DBDS Utilities Version 5.1 Installation Instructions and DNCS Utilities User's Guide

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 Acknowledgements

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

© 2006, 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 ix

Chapter 1 Install the DBDS Utilities 1

Before You Begin ... 3
Check the EMM Deletion Method ... 4
DBDS Utilities Installation Instructions ... 6
Verify the crontab Entry ... 11
Customize the Doctor Report ... 12

Chapter 2 Delete Unneeded EMMs with the dbOptimizer Program 13

The dbOptimizer Options ... 14
List EMMs by Age ... 15
Deletion of EMMs Based Upon Age ... 17
Change the crontab Entry ... 19

Chapter 3 Reset DHCT Configuration with the delete-sm Utility 21

Supported Options for the delete-sm Utility ... 22
Display the Help Window for the delete-sm Utility ... 24
Reset the Configuration of a Single DHCT ... 25
Reset the Configuration of DHCTs in a Prepared Text File ... 26
Reset the Configuration of DHCTs to Support Session-Based Encryption ... 29

Chapter 4 Analyze System Configuration with the Doctor Report 31

Run the Doctor Report ... 33
Understand the Data in the Doctor Report Fields ... 35

Chapter 5 Manage the Database with the dncsDbData Utility 57

Monitor and Eliminate Database Fragmentation ... 59
The dncsDbData Options ... 63
Unload the Database ... 65
Load the Database ... 73
Database Fragmentation, Database Used Capacity, and the Doctor Report ... 79

Obtain System Platform Information 83
Obtain the Version Number of the dncsDbData Utility 84

Chapter 6 Delete RMA DHCTs from the Database with the del-hct-cd Utility 85

Determine the Delete Command Option for Sites Prior to SR 2.0 86
Determine the Delete Command Option for Sites with SR 2.0 or Later 87
Run the del-hct-cd Utility 88
Process RMA DHCTs From a File 94

Chapter 7 Change the DNCS and Application Server Hostname with the hostnmchg Script 97

Run the hostnmchg Script 98
Restart the Applications 101

Chapter 8 Identify and Correct Database Problems with the checkDB Script 103

Overview of the checkDB Script 104
Run the checkDB Script 106

Chapter 9 Chart EMM Expiration Times with the smMix Utility 115

Overview of the smMix Modes 116
DHCT Administrative Statuses 117
How the smMix Utility Works 119
Run the smMix Utility 128

Chapter 10 Find Unique Files and Software Packages with the keyFileFinder Utility 131

How the keyFileFinder Utility Works 132
Run the keyFileFinder Utility 133

Chapter 11 Examine PCI Card Configuration with the slotchk Utility 135

Expected PCI Card Configuration 136
Run the slotchk Utility 139

Chapter 12 Obtain DHCT Information with the tellDhct Utility 141

The tellDhct Options 143
Display the Help Window and Version Number of the tellDhct Utility 145
Display Formatting Details for the tellDhct Utility 147
Display Brick Mode Authorization 148
Display Conditional Access Information 150
Display Return Path Information 152
Display Staging Information 155
Display Model, Revision, and Hub Information 157
Display CableCARD/Host Configuration 159

Chapter 13 Assign DHCTs to Download Groups with the runCvtGroup Utility 161

Run the runCvtGroup Utility 162

Chapter 14 Monitor the Status of System Metadevices with the check_metadevices Utility 165

Understanding the check_metadevices Utility 166

Chapter 15 Monitor the Logfiles of DNCS Processes with the qtail and sesstail Utilities 167

Design of the qtail and sesstail Utilities and the System Logfiles 168
The qtail Utility 169
The sesstail Utility 172

Chapter 16 Convert Binary IPPV Purchase Reports Into Text Format with the parseIppvRept Utility 175

The Data in the IPPV Purchase Report 176
The Options Available with the parseIppvRept Utility 177
Run the parseIppvRept Utility 178
View the Output File 180

Chapter 17 Associate Session IDs with Entitlement IDs with the eutdump Utility 183

Run the eutdump Utility 184

Chapter 18 Obtain DHCT Authorization Data with the tellDhctInfo Utility 185

Options Available with the tellDhctInfo Utility 186
Display the tellDhctInfo Help Window and Version Number 188
Obtain DHCT Authorization Data for a List of DHCTs 190
Obtain DHCT Authorization Data for an Individual DHCT 194
Obtain DNCS Subscription Packages and Segments 196

Chapter 19 Convert POD IDs and MAC Addresses with the podConvert Utility 197

Before You Begin 198
Convert MAC Addresses to POD IDs 199
Convert POD IDs to MAC Addresses 200

Chapter 20 Customer Information 201

Appendix A Stopping System Components 203

Stop System Components 204

Appendix B Restarting System Components 207

Restart System Components 208

Appendix C DBDS Utilities Version 5.1 Removal Procedure 213

Remove DBDS Utilities Version 5.1 214

Appendix D Update the DHCT OUI with the updateOUI Utility 217

Before Using the updateOUI Utility 219
Modes for the updateOUI Utility 220
Run the updateOUI Utility in Information Mode 222
Update the OUI 223
Reset the OUI 228
Miscellaneous updateOUI Options 235

Appendix E The chkSamUrl Utility 237
Run the chkSamUrl Utility 238

Appendix F Guidelines for Text Files Used in DNCS Utilities 243
Prepare the Text File 244
Preparing the Text File 245

About This Guide

Purpose

The DBDS Utilities CD contains four sets of utility programs that system operators and Cisco field service engineers can use to manage and troubleshoot Cisco's Digital Broadband Delivery System (DBDS). This installation and operation guide contains instructions to install the various software utilities contained on the DBDS Utilities CD. Additionally, this guide contains instructions to operate a subset of the DBDS Utilities, called DNCS Utilities.

The DBDS Utilities CD contains the following four sets of utility software:

- DNCS Utilities. The DNCS Utilities includes a collection of utility programs dedicated to managing and troubleshooting conditions on the Digital Network Control System (DNCS).

  Note: Instructions for running the DNCS Utilities are contained in subsequent chapters of this installation and user's guide.

- Application Server Utilities. The Application Server Utilities includes a collection of utility programs designed to help system operators and Cisco engineers test and manage the pay-per-view (PPV) and Interactive Program Guide (IPG) features and data on the Application Server.

  Notes:

  - During installation of the DBDS Utilities, the system automatically transfers the Application Server utilities from the DNCS to the Application Server.
  - Instructions for running the Application Server Utilities are contained in *Application Server Utilities User's Guide*, part number 749639.

- CoolTools Utilities. The CoolTools utilities includes a collection of utility programs designed to improve the efficiency with which system operators manage their DBDS as a whole.

  Note: Instructions for running the CoolTools Utilities are contained in *CoolTools Utilities User's Guide*, part number 749640.

- The DHCT Status Reporting and signonCount Utilities. These two utilities help system operators manage two-way communications between Digital Home Communications Terminals (DHCTs) and the headend.

  Note: Instructions for running the DHCT Status Reporting and signonCount utilities are contained in *DHCT Status Reporting and signonCount Utilities User's Guide*, part number 738186.

Scope

Many of the utilities described in this installation and operation guide pertain to systems running either Cisco or other resident applications. The updateOUI utility (described in Chapter 10), however, is restricted to those sites using Explorer® DHCTs, as are the Application Server Utilities, described in *Application Server Utilities User's Guide*.

Audience

This installation and operation guide is written for system operators of Cisco's Digital Broadband Delivery System (DBDS) and for Cisco field service engineers who help system operators manage their systems.

System Release Compatibility

Refer to the *DBDS Utilities Configuration Guide*, part number 4000828, for system release compatibility information for the DNCS Utilities.

To obtain the most current version of the *DNCS Utilities Configuration Guide*, please access your company's extranet site. For accessing instructions, contact your Cisco marketing manager. Check your extranet site often as the information is updated frequently.

Document Version

This is the eighth 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
podConvert	The podConvert utility appears for the first time in version 5.1 of the DBDS Utilities. See ***Chapter 19*** (see "Convert POD IDs and MAC Addresses with the podConvert Utility" on page 197) for information on the podConvert utility.
dncsPreInstallCheck	This utility was removed from DNCS Utilities.
updateOUI	The updateOUI utility was removed from the main body of the guide and placed in ***Appendix D*** (on page 217).
The Doctor Report was modified to report configuration data for remote sites on systems that support the Regional Control System (RCS) feature.	See ***Chapter 4*** (see "Analyze System Configuration with the Doctor Report" on page 31).

Minor functional changes were added to the following utilities: ■ tellDhct ■ tellDhctInfo	Refer to the Table of Contents in this guide for the appropriate chapter.
chkSamUrl	***Appendix E*** (on page 237) has been added in order to advise system operators on deleting unused SAM URLs from their system.
Guidelines for Text Files Used in DNCS Utilities	***Appendix F*** (on page 243) has been added to provide instructions on preparing text files for use with some DNCS Utilities.

Read This Before Installing the DBDS Utilities

Please read Chapter 1 of this guide in its entirety before installing the DBDS Utilities software. If you are uncomfortable with the installation procedures in Chapter 1, contact Cisco Services for assistance.

Many of the utilities described in this installation and operation guide interact with the DNCS database. Be sure you have a current database backup tape before running any of the utilities described in this guide.

Read These Important Recommendations About the DNCS Utilities

The DNCS Utilities are designed to improve the performance of the DNCS. Cisco engineers want system operators to be aware of the following important recommendations about some of the utilities described in this guide:

- Cisco strongly recommends that system operators run the Doctor Report at least once a day. Instructions for running the Doctor Report are in Chapter 4, ***Analyze System Configuration With the Doctor Report*** (on page 31).
- Cisco strongly recommends that system operators run the checkDB script at least once a month. Instructions for running the checkDB script are in Chapter 8, ***Identify and Correct Database Problems With the checkDB Script*** (on page 103).
- Cisco strongly recommends that system operators run the smMix utility at least every other week. Instructions for running the smMix utility are in Chapter 9, ***Chart EMM Expiration Times With the smMix Utility*** (on page 115).

1

Install the DBDS Utilities

Introduction

The following four software components comprise DBDS Utilities:

- DNCS Utilities
- CoolTools Utilities
- Application Server Utilities
- DHCT Status Reporting and signonCount Utilities

All four components are contained on one DBDS Utilities CD. During the installation process, the DNCS Utilities, CoolTools Utilities, and DHCT Status Reporting and signonCount Utilities install on the DNCS. The Application Server Utilities are initially loaded onto the DNCS, and then the installation process automatically transfers them to the Application Server.

The procedures in this chapter guide you through the installation of the DBDS Utilities. Additional procedures in this chapter accomplish the following tasks:

- Check the crontab file on the DNCS to determine the method currently in use to delete Entitlement Management Messages (EMMs)
- Check the crontab file on the DNCS for the presence of the dbOptimizer program, a program that is used for deleting unneeded EMMs.
- Remove orphaned sessions from the database.
- Remove obsolete Doctor directories.
- Customize the Doctor Report heading.

Follow the procedures in this chapter to install the DBDS Utilities and to complete the previously mentioned post-installation procedures.

In This Chapter

- Before You Begin..... 3
- Check the EMM Deletion Method..... 4
- DBDS Utilities Installation Instructions..... 6
- Verify the crontab Entry 11
- Customize the Doctor Report..... 12

Before You Begin

Introduction

Before you begin installing the DBDS Utilities, note these items of interest.

Uninstalling DBDS Utilities

In the event that your system is unstable after installing DBDS Utilities, Cisco engineers may direct you to uninstall the software. Refer to Appendix C, ***DBDS Utilities Version 5.1 Removal Procedure*** (on page 213), for procedures to uninstall the utility software. Have the CD containing the currently installed version of DBDS Utilities nearby in case you have to re-install the existing version.

Screen-Captured Images

Some of the screens or illustrations included in this chapter, as well as throughout this book, may not match exactly what appears on the system you are operating. Software version numbers or build numbers may vary from site to site.

The Solaris sar Utility

One of the utilities that is installed on the DNCS when you install DBDS Utilities is the Doctor Report. To be most valuable to the system operator, the Doctor Report needs to have the Solaris sar utility running. Refer to the UNIX man pages if you need information on enabling the sar utility.

A Concern About the signonCount Utility

Some sites may have received an unreleased test version of the signonCount utility from Cisco. Version 2.6.04 of the signonCount utility is installed with version 5.1 of DBDS Utilities. If you have a later version of the signonCount utility and wish to retain it, you need to make a backup copy of the signonCount utility before you install DBDS Utilities. Follow these instructions to make a backup copy of the signonCount utility.

1. From an xterm window on the DNCS, type **cp /dvs/dncs/bin/signonCount /dvs/dncs/bin/signonCount.bak** and then press **Enter**.
2. After installation of DBDS Utilities, type **cp /dvs/dncs/bin/signonCount.bak /dvs/dncs/bin/signonCount** and then press **Enter**.

Check the EMM Deletion Method

Introduction

Your system is designed to automatically delete unneeded EMMs through a reference to the dbOptimizer program in the crontab file. The crontab file contains calls to programs that run automatically, without operator intervention. The installation process of DBDS Utilities requests that you specify the method your system will use to delete unneeded EMMs. Before installing the latest version of DBDS Utilities, take a few minutes to run this procedure to determine the EMM-deletion method in use on your system. Possible choices are deletion based upon the age of the EMMs, or deletion based upon impulse pay-per-view (IPPV) purchases.

Important! Cisco is withdrawing support for deletion of EMMs based upon IPPV purchases. Beginning with version 4.1 of DBDS Utilities, all sites should configure their system to delete EMMs based upon the age of the EMMs.

Note: You can skip this procedure if you know for certain that your system deletes EMMs based upon the age of the EMMs.

Checking the EMM Deletion Method

Follow these instructions to inspect the crontab file to determine how your system deletes unneeded EMMs. If your system deletes EMMs based upon IPPV purchases, you need to reconfigure your system to delete EMMs based upon the age of the EMMs.

1 From an xterm window on the DNCS, type **crontab -l** and then press **Enter**. The system displays the contents of the crontab file.

Note: The "l" is a lowercase L.

2 Inspect the crontab file for an entry similar to one of the following examples:

- **$DNCS_TOP/bin/dbOptimizer -d 'cat /dvs/dncs/bin/CED.in'**

  Note: This method deletes EMMs based upon the age of the EMMs.

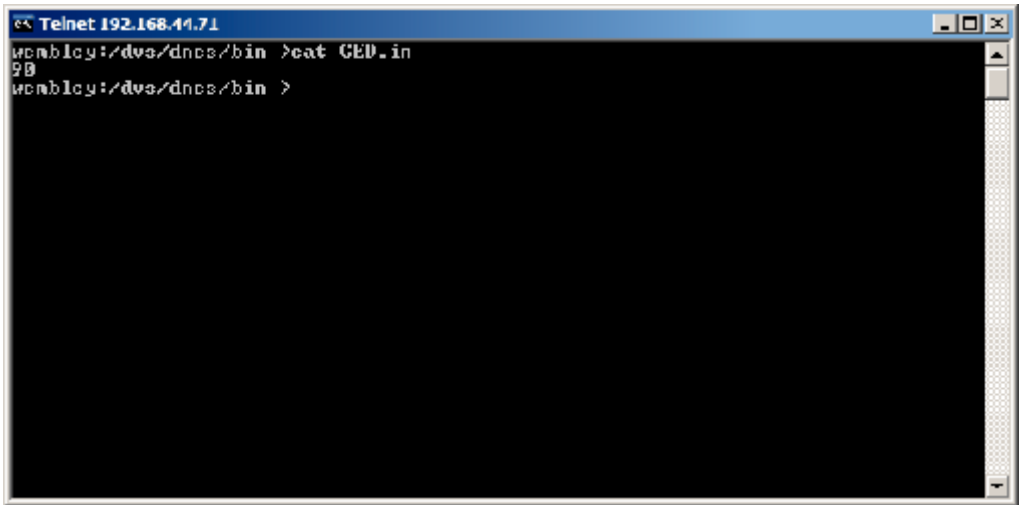
- **$DNCS_TOP/bin/dbOptimizer > /dvs/dncs/tmp/dbOptimizer.out 2>&1**

  Note: This method deletes EMMs based upon IPPV purchases.

3 Does your system delete unneeded EMMs based upon the age of the EMMs?

- If **yes**, go to step 4; you need to determine how old the EMMs must be before the system deletes them.
- If **no** (they are deleted based upon IPPV purchases); go to **DBDS Utilities Installation Instructions**, next in this chapter. During the course of the installation, you need to reconfigure your system to delete EMMs based upon the age of the EMMs.

4 Type **cat /dvs/dncs/bin/CED.in** and then press **Enter**. The system displays how old the EMMs have to be before they are deleted.



Note: A typical setting is 90 days.

5 Go to ***DBDS Utilities Installation Instructions*** (on page 6).

DBDS Utilities Installation Instructions

Installing the DBDS Utilities

Follow these instructions to remove any existing DBDS Utility packages that are on your system and then to install the latest version of DBDS Utilities onto the DNCS and Application Server.

Notes:

- You do not need to stop the system components before installing the DBDS Utilities.
- You should be able to install the DBDS Utilities in about 20 minutes.

1 Open an xterm window on the DNCS.

2 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**.

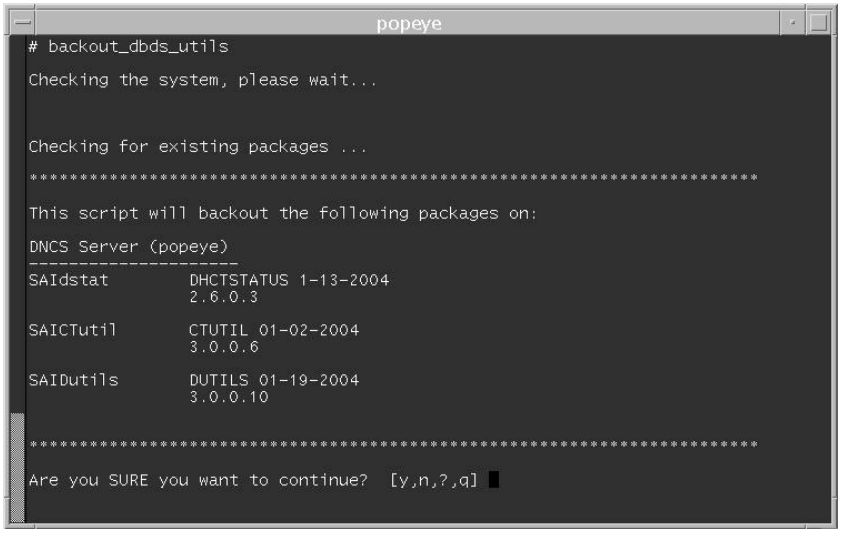
3 Insert the CD labeled **DBDS Utilities 5.1** into the CD-ROM drive of the DNCS.

4 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.

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

6 Type **./backout_dbds_utils** and then press **Enter**. The system lists the DBDS Utility packages it plans to remove and displays a confirmation message.



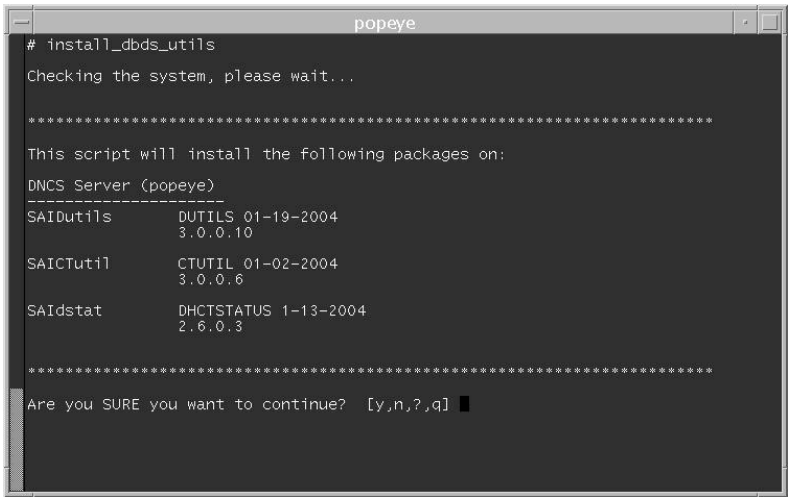
7 Type **y** and then press **Enter**. The system removes existing DBDS Utility packages.

8 When the existing packages have been removed, type **./install_dbds_utils** and then press **Enter**.

Note: Be sure to type the dot (**.**) before typing /install_dbds_utils.

Results:

- The system displays a Checking the system, please wait … message.
- Depending upon the Application Server you support, one of the following occurs:
  - If you support only the Cisco Application Server, the system displays a list of the DBDS Utilities components it will install and then displays an Are you SURE you want to continue message.



Note: The version numbers you see on your system may differ from what is displayed here.

  - If you support the Pioneer Application Server, the system displays an Is this site also usingCisco's AppServer for the Passport overlay message.

9 Did the system display the **Is this site also usingCisco's AppServer for the Passport overlay** message?

- If **yes**, choose one of the following options:
  - Type **n** and then press **Enter** if you are only using the Pioneer Application Server; then go to step 11.

    Result: The system displays a list of the DBDS Utilities components it will install and then displays an **Are you SURE you want to continue** message.
  - Type **y** and then press **Enter** if you are also using the Cisco Application Server.

    Result: The system displays an **Enter the hostname ofCisco's AppServer** message.
- If **no** (you are only using the Cisco Application Server) go to step 11.

10 Are you also using the Cisco Application Server?

- If **yes**, type the hostname of the Cisco Application Server and then press **Enter**.

  Note: If you do not already know the hostname of the Cisco Application Server, obtain the information by typing **hostname** and pressing **Enter** from an xterm window on the Application Server.

  Result: The system displays a list of the DBDS Utilities components it will install and then displays an Are you SURE you want to continue message.

- If **no**, go to step 11.

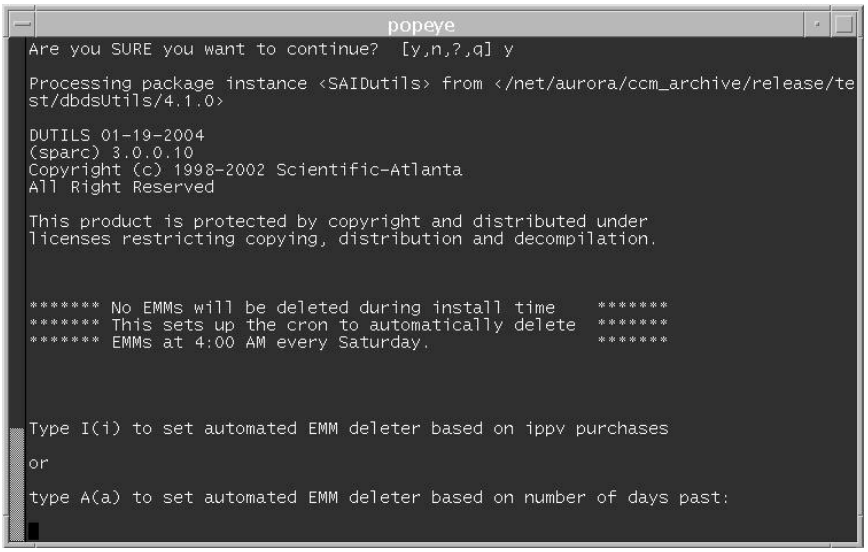
11 At the **Are you SURE you want to continue** message, type **y** and then press **Enter**.

Results:

- The system displays a copyright message.
- The system may display the following message concerning the deletion of unneeded EMMs:

  ***** **No EMMs will be deleted during install time** *****
  ***** **This sets up the cron to automatically delete** *****
  ***** **EMMs at 4:00 AM every Saturday.** *****

  Type I(i) to set automated EMM deleter based on ippv purchases
  or
  type A(a) to set automated EMM deleter based on number of days past:



12 Are you installing DBDS Utilities for the first time?

- If **yes**, read **Recommendation**, **Important**, and **Note** (in this step) for additional information about setting the EMM deletion method.
- If **no**, go to step 13.

Recommendation: Cisco *requires* that you configure your system to delete EMMs based upon age (*-a* option).

Important! In the event that you have DHCTs that were staged improperly, the DNCS Utilities includes the delete-sm utility. You can use this script to reset the configuration of those DHCTs so they can later be refreshed by the billing system with their staging EMMs. Refer to Chapter 3, ***Reset DHCT Configuration With the delete-sm Utility*** (on page 21) for additional information and instructions on running the delete-sm utility.

Note: When you choose to delete EMMs based upon the age of the EMMs, the first time this cron job runs, your system may take a very long time to delete excess EMMs. This is normal and should be expected.

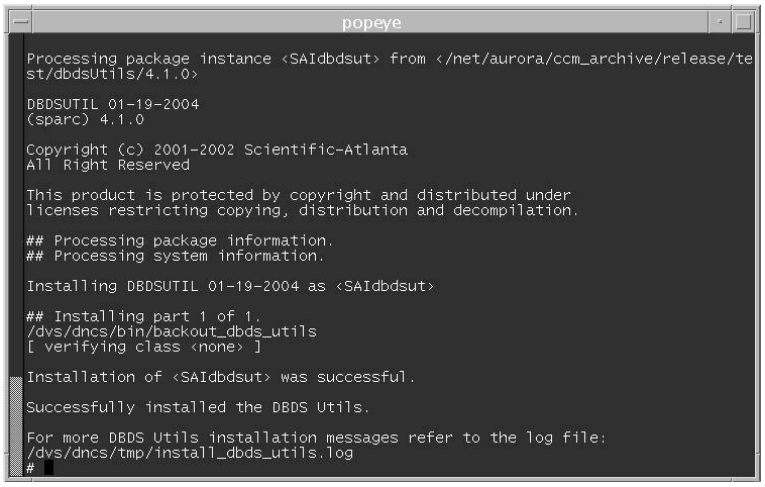
13 Type **a** (as stated in the message in step 11) and then press **Enter**. The following message appears:
Enter the number of days past, or type "d" for default of 90 days.

14 Type the number of days that correspond with how old you want EMMs to be before you delete them, or type **d** (for a default value of 90 days), and then press **Enter**.

15 Wait for the xterm window to update with the following message:

Installation of <SAIdbdsut> was successful.

Successfully installed the DBDS Utils.



Note: Note that the system points out that the installation log file is stored in the /dvs/dncs/tmp directory.

16 Type **cd** and then press **Enter**. The home directory becomes the working directory.

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

18 Remove the CD.

19 Type **exit** and then press **Enter**. The system logs out the root user.

20 Go to ***Verify the crontab Entry*** (on page 11).

Verify the crontab Entry

Verifying the crontab Entry

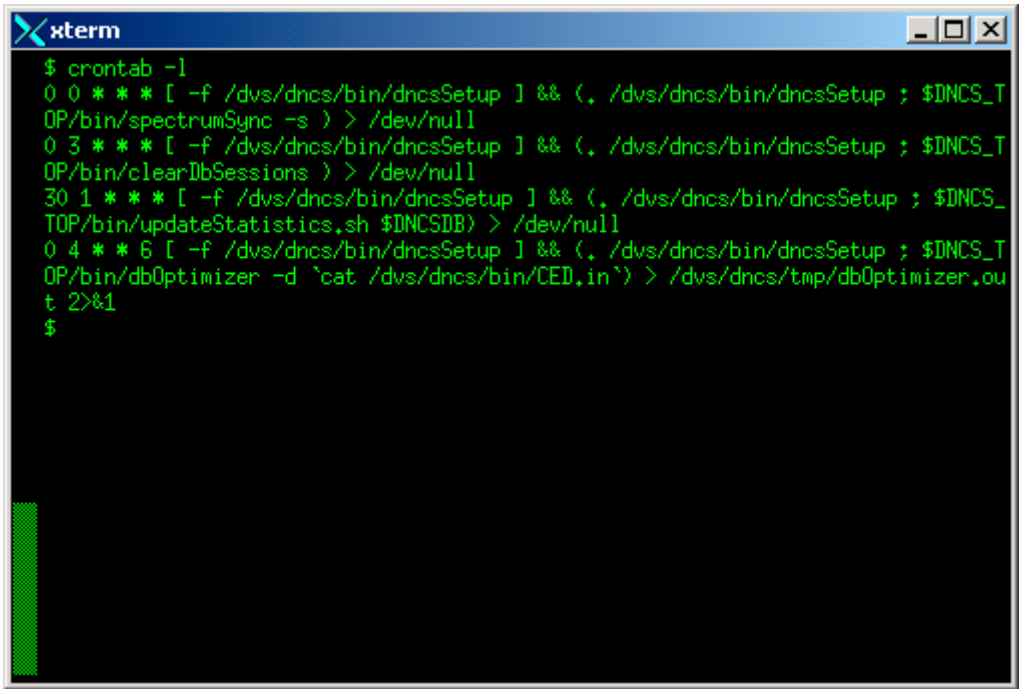
After installing the DBDS Utilities software onto the DNCS, inspect the crontab file to verify that the file contains an entry for the dbOptimizer program, and that it contains no entry for the camEmmDeleter program. Follow these instructions to inspect the crontab file.

Note: Your system executes the dbOptimizer program in the crontab file each Saturday at 4:00 AM.

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

2 Type **crontab -l** and then press **Enter**. The system lists the entries in the crontab file.

Note: The "l" is a lowercase L.



3 Does the crontab file include an entry for **dbOptimizer**?

- If **yes**, go to step 4.
- If **no**, call Cisco Services for assistance in adding an entry for dbOptimizer.

4 Does the crontab file include an entry for **camEmmDeleter**?

- If **yes**, call Cisco Services for assistance in removing the entry.
- If **no**, go to ***Customize the Doctor Report*** (on page 12).

Customize the Doctor Report

Introduction

The DBDS Utilities software includes the latest version of the Doctor Report, which system operators can use to generate a report of system configuration information.

By default, the hostname of the DNCS appears in the heading whenever you generate the Doctor Report. You can customize the Doctor Report, however, so that your system name, and whatever other information you choose, replaces the DNCS hostname field in the heading of the Doctor Report. By customizing the Doctor Report with the name of your system, any Doctor Report you may send to Cisco for analysis is clearly identified.

Important! Do not attempt to customize the Doctor Report unless you are knowledgeable in the use of the UNIX vi text editor.

Customizing the Doctor Report

Follow these instructions to customize your Doctor Report with the name of your system.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/doctor** and then press **Enter**. The /export/home/dncs/doctor directory becomes the working directory.
3. Type **vi doctor** and then press **Enter**. The doctor file opens using the UNIX vi editor.
4. Type **/SYS_NAME** and then press **Enter**. The system places the cursor on the line that contains SYS_NAME.
5. Type **:s/`uname -n`/"Site Name, location"/** and then press **Enter**. The UNIX search and replace function automatically replaces the uname -n variable with the name and location of your headend.

   Note: Substitute the site name and location (city), for Site Name, location.

   Important! Be sure to enclose the site name and location in quotes.
6. Type **:wq** to save the file and exit the vi editor. When you generate a Doctor Report, your system name is clearly displayed at the top of the output file.

2

Delete Unneeded EMMs with the dbOptimizer Program

Introduction

Cisco engineers developed the dbOptimizer program to delete EMMs that are no longer needed by DHCTs. Most EMMs are assigned to DHCTs during the staging process when DHCTs are prepared for deployment in the homes of subscribers. These EMMs are also stored in the database of the DNCS. When a DHCT has been successfully staged, those EMMs associated with the staging process are no longer needed and should be removed from the DNCS database.

The dbOptimizer program is configured to run by default each Saturday at 4 AM. The procedures in this chapter describe how to run this utility manually, as well as how to change when the utility is run.

Screen-Captured Images

Some of the screens or illustrations displayed in this chapter may not match exactly what appears on the system you are operating. Software version numbers, build numbers, and data may vary from site to site.

In This Chapter

- The dbOptimizer Options 14
- List EMMs by Age 15
- Deletion of EMMs Based Upon Age 17
- Change the crontab Entry 19

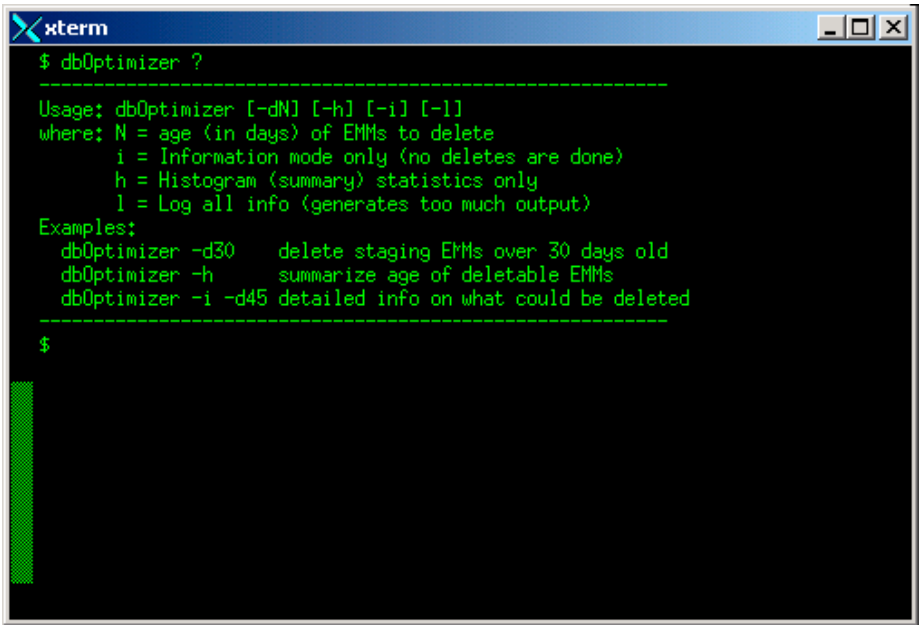
The dbOptimizer Options

Familiarizing Yourself with the dbOptimizer Options

Follow these instructions to generate a list of options you can use to configure your system to delete unneeded EMMs.

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

2 Type **dbOptimizer ?** and then press **Enter**. The system generates a list of options you can use when you execute the dbOptimizer program.



Note: The procedures in the remainder of this chapter guide you through each of the options.

List EMMs by Age

Summarizing the Ages of EMMs on Your System

Use the following procedure to generate a list that shows the ages of EMMs that are in your database.

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

2 Type dbOptimizer -h and then press Enter. The system generates a list of EMMs by age.

```
 dboptimizer -h
-------------------------------------------------------------------------------------------
Mar 19, 9:09:46 -- dbOptimizer Started
dbOptimizer Options selected: -h
Total DHCTs (secure_micro rows) in the database:      51136
Total DHCTs with IPPV flag set (sm_admin_state=1):    41
Total EMMs in the database:                           1700549
-------------------------------------------------------------------------------------------
Non-staging EMMs req'd for operation:    348893      21%
Staging EMMs 10 days old or less:        46473       3%
Staging EMMs over 10 days old:           1298028     76%
Staging EMMs over 20 days old:           1215300     71%
Staging EMMs over 30 days old:           1161462     68%
Staging EMMs over 40 days old:           1065018     63%
Staging EMMs over 50 days old:           972708      57%
Staging EMMs over 60 days old:           873933      51%
Staging EMMs over 70 days old:           788883      46%
Staging EMMs over 80 days old:           755403      44%
Staging EMMs over 90 days old:           718197      42%
Mar 19, 9:20:53  dbOptimizer Ended
-------------------------------------------------------------------------------------------
```

Notes:

- The system depicted in this illustration shows a total of 1700549 EMMs in the database.
- Of those 1700549 EMMs, 348893 are still needed for operation. You may, therefore, be able to delete the other 1351656 EMMs from your database (1700549 - 348893 = 1351656).

Recommendation for Deleting EMMs by Age

Cisco recommends that you configure your system to delete EMMs based upon age, specifically deleting those EMMs that are older than 90 days.

Important! The delete-sm utility lets you reset the configuration of any DHCTs that were staged improperly. The billing system can then modify these DHCTs, forcing the DNCS to rebuild and transmit the staging EMMs. See Chapter 3, ***Reset DHCT Configuration With the delete-sm Utility*** (on page 21), for additional information and instructions on running the delete-sm utility.

Deletion of EMMs Based Upon Age

Introduction

By executing the dbOptimizer program with the *-d* option, and then specifying the number of days, the system deletes unneeded EMMs that are older than the number of days specified.

Deleting excess staging EMMs based upon the age of the EMMs does *not* change your entry in the crontab file. After initial installation of the DNCS Utilities, you can change your crontab entry by running the setDbOptCron script, described in ***Change the crontab Entry*** (on page 19).

Deleting EMMs Based Upon Age

Follow these instructions to delete excess staging EMMs based upon the age of the EMMs.

1. If necessary, open an xterm window on the DNCS.
2. Choose one of the following options:
   - If you want to review information concerning which DHCTs on your system have staging EMMs that are older than an age you will specify, go to step 3.

     Notes:

     – System operators usually have no need to review information concerning which specific DHCTs on their system have staging EMMs older than a specified age. System operators obtain similar information by running the dbOptimizer program with the -h option, discussed in the previous section, ***List EMMs by Age*** (on page 15).

     – Choosing the *-h* option provides information, only; it does not delete EMMs, nor does it change your configuration.
   - If you want to delete EMMs based upon the age of the EMMs without reviewing which DHCTs are affected, go to step 7.

3 Type

dbOptimizer -d [number of days] -i > /dvs/dncs/tmp/dbOptimizer.info.out 2>&1 and then press **Enter**.

Example: Type

dbOptimizer -d90 -i > /dvs/dncs/tmp/dbOptimizer.info.out 2>&1 and then press **Enter** to display a list of DHCTs that have staging EMMs older than 90 days. Assume the date is November 20. The system considers EMMs assigned to DHCTs on August 21, or earlier, to be older than 90 days.

Result: The system writes the list of DHCTs with staging EMMs older than the number of days you specified to the /dvs/dncs/tmp/dbOptimizer.info.out file.

Note: Depending on the size of your system, it may take 2 to 4 hours to prepare this file.

4 Type **more /dvs/dncs/tmp/dbOptimizer.info.out** and then press **Enter**. The dbOptimizer.info.out file opens for viewing using the UNIX more utility.

5 Examine the dbOptimizer.info.out file to determine whether you want your system to delete the EMMs of these DHCTs from the database.

Notes:

- Press the **Spacebar** to advance through the file.
- When you are finished, press the **Ctrl** and **c** keys simultaneously to exit from the more utility.

6 Do you want to continue configuring your system to automatically delete EMMs based upon the age of the EMMs?

- If **yes**, continue with step 7.
- If **no**, type **exit** and then press **Enter** to close the xterm window.

7 Type

dbOptimizer -d[number of days> > /dvs/dncs/tmp/dbOptimizer.out 2>&1 and then press **Enter**.

Example: Type

dbOptimizer -d90 > /dvs/dncs/tmp/dbOptimizer.out 2>&1 and then press **Enter** to delete staging EMMs older than 90 days.

Results:

- The system deletes excess EMMs from the DNCS database based upon the age of the EMMs.
- The system writes a list of DHCTs with EMMs that were deleted to the /dvs/dncs/tmp/dbOptimizer.out file.

Note: Depending on the size of your system, this step may take up to 4 hours to complete.

8 Type **exit** and then press **Enter** to close the xterm window.

Change the crontab Entry

Changing the crontab Entry

By default, the DNCS Utilities places an entry in the crontab file of the DNCS for the system to execute the dbOptimizer program each Saturday at 4 AM. At any time after installing the DNCS Utilities, you can change the manner in which your system deletes excess EMMs by running the setDbOptCron script. When you run the setDbOptCron script, you replace the dbOptimizer entry in the crontab file with a new dbOptimizer entry. Follow these instructions to run the setDbOptCron script.

1. From an xterm window on the DNCS, type **su** and then press **Enter** to log in as root user.
2. Type the root password and then press **Enter**.
3. Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. This command establishes the DNCS environment as a root user.

   Important! Type the period followed by a space before typing /dvs.

   Note: The system may also return a message that ends with

   -o bad options or **-o: bad options**. Ignore this message; it is normal.
4. Type **setDbOptCron** and then press **Enter**. The following message appears:

   ***** **No EMMs will be deleted during install time** *****

   ***** **This sets up the cron to automatically delete** *****

   ***** **EMMs at 4:00 AM every Saturday.** *****

   Type "i" to set automated EMM deleter based on ippv purchases

   or

   type "a" to set automated EMM deleter based on number of days past:
5. Type **a** (as stated in the message in step 4) and then press **Enter**. The following message appears:

   Enter the number of days past, or type "d" for default of 90 days.
6. Type the number of days that correspond with how old you want EMMs to be before you delete them, or type **d** (for a default value of 90 days), and then press **Enter**. The changing of the crontab entry continues.

7 When the message **The crontab setup is complete** appears, type **exit** and then press **Enter**. The system logs out the root user.

8 Type **exit** and then press **Enter**. The root user logs out.

9 Type **exit** and then press **Enter** to close the xterm window.

Note: Your revised dbOptimizer entry in the crontab file will execute every Saturday at 4 AM.

3

Reset DHCT Configuration with the delete-sm Utility

Introduction

System operators who stage large quantities of DHCTs may occasionally find that some of these DHCTs finish the staging process without having received all of their staging EMMs. System operators know that DHCTs have not received all of their staging EMMs when one of the following conditions occurs:

- The Status and Network Parameters diagnostics screen of the DHCT lists no entry in the ISE(1): field.
- The DHCT displays a PPV 154 error when the subscriber tries to buy an impulse pay-per-view (IPPV) event.

System operators can run the delete-sm utility to reset the configuration of these DHCTs. System operators should then contact their billing system vendor to modify these DHCTs, which triggers the DNCS to create new staging EMMs.

Note: Resetting the configuration of a DHCT is sometimes referred to as de-provisioning the DHCT.

In This Chapter

- Supported Options for the delete-sm Utility 22
- Display the Help Window for the delete-sm Utility..... 24
- Reset the Configuration of a Single DHCT 25
- Reset the Configuration of DHCTs in a Prepared Text File..... 26
- Reset the Configuration of DHCTs to Support Session-Based Encryption..... 29

Supported Options for the delete-sm Utility

The delete-sm Utility Options

The delete-sm utility supports three main options: *-a*, *-o*, and *..OOS..* (dot, dot, OOS, dot, dot). The *-a* and *-o* options are used to reset the configuration of a single DHCT or a list of DHCTs. The delete-sm utility, when used with the *-o* option, checks for the presence of active packages on the DHCT(s) and resets the configuration of out-of-service DHCTs and in-service DHCTs with no active packages. The *-a* option makes no such check and resets the configuration of the DHCT(s) regardless of the presence of active packages.

