System Release 2.8.1/3.8.1/4.3.1

CD Upgrade 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**.

DOCSIS is a registered trademark of Cable Television Laboratories, Inc.

CableCARD, M-Card, and OCAP are trademarks of Cable Television Laboratories, Inc.

Other third party trademarks mentioned are the property of their respective owners.

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

Publication Disclaimer

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

Copyright

© 2010, 2012 Cisco and/or its affiliates. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

About This Guide

Purpose

This guide provides step-by-step instructions for upgrading a Digital Broadband Delivery System (DBDS) to System Release (SR) 2.8.1/3.8.1/4.3.1. Sites that use this guide to upgrade must currently support SR 2.8/3.8/4.3 system software.

SR 2.8.1/3.8.1/4.3.1 Features CDs

This upgrade to SR 2.8.1/3.8.1/4.3.1 is accomplished through the following set of CDs:

- DNCS 4.3.1.6
- DNCS 4.3.1.6p2
- DNCS WUI/GUI 4.3.1.6
- DNCS Online Help 4.3.1.0
- Report Writer 1.0.0.3

How Long to Complete the Upgrade?

The upgrade to SR 2.8.1/3.8.1/4.3.1 is to be completed from within a maintenance window that usually begins at midnight. Upgrade engineers have determined that a typical site can be upgraded within one maintenance window. The maintenance window should begin when you stop system components in Chapter 2.

System Performance Impact

Interactive services will not be available during the maintenance window.

Audience

This guide is written for field service engineers and system operators who are responsible for upgrading an existing DBDS to SR 2.8.1/3.8.1/4.3.1.

Read the Entire Guide

Please review this entire guide before beginning the installation. If you are uncomfortable with any of the procedures, contact Cisco Services at 1-866-787-3866.

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

Required Skills and Expertise

System operators or engineers who upgrade ISDS software need the following skills:

- Advanced knowledge of UNIX
  - Experience with the UNIX vi editor. Several times throughout the system upgrade process system files are edited using the UNIX vi editor. The UNIX vi editor is not intuitive. The instructions provided in this guide are no substitute for an advanced working knowledge of vi.
  - The ability to review and edit cron files
- Extensive DBDS system expertise
  - The ability to identify keyfiles that are unique to the site being upgraded
  - The ability to add and remove user accounts

Requirements

Before beginning the upgrade to SR 2.8.1/3.8.1/4.3.1, be sure that the site you are upgrading meets these requirements:

- SR 2.8/3.8/4.3, or later is currently installed on your system.
- You have the CD labeled DBDS Maintenance CD 3.3.x in order to complete the required backups of the database and the filesystem.
- 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. This DVD will only be provided to customers that have an active RNCS system.
- Sites that are using the OCAP component of the DBDS need the DVD labeled similarly to OCAP Install DVD

  Note: Note that this is a DVD and not a CD. This DVD will only be provided to customers that have an active OCAP system.

- The system must support one of the following combinations of the SA Resident Application (SARA) and PowerTV® operating system code, or higher:
  - SARA 1.54 and OS 3.10
  - SARA 1.43.5a3 and OS 3.3.4.1008
- The latest version of DBDS Utilities is installed on your system.

Non-Cisco Application Server and/or Third-Party Application

If the site you are upgrading supports a non-Cisco Application Server, contact the vendor of that Application Server in order to obtain upgrade requirements, as well as upgrade and rollback procedures.

If the site you are upgrading runs a third-party software application, contact the supplier of that application in order to obtain any upgrade requirements.

Important: Be certain that all third-party vendors are aware that the SR 2.8.1/3.8.1/4.3.1 upgrade is built upon a Solaris 10 software platform.

Supported Server Platforms

The following DNCS server and Application Server hardware platforms are supported by the SR 2.8.1/3.8.1/4.3.1 release:

DNCS Server

Platform	Hard Drives	Memory
Sun Fire V890	■ 6 X 146 GB ■ 12 X 146 GB	■ 8 GB minimum ■ 16 GB minimum
Sun Fire V880	■ 6 X 73 GB ■ 12 X 73 GB	■ 4 GB minimum ■ 8 GB minimum
Sun Fire V445	2 X 73 GB	512 MB minimum

Application Server

Platform	Hard Drives	Memory
Sun Fire V240	2 X 36 GB	512 MB minimum
Sun Blade 150	■ 1 X 40 GB ■ 1 X 80 GB	512 MB minimum

Application Platform Release Dependencies

The following table shows the set-top and Multi-Stream CableCARD™ (M-Card™) module software application platform release dependencies for this software release.

Important: Failure to have the correct application platform software *or later* installed on your system *prior* to installing the software can result in video freezing and black screens when using video-on-demand (VOD) or xOD applications.

Set-Top or M-Card Platform	Operating System (OS)	SARA	PowerKEY® Conditional Access Version
Explorer® 8300 DVR			
v. 1.4.3a10 or later	OS 6.14.74.1	1.88.22.1	3.9
v. 1.5.2	OS 6.14.79.1	1.89.16.2	3.9

Set-Top or M-Card Platform	Operating System (OS)	SARA	PowerKEY® Conditional Access Version
Explorer 8000/8010 DVR v. 1.4.3a10 or later v. 1.5.2	 OS 6.12.74.1 OS 6.12.79.1	 1.88.21.1 1.89.16.2	 3.7.5 3.7.5
Explorer 3250HD MR4 P1 or later	OS 3.24.5.2	1.59.18.1	3.9
Explorer 2xxx, 31xx, 3200, 3100HD	OS 3.13.6.1	1.60.6.2	1.0.6.20 (Explorer 2000s) 1.0.7 (all others)
Explorer 4250HDC Exp. 2.0.0 (0701) or later	OS 6.20.28.1	1.61.5.a100	4.0.1.1
Explorer 8300HDC DVR 1.5.3 (0801) or later	OS 6.20.28.1	1.90.5a101	3.9.7.13
M-Card OS 1.1.10p5 or later	OS 1.1.10p5	Not applicable	Not applicable
Explorer 8550HDC Explorer 8540HDC RNG200 DVR1.5.5	OS 8.0.42.1	1.90.19.1	Not applicable

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

Document Version

This is the second formal release of this document.

1

SR 2.8.1/3.8.1/4.3.1 Pre-Upgrade Procedures

Introduction

This chapter contains procedures that must be completed before you begin the actual upgrade to SR 2.8.1/3.8.1/4.3.1. These pre-upgrade procedures consist mainly of system checks, backups, and various operations upon the metadevices of the DNCS.

The actual upgrade to SR 2.8.1/3.8.1/4.3.1, including some of the procedures in this chapter, must be completed while within a maintenance window. Some of the procedures of this chapter, however, can be completed before the maintenance window begins. See ***When to Complete These Procedures*** (on page 3), for a list of those procedures that can be completed before the start of the maintenance window.

Important: Do not remove any third-party applications files from the DNCS or change any of their settings before performing the SR 2.8.1/3.8.1/4.3.1 upgrade.

Before You Begin

Before you begin the upgrade, attend to these two matters:

- Call Cisco Services and open an Upgrade Tracking Case.
- Verify that you have easy access to the CD-ROM containing your current version of Application Server software. You may need this CD if you ever have to roll back to the previous system release.

In This Chapter

When to Complete These Procedures

Upgrade Process

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

All procedures in this chapter should be completed before entering the maintenance window. Installation CDs should be verified as soon as possible after they are received. This allows time to identify and ship replacement CDs, if necessary. File system backups should be started the morning of the upgrade to ensure that they complete prior to the maintenance window.

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.

- ***Plan Which Optional Features will be Supported*** (on page 5)
- ***Verify the Integrity of the CDs*** (on page 8)
- ***Verify the Integrity of the DBDS Maintenance CD*** (on page 10)
- ***Check Available Disk Space*** (on page 11)
- ***Run the Doctor Report*** (on page 12)
- ***Examine Mirrored Devices*** (on page 13)
- ***Verify DBDS Stability*** (on page 14)
- ***Obtain System Configuration*** (on page 15)
- ***Collect Network Information*** (on page 17)
- ***Check SAM Timers*** (on page 19)
- ***Check CableCARD Server*** (on page 20)

Plan Which Optional Features Will Be Supported

Optional Features

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

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

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

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

Licensed Features

The following list briefly describes the licensed features available with SR 2.8.1/3.8.1/4.3.1:

- EAS FIPS Code Filtering — Support for the use of Federal Information Processing Standards (FIPS) codes to filter EAS message traffic
- DOCSIS DHCT Support — Support for DOCSIS® Digital Home Communication Terminals (DHCTs)
- Enhanced VOD Session Throughput — Support for session performance greater than two sessions per second
- VOD Session Encryption — Support for session-based encryption for video-on-demand (VOD) sessions
- Distributed DNCS — Support for operating the DNCS through a Regional Control System (RCS)
- OpenCable Application Platform (OCAP™) — Support for the Open Cable Access Platform

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

- Conditional Access Mode — Indicates whether the DNCS provides PowerKEY conditional access or non-Cisco conditional access, such as NDS
- DBDS Network Overlay — Enables DNCS support for "Overlay" of a third-party system within an SA system
- SI Type to Use — Specifies the type of system/service information (SI) that the given system will use
- PID Mapping Mode — Specifies whether the transport stream ID (TSID) the system will use is "Dynamic Unique" or "Static non-Unique"
- PreAllocated Session Management — Support for the pre-allocation of sessions by the shared resource manager (SRM) process of the DNCS
- Direct ASI — Enables the system to eliminate the need for the Broadband Integrated Gateway (BIG) to transmit Broadcast File System (BFS) data to modulators
- Third-Party Source — Support for third-party SI sources
  Note: For additional information, refer to the technical bulletin *Program and System Information Protocol Configuration for System Releases 2.5, 2.7, 3.5, 3.7, 4.0, 4.2, and CV 3.4* (part number 4011319).
- Split Channels — Support for split channels in defined channel maps
- Multiflow Multicast — Support for the Multiflow Multicast feature to work with the DOCSIS Settop Gateway (DSG) in the DBDS
- SSP 2.4 Compliant — Support for a Server Interactive Session Request and a Server Interactive Session Release
- OOB Staging Bridge — Support for the use of a subset of the out-of-band (OOB) bridge population within the DBDS to be dedicated to the staging of DHCTs
- Switched Digital Video — Support for the Switched Digital Video (SDV) feature
- Trusted Domain — Support for the MSO Trusted Domain feature, which includes "Home Account" support
- Fixed Key Encryption — Support for the use of the "Fixed Key" algorithm to be used in encryption tasks
- DNO Encrypted VOD — Support for encrypted VOD in an Overlay environment
- OpenCAS PowerKEY Interface — Support for an OpenCAS interface for applying PowerKEY encryption to an established "in the clear" session

- Overlay Netcrypt Bulk Encryptor — Support for the Netcrypt Bulk Encryptor feature
- Content Delivery Mode — Support for the IPTV Service Delivery System (ISDS) feature
- Generic QAM Support — Support for third-party QAMs, allowing the DNCS/ISDS to manage broadcast, SVD, and VOD sessions
- Downloadable CAS — Support for downloadable conditional access subsystem
- Open Cable MP3 Audio Support — Support for the encoding of EAS audio messages to MP3 format for distribution over the TS Broadcaster
- SRM CAS PowerKEY Interface — Support for RPC-based Open Conditional Access Interface (OCAI) such as USRM, GSRM, or any external session and resource manager that is RPC OCAI-compliant.
- iGuide IPG Support — Enables the DREDD proxy on the DNCS/ISDS to provide support for Macrovision iGuide IPG data

Verify the Integrity of the CDs

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

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

1. If necessary, open an xterm window on the DNCS.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Insert a CD into the CD drive on the DNCS.

   Note: If a File Manager window opens after you insert the CD, close the window.
4. Type the following command and press **Enter**. The /cdrom/cdrom0 directory becomes the working directory.

   ```
   cd /cdrom/cdrom0
   ```
5. Type the following command and press **Enter**. The system lists the contents of the CD.

   ```
   ls -la
   ```
6. Did the system list the contents of the CD as expected?
   - If **yes**, go to step 7.
   - If **no**, the CD might be defective. Call Cisco Services for assistance.
7. Type the following command and press **Enter**. The system lists the contents of the CD.

   ```
   pkgchk -d . SAI*
   ```

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

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

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

8 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**.

9 Repeat steps 3 through 8 for each CD received in the software binder.

Verify the Integrity of the DBDS Maintenance CD

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

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

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

2 Type the following command and press **Enter**. The /cdrom/cdrom0 directory becomes the working directory.

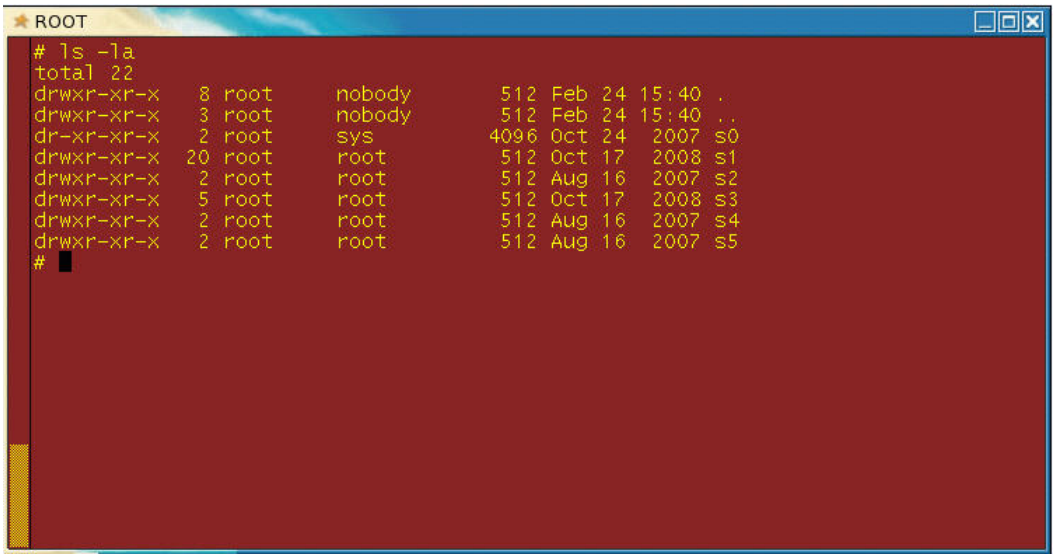
```
cd /cdrom/cdrom0
```

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

```
ls -la
```

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

Example:



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

- If **yes**, complete the following steps.
  - **a** Type **cd /** and then press **Enter**.
  - **b** Type **eject cdrom** and then press **Enter**.
- If **no**, call Cisco Services.

