DBDS Utilities Version 6.3

Installation Instructions and User 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, OCAP, and tru2way are trademarks of Cable Television Laboratories, Inc.

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

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

Publication Disclaimer

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

Copyright

Contents

About This Guide

Purpose

The DBDS Utilities CD contains utility programs that system operators and support engineers can use to manage and troubleshoot the Digital Broadband Delivery System (DBDS). This installation and operation guide contains instructions to install and operate the various software utilities contained on the DBDS Utilities CD.

Scope

The utilities described in this installation and operation guide pertain to systems running the Cisco resident application (SARA), as well as other resident applications.

Audience

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

System Release Compatibility

Refer to *DBDS Utilities Version 6.3 Release Notes* (part number 4031373) for system release compatibility information for the DBDS Utilities.

To obtain the most current version of the *DBDS Utilities Version 6.3 Release Notes* (part number 4031373), please access your company's extranet site. Check your extranet site often as the information is updated frequently.

Document Version

This is the second formal release of this document.

Read These Important Recommendations About the DBDS Utilities

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

- Many of the utilities described in this installation and operation guide interact with the Digital Network Control System (DNCS) database. Be sure you have a current database backup tape before running any of the utilities described in this guide.
- We strongly recommend that system operators run the Doctor Report at least once a day. Instructions for running the Doctor Report are in Chapter 2, ***Analyze System Configuration With the Doctor Report*** (on page 7).
- We strongly recommend that system operators run the checkDB script at least once a month. Instructions for running the checkDB script are in Chapter 4, ***Identify and Correct Database Problems With the checkDB Script*** (on page 41).

1

Install the DBDS Utilities

Introduction

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

- Check the crontab file on the DNCS for the presence of the dbOptimizer program, a program that is used for deleting unneeded EMMs.
- Customize the Doctor Report heading.

In This Chapter

Before You Begin

Introduction

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

Screen-Captured Images

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

The Solaris sar Utility

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

Example: Type **man sar** and then press **Enter** from the command line.

Installation of the Doctor Report Utility

The DBDS Utilities installation script removes the old version of the Doctor Report software from the /export/home/dncs/doctor directory, and installs the new version of the utility in the /dvs/dncs/Utilities/doctor directory. Be aware, however, that the installation process removes only the old executable Doctor Report scripts. Any old Doctor Report text files that you might have saved to the DNCS are not removed during installation.

DBDS Utilities Installation Instructions

Follow these instructions to install the latest version of DBDS Utilities onto the DNCS and Application Server.

Notes:

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

1 Open an xterm window on the DNCS.

2 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 Choose one of the following options:

   - If you are going to install the DBDS Utilities from a CD, continue with step 4.
   - If you are going to install the DBDS Utilities from a directory on the DNCS, follow these instructions.

     a Type **cd [DBDS Utilities package source directory]** and then press **Enter**.

     Note: Substitute for [DBDS Utilities package source directory] the directory in which the installation package already resides.

     b Skip to step 7.

4 Insert the DBDS Utilities CD into the CD-ROM drive of the DNCS.

5 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

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

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

7 Type **install_pkg** and then press **Enter**. The system lists the DBDS Utility packages it plans to install and displays a confirmation message.

8 Type **y** and then press **Enter**. The system installs the DBDS Utilities.

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

DBDS Utilities installation complete
Be sure to review for errors and save a log file!
dbOptimizer cron entries are no longer configured
by package installation. You must run
/dvs/dncs/bin/setDbOptCron if you wish for
dbOptimizer to run automatically.

Note: For additional SAIdbdsutils package installation messages, refer to the installation log file stored at **/var/sadm/system/logs/SAIdbdsutils_x.x.x.x_install.log**.

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

11 If you installed from a CD, type **eject** and then press **Enter**. The system ejects the CD.

12 Remove the CD, if necessary.

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

14 Go to ***Verify the crontab Entry*** (on page 5).

Verify the crontab Entry

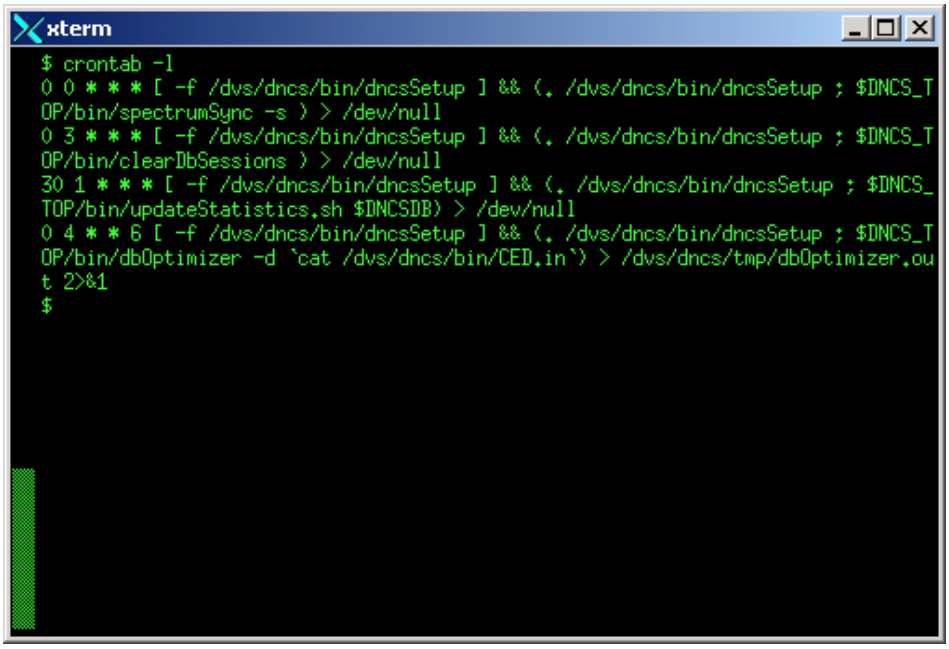
After installing the DBDS Utilities software onto the DNCS, inspect the crontab file to verify that the file contains an entry for the dbOptimizer program, and that it contains no entry for the camEmmDeleter program. Follow these instructions to inspect the crontab file.

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

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

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

Note: The "l" is a lowercase L.



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

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

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

- If **yes**, call Cisco Services for assistance in removing the entry.
- If **no**, go to ***Customize the Doctor Report*** (on page 6).

Customize the Doctor Report

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

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

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

Customizing the Doctor Report

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

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

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

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

2

Analyze System Configuration with the Doctor Report

Introduction

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

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

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

Important: We strongly recommend that system operators run the Doctor Report at least once a day.

This chapter provides the following information about the Doctor Report:

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

In This Chapter

Run the Doctor Report

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

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/Utilities/doctor** and press **Enter**. The /dvs/dncs/Utilities/doctor directory becomes the working directory.
3. Type **doctor** and press **Enter**. The system generates a list of parameters that you can use to run the Doctor Report.

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

```
scooby:/dvs/dncs/Utilities/doctor$ doctor

= Doctor sofware version 6.2.0.2 =
= Doctor package version  =
  doctor -agestpbinqhcrx [ vd ] or
  doctor [-c<number>]

        a - (almost) All options (except q and x)
        g - General Info: DNCS info, installed software info, DNCS and
            App Server disk utilization, DNCS and App Server swap space,
            database utilization, database extents, load average, DNCS
            and App Server debug flags, tracing levels, DNCS and App
            Server processes, DNCS and App Server corefiles, DNS, check
            force tune for valid service, dncs license check, large log file che
ck
            DNCS install options
        e - Element Info: DHCT state summary, DHCT type summary, active
            elements, mod slot tolerance, source, source definitions,
            segments, sessions, subscription packages, EMMs expiring soon.
        s - SI Info: SI_INSERT_RATE, system time message, distinguished
            SI QAM, SI out of band interval.
        t - Time Info: DNCS and App Server time sync, timezone, DST.
        p - PPV Info: PPV services and events, PPV and SAM service
            discrepancies, event use services, PPV files, phoneactivetime,
            EUT, GBAMs.
        b - BFS Info: BFS carousels, BFS sessions, BFS source definitions.
        i - IPG Info: IPG collector, IPG data files.
        n - Ping Elements: QPSK Ethernet, QPSK RF, QAM, NETCRYPT, BIG, TED.
        q - Check for quarantined qams and ping elements.
            This option is NOT included in all (-a).
        x - Check one-one correspondence of DHCTs and serial numbers.
            This option is NOT included in all (-a).
        v - Verbose mode: Detailed output, even if OK.
        d - Suppress screen output. Write to output file only.
        h - Generate this help text.
        c - Clean up (delete) all but the last (number) doctor reports.
            Use this switch independently of all others. Report NOT GENERATED.


        r - and one of the following options:
            hubqamList      - list what hub are associated to which QAMs
            smdgInfo        - list SMDG (StatMUX Dejitter Group) and respective
GQAM
            sdbsgInfo       - list SDB Service Group Mini Carousel Info
            genericQamInfo  - display generic QAMs and IPs
            dualGbeGqamInfo - display generic QAMs and IPs
            sdbInfo         - display SDB server info and status
            pcgInfo         - display PCGs info and status


One or more of the a, g, e, s, t, p, b, i, n, c, x or q options is required.
d and v are optional but should be used with a required option.
Option order is irrelevant.

        Note the q option must be explicitly chosen.  It can be time consuming.
        The q option automatically sets the v (verbose) option and pings and che
cks rpc bind for qams.
scooby:/dvs/dncs/Utilities/doctor$
```

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

Results:

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

Example: The system saves the report with a name similar to **report.061026_0921.doc**.

Notes:

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

Test the Connection to the DNCS (-q Option of the Doctor Report)

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

Understand the Data in the Doctor Report Fields

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

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

Important:

- Anytime an unexpected or new error appears in the Doctor Report output or if defined thresholds are about to be reached, contact Cisco Services for assistance.
- The Doctor report uses the term "DHCT," which is an acronym for Digital Home Communications Terminal. DHCT. DHCT is a specialized name for a digital set-top box.

Important Note Regarding Rovi Corporation Sites

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

System Name

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

Note: If the System Name field does not reflect the name of your system, follow the instructions in ***Customize the Doctor Report*** (on page 6) in Chapter 1.

All SAI Installed Package Information

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

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

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

DNCS Info

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

Platform & CPU

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

RAM

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

Swap Partition

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

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

Disk Info

The Disk Info field displays configuration information for the server from a partition point of reference (rather than a metadevice point of reference).

Additionally, the Disk Info field reports on the configuration of the server's mirrors.

Checking the Status of the Meta Devices of the System

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

Solaris Uptime

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

DNCS Uptime

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

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

DNCS Disk Partition Utilization

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

Important: Our engineers recommend that no partition exceed 85 percent utilization.

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

App Server Disk Partition Utilization

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

Important: Our engineers recommend that no partition exceed 85 percent utilization.

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

DNCS and App Server Swap Space

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

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

Important: Our engineers recommend that the DNCS and Application Server swap space be greater than 200 MB.

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

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

Basic System Performance Stats

There are 5 sets of performance statistics reported under the Basic System Performance Stats header. An explanation of each set follows.

CPU Performance

The CPU Performance field uses the prstat utility to iteratively examine all active processes on the system. As used in the Doctor Report (prstat -c 5 5), the prstat utility sorts output according to CPU usage, takes CPU measurements in 5-second intervals, and issues five separate reports.

Memory Usage

The Memory Usage field uses the prstat utility to iteratively examine all active processes on the system and report upon memory usage of the processes. As used in the Doctor Report (prstat -s size -c 5 5), the utility sorts output according to the size of the process image, takes memory measurements in 5-second intervals, and issues five separate reports.

Per-Processor Stats

The Per-Processor Stats field uses the mpstat utility to report processor statistics in tabular form. Each row in the tabular output represents the activity of one processor. The first table summarizes all processor activity since the last reboot. Subsequent tabular output summarizes activity for the preceding, specified interval. All values in the output are rates listed as events/second, unless specifically noted.

The mpstat utility, as used in the Doctor Report (mpstat 5 5), collects processor statistics in 5-second intervals and produces five reports.

Virtual Memory Stats

The Virtual Memory Stats field uses the vmstat utility to report statistics about kernel threads in the run and wait queue, memory, paging, disks, interrupts, system calls, context switches, and CPU activity.

As used in the Doctor Report (vmstat 5 5), the vmstat utility collects virtual memory statistics every 5 seconds and issues five separate reports.

Disk Stats

The Disk Stats field uses the iostat utility to iteratively examine terminal, disk, and tape input/output activity, as well as CPU utilization. The first line of output pertains to the time since the last reboot. Subsequent lines pertain to the specified prior interval, only.

For the Doctor Report (iostat -xPnMz 5 5), the utility produces extended statistics and displays names in descriptive per-partition format (rather than per-device format). Data is displayed in MB/second terms. The utility collects statistics every 5 seconds and issues five separate reports.

Database Tablespace Report

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

- **Database space usage summary**—provides detailed and summary information about database tables and extents.
  Notes:
  - This data appears only if there are database tables or indexes with 10 percent or less of free allocated space. If there is a table or an index that has 10 percent or less of free allocated space, the system will provide another extent for that table or index to grow.

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

- **Preallocated summary database space usage**—provides summary data for the preallocated database space.
- **Current physical database space usage**—provides summary data for the physical database space.
- **Total free database space**—reports the total amount of free pre-allocated and physical database space.

- **Recalculated future free database space** —If the detail under the **Database space usage summary** section lists a table or an index that has 10 percent or less of free allocated space, this section provides a new calculation of preallocated database space based upon the additional extent that will be used.
  Notes:
  - This data appears only if there are database tables or indexes with 10 percent or less of free allocated space.
  - Call Cisco Services if the Recalculated future free database space section produces a warning.

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

DNCS Database Check

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

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

Database Spaces and Chunks

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

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

Database Extents for dncsdb

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

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

Database Extents for appdb

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

Database Backup Check

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

Notes:

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

Check for clearDbSessions Activity

The Doctor Report checks to ensure that the clearDbSessions entry in the crontab file of the DNCS is active, and has not been converted into a comment.

DNCS Load Average

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

Important: Our engineers recommend that your DNCS load average remain under 2.0.

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

Current Appserv Debug Flags Set

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

Notes:

- Under most conditions, we recommend that only debugging flags R or J be enabled for the Application Server.

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

Appserv Tracing Levels

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

Notes:

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

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

DNCS Logging Levels

The DNCS Logging Levels field lists all DNCS processes and the level of logging activity that is associated with each process.

System operators can set logging levels for the DNCS processes by clicking **Logging** from the **Utilities** tab of the Administrative Console.

DNCS Processes

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

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

- Check the DNCS for core files.
  Note: The ***Recent DNCS Corefiles (last 2 days)*** (on page 21) field, lists recent DNCS core files.
- If the DNCS has a core file, contact Cisco Services.
  Note: Cisco Services may request that you send them the core file for analysis.
- Use the dncsControl utility to restart the stopped process(s).

App Server Processes

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

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

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

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

- Check the Application Server for core files.
- If the Application Server has a core file, contact Cisco Services.
  Note: Cisco Services may request that you copy the core file and send it to them for analysis.
- Use the appControl utility to restart the stopped process(s).

Recent DNCS Corefiles (last 2 days)

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

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

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

Recent App Server Corefiles (last 2 days)

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

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

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

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

DNS Check

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

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

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

Force Tune / Valid Service Check

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

DNCS License Check

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

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

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

Unused SAM URL Check

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

DNCS Non-Cisco Conditional Access Check

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

DNCS File Size Check

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

Last Logging Time Stamp for Selected Processes

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

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

OCAP and TSBroadcaster Information

The data in the OCAP™ and TSBroadcaster Information field supplies the following information:

- Checks to see if OCAP is enabled as a licensed feature
- Checks to see if the OCAP Manager process is running
- Pings the third-party TSBroadcaster server for connectivity
- Reports on the data in the extended application index table (XAIT)

DHCT Status Summary

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

DHCT Type Summary

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

Notes:

- The system also reports the number of DHCTs in the database of type NULL.
- A DHCT of type NULL represents a DHCT that has no record in the database, but has attempted to sign on to the system.
  Important: Call Cisco Services if you have a large number of DHCTs, relative to system size, with a type of NULL.

DHCTs with EMMs Expiring in 15 days

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

Notes:

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

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

EMM Distributor Cycle Summary

The EMM Distributor Cycle Summary field shows data from the emmDistributor process at two moments in time: just prior to the start of a cycle, and then at end of a cycle.

Data pertaining to the start of a cycle (which is actually shown in the second block of output), **EMM Distributor Cycle Start**, lists the parameters that the emmDistributor process is using to calculate the expected cycle duration. Additionally, a summary of the allocation of bridges (and associated DHCT population numbers) to emmDistributor threads, is also displayed.

The second snapshot, **EMM Distributor Cycle Complete**, displays data that was captured as the cycle completes. This data contrasts the expected cycle completion time to the actual cycle completion time.

VER, OS and ResApp files

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

CVT Configuration Check

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

DHCT counts per QPSK/CMTS Bridge

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

Active Elements

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

Offline QAMs

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

Mod Slot Tolerance

The data in the Mod Slot Tolerance field confirms that the slot tolerances of all QPSK

modulators is 2.2 microseconds.

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

Sources, Source Definitions, Segments and Sessions

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

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

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

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

Source Definitions for Active CF Sessions

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

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

Active Subscription Packages

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

In-Band SI_INSERT_RATE Check

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

the SI_INSERT_RATE variable.

Notes:

- The SI_INSERT_RATE variable represents how long it takes for a DHCT to get system information (SI).
- The calculated value is based on the number of hubs and virtual channel table (VCT) entries.

- The Doctor Report verifies that the current value of the SI_INSERT_RATE variable is 100 percent of the calculated value. A rate of 0 (zero) indicates that SI is only being sent out-of-band.
- The Doctor Report also verifies that the SI_INSERT_RATE variable is spelled correctly and is shown with all capital letters in the DNCS .profile file.

Important: Note these important points about the SI_INSERT_RATE variable:

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

SI Out-of-band Interval

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

System Time Message Delivery

If debug flag **+DE** is set for the siManager process, the data in the System Time Message Delivery field confirms whether the system time message (STM) has been sent to DHCTs within the past 12 seconds.

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

Distinguished SI QAM

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

Notes:

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

QAMs Not Associated With Either a Hub or Service Group

The data in the QAMs Not Associated with either a Hub or Service Group field lists those QAM modulators that are not associated with a hub or a service group. Unless

a QAM is configured to deliver SI, it should be associated with a hub.

Duplicate QAM Frequencies Within Service Groups

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

Primary Netcrypt

The Primary Netcrypt field provides data concerning the Netcrypt Bulk Encryptor. Data displayed includes:

- Netcrypt system time
- Software versions
- Status, including component, process, and processor status
- Hostnames
- IP addresses

SDB Servers Information

The SDB Servers Information field provides system operators with data that pertains to their Switched Digital Video servers. Information provided in the SDB Servers Information field includes:

- Server name
- Server IP address
- Online status
- Primary or secondary status
- Installed software version
- Software image download string
- Software image executable string
- Maximum number of sessions
- Server status (active, offline, standby, unresponsive)

SDB Service Group Mini Carousel Info

The SDB Service Group Mini Carousel Info field displays information that pertains

to where set-tops obtain SDV service group mapping and configuration data.

StatMUX Dejitter Groups

The StatMUX Dejitter Groups field provides a list of statMux dejitter groups, as well as the GQAM and output ports to which they are assigned.

Generic QAMs

The Generic QAM field provides a list of third-party QAMs, and includes the type of QAM, the name of the QAM, as well as the IP address of the QAM.

Dual GbE GQAMs

The Dual GbE GQAMs field lists the GQAMs that have dual GbE input, as well as the port configurations for each GbE port.

DNCS/App Server Time Sync

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

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

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

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

Timezone and Daylight Savings Time Check

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

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

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

PPV Services and Events

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

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

PPV and SAM Service Discrepancies Found

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

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

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

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

PPV Event Use Service Information

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

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

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

PPV File Check

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

- The files (**advance0, immediate, index,** and **services0**) in the /dvs/appFiles directory have been updated within the last hour.
  Note: On a live system, this is a general health indicator of PPV service because it confirms that the **ppvServer** and **ppvFileserver** processes are regularly updating PPV files.
- All events in the **immediate** file are also in the **advance0** file.

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

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

PPV Events phoneactivetime Check

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

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

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

EUT Update Check

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

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

GBAM Delivery

Assuming debug flag **+DE** is enabled for the camPsm process, the data in the GBAM Delivery field verifies that time of day (TOD) and purchase GBAMs are delivered.

Notes:

- Purchase GBAMs can be verified only if there are PPV events with an open Buy window.

- Ideally, purchase GBAMs are delivered every 20 seconds and TOD GBAMs every 15 seconds. However, the Doctor Report verifies that these GBAMs have been delivered within the previous 60 seconds.

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

BFS Carousel and OSM Sessions Status

The data in the BFS Carousel and OSM Sessions Status field reports on the status of the BFS carousels and the OSM sessions. The output identifies whether carousels are inband (IB) or out-of-band (OOB), the source ID, the operational status of the carousels, the data rate, the amount of data carried, the indication interval of each carousel, the enabled state, as well as the total time required for each carousel to transmit all its data in one cycle (ACCT).

Additionally, the output lists the aggregate data rate for the inband and out-of-band carousels, which does not include data rates for disabled sources. This field reports for site DNCS as well as any remote site, if applicable.

BFS Session Status

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

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

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

Miscellaneous BFS Check

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

- No more than one dataCarousel process is running for a given BFS source.
- All BFS source definitions are present and are not duplicated.
  Note: If a BFS source definition is not present, the source definition will not be in SI and the DHCT will be unable to tune to that carousel.
- No BFS source is encrypted.

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

- Refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377), or your appropriate upgrade installation instructions for assistance in setting data rates.
- Rovi sites, or sites running interactive applications (VOD, games, etc.) may

generate data rate errors. Refer to one of the previously mentioned documents for assistance in setting data rates.

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

IPG Collector Report

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

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

IPG Data Files

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

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

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

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

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

Ping All Active Elements

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

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

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

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

DoctorRemote

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

- System Name
- All SAI Installed Package Information
- LIONN Info
- Virtual CPUs
- Physical Memory Configuration
- IO Devices
- Disk Info
- Checking the Status of the Metadevices
- LIONN Disk Partition Utilization
- LIONN Swap Space

- LIONN Basic System Performance Stats
- LIONN Database Log Check
  Note: This field appears only for remote sites. The LIONN Database Log Check field reports on the size of the /dvs/lionndb/liondb.log and /dvs/lionndb/lionnconnection.log files.
- LIONN Database Process Check
  Note: This field appears only for remote sites. The LIONN Database Process Check field reports on whether the Informix daemon processes are running.
- LIONN Load Average
- Current LIONN Debug Flags Set
- LIONN Processes
- Recent LIONN Corefiles (last 2 days)
- DNS Check
- Force Tune / Valid Service Check
- LIONN File Size Check
- Timezone and Daylight Savings Time Check
- EUT Update Check
- Ping All Active Elements

3

Monitor the Status of System Metadevices with the check_metadevices Utility

Introduction

The check_metadevices utility constantly monitors the state of the metadevices on an Enterprise 450 or Sun Fire V440, V445, V880, and V890 server, and then reports any errors it finds. The utility runs automatically after you install the DBDS Utilities; system operators or engineers do not have to invoke any specific commands to run the check_metadevices utility.

Note: A metadevice is a group of physical devices accessed through a virtual or logical device.

In This Chapter

Understanding the check_metadevices Utility

Supported Hardware Platforms

The check_metadevices utility runs on an Enterprise 450, Sun Fire V440, V445, V880, and V890 server, and the Sun Netra T5440 server; the utility does not run on an Enterprise 250 server. System operators do not have to run any special command to run the check_metadevices utility. The utility runs automatically after you install the DBDS Utilities.

Three Ways of Reporting Errors

The check_metadevices utility reports any metadevice errors it finds in the following three ways:

- The utility displays a window on the DNCS that describes the error, as well as the time and date the error occurred.
- The utility sends e-mail that notifies the dncs user and root user of the error.
- If the site supports the Alarm Manager network management system, the check_metadevices utility reports those errors to the Alarm Manager software.

Call Cisco Services

System operators should always call Cisco Services before troubleshooting or trying to correct any errors reported by the check_metadevices utility.

Important: Do not try to correct any errors reported by the check_metadevices utility yourself. Always call Cisco Services first.

4

Identify and Correct Database Problems with the checkDB Script

Introduction

The checkDB script was developed to identify and correct various potential problems in the DNCS database. This chapter describes some of the potential database problems identified by the checkDB script, and provides instructions for running the script.

In This Chapter

Overview of the checkDB Script

Types of Database Problems

The following list identifies some of the potential problems that the checkDB script identifies:

- DHCT records in the DNCS database that do not have serial numbers
  Notes:
  - DHCTs are required to have serial numbers. DHCT serial numbers are now used mainly with third-party applications such as the video-on-demand application.
  - If the output of the checkDB script shows that you have DHCTs in your database without serial numbers, you can contact Cisco Services to assign serial numbers to those DHCTs.
- Records in various tables in the DNCS database that do not have required corresponding records in other tables
  Notes:
  - Records that do not have required corresponding records in other tables are known as orphaned records.
  - You can configure the checkDB script to automatically remove orphaned records from the DNCS database.
- DHCTs with a status of in-service that have EMMs ready to expire
  Note: The checkDB.sh script will prompt you to either restage or delete DHCTs with EMMs ready to expire.
- Sites that are likely to experience a problem due to the DNCS generating duplicate subscription EMMs. (This is a very rare condition and is included in the checkDB utility as a precaution.)
  Notes:
  - The checkDB script identifies this condition through the Highest eu_eid used for subscription pkgs field.
  - Sites where this value exceeds 220 should report this condition to Cisco Services.

Prerequisite

Be sure that you have a current backup of your DNCS database before running the checkDB script with the *-f* or *-F* options. Refer to the appropriate copy of the backup and restore procedures for detailed instructions on how to back up the DNCS database.

Note: The checkDB script makes no database changes when run with no options or with the *-v* option. The script may change the database when run with the *-f* or *-F* options. Refer to ***Run the checkDB Script*** (on page 44) for additional information concerning the options associated with the checkDB script.

The deleteDhct Utility

When used with the *-f* or *-F* options, the checkDB script calls the deleteDhct utility in order to delete DHCT records from the database. The logic of the checkDB script is such that all references to the deleteDhct utility occur automatically; no user intervention is required. The deleteDhct utility is included on the DBDS Utility CD.

We designed the deleteDhct utility to completely delete DHCT records from the DNCS database. It deletes a single DHCT or can delete all DHCTs in a list containing DHCT MAC addresses that are presented in a text file.

The logic in the deleteDhct utility is very good at finding all database rows in all the different DHCT tables that contain or used to contain records for the specified DHCT(s). The deleteDhct utility deletes orphaned DHCT records. While orphaned DHCT records are less common now than they have been in the past, at one time duplicate database rows were generated for RMA DHCTs when they were returned from repair with a changed secure_micro address.

Run the checkDB Script

The checkDB script examines the following tables in your DNCS database for possible error conditions:

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

You can run the checkDB script in three possible modes:

- Run the checkDB script in default mode (with no options) to generate a detailed report listing possible error conditions in the database. When the checkDB script is run in default mode, the script does not correct any error conditions it finds. The script merely generates a report listing potential error conditions.
- Run the checkDB script in "fix" mode to automatically delete certain orphaned records from the database. When run in "fix" mode, with the *-f* or *-F* option, the script generates a report listing potential error conditions and lists any changes it made to the database as a result of running the script in "fix" mode.

  Important: Our engineers recommend that you run the script with no options before running the script with one of the "fix" mode options.
- Run the checkDB script with the *-v* option to display only the version number of the checkDB script.

Running the checkDB Script with No Options

Running the checkDB script with no options generates a detailed report that lists possible error conditions in the database. Follow these instructions to run the checkDB script with no options, and then to examine the logfile.

1. If necessary, open an xterm window on the DNCS.
2. Type **checkDB.sh > /dvs/dncs/tmp/checkDB.[today's date]** and then press **Enter**.

   Notes:

   - Substitute today's date for [today's date].

     Example: checkDB.sh > /dvs/dncs/tmp/checkDB.081601
   - This command directs the output from the checkDB script to a file in the /dvs/dncs/tmp directory on the DNCS. We recommend that you direct the output to a file for you to examine later because the output would otherwise

scroll too quickly off the screen for you to examine.

3 After the script has finished running, type **cd /dvs/dncs/tmp** and then press **Enter**. The /dvs/dncs/tmp directory becomes your working directory.

4 Type **more [name of logfile]** and then press **Enter**. The logfile opens using the UNIX more utility.

Note: Substitute the name of the logfile you created in step 2 for [name of logfile].

Example: more checkDB.081601

5 Refer to ***Sample Logfile and Analysis*** (on page 45) as you examine the logfile created by the checkDB script.

Notes:

- Press the **Spacebar** to page through the output file.
- Press the **Ctrl** and **C** keys simultaneously to close the output file when you are finished.

Sample Logfile and Analysis

Use the following example when you examine the logfile you opened in step 4.

Note: The following example of the logfile contains line numbers. Line numbers do not actually appear in the logfile, but are included here to facilitate an explanation of some of the items contained in the logfile.

Sample Logfile

==========

1 # Tue Dec 2 15:25:43 EST 2003

2 # The total number of rows in hct_profile = 156278.

3 # The total number of rows in secure_micro = 40378.

4 # Highest eu_eid used for subscription pkgs = 111.

5 # DHCT Registration is set to 'Administrative Gateway'.

6 # There are 65407 MAC addresses with No DHCT Serial Number

7 # Rows defining SN/MAC should be added for these boxes in 'pdsernummap'

8 00:02:DE:11:72:EE

9 00:02:DE:14:C3:72

10 (65405 other addresses listed here)

11 # There are 233 SN/MAC matches that should be DELETED from 'pdsernummap'

12 SABBGZJWC|00:02:DE:49:F7:6C|

```
SABBHCQTS|00:02:DE:4A:73:20|
SABBHBQRF|00:02:DE:4A:34:3A|
(230 other addresses listed here)
# There are 0 secure_micro rows with mac_addr not in 'hct_profile'
# There are 5 secure_micro MACs with sm_serial_num not in 'hct_profile'
# These sm_host_mac_addr rows MUST be deleted from 'secure_micro'!
# (They cause 'mismatch' problems with EMM regeneration in camAuditor)
# (Use the 'deleteDhct' utility to delete these.)
00:01:A6:05:33:70|00:02:DE:FC:50:14|
00:01:A6:20:66:1A|00:02:DE:F0:A0:5B|
00:01:A6:41:B2:80|00:02:DE:F0:93:8E|
00:01:A6:30:A3:A4|00:01:A6:7C:53:F6|
00:01:A6:41:35:64|00:01:A6:80:EE:8E|
# There are 0 sm_auth_profile rows with no secure_micro parent
# There are 0 sm_pkg_auth SMSNs with no secure_micro parent
# There are 502 boxes having EMMs with sm_serial_num not in 'hct_profile'
# All rows having these sm_serial_num should be deleted from 'emm'
00:01:A6:5D:10:92
00:01:A6:67:54:24
(500 other addresses listed here)
# There are 0 pdkeycertificates having no parent 'hct_profile'
# There are 0 boxes with no 'pdkeycertificates'
# There are 14 boxes with no 'secure_micro', but with very-old EMMs.
# These boxes are in the database, but were incompletely staged
# over 90 days ago.  They should be re-staged or deleted.
00:02:DE:1D:4C:5A
00:02:DE:1B:6E:6A
00:02:DE:53:E4:6A
00:02:DE:58:6A:64
00:02:DE:1C:13:D6
00:02:DE:B2:9F:E6
00:02:DE:14:E1:18
00:02:DE:14:67:EA
00:02:DE:49:BF:3A
00:02:DE:14:16:B8
```

```
48  00:02:DE:13:21:52
49  00:02:DE:16:5A:36
50  00:02:DE:A1:04:D0
51  00:02:DE:10:D9:9C
52  # There are 0 'In-Service' boxes with 'almost-expired' EMMs.
53  # No orphaned authorizations exist...
54  # 3600 boxes have NULL in the hctt_oui, hctt_id, or hctt_revision parameters!
55  # 2 percent is MORE than should be tolerated!!
============================================================
```

Analysis of Logfile

Refer to the preceding logfile as you read through this analysis. Your logfiles are likely to contain similar points of interest.

Analysis of checkDB Logfile	
Line Numbers	**Explanation**
Lines 2 and 3	Lines 2 and 3 indicate how many records exist in the hct_profile and secure_micro tables in the database.
Line 4	Line 4 indicates the maximum value for subscription packages in the eu_eid column in the package table. **Important:** Sites where this value exceeds 220 should report this condition to Cisco Services.
Line 5	Line 5 reports registration configuration. Options are Open Registration and Administrative Gateway. Our engineers recommend Administrative Gateway to prevent DHCTs from being added to your system without your knowledge.
Lines 6 through 10	These lines identify DHCTs that are in the database without serial numbers. Line 6 indicates that there are 65,407 DHCTs in the database without a serial number. Line 8 begins to list them, but the list has been truncated in this example to conserve space. Contact Cisco Services if your logfile indicates that you have DHCTs in the database without serial numbers. Cisco Services will retrieve the list from your DNCS and will insert the correct serial numbers into your database.
Lines 11 through 15	These lines identify 233 DHCTs with serial number and MAC address entries in the pdsernummap table, but without a required corresponding entry in the hct_profile table. The checkDB script therefore concludes that these are orphaned records and recommends that they be deleted.

