System Release 2.7/3.7/4.2 Service Pack 0.2

Release Notes and Installation Instructions

Please Read

Important

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

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

CableCARD is a trademark of Cable Television Laboratories, Inc.

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

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

Publication Disclaimer

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

Copyright

Contents

About This Guide

Introduction

System Release 2.7/3.7/4.2 Service Pack 0.2 (SR 2.7/3.7/4.2 SP 0.2) is the latest DNCS release that provides combo-binding support for separable security (SSC) host set-tops, DNCS database support for new organizational unique identifiers (OUIs), and emergency patches that have been developed since the release of SR 2.7/3.7/4.2.

Audience

This document was written for Digital Network Control System (DNCS) operators. Cisco field service engineers and Cisco Service engineers may also find the information in this document helpful.

Read Me

Please read this entire guide before beginning the upgrade. If you are uncomfortable with any of the procedures, contact Cisco Services for assistance.

Important: Complete all 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 the DBDS network need the following skills:

- Advanced knowledge of UNIX
- Experience with the UNIX vi editor. Several times throughout the 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

Related Publications

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

- *Configuring and Troubleshooting the Digital Emergency Alert System (part number 4004455)*
- *DBDS Backup and Restore Procedures For SR 2.2 Through 4.2* (part number 4013779 Revision A)
- *DBDS Utilities Version 6.1 Installation Instructions and DNCS Utilities User's Guide* (part number 4020695)
- *Installing the SAI Tools Patch* (part number 4018566)
- *Recommendation for Setting System Information to Out-of-Band* (part number 738143)
- *Recommended Patch for All DBDS Platforms Using Solaris 10* (part number 4015090)
- *RNCS Installation and Upgrade Instructions* (part number 4003191)
- *Separable Security Host Staging Guide* (part number 736107)

Document Version

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

Description	See Topic
Added CRs 70590 and 70989	***Known Issues*** (on page 9)
Added new sections to ***Post-Upgrade Procedures*** (on page 49)	***Configure the CableCARD Server*** (on page 50); ***Reinstall the NMI Software*** (on page 55)

1

Introducing System Release 2.7/3.7/4.2 SP 0.2

Introduction

This chapter provides important system information, major improvements, and beneficial operational changes for the DNCS. This chapter also describes the key feature in this release—support for SSC binding. Review this chapter to learn about this latest software release.

In This Chapter

Support for Separable Security Set-Tops

Introduction

The Federal Communication Commission requires that, after July 2007, no set-top boxes are to be deployed using embedded security. In response to this mandate, Cisco has begun producing and distributing set-tops that require PowerKey® CableCARD™ modules for all conditional access security. Cisco has also modified the DNCS to support a method of binding a CableCARD module to the associated host set-top without user interaction or two-way staging. This binding process is known as combo-binding.

Combo-Binding

Combo-binding is a process that the SSC DHCT and CableCARD module pair go through after the CableCARD module downloads its EMMs. The process is as follows.

1. The SSC DHCT and its paired CableCARD module exchange keys to authenticate each other.
2. The DNCS sends the pairing information (as a file named pod_data) to the BFS. The POD_Data file contains two lists: an authorized list and an unauthorized list. Each list contains information on the SSC DHCT and its paired CableCARD module.

   Note: The DNCS populates its database with the SSC pairing information from the inventory file during the batch load process.
3. The CableCARD module reads the pairing information from the file. If the CableCARD module finds its SSC pairing in the authorized list, it authorizes the binding between it and the SSC host. If it finds its SSC pairing in the unauthorized list, or if it does not find its SSC pairing in either list, it does not authorize the binding.

You do not need to turn combo-binding "on." It is an automatic process available for SSC DHCTs as long as you load the correct DHCT types, have the correct EMMs, and have one of the following System Releases:

- SR 2.5/3.5/4.0 Service Pack 3 (and later)
- SR 2.7/3.7/4.2 Service Pack 0.2 (and later)
- SR 2.8/3.8/4.3

Support New OUIs in the DNCS Database

Recently, Cisco began manufacturing CableCARD modules with the new OUI 00:1A:C3. Beginning with this system release, this OUI is supported in the DNCS database.

Note: OUIs refer to the first three octets of a MAC address. Within each range of MAC addresses there are several million unique addresses.

Implemented Change Requests

This list highlights some of the major improvements to the DNCS since the release of SR 2.7/3.7/4.2. Contact your Cisco marketing manager for additional details on any of these change requests (CRs).

CR 62542: DSM Process on DNCS No Longer Crashes

Cisco has corrected a condition that caused an occasional crash of the DSM process on the DNCS.

CR 63755: QAM Channels Calculate Bandwidth Correctly After Reboot

When a QAM modulator reboots, the bandwidth is calculated correctly for the QAM channels.

CR 63777: DRM Process Allocates Bandwidth to a Third-Party QAM Channel

If the DNCS operator is selecting a third-party QAM channel from a service group, the DRM process now correctly allocates bandwidth.

CR 63897: DRM Process Releases a Third-Party QAM Session

When a session for a third-party QAM is released, the DRM process handles the release correctly.

CR 63957: Adding or Deleting QAM Ports No Longer Causes the bfsRemote Process to Go into a Recovery State

If the DNCS operator is adding and deleting several QAM ports to a service group, the bfsRemote process no longer goes into a recovery state and set-tops continue to receive information from the DNCS.

