System Release 4.0 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**.

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

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

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

Copyright

Contents

About This Guide

Introduction

This guide provides step-by-step instructions for upgrading a Cisco Digital Broadband Delivery System (DBDS) to System Release (SR) 4.0 Service Pack 2 (SP2). Sites that use this guide to upgrade must currently support SR 4.0.

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 Cisco Resident Application (SARA) or another resident application.

Audience

These release notes and installation instructions are written for system operators of Cisco's DBDS, as well as for Cisco engineers who install the SR 4.0 SP2 software onto a Digital Network Control System (DNCS) and a Cisco Application Server.

Related Publications

You may find the following publications useful as resources when you implement the procedures in this document. Check the copyright date on your resources to assure that you have the most current version. The publish dates for the following documents are valid as of this printing. However, some of these documents may have since been revised:

- *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455, published October 2006)
- *DBDS Utilities Version 5.1 Installation Instructions and DNCS Utilities User's Guide* (part number 740020, published June 2006)
- *DBDS Backup and Restore Procedures for SR 2.2/3.2, SR 2.5/3.5, SR 2.6/3.6, SR 3.3, CV SR 3.4, and SR 4.0* (part number 4011040, published September 2005)
- *Program and System Information Protocol Configuration for System Releases 2.5, 3.5, and 4.0* (part number 4011319, published September 2005)
- *RNCS Installation and Upgrade Instructions* (part number 4003191, published September 2005)

- *DBDS Alarm Manager 1.0 Installation Instructions* (part number 745262, published June 2005)
- *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377, published June 2005)
- *DHCT Status Reporting and signonCount Utilities User's Guide* (part number 738186, published November 2004)
- *CoolTools Utilities User's Guide* (part number 749640, published October 2004 [revision expected date: early 2007])
- *Configuring Variable Length Subnet Masks in System Release 2.1 or 3.0 Upgrades Technical Bulletin* (part number 4000375, published November 2002)
- *Daylight Saving Time Configuration Guide* (part number 749233, expected publish date: early 2007)

Document Version

This is the third release of this document.

1

Introducing System Release 4.0 Service Pack 2

Introduction

This chapter lists major improvements and beneficial operational changes for the DNCS as a result of installing an 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 4.0. This guide provides instructions for upgrading to SR 4.0 SP2.

Daylight Savings Time Patch

The SR 4.0 SP2 software contains a Daylight Savings Time (DST) patch that loads onto the DNCS and the Application Server. This patch allows the system to be configured to accommodate new rules that extend DST by 4 weeks beginning with the spring 2007 time change.

Time to Complete the Upgrade

The upgrade to SR 4.0 SP2 must be completed within a maintenance window. Cisco engineers have determined that a typical site can be upgraded in approximately 6 hours.

In This Chapter

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 Cisco marketing manager for additional details on any of these change requests (CRs).

CR 51103-02

Cisco engineers have corrected a condition that sometimes caused the eventManager process on the DNCS (and the RNCS) to crash.

CR 52217-02

A condition that caused the siteStop and siteStart commands to function incorrectly has been corrected.

CR 52962-03

During new installations of SR 2.5/3.5 code, the BFS Admin user interface on the DNCS would not permit a host to be created. This condition has been corrected.

CR 54437-03

A condition which caused an EAS message to display correctly on the subscriber's TV, while displaying a "Send Message Failed" message on the DNCS user interface, has been corrected.

CR 54851-03

Cisco has corrected a condition which caused EAS filters to revert to default values following UniPack upgrades to SRs 4.0, 4.1, and CV3.4.

CR 55465-03

Cisco has corrected an issue that had prevented the NO_CCCM modifier from working correctly with the PPV SAM Service application URL.

CR 56334

Cisco has added the checkimage script to the DNCS. The checkimage script examines image file descriptions for spaces and other invalid characters.

CR 56379

Implementation of this CR corrects a condition whereby the drm process does not re-use User Datagram Protocol (UDP) ports on a QAM modulator after the maximum UDP port limit is reached.

CR 56404-02

Cisco engineers have corrected a condition which caused an occasional crash of the dsm process while recovering or setting up large numbers of group sessions.

CR 56436

Changes to the ippvReceiver process now provide the system with the ability to disable the reporting of impulse-pay-per-view (IPPV) purchases from DHCTs for which there is no matching event record in the database.

CR 56569-01

After upgrades from SR 2.2 to SR 4.4, some sessions for third-party applications could not be restarted. Cisco engineers have corrected this condition.

CR 56867-03

When a headend is created with an ID of 0 (zero), the osm and PassThru processes of the DNCS are unable to send CVT messages. The user interface of the DNCS was modified so that system operators can no longer create headends with an ID of 0 (zero).

CR 58501-03

The bfsServer process of the DNCS has been modified so that IDs from server registrations that fail are released, resulting in a conservation of system resources.

CR 58700

Cisco engineers have corrected a condition that caused the install_pkg script to erroneously remove the SAISP package from the system during execution.

CR 59170-03

The hctmConfig process of the DNCS has been modified so that it can process the null terminator portion of the DHCT serial number, which is part of UNConfig data.

CR 59523-01

Cisco engineers have corrected a condition whereby the oxaitManager process failed to parse certain types of transaction header information correctly.

CR 59525

The EAS functionality of the DNCS has been improved so that multiple EAS messages can be sent from the user interface of the DNCS without causing a crash of the mmmui process.

CR 60381-03

The event timer for the camPsm process has been modified to allow for rounding differences in the data it processes.

CR 60524

The siManager, qpskManager, and QpskManager Api processes have been modified so that the system no longer transmits multiple virtual channel tables (VCTs), while the qpskManager process is down or delayed, during System Information (SI) generation.

CR 60767-01

Cisco engineers have created Solaris patches to provide daylight savings time (DST) support to SR 4.0 SP2.

CR 60796-01

A condition that causes an occasional crash of the qamManager process when processing QAM configuration data entered through the DNCS user interface has been corrected.

CR 60803-04

Cisco engineers have modified the System Time Table's section_length field so that it now accommodates an optional descriptor.

CR 60809-01

Cisco engineers have corrected a condition that caused an occasional crash of the sourceui process during session setup.

CR 60986

Cisco engineers have corrected a condition that caused an occasional crash of the snmpRemote process during upgrades of an RNCS system.

CR 60995-01

Cisco engineers have corrected a condition which caused an occasional crash of the SourceUI process when a session is restarted with the auto-output selection.

CR 60996

Cisco has corrected a condition that occasionally caused Remote Procedure Call (RPC) errors and a crash of the hctmInd process when setting DHCT parameters from the DHCT Manager window.

CR 61004

System operators no longer have to stop and then restart the qamManager process of the DNCS in order to provision the Gigabit Interface (Gbe) of a QAM modulator.

CR 61093

The hctmInd process has been modified so that a condition that prevented UNConfig messages from reaching DHCTs has been corrected.

CR 61277-02

Code for the ocdlManager process has been modified so that it now correctly streams download image data to the Common Download Version Table (CDVT) rather than the Program Map Table (PMT).

CR 61526-02

Code for the Daylight Savings Time (DST) Rules Web user interface (WUI) has been modified to use the term "Last" rather than "Fifth" as the Day Rank in Month.

CR 61633-02

A condition that led to a memory leak in the drm process of the DNCS has been corrected.

CR 61911

RNCS software (SAIlionn 1.0.0.32) has been updated for SR 4.0 SP2.

CR 62095-01

The UNConfig ncExtensions parameter has been modified so that it no longer contains a null value for the DHCT serial number.

What Are the Site Requirements?

Introduction

This section provides the following information:

- Identifies the CDs that are needed to install the service pack software
- List 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 4.0 is currently installed on your system
- You have the CD labeled **DBDS Maintenance CD 2.1.11** (or later) in order to complete the required backups of the database and the filesystem

  Note: DBDS Maintenance CD 2.1.11 is the minimum version that is certified for SR 4.0.
- Sites that are using the RNCS component of the DBDS need the DVD labeled similarly to **RNCS Install DVD**

  Note: Note that this is a DVD and not a CD.
- DBDS Utilities Version 5.1.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 4.0.0.31
- DNCS GUI/WUI 4.0.0.31
- DNCS/Application Server Platform 3.5.0.3p2
- Solaris Patches 3.5.0.3p1

- MQAM 2.6.2
- QAM Application 2.5
- GQAM 3.1.8
- QPSK E14/A62

This service pack can be applied to DBDS networks operating at SR 4.0.

For a list of all available patches to date for SR 4.0 and a complete configuration listing for SR 4.0 SP2, please contact Cisco Services.

Application Platform Release Dependencies

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

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, then subscribers may see video freezing and black screens when using VOD or *anything*-On-Demand (xOD) applications.

Note: This table does not apply if you are using Enhanced Channel Maps.

Set-Top Platform	Operating System (OS)	SARA*	PowerKEY Version
Explorer 8300 DVR v. 1.3.1a17 (or later)	OS 6.14.10.1	1.87.14.1	3.7.5
Explorer 8000/8010 DVR v. 1.3.1a17 (or later)	OS 6.12.7.1	1.87.13.1	3.7.5
Explorer 3250HD MR4 P1 (or later)	OS 3.12.8.1	1.57.8.1	3.7.5
Explorer 2xxx, 31xx, 3200, 3100HD	OS 3.10.9	1.54.23.1	1.0.6.20 (Explorer 2000s) 1.0.7 (all others)

* *Cisco Resident Application*

Important! If you are not using the Cisco Resident Application, contact your resident application provider to verify that you have the most recent version.

Server Platforms

The following Digital Network Control System (DNCS) and Application Server hardware platforms are supported by this software release.

DNCS

Platform	Hard Drives	Memory
Sun Fire V880	12 X 73 GB	1 GB minimum **Note:** The Sun Fire V880 server ships with 8 GB of memory.
Sun Enterprise 450	■ 7 X 9 GB ■ 7 X 18 GB ■ 10 X 9 GB ■ 10 X 18 GB	1 GB minimum
Sun Enterprise 250	■ 2 X 9 GB ■ 2 X 18 GB	1 GB minimum

Application Server

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

What Are the Known Issues?

Introduction

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

CR 52037-06

A condition whereby the automatically generated mmi.txt and gfc.txt files would not link to the BFS POD_Data server if manually created links existed has been corrected.

CR 57524

The alarmCollector process needs modification to improve the efficiency with which system memory is used.

CR 61178

The Web User Interface (WUI), used for configuring daylight savings time (DST) rules needs to be modified so that non-US zones cannot be selected. DST pertains only to US zones.

2

DNCS Pre-Upgrade Procedures

Introduction

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

The first few 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 13), 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 day of 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 in the planning process to ensure that your system is not accessing 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 following 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 these procedures.

- ***Verify the Integrity of the CDs*** (on page 17)
- Check Available Disk Space
- ***Run the Doctor Report*** (on page 19)
- ***Examine Mirrored Devices*** (on page 20)
- ***Verify DBDS Stability*** (on page 21)
- Verify and Back Up the Current Modulator Software
- ***Check the EAS Configuration—Pre-Upgrade*** (on page 22)
- ***Obtain System Configuration*** (on page 23)
- ***Collect Network Information*** (on page 24)
- ***Check and Remove Sessions*** (on page 26)
- ***Back Up the DNCS FileSystem and Application Server*** (see "Back Up the DNCS and Application Server Filesystems" on page 28)
- ***Stop the dhctStatus and signonCount Utilities*** (on page 31)
- ***Back Up and Delete the copyControlParams File*** (on page 33)
- ***Back Up the Informix Database*** (on page 29)

During the Maintenance Window

At the beginning of the maintenance window you should start with ***Suspend Billing and Third-Party Interfaces*** (on page 30) procedure and continue to 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 Cisco 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

Enabled Features

The following optional features can be enabled by engineers at Cisco Services, without a special license:

- Conditional Access Mode—Specifies whether the Cisco (PowerKEY®) encryption method or a non-Cisco encryption method is used for DHCTs in the network
- DBDS Network Overlay—Allows Cisco 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 Cisco 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 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, 3.5, and 4.0*.
- 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, using up to three distinct conditional access systems

Verify the Integrity of the CDs

1. 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**.
2. Insert the CD into the CD drive on the DNCS.

   Note: If a File Manager window opens after you insert the CD, close the window.
3. Type **cd /cdrom/cdrom0** and then press **Enter**. The /cdrom/cdrom0 directory becomes the working directory.
4. Type **ls -la** and then press **Enter**. The system lists the contents of the CD.
5. Did the system list the contents of the CD as expected?
   - If **yes**, go to step 6.
   - If **no**, the CD might be defective. Call Cisco Services for assistance.
6. 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 clearly lists any errors found during the package check.
7. 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.
8. Repeat steps 1 through 7 for each CD received in the software binder.

Back Up the Current Modulator Configuration Files

Backing Up the Current Modulator Configuration Files

Follow these instructions to back up your current QAM, MQAM, GQAM, and QPSK configuration files.

1. Type **cd /tftpboot** and then press **Enter**. The /tftpboot directory becomes the working directory.
2. Depending upon which configuration files you need to back up, choose one or more of the following options:
   - To back up the QAM configuration file, type **cp -p qam.config qam.config.<version number>** and then press **Enter**.
   - To back up the MQAM configuration file, type **cp -p mqam.config mqam.config.<version number>** and then press **Enter**.
   - To back up the GQAM configuration file, type **cp -p gqam.config gqam.config.<version number>** and then press **Enter**.
   - To back up the QPSK configuration file, type **cp -p qpsk.config qpsk.config.<version number>** and then press **Enter**.

