CoolTools Utilities Version 6.1
Users 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

Contents

About This Guide

Purpose

This guide provides procedures for running the various CoolTools utilities that are included as part of the suite of Digital Broadband Delivery System (DBDS) Utilities. The CoolTools utilities are a collection of utility programs designed to improve the efficiency with which system operators manage their DBDS, as a whole.

Installation of the CoolTools Utilities

Installation of the CoolTools utilities occurs automatically when you install the DBDS Utilities. Refer to *DBDS Utilities Version 6.1 Installation Instructions and DNCS Utilities User Guide* (part number 4020695) for installation instructions for the DBDS Utilities.

Notes:

- Some of the chapters in this guide include a procedure for removing the specific CoolTool utility discussed in that chapter. Be sure you call Cisco Services before you remove any CoolTool utility from the DNCS or the Application Server.
- Procedures for removing the entire suite of DBDS Utilities are contained in Appendix C of the *DBDS Utilities Version 6.1 Installation Instructions and DNCS Utilities User Guide* (part number 4020695).

Scope

The utilities described in this installation and operation guide pertain to systems running either the Cisco Resident Application (SARA) or other resident applications.

Audience

This document is written for system operators of the DBDS. Our engineers, who help system operators manage and troubleshoot their system, may also find this document useful.

Read Me

Some of the utilities described in this guide interact with the DNCS and Application Server databases. Be sure you have a current database backup tape before running any of the utilities described in this guide.

System Release Compatibility

Refer to the *DBDS Utilities Version 6.1 Configuration Guide* (part number 4020693) for system release compatibility information for the CoolTools Utilities.

To access the most current version of the *DBDS Utilities Version 6.1 Configuration Guide* (part number 4020693), please access your company's extranet site. For accessing instructions, contact your marketing manager. Check your extranet site often as the information is updated frequently.

Related Publications

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

- *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455)
- *DBDS Backup and Restore Procedures for SR 2.1.1, SR 3.0.1, and SR 2.1.1 and SR 3.0.1 Service Pack 1* (part number 4003238)
- *DBDS Backup and Restore Procedures For SR 2.2 Through 4.2* (part number 4013779 Revision A)
- *DBDS Utilities Version 6.1 Configuration Guide* (part number 4020693)
- *DBDS Utilities Version 6.1 Installation Instructions and DNCS Utilities User Guide* (part number 4020695)
- *DBDS Utilities Version 6.1 Release Notes* (part number 4020692)
- *Using Disk Mirroring During an Enterprise 450 DNCS Upgrade* (part number 745251)

Document Version

This is the second release of this guide. In addition to minor text and graphics changes, the following table lists the differences between this guide and the previous version of the CoolTools utilities, described in *CoolTools Utilities User's Guide* (part number 749640).

Description	See Topic
The type8helper utility has been added to the CoolTools utilities in version 6.1 of DBDS Utilities.	See ***Ensure the Presence of Type-8 Staging EMMs with the type8helper Utility*** (on page 107).
The preserveLog utility has been added to the CoolTools utilities in version 6.1 of DBDS Utilities.	See ***Preserve Log Files with the preserveLog Utility*** (on page 113).
The getCCdata utility has been added to the CoolTools utilities in version 6.1 of DBDS Utilities.	See ***Retrieve CableCARD Data with the getCCdata Utility*** (on page 127).
The mgrep utility has been added to the CoolTools utilities in version 6.1 of DBDS Utilities.	See ***Perform a Multi-Line grep with the mgrep Utility*** (on page 133).
The emm_check utility, which first appeared as a CoolTools utility in version 2.2 of DBDS Utilities (August 2002), has been removed from version 6.1 of DBDS Utilities.	

1

Obtain Common Database Information with the dblook Utility

Introduction

System operators and support engineers can use the dblook utility to query the database for some commonly requested information related to DHCTs, QAM and MQAM modulators, QPSK modulators and demodulators, and the BFS server. The utility displays a menu that features a numbered list of database queries when it is first run. To query the database, the system operator just types the number associated with the query the system operator wishes to perform. The system then displays the results of the query to the screen of the DNCS.

In This Chapter

Run the dblook Utility

Running the dblook Utility

Follow these instructions to run the dblook utility.

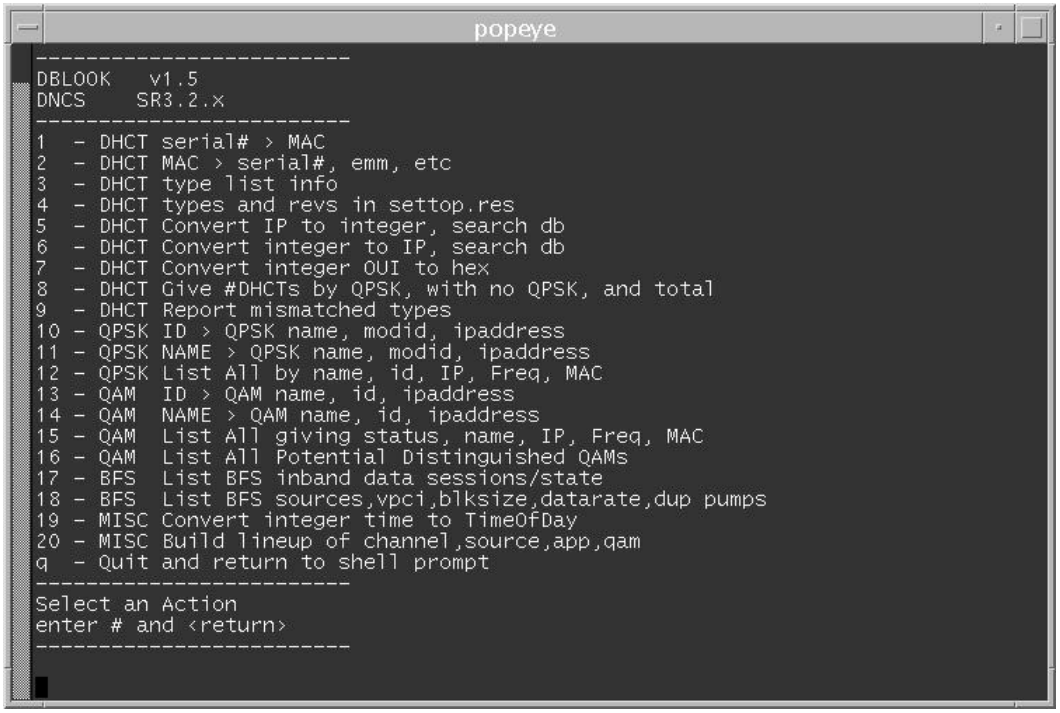
Important: You must be logged on to the DNCS as dncs user to run this utility.

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

2 Click and drag the corner of the xterm window to resize it so that it is at least 100 columns wide.

Note: As you resize the window, numbers appear on the window that indicate the current number of columns and rows.

3 Type **dblook.ksh** and then press **Enter**. The system displays a menu listing the various database queries you can perform.



4 Type the number associated with the query and then press **Enter**. The system displays the results of the query.

Note: Refer to ***The dblook Utility Options*** (on page 3) for details related to each of the queries.

The dblook Utility Options

Options for the dblook Utility

Refer to the following table for an explanation of the options associated with the dblook utility.

Number	Function
1	**DHCT serial# > MAC** The system prompts the user to type a DHCT serial number and to then press Enter. The system then displays the DHCT serial number and the associated MAC address.
2	**DHCT MAC > serial#, emm, etc** The system prompts the user to type the last portion of a MAC address for a DHCT and to press **Enter**. **Example:** Type **F3:3F:8E** and then press **Enter**. The system then displays the following information: ■ Number of EMMs associated with the DHCT ■ Serial number of the DHCT ■ MAC address of the DHCT ■ Data for the DHCT from the hct_profile table ■ Data for the DHCT from the secure_micro table **Note:** If several DHCTs meet the search criteria, then data for each DHCT is displayed. To prevent data for more than one DHCT from appearing in the output, submit as much of the DHCT MAC address as possible to the dblook query.

Number	Function
3	**DHCT type list info** A six-column table with the following information appears: **1** DHCT types and revisions loaded onto the system **2** OUI for each type/revision combination **3** Software Table of Contents (SWTOC) file associated with each type/revision/OUI combination **4** Y (for yes) or N (for no) indicating whether the type/revision/OUI combination is contained in the settop.res file currently loaded on the DNCS **5** Image file associated with each type/revision/OUI combination **6** Indicates potential conflicts based upon the values of the five previous columns. **Examples:** – **NO_SWTOC_OR_IMAGE** appears if there is neither a SWTOC file or an image file associated with a type/revision/OUI combination. – **SWTOC_AND_IMAGE** appears if a type/revision/OUI combination has both a SWTOC file and an image file.
4	**DHCT types and revs in settop.res** A list appears that contains the various type/revision/OUI combinations included in the settop.res file loaded into the Broadcast File System (BFS) server.
5	**DHCT Convert IP to integer, search db** The system prompts the user for a DHCT IP address, and then displays the integer form of that IP address as it is stored in the DNCS database. The system then asks the user if it should search the database for that IP address. The user can respond with an **s** (for search) or any other key to return to the menu. If the user responds with an **s**, the system displays the data for that DHCT as listed in the hct_profile table.
6	**DHCT Convert integer to IP, search db** The system prompts the user for a 9-digit integer, which it converts to a DHCT IP address. The system then asks the user if it should search the database for that IP address. The user can respond with an s (for search) or any other key to return to the menu. If the user responds with an s, the system displays the data for that DHCT as listed in the hct_profile table.

Number	Function
7	**DHCT Convert integer OUI to hex** The system prompts the user for an integer, which it converts to a hexadecimal OUI.
8	**DHCT Give #DHCTs by QPSK, with no QPSK, and total** A list appears that contains the number of DHCTs associated with each QPSK, the number of DHCTs associated with no QPSK, and totals.
9	**DHCT Report mismatched types** A list appears that contains mismatched DHCT types as reported in the dncsLogs files. The system then asks if it should display the MAC addresses of these DHCTs.
10	**QPSK ID > QPSK name, modid, ipaddress** The system prompts the user to enter the ID of a QPSK. The system then displays the data for that QPSK as listed in the davic_qpsk table.
11	**QPSK NAME > QPSK name, modid, ipaddress** The system prompts the user to enter the name of a QPSK. The system then displays the data for that QPSK as listed in the davic_qpsk table.
12	**QPSK List All by name, id, IP, Freq, MAC** The system displays the following information about each QPSK in the database: ■ ID ■ name ■ IP address ■ frequency ■ MAC address
13	**QAM ID > QAM name, id, ipaddress** The system prompts the user to enter the ID of a QAM. The system then displays the data for that QAM as listed in the pdcaqam table.
14	**QAM NAME > QAM name, id, ipaddress** The system prompts the user to enter the name of a QAM. The system then displays the data for that QAM as listed in the pdcaqam table.

Number	Function
15	**QAM List All giving status, name, IP, Freq, MAC** The system displays the following information about each QAM in the database: ■ On-line status ■ name ■ IP address ■ frequency ■ MAC address
16	QAM List All Potential Distinguished QAMs The system searches the database for all QAMs that are not associated with a hub, and could thus potentially become a distinguished QAM. **Note:** This information is useful only to those systems supporting SR 1.4 or later software.
17	**BFS List BFS inband data sessions/state** The system displays a list containing even-numbered BFS sessions (between 2 and 22) and the session state for each session.
18	**BFS List BFS sources, vpci, blksize, datarate, dup pumps** The system lists the sources for the inband and out-of-band BFS sessions, along with the name, vpci number, blocksize, and datarate of each source. Additionally, the system looks for duplicate BFS and datapump processes and reports any that are found.
19	**MISC Convert integer time to TimeOfDay** The system prompts the user to enter a time in UNIX system time format (number of seconds from January 1, 1970). The system then displays the equivalent local time.

Number	Function
20	**MISC Build lineup of channel, source, app, qam** The system displays the following data for each source and for each channel in the displaychannels table: ■ hub number ■ hub name ■ channel number and description ■ source ID ■ display application ■ QAM and frequency for digital channels The user is then offered the opportunity to save the information to a tab-delimited text file, which can easily be imported into a spreadsheet.

2

Save Core Files with the savecore Utility

Introduction

The savecore utility enables system operators to save the contents of system memory to a file for later analysis when the DNCS or the Application Server crashes.

Note: The contents of system memory at crash time is commonly referred to as a *core dump*.

System operators run the savecore utility once on the DNCS and once on the Application Server. The utility modifies system configuration files on the DNCS and the Application Server so that the contents of a core dump are written automatically to a file upon reboot. The system operator, our engineers, or Sun Microsystems engineers can later examine the file to determine why the system crashed.

Important: The savecore utility modifies the /etc/init.d/sysetup file when it executes for the first time. However, before modifying the file, the utility saves a copy of the original file so that the original file can later be restored if the system operator should decide to no longer automatically save the contents of a core dump.

What System Releases Benefit From the savecore Utility?

Systems running SR 1.5.x and earlier benefit from running the savecore utility. These systems run on the Solaris version 2.5.1 Operating System (OS).

There is no need to run the savecore utility on sites that support SR 2.x or later system software. These systems run on the Solaris version 8 OS. Functionality of the savecore utility is enabled automatically by default in this OS.

In This Chapter

Run the savecore Utility on the DNCS

Running the savecore Utility on the DNCS

Follow these instructions to run the savecore utility on the DNCS.

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

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

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

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

3 Type **. /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 **savecore.ksh** and then press **Enter**.

   Results:

   - The system checks available free space in the /export/home directory.

     Note: Our engineers recommend that the /export/home directory has at least 1 GB of free space available in which to create the core dump directory.

   - The system creates the core dump directory.

     Note: This directory is called /export/home/crash/[DNCS name] on the DNCS.

   - The system copies the /etc/init.d/sysetup file to sysetup.[date].

   - The system modifies the /etc/init.d/sysetup file.

     Note: The purpose of the file modification is to enable the system to check for core dumps and to write core dump output to the appropriate directory when the system reboots.

   Example: The system displays the following messages as the savecore utility executes:

   # savecore.ksh
   /export/home has 2439964 MB of available space.
   We will use /export/home for the base dump path.
   The dump directory will be /export/home/crash/[DNCS name]
   Creating the dump directory.
   Editing the /etc/init.d/sysetup file.
   Putting new sysetup file in place and change ownership and permissions.
   Removing temp files.
   SAVECORE has been enabled.

Run the savecore Utility on the Application Server

Transferring the savecore Utility to the Application Server

Before you can run the savecore utility on the Application Server, you must first transfer the file from the DNCS to the Application Server. Follow these instructions to transfer the savecore file from the DNCS to the Application Server.

1. From an xterm window on the Application Server, type **cd /dvs/appserv/bin** and then press **Enter**. The /dvs/appserv/bin directory becomes the working directory.
2. Type **ftp dncsatm** and then press **Enter**. A log in prompt appears.
3. Log in to the DNCS as **dncs** user. An ftp session between the DNCS and the Application Server is established.
4. Type **cd /dvs/dncs/bin** and then press **Enter**. The /dvs/dncs/bin directory becomes the working directory on the DNCS.
5. Type **bin** and then press **Enter**. The system prepares the file transfer for binary mode.
6. Type **hash** and then press **Enter**. The system is instructed to display hash marks (**#**) as the file transfers to show transfer progress.
7. Type **get savecore.ksh** and then press **Enter**. The system transfers a copy of the savecore.ksh utility from the DNCS to the Application Server.
8. Type **bye** and then press **Enter**. The ftp session closes.
9. Follow these instructions to log in as root user in the xterm window on the Application Server.
   a. Type **su -** and then press **Enter**.
   b. Type the root password and then press **Enter**.
10. Type **chmod +x savecore.ksh** and then press **Enter**. The system applies executable permissions to the savecore.ksh utility.

Running the savecore Utility on the Application Server

After transferring the savecore utility from the DNCS, run it next on the Application Server. Follow these instructions to run the savecore utility on the Application Server.

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

3 Type **savecore.ksh** and then press **Enter**.

Results:

- The system checks available free space in the /export/home directory.

  Note: The /export/home directory needs at least 1 GB of free space available in which to create the core dump directory.

- The system creates the core dump directory.

  Note: This directory is called /export/home/crash/[Application Server name] on the Application Server.

- The system copies the /etc/init.d/sysetup file to sysetup.[date].

- The system modifies the /etc/init.d/sysetup file.

  Note: The purpose of the file modification is to enable the system to check for core dumps and to write core dump output to the appropriate directory when the system reboots.

Example: The system displays the following messages as the savecore utility executes:

 # savecore.ksh
/export/home has 2439964 MB of available space.
We will use /export/home for the base dump path.
The dump directory will be /export/home/crash/[Application Server name]
Creating the dump directory.
Editing the /etc/init.d/sysetup file.
Putting new sysetup file in place and change ownership and permissions.
Removing temp files.
SAVECORE has been enabled.

Examine a Core File

Examining a Core File

When the savecore utility is enabled on the DNCS or the Application Server, the system automatically writes the contents of a core dump to a file on the DNCS or the Application Server. The system writes the contents of the core dump when the system reboots.

Note: The system names the core dump files **vmcore.0**, **vmcore.1**, **vmcore.2**, etc.

Follow these instructions to view the contents of a core dump.

1. If necessary, open an xterm window on the DNCS or Application Server, depending upon which server contains the core file you want to examine.
2. Choose one of the following options:
   - To examine a core file on the DNCS, type **cd /export/home/crash/[DNCS name]** and then press **Enter**.
   - To examine a core file on the Application Server, type **cd /export/home/crash/[Application Server name]** and then press **Enter**.

   Result: The directory to which the core dump output was written becomes the working directory.
3. Type **ls -ltr** and then press **Enter**. The system lists the files in the current directory according to modification time (most recently written files last).

   Note: The newest file, named similar to **vmcore.#**, contains the contents of system memory from the most recent system crash.
4. Type **strings vmcore.# | more** and then press **Enter**. The system opens the core file using the UNIX *strings* and *more* utilities.

   Note: Substitute the number associated with the core file you want to examine for #.

   Example: strings vmcore.0 | more
5. Examine the core file to determine why the system crashed.

   Notes:
   - Press the **Spacebar** to advance through the file.
   - Press the **Ctrl** and **c** keys simultaneously to close the core file.
   - Call Cisco Services for help in examining the core file.

Disable the savecore Utility

Disabling the savecore Utility

If you have run the savecore utility on your DNCS and Application Server, the system will automatically save your core files when the DNCS or the Application Server reboots following a system crash. If you ever want to prevent your system from saving these core files automatically, you need to reverse the system changes brought about when you first ran the savecore utility. Follow these instructions to reverse those system changes.

1. If necessary, open an xterm window on the DNCS and the Application Server.
2. Follow these instructions to log in as root user in the xterm window on the DNCS.
   a. Type **su -** and then press **Enter**.
   b. Type the root password and then press **Enter**.
3. Type **rm -ir /export/home/crash** and then press **Enter**. A confirmation message appears.
4. Type **y** (for yes) and then press **Enter**. The system deletes the core dump directory and subdirectory.
5. Type **cd /etc/init.d** and then press **Enter**. The /etc/init.d directory becomes the working directory.
6. Type **ls -l sysetup*** and then press **Enter**. The system displays all the files that start with the name sysetup.

   Important: Be sure to type the asterisk (*) after typing sysetup.
7. Type **cp /etc/init.d/sysetup.[date] /etc/init.d/sysetup** and then press **Enter**. The system restores your original /etc/init.d/sysetup file.

   Note: Use the output from the command you executed in step 6 to substitute the date that the savecore utility changed your original sysetup file for [date].

   Example: Type **cp /etc/init.d/sysetup.021802 /etc/init.d/sysetup** and then press **Enter** if your sysetup file was changed by the savecore utility on February 18, 2002.
8. Repeat steps 2 through 7 on the Application Server.

3

Improve Backup Reliability with the bkchk Utility

Introduction

System operators can use the bkchk utility for help in managing backups of their DNCS database and file system. The bkchk utility displays messages on the DNCS that provide system operators with the following information:

- The date of the last successful backup
- Notification that an automated backup attempt failed
- Whether the backup tape from the previous day is still in the tape drive (and in danger of being overwritten)
- Reminder when a file system backup is due

System operators can elect to configure the bkchk utility to run automatically from the crontab file of the DNCS, or they can run the utility from the command line.

Note: Large systems require multiple tapes for backing up the database. These systems should consider the Autobackup Server as an alternative to the bkchk utility. Contact Cisco Services for information about the Autobackup Server.