CR 64409: The qamManager Logs No Longer Show Errors If Changes are Made on the QAM GUI

If the DNCS operator makes changes on the QAM GUI, the changes save correctly and the qamManager logs do not show errors.

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

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

CR 64714: Enabling SSP2.3 Support Allows Third-Party QAMs to Receive the Correct Program Number

Third-party QAMs now receive the correct program number if SSP2.3 support is enabled, which allows subscribers to see video.

CR 66380: Rogue Wave Libraries Are Updated

The Rogue Wave libraries are now updated to include the new U.S. daylight saving time (DST) rules that became effective on March 11, 2007.

CR 67052: Split Channels Display Correctly During DST

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

Site Requirements

Introduction

This section provides the following information:

- Identifies the CDs that are needed to install with this software release
- List the software components tested and released as part of this software release
- Provides the antecedents and prerequisites required before installation

Antecedents

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

Prerequisites

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

- SR 2.7/3.7/4.2 or SR 2.7/3.7/4.2 Service Pack 0.1 is currently installed on your system.
- You have the CD labeled **DBDS Maintenance CD 3.0.14** (or later) in order to complete the required backups of the database and the filesystem.

  Note: DBDS Maintenance CD 3.0.14 is the minimum version that is certified for SR 2.7/3.7/4.2.
- You have two CDs labeled similarly to **Solaris Patches**.
- Sites that are using the RNCS component of the DBDS need the DVD labeled similarly to **RNCS Install DVD.**

  Note: Note that this is a DVD and not a CD.
- DBDS Utilities Version 5.1.x or later is installed on your system.

System Release Compatibility

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

- DNCS Application 4.2.0.24p2.1
- DNCS GUI/WUI 4.2.0.24p2
- DNCS/AppServer Tools 4.2.0.13p1

This software can be applied to DBDS networks operating at SR 2.7, 3.7, or 4.2.

For a list of all available patches to date for SR 2.7, 3.7, or 4.2, please contact Cisco Services.

Application Platform Release Dependencies

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

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

Set-Top Platform	Operating System (OS)	SARA*	PowerKEY Conditional Access Version
Explorer 8300 DVR v. 1.4.3a10 (or later) v. 1.5.2	 OS 6.14.74.1 OS 6.14.79.1	 1.88.22.1 1.89.16.2	 3.9 3.9
Explorer 8000/8010 DVR v. 1.4.3a10 (or later) v. 1.5.2	 OS 6.12.74.1 OS 6.12.79.1	 1.88.22.1 1.89.16.2	 3.7.5 3.7.5
Explorer 3250HD HD 1.6.0 (or later)	OS 3.24.5.2	1.59.18.1	3.9
Explorer 2xxx, 31xx, 3200, 3100HD	OS 3.13.6.1	1.60.6.2	1.0.6.20 (Explorer 2000s) 1.0.7 (all others)

* *Cisco Resident Application*

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

Server Platforms

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

DNCS

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

Application Server

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

Known Issues

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

CR 64735: The siManager Process Intermittently Core Dumps

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

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

If the image ID of a CVT file is greater than 32,000 and that image ID is associated to a software download for a group of DHCTs that also has a default group, both the default group and the download group receive the same CVT image.

Workaround: A software patch is currently in development at Cisco. Contact your North American Marketing manager for further details.

CR 69674: The modDhctConfig Message Contains 300 Messages

Currently, the billing system can create a large number of modDhctConfig messages and send them to the DNCS. The DNCS can process a large number of messages. However, the modDhctConfig message can only contain a maximum of 300 packages.

CR 70590: Error 218 Occurs on a GQAM

Error 218 occurs if there is a stranded session on the GQAM. This error allows new VOD session requests to fail on the DNCS.

Workaround: Run auditQAM utility to correct this error condition.

CR 70989: A Service Group is Created for Each RF Port

The DNCS automatically creates a service group for each RF port on a table-based QAM.

2

DNCS Pre-Upgrade Procedures

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

The first several procedures of this chapter can be completed before the maintenance window begins, while the actual upgrade of DNCS software must be completed during a maintenance window. See ***When to Complete These Procedures*** (on page 12) for a list of those procedures that can be completed before the start of the maintenance window.

In This Chapter

When to Complete These Procedures

Upgrade Process

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

Complete These Procedures

Pre-Maintenance Window

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

- ***Verify the Integrity of the CDs*** (on page 13)
- ***Check Available Disk Space*** (on page 14)
- ***Run the Doctor Report*** (on page 15)
- ***Check the EAS Configuration—Pre-Upgrade*** (on page 16)
- ***Collect Network Information*** (on page 17)
- ***Back Up the DNCS and Application Server File Systems*** (on page 19)
- ***Verify DBDS Stability*** (on page 20)
- ***Back Up the Informix Database*** (on page 21)

During the Maintenance Window

At the beginning of the maintenance window, you should start with ***Suspend Billing and Third-Party Interfaces*** (on page 22) and complete all of the remaining procedures in Chapter 2. You should also complete the procedures in Chapter 3 during the same maintenance window.

Verify the Integrity of the CDs

Complete the following steps for each CD contained in the software binder.