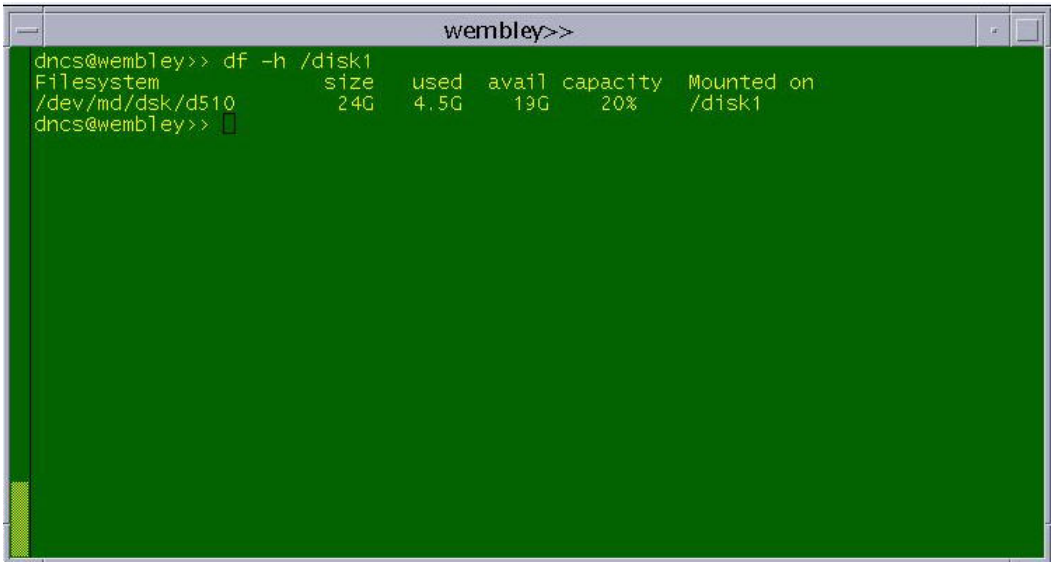
Check Available Disk Space

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

Checking Available Disk Space

1 From an xterm window on the DNCS, type the following command and press **Enter**. The system displays the amount of used and available space on the /disk1 filesystem.

```
df -h  /disk1
```



2 Does the **avail** column show that at least 700 MB of disk space is available?

- If **yes**, go to ***Run the Doctor Report*** (on page 12). You have sufficient space in which to perform the upgrade.
- If **no**, call Cisco Services. Engineers at Cisco Services can advise you regarding disk clean-up procedures.

Run the Doctor Report

Before upgrading the DNCS to SR 2.8.1/3.8.1/4.3.1, run the Doctor Report as **dncs** user. Use the instructions provided in *DBDS Utilities Version 6.3 Installation Instructions and User Guide* (part number 4031374). The Doctor Report provides key system configuration data that might be useful before you begin the upgrade process.

Note: On a typical system, the Doctor Report takes about 10 minutes to run.

Analyze the Doctor Report

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

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

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

Important: Do *not* go to the next procedure until you have completed running and analyzing the Doctor report and correcting any problems it reports.

Examine Mirrored Devices

Before you disable the disk mirroring functions in preparation of an upgrade, you should examine the status of the mirrored drives on your system. All the disk mirroring functions must be working normally before proceeding with the upgrade.

CAUTION:

If the disk mirroring functions of the DNCS are not working properly before the upgrade, you may not be able to easily recover from a failed upgrade.

Examining the Mirrored Devices

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

1. If necessary, open an xterm window on the DNCS.
2. Type the following command and press **Enter**. The system displays the status of all of the metadevices on the DNCS.

   ```
   metastat -c
   ```

   Note: Press the **Spacebar**, if necessary, to page through all of the output.
3. Check for any devices that the system reports that need maintenance.
4. Do any devices need maintenance?
   - If **yes**, call Cisco Services for help in resolving these issues with the metadevices.
   - If **no**, go to the next procedure in this chapter.

Verify DBDS Stability

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

      Note: Do *not* press the Power button.

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

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

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

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

Obtain System Configuration

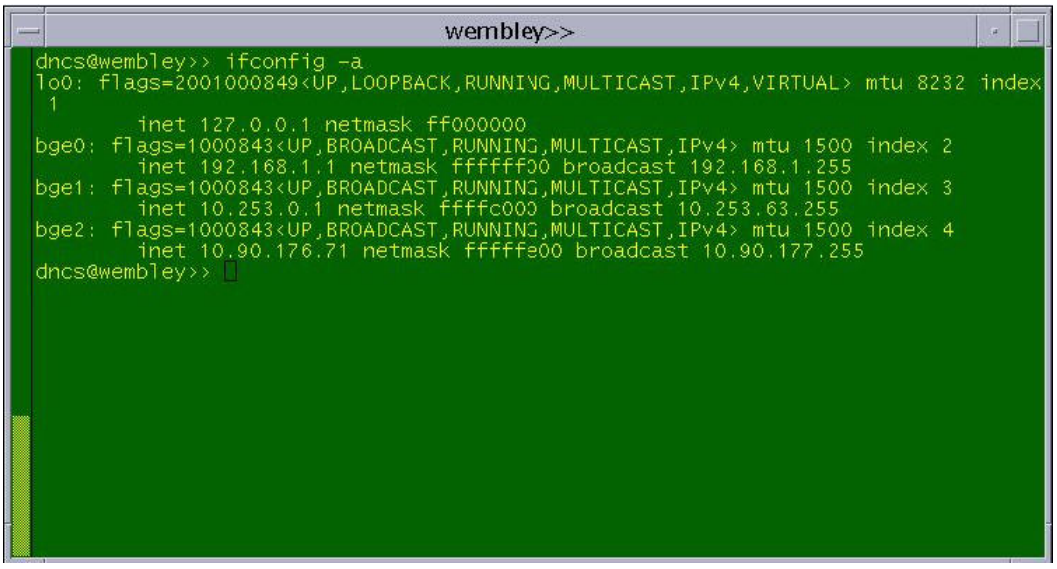
Complete the following steps to obtain basic system configuration data for *both* the DNCS and the Application Server. You may need some of this information later during the upgrade.

1. From an xterm window on the DNCS, type the following command and press **Enter**. A list of IP (Internet Protocol) addresses and hostnames appears.
   ```
   more /etc/hosts
   ```
2. On a sheet of paper, write down the IP addresses of the hosts that appear in the /etc/hosts file.

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

   - appservatm _____
   - dncsatm _____
   - dncseth _____
   - dncsted _____
3. Type the following command and press **Enter**. The hostname for the DNCS appears.
   ```
   uname  -n
   ```
   Important: Call Cisco Services if the hostname contains a period (.). Cisco Services engineers will help you change it to a valid hostname.
4. Write down the hostname for the DNCS, as displayed in step 3: _____
5. Type the following command and press **Enter** to verify that the network interfaces have been plumbed and configured correctly. Output should look similar to the following example:

```
ifconfig -a
```



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

```
more  /etc/hosts
```

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

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

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

```
uname  -n
```

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

_____

Collect Network Information

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

1. If necessary, open an xterm window on the DNCS.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type **cd /export/home/dncs** and then press **Enter**. The /export/home/dncs directory becomes the working directory.
4. Type **mkdir network.pre431** and then press **Enter**. The system creates a directory called network.pre431.
5. Type **cd network.pre431** and then press **Enter**. The /export/home/dncs/network.pre431 directory becomes the working directory.
6. Type the following commands to copy the necessary files to this newly created directory.

   Important:

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

   a. **cp -p /etc/hosts .**
   b. **cp -p /etc/hostname.* .**
   c. **cp -p /etc/inet/hosts inet.hosts**
   d. **cp -p /etc/netmasks .**
   e. **cp -p /etc/defaultrouter .**

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

      Note: If this file is not present, you will receive the **cp: cannot access /etc/defaultrouter** message. In this case, continue with the next command.
   g. **cp -p /etc/vfstab .**
   h. **cp -p /etc/nsswitch.conf .**
   i. **cp -p /etc/rc2.d/S82atminit .**
   j. **cp -p /etc/rc2.d/S85SAspecial .**
   k. **cp -p /etc/inet/ipnodes .**

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

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

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

o **eeprom nvramrc > nvramrc.out**

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

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

Note: Replace < date > with the current date.

Example: tar cvf crontabs.020107.tar crontabs

9 Type **mv crontabs.< date >.tar /export/home/dncs/network.pre431** and then press **Enter**.

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

11 Type **cd /export/home/dncs/network.pre431** and then press **Enter**.

12 Type **ls -ltr** and then press **Enter** to verify that each file copied successfully to the /export/home/dncs/network.pre431 directory and that no file has a size of 0 (zero).

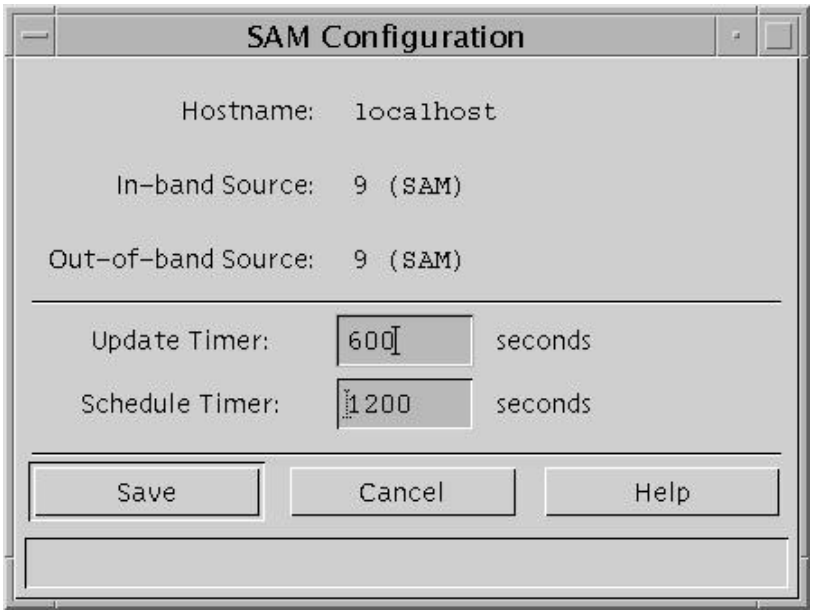
Note: The "l" in **ls** and **-ltr** is a lowercase letter L.

Check SAM Timers

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

Important: The Cisco-recommended value for **Update Timer** is 600. The recommended value for **Schedule Timer** is 1200. The values currently set on the DNCS may differ. Do not make any change without first verifying with the system operator.

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



2 Record the current **Update Timer** value here: _____.

Note: If you change the value, record the new value here: _____.

3 Record the current **Schedule Timer** value here: _____.

Note: If you change the value, record the new value here: _____.

4 Save any changes that you made.

Check CableCARD Server

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

1. From the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab and then click **CableCARD**. The CableCARD Data Summary screen opens.
3. Click **Server Configuration**. The CableCARD Data Summary screen updates to display the Server Configuration portion of the screen.
4. Follow these instructions to record specific CableCARD parameters.
   a. In the space provided, record the **Authorization Time-out Period**.

      _____

   b. In the space provided, record the **DeAuthorization Time-out Period**.

      _____

   Note: In a later procedure, ***Configure the CableCARD Server*** (on page 77), you will ensure that these values are present after the upgrade.
5. Click **Exit** to close the current window.
6. Click **Exit all CableCARD Screens**.

Check the EAS Configuration -- Pre-Upgrade

Before installing the SR 2.8.1/3.8.1/4.3.1 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 Chapter 5, **Testing the EAS**, of *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455).

After completing the procedures in Chapter 5, **Testing the EAS**, verify that you can generate an EAS message for the Emergency Alert Controller (EAC), itself.

Verify the .profile Entries

Verify the EAS Variable

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 the following command and press **Enter**. The system searches for LOCAL_EAS_IP in the /export/home/dncs/.profile file.

```
grep -i LOCAL_EAS_IP /export/home/dncs/.profile
```

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

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

- If **yes**, go to the next procedure in this chapter.
- If **no**, go to step 4.

4 Type the following command and press **Enter**. The system displays the value of the dncseth variable in the /etc/hosts file.

```
cat /etc/hosts | grep dncseth
```

5 Type the following command and press **Enter**. The system displays the value of the eac variable in the /etc/hosts file.

```
cat /etc/hosts | grep eac
```

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

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

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

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

- If **yes**, skip to step 11.
- If **no** (they are on different networks), go to step 8.

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

```
export LOCAL_EAS_IP=[Ethernet address of the DNCS]
```

Note: Substitute the Ethernet address of the DNCS for [Ethernet address of the

DNCS], displayed in step 4.
Example: `LOCAL_EAS_IP=192.168.2.1`

9 Save and close the file.

10 Go to the next procedure in this chapter.

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

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

Example:

```
hme0: flags=1000843< UP,BROADCAST,RUNNING,MULTICAST,IPv4 >
mtu 1500 index 2
   inet 192.168.2.1 netmask ffffff00 broadcast 192.168.2.255
ci0: flags=1000842< BROADCAST,RUNNING,MULTICAST,IPv4 > mtu
9180 index 5
   inet 192.168.4.1 netmask ffffff00 broadcast
192.168.40.255
```

12 Using a text editor, append the following line to the /export/home/dncs/.profile file

```
export LOCAL_EAS_IP=[Ethernet address of the DNCS]
```

Note: Substitute the Ethernet address of the DNCS for [Ethernet address of the DNCS], displayed in step 11.
Example: `LOCAL_EAS_IP=192.168.4.1`

13 Save and close the file.

Verify the PSIP and SI_REGENERATION_TIME Variables

The following procedure checks the PSIP_INSERT_RATE and SI_REGENERATION_TIME variables for their recommended values. A brief explanation of why you are checking these variables follows.