In This Chapter

Configure the bkchk Utility

Introduction

System operators should decide the following configuration issues before using the bkchk utility:

- Whether to run the bkchk utility automatically everyday from the crontab file of the DNCS
- How the bkchk utility evaluates the tape in the tape drive of the DNCS
- How often the bkchk utility should remind the system operator to perform a file system backup

Read the remainder of this section for help in deciding each of these configuration issues.

crontab File Entry

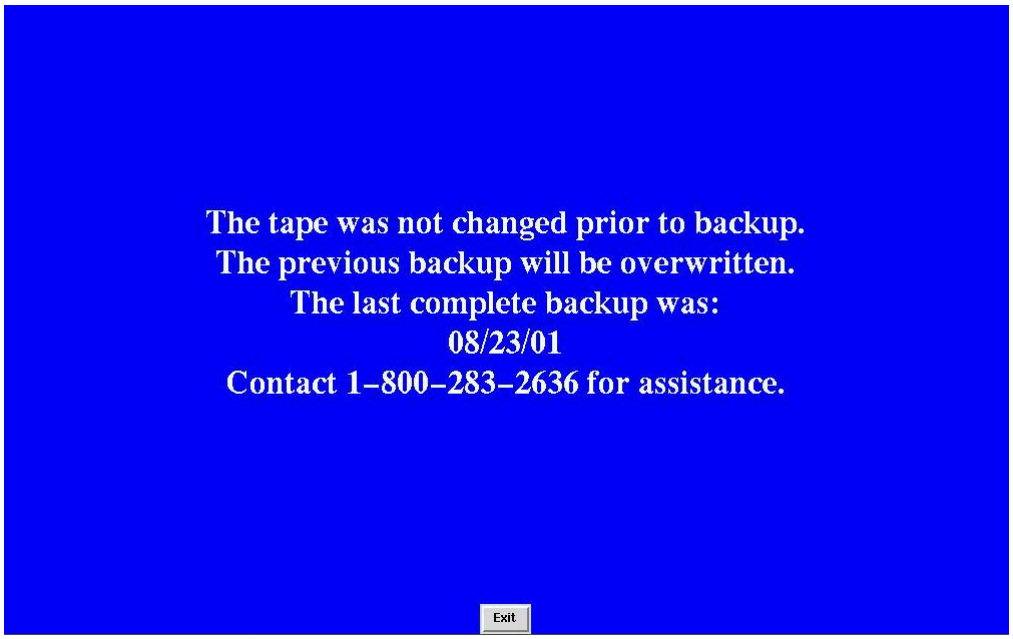
System operators can run the bkchk utility with the *-i* option to create an entry in the crontab file of the DNCS. When an entry for the bkchk utility is placed in the crontab file, the system runs the bkchk utility automatically at 11:45 every evening, Monday through Saturday. System operators can later modify the crontab file entry for the bkchk utility if they want to run the utility at a different time.

Important: Our engineers recommend that system operators elect to run the bkchk utility automatically through the crontab file.

Tape Evaluation

The bkchk utility contains a configurable parameter called DAYOFFSET. The DAYOFFSET parameter can be set to 0 or 1. The bkchk utility uses the DAYOFFSET parameter to evaluate the suitability of the tape in the tape drive of the DNCS. If the bkchk utility determines that the tape in the tape drive represents the previous day's backup, the system will display a message to the DNCS that warns that the previous backup is in danger of being overwritten by the current backup. System operators or headend personnel who see this message are thereby reminded to switch tapes.

Example: The DNCS displays a message similar to the following when a backup tape is in danger of being overwritten.



Refer to ***Deciding on the DAYOFFSET Parameter*** (on page 19) for guidance on configuring the DAYOFFSET parameter.

Deciding on the DAYOFFSET Paramater

When an entry for the bkchk utility is added to the crontab file, the system runs the utility by default at 11:45 each evening, Monday through Saturday. The default value for the DAYOFFSET parameter is 0. These default conditions are most useful for systems that back up their DNCS database after-hours, when headend personnel have gone home. When headend personnel return in the morning, the DNCS displays the message noted in the preceding example. The message indicates that the tape in the tape drive is in danger of being overwritten. Headend personnel who see this message are therefore reminded to switch tapes in preparation for the current day's backup.

System operators who back up their DNCS database when headend personnel are still on duty, may find it beneficial to set their DAYOFFSET parameter to 1. Additionally, system operators may need to edit the bkchk.ksh entry in the crontab file so that the system runs the utility *before* the scheduled database backup. This way, if the tape in the tape drive represents the previous day's backup, headend personnel on duty are reminded to change the tape before it is overwritten by the current day's backup.

Important: Call Cisco Services if you have any questions related to the interaction of the crontab file and the DAYOFFSET parameter. Cisco Services engineers will question you about when you perform your database backups and can advise you on how to configure your crontab file entry and the DAYOFFSET parameter.

Changing the DAYOFFSET Parameter

Follow these instructions to change the DAYOFFSET parameter in the bkchk.ksh file.

Important: Note these important points:

- Call Cisco Services before changing the DAYOFFSET parameter. Cisco Services engineers will ensure that you understand the relationship between the DAYOFFSET parameter and the bkchk.ksh entry in your crontab file.
- Do not attempt to change the DAYOFFSET parameter unless you are knowledgeable in the use of the UNIX vi editor.

1. If necessary, open an xterm window on the DNCS.
2. Type **vi /dvs/dncs/bin/bkchk.ksh** and then press **Enter**. The bkchk.ksh file opens for editing using the UNIX vi editor.
3. Locate the following line in the bkchk.ksh file:
   DAYOFFSET="0"

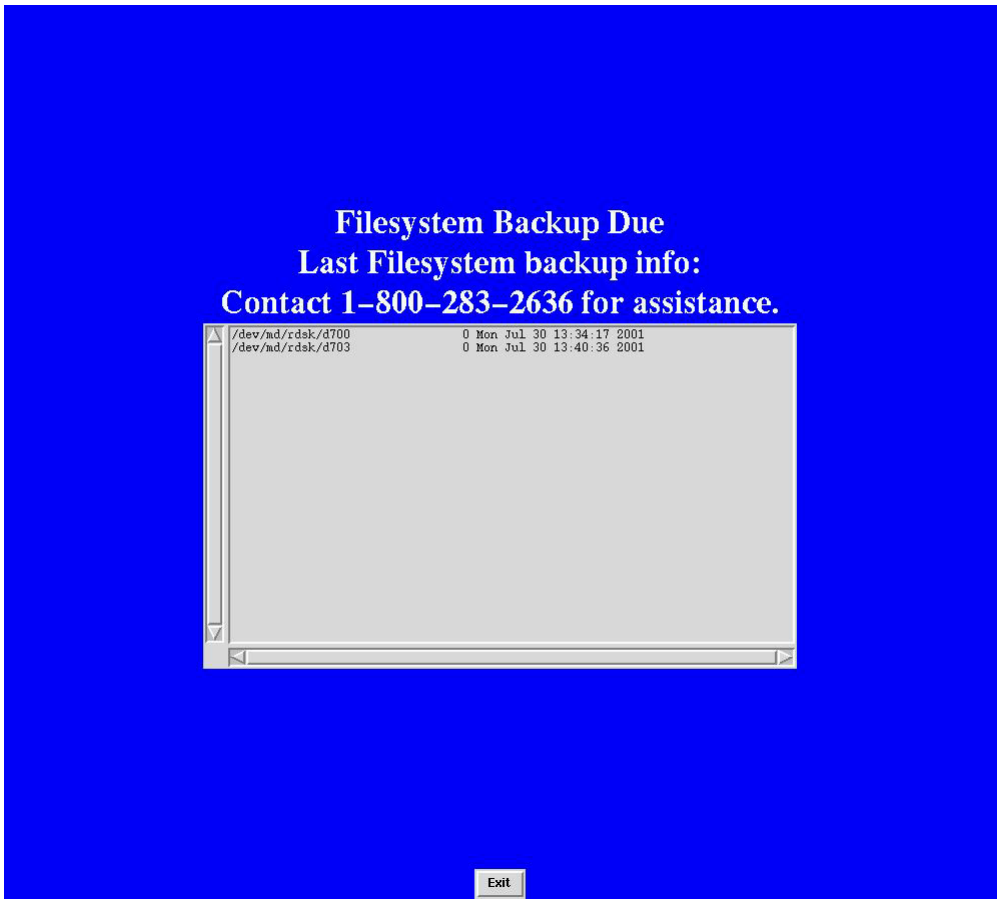
   Note: If you have previously changed the parameter, your DAYOFFSET parameter may already be set to 1.
4. Change the number between the quotation marks to **1** or **0**, whichever is appropriate.
5. Save the bkchk.ksh file and close the vi editor.

File System Backup Recommendation

System operators should back up their DNCS file system at least once a month. In addition, system operators should back up the DNCS file system immediately following major change to system configuration.

Note: Procedures for backing up the DNCS file system are found in the set of backup and restore procedures that pertains to your system.

System operators can configure the bkchk utility to display the following message to the screen of the DNCS when the file system backup is due.



Decide how often you want to back up the DNCS file system and then complete the procedure in ***Configuring the bkchk Utility for a File System Backup Reminder*** (on page 21).

Configuring the bkchk Utility for a File System Backup Reminder

Follow these instructions to configure the bkchk utility to remind you when to perform a file system backup.

Note: This procedure reminds you to perform a file system backup; it does not actually perform the file system backup for you.

Important: Do not attempt to configure the bkchk utility unless you are knowledgeable in the use of the UNIX vi editor.

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

2 Type **vi /dvs/dncs/bin/bkchk.ksh** and then press **Enter**. The bkchk.ksh file opens for editing using the UNIX vi editor.

3 Locate the following two sequential lines in the bkchk.ksh file :
#REMIND="01/05 03/05 05/05 07/05 09/05 11/05"
REMIND=""

4 Insert dates between the quotation marks in the second line you located in step 3.

Notes:

- The dates you insert represent the dates you want to be reminded to perform a file system backup.
- Use the line beginning with the number symbol (#) as an example.

Example: To be reminded to perform a file system backup on the 5th of every month, edit the line in step 3 so that it looks like the following example:

"REMIND="01/05 02/05 03/05 04/05 05/05 06/05 07/05 08/05 09/05 10/05 11/05 12/05"

5 Save the bkchk.ksh file and close the vi editor.

Run the bkchk Utility

Introduction

System operators can run the bkchk utility with the following options:

- *-i* - installs an entry for the bkchk utility in the crontab file of the DNCS.
- *-t* - displays the backup date associated with the tape in the tape drive.
- *-h* - displays a screen that shows all the options with which the bkchk utility can be run.
- *-v* - displays the version number of the bkchk utility on your system

The procedures in this section guide you through the steps required to run the bkchk utility.

Creating a crontab Entry

Follow these instructions to configure your system to create an entry in the crontab file of the DNCS so that the system executes the bkchk utility automatically every day.

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

2 Type **bkchk.ksh -i** and then press **Enter**. The system creates an entry in the crontab file of the DNCS so that the bkchk utility executes every night at 11:45, Monday through Saturday.

Note: System operators can later edit the crontab file to change the time during which the system runs the bkchk utility.

Important: Do not attempt to edit the crontab file unless you are a skilled user of the UNIX vi text editor and have experience in editing the crontab file. Call Cisco Services for assistance.

Confirming the Date on a Backup Tape

System operators may occasionally have to restore a system using data from a previous day's backup tape. Because it is crucial that a system be restored using the correct data, system operators can use the bkchk utility with the -t option to confirm the date that a backup tape was made. Follow these instructions to confirm the date on a backup tape.

1 Insert your backup tape into the tape drive of the DNCS.

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

3 Type **bkchk.ksh -t** and then press **Enter**. The system examines the tape and displays a message similar to the following:

Date on tape in [device name] = [date]

Note: The system substitutes the device name of the tape drive for [device name] and the date the backup tape represents for [date].

4 Compare the date shown in the message from step 3 with the date of the tape backup you need and then choose one of the following options.

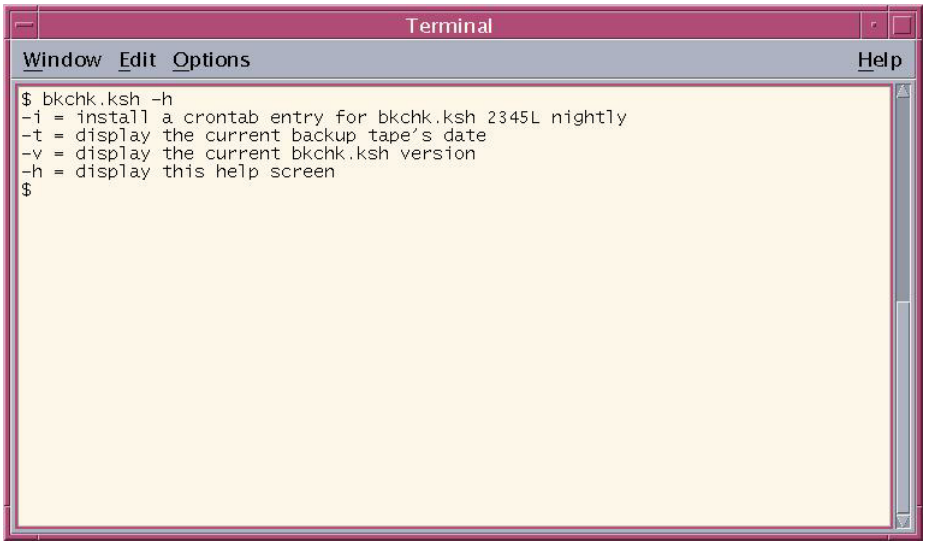
- If the tape has the correct date, proceed with the restoration.
- If the tape has the incorrect date, eject the tape, obtain the correct backup tape, and repeat these steps.

Examining bkchk Utility Options

Run the bkchk utility with the *-h* option to display a list that shows all the options with which you can run the bkchk utility.

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

2 Type **bkchk.ksh -h** and then press **Enter**. The system displays a list of all the options you can use to run the bkchk.ksh utility.



Note: In addition to the options described earlier in this section, the list also shows that you can type **bkchk.ksh -v** and then press **Enter** to display the version number of the bkchk utility.

Remove the crontab Entry for the bkchk Utility

Introduction

Follow these procedures to remove the crontab entry for the bkchk utility from your system.

Removing the crontab Entry for the bkchk Utility

Follow this procedure only if you have created an entry in the crontab file of the DNCS that automatically executes the bkchk utility every day.

1. If necessary, open an xterm window on the DNCS.
2. Follow these procedures to specify the editor with which you will edit the crontab file.
   a. Type **EDITOR=vi** and then press **Enter**.
   b. Type **export EDITOR** and then press **Enter**.
3. Type **crontab -e** and then press **Enter**. The crontab file opens for editing using the UNIX vi editor.
4. Remove the entry for the bkchk.ksh utility.
5. Save the crontab file and close the UNIX vi editor.

4

Monitor Submirror Synchronization with the syncwait Utility

Introduction

Disk mirroring is supported on the Sun Enterprise 450 and the Sun Fire V445, V880, and V890 Digital Network Control System (DNCS) platforms. Through disk mirroring, the DNCS stores identical information across sets of hard drives. The syncwait utility was developed to monitor the progress of mirrored disks as they synchronize their data.

Important: The syncwait utility is useful only on a Sun Enterprise 450, Sun Fire V445, V880, or V890 DNCS. These are the only DNCS platforms that support disk mirroring.

In This Chapter

Run the syncwait Utility

Introduction

Mirrored disks lose their synchronization whenever the disk mirroring function of the Sun Enterprise 450, Sun Fire V445, V880, or V890 DNCS is disabled. System operators or support engineers may disable disk mirroring on these DNCS servers just prior to a system upgrade. Then, after a successful upgrade, the disk mirroring function is re-enabled on the DNCS and the secondary mirrored disk synchronizes with the primary mirrored disk.

Additionally, mirrored disks are out of synchronization whenever disk mirroring is first configured on a Sun Enterprise 450, Sun Fire V445, V880, or V890 DNCS, or when a hard drive that failed is replaced.

System operators and support engineers can use the syncwait utility to monitor progress as mirrored disks synchronize their data.

Running the syncwait Utility

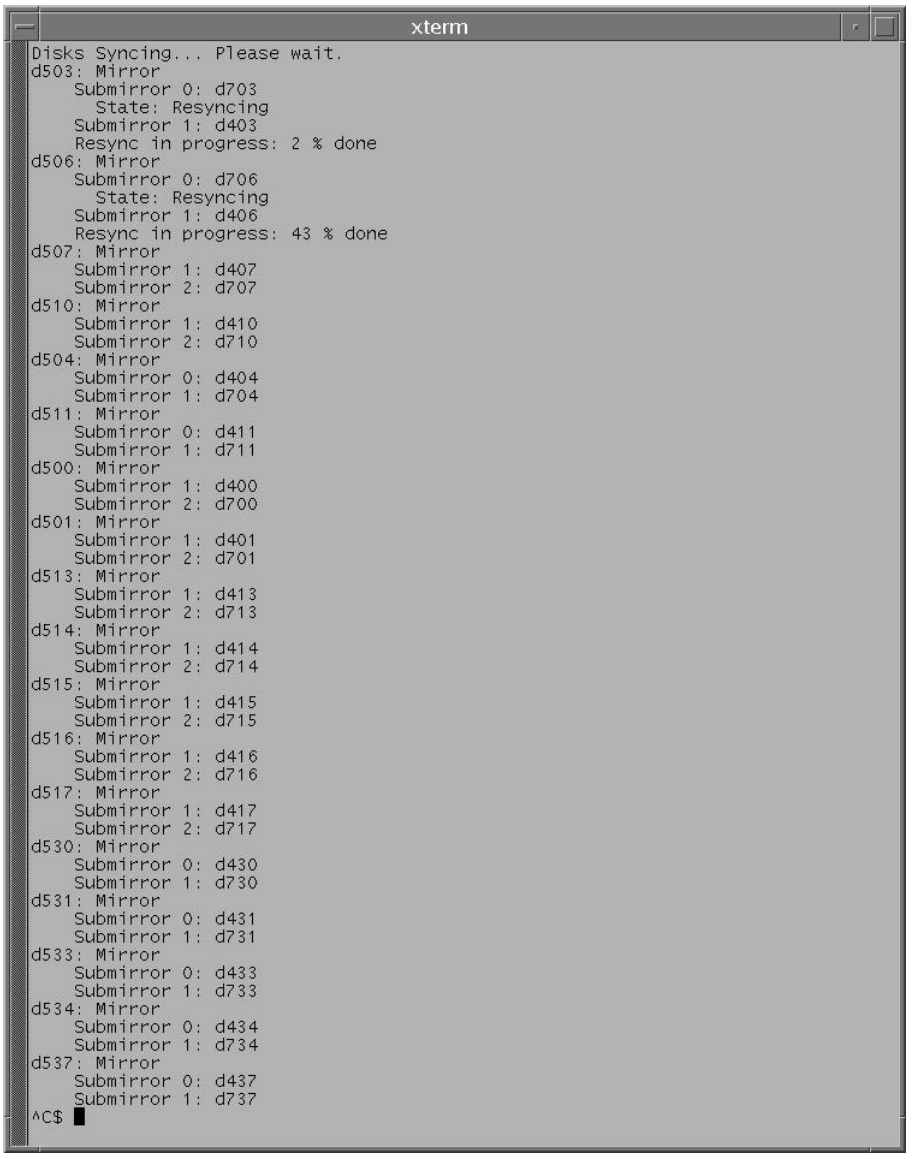
Use the following instructions to monitor progress as mirrored disks synchronize their data.

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

2 Type **syncwait.ksh** and then press **Enter**. The system displays a message stating the percentage of the mirror-synchronization process that is complete.

Notes:

- The following example shows two mirrored disk sets: d503 and d506. The submirrors associated with d503 are 2 percent synchronized. The submirrors associated with d506 are 43 percent synchronized.
- The syncwait utility updates the display every 20 seconds.



3 When the system displays the following message, type **n** (for no) and then press **Enter**:

No Resync in progress …

Continue monitoring status?

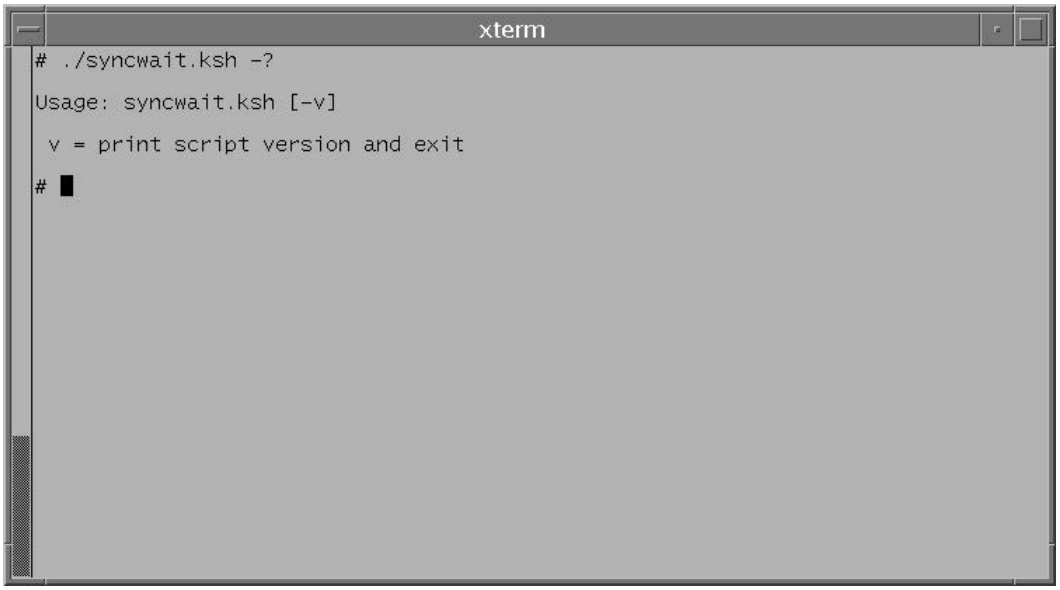
Result: The syncwait utility exits.

Examining the syncwait Utility Options

Run the syncwait utility with the -? option to display a list that shows the other options with which you can run the syncwait utility.

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

2 Type **syncwait.ksh -?** and then press **Enter**. The system shows that the syncwait.ksh utility can be run with the -v option.



Note: You can type **syncwait.ksh -v** and then press **Enter** to display the version number of the syncwait utility.

5

Track Progress of the emmDistributor with the emmlst Utility

Introduction

The camAuditor process in the DNCS keeps EMMs from expiring and stores newly encrypted EMMs in the DNCS database. The DNCS then uses the emmDistributor process to refresh DHCTs with their EMMs. The emmDistributor process runs continuously. It constantly cycles through the database, assigning EMMs to the appropriate DHCT.

With DNCS version 1.5, it typically takes several days for the emmDistributor process to cycle through a database with more than 100,000 DHCTs. System operators and support engineers may want to know how far through the database the emmDistributor process is at any given time. The emmlst utility was developed to keep track of the progress made by the emmDistributor process as it cycles through the DNCS database.