   Note: Substitute the current version of your modulator software for <version number>.
3. Go to ***Run the Doctor Report*** (on page 19).

Run the Doctor Report

Introduction

Before upgrading the DNCS, run the Doctor Report using the instructions provided in the *DBDS Utilities Version 5.1 Installation Instructions and DNCS Utilities User's Guide*. 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 *Recommendations for Setting System Information to Out-of-Band*, 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 880 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

Follow these instructions to examine the status of the mirrored drives on your Enterprise 450 or the Sun Fire 880 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 DBDS Stability*** (on page 21).
   - If **no** (to either or both conditions listed in step 3), call Cisco Services for help in resolving these issues with the metadevices.

Verify DBDS Stability

Verifying DBDS Stability

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

      Note: Do *not* press the Power button.

   b. Access the Power On Self Test and Boot Status diagnostic screen on the DHCT and verify that all parameters, except UNcfg, display **Ready**. UNcfg displays **Broadcast**.

      Note: The fields on this screen may take 1-2 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 video-on-demand and /or xOD program.

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*.

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. If necessary, open an xterm window on the DNCS.
2. Type **more /etc/hosts** and then press **Enter**. A list of IP (Internet Protocol) addresses and hostnames appears.
3. 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 _____
4. Type **uname -n** and then press **Enter**. The hostname for the DNCS appears.

   Important! Call Cisco Services if the hostname contains a period (.). Cisco Services engineers will help you change it to a valid hostname.
5. Write down the hostname for the DNCS, as displayed in step 4: _____
6. From an xterm window on the Application Server, type **more /etc/hosts** and then press **Enter**. A list of IP addresses and hostnames appears.
7. Write down the IP addresses and hostnames for the following hosts:

   - dncsatm _____
   - appservatm (if appservatm is not 10.253.0.10) _____
8. At the Application Server, type **uname -n** and then press **Enter**. The hostname for the Application Server appears.
9. 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 On the DNCS, complete these 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**.

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

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

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

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

   Note: Press **Enter** after typing each command.

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

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

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

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

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

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

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

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

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

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

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

   j **netstat -nrv > netstat.out**

   k **ifconfig -a > ifconfig.out**

   l **df -k > df.out**

   m **eeprom nvramrc > nvramrc.out**

   n **cd /var/spool/cron**

   o **tar cvf crontabs.< date >.tar crontabs**

   p **cp crontabs.< date >.tar /export/home/dncs/network**

   Note: <date> is the current date.

   q **cd /export/home/dncs/network**

6 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.

7 Go to ***Check and Remove Sessions*** (on page 26).

Check and Remove Sessions

Introduction

After you have obtained 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 is done both before and after the installation process is complete to provide a comparison of the number of sessions. This comparison indicates a successful upgrade by ensuring the correct number of sessions were built after the upgrade process is complete.

Checking the BFS Sessions on the BFS QAM

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> 2** and press **Enter**.

  Important! You must be logged in as dncs user.

  Note: <IPAddr> is the IP address of the data QAM.

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

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 be running 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.

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: A cron job refers to programs that run automatically, without specific user intervention.

Stopping the cron Jobs on the DNCS

Complete the following steps to stop cron jobs on the DNCS.

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

1. Type **ps -ef | grep cron** and then press **Enter**. The system lists running processes that include the word cron.
2. Did the results from step 1 include **/usr/sbin/cron**?
   - If **yes**, type **/etc/rc2.d/S75cron stop** and then press **Enter**. The system stops all cron jobs.
   - If **no**, go to Stopping the cron Jobs on the Cisco Application Server; the cron jobs are already stopped on the DNCS.
3. Confirm that the cron jobs have stopped by typing **ps -ef | grep cron** again and then press **Enter**. The system should list only the grep process.

Stopping the cron Jobs on the Cisco Application Server

Follow these instructions to stop cron jobs on the Cisco Application Server.

1. Are you already logged on to an xterm window as root user?
   - If **yes**, go to step 2.
   - If **no**, log on to an xterm window as root user.
2. Type **ps -ef | grep cron** and then press **Enter**. The system lists running processes that include the word "cron".
3. Did the results from step 2 include /usr/sbin/cron?
   - If **yes**, follow these instructions.
     a. Type **/etc/rc2.d/S75cron stop** and then press **Enter**.
     b. Type **ps -ef | grep cron** and then press **Enter** to confirm that the cron jobs have stopped. The system should list only the grep process.
   - If **no**, the cron jobs are already stopped.

Back Up the DNCS and Application Server Filesystems

Perform a complete backup of the filesystem now. Procedures for backing up the filesystem are contained in *DBDS Backup and Restore Procedures for SR 2.2/3.2, SR 2.5/3.5, SR 2.6/3.6, SR 3.3, CV SR 3.4, and SR 4.0*. 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 filesystem are found in the **Backing Up and Restoring the DNCS and Application Server** chapter of the *DBDS Backup and Restore Procedures for SR 2.2/3.2, SR 2.5/3.5, SR 2.6/3.6, SR 3.3, CV SR 3.4, and SR 4.0*.
- It may take up to 2 hours to back up a DNCS filesystem; you can usually back up an Application Server filesystem in about 30 minutes.

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 2.2/3.2, SR 2.5/3.5, SR 2.6/3.6, SR 3.3, CV SR 3.4, and SR 4.0*. If necessary, call Cisco Services to obtain a copy of these backup and restore procedures.

Notes:

- Procedures for backing up the Informix database are found in the *DBDS Backup and Restore Procedures for SR 2.2/3.2, SR 2.5/3.5, SR 2.6/3.6, SR 3.3, CV SR 3.4, and SR 4.0*.
- It takes about 45 minutes to back up the database on a typical system.

Suspend Billing and Third-Party Interfaces

Important Note About the Maintenance Window

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 dhctStatus and signonCount Utilities

Introduction

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

Terminating the dhctStatus Utility Polling Operation

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

1. 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. If applicable, 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 each process ID displayed in step 4.

   Example: Kill -9 12556
6. Repeat steps 4 and 5 for any process that continues to display active. Once completed the system should only display the grep process.

Removing the signonCount Utility from System Memory

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

2 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.

3 Type **ps -ef | grep signonCount** and then press **Enter**. A list of DNCS processes and process IDs display on the screen.

4 Type **kill -9 <processid>** and then press **Enter** for each process ID displayed in step 3.

5 Type **ps -ef | grep signonCount** and then press **Enter** to ensure all the processes are terminated.

6 Repeat steps 4 and 5 for any process that continues to display active. Once completed the system should only display the grep process.

Back Up and Delete the copyControlParams File

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

1. Check with the system operator and determine whether the site you are upgrading has any customized entries in the copyControlParams.inf file.

   Note: If the copyControlParams.inf file has customized entries, you will make a back up copy of the file (in step 4) before deleting it.

2. If necessary, open an xterm window on the DNCS.
3. Type **cd /export/home/dncs** and then press **Enter**. The /export/home/dncs directory becomes the working directory.
4. 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 5.
5. 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.

Remove the NMI Software

1. Are you already root user in an xterm window on the DNCS?
   - If **yes**, go to step 3.
   - If **no**, go to step 2.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The **password** prompt appears.
   b. Type the root password and press **Enter**.
3. Type **pkginfo -l | grep SAInmi** and then press **Enter**. The system lists the SAInmi package if it is installed.
4. Is SAInmi installed?
   - If **yes**, go to step 5.
   - If **no**, you do not have NMI loaded onto your system. Skip the rest of this procedure, and go to ***Stop System Components*** (on page 35).
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

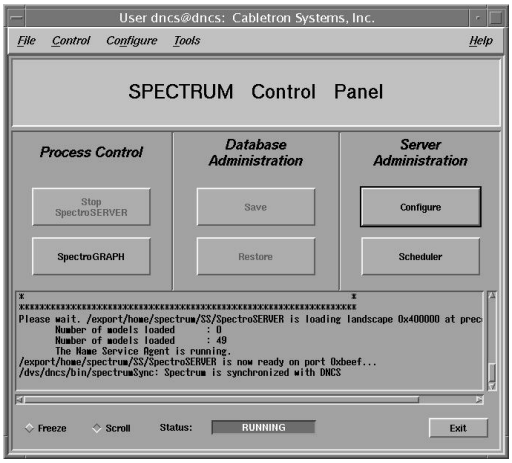
Before continuing with the installation process, follow the instructions in this section to stop the Spectrum Network Management Service (Spectrum), the Application Server, and the DNCS.

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 Spectrum

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



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

Stopping the Application Server

This section provides procedures for stopping either a SARA Server or an Aptiv Application 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.

Stopping the Application Server at Aptiv Sites

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.

   Note: If the word **No** does not appear next to each driver within a minute or two, repeat steps 2 and 3 again.

Stopping the DNCS

1. At the DNCS, press the middle mouse button and then select **DNCS Stop**.
2. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The Dncs Control window appears.
3. 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.
4. When the **Curr Stt** (Current State) field of the Dncs Control window indicates that all of the DNCS processes have stopped, follow the on-screen instructions to close the Dncs Control window.

Ensure No Active Database Sessions on the DNCS

1. Close all windows and GUIs that are open except for the xterm window you are working in.
2. Are you already root user in an 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.
4. Type the root password and press **Enter**.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.
5. Type **ps -ef | 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 **ps -ef | 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. Type **ps -ef | grep -i ui** and then press **Enter** to confirm that UI processes have stopped.

   Note: If any GUI processes are still running, repeat step 8.
10. Type **ps -ef | grep -i ui** and then press **Enter** to confirm that ui process have stopped.
11. Are any ui processes running?
    - If **yes**, type **kill -9 [PID]** and then press **Enter** for any consoleui process that was still running.
    - If **no**, go to step 13.

12 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

13 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.

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

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

16 If the dncsInitd process is still running, repeat this procedure from step 15.

3

System Release 4.0 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 back up. Detaching the mirrors allows you the option of recovering quickly in the event of a failed upgrade by booting from the standby drives.

Important! Skip this procedure if the DNCS you are upgrading is an Enterprise 250. Disk mirroring pertains only to the Enterprise E450 or Sun Fire V880 DNCS.

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 4.0 SP2.

1 Insert the CD labeled **DBDS Maintenance CD** 4.0 SP2 (or later) into the CD drive of the DNCS.

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.