PSIP_INSERT_RATE

If the site you are upgrading does *not* use the DNCS for PSIP and inband EAS messages that are targeted to hosts, such as QAM tuner TVs, you can disable delivery of these messages from the DNCS by setting the **PSIP_INSERT_RATE** variable to 0 in the .profile file. If you are not using the DNCS to provide these messages, you should make provisions to provide these signals by other PSIP aggregation/EAS equipment in your system.

Important:

- Be aware that there are FCC regulatory requirements to provide PSIP and EAS to these devices.
- If the DNCS is used for PSIP and inband EAS messages that are targeted to hosts, such as QAM tuner TVs, the **PSIP_INSERT_RATE** variable should not be present in the .profile. If it is present in the .profile file, it should not be set to 0.

SI_REGENERATION_TIME

The **SI_REGENERATION_TIME** variable in the .profile file needs to be set to **1200** (20 minutes) so that SI updates happen, at most, once every 20 minutes.

Complete the following steps to check the **PSIP_INSERT_RATE** and **SI_REGENERATION_TIME** variables in the .profile file.

1. If necessary, open an xterm window on the DNCS.
2. Type the following command and press **Enter**:
   ```
   grep PSIP_INSERT_RATE  /export/home/dncs/.profile
   ```
3. Do the results from step 2 reveal that the PSIP variable already exists in the .profile file?
   - If **yes**, and if the DNCS is NOT used for PSIP and inband EAS targeted to hosts, continue with step 4.
   - If **no**, and if the DNCS is NOT used for PSIP and inband EAS targeted to hosts, skip to step 5.
   - If **no**, and if the DNCS is used for PSIP and inband EAS targeted to hosts, go to step 8; no .profile changes for the PSIP_INSERT_RATE are required.
4. Is the **PSIP_INSERT_RATE** variable already set to **0**?
   - If **yes**, go to step 8; no .profile changes for the PSIP_INSERT_RATE are required.
   - If **no**, continue with step 5.
5. Open the .profile file with a text editor.
6. Is the **PSIP_INSERT_RATE** variable already in the file?
   - If **yes**, set the value of this variable to **0**.
   - If **no**, add the following entries to the bottom of the file:
     ```
     PSIP_INSERT_RATE=0
     export PSIP_INSERT_RATE
     ```
7. Save and close the file.
8. From the xterm window on the DNCS, type the following command and press **Enter**:
   ```
   grep SI_REGENERATION_TIME  /export/home/dncs/.profile
   ```

9 Does your output from step 8 show that the **SI_REGENERATION_TIME** variable exists *and* is set to **1200**?

- If **yes** (to both requirements), go to the next procedure in this chapter.
- If **no**, go to step 10.

10 Open the .profile file with a text editor.

11 Choose one of the following options:

- If the **SI_REGENERATION_TIME** variable is not yet present in the .profile file, append the variable to the file and set it to **1200**.
- If the **SI_REGENERATION_TIME** variable is present in the .profile file but is set incorrectly, change it to **1200**.

  Example: When you are finished, your entry should be:
  `SI_REGENERATION_TIME=1200`

12 Save and close the file.

Bounce the siManager Process

If you made any edits to the .profile file for the **PSIP_INSERT_RATE** or the **SI_REGENERATION_TIME** variables, you need to bounce the siManager process of the DNCS in order for the system to recognize those changes.

1 When completing the ***Verify the PSIP and SI_REGENERATION_TIME Variables*** (on page 23) procedure, did you make any changes to the .profile file?

- If **yes**, continue with step 2.
- If **no**, skip to the next procedure in this chapter. You have no need to bounce the siManager process.

2 Log out of the DNCS.

3 Log back onto the DNCS as dncs user. The changes you made to the .profile file are now available to the siManager process.

4 Follow these instructions to stop the siManager process.

a Select **siManager** in the DNCS Control window.

b Click **Process**.

c Select **Stop Process**.

d Wait for the indicator of the siManager process to become red.

5 Follow these instructions to restart the siManager process.

a Select **siManager** in the DNCS Control window.

b Click **Process**.

c Select **Start Process**.

d Wait for the indicator of the siManager process to become green.

Check and Record Sessions

Checking the BFS Sessions on the BFS QAM or GQAM

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

1. Follow these instructions to check the number of active sessions on the BFS QAM and/or GQAM.
   a. Press the **Options** button on the front panel of the modulator until the **Session Count** total appears. Record the **Session Count** here. _____
   b. Record the **Options** button again and record the **Program Count** here. _____
2. In an xterm window on the DNCS, type the following command and press **Enter**:
   `auditQam -query [IP address] [output port number]`
3. Record the output from step 2 here: _____
4. Type the following command and press **Enter**.
   `/opt/solHmux64/vpStatus -d /dev/Hmux0 -P 0`
5. Record the **Active Streams Count** here. _____
6. Do the results of steps 1 through 5 all show the same number of sessions?
   - If **yes**, continue with the next procedure in this chapter.
   - If **no**, contact Cisco Services for help in resolving this issue.

Back Up the DNCS and Application Server File Systems

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

Stop the dhctStatus, signonCount, and cmd2000 Processes

When sites are being upgraded, the dhctStatus utility may occasionally be in the process of polling DHCTs. Additionally, the signonCount utility may be active in system memory. Our engineers have discovered that upgrades proceed more smoothly when the dhctStatus utility is not actively polling DHCTs and when the signonCount and cmd2000 processes are not active in system memory. The instructions in this chapter guide you through the steps required to stop these processes.

Terminating the dhctStatus Utility Polling Operation

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

1. If necessary, open an xterm window on the DNCS.
2. Type **ps -ef | grep dhctStatus** and then press **Enter** to determine if the dhctStatus utility is running.

   Example: (if it is running)

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

3. Do the results from step 2 show that the dhctStatus utility is running?
   - If **yes**, type **dhctStatus** and press **Enter** to display the dhctStatus menu.
   - If **no**, skip the rest of this procedure.
4. To terminate the polling operation, follow these instructions.
   a. Type **p** and then press **Enter**. The system displays a polling menu.
   b. Type **t** and then press **Enter**. The system terminates the polling operation.
   c. Press **Enter** to return to the main menu.
   d. Press **q** and then press **Enter** to exit the menu.

5 Type **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
```

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

Example: kill -9 12449

Removing the signonCount Utility from System Memory

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

2 Do the results from step 1 show that the signonCount utility is running?

- If **yes**, continue with step 3.
- If **no**, you can skip the rest of this procedure.

3 From a dncs xterm window, type **signonCount uninstall** and press **Enter**.

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

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

5 Type **kill -9 [processid]** and then press **Enter** for each process ID displayed in step 4.

Note: The process ID(s) to kill is/are located starting with the second column of the output from step 4.

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

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

Terminating the cmd2000 Processes

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

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

Back Up Various Data Files

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

Backing Up Various Data Directories

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

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

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

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

Back Up and Delete the copyControlParams File

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

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

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

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

2

SR 2.8.1/3.8.1/4.3.1 Upgrade Procedures

Introduction

In this chapter, you will install the SR 2.8.1/3.8.1/4.3.1 software. The SR 2.8.1/3.8.1/4.3.1 software includes new software for the DNCS, as well as for the graphical and Web user interfaces (GUI and WUI) of the DNCS.

Important: Do not attempt to perform the procedures in this chapter more than once. If you encounter any problems while upgrading the DNCS or Application Server to SR 2.8.1/3.8.1/4.3.1, contact Cisco Services at 1-866-787-3866.

In This Chapter

Suspend Billing and Third-Party Interfaces

Important Note About the Maintenance Window

CAUTION:

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

Suspending Billing and Third-Party Interfaces

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

Stopping the ippvReceiver Process

Follow these instructions to stop the ippvReceiver process.

1. On the DNCS Control window, select **ippvReceiver**.
2. Click **Process**.
3. Click **Stop Processes**. The indicator for the ippvReceiver processes changes from green to red.

Stop the cron Jobs

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

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

Stopping the cron Jobs on the DNCS

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

Note: You need to 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 **svcadm -v disable -s cron** and then press **Enter**.
   - If **no**, go to **Stopping the cron Jobs on the 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 Application Server

Complete the following steps to stop cron jobs on the Application Server.

Note: You should be logged on to an xterm window on the Application Server 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 **svcadm -v disable -s cron** and then press **Enter**.
   - If **no**, the cron jobs are already stopped on the Application Server; go to the next procedure in this chapter.

Back Up the Informix Database

Backing Up the Informix Database

This procedure should be completed as close to the maintenance window as possible, thereby allowing sufficient time to complete the backup before entering the maintenance window. Use these procedures to back up the DNCS and Application Server databases.

Notes:

- The system components can be running while you back up the Informix database.
- It may take up to 30 minutes to back up a typical database with approximately 100,000 DHCTs.
- If you are using an external DVD drive, substitute *cdrom1* for *cdrom0*.

1 From a root xterm window, type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

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

2 Label your backup tape with the following information:

[DNCS or Application Server] Database Backup [Day of the Week]
[Site Name]
[Software Version]
SR 2.8.1/3.8.1/4.3.1 DVD [version]
[Tape #]

Notes:

- Customize the label with the day of the week, site name, and software version for the site you are backing up.
- If your database backup requires more than one tape, be sure to note the tape number on the label.

3 Insert the tape into the tape drive of the DNCS and wait until the green light stops flashing.

Important: Be sure that you are using different tapes for each day of the week.

4 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.

5 Choose one of the following options.

- If you are using the standard tape drive configuration, follow these instructions.
  - **a** Type **/cdrom/cdrom0/s3/backup_restore/backupDatabase -v** and then press **Enter**.
    Result: The system displays the following message:
    Please mount tape 1 on /dev/rmt/0h and then press Return to continue.
  - **b** Go to step 6.
- If you are using a custom tape drive configuration, go to step 6.

6 If you are using a custom tape drive configuration, type **/cdrom/cdrom0/s3/backup_restore/backupDatabase -v -b [blocksize] -s [tapesize]** and then press **Enter**.

Note: Substitute the blocksize and tapesize that pertain to your system for [blocksize] and [tapesize].

Example:
/cdrom/cdrom0/s3/backup_restore/backupDatabase -v -b 128 -s 13212058

Result: The system displays the following message:
Please mount tape 1 on /dev/rmt/0h and then press Return to continue.

7 Press **Enter**. The system backs up your Informix database.

Notes:

- The system will prompt you to insert additional tapes if your backup requires more than one tape.
- The message **Successfully completed the database backup** appears when the backup has completed successfully.
- If the database backup was not successful, the system displays an error message. Call Cisco Services at 1-866-787-3866 for assistance in resolving the error message.

8 Remove the tape(s) and store it/them in a safe place.

Stop Basic Backup or Auto Backup Servers

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

Stop System Components

Before continuing with the installation of SR 2.8.1/3.8.1/4.3.1, follow the instructions in this section to stop the Application Server and the DNCS.

Important: You must be within a maintenance window when you complete this and the remaining procedures in this chapter.

CAUTION:

Do not proceed if you are NOT in the maintenance window. These procedures that stop the system components disrupt services.

Stop Third-Party Servers

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

Stopping the Application Server

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

Stopping the Application Server at SARA Sites

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

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

Preparing the Rovi Application Server

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

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

Stopping the DNCS

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

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

Ensuring No Active Database Sessions on the DNCS

Follow these instructions to ensure that there are no active database sessions running on the DNCS.

Notes:

- You need to be root user to run some of the commands in this procedure.
- If you have followed the instructions so far, you should still have a xterm window open and be logged into it as **root** user.

1. Are you already logged on to an xterm window as **root** user?
   - If **yes**, go to step 2.
   - If **no**, log on to the xterm window as root user.
2. 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.
3. Type **showActiveSessions** and then press **Enter**. One of the following messages appears:

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

4 Did the message in step 3 indicate that there are active sessions?

- If **yes**, go to step 5.
- If **no**, go to step 6.

5 Follow these instructions to kill active sessions.

   a Type **killActiveSessions** and then press **Enter**. The system removes all active sessions from the database.

   b Type **showActiveSessions** again and then press **Enter**.

   c Did a message appear indicating that there are active sessions?

   – If **yes**, call Cisco Services.

   – If **no**, go to step 6.

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

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

8 Is the dncsInitd process still running?

- If **yes**, repeat steps 6 through 8.
- If **no**, go to step 9.

9 Type **clearDbSessions** and press **Enter**.

Detach Disk Mirrors on the DNCS

In ***Examine Mirrored Devices*** (on page 13), sites confirm the disk mirroring function is working correctly before beginning the upgrade process. In this procedure you now disable the mirroring functions on the DNCS to ensure that the contents of the mirrored disk reflects the data and configuration of the DNCS prior to an upgrade. If the upgrade fails for any reason, you can then swap the positions of the mirrored disks to restore your system to its condition prior to the upgrade attempt.

Note: Disabling disk mirroring is usually referred to as detaching disk mirroring.

Detaching Disk Mirrors on the DNCS

Follow these instructions to detach the disk mirroring function of the Enterprise 450 or Sun Fire V445, V880, or V890 DNCS.

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

1. Insert the CD labeled **DBDS Maintenance CD** into the CD-ROM 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 **eject cdrom** and then press **Enter**. The system ejects the CD.

Install the DNCS Software

Complete these steps to install the SR 2.8.1/3.8.1/4.3.1 DNCS software.

Notes:

- You should still be logged in as root user to the xterm window on the DNCS.
- It may take as long as 1 hour to install the DNCS software.

1 Insert the CD labeled similar to **DNCS Application x.x.x.x** into the CD drive of the DNCS. The system automatically mounts the CD to /cdrom within 30 seconds.

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

4 Type **install_pkg** and then press **Enter**. A confirmation message appears.

5 Type **y** and then press **Enter**. The system displays a **Press Enter to continue** message.

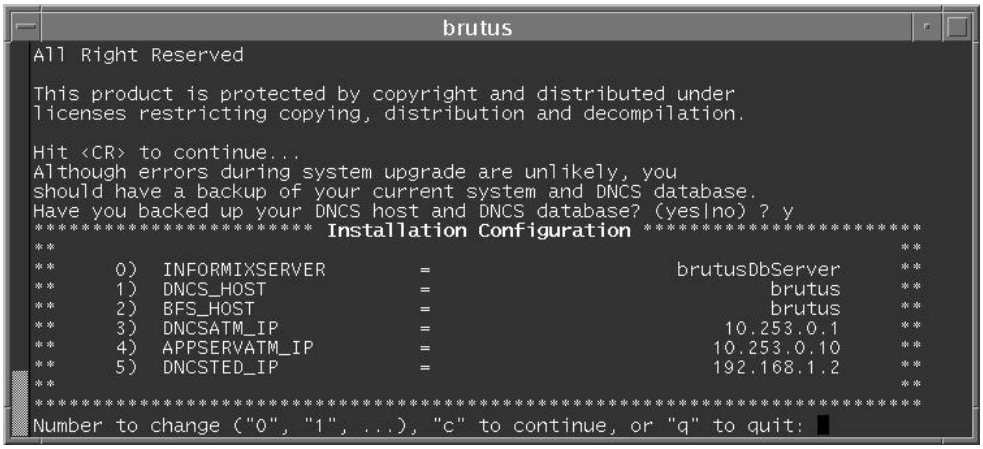
6 Press **Enter**. The system displays a message that asks whether you have backed up the database

7 Type **y** and then press **Enter**. The system displays a message that asks you to define the number of days until EMMs are deleted from the system.

Note: To see current value used by the system, type **less /dvs/dncs/bin/CED.in** and press **Enter**.

8 Type **d** (for default), or enter a valid integer representing the number of days, and then press **Enter**. A confirmation message appears.

9 Type **y** and then press **Enter**. The system lists some configuration parameters of system components and asks that you confirm their accuracy.



10 Refer to the notes you took in the ***Obtain System Configuration*** (on page 15) section of Chapter 1 and verify that the configuration parameters are listed correctly; then press **c** to continue. The DNCS software installs on the DNCS.

Note: If you have to change any parameters, follow the on-screen instructions to do so. Only in rare cases will you have to modify a parameter.

11 After the upgrade has completed, follow these instructions to eject the CD.

a Type **cd /** and then press **Enter**.

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

12 Check the log file for errors. Go to the next procedure in this chapter if the log file indicates that the DNCS software installed without error.

Notes:

- The installation log file is in the /var/sadm/system/logs directory of the DNCS.
- The log file for the DNCS software is called **SAIdncs_[version #]_install.log**.
- Call Cisco Services for assistance if the log file reveals errors.

Install the DNCS GUIs and WUIs

Complete these steps to install the SR 2.8.1/3.8.1/4.3.1 DNCS GUI and WUI software.

Note: It should take no more than 15 minutes to install the DNCS GUI and WUI software.

1. Insert the CD labeled similar to **DNCS GUI/WUI x.x.x.x** into the CD drive of the DNCS. The system automatically mounts the CD to /cdrom within 30 seconds.
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 **cd /cdrom/cdrom0** and then press **Enter**. The /cdrom/cdrom0 directory becomes the working directory.
4. Type **install_pkg** and then press **Enter**. A confirmation message appears.
5. Type **y** and then press **Enter**. The software installs on the DNCS.
6. After the upgrade has completed, follow these instructions to eject the CD.
   a. Type **cd /** and then press **Enter**.
   b. Type **eject cdrom** and then press **Enter**.
7. Check the log file for errors. Go to ***Install Additional Software*** (on page 50) if the log file indicates that the DNCS GUI and WUI software installed without error.

   Notes:

   - The installation log file is in the /var/sadm/system/logs directory of the DNCS.
   - The log file for the DNCS GUI is called **SAIgui_[version #]_install.log**.
   - The log file for the DNCS WUI is called **SAIwebui_[version #]_install**.log.
   - Call Cisco Services for assistance if the log file reveals errors.

Install Additional Software

Install the following SR 4.3.1 software now:

- DNCS Online Help 4.3.1.0
- Report Writer r1.0.0.3

Complete these steps for each software CD.

1. Insert the CD into the CD drive of the DNCS. The system automatically mounts the CD to /cdrom within 30 seconds.
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 **cd /cdrom/cdrom0** and then press **Enter**. The /cdrom/cdrom0 directory becomes the working directory.

   Note: Most CDs come with a README file that you can read at this point.
4. Type **install_pkg** and then press **Enter**. A confirmation message appears.
5. Type **y** and then press **Enter**. The software installs on the DNCS.
6. After the upgrade has completed, follow these instructions to eject the CD.
   a. Type **cd /** and then press **Enter**.
   b. Type **eject cdrom** and then press **Enter**.
7. Check the appropriate log file for errors.

   Notes:
   - The log files are in the /var/sadm/system/logs directory of the DNCS.
   - Call Cisco Services for assistance if the log file reveals errors.

Patch Software

Install the DNCS 4.3.1.6p2 patch software now. The patch CD should have a README file. Follow the instructions in the README file to install the patch software.

Check the SR 2.8.1/3.8.1/4.3.1 Installed Components Version

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

Note: Running the Doctor Report with the *–g* option also displays installed software versions. Feel free to obtain this information from the Doctor Report if you prefer.

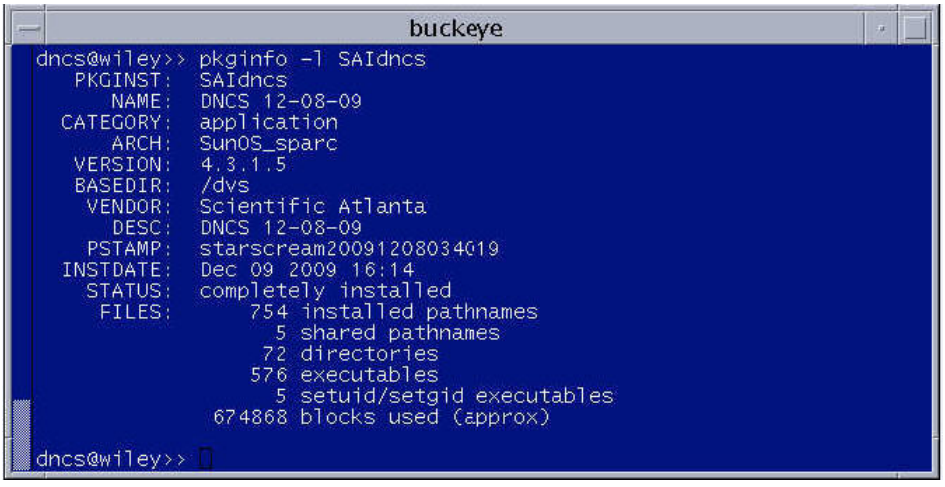
Verifying DNCS Versions

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 is a lowercase 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 4.3.1.x 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	4.3.1.6p2	
DNCS GUI	SAIgui	4.3.1.6	
DNCS WUI	SAIwebui	4.3.1.6p2	
DNCS Online Help	SAIhelp	4.3.1.0	
DNCS Report Writer	SAIrptwrt	r1.0.0.3	

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 the next procedure in this chapter.
- If **no**, call Cisco Services and inform them of the discrepancy.

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

Enable Optional and Licensed Features

If you have properly followed all of the instructions so far, the system components should be stopped. Now is the time to enable any optional or licensed features that pertain to this install. Contact Cisco Services to enable any optional or licensed features.

Verify the .profile Entries

Verify the EAS Variable

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 the following command and press **Enter**. The system searches for LOCAL_EAS_IP in the /export/home/dncs/.profile file.