Restricted to SR 1.5.x Systems

The emmlst utility is only useful at sites that support version 1.5.x of DNCS software. The emmDistributor process at sites running DNCS software later than version 1.5.x is multi-threaded. When the emmDistributor process is multi-threaded, there is no single point in the database from where EMMs are read and distributed. For multi-threaded systems, the cycle time of the emmDistributor process is far shorter; hence the utility is no longer useful.

In This Chapter

Run the emmlst Utility

Introduction

The emmlst utility creates a list of DHCTs on the DNCS in the order that they are processed by the emmDistributor process. This list is written to a file in the /tmp directory of the DNCS. As system operators run the emmlst utility successive times, the utility may ask if the current list should be recreated or if the current list should be re-used.

Running the emmlst Utility

Follow these instructions to run the emmlst utility.

1. If necessary, open an xterm window on the DNCS.
2. Type **emmlst.ksh** and then press **Enter**. The system displays a message similar to the following:

   A Distribution List already exists.
   Reusing this list will save execution
   time. Would you like to re-use the
   existing Distribution List? (y/n)

   Notes:

   - The previous message only appears if the distribution list does, in fact, already exist. The distribution list will not exist if the emmlst utility has not been run since the last time the DNCS rebooted.
   - Whether or not the distribution list already exists on the DNCS is a relatively minor point. System operators should focus on the output of the emmlst utility, displayed in step 3.

3 Choose one of the following options:

- If it has been a very short time (within the hour) since you last ran the emmlst utility, type **y** and then press **Enter**.

  Note: If it has been a very short time since you last ran the emmlst utility, the number of DHCTs in the database probably has not changed. You can safely use the existing distribution list.

- If it has been several hours (or longer) since you last ran the emmlst utility, type **n** and then press **Enter**.

  Note: If it has been several hours or if a lot of staging activity has taken place since you last ran the emmlst utility, the number of DHCTs in the database may have changed. You should probably request that the emmlst utility generate a fresh list.

Result: The emmlst utility runs and displays information pertaining to the progress of the emmDistributor process as it cycles through the database, as well as how long it takes the emmDistributor process to distribute EMMs to the entire DHCT population.

Example: Sample output from the emmlst utility follows:

The last MAC sent EMMs was: 00:01:A6:55:BC:3C
This is MAC 82007 of 101012
This is 81% of the way through the list of MACS

EMMS are being sent to DHCTs
at 5.0 second intervals on this system
To change this value, update/add the variable
EMM_DIST_THROTTLE in the dncs .profile, and
bounce the emmDistributor process.

It would take 1 days, 3 hours, and 0 minutes
to complete the distribution list from this point.

Total cycle time is: 5 days, 22 hours, and 5 minutes.

How to Use the emmlst Utility

How EMMs are Distributed

The DNCS is typically configured to have EMMs expire within 30 days. The camAuditor process is designed to re-encrypt EMMs when the EMMs age to the point where they will expire within 19 days, or less. As stated in the Overview section of this chapter, the emmDistributor process cycles through the database and refreshes DHCTs with their newly encrypted EMMs. It may take several days for the emmDistributor process to completely cycle through a large database.

DHCTs may not receive their newly encrypted EMMs under the following circumstances:

- The DHCT is rebooting.
- The subscriber has powered-off the DHCT.
- Network problems prevent the delivery of EMMs to a DHCT.

Important: DHCTs that do not receive EMMs will time out and will be unable to support encrypted services.

Recommendation for Systems Running SR 1.5.1

System operators should run the emmlst utility at least once a day to ensure that the emmDistributor process is making steady progress through the database. System operators should ensure that it is taking the emmDistributor process no longer than 5 days to cycle through the database.

Important: Call Cisco Services if it appears that your emmDistributor process is taking longer than 5 days to cycle through the database. Cisco Services engineers may instruct you to change the value of the **EMM_DIST_THROTTLE** parameter in the .profile file on the DNCS.

Possible Error Condition

System operators who see the following message when running the emmlst utility should call Cisco Services immediately:
EMM distributor is not logging at this time.

Important: This message indicates that the emmDistributor process is not running. If the emmDistributor process is not running, the system is not updating DHCTs with EMMs. If this problem is not corrected, DHCTs may lose authorization for secure services.

6

Reboot DHCTs or Obtain Sign-on Data with the listQpsk Utility

Introduction

The listQpsk utility provides system operators and support engineers with the following capabilities:

- The ability to reboot DHCTs assigned to a specific Quadrature Phase-Shift Keying (QPSK) modulator
- A means for finding out how many DHCTs are signed on to the network through each modulator in the system

The information in this chapter provides instructions and examples for running the listQpsk utility.

In This Chapter

Run the listQpsk Utility

Introduction

When DHCTs sign on to the network, each DHCT is assigned to a specific QPSK modulator. System operators and support engineers can use the listQpsk utility to reboot DHCTs or to examine DHCT signon data.

Note: The output of the listQpsk utility uses the terms signon data or SignOn when referring to the number of DHCTs assigned to each QPSK.

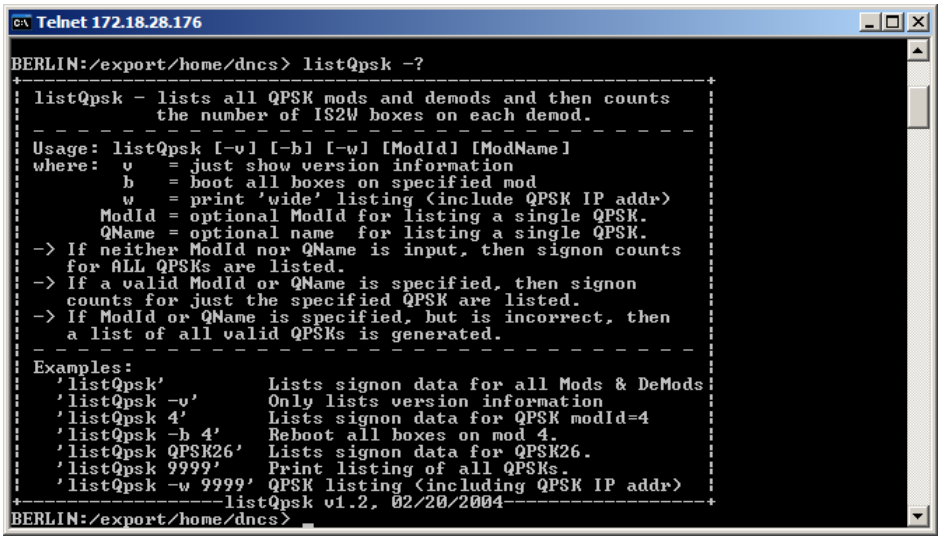
The information in the following sections, provide detailed instructions and examples for running the listQpsk utility.

Displaying the listQpsk Help Window

Use this procedure to display a window detailing the various options with which the listQpsk utility can be run.

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

2 Type **listQpsk -?** and then press **Enter**. The system displays the options you can use when you run the listQpsk utility.



Rebooting DHCTs

Follow these instructions to use the listQpsk utility to reboot DHCTs.

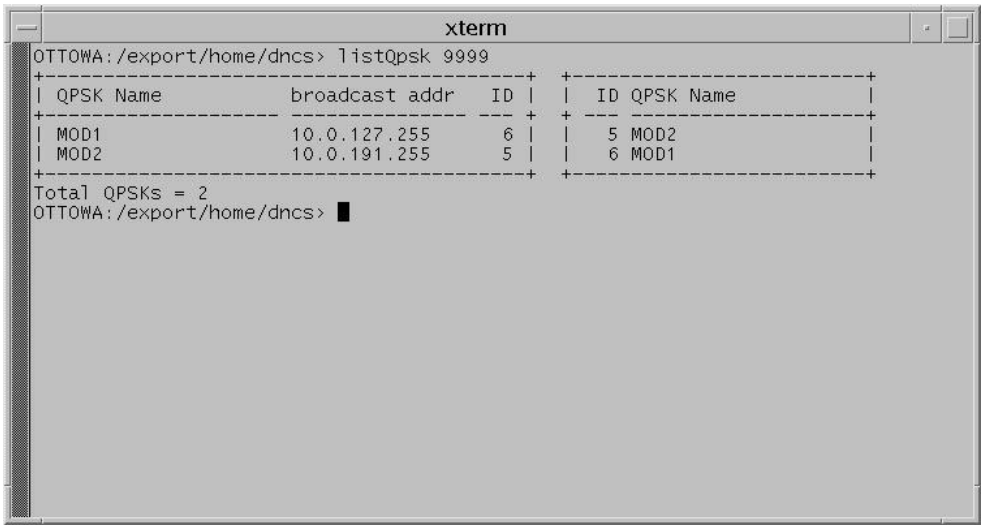
Important: Service to subscribers is interrupted while the DHCT reboots.

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

2 Do you know the modulator name or modulator ID associated with the DHCTs that you want to reboot?

- If **yes**, go to step 3.
- If **no**, follow these instructions.

  a Type **listQpsk 9999** and then press **Enter**. The system lists all QPSK modulators by name and ID.



  b Note the modulator name or ID associated with the DHCTs that you want to reboot.

3 Type **listQpsk -b [modulator ID or modulator name]** and then press **Enter**.

Note: Substitute the ID or the name of the QPSK modulator for [modulator ID or modulator name].

Example: Type **listQpsk -b QPSK1** and then press **Enter**.

Result: The utility displays a message similar to the following:

I plan to Reboot all boxes on QPSK '[modulator name or modulator ID]' (using [broadcast address]).
Do you want to continue? (Y/N)

4 Type **y** and then press **Enter**. The system reboots the DHCTs assigned to the specified modulator.

Displaying DHCT Sign-on Data for All QPSK Modulators and Demodulators

Follow these instructions to use the listQpsk utility to display DHCT sign-on data for all QPSK modulators and demodulators.

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

2 Type **listQpsk** and then press **Enter**.

Result: The xterm window updates to list the following information:

- Each QPSK, identified by ID and name
- The demodulators associated with each modulator
- The number of IS2W DHCTs associated with each QPSK

  Note: IS2W is an acronym for *in-service, two-way*. This figure represents the number of DHCTs that have attempted to sign on to the network through the associated QPSK.
- The number and percentage of DHCTs that have successfully signed on to the network through each QPSK

ID	QPSK Name	Demod	IS2W	SignOn	% SignOn
72	QPSK1	--	26444	26581	100

70	QPSK2	--	61297	61464	100

129	QPSK3	--	0	0	--

88	QPSK4	--	1258	1280	101

57	QPSK5	--	4130	4149	100

29	QPSK6	--	0	0	--
29	QPSK6	1	1075	1035	96
29	QPSK6	2	2032	1971	96
29	QPSK6	3	1164	1130	97
29	QPSK6	4	1176	1144	97
29	QPSK6	5	351	331	94
29	QPSK6	6	0	0	--

Note: QPSK modulators without an associated demodulator have been assigned DHCTs that use the DOCSIS sign-on method. DHCTs that use the DOCSIS method to sign on to the network do not require a demodulator.

Displaying DHCT Sign-on Data for a Specific QPSK Modulator

Follow these instructions to use the listQpsk utility to display DHCT sign-on data for a specific QPSK modulator.

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

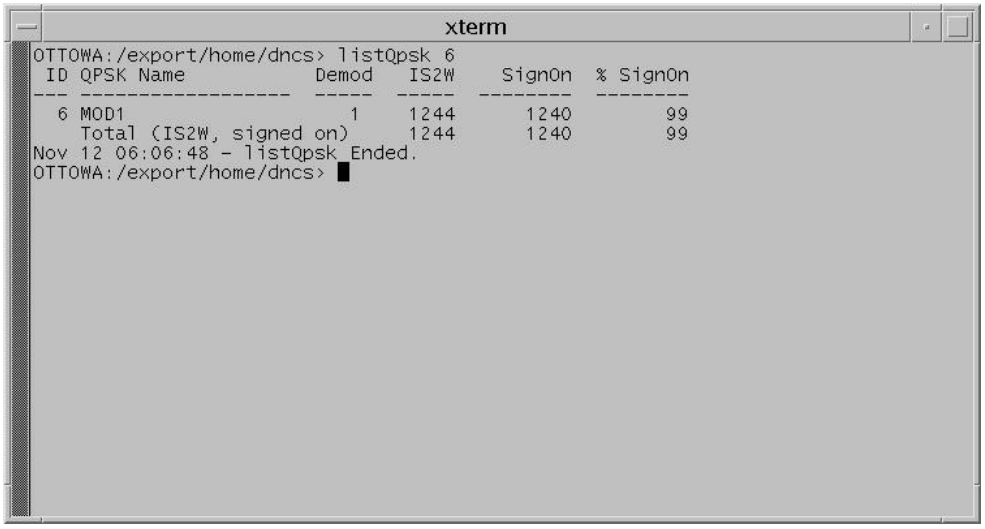
2 Choose one of the following options:

- To display DHCT sign-on data for a QPSK identified by modulator ID, go to step 3.
- To display DHCT sign-on data for a QPSK identified by modulator name, go to step 4.

3 Type **listQpsk [modulator ID]** and then press **Enter**. The xterm window updates to display DHCT sign-on data for the selected QPSK.

Note: Substitute the QPSK modulator ID for [modulator ID].

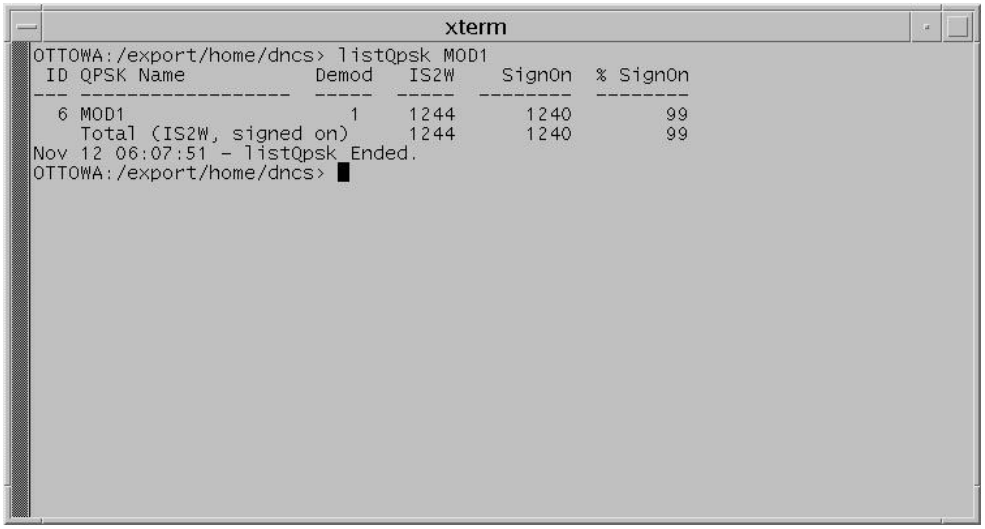
Example: Type **listQpsk 6** and then press **Enter** to obtain a list of DHCT sign-on data for a QPSK with a modulator ID of 6.



4 Type **listQpsk [modulator name]** and then press **Enter**. The xterm window updates to display DHCT sign-on data for the selected QPSK.

Note: Substitute the QPSK modulator name for [modulator name].

Example: Type **listQpsk MOD1** and then press **Enter** to obtain a list of DHCT sign-on data for a QPSK with a modulator name of MOD1.



Displaying a List of All QPSKs

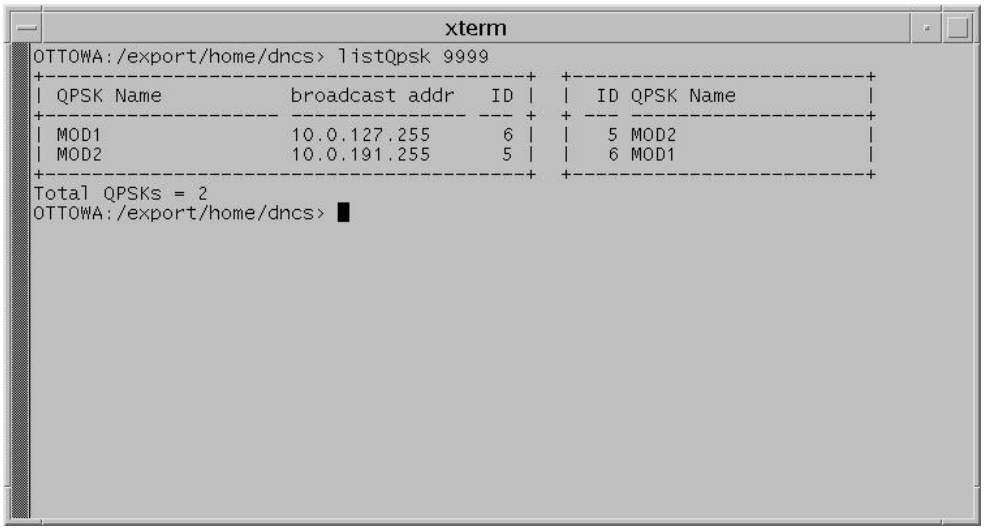
Follow these instructions to display a list of all QPSKs in the system.

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

2 Choose one of the following options:

- To list each QPSK by name, broadcast address, and ID, go to step 3.
- To list each QPSK using wide format, whereby the QPSK IP address is listed, in addition to the QPSK name, broadcast address, and ID, go to step 4.

3 Type **listQpsk 9999** and then press **Enter**. The xterm window updates to list each QPSK by name, broadcast address, and ID.



Note: The output displays two parallel lists. The list on the left contains QPSKs sorted alphabetically by name. The list on the right contains QPSKs sorted numerically by ID.

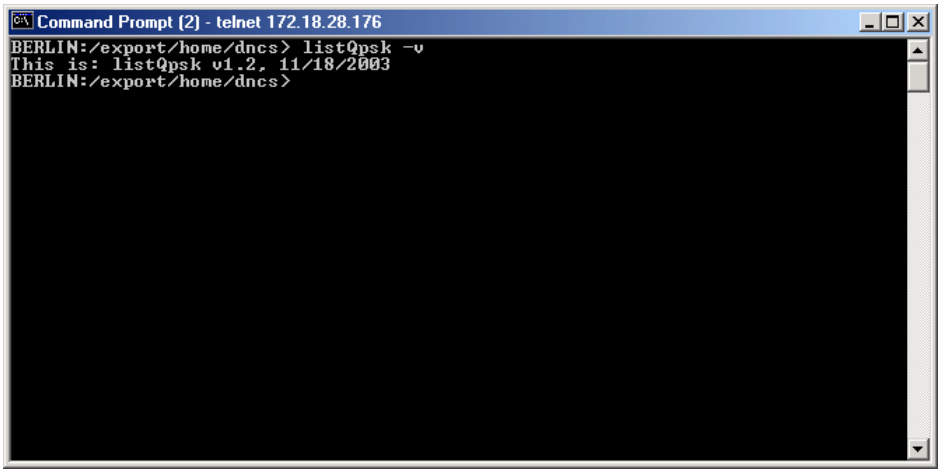
4 Type **listQpsk -w 9999** and then press **Enter**. The system lists each QPSK, identified by name, broadcast address, ID, and IP address in wide format.

Displaying the Version Number of the listQpsk Utility

Use these instructions to display the version number of the listQpsk utility.

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

2 To display the version number of the listQpsk utility on your system, type **listQpsk -v** and then press **Enter**. The xterm window updates to display the version number of the listQpsk utility.



7

Transmit DHCT Billing Transactions with the IIH Utility

Introduction

System operators and support engineers can use the IIH utility to transmit the following four types of billing transactions to DHCTs:

- dhctInstantHit
- resetClientNvm
- bootDhct
- setPin

These transactions can be transmitted to an individual DHCT, a list of DHCTs, DHCTs supported by a specific Quadrature Phase-Shift Keying (QPSK) modulator or demodulator, or a specific model number of DHCT. This chapter contains details of the four types of billing transactions supported by the IIH utility, as well as instructions and examples on using the utility.

Note: Each of these transactions can be run using a list of DHCTs. Each DHCT in the list is identified by MAC address. System operators typically prepare the list of DHCTs beforehand by using any text editor, such as vi. Instructions for preparing the list of DHCTs are found in ***Prepare a Text File*** (on page 49).

In This Chapter

Four Billing Transactions

The IIH utility was developed to transmit four separate billing transactions to DHCTs. The system determines which billing transaction you want to transmit through the specific parameters you use when you run the IIH utility. The following list contains the four billing transactions, as well as the identifying parameter(s):

- dhctInstantHit-specified by the *-i* parameter
- resetClientNvm-specified by the *-r* parameter

  Note: The *-r* parameter is only supported by sites that use the SARA Application Server.
- bootDhct-specified by the *-b* parameter
- setPin-specified by the *-bp* and *-pp* parameters

Each transaction is discussed in some detail in the remainder of this section.

dhctInstantHit

The dhctInstantHit transaction refreshes DHCTs with their Entitlement Management Messages (EMMs).

Note: EMMs are encrypted packets of information that the DNCS uses to supply secured service authorizations to DHCTs. EMMs enable DHCTs to use many digital and interactive broadcast services.

resetClientNvm

The resetClientNvm transaction resets the non-volatile memory (NVM) of a DHCT to default values established at the factory.

Note: While the resetClientNvm transaction can be run to reset the NVM of DHCTs associated with a specific QPSK modulator or demodulator, the need to use this application in this manner is unlikely.

bootDhct

The bootDhct transaction is used to reboot a single DHCT, a list of DHCTs, or DHCTs associated with a specific QPSK.

setPin

The setPin transaction is used to reset two possible personal identification numbers (PINs) configured on the DHCT:

- The blocking PIN is used to restrict access to specific channels.
- The PPV PIN is used to authenticate the purchase of a pay-per-view (PPV) movie.