5 Type **metastat -p** and then press **Enter**. The system displays output similar to the following example of a DNCS E450:

```
$ 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).

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.

8 Go to ***Install the Service Pack*** (on page 45).

Install the Service Pack

Installing the Service Pack

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 is open?
   - If **yes**, select **File** and choose **Close**, then go to step 3.
   - If **no**, go to step 3.
3. Type **df -n** and then press **Enter**. A list of the mounted file systems appears.

   Note: The presence of /cdrom in the output confirms that the system correctly mounted the CD.
4. Type **/cdrom/cdrom0/install_SP -i** and then press **Enter**. A list of packages displays.
5. Type **y** and then press **Enter**. The software begins to install on the DNCS.

   Note: The system displays a message notifying the installation engineer that interactive mode is enabled.
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 configuration parameters on the screen.
   - 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. Follow these instructions regarding the configuration parameters that are displayed on the screen.
   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.
9. Type **eject cdrom** and then press **Enter** when the installation is complete.

10 Check the log file for errors. Go to ***Install DST Patches on the Application Server*** (on page 47) if the log file indicates that the service pack software installed without error.

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.

Install DST Patches on the Application Server

In this section, you will use the DBDS Service Pack CD to install the daylight savings time (DST) patches on the Application Server.

Installing the DST Patches on the Application Server

Follow these instructions to install the DST patches on the Application Server.

1. Log onto the Application Server as **root** user.
2. Open an xterm window on 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. Insert the CD labeled **DBDS Service Pack** into the CD drive of the Application Server. The system automatically mounts the CD.
5. Type cd /cdrom/cdrom0/SolarisPatches and then press Enter.
6. Type ./install_patches and then press Enter. The system installs patches **109809-3** and **108993-53**.

   Important! Be certain to type the period (**.**) before typing /install_patches.
7. Type **cd /** and then press **Enter**. The home directory on the DNCS becomes the working directory.
8. Type **eject cdrom** and then press **Enter**.
9. Type **exit** and then press **Enter** to log out the root user.

Install Additional Software

Installing Additional Software

Cisco 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. Either type of 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 49).

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 help.

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

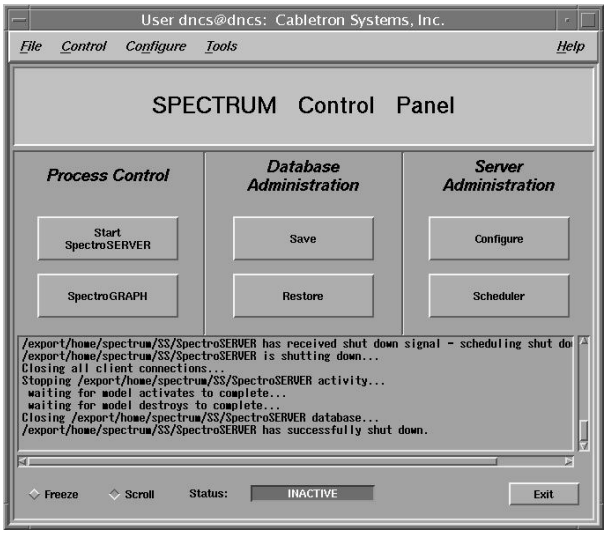
Verifying DNCS Versions

Follow these instructions to verify the installed software versions on the DNCS.

1 From an xterm window on the DNCS, type **pkginfo -l [Package Name]** and then press **Enter**.

Notes:

- The "l" in **-l** is a lowercase letter L.
- Substitute the software component you are verifying for [Package Name].
- Use **SAIdncs** for Package Name the first time you run this procedure.



Example: Notice that the Version field indicates that DNCS version 3.0.0.12 is installed on the DNCS, and the Status field indicates that the software is completely installed.

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

Component	Pkg Name	Expected Results	Actual Results
DNCS Application	SAIdncs	4.0.0.31	
DNCS/App Tools	SAItools	3.5.0.7	
DNCS GUI	SAIgui	4.0.0.31	
DNCS WUI	SAIwebui	4.0.0.31	
Spectrum Kit	SAIspkit	2.0.0.8	
DNCS Online Help	SAIhelp	3.5.0.5	
DNCS Report Writer	SAIrptwrt	3.5.0.2	
QAM	SAIqam	2.4.0	
MQAM	SAImqam	2.6.2	
GQAM	SAIgqam	3.1.6	
GoQAM	SAIgoqam	1.1.2	
QPSK	SAIqpsk	E14 / A62	

3 Repeat steps 1 and 2 for each Package Name in the table in step 2.

4 Do the first three digits of the **Actual Results** match the first three digits of the **Expected Results** for each component in the table in step 2?

- If **yes**, go to ***Disable the SAM Process on Aptiv Systems*** (on page 51) for Aptiv sites or ***Add an EAS Variable to the .profile File*** (on page 52) 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.

Disable the SAM Process on Aptiv Systems

Disabling 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 reboot the DNCS. Follow these instructions to disable the SAM process.

Important! Skip this procedure if the site you are upgrading does not use the Pioneer application server.

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 conformation 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.

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

3 In the space provided, record the IP address associated with dncseth.

_____

Note: This IP address represents the Ethernet address of the DNCS, which you will need in step 8.

4 Type **grep -i LOCAL_EAS_IP /export/home/dncs/.profile** and then press **Enter** and you will search the /export/home/dncs/.profile file.

Note: Type a space between grep -i LOCAL_EAS_IP and/export/home/dncs/.profile.

5 Verify if the entry LOCAL_EAS_IP is in the file and go to step 6.

6 Does the entry contain the IP address of the dncseth entry in the /etc/hosts file?

- If **yes**, go to ***Enable Optional and Licensed Features*** (on page 53).
- If **no**, go to step 7.

7 Type **vi .profile** and then press **Enter**. The .profile file opens for editing using the Unix vi text editor.

8 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] that you recorded in step 3.

9 Save the file and close the vi text editor.

Note: Your changes to the .profile will take effect when you restart the system components in the next procedure.

10 Go to ***Enable Optional and Licensed Features*** (on page 53).

Enable Optional and Licensed Features

Enabling 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. Contact Cisco Services to have the licensed or optional features enabled on your network.

Exception: The Direct ASI feature requires extensive system configuration. If the system you are upgrading is to support this feature, go to ***Direct ASI Installation and Configuration Procedures*** (on page 103) for instructions to install and configure this feature.

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 Cisco wrote to bounce the Pass-Through process are called **elop.sh** and **bouncePassThru**.

Removing Scripts That Bounce the Pass-Through Process

Follow these instructions 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**, then go to ***Reboot the DNCS*** (on page 56).

     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, Cisco recommends 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.

9 Go to ***Reboot the DNCS*** (on page 56).

Reboot the DNCS

After installing the software onto the DNCS, complete the following steps to reboot the DNCS and 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. From an xterm window on the Application Server, type **/usr/sbin/shutdown -g0 -y -i0** and then press **Enter**. The Application Server shuts down.
4. From an xterm window on the DNCS, type **/usr/sbin/shutdown -g0 -y -i6** and then press **Enter**. The DNCS reboots and the CDE Login window appears.
5. Log on to the DNCS as **dncs** user.
6. At the **ok** prompt on the Application Server, type **boot** and then press **Enter**. The Application Server reboots.
7. Log on to the Application Server as **dncs** user.
8. Go to ***Restart the System Components*** (on page 57).

Restart the System Components

Introduction

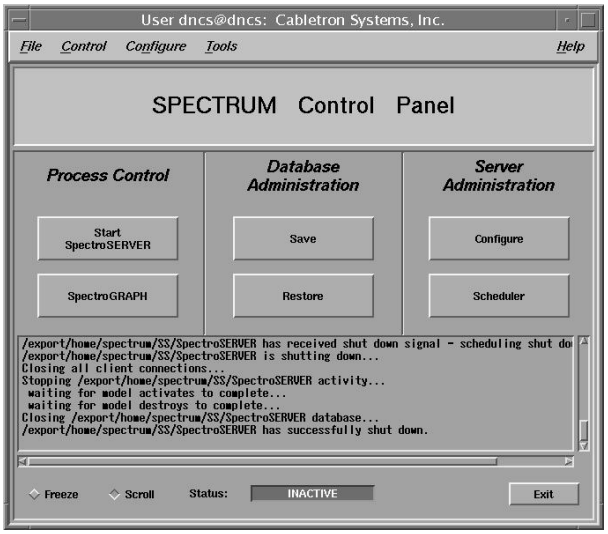
After installing this software, follow these instructions to restart the system components.

Restarting Spectrum

Important! Skip this procedure if you are using DBDS Alarm Manager 1.0 instead of Spectrum.

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

2 Select the Host Machine (usually DEFAULT), and then click **OK**. The Spectrum Control Panel window opens.



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

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

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

Restarting the DNCS

1. 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 Monitor**.

   Results:

   - The DNCS Monitor window opens.
   - Green indicators begin to replace red indicators on the DNCS Monitor window.
4. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The Dncs Control 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 Monitor will all become green when the processes and servers have restarted.

Restarting the Cisco Application Server

Note: If the site you are upgrading uses the Pioneer Application Server, skip this procedure and go to ***Restart the Application Server at Aptiv Sites*** (on page 60).

1. If necessary, open an xterm window on the Application Server.
2. 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.
4. Does the word **running** appear next to the current state field (Curr Stt) of each process?
   - If **yes**, skip the rest of this procedure and go to ***Restart the Billing and Third-Party Interfaces*** (on page 61).
   - If **no**, go to step 5.
5. Press the middle mouse button, and then select **App Serv Start**.
6. When the Application Control window indicates that the current state (Curr Stt) of each process is **running**, go to step 7.

   Note: On some systems, the BFS Remote process may remain at **Stopped**; this is normal.
7. Follow the on-screen instructions to close the Applications Control window.

Restart the Application Server at Aptiv Sites

Introduction

Follow this procedure *only* if the site you are upgrading supports the Aptiv Application Server. If the site you are upgrading supports the Cisco Application Server, skip this section and go to ***Restart the Billing and Third-Party Interfaces*** (on page 61).

Restarting the Application Server at an Aptiv Site

Follow these instructions to check if the Aptiv application has started on the Application Server, and then to start it, if necessary.

1. If necessary, 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?
   - If **yes**, skip the rest of this procedure and go to ***Restart the Billing and Third-Party Interfaces*** (on page 61).
   - If **no**, go to step 4.

   Note: The word **Yes** next to a driver indicates that the process has started.
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 Aptiv drivers.

Restart the Billing and Third-Party Interfaces

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 then the interfaces should be restarted. After checking the third-party interfaces, then check cron to see if any third-party interfaces were scheduled to start during the installation process while the system was stopped. These scheduled interfaces should now be started. For example, if the IPG collector was scheduled to start during the installation, then you would need to start that process at this point in the process.

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

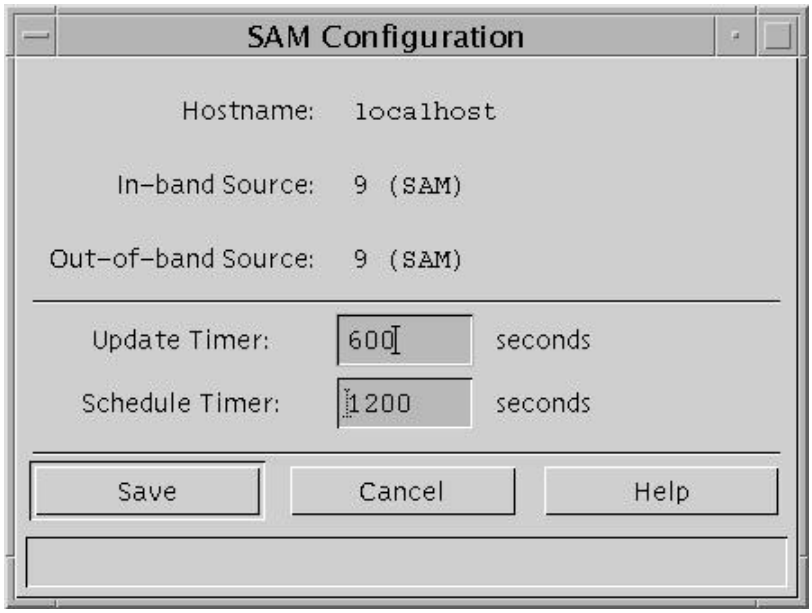
Follow these instructions to set the Update Timer and Schedule Timer fields on the SAM Configuration window.

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

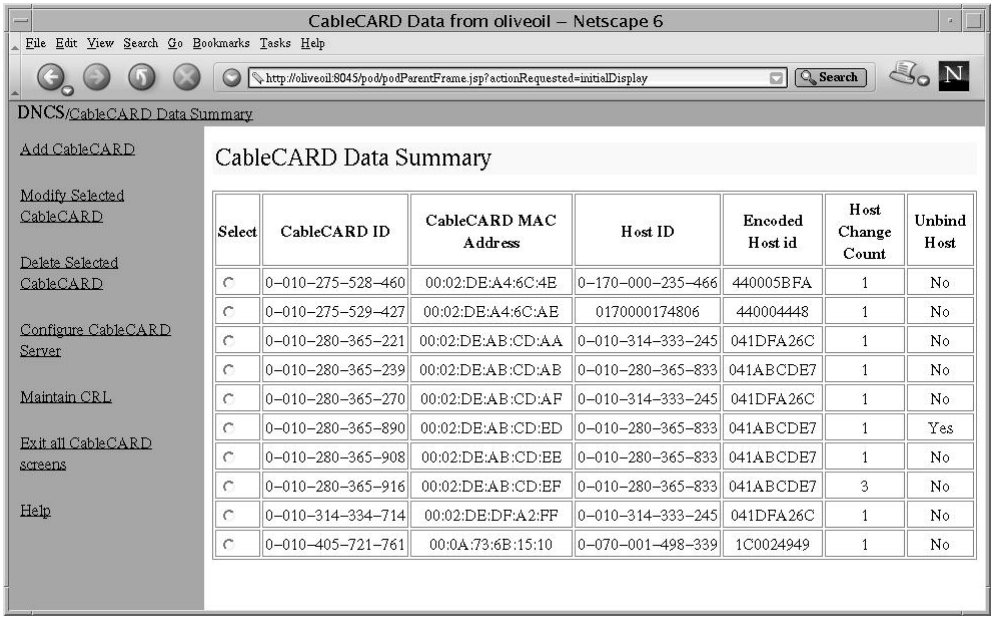
Introduction

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 at 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

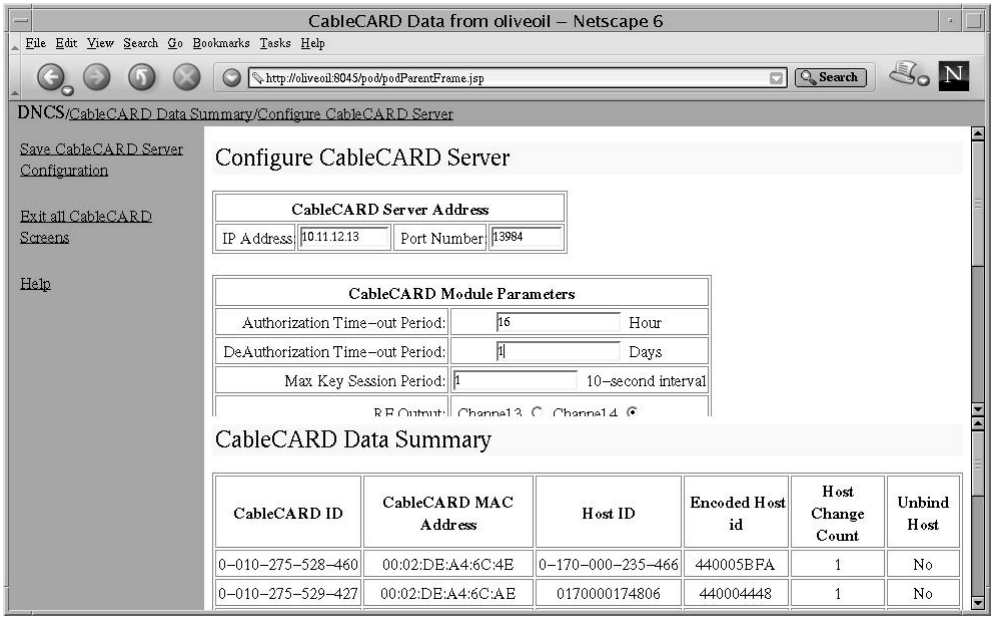
Follow these instructions to configure the minimum Set Authorization Time-out Period and Set DeAuthorization Time-out Period fields on the Configure CableCARD Server window.

1. From the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Element Provisioning** tab and then click **CableCARD**. The CableCARD Data Summary screen opens.



Select	CableCARD ID	CableCARD MAC Address	Host ID	Encoded Host id	Host Change Count	Unbind Host
○	0–010–275–528–460	00:02:DE:A4:6C:4E	0–170–000–235–466	440005BFA	1	No
○	0–010–275–529–427	00:02:DE:A4:6C:AE	0170000174806	440004448	1	No
○	0–010–280–365–221	00:02:DE:AB:CD:AA	0–010–314–333–245	041DFA26C	1	No
○	0–010–280–365–239	00:02:DE:AB:CD:AB	0–010–280–365–833	041ABCDE7	1	No
○	0–010–280–365–270	00:02:DE:AB:CD:AF	0–010–314–333–245	041DFA26C	1	No
○	0–010–280–365–890	00:02:DE:AB:CD:ED	0–010–280–365–833	041ABCDE7	1	Yes
○	0–010–280–365–908	00:02:DE:AB:CD:EE	0–010–280–365–833	041ABCDE7	1	No
○	0–010–280–365–916	00:02:DE:AB:CD:EF	0–010–280–365–833	041ABCDE7	3	No
○	0–010–314–334–714	00:02:DE:DF:A2:FF	0–010–314–333–245	041DFA26C	1	No
○	0–010–405–721–761	00:0A:73:6B:15:10	0–070–001–498–339	1C0024949	1	No

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 **Set Authorization Time-out Period** field, type **16**.

   b In the **Set DeAuthorization Time-out Period** field, type **1**.

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*. 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 have obtained 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 is done both before and after the installation process is complete to provide a comparison of the number of sessions. This comparison indicates a successful upgrade by ensuring the correct number of sessions were built after the upgrade process is complete.