```
grep -i LOCAL_EAS_IP /export/home/dncs/.profile
```

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

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

- If **yes**, go to the next procedure in this chapter.
- If **no**, go to step 4.

4 Type the following command and press **Enter**. The system displays the value of the dncseth variable in the /etc/hosts file.

```
cat /etc/hosts | grep dncseth
```

5 Type the following command and press **Enter**. The system displays the value of the eac variable in the /etc/hosts file.

```
cat /etc/hosts | grep eac
```

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

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

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

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

- If **yes**, skip to step 11.
- If **no** (they are on different networks), go to step 8.

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

```
export LOCAL_EAS_IP=[Ethernet address of the DNCS]
```

Note: Substitute the Ethernet address of the DNCS for [Ethernet address of the

DNCS], displayed in step 4.
Example: `LOCAL_EAS_IP=192.168.2.1`

9 Save and close the file.

10 Go to the next procedure in this chapter.

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

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

Example:

```
hme0: flags=1000843< UP,BROADCAST,RUNNING,MULTICAST,IPv4 >
mtu 1500 index 2
   inet 192.168.2.1 netmask ffffff00 broadcast 192.168.2.255
ci0: flags=1000842< BROADCAST,RUNNING,MULTICAST,IPv4 > mtu
9180 index 5
   inet 192.168.4.1 netmask ffffff00 broadcast
192.168.40.255
```

12 Using a text editor, append the following line to the /export/home/dncs/.profile file

```
export LOCAL_EAS_IP=[Ethernet address of the DNCS]
```

Note: Substitute the Ethernet address of the DNCS for [Ethernet address of the DNCS], displayed in step 11.
Example: `LOCAL_EAS_IP=192.168.4.1`

13 Save and close the file.

Verify the PSIP and SI_REGENERATION_TIME Variables

The following procedure checks the PSIP_INSERT_RATE and SI_REGENERATION_TIME variables for their recommended values. A brief explanation of why you are checking these variables follows.

PSIP_INSERT_RATE

If the site you are upgrading does *not* use the DNCS for PSIP and inband EAS messages that are targeted to hosts, such as QAM tuner TVs, you can disable delivery of these messages from the DNCS by setting the **PSIP_INSERT_RATE** variable to 0 in the .profile file. If you are not using the DNCS to provide these messages, you should make provisions to provide these signals by other PSIP aggregation/EAS equipment in your system.

Important:

- Be aware that there are FCC regulatory requirements to provide PSIP and EAS to these devices.
- If the DNCS is used for PSIP and inband EAS messages that are targeted to hosts, such as QAM tuner TVs, the **PSIP_INSERT_RATE** variable should not be present in the .profile. If it is present in the .profile file, it should not be set to 0.

SI_REGENERATION_TIME

The **SI_REGENERATION_TIME** variable in the .profile file needs to be set to **1200** (20 minutes) so that SI updates happen, at most, once every 20 minutes.

Complete the following steps to check the **PSIP_INSERT_RATE** and **SI_REGENERATION_TIME** variables in the .profile file.

1. If necessary, open an xterm window on the DNCS.
2. Type the following command and press **Enter**:
   ```
   grep PSIP_INSERT_RATE  /export/home/dncs/.profile
   ```
3. Do the results from step 2 reveal that the PSIP variable already exists in the .profile file?
   - If **yes**, and if the DNCS is NOT used for PSIP and inband EAS targeted to hosts, continue with step 4.
   - If **no**, and if the DNCS is NOT used for PSIP and inband EAS targeted to hosts, skip to step 5.
   - If **no**, and if the DNCS is used for PSIP and inband EAS targeted to hosts, go to step 8; no .profile changes for the PSIP_INSERT_RATE are required.
4. Is the **PSIP_INSERT_RATE** variable already set to **0**?
   - If **yes**, go to step 8; no .profile changes for the PSIP_INSERT_RATE are required.
   - If **no**, continue with step 5.
5. Open the .profile file with a text editor.
6. Is the **PSIP_INSERT_RATE** variable already in the file?
   - If **yes**, set the value of this variable to **0**.
   - If **no**, add the following entries to the bottom of the file:
     ```
     PSIP_INSERT_RATE=0
     export PSIP_INSERT_RATE
     ```
7. Save and close the file.
8. From the xterm window on the DNCS, type the following command and press **Enter**:
   ```
   grep SI_REGENERATION_TIME  /export/home/dncs/.profile
   ```

9 Does your output from step 8 show that the **SI_REGENERATION_TIME** variable exists *and* is set to **1200**?

- If **yes** (to both requirements), go to the next procedure in this chapter.
- If **no**, go to step 10.

10 Open the .profile file with a text editor.

11 Choose one of the following options:

- If the **SI_REGENERATION_TIME** variable is not yet present in the .profile file, append the variable to the file and set it to **1200**.
- If the **SI_REGENERATION_TIME** variable is present in the .profile file but is set incorrectly, change it to **1200**.

  Example: When you are finished, your entry should be:
  `SI_REGENERATION_TIME=1200`

12 Save and close the file.

Bounce the siManager Process

If you made any edits to the .profile file for the **PSIP_INSERT_RATE** or the **SI_REGENERATION_TIME** variables, you need to bounce the siManager process of the DNCS in order for the system to recognize those changes.

1 When completing the ***Verify the PSIP and SI_REGENERATION_TIME Variables*** (on page 52) procedure, did you make any changes to the .profile file?

- If **yes**, continue with step 2.
- If **no**, skip to the next procedure in this chapter. You have no need to bounce the siManager process.

2 Log out of the DNCS.

3 Log back onto the DNCS as dncs user. The changes you made to the .profile file are now available to the siManager process.

4 Follow these instructions to stop the siManager process.

a Select **siManager** in the DNCS Control window.

b Click **Process**.

c Select **Stop Process**.

d Wait for the indicator of the siManager process to become red.

5 Follow these instructions to restart the siManager process.

a Select **siManager** in the DNCS Control window.

b Click **Process**.

c Select **Start Process**.

d Wait for the indicator of the siManager process to become green.

Remove Scripts That Bounce the Pass-Through Process

In order to correct some issues associated with the Pass-Through process on the DNCS, some sites have been regularly bouncing this process through scripts that reside in the crontab file. SR 2.8.1/3.8.1/4.3.1 contains software that 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

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

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

   Note: While you can edit the crontab directly, we recommend that you first redirect the contents of the crontab to dncs.crontab so you can recover the original crontab if necessary.
5. Type **vi /tmp/dncs.crontab** and then press **Enter**. The dncs.crontab file opens for

editing using the vi text editor.

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

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

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

Reboot the DNCS and Application Server

After installing the software onto the DNCS, complete the following steps to reboot the DNCS and Application Server.

1. Choose one of the following options:
   - If you are using a Cisco Application Server, open an xterm window (if necessary) on the Application Server.
   - If you are using a Rovi Corporation Application Server, skip to step 4.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. From the xterm window on the Application Server, type **/usr/sbin/shutdown -g0 -y -i0** and then press **Enter**. The Application Server shuts down.
4. If necessary, open an xterm window on the DNCS.
5. 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**.
6. From the 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.
7. Log on to the DNCS as **dncs** user.
8. At the **ok** prompt on the Cisco Application Server, type **boot** and then press **Enter**. The Application Server reboots.
9. Log on to the Application Server as **dncs** user.

Disable the SAM Process on Rovi and MDN/ODN Systems

If the site you are upgrading uses the Rovi Corporation application server, you need to disable the SAM process before you restart the system components. Complete the following steps to disable the SAM process.

Notes:

- If the site you are upgrading does not use the Rovi Corporation application server, skip this procedure and go to the next procedure in this chapter.
- You should be logged on to the DNCS as **dncs** user.

1. In the DNCS section of the DNCS Administrative Console Status window, click **Control**. The DNCS Monitor window opens.
2. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The DNCS Control window opens.
3. Type **4** (for Define/Update Grouped Elements) and then press **Enter**. The window updates to list a series of element groups.
4. Type **14** (for saManager) and then press **Enter**. The window updates to list the elements in the group.
5. Type **1** (for /dvs/dncs/bin/saManager) and then press **Enter**. The first in a series of confirmation messages appears.
6. Press **Enter** at each 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.

Restart the System Components

After installing the SR 2.8.1/3.8.1/4.3.1 software, follow these instructions to restart the system components.

Restarting the DNCS

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

   Results:

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

   Notes:

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

Restarting the SARA Application Server

Important: If the site you are upgrading uses the Rovi Corporation Application Server, skip this procedure and go to ***Restart the Application Server at Rovi Sites*** (on page 66).

Note: The Application Server should be at an **OK** prompt.

1. Type **boot** and press **Enter**. The server reboots.
2. Log on as **dncs** user.

3 Open an xterm window on the Application Server.

4 Type **appControl** and then press **Enter**. The Applications Control window opens.

5 Select option **2** on the Applications Control window. The system displays a list of Application Server processes and their current status.

6 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 the next procedure in this chapter.
- If **no**, go to step 7.

7 Press the middle mouse button, and then select **App Serv Start**.

8 When the Application Control window indicates that the current state (Curr Stt) of each process is **running**, go to step 9.

Note: On some systems, the BFS Remote process may remain at **Stopped**; this is normal.

9 Follow the on-screen instructions to close the Applications Control window.

Restart the Application Server at Rovi Sites

Follow this procedure *only* if the site you are upgrading supports the Rovi Corporation Application Server. If the site you are upgrading supports the SARA Server, skip this section and go to the next procedure in this chapter.

Restarting the Application Server at a Rovi Site

Complete the following steps to check if the Rovi 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 the next procedure in this chapter.
   - 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 Rovi drivers.

   Note: The AppServer Control window on the DNCS Administrative Console Status window may display an inactive status. This is normal for a Rovi site.

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 prior to installing the SR 2.8.1/3.8.1/4.3.1 software, restart those interfaces, as well.

Restarting the Time Warner Mystro Application Server

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

Restart the cron Jobs

Restarting the cron Jobs on the DNCS

1. If necessary, open an xterm window on the DNCS.
2. Type **ps -ef | grep cron** and then press **Enter**. The system should list /usr/sbin/cron. Have the cron jobs restarted on the DNCS?
   a. If **yes**, go to ***Restarting the cron Jobs on the Application Server*** (on page 68).
   b. If **no**, go to step 3.
3. Follow these instructions to log in 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**.
4. Type the following command and press **Enter** to restart all cron jobs:
   ```
   svcadm -v enable -rs cron
   ```
5. Confirm that the cron jobs have restarted by typing **ps -ef | grep cron** and then press **Enter**. The system should list /usr/sbin/cron.
6. Go to ***Restarting the cron Jobs on the Application Server*** (on page 68).

Restarting the cron Jobs on the Application Server

If necessary, follow these instructions to restart the cron jobs on the Application Server. The cron jobs on the Application Server may have restarted on their own when you booted the Application Server, earlier in this chapter.

Important: This procedure pertains to the SARA Server, only. If the site you are upgrading supports the Rovi Application Server, check with Rovi for the appropriate procedure.

1. If necessary, open an xterm window on the Application Server.
2. Type **ps -ef | grep cron** and then press **Enter**. The system should list /usr/sbin/cron. Have the cron jobs restarted on the Application Server?
   a. If **yes**, go to the next procedure in this chapter.
   b. If **no**, go to step 3.
3. Follow these instructions to log in 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**.

4 Type the following command and press **Enter** to restart all cron jobs:

```
svcadm -v enable -rs cron
```

5 Confirm that the cron jobs have restarted by typing **ps -ef | grep cron** and then press **Enter**. The system should list /usr/sbin/cron.

6 Type **exit** and then press **Enter** to log out the root user.

Check cron Jobs

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

Follow these instructions to check the crontab files.

1. From an xterm window on the DNCS, type the following command and press **Enter**.
   ```
   cd /export/home/dncs/network
   ```
2. Type the following command and press **Enter**.
   ```
   tar xvf crontabs.tar
   ```
3. Type **cd crontabs** and press **Enter**.
4. Follow these instructions to compare the dncs crontab file to the actual post-upgrade entries.
   a. Type **less dncs** and press **Enter**.
   b. Type `crontab -l dncs` and press **Enter**.
   c. Compare the output from steps a and b. Verify that customer-specific cron entries in step a are included in step b.
   d. Add any missing entries from step a to the dncs crontab file.
5. Repeat step 4 for the root crontab file.

Restart Utilities

Restart the dhctStatus Utility

The dhctStatus Utility usually runs from cron and will start at its scheduled time.

Restarting the signonCount Utility

If the signonCount utility was running prior to the upgrade, follow these steps to restart the utility. If you do not want to start the signonCount utility at this time, skip this procedure and go to the next procedure in this chapter.

1. Type **signonCount** and press **Enter**. The signonCount process starts and begins displaying settop sign-on status.
2. Press the **Ctrl** and **C** keys simultaneously to stop the terminal output.
3. Type `tail -f /dvs/dncs/tmp/signonCount.out` and press **Enter** to monitor the signonCount utility status. The terminal displays the last 10 lines in the output file, as well as any new entries made to the output file.
4. Press the **Ctrl** and **C** keys simultaneously to terminate the *tail* process.

Restart the cmd2000 Utility

1. To restart the cmd2000 utility, type the following command and then press **Enter**:
   ```
   /dvs/resapp/Tools cmd2000 -log -listen &
   ```
2. To confirm that the cmd2000 utility is running, type the following command and press **Enter**:
   ```
   ps -ef | grep cmd2000
   ```

3

SR 2.8.1/3.8.1/4.3.1 Post-Upgrade Procedures

Introduction

After installing the SR 2.8.1/3.8.1/4.3.1 software, follow the procedures in this chapter to complete the upgrade process.

In This Chapter

Restore the Data Files

In this procedure, you will restore the data files you backed up to tape in the ***Back Up Various Data Files*** (on page 32) section in Chapter 1.

Note: This procedure references the device name of the DNCS tape drive. If you are unsure of the device name, or simply wish to confirm it, run the procedure in Appendix B, ***How to Determine the Tape Drive Device Name*** (on page 97).

Restoring the Data Files

Follow this procedure to restore the data files.

1. Insert the tape you used in the **Back Up Various Data Files** section of Chapter 1 into the tape drive of the DNCS.

   Note: Be sure that the tape is write-protected.
2. If necessary, open an xterm window on the DNCS.
3. Type **tar xvf [device name]** and then press **Enter**. The system restores the specified files.

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

   Example: tar xvf /dev/rmt/0h
4. When the restoration is complete, eject the tape and store it in a safe place.

Verify SAM Timers

After you upgrade your system to SR 2.8.1/3.8.1/4.3.1, the **Update Timer** and **Schedule Timer** fields on the SAM Configuration window should be set to the values they held prior to the upgrade. These values ensure that channel maps and the database have sufficient time to update. You recorded these values in ***Check SAM Timers*** (on page 19). Follow the instructions in this section to set the **Update Timer** and **Schedule Timer** fields to their appropriate values.

Note: This procedure pertains only to sites that support SARA. Skip this procedure if the site you have upgraded does not support SARA.

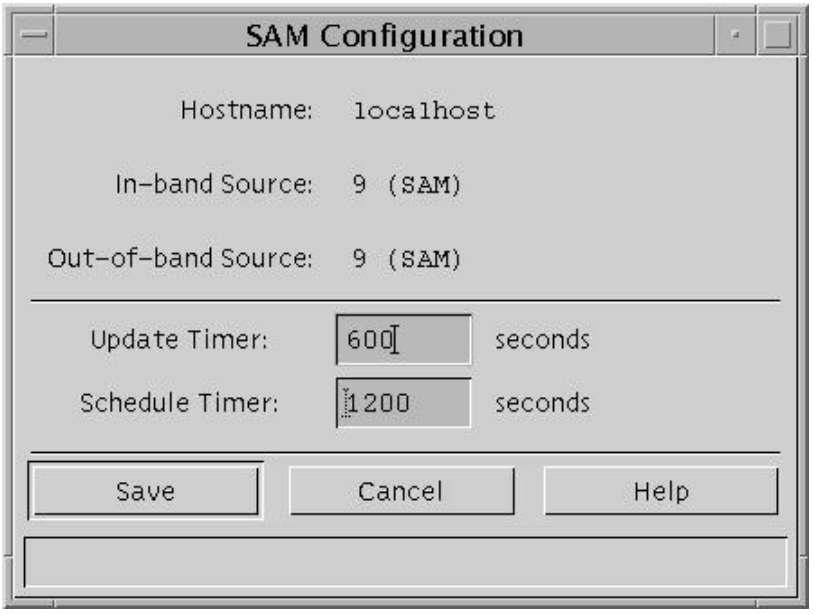
Verifying the SAM Timers

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

Note: These examples show values of **600** and **1200** for the **Update Timer** and **Schedule Timer** fields, respectively, which are the Cisco-recommended values. You should actually set these fields to the values required by your system.

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** or the value required by your system.

b In the **Schedule Timer** field, type **1200** or the value required by your system.



3 Click **Save**.

Configure the CableCARD Server

After you upgrade your system to SR 2.8.1/3.8.1/4.3.1, 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.

Note: Beginning with the upgrade to SR 4.2, the value stored in the Max Key Session Period is multiplied by a factor of 10. This does not change the value received by the CableCARD, however. See CR **46084** for additional information.

Configuring the CableCARD Server

Complete the following steps to ensure that the minimum Set Authorization Time-out Period and Set DeAuthorization Time-out Period fields on the Configure CableCARD Server window are configured correctly. Reference the numbers you recorded when you completed ***Check CableCARD Server*** (on page 20).

1. From the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab and then click **CableCARD**. The CableCARD Data Summary screen opens.
3. Click **Server Configuration**. The CableCARD Data Summary screen updates to display the Server Configuration portion of the screen.
4. Examine the **Authorization Time-out Period** field. Make sure its value is identical to what you recorded in ***Check CableCARD Server*** (on page 20).
5. Examine the **DeAuthorization Time-out Period** field. Make sure its value is identical to what you recorded in ***Check CableCARD Server*** (on page 20).
6. Click **Save CableCARD Server Config**.
7. Click **Exit all CableCARD Screens**.

Check the EAS Configuration—Post Upgrade

Checking the EAS Configuration

After installing the SR 2.8.1/3.8.1/4.3.1 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 Chapter 5, **Testing the EAS**, of *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455).

After completing the procedures in Chapter 5, **Testing the EAS**, of the *Configuring and Troubleshooting the Digital Emergency Alert System, For Use With All System Releases* guide, verify that you can generate an EAS message for the Emergency Alert Controller (EAC), itself.

Check BFS QAM Sessions

The number of BFS sessions after the upgrade needs to be the same as the number of BFS sessions before the upgrade. The procedures in this section guide you through the steps that are required in validating the number of BFS sessions.

Verifying the Number of Recovered BFS Sessions

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

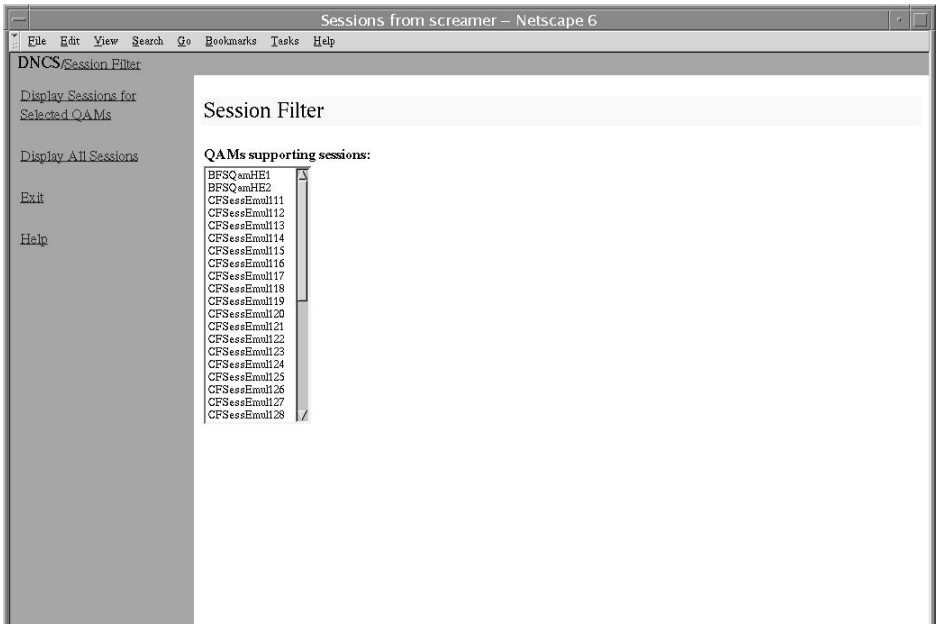
1. Choose one of the following options to check the number of BFS sessions:
   - Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.
   - Type **/dvs/dncs/bin/auditQam -query <IPAddr> 2** and press **Enter**.
     Note: <IPAddr> is the IP address of the data QAM.
2. Does the **Session Count** total equal the number of sessions you recorded in ***Check and Record Sessions*** (on page 27)?
   - If **yes**, skip the remainder of this section, and go to ***Authorize the BRF as a BFS Server (Optional)*** (on page 82). The system recovered all of the BFS sessions.
   - If **no**, go to ***Tear Down BFS and OSM Processes*** (on page 79).

Tear Down BFS and OSM Processes

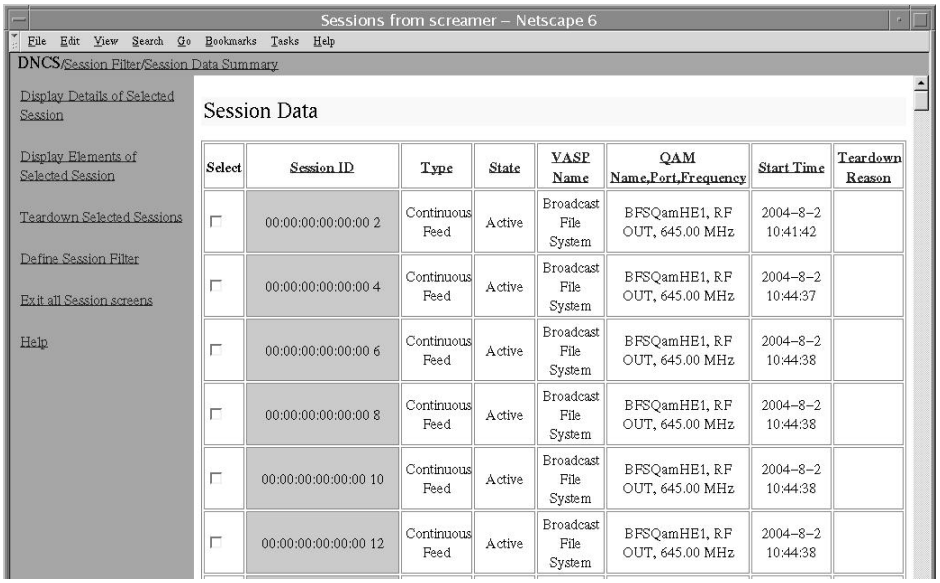
Complete the following steps to tear down the BFS and OSM processes in order to return the BFS session count to the expected number of sessions.

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

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



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



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

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

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

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

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

process.

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

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

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

16 Does the **Session Count** total now equal the number of sessions you recorded in ***Check and Record Sessions*** (on page 27)?

- If **yes**, go to the next procedure in this chapter. The system recovered all of the BFS sessions.
- If **no**, call Cisco Services for assistance.

Authorize the BRF as a BFS Server (Optional)

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.

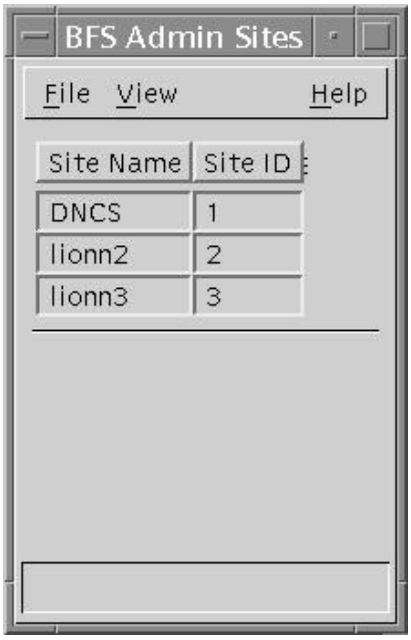
Authorizing the BRF

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)?

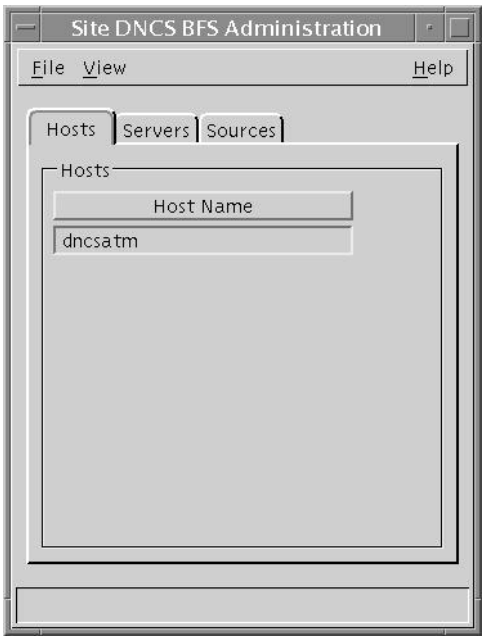
a If **yes**, click **BFS Admin**. The BFS Admin Sites window opens.



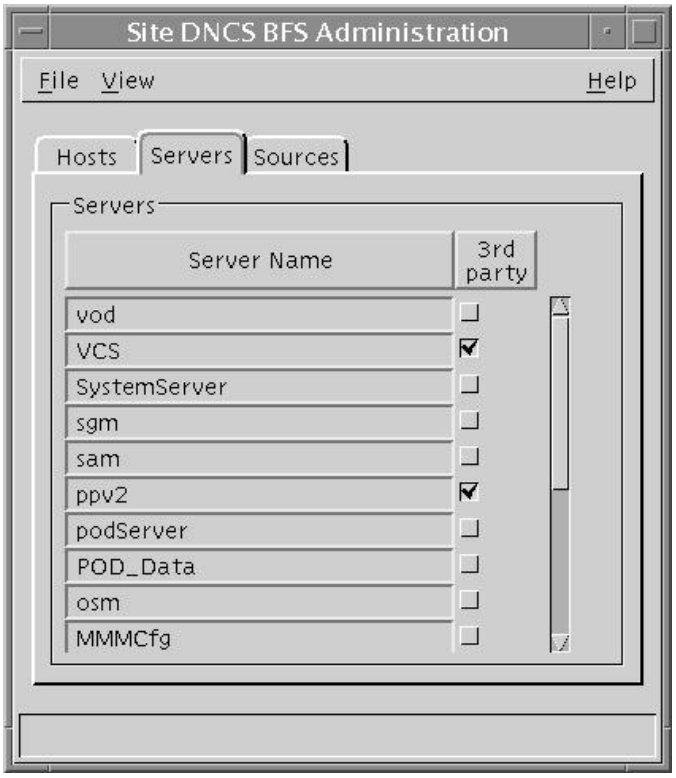
b If **no**, go to step 3.

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 the next procedure in this chapter.

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

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

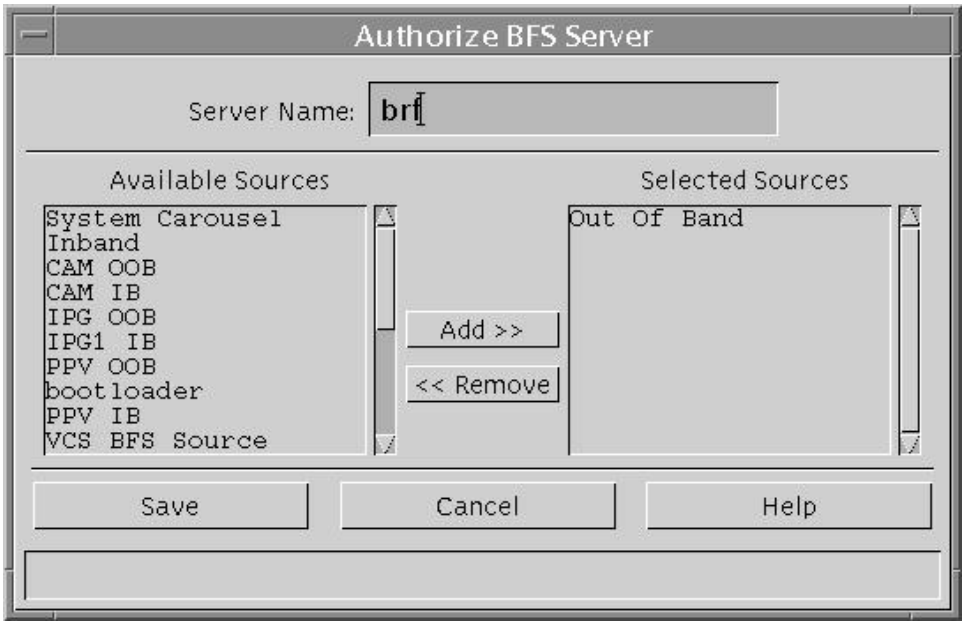
6 Click **File** and then select **New**. The Authorize BFS Server window appears.

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 the next procedure in this chapter.

Restart Basic Backup or Auto Backup Servers

If the site you are upgrading uses the Basic Backup or Auto Backup server and if these server backups were disabled or rescheduled for the upgrade, re-enable the backups now, or change them back to the original schedule.

Final System Validation Tests

Verifying a Successful Installation of SR 2.8.1/3.8.1/4.3.1

Follow these instructions to verify a successful installation of the SR 2.8.1/3.8.1/4.3.1 software. The DHCT(s) that you use for these tests should comply with the following specifications:

- Unauthorized to view a PPV event without specifically buying the PPV event
- Authorized for all third-party applications

Important: 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. Wait 5 minutes.
   c. Press the power button on the DHCT. Power to the DHCT is turned on.
2. Stage at least one new DHCT to the system operator's specifications.
3. After staging, did the DHCT successfully load the current client release software?
   - If **yes**, go to step 4.
   - If **no**, call Cisco Services for assistance.
4. Did the DHCT receive at least 32 EMMs (Entitlement Management Messages) and successfully receive its Entitlement Agent?
   - If **yes**, go to step 5.
   - If **no**, call Cisco Services for assistance.
5. Does the IPG display 7 days of valid and accurate data?
   - If **yes**, go to step 6.
   - If **no**, call Cisco Services for assistance.
6. Do the PPV barkers appear on the PPV channels correctly?
   - If **yes**, go to step 7.
   - If **no**, call Cisco Services for assistance.
7. Do third-party applications load and run properly?
   - If **yes**, go to step 8.

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

8 Can test DHCTs buy a video-on-demand and/or an xOD program?

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

9 If applicable, are the SDV channels available?

- If **yes**, the BRF is successfully authorized.
- If **no**, call Cisco Services for assistance.

Re-Enable the Disk Mirroring Function

In ***Detach Disk Mirrors on the DNCS*** (on page 46), you detached the mirroring function of the DNCS. If your system upgrade appears successful, wait a day to verify that the DNCS functions properly with the new software. Then, re-enable the disk mirroring function so that the DNCS can continue storing identical information across several sets of hard drives.

Important: If your upgrade is unsuccessful, refer to Appendix A, ***SR 2.8.1/3.8.1/4.3.1 Rollback Procedures*** (on page 93).

Re-Enabling the Disk Mirroring Function

Follow these instructions to re-enable the disk mirroring function of the Enterprise 450 or Sun Fire V880 DNCS.

Important: Before following these instructions, wait at least 24 hours after the upgrade to verify that your DNCS operates properly with the new software.

1. From an xterm window on the DNCS, type **su** and then press **Enter**. The **password** prompt appears.
2. Type the root password and then press **Enter**. You have root permissions in the xterm window.
3. Insert the **DBDS Maintenance CD** into the cdrom drive of the DNCS.
4. 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 Controller 2 submirrors.
   Are you certain you want to proceed?
5. 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 to mirror all of the data on the mirrored disks.

Monitoring the Disk-Mirroring Process

The syncwait utility allows engineers to monitor the progress of the disk mirroring process. Follow these instructions to run the syncwait utility.

1. Open another xterm window on the DNCS.
2. Type **syncwait.ksh** and then press **Enter**. The system displays a message stating the percentage of the mirror-synchronization process that is complete.
3. When the system displays the following message, the disk mirroring process is complete; type **n** (for no) and then press **Enter**. The syncwait utility exits.

   No Resync in progress …
   Continue monitoring status? (n,y, or q)
4. Type **q** and then press **Enter** to exit from the monitoring process.
5. 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.
6. Examine the output from the metastat command for the following two conditions, and then go to step 7:
   - The designation **ok** appears in the **State** column next to each metadevice.
   - *No* **Hot Spare** indicates **In Use**.
7. Are *both* of the conditions described in step 6 true?
   - If **yes** (to both conditions), go to step 8; disk mirroring was successfully enabled.
   - If **no** (to either or both conditions), call Cisco Services for help in resolving the issues with disk mirroring.
8. In the xterm window from which you ran the mirrstate –a command, type **eject cdrom** and then press **Enter**. The system ejects the DBDS Maintenance CD.
9. Type **exit** and then press **Enter** to close the xterm window.

4

Customer Information

If You Have Questins

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

SR 2.8.1/3.8.1/4.3.1 Rollback Procedures

In This Appendix

Introduction

This appendix is intended for field service engineers who encounter problems while upgrading an existing digital system to SR 2.8.1/3.8.1/4.3.1. Prior to executing these rollback procedures, contact Cisco Services at 1-866-787-3866.

This appendix contains procedures for rolling back to the SR that was in place prior to the upgrade.

Roll Back the DNCS

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*** (on page 88) procedure in Chapter 3. 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 SR 2.8.1/3.8.1/4.3.1.

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 the ***Stop System Components*** (on page 42) section of Chapter 1, follow the ***Stopping the Application Server*** (on page 42) and ***Stopping the DNCS*** (on page 43) procedures, if necessary.
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 4.3.1.x?

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

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

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

Results:

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

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

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

17 Type **shutdown -y -g0 -i6** and press **Enter** to reboot the server again.

18 Log on to the DNCS as **root** user.

19 Open an xterm window on the DNCS.

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

20 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?

21 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.

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

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

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

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

B

How to Determine the Tape Drive Device Name

In This Appendix

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.

Determine the Tape Drive Device Name

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

Notes:

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

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

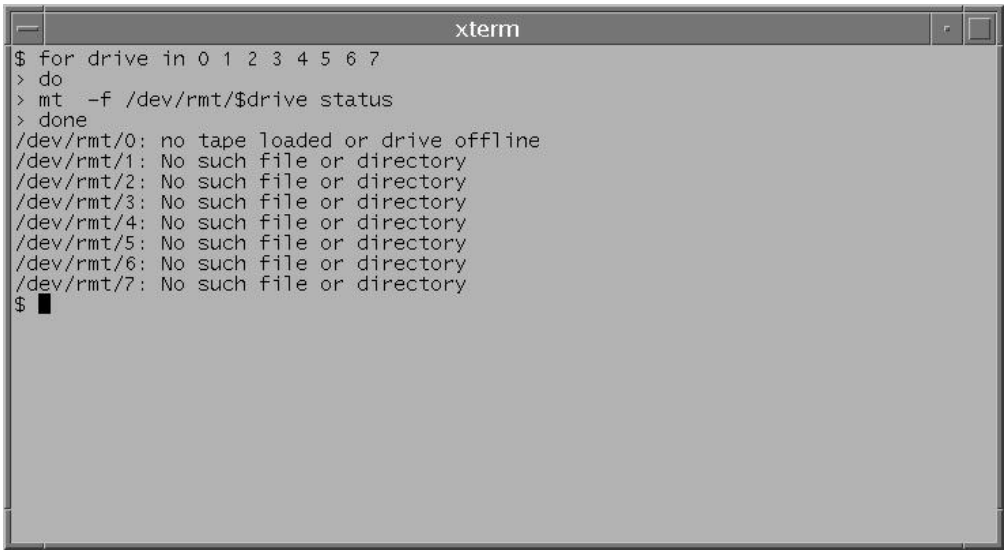
2 Ensure that no tape is currently in your tape drive.

3 Type the following UNIX routine. The system checks the status of eight possible tape drive configurations and displays the results.

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

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

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



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

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

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

_____

C

SSL Configuration for the LoadPIMS Web Service

Introduction

The LoadPIMS web service provides a web service interface to the customer's automation services to programmatically load PIMS files on the DNCS for STB activation. To secure this service on the DNCS, the following two configuration changes have to be performed:

- Enable SSL on the Apache web server
- Setup basic authentication configuration on loadDhctService

The SSL configuration requires server key and certificates. The certificate can be generated using the openssl utilities or the customer can choose to provide these certificates for SSL configuration. These configuration changes are applicable to DNCS SR 4.3.1 with Apache server release 2.0.53.

Note: We also suggest that the same certificate key pair be utilized on each DNCS because of the possibility of the client having to access multiple DNCSs and the maintainability of certificate usage.

In This Appendix

Install the Certificates on the DNCS

Root shell access is required to perform all SSL and Apache web server configuration operations.

The following steps are required to install the SSL certificate on the DNCS:

- A Certificate Signing Request (CSR) is generated on the DNCS and sent to a trusted Certificate Authority (CA).
- The Certificate Authority issues a corresponding digital certificate to be installed on the DNCS. (The root certificate of the CA will probably need to be installed as well.)
- The certificate (along with its corresponding public and private keys) must be manually copied to any other DNCS.

Install the Digital Certificate from the CA

At this point, the following certificate and key files should reside on your system:

- server.crt: The CA-signed server certificate
  Note: See ***Creating a Self-Signed Server Key Certificate*** (on page 120) for creating self-signed certificates.
- server.key: The private server key; this does not require a password when starting Apache
- server.key.secure: The private passphrase protected key

Note: If you do not have the digital certificate files and the server's private key and need to generate one, see ***Generate the CSR*** (on page 123) to create the server.key private file and the procedure to request the Certificate Authority for the digital certificates.

1. Upload the signed server.crt received from the CA on the DNCS server into the /etc/opt/certs/ directory.
2. Type the following command and then press **Enter** to copy the server.crt file to cacert.crt.
   ```
   cp /etc/opt/certs/server.crt /etc/opt/certs/cacert.crt
   ```

Install the Root Certificate of the Trusted Root Authority

If the client certificate authentication is required, then the CA root authority's certificate, which signs the client certificate, should be installed in the /etc/opt/certs/cacert.pem file. We recommended that the CA root certificate be added to this file, but it is not required.

Type the following commands and then press **Enter** to install the root certificate of the trusted root authority.