Prepare a Text File

The four individual transactions supported by the IIH utility can act upon a single DHCT or upon a group of DHCTs. When processing a group of DHCTs, system operators will find it advantageous to input to the IIH utility a list of DHCT MAC addresses as contained in a text file. The information in this section provides guidelines and instructions for preparing the text file of MAC addresses.

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 per line.

  Important: MAC addresses must be in hexadecimal format, and any letter characters must be uppercase.

  Example: 00:02:DE:4A:11:92
  00:02:DE:4A:11:93
  00:02:DE:4A:11:94

- Each MAC address or serial number must be left-justified on each line of text.

  Note: A MAC address contains 17 characters. The IIH utility reads only the first 17 characters of each line. Any additional characters per line are ignored and are treated as comments.

- 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.

  Example: iih-in_11.13.02 for a file that was created on November 13, 2002.

- Our engineers recommend that you save the file to the /tmp directory on the DNCS. However, files in the /tmp directory are lost whenever the DNCS reboots. Store the file here only for one-time use.

Preparing a Text File

Follow these instructions to prepare a text file for use with the IIH utility.

Important: These instructions use the vi text editor as an example. The vi text editor is not intuitive. These instructions are not a 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: Our engineers recommend 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.

   Example: vi iih-in_11.31.02
4. Insert your list of MAC addresses into the file you have just opened.

   Note: Use the guidelines set forth in ***Guidelines for Preparing the Text File*** (on page 49).

   Important: Type only one MAC address per line.
5. Save the file and close the vi editor.

Display the IIH Utility Help Window and Version Number

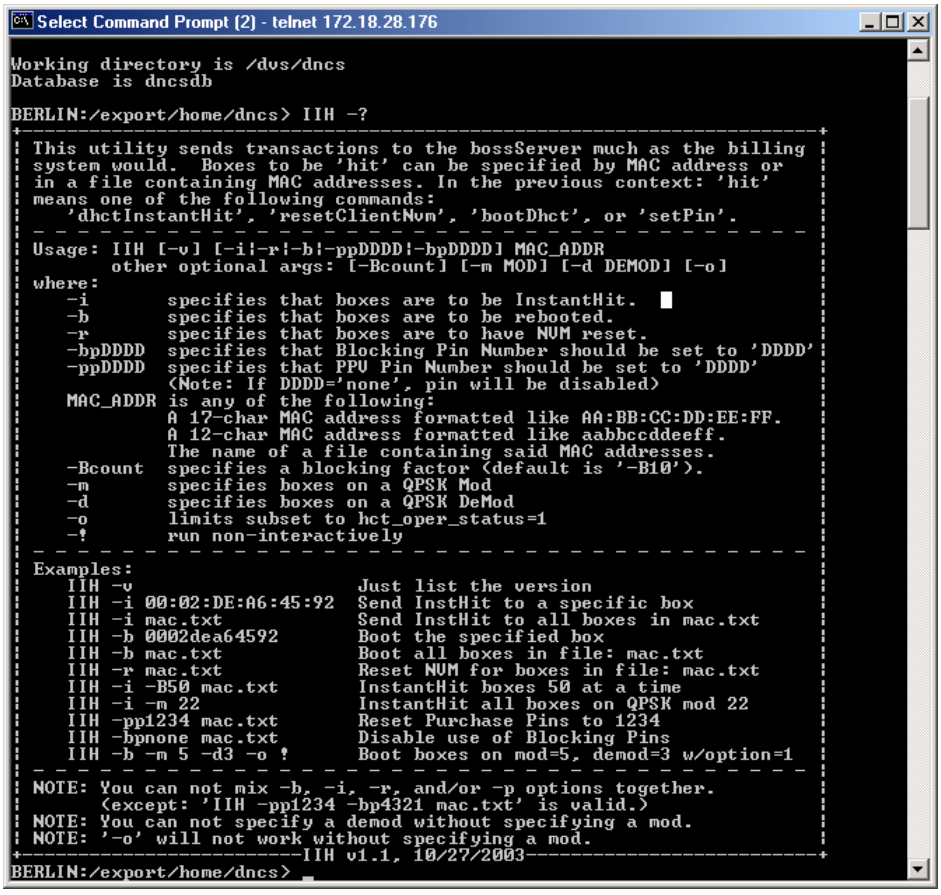
The IIH utility can be configured to send four separate billing transactions to DHCTs. Each transaction is identified by the system through specific parameters that are used in conjunction with the IIH utility. In addition to supporting four billing transactions, the IIH utility can be run to display a help window, as well as a window that displays the current version number of the utility. The IIH help window is especially useful in that it shows specific examples of how the IIH utility can be used. The remainder of this section provides detailed instructions on running the IIH utility.

Displaying the IIH Utility Help Window

The IIH help window displays all of the parameters that can be used in running the IIH utility. Follow these instructions to display the IIH help window.

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

2 Type **IIH -?** and then press **Enter**. The IIH help window opens.



Displaying the IIH Utility Version Number

Follow these instructions to display the version number of the IIH utility loaded onto your system.

1. If necessary, open an xterm window on the DNCS.
2. Type **IIH -v** and then press **Enter**. The system displays the version number of the IIH utility loaded onto your system.

What's Next

Choose one of the following options:

- To refresh DHCT EMMs, see ***Refresh DHCT EMMs With the dhctInstantHit Transaction*** (on page 53).
- To reset the DHCT NVM, see ***Reset DHCT NVM With the resetClientNvm Transaction*** (on page 56).
- To reboot a DHCT, see ***Reboot a DHCT With the bootDhct Transaction*** (on page 58).
- To reset the DHCT PIN number, see ***Reset DHCT PINs With the setPin Transaction*** (on page 61).

Refresh DHCT EMMs with the dhctInstantHit Transaction

The dhctInstantHit transaction refreshes DHCTs with EMMs from the database. The following procedures provide detailed instructions for sending a dhctInstantHit transaction to an individual DHCT, DHCTs contained in a list, DHCTs associated with a specific QPSK modulator or demodulator, or DHCTs of a specific model type.

Refreshing the EMMs of an Individual DHCT

Follow these instructions to refresh the EMMs of an individual DHCT.

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

2 Type **IIH -i [DHCT MAC address]** and then press **Enter**. The system refreshes the specified DHCT with its EMMs.

Notes:

- Substitute the MAC address of the DHCT for [DHCT MAC address].
- The MAC address can be formatted with or without colons (:).

Examples:

- **IIH -i 00:02:DE:A6:45:92**
- **IIH -i 0002DEA64592**

Refreshing the EMMs of a List of DHCTs

Follow these instructions to refresh the EMMs of a list of DHCTs. You should already have prepared the list of DHCTs, identified by MAC address, according to the guidelines and instructions in ***Prepare a Text File*** (on page 49).

Note: When the IIH utility processes a list of DHCTs, ten DHCTs are processed at a time, by default. The reason ten DHCTs are processed at a time is to avoid monopolizing the bossServer process of the DNCS. If you have an urgent need to process more than ten DHCTs at a time, you can override the default value through use of the -C parameter.

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

2 Do you want to force the system to process more than ten DHCTs at a time?

- If **yes**, type **IIH -i -C[# of DHCTs] [text file name]** and then press **Enter**.

  Notes:

  – Substitute the number of DHCTs you want to process at once for [# of DHCTs].

  – Substitute the name (including path) of the text file for [text file name].

  Example: IIH -i -C50 /tmp/iih-in_11.31.02

- If **no**, type **IIH -i [text file name]** and then press **Enter**.

  Note: Substitute the name (including path) of the text file for [text file name].

  Example: IIH -i /tmp/iih-in_11.31.02

Result: A confirmation message, similar to the following, appears:

DHCTs listed in file "[filename]" will be Instant-Hit …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N) y

3 Type **y** and then press **Enter**. The system lists the MAC addresses of the DHCTs as it sends a dhctInstantHit transaction to each one.

Refreshing the EMMs of DHCTs Associated with a QPSK Modulator or Demodulator

The dhctInstantHit transaction can be configured to refresh the EMMs of DHCTs associated with a specific QPSK modulator or demodulator. Follow these instructions to refresh the EMMs of DHCTs associated with a specific modulator or demodulator.

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

2 Choose one of the following options:

- To send a dhctInstantHit transaction to DHCTs associated with a specific modulator, type **IIH -i -m [modulator ID]** and then press **Enter**.
- To send a dhctInstantHit transaction to DHCTs associated with a specific demodulator, type **IIH -i -m [modulator ID] -d [demodulator ID]** and then press **Enter**.

  Important: You must also specify a modulator when you specify a demodulator.

Note: Substitute the ID of the modulator or demodulator for [modulator ID] and/or [demodulator ID].

Examples:

- **IIH -i -m 22**
- **IIH -i -m 22 -d 8**

Result: The system sends a dhctInstantHit transaction to each DHCT associated with the specific modulator or demodulator.

Refreshing the EMMs of DHCTs of a Specific Model Number

The dhctInstantHit transaction can be configured to refresh the EMMs of a specific model number of DHCT. Follow these instructions to refresh the EMMs of DHCTs of a specific model number.

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

2 Type **IIH -i -M[model number]** and then press **Enter**.

Note: Substitute the model number of DHCT for [model number].

Example: IIH -i -M2100

Result: A confirmation message, similar to the following, appears:

DHCTs with DHCT Model=[model number] will be Instant-Hit …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)

3 Type **y** and then press **Enter**. The system sends a dhctInstantHit transaction to each DHCT of the specified model number.

Reset DHCT NVM with the resetClientNvm Transaction

The resetClientNvm transaction resets the non-volatile memory (NVM) of a DHCT to default settings established at the factory. The procedures in this section provide detailed instructions on resetting the NVM of an individual DHCT, a list of DHCTs, or DHCTs of a specific model number.

Note: The *-r* option, which is used to reset the NVM, is not a valid option at sites that use the Aptiv Digital application server. The *-r* option is valid only at sites that use the SARA Application Server. When the *-r* option is used at a site that uses the Aptiv Digital application server, the system displays the following message:
'r' function is not supported by Pioneer AppServer
(assumed since saManager is not running)

Resetting the NVM of an Individual DHCT

Follow these instructions to reset the NVM of an individual DHCT.

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

2 Type **IIH -r [DHCT MAC address]** and then press **Enter**. The system resets the NVM of the specified DHCT.

Notes:

- Substitute the MAC address of the DHCT for [DHCT MAC address].
- The MAC address can be formatted with or without colons (:).

Examples:

- **IIH -r 00:02:DE:A6:45:92**
- **IIH -r 0002DEA64592**

Resetting the NVM of a List of DHCTs

Follow these instructions to reset the NVM of a list of DHCTs. You should already have prepared the list of DHCTs, identified by MAC address, according to the guidelines and instructions in ***Prepare a Text File*** (on page 49).

Note: When the IIH utility processes a list of DHCTs, the transaction processes ten DHCTs at a time, by default. The reason ten DHCTs are processed at a time is to avoid monopolizing the bossServer process of the DNCS. If you have an urgent need to process more DHCTs than ten at a time, you can override the default value through use of the *-C* parameter.

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

2 Do you want to force the system to process more than ten DHCTs at a time?

- If **yes**, type **IIH -r -C[# of DHCTs] [text file name]** and then press **Enter**.

  Notes:

  – Substitute the number of DHCTs you want to process at once for [# of DHCTs].

  – Substitute the name (including path) of the text file for [text file name].

  Example: IIH -r -C50 /tmp/iih-in_11.31.02

- If **no**, type **IIH -r [text file name]** and then press **Enter**.

  Note: Substitute the name (including path) of the text file for [text file name].

  Example: IIH -r /tmp/iih-in_11.31.02

Result: A confirmation message, similar to the following, appears:

DHCTs listed in file "[filename]" will be NVM reset …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N) y

3 Type **y** and then press **Enter**. The system lists the MAC addresses of the DHCTs as it sends a resetClientNvm transaction to each.

Resetting the NVM of DHCTs of a Specific Model Number

The resetClientNvm transaction can be configured to reset the NVM of a specific model number of DHCT. Follow these instructions to reset the NVM of DHCTs of a specific model number.

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

2 Type **IIH -r -M[model number]** and then press **Enter**.

Note: Substitute the model number of DHCT for [model number].

Example: IIH -r -M2100

Result: A confirmation message, similar to the following, appears:

saManager is running
DHCTs with DHCT model=[model number] will be NVM-Reset
 # MAC addresses will be involved.
Do you want to continue (Y/N)?

3 Type **y** and then press **Enter**. The system resets the NVM of the specified DHCTs.

Reboot a DHCT with the bootDhct Transaction

The bootDhct transaction reboots a single DHCT, a list of DHCTs, DHCTs associated with a specific QPSK, or DHCTs of a specific model number. Follow these instructions to configure the IIH utility to send a bootDhct transaction.

Rebooting an Individual DHCT

Follow these instructions to reboot an individual DHCT.

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

2 Type **IIH -b [DHCT MAC address]** and then press **Enter**. The system reboots the specified DHCT.

Notes:

- Substitute the MAC address of the DHCT for [DHCT MAC address].
- The MAC address can be formatted with or without colons (:).

Examples:

- **IIH -b 00:02:DE:A6:45:92**
- **IIH -b 0002DEA64592**

Rebooting a List of DHCTs

Follow these instructions to reboot a list of DHCTs. You should already have prepared the list of DHCTs, identified by MAC address, according to the guidelines and instructions in ***Prepare a Text File*** (on page 49).

Note: When the IIH utility processes a list of DHCTs, it processes ten DHCTs at a time, by default. The reason ten DHCTs are processed at a time is to avoid monopolizing the bossServer process of the DNCS. If you have an urgent need to process more DHCTs than ten at a time, you can override the default value through use of the *-C* parameter.

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

2 Do you want to force the system to process more than ten DHCTs at a time?

- If **yes**, type **IIH -b -C[# of DHCTs] [text file name]** and then press **Enter**.

  Notes:

  – Substitute the number of DHCTs you want to process at once for [# of DHCTs].

  – Substitute the name (including path) of the text file for [text file name].

  Example: IIH -b -C50 /tmp/iih-in_11.31.02

- If **no**, type **IIH -b [text file name]** and then press **Enter**.

  Note: Substitute the name (including path) of the text file for [text file name].

  Example: IIH -b /tmp/iih-in_11.31.02

Result: A confirmation message, similar to the following, appears:

DHCTs listed in file "[filename]" will be Rebooted …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N) y

3 Type **y** and then press **Enter**. The system lists the MAC addresses of the DHCTs as it sends a bootDhct transaction to each.

Rebooting DHCTs Associated with a QPSK Modulator or Demodulator

Follow these instructions to reboot DHCTs associated with a specific QPSK modulator or demodulator.

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

2 Choose one of the following options:

- To reboot DHCTs associated with a specific modulator, type **IIH -b m [modulator ID]** and then press **Enter**.
- To reboot DHCTs associated with a specific demodulator, type **IIH -b -m [modulator ID] -d [demodulator ID]** and then press **Enter**.

  Important: You must also specify a modulator when you specify a demodulator.

Note: Substitute the ID of the modulator and/or demodulator for [modulator ID] and [demodulator ID].

Examples:

- **IIH -b -m 22**
- **IIH -b -m 22 -d 8**

Result: The system reboots the DHCT associated with the specific modulator or demodulator.

Rebooting DHCTs of a Specific Model Number

Follow these instructions to reboot DHCTs of a specific model number.

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

2 Type **IIH -b -M[model number]** and then press **Enter**.

Note: Substitute the model number of DHCT for [model number].

Example: IIH -b -M2100

Result: A confirmation message, similar to the following, appears:

saManager is running
DHCTs with DHCT model=[model number] will be Rebooted
 # MAC addresses will be involved.
Do you want to continue (Y/N)?

3 Type **y** and then press **Enter**. The system reboots the specified DHCTs.

Reset DHCT PINs with the setPin Transaction

Subscribers who use our DHCTs have two personal identification numbers (PIN) they can use to enhance their digital interactive services. One PIN can be set to limit access to specific channels. Another PIN can be used to authenticate PPV purchases.

Notes:

- The PIN used to restrict access to specific channels is often referred to as the blocking PIN.
- The PIN used to authenticate PPV purchases is often referred to as the PPV PIN.

Follow the instructions in this section to reset the blocking and/or PPV PIN(s).

Resetting the PINs of Individual DHCTs

Follow these instructions to reset the PINs of individual DHCTs.

1. If necessary, open an xterm window on the DNCS.
2. Choose one of the following options:
   - To reset the blocking PIN, go to step 3.
   - To reset the PPV PIN, go to step 4.
3. To reset the blocking PIN of an individual DHCT, choose one of the following options:
   - Type **IIH -bp[####] [DHCT MAC address]** and then press **Enter** to reset the blocking pin to [####].

     Notes:

     – Substitute the new PIN for [####].

     – Substitute the MAC address of the DHCT for [DHCT MAC address].

     Examples:

     – **IIH -bp1234 00:02:DE:A6:45:92**

     – **IIH -bp1234 0002DEA64592**
   - Type **IIH -bpnone [DHCT MAC address]** and then press **Enter** to stipulate that the blocking PIN be disabled on this specific DHCT.

     Note: Substitute the MAC address of the DHCT for [DHCT MAC address].

     Examples:

     – **IIH -bpnone 00:02:DE:A6:45:92**

     – **IIH -bpnone 0002DEA64592**

4 To reset the PPV PIN of an individual DHCT, choose one of the following options:

- Type **IIH -pp[####] [DHCT MAC address]** and then press **Enter** to reset the PPV pin to [####].

  Notes:

  – Substitute the new PIN for [####].

  – Substitute the MAC address of the DHCT for [DHCT MAC address].

  Examples:

  – **IIH -pp1234 00:02:DE:A6:45:92**

  – **IIH -pp1234 0002DEA64592**

- Type **IIH -ppnone [DHCT MAC address]** and then press **Enter** to stipulate that the PPV PIN be disabled on this specific DHCT.

  Note: Substitute the MAC address of the DHCT for [DHCT MAC address].

  Examples:

  – **IIH -ppnone 00:02:DE:A6:45:92**

  – **IIH -ppnone 0002DEA64592**

Resetting the PINs of a List of DHCTs

Follow these instructions to reset the PINs of a list of DHCTs.

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

2 Choose one of the following options:

- To reset the blocking PIN, go to step 3.
- To reset the PPV PIN, go to step 4.

3 To reset the blocking PIN for a list of DHCTs, choose one of the following options:

- Type **IIH -bp[####] [text file name]** and then press **Enter** to reset the blocking PIN to [####].

  Notes:

  – Substitute the new PIN for [####].

  – Substitute the name (including path) of the text file for [text file name].

  Example: IIH -bp1234 /tmp/iih-in_11.31.02

- Type **IIH -bpnone [text file name]** and then press **Enter** to stipulate that the blocking PIN be disabled for the list of DHCTs.

  Note: Substitute the name (including path) of the text file for [text file name].

  Example: IIH -bpnone /tmp/iih-in_11.31.02

4 To reset the PPV PIN for a list of DHCTs, choose one of the following options:

- Type **IIH -pp[####] [text file name]** and then press **Enter** to reset the PPV pin to [####].

  Notes:

  – Substiltute the new PIN for [####].

  – Substitute the name (including path) of the text file for [text file name].

  Example: IIH -pp1234 /tmp/iih-in_11.31.02

- Type **IIH -ppnone [text file name]** and then press **Enter** to stipulate that the PPV PIN be disabled for the list of DHCTs.

  Note: Substitute the name (including path) of the text file for [text file name].

  Example: IIH -ppnone /tmp/iih-in_11.31.02

Resetting the PINs of DHCTs of a Specific Model Number

Follow these instructions to reset the PINs of DHCTs of a specific model number.

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

2 Choose one of the following options:

- To reset the blocking PIN, go to step 3.
- To reset the PPV PIN, go to step 4.

3 To reset the blocking PIN for DHCTs of a specific model number, choose one of the following options:

- Type **IIH -bp[####] -M[model number]** and then press **Enter** to reset the blocking pin to [####].

  Notes:

  – Substitute the new PIN for [####].

  – Substitute the model number of DHCTs for [model number].

  Example: IIH -bp1234 -M2100

- Type **IIH -bpnone -M[model number]** and then press **Enter** to stipulate that the blocking PIN be disabled for DHCTs of the specified model number.

  Note: Substitute the model number of DHCTs for [model number].

  Example: IIH -bpnone -M2100

4 To reset the PPV PIN for DHCTs of a specific model number, choose one of the following options:

- Type **IIH -pp[####] -M[model number]** and then press **Enter** to reset the PPV PIN to [####].

  Notes:

  – Substitute the new PIN for [####].

  – Substitute the model number of DHCTs for [model number].

  Example: IIH -pp1234 -M2100

- Type **IIH -ppnone -M[model number]** and then press **Enter** to stipulate that the PPV PIN be disabled for DHCTs of the specified model number.

  Note: Substitute the model number of DHCTs for [model number].

  Example: IIH -ppnone -M2100

8

Change DHCT Status to Out-of-Service with the 2way2oos Utility

Introduction

System operators sometimes need a way to reclaim IP addresses of DHCTs that have been disconnected but never officially changed to "out-of-service" in the database. A DHCT that is no longer in use must have a status of out-of-service in the database in order for the system operator to use the IP address of the DHCT again. Systems that do not reclaim these IP addresses may run out of IP addresses when they try to deploy new DHCTs in the homes of subscribers.

The 2way2oos utility was developed to change the status of DHCTs to out-of-service in the database. System operators prepare a text file that contains a list of MAC addresses of DHCTs that they want to change to out-of-service and then use this text file as a parameter when they run the 2way2oos utility. The instructions in this chapter provide guidelines for preparing the text file and for running the 2way2oos utility.

In This Chapter

Prepare the Text File

System operators who want to use the 2way2oos utility to change the database status of DHCTs to out-of-service must first prepare a text file that contains the MAC address of each DHCT that must be changed. This section contains guidelines and instructions for preparing the text file.