Analysis of checkDB Logfile	
Line Numbers	**Explanation**
Line 16	This line reports that there are no entries in the secure_micro table of DHCTs that have a MAC address but have no corresponding entry in the hct_profile table.
Lines 17 through 25	These lines identify 5 DHCTs with MAC address entries in the secure_micro table, but without a required corresponding entry in the hct_profile table. The checkDB script therefore concludes that these are orphaned records and recommends that they be deleted.
Lines 26 and 27	These lines indicate that there are no orphaned records in the sm_auth_profile and the sm_pkg_auth tables with respect to the secure_micro table.
Lines 28 through 32	These lines identify 502 DHCTs with serial number entries in the emm table, but without a required corresponding entry in the hct_profile table. The checkDB script therefore recommends that they be deleted.
Lines 33 and 34	These lines indicate that there are no potential error conditions with the pdkeycertificates table.
Lines 35 through 51	These lines identify 14 DHCTs with very old EMMs. The checkDB script prompts you to either restage or delete them.
Line 52	Line 52 indicates that there are no DHCTs in the database with EMMs that are in danger of expiring
Line 53	Line 53 indicates that there are no orphaned authorization records in the database.

Analysis of checkDB Logfile	
Line Numbers	**Explanation**
Lines 54 and 55	These lines indicate that there are 3600 DHCT entries in the hct_profile table with NULL values in the hctt_oui, hctt_id, or hctt_revision fields. These NULL values result from running a script for handling mismatched hardware type errors. **Note:** When the quantity of DHCTs with NULL values in the previously mentioned fields exceeds 1 percent of the DHCTs in the hct_profile table, the checkDB script notifies you.

Running the checkDB Script in "Fix" Mode

Use options *-f* or *-F* to run the checkDB script in "fix" mode. When run in "fix" mode, the script removes certain orphaned records from the database and generates a report that lists potential error conditions.

Follow these instructions to run the checkDB script in "fix" mode.

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

2 Choose one of the following options:

- To run the checkDB script with the *-f* option, type **checkDB.sh -f > /dvs/dncs/tmp/checkDB.[today's date]** and then press **Enter**.

  Example: checkDB.sh -f > /dvs/dncs/tmp/checkDB.081601

- To run the checkDB script with the *-F* option, type **checkDB.sh -F > /dvs/dncs/tmp/checkDB.[today's date]** and then press **Enter**.

  Example: checkDB.sh -F > /dvs/dncs/tmp/checkDB.081601

Notes:

- Substitute today's date for [today's date].
- These commands directs the output from the checkDB script to a file in the /dvs/dncs/tmp directory on the DNCS. Our engineers recommend that you direct the output to a file for you to examine later because the output would otherwise scroll too quickly off the screen for you to examine.

Summary of Conditions Addressed by "Fix" Mode

The following conditions are addressed by running the checkDB script in "fix" mode, using either the *-f* or the *-F* option:

- DHCT serial numbers with missing parent (extra rows in pdsernummap table)
- Records in hct_profile table with no corresponding record in the pdkeycertificate table
- Records in secure-micro table (with MAC address or serial number) with no corresponding record in the hct_profile table
- Records in sm_pkg_auth table with no corresponding record in sm_auth_profile table
- Records in emm table with no corresponding record in hct_profile table

- Orphaned authorization packages

In addition, the -F option can also be used to remove records in the sm_auth_profile table when there is no corresponding record in secure_micro table.

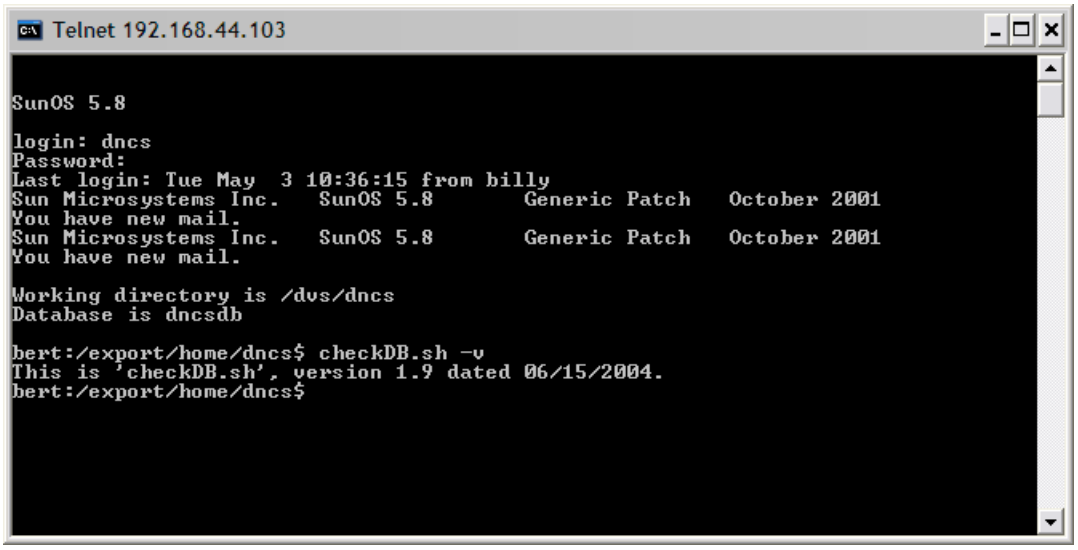
Running the checkDB Script to Display the Version

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

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

2 Type **checkDB.sh -v** and then press **Enter** to display the version number of the checkDB script installed on your system. The system displays the version number of the checkDB script installed on your system.

Example: The version number of the checkDB script displayed in this example is version 1.9.



5

Delete Unused SAM URLs with the chkSamUrl Utility

Introduction

Each time a cable service provider registers a service with the Service Application Manager (SAM), the DNCS assigns the service a unique service ID and, in some cases, a new URL. These URLs are stored in the bulk.tbl file, which is located in the /dvs/dvsFiles/SAM directory of the DNCS.

One of the conditions of the DNCS that the Doctor Report monitors is the size of the bulk.tbl file. When the bulk.tbl file grows too large, the SAM server may be unable to generate valid SAM files. DHCTs may then reboot and display a black screen.

The bulk.tbl file has a maximum file size limit of 65 KB. The Doctor Report displays a warning when the file size exceeds 45 KB and displays an error message when the file size exceeds 55 KB. When the Doctor Report displays a warning or an error message about the bulk.tbl file growing too large, system operators should run the chkSamUrl utility. The chkSamUrl utility allows system operators to delete unused SAM URLs from the DNCS, which reduces the size of the bulk.tbl file.

The instructions in this chapter guide you through the steps of running the chkSamUrl utility.

In This Chapter

Run the chkSamUrl Utility

If the **Unused SAM URL Check** field of the Doctor Report displays a warning or an error message about the size of the bulk.tbl file being too large, you need to run the chkSamUrl utility in order to delete unused SAM URLs. The instructions in this section guide you through the steps of running the chkSamUrl utility.

Example: The following example illustrates a typical warning message from a system where the bulk.tbl file is too large.

Unused SAM URL Check
==========

Used URL Entries: 57
Unused Entries: 261

Warning: SIZE of bulk.tbl above threshold

****

*** Reduce file size and unused SAM URLs, run "chkSamUrl -r" ***
****

Running the chkSamUrl Utility

Complete these instructions to run the chkSamUrl utility in order to delete unused SAM URLs from the system.

1 From an xterm window on the DNCS, type **cd /dvs/dncs/Utilities** and then press **Enter**. The /dvs/dncs/Utilities directory becomes the working directory.

2 Type **chkSamUrl -r** and then press **Enter**.

Results:

- The chkSamUrl script runs and the current database statistics appear.
- A confirmation message appears and asks you to confirm the removal of unused SAM URLs.

```
/export/home/dncs> chkSamUrl -r
-------------------------------------------------------------------------------------------
Removing unused SAM URLs from the database
-------------------------------------------------------------------------------------------
- List current database stats:
SAM URL bulk table:          /dvs/dvsFiles/SAM/bulk.tbl
Last Updated:          Jan 20 23:37
Size:                  51694
Used URL Entries:            57
Unused URL Entries:          261
Warning: size of bulk.tbl above threshold
Do you wish to continue with removal of unused SAM URLs? [y/n]: y
```

3 Type **y**. The chkSamUrl script runs to completion.

Note: If unused URLs were removed from the DNCS, the bulk.tbl file size will not change at this point in the procedure.

Example: Refer to the following example for sample output from the chkSamUrl script:

```
First, backup affected database tables:
DATABASE Table              DATABASE Backup file location
------------------         ---------------------------------
applicationurl                  --> /tmp/applicationurl.unl
samservices                     --> /tmp/samservices.unl
displaychannels.unl             --> /tmp/displaychannels.unl
Backups created:
-rw-r--r--  1 dncs dncs  30839 Jan 25 15:41 /tmp/applicationurl.unl
-rw-r--r--  1 dncs dncs   3442 Jan 25 15:41 /tmp/displaychannels.unl
```

-rw-r--r-- 1 dncs dncs 12593 Jan 25 15:41 /tmp/samservices.unl

Now removing unused SAM URL entries from the database

Database selected
261 row(s) deleted
Database closed

List updated database stats:

SAM URL bulk table:	**/dvs/dvsFiles/SAM/bulk.tbl**
Last Updated:	**Jan 20 23:37**
Size:	**51694**
Used URL Entries:	**57**
Unused URL Entries:	**0**

****

Although the unused SAM URLs have been removed from the database, a SAM Services save will need to be performed in order to get the saManager to acknowledge the changes made to the database.

****

4 Review the updated database statistics, locate the **Size** field, and record the bulk.tbl file size in the following space: _____ KB

5 Locate the **Unused URL Entries** field. Were unused URL entries identified and removed from the database?

- If **yes**, go to step 6.
- If **no** and the bulk.tbl file size is greater than 45 KB, call Cisco Services.
- If **no** and the bulk.tbl file size is less than 45 KB, go to *Minimizing the bulk.tbl File Size* (on page 51).

6 From the DNCS Administrative Console, click the **Application Interface Modules** tab, and then click SAM Service. The SAM Service List window opens.

7 Select any service in the list, click **File**, and then select **Open**. The Set Up SAM Service window opens.

8 Click **Save**. The SAM service is updated and, within 20 minutes, the saManager process will update all files with the current system configuration.

9 Wait at least 20 minutes and, in an xterm window, type **chkSamUrl -l** from the /export/home/dncs directory. The output lists the updates of the current file size and available space in the bulk.tbl file.

Note: The "l" is a lower case L.

10 Verify that the new bulk.tbl file size is smaller than the file size recorded in step 4.

Important: If the new bulk.tbl file size is not smaller than the file size recorded in step 4, call Cisco Services.

11 Go to ***Minimizing the bulk.tbl File Size*** (on page 51).

Minimizing the bulk.tbl File Size

To minimize the bulk.tbl file size and prevent file size issues that could be detrimental to your system, complete the following procedures each time you edit a SAM URL.

1. From the DNCS Administrative Console, click the **Application Interface Modules** tab, and then click **SAM Service**. The SAM Service List window opens.
2. Select the service that you want to update.
3. Click **File** and then select **Open**. The Set Up SAM Service window opens.
4. Record the URL that you are about to edit, _____, and then edit the URL, as needed (for example, to change the application version number in the URL).
5. Click **Save**. The SAM Service List window returns to the forefront.
6. Is the SAM URL that you modified used by multiple services?
   - If **yes**, update the other services to use the new URL, and then go to step 7.
   - If **no**, go to step 7.
7. Select the SAM service that you selected in step 2, and then click the **Select** button that is adjacent to the Application URL box. The Application URL window opens.

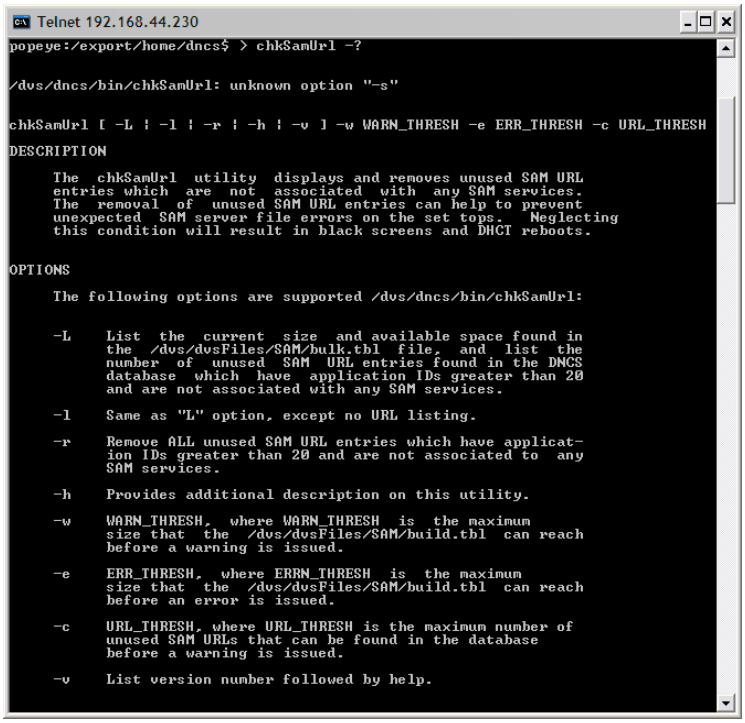
   Important: You are about to perform a deletion procedure. The watchtv, ippv, music, virtchan, and msgview URLs should *never* be deleted from the system.
8. Find and select the URL that you recorded in step 4, and then click **Delete URL**. A confirmation window opens.
9. Click **Yes** to confirm the deletion. The Set Up SAM Service window returns to the forefront.
10. Click **Cancel**. The Set Up SAM Service window closes.

To Learn More About the chkSamUrl Utility

To learn more about the chkSamUrl utility, access the help screen. Follow these instructions to access the help screen.

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

2 Type **chkSamUrl -?** and then press **Enter**. The system displays the help screen associated with the chkSamUrl utility.



3 Call Cisco Services to learn more about any option available for use with the chkSamUrl utility.

6

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 network. 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

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|

Error Report	Data Report
*****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|
****Check 16: Cable Card on Type List:**** ========== Yes	*****Check 16: Cable Card on Type List:***** ========== 10|600|734|Explorer 600 CableCARD Rev 1.0|Scientific-Atlanta|||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

7

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

Important: The use of the getEASdata utility is only intended for those sites that use the DNCS for EAS messages.

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 62) for additional system requirements that must be true for the getEASdata utility to be useful.

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 DNCS is used for EAS functionality.
- The MMMServer debug flag must be checked in the logging WebUI on the DNCS.

Select	Program Name	Emergency	Alert	Critical	Error	Warning	Notice	Info	Debug
○	MMMServer	☑	☑	☑	☑	☑	☑	☑	☑

Note: Refer to the online help for your system for assistance in setting log levels.

- 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 MAC or IP address of a test DHCT in the headend that should have received the EAS message.
- You know which DHCT diagnostic screen displays EAS-related data.

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.

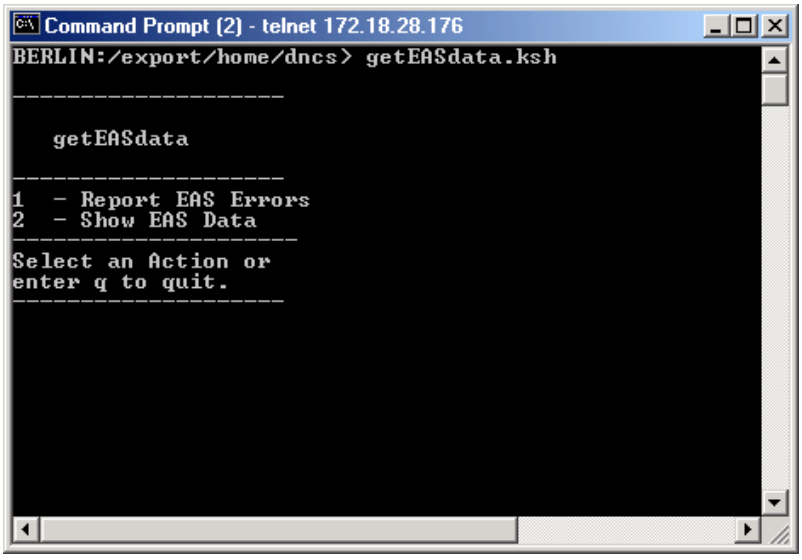
Our engineers recommend that system operators generate each report whenever they run the getEASdata utility, even if the EAS Error Report shows no errors. Examining EAS configuration data may be useful in preventing errors before they develop.

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

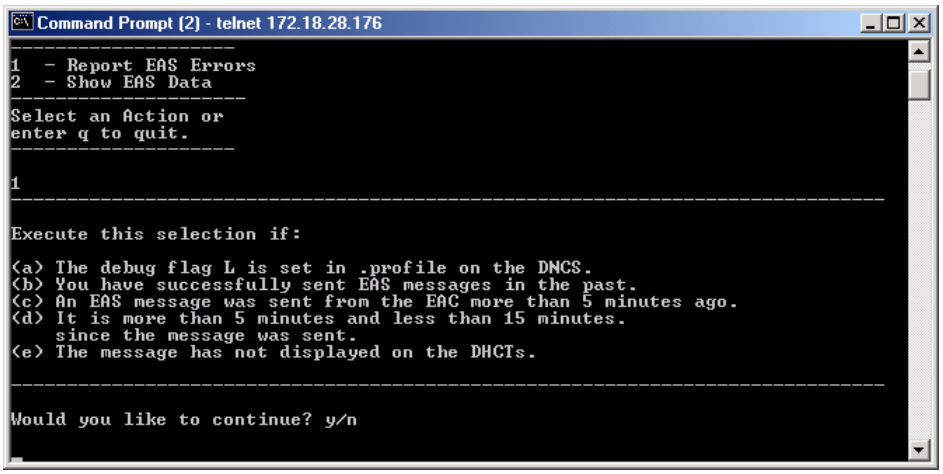
Running the getEASdata Utility

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 displays a confirmation message about 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 71).

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

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:

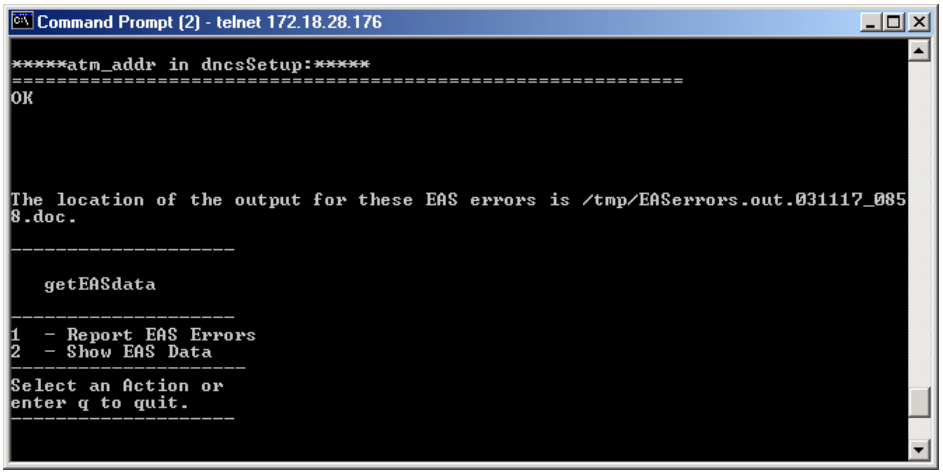
Enter the diagnostic screen the EAS data is on and/or hit return to continue.

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**.

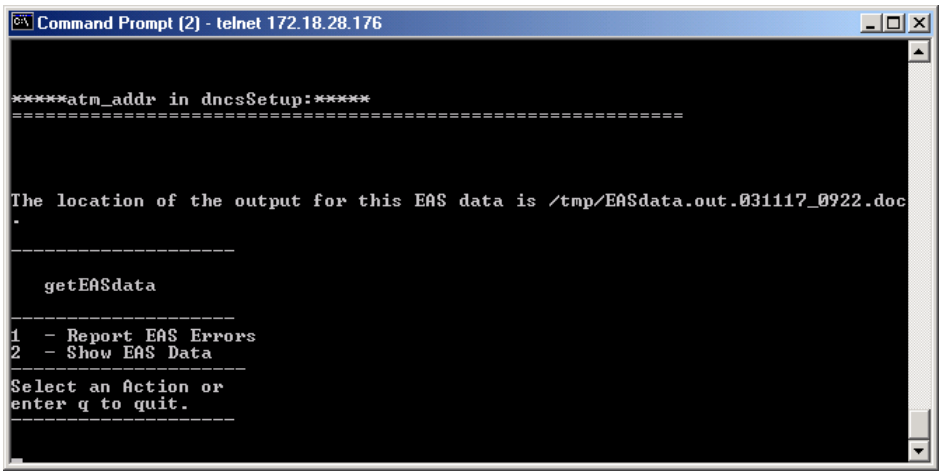
8 Type the IP address of a test DHCT that did not receive the EAS message, and then press **Enter**. The following message appears:

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 76).

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 77) 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 77) 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.

Note: 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.

8

Examine TFTP Information with the listTftpConfigs Utility

Introduction

Each device on the DBDS network has configuration data for that device stored in a specific file on the DNCS. Through the listTftpConfigs file, system operators and support engineers can examine this data at a glance, without having to access the GUI or WebUI for each device, one at a time.

In This Chapter

Supported Options for the listTftpConfigs Utility

The listTftpConfigs Utility Options

The following options are available for use by the listTftpConfigs utility:

- *-a* — The listTftpConfigs utility examines all network element configuration files in the DNCS database for the DNCS and remote sites. When complete, the utility lists those files to the screen of the DNCS. Displayed information includes the name and path of the configuration file, the site ID, the name of the network element, as well as the IP address and MAC address of the network element. Additionally, the output concludes by listing what are known as drop point values ("droppoint" in the output). Drop point values include the current version of code for each component of the network element, as well as the IP address that the network element uses to communicate with the various processes associated with the network element.
- *-f* — The listTftpConfigs utility, by nature, uses cached data to increase speed of reporting. Use of the *-f* option forces the utility to remove cached data and to reload data from the database.
- *-v* — Verbose mode. The *-v* option forces the utility to increase the detail in the data it reports.
- *-V* — The utility displays its version number.
- *-c CFGFILE* — Use [CFGFILE] to display configuration data and drop point values for the specified configuration file, only.
- *-n NENAME* — Use [NENAME] to display configuration data and drop point values for the specified network element, only.
  Example: QAM1
- *-s SITE* — Use [SITE] to display configuration data and drop point values for the specified site, only.
  Example: DNCS(1)

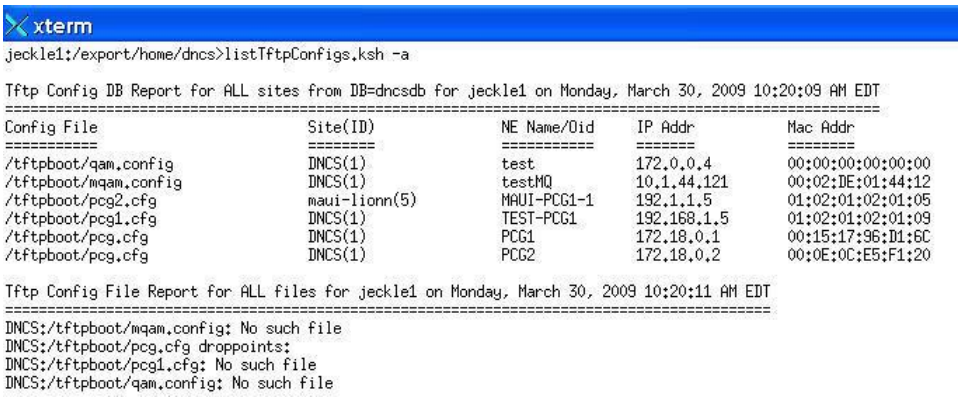
Examine All Configuration Files

When run with the *-a* option, the listTftpConfigs utility displays configuration data and drop point values for all devices on the network. Output from the listTftpConfigs utility, when the *-a* option is used, includes the following:

- Name of the configuration file
- Site (local DNCS or remote server), plus ID
- Name of the network device
- IP address
- MAC address

Complete these steps to run the listTftpConfigs utility with the *-a* option.

1. If necessary, open an xterm window on the DNCS.
2. Type **listTftpConfigs.ksh -a** and then press **Enter**.



Examine a Specific Configuration File

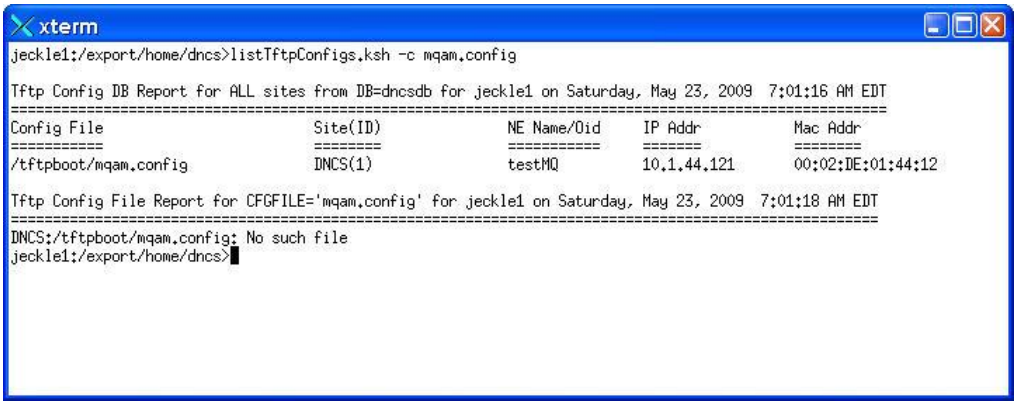
When run with the -c [CFGFILE] option, the listTftpConfigs utility displays configuration data and drop point values for the specific configuration file.

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

2 Type **listTftpConfigs.ksh -c [CFGFILE]** and then press **Enter**.

Note: Substitute the name of the specific configuration file for [CFGFILE].

Example: listTftpConfigs.ksh -c mqam.config



Examine the Configuration Files for a Specific Network Element

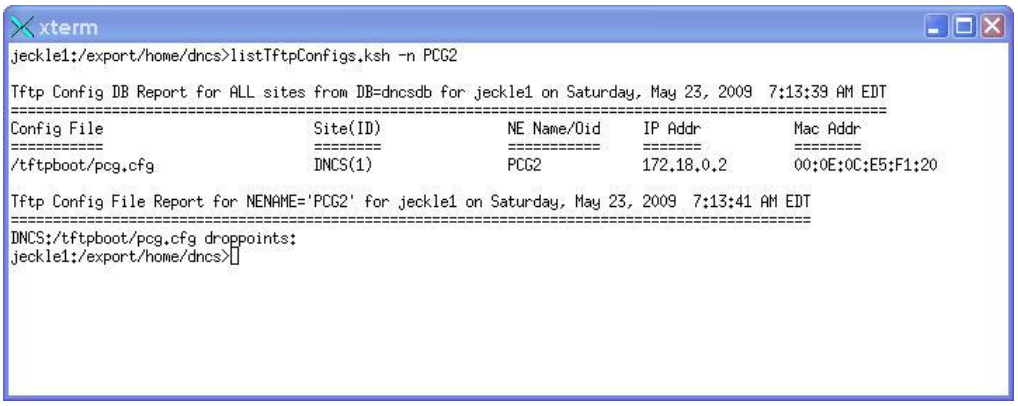
When run with the -n [NENAME] option, the listTftpConfigs utility displays configuration data and drop point values for the specific network element.

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

2 Type **listTftpConfigs.ksh -n [NENAME]** and then press **Enter**.

Note: Substitute the name of the specific network element for [NENAME].

Example: listTftpConfigs.ksh -n PCG2



Examine the Configuration Files for a Specific Site

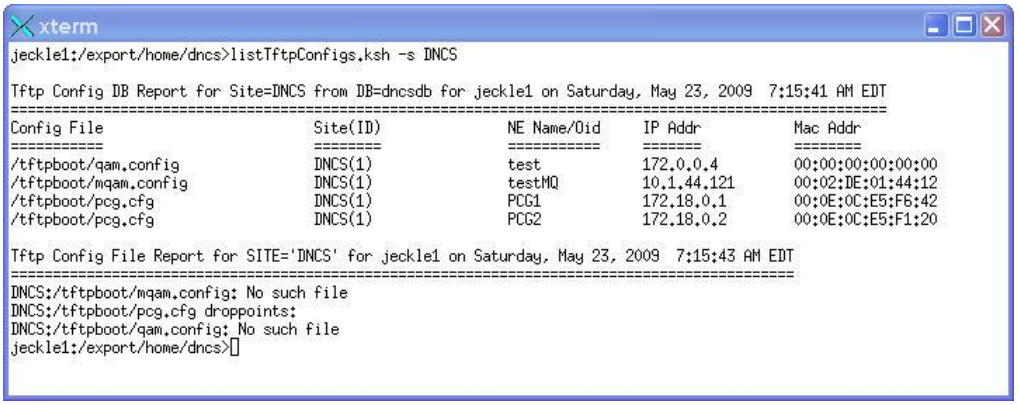
When run with the -s [SITE] option, the listTftpConfigs utility displays configuration data and drop point values for the specified site.

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

2 Type **listTftpConfigs.ksh -s [SITE]** and then press **Enter**.

Note: Substitute the name of the specific site for [SITE].

Example: listTftpConfigs.ksh -s DNCS



Display the Version Number of the listTftpConfigs Utility

Use the *-V* option to display the version number of the listTftpConfigs utility that is currently loaded on the DNCS.

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

2 Type **listTftpConfigs.ksh -V** and then press **Enter**.

9

Monitor DHCTs with the DHCT Status Reporting Utility

Introduction

The DHCT Status Reporting Utility is useful in helping system operators monitor two-way communications between DHCTs and the headend. DHCTs without two-way communications are said to be *non-responding*. Subscribers with a non-responding DHCT are unable to participate fully in the interactive features of the DHCT, while system operators are unable to maximize the revenue potential associated with a DHCT that can establish and maintain two-way communication.

The next section of this chapter, ***Defining Non-Responding DHCTs*** (on page 92), develops the definition of non-responding DHCTs, from the point of view of our support engineers, as well as from the point of view of the system operator. Subsequent sections of this chapter describe the interface of the utility, provide instructions on how to use the utility to poll DHCTs, and explain how to run and interpret the various lists and reports generated by the utility.

Linux Restriction

Note that the DHCT Status Reporting Utility is not compatible with set-tops that use the Linux operating system.

Screen-Captured Images

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

In This Chapter

Defining Non-Responding DHCTs

The DHCT Status Reporting Utility helps system operators minimize system impact caused by non-responding DHCTs. This chapter provides two definitions of non-responding DHCTs, explores some of the reasons DHCTs cannot respond, and describes some of the utilities that are available for system operators to use when managing non-responding DHCTs.

What is a Non-Responding DHCT?

Definition of Non-Responding DHCTs

A non-responding DHCT is a DHCT that is installed in the home of a subscriber and has been configured by the billing vendor to be capable of two-way communication. However, for some reason, the DHCT is unable to maintain or establish a two-way connection.

Note: Two-way communication (or connection) means that a working communication path exists between the headend and the DHCT, as well as between the DHCT and the headend.

What Causes DHCTs to Become Non-Responders?

This section lists some of the conditions that may contribute to DHCTs becoming non-responders.

Conditions in the Subscriber's Home

Subscribers themselves may be responsible for causing some DHCTs to become non-responders. The following list contains a few examples of conditions that might exist in a subscriber's home that could cause the subscriber's DHCT to be a non-responder:

- Subscriber installs a one-way power amplifier — A one-way power amplifier blocks return transmissions.
- Subscriber installs a signal splitter — A signal splitter may reduce the strength of return transmissions or, in some cases, completely block the return transmission.
- Subscriber connects the DHCT to a light switch or a power strip — The DHCT receives no power when the light switch or power strip is turned off.

DHCT Memory and Hardware Issues

The following list contains some examples of DHCT memory and hardware issues that might cause a DHCT to become a non-responder:

- Outdated DHCT operating system — Early versions of the operating system used in DHCTs had memory issues that might cause a DHCT to malfunction.
- Miscellaneous internal failures — Internal components of the DHCT may fail and cause the DHCT to become a non-responder.

Return-Path Network Conditions

The following list contains some return-path network conditions that might cause a DHCT to become a non-responder:

- Laser clipping — Lasers that assist in return path communications may be calibrated incorrectly, resulting in a distortion of signal.
- Over-utilization of existing design — installation technicians may have installed more signal splitters on the network than designed.
- Signal interference — The quality of the return transmission may be poor due to ingress or intermodulation.