```
cp /etc/opt/certs/cacert.pem /etc/opt/certs/cacert.pem.`date +%m%d%y`
```

```
cat CA_NSO.crt.txt >> /etc/opt/certs/cacert.pem
```

The following table displays the relevant files and permissions:

File	Permission		Owner: Group	Comments
server.key	400	-r--------	root:root	This is the private key generated on the DNCS (first step in the ***Generate the CSR*** (on page 123) process). If you want to skip the Generate the CSR process and use the same dncs_server.csr.crt received from the NSO on all DNCSs, you need to copy the server.key file to all other DNCS controllers. Please note that this file does not contain the passphrase, and consequently should be guarded appropriately. One way to copy this file from a configured DNCS controller to another DNCS being configured would be to copy the server.key.secure file instead. However you will need the passphrase that was used when extracting the server.key file (***Generate the CSR*** (on page 123) first step) from the server.key.secure file.
server.crt	444	-r--r--r--	root:root	This is the dncs_server.csr.crt file renamed as server.crt.

File	Permission		Owner: Group	Comments
server.key.secure	400	-r--------	root:root	This file is a passphrase-protected server key, suitable for copying/backup etc. The following command extracts the server.key file if you choose to copy server.key.secure from another DNCS (and did not copy the server.key file): `openssl rsa –in server.key.secure –out server.key`
cachain.crt	444	-r--r--r--	root:root	This can be the same as server.crt so you can copy server.crt onto cachain.crt.
cacert.pem	444	-r--r--r--	root:root	The CA_NSO.crt file is concatenated into this file by this command: `cp /etc/opt/certs/cacert.pem /etc/opt/certs/cacert.pem.`date +%m%d%y` cat CA_NSO.crt.txt >> /etc/opt/certs/cacert.pem`

Configure Apache to Allow the Client Connection

Create the Directive for the loadPIMS Service

1 Use a text editor to create the /etc/apache2/conf/loadPIMS.https file with the following directives.

Note: If this file already exists, see ***Configure Client IP Addresses for the loadPIMS Service*** (on page 108) to allow a connection to the loadPIMS web service.

Example: The file should look similar to the following example:

```
<Location /dncs/soap/loadPIMS>
   # SSLVerifyClient none
   # SSLCipherSuite      +ADH-RC4-MD5
   ProxyPass
   http://localhost:18284/dncs/soap/loadPIMS
   ProxyPassReverse
   http://localhost:18284/dncs/soap/loadPIMS
   Order Deny,Allow
   Allow from localhost
   Allow from dncs
   Allow from appservatm
   #Allow from client_ip
   Deny from all
</Location>
```

Note: Port number 18284, used in the example, should match with the value of the **SERVER_PORT** variable in the /dvs/dncs/etc/LoadDhctServerSOAPCfg.cfg file.

2 Comment out, if applicable, the following lines in rpcserver.conf file:

```
#ProxyPass         /dncs/soap/loadPIMS
http://localhost:18284/dncs/soap/loadPIMS
#ProxyPassReverse  /dncs/soap/loadPIMS
http://localhost:18284/dncs/soap/loadPIMS
```

Configure the WS-BOSS Directives

This configuration step is optional and is only required if access to the WS-BOSS interface is desired. The WS-BOSS configuration is performed through the /etc/apache2/conf/boss.http file. Note that in systems older than SR 4.5, the WS-BOSS configuration is maintained in the rpcserver.conf file. If your system has the rpcserver.conf file, follow these steps.

1 Comment out the following lines in rpcserver.conf file:

```
#ProxyPass         /dncs/soap/bossreq
http://localhost:18084/dncs/soap/bossreq
#ProxyPassReverse  /dncs/soap/bossreq
http://localhost:18084/dncs/soap/bossreq
```

2 Use a text editor to create the /etc/apache2/conf/boss.http file with the following directives:

```
<Location /dncs/soap/bossreq>
   # The SSL configuration is not supported prior to 4.5
   #SSLVerifyClient      require
   #SSLVerifyDepth       5
   ProxyPass     http://localhost:18084/dncs/soap/bossreq
   ProxyPassReverse
   http://localhost:18084/dncs/soap/bossreq

   # The following directives will not be present after 4.5
as client-cert
   # authentication will be used. This should be present if
client access to WS-BOSS
   # over HTTP is required.
   Order Deny,Allow
   Allow from localhost
   Allow from dncs
   Allow from appservatm
   #Allow from client_ip
   Deny from all
</Location>
```

Note: Requests to these relative URLs will be defined unless an *allow* is specifically added to allow a client to connect to the Apache server. The following procedure, **Configure Client IP Addresses for the loadPIMS Service**,

details how to add a client's IP address to the list of IP addresses allowed to connect to the DNCS web services.

Configure Client IP Addresses for the loadPIMS Service

1. Obtain a list of client IP addresses that will be connecting to the DNCS server.
2. Open the /etc/apache2/conf/loadPIMS.https file and find the section with the <Location /dncs/soap/loadPIMS> directive. Add those client IP addresses there, according to the following example:

```
<Location /dncs/soap/loadPIMS>
   #SSLVerifyClient none
   #SSLCipherSuite +ADH-RC4-MD5
            Order Deny, Allow
            Allow from localhost
            Allow from dncs
            Allow from appservatm
   #Allow from client_ip
         Allow from client_ip1
         Allow from client_ip2
         Deny from all
</Location>
```

Note: This example shows the addition of **client_ip1** and **client_ip2** to the list of clients that are allowed to access the server.

Configure the Client IP Addresses for the WS-BOSS

The SSL is currently not supported for the WS-BOSS interface. If no WS-BOSS support is required, ignore this section. Otherwise, the file /etc/apache2/conf/boss.http needs to be edited to add the client IP addresses, according to the following example:

```
<Location /dncs/soap/bossreq>
      # The SSL configuration is currently not supported
      #SSLVerifyClient      require
      #SSLVerifyDepth       5
      ProxyPass
      http://localhost:18084/dncs/soap/bossreq
      ProxyPassReverse
      http://localhost:18084/dncs/soap/bossreq


      # The following directives will not be present after 4.5
as client-cert
      # authentication will be used. This should be present if
client access to WS-BOSS
      # over HTTP is required.
      Order Deny,Allow
            Allow from localhost
            Allow from dncs
            Allow from appservatm
      #Allow from client_ip
            Allow from client_ip1
            Allow from client_ip2
      Deny from all
</Location>
```

Note: This example shows the addition of client_ip1 and client_ip2 to the list of clients that are allowed to access the WS-BOSS service.

Required Changes to the /etc/apache2/httpd.conf File

Add a new Import directive within the <VirtualHost *:80 *:8045> directive, just before the </VirtualHost> line. Use the following example as a guide:

```
<VirtualHost *:80 *:8045>
    #
    # "/var/apache2/cgi-bin" should be changed to whatever
your ScriptAliased
    # CGI directory exists, if you have that configured.
    #
    # Allow cgi-bin access only on local box or if
authenticated
     <Directory "/var/apache2/cgi-bin">
               AllowOverride None
          Options None
               Order Allow,Deny
               Allow from all
     </Directory>
     <Location />
           Order Allow,Deny
           Allow from localhost
           Allow from dncs
           Allow from appservatm
           ErrorDocument 403 "<html><head><title>Error
403</title></head><body><h2>SECURITY WARNING</h2>Web
connections are only allowed from localhost.</body></html>"
     </Location>
Include /etc/apache2/conf/*.http
</VirtualHost>
```

Enable the Secure Socket Layer (SSL) with Apache2

Required Changes to the /etc/apache2/ssl.conf File

The following table shows the SSL configuration properties that are modified in the ssl.conf file:

SSL Configuration Parameters

ssl.conf variables		
SSLCipherSuite		Need to add ADH-RC4-MD5
SSLCertificateFile	/etc/opt/certs/server.crt	
SSLCertificateKeyFile	/etc/opt/certs/server.key	
SSLCertificateChainFile	/etc/opt/certs/cachain.crt	The server certificate CA certificate chain. This file must contain the entire CA certificate chain used to sign the server certificate. The NSO CA certificate should be added to this file.
SSLCACertificateFile	/etc/opt/certs/cacert.pem	The certificate authority's certificates should be placed in here, if certificate-authentication for the client is required. This may be required for the billing interface (SR 4.5).

The following steps outline the changes required to enable SSL on the DNCS server. Be sure that you are root user.

1 Follow these instructions to disable the Apache2 service on a Solaris 10 system.

   a Type **svcs -a | grep apache** and then press **Enter**.

   b Do the results from step a show that the Apache2 service is running (online)?

   Example: `online 0:45:44 svc:/network/http:apache2`

   – If **yes**, type **svcadm disable apache2** and then press **Enter**.

   – If **no**, go to step 2.

2 Type the following commands and then press **Enter** to enable SSL using svccfg.

```
svccfg
svc:> select apache2
svc:/network/http:apache2> listprop httpd/ssl
httpd/ssl boolean false
svc:/network/http:apache2> setprop httpd/ssl = true
svc:/network/http:apache2> exit
```

3 Edit the /etc/apache2/ssl.conf file and modify the "SSLCipherSuite" property to add "ADH-RC4-MD5". This enables the CipherSuite ADH-RC4-MD5 on the Apache service. The updated line should look like this example:

```
SSLCipherSuite ALL:!EXPORT56:-AES256-SHA:-DHE-RSA-AES256-
SHA:-DHE-DSS-AES256-SHA:RC4+RSA:+ADH-RC4-
MD5:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

Note: The default attribute of the SSLCipherSuite is `'ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP''`. This is being changed to allow Anonymous Diff-Hellman key exchange, RC4 encoding, and the MD5 digest algorithm as per the loadPIMS ICD. The ADH-RC4-MD5 digest algorithm should be preserved for all future versions of the DNCS. The default '!ADH' does not allow ADH to be added again and should be removed.

4 Follow these instructions to edit the ssl.conf file.

Note: A bug in the Apache 2.0.53 code requires that this edit be made.

a Type the following command and then press **Enter**.

```
cp ssl.conf  ssl.conf.`date +%m%d%y`
```

b Open the ssl.conf file in a text editor.

c Search for the following entry:

```
VirtualHost _default_
```

d Change the entry to `<VirtualHost *:443>`.

```
:%s/VirtualHost _default_/VirtualHost */
```

e Search now for `ServerName acme:443 or ServerName %%%localhost%%%:443`.

f Change the entry to `ServerName <hostname>:443`.

g Save and close the file.

5 Add a new Location and Import directive within the <VirtualHost *:443> directive, just before the </VirtualHost> line. The changes should look like the following example:

```
<VirtualHost *:443>
   # contents omitted below
   .
   .
   <Location />
            Order Deny,Allow
            Allow from localhost
            Allow from dncs
            Deny from all
            ErrorDocument 403 "<html><head><title>Error
403</title></head><body><h2>SECURITY WARNING</h2>Web
connections are only allowed from localhost.</body></html>"
        </Location>
   Include /etc/apache2/conf/*.https
</VirtualHost>
```

6 Test the configuration changes, before the Apache service is refreshed, by typing the following command and then pressing **Enter**.