Guidelines for Preparing the Text File

Use the following guidelines when preparing the text file:

- Prepare the file using a standard text editor, such as vi.
- Prepare the file with one MAC address per line.

  Important: MAC addresses must be in hexadecimal format, and any letter characters must be uppercase.

  Example: 00:02:DE:4A:11:92
  00:02:DE:4A:11:93
  00:02:DE:4A:11:94

- Each MAC address must be left-justified on each line of text.
- The file must be saved in the /dvs/dncs/tmp directory of the DNCS and must be named 2way2oos.txt.

  Important: The file **must** be saved to the specified directory under the specified name. The directory path and file name *are hard-coded* as part of the utility.

Preparing the Text File

Follow these instructions to prepare the text file for use with the 2way2oos utility.

Important: These instructions use the vi text editor as an example. The vi text editor is not intuitive. These instructions are not a substitute for a good working knowledge of the vi text editor.

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.

   Note: The file **must** be saved to the /dvs/dncs/tmp directory of the DNCS.
3. Type **vi 2way2oos.txt** and then press **Enter**. The file opens for editing.
4. Insert your list of MAC addresses into the file you have just opened.

   Note: Use the guidelines set forth in ***Guidelines for Preparing the Text File*** (on page 66).

   Important: Type only one MAC address per line.
5. Save the file and close the vi editor.

Run the 2way2oos Utility

Before running the 2way2oos utility, be sure that you have followed the instructions in Prepare the Text File, and you have properly created and saved the file of MAC addresses that is to be used as input for the 2way2oos utility.

Be sure of the following important points:

- The file must contain only one MAC address per line.
- The file must be saved in the /dvs/dncs/tmp directory.
- The file must be named 2way2oos.txt.

Note: As a further precaution, system operators may want to examine the file before running the 2way2oos utility to ensure that the file contains only those MAC addresses of DHCTs that are to be marked out-of-service in the database.

Running the 2way2oos Utility

Follow these instructions to run the 2way2oos utility.

1. If necessary, open an xterm window on the DNCS.
2. Type **2way2oos.ksh** and then press **Enter**. A message similar to the following appears:

   ## Total Settops to process
   This could take approximately #.### hrs to complete.
   Do you want to continue? (y/n)

   Note: The number of DHCTs and the length of time it takes to process them varies depending upon the number of DHCTs you have included in your text file.
3. Type **y** and then press **Enter**.

   Results:

   - The **Beginning processing MAC addresses** message appears.
   - The **All MACs have been processed** message appears when the utility has finished running.
4. Go to *Stop and Restart the HCT Manager Process* (on page 68).

   Note: You need to stop and restart the HCT Manager process to make the IP addresses available for reuse.

Stop and Restart the HCT Manager Process

You need to stop and restart the HCT Manager process on the DNCS in order to reclaim the IP addresses associated with the DHCTs in your text file. The instructions in this section guide you through the steps of stopping and restarting the HCT Manager process.

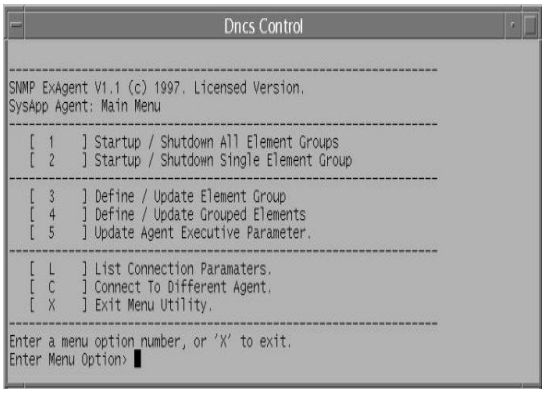
Note: Stopping and then restarting a process is often referred to as "bouncing" the process.

Stopping the HCT Manager Process

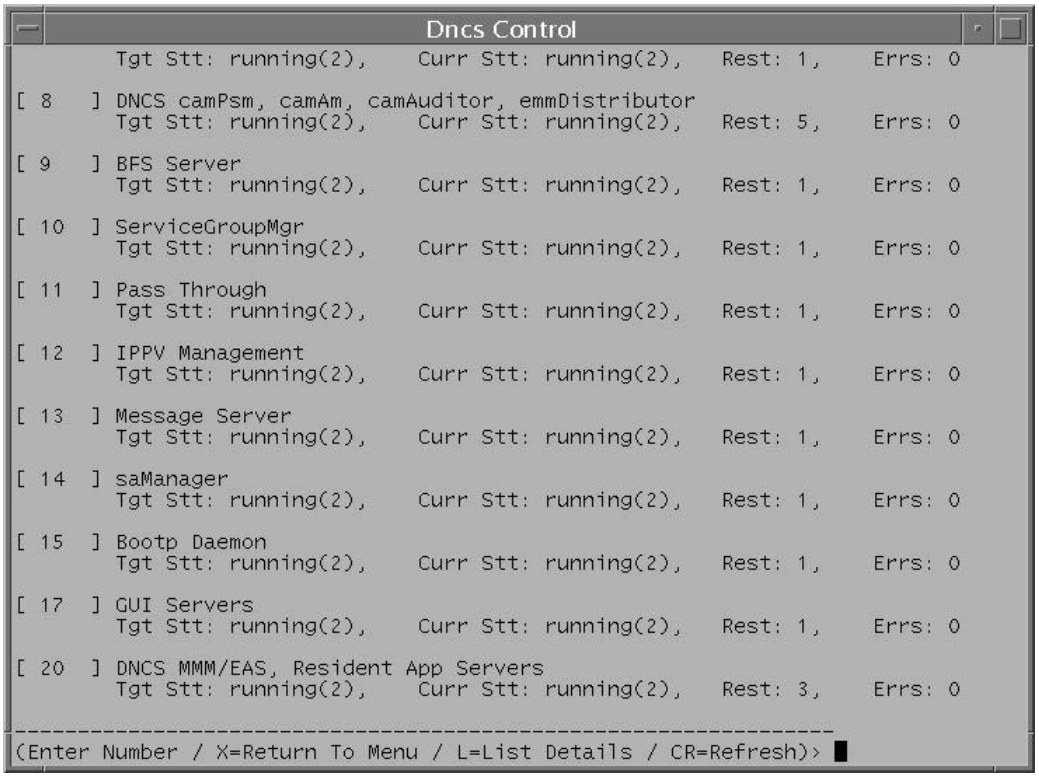
Follow these instructions to stop the HCT Manager process on the DNCS.

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

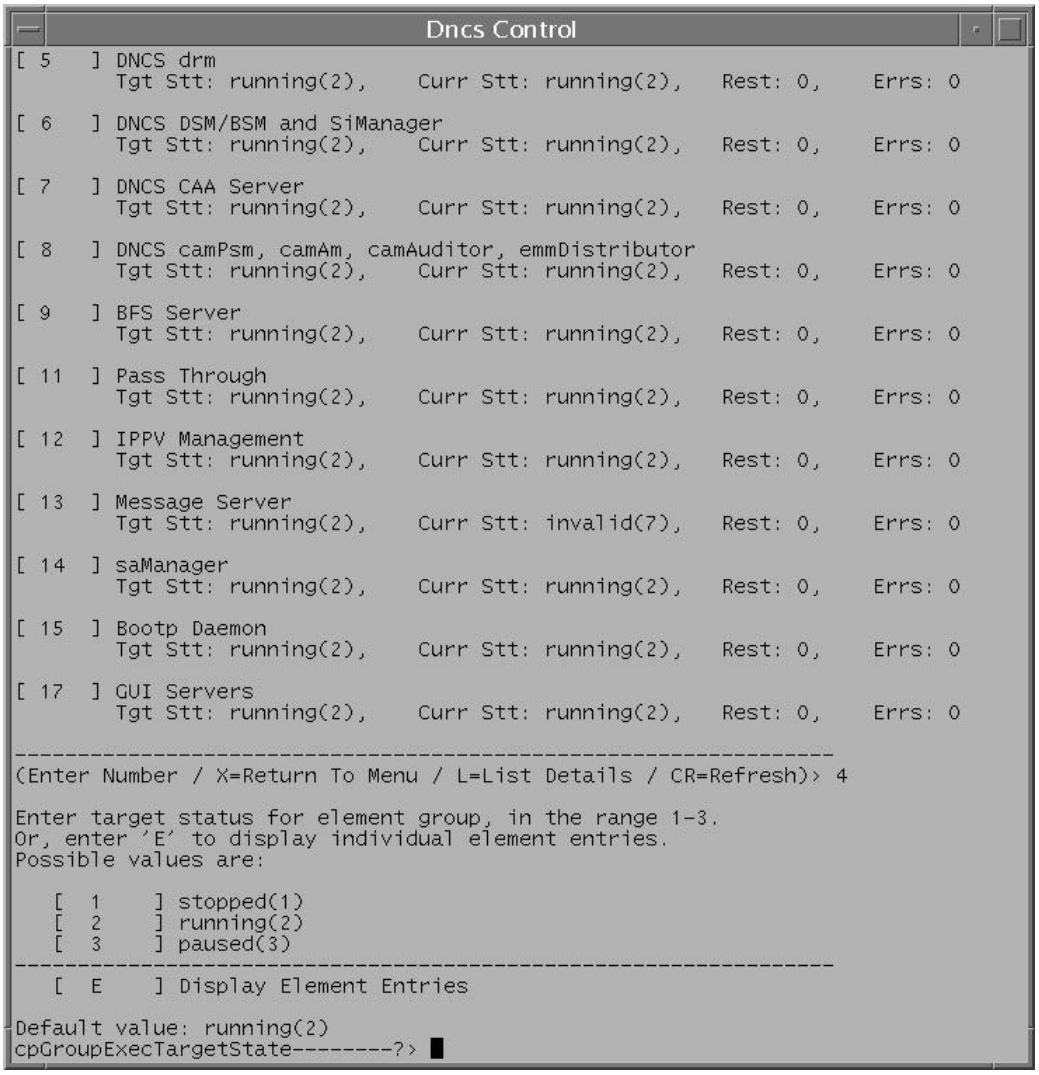
2 Type **dncsControl** and then press **Enter**. The Dncs Control window opens.



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



4 Type the number associated with **DNCS HCT Manager & OSM** and then press **Enter**. The Dncs Control window updates to display a message that instructs you to enter the target status for the selected element group, or to type 'E' to display all of the elements in the group.



5 Type **1** (for stopped) and then press **Enter**. A confirmation message appears.

6 Type **y** (for yes) and then press **Enter**. The Dncs Control window updates to list the status of all the processes and servers running on the DNCS.

7 Wait until the current status (Curr Stt) of DNCS HCT Manager & OSM is **stopped**.

Note: The Dncs Control window updates automatically every few seconds or you can press Enter to force an update.

8 When the current status of DNCS HCT Manager & OSM is stopped, go to ***Restarting the HCT Manager Processes*** (on page 71).

Restarting the HCT Manager Process

After stopping the HCT Manager process on the DNCS, follow these instructions to restart the process.

1. Type the number associated with the DNCS HCT Manager & OSM processes and then press **Enter**. The Dncs Control window updates and displays a message that instructs you to enter the target status for the selected element group or to type 'E' to display all of the elements in the group.
2. Type **2** (for running) and then press **Enter**. A confirmation message appears.
3. Type **y** (for yes) and then press **Enter**. The Dncs Control window updates to list the status of all the processes and servers running on the DNCS.
4. Wait until the current status (Curr Stt) of DNCS HCT Manager & OSM is **running**.

   Note: The Dncs Control window updates automatically every few seconds or you can press Enter to force an update.
5. When the current status of the DNCS HCT Manager & OSM processes is **running**, follow the on-screen instructions to close the Dncs Control window.

9

Detach and Attach Submirrors with the mirrState Utility

Introduction

The Sun Enterprise 450 and the Sun Fire V445, V880, and V890 DNCS platforms support disk mirroring. Through disk mirroring, the DNCS stores identical information across sets of hard drives. System operators and support engineers who perform maintenance operations on a Sun Enterprise 450 or the Sun Fire V445, V880, and V890 DNCS may first be required to disable the mirroring functions on the DNCS. Then, after the maintenance operations are complete, the mirroring functions must be re-enabled.

Note: The disabling and re-enabling of the mirroring functions are usually referred to as "detaching" and "re-attaching" the mirrors.

The mirrState utility helps system operators and support engineers detach and re-attach the mirroring functions of the DNCS. Refer to the procedures in this chapter for information on how to run the mirrState utility.

In This Chapter

Run the mirrState Utility

Select one of the following options when you run the mirrState utility:

- To disable the disk mirroring functions, go to ***Detaching Mirrored Disks*** (on page 74).
- To re-enable the disk mirroring functions, go to ***Re-Attaching Mirrored Disks*** (on page 75).
- To obtain the version number of the mirrState utility currently loaded onto the DNCS, go to ***Determining the Version Number of the mirrState Utility*** (on page 75).

Important: The mirrState utility is restricted for use on the Sun Enterprise 450, Sun Fire V445, V880, or V890 DNCS, only. If the mirrState utility is run on a DNCS using another platform (for instance, a Sun Enterprise 250), the system will display a message stating that no metadatabases are found and the utility will exit.

Detaching Mirrored Disks

Follow these instructions to detach the mirrored disks on the Sun Enterprise 450, Sun Fire V445, V880, or V890 DNCS.

1. Has the output of the check_metadevices utility revealed any errors associated with the metadevices on your system?
   - If **yes**, correct those errors before proceeding any further.

     Important: The metadevices on your system must be working correctly before you can detach mirrored disks.
   - If **no**, go to step 2.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type **mirrState.ksh -d** and then press **Enter**. The system displays the following message:

   WARNING!!
   Proceeding beyond this point will DETACH all Controller 2 submirrors.
   Are you certain you want to proceed?
4. Type **y** and then press **Enter**. The system disables the disk mirroring functions on the DNCS.
5. Type **exit** and then press **Enter**. You log out as root user in the xterm window.
6. Perform your maintenance operations on the DNCS and then go to ***Re-Attaching Mirrored Disks*** (on page 75).

Re-Attaching Mirrored Disks

Follow these instructions to use the mirrState utility to re-attach the mirrored disks.

1. If necessary, open an xterm window on the DNCS.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type **mirrState.ksh -a** and then press **Enter**. The system displays the following message:

   WARNING!!
   Proceeding beyond this point will ATTACH all Controller 2 submirrors.
   Are you certain you want to proceed?
4. Type **y** and then press **Enter**. The system re-enables the disk mirroring functions on the DNCS.
5. Type **exit** and then press **Enter**. You log out as root user in the xterm window.

Determining the Version Number of the mirrState Utility

Follow these instructions to obtain the version number of the mirrState utility that is loaded on the DNCS.

1. If necessary, open an xterm window on the DNCS.
2. Type **mirrState.ksh -v** and then press **Enter**. The system displays the version number of the mirrState utility.

10

Convert IP Addresses with the convertIP Utility

Introduction

The DNCS database stores DHCT IP addresses in decimal format, our normal base-10 numbering system. IP addresses, however, are usually displayed in dotted-decimal notation, a format consisting of four 8-bit numbers separated by a dot.

Example: An example of an IP address in dotted-decimal notation is **10.1.64.86**. That very same IP address is stored in the database in decimal format as **167854166**.

The convertIP utility was developed to enable a quick conversion between the two formats. The utility converts an IP address in one format to an IP address in the other format.

Available Options When Running the convertIP Utility

The convertIP utility accepts as an argument either a single IP address, or the name of a file containing a list of IP addresses. In general, use the single IP address when you have only one or two IP addresses to convert. When you have many IP addresses to convert, consider creating a text file that contains the IP addresses that you want to convert.

This chapter provides instructions on preparing the text file, and then describes how to run the convertIP utility.

In This Chapter

Prepare the Text File

System operators who want to use the convertIP utility to convert many IP addresses should prepare a text file beforehand. System operators can then run the convertIP utility with the name of the text file as an argument. This section contains guidelines and instructions for preparing the text file.

Guidelines for Preparing the Text File

Use the following guidelines when preparing the text file:

- Prepare the file using a standard text editor, such as vi.
- Prepare the file with one IP address per line.
- Use either format (decimal or dotted-decimal notation) when preparing the text file. The convertIP utility automatically recognizes the input format and converts the IP address to the other format.

  Note: You can even mix formats in the text file.
- Our engineers recommend that you save the file in the **/dvs/dncs/tmp** directory of the DNCS.

Preparing the Text File

Follow these instructions to prepare the text file for use with the convertIP utility.

Important: These instructions use the vi text editor as an example. The vi text editor is not intuitive. These instructions are not a substitute for a good working knowledge of the vi text editor.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/tmp** and then press **Enter**.

   Note: Our engineers recommend that you save the file in the /dvs/dncs/tmp directory of the DNCS.
3. Type **vi [file name].txt** and then press **Enter**. The file opens for editing.

   Note: Substitute the name of the input file you are creating for [file name].

   Example: Type **vi IP_input_file** and then press **Enter**.
4. Insert your list of IP addresses into the file you have just opened.

   Note: Use the guidelines set forth in ***Guidelines for Preparing the Text File*** (on page 79).
5. Save the file and close the vi editor.

Run the convertIP Utility

To run the convertIP utility, choose one of the following options:

- To convert a single IP address, follow the instructions in **Converting a Single IP Address**.
- To convert IP addresses listed in a file of IP addresses, follow the instructions in **Converting a File of IP Addresses**.

Converting a Single IP Address

1. If necessary, open an xterm window on the DNCS.
2. Type **convertIP** and then press **Enter**. The **Enter IP address to convert** message appears.
3. Type the IP address you want to convert and then press **Enter**. The convertIP utility converts the IP address and displays both the original value and the converted value on the screen of the DNCS.

   Note: You can type the IP address in either format, decimal or dotted-decimal notation.

   Examples:

   - Decimal-**167854166**
   - Dotted-decimal notation-**10.1.64.86**

Converting a File of IP Addresses

Follow these instructions to use the convertIP utility to convert a file of IP addresses. When the convertIP utility runs, it displays each original and converted IP address on the screen of the DNCS, as well as writes the output to a user-specified file.

Important: You should already have prepared a text file containing IP addresses using the guidelines and directions in ***Prepare the Text File*** (on page 79).

1. If necessary, open an xterm window on the DNCS.
2. Type **convertIP -f** and then press **Enter**. The **Enter the file name (full path) containing IP addresses to convert** message appears.
3. Type the name of the file you prepared (including the full directory path) and then press **Enter**. The message **Enter the file name (full path) in which to store the converted IP addresses** appears.

   Example: Type **/dvs/dncs/tmp/IP_input_file** and then press **Enter**.

4 Type the name of the file (including the full directory path) in which you want to store the output and then press **Enter**.

Example: Type **/dvs/dncs/tmp/IP_output_file** and then press **Enter**.

Results:

- The convertIP utility converts the IP addresses and displays both the original value and the converted value on the screen of the DNCS.
- The convertIP utility displays the number of IP addresses that were converted and suggests that you review the converted IP addresses by examining the output file.

  Example: There are 16 IP addresses in the /dvs/dncs/tmp/IP_input_file file that were converted.
  Please review the converted IP addresses in the /dvs/dncs/tmp/IP_output_file file.

11

Troubleshoot the EAS with the getEASdata Utility

Introduction

The Federal Communications Commission established the Emergency Alert System (EAS) in 1994 as a tool for government officials to quickly transmit important emergency information that is targeted to specific geographical areas. Digital cable system operators need a reliable EAS at their headend to ensure that their subscribers receive national, state, and local warning messages about emergency conditions.

The getEASdata utility was developed to ensure the reliability of a system operator's EAS. The utility helps system operators troubleshoot their EAS by reporting EAS-related errors and retrieving data associated with system components that pertain to the EAS. The following list includes some of the EAS-related data retrieved by the getEASdata utility:

- Emergency Alert Controller (EAC) network configuration
- Emergency Alert Receiver (EAR) and Multi-Media Message (MMM) Server processes

  Note: The EAR server monitors and receives EAS-related messages and then passes the messages to the MMM server for formatting and processing.
- Files in the /export/home/easftp directory
- Files converted to audio interchange file format (AIFF) and loaded onto the broadcast file server (BFS) carousel

  Note: Files in AIFF are high-quality sound files
- EAS timing data

In This Chapter

When to Use the getEASdata Utility

The getEASdata utility is a troubleshooting tool. Use the getEASdata utility if you discover that EAS messages are not displaying on test DHCTs in the headend within 5 minutes of transmitting that EAS message.

Note: Refer to ***Before Running the getEASdata Utility*** (on page 86) for additional system requirements that must be true for the getEASdata utility to be useful.

Related Publication

Refer to *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455) as you run the getEASdata utility. This guide provides valuable tips that can help you troubleshoot the EAS.

Before Running the getEASdata Utility

These Conditions Must Exist on Your System

Before you run the getEASdata utility, the following system conditions must be true:

- The debug flag **L** must be set in the .profile file.

  The L debug flag indicates that logging is turned on for the MMM server group. The getEASdata utility needs access to the MMM server logs in order to retrieve EAS-related data.

  Note: For System Release (SR) 2.1 and later, the .profile file containing debug flag L is on the DNCS; for system software earlier than SR 2.1, the .profile file is on the Application Server.

- You have successfully sent EAS messages in the past.

  The getEASdata utility is a troubleshooting tool. Use the getEASdata utility only if you know that the EAS has worked successfully in the past.

- It has been at least 5 minutes and less than 15 minutes since you transmitted the EAS message.

  It sometimes takes up to 5 minutes for EAS data to reach the necessary system components. EAS data typically remains in the system for up to 15 minutes.

- You know the IP address of a test DHCT in the headend that should have received the EAS message.

- The DHCT is currently responding to a ping request.

- You know which DHCT diagnostic screen displays EAS-related data.