Note: Ingress refers to noise from an external source; intermodulation refers to noise generated from within the network.

Hardware Failures on the DBDS Network

The following list contains some DBDS network components that could cause DHCTs to become non-responders should the network components fail:

- QPSK Modulator/Demodulator
  - Buffers full-Available memory for the standard operation of a modulator is limited. Abnormal activity through the modulator may exhaust the available memory and cause the modulator to reboot.
  - DHCT chattering-Numerous DHCTs trying to simultaneously sign on to the network may interfere with return path transmissions and cause modulators to reboot.
  - Excessive numbers of DHCTs assigned to modulator-Too many DHCTs assigned to a single modulator may overwhelm the modulator.
- Router/switch
  - The router or switch is improperly configured.

- The router or switch lacks sufficient processing capability. The router or switch can act as a choke-point in the communication path. In extreme cases, the QPSK modulator may reboot.

DBDS Configuration and Management Issues

The following list contains some conditions that might exist in the configuration of the DNCS that may cause a DHCT to become a non-responder:

- Improper demodulator attenuation management — To maintain a communication link with the QPSK demodulator, DHCTs should transmit at a level between (and including) 25 to 55 dBmV (decibels with respect to 1 millivolt). Over time, DHCT transmission levels may shift too high or too low. The shifting levels may cause significant numbers of DHCTs assigned to a demodulator to become non-responders.
- Improper DHCT inventory management — The DNCS database may fall out of synchronization with the database of the billing vendor. This loss of synchronization may cause the DNCS to try to poll DHCTs that are not actually in subscribers' homes.
- Failure to run the updateOUI utility — DHCTs that attempt to sign on to the network using an incorrect organizationally unique identifier (OUI) are unsuccessful.

What Activities Can Minimize the Non-Responding Condition?

This section summarizes some actions that system operators can take to reduce the non-responding condition on their network.

Review Network Configuration

Often, an examination of your basic network configuration can eliminate some conditions that cause DHCTs to become non-responders. Consider these points as you examine your network:

- Review your existing network topology. Verify that you have separately partitioned each hub. You do not want noise or interference on one hub to affect another hub.
- Review the concentration of DHCTs assigned to your system's QPSK modulators. Verify that DHCTs are assigned as evenly as possible to your system's modulators. Be certain that you never have more than 16,000 DHCTs assigned to any one modulator.
- Verify the integrity of all network elements. Examine your routers and switches for proper throughput. Examine your power supplies, amplifiers, nodes, and taps, elements that are frequently overlooked during an examination of a

network.

- Examine and correct any laser calibration issues present on your network. A laser that is incorrectly calibrated may produce a distorted signal.

Run the signonCount Utility When Downloading DHCT Software

DHCTs lose the contents of their volatile memory when they reboot. After they reboot, DHCTs sign back on to the network and their network configuration data is then reloaded. Too many sign-on attempts by DHCTs contribute to network congestion and could cause DHCTs to become non-responders.

The signonCount utility can help the system operator monitor the following DHCT network sign-on activities:

- DAVIC connections and UN-Config requests on a minute-by-minute basis
- Excessive DHCT sign-on requests
- QPSK modulator reboots
- DHCTs signing on with an incorrect type, revision, or OUI
- Successful sign-on statistics

Regularly Run the DHCT Status Reporting Utility

Run the DHCT Status Reporting Utility regularly. The DHCT Status Reporting Utility is designed to test and analyze two-way communications between the DHCT and the headend. The DHCT Status Reporting Utility provides system operators with the following data:

- Provides a current summary of the statuses of a system's DHCT population
- Polls all DHCTs that have an IP address and reports the following data:
  - DHCT transmit levels
  - DHCT delay values
  - Currently loaded resident application and operating system
- Provides the following reports:
  - DHCT non-responders by QPSK modulator and demodulator
  - DHCT transmit levels by QPSK modulator and demodulator
  - DHCT delay values by QPSK modulator and demodulator
  - Operating system and resident application by DHCT type and revision
  - General DHCT summary

Inventory Handling

Only DHCTs that are in homes of subscribers, labs, or ready to be immediately re-issued should have a status of in-service, two-way in the DNCS. DHCTs that have been returned from subscribers and are being processed in anticipation of being re-issued should have a status of out-of-service.

Interface of the DHCT Status Reporting Utility

Two-way communication between DHCTs and the headend is vital if subscribers are to take full advantage of the interactive features of the DBDS. The DHCT Status Reporting Utility is designed to test and analyze two-way communications between the DHCT and the headend.

The information in this chapter tells you how to access the user interface of the DHCT Status Reporting Utility and how to interpret the data it displays. Subsequent chapters in this guide provide instructions for running the various features included as part of the DHCT Status Reporting Utility.

DHCT Status Reporting Utility Interface

This section provides instructions on how to access the interface of the DHCT Status Reporting Utility.

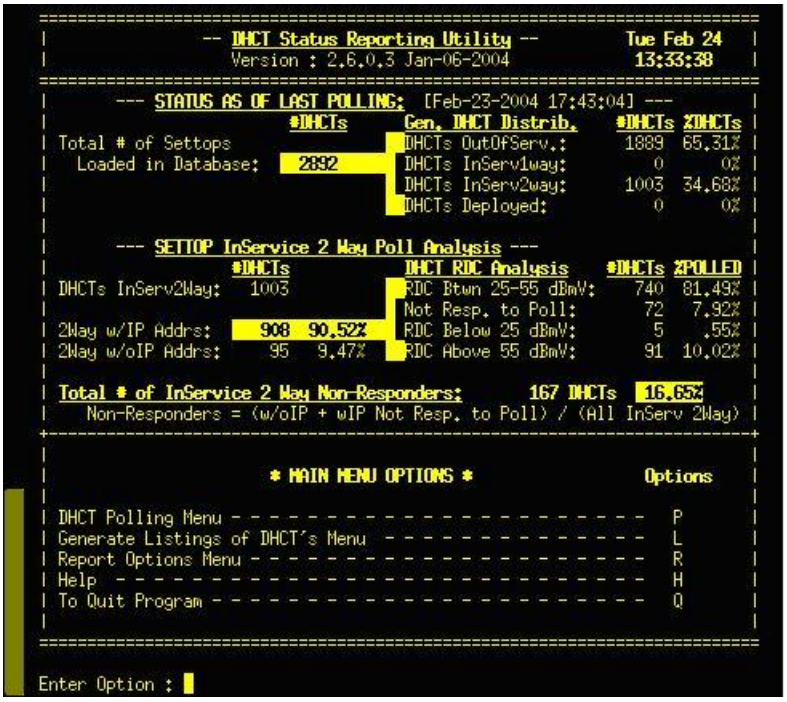
Accessing the Interface

Follow these instructions to access the interface of the DHCT Status Reporting Utility.

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

Important: You must be **dncs** user in the xterm window. You cannot run the DHCT Status Reporting Utility as root user.

2 Type **dhctStatus** and then press **Enter**. The initial screen of the DHCT Status Reporting Utility appears.



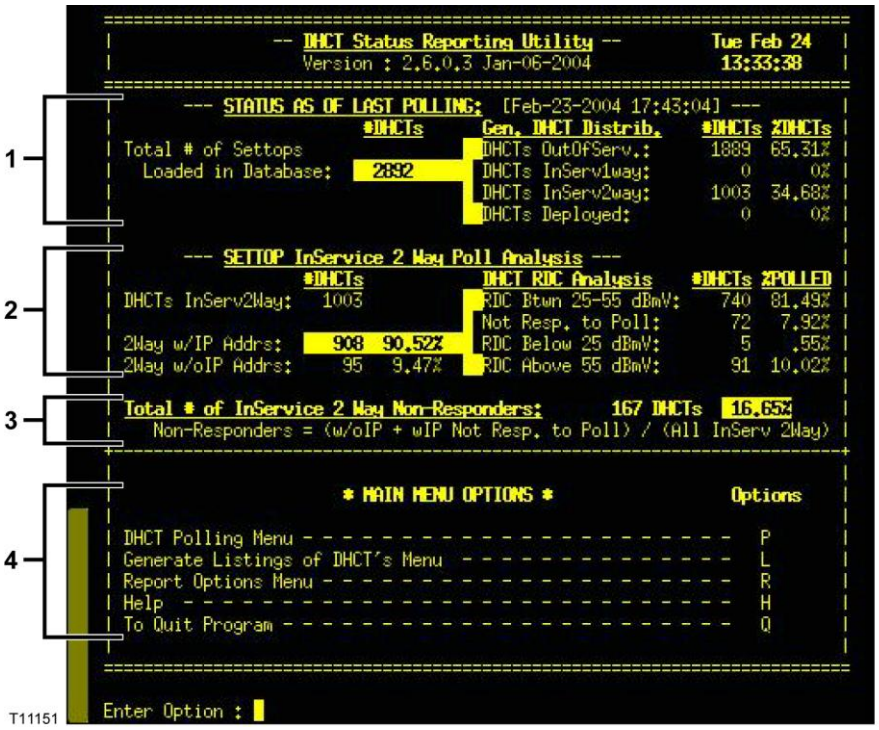
3 Go to ***Understanding the Interface*** (on page 98) for help in interpreting the information displayed on the initial window of the DHCT Status Reporting Utility.

Understanding the Interface

Introduction

An example of the initial screen of the DHCT Status Reporting Utility is presented here for reference. The major sections of the initial screen are referenced by section numbers **1** through **4**. Refer to this illustration as you read the remainder of this section.

Note: Data referenced by the numbers will not appear the first time you run the utility because there is no data to report. After the system is polled for the first time, the utility populates the fields referenced by these numbers with data from the entire DHCT population.



As you progress through this guide and run the various options offered by the DHCT Status Reporting Utility, you will see that the data displayed at numbers 1 and 2 appears at the top of many DHCT Status Reporting Utility screens. By displaying this data on many DHCT Status Reporting Utility windows, system operators can readily compare new data with old.

Section 1 - Status As Of Last Polling

The **Status As Of Last Polling** section appears near the top of the initial screen and is referenced by the number **1**. This area of the screen lists the total number of settops (DHCTs) in the database and summarizes, by total and percentage, the number of DHCTs with the following statuses:

- Out-of-service (**DHCTs OutOfServ**) — DHCTs that are new or in inventory and may not yet be staged or installed into subscribers' homes should have a status of *out-of-service*.
- In-service, two-way (DHCTs InServ2way) — DHCTs with an *in-service two-way*

status support communication between the headend and the DHCT, as well as return communication. DHCTs need two-way communication capability to take full advantage of interactive services.

Example: Interactive services include IPPV, VOD, xOD, and PPV.

- In-service, one-way (**DHCTs InServ1way**) — DHCTs with an *in-service one-way* status support communications between the headend and the DHCT, only. These DHCTs are considered to be in broadcast-only mode and have no two-way services assigned to them. These DHCTs have most-likely been staged and may have been installed into subscribers' homes.

  Note: Systems designed to have 100 percent of DHCTs with in-service, two-way status should not have any DHCTs with this configuration.

- Deployed (**DHCTs Deployed**) — DHCTs with a status of *deployed* are usually in transit. The DHCTs are not technically out-of-service, but not quite in-service, either. These DHCTs have been staged and will shortly be installed in the homes of subscribers. DHCTs with a status of deployed can sign on to the network.

  Note: Most billing vendors do not yet support the Deployed status.

For the DHCT Status Reporting Utility to retrieve and analyze non-responder data from DHCTs, the DHCTs must have a status of in-service, two-way. DHCTs that have a status of in-service, two-way can generate revenue for the system operator. Ultimately, the system operator's billing system dictates which DHCTs can generate revenue.

Section 2 - SETTOP InService 2 Way Poll Analysis

DHCT Analysis

The **SETTOP InService 2 Way Poll Analysis** section is referenced by the number **2**. This area of the interface of the DHCT Status Reporting Utility presents a detailed analysis of those DHCTs listed in the database that are capable of two-way communication. The **SETTOP InService 2 Way Poll Analysis** section includes the following items:

- The number of DHCTs with two-way capability that *have* an IP address (**2Way w/IP Addrs**) and the number of DHCTs with two-way capability that *do not have* an IP address (**2Way w/oIP Addrs**).
- For DHCTs *with* an IP address, the totals and percentages that transmit at the following transmit levels:
  - Between and including 25 and 55 dBmV (decibels referenced to 1 millivolt) (**RDC Btwn 25-55 dBmV**)-DHCTs communicate with the headend between and including 25 and 55 dBmV.
  - No response (**Not Resp. to Poll**)-The DNCS is unable to get a response after polling these DHCTs.
  - Below 25 dBmV (**RDC Below 25 dBmV**)-DHCTs respond to the poll, but respond at a transmit level below the optimum level specified by our engineers.
  - Higher than 55 dBmV (**RDC Above 55 dBmV**)-DHCTs respond to the poll, but respond at a transmit level higher than the optimum level specified by our engineers.

High or Low Transmit Levels

Even though DHCTs can transmit successfully at levels higher than 55 dBmV or lower than 25 dBmV, the fact that these DHCTs exist on a system may indicate a serious configuration problem. Occasionally, the entire population of DHCTs assigned to a specific QPSK modulator or demodulator may transmit at levels that are too high or too low. The system can support two-way communications with a portion of these DHCTs; other DHCTs assigned to this modulator or demodulator may transmit at levels that are too high or too low to even be recognized.

Consider this rule of thumb: if 3 percent or more of successfully responding DHCTs respond at levels higher than 55 dBmV or lower than 25 dBmV, you can assume that there are other DHCTs responding with signals too high or too low to be recognized.

Note: You can see an illustration of this concept in the graph under **Examples of**

Systems Needing Recalibration, under ***DHCT Transmit Level Saturation Report*** (on page 113).

System operators can use the information provided by the DHCT Status Reporting Utility to identify modulators or demodulators associated with non-responding DHCTs. System operators can then take measures to adjust transmit levels so that they conform with our recommendations. This issue is discussed in more detail in **DHCT Transmit Level Saturation Report**.

Section 3 - Total # of InService 2 Way Non-Repsonders

The **Total # of InService 2 Way Non-Responders** section is referenced by number **3**. This short section summarizes the total number and percentage of DHCTs that have two-way communication capability, but these DHCTs do not respond to poll requests from the DHCT Status Reporting Utility.

Section 4 - Main Menu Options

The **Main Menu Options** section is referenced by number **4**. This area lists the various options you can use when you run the DHCT Status Reporting Utility. Subsequent sections in this chapter provide detailed instructions for running each option.

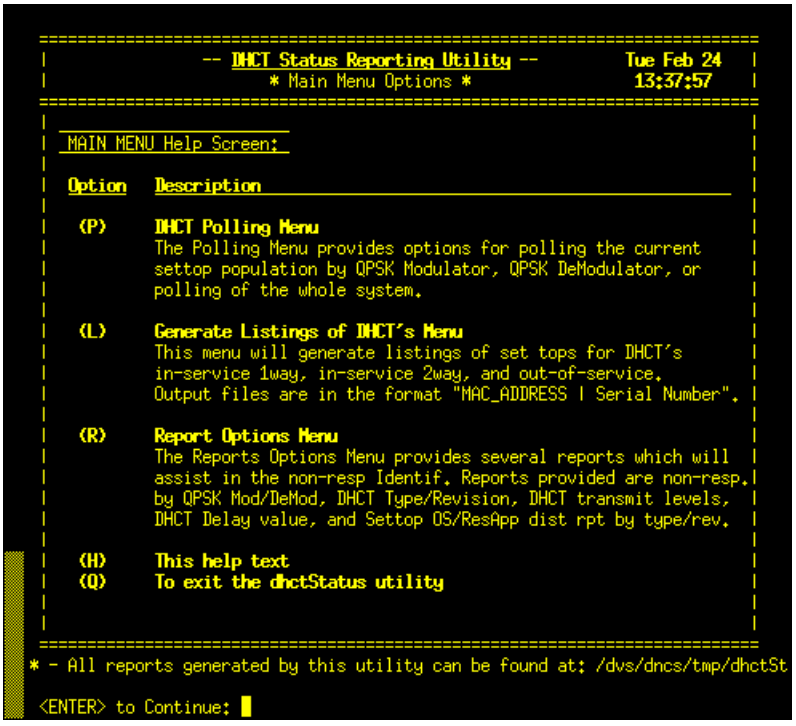
Note: The **Help** option of the DHCT Status Reporting Utility briefly describes each of the options included in the utility. Go to ***The DHCT Status Reporting Utility Help Option*** (on page 90).

DHCT Status Reporting Utility Help Option

Displaying the Help Screen for the DHCT Status Reporting Utility

Follow these instructions to display the Help screen for the DHCT Status Reporting Utility.

1 From the DHCT Status Reporting Utility screen, type **h** and then press **Enter**. The screen updates to display the Main Menu Help Screen, which lists information that explains the options on the main menu.



2 Read the description of the **P**, **L**, and **R** options and then press **Enter** to return to the DHCT Status Reporting Utility window. Press **Q** to exit from the Help screen.

Note: Refer to subsequent sections of this chapter for detailed information (including examples) regarding these menu options.

DHCT Polling Option

The DHCT Status Reporting Utility polls DHCTs to assess how well they are performing in the field, as well as providing the mechanism for identifying and correcting non-responding issues. By examining polling data, system operators can make changes to their system configuration that improve DHCT performance and reduce the number of non-responding DHCTs on a specific QPSK modulator or demodulator.

The information in this chapter provides instructions for using the DHCT Status Reporting utility to poll DHCTs.

Poll DHCTs

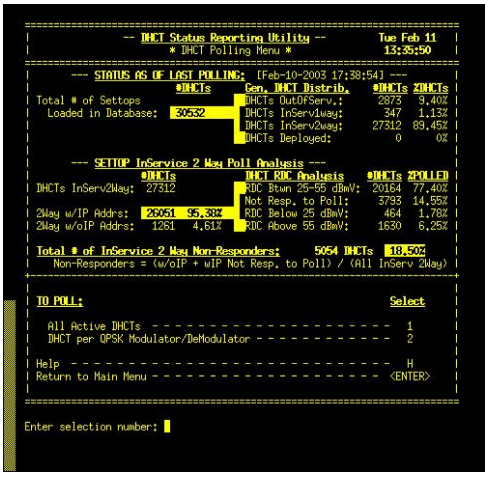
The instructions in this section describe how to use the DHCT Status Reporting Utility to poll DHCTs.

Note: All procedures in this section assume that the DHCT Status Reporting Utility screen is open on the DNCS.

Polling DHCTs

Follow these instructions to poll the DHCTs on the system.

1 From the DHCT Status Reporting Utility screen, type **p** and then press **Enter**. The DHCT Polling Menu screen appears.



2 Choose one of the following options:

- To poll all active DHCTs on the network, go to ***Polling All Active DHCTs*** (on page 105).
- To poll DHCTs associated with a specific QPSK modulator or demodulator,

go to ***Polling DHCTs per QPSK Modulator or Demodulator*** (on page 108).

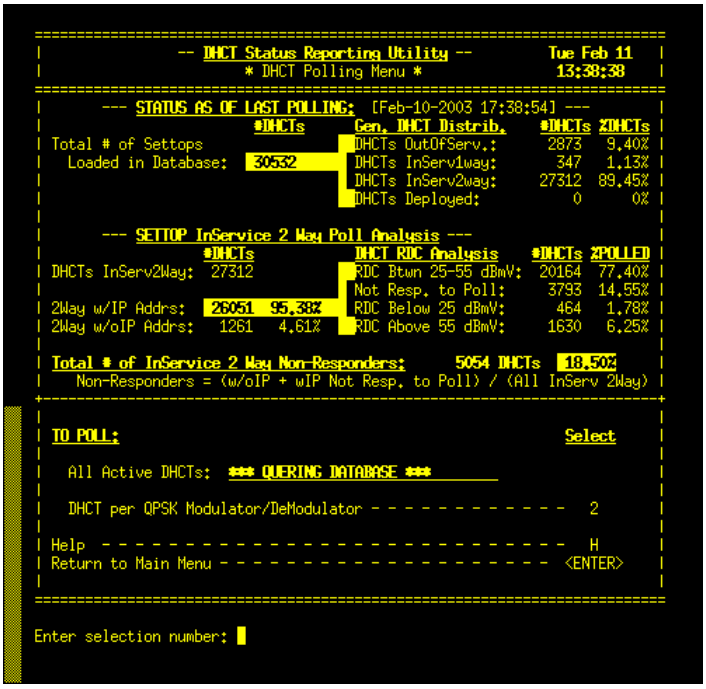
Note: The first time you run the DHCT Status Reporting Utility, you must poll all active DHCTs.

Polling All Active DHCTs

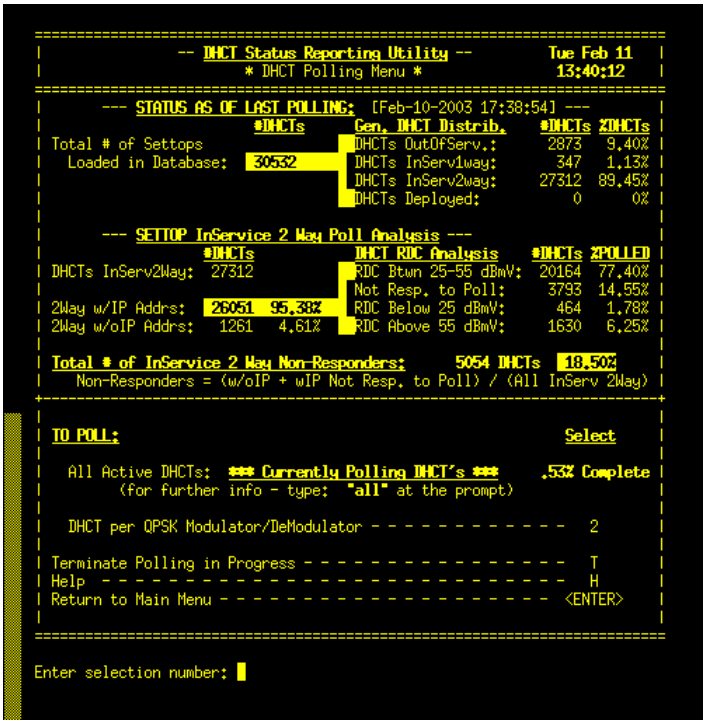
Follow these instructions to poll all active DHCTs on the network.

1 To poll all active DHCTs on the network, type **1** and then press **Enter**. The DHCT Polling Menu screen updates to briefly display a **Querying Database** message in the **To Poll** section of the screen.

Note: The Querying Database message means that the system is collecting information on the DHCTs so that the DHCTs can be efficiently polled.



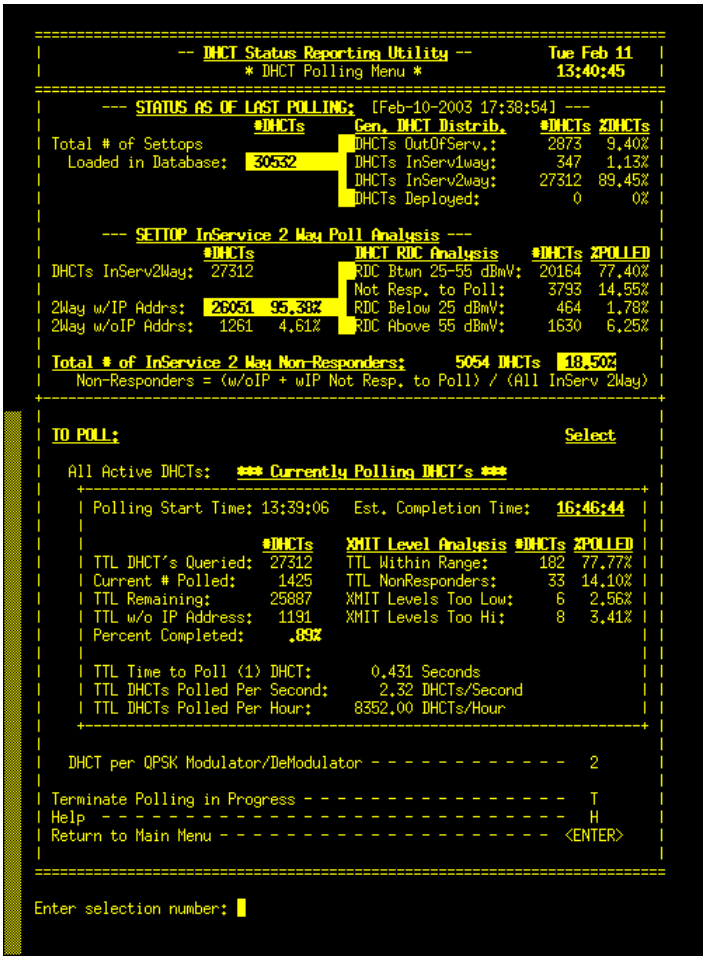
2 Type **u** (for update) and then press **Enter**. The Status of Last Polling portion of the window updates.



3 Type **all** and then press **Enter**. The DHCT Polling Menu screen updates to display the polling data collected so far.

Notes:

- The screen continues to display data from the previously completed polling operation, so that you can compare the newly collected data with data from the previous polling operation.
- The screen also displays the estimated poll completion time. In this example, the system expects polling to complete at 16:46:44, approximately 3 hours from the start of polling.
- The estimated completion time does not remain constant as the poll progresses. Type **all** and then press **Enter** again to obtain the latest estimate.



Polling DHCTs per QPSK Modulator or Demodulator

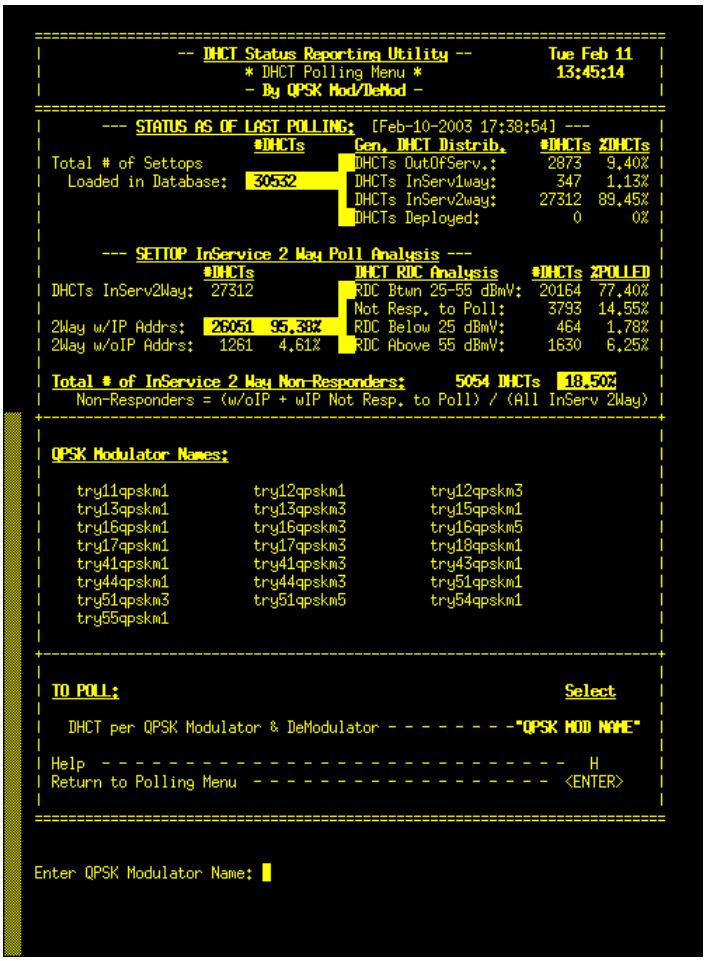
Follow this procedure to poll DHCTs associated with a specific QPSK modulator or demodulator.

1 To poll DHCTs associated with a specific QPSK modulator or demodulator, type **2** and then press **Enter**.

Results:

- The DHCT Polling Menu By QPSK Mod/DeMod window appears.
- The Enter QPSK Modulator Name prompt appears.

Note: Note that the screen lists the QPSK modulators on the system.

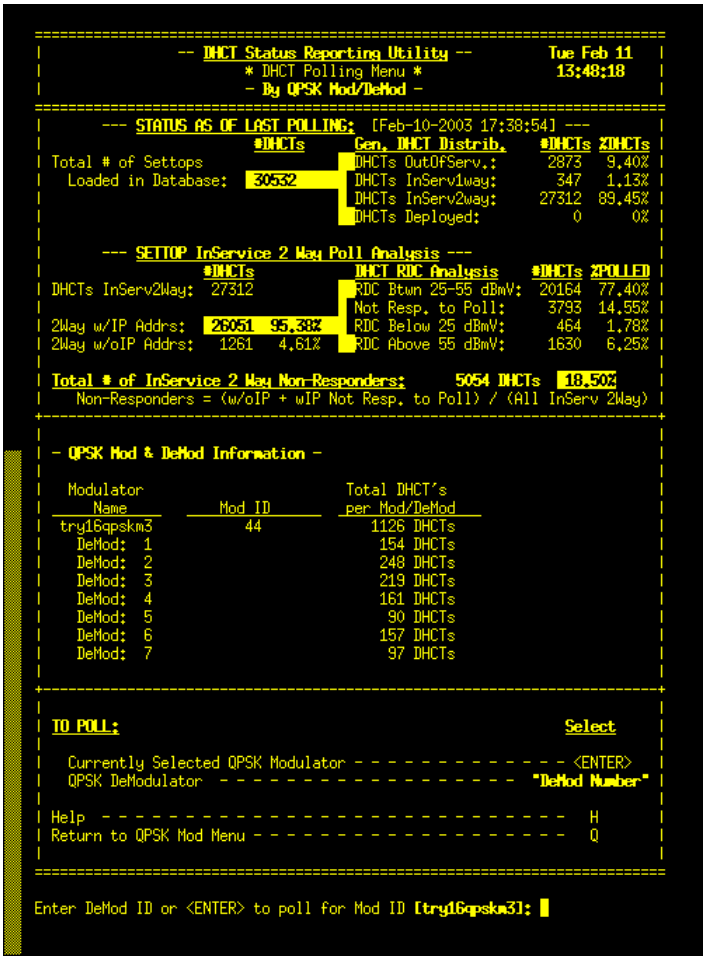


2 Type the name of a QPSK modulator and then press **Enter**.

Important! The modulator name is case-sensitive; be sure to type it exactly as it appears.

Results:

- The DHCT Polling Menu By QPSK Mod/DeMod screen updates to list the QPSK demodulators associated with the selected modulator, as well as the number of DHCTs assigned to the modulator and demodulator(s).
- The **Enter DeMod ID or <ENTER> to poll for Mod ID** prompt appears.



3 Choose one of the following options:

- Press Enter to poll all of the DHCTs associated with the selected modulator.
- Type the demodulator ID and then press Enter to poll DHCTs associated with a specific demodulator.

Note: The next two steps, step 4 and step 5, develop an example based upon polling DHCTs by demodulator ID.

Result: The utility displays polling data after the entire polling operation has completed.

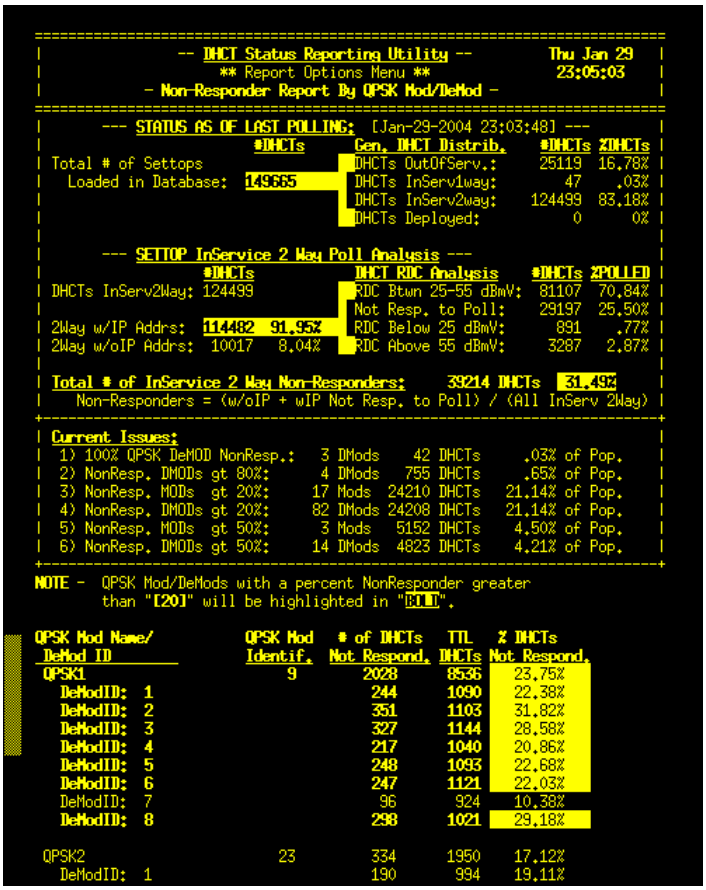
Important: Do not interrupt the polling operation while it is in progress. If you interrupt the polling operation before it has completed, you will not be able to poll this modulator or demodulator again until you remove a specific file from the /tmp directory of the DNCS that tells the DNCS that a polling operation is in progress. The file in the /tmp directory is in the form of dhctStatus.[mod ID or demod ID].