The *..OOS..* option of the delete-sm utility is a special feature reserved for helping a site prepare to support session-based encryption (SBE).

Note: SBE is a feature that provides a high degree of security for video-on-demand (VOD) content. Through SBE, the DBDS is capable of sending secured VOD content only to those DHCTs that are authorized to receive VOD.

The *..OOS..* option provides the following services:

- When used with the *..OOS..* option by itself, the utility de-provisions all DHCTs marked as out-of-service in the database. No list of MAC addresses is required.
- When the *-o* option is used in conjunction with the *..OOS..* option, in addition to de-provisioning DHCTs marked out-of-service in the database, the utility also deletes records from the secure_micro table for DHCTs with an in-service status that have no active packages. When DHCT records are removed from the secure_micro table, the DHCT can be re-staged through transactions transmitted by the billing vendor.

When you run the delete-sm utility with no options, the utility resets the DHCT configuration only if the DHCT is not already listed as in-service in the database.

In most cases, when the configuration of a DHCT is reset, the DHCT is assigned a status of out-of-service. Some sites, however, use an environmental variable called HCTM_PROVISIONING_APP to facilitate the deployment of DHCTs at those sites. When the configuration of a DHCT is reset at sites that use the HCTM_PROVISIONING_APP variable (variable set to 1), the DHCT is assigned a status of deployed.

Note: Refer to Instastaging Guide, part number 4010008, for additional information on the HCTM_PROVISIONING_APP variable.

Single DHCT or a List of DHCTs

You can use the delete-sm utility to reset the configuration of a single DHCT, or for a series of DHCTs. When you use the delete-sm utility to reset the configuration of a series of DHCTs, you need to prepare a text file that contains the MAC addresses of the DHCTs that require their configuration to be reset. Then, you use the name of that text file as an argument when you run the delete-sm utility.

Refer to Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243), for general instructions on using a text file in conjunction with the delete-sm utility.

Display the Help Window for the delete-sm Utility

Introduction

The information in this section describes how to display the delete-sm help window.

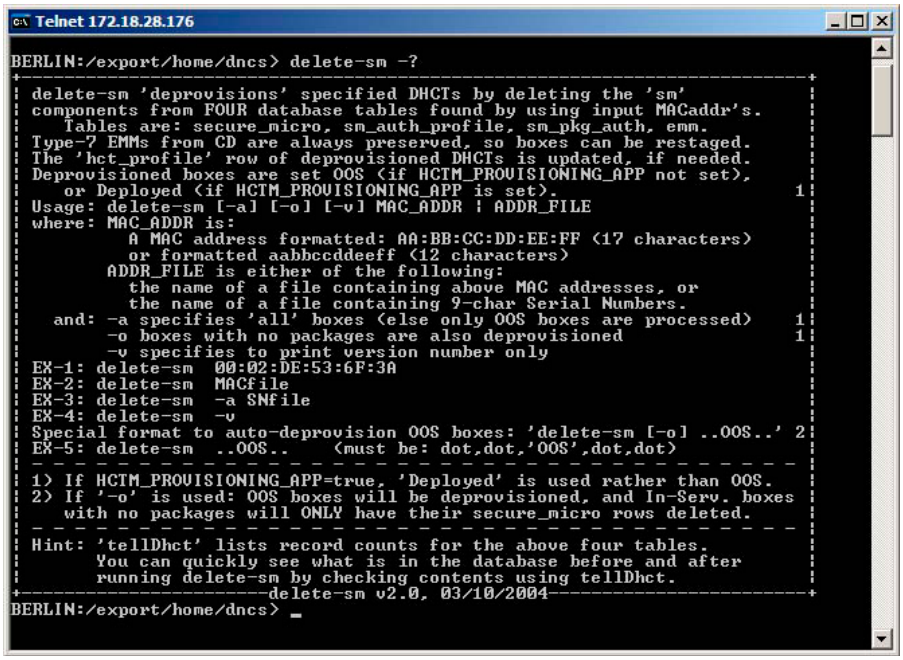
Tip: Many utilities include a help window. The help window is frequently a good place to start if you are unfamiliar with a utility.

Displaying the delete-sm Help Window

Follow these instructions to display the delete-sm help window.

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

2 Type **delete-sm -?** and then press Enter. The system displays a window showing the options with which the delete-sm utility is run.



Reset the Configuration of a Single DHCT

Introduction

The instructions in this section describe how to use the delete-sm utility to reset the configuration of a single DHCT.

Resetting the Configuration of a Single DHCT

Follow these instructions to reset the configuration of a single DHCT.

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

2 Choose one of the following options:

- To reset the configuration only if the DHCT is either out-of-service or is in-service but contains no active packages, type **delete-sm -o [DHCT MAC Address]** and then press **Enter**.

  Example: delete-sm -o 00:E0:36:01:52:8C

- To reset the configuration of the DHCT regardless of service status or whether it contains active packages, type **delete-sm -a [DHCT MAC Address]** and then press **Enter**.

  Example: delete-sm -a 00:E0:36:01:52:8C

Result: The system resets the configuration of the DHCT specified by the MAC address.

3 Do you want to transmit staging EMMs to the DHCT for which you just reset the configuration?

Note: You may prefer, instead, to leave the DHCT without any staging EMMs for a while.

- If **yes**, notify your billing system vendor to transmit a **ModifyDhctConfiguration** transaction that refreshes the DHCT with the set of staging EMMs.

  Important! An InstantHit transaction from the billing system is not sufficient.

  Note: You can also add services to DHCTs through the DNCS GUI. Billing system transactions, however, will overwrite any configuration changes you make through the DNCS GUI.

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

Reset the Configuration of DHCTs in a Prepared Text File

Introduction

The procedures in this section describe how to use the delete-sm utility to reset the configuration of DHCTs that are listed in a prepared text file.

Resetting the Configuration of DHCTs in a Prepared Text File

Follow these instructions to reset the configuration of DHCTs listed in a prepared input file.

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

2 Choose one of the following options:

- To reset the configuration of out-of-service DHCTs and in-service DHCTs with no active packages, type **delete-sm -o [input file name] > [output file name]** and then press **Enter**.
- To reset the configuration of all out-of-service and in-service DHCTs, regardless of the packages assigned to them, type **delete-sm -a [input file name] > [output file name]** and then press **Enter**.

Notes:

- Substitute the name of your prepared text file for [input file name].
- Substitute the name of the file to which you want to direct the output for [output file name].

Examples:

- **delete-sm -o del-sm-in_08.31.03 > del-sm-out_08.31.03**
- **delete-sm -a del-sm-in_08.31.03 > del-sm-out_08.31.03**

Results:

- The delete-sm utility resets the configuration for the DHCTs listed in [input file name].
- The delete-sm utility generates a list of DHCTs processed by the delete-sm utility.
- Cisco recommends that you direct this list to a file so that you can later examine it, if necessary.

3 Do you want to transmit staging EMMs to the DHCTs for which you just reset the configuration?

Note: You may prefer, instead, to leave the DHCTs without any staging EMMs for a while.

- If **yes**, notify your billing system vendor to transmit a **ModifyDhctConfiguration** transaction that refreshes the DHCTs with the set of staging EMMs.

  Important! An InstantHit transaction is not sufficient.

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

Resetting the Configuration of DHCTs in a Text File That Are Not In-Service

DHCTs are usually considered to be not in-service when they have a status of out-of-service. On systems that use the HCTM_PROVISIONING_APP variable, DHCTs that have a status of deployed are also considered to be not in-service. Follow these instructions to reset the configuration of DHCTs that already have a status of out-of-service (or deployed).

Notes:

- If the site uses the HCTM_PROVISIONING_APP variable, this procedure will de-provision those DHCTs that have a status of deployed or out-of-service.
- If the site does not use the HCTM_PROVISIONING_APP variable, this procedure will de-provision those DHCTs that have a status of out-of-service.

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

2 Type **delete-sm [input file name] > [output file name]** and then press **Enter**.

Notes:

- Substitute the name of your prepared text file for [input file name].
- Substitute the name of the file to which you want to direct the output for [output file name].

Example: delete-sm del-sm-in_08.31.01 > del-sm-out_08.31.01

Results:

- The delete-sm utility resets the configuration for every DHCT listed in [input file name] that is marked as out-of-service or deployed (depending upon whether the site uses the HCTM_PROVISIONING_APP variable) in the database.

  Note: The delete-sm utility skips over DHCTs marked as in-service.

- The delete-sm utility generates a list of DHCTs processed by the delete-sm utility.
- Cisco recommends that you direct this list to a file so that you can later examine it.

3 Do you want to transmit staging EMMs to the DHCTs for which you just reset the configuration?

Note: You may prefer, instead, to leave the DHCTs without any staging EMMs for a while.

- If **yes**, notify your billing system vendor to transmit a **ModifyDhctConfiguration** transaction that refreshes the DHCTs with the set of staging EMMs.

  Important! An InstantHit transaction from the billing system is not sufficient.

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

Reset the Configuration of DHCTs to Support Session-Based Encryption

Introduction

The procedures in this section describe how to use the delete-sm utility in conjunction with the ..OOS.. option in order to prepare a site to support SBE.

Resetting the Configuration of DHCTs to Support Session-Based Encryption

Follow these instructions to use the ..OOS.. option of the delete-sm utility in order to help a site support SBE.

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

2 Choose one of the following options:

- To reset the configuration of out-of-service DHCTs without also deleting records from the secure_micro table for in-service DHCTs with no active packages, type **delete-sm ..OOS..** and then press **Enter**.
- To reset the configuration of out-of-service DHCTs and to also delete the records from the secure_micro table for in-service DHCTs with no active packages, type **delete-sm -o ..OOS..** and then press **Enter**.

4

Analyze System Configuration with the Doctor Report

Introduction

The Doctor Report is one of the most important tools that system operators and Cisco engineers can use to evaluate the configuration and operation of a Cisco DBDS. Output from the Doctor Report appears on the screen of the DNCS and is written to an output file for later analysis.

Cisco developed the Doctor Report to generate a snapshot of system configuration. The following list contains some of the system configuration information reported by the Doctor Report:

- Installed software versions
- DNCS and Application Server disk partition utilization
- Status of DNCS and Application Server processes
- Summary of supported DHCT types
- Summary of sources, source definitions, segments, and sessions
- Summary of PPV services and events
- Data carousel/pump status and rates
- Configuration data for remote sites
- Common configuration errors that may lead to problems later

Important! Cisco strongly recommends that system operators run the Doctor Report at least once a day.

This chapter provides the following information about the Doctor Report:

- Running the Doctor Report
- Understanding the data produced by the Doctor Report

In This Chapter

- Run the Doctor Report 33
- Understand the Data in the Doctor Report Fields..... 35

Run the Doctor Report

Running the Doctor Report

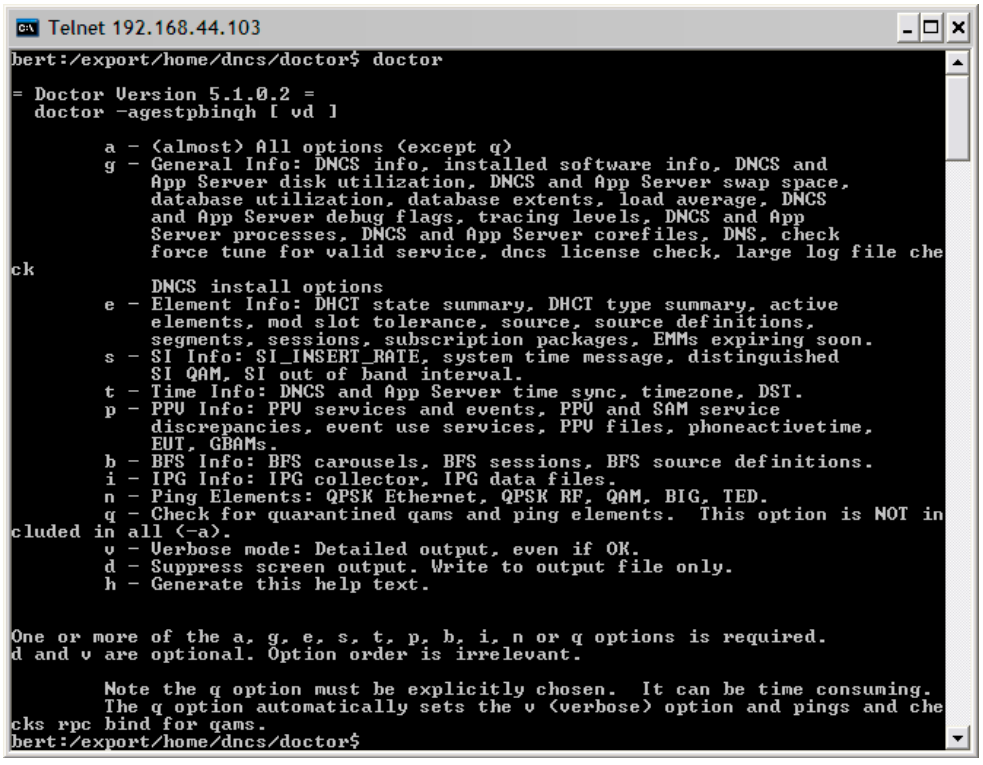
Use the following procedure to run the Doctor Report on the DNCS.

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

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

3 Type **doctor** and then press **Enter**. The system generates a list of parameters that you can use to run the Doctor Report.

Note: Each parameter causes the Doctor Report to generate output with specific configuration information.



4 To generate a complete Doctor Report, type **doctor -av** and then press **Enter**.

Results:

- The system generates the Doctor Report listing all system configuration information and directs the output of the report to the screen.
- The system also saves the output of the Doctor Report to a file in the current directory on the DNCS.

Example: The system saves the report with a name similar to **report.001026_0921.doc**.

Notes:

- Depending upon the size of your system, it may take a few minutes for the report to generate.
- The final line of the report generated to the screen lists the file to which the output was saved.
- The report is a plain text file. You can view the report in a text editor of your choice.

A Special Note About the –q Option

The Doctor Report includes the *–q* option. Through the *–q* option, system operators can ping the QAM, MQAM, GQAM, and GoQAM modulators and test the remote procedure call (RPC) connection between the modulators and the DNCS. Furthermore, the *–q* option generates a report that lists all the modulators, specifies whether the modulators are in a quarantined condition, and notes the date and time stamp of the quarantine, if applicable.

Understand the Data in the Doctor Report Fields

Introduction

The information in this section provides an explanation of the data produced by generating the Doctor Report. Some of the data is only for informational purposes. Other data is preceded by the words **OK, Error**, or **Warning**.

Data in the report preceded by the word OK indicates that the data meets Cisco's recommendations regarding the field to which the data applies. Data in the report preceded by the word Error may indicate that some system process or function is not operating as it should. Where appropriate, this section includes troubleshooting tips so that system operators can investigate and correct a situation producing an error in a data field. A warning indicates that a potentially serious condition, such as a disk partition nearing capacity, or that certain data does not meet Cisco's recommendations, has been detected.

Important! Anytime an unexpected or new error appears in the Doctor Report output or if defined thresholds are about to be reached, contact Cisco Services for assistance.

Important Note Regarding Pioneer Sites

Due to the unique implementation of the Passport Application Server, sites using Pioneer resident applications may see Application Server-related errors in their Doctor Report. Ignore these errors; these errors are normal for sites that use Pioneer resident applications. The fields in the Doctor Report that are affected by Pioneer resident applications are noted in this section by the words Pioneer Note.

System Name

The System Name field appears at the top of the Doctor Report. This field can be customized by the system operator to display the name of the system whose data is displayed in the report.

Note: If the System Name field does not reflect the name of your system, follow the instructions in ***Customize the Doctor Report*** (on page 12) in Chapter 1.

All SAI Installed Package Information

The data in the **All SAI Installed Package Information** field contains the following information about the software packages installed on your system:

- The name of the package
- The version number of the package
- The date the package was installed
- The platform on which the package was installed

Pioneer Note: Ignore any Application Server-related errors at sites that run the Pioneer resident application.

DNCS Info

Data fields included under DNCS Info contain information that pertains to the hardware configuration of your DNCS.

Platform & CPU

The Platform & CPU field contains configuration information that pertains to the central processing unit (CPU) of the DNCS.

RAM

The RAM field displays how much physical memory is installed in the DNCS.

Swap Partition

The Swap Partition field lists the configured swap partitions in the DNCS and how large they are.

Note: You may sometimes hear the swap partition referred to as extended, virtual memory.

Disk Info

The Disk Info field displays information similar to what is displayed in the Disk Partition Info field. However, the information in the Disk Info field is displayed from a partition point of reference, rather than a metadevice point of reference.

Checking the Status of the Meta Devices of the System

The Checking the Status of the Meta Devices of the System field reports on the status of the system's mirrored disks and reports any disks that have failed.

Solaris Uptime

The Solaris Uptime field shows how long the Solaris operating system processes have been running without interruption.

DNCS Uptime

The DNCS Uptime field shows how long the DNCS processes have been running without interruption.

Note: To determine how long the DNCS processes have been running without interruption, the Doctor Report examines the **bootpd** process and determines how long the bootpd process has been running without interruption. The bootpd process is usually only restarted when the DNCS processes are reset.

DNCS Disk Partition Utilization

The data in the DNCS Disk Partition Utilization field lists all the disk partitions on the DNCS and displays the "in-use" percentage of each partition.

Important! Cisco recommends that no partition exceed 85 percent utilization.

Note: To decrease partition utilization, you can delete files that are no longer needed and core files that do not require analysis.

App Server Disk Partition Utilization

The data in the App Server Disk Partition Utilization field lists all the disk partitions on the Application Server and displays the "in-use" percentage of each partition.

Important! Cisco recommends that no partition exceed 85 percent utilization.

Note: To decrease partition utilization, you can delete files that are no longer needed and core files that do not require analysis.

DNCS and App Server Swap Space

The data in the DNCS and App Server Swap Space field lists the amount of available swap space on the DNCS and the Application Server.

Pioneer Note: Ignore swap space errors for sites that run the Pioneer resident application.

Important! Cisco recommends that the DNCS and Application Server swap space be greater than 200 MB.

Note: Completing the following tasks may increase your swap space:

- Close windows that do not need to be open.
- Stop and restart the DNCS.
- Run the **/usr/local/bin/top** utility and look for processes that use more than 50 MB of swap space. Use the dncsControl utility to stop and restart those processes.
- Look for large files in the /tmp directory. You can delete them or move them to another file system.

Database Tablespace Report

The data in the Database Tablespace Report field is divided into five sections and provides the following information about the database:

- **Database space usage summary**—provides detailed and summary information about database tables and extents.

  Notes:

  - This data appears only if there are database tables or indexes with 10 percent or less of free allocated space. If there is a table or an index that has 10 percent or less of free allocated space, the system will provide another extent for that table or index to grow.
  - System operators do not necessarily need to take any action if the system reports that there is a table or an index with 10 percent or less of free allocated space. As long as the calculations in the Recalculated future free database space section (later in this heading) do not produce an error, the system has enough room for the database to grow.

- **Preallocated summary database space usage**—provides summary data for the preallocated database space.
- **Current physical database space usage**—provides summary data for the physical database space.

- **Total free database space**—reports the total amount of free pre-allocated and physical database space.
- **Recalculated future free database space** —If the detail under the **Database space usage summary** section lists a table or an index that has 10 percent or less of free allocated space, this section provides a new calculation of preallocated database space based upon the additional extent that will be used.

  Notes:

  - This data appears only if there are database tables or indexes with 10 percent or less of free allocated space.
  - Call Cisco Services if the Recalculated future free database space section produces a warning.

Important! This data should be interpreted only by those individuals knowledgeable in database management.

DNCS Database Check

The data in the DNCS Database Check field summarizes the usage of tempspace and dataspace in the DNCS database.

Important! This data should be interpreted only by those individuals knowledgeable in database management.

Database Spaces and Chunks

The Database Spaces and Chunks field reports on the contents and structure of the database shared memory by running the Informix *onstat -d* command.

Important! This data should be interpreted only by those individuals knowledgeable in database management.

Database Extents for dncsdb

The data in the Database Extents for dncsdb field lists the number of extents associated with specific tables in the DNCS database.

Important! Be sure to read the section on ***Database Fragmentation, Database Used Capacity, and the Doctor Report*** (on page 79). The information in that section describes a condition under which system operators may see a significant increase in the percentage of the database in use after defragmenting the database than existed before defragmenting the database.

Notes:

- The number of database extents refers to the number of times a specific table is fragmented across the hard drive.
- A badly fragmented database may slow down database performance. Refer to the ***Monitor and Eliminate Database Fragmentation*** (on page 59) section in Chapter 5 if any of the following tables show 10 or more extents:
  - emm
  - hct_profile
  - pdkeycertificate
  - pdsernummap
  - secure_micro
  - sm_auth_profile
  - sm_pkg_auth

Database Extents for appdb

The data in the Database Extents for appdb field lists the number of extents associated with specific tables in the Application Server database.

Important! Be sure to read the section on ***Database Fragmentation, Database Used Capacity, and the Doctor Report*** (on page 79). The information in that section describes a condition under which system operators may see a significant increase in the percentage of the database in use after defragmenting the database than existed before defragmenting the database.

Notes:

- The number of database extents refers to the number of times a specific table is fragmented across the hard drive.
- A badly fragmented database may slow down database performance. Refer to the ***Monitor and Eliminate Database Fragmentation*** (on page 59) section in Chapter 5 if the prvdrneutraldata table shows 10 or more extents.

Database Backup Check

This field reports on the presence of a cron job to automatically back up the DNCS databases. If a cron job is present, this field reports whether the previous database backup was successful or if it failed.

Notes:

- A cron job is a program that runs automatically, without user intervention.
- The program that automatically backs up the database is a shell script called noinputDbBackup.sh. Your most recent system upgrade installation instructions may contain an appendix that describes how to configure your system for the automated database backup. The title of the appendix is **Setting Up an Automated Database Backup**.

DNCS Load Average

The data in the DNCS Load Average field shows the average number of DNCS processes simultaneously waiting for CPU time on the previous day.

Important! Cisco recommends that your DNCS load average remain under 2.0.

Note: The Doctor Report can determine the DNCS Load Average only if the Solaris **sar** utility is running. Refer to the UNIX man pages if you need to enable the sar utility.

Current DNCS Debug Flags Set

The data in the Current DNCS Debug Flags Set field lists the debugging flags that are currently enabled on the DNCS.

Important! The Doctor Report displays an error when debugging flag **A** or **a** – (DATA_CAROUSEL_CLASS) is enabled. When this flag is enabled, the Broadcast File System (BFS) server tends to run slowly.

Note: Debugging flags are enabled and disabled through the EMCDEBUG parameter in the .profile file on the DNCS. Call Cisco Services if you have any questions about your debugging flags.

Current Appserv Debug Flags Set

The data in the Current Appserv Debug Flags Set field lists the debugging flags that are currently enabled on the Application Server.

Pioneer Note: Debug flags do not apply to sites that run the Pioneer resident application.

Notes:

- Under most conditions, Cisco recommends that only debugging flags R or J be enabled for the Application Server.
- Debugging flags are enabled and disabled through the EMCDEBUG parameter in the .profile file on the Application Server. Call Cisco Services if you have any questions about your debugging flags.

DNCS Tracing Levels

This field appears in the Doctor Report only on systems that support code earlier than SR 2.5/SR 3.5.

The DNCS allows you to configure the level of detail reported by various system processes. The data in the DNCS Tracing Levels field lists all DNCS tracing levels that are set higher than 0 (zero).

Notes:

- Tracing is logged into the /var/log/dncsLog file on the DNCS.
- Tracing levels set higher than 0 (zero) run the risk of filling up the DNCS hard drives and slowing system performance.

Important! Unless you are using tracing for a specific reason, Cisco recommends that you set all of your DNCS tracing levels to 0 (zero). Call Cisco Services if you need help setting your DNCS tracing levels.

Appserv Tracing Levels

The Application Server allows you to configure the level of detail reported by various system processes. The data in the Appserv Tracing Levels field lists all Application Server tracing levels that are set higher than 0 (zero).

Notes:

- Tracing is logged into the /var/log/dncsLog file on the Application Server.
- Tracing levels set higher than 0 (zero) run the risk of filling up the Application Server hard drives and slowing system performance.

Important! Unless you are using tracing for a specific reason, Cisco recommends that you set all of your Application Server tracing levels to 0 (zero). Call Cisco Services if you need help setting your Application Server tracing levels.

DNCS Processes

The data in the DNCS Processes field lists all the DNCS processes and reports whether those processes are running, or not. Processes that are running are listed as **OK**; processes that are not running are listed as **Error**.

Important! Note the following recommendations regarding other processes that may not be running:

- Check the DNCS for core files.

  Note: The ***Recent DNCS Corefiles (last 2 days)*** (on page 44) field, lists recent DNCS core files.

- If the DNCS has a core file, contact Cisco Services.

  Note: Cisco Services may request that you send them the core file for analysis.

- Use the dncsControl utility to restart the stopped process(s).

App Server Processes

The data in the App Server Processes field lists all the Application Server processes and reports whether those processes are running, or not.

Pioneer Note: Ignore errors at sites that run the Pioneer resident application.

Note: It may be normal for the orbixd process to show as not running.

Important! Note the following recommendations regarding other processes that may not be running:

- Check the Application Server for core files.
- If the Application Server has a core file, contact Cisco Services.

  Note: Cisco Services may request that you copy the core file and send it to them for analysis.
- Use the appControl utility to restart the stopped process(s).

Recent DNCS Corefiles (last 2 days)

The data in the Recent DNCS Corefiles (last 2 days) field lists any core files saved to the DNCS within the last 48 hours.

Note: A core file indicates that a process on the DNCS failed unexpectedly.

Important! Call Cisco Services if the Recent DNCS Corefiles (last 2 days) section lists any core files. Cisco Services may request that you copy the core file and send it to them for analysis.

Recent App Server Corefiles (last 2 days)

The data in the Recent App Server Corefiles (last 2 days) field lists any core files saved to the Application Server within the last 48 hours.

Pioneer Note: Ignore errors at sites that run the Pioneer resident application.

Note: A core file indicates that a process on the Application Server failed unexpectedly.

Important! Call Cisco Services if the Recent App Server Corefiles (last 2 days) section lists any core files. Cisco Services may request that you copy the core file and send it to them for analysis.

DNS Check

The data in the DNS Check field reports whether the Domain Name Service (DNS) is running on the DNCS. The system lists **OK** when the DNS is not running; the system lists **Error** when the DNS is running.

Note: Having the DNS enabled on the DNCS may result in communication failures between the DNCS and modulators.

Important! If the DNS is enabled on the DNCS, disable it by editing the **/etc/nssswitch.conf** file so that the **hosts:dns** line reads as **hosts:files**.

Force Tune / Valid Service Check

The data in the Force Tune / Valid Service Check field lists all force-tune service IDs in the system that do not correspond to a valid SAM service. If the Doctor Report lists a service ID that is not associated with a valid service, reconfigure the service ID so that it is associated with a valid service.

DNCS License Check

The data in the DNCS License Check field reveals whether the following DNCS optional features are licensed or unlicensed:

- EAS FIPS Code Filtering
- DOCSIS DHCT Support
- Enhanced VOD Session Throughput
- VOD Session Encryption

Note: These optional features pertain only to sites running SR 2.1 and later system software. Contact Cisco to obtain licensing for a feature.

Unused SAM URL Check

The Unused SAM URL Check field provides a warning and a recommendation to run the chkSamUrl utility when the size of the bulk.tbl file is in danger of growing too large. When the bulk.tbl file grows too large, DHCTs may reboot and display a black screen.

Note: For information on running the chkSamUrl utility in order to reduce the size of the bulk.tbl file, see Appendix E, ***The chkSamUrl Utility*** (on page 237).

DNCS Install Options

The DNCS Install Options field reveals whether the following DNCS installation options, for SR 2.1 and later, have been enabled:

- DVB_SI

  Note: DVB_SI is the European standard for digitally broadcast channels.

- DNO

  Note: DNCS Network Overlay — refers to the Overlay feature.

- DNCS_NONSA

  Note: Pertains to the encryption method in use on the system — PowerKey or non-PowerKey. (DNCS_NONSA is non-PowerKey)

DNCS Non-Cisco Conditional Access Check

The DNCS Non-Cisco Conditional Access Check field examines the site configuration for the existence of certain files and variables to determine whether the site supports a non-Cisco conditional access method.

DNCS File Size Check

The DNCS File Size Check field lists files 50 MB or larger in the /dvs/dncs/tmp, /var/log, and /tmp directories.

Last Logging Time Stamp for Selected Processes

The Last Logging Time Stamp for Selected Processes field reports the current time and then lists the timestamp associated with the last time the emmDistributor and camAuditor processes wrote to their respective logfiles. System operators can compare the timestamps with the current time to determine whether the emmDistributor and camAuditor processes are running properly.

Note: The timestamp should not be more than a few minutes behind the current time. If you notice that the timestamp associated with the logfiles is more than 15 minutes behind the current time, contact Cisco Services.

DHCT Status Summary

The data in the DHCT Status Summary field provides a status summary of all DHCTs in the database, local and remote sites.

DHCT Type Summary

The data in the DHCT Type Summary field summarizes the number of DHCTs in the database, using each unique combination of DHCT type, revision, OUI, and software table of contents file (if any).

Notes:

- The system also reports the number of DHCTs in the database of type NULL.
- A DHCT of type NULL represents a DHCT that has no record in the database, but has attempted to sign on to the system.

  Important! Call Cisco Services if you have a large number of DHCTs, relative to system size, with a type of NULL.

DHCTs with EMMs Expiring in 15 days

The data in the DHCTs with EMMs Expiring in 15 days field lists the MAC addresses of up to 50 DHCTs in the database that have EMMs set to expire within 15 days.

Notes:

- If the number of DHCTs with EMMs set to expire within 15 days exceeds 50, the system creates a file containing a complete list of those DHCTs.
- The file is called emms.expiring.soon and is found in the /export/home/dncs/doctor directory.

Important! Call Cisco Services if you have any DHCTs with EMMs set to expire within 15 days.

VER, OS and ResApp files

The data in the VER, OS and ResApp files field lists all software table of contents (VER), operating system (OS), and resident application (RES APP) files loaded on to the DNCS.

CVT Configuration Check

The data in the CVT Configuration Check field includes the names and sizes of all of the DHCT image files loaded onto the system. In addition, the CVT Configuration Check field lists all of the DHCT groups that currently have DHCT download assignments.

DHCT counts per QPSK

The data in the DHCT counts per QPSK field lists the number of DHCTs that communicate with each QPSK modulator and demodulator in the system. In addition, under the Node Set Name / HCT Count subheading, the field lists all of the defined node sets on the system, as well as the number of DHCTs assigned to each node set.

Active Elements

The data in the Active Elements field reports the number of active QAM, MQAM, GQAM, and GoQAM modulators, QPSK modulators and demodulators, hubs, headends, channel maps, and service groups active on the DNCS.

Offline QAMs

The data in the Offline QAMs field lists any QAM modulator listed in the database as offline.

Mod Slot Tolerance

The data in the Mod Slot Tolerance field confirms that the slot tolerances of all QPSK modulators is 2.2 microseconds.

Important! If the system reports a QPSK modulator with a slot tolerance that is not 2.2 microseconds, change the slot tolerance for that modulator and then reset the modulator.

Sources, Source Definitions, Segments and Sessions

The data in the Sources, Source Definition, Segments and Sessions field lists the number of the following items configured on the DNCS:

- Digital and Analog Sources
- Digital and Analog Source Definitions
- Digital and Analog Encrypted Sources
- Digital and Analog Segments
- Digital and Analog Encrypted Segments
- Active continuous feed sessions
- Active exclusive sessions

In addition, the Sources, Source Definition, Segments and Sessions section flags as an error source IDs that have multiple segments.

Note: Unless your system is configured for analog descrambling, you should have no encrypted analog sources or segments.

Source Definitions for Active CF Sessions

The data in the Source Definitions for Active CF Sessions field verifies that a source definition exists for each active digital session configured on the DNCS. The system records an Error for each session that does not have a source definition.

Important! If a source definition does not exist for an active session, use the DNCS user interface to create one.

Active Subscriber Packages

The data in the Active Subscriber Packages field lists the number of active subscriber packages configured on the DNCS.

SI_INSERT_RATE

The data in the SI_INSERT_RATE field lists the calculated and the current value of the SI_INSERT_RATE variable.

Notes:

- The SI_INSERT_RATE variable represents how long it takes for a DHCT to get system information (SI).
- The calculated value is based on the number of hubs and virtual channel table (VCT) entries.
- The Doctor Report verifies that the current value of the SI_INSERT_RATE variable is 100 percent of the calculated value. A rate of 0 (zero) indicates that SI is only being sent out-of-band.
- The Doctor Report also verifies that the SI_INSERT_RATE variable is spelled correctly and is shown with all capital letters in the DNCS .profile file.

Important! Note these important points about the SI_INSERT_RATE variable:

- If the system reports that the current SI_INSERT_RATE variable is less than 100 percent of the calculated variable, contact Cisco Services for assistance.
- If the system reports that the SI_INSERT_RATE variable is misspelled in the .profile file, use a text editor to correct the spelling.

SI Out-of-band Interval

The SI Out-of-band Interval lists how often out-of-band data is sent to DHCTs.

System Time Message Delivery

If debug flag **D** is set in the EMCDEBUG variable in the .profile file, the data in the System Time Message Delivery field confirms whether the system time message (STM) has been sent to DHCTs within the past 12 seconds.

Important! If the Doctor Report reports that STMs are not being delivered every 12 seconds, use the dncsControl utility to restart the siManager process.

Distinguished SI QAM

The data in the Distinguished SI QAM field identifies the QAM modulator that is used by DHCTs for SI retrieval, as well as the IP address of that QAM modulator.

Notes:

- In SR 2.2 and later systems, a candidate for the Distinguished QAM is any QAM that is not associated with a hub.
- If the qamManager logs are not available, the QAM frequency, the QAM IP address, and the QAM name display as UNKNOWN.

QAMs Not Associated With Either a Hub or Service Group

The data in the QAMs Not Associated with either a Hub or Service Group field lists those QAM modulators that are not associated with a hub or a service group. Unless a QAM is configured to deliver SI, it should be associated with a hub.

Duplicate QAM Frequencies Within Service Groups

The data in the Duplicate QAM Frequencies within service groups field lists any QAM modulator configured with a frequency used by another QAM modulator in the same service group.

DNCS/App Server Time Sync

The data in the DNCS/App Server Time Sync field reports on the following system time details:

- Time differences between the DNCS and the Application Server
- Network time protocol used on the DNCS and the Application Server (xntpd or ntpd)
- Time synchronization source (local or GPS)

Pioneer Note: Ignore errors at sites that run the Pioneer resident application.

Important! If the system reports an error in the time synchronization between the DNCS and the Application Server, change the time on the Application Server.

Timezone and Daylight Savings Time Check

The data in the Timezone and Daylight Savings Time Check field summarizes the time zone and daylight savings time (DST) settings for hubs and DHCTs.

Note: The DHCT Summary section should show **Follow hub** in the columns **Timezone Offset** and **DST Observed**.

Important! If the DHCT Summary section shows **Yes** or **No** in the **DST Observed** column, contact Cisco Services for assistance in configuring all DHCTs to follow the time of the hub to which they belong.

PPV Services and Events

The data in the PPV Services and Events field reports the number of active PPV services and the total number of PPV events defined on the system. In addition, this section reports the number of PPV events inside the various Marketing, Advertising, Buy (GBAM), and Event windows.

Pioneer Note: It is normal for sites that run the Pioneer resident application to show NONE.

PPV and SAM Service Discrepancies Found

The data in the PPV and SAM Service Discrepancies field verifies that the PPV service data for active PPV services matches the associated SAM service data. The following items are verified:

- Count of services
- PPV service index
- SAM service ID
- PPV and SAM service short descriptions

Pioneer Note: It is normal for sites that run the Pioneer resident application to show NONE.

Important! Resolve discrepancies by using the DNCS user interface to modify the incorrect PPV services. Call Cisco Services if you need assistance.

PPV Event Use Service Information

The data in the PPV Event Use Service Information field verifies that the event use service (EUS) for each active PPV service is an active, encrypted digital service.

Pioneer Note: It is normal for sites that run the Pioneer resident application to show NONE.

Important! If the EUS for each active PPV service is not an active, encrypted digital service, call Cisco Services for assistance in making the necessary corrections.

PPV File Check

The data in the PPV File Check field verifies the following two conditions:

- The files (**advance0, immediate, index,** and **services0**) in the /dvs/appFiles directory have been updated within the last hour.

  Note: On a live system, this is a general health indicator of PPV service because it confirms that the **ppvServer** and **ppvFileserver** processes are regularly updating PPV files.

- All events in the **immediate** file are also in the **advance0** file.

Pioneer Note: Ignore errors at sites that run the Pioneer resident application.

Important! If the Doctor Report indicates an error, call Cisco Services for assistance in making any necessary corrections.

PPV Events phoneactivetime Check

The data in the PPV Events phoneactivetime Check field verifies that the **phoneactivetime** parameter for all PPV events is a meaningful value and that the base time in the PPV files is appropriate. Infrequently, a problem in defining PPV events from a billing system will result in a **phoneactivetime** of zero, which leads to a false PPV base time.

Pioneer Note: It is normal for sites that run the Pioneer resident application to show NONE.

Important! If the Doctor Report indicates an error, call Cisco Services for assistance in making any necessary corrections.

EUT Update Check

The data in the EUT Update Check field verifies that the entitlement unit table (EUT) has been updated within the last hour. An EUT that has been updated within the last hour indicates that the camPsm process on the DNCS is functioning properly.

Important! If the Doctor Report indicates an error, call Cisco Services for assistance in making any necessary corrections.

GBAM Delivery

Assuming debug flag **K** is enabled in the EMCDEBUG parameter, the data in the GBAM Delivery field verifies that time of day (TOD) and purchase GBAMs are delivered.

Notes:

- Purchase GBAMs can be verified only if there are PPV events with an open Buy window.
- Ideally, purchase GBAMs are delivered every 20 seconds and TOD GBAMs every 15 seconds. However, the Doctor Report verifies that these GBAMs have been delivered within the previous 60 seconds.

Important! If the Doctor Report indicates that GBAMs are not being delivered in a timely manner, call Cisco Services.

BFS Carousel and OSM Sessions Status

The data in the BFS Carousel and OSM Sessions Status field verifies that all BFS carousels are running and reports the data rate and indication interval of each carousel. The BFS Carousel Status field reports the combined total of all out-of-band carousels and of all inband carousels. This field reports for site DNCS as well as any remote site, if applicable.

Important! Refer to *Recommendations for Data Carousel Rate Management Technical Bulletin*, for the latest data rate recommendations.

BFS Session Status

The data in the BFS Session Status field verifies the following conditions:

- All BFS sources have an active session
- All sessions have a defined source

Important! If a BFS source does not have an active session, or if all sessions do not have a defined source, you have to create them. Call Cisco Services if you need help in creating a session or a source.

Miscellaneous BFS Check

The data in the Miscellaneous BFS Check field verifies the following conditions:

- No more than one dataCarousel process is running for a given BFS source.
- All BFS source definitions are present and are not duplicated.

  Note: If a BFS source definition is not present, the source definition will not be in SI and the DHCT will be unable to tune to that carousel.
- No BFS source is encrypted.

Important! Note these important points about errors in the Miscellaneous BFS Check field:

- Refer to *Recommendations for Data Carousel Rate Management Technical Bulletin*, or your appropriate upgrade installation instructions for assistance in setting data rates.
- Passport sites, or sites running interactive applications (VOD, games, etc.) may generate data rate errors. Refer to one of the previously mentioned documents for assistance in setting data rates.

Note: The dataCarousel processes are referred to as dataPump processes in SR 1.4 and later.

IPG Collector Report

The data in the IPG Collector Report field reports on the success or failure of the last running of the IPG Collector process.

Important! If your data reveals that the IPG Collector failed to run, verify that you can log on to the site of your content provider. You may have network issues that prevent the IPG Collector from running.

IPG Data Files

The data in the IPG Data Files field verifies that the number of days of IPG data files on the system matches the number specified in the ipgcollectconfig table in the database. Additionally, the data in the IPG Data Files field reports the size of the IPG data files.

Pioneer Note: Ignore errors at sites that run the Pioneer resident application.

Important! Note these important points about errors in the IPG Data Files field:

- You may not have your IPG services mapped correctly.
- Your content provider may not be providing you with data for the channels you need.
- The content provider may be posting files after your IPG Collector runs. You may need to reschedule the time you run the IPG Collector.
- If IPG data files are smaller than expected, your IPG provider probably did not create or post your files correctly. Contact your IPG provider.
- Finally, run the ipgCollector manually. Then, use the appControl utility to stop and restart the ipgServer process on the Application Server.

Note: IPG data files typically are large files (100 KB). Small files are therefore flagged as errors.

Ping All Active Elements

The data in the Ping All Active Elements field reports whether the communication path between the DNCS and the following system devices is active:

- All active QAM-family modulators
- All active QPSK modulators (Ethernet and RF)
- The BIG
- The TED

Important! If the Doctor Report reports an error, complete the following tasks to troubleshoot the error:

- Visually check that the device is powered on and that the cabling is secure.
- Use a network analyzer to confirm that IP traffic is reaching the device.
- Reboot the device.

DoctorRemote

The Doctor Report reports on the configuration of any remote site supported by the system. The information collected from remote sites is similar to the information collected from the DNCS. The following list contains the fields reported on for the remote sites:

- System Name
- All SAI Installed Package Information
- LIONN Info
- LIONN Disk Partition Utilization
- LIONN Swap Space
- LIONN Database Log Check

  Note: This field appears only for remote sites. The LIONN Database Log Check field reports on the size of the /dvs/lionndb/liondb.log and /dvs/lionndb/lionnconnection.log files.
- LIONN Database Process Check

  Note: This field appears only for remote sites. The LIONN Database Process Check field reports on whether the Informix daemon processes are running.
- LIONN Load Average
- Current LIONN Debug Flags Set
- LIONN Processes
- Recent LIONN Corefiles (last 2 days)
- DNS Check
- Force Tune / Valid Service Check
- LIONN File Size Check
- Timezone and Daylight Savings Time Check
- EUT Update Check
- BFS Carousel and OSM Sessions Status
- Miscellaneous BFS Check
- Ping All Active Elements

5

Manage the Database with the dncsDbData Utility

Introduction

The dncsDbData utility helps system operators and Cisco engineers manage the database of the DNCS and the Application Server. Through dncsDbData, system operators and Cisco engineers can perform the following operations on their database:

- Unload and load the DNCS and Application Server database to/from a tape or the hard drive of the DNCS
- Obtain DNCS platform information
- Defragment the DNCS and Application Server databases

  Note: For an explanation of database fragmentation and instructions on how to defragment the database, read ***Monitor and Eliminate Database Fragmentation*** (on page 59).