Verifying the Number of Recovered BFS Sessions

Follow these steps to check the number of post-upgrade BFS sessions.

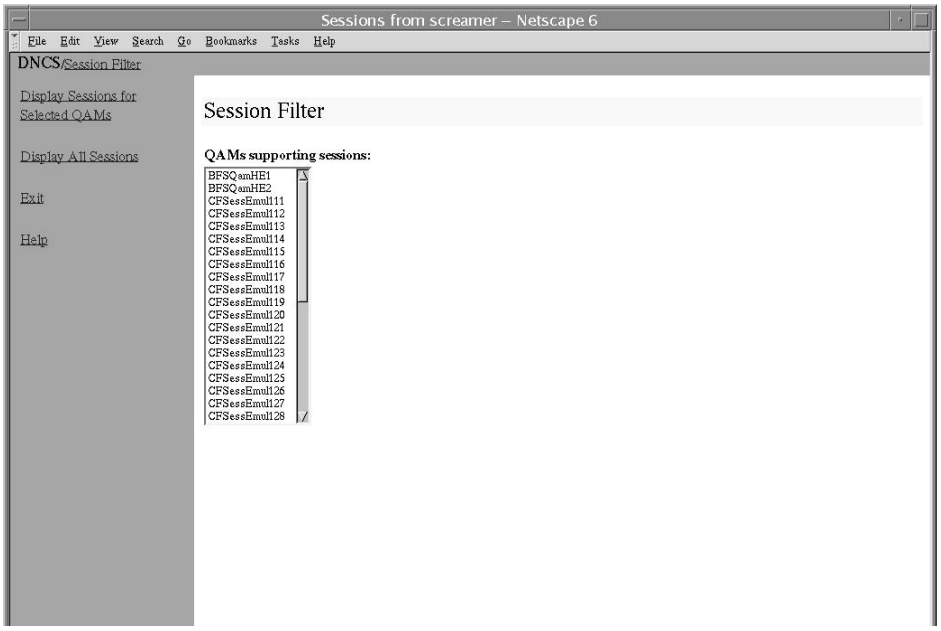
1. Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.
2. Does the **Session Count** total equal the number of sessions you recorded in the ***Checking the BFS Sessions on the BFS QAM*** (on page 26) procedure?
   - If **yes**, skip the remainder of this section, and go to ***Authorize the BRF as a BFS Server (Optional)*** (on page 71). The system recovered all of the BFS sessions.
   - If **no**, ***Tear Down BFS and OSM Sessions*** (on page 68).

Tear Down BFS and OSM Sessions

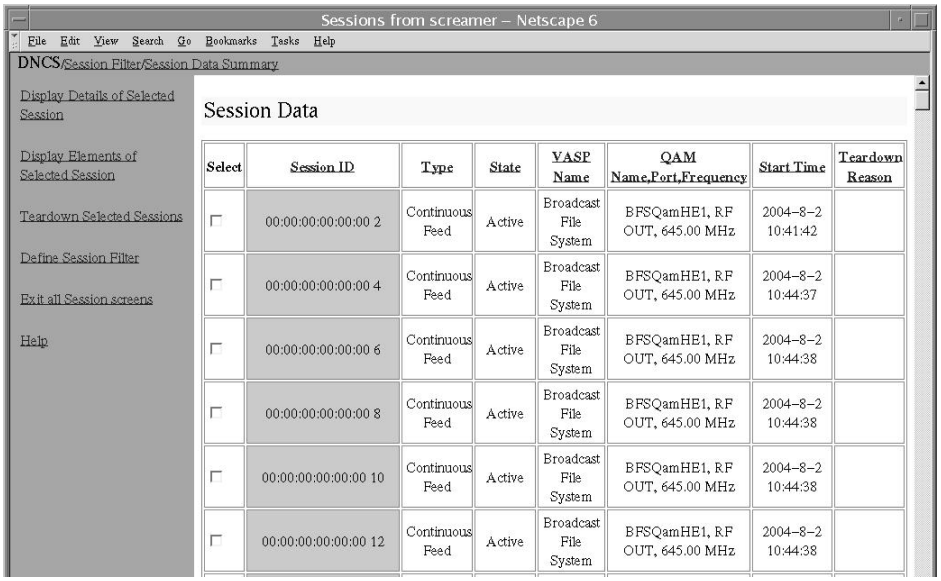
Complete these steps to tear down the BFS and OSM sessions in order to return the BFS session count to the expected number of sessions.

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 List and then click **Display Sessions** for the sessions associated with the BFS QAMs.



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 ***Check and Remove Sessions*** (on page 26) procedure?

- If **yes**, go to ***Authorize the BRF as a BFS Server (Optional)*** (on page 71). The system recovered all of the BFS sessions.
- 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.

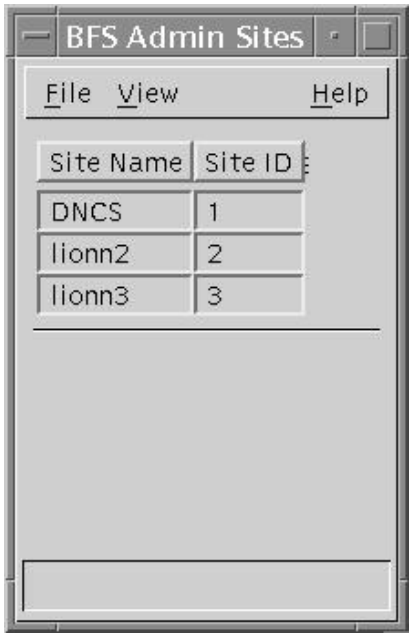
Authorizing the BRF

Follow these instructions 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)?

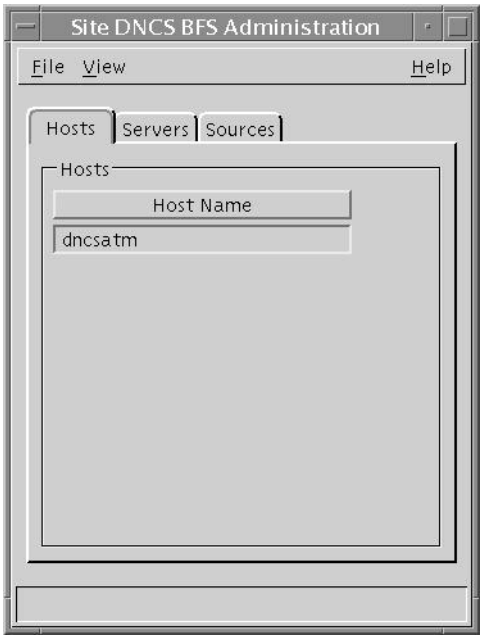
a If **yes**, click **BFS Admin**. The BFS Admin Sites window opens.



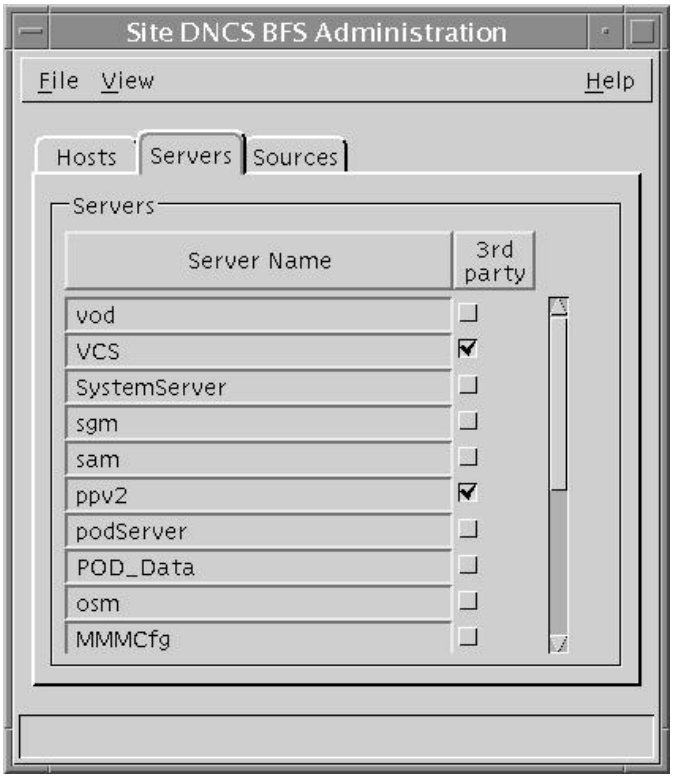
b If **no**, go to step 3.

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?

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

- If **yes**, click **File** and then select **Close** to close the Site DNCS BFS Administration window. You have completed this procedure; go to ***System Validation Tests (Before Modulator Reset)*** (on page 74).

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

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

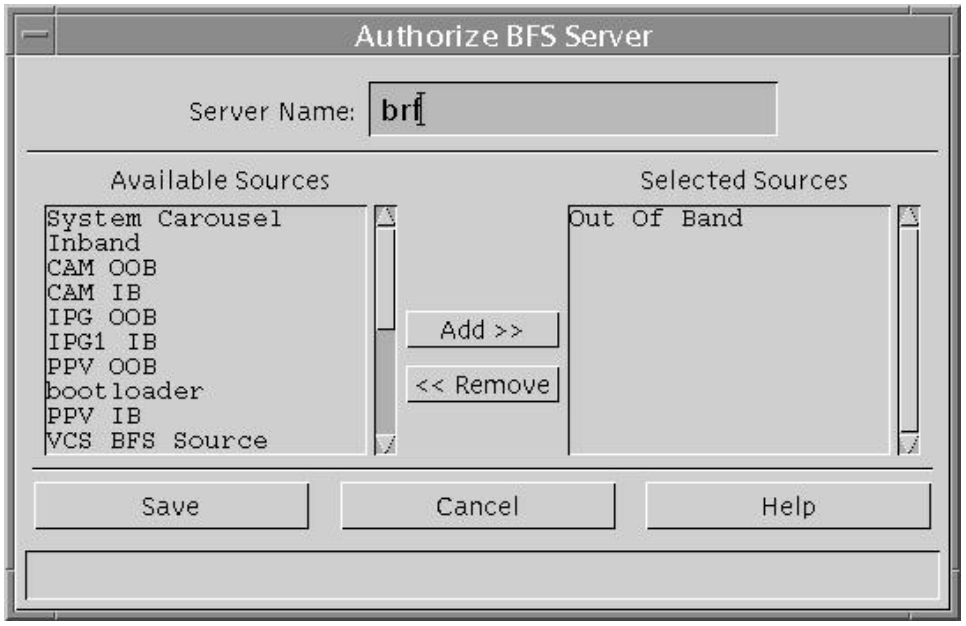
6 Click **File** and then select **New**. The Authorize BFS Server window appears.

7 Follow these instructions 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 ***System Validation Tests (Before Modulator Reset)*** (on page 74).

System Validation Tests (Before Modulator Reset)

Verifying a Successful Installation of SR 4.0 SP2

Follow these instructions to verify a successful installation of this software. The DHCTs that you use for these tests should comply with the following specifications:

- Unauthorized to view a PPV event without specifically buying the PPV event
- Capable of booting into two-way mode
- Authorized for all third-party applications

Important! Note the following important points about these tests:

- These tests apply only to systems running SARA. Check with Aptiv for equivalent tests if your system supports the Passport application.
- If any of these tests are unsuccessful, contact Cisco Services before rolling back from this upgrade.

1 Complete these 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 8.
- 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 video-on-demand 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.

Reset the Modulators

Resetting the Modulators

Introduction

The upgrade to SR 4.0 SP2 updates your QAM, MQAM, GQAM, and GoQAM modulator code. After the upgrade, you need to reset the modulators in order for the modulators to operate with the new code.

Note: Depending upon your upgrade scenario, you may not have to complete this procedure. If your upgrade did not modify QAM, MQAM, GQAM, or GoQAM modulator code, you can skip this procedure.

You have the following methods available when you reset modulators:

- You can use the traditional method of resetting modulators through the DNCS GUI.
- You can reset the modulators (except the QAM modulator) through the front panel of the modulators. The QAM modulator resets through the power switch on the back panel.
- You can use the auditQam utility to reset the modulators through the command line of the DNCS.

Important Notice Regarding the Reset of Modulators

On occasion, for testing purposes, default configuration files for headend components are changed. For example, a site might substitute a file called mqam250.config, instead of mqam.config, for the MQAM configuration file. If the site you have upgraded uses a custom configuration file, and if you are now ready to use the default configuration file again, you need to update the configuration file settings for your headend equipment.

The following list includes the default configuration files for the QAM-family of devices:

- CAQAM-/tftpboot/qam.config
- GQAM-/tftpboot/gqam.config
- GOQAM-/tftpboot/goqam.config
- MQAM-/tftpboot/mqam.config

Important! Failure to update the configuration file(s) will result in the device remaining in the uniquely specified configuration. The device will not load new code. Instead, it will continue to load the code specified in the custom configuration file.

If the headend device fails to load the code you intended it to receive, check to see if either a unique file was specified in the DNCS GUI or in the /etc/bootptab file before contacting Cisco Services for assistance.

Which Reset Method to Use

Resetting modulators from the DNCS GUI or the front panel can be time-consuming. If you have many modulators to reset, consider using the new auditQam utility. The auditQam utility takes, as an argument, the IP address of the modulator that you want to reset. While the auditQam utility script runs, engineers are free to complete other upgrade-related tasks.

Notes:

- Instructions for resetting modulators through the DNCS GUI are found in ***Resetting Modulators Through the DNCS GUI*** (on page 77).
- Instructions for resetting modulators through the front panel are found in ***Resetting Modulators Through the Modulator Panel*** (see "Resetting the Modulators Through the Modulator Panel" on page 79).
- Instructions for resetting modulators through the auditQam utility are found in ***Resetting Modulators Through the auditQam Utility*** (on page 80).

Resetting Modulators Through the DNCS GUI

When you reset the modulators, the modulators download their new SR 4.0 code. Follow these instructions to reset the modulators through the DNCS GUI.

Important! Never reset more than four modulators at once or the DNCS may become overloaded. The following instructions alert you to this important point at the appropriate step.

1 Follow these instructions to record the Session Count, the Program Count, and the IP address of your modulators.

Note: Skip this step for any modulator that is used for video-on-demand (VOD).

a Press the **Options** button on the front panel until the **Session Count** total appears.

b Record the Session Count on a piece of paper.

c Press the **Options** button on the front panel until the **Program Count** total appears.

d Record the Program Count on a piece of paper.

e Press the **Options** button on the front panel until the **IP address** appears.

f Record the IP address on a piece of paper.

g Repeat steps a) through f) for all of your QAM and MQAM modulators.

2 Open an xterm window on the DNCS.

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

4 Click **QAM**. The QAM List window appears.

5 From the QAM List window, highlight a modulator.

Notes:

- Refer to the QAM Type column to differentiate between types of modulators.
- Each MQAM, GQAM, and/or GoQAM modulator appears multiple times on the QAM List window; highlight only the first occurrence.

6 Click **File** and then select **Reset**. A confirmation message appears.

7 Click **Yes** on the confirmation message. The modulator resets.

8 Repeat steps 5 through 7 for up to three additional modulators, and then go to step 9.

Important! Never reset more than four modulators at once, or you may overload the DNCS.

Note: In step 10, you will have the opportunity to reset additional modulators.

9 Wait a few minutes and then type **ping [IP address]** and press **Enter** to ping each modulator you just reset. The ping command displays a message similar to Device is alive when the modulator has been reset.

Example: ping 172.16.4.4

Note: It may take up to 5 minutes for each modulator to reset.

10 Do you have additional modulators to reset?

- If **yes**, repeat steps 5 through 9 as many times as necessary until all of your modulators have been reset, and then go to step 11.
- If **no**, go to step 11.

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

12 Did you record the Program Count and the Session Count for each modulator not used for VOD, as specified in step 1?

- If **yes**, repeat step 1 to verify that the Program Count and Session Count totals match what you recorded before resetting the modulators, and then go to ***Final System Validation Tests*** (on page 82).

  Important! If the Program Count and Session Count totals do not match what you recorded prior to resetting the modulators, call Cisco Services.

- If **no**, go to ***Final System Validation Tests*** (on page 82).

Resetting the Modulators Through the Modulator Panel

When you reset the modulators, the modulators download their new code. Follow these instructions to reset the modulators through the modulator panel.

1 Follow these instructions to record the Session Count, the Program Count, and the IP address of your modulators.

Note: Skip this step for any modulator that is used for video-on-demand (VOD).

a Press the **Options** button on the front panel until the **Session Count** total appears.

b Record the Session Count on a piece of paper.

c Press the **Options** button on the front panel until the **Program Count** total appears.

d Record the Program Count on a piece of paper.

e Press the **Options** button on the front panel until the **IP address** appears.

f Record the IP address on a piece of paper.

g Repeat steps a) through f) for all of your QAM and MQAM modulators.

2 Choose one of the following options:

- To reset an MQAM, GQAM, or GoQAM modulator, go to step 3.
- To reset a QAM modulator, go to step 4.

3 To reset an MQAM, GQAM, or GoQAM modulator, follow these instructions.

a Press the **Options** button on the front panel until the **Reset** option appears.

b Follow the instructions that appear alongside the Reset option.

c Go to step 5.

4 To reset a QAM modulator, turn off the power switch on the back of the QAM modulator, wait a few seconds, and then turn it back on.

5 Repeat steps 3 and 4 for up to three additional modulators, and then go to step 6.

Important! Never reset more than four modulators at once, or you may overload the DNCS.

Note: In step 7, you will have the opportunity to reset additional modulators.

6 Wait a few minutes and then from an xterm window on the DNCS, type **ping [IP address]** and press **Enter** to ping each modulator you just reset. The ping command displays a message similar to Device is alive when the modulator has been reset.

Example: ping 172.16.4.4

Note: It may take up to 5 minutes for each modulator to reset.

7 Do you have additional modulators to reset?

- If **yes**, repeat steps 3 through 6 as many times as necessary until all of your modulators have been reset, and then go to step 8.
- If **no**, go to step 8.

8 Did you record the Program Count and the Session Count for each modulator not used for VOD, as specified in step 1?

- If **yes**, repeat step 1 to verify that the Program Count and Session Count totals match what you recorded before resetting the modulators, and then go to ***Final System Validation Tests*** (on page 82).

  Important! If the Program Count and Session Count totals do not match what you recorded prior to resetting the modulators, call Cisco Services.

- If **no**, go to ***Final System Validation Tests*** (on page 82).

Resetting Modulators Through the auditQam Utility

The *reset* option of the auditQam utility allows upgrade engineers to reset a modulator from the command line of the DNCS, a process that is usually quicker than resetting the modulator through the DNCS GUI or modulator panel. If you have only a few modulators to reset, you can just type the IP address of the modulator as an argument to the **auditQam -reset** command. If you have many modulators to reset, consider creating a script. Instructions and guidelines for both situations follow.

Resetting a Few Modulators

If you want to reset only a few modulators, complete this procedure for each modulator.

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

2 Type the following command and press **Enter**. The system shuts down and reinitializes the modulator.

auditQam -reset [qam ip address or mqam ip address]

Note: The system also performs an audit to ensure that the session list for the modulator matches the session list from the DNCS.

Resetting Many QAM and MQAM Modulators

Upgrade engineers frequently do not have time to manually reset hundreds of modulators from the DNCS GUI. To save time, engineers can create a script that runs automatically. Refer to the following example for a sample script.