4 Open an xterm window on the DNCS and type **cd /dvs/dncs/tmp/dhctStatus2/[DATE]/ALL/GR_REPORTS** and then press **Enter**. The selected directory becomes the working directory.

Note: Substitute the current date (or the date you ran the poll) in YYYYMMDD format for [DATE].

Example: For a poll conducted on February 12, 2003, type **cd /dvs/dncs/tmp/dhctStatus2/20030212/ALL/GR_REPORTS** and then press **Enter**.

5 To see the non-responder report associated with the poll you just completed, type page NR_M* and then press Enter. The system displays the data associated with the poll you just completed.



Note: Refer to ***Explanation of Output From Non-Responder Report*** (on page 111) for an explanation of some of the findings revealed in this non-responder report.

Explanation of Output From Non-Responder Report

The **Current Issues** section of the report output lists those modulators and demodulators where non-responding DHCTs make up a significant percentage of the total number of DHCTs assigned to the modulator or demodulator. Using the example in step 5, three demodulators have 100 percent of their DHCTs in a non-responding state. This constitutes 42 DHCTs, or .03 percent of the total number of DHCTs supported by the system. Using another example from step 6, fourteen demodulators have 50 percent of their assigned DHCTs in a non-responding state. This constitutes 4,823 DHCTs, or 4.21 percent of the entire DHCT population.

The lower, unlabeled section of the report output displays all the modulators and demodulators running on the system. This section lists the number of non-responding DHCTs assigned to each modulator or demodulator, the total number of DHCTs supported by the modulator or demodulator, as well as the percentage of assigned DHCTs that are non-responders. The report highlights the percentage of non-responding DHCTs whenever that percentage exceeds 20 percent.

Note: System operators may want to examine the following conditions in order to troubleshoot the significant percentage of non-responding DHCTs revealed in the data from step 5:

- The system may lack proper attenuation
- The modulator may just have rebooted
- The cabling for the modulator or demodulator may have become loose
- The system may have just experienced a power outage

Data Files Resulting From Polling Operations

The following list contains the data files that are generated by the polling operation, as well as a description of the type of data contained in the file:

Note: Type **page [file name]** and then press **Enter** from the /dvs/dncs/tmp/dhctStatus2/[DATE]/ALL/GR_REPORTS directory to view the output.

- OS_TypeRev.txt — OS version sorted by DHCT type and revision
- NR_TypeRev.txt — Non-responder data sorted by DHCT type and revision
- NR_ModDeMod.txt — Non-responder data sorted by QPSK modulator and demodulator
- DL_ModDeMod.txt — DHCT delay values sorted by QPSK modulator and demodulator
- TL_ModDeMod.txt — DHCT transmit levels sorted by QPSK modulator and demodulator

List DHCTs

The DHCT Status Reporting Utility provides system operators and engineers with the ability to query the database for a listing of MAC addresses and serial numbers of DHCTs that have a specific status. The utility can generate a list for DHCTs with the following statuses:

- DHCTs with a one-way status
  Note: DHCTs with a one-way status support communication between the headend and the DHCT.
- DHCTs with a two-way status
  Note: DHCTs with a two-way status support communication between the headend and the DHCT, as well as return communication between the DHCT and the headend.
- DHCTs with an out-of-service status
  Note: DHCTs with a status of out-of-service are usually DHCTs that have yet to be installed in a subscriber's home or have been returned by subscribers. These DHCTs will eventually be redeployed to other subscribers.
- DHCTs with a deployed status
  Note: DHCTs with a status of deployed are usually in a transition period. They have been staged and are awaiting placement in a subscriber's home. Most systems do not currently use the deployed status.

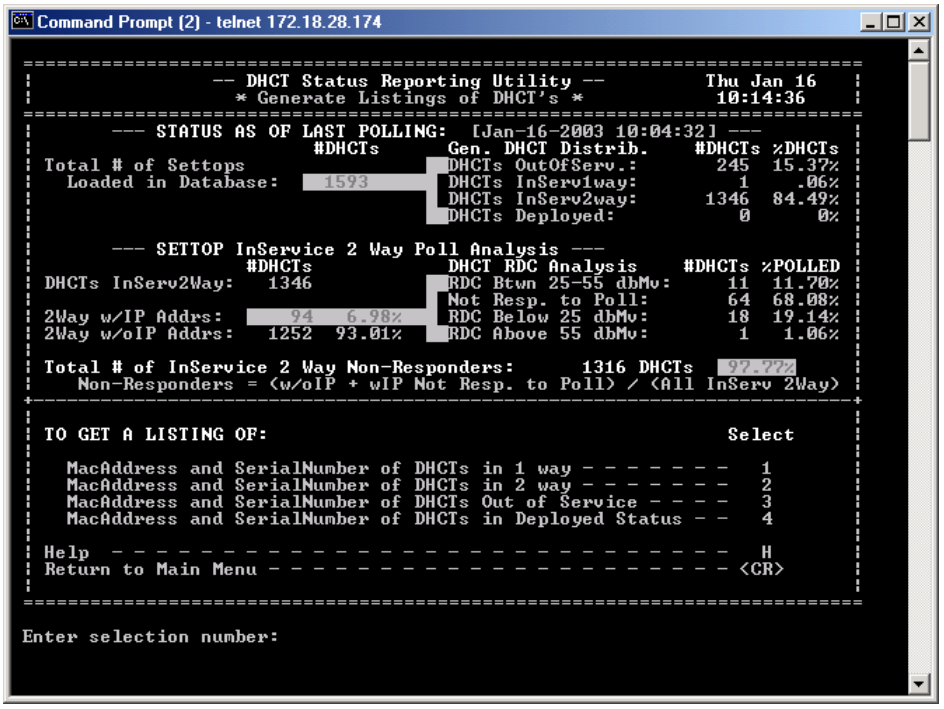
The lists of DHCTs that the DHCT Status Reporting Utility generates can become quite lengthy. For this reason, the utility does not display the lists on the screen of the DNCS. Instead, output is written to a file in the /dvs/dncs/tmp/dhctStatus2/[DATE] directory of the DNCS, where system operators and engineers can view it at their convenience. Instructions for viewing these output files are included later in this section.

Generate a Listing of DHCTs

Follow these instructions to use the DHCT Status Reporting Utility to generate various listings of DHCTs.

1 From the DHCT Status Reporting Utility screen, type **l** and then press **Enter**. The Generate Listings of DHCTs screen appears.

Note: The "l" is a lowercase L.



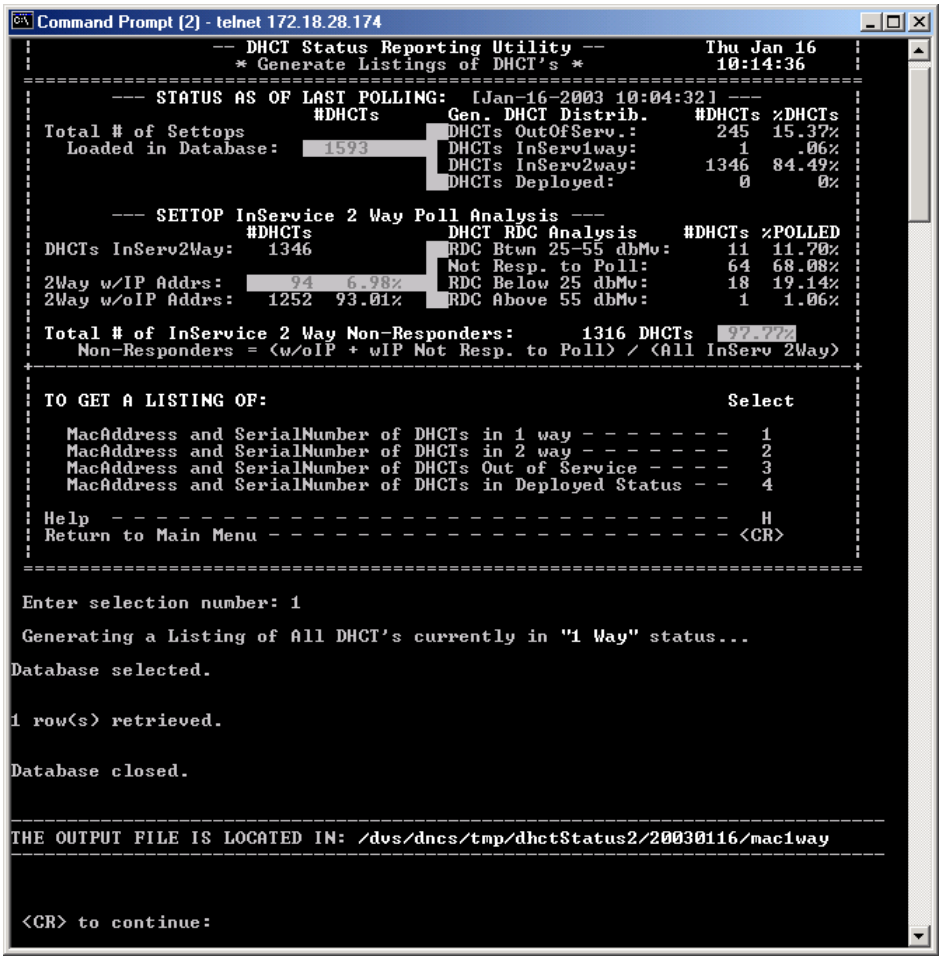
2 Choose one of the following options:

- To generate a listing of DHCTs with a one-way status, go to step 3.
- To generate a listing of DHCTs with a two-way status, go to step 5.
- To generate a listing of DHCTs with a status of out-of-service, go to step 7.
- To generate a listing of DHCTs with a status of deployed, go to step 9.

3 Type **1** and then press **Enter** to generate a listing of DHCTs with a one-way status.

Results:

- The system reports the number of database rows that matched the requirements of the selected list.
- The system displays a message that indicates the directory in which the output file can be found.

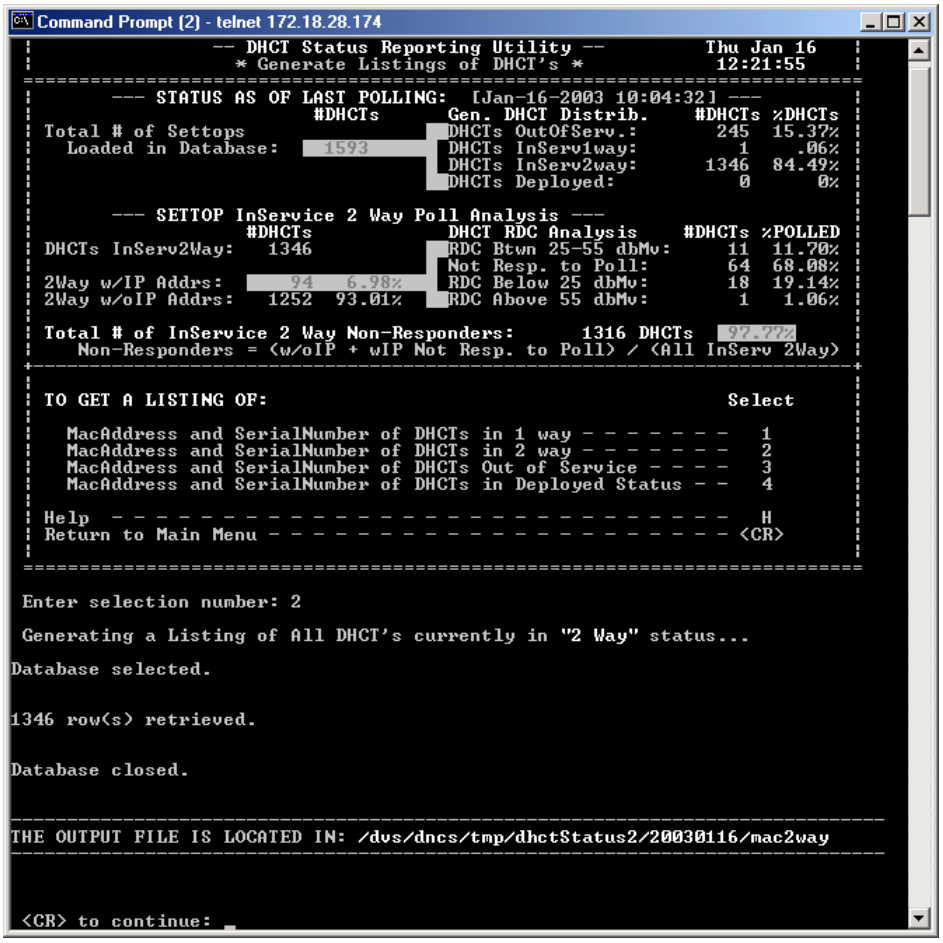


4 Go to *View the Output File* (on page 106) for instructions on how to view the contents of the output file generated by the DHCT Status Reporting Utility.

5 Type **2** and then press **Enter** to generate a listing of DHCTs with a two-way status.

Results:

- The system reports the number of database rows that matched the requirements of the selected list.
- The system displays a message that indicates the directory in which the output file can be found.

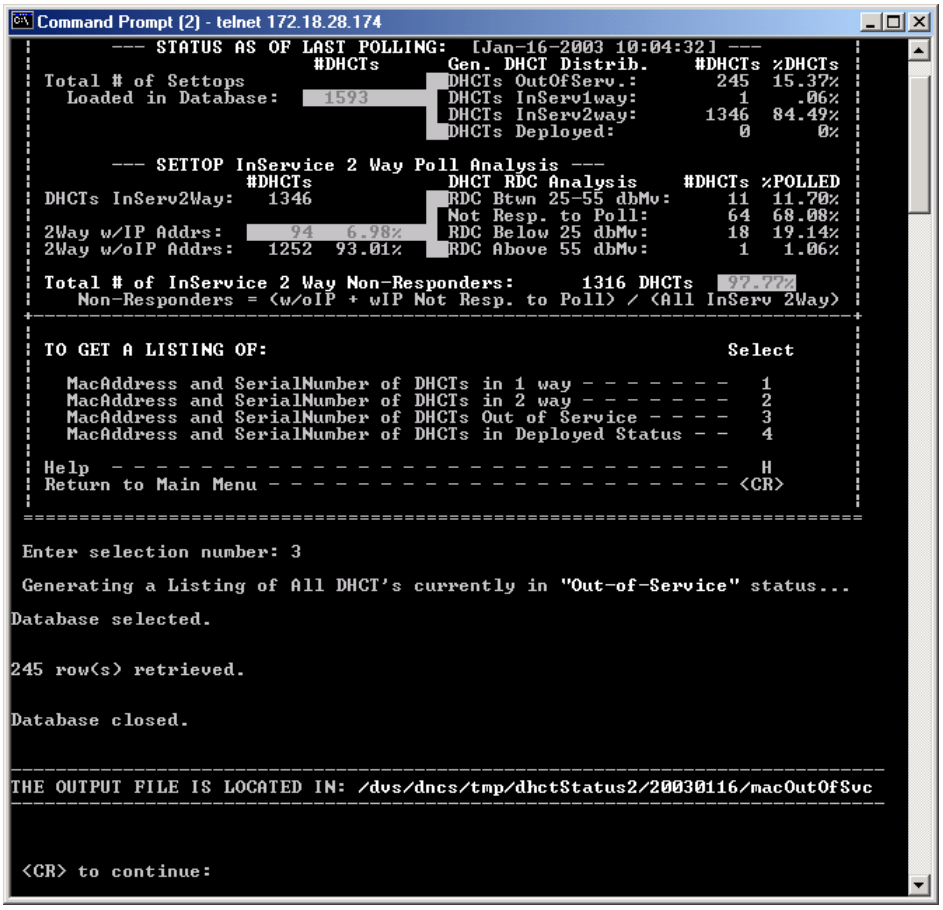


6 Go to *View the Output File* (on page 106) for instructions on how to view the contents of the output file generated by the DHCT Status Reporting Utility.

7 Type **3** and then press **Enter** to generate a listing of DHCTs with a status of out-of-service.

Results:

- The system reports the number of database rows that matched the requirements of the selected list.
- The system displays a message that indicates the directory in which the output file can be found.

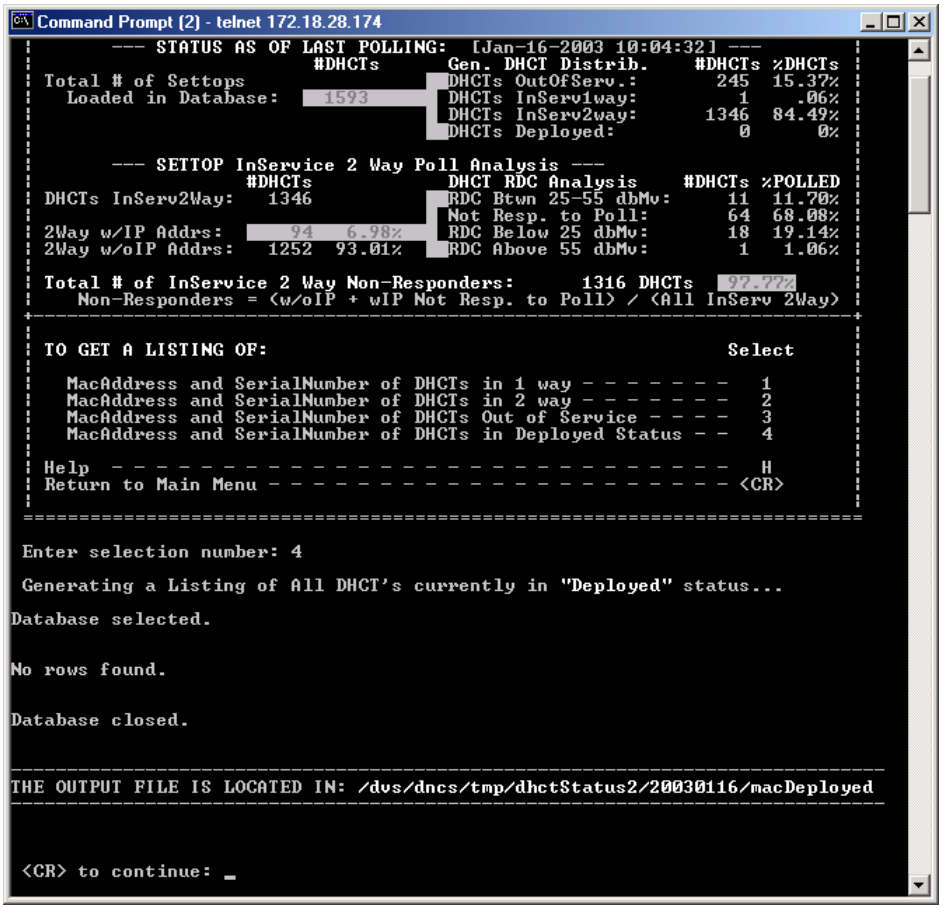


8 Go to *View the Output File* (on page 106) for instructions on how to view the contents of the output file generated by the DHCT Status Reporting Utility.

9 Type **4** and then press **Enter** to generate a listing of DHCTs with a status of deployed.

Results:

- The system reports the number of database rows that matched the requirements of the selected list.
- The system displays a message that indicates the directory in which the output file can be found.



10 Go to *View the Output File* (on page 106) for instructions on how to view the contents of the output file generated by the DHCT Status Reporting Utility.

View the Output File

After using the DHCT Status Reporting Utility to generate a list of DHCTs, follow these instructions to view the list that the utility generated.

Note: The list contains DHCT MAC addresses and serial numbers.

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

Note: You can be logged on as dncs user in the xterm window.

2 Type **more /dvs/dncs/tmp/dhctStatus2/[DATE]/[filename]** and then press **Enter**. The output file opens for viewing.

Notes:

- Substitute the date you polled the DHCTs, in YYYYMMDD format, for [DATE].
- Substitute the name of the file you want to view for [filename].
  - Use **mac1way** for DHCTs with a one-way status.
  - Use **mac2way** for DHCTs with a two-way status.
  - Use **macOutofSvc** for DHCTs with a status of out-of-service.
  - Use **macDeployed** for DHCTs with a status of deployed.

Example: more /dvs/dncs/tmp/dhctStatus2/20030114/mac2way

3 Use these guidelines to navigate through the list, which may be very lengthy.

a Press the **Spacebar** to advance to the next page of the list.

b Press the **Ctrl** and **C** keys simultaneously to close the file when you are finished.

The Reporting Option

The DHCT Status Reporting Utility includes several reports that summarize various types of DHCT polling data. System operators or support engineers can run the reports and examine the data in order to assess network conditions of the system.

This section contains a description of each report offered by the DHCT Status Reporting Utility, as well as detailed instructions on running the reports.

Description of Reports

DHCT Status Reporting Utility Reports

The DHCT Status Reporting Utility includes the following reports that system operators can generate to summarize various DHCT polling data:

- Non-responder reports-DHCTs with an IP address that fail to respond to poll requests from the DNCS are commonly known as non-responders. The utility generates two types of DHCT non-responder reports:
  - DHCT non-responders identified by QPSK modulator and demodulator
  - DHCT non-responders identified by DHCT type and revision

  By analyzing the report, system operators can spot trends that may indicate that a disproportionate share of non-responding DHCTs are associated with a specific QPSK, or are DHCTs of a specific type or revision.
- Transmit level report-When a DHCT signs on to the network, the QPSK modulator informs the DHCT of the signal needed to maintain a communication link between the DHCT and the modulator. The DHCT Transmit Level Saturation Report summarizes the transmit levels of DHCTs associated with each QPSK modulator and demodulator in the system. By analyzing the transmit levels, system operators can quickly spot when network conditions are preventing effective communication between the headend and the DHCTs.
- Delay value report-When a DHCT signs on to the network, the QPSK modulator performs a test that evaluates the distance from the DHCT to the modulator. Based upon this distance, the modulator assigns a "delay value," which indicates how often a DHCT will check in with the QPSK modulator. The closer the DHCT is to the modulator, the greater the delay value; the farther the DHCT is from the modulator, the shorter the delay value.

  The DHCT Delay Value Saturation Report summarizes the delay values of DHCTs associated with each QPSK modulator and demodulator in the system. By analyzing the delay values, system operators can spot conditions under which it may be advantageous to configure a QPSK modulator for the QPSK

Range Extension Feature.

Note: The QPSK Range Extension Feature allows DHCTs to sign on to the system and operate properly at extended distances from the QPSK modulator.

- Operating system and resident application report-The DHCT Status Reporting Utility generates a report that lists the version of operating system (OS) and resident application code running on each DHCT type and revision supported by the system.

Reports Menu

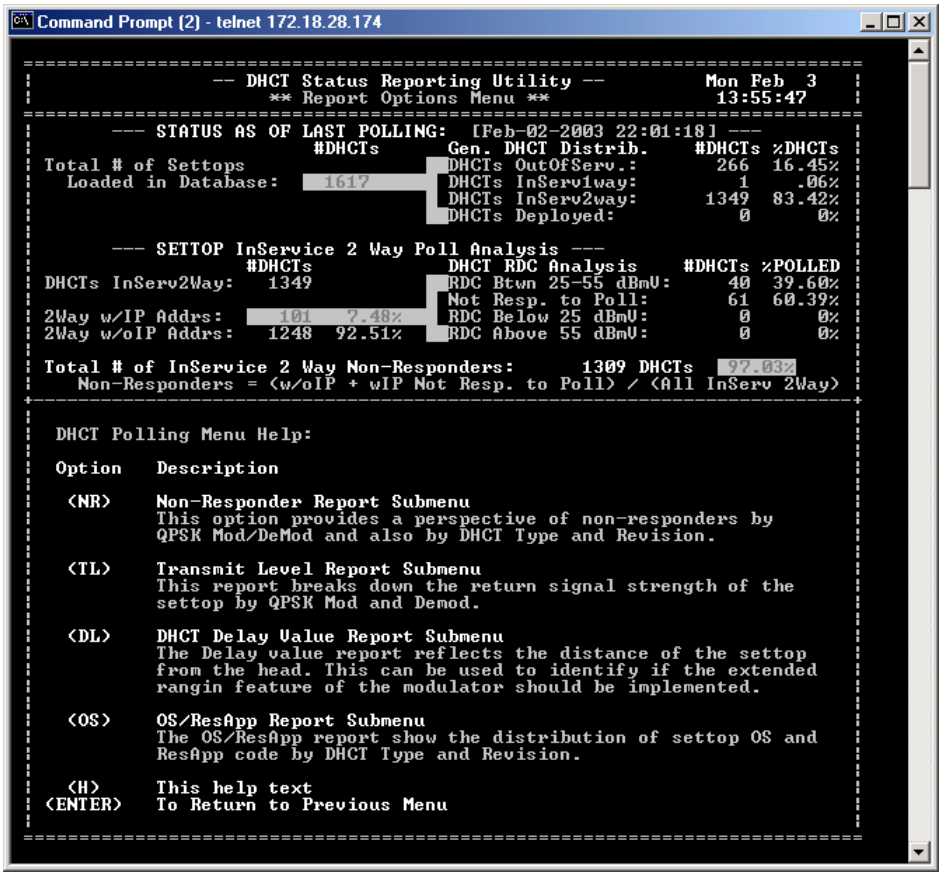
Accessing the Reports Menu

Follow these instructions to access the menu from which the various DHCT Status Reporting Utility reports can be run.

1 From the main menu of the DHCT Status Reporting Utility, type **r** and then press **Enter**. The Report Options Menu screen appears.

2 Type **h** and then press **Enter** to display the DHCT Status Reporting Utility help screen.

Note: The help screen summarizes the purpose of each report included in the DHCT Status Reporting Utility.



3 Choose one of the following options:

- To generate DHCT non-responder reports, go to ***Non-Responder Reports*** (on page 110).
- To generate a DHCT transmit level report, go to ***DHCT Transmit Level Saturation Report*** (on page 113).
- To generate a DHCT delay value report, go to ***DHCT Delay Value Saturation Report*** (on page 119).
- To generate a report that lists the operating system and resident application software running on each DHCT type and revision on your system, go to ***DHCT OS and ResApp Evaluation by Set Top Type and Rev Report*** (on page 137).

Non-Responder Reports

Generating Non-Responder Reports

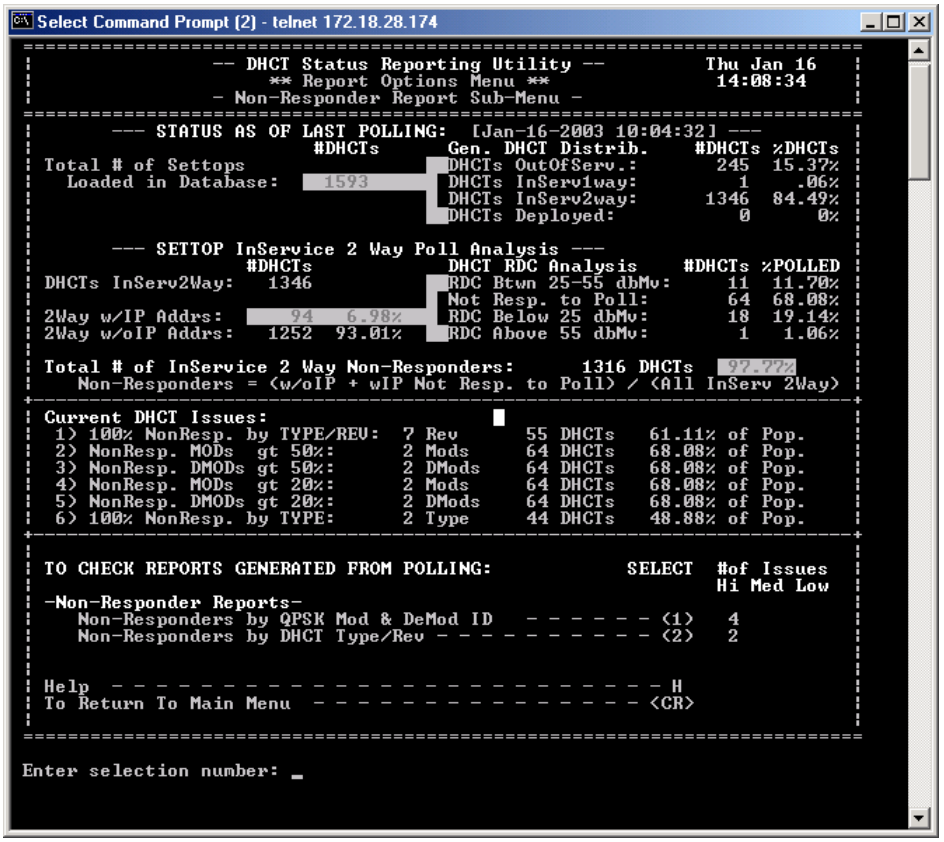
Follow these instructions to generate the Non-Responder Reports.

Note: A non-responding DHCT refers to a DHCT that does not respond to poll requests from the DNCS.

1 From the main menu of the DHCT Status Reporting Utility, type **nr** and then press **Enter**. The Non-Responder Report Sub-Menu screen appears.

Note: The Non-Responder Report Sub-Menu screen shows that you can generate the following two types of DHCT non-responder reports:

- Non-Responders by QPSK Mod and DeMod ID
- Non-Responders by DHCT Type/Rev



2 Choose one of the following options:

- To generate a Non-Responder Report for DHCTs based upon QPSK

modulator and demodulator ID, go to step 3.

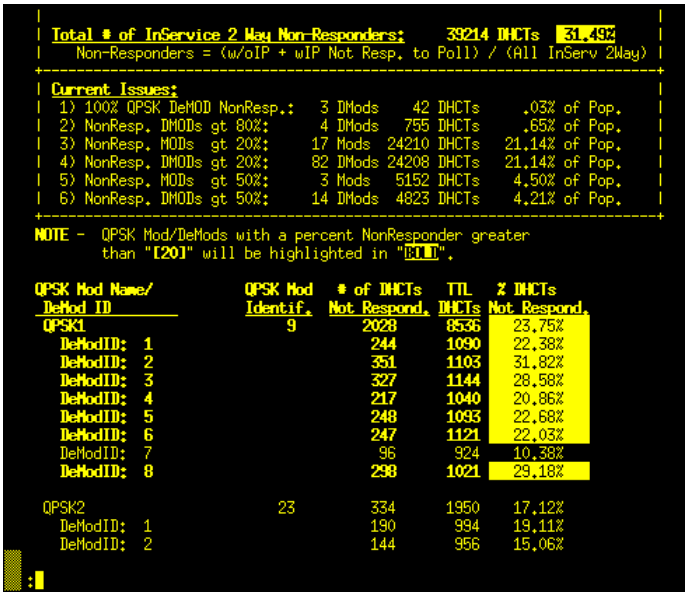
- To generate a Non-Responder Report for DHCTs based upon DHCT type and revision, go to step 5.

3 To generate a Non-Responder Report for DHCTs based upon QPSK modulator and demodulator ID, type **1** (for Non-Responders by QPSK Mod & DeMod ID) and then press **Enter**.

Result: The Non-Responder Report Sub-Menu screen updates to display the following information:

- QPSK modulator(s) name, ID, and demodulator ID
- The number of DHCTs associated with each modulator and demodulator
- The total number and percentage of DHCTs assigned to each modulator and demodulator that are classified as non-responders

Note: The report automatically highlights the data when more than 20 percent of DHCTs associated with a specific modulator or demodulator are non-responders.



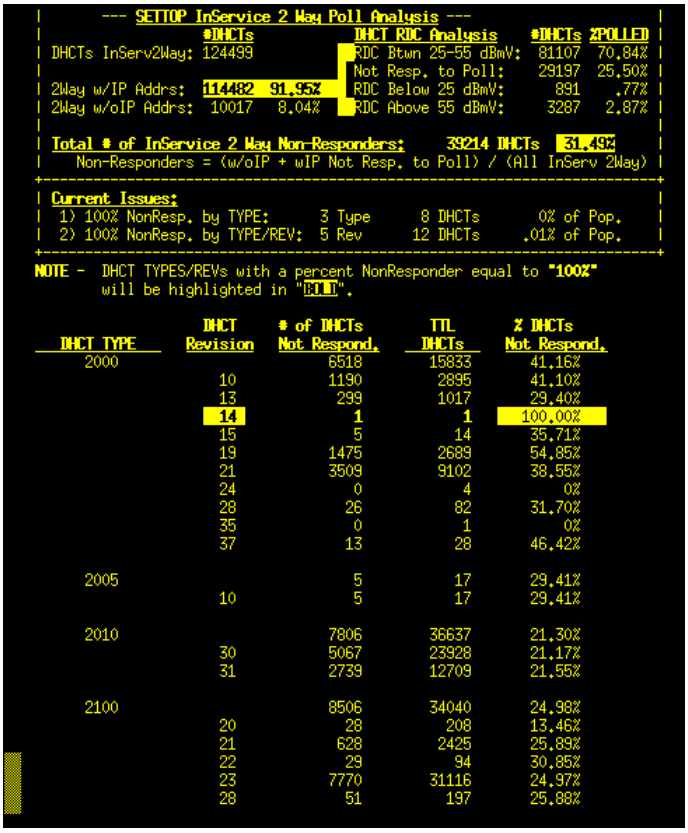
4 Press **Enter** to return to the Non-Responder Report Sub-Menu screen.