  Note: The diagnostic screen on which EAS-related data displays depends upon the version of SARA your system supports. Most systems now use page 14 for EAS-related data. Call Cisco Services if you are not sure.

  Example: A typical EAS diagnostic screen looks similar to this example:

Run the getEASdata Utility

The getEASdata utility generates two reports, the **EAS Error Report** and the **EAS Data Report**. The EAS Error Report highlights errors that the utility discovers in its examination of the EAS configuration. The EAS Data Report displays EAS configuration data that the system operator can then examine to identify the source of the error.

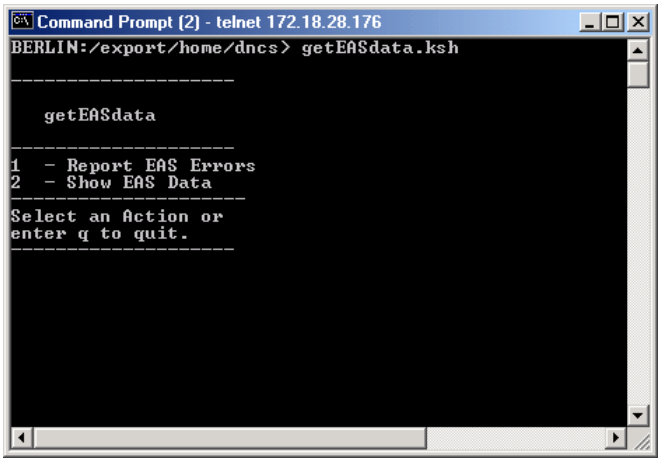
Our engineers recommend that system operators generate each report whenever they run the getEASdata utility, even if the EAS Error Report shows no errors. Examining EAS configuration data may be useful in preventing errors before they develop.

The remainder of this section provides procedures for generating the EAS Error Report and the EAS Data Report.

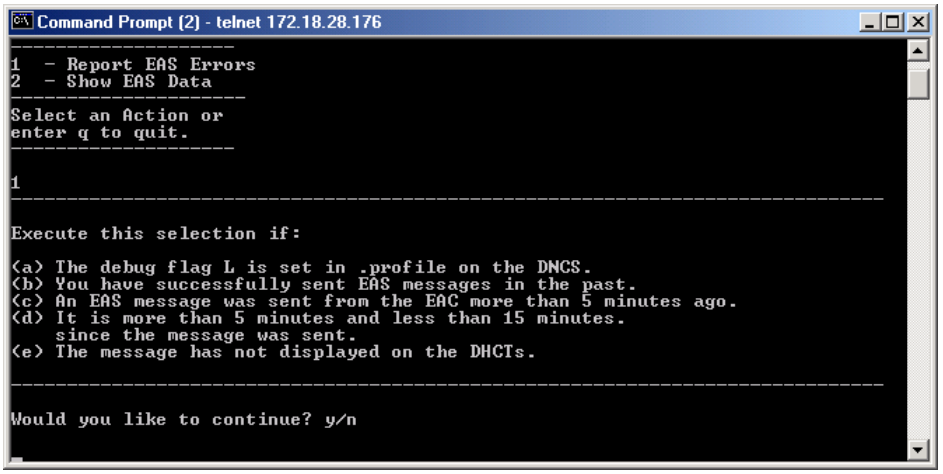
Running the getEASdata Utility

Follow these instructions to run the getEASdata utility.

1. If necessary, open an xterm window on the DNCS.
2. Type **getEASdata.ksh** and then press **Enter**. The utility displays a menu instructing you to select 1 to generate an EAS Error Report or to select 2 to generate an EAS Data Report.



3 Type **1** (for Report EAS Errors) and then press **Enter**. The utility lists several conditions that must be true before you should run the report.



Note: These conditions were discussed in ***Before Running the getEASdata Utility*** (on page 86).

4 Type **y** and then press **Enter**. The following message appears:

Enter the IP address of a DHCT that should have received the EAS message and/or hit return to continue.

5 Type the IP address of a test DHCT that did not receive the EAS message, and then press Enter.

Note: If you fail to provide an IP address, the utility will still run but it will not provide data in the EAS data on a DHCT section of the EAS Error Report.

Result: The following message appears:

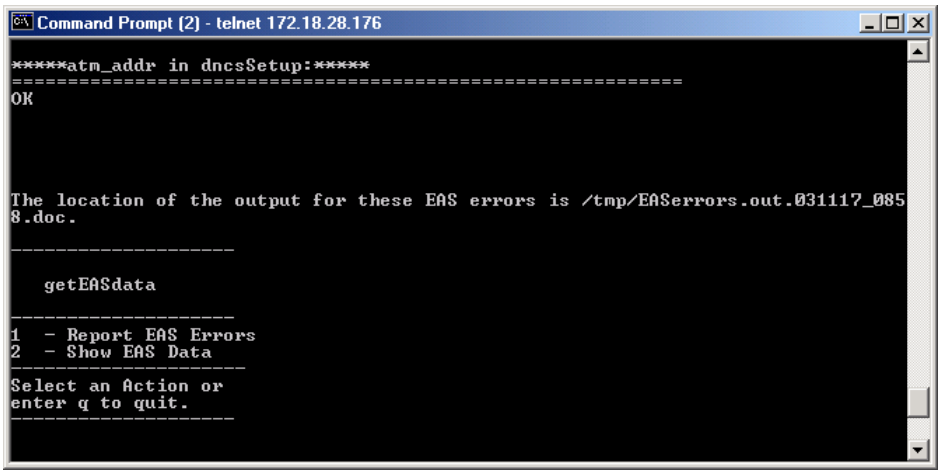
Enter the diagnostic screen the EAS data is on and/or hit return to continue.

6 Type the number of the DHCT diagnostic screen that contains EAS-related data and then press **Enter**.

Note: If you fail to provide the number of the diagnostic screen, the utility will still run but it will not provide data in the EAS data on a DHCT section of the EAS Error Report.

Results:

- The system runs the EAS Error Report and displays the output to the screen of the DNCS.
- The system displays a message that states that the EAS Error Report can also be found in the /tmp/EASerrors.out.[Date].doc file.
- The system redisplays the menu of the getEASdata utility.



7 Type **2** (for Show EAS Data) and then press **Enter**. The following message appears:

Enter the IP address of a DHCT that should have received the EAS message and/or hit return to continue.

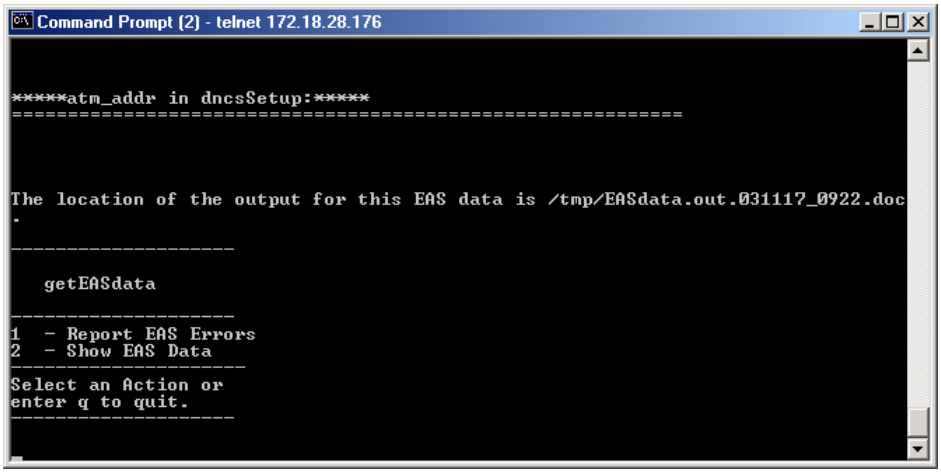
8 Type the IP address of a test DHCT that did not receive the EAS message, and then press **Enter**. The following message appears:

Enter the diagnostic screen the EAS data is on and/or hit return to continue.

9 Type the number of the DHCT diagnostic screen that contains EAS-related data and then press **Enter**.

Results:

- The system runs the EAS Data Report and displays the output to the screen of the DNCS.
- The system displays a message that states that the EAS Data Report can also be found in the /tmp/EASdata.out.[Date].doc file.
- The system redisplays the menu of the getEASdata utility.



10 Type **q** (for quit) and then press **Enter**. The getEASdata utility closes.

11 Go to ***Open and Examine the getEASdata Utility Reports*** (on page 92).

Open and Examine the getEASdata Utility Reports

This section provides instructions on opening the two reports generated and saved by the getEASdata utility, provides some guidance on examining the data, and shows a few examples of EAS-related errors that you might find.

Opening the getEASdata Utility Reports

Follow these instructions to open the two reports generated and saved by the getEASdata utility. The instructions direct you to open the reports side-by-side in two xterm windows. By examining the two reports simultaneously, you can better understand the relationship of the reports.

1. If necessary, open two xterm windows on the DNCS.
2. Type **cd /tmp** in both of the xterm windows and then press **Enter**. The /tmp directory becomes the working directory.
3. In one xterm window, type **ls EASerrors*** and then press **Enter**. The system lists all files in the /tmp directory that begin with EASerrors.

   Notes:

   - The system stores EAS Error Report files in EASerrors.out.[date].doc format, where the date is expressed in terms of YYMMDD_HHMM.
   - By listing all EAS Error Report files, you can easily identify which one pertains to the most recent report you generated.
4. In the same xterm window, type **more [EAS Error Report name]** and then press **Enter**. The selected EAS Error Report opens in the xterm window using the UNIX *more* utility.

   Note: Substitute the name of the EAS Error Report file that you want to open for [EAS Error Report name].

   Example: Type **more EASerrors.out.031008_1541.doc** and then press **Enter**.
5. In the other xterm window, type **ls EASdata*** and then press **Enter**. The system lists all files in the /tmp directory that begin with EASdata.

   Notes:

   - The system stores EAS Data Report files in EASdata.out.[date].doc format, where the date is expressed in terms of YYMMDD_HHMM.
   - By listing all EAS Data Report files, you can easily identify which one pertains to the most recent report you generated.
6. In the xterm window you used in step 5, type **more [EAS Data Report name]** and then press **Enter**. The selected EAS Data Report opens in the xterm window.

   Note: Substitute the name of the EAS Data Report file that you want to open for [EAS Data Report name].

   Example: Type **more EASdata.out.031008_1542.doc** and then press **Enter**.

7 Go to ***Examining the getEASdata Utility Reports*** (on page 93) for help in understanding the reports.

Examining the getEASdata Utility Reports

Refer to these instructions for general guidance in reviewing the two reports generated by the getEASdata utility. These instructions provide an example of one error that you might find. Refer to ***Sample EAS-Related Errors*** (on page 93) for additional examples.

1 Scroll through the EAS Error Report. As you scroll through the various headings contained in the report, look for errors. Errors are clearly marked in the report by the word **Error**.

Example: The ***** **eac in /etc/hosts.equiv** ***** heading in the EAS Error Report might include an error message similar to the following:
Error: There is no entry for eac in the hosts.equiv file.

Note: The eac needs to have one entry in the /etc/hosts.equiv file.

2 After locating an error in the EAS Error Report, look for the corresponding data in the EAS Data Report.

Example: Using the example in step 1, the ***** **eac in /etc/hosts.equiv** ***** heading in the EAS Data Report might show that there is no line in the /etc/hosts/equiv file that contains **eac**.

3 Troubleshoot each error you find to the best of your ability.

Notes:

- The *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455) may be very useful in helping you troubleshoot and correct EAS-related errors.
- Call Cisco Services for assistance if you need it.

4 After correcting errors, transmit another EAS message and run the getEASdata utility again.

Sample EAS-Related Errors

Refer to the following list for a discussion of a few additional EAS-related errors:

- The EAS Error Report may list the word **Error** under the ***** **Orbix.hosts on the DNCS configuration** ***** heading. The corresponding ***** **Orbix.hosts on the DNCS configuration** ***** heading in the EAS Data Report may then list a blank line.

  Solution: An entry for **NS:dncsatm:**, using the full path, is required in the Orbix.hosts file.

- The EAS Error Report may include an error under the ***** **VASP data for the MMM Server in the database** ***** heading. The error may be similar to **Error: VASP IP**. Meanwhile, the corresponding ***** **VASP data for the MMM Server in the database** ***** heading in the EAS Data Report may indicate that the asynchronous transfer mode (ATM) address of the DNCS or the Application Server is incorrect.

  Solution: Correct the IP address for the MMM server on the DNCS.

- The EAS Error Report may include the following error under the ***** **Timing Analysis** ***** heading: **Error: The message Origination Time and Appserver time are out of sync**. Under the ***** **EAS messages sent** ***** heading of the EAS Data Report, the data may show that too much time expired between when an EAS message was transmitted and then received.

  Solution: Call Cisco Services. Resolving timing issues requires the help of engineers from Cisco Services.

- The EAS Error Report may include the following error under the ***** **atm_addr in .profile** ***** heading: **Error: atm_addr=dncseth** is no longer required for EAS in SR 2.1 and higher. Meanwhile, an entry for **atm_addr=dncseth** may be listed under the ***** **atm_addr in .profile** ***** heading in the EAS Data Report.

  Solution: Remove the atm_addr=dncseth entry in the /export/home/dncs/.profile file.

12

Transmit the ModifyDhctConfiguration Transaction with the modDhctCfg Utility

Introduction

System operators can use the modDhctCfg utility to transmit the ModifyDhctConfiguration transaction to DHCTs. The ModifyDhctConfiguration transaction modifies the status and authorizations of one or more DHCT records.

Note: Consult your copy or your billing vendor's copy of the Business Operations Support System (BOSS) Interface Specification document for a complete description of the ModifyDhctConfiguration transaction.

The modDhctCfg utility retrieves authorization and package data from the database, formats it into the ModifyDhctConfiguration transaction, and transmits it to the appropriate DHCT(s). The main purpose of the utility is to regenerate and send EMMs to DHCTs. The utility essentially refreshes a DHCT by sending the last ModifyDhctConfiguration transaction that the DNCS received for the DHCTs.

Note: To generate and transmit staging EMMs, use the -s option with the modDhctCfg utility. Instructions for using the -s option, as well as other options supported by the modDhctCfg utility, are provided throughout this chapter.

In This Chapter

The modDhctCfg Utility at a Glance

The modDhctCfg utility can transmit the ModifyDhctConfiguration transaction to a single DHCT or to a list of DHCTs. When you want to transmit the ModifyDhctConfiguration transaction to a single DHCT, supply the modDhctCfg utility with the MAC address of that DHCT. When you want to transmit the ModifyDhctConfiguration transaction to several DHCTs, supply the modDhctCfg utility with the name of a file that contains the MAC address of the appropriate DHCTs.

Staging Operations and the Billing Interface

When the modDhctCfg utility runs, it tends to compete for system resources with staging operations, as well as with the activities of the billing computer. If you have to process a large number of DHCTs with the modDhctCfg utility, and if time is important, consider temporarily disabling the billing interface and suspending staging operations.

Options Available with the modDhctCfg Utility

This section describes the options that are available for use with the modDhctCfg utility.

Supported Options for the modDhctCfg Utility

Refer to the following table for an explanation of the options available with the modDhctCfg utility.

Option	Purpose
-?	The *-?* option displays the help window associated with the modDhctCfg utility. **Example: modDhctCfg -?**
-v	The *-v* option displays the version number of the modDhctCfg that is installed on your system. **Example: modDhctCfg -v**
-h	The *-h* option is used to specify the hostname or IP address of the DNCS in the event that the modDhctCfg utility executes on a remote computer. **Example: modDhct -h172.18.28.176 +dms [DHCT MAC address]**
+a / -a	The *+a* and *-a* options specify how the analog_enable parameter is set for the DHCT. The setting of the analog_enable parameter determines whether the DHCT supports analog descrambling. **Example: modDhctCfg +a [DHCT MAC address]**
-B#	The *-B* option sets the blocking factor for the modDhctCfg transaction. The blocking factor refers to the number of DHCT records transmitted at one time in the modDhctCfg transaction. **Example: modDhctCfg -B50 [file name]** **Note:** The default blocking factor is 10.
-c#	The *-c#* option specifies the credit limit assigned to the DHCT for IPPV purchases. This value is decremented with each DHCT IPPV purchase. **Example: modDhctCfg -c100 [DHCT MAC address]**
+dms / -dms	The *+dms* and *-dms* options enable or disable digital packages for the DHCT. **Example: modDhctCfg +dms [DHCT MAC address]**

Option	Purpose
+dis / -dis	The *+dis* and *-dis* options are used to enable or disable the decryption of encrypted sessions. **Example: modDhctCfg +dis [DHCT MAC address]**
-e#	The *-e#* option specifies the maximum number of IPPV purchases that the DHCT can make before IPPV purchase data is collected by the DNCS. **Example: modDhctCfg -e10 [DHCT MAC address]**
+f / -f	The *+f* and *-f* options determine whether the fast_refresh parameter is set to on or off. The DNCS sends EMMs to DHCTs that are on the "fast refresh list" automatically; subscribers or installation engineers are not required to telephone the headend when they want a DHCT enabled. **Example: modDhctCfg +f [file name]**
-I	The *-I* option instructs the DNCS to process imported DHCT records from another DNCS. This option deletes the secure_micro record from the database and sets to null the qpsk_mod, qpsk_demod, and ip_address fields. To restore this data, the DHCTs must reboot. **Example: modDhctCfg -I [file name]**
+i / -i	The *+i* and *-i* options determine whether a DHCT is enabled for IPPV. **Example: modDhctCfg +i -e10 [DHCT MAC address]**
+pXX / -pXX	The *+pXX* and *-pXX* options add or remove package XX from a DHCT. **Example: modDhctCfg +pHBO [DHCT MAC address]**
!pQQQ	The *!pQQQ* option replaces all packages assigned to a DHCT with the packages included in file QQQ. **Note:** File QQQ must contain only one package name per line. **Example: modDhctCfg !p[package file name] [DHCT MAC address]**
-s	The *-s* option restages DHCTs. The secure_micro record in the database is deleted and then re-added. **Example: modDhctCfg -s [file name]**

Prepare a Text File

When you want to use the modDhctCfg utility to set authorization data for several DHCTs, you can usually save time by preparing a text file that contains a list of pertinent MAC addresses. This section contains guidelines and instructions for preparing the 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 per line.

  Examples:

  - **00:02:DE:4A:11:92**
    00:02:DE:4A:11:93
    00:02:DE:4A:11:94
  - **0002DE4A1192**
    0002DE4A1193
    0002DE4A1194
  - **0002de4a1192**
    0002de4a1193
    0002de4a1194
- If you use the ":" character in the MAC address, the ":" character must either be all present or all absent in the file. The system cannot process a file where some MAC addresses contain the ":" character and some do not.
- Alphabetic characters in the MAC address can be all uppercase, all lowercase, or mixed.
- 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.

  Example: modDhctCfg-in_11.13.03 for a file that was created on November 13, 2003.
- Our engineers recommend that you save the file to the /tmp directory on the DNCS.

Preparing a Text File

Follow these instructions to prepare a text file for use with the modDhctCfg utility.

Important: These instructions use the vi text editor as an example. The vi text editor is not intuitive. These instructions are not a 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: Our engineers recommend 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.

   Example: vi modDhctCfg-in_11.13.03
4. Insert your list of MAC addresses or serial numbers into the file you have just opened.

   Note: Use the guidelines set forth in ***Guidelines for Preparing the Text File*** (on page 100).

   Important: Type only one MAC address or serial number per line.
5. Save the file and close the vi editor.

Display the modDhctCfg Help Window and Version Number

The information in this section describes how to display the modDhctCfg help window and version number.

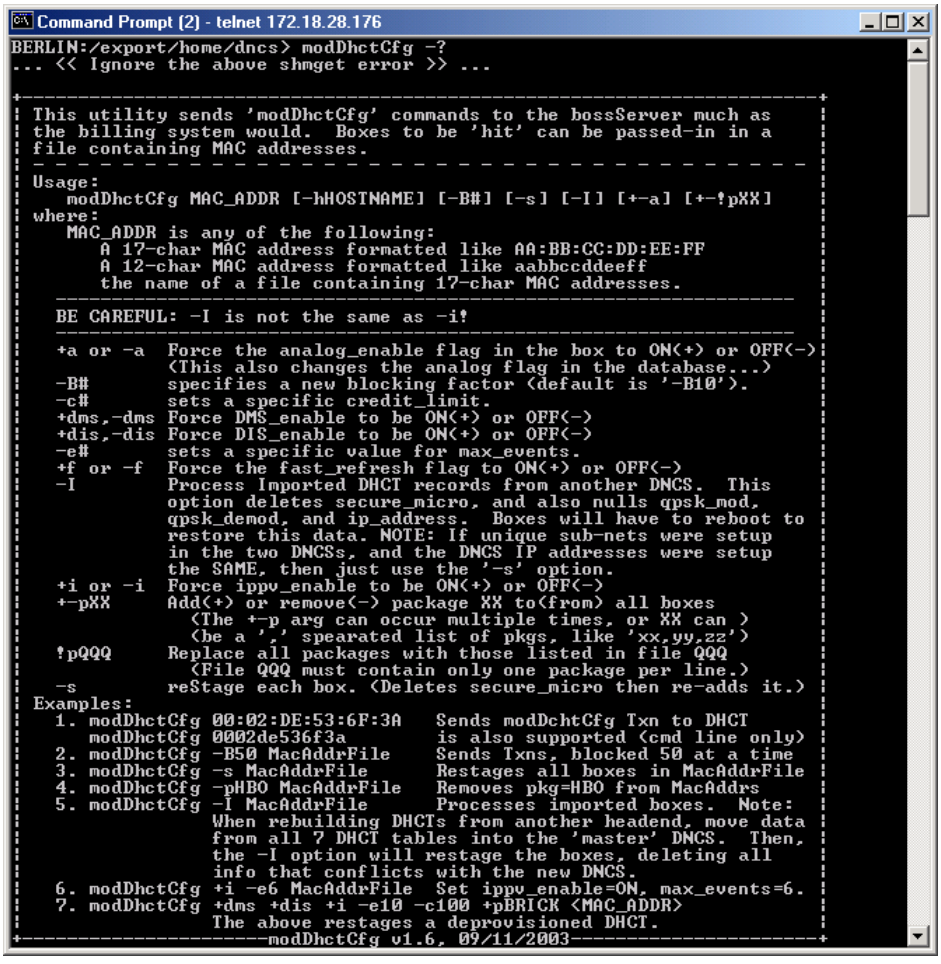
Tip: Many utilities include a help window. The help window is frequently a good place to start if you are unfamiliar with a utility.