Read the remainder of this chapter for details on each operation.

Important! The procedures to unload and load the database require that the system components be shut down-often for an extended period of time. Be sure to perform these operations during a time frame when system activity is at a minimum, or during a maintenance window.

In This Chapter

- Monitor and Eliminate Database Fragmentation 59
- The dncsDbData Options 63
- Unload the Database 65
- Load the Database 73
- Database Fragmentation, Database Used Capacity, and the Doctor Report 79
- Obtain System Platform Information 83
- Obtain the Version Number of the dncsDbData Utility 84

Monitor and Eliminate Database Fragmentation

Introduction

Over time, the database on the DNCS becomes fragmented as related data is divided into pieces and stored at various locations throughout the hard drive. Database fragmentation occurs normally as the system is continually creating, deleting, and modifying records. A badly fragmented database slows down system performance as the system must search the entire hard drive to build or retrieve a record.

Several of the utilities contained in the DNCS Utilities are designed to help system operators minimize the effects of database fragmentation. System operators who want to avoid a fragmented database should follow the recommendations set forth in the remainder of this section.

Run and Analyze the Doctor Report

Run and analyze the output of the Doctor Report on a regular basis. Pay attention to the headings in the report called **Database Table Extents for dncsdb** and **Database Table Extents for appdb**. The number of extents associated with a few specific tables provides the operator with some warning that the database is becoming fragmented.

Note: The *number of table extents* refers to the number of times a specific table is fragmented across the hard drive.

System operators should monitor the Doctor Report for the number of extents associated with the following DNCS database tables:

- emm
- hct_profile
- pdkeycertificate
- pdsernummap
- secure_micro
- sm_auth_profile
- sm_pkg_auth

Additionally, system operators should monitor the Doctor Report for the number of extents associated with the prvdrneutraldata table in the Application Server database.

If the Doctor Report indicates that the number of extents for any of these tables has reached 10, system operators should plan to run specific utilities designed to defragment the database. Once the number of extents has reached 30, system performance is negatively affected.

Select Which Database to Defragment

Choose one of the following database defragmentation procedures:

- Go to ***Eliminating Database Fragmentation in the DNCS Database*** (on page 60) to defragment the DNCS database.
- Go to ***Eliminating Database Fragmentation in the Application Server Database*** (on page 61) to defragment the Application Server database

Eliminating Database Fragmentation in the DNCS Database

When the Doctor Report indicates that the number of extents associated with any of the previously mentioned DNCS database tables has reached 10, system operators should plan to run the following procedures.

Important! The following procedures are in outline form, only. Be sure to refer to the specific procedures referenced in each step when eliminating database fragmentation.

1 Run the dbOptimizer program to delete unneeded EMMs from the database.

Note: Procedures for running the dbOptimizer program are found in Chapter 2, Delete Unneeded EMMs With the dbOptimizer Program.

2 Back up the database.

Notes:

- Refer to the appropriate backup and restore procedures for instructions on how to back up the database.
- When you back up the database, the system backs up both the DNCS database and the Application Server database

3 Run the dncsDbData utility using the -*z* option to determine whether you can unload the DNCS database to the hard drive of the DNCS.

Note: Refer to ***Unloading the Database to the Hard Drive*** (on page 68) procedure for specific instructions on how to use the -*z* option.

4 Run dncsDbData with the -*u* option to unload the DNCS database.

Notes:

- Procedures for running the dncsDbData utility with the -*u* option are found in ***the Unload the Data***base (on page 65) section, later in this chapter.
- You may have old backup files on your DNCS that you can remove in order to conserve space. Contact Cisco Services for help in removing old files.

5 Run dncsDbData with the *-l* option to drop the DNCS database and then reload it.

Notes:

- Dropping the database and then reloading it eliminates the fragmentation.
- Procedures for running the dncsDbData utility with the *-l* option are found in ***Load the Database*** (on page 73).
- You are instructed to restart the system components after reloading the database.

6 Back up the database again.

Eliminating Database Fragmentation in the Application Server Database

When the Doctor Report indicates that the number of extents associated with the prvdrneutraldata table in the Application Server database has reached 10, system operators should plan to run the following procedures on the DNCS.

Important! The following procedures are in outline form, only. Be sure to refer to the specific procedures referenced in each step to eliminate database fragmentation.

1 Run the dbOptimizer program to delete unneeded EMMs from the database.

Note: Procedures for running the dbOptimizer program are found in Chapter **2, *Delete Unneeded EMMs with the dbOptimizer Prog***ram (on page 13).

2 Back up the database.

Notes:

- Refer to the appropriate backup and restore procedures for instructions on how to back up the database.
- When you back up the database, the system backs up both the DNCS database and the Application Server database.

3 Run the dncsDbData utility using the *-z* option to determine whether you can unload the Application Server database to the hard drive of the DNCS.

Note: Refer to ***Unloading the Database to the Hard Drive*** (on page 68) for specific instructions on how to use the *-z* option.

4 Run dncsDbData with the *-u* option to unload the Application Server database.

Note: Procedures for running the dncsDbData utility with the *-u* option are ***found in Unload the*** Database (on page 65).

5 Run dncsDbData with the *-l* option to drop the Application Server database and then reload it.

Notes:

- Dropping the database and then reloading it eliminates the fragmentation.
- Procedures for running the dncsDbData utility with the *-l* option are found in ***Load the Database*** (on page 73).
- You will restart the system components after reloading the database.

6 Back up the database again.

The dncsDbData Options

Generating a List of dncsDbData Options

Follow these steps to generate a list of options that you can use when you run the dncsDbData utility.

1 Open an xterm window on the DNCS.

2 Type **su** and then press **Enter** to log in as root user.

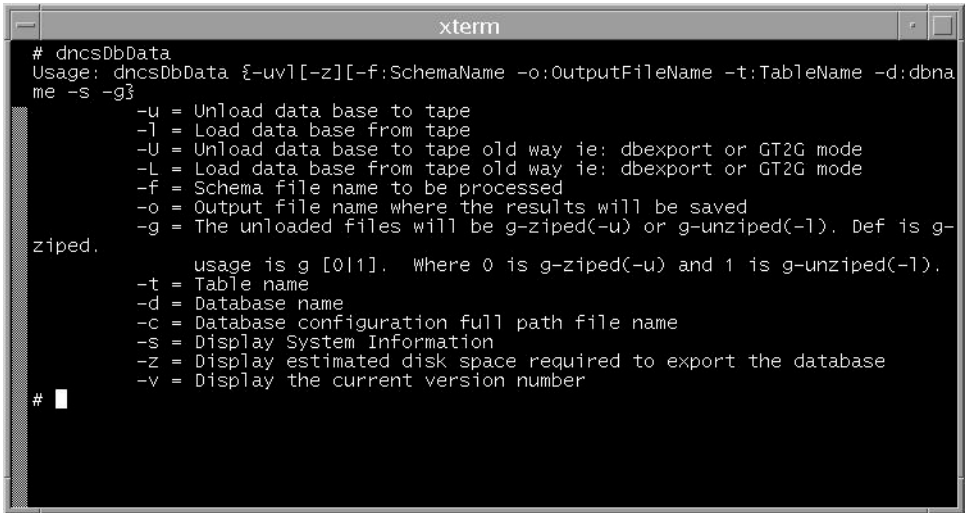
3 Type the root password and then press **Enter**.

4 Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. This command establishes the DNCS environment as a root user.

Important! Type the period followed by a space before typing /dvs.

Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.

5 Type **dncsDbData** and then press **Enter**. The system displays a list of options you can use when you run the dncsDbData utility.



Note: Refer to the remaining sections in this chapter for specific instructions regarding the use of the dncsDbData options listed in the illustration.

Comments on Three Options

The following dncsDbData options require special comment:

- *-U* and *-L*. Cisco engineers may occasionally want to unload and load a database without using the high-performance features introduced with SR 2.1 and SR 3.0.

  Important! Cisco recommends that use of the *-U* and *-L* options be restricted to Cisco engineers, only.

- *-g*. Cisco engineers designed the *-g* option to implement the gzip and gunzip file compression and uncompression utilities when loading and unloading database tables to the hard drive. In some cases, a database unload operation that would otherwise not fit into an existing filesystem on the DNCS or Application Server, will fit if the *-g* option is used in conjunction with the *-u* option. Instructions later in this chapter advise system operators to call Cisco if they discover that an unload of their database will not fit into an existing filesystem.

  Important! Cisco recommends that system operators do not use the *-g* option when unloading their database unless instructed to do so by Cisco Services.

Unload the Database

Introduction

The dncsDbData utility enables you to unload the DNCS and Application Server database to tape or to the hard drive on the DNCS. Follow the instructions in this section to unload the DNCS or Application Server database.

Note: When you unload a database, you write the contents of the database to a file.

Before You Begin

Before you unload your database, Cisco recommends that you first run the dbOptimizer script. The dbOptimizer script removes unneeded EMMs from the database, reducing the size of the database that you unload. If you have not previously configured dbOptimizer to run automatically in a cron job, follow the procedures in Chapter 2, ***Delete Unneeded EMMs with the dbOptimizer Program*** (on page 13), to remove unneeded EMMs from your database.

Unloading the Database to Tape

If you want to unload your DNCS or Application Server database to the hard drive of the DNCS, go to ***Unloading the Database to the Hard Drive*** (on page 68).

You need a blank 4-mm or 8-mm tape (depending upon your tape drive) to unload the DNCS or Application Server database to tape.

Follow these instructions to unload your DNCS or Application Server database to tape.

1. Stop all third-party applications.
2. Follow the procedures in Appendix A, ***Stopping System Components*** (on page 203), to shut down Spectrum, the Application Server, and the DNCS.

   Important! All processes on the DNCS and the Application Server must be stopped when you unload or load the database.
3. Open an xterm window on the DNCS.
4. Type **su -** and then press **Enter** to log in as root user. The password prompt appears.
5. Type the root password and then press **Enter**.
6. Type **/etc/rc2.d/S75cron stop** and then press **Enter**. The system stops all cron jobs on the DNCS.

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

   a Type **rsh appservatm** and then press **Enter**.

   b Type **/etc/rc2.d/S75cron stop** and then press **Enter**.

   c Type **exit** and then press **Enter**.

8 Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. This command establishes the DNCS environment as a root user.

   Important! Type the period followed by a space before typing /dvs.

   Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.

9 Type **showActiveSessions** and then press **Enter**. A display showing any active DNCS sessions appears.

10 Are there any active DNCS sessions?

   - If **yes**, type one of the following commands:
     - To kill all active sessions *at once*, type **killActiveSessions** and then press **Enter**; go to step 11.
     - To kill each process *individually*, type **kill [PID]** and then press **Enter**, where [PID] is the process ID associated with the active session; go to step 11.
   - If **no**, the DNCS will display a message similar to **dncsDbServer is idle**; go to step 11.

11 Label a blank tape with the following information:

   [DNCS or Application Server] Database Unload

   [Site Name]

   [Date]

   Notes:

   - Substitute DNCS or Application Server for [DNCS or Application Server], depending on which database you are unloading.
   - Substitute your site name for [Site Name].
   - Substitute today's date for [Date]

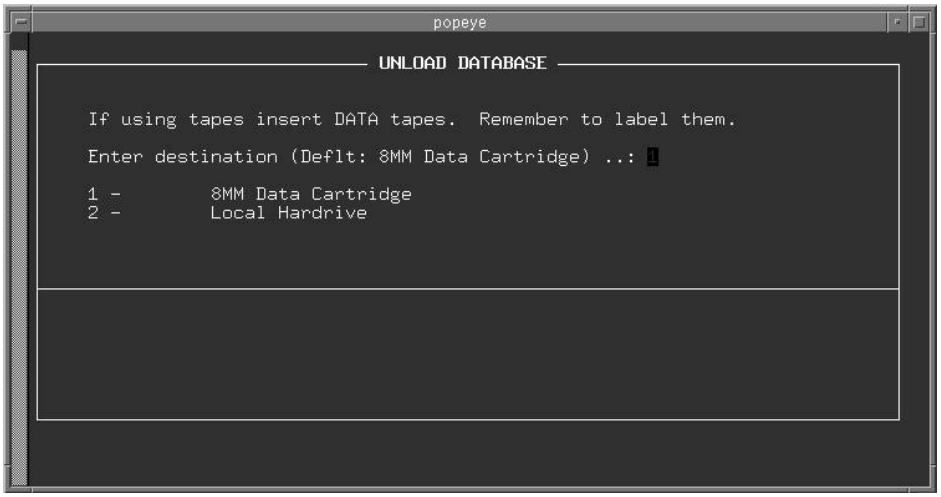
12 Insert the blank tape into the tape drive of the DNCS.

13 Choose one of the following options:

- If you are unloading the DNCS database to tape, type **dncsDbData -u** and then press **Enter**.
- If you are unloading the Application Server database to tape, type **dncsDbData -u -d appdb -c /dvs/appFiles/dbConfig/appDbConfig** and then press **Enter**.

  Note: The directory path following the *-c* option specifies the location of the appdb configuration files.

Result: The Unload Database window appears.



14 Press **Enter**. The **Is the above information correct? (Y/N)** message appears.

Note: The tape drive is the default destination.

15 Type **y** (for yes) and then press **Enter**. The following message appears:

Please wait while unloading data to tape.

Performing export on database [dncsdb or appdb].

Please mount the tape and press return to continue.

16 When the database has been unloaded, eject the tape and store it in a safe place.

17 Are you planning to load your database immediately?

- If **yes**, skip to **Load the Database**, later in this chapter.
- If **no**, type **/etc/rc2.d/S75cron start** and then press **Enter**.

Note: You should still be root user.

Result: The system restarts the DNCS cron jobs.

18 Follow the procedures in Appendix B, ***Restarting System Components*** (on page 207), to restart the DNCS, the Application Server, and Spectrum.

19 Follow these instructions to restart the Application Server cron jobs.

a Type **rsh appservatm** and then press **Enter**.

b Type **/etc/rc2.d/S75cron start** and then press **Enter**.

c Type **exit** and then press **Enter**.

20 Examine the cron files on both the DNCS and Application Server and determine whether any cron jobs should have executed during the period when the cron jobs were stopped.

Note: You may have to manually execute these cron jobs.

Unloading the Database to the Hard Drive

Follow these instructions to unload your DNCS or Application Server database to the hard drive of the DNCS.

1 Stop all third-party applications.

2 Follow the procedures in Appendix A, ***Stopping System Components*** (on page 203), to shut down Spectrum, the Application Server, and the DNCS.

Important! All processes on the DNCS and the Application Server must be stopped when you unload or load the database.

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

4 Type **su -** and then press **Enter** to log in as root user. The password prompt appears.

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

6 Type **/etc/rc2.d/S75cron stop** and then press **Enter**. The system stops all cron jobs on the DNCS.

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

a Type **rsh appservatm** and then press **Enter**.

b Type **/etc/rc2.d/S75cron stop** and then press **Enter**.

c Type **exit** and then press **Enter**.

8 Type **cd /dvs/backups** and then press **Enter**. The /dvs/backups directory becomes the working directory.

Note: Cisco recommends that you store your database backups in a subdirectory within the /dvs/backups directory.

9 Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. This command establishes the DNCS environment as a root user.

Important! Type the period followed by a space before typing /dvs.

Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.

10 Type **showActiveSessions** and then press **Enter**. A display showing any active DNCS sessions appears.

11 Are there any active DNCS sessions?

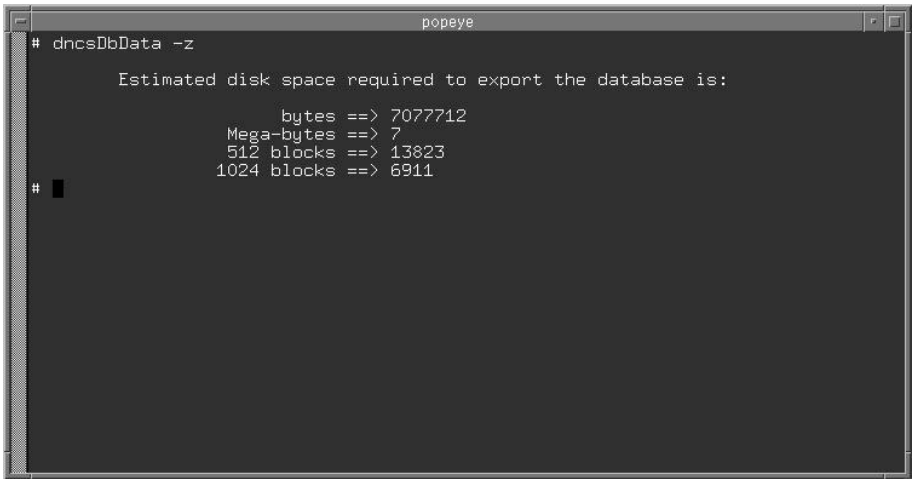
- If **yes**, type one of the following commands:
  - To kill all active sessions *at once*, type **killActiveSessions** and then press **Enter**; go to step 12.
  - To kill each process *individually*, type **kill [PID]** and then press **Enter**, where [PID] is the process ID associated with the active session; go to step 12.
- If **no**, the DNCS will display a message similar to **dncsDbServer is idle**; go to step 12.

12 Choose one of the following options:

- If you are unloading the DNCS database to the hard drive of the DNCS, type **dncsDbData -z** and then press **Enter**.
- If you are unloading the Application Server database to the hard drive of the DNCS, type **dncsDbData -z -d appdb -c /dvs/appFiles/dbConfig/appDbConfig** and then press **Enter**.

  Note: The directory path following the *-c* option specifies the location of the appdb configuration files.

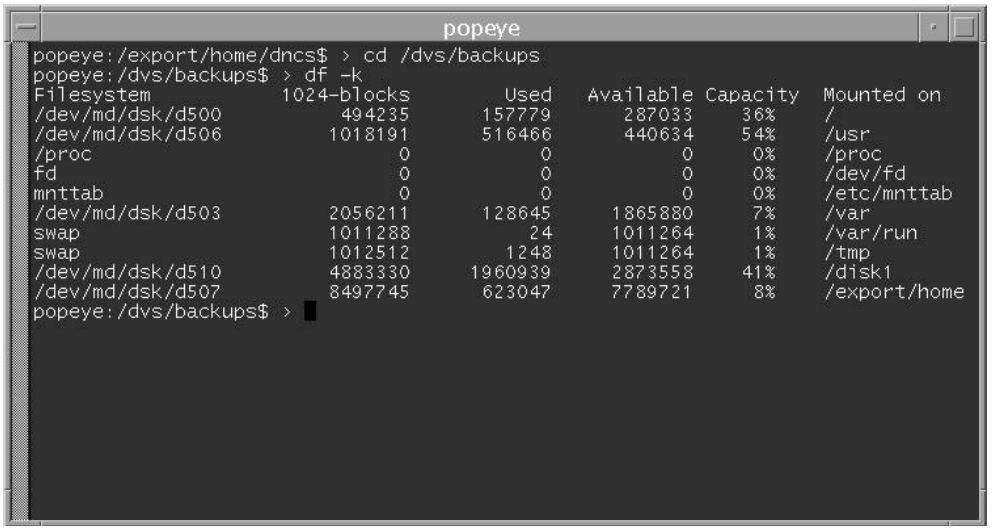
Result: The system displays how much disk space is required to store the unloaded database.



Example: Notice the number of 1024-blocks required to store the database. In this example, the system requires 6,911 1024-blocks to store the DNCS database.

13 Write the number of 1024-blocks required to store the database in the space provided: _____

14 Type **df -k** and then press **Enter**. The system displays the number of free disk blocks available in the mounted filesystems on the DNCS.



15 Do any one of the /disk1, /var, or /export/home filesystems have more free disk blocks than the number you recorded in step 13?

- If **yes**, go to step 16.
- If **no**, call Cisco Services.

  Notes:

  – Cisco Services engineers may instruct you to unload your database using the *-g* option. The *-g* option compresses your database as the database unloads.

  – If Cisco Services engineers advise you against using the *-g* option, they may then advise you to remove unneeded files from your system.

  – If you still do not have enough room on your hard drive to unload your database, you have no alternative other than to unload your database to a tape. Follow the instructions in ***Unloading the Database to Tape*** (on page 65).

16 Follow these instructions.

a Type **cd [filesystem]** and then press **Enter**.

Example: cd /export/home

b Type **df -k .** and then press **Enter**. The system displays how much space is available in the selected filesystem.

Important! Be sure to type the period, preceded by a space, after typing df -k.

c Double-check that the selected filesystem has more space available than the number you recorded in step 13.

Note: Try another filesystem if the filesystem you selected does not have enough space.

17 Type **mkdir db_dir.[MM.DD.YY_HH.MM]** and then press **Enter** to create a subdirectory within the current directory.

Note: Substitute the current month, date, year, hour, and minute for [MM.DD.YY_HH_MM].

Example: mkdir db_dir.12.15.00_08.45

18 Type **cd [directory name]** and then press **Enter**. The directory you just created becomes the working directory.

Example: cd db_dir.12.15.00_08.45

19 Type **pwd** and then press **Enter**. The system displays the complete path to the directory you just created.

20 Write the complete path name on the line provided.

_____

Note: You will need this path name when you load the database.

21 Choose one of the following options:

- If you are unloading the DNCS database to the hard drive of the DNCS, type **dncsDbData -u** and then press **Enter**.
- If you are unloading the Application Server database to the hard drive of the DNCS, type **dncsDbData -u -d appdb -c /dvs/appFiles/dbConfig/appDbConfig** and then press **Enter**.

  Note: The directory path following the -c option specifies the location of the appdb configuration files.

Result: The Unload Database window appears.

22 Type **2** and then press **Enter**. The **Is the above information correct? (Y/N)** message appears.

23 Type **y** and then press **Enter**. The **Enter backup directory (Default: Current Directory)** message appears.

24 Press **Enter**. The Is the above information correct? (Y/N) message appears.

25 Type **y** and then press **Enter**. The system unloads your database to the current directory.

26 Have you just unloaded your database as part of the defragmentation process, as described in the ***Monitor and Eliminate Database Fragmentation*** (on page 59) section, or are you planning to load your database immediately?

- If **yes**, go to ***Load the Database*** (on page 73).

  Note: System components must remain stopped when you load the database.
- If **no**, type **/etc/rc2.d/S75cron start** and then press **Enter**. The system restarts the DNCS cron jobs.

27 When the database has been unloaded, follow the procedures in Appendix B, ***Restarting System Components*** (on page 207), to restart the DNCS, the Application Server, and Spectrum.

28 Follow these instructions to restart the Application Server cron jobs.

   a Type **rsh appservatm** and then press **Enter**.

   b Type **/etc/rc2.d/S75cron start** and then press **Enter**.

   c Type **exit** and then press **Enter**.

29 Examine the cron files on both the DNCS and Application Server and determine whether any cron jobs should have executed during the period when the cron jobs were stopped.

   Note: You may have to manually execute these cron jobs.

Load the Database

Introduction

The dncsDbData utility enables you to load the DNCS or Application Server database from tape or from your local hard drive.

Note: To load the database means to insert data from a file into an existing database.

CAUTION:

If your DNCS has been running since you unloaded the database, the load process will overwrite any changes to the database since the unload process began.

Defragmenting the Database

When you load the database, the following actions occur:

- The system drops the existing database.
- The system rebuilds the database as it reloads the data from the ASCII files created during the unload procedure. See ***Unload the Database*** (on page 65).
- The system turns on database logging.

When your system rebuilds the database, it rebuilds it at one contiguous location on the hard drive, which eliminates any previous database fragmentation. As a result, system performance is improved.

Loading the Database from Tape

Follow these instructions to load your DNCS or Application Server database from tape.

1 Stop all third-party applications.

2 If necessary, follow the procedures in Appendix A, ***Stopping System Components*** (on page 203), to shut down Spectrum, the Application Server, and the DNCS.

Important! All processes on the DNCS and the Application Server must be stopped when you unload or load the database.

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

Important! Skip steps 4, 5, and 6 if you have already logged in to the xterm window as root user and have executed the dncsSetup command.

4 Type **su -** and then press **Enter** to log in as root user. The password prompt appears.

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

6 Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. This command establishes the DNCS environment as a root user.

Important! Type the period followed by a space before typing /dvs.

Note: The system may also return a message that ends with -o bad options or -o: bad options. Ignore this message; it is normal.

7 Have you just unloaded your database?

- If **yes**, you have already stopped the DNCS and Application Server cron jobs; go to step 9.
- If **no**, type **/etc/rc2.d/S75cron stop** and then press **Enter**. The system stops all cron jobs on the DNCS.

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

a Type **rsh appservatm** and then press **Enter**.

b Type **/etc/rc2.d/S75cron stop** and then press **Enter**.

c Type **exit** and then press **Enter**.

9 Insert the tape containing your most recent unload of the database into the tape drive of the DNCS.

10 Type **showActiveSessions** and then press **Enter**. A display showing any active DNCS sessions appears.

11 Are there any active DNCS sessions?

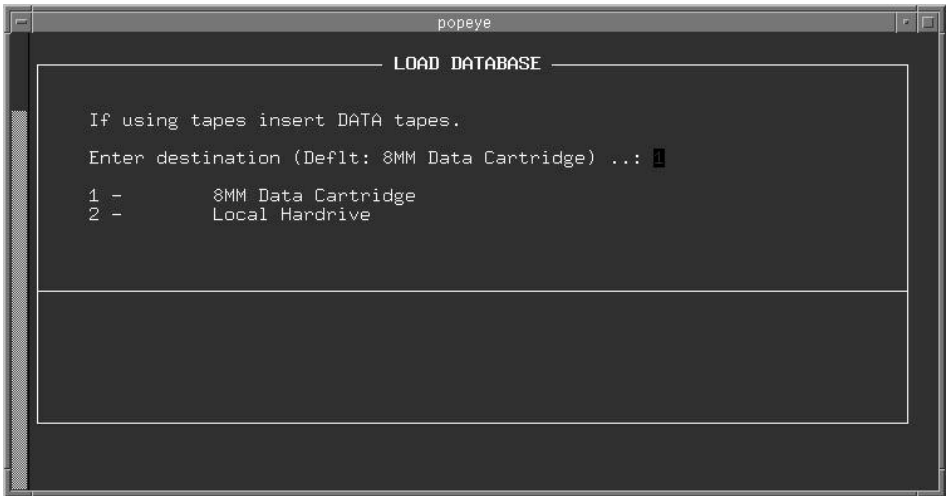
- If **yes**, type one of the following commands:
  - To kill all active sessions *at once*, type **killActiveSessions** and then press **Enter**; go to step 12.
  - To kill each process *individually*, type **kill [PID]** and then press **Enter**, where [PID] is the process ID associated with the active session; go to step 12.
- If **no**, the DNCS will display a message similar to **dncsDbServer is idle**; go to step 12.

12 Choose one of the following options:

- If you are loading the DNCS database from a tape in the tape drive of the DNCS, type **dncsDbData -l** and then press **Enter**.
- If you are loading the Application Server database from a tape in the tape drive of the DNCS, type **dncsDbData -l -d appdb -c /dvs/appFiles/dbConfig/appDbConfig** and then press **Enter**.

Note: The directory path following the *-c* option specifies the location of the appdb configuration files.

Result: The Load Database window appears.



13 Press **Enter**. The **Is the above information correct? (Y/N)** message appears.

Note: The tape drive is the default destination.

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

Note: The **Please mount tape #1 and press Return** message appears.

15 Press **Enter**.

Note: You already inserted the tape in an earlier step.

16 Wait for the **Process is complete** message to appear.

Note: This message signifies that the database is finished loading.

17 Eject the tape and store it in a safe place.

18 Follow the procedures in Appendix B, ***Restarting System Components*** (on page 207), to restart the DNCS, the Application Server, and Spectrum.

19 Type **/etc/rc2.d/S75cron start** and then press **Enter**. The system restarts cron jobs on the DNCS.

20 Follow these instructions to restart the Application Server cron jobs.

a Type **rsh appservatm** and then press **Enter**.

b Type **/etc/rc2.d/S75cron start** and then press **Enter**.

c Type **exit** and then press **Enter**.

21 Generate the Doctor Report and examine the output file for system conditions that may present a problem.

Note: Refer to Chapter 4, ***Analyze System Configuration with the Doctor Report*** (on page 31), for instructions on generating the Doctor Report and examining the output file.

22 Examine the cron files on both the DNCS and Application Server and determine whether any cron jobs should have executed during the period when the cron jobs were stopped.

Note: You may have to manually execute these cron jobs.

Loading the Database from the Hard Drive

Follow these instructions to load your DNCS or Application Server database from the hard drive of the DNCS.

1 Suspend any third-party applications.

2 If necessary, follow the procedures in Appendix A, ***Stopping System Components*** (on page 203), to shut down Spectrum, the Application Server, and the DNCS.

Important! All processes on the DNCS and the Application Server must be stopped when you unload or load the database.

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

Important! Skip steps 4, 5, and 6 if you have already logged in to the xterm window as root user and have executed the dncsSetup command.

4 Type **su -** and then press **Enter** to log in as root user. The password prompt appears.

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

6 Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. This command establishes the DNCS environment as a root user.

Important! Type the period followed by a space before typing /dvs.

Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.

7 Have you just unloaded your database?

- If **yes**, you have already stopped the cron jobs; go to step 9.
- If **no**, type **/etc/rc2.d/S75cron stop** and then press **Enter**. The system stops the DNCS cron jobs.

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

a Type **rsh appservatm** and then press **Enter**.

b Type **/etc/rc2.d/S75cron stop** and then press **Enter**.

c Type **exit** and then press **Enter**.

9 Type **cd [directory name]** and then press **Enter**.

Example: cd /dvs/backups/db_dir.12.15.00_08.45

Notes:

- Substitute the complete path and directory name of where you previously unloaded your database.
- You recorded the path and directory name in step 19 of ***Unloading the Database to the Hard Drive*** (on page 68).

10 Type **showActiveSessions** and then press **Enter**. A display showing any active DNCS sessions appears.

11 Are there any active DNCS sessions?

- If **yes**, type one of the following commands:
  - To kill all active sessions *at once*, type **killActiveSessions** and then press **Enter**; go to step 12.
  - To kill each process *individually*, type **kill [PID]** and then press **Enter**, where [PID] is the process ID associated with the active session; go to step 12.
- If **no**, the DNCS will display a message similar to **dncsDbServer is idle**; go to step 12.

12 Choose one of the following options:

- If you are loading the DNCS database from the hard drive of the DNCS, type **dncsDbData -l** and then press **Enter**.
- If you are loading the Application Server database from the hard drive of the DNCS, type **dncsDbData -l -d appdb -c /dvs/appFiles/dbConfig/appDbConfig** and then press **Enter**.

Note: The directory path following the -c option specifies the location of the appdb configuration files.

Result: The Load Database window appears.

13 Type **2** and then press **Enter**. The **Is the above information correct? (Y/N)** message appears.

14 Type **y** and then press **Enter**. The **Enter backup directory (Default: Current Directory)** message appears.

15 Press **Enter**. The **Is the above information correct? (Y/N)** message appears.

16 Type **y** and then press **Enter**. The database loads from the hard drive.

17 When the database has loaded, follow the procedures in Appendix B, ***Restarting System Components*** (on page 207), to restart the DNCS, the Application Server, and Spectrum.

18 Type **/etc/rc2.d/S75cron start** and then press **Enter**. The system restarts its cron jobs.

19 Follow these instructions to restart the Application Server cron jobs.

a Type **rsh appservatm** and then press **Enter**.

b Type **/etc/rc2.d/S75cron start** and then press **Enter**.

c Type **exit** and then press **Enter**.

20 Generate the Doctor Report and examine the output file for system conditions that may present a problem.

Note: Refer to Chapter 4, ***Analyze System Configuration with the Doctor Report*** (on page 31), for instructions on generating the Doctor Report and examining the output file.

21 Examine the cron files on both the DNCS and Application Server and determine whether any cron jobs should have executed during the period when the cron jobs were stopped.

Note: You may have to manually execute these cron jobs.

Database Fragmentation, Database Used Capacity, and the Doctor Report

Introduction

System operators who use the dncsDbData utility to defragment their database may notice that the Doctor Report shows that the percentage of the database in use is significantly higher *after* defragmenting the database than it was before defragmenting the database. The reason for the significant increase in the percentage of the database in use is that the dncsDbData utility associated with version 1.1 and later of DNCS Utilities preallocates a large amount of database space to the emm table when the table is reloaded during the defragmentation process. When the Doctor Report then analyzes the condition of the database, the Doctor Report considers the space allocated to the emm table to be in use, even though it may initially be empty.

The Doctor Report Output Before Defragmenting the Database

The ***Monitor and Eliminate Database Fragmentation*** (on page 59) section lists several tables in the DNCS and the Application Server databases that system operators should monitor for the presence of fragmentation. System operators use the Doctor Report to monitor these tables.

If any of these tables contains ten or more extents, system operators are advised to use the dncsDbData utility to unload and reload the database. Under the reload process, related data is loaded into contiguous locations in the database, and the fragmentation is eliminated.

Note: The *number of table extents* refers to the number of times a specific table is fragmented across the hard drive.

Refer to ***Example of a Fragmented Database*** (on page 80) for an example of the Doctor Report output showing a fragmented database.

Example of a Fragmented Database

The following example from the Doctor Report illustrates a fragmented database.

DNCS Database Check

==========

Total tempspace = 20520 pages (40.0 M)

Free tempspace = 20083 pages (39.2 M)

Database tempspace is at 2.2% used capacity.

Total dataspace = 2097150 pages (4095.9 M)

Free dataspace = 1919078 pages (3748.1 M)

OK: Database dataspace is at 8.5% used capacity.

Database Table Extents

==========

=Database Table=	=Extents=
atm_connection	7
displaychannels	2
elementary_stream	5
elementtable	5
elementtosource	3
emm	161
filemoduleinfo	6
hct_profile	65

==========

Explanation of the Doctor Report Output

The preceding example shows output from two headings of the Doctor Report: **DNCS Database Check** and **Database Table Extents**. Notice that two of the tables under the **Database Table Extents** heading consist of more than ten extents. The emm and hct_profile tables consist of 161 and 65 extents, respectively. The system operator of this database should take steps to defragment this database.

Note: Because system operators regularly load EMM CDs, the emm table is especially subject to fragmentation.

Notice also the last line of data under the **DNCS Database Check** heading. This line of data indicates that the database is at 8.5 percent used capacity. The Doctor Report displays an error condition once the database reaches 75 percent used capacity.

The next section, **The Doctor Report Output After Defragmenting the Database**, shows the Doctor Report output of the same database after using the dncsDbData utility to defragment the database.

The Doctor Report Output After Defragmenting the Database

The following example from the Doctor Report depicts the same database after you have used the dncsDbData utility to defragment the database.

Example of a Defragmented Database

The following example from the Doctor Report illustrates a defragmented database.

DNCS Database Check

==========

Total tempspace = 20520 pages (40.0 M)

Free tempspace = 20467 pages (39.9 M)

Database tempspace is at 0.3% used capacity.

Total dataspace = 2097150 pages (4095.9 M)

Free dataspace = 565463 pages (1104.4 M)

OK: Database dataspace is at 73.1% used capacity.

Database Table Extents

==========

=Database Table=	=Extents=
authorization	3
elementtable	2
pdsegment	2

==========

Explanation of the Doctor Report Output

In the preceding example, no table lists more than 10 extents. Therefore, the database has been successfully defragmented.

Notice, however, the last line of data under the **DNCS Database Check** heading. The Doctor Report now shows that the database is at 73.1 percent used capacity. This significant increase in database used capacity might be disconcerting to the system operator. Refer to ***An Explanation of Database Used Capacity*** (on page 82) for an explanation of how the database increased from 8.5 percent used capacity to 73.1 percent used capacity after defragmenting the database.

An Explanation of Database Used Capacity

Prior to version 1.1 of DNCS Utilities, when system operators used the dncsDbData utility to defragment the database, related data was reloaded contiguously into the database, but no additional space was allocated to the emm table. The database was then subject to fragmentation again as the emm table grew.

Beginning with version 1.1 of DNCS Utilities however, the reload function of the dncsDbData utility preallocates a significant amount of space to the emm table. By preallocating space to the emm table, the table can grow substantially without it becoming fragmented across the hard drive as it grows. The Doctor Report considers this preallocated space as used, even though it may consist largely of empty space. Therefore, Doctor Reports generated after defragmenting the database are likely to show a significant increase in the percentage of database used capacity.

Note: The amount of space preallocated to the emm table is based upon the following factors:

- The number of database spaces configured on the system
- The hardware platform of the DNCS
- The number of disks assigned to the database

Conclusion

System operators of sites that see the condition described in this section, after defragmenting the database, can safely ignore this condition.

Obtain System Platform Information

Obtaining System Platform Information

Through use of the *-s* option, system operators can use the dncsDbData utility to obtain information about the DNCS hardware platform. Follow these instructions to use the dncsDbData utility to obtain system platform information.

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

Note: Skip steps 2, 3, and 4 if you have already logged in to the xterm window as root user and have executed the dncsSetup command.

2 Type **su -** and then press **Enter** to log in as root user.

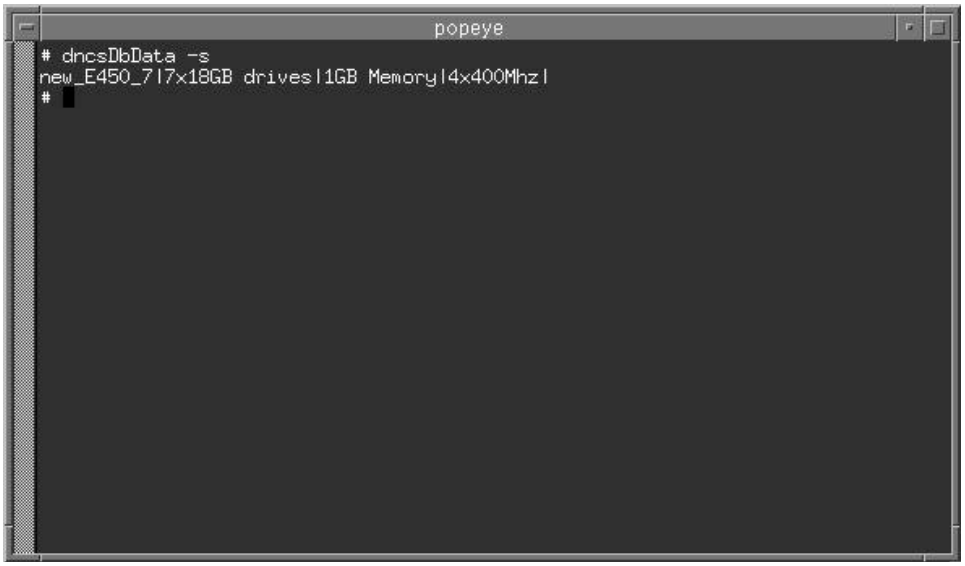
3 Type the root password and then press **Enter**.

4 Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. This command establishes the DNCS environment as a root user.

Important! Type the period followed by a space before typing /dvs.

Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.

5 Type **dncsDbData -s** and then press **Enter**. The system displays DNCS hardware platform information.



6 Type **exit** and then press **Enter** to log off as root user.

Obtain the Version Number of the dncsDbData Utility

Obtaining the Version Number of the dncsDbData Utility

Through use of the *-v* option, system operators can obtain the version number of the dncsDbData utility. Follow these instructions to obtain the version number of the dncsDbData utility.

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

Note: Skip steps 2, 3, and 4 if you have already logged in to the xterm window as root user and have executed the dncsSetup command.

2 Type **su -** and then press **Enter** to log in as root user.

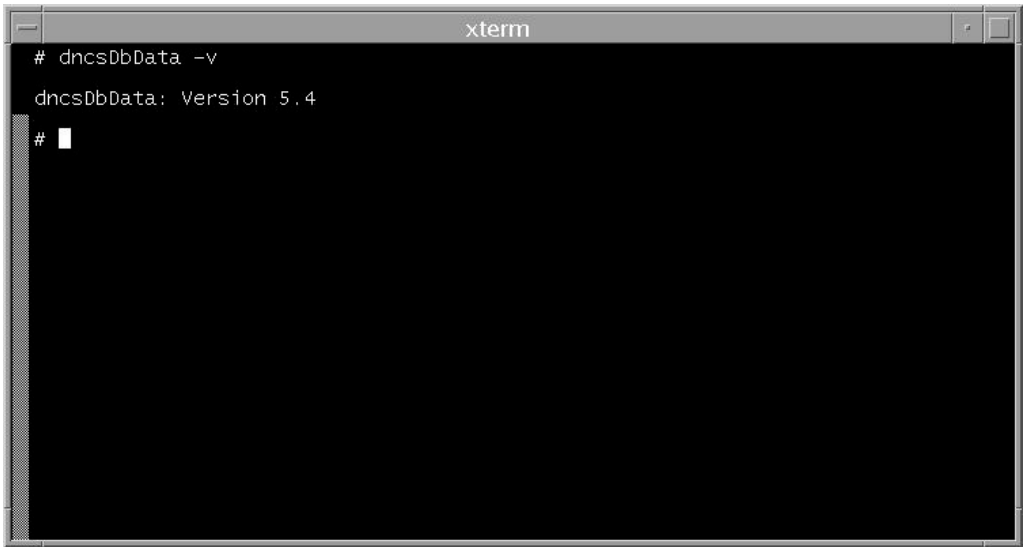
3 Type the root password and then press **Enter**.

4 Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. This command establishes the DNCS environment as a root user.

Important! Type the period followed by a space before typing /dvs.

Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.

5 Type **dncsDbData -v** and then press Enter. The system displays the version number of the dncsDbData utility.



6 Type **exit** and then press **Enter** to log off as root user.

6

Delete RMA DHCTs from the Database with the del-hct-cd Utility

Introduction

Cisco developed the del-hct-cd utility so that system operators can delete a DHCT or a list of DHCTs from the DNCS database. System operators typically delete DHCTs from the database when it is uneconomical to repair a DHCT or if a DHCT is moved from one system to another.

