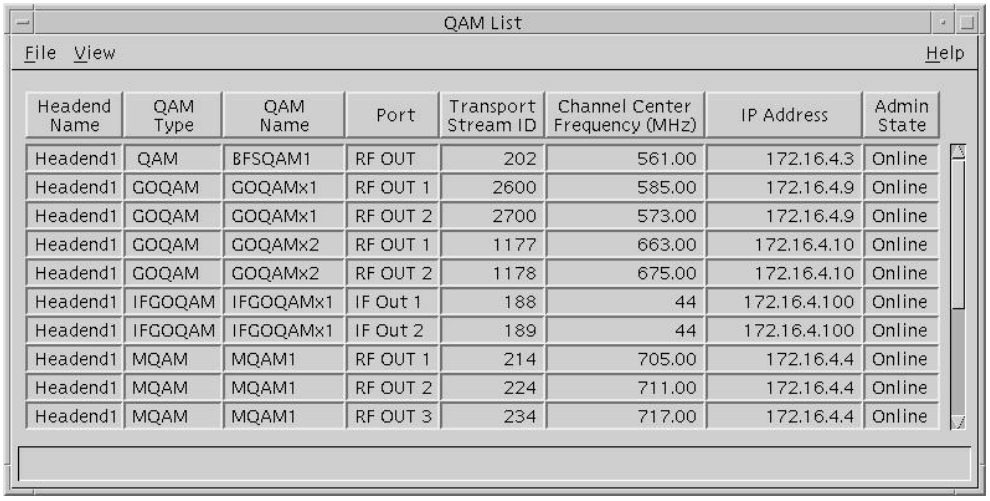
7 Click **Close**. The Set Up MPEG Source window closes.

8 Go to ***Set Up the QAM*** (on page 152).

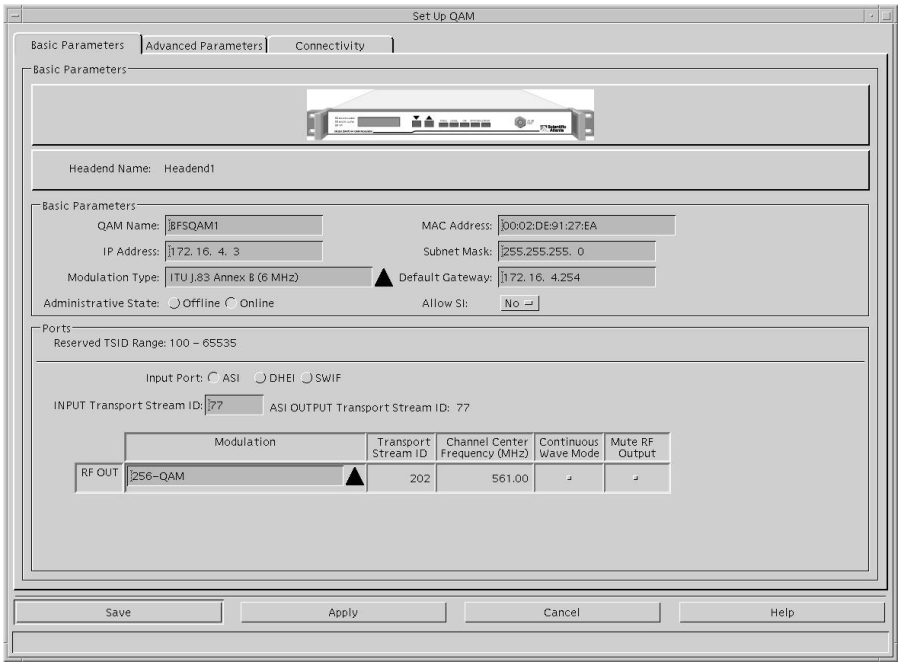
Set Up the QAM

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, ***Creating an MPEG Source*** (on page 149).

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.