Displaying the modDhctCfg Help Window

Follow these instructions to display the modDhctCfg help window.

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

2 Type **modDhctCfg -?** and then press **Enter**. The system displays the modDhctCfg help window.

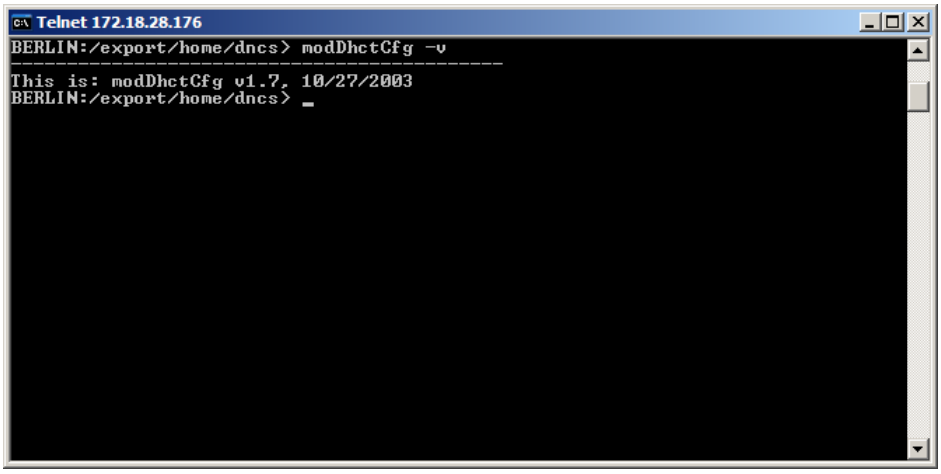


Displaying the modDhctCfg Version Number

Follow these instructions to display the version number of the modDhctCfg utility that is installed on your system.

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

2 Type **modDhctCfg -v** and then press **Enter**. The system displays the modDhctCfg version number.



How to Use the modDhctCfg Utility

The instructions and examples in this section describe how to use the modDhctCfg utility. This section covers those options that our engineers think system operators are most likely to use. Refer to ***Options Available With the modDhctCfg Utility*** (on page 98) for examples showing how to use the various supported options.

Running the modDhctCfg Utility

Refer to the following procedures to run the modDhctCfg utility.

Note: The transaction that the utility sends is the same ModifyDhctConfiguration transaction that was sent to the DHCT(s) the last time the DHCTs received a ModifyDhctConfiguration transaction. The utility simply retrieves the data from the database and re-transmits it.

Sending the ModifyDhctConfiguration Transaction to a Single DHCT

Follow these instructions to send the ModifyDhctConfiguration transaction to a single DHCT.

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

2 Type **modDhctCfg [DHCT MAC address]** and then press **Enter**. The system sends the ModifyDhctConfiguration transaction to the specified DHCT.

Note: Substitute the MAC address of the DHCT for [DHCT MAC address].

Example: modDhctCfg 00:02:DE:4A:11:92

Sending the ModifyDhctConfiguration to a List of DHCTs

Follow these instructions to send the ModifyDhctConfiguration transaction to a list of DHCTs.

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

2 Type **modDhctCfg [file name]** and then press **Enter**. The system sends the ModifyDhctConfiguration transaction to all the DHCTs represented in the file.

Note: Substitute the name of the file you prepared for [file name].

Example: modDhctCfg modDhctCfg-in_11.13.03

Sending the ModifyDhctConfiguration Transaction with a Specified Blocking Factor

The blocking factor option specifies now many DHCT records the modDhctCfg utility transmits as a block. When the blocking factor is not specified with the modDhctCfg utility, the utility uses a default blocking factor of 10. When you urgently need to use the utility to send the ModifyDhctConfiguration transaction to a large number of DHCTs, you might want to increase the blocking factor. An increased blocking factor has the effect of increasing the priority of the transactions.

Important: Keep in mind, however, that increasing the blocking factor associated with the modDhctCfg utility increases the claim the utility has upon system resources. When practical, suspend staging activities and shut down the billing interface before running the modDhctCfg utility with a large blocking factor.

Follow these instructions to specify the blocking factor used with the modDhctCfg utility.

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

2 Type **modDhctCfg -B# [file name]** and then press **Enter**.

Notes:

- Substitute the blocking factor that you want to use for #.
- Substitute the name of the file you prepared for [file name].

Examples:

- **modDhctCfg -B100 modDhctCfg-in_11.13.03**

  Result: The system sends the ModifyDhctConfiguration transactions, blocked 100 at a time, to the DHCTs represented in the specified file.

- **modDhctCfg -B2 modDhctCfg-in_11.13.03**

  Result: The system sends the ModifyDhctConfiguration transactions, blocked 2 at a time, to the DHCTs represented in the specified file.

  Important: This example (using a small blocking factor) minimizes the claim that the utility has upon system resources. Consider using a small blocking factor while staging operations are ongoing or during periods of high customer service representative (CSR) activity.

Sending the ModifyDhctConfiguration Transaction to Enable or Disable Session-Based Encryption

The *dis* option is used to enable or disable session-based encryption. Follow these instructions to use the modDhctCfg utility with the dis option.

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

2 Choose one of the following options:

- Type **modDhctCfg +dis [DHCT MAC address]** and then press **Enter** to enable session-based encryption for the specified DHCT.
- Type **modDhctCfg -dis [DHCT MAC address]** and then press **Enter** to disable session-based encryption for the specified DHCT.

Note: Substitute the MAC address of the appropriate DHCT for [DHCT MAC address].

Sending the ModifyDhctConfiguration Transaction to Restage DHCTs

When used with the modDhctCfg utility, the *-s* option generates staging EMMs. Refer to the following instructions when using the modDhctCfg utility to stage DHCTs.

Important: The modDhctCfg utility cannot be used to stage a DHCT for the first time. The utility reads information about the DHCT from the database in order to formulate a valid ModifyDhctConfiguration transaction. DHCTs must be staged according to normal staging procedures in order to populate the database properly.

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

2 Type **modDhctCfg -s [file name]** and then press **Enter**. The system generates staging EMMs for the DHCTs listed in the specified file.

Notes:

- Substitute the name of the file you prepared for [file name].
- Guidelines and instructions for preparing the file are in ***Prepare a Text File*** (on page 100).

Example: modDhctCfg -s modDhctCfg-in_11.13.03

13

Ensure the Presence of Type-8 Staging EMMs with the type8helper Utility

Introduction

Digital Home Communications Terminals (DHCTs) and CableCARD modules need type-8 Entitlement Management Messages (EMMs) in order to decode encrypted, interactive sessions. Devices without type-8 EMMs cannot purchase *anything*-On-Demand (xOD) events.

System operators sometime inadvertently stage devices before type-8 EMMs can be assigned. The type8helper utility was developed in order to ensure that type-8 EMMs are created for all staged devices. The type8helper utility scans the database for all devices that have staging EMMs and identifies those that lack type-8 EMMs. The utility then creates type-8 EMMs for these devices using the modDhctCfg utility, and transmits the EMMs to the devices through the IIH utility.

In This Chapter

Overview of the type8helper Utility

Limited to SR 2.2/3.2 Systems

The type8helper utility is only useful at sites that support System Release 2.2 or 3.2 (SR 2.2/3.2) software. With the development of SR 2.5 and higher, the system assigns type-8 EMMs to a device automatically whenever the device is enabled for encrypted sessions.

Three Working Files

When it runs, the type8helper utility creates the following three working files:

- macRecent—Contains the MAC addresses of all recently staged, in-service, two-way devices
- mac8—Contains the MAC addresses of all devices that already have type-8 EMMs
- need_T8.txt—Generated by comparing the previous two files; contains the MAC addresses of devices for which type-8 EMMs were just generated

Run Manually, Then Put in cron

The type8helper utility is designed to run from the crontab (cron) file on the DNCS. Programs that run from cron run automatically on a pre-defined schedule, without user intervention. When run from cron, the system regularly assigns type-8 EMMs to newly staged devices that lack type-8 EMMs.

Our engineers recommend, however, that system operators run the type8helper utility manually the first time. The first time the utility runs, the system may have an inordinately large number of devices without type-8 EMMs. The utility is designed to seek user confirmation whenever it encounters more than 500 devices that lack type-8 EMMs, a condition the utility is unlikely to encounter when it is subsequently run from cron.

Running the type8helper Utility Manually

Before you place the type8helper utility into the crontab file of the DNCS, our engineers recommend that you first run the utility manually. When run manually, the utility assigns type-8 EMMs to devices that lack them, provided that there are fewer than 500 devices that need type-8 EMMs. As noted in the message displayed in the second bullet of step 2, if the utility finds more than 500 devices that need type-8 EMMs, you are prompted to run the modDhctCfg utility in order to assign these EMMs.

Follow these instructions to run the type8helper utility manually.

1. If necessary, open an xterm window on the DNCS.
2. Type **type8helper.sh** and then press **Enter**.

   Result: One of two types of messages appears:

   - If the utility encounters fewer than 500 devices that need type-8 EMMs, the utility generates a message similar to the following:
     Getting a list of all boxes having type-8 EMMs into file 'mac8'.
     Getting a list of recently staged IS2W boxes into file 'macRecent'.
     Generating a list of all recently staged boxes still needing type-8 EMMs.
     Recently staged boxes needing type-8 EMMs are in file 'need_T8.txt'.
     Now generating type-8 EMMs for all boxes in the list.
   - If the utility encounters 500 or more devices that need type-8 EMMs, the utility generates a message similar to the following:
     #### boxes need type-8 EMMs. Check that this is reasonable.
     (Sometimes the lists generated in mac8 or macRecent are wrong.)
     If this IS reasonable, then you must manually run:
     /dvs/dncs/bin/modDhctCfg +dis -s need_T8.txt

     Note: There are no hard-and-fast rules concerning what is "reasonable". If the number of devices without type-8 EMMs represents a small percentage of your total population, regardless of how many, then it is probably "reasonable". Call Cisco Services if you need help determining whether you should now run the modDhctCfg utility against the need-T8.txt file.
3. Do you need to run the modDhctCfg utility?
   - If **yes**, type **/dvs/dncs/bin/modDhctCfg +dis -s need_T8.txt** and then press **Enter**. Then, go to ***Place the type8helper utility in cron*** (on page 110).
   - If **no** (fewer than 500 devices lacked type-8 EMMs), go to ***Place the type8helper utility in cron*** (on page 110).

Place the type8helper Utility into cron

After running the type8helper utility manually the first time, you are now ready to place the utility into the crontab file of the DNCS. When the utility runs from cron, it automatically generate type-8 EMMs for newly staged devices that need type-8 EMMs. When you place the utility in cron, be sure to schedule execution for no more than once a day. Furthermore, our engineers recommend that you schedule execution for off-peak hours.

Important: Do not attempt to edit the crontab file unless you are skilled in the use of the UNIX vi editor, and have a good working knowledge regarding how crontab entries are structured. Call Cisco Services if you need help in adding this utility to the crontab file.

1. If necessary, open an xterm window on the DNCS.
2. Type **export EDITOR=vi** and then press **Enter**.
3. Type **crontab -e** and then press **Enter**. The crontab file opens for editing using the UNIX vi text editor.
4. Append an entry to the crontab file similar to the following example for the type8helper utility.

   Example:
   40 2 * * * (. /dvs/dncs/bin/dncsSetup ; /dvs/dncs/bin/delete-sm -o ..OOS..) > /dvs/dncs/tmp/deprovisioned.out 2>&1

   10 3 * * * (. /dvs/dncs/bin/dncsSetup ; /dvs/dncs/bin/type8helper.sh) > /dev/null

   Notes:

   - In this example, the delete-sm utility executes at 2:40 AM each day. The type8helper utility then executes at 3:10 AM each day.
   - The reason the delete-sm utility is coupled with the type8helper utility in the crontab entry, is so the delete-sm utility will delete all secure_micro row entries from the database for out-of-service devices. These devices will then automatically restage (and receive type-8 EMMs) the next time the billing system transmits a modifyDhctConfiguration transaction. Without the delete-sm entry, if these devices are suddenly placed back into service, the type8helper utility might encounter its 500-devices limit the next time it tries to run from cron.
5. Save the crontab file and close the vi editor.

Displaying the Help Window and Version Number of the type8helper Utility

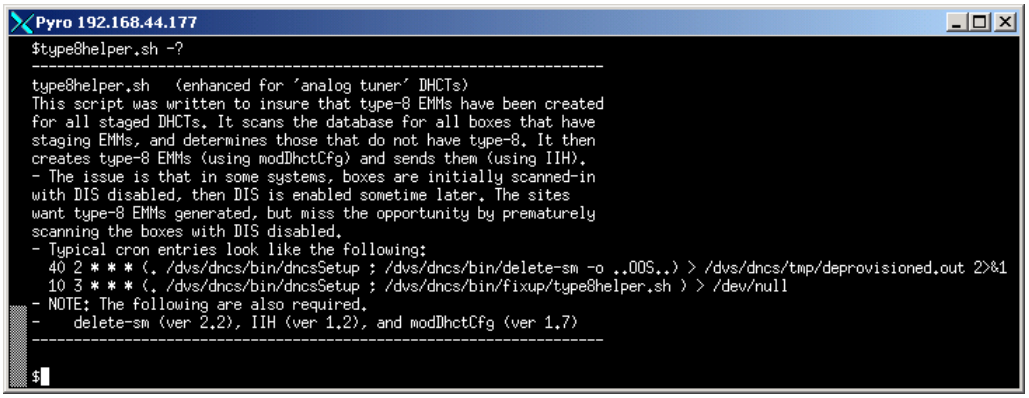
Most utilities developed by our engineers include a help window, as well as a means for displaying the current version number of the utility. Follow these instructions to display the help window and version number of the type8helper utility.

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

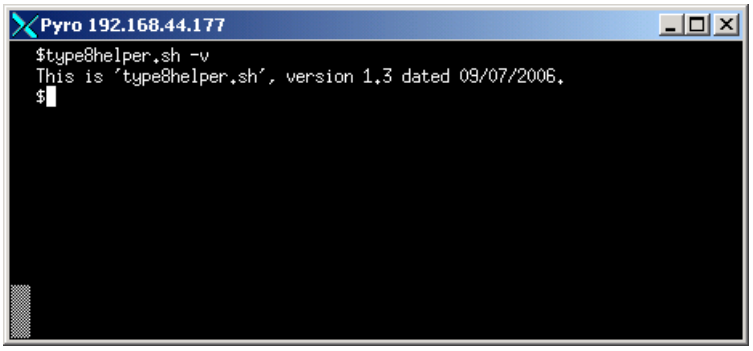
2 Choose one of the following options:

- To display the help window, go to step 3.
- To display the version number, go to step 4.

3 Type **type8helper.sh -?** and then press **Enter**. The system displays the help window of the type8helper utility.



4 Type **type8helper.sh -v** and then press **Enter**. The system displays the version number of the type8helper utility.



14

Preserve Log Files with the preserveLog Utility

Introduction

The processes that run on the Digital Broadband Delivery System (DBDS) create log files when they run. These log files contain data, such as the values of parameters at process entry and exit points, that help system operators and engineers troubleshoot the system.

In order to conserve space, the system places limitations on the number and size of each log file that it keeps on hand. When this limit is reached, old log files "roll over" or "roll off" and are replaced with new log files, often before anyone has had an opportunity to examine the old files. Log files associated with some processes, such as drm, dsm, and qamManager, roll over at an especially quick rate, often as rapidly as every 5 minutes. In addition, whenever a process is stopped and then restarted (known as "bouncing" the process), existing log files are erased.

The preserveLog utility was developed in order to allow the system to save log files for later examination. The preserveLog utility can save log files for processes that run on the DNCS, log files for processes that run on the Application Server, and the log file for the xod process that runs on the ASI server.

In This Chapter

More About the preserveLog Utility

Usage

The following usage diagram shows at a glance how to run the preserveLog utility: **preserveLog.ksh [-v/-h] <logname> <logname> <logname>** etc.

Notes:

- The **-v** and **-h** switches refer to the version number and the help window, respectively and are optional.
- To preserve a log file, at least one **<logname>** is required.

What Log Files Can be Preserved

The preserveLog utility can save log files for every process that runs on the DNCS. For the Application Server, the preserveLog utility saves "types" of log files. Supported types include all pay-per-view (PPV) logs, all Interactive Program Guide (IPG) logs, virtual channel (VCS) logs, and Orbix logs. The preserveLog utility can also save xod logs from the ASI server for sites that support the *anything*-On-Demand (xOD) feature.

When the preserveLog utility runs, it begins by creating a unique date directory in the /export/home/dncs/scripts/saInternalTools/preserveLog/directory structure on the DNCS. The utility then creates a directory for each unique log file and copies the specified log files from the /dvs/dncs/tmp directory on the DNCS to this newly created directory. For Application Server log files, the utility uses remote procedure calls to transfer the log files from Application Server to the DNCS. For the xod log files on the ASI server, the utility uses the FTP utility to transfer files to the DNCS. Finally, to minimize disk usage, the preserveLog utility uses the gzip utility to compress the log files to be preserved.

Example: The following is an example of what the preserveLog directory structure looks like:
/export/home/dncs/scripts/saInternalTools/preserveLog/06_10_08/drm

Inside of the drm directory (as noted in this example) are the various compressed log files that pertain to the drm logs.

By default, the utility keeps two days of preserved log files. When the third day's log files are received, the utility deletes log files from the earliest day. System operators can change the number of days of log files that are preserved by modifying preserveLog file in the /export/home/dncs/scripts/saInternalTools/preserveLog directory. See ***Customize the preserveLog Utility*** (on page 117), for additional information.

Command Line or crontab File

The preserveLog utility can run from the command line of an xterm window on the DNCS. In addition, an entry for the preserveLog utility can be placed in the crontab (cron) file of the DNCS where it can be configured to automatically preserve log files for specific processes on a regular basis.

Confirmation of Sufficient Space

Before the preserveLog utility runs, the utility confirms that there is sufficient space in the /export/home file system in order to save the log files. If the preserveLog utility determines that the /export/home file system is at, or over, 80 percent capacity, the utility displays a message similar to the following:

Tue Jun 20 08:39:09 EDT 2006
PROGRAM TERMINATED. /export/home is at or over 80%!

Additionally, the utility transmits a message similar to the following to every open terminal on the system:

Broadcast Message from dncs (pts7) on lville Tue Jun 20 08:39:09
/export/home at 80%
PROGRAM TERMINATED!

Please check disk space!

The system operator should then proceed to free up space in the /export/home file system.

Customize the preserveLog Utility

By default, the preserveLog utility keeps two days of preserved files for each process before deleting old files. System operators or engineers can change the number of days of log files that are preserved by modifying the code for the preserveLog utility. For example, video-on-demand (VOD) and xOD activity is usually higher on weekends than it is during the week. Before leaving for the weekend, system operators might want to ensure that the system preserves all log files associated with VOD and xOD. A simple edit to the preserveLog file accomplishes this.

Important: Before editing the preserveLog file, note these important points:

- Do not attempt to edit the preserveLog file unless you are a skilled user of the UNIX vi text editing utility. Call Cisco Services for assistance in editing this file if you are unsure of your ability to make the edit yourself.
- We recommend that you use only the UNIX vi text editor to make the edits. A Windows-based utility may inadvertently introduce Windows control characters into the file, often with unpredictable results.

Customizing the preserveLog Utility

By default, the preserveLog utility saves two days of log files. Follow these instructions to change the number of days of log files that are saved by the preserveLog utility.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/bin** and then press **Enter**.
3. Type **vi preserveLog.ksh** and then press **Enter**. The preserveLog file opens for editing using the UNIX vi text editor.
4. Locate the following line: **if [[$c -gt 2]]**

   Note: The **2** in this line represents the number of days of log files that are to be preserved.
5. Replace the 2 with however many days of log files you want to preserve.

   Example: To save 3 days of data, the line should look like: **if [[$c -gt 3]]**. For 4 days, the line should look like: **if [[$c -gt 4]]**.
6. Save the file and close the UNIX vi editor.

Note: Remember to change the command back to the default value of 2 days when you no longer need the customized entry.

Display the preserveLog Help Window and Version Number

Most of the utilities developed by our engineers include a help window. The help window describes what the utility does and often provides examples on how to use the utility. The help window is often the best place to begin when you are unfamiliar with a utility. Use the instructions in this section to display the help window associated with the preserveLog utility, as well as a window that displays the current version number of the utility.