Sites supporting system software prior to SR 2.0 run the del-hct-cd utility through the UNIX command line. Sites supporting SR 2.0 and later system software run the del-hct-cd utility through a combination of the UNIX command line and the DNCS user interface. This chapter provides detailed instructions for using the del-hct-cd utility for all system releases.

In This Chapter

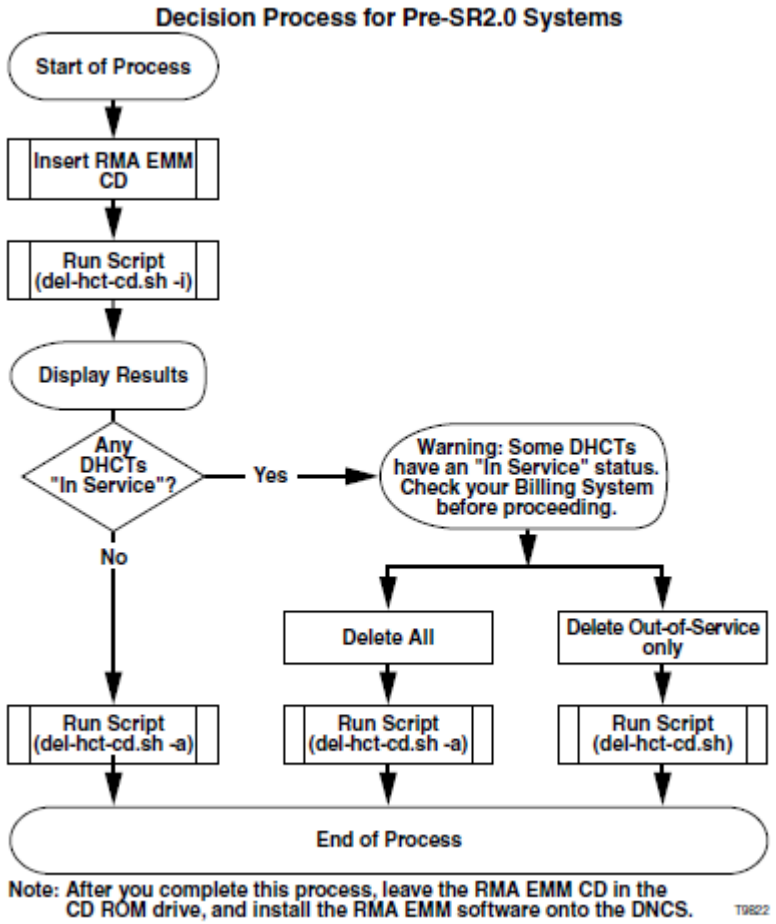
- Determine the Delete Command Option for Sites Prior to SR 2.0 86
- Determine the Delete Command Option for Sites with SR 2.0 or Later 87
- Run the del-hct-cd Utility 88
- Process RMA DHCTs From a File 94

Determine the Delete Command Option for Sites Prior to SR 2.0

The del-hct-cd Utility Decision Flowchart

The following flowchart shows the decision process for determining which delete command option to use for in-service or out-of-service RMA DHCTs at sites with system software releases prior to SR 2.0.

Note: Cisco and system operators sometimes use the terms "del-hct-cd utility" and "Repaired DHCT Staging Script" interchangeably.

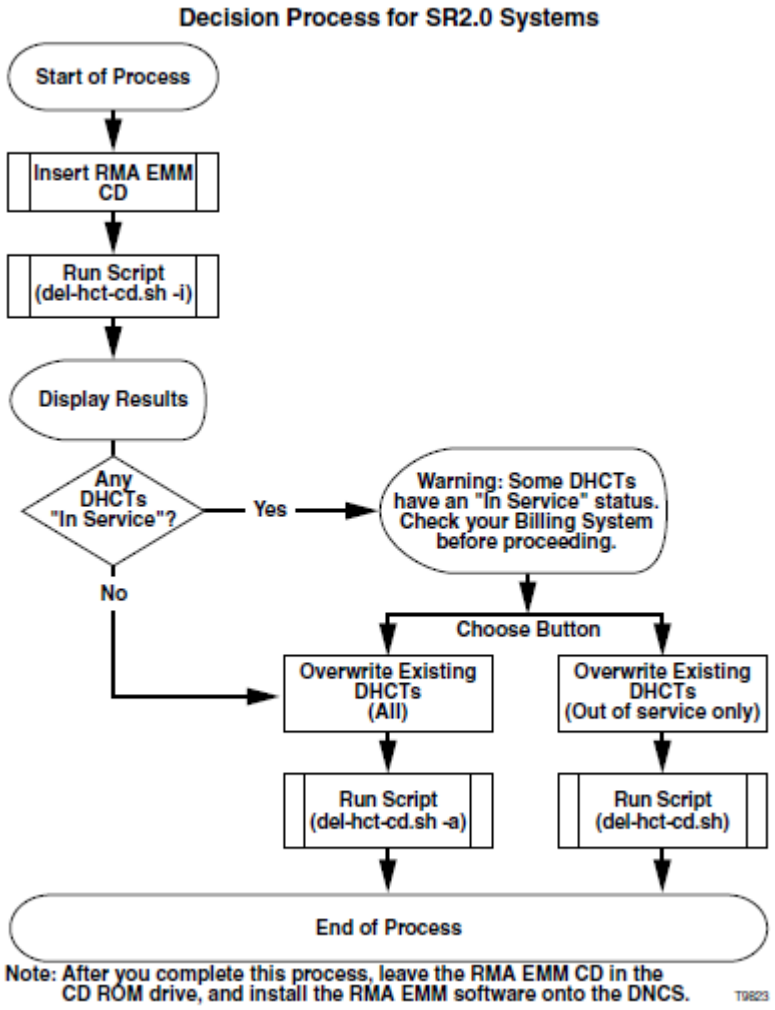


Determine the Delete Command Option for Sites with SR 2.0 or Later

The del-hct-cd Utility Decision Flowchart

The following flowchart shows the decision process for determining which delete command option to use for in-service or out-of-service RMA DHCTs in sites with SR 2.0 or later.

Note: Cisco and system operators sometimes use the terms "del-hct-cd utility" and "Repaired DHCT Staging Script" interchangeably.



Run the del-hct-cd Utility

Introduction

When you install the DNCS Utilities onto your system, you install a program that the system uses to purge your database of records pertaining to RMA DHCTs. You can run the del-hct-cd utility in any of the following modes:

- Information mode-implemented with the *-i* switch, counts and lists the DHCTs found on the RMA CD and reports on their database status.

  Note: No deletions from the database occur when the del-hct-cd utility is run in Information mode.

- Default mode-deletes from the Informix database those DHCTs contained on the RMA CD that have a status of out-of-service in the Informix database.

- Delete All mode-implemented with the *-a* switch, deletes all DHCTs, regardless of status, that are found on the RMA CD and contained in the Informix database.

All System Operators Run Script in Information Mode First

All system operators should run the del-hct-cd utility in Information mode first to learn how many DHCTs contained on the RMA CD are listed as in-service and out-of-service in the DNCS database. Then, based upon this information, system operators should decide whether to delete from the database all DHCTs listed on the RMA CD, or to delete from the database only out-of-service DHCTs.

System operators actually delete RMA DHCTs from the database in the following way:

- Operators of systems prior to SR 2.0 use the UNIX command line to execute the del-hct-cd utility to delete RMA DHCTs.

- Operators of systems at SR 2.0, or later, use the DNCS user interface to execute the built-in del-hct-cd.sh code to delete RMA DHCTs.

Refer to one of the following procedures to run the del-hct-cd utility in Information mode, and then to delete RMA DHCTs:

- ***Running the del-hct-cd Utility on Systems Prior to SR 2.0*** (on page 89)
- ***Running the del-hct-cd Utility on SR 2.0 and Later Systems*** (on page 92)

Running the del-hct-cd Utility on Systems Prior to SR 2.0

Follow these instructions to run the del-hct-cd utility on your DNCS if your system software is prior to SR 2.0.

Note: See ***Process RMA DHCTs From a File*** (on page 94) for instructions on how to run the del-hct-cd utility if an RMA CD is not available.

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

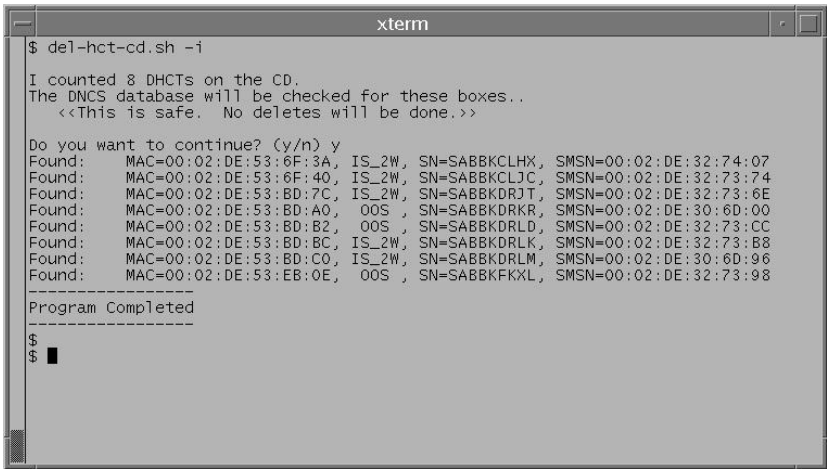
2 Insert the CD containing the RMA DHCT information into the CD drive of the DNCS.

Notes:

- Keep the CD in the CD drive of the DNCS throughout this procedure.
- The script detects when you do not have the RMA CD in the CD drive of the DNCS and displays an error message.

3 Type **del-hct-cd.sh -i** and then press **Enter**. The script counts the DHCTs found on the RMA CD and displays a message that inquires whether the database should be checked for the presence of these DHCTs.

4 Type **y** (for yes) and then press **Enter**. The script lists the DHCTs found on the CD and displays their database status.



Notes:

- An RMA EMM CD may contain several hundred DHCTs. To create a log file of the DHCTs on the RMA CD, type del-hct-cd.sh -i | tee hct.log and then press Enter.
- The script does not delete any DHCTs from the database when run in Information Mode.
- The following list expands the acronyms used in the accompanying illustration:
  - **IS_2W** represents "in service, two-way" DHCTs.
  - **OOS** represents DHCTs marked as out-of-service.

5 Choose one of the following options:

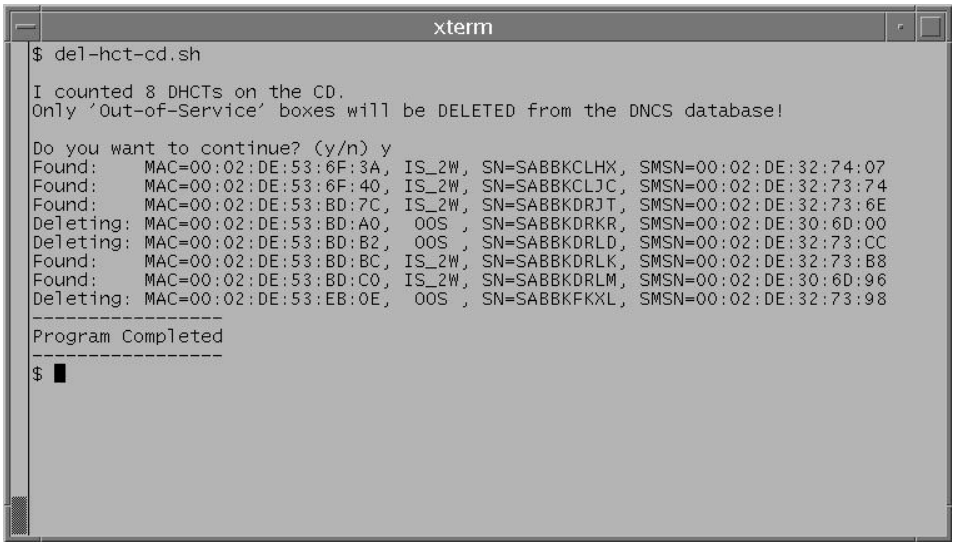
- To run the del-hct-cd utility in Default mode, go to ***Choosing Default Mode*** (on page 90).
- To run the del-hct-cd utility in Delete All mode, go to ***Choosing Delete All Mode*** (on page 91).

Choosing Default Mode

Running the del-hct-cd utility in Default mode deletes from the DNCS database those DHCTs included on the RMA CD and marked out-of-service in the database. Follow these instructions to run the del-hct-cd utility in Default mode.

1 Type **del-hct-cd.sh** and then press **Enter**. The script counts the DHCTs found on the RMA CD and displays a message that inquires whether out-of-service DHCTs should be deleted from the database.

2 Type **y** (for yes) and then press **Enter**. The script lists the DHCTs found on the CD and indicates which DHCTs it is deleting.



Notes:

- As indicated in the accompanying illustration, the script is deleting the three DHCTs marked **Deleting**.
- The five DHCTs marked **Found** are likely to be found in a subscriber's home and will not be deleted.

3 Type **eject** and then press **Enter** to eject the RMA CD.

Choosing Delete All Mode

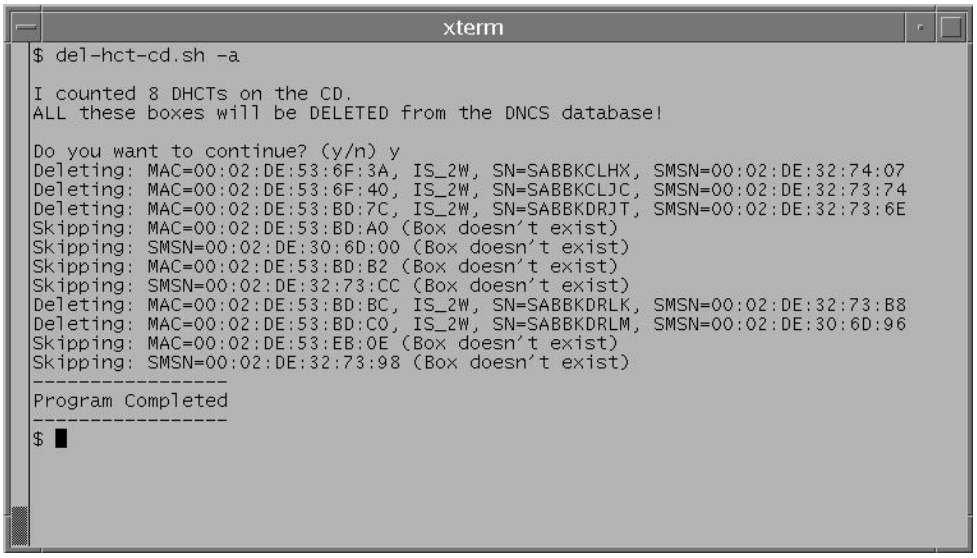
Follow these instructions to run the del-hct-cd utility in Delete All mode.

CAUTION:

Cisco recommends that you exercise extreme caution before running the del-hct-cd utility in Delete All mode. Running the script in Delete All mode deletes from the database those DHCTs that may already be in subscriber's homes. These DHCTs will be inoperable after deletion from the database.

1 Type **del-hct-cd.sh -a** and then press **Enter**. The script counts the DHCTs found on the RMA CD and displays a message that inquires whether all DHCTs found on the RMA CD should be deleted from the database.

2 Type **y** (for yes) and then press **Enter**. The script lists the DHCTs found on the CD and indicates which DHCTs it is deleting.



Notes:

- As indicated in the accompanying illustration, the script is deleting the five DHCTs marked **Deleting**.
- The script lists three DHCTs that it is **Skipping**. These three DHCTs are skipped in this example because they were deleted from the database when the del-hct-cd utility was run in the previous procedure, **Default Mode**.

3 Type **eject** and then press **Enter** to eject the RMA CD

Running the del-hct-cd Utility on SR 2.0 and Later Systems

Follow these instructions to run the del-hct-cd utility on your DNCS if your system software is at SR 2.0 or later.

Note: See ***Process RMA DHCTs From a File*** (on page 94) for instructions on how to run the del-hct-cd utility if an RMA CD is not available.

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

2 Insert the CD containing the RMA DHCT information into the CD drive of the DNCS.

Notes:

- Keep the CD in the CD drive of the DNCS throughout this procedure.
- The script detects when you do not have the RMA CD in the CD drive of the DNCS and displays an error message.
- On some SR 2.x systems, a File Manager window may open. You can close it.

3 In the open xterm window, type **del-hct-cd.sh -i** and then press **Enter**. The script counts the DHCTs found on the RMA CD and displays a message that inquires whether the database should be checked for the presence of these DHCTs.

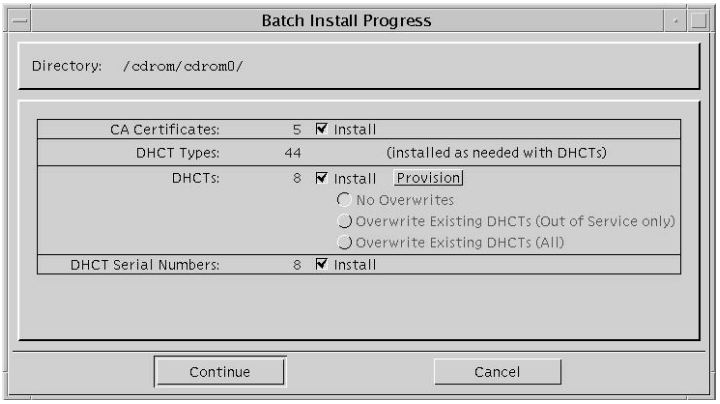
4 Type **y** (for yes) and then press **Enter**. The script lists the DHCTs found on the CD and displays their database status.

Notes:

- An RMA EMM CD may contain several hundred DHCTs. To create a log file of the DHCTs on the RMA CD, type **del-hct-cd.sh -i | tee hct.log** and then press **Enter**.
- The script does not delete any DHCTs from the database when run in Information Mode.
- The following list expands the acronyms used in the accompanying illustration:
  - **IS_2W** represents "in service, two-way" DHCTs.
  - **OOS** represents DHCTs marked as out-of-service.

5 Continue with your normal batch install procedure. The Batch Install Progress window appears.

Note: On SR 2.0 and later systems, the Batch Install Progress window looks similar to the following example.



6 Use the output displayed in step 4 to determine whether you want to delete and install all DHCTs listed on the RMA CD, or only those marked out-of-service.

7 Choose one of the following options on the Batch Install Progress window:

- To delete and re-install out-of-service RMA DHCTs from the database, select **Overwrite Existing DHCTs (Out of Service only)**.
- To delete and re-install all RMA DHCTs, select **Overwrite Existing DHCTs (All)**.

CAUTION:

Cisco recommends that you exercise extreme caution before selecting Overwrite Existing DHCTs (All). Deleting all RMA DHCTs removes from the database those DHCTs that may already have been repaired and placed in subscriber's homes. These DHCTs will be inoperable after deletion from the database.

Note: If you select **No overwrites**, the system loads the EMMs without deleting or overwriting existing information in the database.

8 Click **Continue**. The system deletes from the database those RMA DHCTs you selected in step 7.

9 Type **exit** and then press **Enter** to close the xterm window.

Process RMA DHCTs From a File

Overview

Operators of sites where the staging area is remotely located from the DNCS may find it difficult to supply the DNCS operator with the RMA CD so that the DNCS operator can execute the del-hct-cd utility in conjunction with RMA DHCTs. To support these sites, Cisco has included an option in the del-hct-cd.sh script, implemented by the *-p* switch, that enables the script to read from a file rather than from the RMA CD.

Important! System operators and network administrators who currently use the *-p* switch when processing RMA DHCTs already have a thorough understanding of the directory structure of the RMA CD because they must model the directory structure of their DNCS to reflect that of the CD. Other than a brief mention, this section provides no instructions on analyzing the directory structure of the RMA CD, nor on modeling the directory structure of the DNCS to reflect that of the CD. Any site that is interested in using the *-p* switch to process RMA DHCTs from a file rather than from the CD should contact Cisco Services for guidance.

Guidelines for Processing RMA DHCTs From a File

On the RMA CD, the individual DHCT definition files that are used when processing RMA DHCTs are stored in the …/dncs/dhcts directory. To use the *-p* switch, system operators must have a similar directory structure in place on their DNCS.

Examples:

- /export/home/ftp/**dncs/dhcts**
- /tmp/ftp/**dncs/dhcts**

In the examples provided above, system operators duplicate the entire CD directory structure and contents at /export/home/ftp or /tmp/ftp on the DNCS.

Note: Even though the entire directory structure is copied to the DNCS, the del-hct-cd.sh script, when used with the *-p* switch, only accesses the dncs/dhcts subdirectory.

To run the del-hct-cd utility using the *-p* and *-a* switches, system operators execute the **del-hct-cd.sh -a -p/[directory path name]** command, and then press **Enter**.

Example: del-hct-cd.sh -a -p/export/home/ftp/dncs/dhcts

To run the del-hct-cd utility using the *-p* switch to delete only out-of-service DHCTs, system operators execute the **del-hct-cd.sh -p/[directory path name]** command and then press **Enter**.

Example: del-hct-cd.sh -p/export/home/ftp/dncs/dhcts

Note: If you want to use the -p switch in conjunction with the del-hct-cd.sh script, call Cisco Services for assistance.

7

Change the DNCS and Application Server Hostname with the hostnmchg Script

Introduction

When Cisco ships a new DNCS and Application Server, the DNCS ships preconfigured with a hostname of dncseth associated with an IP address of 192.168.2.1. The Application Server ships preconfigured with a hostname of app associated with an IP address of 192.168.2.10.

System operators can change these hostnames and the IP addresses if they want to connect their DNCS and Application Server to a different network. The hostnmchg script changes the hostname, the IP address, and all associated files required to connect the DNCS and Application Server to the local network.

Important! The /etc/hosts file in the DNCS must always have the following entry: **192.168.1.1 dncs**. This interface is used for communication between the DNCS and the TED. Do not change this entry in the /etc/hosts file.

In This Chapter

- Run the hostnmchg Script 98
- Restart the Applications..... 101

Run the hostnmchg Script

Running the hostnmchg Script on the DNCS

Follow these instructions to run the hostnmchg script on the DNCS.

1. Follow the instructions in Appendix A, ***Stopping System Components*** (on page 203), to shut down the DNCS, the Application Server, and Spectrum.
2. Click **EXIT** on the bottom of the DNCS terminal, and then click **OK**. The user logs out of the DNCS and the CDE Login window appears.
3. Log in to the DNCS as root user.
4. From an xterm window on the DNCS, type **su - informix** and then press **Enter**. You become informix user in the xterm window.
5. Type **onmode -ky** and then press **Enter**. The Informix database shuts down.
6. Type **exit** and then press **Enter**. You log out as informix user in the xterm window.
7. Type the following command:

   /dvs/dncs/bin/hostnmchg.sh [new_hostname] [new_ip_address] and then press **Enter**.

   Notes:

   - Substitute your new hostname for [new_hostname].
   - Substitute your new IP address for [new_ip_address].

   Result: The following message appears:

   This script will modify the system as follows:
   Old hostname = <old_hostname>
   Old IP address = <old_IP_address>
   New hostname = <new_hostname>
   New IP address = <new_ip_address>
   Primary network interface file = /etc/hostname.hme1
   Continue [y,n,?,q]
8. Type **y** to continue (or press n to exit) and then press **Enter**.

   Results:

   - The script displays a list of affected files as it changes the hostname variable and IP address.

     Note: If the script detects that the hostname variable has been changed before, the script requires confirmation from the operator before changing some hostname variables.
   - If your system supports Spectrum, a **Do you want to change the Spectrum files** message appears.

9 Did the **Do you want to change the Spectrum files** message appear?

- If **yes**, type **y** and then press **Enter**.

  Results:

  – The system lists the Spectrum files that will be changed.

  – The system displays a **You MUST reboot your system NOW** message.

  Important! Ignore this message now; you will reboot the DNCS later.

- If **no**, go to step 10.

10 Does your Application Server run the Cisco Resident Application?

- If **yes**, go to ***Running the hostnmchg Script on the Application Server*** (on page 99).
- If **no** (your system runs another resident application), go to ***Restart the Applications*** (on page 101).

Running the hostnmchg Script on the Application Server

Follow these instructions to run the hostnmchg.sh script on the Application Server.

1 At the DNCS, type **cd /dvs/dncs/bin** and then press **Enter**. The /dvs/dncs/bin directory becomes the working directory.

2 At the DNCS, type **rcp -p hostnmchg.sh appservatm:/dvs/appserv/bin** and then press **Enter**. The DNCS copies the hostnmchg.sh script to the Application Server.

3 Are you already logged in to the Application Server?

- If **yes**, go to step 4.
- If **no**, log in to the Application Server CDE Login window as **root** user.

4 In an xterm window on the Application Server, type **id** and then press **Enter**. The system displays the user id in the xterm window.

5 Choose one of the following options:

- If you are **root** user in the xterm window, go to step 7.
- If you are **dncs** user in the xterm window, go to step 6.

6 Follow these instructions to log on to the xterm window on the Application Server as **root** user.

a Type **su -** and then press **Enter**.

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

7 Type the following command:

chmod +x /dvs/appserv/bin/hostnmchg.sh and then press **Enter**. Executable permissions are applied to the hostnmchg.sh file.

8 Type the following command:

/dvs/appserv/bin/hostnmchg.sh [new_hostname] [new_ip_address] and then press **Enter**.

Notes:

- Substitute your new hostname for [new_hostname].
- Substitute your new IP address for [new_ip_address].

Result: The following message appears:

This script will modify the system as follows:

Old hostname = <old_hostname>
Old IP address = <old_ip_address>
New hostname = <new_hostname>
New IP address = <new_ip_address>
Primary network interface file = /etc/hostname.hme0

Continue [y,n,?,q]

9 Type **y** to continue (or press n to exit) and then press **Enter**.

Results:

- The script changes the hostname of the Application Server.
- A message instructing you to reboot the Application Server appears.

10 Type **/usr/sbin/shutdown -y -g0 -i0** and then press **Enter**. The Application Server shuts down.

11 Go to ***Restart the Applications*** (on page 101).

Restart the Applications

Restarting the Applications

After running the hostnmchg script on the DNCS and the Application Server, follow these instructions to restart the system applications.

1. In the xterm window on the DNCS, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The DNCS reboots.
2. After the DNCS reboots, log in to the CDE of the DNCS as **dncs** user.
3. Does your Application Server run the Cisco resident application?
   - If **yes**, go to step 4.
   - If **no** (your system runs another resident application), go to step 6.
4. At the **ok** prompt on the Application Server, type **boot** and then press **Enter**. The Application Server boots.
5. Log in to the Application Server as **dncs** user.
6. If necessary, follow the instructions in Appendix B, ***Restarting System Components*** (on page 207), to restart Spectrum, the DNCS, and the Application Server.

   Note: The system applications may have restarted after you rebooted the DNCS and the Application Server.

8

Identify and Correct Database Problems with the checkDB Script

Introduction

Cisco engineers developed the checkDB script to identify and correct various potential problems in the DNCS database. This chapter describes some of the potential database problems identified by the checkDB script, and provides instructions for running the script.

In This Chapter

- Overview of the checkDB Script 104
- Run the checkDB Script 106

Overview of the checkDB Script

Types of Database Problems

The following list identifies some of the potential problems that the checkDB script identifies:

- DHCT records in the DNCS database that do not have serial numbers

  Notes:

  - Prior to DNCS version 1.2.5, the DNCS did not require DHCTs to have serial numbers. DHCT serial numbers are now used mainly with third-party applications such as the video-on-demand application.
  - If the output of the checkDB script shows that you have DHCTs in your database without serial numbers, you can contact Cisco Services to assign serial numbers to those DHCTs.

- Records in various tables in the DNCS database that do not have required corresponding records in other tables

  Notes:

  - Records that do not have required corresponding records in other tables are known as orphaned records.
  - You can configure the checkDB script to automatically remove orphaned records from the DNCS database.

- DHCTs with a status of in-service that have EMMs ready to expire

  Note: The checkDB.sh script will prompt you to either restage or delete DHCTs with EMMs ready to expire.

- Sites that are likely to experience a problem due to the DNCS generating duplicate subscription EMMs. (This is a very rare condition and is included in the checkDB utility as a precaution.)

  - The checkDB script identifies this condition through the Highest eu_eid used for subscription pkgs field.
  - Sites where this value exceeds 220 should report this condition to Cisco Services.

Prerequisites

Consider the following important prerequisites before you run the checkDB script:

- Be sure that you have a current backup of your DNCS database before running the checkDB script with the *-f* or *-F* options. Refer to the appropriate copy of the backup and restore procedures for detailed instructions on how to back up the DNCS database.

  Note: The checkDB script makes no database changes when run with no options or with the *-v* option. The script may change the database when run with the *-f* or *-F* options. Refer to ***Run the checkDB Script*** **(on page 106)** for additional information concerning the options associated with the checkDB script.

- If you configure the checkDB script to automatically remove orphaned records from the DNCS database, you need two other utilities installed on your DNCS to complete the task: delete-sm and deleteDhct. Both utilities are included on the DBDS Utilities CD.

  Note: Refer to Chapter 3, ***Reset DHCT Configuration With the delete-sm Utility*** (on page 21), of this *DBDS Utilities Version 5.1 Installation Instructions and DNCS Utilities User's Guide* for information about the delete-sm utility. Refer to ***The deleteDhct Utility*** (on page 105) for information about the deleteDhct utility.

The deleteDhct Utility

When used with the *-f* or *-F* options, the checkDB script calls the deleteDhct utility in order to delete DHCT records from the database. The logic of the checkDB script is such that all references to the deleteDhct utility occur automatically; no user intervention is required. The deleteDhct utility is included on the DBDS Utility CD.

The deleteDhct utility was designed by Cisco to completely delete DHCT records from the DNCS database. It deletes a single DHCT or can delete all DHCTs in a list containing DHCT MAC addresses that are presented in a text file.

The logic in the deleteDhct utility is very good at finding all database rows in all the different DHCT tables that contain or used to contain records for the specified DHCT(s). The deleteDhct utility deletes orphaned DHCT records. While orphaned DHCT records are less common now than they have been in the past, at one time duplicate database rows were generated for RMA DHCTs when they were returned from repair with a changed secure_micro address.

Run the checkDB Script

Introduction

The checkDB script examines the following tables in your DNCS database for possible error conditions:

- emm
- hct_profile
- pdkeycertificate
- pdsernummap
- secure_micro
- sm_auth_profile
- sm_pkg_auth

You can run the checkDB script in three possible modes:

- Run the checkDB script in default mode (with no options) to generate a detailed report listing possible error conditions in the database. When the checkDB script is run in default mode, the script does not correct any error conditions it finds. The script merely generates a report listing potential error conditions.
- Run the checkDB script in "fix" mode to automatically delete certain orphaned records from the database. When run in "fix" mode, with the *-f* or *-F*' option, the script generates a report listing potential error conditions and lists any changes it made to the database as a result of running the script in "fix" mode.

  Important! Cisco recommends that you run the script with no options before running the script with one of the "fix" mode options.
- Run the checkDB script with the *-v* option to display only the version number of the checkDB script.

Running the checkDB Script with No Options

Running the checkDB script with no options generates a detailed report that lists possible error conditions in the database. Follow these instructions to run the checkDB script with no options, and then to examine the logfile.

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

2 Type **checkDB.sh > /dvs/dncs/tmp/checkDB.[today's date]** and then press **Enter**.

Notes:

- Substitute today's date for [today's date].

  Example: checkDB.sh > /dvs/dncs/tmp/checkDB.081601

- This command directs the output from the checkDB script to a file in the /dvs/dncs/tmp directory on the DNCS. Cisco recommends that you direct the output to a file for you to examine later because the output would otherwise scroll too quickly off the screen for you to examine.

3 After the script has finished running, type **cd /dvs/dncs/tmp** and then press **Enter**. The /dvs/dncs/tmp directory becomes your working directory.

4 Type more [name of logfile] and then press Enter. The logfile opens using the UNIX more utility.

Note: Substitute the name of the logfile you created in step 2 for [name of logfile].

Example: more checkDB.081601

5 Refer to ***Sample Logfile and Analysis*** (on page 107) as you examine the logfile created by the checkDB script.

Notes:

- Press the **Spacebar** to page through the output file.
- Press the **Ctrl** and **C** keys simultaneously to close the output file when you are finished.

Sample Logfile and Analysis

Use the following example when you examine the logfile you opened in step 4.

Note: The following example of the logfile contains line numbers. Line numbers do not actually appear in the logfile, but are included here to facilitate an explanation of some of the items contained in the logfile.

Sample Logfile

==========

1 # Tue Dec 2 15:25:43 EST 2003

2 # The total number of rows in hct_profile = 156278.

3 # The total number of rows in secure_micro = 40378.

```
4  # Highest eu_eid used for subscription pkgs = 111.
5  # DHCT Registration is set to 'Administrative Gateway'.
6  # There are 65407 MAC addresses with No DHCT Serial Number
7  # Rows defining SN/MAC should be added for these boxes in 'pdsernummap'
8  00:02:DE:11:72:EE
9  00:02:DE:14:C3:72
10 (65405 other addresses listed here)
11 # There are 233 SN/MAC matches that should be DELETED from
   'pdsernummap'
12 SABBGZJWC|00:02:DE:49:F7:6C|
13 SABBHCQTS|00:02:DE:4A:73:20|
14 SABBHBQRF|00:02:DE:4A:34:3A|
15 (230 other addresses listed here)
16 # There are 0 secure_micro rows with mac_addr not in 'hct_profile'
17 # There are 5 secure_micro MACs with sm_serial_num not in 'hct_profile'
18 # These sm_host_mac_addr rows MUST be deleted from 'secure_micro'!
19 # (They cause 'mismatch' problems with EMM regeneration in camAuditor)
20 # (Use the 'deleteDhct' utility to delete these.)
21 00:01:A6:05:33:70|00:02:DE:FC:50:14|
22 00:01:A6:20:66:1A|00:02:DE:F0:A0:5B|
23 00:01:A6:41:B2:80|00:02:DE:F0:93:8E|
24 00:01:A6:30:A3:A4|00:01:A6:7C:53:F6|
25 00:01:A6:41:35:64|00:01:A6:80:EE:8E|
26 # There are 0 sm_auth_profile rows with no secure_micro parent
27 # There are 0 sm_pkg_auth SMSNs with no secure_micro parent
28 # There are 502 boxes having EMMs with sm_serial_num not in 'hct_profile'
29 # All rows having these sm_serial_num should be deleted from 'emm'
30 00:01:A6:5D:10:92
31 00:01:A6:67:54:24
32 (500 other addresses listed here)
33 # There are 0 pdkeycertificates having no parent 'hct_profile'
34 # There are 0 boxes with no 'pdkeycertificates'
35 # There are 14 boxes with no 'secure_micro', but with very-old EMMs.
36 # These boxes are in the database, but were incompletely staged
37 # over 90 days ago.  They should be re-staged or deleted.
38 00:02:DE:1D:4C:5A
39 00:02:DE:1B:6E:6A
```

00:02:DE:53:E4:6A
00:02:DE:58:6A:64
00:02:DE:1C:13:D6
00:02:DE:B2:9F:E6
00:02:DE:14:E1:18
00:02:DE:14:67:EA
00:02:DE:49:BF:3A
00:02:DE:14:16:B8
00:02:DE:13:21:52
00:02:DE:16:5A:36
00:02:DE:A1:04:D0
00:02:DE:10:D9:9C
There are 0 'In-Service' boxes with 'almost-expired' EMMs.
No orphaned authorizations exist...
3600 boxes have NULL in the hctt_oui, hctt_id, or hctt_revision parameters!
2 percent is MORE than should be tolerated!!
==========

Analysis of Logfile

Refer to the preceding logfile as you read through this analysis. Your logfiles are likely to contain similar points of interest.

Analysis of checkDB Logfile	
Line Numbers	**Explanation**
Lines 2 and 3	Lines 2 and 3 indicate how many records exist in the hct_profile and secure_micro tables in the database.
Line 4	Line 4 indicates the maximum value for subscription packages in the eu_eid column in the package table. **Important!** Sites where this value exceeds 220 should report this condition to Cisco Services.
Line 5	Line 5 reports registration configuration. Options are Open Registration and Administrative Gateway. Cisco recommends Administrative Gateway to prevent DHCTs from being added to your system without your knowledge.
Lines 6 through 10	These lines identify DHCTs that are in the database without serial numbers. Line 6 indicates that there are 65,407 DHCTs in the database without a serial number. Line 8 begins to list them, but the list has been truncated in this example to conserve space. Contact Cisco Services if your logfile indicates that you have DHCTs in the database without serial numbers. Cisco will retrieve the list from your DNCS and will insert the correct serial numbers into your database.
Lines 11 through 15	These lines identify 233 DHCTs with serial number and MAC address entries in the pdsernummap table, but without a required corresponding entry in the hct_profile table. The checkDB script therefore concludes that these are orphaned records and recommends that they be deleted.
Line 16	This line reports that there are no entries in the secure_micro table of DHCTs that have a MAC address but have no corresponding entry in the hct_profile table.

Analysis of checkDB Logfile	
Line Numbers	**Explanation**
Lines 17 through 25	These lines identify 5 DHCTs with MAC address entries in the secure_micro table, but without a required corresponding entry in the hct_profile table. The checkDB script therefore concludes that these are orphaned records and recommends that they be deleted.
Lines 26 and 27	These lines indicate that there are no orphaned records in the sm_auth_profile and the sm_pkg_auth tables with respect to the secure_micro table.
Lines 28 through 32	These lines identify 502 DHCTs with serial number entries in the emm table, but without a required corresponding entry in the hct_profile table. The checkDB script therefore recommends that they be deleted.
Lines 33 and 34	These lines indicate that there are no potential error conditions with the pdkeycertificates table.
Lines 35 through 51	These lines identify 14 DHCTs with very old EMMs. The checkDB script prompts you to either restage or delete them.
Line 52	Line 52 indicates that there are no DHCTs in the database with EMMs that are in danger of expiring
Line 53	Line 53 indicates that there are no orphaned authorization records in the database.
Lines 54 and 55	These lines indicate that there are 3600 DHCT entries in the hct_profile table with NULL values in the hctt_oui, hctt_id, or hctt_revision fields. These NULL values result from running a script for handling mismatched hardware type errors. **Note:** When the quantity of DHCTs with NULL values in the previously mentioned fields exceeds 1 percent of the DHCTs in the hct_profile table, the checkDB script notifies you.

Running the checkDB Script in "Fix" Mode

Use options *-f* or *-F* to run the checkDB script in "fix" mode. When run in "fix" mode, the script removes certain orphaned records from the database and generates a report that lists potential error conditions.

Follow these instructions to run the checkDB script in "fix" mode.

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

2 Choose one of the following options:

- To run the checkDB script with the *-f* option, type **checkDB.sh -f > /dvs/dncs/tmp/checkDB.[today's date]** and then press **Enter**.

  Example: checkDB.sh -f > /dvs/dncs/tmp/checkDB.081601

- To run the checkDB script with the *-F* option, type **checkDB.sh -F > /dvs/dncs/tmp/checkDB.[today's date]** and then press **Enter**.

  Example: checkDB.sh -F > /dvs/dncs/tmp/checkDB.081601

Notes:

- Substitute today's date for [today's date].
- These commands directs the output from the checkDB script to a file in the /dvs/dncs/tmp directory on the DNCS. Cisco recommends that you direct the output to a file for you to examine later because the output would otherwise scroll too quickly off the screen for you to examine.

Chart Summarizing Conditions Addressed by "Fix" Mode

The following chart summarizes the conditions addressed by running the checkDB script in "fix" mode:

Note: As the chart shows, the *-f* and *-F* options accomplish identical tasks, except that the *-F* option is also used to remove records in the sm_auth_profile table when there is no corresponding record in secure_micro table.

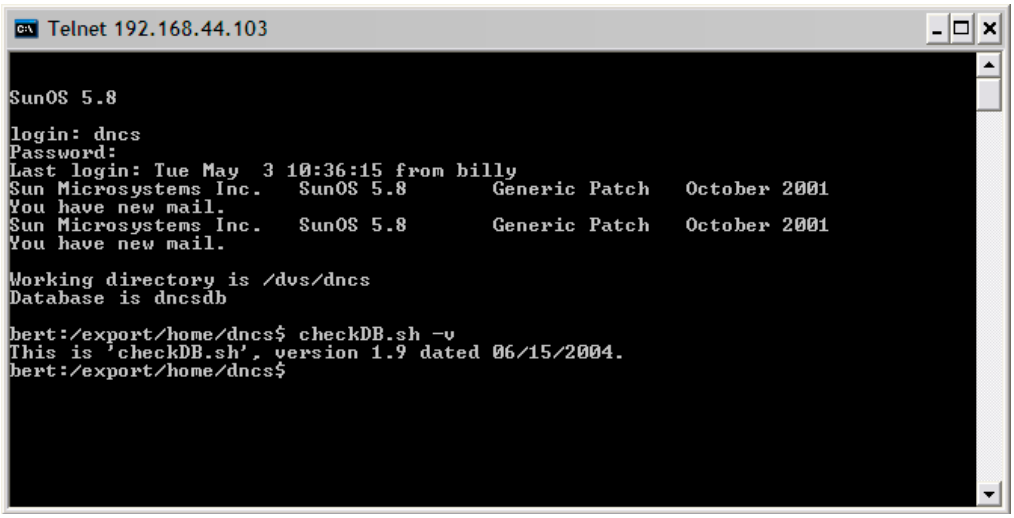
Condition	**checkDB Option**	
	-f	**-F**
DHCT serial numbers with missing parent (extra rows in pdsernummap table)	x	x
Records in hct_profile table with no corresponding record in the pdkeycertificate table	x	x
Records in secure-micro table (with MAC address or serial number) with no corresponding record in the hct_profile table	x	x
Records in sm_auth_profile table with no corresponding record in secure_micro table		x
Records in sm_pkg_auth table with no corresponding record in sm_auth_profile table	x	x
Records in emm table with no corresponding record in hct_profile table	x	x
Orphaned authorization packages	x	x

Running the checkDB Script to Display the Version

Follow these instructions to display the version number of the checkDB script that is installed on your system.

1. If necessary, open an xterm window on the DNCS.
2. Type **checkDB.sh -v** and then press **Enter** to display the version number of the checkDB script installed on your system. The system displays the version number of the checkDB script installed on your system.

   Example: The version number of the checkDB script displayed in this example is version 1.9.