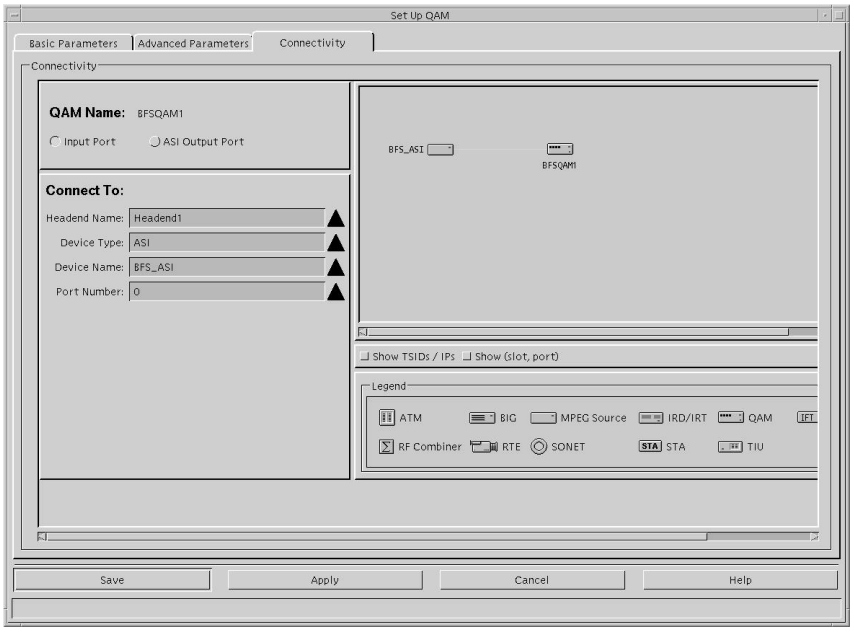
a Click the arrow to the right of the **Headend Name** field and choose the appropriate headend.

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.

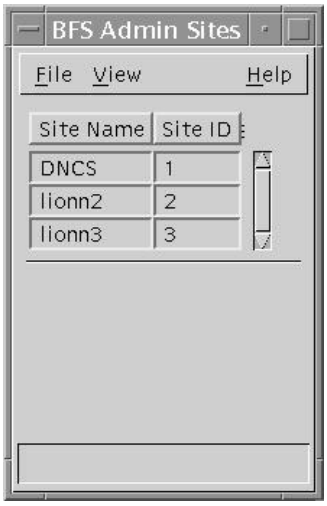
10 Close the Set Up QAM window.

11 Go to ***Set Up the BFS Host*** (on page 155).

Set Up the BFS Host

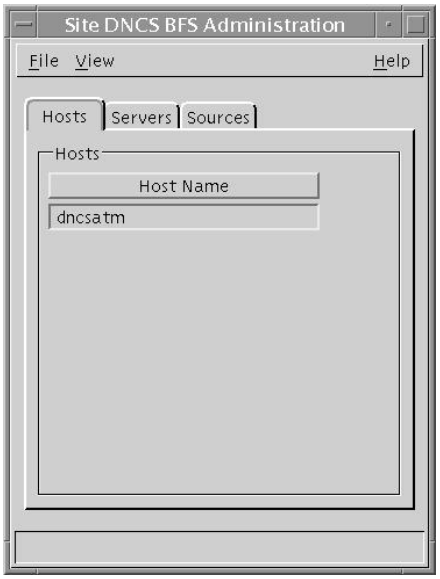
After setting up the QAM, follow these instructions to set up the BFS host.