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 **cd /cdrom/cdrom0** and then press **Enter**. The /cdrom/cdrom0 directory becomes the working directory.
5. Type **ls -la** and then press **Enter**. The system lists the contents of the CD.
6. Did the system list the contents of the CD as expected?
   - If **yes**, go to step 7.
   - If **no**, the CD might be defective. Call Cisco Services for assistance.
7. Type **pkgchk -d . SAI*** and then press **Enter**.

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

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

   Note: The system may list some warnings, which are normal and can be ignored. The system clearly lists any errors found during the package check.
8. Did the package check reveal any errors?
   - If **yes**, contact Cisco Services for assistance.

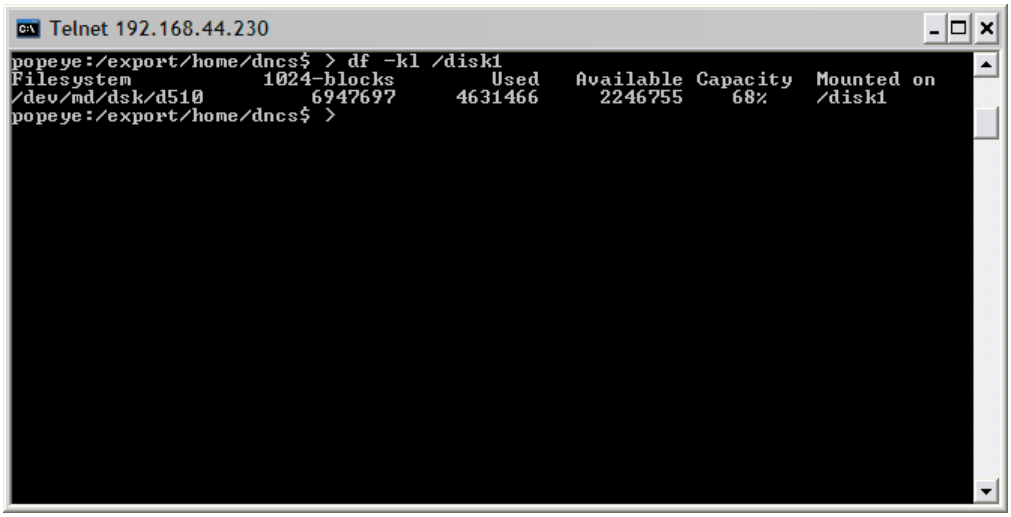
     Important! Do *not* proceed with the upgrade if the CD contains errors.
   - If **no**, follow these instructions.
     a. Type **cd /** and then press **Enter**.
     b. Type **eject cdrom** and then press **Enter**.
     c. Type **exit** and then press **Enter** to log out as root user.
9. Repeat steps 3 through 8 for each CD received in the software binder.

Check Available Disk Space

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

Checking Available Disk Space

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



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

- If **yes**, go to ***Run the Doctor Report*** (on page 15). You have sufficient space in which to perform the upgrade.
- If **no**, call Cisco Services. Engineers at Cisco Services can advise you regarding disk clean-up procedures.

Run the Doctor Report

Introduction

Before upgrading the DNCS, run the Doctor report using the instructions provided in the *DBDS Utilities Version 6.1 Installation Instructions and DNCS Utilities User's Guide* (part number 4020695). The Doctor report provides key system configuration data that might be useful before you begin the upgrade process.

Notes:

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

Analyze the Doctor Report

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

Also analyze the output of the Doctor report to verify that the inband SI_INSERT_RATE is *not* greater than 0 (zero). If the inband SI_INSERT_RATE is greater than 0 (zero), refer to *Recommendations 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.

Check the EAS Configuration—Pre-Upgrade

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

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

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.

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

   b Type su - and press Enter. The password prompt appears.

   c Type the root password and press Enter.

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

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

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

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

   Important:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   n **eeprom nvramrc > nvramrc.out**

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

7 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

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

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

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

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

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

Back Up the DNCS and Application Server File Systems

Perform a complete backup of the DNCS and Application Server file system now. Procedures for backing up the file system are contained in *DBDS Backup and Restore Procedures For SR 2.2 Through 4.2* (part number 4013779). The backup procedures have been modified so that you no longer have to shut down the DNCS or the Application Server to complete the backup. If necessary, call Cisco Services to obtain a copy of these backup and restore procedures.

Notes:

- Procedures for backing up the file system are found in the **Backing Up and Restoring the DNCS and Application Server** chapter of the *DBDS Backup and Restore Procedures For SR 2.2 Through 4.2* (part number 4013779).
- It may take up to 2 hours to back up a DNCS file system; you can usually back up an Application Server file system in about 30 minutes.

Verify DBDS Stability

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

      Note: Do *not* press the Power button.

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

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

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

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

Back Up the Informix Database

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

Procedures for backing up the database are contained in *DBDS Backup and Restore Procedures For SR 2.2 Through 4.2* (part number 4013779). If necessary, call Cisco Services to obtain a copy of these backup and restore procedures.

Suspend Billing and Third-Party Interfaces

Important Note About the Maintenance Window

CAUTION:

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

Suspending Billing and Third-Party Interfaces

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

Stop the cron Jobs

Introduction

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

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

Stop the cron Jobs on the DNCS

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

     Important: List the PIDs in reverse order.