9

Chart EMM Expiration Times with the smMix Utility

Introduction

System operators should run the smMix utility at least once every two weeks to generate a chart and a histogram of the registered expiration times of DHCT EMMs. Ideally, approximately 10 percent of DHCT EMMs should be scheduled to expire daily from 21 days to 30 days in the future. The camAuditor process on the DNCS may not be working properly if the system has DHCTs with EMMs that expire sooner than 20 days.

Exception: At a few sites, the DNCS is configured to have EMMs expire later than 30 days in the future. The smMix utility automatically detects when EMMs are configured to expire and properly reports the data for these non-standard configurations.

In This Chapter

- Overview of the smMix Modes 116
- DHCT Administrative Statuses 117
- How the smMix Utility Works 119
- Run the smMix Utility 128

Overview of the smMix Modes

The smMix Modes

System operators can run smMix in the three following modes:

- smMix-default mode (with no options) to summarize the age mix in the secure_micro table in the DNCS database.
- smMix -v-to display the version number of the smMix utility.
- smMix -?-to display information that explains how the smMix utility works.

Notes:

- System operators who run smMix and discover that their systems have DHCTs with EMMs set to expire in fewer than 20 days should call Cisco Services.
- System operators who run smMix and discover that their systems have an unusually high number of EMMs set to expire on the same day should call Cisco Services.

  Important! Approximately 10 percent of EMMs should expire daily from 21 days to 30 days in the future. An unusual condition exists when significantly more than 10 percent of EMMs are scheduled to expire on any one day within the 21 to 30 day timeframe. See ***DHCT Distribution in a System With an Uneven EMM Expiration Schedule*** **(on page 124)** for an example.

DHCT Administrative Statuses

Introduction

This section describes the various statuses that the DNCS database maintains for DHCTs. In addition, this section explains how the DNCS refreshes EMMs based upon the status of the DHCT.

Understanding the Status of DHCTs

The DNCS database maintains four administrative statuses for DHCTs. These statuses are described in the following list:

- In service, two-way-DHCTs with a status of *in service two-way* support communication between the headend and the DHCT, as well as return communication. DHCTs need two-way communication capability to take full advantage of Cisco's interactive services.

  Example: Examples of Cisco's interactive services include impulse pay-per-view (IPPV), video-on-demand (VOD), and anything on-demand (xOD).

- In service, one-way-DHCTs with a status of *in service one-way* support communication from the headend to the DHCT, only. These DHCTs are considered to be in broadcast-only mode and have no two-way services assigned to them.

- Out of service-DHCTs that are new and have not yet been staged or installed in subscribers' homes have a status in the database of *out-of-service*. DHCTs with a status of out-of-service cannot sign on to the network.

- Deployed-DHCTs with a status of *deployed* are usually in transit. The DHCTs are not technically out-of-service, but not quite in-service, either. These DHCTs have been staged and will shortly be installed in the homes of subscribers. DHCTs with a status of deployed can sign on to the network.

  Note: Not all billing vendors support the deployed state.

DHCT Status and EMMs

The following list describes how the DNCS maintains EMMs based upon DHCT status:

- The DNCS maintains and refreshes EMMs on all DHCTs with a status of in service, two-way and in service, one-way.
- The DNCS does not maintain or refresh EMMs on DHCTs with a status of out-of-service.
- The DNCS may or may not maintain EMMs on DHCTs with a status of deployed, based upon the value of the HCTM_PROVISIONING_APP variable.

  Note: Refer to *Instastaging Guide*, part number 4010008, for additional information on the HCTM_PROVISIONING_APP variable.

How the smMix Utility Works

Introduction

DHCTs need active EMMs to receive secured services. DHCTs that have EMMs will time-out if the EMMs have expired. The camAuditor process of the DNCS examines the expiration times of EMMs and regenerates those EMMs that are set to expire in fewer than 20 days. The newly regenerated EMMs are configured so that they expire in 30 days. Healthy systems therefore have EMMs that are scheduled to expire from 20 days to 30 days in the future.

DHCT Distribution in a Healthy System

Examine the following smMix output from a healthy system. The output depicts both the chart and the histogram representing EMM distribution times. Notice how all DHCTs have EMM expiration times from 20 days to 29 days in the future.

Notes:

- You will notice that a few DHCTs have EMMs with expiration times greater than 29 days. An examination of these records would show that these EMMs actually expire a few hours into the 30th day.
- The data in the following example comes from running the smMix utility in default mode, with no options.

Based on the distribution of DHCTs in the following example, the system operator can conclude that the camAuditor process is operating normally and regenerating EMMs as they age.

Chart Representing EMM Distribution

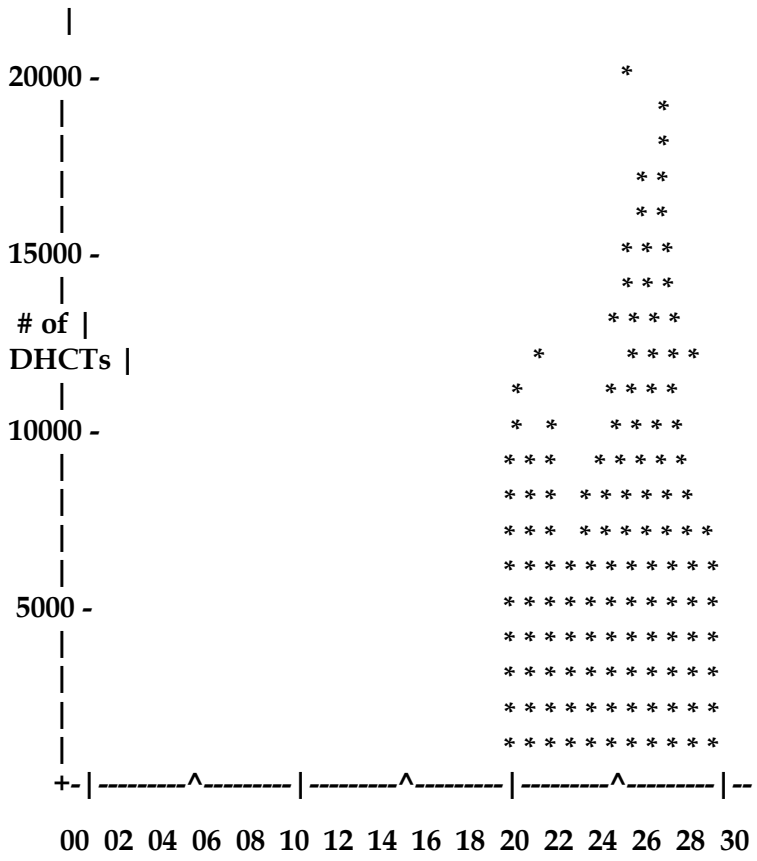
The following chart illustrates the distribution of expiring EMMs in a healthy system.

```
-------------------------------------------------------
Nov 20, 14:43:08 - ./smMix Started.
Total DHCTs (hct_profile rows)  in the database..... 186263
Total DHCTs (secure_micro rows) in the database..... 184178
-------------------------------------------------------
Expiration schedule date   InServ   Out-of
for Secure_Micro records    boxes  Service
 already expired...      0       0
 in  1 days              0       0
 in  2 days              0       0
 in  3 days              0       0
 in  4 days              0       0
 in  5 days              0       0
 in  6 days              0       0
 in  7 days              0       0
 in  8 days              0       0
 in  9 days              0       0
 in 10 days              0       0
 in 11 days              0       0
 in 12 days              0       0
 in 13 days              0       0
 in 14 days              0       0
 in 15 days              0       0
 in 16 days              0       0
 in 17 days              0       0
 in 18 days              0       0
 in 19 days              0       0
 in 20 days          12624    4571
 in 21 days           9734    5476
 in 22 days          10458    6212
 in 23 days           6578    1255
 in 24 days           8150    2499
 in 25 days           9821    5317
 in 26 days          13058    4622
 in 27 days          15701    6567
 in 28 days          17071    6553
 in 29 days          20866    7008
 in > 29 days         7490    2547

       TOTALS..... 131551    52627

--> emmDistributor is updating correctly!
Nov 20, 14:58:29 - ./smMix Ended.
```

Histogram Representing EMM Distribution

The following histogram illustrates the distribution of expiring EMMs in a healthy system.

Note: The data that comprises this histogram uses the same data used to generate the previous chart. Subsequent illustrations in this chapter show just the chart.



Number of Days to EMM Expiration
(131551 Total boxes reported)

DHCT Distribution in a System Where camAuditor Malfunctioned

The camAuditor process on the DNCS is designed to regenerate EMMs that are scheduled to expire in fewer than 20 days. If the camAuditor process malfunctions, it may not regenerate EMMs, and the EMMs would eventually expire. DHCTs with EMMs that have expired may not receive secured services and may go into Brick mode.

Examine the following smMix output obtained from a system on which the camAuditor process malfunctioned for an extended period of time.

Important! System operators who run smMix and discover that their system has EMMs set to expire in a few days, as illustrated in this example, should call Cisco Services.

Notes:

- Notice that many DHCTs have EMMs that have either already expired or are set to expire in a few days.
- The data in the following example comes from running the smMix utility in default mode, with no options.

May 24, 9:51:14 - smMix Started.

Total DHCTs (secure_micro rows) in the database.....298325

DHCTs with IPPV flag set (sm_admin_state=1)... 46702

Expiration Schedule Date for Secure_Micro records	InServ boxes	Out-of Service
already expired	0	29012
in 1 days	1100	3342
in 2 days	4437	4541
in 3 days	4619	4910
in 4 days	2974	3423
in 5 days	5359	6981
in 6 days	5380	5449
in 7 days	3564	2974
intentional break in data		
in 17 days	1274	3
in 18 days	1382	14

Expiration Schedule Date for Secure_Micro records	InServ boxes	Out-of Service
in 19 days	711	27
in 20 days	4023	913
in 21 days	4092	1050
in 22 days	4293	911
in 23 days	4037	966
in 24 days	15187	6455
in 25 days	8865	5962
in 26 days	2226	366
in 27 days	14734	5975
in 28 days	17554	4175
in 29 days	34523	23910
in 30 days	19329	16557
in > 30 days	0	0
Totals	169989	128336

May 24, 10:22:08 -- smMix Ended

DHCT Distribution in a System with an Uneven EMM Expiration Schedule

Examine the following smMix output from a system that has an uneven EMM expiration schedule.

Important! System operators who run smMix and discover that their system has an uneven distribution of EMMs, as illustrated in this example, should call Cisco Services.

Notes:

- Notice the peak in the number of DHCTs (almost 17,000) with EMMs set to expire on day 25 and day 26.
- The data in the following example comes from running the smMix utility in default mode, with no options.

Expiration schedule date for Secure_Micro records	InServ boxes	Out-of Service
already expired	0	2377
in 1 days	0	301
in 2 days	0	271
in 3 days	0	290
in 4 days	0	284
in 5 days	0	227
in 6 days	0	396
in 7 days	0	287
Intentional break in data		3000
in 17 days	0	367
in 18 days	0	299
in 19 days	0	482
in 20 days	0	526
in 21 days	4757	548
in 22 days	8191	591
in 23 days	12442	344
in 24 days	13908	1259

Expiration schedule date for Secure_Micro records	InServ boxes	Out-of Service
in 25 days	16977	1238
in 26 days	16924	1003
in 27 days	11930	1341
in 28 days	13059	1624
in 29 days	12694	1465
in 30 days	14404	839
in > 30 days	1625	30
Total	126911	19389

May 24, 18:52:36 -- smMix Ended

DHCT Distribution in a System That Uses the HCTM_PROVISIONING_APP Variable

Examine the following smMix output from a system that uses the HCTM_PROVISIONING_APP variable. The presence of a substantial number of DHCTs scheduled to expire within fewer than 21 days should not be alarming. These DHCTs are counted in the **OOS or Deployed** column. Recall that the DNCS does not maintain or refresh EMMs with a status of deployed at sites that use the HCTM_PROVISIONING_APP variable.

May 12, 18:33:15 - smMix Started.
Total DHCTs (hct_profile rows) in the database…….947889
Total DHCTs (secure_micro rows) in the database.....277325

Expiration schedule date for Secure_Micro records	InServ boxes	OOS or Deployed
already expired	0	5470
in 1 days	0	65
in 2 days	0	734
in 3 days	0	451
in 4 days	0	638
in 5 days	0	98
in 6 days	0	277
in 7 days	0	314
Intentional break in data		
in 17 days	0	583
in 18 days	110	139
in 19 days	6649	906
in 20 days	12311	1006
in 21 days	10602	1185
in 22 days	6391	660
in 23 days	10050	1165
in 24 days	11739	1851
in 25 days	7955	1142

Expiration schedule date for Secure_Micro records	InServ boxes	OOS or Deployed
in 26 days	13305	1466
in 27 days	14983	1530
in 28 days	9426	978
in 29 days	108262	3156
in > 29 days	38537	149
Totals	250320	27216

May 12, 18:52:36 - smMix ended

Run the smMix Utility

Running the smMix Utility

Choose one of the following options:

- To display information pertaining to how smMix works and the various options with which it can be used, go to ***Displaying the smMix Help*** (on page 128).
- To display the version number of the smMix utility loaded onto your system, go ***to Displaying smMix Version Num***ber (on page 129).
- To generate a histogram showing the age distribution of EMMs, go to ***Generating EMM Age Distribution*** (on page 129).

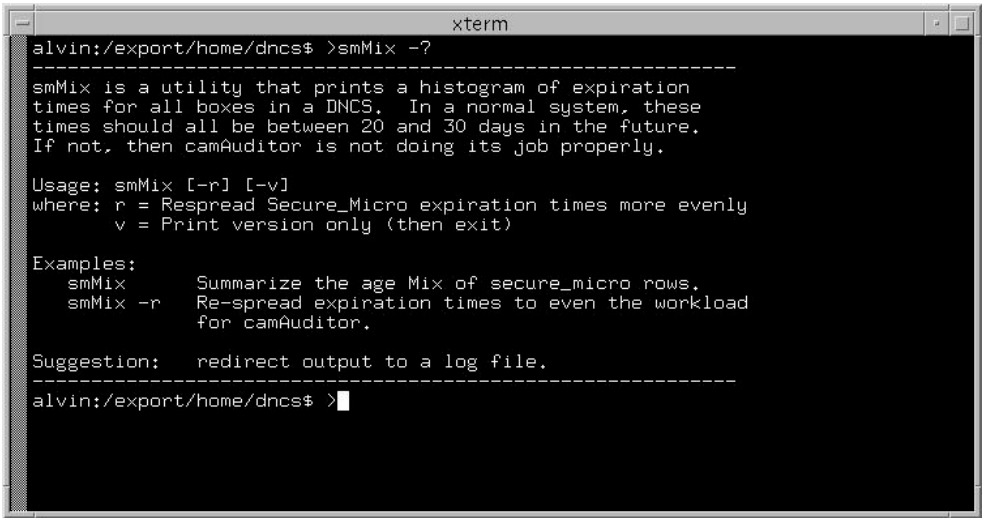
Displaying the smMIx Help

Follow these instructions to display information that describes how smMix works and the various options with which it can be used.

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

2 Type **smMix -?** and then press **Enter**. The smMix utility displays the following information pertaining to how smMix works and the various options with which it can be used.

Important! This output of this example lists the -r option. System operators should never run the smMix utility with the -r option without first contacting Cisco Services.



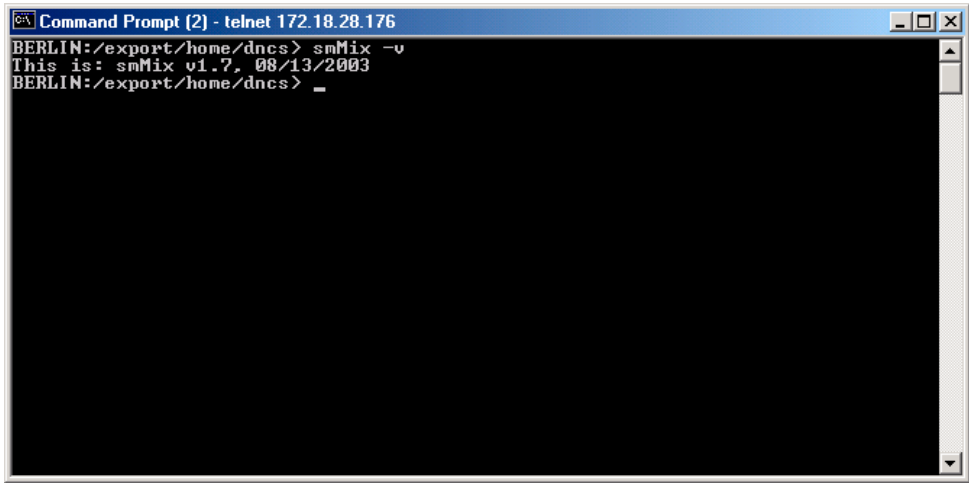
Displaying smMIx Version Number

Follow these instructions to display the version number of the smMix utility installed on your system.

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

2 Type **smMix -v** and then press **Enter**. The system displays the version number of the smMix utility.

Example: In this example, the version number of the smMix utility is v1.7.



Generating EMM Age Distribution

Follow these instructions to generate a histogram showing the age distribution of DHCT EMMs. Since the information in the histogram quickly scrolls off the screen, Cisco recommends that you direct the output to a log file that you can later examine.

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

2 Type **smMix > /tmp/smMix.[today's date]** and then press **Enter** to generate a histogram depicting the distribution of DHCT EMMs.

Notes:

- Substitute today's date for [today's date].

  Example: smMix > /tmp/smMix.081601

- Running the smMix utility without any options is for informational purposes, only. It does not change EMM expiration dates in the DNCS database.

- This command directs the output of the smMix utility to a logfile in the /tmp directory of the DNCS. Cisco recommends that you direct the output to a logfile that you can examine later because the output scrolls too quickly off of the screen.

3 Follow these instructions to examine the logfile you created when you completed step 2:

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

   b Type **more [name of logfile]** and then press **Enter**. The logfile opens using the UNIX more utility.

   Note: Substitute the name of the logfile you created in step 2 for [name of file].

   Example: more smMix.081601

   c Examine the distribution of DHCT EMMs in the logfile.

   Notes:

   – Press the **Spacebar** to page through the output file.

   – Press the **Ctrl** and **c** keys simultaneously to close the output file when you are finished.

4 Does the output you examined in step 3 indicate that your system has EMMs set to expire in less than 20 days?

- If **yes**, call Cisco Services.
- If **no**, continue with step 5.

5 Does the output you examined in step 3 indicate that your system has an unusually high number of EMMs set to expire on the same day?

- If **yes**, call Cisco Services.

  Note: Cisco Services may direct you to run a script that better distributes DHCT EMMs.

- If **no**, you are finished.

  Note: Cisco recommends that you run the smMix utility at least once every 2 weeks.

10

Find Unique Files and Software Packages with the keyFileFinder Utility

Introduction

Cisco developed the keyFileFinder utility to aid system operators as they upgrade system software to SR 2.5/3.5 or SR 4.0 using the UniPack.

The keyFileFinder utility detects files or packages that may be lost or replaced during the upgrade and records these files or packages in a logfile. System operators then send the logfile to Cisco Services for examination.

Important! System operators should run the keyFileFinder utility at least 1 week prior to upgrading their system software.

Cisco Services will examine the logfile and highlight any files or packages that should be backed up separately prior to the upgrade. The Cisco field service engineer responsible for upgrading a DBDS will have this list of files during the upgrade, and will ensure that any special files or packages are backed up prior to the upgrade and restored after the upgrade.

In This Chapter

- How the keyFileFinder Utility Works 132
- Run the keyFileFinder Utility 133

How the keyFileFinder Utility Works

Reports on Three Categories of Files

When system operators run the keyFileFinder utility, the utility compares the set of files installed during the upgrade with the files that currently exist on the system to be upgraded. The keyFileFinder utility reports on the following three categories of files:

- Files that were installed as part of a Solaris package and have since been changed or customized
- Files that have been installed or modified on the system, but are not part of any Solaris package

  Example: The keyFileFinder utility lists any software added to the system that is not in Solaris format, as well as any dedicated utilities used only at the site to be upgraded.
- Packages that have been installed on the system that will not be installed as part of the upgrade

  Note: Cisco field service engineers may need to reinstall these packages after the upgrade.

Run the keyFileFinder Utility

Running the keyFileFinder Utility

Follow these instructions to run the keyFileFinder utility.

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

Important! Skip steps 2 and 3 if you are already logged in to an xterm window as root user.

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

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

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

5 Choose one of the following options:

- If you are upgrading to SR 2.5/3.5, type **./keyFileFinder.ksh -r 2.5** and then press **Enter**.
- If you are upgrading to SR 4.0, type **./keyFileFinder.ksh -r 4.0** and then press **Enter**.

Results:

- The keyFileFinder utility executes and displays to the screen files and packages that may have to be backed up separately.
- A logfile is generated in the /export/home/dncs/check directory.

  Note: The logfile is named keyFileFinder.log.

6 Contact Cisco Services for instructions on how to send the logfile to Cisco.

11

Examine PCI Card Configuration with the slotchk Utility

Introduction

System operators run the slotchk utility to ensure that the Peripheral Component Interconnect (PCI) cards required for system upgrades are installed in the proper DNCS slots. Embedded within the slotchk utility is an array listing the expected PCI card configuration for the Sun Enterprise 250, the Sun Enterprise 450, and the Sun Fire V880 DNCS servers. The slotchk utility compares the actual PCI card configuration with the expected configuration and records the results in a logfile. System operators then send the logfile to Cisco Services for examination.

Important! System operators should run the slotchk utility at least a week prior to upgrading their systems.

Cisco Services will examine the logfile and report any discrepancies to the system operator.

In This Chapter

- Expected PCI Card Configuration..... 136
- Run the slotchk Utility 139

Expected PCI Card Configuration

Introduction

This section lists the expected PCI card configuration for the Sun Enterprise 250, the Sun Enterprise 450, and the Sun Fire V880 DNCS servers. The slotchk utility will log an error if a PCI slot does not contain the expected card, or if a slot that is supposed to be empty contains a card.

Enterprise 250 DNCS Server

The following table lists the expected PCI card configuration for an Enterprise 250 DNCS server.

Slot Number	Expected PCI Card
0	ATM card (FORE or OC3)
1	network adapter (SUNW, qsi-cheerio)
2	ASI card (video-pci5555), or empty
3	graphics card (GFXP)

Enterprise 450 DNCS Server

The following table lists the expected PCI card configuration for an Enterprise 450 DNCS server.

Slot Number	Expected PCI Card
1	graphics card (GFXP)
2	SCSI controller (Symbios, 53C875)
3	SCSI controller (Symbios, 53C875)
4	ASI card (video-pci5555), or empty
5	ASI card (video-pci5555), or empty
6	empty
7	network adapter (SUNW, qsi-cheerio)
8	empty
9	empty
10	ATM card (FORE or OC3)

Sun Fire V880 DNCS Server

The following table lists the expected PCI card configuration for the Sun Fire V880 DNCS server.

Slot Number	Expected PCI Card
0	graphics card (XVR-100)
1	ATM card (FORE or OC3)
2	ASI card (video-pci5555) or empty
3	empty
4	empty
5	empty
6	network adaptor
7	ASI card (video-pci5555) or empty
8	fiber channel card (SUNWqlc)

Known Error Condition

The slotchk utility uses the UNIX prtdiag maintenance command to analyze and display system configuration. The prtdiag command does not always work properly on an Enterprise 250 DNCS server running the Solaris 2.5.1 operating system.

The slotchk utility will always accurately report the condition of an Enterprise 250 DNCS server that is configured correctly. The results from an incorrect configuration, however, are unpredictable as even those PCI cards installed in the correct slots may go undetected.

System operators can draw the following conclusions about running the slotchk utility on an Enterprise 250 DNCS server running the Solaris 2.5.1 operating system:

- The slotchk utility will always correctly report an Enterprise 250 DNCS server that is configured properly.
- The slotchk utility will always record an error on an Enterprise 250 DNCS server that is configured incorrectly. The utility, however, may be unable to identify the error with precision.

Run the slotchk Utility

Running the slotchk Utility

Follow these instructions to run the slotchk utility.

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

Important! Skip steps 2 and 3 if you are already logged in to an xterm window as root user.

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

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

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

5 Type **./slotchk.pl** and then press **Enter**.

Results:

- The slotchk utility runs and displays the following information on the screen:
  - The PCI card configuration found on the DNCS server
  - Whether the configuration passes or fails.
- A logfile is generated in the /export/home/dncs/check directory that also reports on the PCI card configuration.

  Note: The logfile is named slotchk.log.

6 Contact Cisco Services for instructions on how to send the logfile to Cisco.

12

Obtain DHCT Information with the tellDhct Utility

Introduction

The tellDhct utility provides system operators and Cisco engineers with an easy way to query the database for DHCT information. The utility supports several options that can query the database for the following DHCT information:

- Whether a DHCT is assigned the brick mode package
- Conditional access configuration
- Return path capability
- Staging information
- DHCT model, revision, and hub information
- CableCARD Module and host information

The utility provides information for a single DHCT or for a list of DHCTs.

The information in this chapter provides instructions and examples for running the tellDhct utility.

In This Chapter

- The tellDhct Options 143
- Display the Help Window and Version Number of the tellDhct Utility 145
- Display Formatting Details for the tellDhct Utility 147
- Display Brick Mode Authorization 148
- Display Conditional Access Information 150
- Display Return Path Information 152
- Display Staging Information 155
- Display Model, Revision, and Hub Information 157
- Display CableCARD/Host Configuration 159

The tellDhct Options

Introduction

The information in this section provides an overview of the various options that apply to the tellDhct utility. Detailed instructions for running the tellDhct utility, as well as examples, are provided in later sections of this chapter.

Types of Data

Depending upon the options you use when you run the tellDhct utility, the utility queries various tables in the database and can report on the following types of data:

- When run in default mode (with no options), the utility queries the database for conditional access data.

  Examples: The utility provides the following information:

  - Whether the DHCT is enabled for two-way communication
  - The number of days remaining until EMMs belonging to the DHCT expire
  - Whether the DHCT has been staged
  - The number of packages and EMMs assigned to the DHCT
  - Whether the DHCT has a secure micro key certificate needed for encrypted services

- When run with the *-b* option, the utility identifies DHCTs that are assigned the brick mode package.

  Note: DHCTs need the brick mode package to operate. DHCTs without the brick mode package are rendered inoperative.

- When run with the *-h* option or the *-h2* option, the utility queries the hct_profile table for return path, or two-way, data.

  Note: The *-h* option and the *-h2* option provide identical information, with one exception. The *-h* option displays the IP address of the DHCT; the *-h2* option displays the billing ID of the DHCT.

  Examples: In addition to the IP address or the billing ID of the DHCT, the utility provides the following data:

  - Whether the DHCT is enabled for two-way communication
  - The OUI for the DHCT
  - The modulator and demodulator to which the DHCT is assigned

- When run with the *-s* option, the utility displays DHCT staging information.

  Examples: The utility provides the following information:

  - Whether the DHCT is enabled for two-way communication
  - The number of days remaining until EMMs belonging to the DHCT expire
  - The date the DHCT was last staged
- When run with the *-c* option, the utility displays DHCT model, revision, and hub information.
- When run with the *-C* option, the utility displays configuration data related to the CableCARD/host relationship.

Single DHCT or a List of DHCTs

The tellDhct utility provides information about a single DHCT or a list of DHCTs.

To obtain information about a single DHCT, provide the MAC address or the Secure Micro Serial Number (SMSN) of the DHCT.

To obtain information about a list of DHCTs, provide the name of a file that contains a list of MAC addresses, SMSNs, or DHCT serial numbers as an input parameter.

Note: Refer to Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243), for guidelines on preparing a text file for use with the tellDhct utility.

Formatting Details

In addition to the options listed earlier in this section, the tellDhct utility also supports the *-??* option. When run with the *-??* option, the tellDhct utility displays all of the data fields included in the output of the tellDhct utility and provides a brief explanation of each field.

Note: Refer to ***Display Formatting Details for the tellDhct Utility*** (on page 147) for instructions and an example for running the tellDhct utility with the *-??* option.

Display the Help Window and Version Number of the tellDhct Utility

Introduction

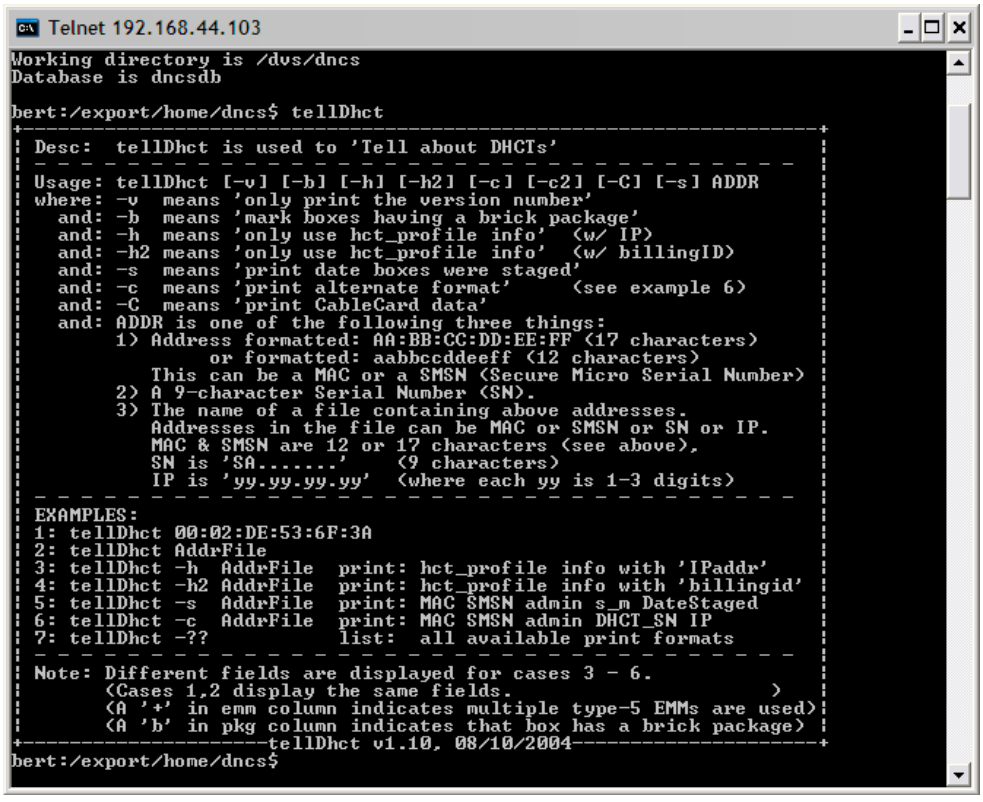
The information in this section describes how to display the help window and version number of the tellDhct utility.

Tip: Many utilities include a help window. The help window is frequently a good place to start if you are unfamiliar with a utility.

Displaying the tellDhct Help Window

Follow these instructions to display the help window for the tellDhct utility.

1. If necessary, open an xterm window on the DNCS.
2. Type **tellDhct** and then press **Enter**. The system displays the tellDhct help window.

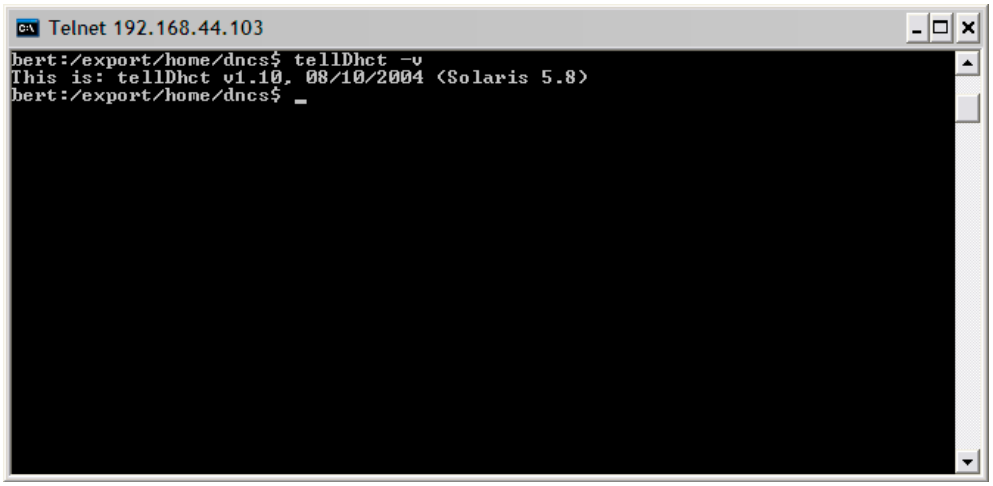


Displaying the Version Number of the tellDhct Utility

Follow these instructions to display the version number of the tellDhct utility.

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

2 Type **tellDhct -v** and then press **Enter**. The system displays the version number of the tellDhct utility.



Display Formatting Details for the tellDhct Utility

Introduction

The tellDhct utility includes the *-??* option. The *-??* option describes the various output formats for the tellDhct utility.

Displaying Formatting Details for the tellDhct Utility

Follow these instructions to display the output formats for the tellDhct utility.

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

2 Type **tellDhct -??** and then press **Enter**. The system displays the formatting details associated with the tellDhct utility.

Display Brick Mode Authorization

Introduction

The information in this section describes how to use the tellDhct utility to indicate which DHCTs are assigned the brick mode package.

Displaying Brick Mode Authorization

Follow these instructions to run the tellDhct utility in order to indicate which DHCTs are assigned the brick mode package.

Notes:

- DHCTs that are assigned the brick mode package appear with a "b" in the **pkg** column of the output.
- Refer to ***Display Formatting Details for the tellDhct Utility*** (on page 147) for a detailed description of the fields displayed in the output.

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

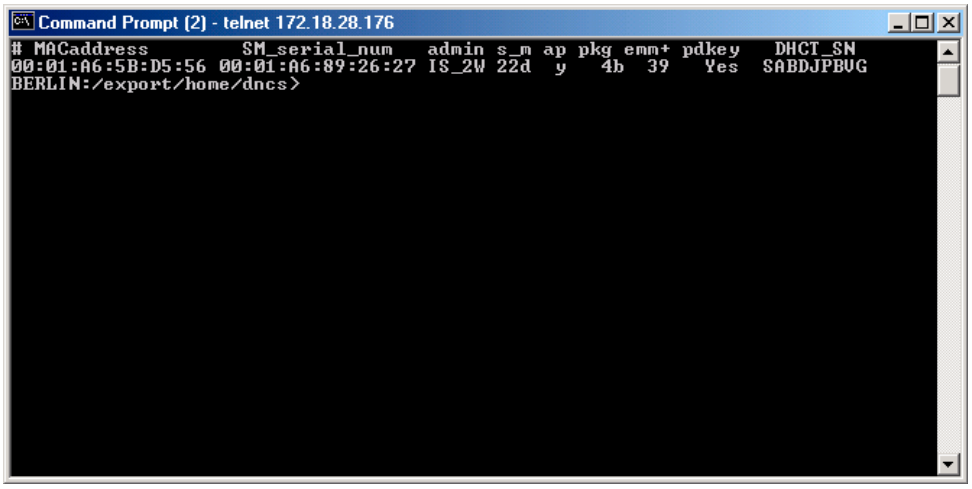
2 Choose one of the following options:

- To determine whether a single DHCT has the brick mode package, go to step 3.
- To identify DHCTs in a list of DHCTs that have the brick mode package, go to step 4.

3 Type **tellDhct -b [MAC address or SMSN]** and then press **Enter**.

Note: Substitute the MAC address or SMSN of the DHCT for [MAC address or SMSN].

Example: tellDhct -b 00:40:7B:D6:02:3A



4 Type **tellDhct -b /tmp/[file name]** and then press **Enter**. The system identifies the DHCTs in the file that have the brick mode package.

Notes:

- Substitute the name of your prepared input file for [file name].
- Refer to Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243), for guidelines and instructions on preparing a text file for use with the tellDhct utility.

Example: tellDhct /tmp/tellDhct-input.04.30.02

# MACaddress	SM_serial_num	admin	s_m	ap	pkg	emm	pdkey	DHCT_SN
00:40:7B:D6:02:3A	00:40:7B:95:5F:E6	IS_2W	25d	y	4b	39	Yes	SABGDNKSN
00:40:7B:D6:02:44	00:40:7B:95:5F:E4	IS_2W	25d	y	4b	39	Yes	SABGDNKST
00:40:7B:D6:02:48	00:40:7B:95:5F:FA	IS_2W	25d	y	6b	39	Yes	SABGDNKSW
00:40:7B:D6:02:58	00:40:7B:95:5F:FF	OOS	--	--	--	2	Yes	SABGDNKTH
00:40:7B:C1:C5:C0	00:40:7B:8F:E7:F5	IS_2W	25d	y	4	39	Yes	SABFXJLFW
00:40:7B:C1:C5:DE	00:40:7B:35:CF:4A	IS_2W	25d	y	4	39	Yes	SABFXJLGQ
00:40:7B:C1:C6:04	00:40:7B:8F:E7:E0	IS_2W	25d	y	4	39	Yes	SABFXJLHP
00:40:7B:C1:C6:7E	00:40:7B:8F:E8:0D	IS_2W	25d	y	4	39	Yes	SABFXJLLQ
00:40:7B:C1:C7:6E	00:40:7B:8F:E7:EB	IS_2W	25d	y	8b	39	Yes	SABFXJLSQ
00:40:7B:C1:C7:BC	00:40:7B:8F:E7:0F	IS_2W	25d	y	4	39	Yes	SABFXJLVP
00:40:7B:C1:C8:90	00:40:7B:35:CE:03	IS_2W	25d	y	4	39	Yes	SABFXJMCW
00:40:7B:C1:C9:82	00:40:7B:35:CD:48	IS_2W	25d	y	4	39	Yes	SABFXJMKX
00:40:7B:C1:C9:F8	00:40:7B:8F:E7:14	IS_2W	25d	y	4	39	Yes	SABFXJMNW

Display Conditional Access Information

Introduction

The information in this section describes how to use the tellDhct utility to display conditional access information for DHCTs.

Displaying Conditional Access Information

Follow these instructions to run the tellDhct utility to display conditional access information for a single DHCT or a list of DHCTs.

Note: Refer to ***Display Formatting Details for the tellDhct Utility*** (on page 147) for a detailed description of the fields displayed in the output.

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

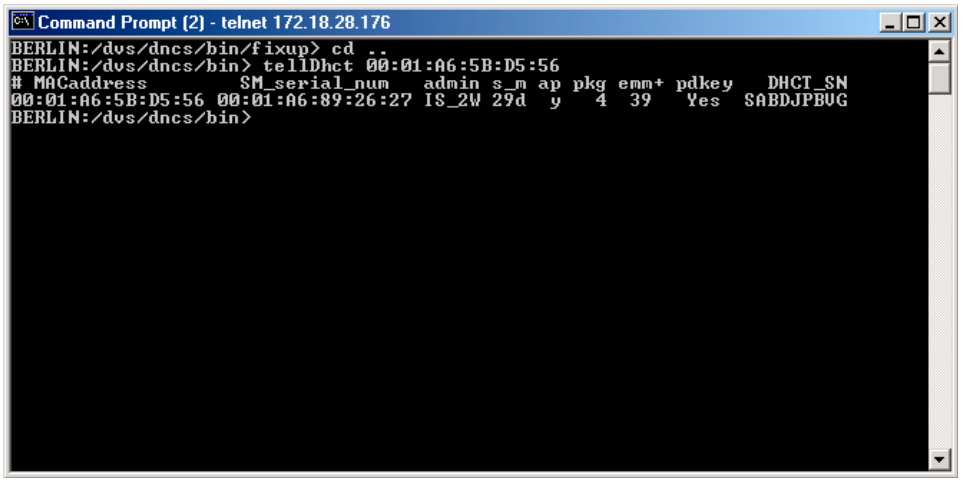
2 Choose one of the following options:

- To display conditional access information for a single DHCT, go to step 3.
- To display conditional access information for a list of DHCTs, go to step 4.

3 Type **tellDhct [MAC address or SMSN]** and then press **Enter**. The system displays conditional access information for the DHCT.

Note: Substitute the MAC address or SMSN of the DHCT for [MAC address or SMSN].

Example: tellDhct 00:01:A6:5B:D5:56

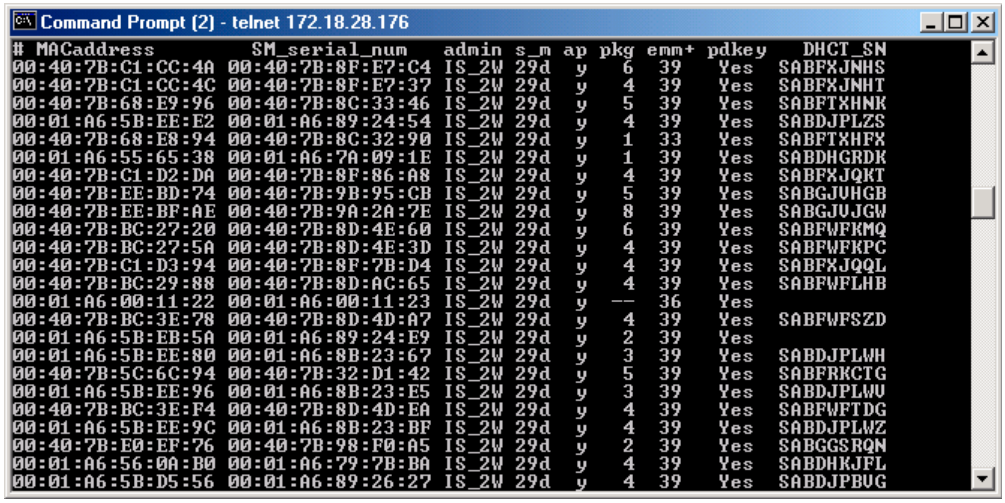


4 Type **tellDhct /tmp/[file name]** and then press **Enter**. The system displays conditional access information for the DHCTs listed in the input file.

Notes:

- Substitute the name of your prepared input file for [file name].
- Refer to Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243), for guidelines and instructions on preparing a text file for use with the tellDhct utility.

Example: tellDhct /tmp/tellDhct-input.04.30.02



Display Return Path Information

Introduction

The information in this section describes how to use the tellDhct utility to display return path information for DHCTs.

Displaying Return Path Information

Follow these instructions to run the tellDhct utility to display information about the return path capabilities of a single DHCT or a list of DHCTs.

Note: Refer to Display Formatting Details for the tellDhct Utility, earlier in this chapter, for a detailed description of the fields displayed in the output.