```
auditQam  -reset  123.123.123.123
sleep 1
auditQam  -reset  123.123.123.124
sleep 1
auditQam -reset  123.123.123.125
sleep 1
auditQam  -reset  123.123.123.126
sleep 1
```

Resetting a QAM interrupts all active sessions on the QAM for up to 10 minutes. Complete this task during a maintenance period whenever possible.

Final System Validation Tests

Verifying a Successful Installation of SR 4.0 SP2

Follow these instructions to verify a successful installation of this software. The DHCTs that you use for these tests should comply with the following specifications:

- Unauthorized to view a PPV event without specifically buying the PPV event
- Capable of booting into two-way mode
- Authorized for all third-party applications

Important! Note the following important points about these tests:

- These tests apply only to systems running SARA. Check with Aptiv for equivalent tests if your system supports the Passport application.
- If any of these tests are unsuccessful, contact Cisco Services before rolling back from this upgrade.

1 Complete these 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 8.
- 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 video-on-demand 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.

Reinstall the NMI Software

Reinstalling the NMI Software

If you removed the NMI software as part of this upgrade, you need to reinstall the NMI software now. Follow these instructions 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 section, and go to the next 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* 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. If you have upgraded an Enterprise 250 DNCS, you can skip this procedure.

Additionally, 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

Use this procedure to reattach the disk mirrors of the DNCS.

1. Insert the CD labeled **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 message **Are you sure that you want to proceed?**
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.

   $ metastat -p

   d500 -m d700 d400 1

   d700 1 1 c2t0d0s0 -h hsp120

   d400 1 1 c0t0d0s0 -h hsp120

   d501 -m d701 d401 1

   d701 1 1 c2t0d0s1 -h hsp121

   d401 1 1 c0t0d0s1 -h hsp121

   d503 -m d703 d403 1

   d703 1 1 c2t0d0s3 -h hsp123