5 To generate a Non-Responder Report for DHCTs based upon DHCT type and revision, type **2** (for Non-Responders by DHCT Type/Rev) and then press **Enter**.

Result: The Non-Responder Report Sub-Menu screen updates to display the following information:

- Each DHCT type and revision supported by the system
- The number and percentage of DHCTs of each type and revision that are non-responders
- The total number of DHCTs of each type and revision

Note: The report automatically highlights the data when 100 percent of a specific DHCT type and revision are non-responders.



--- SETTOP InService 2 Way Poll Analysis ---

	#DHCTs		DHCT RDC Analysis	#DHCTs	%POLLED
DHCTs InServ2Way:	124499		RDC Btwn 25-55 dBmV:	81107	70.84%
			Not Resp. to Poll:	29197	25.50%
2Way w/IP Addrs:	114482	91.95%	RDC Below 25 dBmV:	891	.77%
2Way w/oIP Addrs:	10017	8.04%	RDC Above 55 dBmV:	3287	2.87%

Total # of InService 2 Way Non-Responders: 39214 DHCTs 31.49%

Non-Responders = (w/oIP + wIP Not Resp. to Poll) / (All InServ 2Way)

Current Issues:

1) 100% NonResp. by TYPE: 3 Type 8 DHCTs 0% of Pop.
2) 100% NonResp. by TYPE/REV: 5 Rev 12 DHCTs .01% of Pop.

NOTE - DHCT TYPES/REVs with a percent NonResponder equal to "100%" will be highlighted in "RED".

DHCT TYPE	DHCT Revision	# of DHCTs Not Respond.	TTL DHCTs	% DHCTs Not Respond.
2000		6518	15833	41.16%
	10	1190	2895	41.10%
	13	299	1017	29.40%
	14	1	1	100.00%
	15	5	14	35.71%
	19	1475	2689	54.85%
	21	3509	9102	38.55%
	24	0	4	0%
	28	26	82	31.70%
	35	0	1	0%
	37	13	28	46.42%
2005		5	17	29.41%
	10	5	17	29.41%
2010		7806	36637	21.30%
	30	5067	23928	21.17%
	31	2739	12709	21.55%
2100		8506	34040	24.98%
	20	28	208	13.46%
	21	628	2425	25.89%
	22	29	94	30.85%
	23	7770	31116	24.97%
	28	51	197	25.88%

6 Press **Enter** to return to the Non-Responder Report Sub-Menu screen.

7 Press **Enter** again to return to the Report Options Menu screen.

DHCT Transmit Level Saturation Report

The DHCT sign-on process includes establishing the transmission level to use when communicating with QPSK modulators and demodulators. DHCTs transmit at various levels and the QPSK demodulator then measures the quality of the signal. Based upon these measurements, the QPSK modulator then sends a transaction to the DHCT that provides the DHCT with a target transmit level. The DHCT then attempts to communicate with the modulator by using the target transmit level. The DHCT may make several attempts to communicate by increasing the transmit level until the DHCT is able to maintain a communication lock with the modulator.

Over time, however, with the addition of other DHCTs to the network, signal-to-noise ratio issues are likely to affect the performance of the network. Likewise, attenuation issues are likely to surface as network configuration changes. DHCT transmission levels that were first established when the DHCT was added to the network may no longer be valid and the system may require adjustment. System operators can use the DHCT Transmit Level Saturation Report to view data pertaining to the transmission levels of DHCTs on the network and can use the data to adjust their system, if necessary.

Notes:

- DHCT transmit levels are expressed in terms of dBmV. The translation of dBmV is *decibels with respect to 1 millivolt over a characteristic impedance of 75 ohms*.
- Attenuation refers to the decrease in intensity between transmitted and received signals. The loss in intensity is usually a natural consequence of signal transmission over long distances.
- A signal-to-noise ratio is a measurement of signal strength relative to background noise. Competing transmissions from other DHCTs on the network tend to increase the background noise, thereby decreasing the signal-to-noise ratio.
- All demodulators assigned to a specific modulator should be configured to expect approximately the same transmit level from DHCTs. Compensate for variations in DHCT transmit levels by padding and combining. Do not configure transmit levels manually from the front panel of the demodulator.

Generating a DHCT Transmit Level Saturation Report

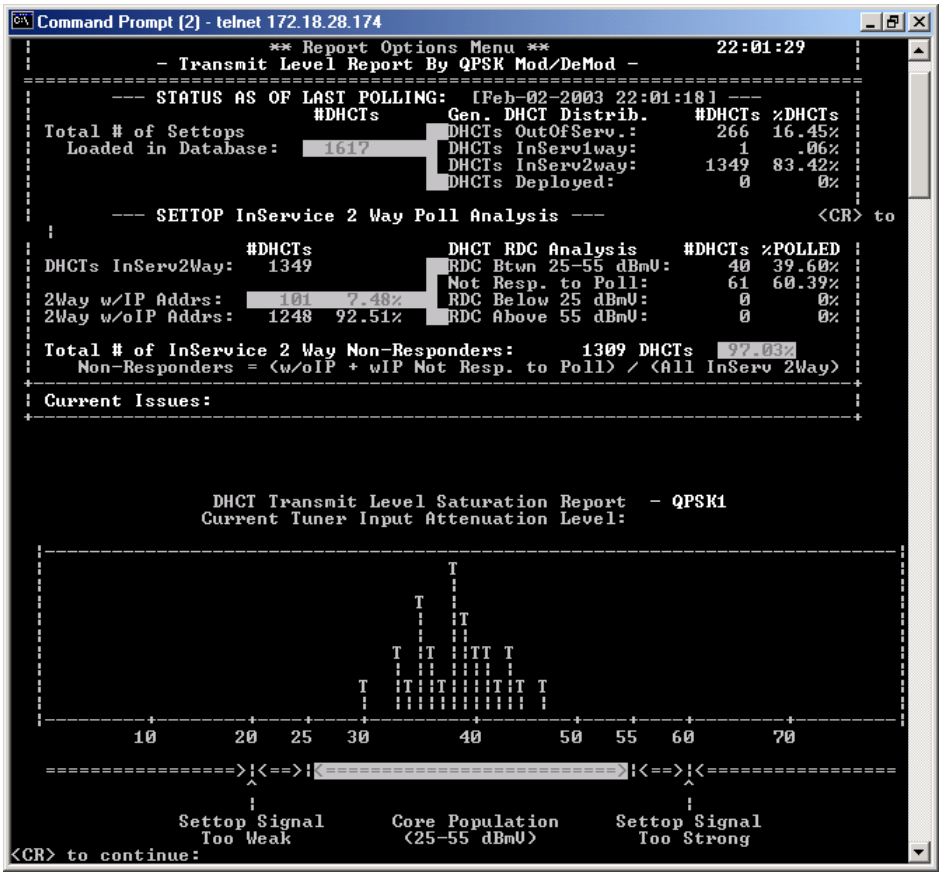
Follow these instructions to generate a DHCT Transmit Level Saturation Report.

1 Maximize the xterm window.

Note: The data in the DHCT Transmit Level Saturation Report is designed to display best if the window is maximized.

2 From the main menu of the DHCT Status Reporting Utility, type **tl** and then press **Enter**. The system generates the DHCT Transmit Level Saturation Report.

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



3 Go to *Understanding the DHCT Transmit Level Saturation Report* (on page 115) for help in interpreting the data displayed in the report.

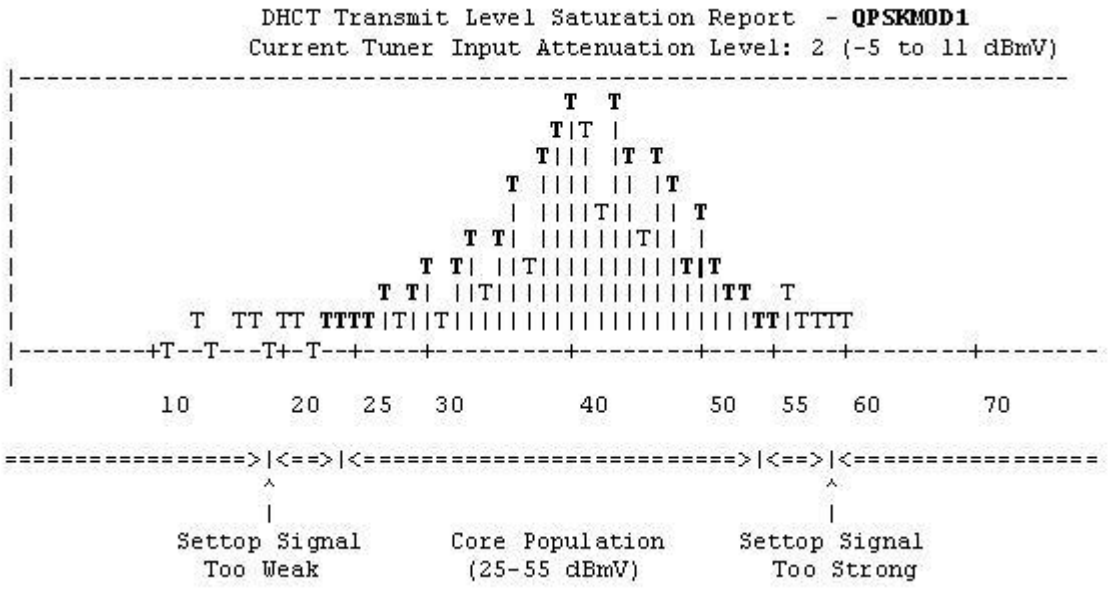
Understanding the DHCT Transmit Level Saturation Report

There are two parts to the DHCT Transmit Level Saturation Report:

- A graphical representation of the distribution of the various transmission levels of DHCTs assigned to each QPSK modulator on the system
  Note: Read ***Graphical Distribution of DHCT Transmission Levels*** (on page 129) for help in interpreting the graphical representation.
- A numerical analysis of the graphical representation of the various transmission levels of DHCTs assigned to each QPSK modulator on the system
  Note: Read ***Transmit Level Analysis*** (on page 130) for help in interpreting the graphical representation.

Graphical Distribution of DHCT Transmit Levels

The first part of the DHCT Transmit Level Saturation Report contains a graph that shows the distribution of the various transmission levels of DHCTs assigned to a specific QPSK modulator. In the following example, the modulator is **QPSKMOD1**. The horizontal axis of the graph plots units of dBmV; the vertical axis (not marked on the report) plots the relative number of DHCTs transmitting at each dBmV level.



Our engineers have determined that DHCTs communicate best with QPSK modulators and demodulators when the DHCT transmits at a level between 25 and 55 dBmV. Notice the bell curve depicted in the illustration (and highlighted in bold for easy recognition). The peak of the bell curve centers around 40 dBmV, the

midpoint between our recommended transmission level of 25 and 55 dBmV. This graph represents a healthy system; the vast majority of DHCTs assigned to this QPSK modulator transmit within our recommended range of 25 to 55 dBmV.

Notice the **Current Tuner Input Attenuation Level** of 2 in the header of this graph. This value is set at the **Tuner Input Attenuator** field, which is located on the **Advanced Parameters** tab in the Set Up QPSK Modulator window on the DNCS. A Current Tuner Input Attenuation Level of 2 corresponds to an attenuation level of -5 to 11 dBmV that currently exists on the network. DHCTs base the strength of their transmitting signal on this Current Tuner Input Attenuation Level. The higher the Current Tuner Input Attenuation Level, the stronger the transmitting signal; the lower the Current Tuner Input Attenuation Level, the weaker the transmitting signal.

Transmit Level Analysis

The second part of the DHCT Transmit Level Saturation Report provides a chart showing the detailed breakdown of the graphical data displayed in ***Graphical Distribution of DHCT Transmit Levels*** (on page 129). This part of the report contains the following data:

- Total number of DHCTs assigned to the modulator and each demodulator that transmit at each transmit level

  Note: In the following example, the QPSKMOD1 modulator is configured with eight demodulators.

- The average and the median transmit level for the modulator and each demodulator

				Transmit Level Breakdown					
QPSK Mod Name	ID	Avg.	Md	20db	25db	30db	50db	55db	60db
QPSKMOD1	8	41.99	42	9	43	219	5865	490	225	0
DMod: 1		40.98	41	2	5	26	755	46	18	0
DMod: 2		43.47	44	0	0	8	633	84	42	0
DMod: 3		39.42	40	7	23	64	713	36	16	0
DMod: 4		40.56	41	0	9	46	718	35	20	0
DMod: 5		43.51	44	0	2	14	828	94	34	0
DMod: 6		41.96	42	0	3	38	1029	84	45	0
DMod: 7		43.12	43	0	1	15	853	74	37	0
DMod: 8		43.33	44	0	0	8	336	37	13	0

The data confirms that the system is healthy. The average and median transmit levels (marked **Avg.** and **Md** respectively in the heading of the chart) for the modulator and each demodulator are reasonably close to the midpoint (40 dBmV) of our recommended range of 25 to 55 dBmV.

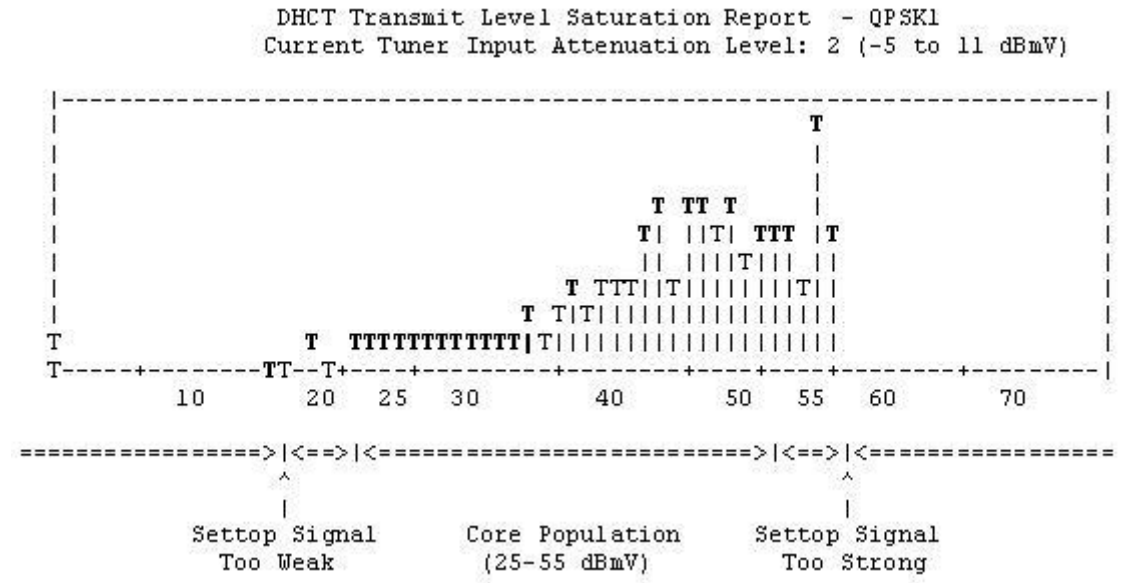
Examples of Systems Needing Recalibration

To further illustrate the value of the information contained in the DHCT Transmit Level Saturation Report, consider these two cases. The first case, ***Case 1*** (on page 131) depicts a system where DHCTs transmit at levels higher than our recommended range of 25 to 55 dBmV. The graph clearly shows the excessively high transmit levels.

The second case, ***Case 2*** (on page 132) illustrates a more subtle example of a system needing recalibration. The graph looks fine but the chart depicts one demodulator transmitting too low and another transmitting too high.

Case 1

This example illustrates a system where DHCTs transmit at levels higher than our recommended range of 25 to 55 dBmV.



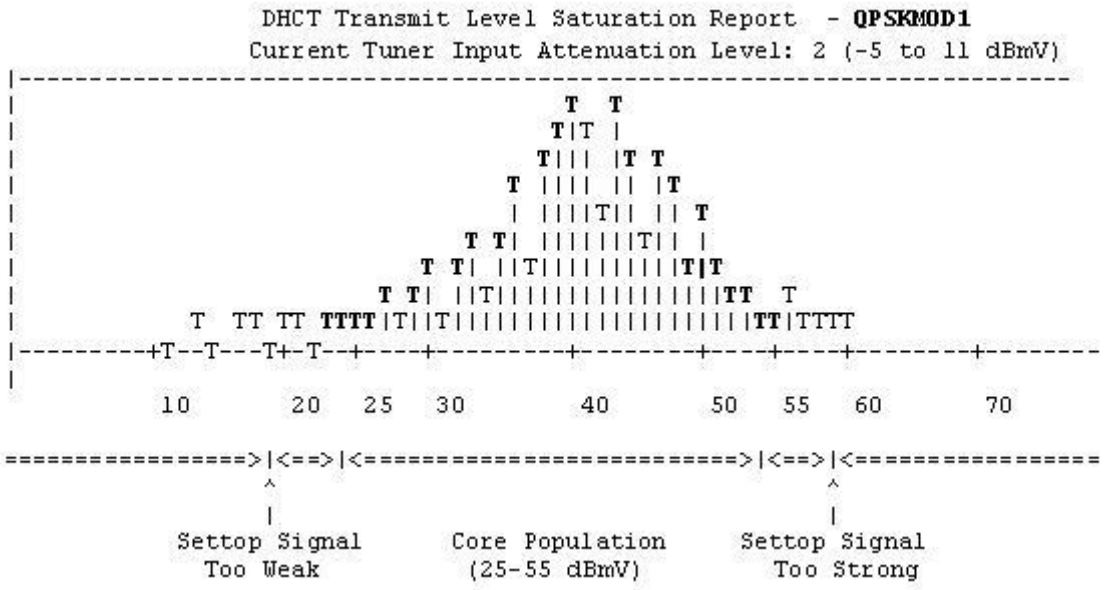
The midpoint of our recommended range of 25 to 55 dBmV is about 40 dBmV. The midpoint of the responding DHCTs depicted in the graph, and confirmed by the data in the following chart, is about 50 dBmV-too high. Furthermore, the graph illustrates a definite drop-off of responding DHCTs at about 55 dBmV, a clear sign that there are additional DHCTs transmitting at levels too high to even be recognized.

QPSK Mod Name	ID	Avg.	Md	Transmit Level Breakdown 20db	25db	30db	50db	55db	60db
QPSK1	13	50.90	52	5	7	27	3549	2250	2421	0
DMod: 1		49.50	50	1	1	11	833	362	413	0
DMod: 2		50.97	52	0	3	0	774	531	506	0
DMod: 3		50.20	51	1	2	11	583	357	336	0
DMod: 4		52.41	53	0	1	5	649	525	725	0
DMod: 5		50.99	51	3	0	0	710	475	441	0

System operators should consider lowering the attenuation level of the QPSK demodulators associated with this QPSK modulator. When the attenuation level is lowered, DHCTs transmit at a lower level.

Case 2

In this example, a quick examination of the graph may lead the system operator to believe that the system is healthy. The graph depicts a bell curve with the peak of the bell curve centered around 40 dBmV, the midpoint between our recommended transmission level of 25 and 55 dBmV.



An examination of the chart, however, shows one demodulator (DMod 2) supports DHCTs that transmit at an average of 25.47 dBmV. Another demodulator (DMod 7) supports DHCTs that transmit at an average of 50.42 dBmV. Demodulators assigned to a specific modulator should be configured to expect approximately the same transmit level from DHCTs. Therefore, system operators should investigate whether adjustments to the combining or padding networks of these demodulators are

necessary.

				Transmit Level Breakdown						
QPSK Mod Name	ID	Avg.	Md	20db	25db	30db	50db	55db	60db	
QPSKMOD	1	8	41.99	42	9	43	219	5865	490	225	0
DMod:	1		40.98	41	2	5	26	755	46	18	0
DMod:	2		25.47	40	0	0	8	633	84	42	0
DMod:	3		39.42	40	7	23	64	713	36	16	0
DMod:	4		40.56	41	0	9	46	718	35	20	0
DMod:	5		43.51	44	0	2	14	828	94	34	0
DMod:	6		41.96	42	0	3	38	1029	84	45	0
DMod:	7		50.42	47	0	1	15	853	74	37	0
DMod:	8		43.33	44	0	0	8	336	37	13	0

DHCT Delay Value Saturation Report

The DHCT Delay Value Saturation Report is primarily used to determine whether the Range Extension feature needs to be enabled on a system.

Generating the DHCT Delay Value Saturation Report

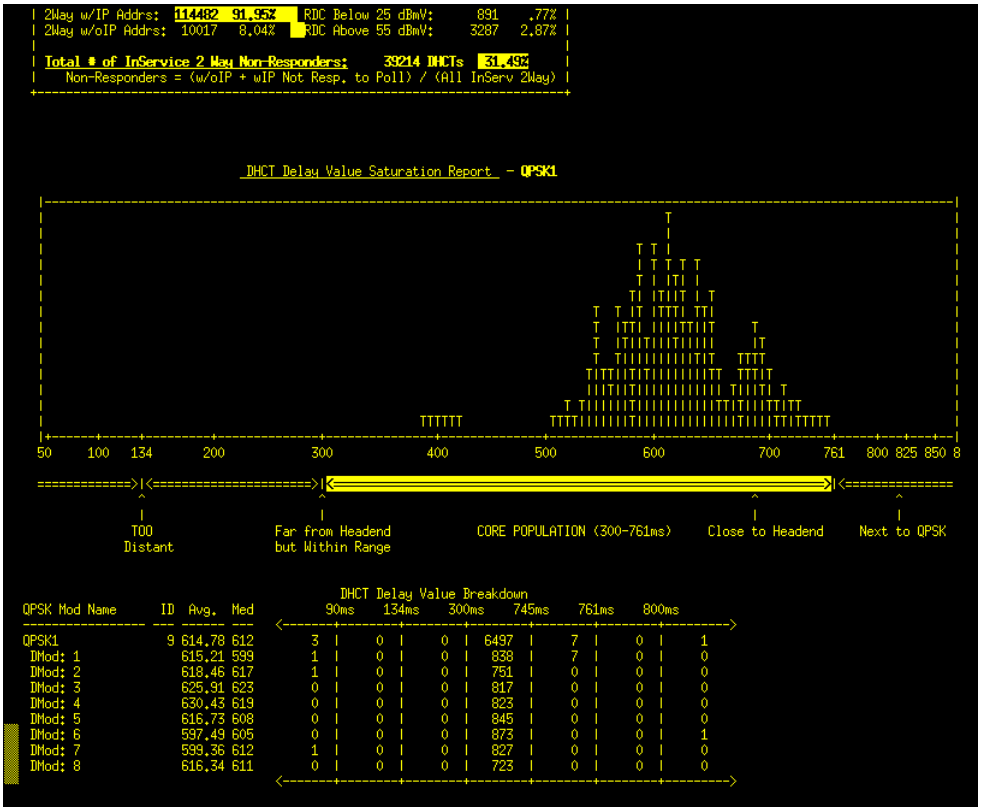
Follow these instructions to generate a DHCT Delay Value Saturation Report.

1 Maximize the xterm window.

Note: The data in the DHCT Delay Value Saturation Report is designed to display best if the window is maximized.

2 From the main menu of the DHCT Status utility, type **dl** and then press **Enter**. The system generates the DHCT Delay Value Saturation Report.

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



3 Go to ***Understanding the DHCT Delay Value Saturation Report*** (on page 120) for help in interpreting the data displayed in the report.

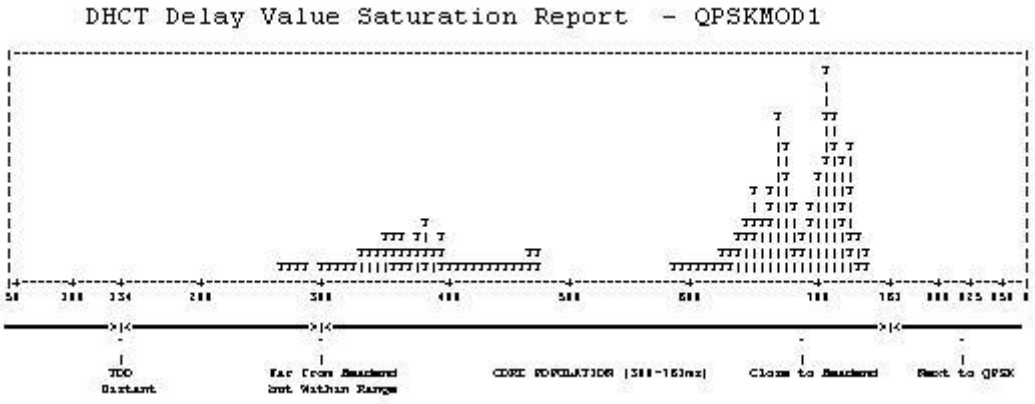
Understanding the DHCT Delay Value Saturation Report

There are two parts to the DHCT Delay Value Saturation Report:

- A graphical representation of the distribution of the various delay values of DHCTs assigned to each QPSK modulator on the system
  Note: Read ***Graphical Distribution of DHCT Delay Values*** (on page 135) for help in interpreting the graphical representation.
- A numerical analysis of the graphical representation of the various delay values of DHCTs assigned to each QPSK modulator on the system
  Note: ***Read Delay Value Analysis*** (on page 136) for help in interpreting the graphical representation.

Graphical Distribution of DHCT Delay Values

The first part of the DHCT Delay Value Saturation Report contains a graph that shows the distribution of the various delay values of DHCTs assigned to a specific QPSK modulator. In the following example, the modulator is **QPSKMOD1**. The horizontal axis of the graph plots units of time in microseconds (ms); the vertical axis (not marked on the report) plots the relative number of DHCTs with each delay value.



The data in this graph shows that the QPSK called QPSKMOD1 supports two distinct clusters of DHCTs. The first cluster of DHCTs is located close to the headend, as confirmed by the **Close to Headend** label along the x-axis. These DHCTs have a delay value centered around 700 ms.

The second cluster of DHCTs is located farther from the headend, as confirmed by the **Far from Headend but Within Range** label along the x-axis. These DHCTs have a delay value centered around 400 ms.

Having multiple clusters of DHCTs, as illustrated in this example, is normally not a problem. Non-responding DHCTs begin to appear only when delay values fall below the 134 microsecond range, as designated by the **Too Distant** label along the x-axis.

Delay Value Analysis

The second part of the DHCT Delay Value Saturation Report provides a detailed breakdown of the graphical data displayed in Graphical Distribution of DHCT Delay Values, earlier in this section. This part of the report contains the following data:

- A listing of the QPSK modulator and associated demodulators
  Note: In the following example, Modulator QPSKMOD1 is configured with eight demodulators.
- The average and the median delay values for the modulator and each demodulator
- A detailed listing showing the number of DHCTs with each delay value

DHCT Delay Value Breakdown

QPSK Mod Name	ID	Avg.	Med	90ms	134ms	300ms	745ms	761ms	800ms
QPSKMOD1	3	618.38	671	0	0	24	7150	0	0	0
DMod: 1		686.80	686	0	0	0	1086	0	0	0
DMod: 2		694.62	705	0	0	0	813	0	0	0
DMod: 3		695.50	708	0	0	0	792	0	0	0
DMod: 4		691.04	709	0	0	0	783	0	0	0
DMod: 5		681.21	669	0	0	0	1079	0	0	0
DMod: 6		664.94	660	0	0	0	1067	0	0	0
DMod: 7		367.46	369	0	0	24	753	0	0	0
DMod: 8		390.88	381	0	0	0	777	0	0	0

The data confirms the existence of two distinct clusters of DHCTs, with each cluster located a distinct radius away from the modulator.

- 7,150 DHCTs have a delay value of approximately 745 ms
  Note: These DHCTs correspond to the cluster situated over the Close to Headend label along the x-axis of the graph shown under the Graphical Distribution of DHCT Delay Values heading, earlier in this section.
- 24 DHCTs have a delay value of approximately 300 ms
  Note: These DHCTs correspond to the cluster located over the Far from Headend but Within Range label along the x-axis of the graph shown under the Graphical Distribution of DHCT Delay Values heading, earlier in this section.

QPSK Range Extension Feature

The Model D9482 QPSK Modulator is designed to be capable of successfully connecting to and operating DHCTs within a distance of approximately 128 km round trip (64 km each way when forward and reverse paths are equal). This distance limitation is mainly due to the width of the ranging slots defined in the Digital Audio-Visual Council (DAVIC) standard for operation over the hybrid fiber coax (HFC) plant.

Some cable service providers prefer to physically locate the QPSK hardware in the headend and extend coverage to DHCTs that are farther from the QPSK modulator than the currently allowable maximum distance. This optional feature, known as the QPSK Range Extension Feature for the Model D9482 QPSK Modulator, allows Explorer DHCTs to sign on to the system and operate properly at extended distances from the QPSK modulator.

DHCT OS and ResApp Evaluation by Set Top Type and Rev Report

A typical DBDS supports DHCTs of many types and revisions. The DHCT Status utility includes an option that generates a report that lists the following data:

- The number and percentage of each DHCT type and revision supported by the system
- The version of operating system and resident application software running on each DHCT type and revision

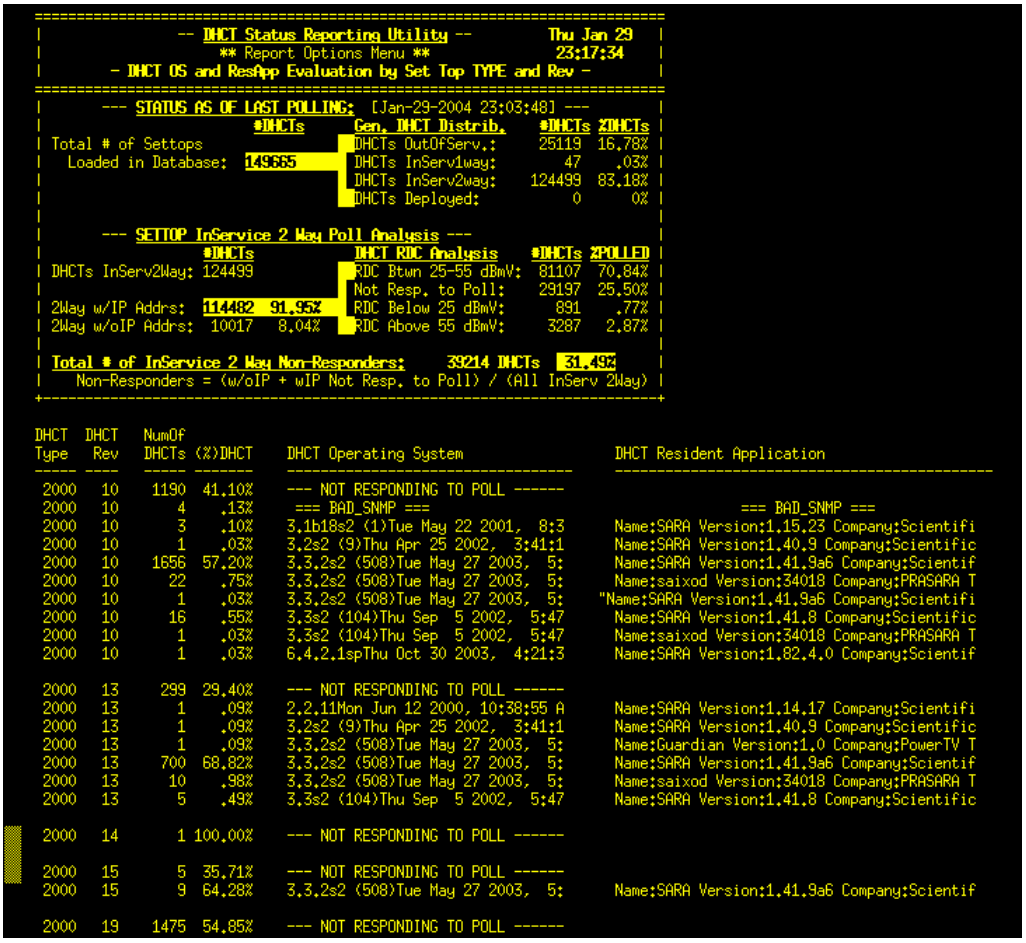
Generating the DHCT OS and ResApp Evaluation by Set Top Type and Rev report

Follow these instructions to generate the DHCT OS and ResApp Evaluation by Set Top Type and Rev Report.

1 Maximize the xterm window.

Note: The data in the DHCT OS and ResApp Evaluation by Set Top Type and Rev Report is designed to display best if the window is maximized.