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

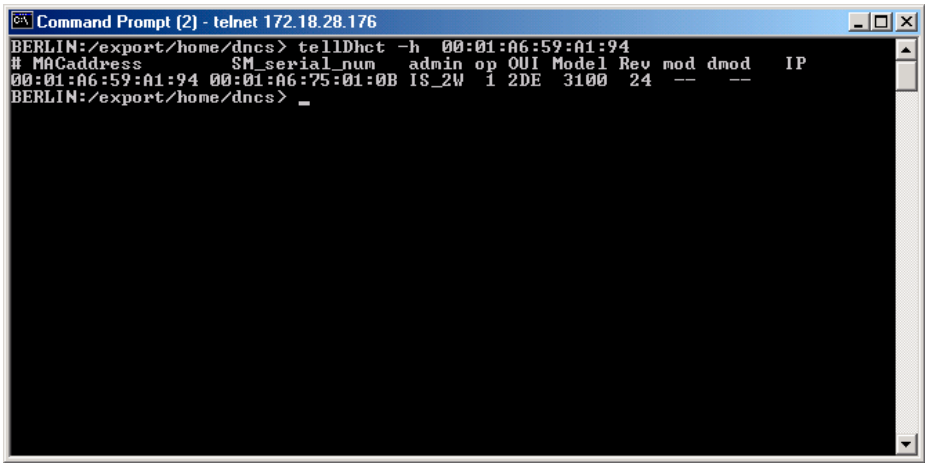
2 Choose one of the following options:

- To obtain information about the return path capabilities for a single DHCT, showing the *IP address* of the DHCT in the output, go to step 3.
- To obtain information about the return path capabilities for a single DHCT, showing the *billing ID* of the DHCT in the output, go to step 4.
- To obtain information about the return path capabilities for a list of DHCTs, showing the *IP address* of the DHCTs in the output, go to step 5
- To obtain information about the return path capabilities for a list of DHCTs, showing the *billing ID* of the DHCTs in the output, go to step 6.

3 Type **tellDhct -h [MAC address or SMSN]** and then press **Enter**. The system displays information about the return path capabilities for the DHCT.

Note: Substitute the MAC address or SMSN of the DHCT for [MAC address or SMSN].

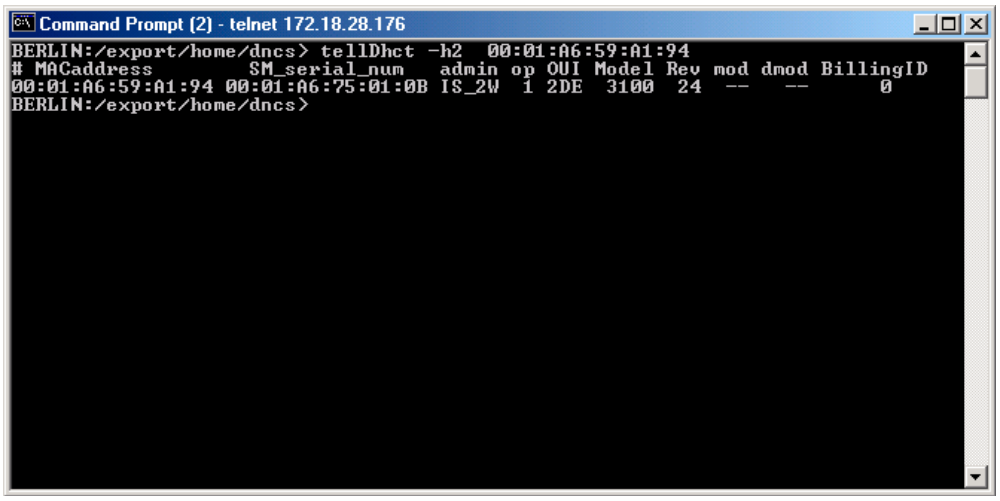
Example: tellDhct -h 00:01:A6:59:A1:94



4 Type **tellDhct -h2 [MAC address or SMSN]** and then press **Enter**. The system displays information about the return path capabilities for the DHCT.

Note: Substitute the MAC address or SMSN of the DHCT for [MAC address or SMSN].

Example: tellDhct -h2 00:01:A6:59:A1:94

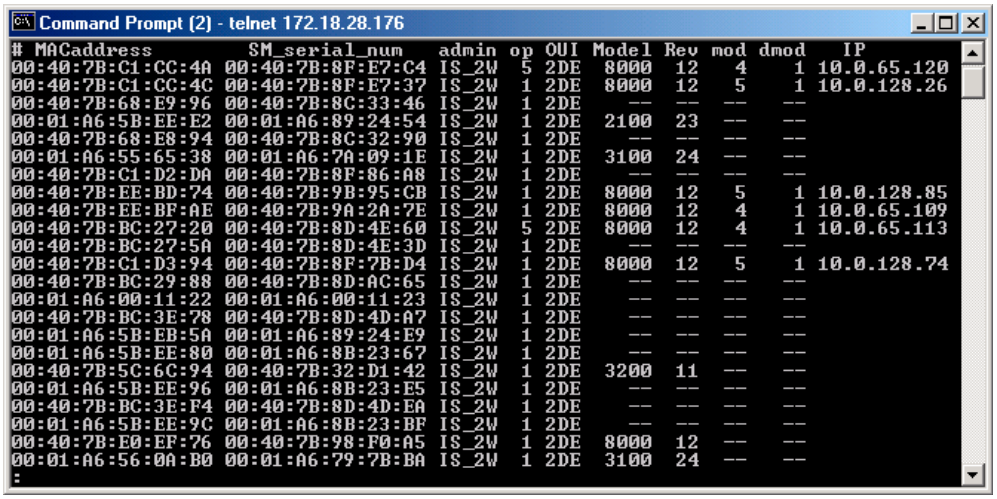


5 Type **tellDhct -h /tmp/[file name]** and then press **Enter**. The system displays information about the return path capabilities for the DHCTs listed in the input file.

Notes:

- Substitute the name of your prepared input file for [file name].
- Refer to Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243), for guidelines and instructions on preparing a text file for use with the tellDhct utility.

Example: tellDhct -h /tmp/tellDhct-input.04.30.02

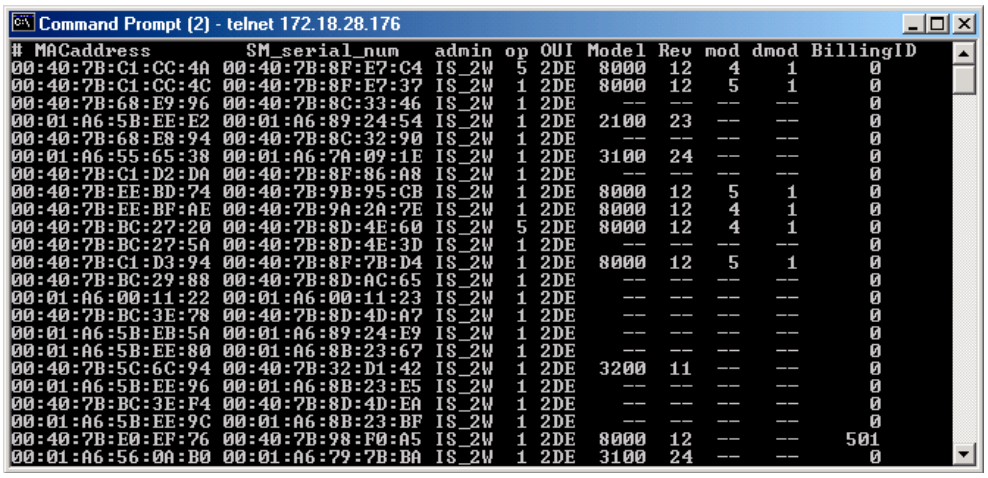


6 Type **tellDhct -h2 /tmp/[file name]** and then press **Enter**. The system displays information about the return path capabilities for the DHCTs listed in the input file.

Notes:

- Substitute the name of your prepared input file for [file name].
- Refer to Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243), for guidelines and instructions on preparing a text file for use with the tellDhct utility.

Example: tellDhct -h2 /tmp/tellDhct-input.04.30.02



Display Staging Information

Introduction

The information in this section describes how to use the tellDhct utility to display DHCT staging information.

Displaying Staging Information

Follow these instructions to run the tellDhct utility to display staging information about a single DHCT or a list of DHCTs.

Note: Included in the staging information is the date that DHCTs were staged. This information is lost when system operators run the dbOptimizer program. The system will display the date DHCTs were staged only for those DHCTs that still have their staging EMMs.

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

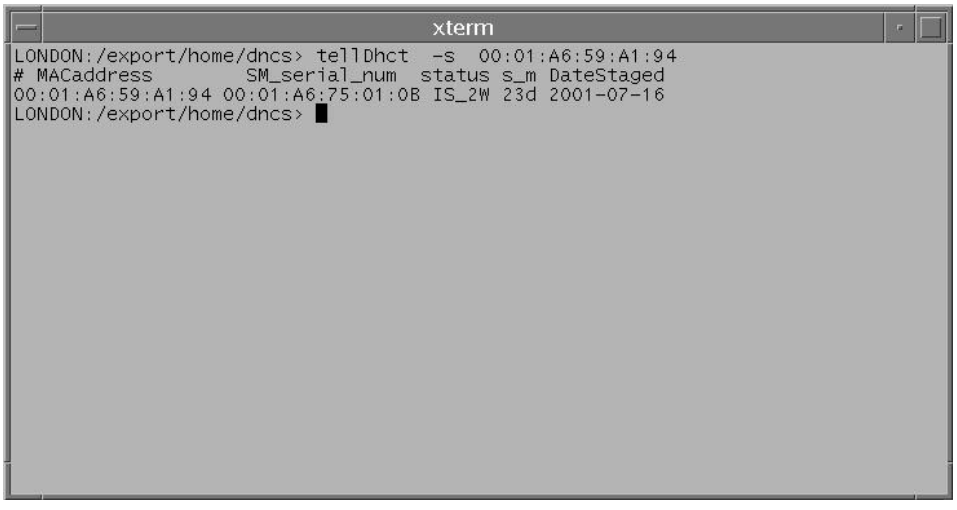
2 Choose one of the following options:

- To display staging information for a single DHCT, go to step 3.
- To display staging information for a list of DHCTs, go to step 4.

3 Type **tellDhct -s [MAC address or SMSN]** and then press **Enter**. The system displays staging information for the DHCT.

Note: Substitute the MAC address or SMSN of the DHCT for [MAC address or SMSN].

Example: tellDhct -s 00:01:A6:59:A1:94

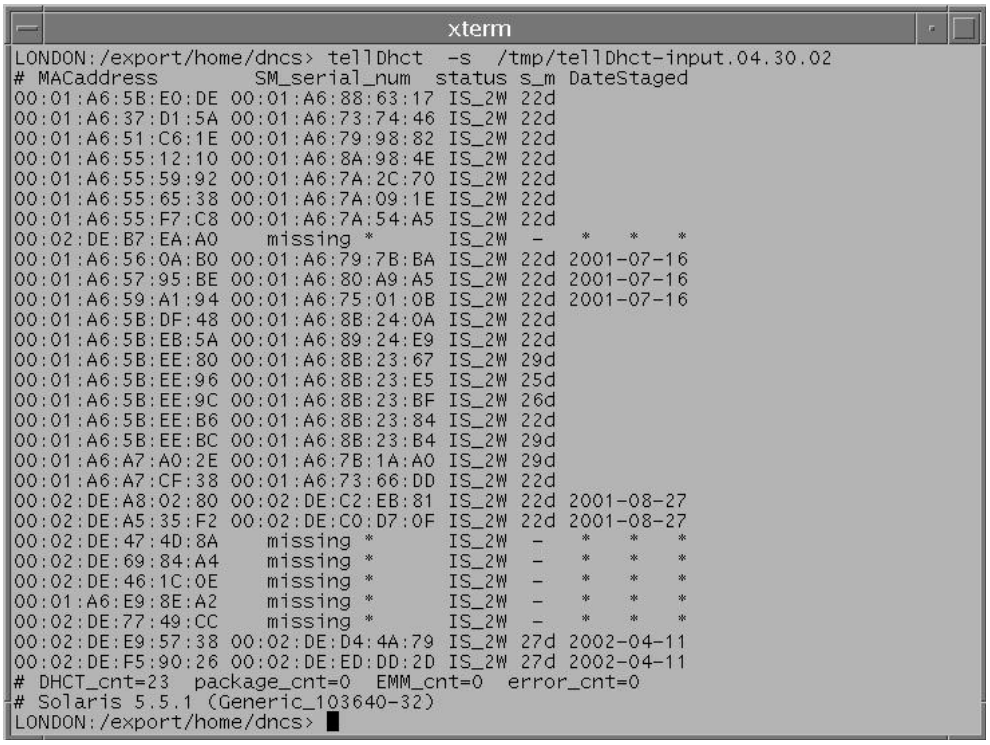


4 Type **tellDhct -s /tmp/[file name]** and then press **Enter**. The system displays staging information for the DHCTs listed in the input file.

Notes:

- Substitute the name of your prepared input file for [file name].
- Refer to Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243), for guidelines and instructions on preparing a text file for use with the tellDhct utility.

Example: tellDhct -s /tmp/tellDhct-input.04.30.02



Display Model, Revision, and Hub Information

Introduction

The information in this section describes how to use the tellDhct utility to display DHCT model, revision, and hub information

Displaying Model, Revision, and Hub Information

Follow these instructions to run the tellDhct utility to display DHCT model, revision, and hub information.

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

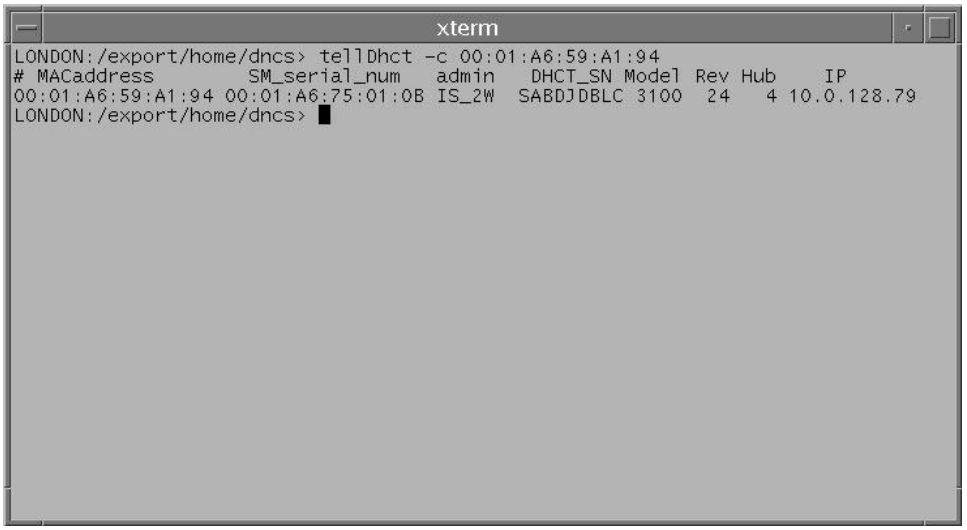
2 Choose one of the following options:

- To display model, revision, and hub information for a single DHCT, go to step 3.
- To display model, revision, and hub information for a list of DHCTs, go to step 4.

3 Type **tellDhct -c [MAC address or SMSN]** and then press **Enter**. The system displays model, revision, and hub information for the single DHCT.

Note: Substitute the MAC address or SMSN of the DHCT for [MAC address or SMSN].

Example: tellDhct -c 00:01:A6:59:A1:94

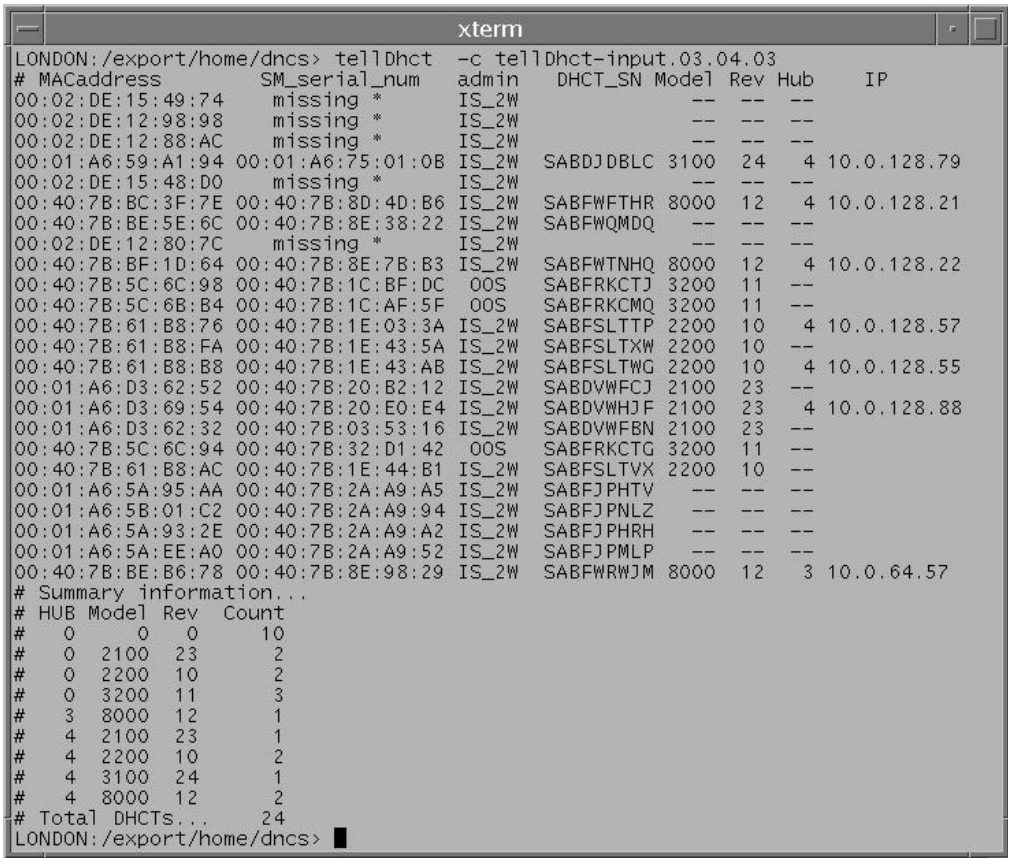


4 Type **tellDhct -c /tmp/[file name]** and then press **Enter**. The system displays model, revision, and hub information for the DHCTs listed in the input file, and then summarizes the information by hub.

Notes:

- Substitute the name of your prepared input file for [file name].
- Refer to Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243), for guidelines and instructions on preparing a text file for use with the tellDhct utility.

Example: tellDhct -c /tmp/tellDhct-input.04.30.02



Display CableCARD/Host Configuration

Introduction

The information in this section describes how to use the tellDhct utility to display configuration data related to the CableCARD/host relationship. When used with the *-C* option, the tellDhct utility displays the following data:

- MACaddress - MAC address of the CableCARD
- SM_serial_num - serial number of the secure micro chip
- Host_id - ID number of the host to which the CableCARD is bound
- active_file_date - the date until which data for the CableCARD/host binding stays in the BFS file
- rev - revoked

  Note: This field can have two values: a dash or REV. A dash indicates that the subscriber can view copy-protected content; REV indicates that the subscriber cannot view copy-protected content.

Displaying CableCARD/Host Configuration

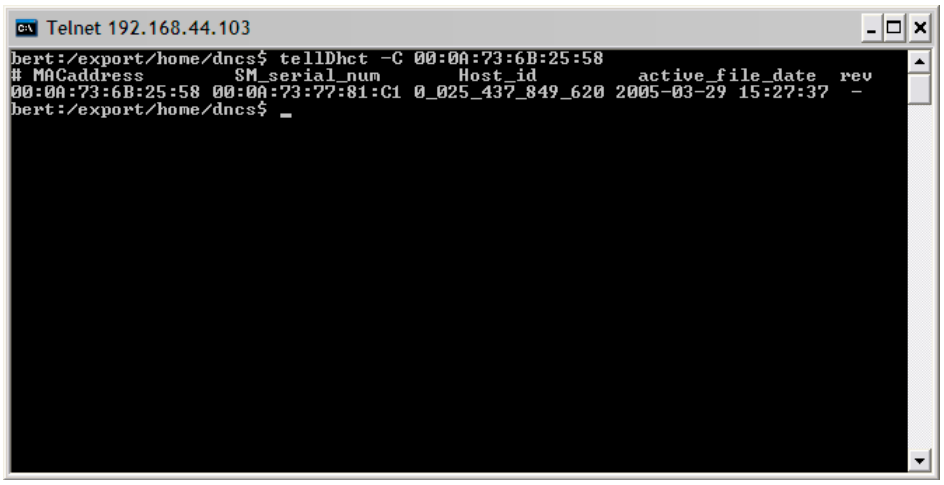
Follow these instructions to run the tellDhct utility to display configuration data related to the CableCARD/host relationship.

1. If necessary, open an xterm window on the DNCS.
2. Choose one of the following options:
   - To display data for a single CableCARD, go to step 3.
   - To display data for a list of CableCARDs, go to step 4.

3 Type **tellDhct -C [MAC address or SMSN]** and then press **Enter**. The system displays data for a single CableCARD.

Note: Substitute the MAC address or SMSN of the CableCARD for [MAC address or SMSN].

Example: tellDhct -C 00:0A:73:6B:25:58

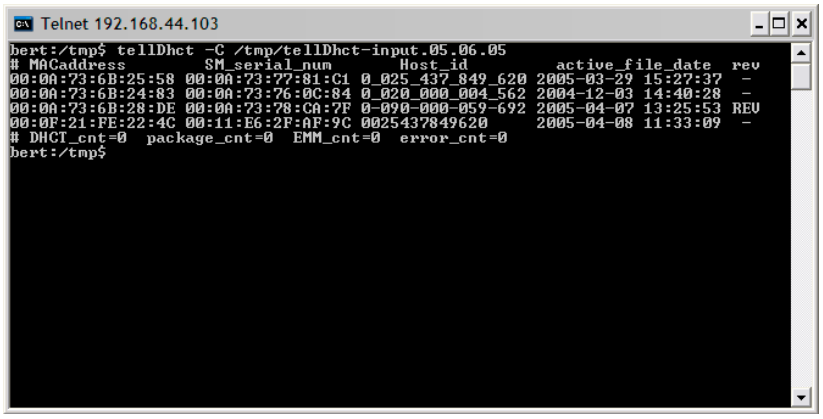


4 Type **tellDhct -C /tmp/[file name]** and then press **Enter**. The system displays CableCARD/host data for the CableCARDs listed in the input file.

Notes:

- Substitute the name of your prepared input file for [file name].
- Refer to Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243), for guidelines and instructions on preparing a text file for use with the tellDhct utility.

Example: tellDhct -C /tmp/tellDhct-input.05.06.05



13

Assign DHCTs to Download Groups with the runCvtGroup Utility

Introduction

When system operators use the CVT method to download DHCT code, they sometimes want to restrict the download to DHCTs that belong to a specific download group. Prior to the release of the runCvtGroup utility, system operators had to use the DNCS user interface to assign DHCTs to the download group. The process of assigning DHCTs to the download group was often quite lengthy; system operators had to type one MAC address at a time.

Cisco developed the runCvtGroup utility to expedite the process by which DHCTs are assigned to download groups. System operators prepare a text file that contains one DHCT MAC address per line. The runCvtGroup utility then reads that text file and quickly assigns the DHCTs associated with those MAC addresses to the specified download group.

Note: The download group must already exist.

The instructions in this chapter tell you how to run the runCvtGroup utility.

In This Chapter

- Run the runCvtGroup Utility 162

Run the runCvtGroup Utility

Running the runCvtGroup Utility

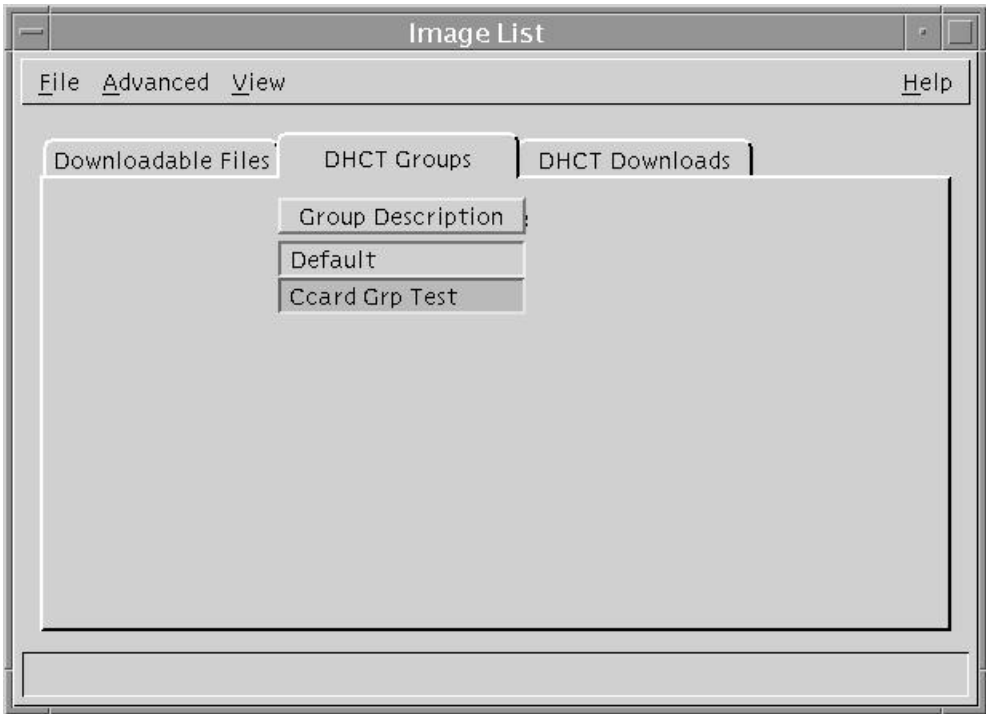
Use these instructions to run the runCvtGroup utility.

1 Do you need to create a download group?

- If **yes**, go to step 2.
- If **no**, go to step 7.

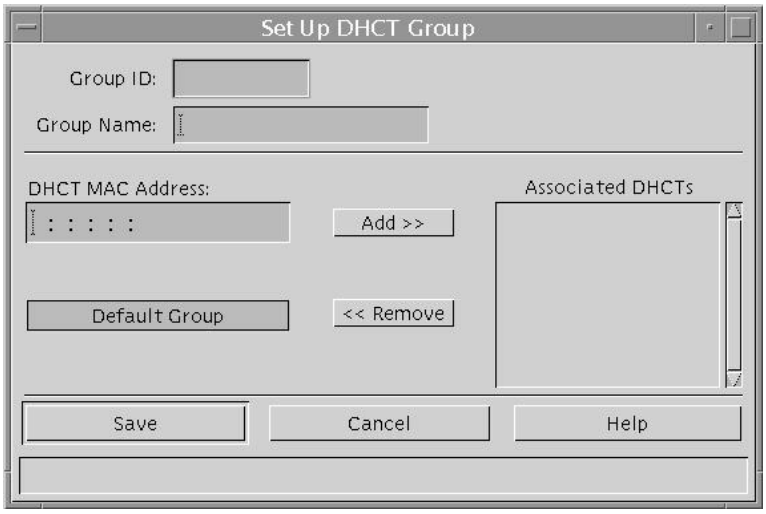
2 From the DNCS Administrative Console, select the **Element Provisioning** tab.

3 Click **Image**. The Image List window opens.



4 Select the **DHCT Groups** tab.

5 Click **File** and then select **New**. The Set Up DHCT Group window opens.



6 Follow these instructions to configure the Set Up DHCT Group window.

a Type an unused group ID in the **Group ID** field.

b Type a name for the group in the **Group Name** field.

c Type the MAC address of a DHCT that you want in the download group in the **DHCT MAC Address** field.

d Click **Add**.

e Repeat steps c) and d) for any other DHCT that you want to belong to the download group.

f Click **Save**.

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

8 Type **runCvtGroup [group ID] [file name]** and then press **Enter**. The system assigns the DHCTs in the text file to the specified download group.

Example: Type **runCvtGroup 2 /tmp/runCvtGroup-in_03.04.03** and then press **Enter** to assign the DHCTs in the text file to download group 2.

Notes:

- Refer to Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243), for instructions on preparing a text file for use with the runCvtGroup utility.
- Substitute the ID of the download group for [group ID].
- Substitute the name of the text file for [file name].

14

Monitor the Status of System Metadevices with the check_metadevices Utility

Introduction

The check_metadevices utility constantly monitors the state of the metadevices on an Enterprise 450 or Sun Fire 880 DNCS and then reports any errors it finds. The utility runs automatically after you install the DBDS Utilities; system operators or engineers do not have to invoke any specific commands to run the check_metadevices utility.

Notes:

- A metadevice is a group of physical devices accessed through a virtual or logical device.
- The check_metadevices utility replaces the sdsCheck utility, which was part of the CoolTools suite of utilities in DBDS Utilities version 2.2.

In This Chapter

- Understanding the check_metadevices Utility..... 166

Understanding the check_metadevices Utility

Supported Hardware Platforms

The check_metadevices utility runs only on an Enterprise 450 or Sun Fire 880 DNCS; the utility does not run on an Enterprise 250 DNCS. System operators do not have to run any special command to run the check_metadevices utility. The utility runs automatically after you install the DBDS Utilities.

Three Ways of Reporting Errors

The check_metadevices utility reports any metadevice errors it finds in the following three ways:

- The utility displays a window on the DNCS that describes the error, as well as the time and date the error occurred.
- The utility sends e-mail that notifies the dncs user and root user of the error.
- If the site supports the Alarm Manager network management system, the check_metadevices utility reports those errors to the Alarm Manager software.

Call Cisco Services

System operators should always call Cisco Services before troubleshooting or trying to correct any errors reported by the check_metadevices utility.

Important! Do not try to correct any errors reported by the check_metadevices utility yourself. Always call Cisco Services first.

15

Monitor the Logfiles of DNCS Processes with the qtail and sesstail Utilities

Introduction

The logfiles in the /dvs/dncs/tmp directory contain important information about how the DNCS processes are operating. As the processes run, they typically write entries into their associated logfiles that provide system operators and Cisco engineers with valuable debugging information. A typical entry into a logfile contains a time-stamp, as well as the current values of the software parameters and variables coded into the processes. Cisco engineers developed the qtail and sesstail utilities to help system operators and engineers monitor the DNCS logfiles.

In This Chapter

- Design of the qtail and sesstail Utilities and the System Logfiles 168
- The qtail Utility 169
- The sesstail Utility 172

Design of the qtail and sesstail Utilities and the System Logfiles

Design of the qtail and sesstail Utilities

The UNIX operating system includes a utility called tail. The tail utility allows someone to monitor a file in real time; as a new line is written to a file, that line is instantly displayed by the tail utility.

Note: To learn more about the tail utility, from an xterm window on the DNCS, type **man tail** and then press **Enter**.

In theory, you can use the tail utility to monitor the logfile of a DNCS process in real time. The problem, however, comes when that logfile reaches its 50,000 line limit. The tail utility has no way of knowing that a limit has been reached and that a new logfile has been created. Hence, no new data can be observed in the logfile monitored by the tail utility.

The qtail utility uses the UNIX tail utility to monitor logfiles of DNCS processes in real time. When the limit of a specific logfile is reached, however, the qtail utility automatically starts monitoring the newly created file.

The sesstail utility is very similar to the qtail utility but is specifically designed to monitor the dsm process logfiles video-on-demand (VOD) session-related activities.

Design of the System Logfiles

Cisco places a limit on how large the logfiles in the /dvs/dncs/tmp directory can grow. If the logfiles were designed to grow without limit, the logfiles might eventually grow so large that they would slow down the performance of the DNCS. By default, Cisco places a 50,000 line limit on individual logfiles. Each DNCS process supports up to 10 logfiles; the first logfile has a **.000** extension, the second logfile has a **.001** extension, and so on.

Example:

- camPsm.000
- camPsm.001
- camPsm.002

When a process reaches its 10-logfile limit, the system overwrites the first logfile with new data. By supporting 10 logfiles, the DNCS allows system operators and engineers plenty of time to save a specific logfile for later examination.

The qtail Utility

Introduction

The logfiles in the /dvs/dncs/tmp directory of the DNCS have a default limit of 50,000 lines. After 50,000 lines, the system creates a new logfile. The qtail utility allows system operators or Cisco engineers to monitor log activity and automatically switches to the next logfile when the 50,000 line limit has been reached.

The qtail utility was designed to monitor an entire logfile, or you can configure it to display only those lines that contain a particular pattern. When you configure the qtail utility to display lines in a logfile that contain a particular pattern, the utility uses the UNIX grep utility to search for that pattern.

Running the qtail Utility

Follow these instructions to run the qtail utility.

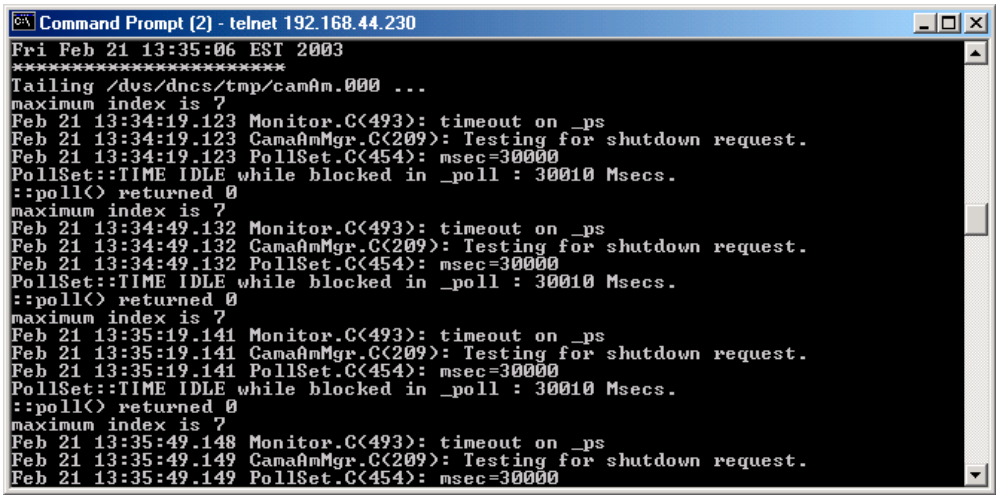
1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/tmp** and then press **Enter**. The /dvs/dncs/tmp directory becomes the working directory.
3. Choose one of the following options:
   - To use the qtail utility to monitor an entire logfile, go to step 4.
   - To use the qtail utility to display only those lines that contain a particular pattern, go to step 6.

4 To use the qtail utility to monitor an entire logfile, type **qtail [process_name]** and then press **Enter**. The qtail utility begins monitoring the logfile of the selected process.

Notes:

- Substitute the process name whose logfile you want to monitor for [process_name].
- You do not have to type the complete process name; you can type just enough to uniquely identify the process name from other processes.
  - Type qamM for qamManager.
  - Type siM for siManager.
  - Type camAu for camAuditor.

Example: Type **qtail camAu** and then press **Enter** to display the logfile associated with the camAuditor process.



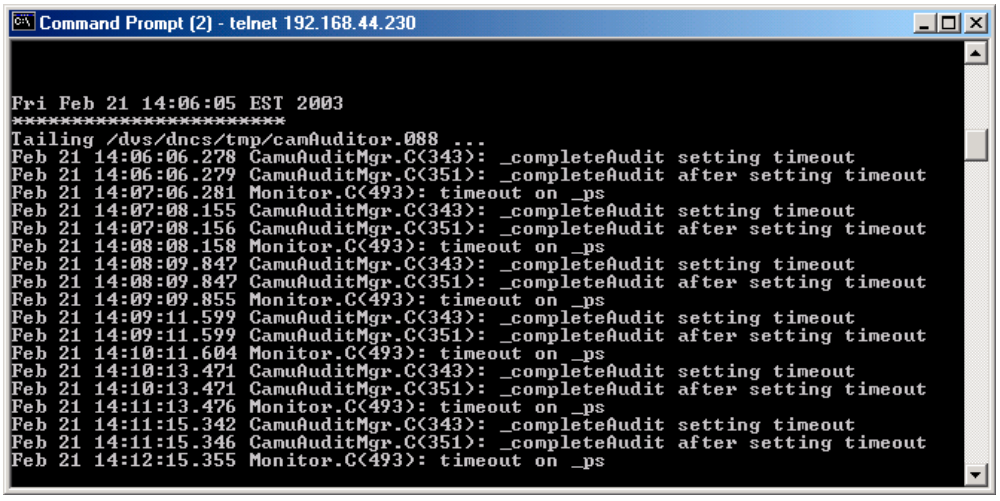
5 Type the **Ctrl** and **c** keys simultaneously to exit from the qtail utility.

6 To use the qtail utility to monitor a logfile and display only those lines that contain a particular pattern, type **qtail [process_name] <pattern>** and then press **Enter**. The qtail utility begins monitoring the logfile of the selected process.

Notes:

- Substitute the process name whose logfile you want to monitor for [process_name].
- You do not have to type the complete process name; you can type just enough to uniquely identify the process name from other processes.
  - Type **qamM** for qamManager.
  - Type **siM** for siManager.
  - Type **camAu** for camAuditor.
- Substitute the pattern you want to find for <pattern>.

Example: Type **qtail camAu timeout** and then press **Enter** to display only those lines that contain the word timeout in the logfiles associated with the camAuditor process.



7 Type the **Ctrl** and **c** keys simultaneously to exit from the qtail utility.

The sesstail Utility

Introduction

The sesstail utility is similar to the qtail utility, except that it is designed to monitor the logfiles of the dsm process for session-related information. Examples of session-related information include session set up and tear-down activity.

You can use the sesstail utility to monitor the logfiles of the dsm process for session-related activity in real time or to search for session-related activity in existing dsm logfiles.

Note: By searching for session-related activity in existing dsm logfiles, you can troubleshoot VOD problems that have already occurred.

Running the sesstail Utility

Follow these instructions to run the sesstail utility.

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

2 Choose one of the following options:

- To monitor the dsm logfiles in real time for session-related activity, go to step 3.
- To review existing dsm logfiles for session-related activity, go to step 5.

3 To monitor the dsm logfiles for session-related activity in real time, type **sesstail** and then press **Enter**. The sesstail utility begins monitoring the dsm logfiles for session-related activity.

Example: Sample output from the sesstail utility is displayed in the following example.

```
$ sesstail
 ++++ 00:40:7B:D6:B5:B3/515 ++++
ClientSessReq:    Feb 19 07:23:50.008
ServerSessInd:    Feb 19 07:23:50.016
ServerAddRsrReq:  Feb 19 07:23:50.207
ServerAddRsrCnf:  Feb 19 07:23:50.270 (response=0)
ServerSessRsp:    Feb 19 07:23:50.335 (response=0)
ClientSessCnf:    Feb 19 07:23:50.346 (response=0)
 ++++ 00:40:7B:D6:B5:B3/515 ++++
ClientRelReq:     Feb 19 07:23:58.683
ServerRelInd:     Feb 19 07:23:58.687
ServerRelRsp:     Feb 19 07:23:58.709 (Response=0)
ClientRelCnf:     Feb 19 07:23:58.713 (Response=0)
```

4 Type the **Ctrl** and **c** keys simultaneously to exit from the sesstail utility.

5 To review an existing dsm logfile for session-related activity, type **sesstail [filename]** and then press **Enter**. The selected file opens for review.

Note: Substitute the path and name of the logfile you want to review for [filename].

Example: sesstail /dvs/dncs/tmp/dsm.000

6 Type the **Ctrl** and **c** keys simultaneously to exit from the sesstail utility.

16

Convert Binary IPPV Purchase Reports Into Text Format with the parseIppvRept Utility

Introduction

The billing system retrieves impulse pay-per-view (IPPV) data from the DNCS database on a regular basis. After retrieving the data, the ippvManager process on the DNCS creates a file in the /dvs/ftp/purchaseReportArchive directory that contains a copy of the data it collected. The file in the /dvs/ftp/purchaseReportArchive directory of the DNCS, called the IPPV purchase report, is in binary format, a format that cannot be read and understood. Cisco engineers developed the parseIppvRept utility to help system operators and Cisco engineers understand the data in the IPPV purchase report.

In This Chapter

- The Data in the IPPV Purchase Report 176
- The Options Available with the parseIppvRept Utility 177
- Run the parseIppvRept Utility 178
- View the Output File 180

The Data in the IPPV Purchase Report

The IPPV Purchase Report

The IPPV purchase report contains the following data:

- Record type-whether purchase or cancellation of a purchase
- MAC address-MAC address of the DHCT that purchases or cancels a purchase
- Package name-name of the package purchased or cancelled
- Purchase time-date and time of day associated with the purchase or cancellation
- Event length-length of the event purchased or cancelled
- Cost-cost of the event purchased or cancelled
- Right to copy-whether the VCR Commander can be used to copy the event
- Billing ID-which billing computer the billing vendor uses to process billing transactions associated with the specific DHCT

The Options Available with the parseIppvRept Utility

Introduction

The information in this section describes the options with which the parseIppvRept utility is run.

The parseIppvRept Utility Options

The following list contains the options that pertain to the parseIppvRept utility:

- *-I-* input file name. The input file name is required when you run the parseIppvRept utility and refers to the name of the IPPV purchase report in the /dvs/ftp/purchaseReportArchive directory that you want to convert to text format. The billing system supplies the name of the IPPV purchase report when it writes the file to the /dvs/ftp/purchaseReportArchive directory. Anyone running the parseIppvRept utility merely has to know which report to convert. Most frequently, the system operator will want to convert the IPPV purchase report from the previous night-the newest file in the directory.
- *-O-* output file name. The output file name is optional and is used only when the system operator wants to direct the converted IPPV report to a file for later examination. When the *-O* option is not used, output goes to the DNCS screen.

  Note: Output from the parseIppvRept utility can be quite lengthy. Cisco recommends that system operators direct the output from the parseIppvRept utility to a text file for later examination.
- *-N-* number of records to process. The *-N* option is optional and pertains to the number of records in the IPPV purchase report that you want the utility to process. When the *-N* option is not used, the utility processes all of the records in the report.
- *-c-* comma-delimited output. Use the *-c* option if you want the parseIppvRept utility to separate each field in the output by a comma. Each record is then separated by a new line. When the *-c* option is not used, each record in the output appears as a separate block of data.
- *-s-* suppress end of report statistics. Use the *-s* option only if you want the parseIppvRept utility to suppress the printing of end-of-run statistics. Unless the *-s* option is used, the report will summarize the number of records processed, the number of actual IPPV purchases, and the number of cancellations.
- *-h-* help window. Use the *-h* option to display the parseIppvRept utility help window.