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

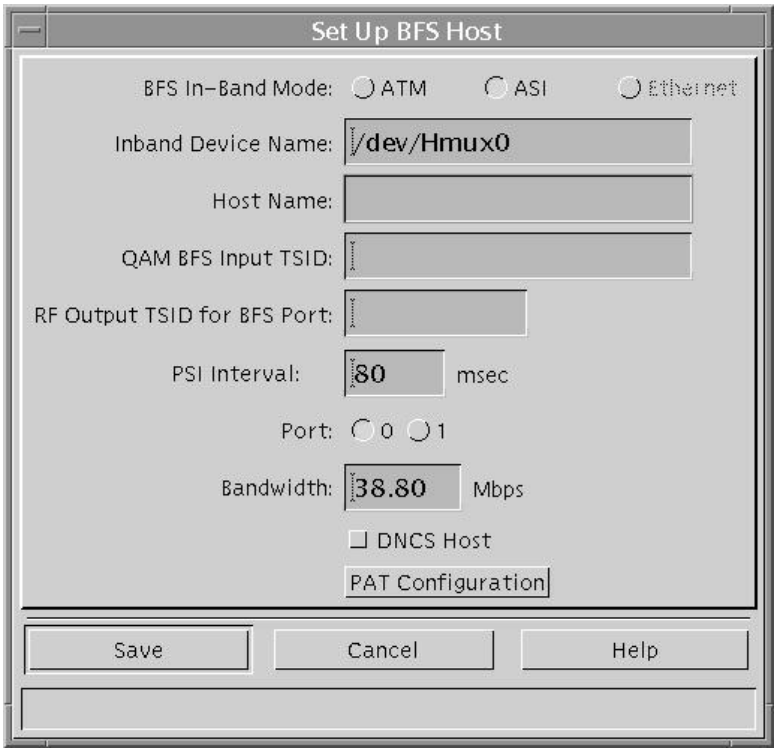


2 Double-click the site name of the system you are setting up. The Site [BFS site] BFS Administration window opens.

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 *Setting the BIG Offline* (on page 158).

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.

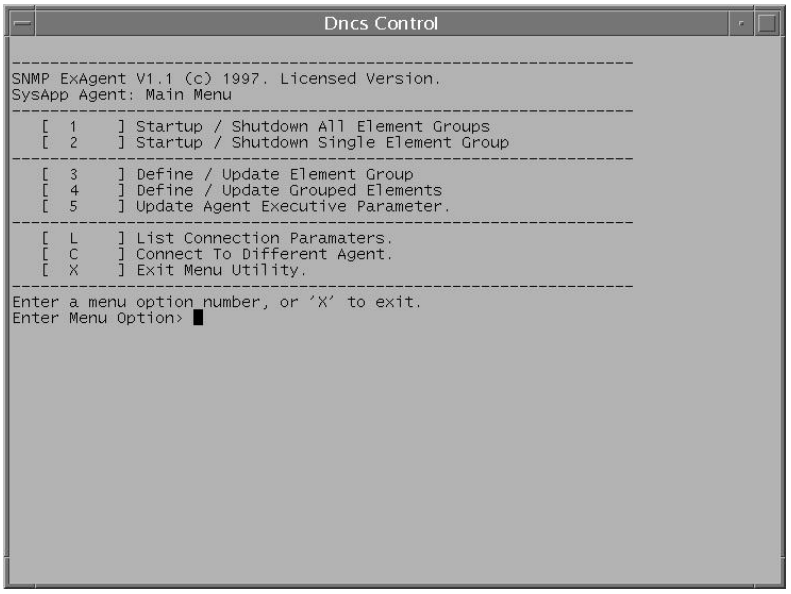
1. From the DNCS Administrative Console, select the **Element Provisioning** tab.
2. Click **BIG**. The BIG List window opens.
3. Double-click the BIG. The Set Up BIG window opens.
4. At the **Administrative Status** field, select **Offline**.
5. Click **Save**. The system saves the BIG status to be offline.
6. Go to ***Stop the BFS and OSM Processes*** (on page 159).