2 From the main menu of the DHCT Status utility, type **os** and then press **Enter**. The system generates the DHCT OS and ResApp Evaluation by Set Top Type and Rev Report.



```
                -- DHCT Status Reporting Utility --          Thu Jan 29
                      ** Report Options Menu **               23:17:34
        - DHCT OS and ResApp Evaluation by Set Top TYPE and Rev -

        --- STATUS AS OF LAST POLLING:  [Jan-29-2004 23:03:48] ---
                          #DHCTs        Gen. DHCT Distrib.     #DHCTs  %DHCTs
 Total # of Settops                     DHCTs OutOfServ.:       25119  16.78%
   Loaded in Database:  149665          DHCTs InServ1way:          47    .03%
                                        DHCTs InServ2way:      124499  83.18%
                                        DHCTs Deployed:             0     0%

        --- SETTOP InService 2 Way Poll Analysis ---
                     #DHCTs             DHCT RDC Analysis     #DHCTs %POLLED
 DHCTs InServ2Way: 124499               RDC Btwn 25-55 dBmV:   81107  70.84%
                                        Not Resp. to Poll:     29197  25.50%
 2Way w/IP Addrs:  114482  91.95%      RDC Below 25 dBmV:       891    .77%
 2Way w/oIP Addrs:  10017   8.04%      RDC Above 55 dBmV:      3287   2.87%

 Total # of InService 2 Way Non-Responders:     39214 DHCTs   31.49%
    Non-Responders = (w/oIP + wIP Not Resp. to Poll) / (All InServ 2Way)

DHCT  DHCT   NumOf
Type   Rev   DHCTs (%)DHCT    DHCT Operating System                 DHCT Resident Application
----- ----   ----- -------    ---------------------------------     -----------------------------------------
 2000   10    1190  41.10%    --- NOT RESPONDING TO POLL ------
 2000   10       4    .13%     === BAD_SNMP ===                                  === BAD_SNMP ===
 2000   10       3    .10%    3,1b18s2 (1)Tue May 22 2001,  8:3     Name:SARA Version:1.15.23 Company:Scientifi
 2000   10       1    .03%    3,2s2 (9)Thu Apr 25 2002,  3:41:1     Name:SARA Version:1.40.9 Company:Scientific
 2000   10    1656  57.20%    3.3.2s2 (508)Tue May 27 2003,  5:     Name:SARA Version:1.41.9a6 Company:Scientif
 2000   10      22    .75%    3.3.2s2 (508)Tue May 27 2003,  5:     Name:saixod Version:34018 Company:PRASARA T
 2000   10       1    .03%    3.3.2s2 (508)Tue May 27 2003,  5:    "Name:SARA Version:1.41.9a6 Company:Scientifi
 2000   10      16    .55%    3.3s2 (104)Thu Sep  5 2002,  5:47     Name:SARA Version:1.41.8 Company:Scientific
 2000   10       1    .03%    3.3s2 (104)Thu Sep  5 2002,  5:47     Name:saixod Version:34018 Company:PRASARA T
 2000   10       1    .03%    6.4.2.1spThu Oct 30 2003,  4:21:3     Name:SARA Version:1.82.4.0 Company:Scientif

 2000   13     299  29.40%    --- NOT RESPONDING TO POLL ------
 2000   13       1    .09%    2.2.11Mon Jun 12 2000, 10:38:55 A     Name:SARA Version:1.14.17 Company:Scientifi
 2000   13       1    .09%    3,2s2 (9)Thu Apr 25 2002,  3:41:1     Name:SARA Version:1.40.9 Company:Scientific
 2000   13       1    .09%    3.3.2s2 (508)Tue May 27 2003,  5:     Name:Guardian Version:1.0 Company:PowerTV T
 2000   13     700  68.82%    3.3.2s2 (508)Tue May 27 2003,  5:     Name:SARA Version:1.41.9a6 Company:Scientif
 2000   13      10    .98%    3.3.2s2 (508)Tue May 27 2003,  5:     Name:saixod Version:34018 Company:PRASARA T
 2000   13       5    .49%    3.3s2 (104)Thu Sep  5 2002,  5:47     Name:SARA Version:1.41.8 Company:Scientific

 2000   14       1 100.00%    --- NOT RESPONDING TO POLL ------

 2000   15       5  35.71%    --- NOT RESPONDING TO POLL ------
 2000   15       9  64.28%    3.3.2s2 (508)Tue May 27 2003,  5:     Name:SARA Version:1.41.9a6 Company:Scientif

 2000   19    1475  54.85%    --- NOT RESPONDING TO POLL ------
```

3 Press **Enter** as often as required to scroll through the entire report.

10

Detach and Attach Submirrors with the mirrState Utility

Introduction

The Sun Enterprise 450 and the Sun Fire V445, V880, and V890 servers 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 server may first be required to disable the mirroring functions on the server. 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 server. 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 140).
- To re-enable the disk mirroring functions, go to ***Re-Attaching Mirrored Disks*** (on page 141).
- 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 141).

Important: The mirrState utility is restricted for use on the Sun Enterprise 450, Sun Fire V445, V880, or V890 servers, only. If the mirrState utility is run on a server 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 server.

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 server.

5 Type **exit** and then press **Enter**. You log out as root user in the xterm window.

6 Perform your maintenance operations on the server and then go to ***Re-Attaching***

Mirrored Disks (on page 141).

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 server.
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.

11

Convert DNCS Source IDs to TV Guide Source IDs with the mvsrcid Utility

Introduction

The mvsrcid utility provides system operators with the ability to convert existing DNCS source IDs to TV Guide source IDs, or to update existing TV Guide source IDs. Through use of this utility, system operators are able to present subscribers with the most current Electronic Program Guide (EPG) information.

Important: Non-Cisco source IDs are not supported by the mvsrcid utility.

In This Chapter

Overview of the mvsrcid Utility

The primary function of the mvsrcid utility is to convert DNCS source IDs to source IDs that are used by TV Guide. The information in this section describes the various steps that the system operator must accomplish in order to convert the source IDs.

1 The system operator begins the process by running the mvsrcid utility with the *-b* option. The *-b* option backs up the database tables that are involved in the conversion process, before the source IDs are converted. This way, should the conversion of source IDs fail for some reason, these database tables can be restored to their original state (*-r* option).

Notes:

- The system stores the backed-up database tables in the /dvs/backups directory of the DNCS.
- The naming convention of the backup file is srcidbackup_mmddyyyy.tar.

2 After the relevant database tables have been backed up, the system operator then runs the mvsrcid utility with the *-g* option. When run with the *-g* option, the mvsrcid utility generates a list of DNCS source IDs that need to be converted to TV Guide source IDs.

Notes:

- The system stores the file generated by the *-g* option in the current directory.
- The naming convention of the generated file is sasourceids_mmddyyyyhhmmss.list.
- Each line of the generated file contains a short description, long description, the application ID, and the current DNCS source ID.

Example: The contents of the sasourceids_mmddyyyyhhmmss.list look similar to this example:

A&E,A049 A&E,17,4101,
AMC,A051 AMC,18,4100,
ANPL,ANIMAL PLNT,19,10021,
BET,BET,20,4103,
BLMBG,Bloomberg,47,12153,
BRAVO,A050 BRAVO,21,4104,
CMT,CMT,22,4108,
CNBC,A043 CNBC,23,4109,
CNN,A044 Cable News Network,24,4110,
CNNIN,CNN International,108,7352,
COM,A069 COMEDY CENTRAL,25,4112,
COURT,A048 Court TV,26,4115,
CSPAN,A095 CSPAN,27,4105,
CSPN2,A096 CSPAN2,28,4106,
CSS,A037 Charter Sports South East,29,6069,
DIS,THE DISNEY CHANNEL,31,10008,
DISC,A053 Discovery Channel,30,4178,
DSCI,Discovery Science Channel,111,12051,
E!,A025 Entertainment TV,70,4117,
ESPN,A032 ESNP Sports TV,33,4119,
ESPN2,A033 ESPN2 Sports TV,32,4120,
ESPNC,A034 ESPN Classic TV,34,4358,
EWTN,A099 EWTN,105,4121,
FAM,Fox Family Channel,1,4179,
FLIXW,FLIX West,1,5508,
FNEWS,A046 Fox News Channel,35,4203,
FOOD,FOOD TV,89,4186,
FUTUR,A078 TELEFUTURA,104,10882,
FX,A031 FX,76,4125,
G4,G4 TECH TV,95,7795,
GALA,A076 GALAVISION,102,4250,
GAME,A075 GAME SHOW,101,12145,

3 At this point, the generated file is ready to be modified by appending the corresponding TV Guide source ID to the end of each line of the file. There are two ways to modify the file. The file can be sent to TV Guide, where TV Guide engineers will modify the file and return it to the system operator. Or, someone on-site at the headend, who is familiar with TV Guide source IDs, can modify the file directly.

Important: The file should be renamed after TV Guide source IDs have been appended to the file. This way, the system operator can readily differentiate between a file that has already been modified and one that has yet to be modified. Consider a name like sasourceids_implemented_mmddyyyyhhmmss.list for a file that has already been modified.

Example: The contents of the sasourceids_mmddyyyyhhmmss.list file, renamed to sasourceids_implemented_mmddyyyyhhmmss.list, will look similar to this example after it has been modified:

```
A&E,A049 A&E,17,4101, 1234
AMC,A051 AMC,18,4100, 5678
ANPL,ANIMAL PLNT,19,10021, 1492
BET,BET,20,4103, 1066
BLMBG,Bloomberg,47,12153, 5440
BRAVO,A050 BRAVO,21,4104,42
CMT,CMT,22,4108,1972
CNBC,A043 CNBC,23,4109,2001
CNN,A044 Cable News Network,24,4110,1955
CNNIN,CNN International,108,7352,1966
COM,A069 COMEDY CENTRAL,25,4112,1977
COURT,A048 Court TV,26,4115,1988
CSPAN,A095 CSPAN,27,4105,1999
```

New Source ID

4 After the sasourceids_mmddyyyyhhmmss.list file has been modified with TV Guide source IDs (and renamed), run the mvsrcid utility with the -i option. The -i option allows you to examine the DNCS source IDs and the corresponding TV Guide source IDs before you update the database.

5 After examining the DNCS source IDs and the corresponding TV Guide source IDs, stop the DNCS. The DNCS needs to be stopped before the database is updated with TV Guide source IDs.

6 After stopping the DNCS, run the mvsrcid utility with the *-u* option. The *-u* option updates the relevant database tables with the TV Guide source IDs.

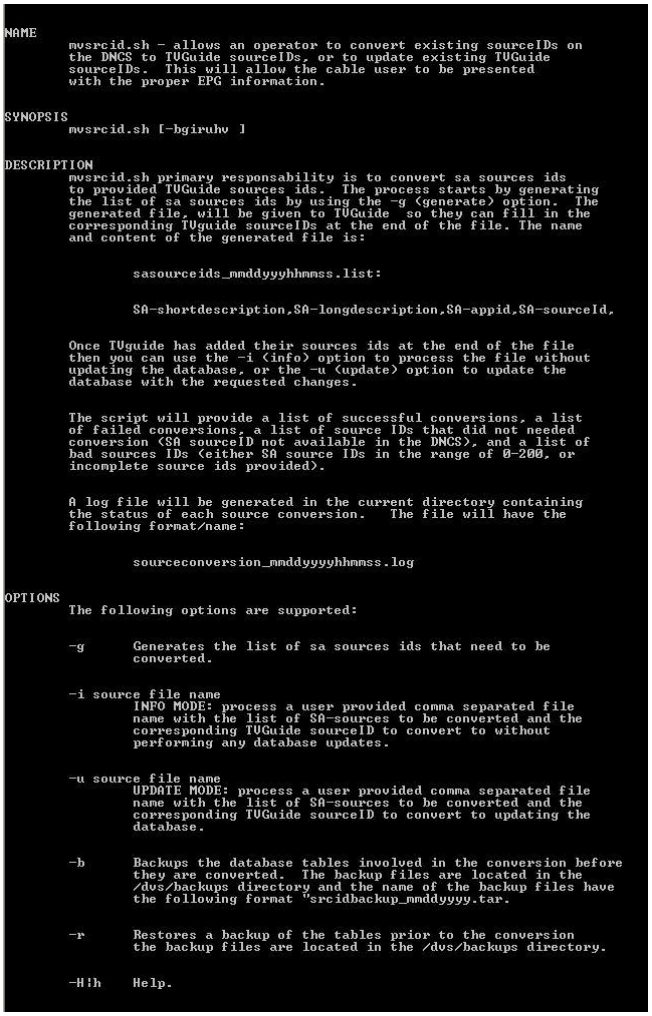
7 Restart the DNCS.

Display the Help Window and Version Number of the mvsrcid Utility

Displaying the Help Window of the mvsrcid Utility

The mvsrcid utility includes a help window that enables you to examine the various options supported by the utility. Follow these instructions to display the help window of the mvsrcid utility.

1. If necessary, open an xterm window on the DNCS.
2. Type **mvsrcid.sh -h** (or **-H**) and then press **Enter**. The system displays the help window for the mvsrcid utility.

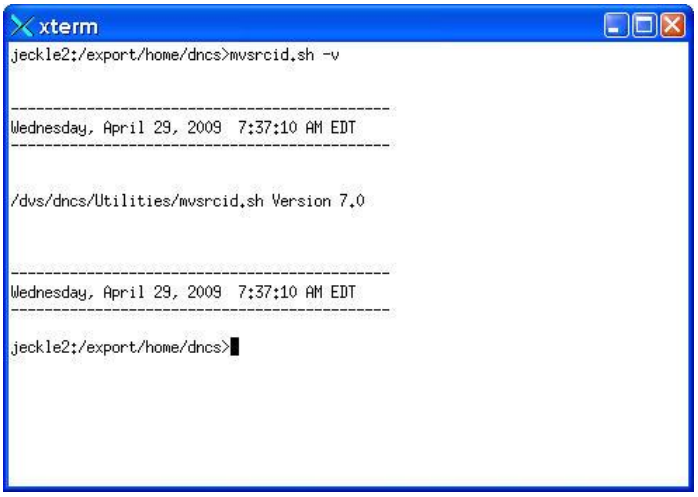


```
NAME
        mvsrcid.sh - allows an operator to convert existing sourceIDs on
        the DNCS to TVGuide sourceIDs, or to update existing TVGuide
        sourceIDs.  This will allow the cable user to be presented
        with the proper EPG information.


SYNOPSIS
        mvsrcid.sh [-bgiruhv ]


DESCRIPTION
        mvsrcid.sh primary responsability is to convert sa sources ids
        to provided TVGuide sources ids.  The process starts by generating
        the list of sa sources ids by using the -g (generate) option.  The
        generated file, will be given to TVGuide  so they can fill in the
        corresponding TVguide sourceIDs at the end of the file. The name
        and content of the generated file is:

                sasourceids_mmddyyyyhhmmss.list:

                SA-shortdescription,SA-longdescription,SA-appid,SA-sourceId,

        Once TVguide has added their sources ids at the end of the file
        then you can use the -i (info) option to process the file without
        updating the database, or the -u (update) option to update the
        database with the requested changes.

        The script will provide a list of successful conversions, a list
        of failed conversions, a list of source IDs that did not needed
        conversion (SA sourceID not available in the DNCS), and a list of
        bad sources IDs (either SA source IDs in the range of 0-200, or
        incomplete source ids provided).

        A log file will be generated in the current directory containing
        the status of each source conversion.   The file will have the
        following format/name:

                sourceconversion_mmddyyyyhhmmss.log

OPTIONS
        The following options are supported:

        -g      Generates the list of sa sources ids that need to be
                converted.

        -i source file name
                INFO MODE: process a user provided comma separated file
                name with the list of SA-sources to be converted and the
                corresponding TVGuide sourceID to convert to without
                performing any database updates.

        -u source file name
                UPDATE MODE: process a user provided comma separated file
                name with the list of SA-sources to be converted and the
                corresponding TVGuide sourceID to convert to updating the
                database.

        -b      Backups the database tables involved in the conversion before
                they are converted.  The backup files are located in the
                /dvs/backups directory and the name of the backup files have
                the following format "srcidbackup_mmddyyyy.tar.

        -r      Restores a backup of the tables prior to the conversion
                the backup files are located in the /dvs/backups directory.

        -H|h    Help.
```

Displaying the Version Number of the mvsrcid Utility

Follow these instructions to display the version number of the mvsrcid utility that is running on your DNCS.

1. If necessary, open an xterm window on the DNCS.
2. Type **mvsrcid.sh -v** (or **-V**) and then press **Enter**. The system displays the version number of the mvsrcid utility.



Note: This example shows that Version 7.0 of the mvsrcid utility is loaded onto the DNCS.

Back Up the Database Tables

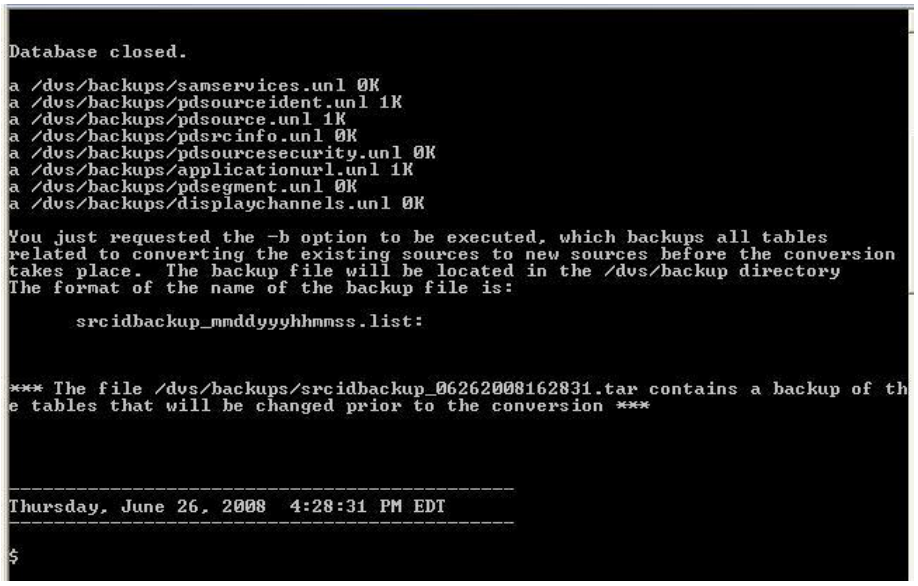
The *-b* option of the mvsrcid utility provides a means for the system operator to back up those database tables that are affected by the mvsrcid utility, before the utility is used to generate source IDs that need to be converted to TV Guide source IDs. While you do not have to back up the database tables before you update the tables with TV Guide source IDs, our engineers recommend that you do so. Should something go wrong when you update your database tables with TV Guide source IDs, your backed-up database tables will enable you to restore your system.

Important: Back up the database tables each time you use the mvsrcid utility to update your system with TV Guide source IDs.

Follow these instructions to back up the database tables that are used by the mvsrcid utility.

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

2 Type **mvsrcid.sh -b** and then press **Enter**.



Important: Note these important points about the backup of your database tables:

- The naming convention of the backup file is srcidbackup_mmddyyyyhhmmss.list.
- Do not modify this backup file. Should you ever need to restore these database tables, you need this backup file to perform the restoration.
- The *-r* option of the mvsrcid utility restores the database tables to their original form. Do NOT use the *-r* option without calling Cisco Services first.

Engineers at Cisco Services will help you assess your restoration needs and will guide you through the process.

Generate a List of Source IDs

After backing up the database tables that areaffected by the mvsrcid utility, you are now ready to generate a file that contains the source IDs that need to be converted to TV Guide source IDs. Follow these instructions to generate the list of source IDs.

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

2 Type **mvsrcid.sh -g** and then press **Enter**. The system generates a file that contains source IDs that need to be converted to TV Guide source IDs.

Notes:

- The naming convention of the generated file is sasourceids_mmddyyyyhhmmss.list.
- The file is stored in the directory from which you ran the mvsrcid utility.
- The file contains the short description, the long description, the application ID, and the current source ID -- all separated by commas.

3 Transmit the file to TV Guide. Engineers at TV Guide will append their own source ID to each line of the file.

Note: As an alternative to sending the file to TV Guide, someone on-site, who is familiar with TV Guide source IDs, can edit the file directly.

4 After the sasourceids_mmddyyyyhhmmss.list has been edited by appending TV Guide source IDs to the file, rename the file.

Note: By renaming the file, the edited file can be easily differentiated from the original file.

Example: Consider something like sasourceids_implemented_mmddyyyyhhmmss.list.

Update the Database Tables

By this time, the sasourceids_mmddyyyyhhmmss.list file should have been edited, either by TV Guide engineers or someone onsite who is familiar with TV Guide source IDs, and returned to engineers at the headend. In addition, the edited sasourceids_mmddyyyyhhmmss.list file should have been renamed, in order to easily differentiate it from the original sasourceids_mmddyyyyhhmmss.list file.

Note: For purposes of an example in this procedure, assume that the edited and renamed file is called sasourceids_implemented_mmddyyyyhhmmss.list.

You will complete the following four procedures when you update the database with TV Guide source IDs.

1. You will run the mvsrcid utility in info mode (*-i* option). The output from the *-i* option allows you to inspect the data with which the database will be updated, before the database is actually updated.
2. If the data appears sound, you will stop the DNCS. The DNCS needs to be stopped before you can update the database.
3. You will run the mvsrcid utility with the *-u* option, which loads the new TV Guide source IDs into the relevant database tables.
4. Finally, you will restart the DNCS.

Inspecting the TV Guide Source IDs

In this procedure, you will run the mvsrcid utility with the *-i* (info mode) option. The output from the *-i* option will allow you to inspect the edited sasourceids file for the addition of TV Guide source IDs. Should a TV Guide source ID be missing, or if you see a duplicate TV Guide source ID or suspect an invalid TV Guide source ID, you can halt the process before the database is erroneously updated.

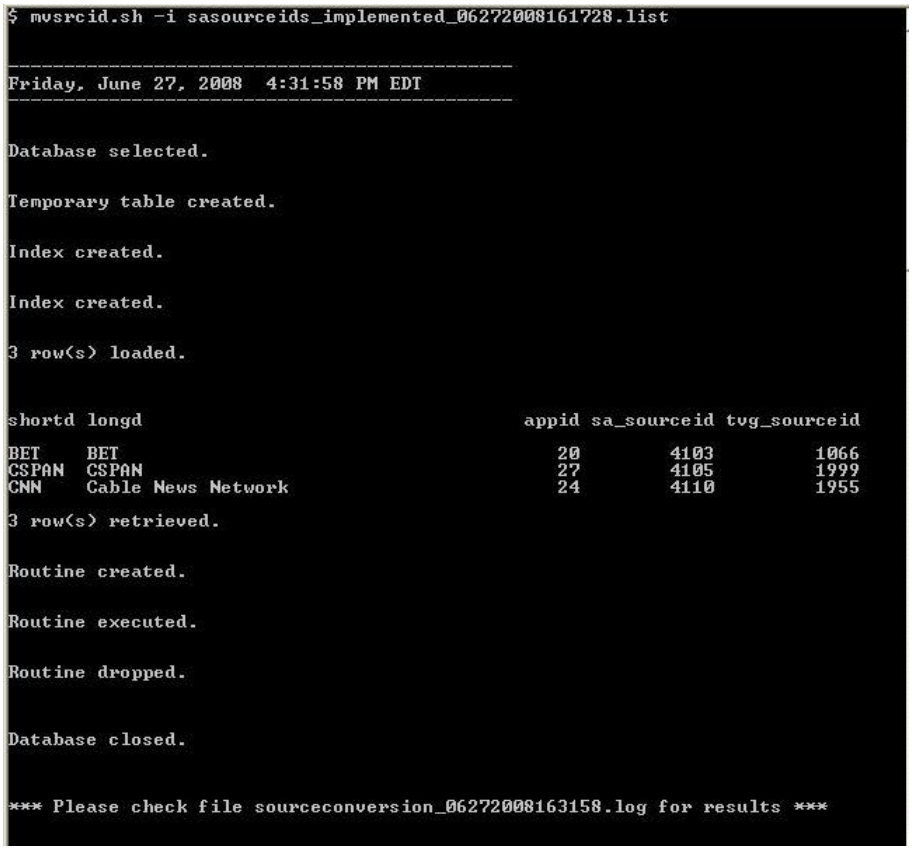
Note: Running the mvsrcid utility with the *-i* option does not update the database. The *-i* option allows you to examine the data before the database is updated.

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

2 Type **mvsrcid.sh -i <name of edited file>** and then press **Enter**. The system displays the data with which the database tables will be updated.

Note: Substitute the name of the edited sasourceids_mmddyyyyhhmmss.list file for <name of edited file>.

Example: mvsrcid.sh -i sasourceids_implemented_06272008161728.list



Stopping the cron Jobs on the DNCS

Follow these instructions to stop cron jobs 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 **pgrep -fl cron** and then press **Enter**. The DNCS displays the cron process ID (PID).

   Example: The following are only examples of sample output. Your output is likely to be different.

   - If the cron process is running without any child processes, you should see something similar to this example:

     pgrep -fl cron
     209 /usr/sbin/cron

   - If the cron process has spawned a child process, you should see something similar to this example:

     pgrep -fl cron
     209 /usr/sbin/cron
     14651 sh -c /export/home/dncs/test/tst 2>&1
     14652 sh -c /export/home/dncs/tst2 2>&1

     Note: The cron process may have spawned multiple child processes.
4. Use the cron PID from step 3, and type **ptree <PID>** and then press **Enter**. The DNCS displays the process tree of all cron processes.
5. Did the results from step 4 only include /usr/sbin/cron?
   - If **yes**, type **svcadm -v disable -st cron** and then press **Enter**.
   - If **no** (results from step 4 show multiple cron processes), type **kill -9 <PIDs>** and then press **Enter**.

     Important: List the PIDs in reverse order.

     Example: kill -9 14652 14651 209
   - If the results from step 4 did not show /usr/sbin/cron, skip the rest of this procedure. The cron jobs are already stopped.

6 Confirm that the cron jobs have stopped by typing **pgrep -fl cron** and then press **Enter**.

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

Result: The command prompt should be the only item displayed; no processes should be displayed.

7 If the results from step 4 show that the cron process is still running, repeat steps 4 through 6.

Note: Call Cisco Services for assistance, if necessary.

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

Stopping the cron Jobs on the Application Server

1 From a root xterm window on the Application Server, type **pgrep -fl cron** and then press **Enter**. The Application Server displays the cron process ID.

2 Use the cron PID from step 1 and type **ptree < PID >** and then press **Enter**. The Application Server displays the process tree of all cron processes.

3 Did the results from step 3 **only** include /usr/sbin/cron?

- If **yes**, type **svcadm -v disable -st cron** and then press **Enter**.
- If **no** (results from step 3 show multiple cron processes), type **kill -9 < PIDs >** and then press **Enter**.

  Important: List the PIDs in reverse order.

  Example: kill -9 14652 14651 209
- If the results from step 3 did *not* show /usr/sbin/cron, then the cron jobs are already stopped. Skip the rest of this procedure.

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

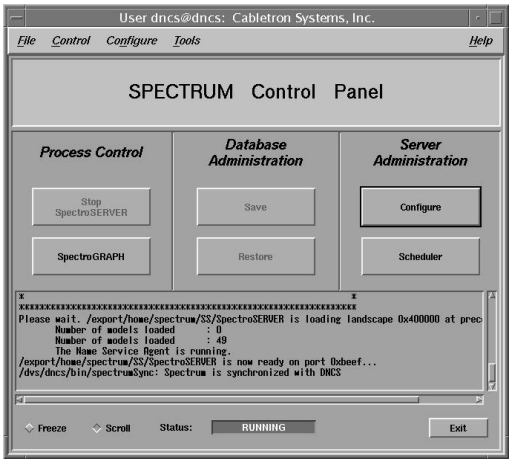
5 If the results from step 5 show that the cron process is still running, repeat steps 2 through 4.

Note: Call Cisco Services for assistance, if necessary.

Stopping Spectrum

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

2 Select the appropriate **Host Machine** and then click **OK**. The Spectrum Control Panel appears.



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

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

Stopping the Application Server

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

Stopping the Application Server at SARA Sites

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

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

Stopping the DNCS

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

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

Ensuring No Active Database Sessions on the DNCS

1. Close all windows and GUIs that are open except for the xterm window in which you are working. Are you already logged into that xterm window as **root** user?

   Note: You need to be root user to run some of the commands in this procedure.

   - If **yes**, go to step 2.
   - If **no**, follow these instructions to log in as root user.

     a Type **su -** and then press **Enter.**
     b Type the root password and then press **Enter**.

2. Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the correct user environment.

   Important: Be sure to type the dot followed by a space prior to typing /dvs.

3. Type **ps -ef | grep tomcat** and then press **Enter**. The system lists running processes that use the tomcat server.
4. Is the tomcat server running?

   - If **yes**, type **/etc/rc2.d/S98tomcat stop** and then press **Enter**.
   - If **no**, go to step 6.

5. Type **ps -ef | grep tomcat** and then press **Enter** to confirm that the tomcat server has stopped.

   Note: If the tomcat server is still running, repeat step 4.

6. Type **ps -ef | grep UI** and then press **Enter**. The system lists running UI processes.
7. Are any UI processes running (**dbUIServer** and **podUIServer**)?

   - If **yes**, type **/dvs/dncs/bin/stopSOAPServers** and then press **Enter**.
   - If **no**, go to step 9.

8. Type **ps -ef | grep UI** and then press **Enter** to confirm that UI processes have stopped.

   Note: If any GUI processes are still running, repeat step 7.

9. Type **ps -ef | grep ui** and then press **Enter** to confirm that ui process have stopped.
10. Are any ui processes running?

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

      Note: The PID to kill is in the second column in the output from step 9.

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

11 Type **showActiveSessions** and then press **Enter**. One of the following messages appears:

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

12 Did the message in step 11 indicate that there are active database sessions?

- If **yes**, follow these instructions:
  - **a** Type **killActiveSessions** and then press **Enter**. The system removes all active sessions from the database.
  - **b** Type **showActiveSessions** again and then press **Enter**.
  - **c** Did a message appear indicating that there are active database sessions?
    - If **yes**, call Cisco Services.
    - If **no**, go to step 13.
- If **no**, go to step 13.

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

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

Note: If the dncsInitd process is still running, repeat step 13.

Terminating the dhctStatus Polling Operation

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

1 From a root xterm window, type **ps -ef | grep dhctStatus** and then press **Enter**. The system reveals whether there are any instances of the dhctStatus process running.

2 Did your results from step 1 show that the dhctStatus process was running?

- If **yes**, go to step 3 to shut down the polling operations.
- If **no**, skip the rest of this procedure and go to ***Removing the signonCount Utility from System Memory*** (on page 162).

3 Type **dhctStatus** and press **Enter** to display the dhctStatus menu.

4 To terminate the polling operation, follow these instructions.

- **a** Type **p** and then press **Enter**. The system displays a polling menu.
- **b** Type **t** and then press **Enter**. The system terminates the polling operation.
- **c** Press **Enter** to return to the main menu.
- **d** Type **q** and then press **Enter** to exit the menu.

5 Type **ps -ef | grep dhctStatus** and then press **Enter** to determine whether all of the processes have been terminated.

6 Type **kill -9 [process ID]** and then press **Enter** for any process ID displayed in

the results from step 5.

Note: The process ID(s) to kill is/are located starting with the second column of the output from step 5.

7 Repeat steps 5 and 6 for any process that continues to remain active.

Removing the signonCount Utility from System Memory

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

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

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

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

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

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

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

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

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

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

Stop the dncstail Utility

Some sites may also have the third-party dncstail utility running. Stop the dncstail utility before updating your database with TV Guide source IDs.

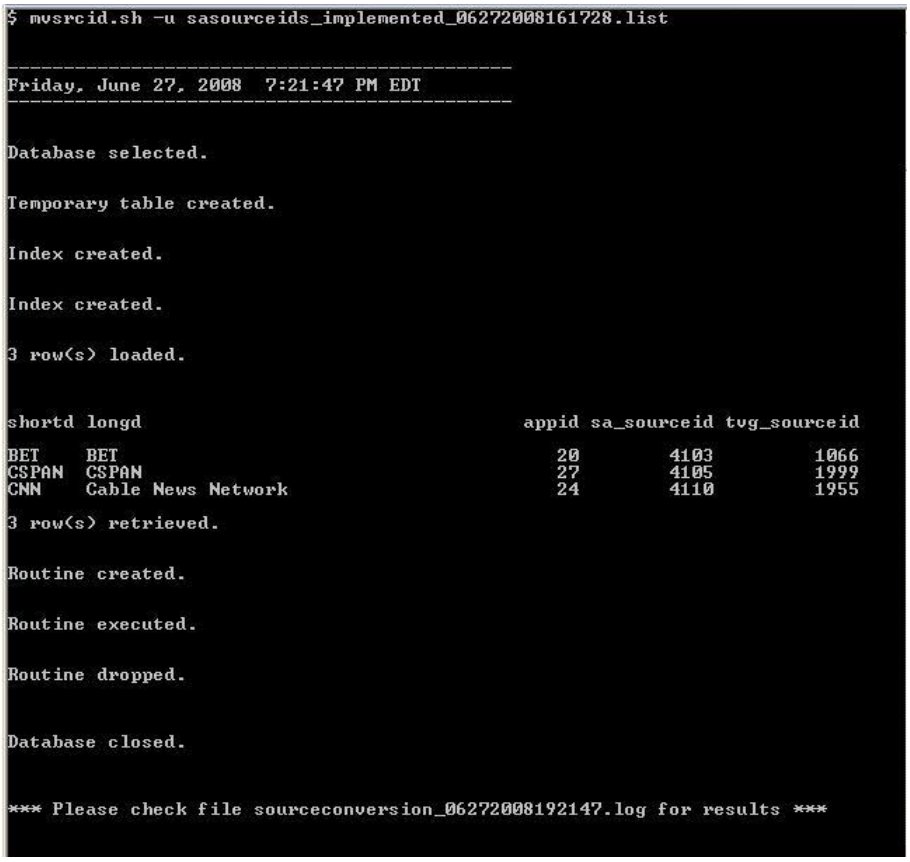
Updating the Database With TV Guide Source IDs

Now that you have inspected the TV Guide source IDs and have stopped the DNCS, you can now update the database. Follow these instructions to update your database with TV Guide source IDs.