```
d403 1 1 c0t0d0s3 -h hsp123
d506 -m d706 d406 1
d706 1 1 c2t0d0s6 -h hsp126
d406 1 1 c0t0d0s6 -h hsp126
d507 -m d707 d407 1
d707 1 1 c2t0d0s7 -h hsp127
d407 1 1 c0t0d0s7 -h hsp127
d510 -m d710 d410 1
d710 1 1 c2t1d0s0 -h hsp220
d410 1 1 c0t1d0s0 -h hsp220
d513 -m d713 d413 1
d713 1 1 c2t1d0s3 -h hsp223
d413 1 1 c0t1d0s3 -h hsp223
d514 -m d714 d414 1
d714 1 1 c2t1d0s4 -h hsp224
d414 1 1 c0t1d0s4 -h hsp224
d515 -m d715 d415 1
d715 1 1 c2t1d0s5 -h hsp225
d415 1 1 c0t1d0s5 -h hsp225
d516 -m d716 d416 1
d716 1 1 c2t1d0s6 -h hsp226
d416 1 1 c0t1d0s6 -h hsp226
d517 -m d717 d417 1
d717 1 1 c2t1d0s7 -h hsp227
d417 1 1 c0t1d0s7 -h hsp227
hsp120 c4t0d0s0
hsp121 c4t0d0s1
hsp123 c4t0d0s3
hsp124 c4t0d0s4
hsp126 c4t0d0s6
hsp127 c4t0d0s7
hsp220 c4t1d0s0
hsp221 c4t1d0s1
hsp223 c4t1d0s3
hsp224 c4t1d0s4
hsp225 c4t1d0s5
hsp226 c4t1d0s6
```

hsp227 c4t1d0s7

7 Are the following two conditions true?

- The designation **ok** appears in the **State** column next to each metadevice.
- No **Hot Spare** indicates **In Use**.
  - If **yes** (to both conditions), the upgrade is complete.
  - If **no** (to either or both conditions), call Cisco Services for help in resolving these issues with the metadevices.

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 two procedures for rolling back the DNCS, based on the type of DNCS that is located at the site. Cisco field service engineers, who encounter problems while upgrading an existing digital system to this system release, should select the appropriate procedure:

- **Roll Back the Enterprise 450 or Sun Fire V880 DNCS**
- **Roll Back the Enterprise 250 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 35), use these procedures, if necessary.
   - **a** ***Stopping Spectrum*** (on page 35)
   - **b** ***Stopping the Application Server*** (on page 36)
   - **c** ***Stopping the DNCS*** (on page 37)

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 4.0.0.27x?

- 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 57).

Roll Back the Enterprise 250 DNCS

Introduction

Use the procedures in this section to roll back the Enterprise 250 DNCS from an unsuccessful upgrade to your previous DNCS release.

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.

Rolling Back the Enterprise 250 DNCS

Follow these instructions to prepare to restore the file system of the Enterprise 250 DNCS.

1. If necessary, open an xterm window on the DNCS.
2. Type **su -** and then press **Enter** to log in as root user. The password prompt appears.
3. Type the root password and then press **Enter**.
4. Insert the CD labeled **DBDS Maintenance CD** into the CD drive of the DNCS.
5. In ***Stop System Components*** (on page 35), use these procedures, if necessary.
   a. ***Stopping Spectrum*** (on page 35)
   b. ***Stopping the Application Server*** (on page 36)
   c. ***Stopping the DNCS*** (on page 37)
6. 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.
7. Type **shutdown -g0 -y -i0** and then press **Enter**. The system halts all processes on the DNCS and an **ok** prompt appears.
8. At the **ok** prompt, type **boot cdrom - SAshell** and then press **Enter**.

   Results:

   - The DNCS boots from the CD.
   - An xterm window opens.
9. Insert your most recent DNCS file system backup tape into the tape drive of the DNCS.
10. Go to ***Restoring the DNCS File System*** (on page 96).

Restoring the DNCS File System

Follow these instructions to restore the file system of the Enterprise 250 DNCS.

1. Type **/tmp/cdrom/backup_restore/restoreFileSystems** and then press **Enter**. The system restores the DNCS or Application Server file system and displays a message when the restoration is complete.
2. When the restoration is complete, remove the tape and store it in a safe place.
3. Type **/usr/sbin/shutdown -y -i0 -i6** and then press **Enter**. The DNCS reboots and the Common Desktop Environment (CDE) login window appears.
4. Log on to the DNCS as **dncs** user.
5. At the **ok** prompt on the Application Server, type **boot** and then press **Enter**. The Application Server reboots.
6. Log on to the Application Server as **dncs** user.
7. Follow the procedures in the ***Restart the System Components*** (on page 57).

Reinstall the NMI Software

Reinstalling the NMI Software

If you removed the NMI software as part of this upgrade, you need to reinstall the NMI software now. Follow these instructions 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 section, and go to the next 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* 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

Determining 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.

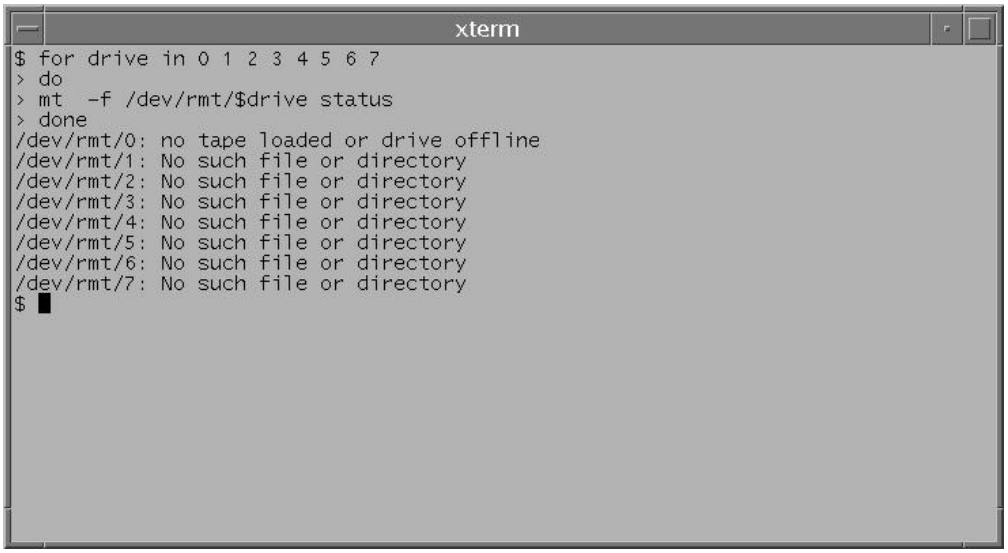
2 Ensure that no tape is currently in your tape drive.

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, Cisco has 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

Checking for the Existence of the ASI Package on the DNCS

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 106).