Displaying the preserveLog Help Window and Version Number

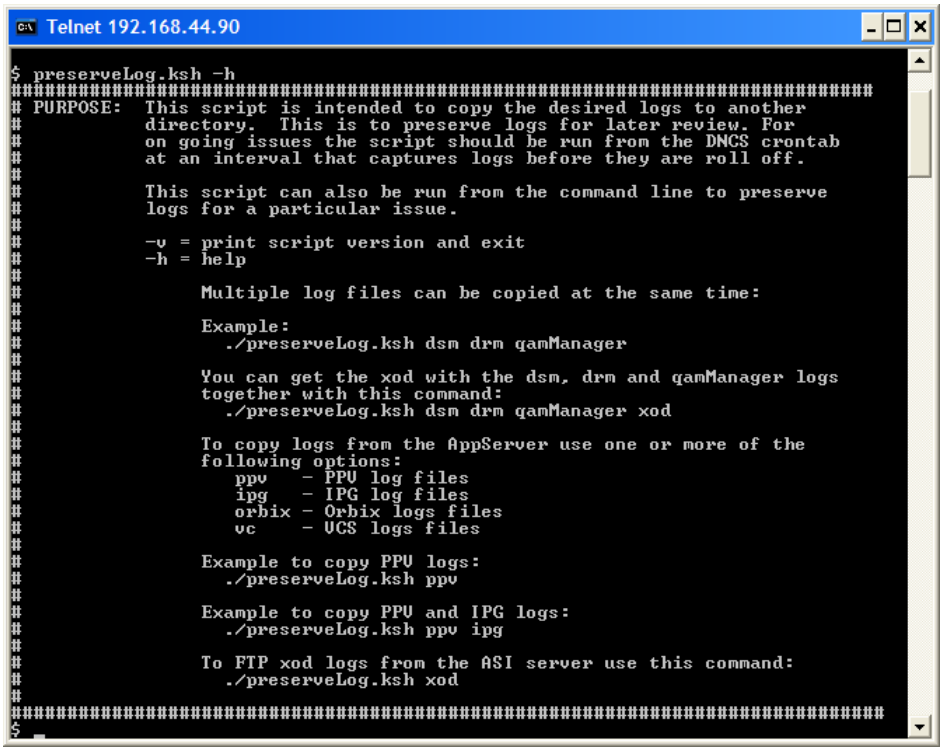
Follow these instructions to display the help window and version number of the preserveLog utility.

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

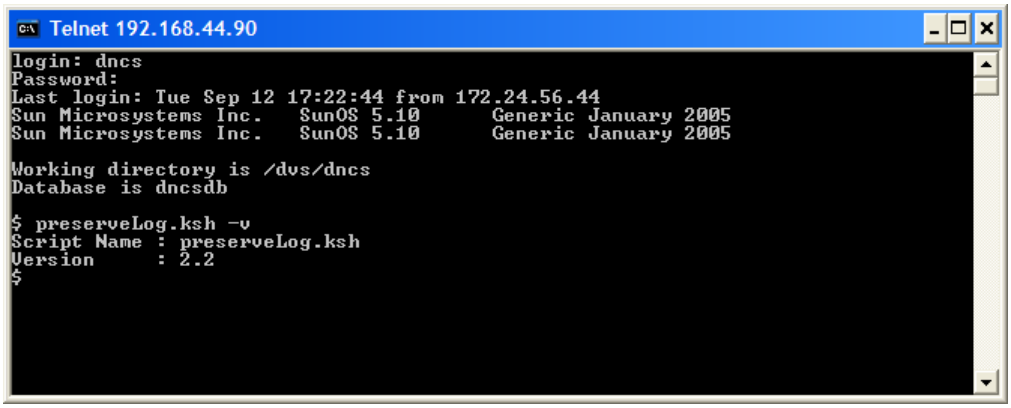
2 Choose one of the following options:

- To display the preserveLog help window, go to step 3.
- To display the version number of the preserveLog utility, go to step 4.

3 To display the help window of the preserveLog utility, type **preserveLog.ksh -h** and then press **Enter**.



4 To display the version number of the preserveLog utility, type **preserveLog.ksh -v** and then press **Enter**.



Run the preserveLog Utility From the Command Line

This section contains instructions and an example for running the preserveLog utility from an xterm window on the DNCS, also known as running the utility "from the command line". In addition, this section contains a procedure for confirming that the utility actually preserved the log files, as intended.

Running the preserveLog Utility From the Command Line

Follow these instructions to run the preserveLog utility from the command line.

1. If necessary, open an xterm window on the DNCS.
2. Type **preserveLog.ksh < logname > < logname > < logname >** and then press **Enter**.

   Note: Substitute the name of the log file for <logname> for as many log files as you want to preserve.

   Example: To preserve log files for the dsm, drm, and qamManager processes on the DNCS, PPV log files on the Application Server, and xOD log files from the ASI server, type:
   preserveLog.ksh dsm drm qamManager PPV xod and then press **Enter**.

Confirming the Presence of the Preserved Log Files

You can confirm that the preserveLog utility saved the log files for future reference by following these instructions. This example used in this procedure references the log files associated with the dsm process.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/scripts/saInternalTools/preserveLog** and then press **Enter**. The specified directory becomes the working directory.
3. Type **ls -la** and then press **Enter**. The system displays a list of directories named according to the date on which the preserveLog utility was run. The format of the directories is YY_MM_DD.

   Example: The directory for July 5, 2006 is **06_07_05**.
4. Select one of the dates revealed in the results of step 3 and type **cd < date >** and then press **Enter**.
5. Type **ls -la** and then press **Enter**. The system displays a list of directories named according to the various log files that it has preserved.

6 Select one of the log file directories and type **cd < directory >** and then press **Enter**.

Example: To change directories into the dsm directory, type **cd dsm** and then press **Enter**.

7 Type **ls -la** and then press **Enter**. The system displays the name or names of however many compressed log files reside within the directory.

Example: This example shows a series of compressed dsm log files.

```
-rw-r--r--  1 dncs    dncs    178152 Jul  5 14:15 dsm.005.gz
-rw-r--r--  1 dncs    dncs    177441 Jul  5 14:15 dsm.006.gz
-rw-r--r--  1 dncs    dncs    178695 Jul  5 14:15 dsm.007.gz
-rw-r--r--  1 dncs    dncs    179044 Jul  5 14:15 dsm.008.gz
-rw-r--r--  1 dncs    dncs    178703 Jul  5 14:15 dsm.009.gz
-rw-r--r--  1 dncs    dncs    184693 Jul  5 14:15 dsm.010.gz
```

Place the preserveLog Utility Into cron

This section describes how to place an entry for the preserveLog utility into the crontab file of the DNCS, commonly referred to as the "cron" file. When run from cron, the utility executes automatically at a pre-defined interval, without user intervention.

Tip: The log files for the drm, dsm, qamManager, and xod processes of the DBDS are especially susceptible to "rolling over" before anyone has had an opportunity to review the contents of the files. The log files for these processes are especially suited for having a cron entry for the preserveLog process save their contents.

Placing the preserveLog Utility Into cron

An entry for the preserveLog utility can be placed into cron in order to run the utility on a regular basis, without user intervention.

Note: Log files for the dsm, drm, qamManager, and xod processes tend to roll over rapidly. It may make sense for system operators to create a cron entry that saves the log files for these processes.

Important: Do not attempt to edit the crontab file on the DNCS unless you are a skilled user of the UNIX vi text editor and are familiar with how cron entries are structured.

1. If necessary, open an xterm window on the DNCS.
2. Type **export EDITOR=vi** and then press **Enter**.
3. Type **crontab -e** and then press **Enter**. The crontab file opens for editing using the UNIX vi text editor.
4. Append an entry in the crontab file similar to the following example for the preserveLog utility:
   00,10,20,30,40,50 * * * *
   /dvs/dncs/bin/preserveLog.ksh < logname > < logname > < logname > 2>&1

   Example: A cron entry that preserves the log files of the dsm, drm, qamManager, and xod processes every 10 minutes would be structured similarly to:
   00,10,20,30,40,50 * * * *
   /dvs/dncs/bin/preserveLog.ksh dsm drm qamManager xod 2>&1
5. Save the crontab file and close the UNIX vi editor.

Examine the Log Files

Choose either ***Examining the Log Files on a Solaris 10 System*** (on page 123), or ***Examining the Log Files on a Solaris 8 System*** (on page 124), based upon the operating system running on your DNCS, to examine the compressed log files.

Examining the Log Files on a Solaris 10 System

Use the gzcat command to examine the compressed log files on a system on which the Solaris 10 operating system runs on the DNCS. The following instructions guide you through the necessary steps.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/scripts/saInternalTools/preserveLog/** and then press **Enter**.
3. Type **ls -la** and then press **Enter**. The system displays all of the date directories that have been created by the preserveLog utility.
4. Type **cd < date >** and then press **Enter**.

   Note: Substitute < date > with the actual date associated with the log files you want to view.
5. Type **ls -la** and then press **Enter**. The system displays all of the log directories that have been created by the preserveLog utility.
6. Type **cd < directory >** and then press **Enter**. The selected log file directory becomes the working directory.
7. Type **ls -la** and then press **Enter**. The system displays a list of the compressed files in the working directory.
8. To view the contents of a specific log, type **gzcat < filename > | less** and press **Enter**.

   Example: gzcat dsm.005.gz | less

   Results:

   - The selected file opens for review using the gzcat utility.
   - The contents of the file are piped to the UNIX *less* utility.

Tips for Maneuvering Through the File

Use the following tips to maneuver through the file piped to the *less* utility:

- To move a whole page (screen) forward, press either the **Spacebar** or the **f** key.
- To move a whole page (screen) backward, press the **b** key.
- To move a single line forward, press the **j** key.
- To move a single line backward, press the **k** key.
- To exit from the file, press **q**.

Examining the Log Files on a Solaris 8 System

Use the gzip command to examine the compressed log files on a system on which the Solaris 8 operating system runs on the DNCS. The following instructions guide you through the necessary steps.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/scripts/saInternalTools/preserveLog/** and then press **Enter**.
3. Type **ls -la** and then press **Enter**. The system displays all of the date directories that have been created by the preserveLog utility.
4. Type **cd < date >** and then press **Enter**.

   Note: Substitute <date> with the actual date associated with the log files you want to view.
5. Type **ls -la** and then press **Enter**. The system displays all of the log directories that have been created by the preserveLog utility.
6. Type **cd < directory >** and then press **Enter**. The selected log file directory becomes the working directory.
7. Type **ls -la** and then press **Enter**. The system displays a list of the compressed files in the working directory.
8. To view the contents of a specific log file, type **gzip -d < filename >** and then press **Enter**. The selected file is uncompressed.

   Example: gzip -d dsm.005.gz
9. Type **more < filename >** and then press **Enter**. The selected file opens for viewing with the UNIX more utility.

   Example: more dsm.005
10. After examining the contents of the file, type **gzip < filename >** and then press **Enter** to re-compress the file. The file re-obtains the .gz extension.

    Example: gzip dsm.005

Tips for Maneuvering Through the File

Use the following tips to maneuver through the file piped to the *more* utility:

- To move a whole page (screen) forward, press either the **Spacebar** or the **f** key.
- To move a whole page (screen) backward, press the **b** key.
- To move a single line forward, press the **Enter** key.
- To exit from the file, press **q**.

Important: Remember to re-zip the file when you are finished reviewing it.

15

Retrieve CableCARD Data with the getCCdata Utility

Introduction

The getCCdata utility was developed for the purpose of reporting errors and retrieving data that pertains to CableCARD modules. Examples of the errors reported and the data retrieved include whether the servers that support the CableCARD modules are running and configured correctly, whether the mmi and gfc files are present and configured correctly on the Broadcast File System (BFS) server, and whether CableCARD data is properly represented in the database.

This chapter provides instructions and recommendations on running the getCCdata utility and offers a description of the type of errors and data reported by the utility.

In This Chapter

More About the getCCdata Utility

Output From the getCCdata Utility

The getCCdata utility generates output to the screen of the DNCS, as well as to two files that are stored in the /tmp directory of the DNCS. Output generated to the screen tends to roll quickly off the screen; output recorded in files stored on the DNCS can be examined at the system operator's convenience.

Output from the getCCdata utility is divided into two parts. The first part lists any errors uncovered during examination of CableCARD-related components of the DBDS. The second part provides supporting data for the first part. Errors uncovered by the getCCdata utility are clearly marked as such. The system operator or engineer can scan the error report for any errors. Should the report reveal the presence of an error or two, the system operator or engineer could then obtain additional information by examining the supporting data.

The final line of each part of output provides the name (including path) of the files that are written to the DNCS.

- For the error part, the entry is similar to **The location of the output file is /tmp/CableCardErrors.out.050510_1424.doc**.
- For the data part, the entry is similar to **The location of the output file is /tmp/CableCardData.out.050510_1423.doc**.

When to Run the getCCdata Utility

The getCCdata utility was designed as a troubleshooting tool. Sites that suspect they are having problems with their CableCARD system are encouraged to run this utility to see what, if any, issues are uncovered.

Some sites take a more hands-on approach to the management of their CableCARD system. Our engineers encourage these sites to run the getCCdata utility on a more regular basis, looking for things that may change from day to day.

In both situations, engineers at Cisco Services can help system operators troubleshoot or interpret the data revealed by the getCCdata utility.

Run the getCCdata Utility

Running the getCCdata Utility

Follow these instructions to run the getCCdata utility.

1. If necessary, open an xterm window on the DNCS.
2. Type **getCCdata.ksh** and then press **Enter**. The utility runs, generating data to the screen of the DNCS, as well as writing data to two files stored in the /tmp directory of the DNCS.

   Note: On most systems, the utility takes only a minute or two to run.

Sample Output from the getCCdata Utility

The following table lists some sample output from the getCCdata utility. The table includes two columns. The first column includes sample output from the error-reporting portion of the utility; the second column contains the supporting data. There is a one-to-one relationship between the two parts of the output. For each entry in the error part, there is a corresponding entry in the data part.

Note: The first row of the following table includes the actual headings that introduce the the error portion and the data portion of the output generated by the getCCdata utility. As shown in the table, the heading contains the name of the corresponding file, the current version of the getCCdata utility, and the version of software that is running on the DNCS.

Error Report	Data Report
CableCardErrors.out.050510_1424.doc getCCdata.ksh v1.09 DNCS Version: 3.5.0.14	CableCardData.out.050510_1423.doc getCCdata.ksh v1.09 DNCS Version: 3.5.0.14
*****Check 1: CCardServer running:***** ========== Yes	*****Check 1: CCardServer running:***** ========== dncs 25974 587 0 Apr 14 ? 0:18 Logger -g -n /dvs/dncs/tmp/CCardServer dncs 26303 25974 0 Apr 14 ? 21:30 /dvs/dncs/bin/CCardServer

Error Report	Data Report
*****Check 2: CCardServer log files:***** ========== Yes: There are multiple CCardServer log files.	*****Check 2: CCardServer log files:***** ========== -rw-r--r-- 1 dncs dncs 2213862 Apr 17 09:58 /dvs/dncs/tmp/CCardServer.000 -rw-r--r-- 1 dncs dncs 2212512 Apr 20 08:12 /dvs/dncs/tmp/CCardServer.001 -rw-r--r-- 1 dncs dncs 2212214 Apr 23 06:22 /dvs/dncs/tmp/CCardServer.002 -rw-r--r-- 1 dncs dncs 2212308 Apr 26 04:33 /dvs/dncs/tmp/CCardServer.003 -rw-r--r-- 1 dncs dncs 2212482 Apr 29 02:46 /dvs/dncs/tmp/CCardServer.004 -rw-r--r-- 1 dncs dncs 2212347 May 2 00:59 /dvs/dncs/tmp/CCardServer.005 -rw-r--r-- 1 dncs dncs 2212411 May 4 23:12 /dvs/dncs/tmp/CCardServer.006 -rw-r--r-- 1 dncs dncs 2212402 May 7 21:25 /dvs/dncs/tmp/CCardServer.007 -rw-r--r-- 1 dncs dncs 2046713 May 10 14:22 /dvs/dncs/tmp/CCardServer.008
****Check 8: loghost in /etc/hosts File***** ========== Yes: There is a single loghost entry in the hosts file.	*****Check 8: loghost in /etc/hosts File***** ========== 192.168.1.1 dncs loghost
****Check 10: Server Defined on BFS:***** ========== Yes	*****Check 10: Server Defined on BFS:***** ========== 41338e6d0000000500002004|podServer|1| 41338e6d0000000700002004|POD_Data|1| 3394330c20a6005e92000001|POD_Data|-1| 3394330c8c5d005e92000001|podServer|-1|
*****Check 12: mmi File on BFS:***** ========== Yes	*****Check 12: mmi File on BFS:***** ========== 563|18|2|9|mmi.txt|/DNCS/POD_Data/mmi.txt|12|41338e6d0000000700002004|3390520b366600293f000001|0|70|-1317659392|1115128521|0|1|

Error Report	Data Report
****Check 16: Cable Card on Type List:**** ========== Yes	*****Check 16: Cable Card on Type List:***** ========== 10|600|734|Explorer 600 CableCARD Rev 1.0|Cisco|||0|
*****Check 24: Files in podServer:***** ========== Yes	*****Check 24: Files in podServer:***** ========== total 2 -rw-r--r-- 1 dncs dncs 60 Apr 14 12:11 podData
*****Check 29: NOTE:***** ========== The location of the output file is /tmp/CableCardErrors.out.050510_1424.doc	*****Check 29: NOTE:***** ========== The location of the output file is /tmp/CableCardData.out.050510_1423.doc

16

Perform a Multi-Line grep with the mgrep Utility

Introduction

The UNIX grep program displays each line of text from a file that matches a specified pattern. Sometimes system operators or engineers might benefit if a few lines preceding and/or following the specified pattern are displayed, as well. Our engineers developed the mgrep utility to accomplish this purpose.

In This Chapter

Display the Help Window for the mgrep Utility

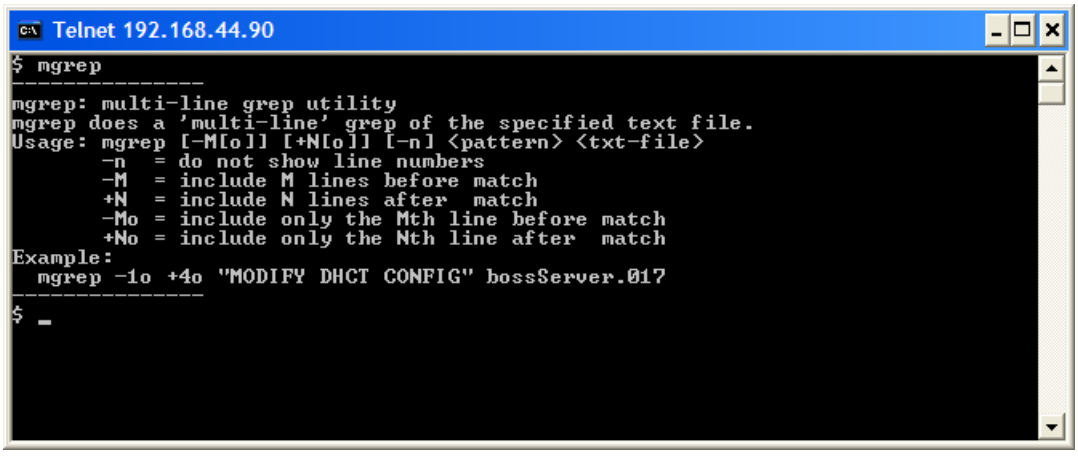
The Help window is often a good place to start when you are unfamiliar with a utility. The instructions in this section describe how to display the Help window for the mgrep utility. In addition, *A Few Notes About the mgrep Options* (on page 134) provides additional detail about the options supported by the mgrep utility.

Displaying the Help Window for the mgrep Utility

Follow these instructions to display the Help window for the mgrep utility.

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

2 Type **mgrep** and then press **Enter**. The system displays the Help window for the mgrep utility.



A Few Notes About the mgrep Options

Reference the preceding illustration as you read through these notes.

- In the example used in the Help window, the mgrep utility is searching through a log file named bossServer.017 for all references to **MODIFY DHCT CONFIG**. Notice that there are quotes around MODIFY DHCT CONFIG. When the pattern for which you are searching consists of multiple words, quotation marks are required around the whole pattern. Notice also that MODIFY DHCT CONFIG is all upper-case. The pattern for which you are searching is case-sensitive.
- The options **-M** and **+N** refer to integers and represent the number of lines before and after the pattern that you want the utility to display. If you want to display 5 lines of data before the pattern and 3 lines of data after the pattern, substitute 5 and 3 for M and N, respectively.
- If you want to display *ONLY* the fifth line of data before the pattern and /or *ONLY* the third line of data after the pattern, append **o** (for only) to the M and/or the N. For example, to display only the fifth line of data before the pattern, and only the third line of data after the pattern, use **-5o** and **+3o**.

The example used in ***Run the mgrep Utility*** (on page 136) helps further illustrate these notes.

Sample Output for the mgrep Utility

This example of sample output uses the following mgrep command:
mgrep -2o +4o "MODIFY DHCT CONFIG" bossServer.017

$ mgrep -2o +4o "MODIFY DHCT CONFIG" bossServer.017

```
  7:Mar 16 08:12:01.221 BossTransManager.C(1668):
  9-MODIFY DHCT CONFIG
 13:DhctMacAddr=00:11:E6:4F:42:7E
---

 22:Mar 16 08:12:01.236 BossTransManager.C(1668):
 24-MODIFY DHCT CONFIG
 28:DhctMacAddr=00:11:E6:4F:F7:84
---
```

Run the mgrep Utility

The instructions in this section describe how to run the mgrep utility.

Running the mgrep Utility

Follow these instructions to run the mgrep utility.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd <required directory>** and then press **Enter**. The specified directory becomes the working directory.

   Example: cd /dvs/dncs/tmp

   Note: The mgrep utility is most likely to be used to search log files. Log files are usually stored in the /dvs/dncs/tmp directory of the DNCS.
3. Type **mgrep [-M[o]] [+N[o]] [-n] <pattern> goqam** and then press **Enter**.

   Example: mgrep -5o +3o "MODIFY DHCT CONFIG" bossServer.017

   Note: This example searches for the pattern MODIFY DHCT CONFIG in the file named bossServer.017. In addition to displaying the lines that contain MODIFY DHCT CONFIG, the utility also displays the fifth line before and the third line after the requested pattern.

17

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.

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

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

May 2012 Printed in USA

Part Number 4020694 Rev B