Stop the BFS and OSM Processes

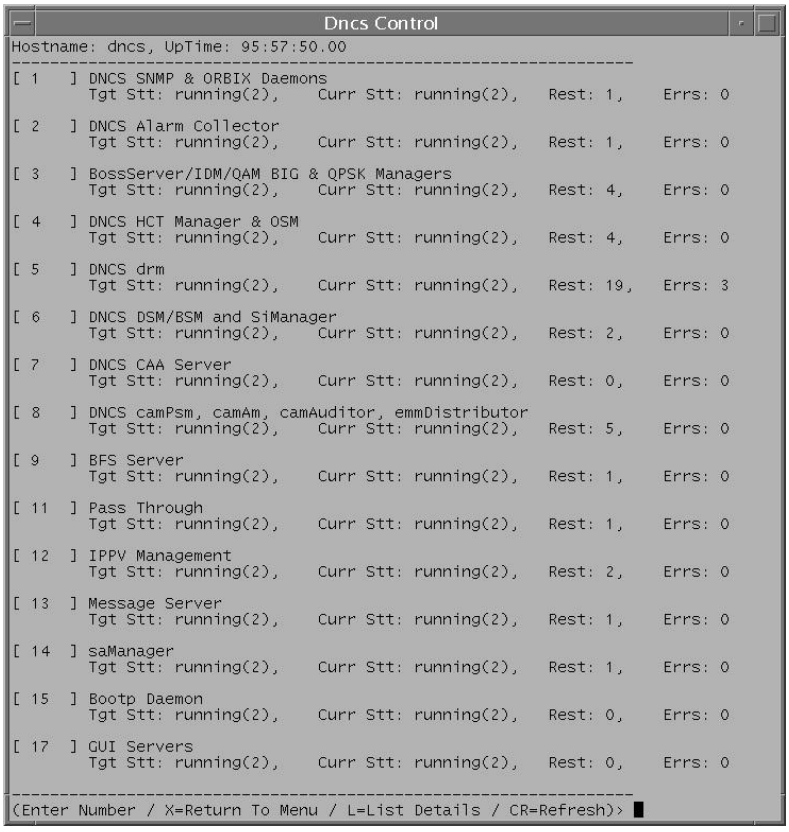
After setting the BIG offline, you need to stop the BFS and OSM processes on the DNCS next. Follow these instructions to stop the processes.

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.

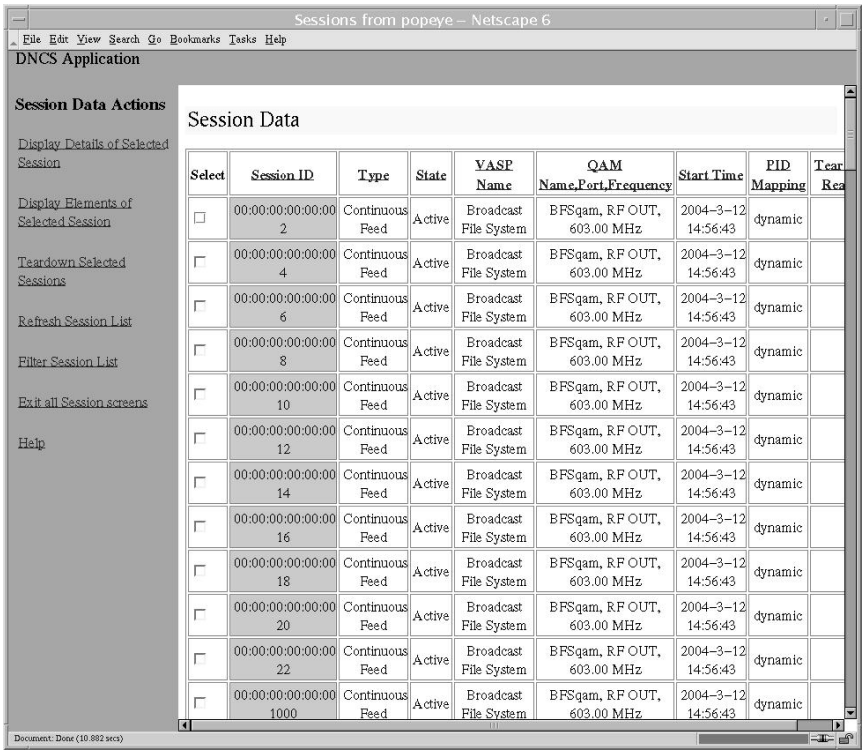
15 Go to ***Tear Down BFS Sessions*** (on page 162).

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 165).
- 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 54).

Verify DBDS Stability

Re-run the procedures in ***Verify DBDS Stability*** (on page 54).