1. If necessary, open an xterm window on the DNCS.
2. Type **mvsrcid.sh -u <name of edited file>** and then press **Enter**. The system loads the relevant database tables with TV Guide source IDs.

   Note: Substitute the name of the edited sasourceids_mmddyyyyhhmmss.list file for <name of edited file>.

   Example: mvsrcid.sh -u sasourceids_implemented_06272008161728.list



Restarting the cron Jobs on the DNCS

1. From a dncs xterm window on the DNCS, type **pgrep -fl cron** and then press **Enter**.

2 Have the cron jobs restarted on their own?
   - If **yes,** skip the rest of this procedure and go to Restarting the cron Jobs on the Application Server.
   - If **no**, continue with step 3.
3 From a root xterm window, type **svcadm -v enable -rs cron** and then press **Enter**. The system restarts all cron jobs.
4 Confirm that the cron jobs have restarted by typing **pgrep -fl cron** and then pressing **Enter**.
5 Go to *Restarting the cron Jobs on the Application Server* (on page 164).

Restarting the cron Jobs on the Application Server

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

Follow these instructions to restart the cron jobs, if necessary, on the Application Server.

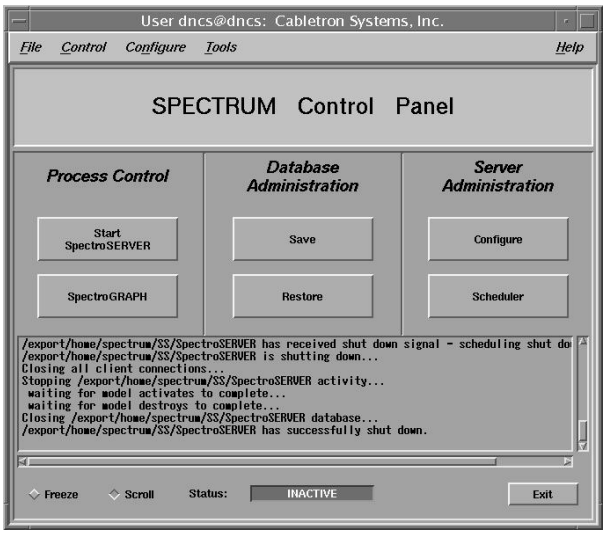
1 **Note:** From a dncs xterm window on the Application Server, type **pgrep -fl cron** and then press **Enter**.
2 Have the cron jobs restarted on their own?
   - If **yes**, skip the rest of this procedure and go to the next procedure in this chapter.
   - If **no**, continue with step 3.
3 From a root xterm window on the Application Server, type **svcadm -v enable -rs cron** and then press **Enter**. The system restarts all cron jobs.
4 Confirm that the cron jobs have restarted by typing **pgrep -fl cron** and then press **Enter**. The system should list /usr/sbin/cron.

Restarting Spectrum

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

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

2 Select the appropriate **Host Machine**, and then click **OK**. The Spectrum Control Panel window opens.



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

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

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

Restarting the DNCS

1 Open an xterm window on the DNCS.

2 Log on to the DNCS as the **root** user (or as yourself) and then type **su - dncs** and press **Enter** to assume the dncs role.

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

4 Click the middle mouse button on the DNCS and select **Administrative Console**.

The Administrative Console opens.

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

Results:

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

6 If any processes continue to display yellow or red after several minutes, try to restart each individually by selecting Process > Start Process on the DNCS Control window.

7 Do all processes display green indicators?

- If **yes**, you are finished with this procedure.
- If **no**, contact Cisco Services.

Restarting the Application Server

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

Restarting the Application Server at SARA Sites

1 Press the middle mouse button on the Application Server and select **App Serv Start**.

2 From an xterm window on the Application Server, type **appControl** and then press **Enter**. The Applications Control window opens.

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

Note: The system updates the display periodically, or you can press **Enter** to force an update.

4 When the Application Control window indicates that the current state (**Curr Stt**) of each process is running, follow the on-screen instructions to close the Applications Control window.

A Workaround for Sites Experiencing Lost Video

Some sites that run the mvsrcid utility may experience black screens or lost video. Completing the following work-around may reduce the length of time that video is lost.

1. From the DNCS Administrative Console, select the **Application Interface Modules** tab.
2. Click **SAM Config**. The SAM Configuration window opens.
3. In the space provided, record the current settings for the **Update Timer** and the **Schedule Timer**.

   Update Timer: _____

   Schedule Timer: _____
4. Change the **Update Timer** to **60** seconds; change the **Schedule Timer** to **120** seconds. These changes force the SAM to update faster.
5. Click **Save** and close the SAM Configuration window.
6. Click **SAM Service** from the DNCS Administrative Console. The SAM Service List window opens.
7. Open one of the SAM services from the SAM Service List window. The Set Up SAM Service window opens.
8. Click **Save**. Normal video should now return within 2 or 3 minutes.
9. Close the SAM Service List window.
10. Click **SAM Config**. The SAM Configuration window opens.
11. Using the settings you recorded in step 3, set the Update Timer and Schedule Timer parameters to their original values.
12. Click **Save** and close the SAM Configuration window.

12

Examine the podData File with the podDataChk Utility

Introduction

Through use of the podDataChk utility, system operators are able to examine, in summary form, the contents of the /dvs/dvsFiles/CCardServer/podData file. The podData file contains data that is communicated to CableCARD modules through the Broadcast File System (BFS) carousel, such as CableCARD configuration data, as well as data that pertains to the authorization and deauthorization of copy protection for CableCARD modules.

The podDataChk utility helps system operators determine what CableCARD/host (Pod/Host) pairs are included in the podData file, and therefore transmitted via the BFS carousel. Furthermore, because the podData file is limited to 1,500 records, the podDataChk utility helps system operators monitor the growth of the file. If the podData file grew larger than 1,500 records, data in the file might not be transmitted on the BFS carousel in a timely fashion.

The podData file contains only "active" records—records for CableCARD/host pairs that are currently authorized or deauthorized. It does not include records that were authorized or deauthorized in the past.

Each time the podDataChk utility runs, it generates the /dvs/dvsFiles/CCardServer/podData.txt file, which contains a complete summary of the data in the podData file. You can then use the UNIX *more* utility to examine the podData.txt file. However, only data that pertains to the option you used when you ran the podDataChk utility is displayed on the screen of the DNCS. Read through this chapter for a description of all the options that are supported by the podDataChk utility.

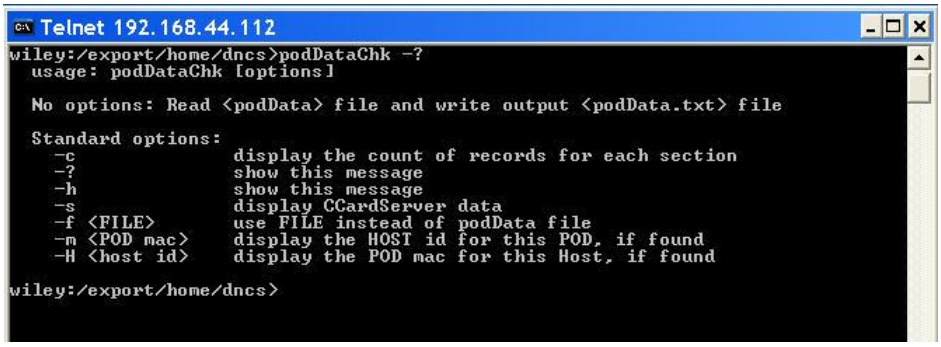
In This Chapter

Display the Help Window for the podDataChk Utility

The podDataChk utility includes a help window that enables you to examine the various options supported by the utility. Follow these instructions to display the help window of the podDataChk utility.

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

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



Note: Alternatively, you could type **podDataChk -h** and then press **Enter** to display the help window. Both the *-?* and *-h* options accomplish the same task.

Options for the podDataChk Utility

The help window reveals that the following options are available for use by the podDataChk utility:

- *-c* — Number (count) of records in the Forced Key Refresh, Pod/Host Pairs Auth, and Pod/Host Pairs Deuth sections of the podData file.
- *-?* — Displays the help window of the podDataChk utility.
- *-h* — Displays the help window of the podDataChk utility.
- *-s* — Displays data that pertains to the CableCARD server.
- *-f <File>* — Allows the user to specify a podData file other than the podData file in the working directory.
- *-m <Pod MAC address>* — Displays the host ID for the specified pod (CableCARD module).
- *-H <host ID>* — Displays the pod (CableCARD module) MAC address for the specified host.

Each of these options is demonstrated later in this section.

Count the Records in the podData File

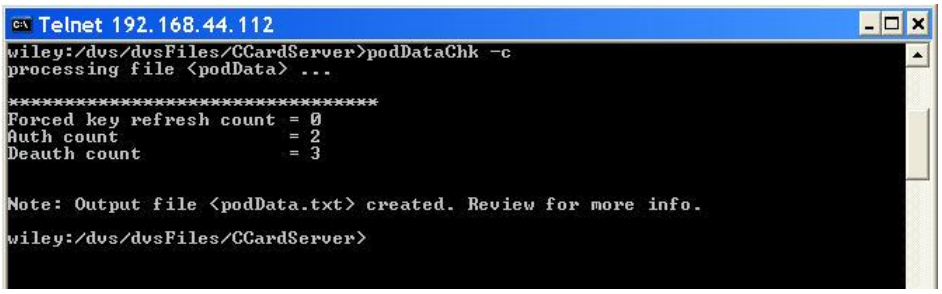
The podDataChk utility sorts the data in the podData file into various categories, or sections. One section, called the **Forced Key Refresh** section, contains the MAC addresses of CableCARD modules that need to initiate a new key exchange with its bound host for the purpose of obtaining secure transmission of data.

Another section, called the **Pod/Host Pairs Auth** section, contains the MAC addresses of CableCARD modules that have active copy protection authorization. A third section, called the **Pod/Host Pairs Deauth** section, contains the MAC addresses of CableCARD modules that have active copy protection deauthorization.

When run with the *-c* option, the podDataChk utility provides a count of the number of records in each section, and displays that data to the screen of the DNCS. In addition, the podDataChk utility generates a detailed summary of the podData file and writes that summary to the /dvs/dvsFiles/CCardServer/podData.txt file.

Follow these instructions to run the podDataChk utility with the *-c* option.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dvsFiles/CCardServer** and then press **Enter**. The /dvs/dvsFiles/CCardServer directory becomes the working directory.
3. Type **podDataChk -c** and then press **Enter**. The system displays the count of records in the three previously mentioned sections of the podData file.



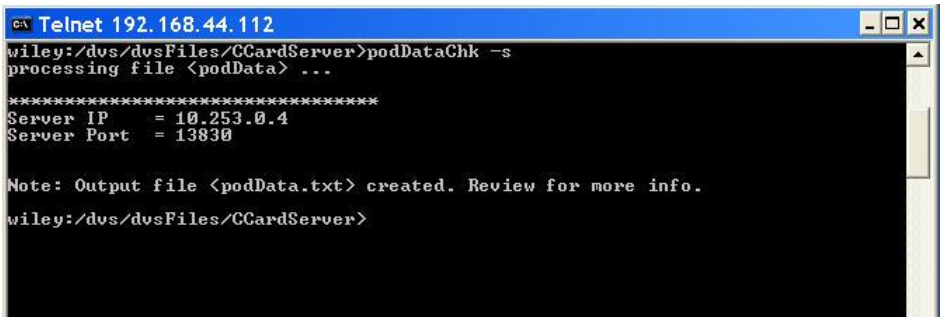
4. If desired, type **more podData.txt** and then press **Enter** to view the complete contents of the podData.txt file.

Display Configuration Data for the CableCARD Server

When run with the *-s* option, the podDataChk utility displays configuration data for the CableCARD server. The system directs output to the screen of the DNCS, as well as to the /dvs/dvsFiles/CCardServer/podData.txt file.

Follow these instructions to run the podDataChk utility with the *-s* option.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dvsFiles/CCardServer** and then press **Enter**. The /dvs/dvsFiles/CCardServer directory becomes the working directory.
3. Type **podDataChk -s** and then press **Enter**. The system displays configuration data for the CableCARD server.



4. If desired, type **more podData.txt** and then press **Enter** to view the complete contents of the podData.txt file.

Display the Host ID for a Specific Module

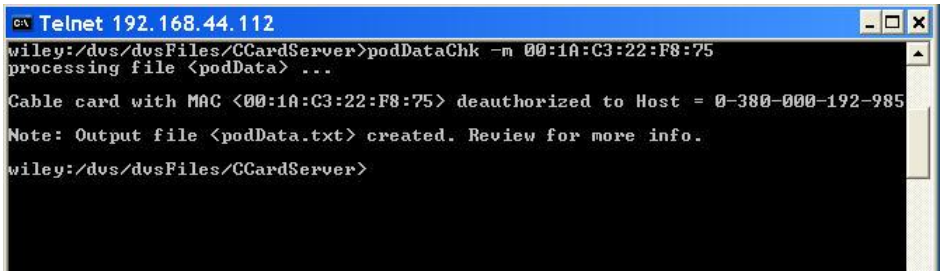
When run with the *-m* option, the podDataChk utility displays the host ID for the specified CableCARD module. The system directs the output to the screen of the DNCS, as well as to the /dvs/dvsFiles/CCardServer/podData.txt file.

Follow these instructions to run the podDataChk utility with the *-m* option.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dvsFiles/CCardServer** and then press **Enter**. The /dvs/dvsFiles/CCardServer directory becomes the working directory.
3. Type **podDataChk -m <MAC Address of CableCARD module>** and then press **Enter**. The system displays the host ID for the specified CableCARD module, provided the CableCARD module/host pair is contained in the podData file.

   Note: Substitute the MAC address of the CableCARD module for <MAC Address of CableCARD module>.

   Example: podDataChk -m 00:1A:C3:22:F8:75



4. If desired, type **more podData.txt** and then press **Enter** to view the complete contents of the podData.txt file.

Display the CableCARD MAC Address for a Specific Host

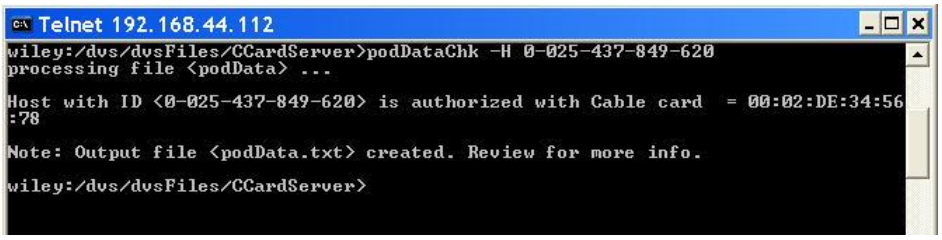
When run with the *-H* option, the podDataChk utility displays the CableCARD MAC address for the specified host. The system directs the output to the screen of the DNCS, as well as to the /dvs/dvsFiles/CCardServer/podData.txt file.

Follow these instructions to run the podDataChk utility with the *-H* option.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dvsFiles/CCardServer** and then press **Enter**. The /dvs/dvsFiles/CCardServer directory becomes the working directory.
3. Type **podDataChk -H <Host ID>** and then press **Enter**. The system displays the CableCARD MAC address for the specified host, provided the CableCARD/host pair is contained in the podData file.

   Note: Substitute the specific host ID for <Host ID>.

   Example: podDataChk -H 0-025-437-849-620



4. If desired, type **more podData.txt** and then press **Enter** to view the complete contents of the podData.txt file.

13

Monitor the Logfiles of DNCS Processes with the qtail and sesstail Utilities

Introduction

The logfiles in the /dvs/dncs/tmp directory contain important information about how the DNCS processes are operating.

As the processes run, they typically write entries into their associated logfiles that provide valuable debugging information. A typical entry into a logfile contains a time-stamp, as well as the current values of the software parameters and variables coded into the processes.

The qtail and sesstail utilities were developed to help system operators and engineers monitor the DNCS logfiles.

In This Chapter

Design of the qtail and sesstail Utilities and the System Logfiles

Design of the qtail and sesstail Utilities

The UNIX operating system includes a utility called **tail**. The tail utility allows you to monitor a file in real time; as a new line is written to a file, that line is instantly displayed by the tail utility.

Note: To learn more about the tail utility, from an xterm window on the DNCS, type **man tail** and press **Enter**.

In theory, you can use the tail utility to monitor the logfile of a DNCS process in real time. The problem, however, comes when that logfile reaches its 50,000 line limit. The tail utility has no way of knowing that a limit has been reached and that a new logfile has been created. Hence, no new data can be observed in the logfile monitored by the tail utility.

The qtail utility uses the UNIX tail utility to monitor logfiles of DNCS processes in real time. When the limit of a specific logfile is reached, however, the qtail utility automatically starts monitoring the newly created file.

The sesstail utility is very similar to the qtail utility but is specifically designed to monitor the dsm process logfiles video-on-demand (VOD) session-related activities.

Design of the System Logfiles

A limit is placed on how large the logfiles in the /dvs/dncs/tmp directory can grow. If the logfiles were designed to grow without limit, the logfiles might eventually grow so large that they would slow down the performance of the DNCS. By default, we place a 50,000 line limit on individual logfiles. Each DNCS process supports up to 10 logfiles; the first logfile has a **.000** extension, the second logfile has a **.001** extension, and so on.

Example:

- camPsm.000
- camPsm.001
- camPsm.002

When a process reaches its 10-logfile limit, the system overwrites the first logfile with new data. By supporting 10 logfiles, the DNCS allows system operators and

engineers plenty of time to save a specific logfile for later examination.

The qtail Utility

The logfiles in the /dvs/dncs/tmp directory of the DNCS have a default limit of 50,000 lines. After 50,000 lines, the system creates a new logfile. The qtail utility allows system operators or support engineers to monitor log activity and automatically switches to the next logfile when the 50,000 line limit has been reached.

The qtail utility was designed to monitor an entire logfile, or you can configure it to display only those lines that contain a particular pattern. When you configure the qtail utility to display lines in a logfile that contain a particular pattern, the utility uses the UNIX grep utility to search for that pattern.

Running the qtail Utility

Follow these instructions to run the qtail utility.

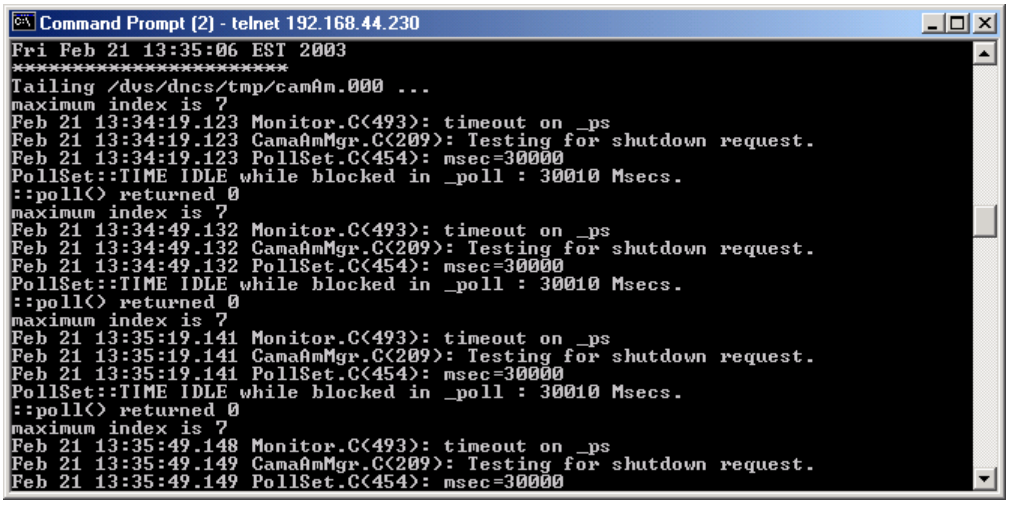
1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/tmp** and then press **Enter**. The /dvs/dncs/tmp directory becomes the working directory.
3. Choose one of the following options:
   - To use the qtail utility to monitor an entire logfile, go to step 4.
   - To use the qtail utility to display only those lines that contain a particular pattern, go to step 6.

4 To use the qtail utility to monitor an entire logfile, type **qtail [process_name]** and then press **Enter**. The qtail utility begins monitoring the logfile of the selected process.

Notes:

- Substitute the process name whose logfile you want to monitor for [process_name].
- You do not have to type the complete process name; you can type just enough to uniquely identify the process name from other processes.
  - Type qamM for qamManager.
  - Type siM for siManager.
  - Type camAu for camAuditor.

Example: Type **qtail camAu** and then press **Enter** to display the logfile associated with the camAuditor process.



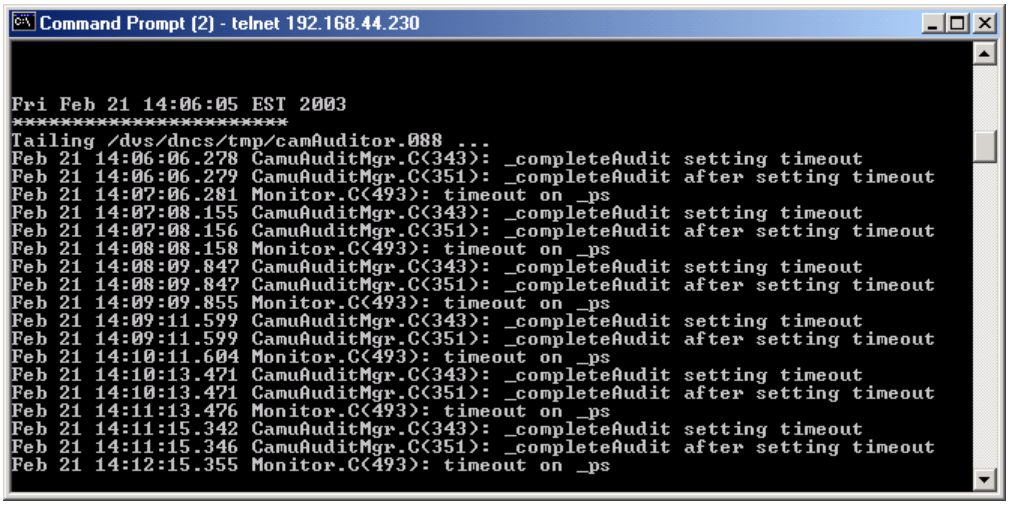
5 Type the **Ctrl** and **c** keys simultaneously to exit from the qtail utility.

6 To use the qtail utility to monitor a logfile and display only those lines that contain a particular pattern, type **qtail [process_name] <pattern>** and then press **Enter**. The qtail utility begins monitoring the logfile of the selected process.

Notes:

- Substitute the process name whose logfile you want to monitor for [process_name].
- You do not have to type the complete process name; you can type just enough to uniquely identify the process name from other processes.
  - Type **qamM** for qamManager.
  - Type **siM** for siManager.
  - Type **camAu** for camAuditor.
- Substitute the pattern you want to find for <pattern>.

Example: Type **qtail camAu timeout** and then press **Enter** to display only those lines that contain the word timeout in the logfiles associated with the camAuditor process.



7 Type the **Ctrl** and **c** keys simultaneously to exit from the qtail utility.

The sesstail Utility

The sesstail utility is similar to the qtail utility, except that it is designed to monitor the logfiles of the dsm process for session-related information. Examples of session-related information include session set up and tear-down activity.

You can use the sesstail utility to monitor the logfiles of the dsm process for session-related activity in real time or to search for session-related activity in existing dsm logfiles.

Note: By searching for session-related activity in existing dsm logfiles, you can troubleshoot VOD problems that have already occurred.

Running the sesstail Utility

Follow these instructions to run the sesstail utility.

1. If necessary, open an xterm window on the DNCS.
2. Choose one of the following options:
   - To monitor the dsm logfiles in real time for session-related activity, go to step 3.
   - To review existing dsm logfiles for session-related activity, go to step 5.
3. To monitor the dsm logfiles for session-related activity in real time, type **sesstail** and then press **Enter**. The sesstail utility begins monitoring the dsm logfiles for session-related activity.

   Example: Sample output from the sesstail utility is displayed in the following example.

   $ sesstail
   ++++ 00:40:7B:D6:B5:B3/515 ++++
   ClientSessReq: Feb 19 07:23:50.008
   ServerSessInd: Feb 19 07:23:50.016
   ServerAddRsrReq: Feb 19 07:23:50.207
   ServerAddRsrCnf: Feb 19 07:23:50.270 (response=0)
   ServerSessRsp: Feb 19 07:23:50.335 (response=0)
   ClientSessCnf: Feb 19 07:23:50.346 (response=0)
   ++++ 00:40:7B:D6:B5:B3/515 ++++
   ClientRelReq: Feb 19 07:23:58.683
   ServerRelInd: Feb 19 07:23:58.687
   ServerRelRsp: Feb 19 07:23:58.709 (Response=0)
   ClientRelCnf: Feb 19 07:23:58.713 (Response=0)

4 Type the **Ctrl** and **c** keys simultaneously to exit from the sesstail utility.

5 To review an existing dsm logfile for session-related activity, type **sesstail [filename]** and then press **Enter**. The selected file opens for review.

Note: Substitute the path and name of the logfile you want to review for [filename].

Example: sesstail /dvs/dncs/tmp/dsm.000

6 Type the **Ctrl** and **c** keys simultaneously to exit from the sesstail utility.

14

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 server 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 server. These are the only server platforms that support disk mirroring.

In This Chapter

Run the syncwait Utility

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

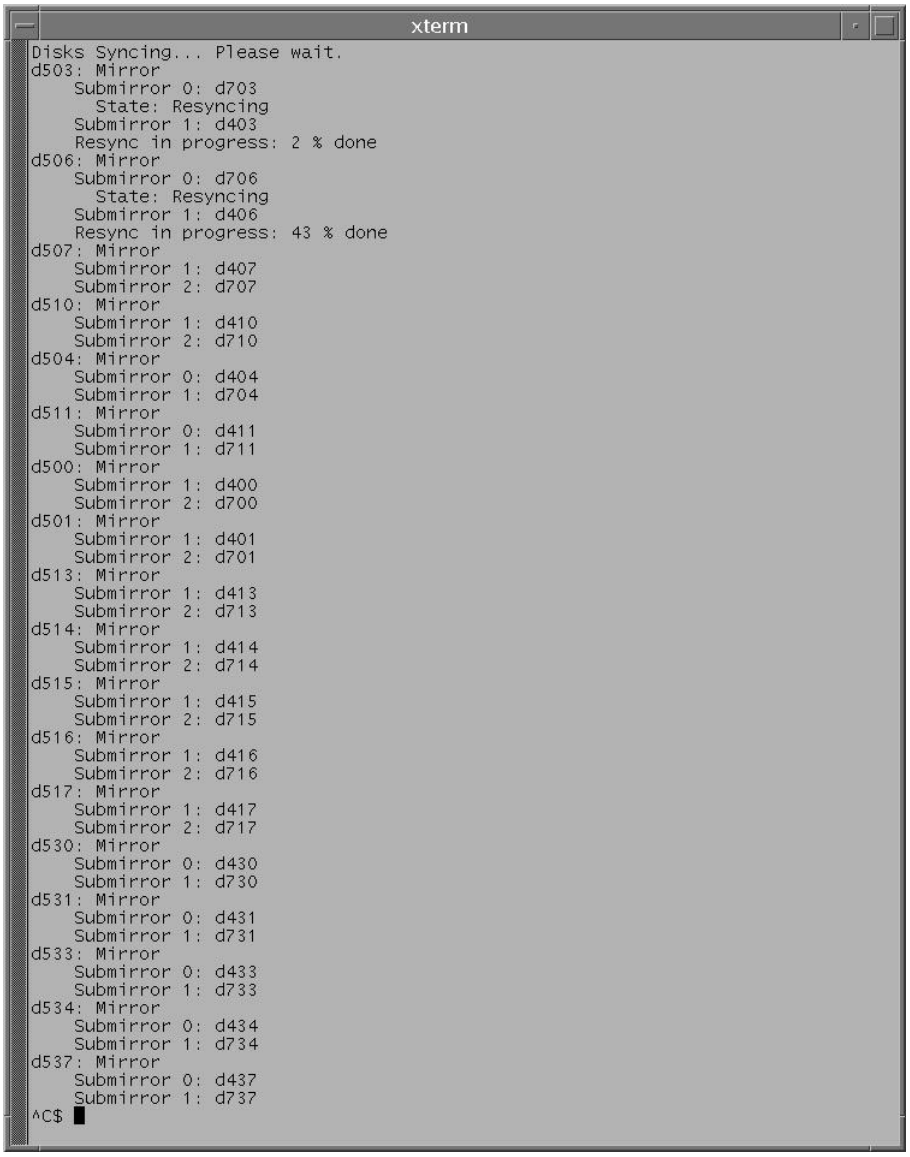
1 If necessary, open an xterm window on the DNCS.

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?

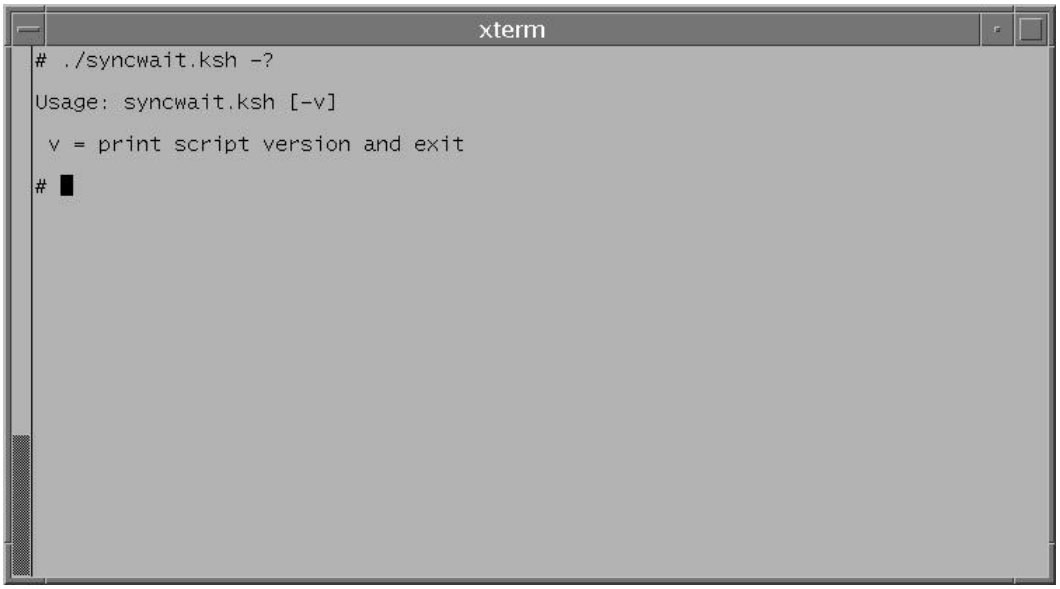
Result: The syncwait utility exits.

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.

15

Manage DHCT Download Groups with the runCVT Utility

Introduction

The runCVT utility allows system operators and lab personnel to manage DHCTs in download groups. Through the runCVT utility, system operators can add DHCTs to download groups, delete DHCTs from download groups, assign DHCTs in a download group to the fast refresh list, and can create an entry in the crontab file for DHCTs in a download group to be continuously fast-refreshed.

The instructions in this chapter describe how to prepare a text file to be used for adding DHCTs to a download group, and then how to run the runCVT utility, along with its supported options.

Limitation

There are specific messages that need to be transmitted between the DNCS GUI and the osm process of the DNCS in order to affect changes to the download groups. Unfortunately, the runCVT cannot be used to transmit these messages. Occasionally, you will need to add or delete one DHCT to or from a download group manually, through the DNCS GUI, in order to get the DNCS to respond to the runCVT utility. Messages displayed by the runCVT utility will tell you when this is necessary.

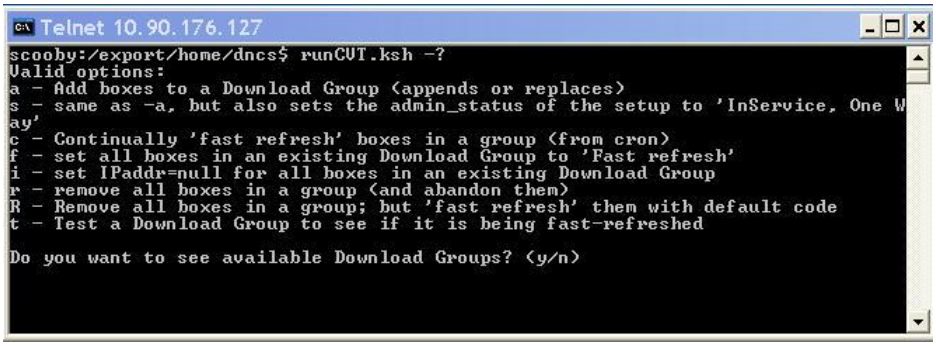
In This Chapter

Display the Help Window for the runCVT Utility

The help window is often a good place to start if you are unfamiliar with a utility. Follow these instructions to display the help window of the runCVT utility.