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 106).

Enable the ASI Feature

Enabling 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

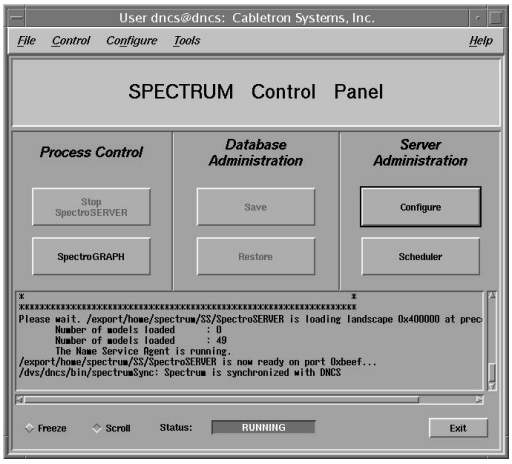
Introduction

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

Stopping Spectrum

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

2 From the Select Host to run on window, click **OK**. The Spectrum Control Panel appears.



3 Click **Stop SpectroSERVER**. A confirmation message appears.

4 Click **OK** at the confirmation message. The Status message on the Spectrum Control Panel shows **Inactive.**

5 Click **Exit** on the Spectrum Control Panel. A confirmation message appears.

6 Click **OK** at the confirmation message. The Spectrum Control Panel closes.

Stopping the Application Server

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

- For sites that support the Cisco 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 Cisco 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 Cisco Application Server

After stopping the Cisco 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 37).

Stopping the DNCS

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

2 From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The Dncs Control window appears.

3 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.

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

Install the ASI Card

Installing 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 250 DNCS, Slot 2
   - 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**
  - ***Install the ASI Package*** (on page 112)
- If **no**, go to ***Install the ASI Package*** (on page 112).

Install the ASI Package

Installing 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 113).

Configure the ASI Card

Configuring 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 114).

Check the Status of the ASI Card

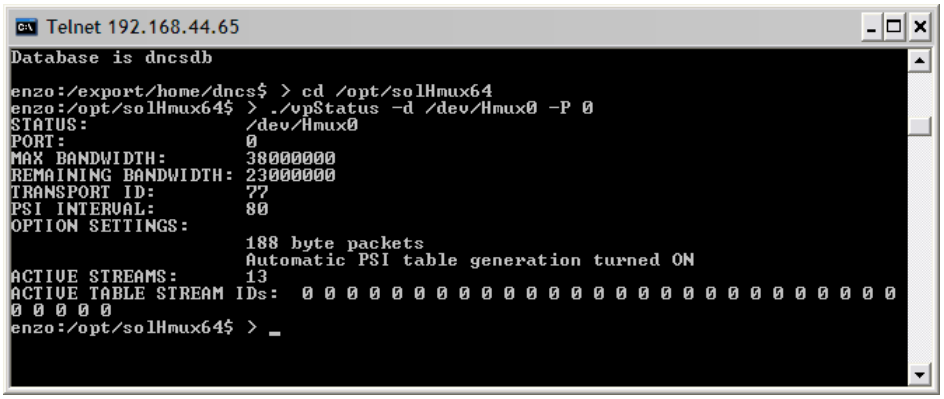
Checking the Status of the Direct ASI Card

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 115).
- If **no**, call Cisco Services for assistance.

Restart System Components

Introduction

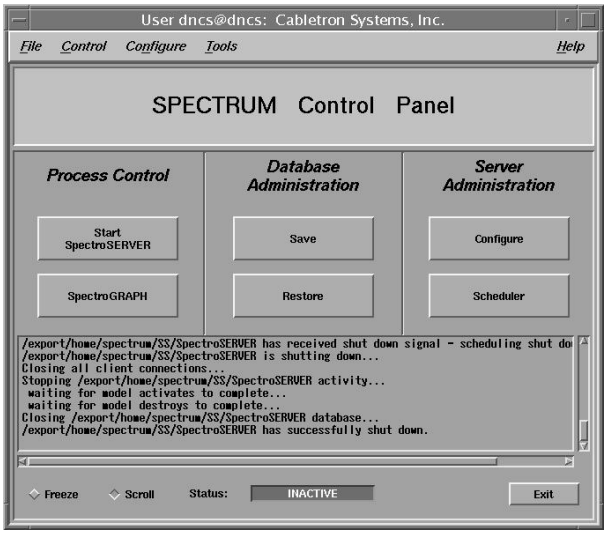
Use the procedures in this section to restart Spectrum, the DNCS, and the Application Server.

Restarting Spectrum

Important! Skip this procedure if you are using DBDS Alarm Manager 1.0 instead of Spectrum.

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

2 Select the Host Machine (usually DEFAULT), and then click **OK**. The Spectrum Control Panel window opens.



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

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

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

Restarting the DNCS

1. 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 Monitor**.

   Results:

   - The DNCS Monitor window opens.
   - Green indicators begin to replace red indicators on the DNCS Monitor window.
4. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The Dncs Control 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 Monitor will 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 an Aptiv Application Server. Choose the procedure that pertains to your system

Restarting the Application Server for SARA Systems

Complete the following steps to check if the Cisco 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 **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.
4. Does the word **running** appear next to the current state field (**Curr Stt**) of each process?
   - If **yes**, you have completed this procedure.
   - If **no**, go to step 5.
5. Press the middle mouse button, and then select **App Serv Start**.
6. When the Application Control window indicates that the current state (**Curr Stt**) of each process is running, go to step 7.

   Note: On some systems, the VOD Server process may remain at **Stopped**; this is normal.
7. Follow the on-screen instructions to close the Applications Control window.

Restarting the Application Server for Aptiv Systems

Complete the following steps to check if the Pioneer 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 Pioneer drivers.

Record Configuration Data

Recording Configuration Details

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.

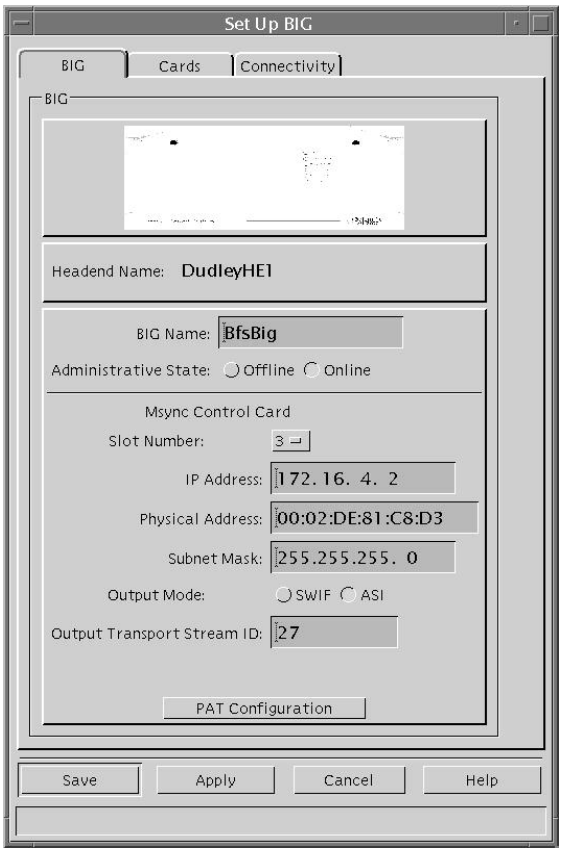
1 From the DNCS Administrative Console, select the **Element Provisioning** tab.

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**.

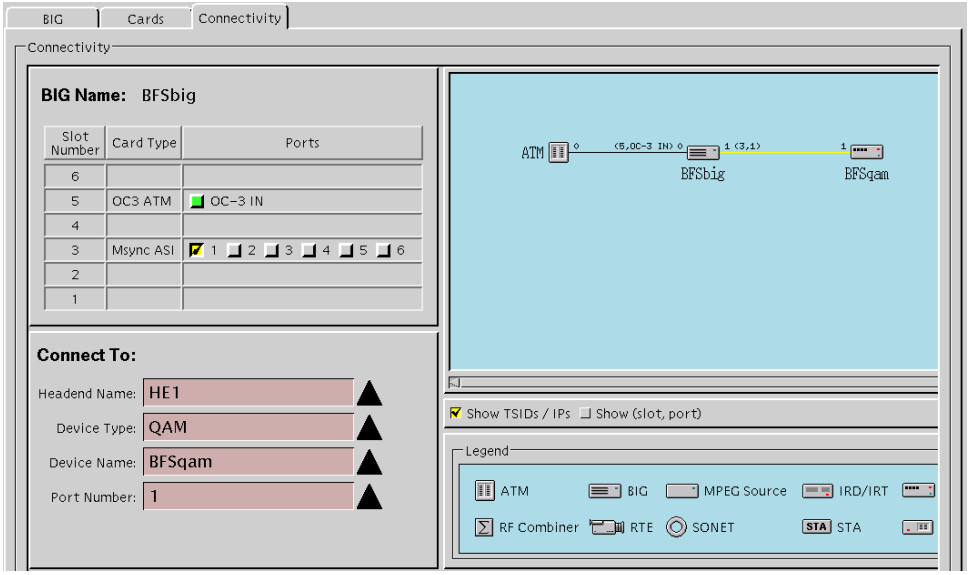
Note: In this example, the Output Transport Stream ID value is 27.



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: _____

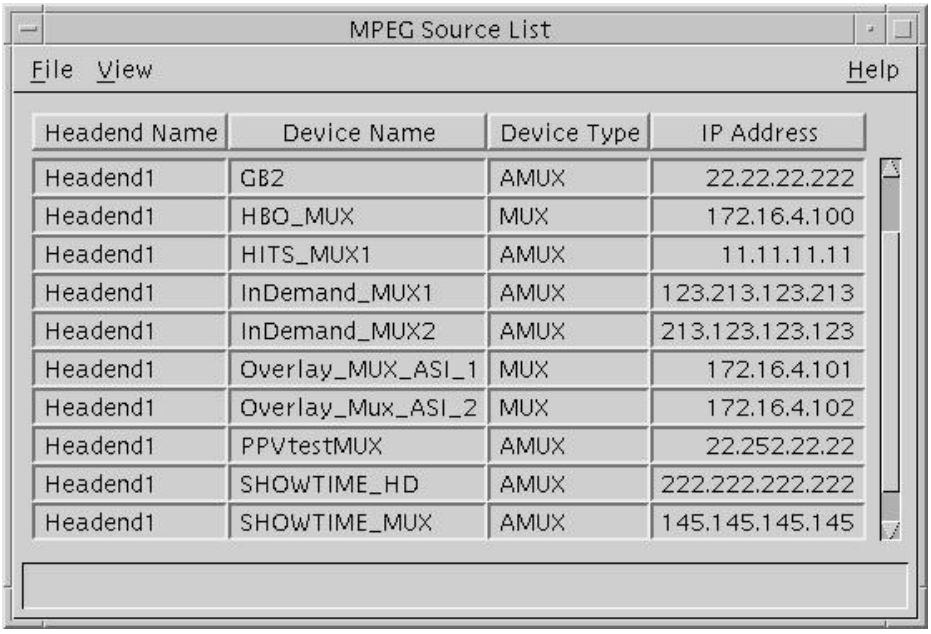
10 Click **Cancel** to close the window.

Create an MPEG Source

Creating 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.

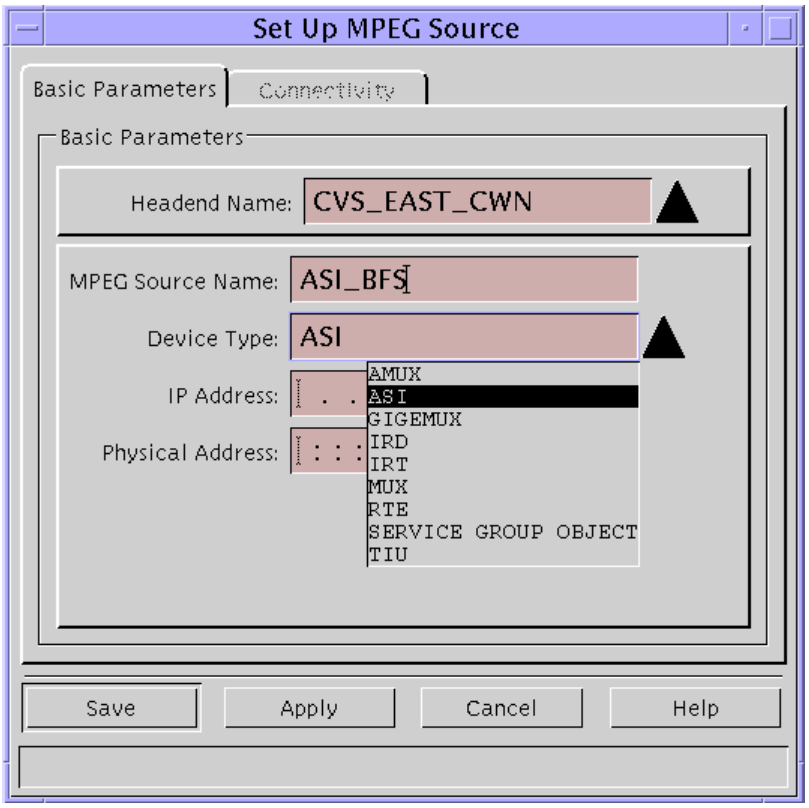
b Type ASI_BFS in the MPEG Source Name field.

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.

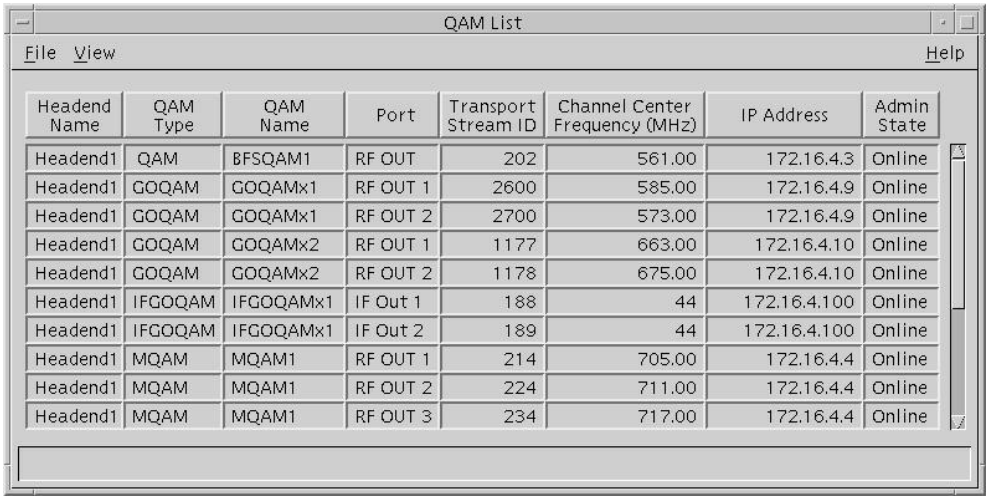