Important: The message **Syntax OK** should then appear.

```
/usr/apache2/bin/httpd -t
```

7 Follow these instructions to restart the Apache2 service.

a Type `svcadm refresh apache2` and then press **Enter**.

b Type `svcadm clear apache2` and then press **Enter**.

Note: If the Apache service is not in an error state, you will see the following message:

```
svcadm: Instance "svc:/network/http:apache2" is not in a
maintenance or degraded state.
```

c Type `svcadm enable apache2` and then press **Enter**.

8 Type **cd /etc/opt/certs** and then press **Enter**.

9 Type the following command and then press **Enter** to create the necessary link.

```
ln -s /etc/opt/certs/server.crt  cachain.crt
```

10 Is client authentication required on this system?

- If **yes**, type `cp server.crt cacert.pem` and then press **Enter**.
- If **no**, comment out in the ssl.conf file the line that includes SSL VerifyClient.

11 Type `ps -ef | grep apache2` and then press **Enter** to verify the Apache2 process is running with SSL.

Example: A message similar to the following should appear:

```
dncs 18058 18054  0 00:45:45 ?   0:00
/usr/apache2/bin/httpd -k start -DSSL
root 18054  1   0 00:45:44 ?  0:03 /usr/apache2/bin/httpd -
k start -DSSL
```

12 Type the following command and then press **Enter** to verify that SSL processing is active.

```
openssl s_client -cipher ADH-RC4-MD5 -connect localhost:443
-state -debug
```

Example: Output similar to the following should appear:

```
CONNECTED(00000004)
SSL_connect:before/connect initialization
write to 0008E7D8 [0008EDE8] (46 bytes => 46 (0x2E))
0000 - 80 2c 01 03 01 00 03 00-00 00 20 00 00 18 23 98
.,........ ...#.
0010 - 3d 9f 16 9f 4c 09 90 92-fe 94 36 81 09 6d e0 b4
=...L.....6..m..
0020 - e1 92 03 52 48 df 2c 57-42 9a 48 f3 98 a1
...RH.,WB.H...
SSL_connect:SSLv2/v3 write client hello A
read from 0008E7D8 [00094348] (7 bytes => 7 (0x7))
0000 - 16 03 01 00 4a 02
....J.
0007 - <SPACES/NULS>
read from 0008E7D8 [0009434F] (72 bytes => 72 (0x48))
0000 - 00 46 03 01 4b 7c 7b a6-99 60 bb 97 1a a6 63 3c
.F..K|{..`....c<
0010 - 86 b0 11 13 a3 8d 53 72-24 aa 68 62 e5 f5 ae 91
......Sr$.hb....
0020 - 80 aa 06 c3 20 49 36 a9-0e fb cf 7a aa 96 c1 21
.... I6....z...!
```

```
0030 - d1 55 75 3a 22 2e 57 cb-1b 4b 2d 88 88 11 43 de
.Uu:".W..K-...C.
0040 - 31 6c 71 84 5d 00 18
1lq.]..
0048 - <SPACES/NULS>
SSL_connect:SSLv3 read server hello A
read from 0008E7D8 [00094348] (5 bytes => 5 (0x5))
```

Note: If this command generates an error, refer to ***Troubleshooting SSL*** (on page 119).

13 Open a browser from a client that is allowed to connect to the DNCS server and type in the IP address of the DNCS. Verify the server certificate.

Enable Client Certificate Authentication

This is an optional step in the SSL configuration and is only required if a client-certificate authentication is needed.

1. Log in to the DNCS as **root** user.
2. Type `cd /etc/opt/certs` and then press **Enter**.
3. Type `cp server.crt  cacert.pem` and then press **Enter** to copy the server.crt file to cacert.pem.

Set Up the loadDhctService for Basic Authentication

Complete these instructions as dncs user.

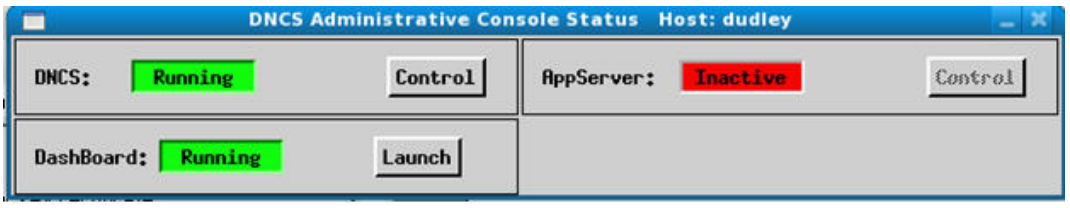
The configuration file for the loadDhctService process is located at: /dvs/dncs/etc/LoadDhctServerSOAPCfg.cfg. A sample portion of the file follows:

```
# Port on which server listens for incoming requests
SOAP_PORT = 18284
# Enable/Disable SOAP SSL
SSL_MODE = DISABLE
# Enable or Disable basic authentication (parameters:
DISABLE/ENABLE)
BASIC_AUTH = ENABLE
# Server User Name
SERVER_USER_NAME = dncs
# Server Password
SERVER_PASSWD = dncs123
```

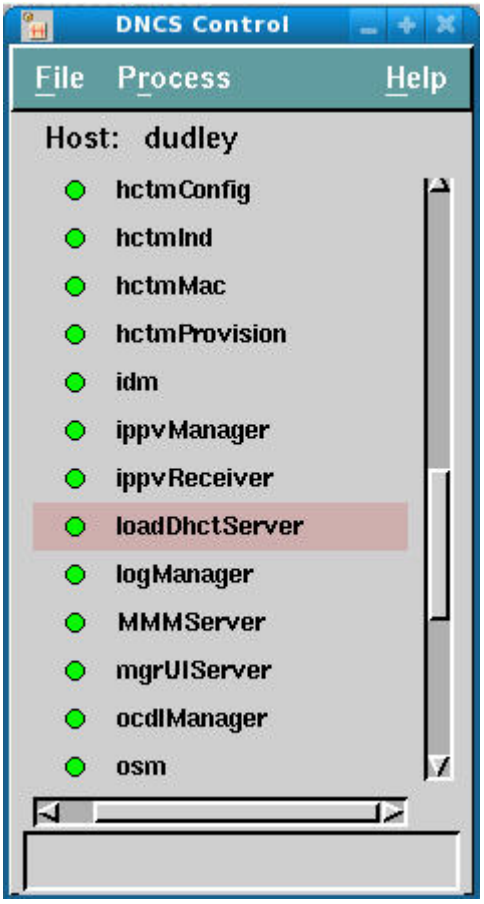
The following list contains a description of the parameters:

- **Server_Port (SOAP_PORT) —** This is the port on which the loadDhctServer listens. This is the proxy port in the loadPIMS.https Apache configuration file.
- **SSL_MODE —** This should always be set to **DISABLE**. The SSL is enabled at the Apache server layer.
- **BASIC_AUTH —** Set it to **ENABLE**.
- **SERVER_USER_NAME —** This configuration parameter defines the user name used by the loadDhctService web service client to perform basic authentication.
- **SERVER_PASSWD —** This configuration parameter defines the password to be used by the client for basic authentication.

1 Launch the DNCS Control processes by clicking **Control** from the DNCS Administrative Console Status window.



2 Highlight the **loadDhctServer** process from the DNCS Control window.



3 Click **Process** and then select **Start Process** to start the loadDhctServer process.

Note: When this procedure is complete, configure the client to use basic authentication over SSL with the user-id and password specified in the /dvs/dncs/etc/LoadDhctServerSOAPCfg.cfg file.

Troubleshooting SSL

- `svcs -a | grep apache2`
  If the output of this command does not list the Apache2 server as being online, the httpd process needs to be killed. Follow these instructions to kill the httpd process.
  a Type `ps -ef | grep httpd` and then press **Enter**.
  b Type `kill [PID]` and then press **Enter**, where [PID] is the process ID returned by the previous command.
- `openssl: not found` error
  If the **openssl** command is not available in the PATH variable, then the path to openssl has to be explicitly specified. The openssl tool is located in the following directory: /usr/sfw/bin/openssl
- If the CSR generation with the aes256 option fails with an error about SUNWcry, then generate the 3DES key by typing the following command and then pressing **Enter**.
  `openssl genrsa -des3 -out server.key 1024`
- If the **openssl** s_client command (step 12 of ***Required Changes to the /etc/apache2/ssl.conf File*** (on page 111)) generates an error, try this command instead.
  `openssl s_client -connect localhost:443 -state -debug`
  If this command is successful, it probably is because the SSLCipherSuite is not configured correctly. Retry the command in bullet 3 and refresh the Apache server.

Good to Know

Creating a Self-Signed Server Key Certificate

Complete the following steps to generate a self-signed certificate. Alternatively, an existing SSL key and certificate can be used.

Note: Execute all commands as root user in an xterm window on the DNCS.

1. Follow these instructions to add the path for the openssl command.
   a. Type `PATH=$PATH:/usr/sfw/bin` and then press **Enter**.
   b. Type `export PATH` and then press **Enter**.
2. Type `cd /etc/apache2` and then press **Enter**.
3. Type the following command and then press Enter to create the server key and certificate.
   ```
   openssl genrsa -out /etc/opt/certs/server.key 1024
   ```
   Note: Additionally, the key encryption format and number of bits in the key can be specified. The following are possible key encryption types:
   - **des** — encrypt the generated key with DES in cbc mode
   - **des3** — encrypt the generated key with DES in ede cbc mode (168 bit key)
   - **aes128**, **aes192**, **aes256** — encrypt PEM output with cbc aes

   Typical values for the number of bits in the key are 1024, 2048, and 4096.
4. Type the following command and then press **Enter** to generate a Certificate Signing Request:
   ```
   openssl req -new -key /etc/opt/certs/server.key -out
   /etc/opt/certs/server.csr
   ```
5. If you want to sign the certificate yourself, (this will generate a certificate that will not expire), type the following command and then press **Enter**.
   ```
   openssl x509 -req -in /etc/opt/certs/server.csr -
   signkey /etc/opt/certs/server.key -out
   /etc/opt/certs/server.crt
   ```
6. Type the following command and press **Enter** to copy the server.crt file to cacert.crt:
   ```
   cp /etc/opt/certs/server.crt /etc/opt/certs/cacert.crt
   ```
7. Is client authentication required?
   - If **yes**, follow the steps outlined in ***Enable Client Certificate Authentication*** (on page 116).

- If **no**, you are finished with this procedure.

Example of Basic Authentication

The following is an example with **ResetStagingState**:

```
GET /dncs/loadPIMS HTTPS/1.0
Host: localhost
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
 xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:loadPIMS="urn:loadPIMS.xsd">
 <SOAP-ENV:Body>
  <loadPIMS:ResetStagingState>
   <loadPIMS:resetStagingStateRequest>
    <loadPIMS:dhctMacAddress></loadPIMS:dhctMacAddress>
   </loadPIMS:resetStagingStateRequest>
  </loadPIMS:ResetStagingState>
 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

In this example, the userid and password (Aladdin:open sesame) is encoded as a base64 string. Refer to the **Order Management ICD** for further details about the authentication mechanisms.

Trust Management on the Client

If you want to disable the validation of certificates for testing purposes, you need to override the default trust manager with one that trusts all certificates. Use this as an example.

```
// Create a trust manager that does not validate certificate
chains
TrustManager[] trustAllCerts = new TrustManager[]{
    new X509TrustManager() {
        public java.security.cert.X509Certificate[]
getAcceptedIssuers() {
            return null;
        }
        public void checkClientTrusted(
            java.security.cert.X509Certificate[] certs, String
authType) {
        }
        public void checkServerTrusted(
            java.security.cert.X509Certificate[] certs, String
authType) {
        }
    }
};


// Install the all-trusting trust manager
try {
    SSLContext sc = SSLContext.getInstance("SSL");
    sc.init(null, trustAllCerts, new
java.security.SecureRandom());

HttpsURLConnection.setDefaultSSLSocketFactory(sc.getSocketFact
ory());
} catch (Exception e) {
}


// Now you can access an https URL without having the
certificate in the truststore
```

```
try {
    URL url = new URL("https://hostname/index.html");
} catch (MalformedURLException e) {
}
```

Generate the CSR

1 Type the following command and then press **Enter** to create the request with an aes256 certificate. (You will be asked to create a passphrase.)

```
openssl genrsa -aes256 -out server.key 1024
```

Note: On the SR 4.3.1 DNCS system, you may receive an error about SUNWcry. In this case you can alternatively create a request with a 3DES key (you will be asked to create a passphrase). See ***Troubleshooting SSL*** (on page 119) (third bullet) for more details.

2 Type the following command and then press **Enter** to generate the CSR using the server.key.

```
openssl req -new -key server.key -out server.csr
```

Note: You will be asked to provide subject fields for the CSR, which include the following:

- **Country Name:** US
- **State:** Pennsylvania
- **Locality Name:** Philadelphia
- **Organization Name:** Comcast Cable Communications Management LLC
- **Organizational Unit Name:** CET
- **Common Name:** [FQDN such as: service.comcast.net]
- **Email Address:** admin@cable.comcast.net
- **A challenge password:** .[input a period "." to leave blank and not use the default]
- **An optional company name:** .[input a period "." to leave blank and not use the default]

3 Type the following commands and then press **Enter** to examine the server.key and the certificate request. (You will be asked to enter the passphrase for server.key)

```
openssl rsa  -text -in server.key
openssl req  -text -in server.csr
```

4 Email the server.csr to the Certificate Authority. Some CAs provide a website to paste the content of the CSR on their website. Then email yourself the signed certificate.

5 Type the following commands and then press **Enter** to create a server key which doesn't cause Apache to prompt for a password.

```
openssl rsa -in server.key -out server.key.insecure
mv server.key server.key.secure
mv server.key.insecure server.key
```

Important: Although this means that you don't have to type in a password when restarting the Apache server, it does mean that anyone obtaining this insecure key will be able to decrypt your transmissions. Guard it for permissions very carefully.

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

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

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc. trademarks used in this document.
Product and service availability are subject to change without notice.

© 2010, 2012 Cisco and/or its affiliates. All rights reserved.

June 2012 Printed in USA

Part Number 4036043 Rev B