     Example: kill -9 14652 14651 209
   - If the results from step 4 did not show /usr/sbin/cron, then the cron jobs are already stopped.
6. Type **cd /usr/sbin** and press **Enter**.
7. Type **chmod -x cron** and press **Enter**.
8. Perform a **ls -l cron** and press **Enter**.

   Result:

   -r--r--r-- 1 root sys 57420 Jan 22 2005 cron
9. Did your result in step 8 show **-r--r--r--** and *not* **-r-xr-xr-x**?
   - If **yes**, go to step 10.
   - If **no**, repeat step 8.

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

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

11 If the results from step 10 show that the cron process is still running, repeat steps 4 though 10.

Note: Call Cisco Services for assistance if necessary.

Stop the cron Jobs on the Cisco Application Server

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

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

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

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

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

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

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

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

  Important: List the PIDs in reverse order.

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

6 Type **cd /usr/sbin** and press **Enter**.

7 Type **chmod -x cron** and press **Enter**.

8 Perform a **ls -l cron** and press **Enter**.

Result:

-r--r--r-- 1 root sys 57420 Jan 22 2005 cron

9 Did your result in step 8 show **-r--r--r--** and *not* **-r-xr-xr-x**?

- If **yes**, go to step 10.
- If **no**, repeat step 8.

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

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

11 If the results from step 10 show that the cron process is still running, repeat steps 4 though 10.

Note: Call Cisco Services for assistance if necessary.

Stop Cisco Basic Backup or Auto Backup Servers

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

Remove the NMI Software

1. Are you already root user in an xterm window on the DNCS?
   - If **yes**, go to step 3.
   - If **no**, go to step 2.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type **pkginfo -l | grep SAInmi** and then press **Enter**. The system lists the SAInmi package if it is installed.
4. Is SAInmi installed?
   - If **yes**, go to step 5.
   - If **no**, you do not have NMI loaded onto your system. Skip the rest of this procedure, and go to ***Stop System Components*** (on page 28).
5. Close any user interfaces that may be open on the DNCS.

   Note: If the DNCS has any open user interfaces, you cannot remove the NMI software.
6. Type **ps -ef | grep ui** and then press **Enter**. The system displays a list of user interface processes that may still be running.
7. On a sheet of paper, write down the process IDs (PIDs) of any user interface process that is still running.
8. Type **kill -9 [PID]** and then press **Enter** for any user interface process that is still running. The system stops the user interface processes.
9. Type **pkgrm SAInmi** and then press **Enter**. The system deletes the NMI software.

Stop System Components

Before installing SARA Server software, use the procedures in this section to stop system components in the proper order. Failing to stop system components in the order described in this section may cause you to encounter difficulties during the installation.

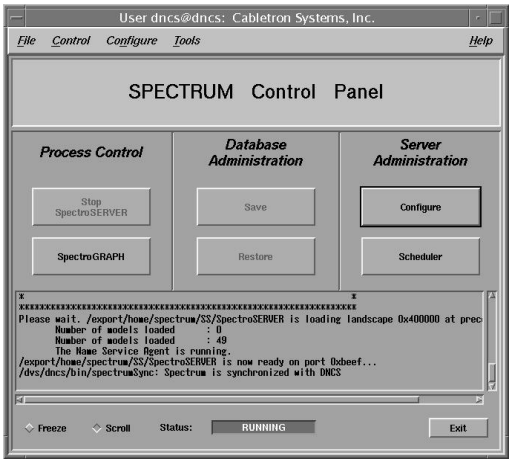
Important! System components must be stopped prior to installing SARA Server software.

Introduction

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

Stopping Spectrum

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



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

Stopping the RNCS Processes on the DNCS

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

Stopping the Application Server

This section provides procedures for stopping either a SARA Server or an Aptiv Application Server. Choose the procedure that pertains to your system.

Stopping the Application Server at SARA Sites

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

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

Stopping the Time Warner Mystro Application Server

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

Preparing the Aptiv Application Server for the Service Pack

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

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

Stopping the DNCS

1. At the DNCS, press the middle mouse button and then select **DNCS Stop**. A confirmation message appears.
2. Click **Yes**.
3. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The Dncs Control window appears.
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 Dncs Control window indicates that all of the DNCS processes have stopped, follow the on-screen instructions to close the Dncs Control window.

Ensure No Active Database Sessions on the DNCS

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

   Important:
   - Be sure to type the dot followed by a space prior to typing /dvs.
   - If **-0 bad options** message displays, ignore the message and go to step 5.
5. Type **/usr/ucb/ps -auxww | grep tomcat** and then press **Enter**. The system lists running processes that use the tomcat server.
6. Is the tomcat server running?
   - If **yes**, type **/etc/rc2.d/S98tomcat stop** and then press **Enter**.
   - If **no**, go to step 7.
7. Type **/usr/ucb/ps -auxww | grep tomcat** and then press **Enter** to confirm that the tomcat server has stopped.

   Note: If the tomcat server is still running, repeat step 5.
8. Type **ps -ef | grep -i ui** and then press **Enter**. The system lists running UI processes.
9. Are any UI processes running (such as dbUIServer or podUIServer)?
   - If **yes**, type **/dvs/dncs/bin/stopSOAPServers** and then press **Enter**.
   - If **no**, go to step 13.
10. Type **ps -ef | grep -i ui** and then press **Enter** to confirm that all UI processes have stopped.