8 Go to ***Set Up the QAM*** (on page 125).

Set Up the QAM

Setting Up the QAM

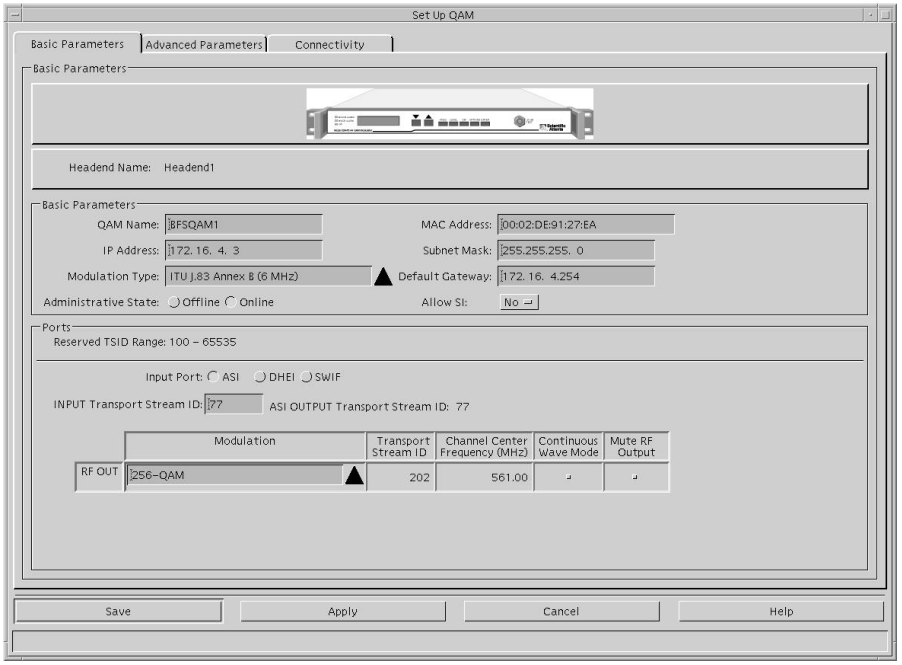
After creating the MPEG source, follow these instructions to set up the QAM.

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



Headend Name	QAM Type	QAM Name	Port	Transport Stream ID	Channel Center Frequency (MHz)	IP Address	Admin State
Headend1	QAM	BFSQAM1	RF OUT	202	561.00	172.16.4.3	Online
Headend1	GQQAM	GQQAMx1	RF OUT 1	2600	585.00	172.16.4.9	Online
Headend1	GQQAM	GQQAMx1	RF OUT 2	2700	573.00	172.16.4.9	Online
Headend1	GQQAM	GQQAMx2	RF OUT 1	1177	663.00	172.16.4.10	Online
Headend1	GQQAM	GQQAMx2	RF OUT 2	1178	675.00	172.16.4.10	Online
Headend1	IFGQQAM	IFGQQAMx1	IF Out 1	188	44	172.16.4.100	Online
Headend1	IFGQQAM	IFGQQAMx1	IF Out 2	189	44	172.16.4.100	Online
Headend1	MQAM	MQAM1	RF OUT 1	214	705.00	172.16.4.4	Online
Headend1	MQAM	MQAM1	RF OUT 2	224	711.00	172.16.4.4	Online
Headend1	MQAM	MQAM1	RF OUT 3	234	717.00	172.16.4.4	Online

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 122).

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 grayed out 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.

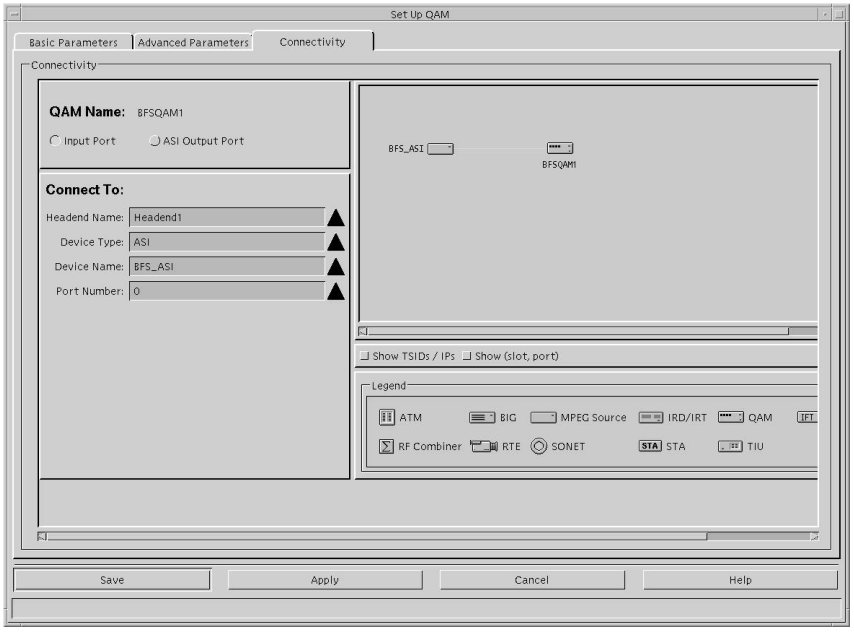
a Click the arrow to the right of the **Headend Name** field and choose the appropriate headend.

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.

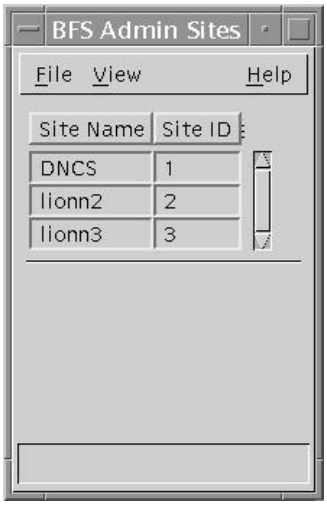
11 Go to ***Set Up the BFS Host*** (on page 128).

Set Up the BFS Host

Setting Up the BFS Host

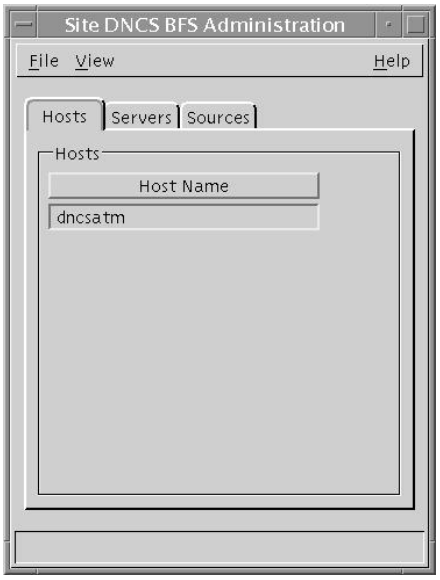
After setting up the QAM, follow these instructions to set up the BFS host.

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

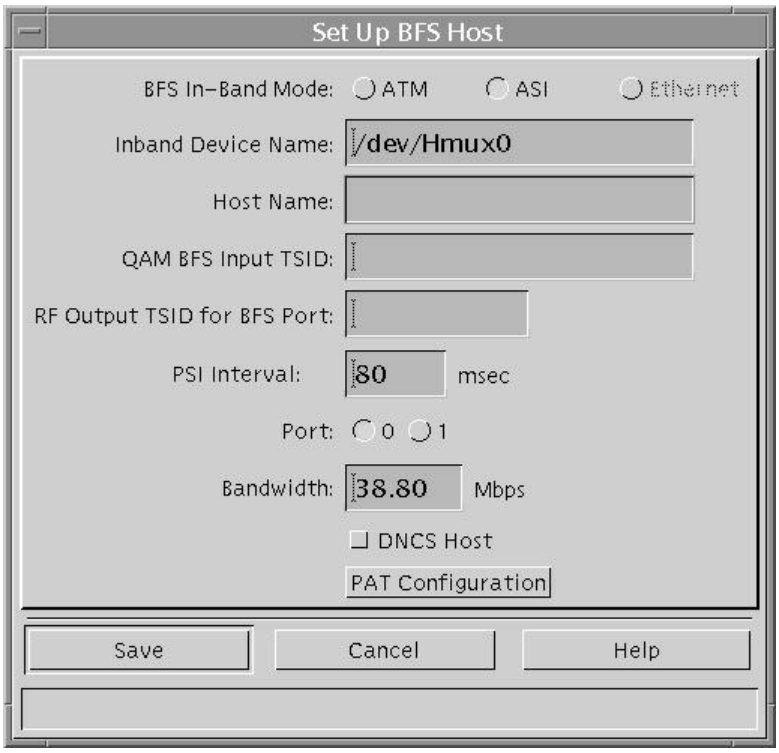


2 Double-click the site name of the system you are setting up. The Site [BFS site] BFS Administration window opens.

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 131).

Set the BIG Offline

Setting 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 132).

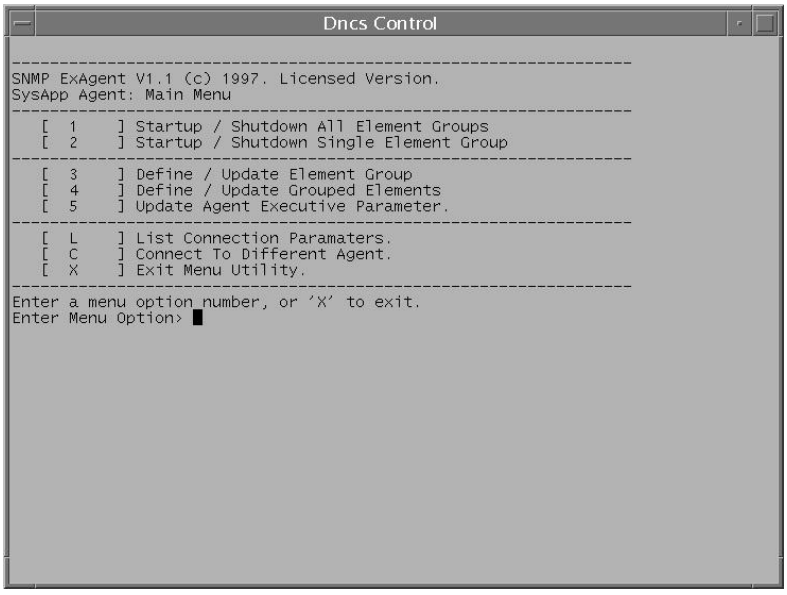
Stop the BFS and OSM Processes

Stopping the BFS and OSM Processes

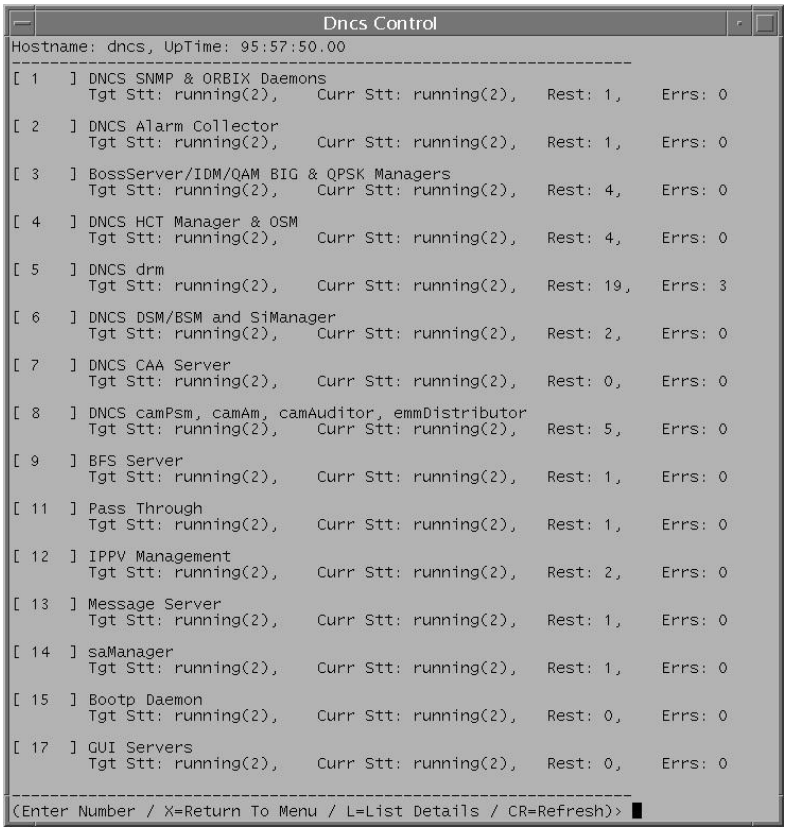
After setting the BIG offline, you need to stop the BFS and OSM processes on the DNCS next. Follow these instructions to stop the processes.

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 135).

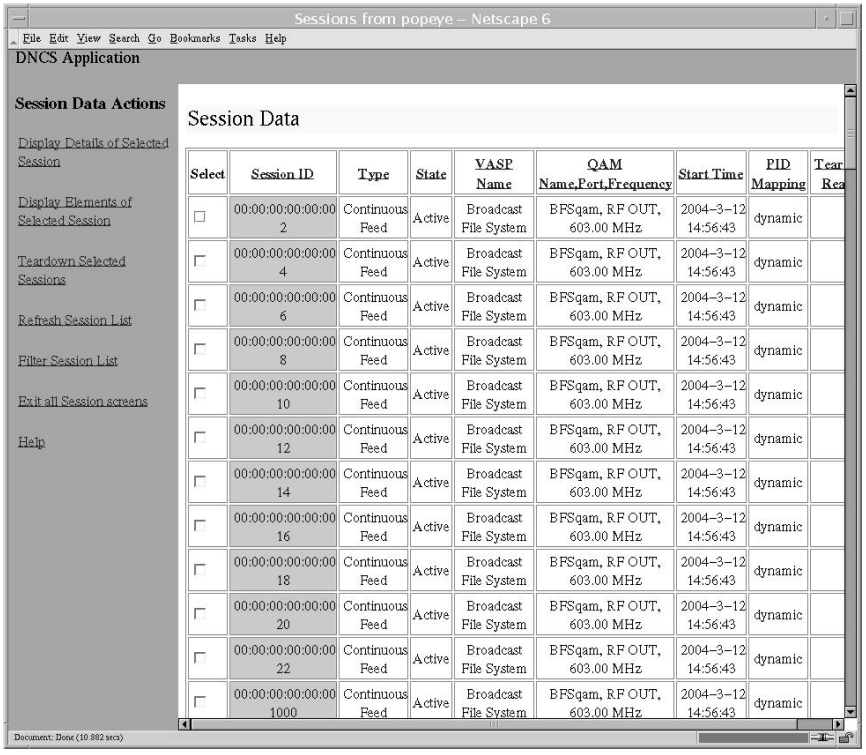
Tear Down BFS Sessions

Tearing 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

Clearing 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 138).
- 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

Restarting 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. Cisco assumes 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. Cisco assumes 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 21).

Verify DBDS Stability

Re-run the procedures in ***Verify DBDS Stability*** (on page 21).

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

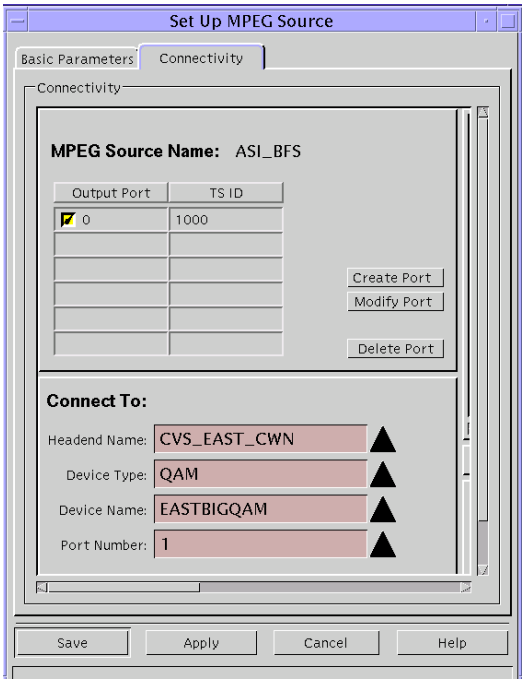
The first step in rolling back the Direct ASI installation requires that you record the current transport stream ID (TSID) values for the BFS MPEG source and the BFS QAM.

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.

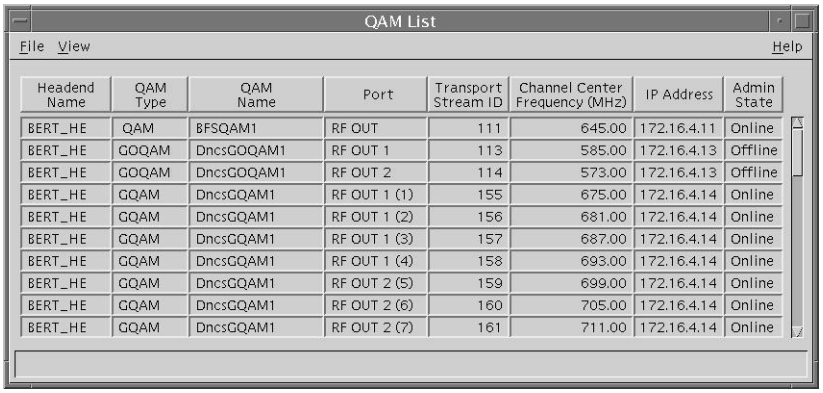


4. Record the value for **TS ID** here: _____
5. Click **Cancel** to close the Set Up MPEG Source window.
6. Click **File** and then select **Close** to close the MPEG Source List window.

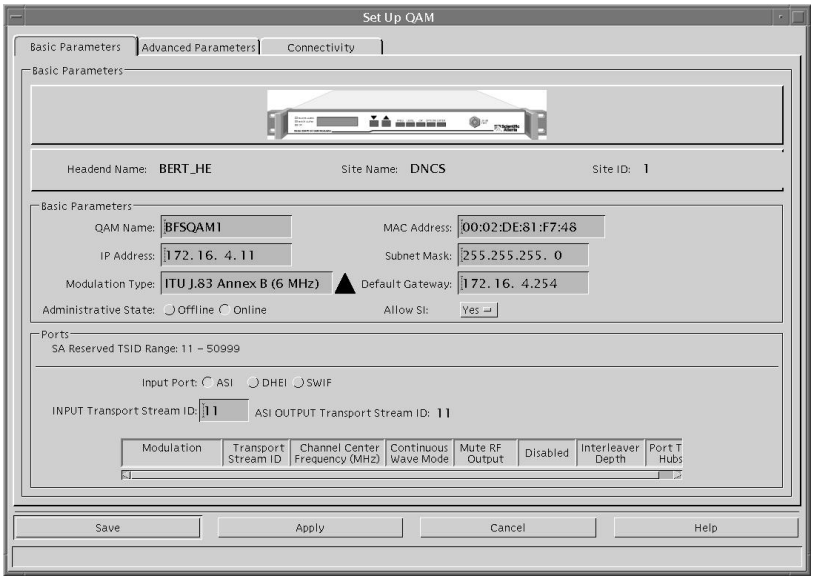
Recording the TSID Value for the BFS QAM

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 VDAT Light is Illuminated

Turn on the BIG and verify that the VDAT light illuminates.

Record Configuration Data

Recording Configuration Details

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 119) procedure when you configured your system for Direct ASI, complete that procedure now.

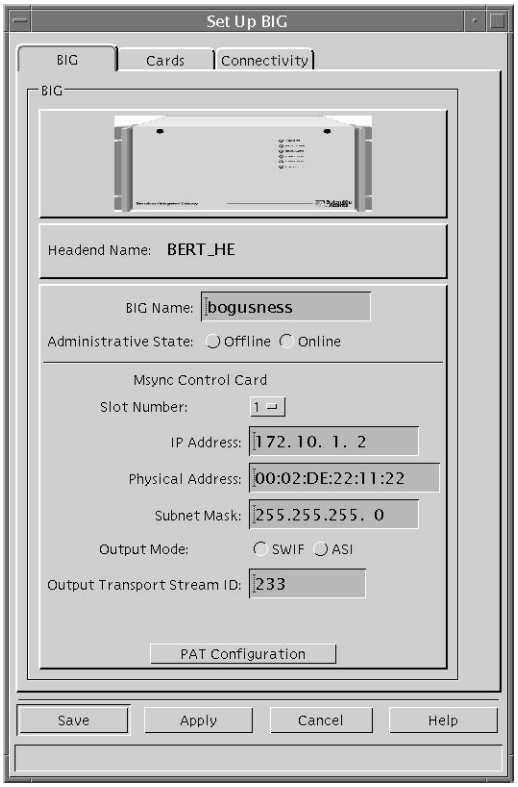
Set the BIG Online

Setting 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

Reconfiguring 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

Reconnecting 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

Configuring 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 153).
- 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

Configuring 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

Setting Up the 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

Stopping 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.

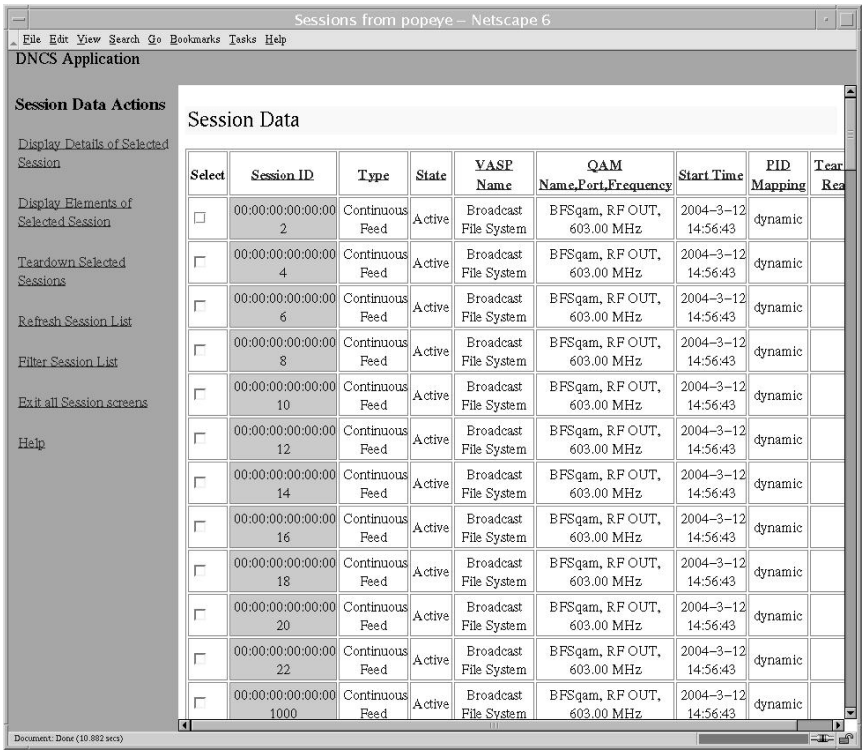
Tear Down BFS Sessions

Tearing 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

Clearing 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

Stopping 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

Restarting 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

Restarting 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.

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

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

June 2012 Printed in USA

Part Number 4013154 Rev C