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

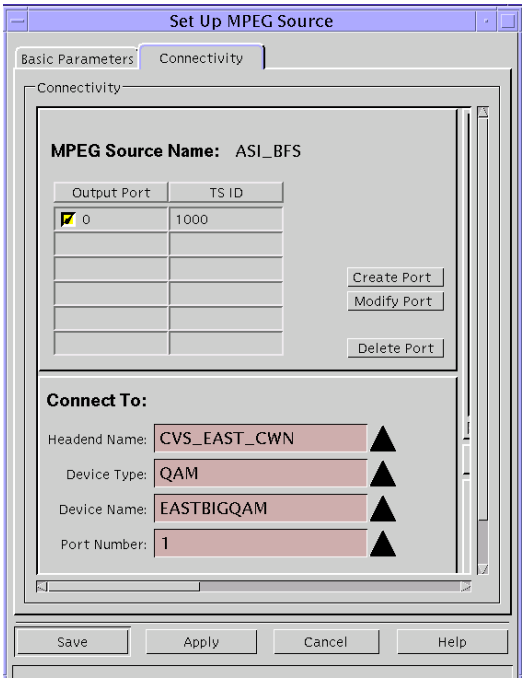
The first step in rolling back the Direct ASI installation requires that you record the current transport stream ID (TSID) values for the BFS MPEG source and the BFS QAM.

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.

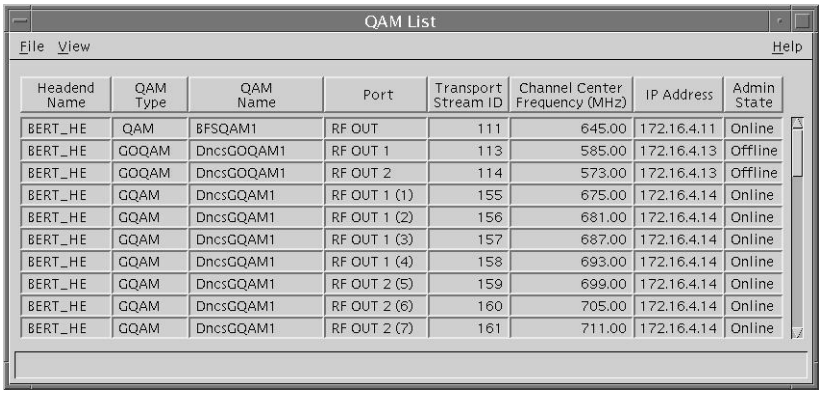


4. Record the value for **TS ID** here: _____
5. Click **Cancel** to close the Set Up MPEG Source window.
6. Click **File** and then select **Close** to close the MPEG Source List window.

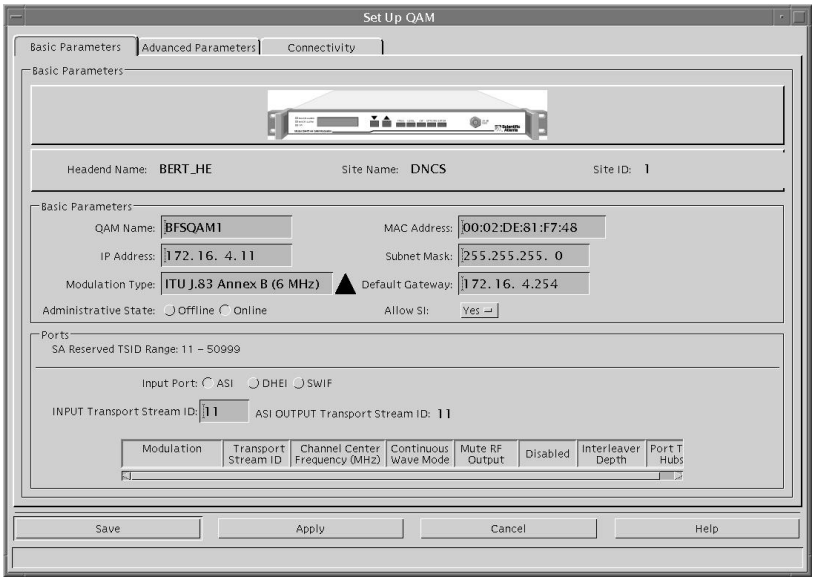
Recording the TSID Value for the BFS QAM