    Note: If any UI processes are still running, type again **/dvs/dncs/bin/stopSOAPServers** and then press **Enter**.
11. Type **ps -ef | grep -i ui** and then press **Enter** to confirm that UI process have stopped.

12 Are any UI processes still running?

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

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

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

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

Result: One of the following messages appears:

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

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

- If **yes**, complete these steps:
  - **a** Type **killActiveSessions** and then press **Enter**. The system removes all active sessions from the database.
  - **b** Type **showActiveSessions** again and then press **Enter**.
  - **c** Did a message appear indicating that there are active database sessions?
    - If **yes**, call Cisco Services.
    - If **no**, go to step 15.
- If **no**, go to step 15.

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

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

17 Is the dncsInitd process still running?

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

3

Install the DNCS Software

Introduction

This chapter provides instructions to install this software onto networks operating with SR 2.7/3.7/4.2 software. This software provides support on the DNCS for SSC binding for Cisco CableCARD Host platforms.

Upgrade Path

Sites that want to upgrade to this software must support System Release 2.7/3.7/4.2.

Time to Complete Upgrade

These instructions require the DNCS operators to stop the system components. Cisco recommends that this software be installed during the maintenance window. The entire procedure to stop the system components, install the DNCS software, and then restart the system components, takes between 15 to 30 minutes to complete.

In This Chapter

Install DNCS 4.2.0.24 SP 0.2 Software

Complete the following steps to install this software onto the DNCS.

Note: If you have properly followed the instructions so far, the system components should be stopped.

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 the CD labeled **DNCS System Release 4.2 SP 0.2** into the CD drive of the DNCS. The system automatically mounts the CD to /cdrom0 within 30 seconds.
4. Type **grep SAISP /var/sadm/install/gz-only-packages** and press **Enter**.
5. Does an entry display on the screen?
   - If **yes**, complete the following steps to remove the package.
     a. Type **pkgrm SAISP** and press **Enter**. The following package is currently installed: **SAISP SR 4.2 Service Pack 0.1 02-13-2007 (sparc) Sr_4.2_SP0.1**.
     b. A message displays **Do you want to remove this package? [y, n, ?,q]**. Type **y** and press **Enter**.
     c. Go to step 6.
   - If **no**, go to step 6.
6. Type **df -n** and then press **Enter**. A list of mounted filesystems appears.

   Note: The presence of /cdrom in the output confirms that the system correctly mounted the CD.
7. Type **/cdrom/cdrom0/install_SP** and then press **Enter**. A message displays Do you want to install this software?
8. Type **y** and press **Enter**. The software installs on the DNCS.
9. Follow these instructions to confirm a successful installation.
   a. Type **pkginfo -l SAIdncs** and then press **Enter**. The system displays an installed version of **4.2.0.24p2.1**.
   b. Type **pkginfo -l SAIgui** and then press **Enter**. The system displays an installed version of **4.2.0.24p2**.
   c. Type **pkginfo -l SAItools** and then press **Enter**. The system displays an installed version of **4.2.0.13p1**.
   d. Type **pkginfo -l SAIwebui** and then press **Enter**. The system displays an installed version of **4.2.0.24p2**.
   e. Type **pkginfo -l SAISP** and then press **Enter**. The system displays an installed version of **SR_4.2_SP0.2**.

10 Did the results from step 9 show installed versions as described?

- If **yes**, type **cd** and then press **Enter**. The home directory on the DNCS becomes the working directory.
- If **no**, call Cisco Services for assistance.

11 Type **eject cdrom** and then press **Enter**. The CD ejects.

Install Additional Software

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

Add an EAS Variable to the .profile File

Introduction

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

Adding an EAS Variable to the .profile File

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

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

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

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

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

- If **yes**, go to ***Enable Optional and Licensed Features*** (on page 39).
- If **no**, go to step 4.

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

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

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

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

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

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

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

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

export LOCAL_EAS_IP=[Ethernet address of the DNCS]

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

9 Go to ***Enable Optional and Licensed Features*** (on page 39).

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

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

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

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

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

12 Go to ***Enable Optional and Licensed Features*** (on page 39).

Enable Optional and Licensed Features

Enabling Optional and Licensed Features

If you have properly followed the instructions in this chapter, the system processes should currently be stopped. Now is the time to enable the optional features you have chosen as part of this upgrade, except for Direct ASI. ASI feature requires extensive system configuration. If the system you are upgrading is planned to support this feature, contact Cisco Services to have the licensed or optional features enabled on your network.

Remove Scripts That Bounce the Pass-Through Process

Introduction

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

Notes:

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

Removing Scripts That Bounce the Pass-Through Process

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

1. If necessary, open an xterm window on the DNCS.
2. Follow these instructions to check on the presence of scripts in the crontab file that bounce the Pass-Through process.
   a. Type **crontab -l | grep -i elop.sh** and then press **Enter**. The system lists the line(s) within the crontab file that contain elop.ksh.
   b. Type **crontab -l | grep -i bouncePassThru** and then press **Enter**. The system lists the line(s) within the crontab file that contain bouncePassThru.
3. Did the output of step 2 contain any references to the elop.sh or the bouncePassThru scripts?
   - If **yes**, go to step 4 to remove those references.
   - If **no**, go to ***Restart System Components*** (on page 42).