Run the parseIppvRept Utility

Introduction

The following information provides instructions to run the parseIppvRept utility.

Running the parseIppvRept Utility

Follow these instructions to run the parseIppvRept utility.

Note: This procedure uses two examples: one showing comma-delimited output, and the other showing output in block-type format. Both examples direct output to a file for later examination.

1. If necessary, open an xterm window on the DNCS.
2. Type **ls -tla /dvs/ftp/purchaseReportArchive** and then press **Enter**. The system lists the contents of the /dvs/ftp/purchaseReportArchive directory, newest files first.
3. Decide which IPPV purchase report you want to convert to text format.

   Note: The most recent files are listed first.
4. Choose one of the following options:
   - To convert an IPPV purchase report with comma delimited output, go to step 5.
   - To convert an IPPV purchase report with block-type output, go to step 7.

5 Type **parseIppvRept -I [input file name] -O [output file name] -c** and then press **Enter**.

Notes:

- Substitute the name of the binary IPPV purchase report in the /dvs/ftp/purchaseReportArchive directory for [input file name].

  Important! Be sure to include the complete path to the purchaseReportArchive directory.

- Substitute the path and name of the output file you want to create for [output file name].

  Important! If you store this file in the /tmp directory of the DNCS, the contents of the /tmp directory are lost whenever the DNCS reboots. To keep this file for an extended period of time, consider storing the file in the /dvs/dncs/tmp directory.

Example: Type (all on one line)

parseIppvRept -I /dvs/ftp/purchaseReportArchive/ippv200303262350.xdr -O /dvs/dncs/tmp/ippv20030326.out -c and then press **Enter**.

Result: The utility converts the binary IPPV purchase report to text format, using comma delimited output, and stores it in the specified directory.

6 For instructions on viewing the output, go to **View the Output File**, next in this chapter.

7 Type **parseIppvRept -I [input file name] -O [output file name]** and then press **Enter**.

Notes:

- Substitute the name of the binary IPPV purchase report in the /dvs/ftp/purchaseReportArchive directory for [input file name].

  Important! Be sure to include the complete path to the purchaseReportArchive directory.

- Substitute the path and name of the output file you want to create for [output file name].

  Important! Cisco recommends that you use the /dvs/dncs/tmp directory to store files of this type.

Example: Type (all on one line)

parseIppvRept -I /dvs/ftp/purchaseReportArchive/ippv200303262350.xdr -O /dvs/dncs/tmp/ippv20030326.out and then press **Enter**.

Result: The utility converts the binary IPPV purchase report to text format, using block-type output, and stores it in the specified directory.

8 For instructions on viewing the output, go to ***View the Output File*** (on page 180).

View the Output File

Introduction

This section provides instructions for viewing IPPV purchase report, after the parseIppvRept utility has converted it to text format.

Viewing the Output File

Follow these instructions to view the output file generated by the parseIppvRept utility.

1 In an xterm window on the DNCS, type **more /dvs/dncs/tmp/[output file name]** and then press **Enter**. The output file opens for viewing.

Note: Substitute the name of the output file for [output file name].

Example: Using the examples developed in steps 5 and 7 in the previous section, type **more /dvs/dncs/tmp/ippv20030326.out** and then press **Enter**.

2 Refer to one of the following headings for an example of the IPPV purchase report in text format:

- For comma delimited output, see ***Example of Comma Delimited Output*** (on page 181).
- For block-type output, see ***Example of Block-Type Output*** (on page 182).

Example of Comma Delimited Output

The following example shows the output from the parseIppvRept utility in comma delimited form.

Record Type, Mac Address, Package Name, Purchase Time, Event Length, Cost, Right to copy, Billing ID

Purchase,00:02:DE:47:F5:EC,Package ADM,Monday April 08 2002 14:45:00,135,1,recordable,0
Purchase,00:02:DE:47:DD:78,Package New,Monday April 08 2002 15:57:00,63,1,recordable,0
Purchase,00:02:DE:47:F5:EC,IPPV593 041602 1615,Tuesday April 16 2002 16:16:00,59,1,recordable,0
Purchase,00:02:DE:47:DD:78,test01,Tuesday April 23 2002 10:45:00,30,1,recordable,0
Cancellation,00:02:DE:47:DD:78,test_buy,Wednesday September 12 2001 08:32:00,533,1,recordable,0
Cancellation,00:02:DE:47:DD:78,test_buy,Wednesday September 12 2001 08:32:00,533,1,recordable,0
Cancellation,00:02:DE:47:DD:78,test_buy,Wednesday September 12 2001 08:32:00,533,1,recordable,0
Cancellation,00:02:DE:47:DD:78,test_buy,Wednesday September 12 2001 08:32:00,533,1,recordable,0
Cancellation,00:02:DE:47:DD:78,test_buy,Wednesday September 12 2001 08:32:00,533,1,recordable,0
Cancellation,00:02:DE:47:DD:78,test_buy,Wednesday September 12 2001 08:32:00,533,1,recordable,0
Finale stats.
Total Records 10
Purchase Records 4
Cancellation Records 6

Example of Block-Type Output

The following example shows partial output from the parseIppvRept utility in block-type format.

Purchase Record
00:02:DE:47:DD:78
Package name test01
Tuesday April 23, 2002 10:45:00
Length 30 minutes
Cost 1 unit.
Event was recordable.
Billing Id 0
----------EOR----------

Cancellation Record
00:02:DE:47:DD:78
Package name test_buy
Wednesday September 12, 2001 08:32:00
Length 533 minutes
Cost 1 unit.
Event was recordable.
Billing Id 0
----------EOR----------

Finale stats.
Total Records 10
Purchase Records 4
Cancellation Records 6

17

Associate Session IDs with Entitlement IDs with the eutdump Utility

Introduction

System operators or Cisco engineers may occasionally want to associate session IDs with entitlement IDs in order to determine what packages are active for a given session. The eutdump utility is designed to read the eut file in the /dvs/dvsFiles/BFS/camPsm directory of the DNCS and to display the contents of the file on the screen.

In This Chapter

- Run the eutdump Utility..... 184

Run the eutdump Utility

Introduction

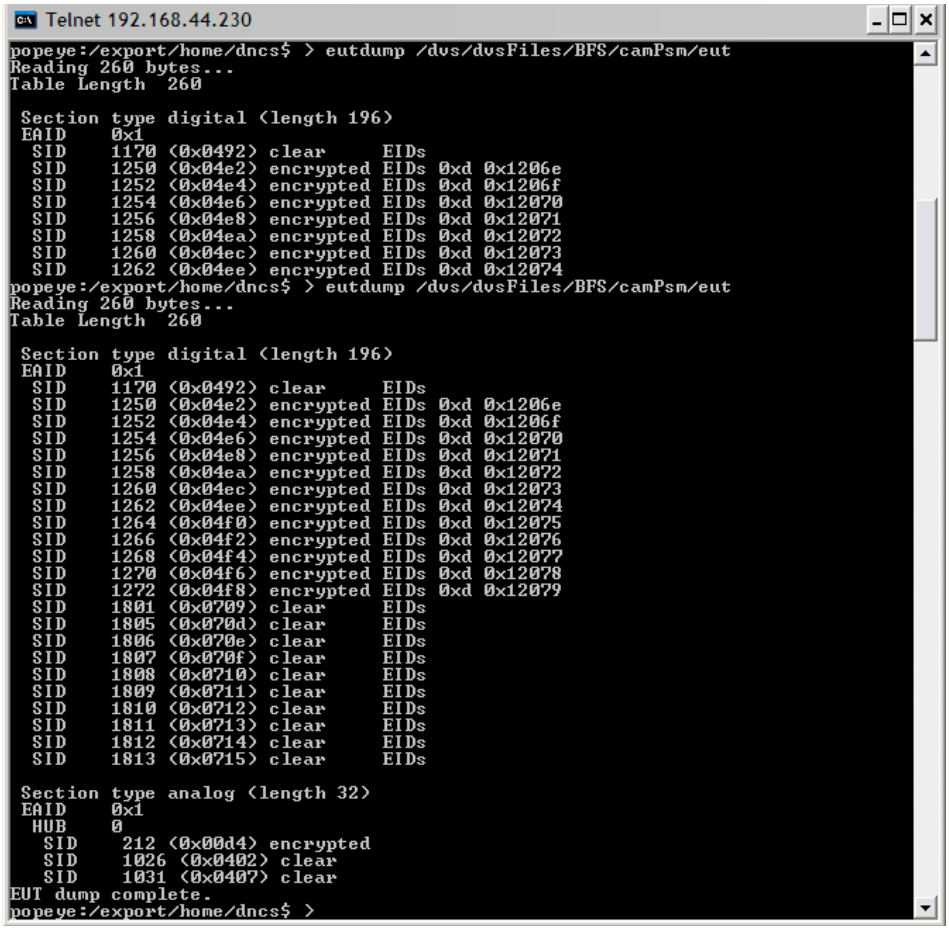
The procedure in this section provides instructions on running the eutdump utility, as well as providing an example of typical output.

Running the eutdump Utility

Follow these instructions to run the eutdump utility.

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

2 Type **eutdump /dvs/dvsFiles/BFS/camPsm/eut** and then press **Enter**. The system displays the contents of the eut file to the screen of the DNCS.



18

Obtain DHCT Authorization Data with the tellDhctInfo Utility

Introduction

System operators and Cisco engineers can use the tellDhctInfo utility to obtain authorization data about a single DHCT or a list of DHCTs. To obtain information about a single DHCT, supply the tellDhctInfo utility with the MAC address or the serial number of the DHCT. To obtain information about a list of DHCTs, supply the tellDhctInfo utility with the name of a file that contains a list of MAC addresses or serial numbers.

In This Chapter

- Options Available with the tellDhctInfo Utility 186
- Display the tellDhctInfo Help Window and Version Number 188
- Obtain DHCT Authorization Data for a List of DHCTs..... 190
- Obtain DHCT Authorization Data for an Individual DHCT 194
- Obtain DNCS Subscription Packages and Segments..... 196

Options Available with the tellDhctInfo Utility

Introduction

This section describes the options that are available for use with the tellDhctInfo utility. Subsequent sections in this chapter provide instructions and examples for using the options.

Supported Options for the tellDhctInfo Utility

Refer to the following table for an explanation of the options available with the tellDhctInfo utility.

Option	Purpose
-?	The *-?* option displays the help window associated with the tellDhctInfo utility. **Example: tellDhctInfo -?**
-v	The *-v* option displays the version number of the tellDhctInfo that is installed on your system. **Example: tellDhctInfo -v**
MAC address or serial number	When used in conjunction with the MAC address or serial number of a single DHCT, the tellDhctInfo utility provides the authorization data for that DHCT. When used in conjunction with a text file containing a list of DHCT MAC addresses or serial numbers, the utility provides authorization data for each DHCT represented in the text file. **Examples:** ■ **tellDhctInfo [DHCT MAC address]** ■ **tellDhctInfo [DHCT serial number]** ■ **tellDhctInfo [file name]**
-b	The *-b* option formats DHCT authorization data into two lines of output. Each line is preceded by the MAC address of the DHCT. This format is referred to as "brief" format. **Note:** While suitable for use with the MAC address or serial number of a single DHCT, this option is most useful when used with a text file containing a list of DHCT MAC addresses or serial numbers. **Example: tellDhctInfo -b [file name]**

Option	Purpose
-d	The *-d* option lists the subscription packages on the DNCS or assigned to a DHCT. **Examples:** ■ **tellDhctInfo -d** ■ **tellDhctInfo -d [DHCT MAC address]**
-d2	The *-d2* options lists the packages on the DNCS, as well as the segments within each package. **Example: tellDhctInfo -d2**
-x	The *-x* option provides DHCT authorization data and formats it in such a way that it is suitable for importation into a Microsoft Excel spreadsheet. **Note:** While suitable for use with the MAC address or serial number of a single DHCT, this option is most useful when used with a text file containing a list of DHCT MAC addresses or serial numbers. **Example: tellDhctInfo -x [file name]**

Display the tellDhctInfo Help Window and Version Number

Introduction

The information in this section describes how to display the tellDhctInfo help window and version number.

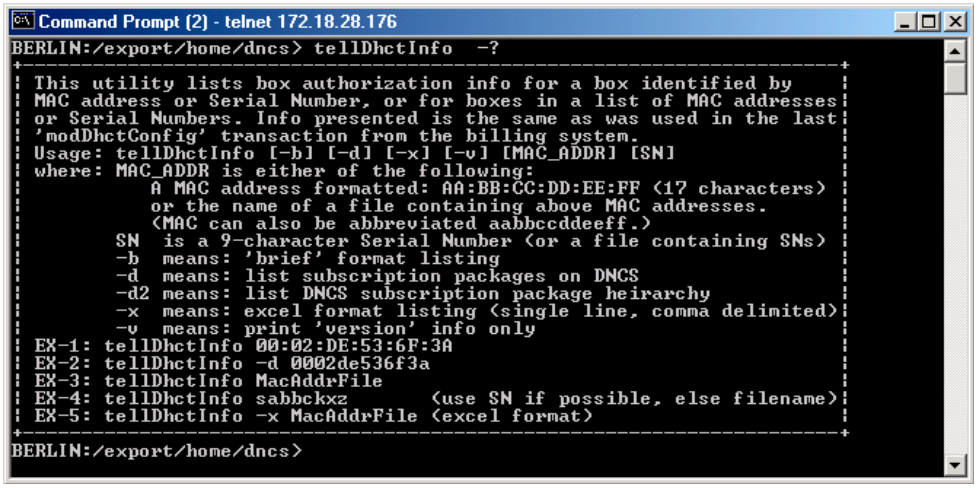
Tip: Many utilities include a help window. The help window is frequently a good place to start if you are unfamiliar with a utility.

Displaying the tellDhctInfo Help Window

Follow these instructions to display the tellDhctInfo help window.

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

2 Type **tellDhctInfo -?** and then press **Enter**. The system displays the tellDhctInfo help window.

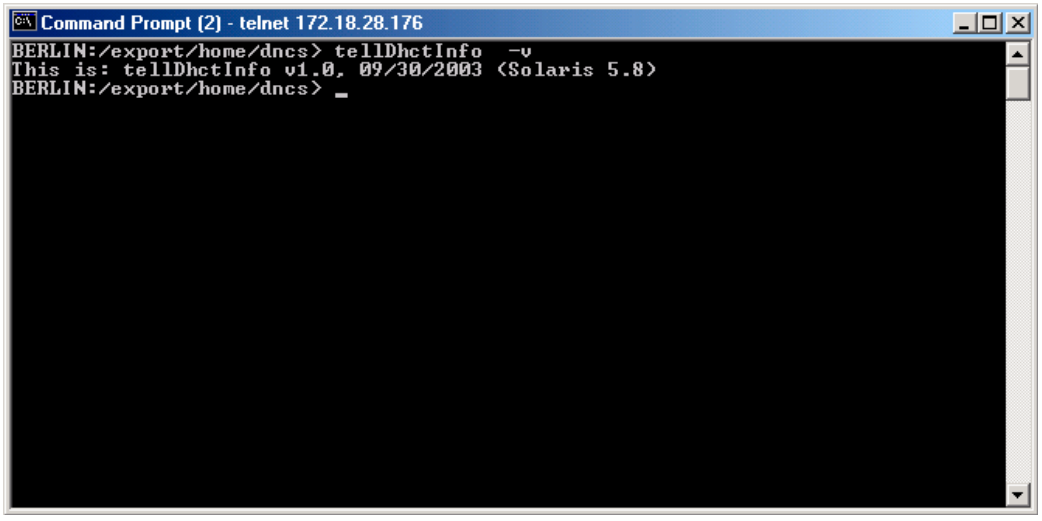


Displaying the tellDhctInfo Version Number

Follow these instructions to display the version number of the tellDhctInfo utility that is installed on your system.

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

2 Type **tellDhctInfo -v** and then press **Enter**. The system displays the tellDhctInfo version number.



Obtain DHCT Authorization Data for a List of DHCTs

Introduction

The information in this section describes how to use the tellDhctInfo utility with a text file that contains a list of DHCT MAC addresses or serial numbers. Be sure that you have already created the text file by following the guidelines and instructions in Appendix F, ***Guidelines for Text Files Used in DNCS Utilities*** (on page 243).

Tip: When using a text file that contains a list of DHCT MAC addresses or serial numbers, direct the output to another file. Output data tends to scroll so quickly off the screen that it might be unusable. When output is stored in a file, you can reference it at your convenience, as well as search for specific items of data. The instructions in this section make use of an output file.

Obtaining DHCT Authorization Data for a List of DHCTs

Refer to the following instructions when using a text file to obtain DHCT authorization data.

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

2 Choose one of the following options:

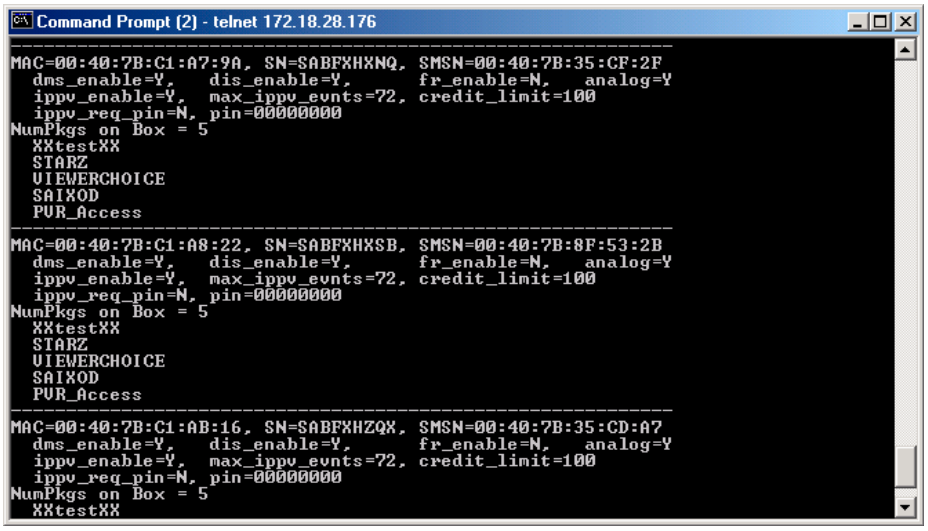
- To obtain DHCT authorization data in standard output format, go to step 3.
- To obtain DHCT authorization data in "brief" output format, go to step 5.

  Note: Data in "brief" output format is spread across two lines, with each line preceded by the DHCT MAC address. This format is especially useful when the output file is searched for a specific MAC address using the UNIX *grep* utility.
- To obtain DHCT authorization data in a format suitable for importation into a Microsoft Excel spreadsheet, go to step 7.

3 To obtain DHCT authorization data in standard output format, type **tellDhctInfo [input file name] > [output file name]** and then press **Enter**. The utility provides authorization data for each DHCT represented in the input file and directs the output to the specified output file.

Note: Substitute the name of the prepared input file for [input file name] and the name of the file where you want to store the output for [output file name].

Example:
tellDhctInfo /tmp/tellDhct-in_11.13.03 > /tmp/tellDhct-out_11.13.03

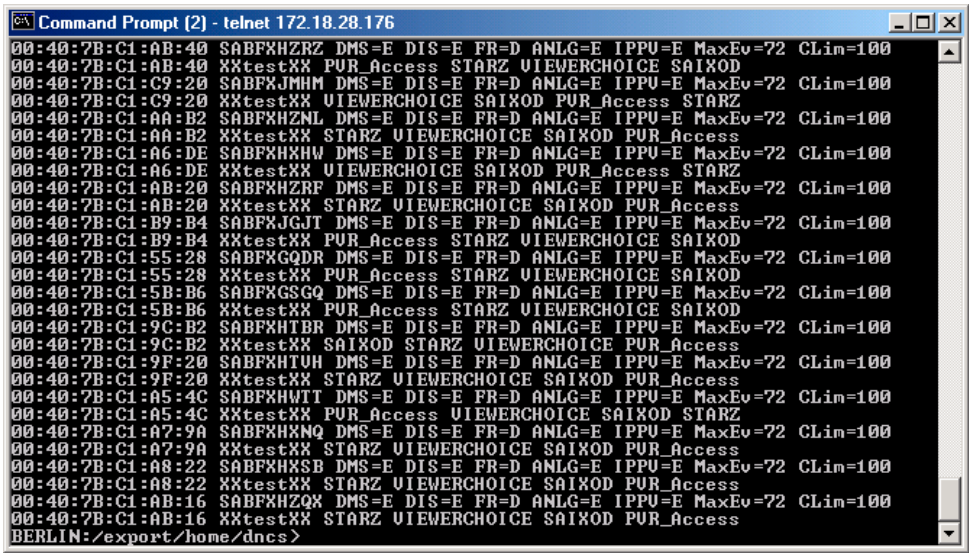


4 Go to step 8.

5 To obtain DHCT authorization data in "brief" output format, type **tellDhctInfo -b [input file name] > [output file name]** and then press **Enter**. The utility provides authorization data for each DHCT represented in the input file and directs the output to the specified output file in "brief" format.

Note: Substitute the name of the prepared input file for [input file name] and the name of the file where you want to store the output for [output file name].

Example:
tellDhctInfo -b /tmp/tellDhct-in_11.13.03 > /tmp/tellDhct-out_11.13.03

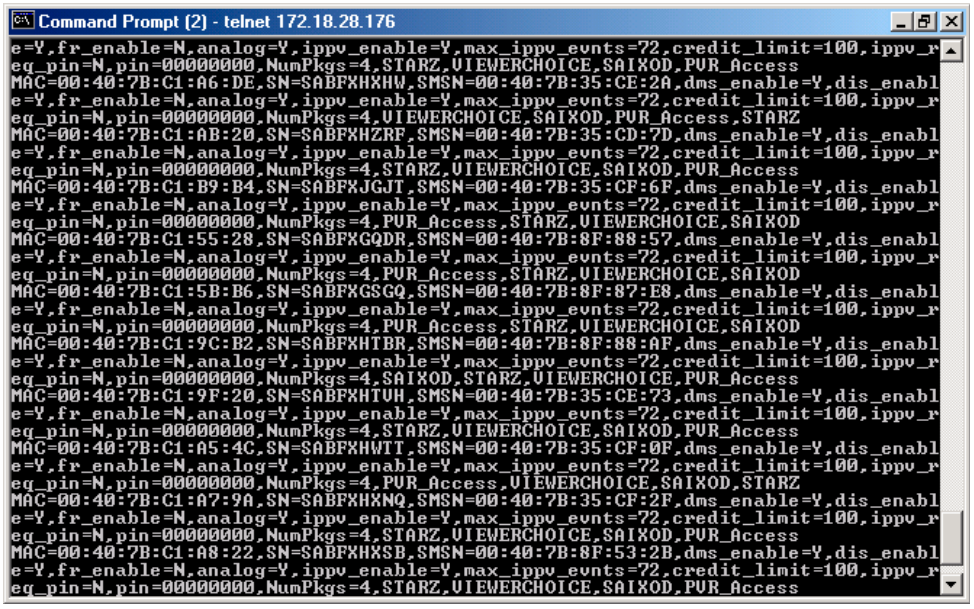


6 Go to step 8.

7 To obtain DHCT authorization data in a format suitable for importation into a Microsoft Excel spreadsheet, type **tellDhctInfo -x [input file name] > [output file name]** and then press **Enter**.

Note: Substitute the name of the prepared input file for [input file name] and the name of the file where you want to store the output for [output file name].

Example:
tellDhctInfo -x /tmp/tellDhct-in_11.13.03 > /tmp/tellDhct-out_11.13.03



8 Use the UNIX *more* utility to review the data in the output file.

Note: You can also import the output file created in step 7 into a Microsoft spreadsheet.

Obtain DHCT Authorization Data for an Individual DHCT

Introduction

The information in this section describes how to use the tellDhctInfo utility to obtain authorization data for an individual DHCT.

Obtaining DHCT Authorization Data for an Individual DHCT

Follow these instructions to obtain authorization data for an individual DHCT.

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

2 Choose one of the following options:

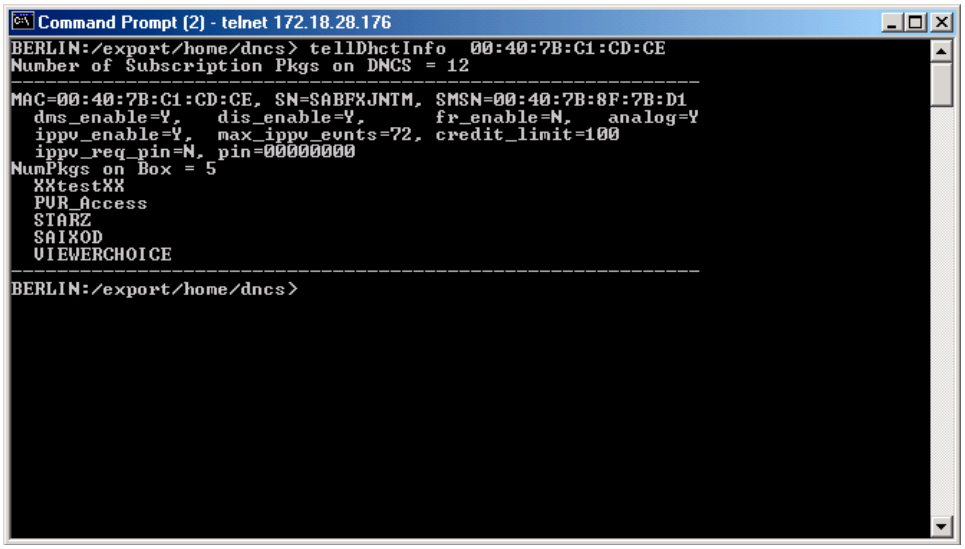
- To obtain authorization data for a DHCT, go to step 3.
- To obtain subscription package authorization data for a DHCT, go to step 5.

3 To obtain authorization data for a DHCT, type **tellDhctInfo [DHCT MAC address or serial number]** and then press **Enter**. The system displays authorization data for the specified DHCT.

Note: Substitute the MAC address or serial number of the DHCT for [DHCT MAC address or serial number].

Examples:

- **tellDhctInfo 00:40:7B:C1:CD:CE**
- **tellDhctInfo SABFXHXNQ**



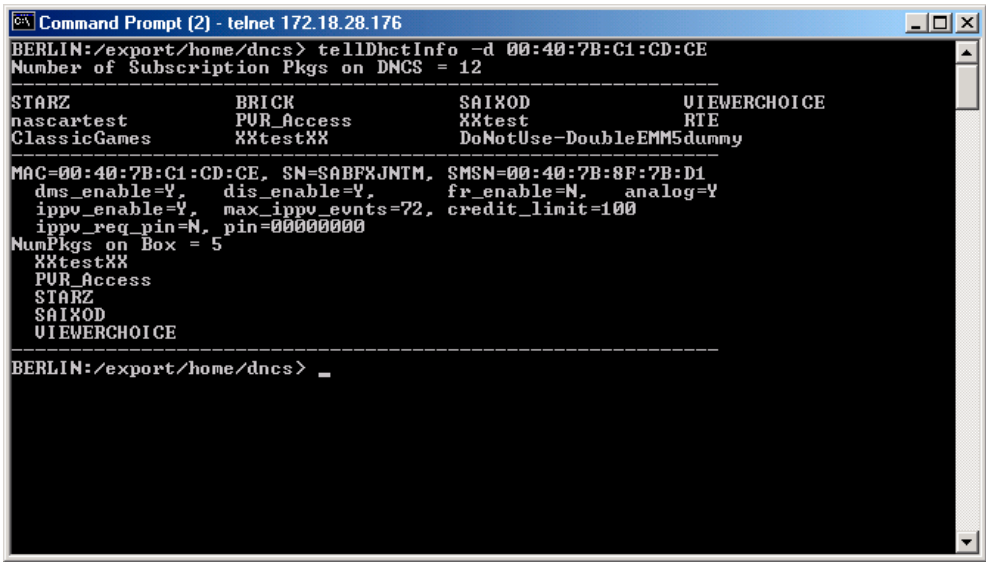
4 Go to step 6.

5 To obtain subscription package authorization data for a DHCT, as well as listing all subscription packages available on the DNCS, type **tellDhctInfo -d [DHCT MAC address or serial number]** and then press **Enter**. The system displays all subscription packages available on the DNCS, as well as subscription package authorization data for the selected DHCT.

Note: Substitute the MAC address or serial number of the DHCT for [DHCT MAC address or serial number].

Examples:

- **tellDhctInfo -d 00:40:7B:C1:CD:CE**
- **tellDhctInfo -d SABFXHXNQ**



6 Repeat the appropriate procedure in this section for any other DHCT for which you want to obtain DHCT authorization data.

Obtain DNCS Subscription Packages and Segments

Introduction

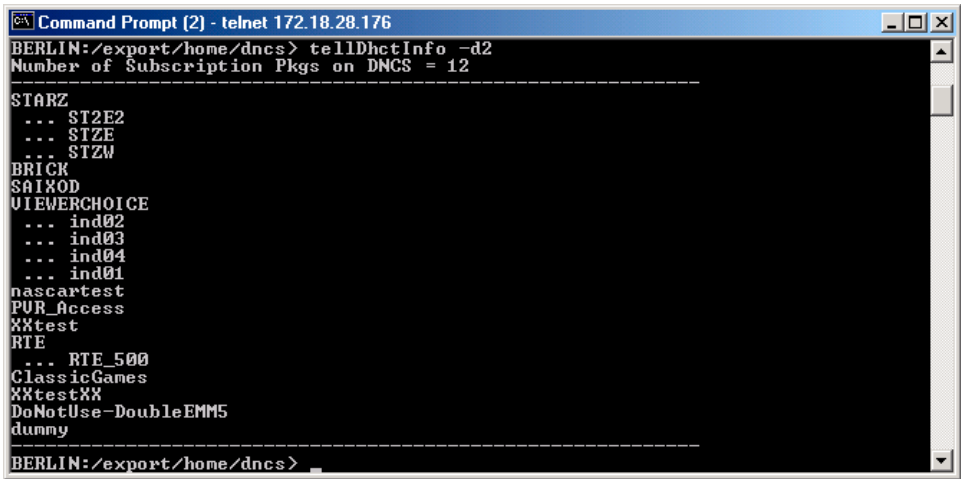
The information in this section describes how to use the tellDhctInfo utility to obtain a list of DNCS subscription packages, as well as the segments contained within each package.

Obtaining DNCS Subscription Packages and Segments

Follow these instructions to obtain a list of DNCS subscription packages, as well as the segments contained within each package.

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

2 Type **tellDhctInfo -d2** and then press **Enter**. The system displays a list of subscription packages and segments.



19

Convert POD IDs and MAC Addresses with the podConvert Utility

Introduction

The Cisco CableCARD module uses two unique identifiers: the CableCARD ID and the CableCARD MAC Address. The CableCARD ID is an 8-byte binary number that is derived from the MAC Address of the CableCARD module. The CableCARD ID appears on the screen when the subscriber inserts the card into the TV. The CableCARD MAC Address is used to provide conditional access and copy protection authorization.

Note: The terms CableCARD ID and POD ID are used interchangeably.

System operators, headend personnel, and lab technicians may occasionally have a need to convert the CableCARD POD ID to the CableCARD MAC Address and vice-versa. The podConvert utility accomplishes these tasks.

In This Chapter

- Before You Begin..... 198
- Convert MAC Addresses to POD IDs..... 199
- Convert POD IDs to MAC Addresses 200

Before You Begin

Before Using the podConvert Utility

System operators or engineers who use the podConvert utility to convert CableCARD MAC Addresses to POD IDs will typically use the toc file as the source of MAC Addresses. The toc file is automatically generated whenever system operators extract an EMM delivery file. When extracted, the toc file is automatically placed in a directory named according to the date of the EMM delivery file.

Important! System operators or engineers who use the podConvert utility to convert CableCARD MAC Addresses to POD IDs must know the following information:

- The directory on the DNCS into which they load the EMM delivery file
- The name of the directory into which the toc file is automatically extracted

  Note: This directory is a subdirectory of where the EMM delivery file is loaded. Engineers at Cisco Services can help you find these directories if you are unsure.

Additionally, during conversion of CableCARD MAC Addresses to POD IDs, the podConvert utility writes the list of POD IDs to a file specified by the user of the utility. System operators must know where they want to store this file, as well as what they want to call it.

Convert MAC Addresses to POD IDs

Introduction

Before using the podConvert utility to convert a list of CableCARD MAC Addresses to CableCARD POD IDs, be sure that you know the following information:

- The directory on the DNCS into which the EMM delivery file is loaded
- The directory on the DNCS into which the toc file is extracted
- The output file name (and full path) into which you want the list of POD IDs written

Converting MAC Address to POD ID

Follow these instructions to use the podConvert utility to convert CableCARD MAC Addresses to CableCARD POD IDs.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/[EMM delivery file directory]/[extracted file directory]** and then press **Enter**. The directory in which the EMM toc file is stored becomes the working directory.

   Example: cd /export/home/dncs/ftp/SP00209081-COMPLETE
3. Type **podConvert -T toc -P [file name]** and then press **Enter**. The system converts the CableCARD MAC Addresses into POD IDs and writes them to the specified file.

   Example: podConvert -T toc -P /tmp/POD_ID_[date].out

Convert POD IDs to MAC Addresses

Introduction

When converting CableCARD POD IDs to CableCARD MAC Addresses, the podConvert utility starts with a file of POD IDs, converts them to MAC Addresses, and then writes the output to a file of the operator's choosing. The user of the podConvert utility needs to know where the source file of POD IDs is located, as well as the name and location of the file to which the MAC Addresses should be written.

Converting POD IDs to MAC Addresses

Follow these instructions to convert a POD ID to a MAC address.

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

2 Type **cd [location of the POD ID source file]** and then press **Enter**. The directory in which the file containing a list of POD IDs is stored becomes the working directory.

Example: cd /tmp

3 Type **podConvert -T [MAC Address output file] -P [POD ID source file] -R** and then press **Enter**. The system converts the POD IDs into MAC Addresses and writes them to the specified file.

Example: podConvert -T MAC_Addr_[date].out -P POD_ID_[date] -R

20

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

Stopping System Components

Introduction

Use the procedures in this appendix to stop the Spectrum Network Management System (Spectrum), the Application Server, and the DNCS.

In This Appendix

- Stop System Components 204

Stop System Components

Introduction

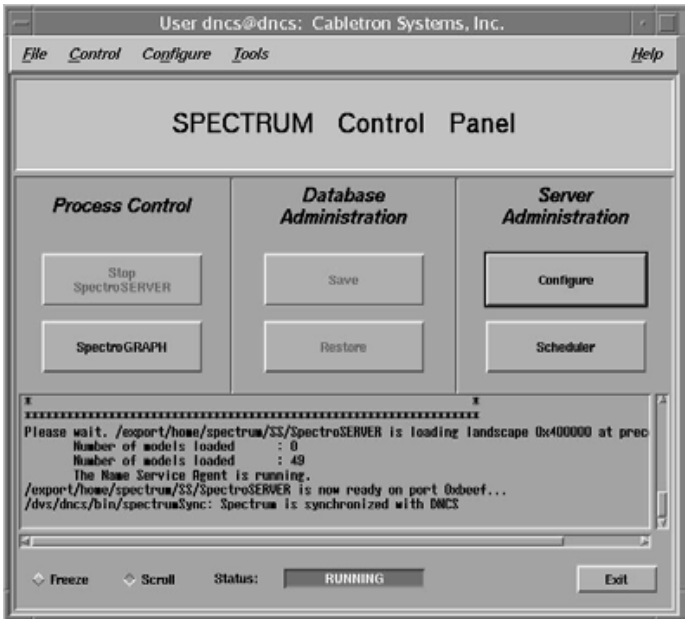
Before following several of the DNCS Utilities procedures, you must first stop Spectrum, the Application Server, and the DNCS. Follow these instructions to stop Spectrum, the Application Server, and the DNCS.

Stopping Spectrum

Complete these steps to stop Spectrum.

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

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



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

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

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

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

Stopping the Application Server

Two procedures follow: ***Stopping the Application Server at SARA Sites*** (on page 205) pertains to sites that currently support the Cisco Resident Application (SARA), and ***Stopping the Application Server at Pioneer Sites*** (on page 205) pertains to sites that support the Pioneer resident application.

Choose the procedure(s) that pertains to your system.

Stopping the Application Server at SARA Sites

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

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

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

Stopping the Application Server at Pioneer Sites

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

1. Press the middle mouse button on the Application Server and select **Passport Stop**.
2. From an xterm window on the Application Server, type **CheckServices** and then press **Enter**. A list of drivers appears.

   Note: Each driver is associated with an Application Server process.
3. Wait until the word **No** appears next to each driver.

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

Stopping the DNCS

Complete these steps to stop the DNCS.

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

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

B

Restarting System Components

Introduction

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

In This Appendix

- Restart System Components 208

Restart System Components

Introduction

Follow these procedures to restart Spectrum, the DNCS, and the Application Server.

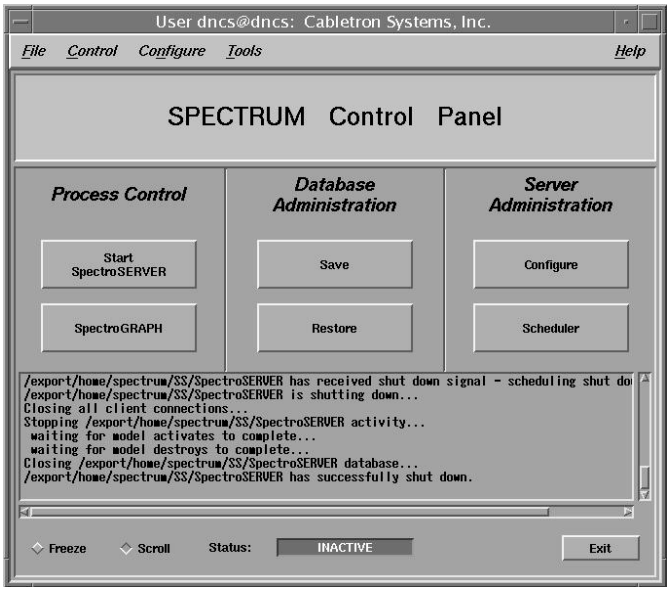
Restarting Spectrum

Follow these instructions to restart Spectrum.

Note: Skip this procedure if you are using 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 Host Machine (usually DEFAULT), and then click **OK**. The Spectrum Control Panel window opens.



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

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

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

Restarting the DNCS

Follow these instructions to restart the DNCS.

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

   Results:

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

   Notes:

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

Restarting the Application Server

Choose one of the following options:

- For sites on which the Cisco Resident Application runs on the Application Server, go to ***Restarting the Application Server for SARA Systems*** (on page 210).
- For sites on which the Pioneer resident application runs on the Application Server, go to ***Restarting the Application Server for Pioneer Systems*** (on page 210).

Restarting the Application Server for SARA Systems

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

1. Open an xterm window on the Application Server.
2. Type **appControl** and then press **Enter**. The Applications Control window opens.
3. Select option **2** on the Applications Control window. The system displays a list of Application Server processes and their current status.
4. Does the word **running** appear next to the current state field (**Curr Stt**) of each process?
   - If **yes**, skip the rest of this procedure.
   - If **no**, go to step 5.
5. Press the middle mouse button, and then select **App Serv Start**.
6. When the Application Control window indicates that the current state (**Curr Stt**) of each process is running, go to step 7.

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

Restarting the Application Server for Pioneer Systems

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

1. Open an xterm window on the Application Server.
2. Type **CheckServices** and then press **Enter**. A list of drivers appears.

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

3 Does the word **Yes** appear next to each driver?

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

- If **yes**, skip the rest of this procedure.
- If **no**, go to step 4.

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

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

6 Follow the on-screen instructions to close the window containing the list of Pioneer drivers.

C

DBDS Utilities Version 5.1 Removal Procedure

Introduction

If your system appears unstable after installing the DBDS Utilities Version 5.1, use the instructions in this appendix to remove the DBDS Utilities from your system. Be sure that you contact Cisco Services before removing DBDS Utilities. Cisco Services engineers may be able to troubleshoot any condition that may have caused you to consider removing DBDS Utilities.

Important! Do not remove DBDS Utilities Version 5.1 from your system without calling Cisco Services first.

In This Appendix

- Remove DBDS Utilities Version 5.1 214

Remove DBDS Utilities Version 5.1

Removing DBDS Utilities Version 5.1

Follow these instructions to remove DBDS Utilities Version 5.1 from your system.

Important! Do not remove DBDS Utilities from your system without first calling Cisco Services. Cisco Services engineers may be able to troubleshoot any conditions that may have caused you to consider removing DBDS Utilities.

1 Open an xterm window on the DNCS.

2 Type **su** and then press **Enter** to log in to the xterm window as root user.

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

4 Insert the CD labeled **DBDS Utilities 5.1** into the CD-ROM drive of the DNCS.

5 Type **df** and then press **Enter** to confirm that the system mounted the CD successfully. The last line of the df command output lists the number of free disk blocks on the CD.

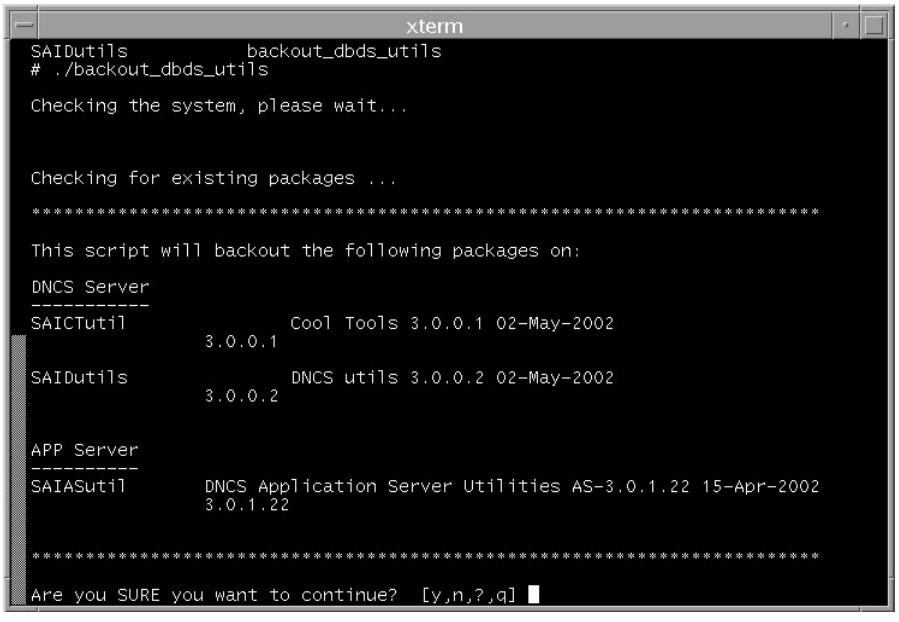
Note: The number of free disk blocks existing on the CD does not matter. The fact that the CD is listed in the df command output verifies that the system successfully mounted the CD.