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

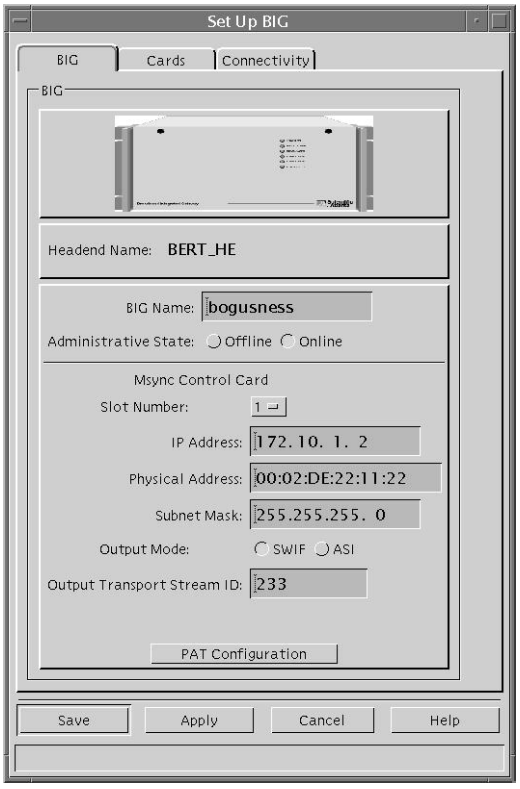
When you configured your system for Direct ASI in Appendix C, one of the procedures called for you to record the BFS TSID and the QAM connection details regarding the Direct ASI card. If you failed to complete the ***Record Configuration Data*** (on page 146) procedure when you configured your system 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 179).
   - 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.

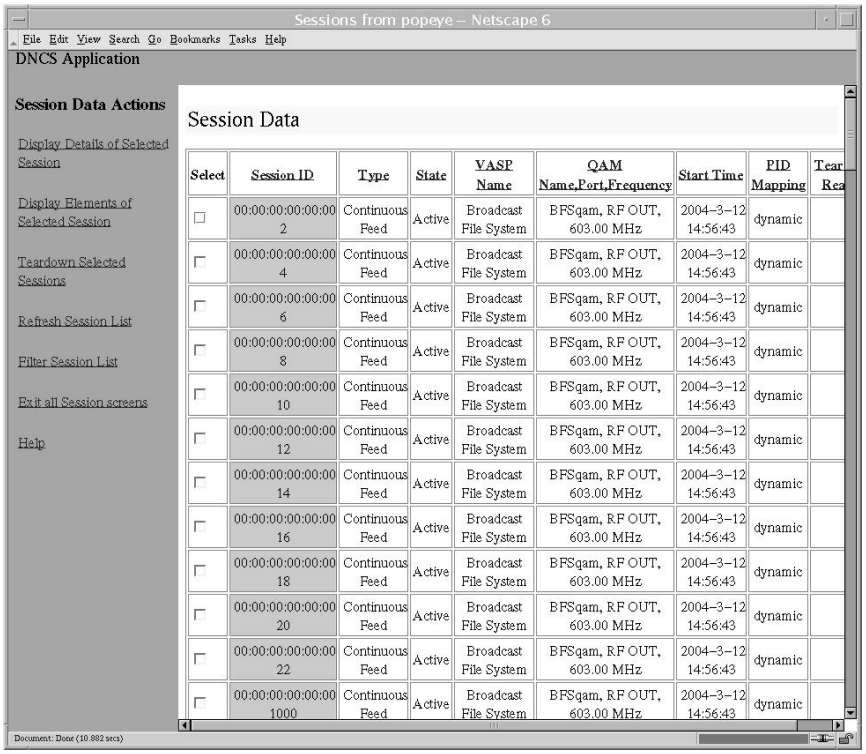
   Important: Do not go to the next procedure until the indicator has changed to red.

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.

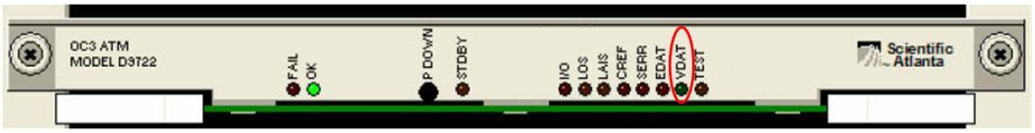
   Important: Do not go to the next procedure until the indicator has changed to green.

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.



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

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

Part Number 4019475 Rev D
May 2012 Printed in USA