     Note: You do not have to remove any references to the scripts from the crontab file.

4 Type **crontab -l > /tmp/dncs.crontab** and then press **Enter**. The system redirects the contents of the crontab into dncs.crontab.

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

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

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

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

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

Restart System Components

Introduction

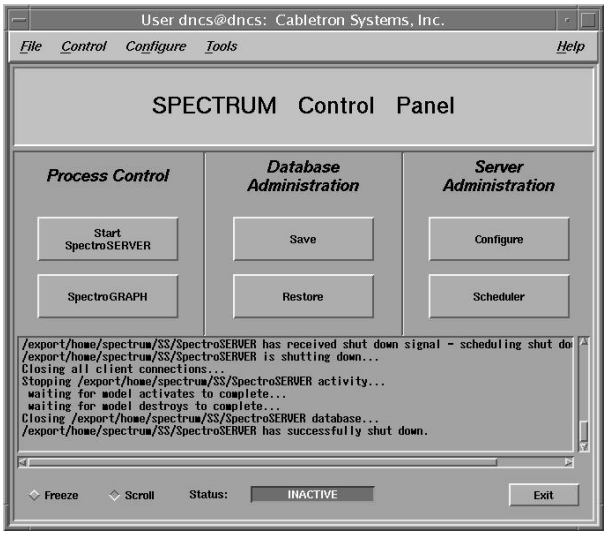
After you reboot the DNCS and the SARA Server, you must complete the procedures in this section to restart the following system components in the order listed:

1. Restart Spectrum NMS.
2. Restart DNCS processes.
3. Restart SARA Server processes.
4. Complete required procedures for Aptiv and MDN servers, if necessary
5. Restart cron jobs, if necessary.
6. Restart the billing system and other third-party applications.
7. If using the RCS feature, restart RNCS processes at each remote site.

Restarting Spectrum

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

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



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

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

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

Restarting the DNCS

1 From an xterm window on the DNCS, type **dncsStart** and press **Enter**. The Informix database, the SOAPServers, and DNCS processes start.

2 Click the middle mouse button on the DNCS and select **Administrative Console**. The DNCS Administrative Console opens.

3 From the DNCS Administrative Console Status window, click **DNCS Control**.

Results:

- The DNCS Control window opens.
- Green indicators begin to replace red indicators on the DNCS Control window.

4 From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The Dncs Control utility window opens.

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

6 Wait for the Dncs Control window to list the current status (Curr Stt) of all the processes and servers as **running**.

Notes:

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

Restarting the RNCS Processes on the DNCS

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

Restarting the Application Server

This section provides procedures for restarting either a SARA Server or an Aptiv Application Server. Choose the procedure that pertains to your system.

Restarting the Application Server at SARA Sites

1. Press the middle mouse button on the Application Server and select **App Serv Start**.
2. From an xterm window on the Application Server, type **appControl** and then press **Enter**. The Applications Control window opens.
3. Select option **2** on the Applications Control window. The system displays a list of Application Server processes and their current status.

   Note: The system updates the display periodically, or you can press **Enter** to force an update.
4. When the Application Control window indicates that the current state (**Curr Stt**) of each process is stopped, follow the on-screen instructions to close the Applications Control window.

Preparing the Aptiv Application Server for the Service Pack

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

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

Restarting the Time Warner Mystro Application Server

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

Restart the Billing and Third-Party Interfaces

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

Enable cron Jobs on the DNCS and Application Server

On the DNCS

1. If you do not already have one open, open an xterm window.
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 /usr/sbin** and press **Enter**.
4. Type **chmod +x cron** and press **Enter**.
5. Perform a **ls -l cron** and press **Enter**.

   Result:

   -r-xr-xr-x 1 root sys 57420 Jan 22 2005 cron
6. Did your result in step 5 show **-r-xr-xr-x** and *not* **-r--r--r--**?
   - If **yes**, go to ***On the Application Server*** (on page 46).
   - If **no**, repeat step 4.

On the Application Server

1. If you do not already have one open, open an xterm window.
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 /usr/sbin** and press **Enter**.
4. Type **chmod +x cron** and press **Enter**.
5. Perform a **ls -l cron** and press **Enter**.

   Result:

   -r-xr-xr-x 1 root sys 57420 Jan 22 2005 cron
6. Did your result in step 5 show **-r-xr-xr-x** and *not* **-r--r--r--**?
   - If **yes**, go to ***Restart the cron Jobs*** (on page 47).
   - If **no**, repeat step 5.

Restart the cron Jobs

Restart the cron Jobs on the DNCS

1. If necessary, open an xterm window on the DNCS.
2. Confirm that the cron jobs are not running by typing **ps -ef | grep cron** and press **Enter**.
3. Have the cron jobs restarted on their own?
   - If **yes**, skip the rest of this procedure and go to ***Restart the cron Jobs on the Application Server*** (on page 47).
   - If **no**, go to step 4.
4. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
5. Type **svcadm -v enable -rs cron** and press **Enter**. The system restarts all cron jobs.
6. Confirm that the cron jobs have restarted by typing **ps -ef | grep cron** and press **Enter**. The system should list **/usr/sbin/cron**.