6 Type **./backout_dbds_utils** and then press **Enter**.

Note: Be sure to type ./ before typing backout_dbds_utils.

Results:

- The system displays a list of the utility components it will remove.
- A confirmation message appears.



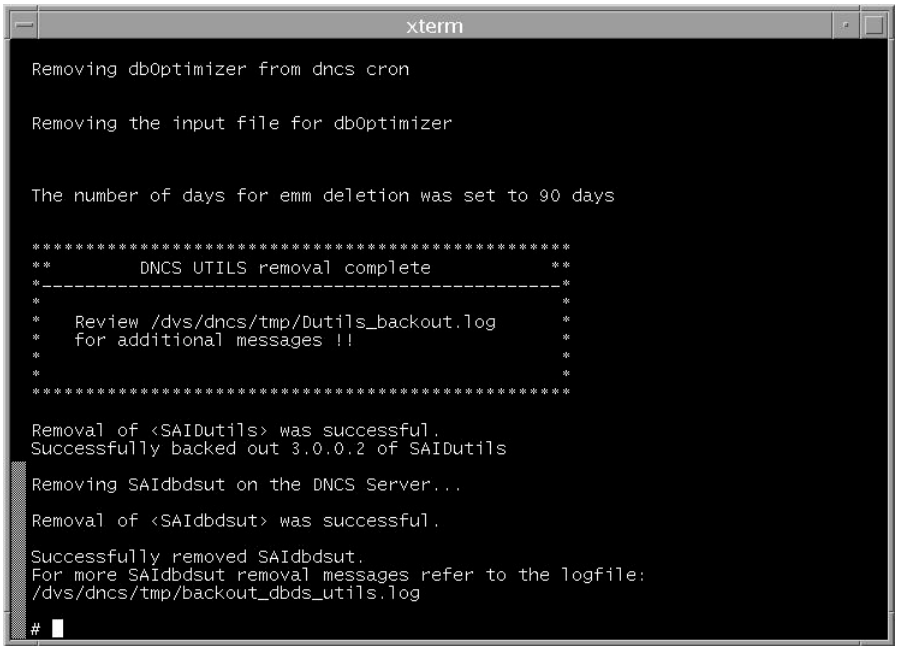
7 Type **y** and then press **Enter**.

Results:

- The system removes the DBDS Utilities from your system.
- The system displays a message stating that it removed the entry for the dbOptimizer program from the crontab file on the DNCS.

  Note: The dbOptimizer program deletes unneeded EMMs from your system.
- The system displays information pertaining to how the dbOptimizer program was configured to remove unneeded EMMs.

  Example: In this example, the dbOptimizer program was configured to remove EMMs older than 90 days.



8 Re-install your old version of DNCS Utilities.

D

Update the DHCT OUI with the updateOUI Utility

Introduction

Prior to the introduction of PowerTV® OS 3.1, Cisco DHCTs signed on to the DBDS network using the Organizationally Unique Identifier (OUI) of *00:01:A6*, *00:40:7B*, or *00:02:DE*. Starting with PowerTV OS 3.1, however, all Cisco DHCTs will sign on to the network using the OUI of *00:02:DE*, regardless of the DHCT MAC address.

Cisco developed the updateOUI utility to modify the DNCS database so that DHCTs with OUIs of *00:01:A6* and *00:40:7B*, are changed to *00:02:DE*. The updateOUI utility updates the hct_profile table in the DNCS database, changing the Cisco DHCT identifier to *00:02:DE*.

Notes:

- Cisco makes use of two additional OUIs, as well: *00:0A:73* and *00:0F:21*. The DHCT installation process, however, causes DHCTs with these OUIs to install with the *00:02:DE* OUI.
- If your system supports set-top converters from other manufacturers, those records remain unchanged when you run the updateOUI utility.
- The system stores the decimal values of the OUIs in the database. The decimal values are:
- 734 for 00:02:DE
  422 for 00:01:A6
  2675 for 00:0A:73
  16507 for 00:40:7B

In This Appendix

- Before Using the updateOUI Utility 219
- Modes for the updateOUI Utility 220
- Run the updateOUI Utility in Information Mode 222
- Update the OUI 223
- Reset the OUI 228
- Miscellaneous updateOUI Options 235

Before Using the updateOUI Utility

Introduction

Read through these important items before you use the updateOUI utility

Resetting the OUI

The updateOUI utility includes the *-r* option that system operators can use if they ever have to roll back from an upgrade to PowerTV OS 3.x. When used with the *-r* option, the updateOUI utility changes the *00:02:DE* identifier back to *00:01:A6* or *00:40:7B*, whichever is appropriate. DHCTs with the *00:0A:73* or *00:0F:21* identifiers are not affected, however, because the installation process of these DHCTs cause the DHCTs to install with the *00:02:DE* identifier.

When to Run the updateOUI Utility

System operators must run the updateOUI utility under the following circumstances:

- System operators must run the updateOUI utility whenever they upgrade to PowerTV OS 3.1 or later.

  Important! DHCTs with the 00:01:A6 or 00:40:7B identifiers will not be capable of two-way services if system operators do not run the updateOUI utility after upgrading to PowerTV OS 3.x.

- Once system operators have upgraded to PowerTV OS 3.1 or later, they must run the updateOUI utility again whenever they add new DHCTs to the system that use *00:01:A6* or *00:40:7B*, as their sign-on identifiers.

- System operators must run the updateOUI utility (with the *-r* option) if they ever need to roll back from an upgrade to PowerTV OS 3.1 or later.

Modes for the updateOUI Utility

Introduction

The following section lists the options available with the update OUI utility.

updateOUI Utility Modes

In default mode (no options) the updateOUI utility changes the OUI of all DHCTs in the database to *00:02:DE*. The following additional modes are available to system operators when running the updateOUI utility:

- *-i* -. Use the *-i* option to display a window showing the number of MAC addresses and OUIs associated with the DHCTs in the database.

  Note: You may sometimes hear the *-i* option referred to as information mode.

  Important! Always run the updateOUI utility in information mode before deciding what other modes to use.

- -[model number]. Use the [model number] option to update the OUI for DHCTs of a specific model number.

- -[model number] [revision number]. Use the [model number] [revision number] option to update the OUI for DHCTs of a specific model and revision number.

- -[MAC address]. Use the [MAC address] option to update the OUI of a DHCT with a specific MAC address.

- *-r* -. Use the *-r* option to reset the OUI for all DHCTs in the database.

  Note: The *-r* option ignores DHCTs with MAC addresses starting with *00:0A:73* and *00:0F:21* because these DHCTs always have an OUI of *00:02:DE* in the DNCS database.

- *-r* [model number]. Use the *-r* [model number] option to reset the OUI for DHCTs of a specific model number.

  Note: The *-r* option ignores DHCTs with MAC addresses starting with *00:0A:73* and *00:0F:21* because these DHCTs always have an OUI of 00:02:DE in the DNCS database.

- *-r* [model number] [revision number]. Use the *-r* [model number] [revision number] option to reset the OUI for DHCTs of a specific model and revision number.

  Note: The *-r* option ignores DHCTs with MAC addresses starting with *00:0A:73* and *00:0F:21* because these DHCTs always have an OUI of *00:02:DE* in the DNCS database.

- *-r* [MAC address]. Use the -r [MAC address] option to reset the OUI for a specific DHCT.

  Note: The *-r* option ignores DHCTs with MAC addresses starting with *00:0A:73* and *00:0F:21* because these DHCTs always have an OUI of *00:02:DE* in the DNCS database.

- *-?* -.Use the *-?* option to display a window listing the various modes in which you can run the updateOUI utility.

- *-v* -.Use the *-v* option to display the version number of the updateOUI utility supported by your system.

- *-z*-. Use the *-z* option in conjunction with the *-r* option (*-rz*) to reset a null OUI back to the first three octets of the DHCT MAC address.

  Note: You cannot use the *-z* option by itself; the *-z* option must be used in conjunction with the *-r* option.

Run the updateOUI Utility in Information Mode

Introduction

Run the updateOUI utility with the *-i* option (information mode) before deciding what other options, if any, to use later. When run in information mode, the updateOUI utility makes no changes to the database.

Running updateOUI in Information Mode

When run in information mode, the updateOUI utility displays a window showing the number of MAC addresses and OUIs associated with the DHCTs in the database. Follow these instructions to run the updateOUI utility in information mode.

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

2 Type **updateOUI -i** and then press **Enter**. The xterm window updates to show the number of MAC addresses and OUIs associated with the DHCTs in the database.

```
> updateOUI -i
------------------------------------------------------------------------------------------

Mar 23, 8:07:23 - updateOUI Started.
updateOUI Options: -i (Information only);
SAFE mode - No database modifications will be done!
Total DHCTs (hct_profile rows) in the database.....   1519
------------------------------------------------------------------------------------------
<---------MACaddr Counts---------> <-----------OUI Counts----------->
 02:DE  01:A6  40:7B  0A:73  other   02:DE  01:A6  40:7B  0A:73  other   Total
 ------  ------  ------  ------  ------  ------  ------  ------  ------  ------  ------
   64     116     551     787     1      1510       8       0       0       1     1519
------------------------------------------------------------------------------------------
'other':        Pace    Panason    Pioneer   SciAtl    Null     UnKnown
-value-:       50:94      80:45      E0:36    0F:21    --:--       ??:??
OUI count:         0          0          0        0        0           1
Mar 23, 8:07:23 - updateOUI Ended.
------------------------------------------------------------------------------------------
```

Update the OUI

Introduction

Refer to one of the following procedures in this section when updating the OUI:

- To update all Cisco DHCTs in the database, go to ***Updating All DHCTs*** (on page 224).
- To update a specific model number of DHCT, go to ***Updating DHCTs by Model Number*** (on page 225).
- To update a specific model and revision number of DHCT, go to ***Updating DHCTs by Model Number and Revision Number*** (on page 226).
- To update a specific DHCT, go to ***Updating DHCTs by MAC Address*** (on page 227).

You may sometimes hear these procedures referred to as running the updateOUI utility in the *forward direction*.

Updating All DHCTs

When the updateOUI utility is run without any options, the utility updates all DHCTs in the database that do not already have the new 00:02:DE identifier.

Important! When you run the updateOUI utility to update the OUI on all DHCTs in the database, the utility does not change the DHCT identifier of those DHCTs having a NULL value in the hctt_oui field in the hct_profile table in the database. System operators may occasionally desire to retain NULL values in the hctt_oui field in order to conduct some testing.

Follow these instructions to use the updateOUI utility to update all DHCTs with the 00:02:DE OUI.

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

2 Type **updateOUI** and then press **Enter**. The system updates all DHCTs with the *00:02:DE* identifier (except those that contain an OUI value of NULL) and displays a message similar to the following:

```
>> updateOUI
-------------------------------------------------------------------------------------------------
Mar 23, 14:10:52 - updateOUI Started.
updateOUI Options: None (Forward direction changes).
CAUTION *** OUI's will be updated! ***
  (Type Ctrl-C now to abort!)
Total DHCTs (hct_profile rows) in the database.....  1519
-------------------------------------------------------------------------------------------------
<---------MACaddr Counts--------->      <-----------OUI Counts----------->
 02:DE  01:A6  40:7B  0A:73  other    02:DE  01:A6  40:7B  0A:73  other   Total
 ------ ------ ------ ------ ------   ------ ------ ------ ------ ------ ------
    64    116    551    787      1     1518      0      0      0      1    1519
-------------------------------------------------------------------------------------------------
Mar 23, 14:10:57 - updateOUI Ended.
-------------------------------------------------------------------------------------------------
```

Updating DHCTs by Model Number

Follow these instructions to use the updateOUI utility to update DHCTs by model number.

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

2 Type **updateOUI [model number]** and then press **Enter**.

Example: updateOUI 2100

Result: The system updates all model number 2100 DHCTs with the 00:02:DE identifier and displays a message similar to the following:

```
AlertServer.210 >> updateOUI 2100
-----------------------------------------------------------------------------------------------

Mar 23, 8:08:48 - updateOUI Started.
updateOUI Options: None (Forward direction changes).

CAUTION *** OUI's will be updated! ***
   (Type Ctrl-C now to abort!)

Total DHCTs (hct_profile rows) in the database.....  1519
-----------------------------------------------------------------------------------------------
<---------MACaddr Counts--------->       <----------OUI Counts---------->
 02:DE  01:A6  40:7B  0A:73  other      02:DE  01:A6  40:7B  0A:73  other   Total
 ------  ------  ------  ------  ------      ------  ------  ------  ------  ------  ------
   10      31       0       0       0          41       0       0       0       0      41
-----------------------------------------------------------------------------------------------

Above counts are for Model 2100 only.
Mar 23, 8:08:53 - updateOUI Ended.
-----------------------------------------------------------------------------------------------
```

Updating DHCTs by Model Number and Revision Number

Follow these instructions to use the updateOUI utility to update DHCTs by model number and revision number.

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

2 Type **updateOUI [model number] [revision number]** and then press Enter.

Example: updateOUI 2100 20

Result: The system updates all model number 2100, revision 20 DHCTs with the 00:02:DE identifier and displays a message similar to the following:

```
AlertServer.210 >> updateOUI 2100 20

-------------------------------------------------------------------------------------------------
Mar 23, 8:12:30 - updateOUI Started.
updateOUI Options: None (Forward direction changes).
 CAUTION *** OUI's will be updated! ***
   (Type Ctrl-C now to abort!)
 Total DHCTs (hct_profile rows) in the database.....  1519
-------------------------------------------------------------------------------------------------
<---------MACaddr Counts--------->          <----------OUI Counts---------->
 02:DE  01:A6  40:7B  0A:73  other      02:DE  01:A6  40:7B  0A:73  other  Total
  ------  ------  ------  ------  ------      ------  ------  ------  ------  ------  ------
   10       0       0       0       0          10       0       0       0       0       10
-------------------------------------------------------------------------------------------------
Above counts are for Model 2100, Rev 20 only.
Mar 23, 8:12:36 - updateOUI Ended.

-------------------------------------------------------------------------------------------------
```

Updating DHCTs by MAC Address

Follow these instructions to use the updateOUI utility to update a DHCT by MAC address.

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

2 Type **updateOUI [MAC address]** and then press **Enter**.

Example: updateOUI 00:01:A6:5B:EE:BC

Result: The system updates the specified DHCT with the 00:02:DE identifier and displays a message similar to the following:

```
AlertServer.210>> updateOUI  00:01:A6:5B:EE:BC

----------------------------------------------------------------------------------------------------
Nov 30, 9:31:33 - updateOUI Started.
updateOUI Options: None  (Forward direction changes).
Update done for MAC=00:01:A6:5B:EE:BC only

----------------------------------------------------------------------------------------------------
```

Reset the OUI

Introduction

System operators should run the updateOUI utility with the *-r* option to reset the OUI of DHCTs in the database. The updateOUI utility, when used with the *-r* option, changes the *00:02:DE* identifier back to *00:01:A6* or *00:40:7B*, whichever is appropriate. System operators are required to run the updateOUI utility with the *-r* option whenever they roll back from an upgrade to PowerTV OS 3.x.

Important! It is very rare for system operators to have a need to use the *-r* option. Be sure you understand the implications of using the *-r* option before proceeding. Call Cisco Services if you have any questions.

Notes:

- The -z option, when used with the -r option, resets a null OUI back to the first three octets of the DHCT MAC address.
- You may sometimes hear these procedures referred to as running the updateOUI utility in the *reverse* direction.

Refer to one of the following procedures in this section when resetting the OUI:

- To reset the OUI for all DHCTs in the database, refer to ***Resetting the OUI for all DHCTs*** (on page 229).
- To reset the OUI for a specific model number of DHCT, refer to ***Resetting the OUI by DHCT Model Number*** (on page 230).
- To reset the OUI for a specific model and revision number of DHCT, refer to ***Resetting the OUI by DHCT Model Number and Revision Number*** (on page 231).
- To reset the OUI for a specific DHCT, refer to ***Resetting the OUI by DHCT MAC Address*** (on page 232).
- To reset the OUI for DHCTs with a null OUI, refer to ***Reset the Null OUI*** (on page 232).

Resetting the OUI for all DHCTs

Follow these instructions to reset the OUI for all DHCTs in the database.

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

2 Type **updateOUI -r** and then press **Enter**. The system restores the identifier on DHCTs in the DNCS database, and displays a message similar to the following:

```
AlertServer.210 >> updateOUI -r

------------------------------------------------------------------------------------------------
Mar 23, 8:15:38 - updateOUI Started.
updateOUI Options: -r (Reset OUI=MAC);
 CAUTION *** OUI's will be updated! ***
   (Type Ctrl-C now to abort!)
 Total DHCTs (hct_profile rows) in the database.....   1519
------------------------------------------------------------------------------------------------
<---------MACaddr Counts--------->      <----------OUI Counts---------->
 02:DE  01:A6  40:7B  0A:73  other      02:DE  01:A6  40:7B  0A:73  other   Total
 ------  ------  ------  ------  ------      ------  ------  ------  ------  ------  ------
   64     116     551     787      1         851     116     551       0       1      1519
------------------------------------------------------------------------------------------------
Mar 23, 8:15:45 - updateOUI Ended.

------------------------------------------------------------------------------------------------
```

Resetting the OUI by DHCT Model Number

Follow these instructions to reset the OUI on DHCTs of a specific model number.

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

2 Type updateOUI -r [model number] and then press Enter.

Example: updateOUI -r 3100

Result: The system restores the identifier on DHCTs of the specified model number, and displays a message similar to the following:

```
AlertServer.210 >> updateOUI -r 3100

------------------------------------------------------------------------------------------------
Mar 23, 8:14:47 - updateOUI Started.
updateOUI Options: -r (Reset OUI=MAC);
 CAUTION *** OUI's will be updated! ***
   (Type Ctrl-C now to abort!)
Total DHCTs (hct_profile rows) in the database.....  1519
------------------------------------------------------------------------------------------------
<---------MACaddr Counts--------->       <-----------OUI Counts----------->
 02:DE  01:A6  40:7B  0A:73  other      02:DE  01:A6  40:7B  0A:73  other   Total
 ------ ------ ------ ------ ------     ------ ------ ------ ------ ------  ------
   5      46     0      0      0          5      46     0      0      0       51
------------------------------------------------------------------------------------------------
Above counts are for Model 3100 only.
Mar 23, 8:14:53 - updateOUI Ended.

------------------------------------------------------------------------------------------------
```

Resetting the OUI by DHCT Model Number and Revision Number

Follow these instructions to reset the OUI on DHCTs of a specific model and revision number.

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

2 Type **updateOUI -r [model number] [revision number]** and then press **Enter**.

Example: updateOUI -r 2100 23

Result: The system restores the identifier on DHCTs of the specified model and revision number, and displays a message similar to the following:

```
AlertServer.210 >> updateOUI -r 2100 23

-------------------------------------------------------------------------------------------------
Mar 23, 8:14:06 - updateOUI Started.
updateOUI Options: -r (Reset OUI=MAC);
 CAUTION *** OUI's will be updated! ***
  (Type Ctrl-C now to abort!)
 Total DHCTs (hct_profile rows) in the database.....  1519
-------------------------------------------------------------------------------------------------
<---------MACaddr Counts--------->        <----------OUI Counts---------->
 02:DE  01:A6  40:7B  0A:73  other      02:DE  01:A6  40:7B  0A:73  other   Total
 ------  ------  ------  ------  ------      ------  ------  ------  ------  ------  ------
   0      31      0       0       0          0       31      0       0       0       31
-------------------------------------------------------------------------------------------------
Above counts are for Model 2100, Rev 23 only.
Mar 23, 8:14:11 - updateOUI Ended.

-------------------------------------------------------------------------------------------------
```

Resetting the OUI by DHCT MAC Address

Follow these instructions to reset the OUI for a specific DHCT.

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

2 Type **updateOUI -r [MAC address]** and then press **Enter**.

Example: updateOUI -r 00:01:A6:5B:EE:BC

Result: The system restores the identifier on the specified DHCT and displays a message similar to the following:

```
AlertServer.210>> updateOUI -r  00:01:A6:5B:EE:BC

------------------------------------------------------------------------------------------
Nov 28, 9:31:33 - updateOUI Started.
updateOUI Options:  -r  (Reset  OUI=MAC).
Update done for MAC=00:01:A6:5B:EE:BC only.

------------------------------------------------------------------------------------------
```

Reset the Null OUI

Introduction

Prior to SR 1.5.1, system operators had been able to set to null in the database the OUI, model number, and revision number of DHCTs that had trouble signing on to the network. Then, when these DHCTs did eventually sign on successfully to the network, the sign-on process automatically replaced these null values with valid values. Beginning with SR 1.5.1, however, DHCTs need a valid OUI to sign on to the network; DHCTs with a null OUI are unable to sign on. System operators can run the updateOUI utility with the *-rz* option to replace null OUIs in the database with the first three octets of the DHCT MAC address. These DHCTs will then be able to sign on to the network.

Important! If your system uses version 3.1 or later of the PowerTV operating system, you must run the updateOUI utility in the forward direction after resetting the null OUI in order for the DHCTs to sign on to the network.

When to Reset the Null OUI

Reset the null OUI whenever more than a very small number of DHCTs have the null OUI. To determine how many DHCTs have the null OUI, run the updateOUI utility in information mode (*-i* option). If the number of DHCTs with the null OUI is more than a few dozen, consider resetting the null OUI on those DHCTs. The following procedure, **Resetting the Null OUI**, provides an example of resetting the null OUI.

Resetting the Null OUI

Follow these instructions for an example of when to reset the null OUI, as well as for instructions on running the updateOUI utility with the *-rz* option, which resets the null OUI.

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

2 Type updateOUI -i and then press **Enter**. The xterm window updates to show the number of MAC addresses and OUIs associated with the DHCTs in the database.

```
> updateOUI -i

-------------------------------------------------------------------------------------------
Mar 23, 8:07:23 - updateOUI Started.
updateOUI Options: -i (Information only);
SAFE mode - No database modifications will be done!
Total DHCTs (hct_profile rows) in the database.....  1519
-------------------------------------------------------------------------------------------
<---------MACaddr Counts---------> <-----------OUI Counts----------->
 02:DE  01:A6  40:7B  0A:73  other  02:DE  01:A6  40:7B  0A:73  other  Total
 ------  ------  ------  ------  ------  ------  ------  ------  ------  ------  ------
    64     116     551     787     1     1510       8       0       0       1    1519
-------------------------------------------------------------------------------------------
'other':        Pace    Panason    Pioneer  SciAtl    Null    UnKnown
-value-:       50:94      80:45      E0:36   0F:21   --:--      ??:??
OUI count:         0          0          0       0       0           1
Mar 23, 8:07:23 - updateOUI Ended.
-------------------------------------------------------------------------------------------
```

3 Check the number of DHCTs that have the null OUI.

Note: If this number is more than what you consider to be reasonable, then these DHCTs should be reset to the first three octets of the DHCT MAC address. Then, you should run the updateOUI utility in the forward direction to set the OUI back to *00:02:DE*, as directed in step 5 of this procedure.

4 To reset the null OUI, type **updateOUI -rz** and then press **Enter**. The system replaces all null OUIs in the database with the first three octets of the DHCT MAC address.

```
>> updateOUI -rz

-------------------------------------------------------------------------------------------------
Mar 23, 8:17:36 - updateOUI Started.
updateOUI Options: -rz (Reset NULLOUI=MAC);
 CAUTION *** OUI's will be updated! ***
   (Type Ctrl-C now to abort!)
 Total DHCTs (hct_profile rows) in the database.....   1519
-------------------------------------------------------------------------------------------------
<---------MACaddr Counts--------->        -<----------OUI Counts---------->
 02:DE  01:A6  40:7B  0A:73  other       02:DE  01:A6  40:7B  0A:73  other   Total
 ------  ------  ------  ------  ------       ------  ------  ------  ------  ------  ------
   64     116    551    787     1           1518     0       0       0       1      1519
-------------------------------------------------------------------------------------------------
Mar 23, 8:17:41 - updateOUI Ended.
-------------------------------------------------------------------------------------------------
```

5 Run the updateOUI utility in the forward direction to properly set the OUI to *00:02:DE*.

Miscellaneous updateOUI Options

Introduction

In addition to updating and resetting DHCT OUIs, the updateOUI utility includes options that display a help window, the version number, and a window that shows the number of MAC addresses and OUIs associated with the DHCTs in the database. Refer to one of the following procedures in this section when running updateOUI in one of these modes:

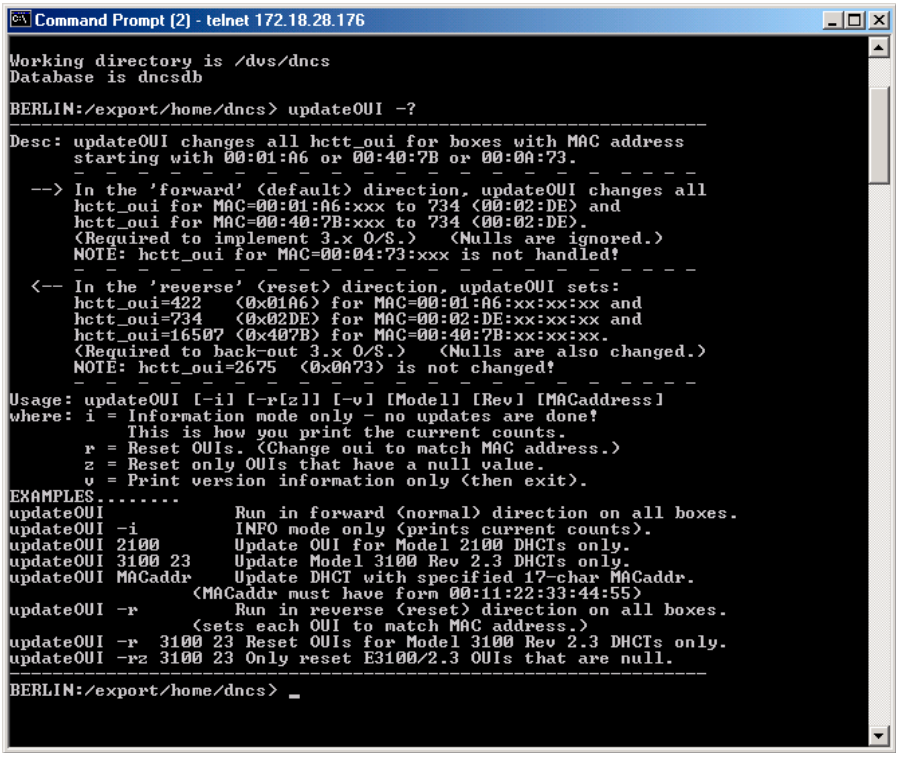
- To display the updateOUI help window, go to ***Displaying the updateOUI Help Window*** (on page 235).
- To display the updateOUI version number, go to ***Displaying the updateOUI Version Number*** (on page 236).

Displaying the updateOUI Help Window

Follow these instructions to display a window listing the various modes in which you can run the updateOUI utility.

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

2 Type **updateOUI -?** and then press **Enter**. The system displays a window showing the various options with which you can run the updateOUI utility.

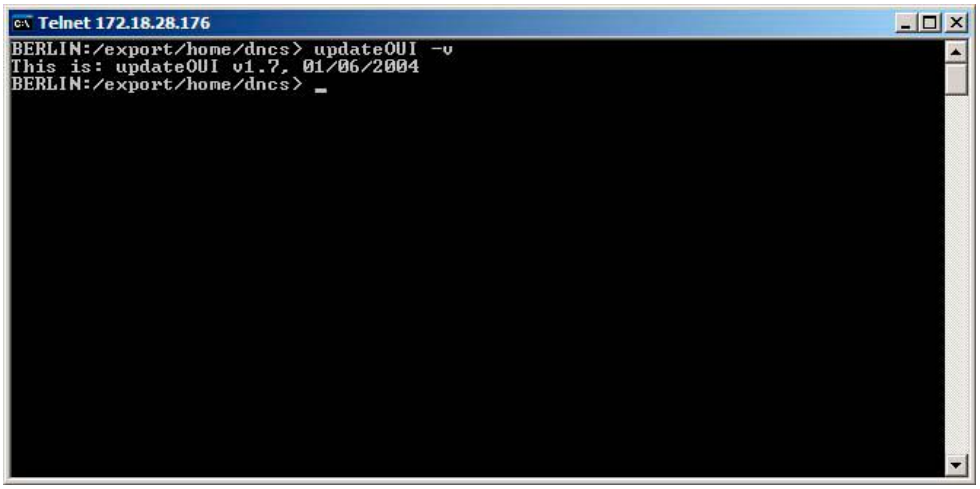


Displaying the updateOUI Version Number

Follow these instructions to display the version number of the updateOUI utility installed on your system.

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

2 Type **updateOUI -v** and then press **Enter**. The system displays the version number of the updateOUI utility.



Example: In this example, the version number of the updateOUI utility is version 1.7.

E

The chkSamUrl Utility

Introduction

Each time a cable service provider registers a service with the Service Application Manager (SAM), the DNCS assigns the service a unique service ID and, in some cases, a new URL. These URLs are stored in the bulk.tbl file, which is located in the /dvs/dvsFiles/SAM directory of the DNCS.

One of the conditions of the DNCS that the Doctor Report monitors is the size of the bulk.tbl file. When the bulk.tbl file grows too large, the SAM server may be unable to generate valid SAM files. DHCTs may then reboot and display a black screen.

The bulk.tbl file has a maximum file size limit of 65 KB. The Doctor Report displays a warning when the file size exceeds 45 KB and displays an error message when the file size exceeds 55 KB. When the Doctor Report displays a warning or an error message about the bulk.tbl file growing too large, system operators should run the chkSamUrl utility. The chkSamUrl utility allows system operators to delete unused SAM URLs from the DNCS, which reduces the size of the bulk.tbl file.

The instructions in this appendix guide you through the steps of running the chkSamUrl utility.

In This Appendix

- Run the chkSamUrl Utility 238

Run the chkSamUrl Utility

Introduction

If the **Unused SAM URL Check** field of the Doctor Report displays a warning or an error message about the size of the bulk.tbl file being too large, you need to run the chkSamUrl utility in order to delete unused SAM URLs. The instructions in this section guide you through the steps of running the chkSamUrl utility.

Example: The following example illustrates a typical warning message from a system where the bulk.tbl file is too large.

Unused SAM URL Check
==========

Used URL Entries: 57
Unused Entries: 261

Warning: SIZE of bulk.tbl above threshold

****

*** Reduce file size and unused SAM URLs, run "chkSamUrl -r" ***
****

Running the chkSamUrl Utility

Complete these instructions to run the chkSamUrl utility in order to delete unused SAM URLs from the system.

1 From an xterm window on the DNCS, type cd /export/home/dncs and then press Enter. The /export/home/dncs directory becomes the working directory.

2 Type chkSamUrl -r and then press Enter.

Results:

- The chkSamUrl script runs and the current database statistics appear.
- A confirmation message appears and asks you to confirm the removal of unused SAM URLs.

```
/export/home/dncs> chkSamUrl -r

-------------------------------------------------------------------------------

Removing unused SAM URLs from the database

-------------------------------------------------------------------------------

- List current database stats:

SAM URL bulk table:          /dvs/dvsFiles/SAM/bulk.tbl
Last Updated:          Jan 20 23:37
Size:                  51694
Used URL Entries:            57
Unused URL Entries:          261

Warning: size of bulk.tbl above threshold

Do you wish to continue with removal of unused SAM URLs? [y/n]: y
```

3 Type **y**. The chkSamUrl script runs to completion.

Note: If unused URLs were removed from the DNCS, the bulk.tbl file size will not change at this point in the procedure.

Example: Refer to the following example for sample output from the chkSamUrl script:

First, backup affected database tables:

```
DATABASE Table              DATABASE Backup file location
------------------         --------------------------------
applicationurl              --> /tmp/applicationurl.unl
samservices                 --> /tmp/samservices.unl
displaychannels.unl         --> /tmp/displaychannels.unl

Backups created:

-rw-r--r--  1 dncs dncs  30839 Jan 25 15:41 /tmp/applicationurl.unl
-rw-r--r--  1 dncs dncs   3442 Jan 25 15:41 /tmp/displaychannels.unl
-rw-r--r--  1 dncs dncs  12593 Jan 25 15:41 /tmp/samservices.unl

    Now removing unused SAM URL entries from the database

Database selected
261 row(s) deleted
Database closed

    List updated database stats:

SAM URL bulk table:         /dvs/dvsFiles/SAM/bulk.tbl
Last Updated:               Jan 20 23:37
Size:                       51694
Used URL Entries:           57
Unused URL Entries:         0
************************************************************

Although the unused SAM URLs have been removed from the database,
a SAM Services save will need to be performed in order to get the
saManager to acknowledge the changes made to the database.
************************************************************
```

4 Review the updated database statistics, locate the **Size** field, and record the bulk.tbl file size in the following space: _____ KB

5 Locate the **Unused URL Entries** field. Were unused URL entries identified and removed from the database?

- If **yes**, go to step 6.
- If **no** and the bulk.tbl file size is greater than 45 KB, call Cisco Services.
- If **no** and the bulk.tbl file size is less than 45 KB, go to *Minimizing the bulk.tbl File Size* (on page 241).

6 From the DNCS Administrative Console, click the **Application Interface Modules** tab, and then click SAM Service. The SAM Service List window opens.

7 Select any service in the list, click **File**, and then select **Open**. The Set Up SAM Service window opens.

8 Click **Save**. The SAM service is updated and, within 20 minutes, the saManager process will update all files with the current system configuration.

9 Wait at least 20 minutes and, in an xterm window, type **chkSamUrl -l** from the /export/home/dncs directory. The output lists the updates of the current file size and available space in the bulk.tbl file.

Note: The "l" is a lower case L.

10 Verify that the new bulk.tbl file size is smaller than the file size recorded in step 4.

Important! If the new bulk.tbl file size is not smaller than the file size recorded in step 4, call Cisco Services.

11 Go to *Minimizing the bulk.tbl File Size* (on page 241).

Minimizing the bulk.tbl File Size

To minimize the bulk.tbl file size and prevent file size issues that could be detrimental to your system, complete the following procedures each time you edit a SAM URL.

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

2 Select the service that you want to update.

3 Click **File** and then select **Open**. The Set Up SAM Service window opens.

4 Record the URL that you are about to edit, _____, and then edit the URL, as needed (for example, to change the application version number in the URL).

5 Click **Save**. The SAM Service List window returns to the forefront.

6 Is the SAM URL that you modified used by multiple services?

- If **yes**, update the other services to use the new URL, and then go to step 7.
- If **no**, go to step 7.

7 Select the SAM service that you selected in step 2, and then click the **Select** button that is adjacent to the Application URL box. The Application URL window opens.

Important! You are about to perform a deletion procedure. The watchtv, ippv, music, virtchan, and msgview URLs should *never* be deleted from the system.

8 Find and select the URL that you recorded in step 4, and then click **Delete URL**. A confirmation window opens.

9 Click **Yes** to confirm the deletion. The Set Up SAM Service window returns to the forefront.

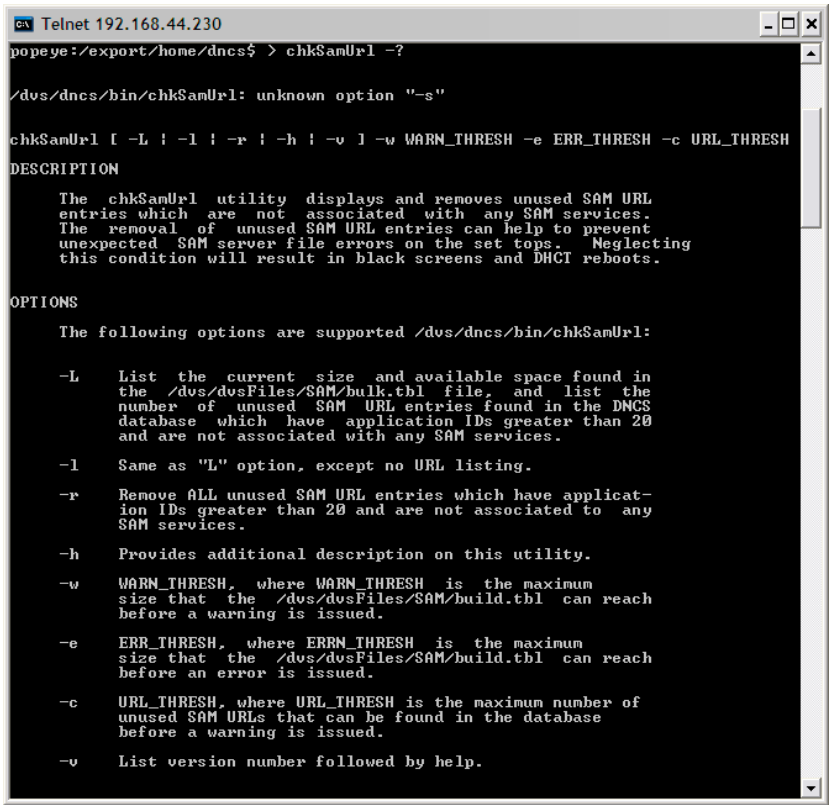
10 Click **Cancel**. The Set Up SAM Service window closes.

To Learn More About the chkSamUrl Utility

To learn more about the chkSamUrl utility, access the help screen. Follow these instructions to access the help screen.

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

2 Type **chkSamUrl -?** and then press **Enter**. The system displays the help screen associated with the chkSamUrl utility.



3 Call Cisco Services to learn more about any option available for use with the chkSamUrl utility.

F

Guidelines for Text Files Used in DNCS Utilities

Introduction

Several utilities described in the *DBDS Utilities Version 5.1 Installation Instructions and DNCS Utilities User's Guide* can act upon a single DHCT or upon a series of DHCTs. When a utility acts upon a series of DHCTs, those DHCTs are usually identified to the utility by a list of MAC addresses or serial numbers that are contained in a pre-prepared text file. This appendix provides general guidelines in preparing a text file containing a list of MAC addresses or serial numbers.

In This Appendix

- Prepare the Text File 244
- Preparing the Text File 245

Prepare the Text File

Introduction

Some DNCS Utilities (such as the delete-sm utility, the tellDhct utility, and the tellDhctInfo utility) can accept, as an argument, an input text file containing a list of DHCT MAC addresses or serial numbers. This section provides general guidelines that you should use when you prepare the input text file.

Guidelines for Preparing the Text File

Use the following guidelines when preparing the input text file:

- Prepare the file using a standard text editor, such as vi.
- Prepare the file with one MAC address or serial number per line.

  Examples: (two examples using MAC addresses followed by one example using serial numbers)

  - 00:02:DE:4A:11:92
    00:02:DE:4A:11:93
    00:02:DE:4A:11:94
  - 0002DE4A1192
    0002DE4A1193
    0002DE4A1194
  - SABFXHXSB
    SABFXHZQX
    SABFXHXNQ
- Each MAC address or serial number must be left-justified on each line of text.
- Save the file using a name that is relevant to the contents of the file. Append the current date to the end of the file name.

  Examples:

  - **tellDhct-in_06.13.05** for a file that was created on June 13, 2005
  - **tellDhctInfo-in_06.13.05** for a file that was created on June 13, 2005
- Cisco recommends that you save the file to the /tmp directory on the DNCS, for a file that you will use only once. For a file that you may re-use, create a directory for the file under /export/home.

Preparing the Text File

Follow these instructions to prepare a text file for use with the tellDhct utility.

Important! These instructions use the vi text editor as an example. The vi text editor is not intuitive. These instructions should be no substitute for a good working knowledge of the vi text editor.

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

2 Type **cd /tmp** and then press **Enter**.

Note: Cisco recommends that you save the text file in the /tmp directory on the DNCS.

3 Type **vi [file name]** and then press **Enter**. The file opens for editing.

Examples:

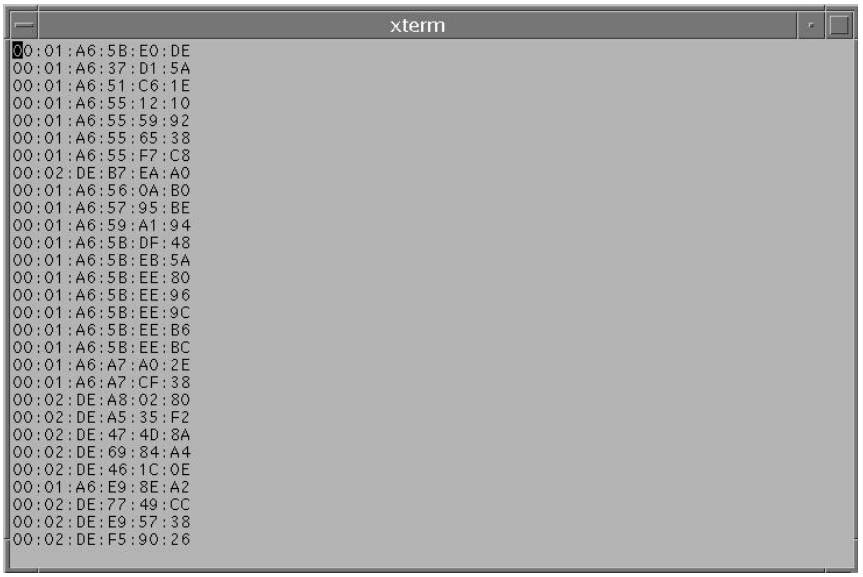
- **vi tellDhct-in_06.13.05**
- **vi tellDhctInfo-in_06.13.05**
- **vi del-sm-in_06.13.05**

4 Insert your list of MAC addresses, SMSNs, or serial numbers into the file you have just opened.

Important! Type only one MAC address or serial number per line.

Note: Use the guidelines in Guidelines for Preparing the Text File, earlier in this section.

Example: If you used a list of MAC addresses when preparing the file, your file should look similar to the following example when you are finished.



5 Save the file and close the vi editor.

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.

©2006, 2012 Cisco and/or its affiliates. All rights reserved.
April 2012 Printed in USA Part Number 740020 Rev H