Restart the cron Jobs on the Application Server

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

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

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

4

Post-Upgrade Procedures

Introduction

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

In This Chapter

Configure the CableCARD Server

Introduction

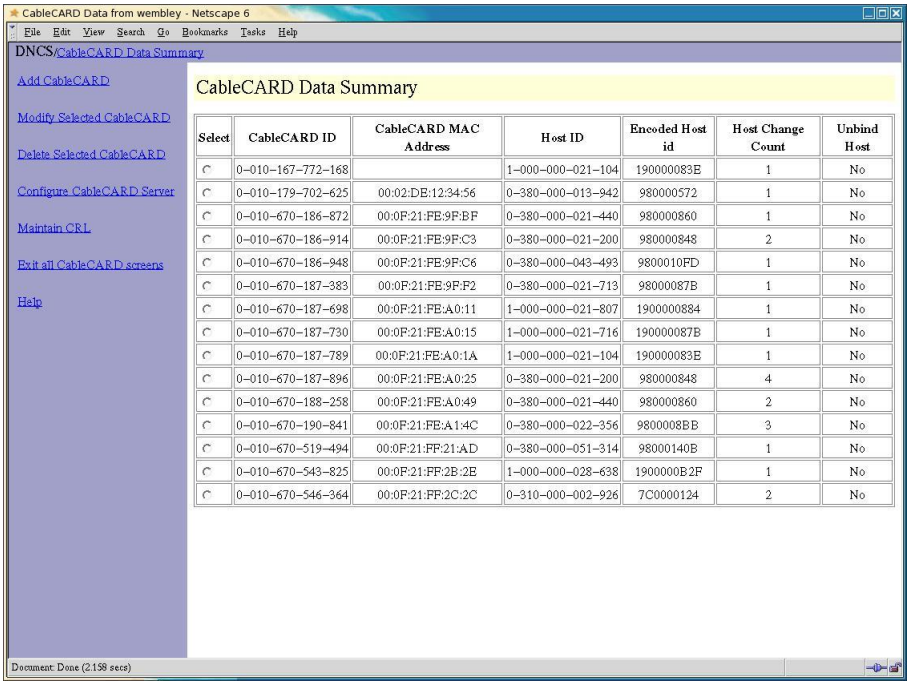
Next in the post-upgrade process, the **Set Authorization Time-out Period** and **Set DeAuthorization Time-out Period** fields on the Configure CableCARD Server window need to be set to specific values. These values instruct the CableCARD server when to stop adding authorization and deauthorization records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

Configuring the CableCARD Server

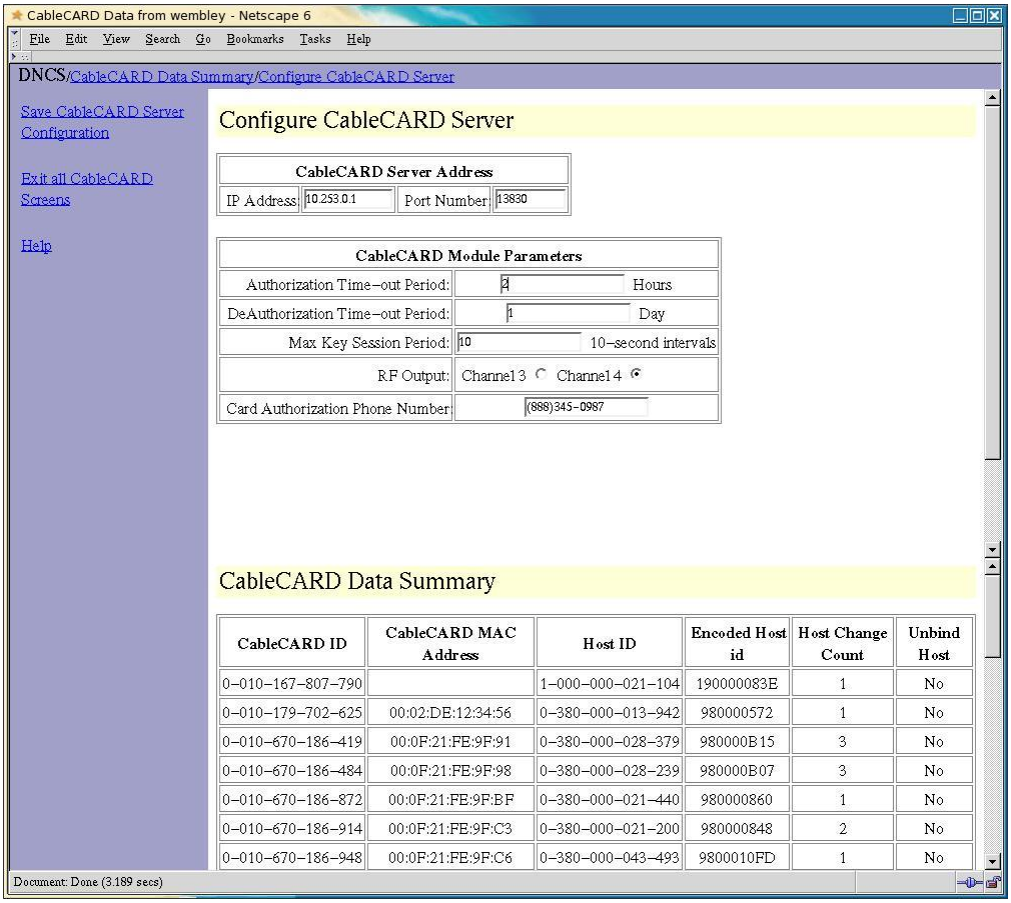
Complete the following steps to configure the minimum Set Authorization Time-out Period and Set DeAuthorization Time-out Period fields on the Configure CableCARD Server window.

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

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



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



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

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

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

5 Click **Save CableCARD Server Config**.

6 Click **Exit all CableCARD Screens**.

Check the EAS Configuration—Post Upgrade

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

Complete System Validation Tests

Introduction

The DHCTs that you use to verify a successful installation should comply with the following specifications:

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

Important! Note the following important points about these tests:

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

Verifying a Successful Installation

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

      Note: Do *not* press the Power button.

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

      Note: UNcfg displays Broadcast.

   c. Wait 5 minutes.

   d. Press the power button on the DHCT. Power to the DHCT is turned on.

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

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

      – If **yes,** go to step 2.

      – If **no**, contact Cisco Services.
2. Ping a test DHCT.
3. Did the DHCT receive the ping?
   - If **yes**, go to step 4.
   - If **no**, call Cisco Services.
4. Stage at least one new DHCT to the system operator's specifications.

5 After staging, did the DHCT successfully load the current client release software?

- If **yes**, go to step 6.
- If **no**, call Cisco Services for assistance.

6 Did the DHCT receive at least 33 EMMs (Entitlement Management Messages) and successfully receive its Entitlement Agent?

- If **yes**, go to step 7.
- If **no**, call Cisco Services for assistance.

7 Does the IPG display 7 days of valid and accurate data?

- If **yes**, go to step 8.
- If **no**, call Cisco Services for assistance.

8 Do the PPV barkers appear on the PPV channels correctly?

- If **yes**, go to step 9.
- If **no**, call Cisco Services for assistance.

9 Do third-party applications load and run properly?

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

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

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

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

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

Reinstall the NMI Software

If you removed the NMI software prior to the installation of SR 1.0, you need to reinstall the NMI software now. To reinstall the NMI software, refer to *DBDS Alarm Manager 1.0 Installation Instructions* (part number 745262) and follow the **Install the NMI Software Directly Onto the DNCS** procedure.

5

Customer Information

If You Have Questions

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

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

A

System Release Rollback Procedures

Introduction

This appendix contains a procedure for rolling back the DNCS, based on the software release that was on your DNCS before the upgrade. Prior to executing this rollback procedure, contact Cisco Services.

In This Appendix

Backing Out SR 4.2.0.24 SP 0.2 on the DNCS

1. Complete all the procedures in ***Stop System Components*** (on page 28) and ***Ensure No Active Database Sessions on the DNCS*** (on page 31).
2. If necessary, open an xterm window on the DNCS.
3. Type **su -** and then press **Enter**. The password prompt appears.
4. Type the root password and then press **Enter**. The system logs you on to the xterm window as **root** user.
5. Insert the CD labeled **DNCS Patch System Release 4.2 SP 0.2** into the CD drive of the DNCS. The system automatically mounts the CD to /cdrom0 within 30 seconds.
6. Type **df -n** and then press **Enter**. A list of mounted filesystems appears.

   Note: The presence of /cdrom in the output confirms that the system correctly mounted the CD.
7. Type **cd /cdrom/cdrom0** and then press **Enter**. The /cdrom/cdrom0 directory becomes the working directory.
8. Type **./backout_SP** and then press **Enter**. The script checks and saves existing packages on the DNCS.

   Important: Type a period before the /.
9. The following message displays: **Are you SURE you want to continue?** Type **y** and press **Enter** to continue the rollback procedure.

   Important! This command returns you to the DNCS version that was loaded on your system prior to loading this software.
10. Follow these instructions to confirm your DNCS has returned to it's previous software version.
    a. Type **pkginfo -l SAIdncs** and then press **Enter**.
    b. Type **pkginfo -l SAIgui** and then press **Enter**.
    c. Type **pkginfo -l SAItools** and then press **Enter**.
    d. Type **pkginfo -l SAIwebui** and then press **Enter**.
11. Type **pkginfo -l SAISP** and then press **Enter**. Choose one of the following options:
    - If SR 4.2 SP0.1 *was installed*, then the pkginfo command should display a value of SR 4.2 SP0.1.
    - If SR 4.2 SP0.1 *was not installed*, then the package does not exist and error message displays **Information in SAISP was not found**.

12 Did the system support version 4.2.0.24p1 before the SAI Tools patch installation?

- If **yes**, do the results of step 10 show SAItool version as 4.2.0.13p1 and the SAIgui and SAIwui versions as 4.2.0.24p1?
  - If **yes**, go to step 13.
  - If **no**, follow the instructions in *Installing the SAI Tools Patch* (part number 4018566) to reinstall the SAI tools patch.
- If **no** (the system had earlier code), go to step 13. The SAIgui and SAIwebui packages do not have to be upgraded.

13 Type **eject cdrom** and then press **Enter**. The CD ejects.

14 Complete all the procedures ***Restart System Components*** (on page 42) to restart Spectrum, the DNCS, and the Application Server.

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

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

May 2012 Printed in USA

Part Number 4019303 Rev C