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

2 Type **runCVT.ksh -?** and then press **Enter**. The system displays the valid options for the runCVT utility.



Note: If desired, you can press **Enter** after the help window displays to see a list of available download groups.

Options for the runCVT Utility

The help window reveals that the following options are available for use by the runCVT utility:

- *a* – Adds DHCTs to an existing download group.
- *s* – Provides support for adding a host or hosts to the CVT download group. This option sets the administrative status of DHCTs to in-service one-way so that the host can receive CVT group assignment messages from the PassThru process.
  Important: Do not use the *-s* option with DHCTs or CableCARD modules. The -s option is used only to add a host or hosts to the CVT download group.
- *c* – Continually "fast refreshes" DHCTs in a download group.
  Note: This option is run from the crontab file.
- *f* – Sets all DHCTs in an existing download group to "fast refresh".
- *i* – Sets the IP address of all DHCTs in an existing download group to null.
- *r* – Removes (and abandon) all DHCTs from a specified download group.
- *R* – Removes all DHCTs from a specified download group, and then "fast refresh" them with default DHCT code.
- *t* – Tests a download group to confirm that DHCTs within the group are being

"fast refreshed".

Prepare the Text File

Prior to using the runCVT utility to add DHCTs to a download group, system operators prepare a text file that contains the MAC addresses of the DHCTs that are to be assigned to the download group. System operators can then run the runCVT utility with the *-a* option, and refer to the text file, when prompted. The system will then assign each DHCT contained in the text file to the specified download group.

Guidelines for Preparing the Text File for the runCVT Utility

Use the following guidelines when preparing the input text file:

- Prepare the file using a standard UNIX 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
- 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: runCVT-in_01.30.08 for a file that was created on January 30, 2008.

Preparing the Text File

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

Important: These instructions use the vi text editor as an example. The vi text editor is not intuitive. These instructions are no substitute for a good working knowledge of the vi text editor.

1. If necessary, open an xterm window on the DNCS.
2. Type **vi < complete path and file name >** and then press **Enter**.
   Example: vi /tmp/runCVT-in_01.30.08
3. 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 for the runCVT Utility*** (on page 199).
4. Save the file and close the vi editor.

Add DHCTs to a Download Group

The most common use of the runCVT utility is to add DHCTs to a download group. When DHCTs belong to a specific download group, they can download software that is intended only for DHCTs that belong to that group. System operators can add DHCTs to a specified download group through use of the *-a* option of the runCVT utility.

When run with the *-a* option, the runCVT utility will first seek to confirm the operator's intent to add DHCTs to a download group. The operator is then prompted to specify the Group ID of the download group that is to have DHCTs added to it, as well as the name of the file that contains the DHCT MAC addresses.

The utility then prompts the operator to indicate whether existing DHCTs in the download group should be deleted before new DHCTs are added to the group. Any DHCTs that are deleted are placed on a fast refresh list to download default DHCT code.

Note: The fast refresh list describes a list of recently modified DHCTs that are notified by the DNCS to download new code. DHCTs typically remain on the fast refresh list for about an hour.

Important: Be certain the following conditions are true before you try to add DHCTs to a download group by way of the runCVT utility:

- You know the ID of the existing download group to which you want to add DHCTs.
  Note: See ***Display the Help Window for the runCVT Utility*** (on page 197) for information on how to generate a list of existing download groups.
- You have created a text file that contains the MAC addresses of DHCTs that are to be added to the download group.
  Note: See ***Prepare the Text File*** (on page 199) for guidelines and instructions on preparing the file of MAC addresses.

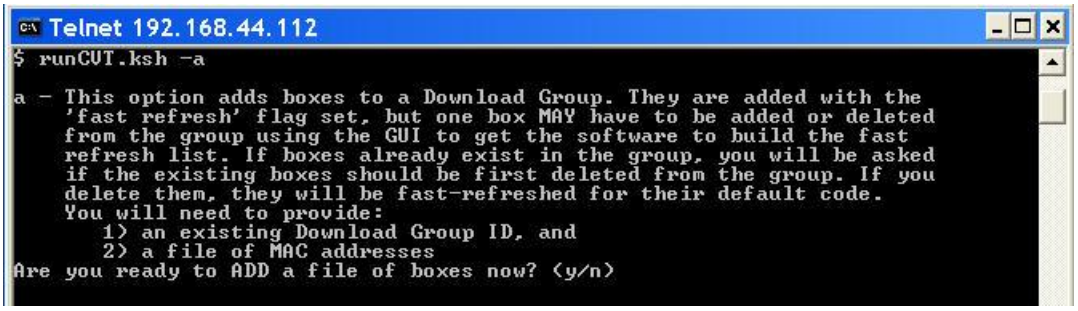
Adding DHCTs to a Download Group

Follow these instructions to add DHCTs to a download group.

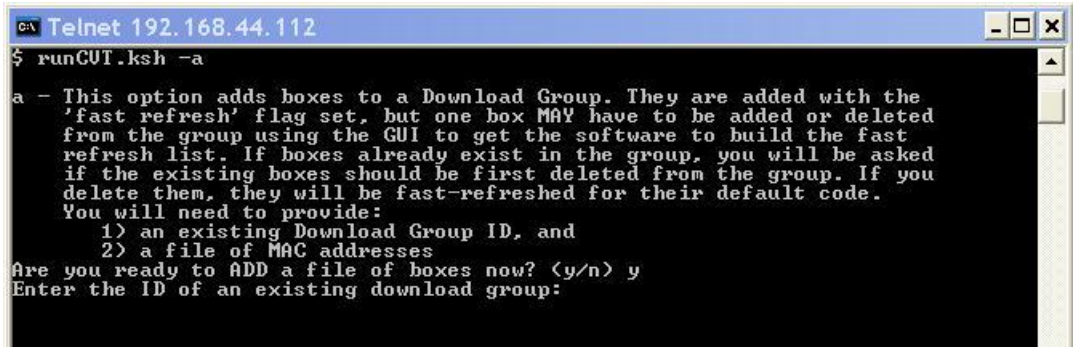
1 If necessary, open an xterm window on the DNCS.

2 Type **runCVT.ksh -a** and then press **Enter**. The system displays a message that describes the actions of the *-a* option, and then seeks confirmation of your intent to add DHCTs to a download group.

Important: Read the confirmation message thoroughly.

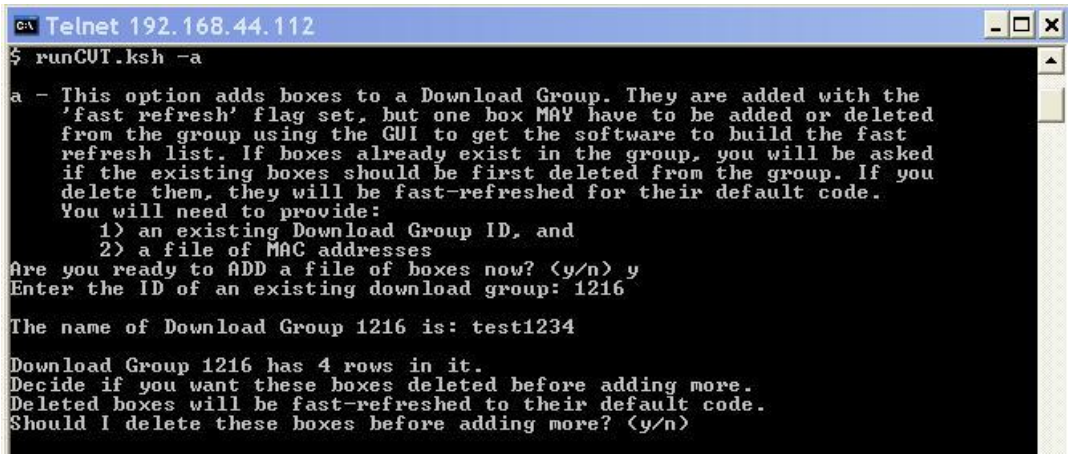


3 Type **y** and then press **Enter**. The message updates to prompt you to type the ID of the existing download group that you want to use.



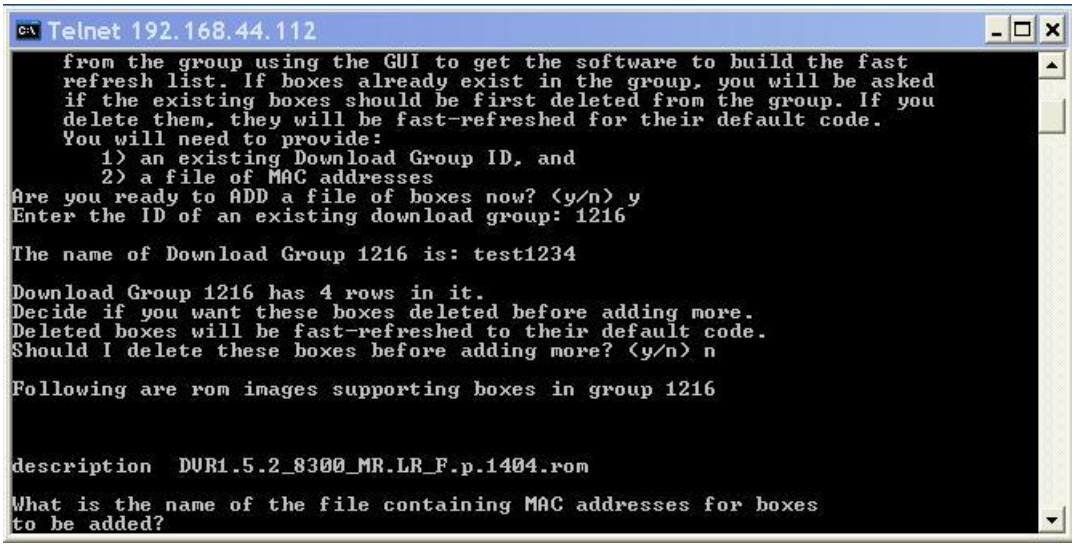
4 Type the ID of the appropriate download group and then press **Enter**. The message updates by prompting you to decide whether you want to delete any existing DHCTs in the download group.

Note: Any deleted DHCTs will be placed on a fast refresh list to receive default DHCT code.



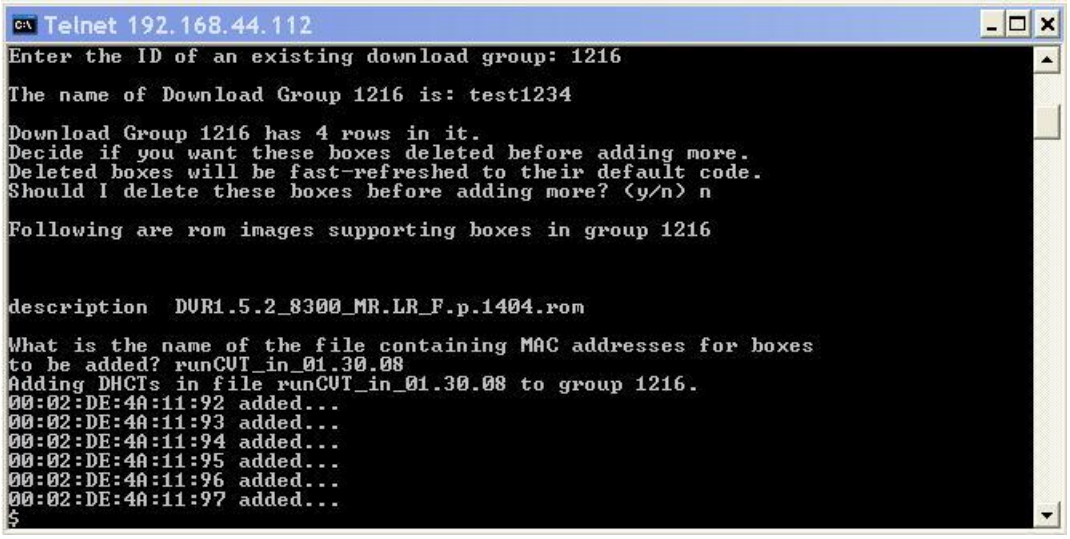
5 Type **y** or **n**, whichever is appropriate, and then press **Enter**. The message updates by prompting you to type the name of the text file that contains the MAC addresses of the DHCTs that you want to add.

Example: runCVT_in_01.30.08



6 Type the name of the text file and then press **Enter**. The message updates by listing the MAC addresses of the DHCTs as they are added to the download group.

Note: Be sure to type the complete path to the text file, if you are not already in the directory that contains the text file.

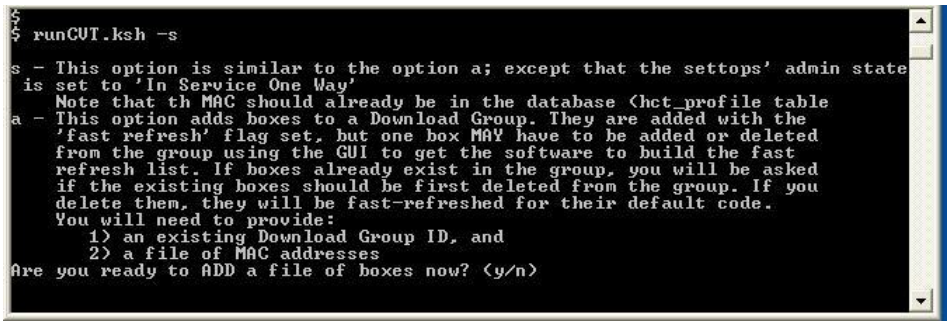


Assign a Host or Hosts to the CVT Download Group

Follow these instructions to use the *-s* option of the runCVT utility to assign a host or hosts to the CVT download group.

1. If necessary, open an xterm window on the DNCS.
2. Type **runCVT.ksh -s** and then press **Enter**. The system displays a message that describes the actions of the *-s* option, and then displays a conformation message.

   Important: Read the confirmation message thoroughly.



3. Type **y** and then press **Enter**. The message updates to prompt you to type the ID of the existing download group that you want to use.
4. Type the ID of the appropriate download group and then press **Enter**. The message updates by prompting you to decide whether you want to delete any existing DHCTs in the download group.

   Note: Any deleted DHCTs will be placed on a fast refresh list to receive default DHCT code.
5. Type **y** or **n**, whichever is appropriate, and then press **Enter**. The message updates by prompting you to type the name of the text file that contains the MAC addresses of the DHCTs that you want to add.**Example: runCVT_in_01.30.08**
6. Type the name of the text file and then press **Enter**. The message updates by listing the MAC addresses of the DHCTs as they are added to the download group.

   Note: Be sure to type the complete path to the text file, if you are not already in the directory that contains the text file.

Add an Entry for the runCVT Utility to the crontab File

The *-c* option of the runCVT utility adds an entry to the crontab file of the DNCS that continually resets the fast refresh counter for DHCTs in a specific download group. These DHCTs will stay on the fast refresh list forever; you need to remove them from the fast refresh list by running the runCVT utility with either the *-r* option or the *-R* option, both of which are described later in this chapter.

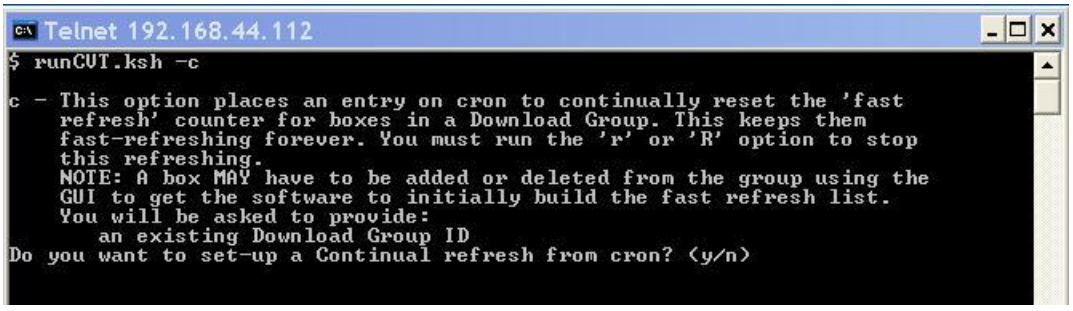
You need to know the ID number of the specific download group before you run the runCVT utility with the *-c* option.

Adding an Entry for the runCVT Utility to the crontab File

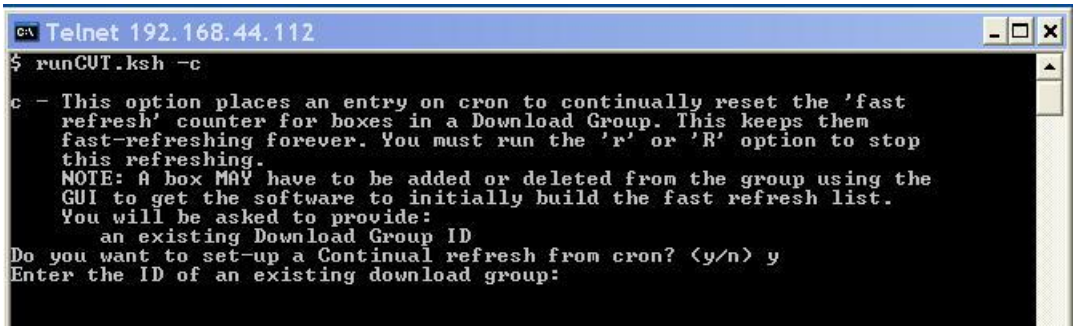
Follow these instructions to add an entry for the runCVT utility (and a specific download group) to the crontab file of the DNCS.

1. If necessary, open an xterm window on the DNCS.
2. Type **runCVT.ksh -c** and then press **Enter**. The system displays a message that describes the actions of the *-c* option, and then seeks confirmation of your intent to add an entry to the crontab file.

   Important: Be sure to read the confirmation message carefully.



3. Type **y** and then press **Enter**. The message updates to prompt you for the ID of the existing download group for which you want a crontab entry.



4 Type the ID of the appropriate download group and then press **Enter**. The system adds a fast refresh entry for the download group to the crontab file.

Assign DHCTs in a Download Group to the Fast Refresh List

The *-f* option of the runCVT utility places all of the DHCTs in a specific download group onto the fast refresh list, where they will remain for one hour. To run the runCVT utility with the *-f* option, you need to know the ID number of the appropriate download group.

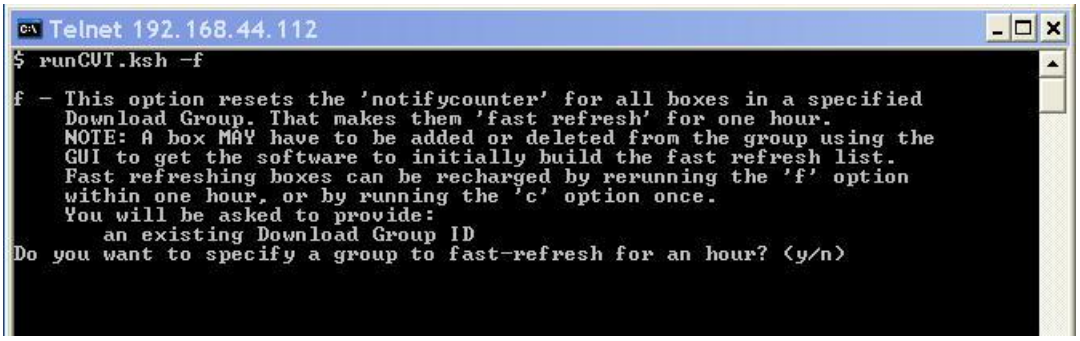
Assigning DHCTs in a Download Group to the Fast Refresh List

Follow these instructions to assign DHCTs in a download group to the fast refresh list.

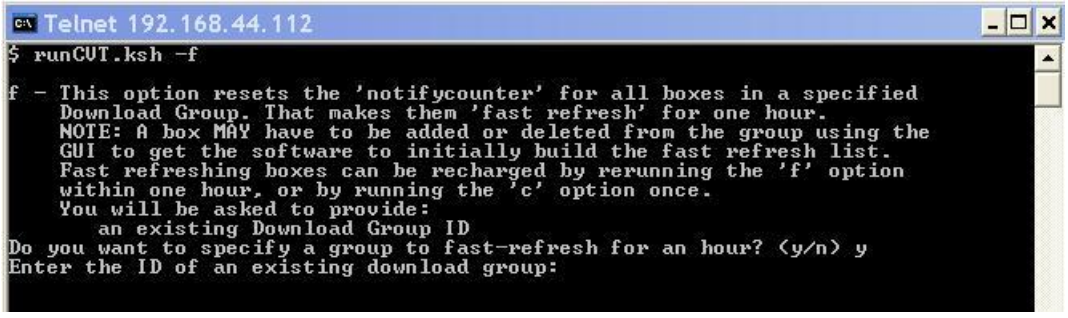
1 If necessary, open an xterm window on the DNCS.

2 Type **runCVT.ksh -f** and then press **Enter**. The system displays a message that describes the actions of the *-f* option, and seeks confirmation of your intent to place all DHCTs in a download group onto the fast refresh list.

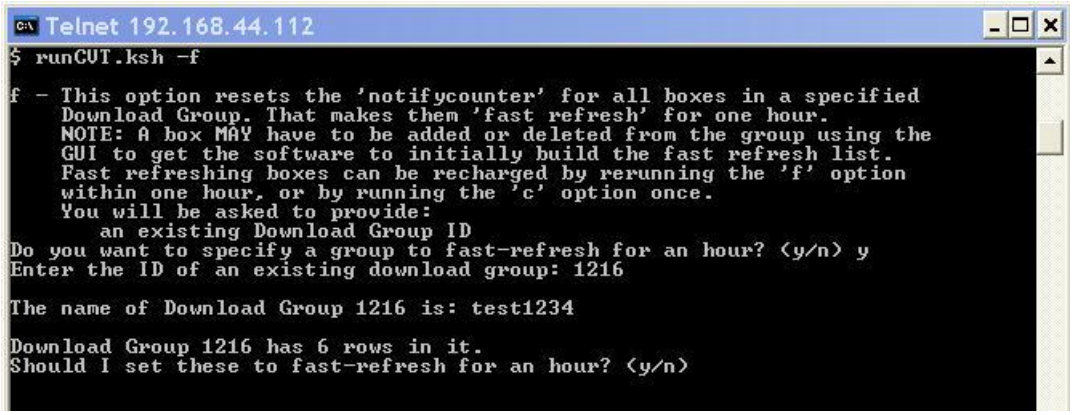
Important: Be sure to read through the message carefully.



3 Type **y** and then press **Enter**. The message updates to prompt you to enter the ID number of the appropriate download group.



4 Type the ID number of the appropriate download group and then press **Enter**. The message updates to seek confirmation of your intent to place DHCTs from the download group onto the fast refresh list for one hour.



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

Set IP Address of DHCTs in a Download Group to Null

Use the *-i* option of the runCVT utility to set the IP address of DHCTs in a specified download group to null. System operators may need to set the IP address of DHCTs in a download group to null in order to enable one-way DHCTs to accept their group number.

To use the *-i* option of the runCVT utility, you need to know the ID number of the appropriate download group.

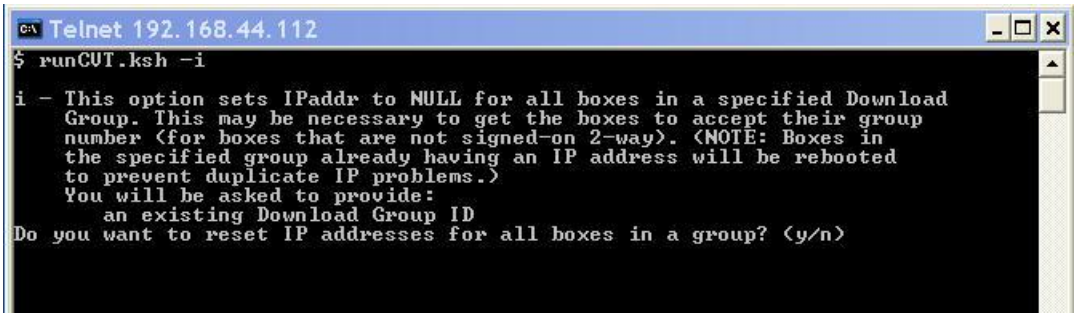
Setting the IP Address of DHCTs in a Download Group to Null

Follow these instructions to set the IP address of DHCTs in a download group to null.

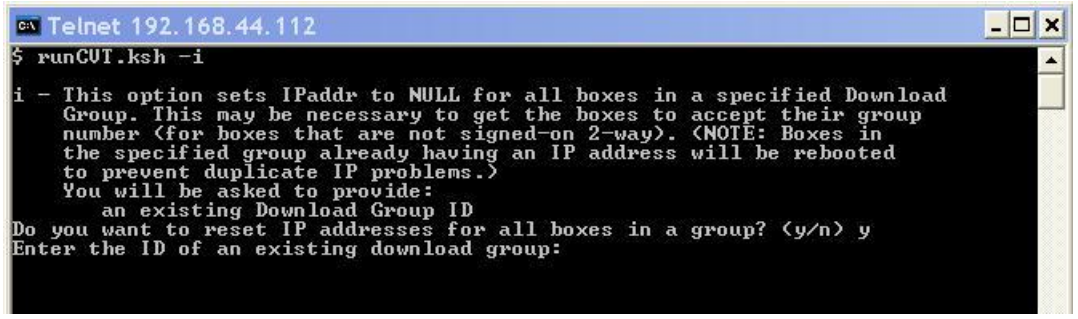
1 If necessary, open an xterm window on the DNCS.

2 Type **runCVT.ksh -i** and then press **Enter**. A message appears that describes the *-i* option, and then seeks confirmation of your intent to set the IP address of DHCTs in a download group to null.

Important: Read through the message thoroughly.

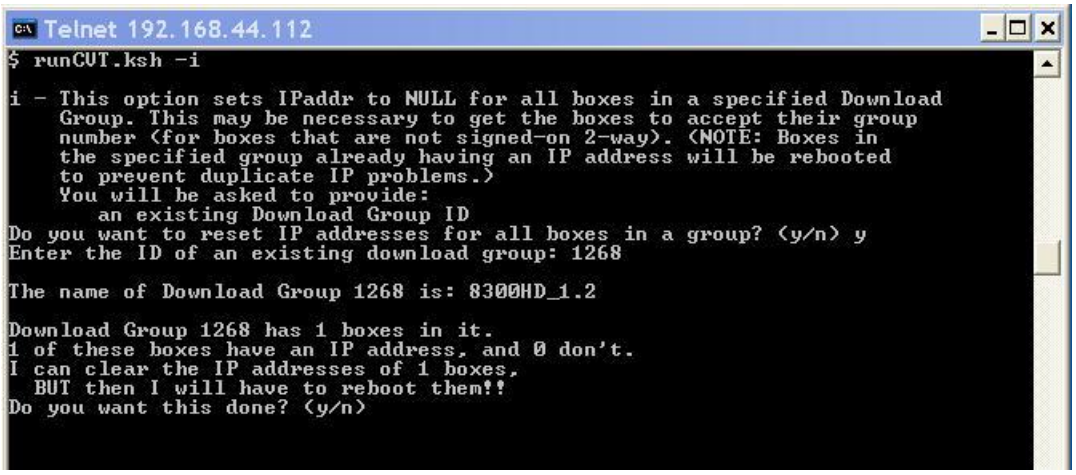


3 Type **y** and then press **Enter**. The message updates to prompt you to enter the ID of the appropriate download group.



4 Type the ID number of the appropriate download group and then press **Enter**. The message updates to list the number of DHCTs in the download group that

have an IP address (and the number of those that do not), and then seeks confirmation of your intent to reboot the DHCTs that have an IP address.



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

Remove DHCTs from a Download Group

Use either the *-r* or the *-R* options of the runCVT utility to remove all DHCTs from a specified download group.

- The *-r* option removes all DHCTs from a specified download group, and then "abandons" them. The DHCTs are removed from the database and are not assigned to any fast refresh list. Any entries for the download group are deleted from the crontab file, as well.

  Note: The *-r* option is appropriate for those cases when you do not want DHCTs to download new code immediately.

- The *-R* option removes all DHCTs from a specified download group, but does not "abandon" them. Instead, these DHCTs are assigned to a fast refresh list to receive default DHCT code. Any entries for the download group are deleted from the crontab file, as well.

  Note: The *-R* option is appropriate for those cases when you want DHCTs to download default code. In most cases, this is the preferred method for removing DHCTs from a download group.

To use either the *-r* or the *-R* option, you need to know the ID number of the download group from which you want to remove all DHCTs.

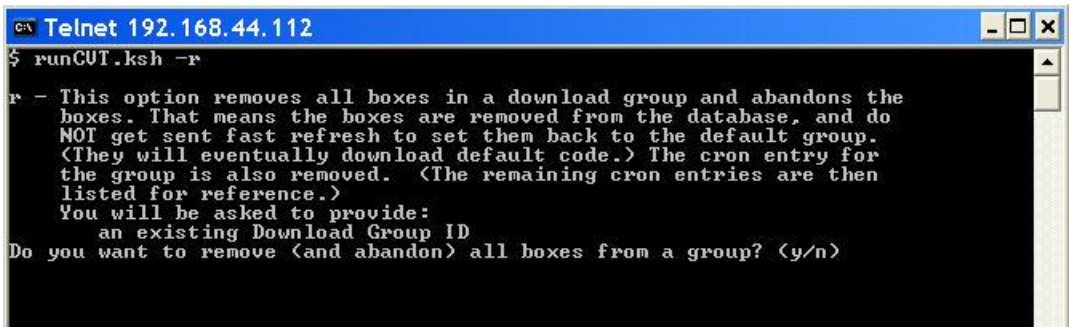
Removing DHCTs from a Download Group and Abandoning Them

In this procedure, you will use the *-r* option of the runCVT utility to remove all DHCTs from a download group, and then abandon them—that is, they are removed from the database, as well.

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

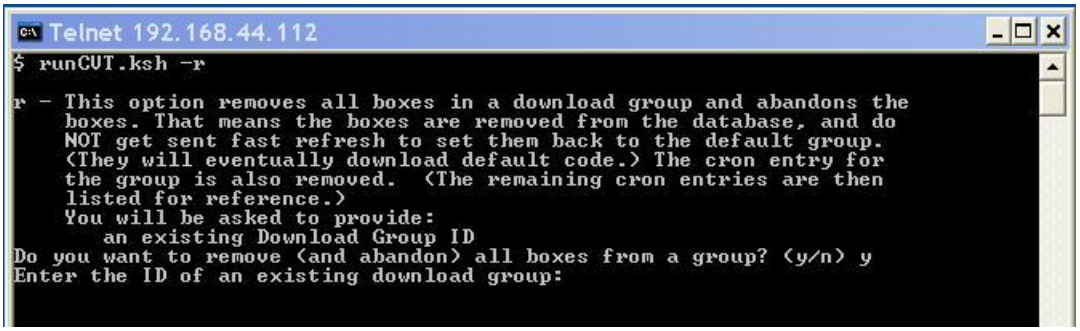
2 Type **runCVT.ksh -r** and then press **Enter**. The system displays a message that describes the actions of the *-r* option, and seeks confirmation of your intent to remove and abandon DHCTs from the download group.

Important: Be sure to read the message thoroughly.

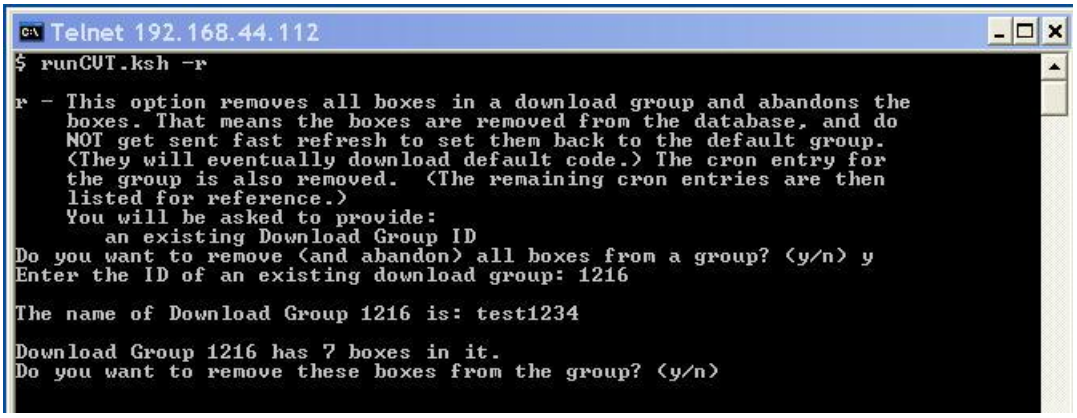


3 Type **y** and then press **Enter**. The message updates to prompt you for the ID

number of the download group.



4 Type the ID number of the appropriate download group and then press **Enter**. The message updates to seek confirmation of your intent to remove the DHCTs from the download group.



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

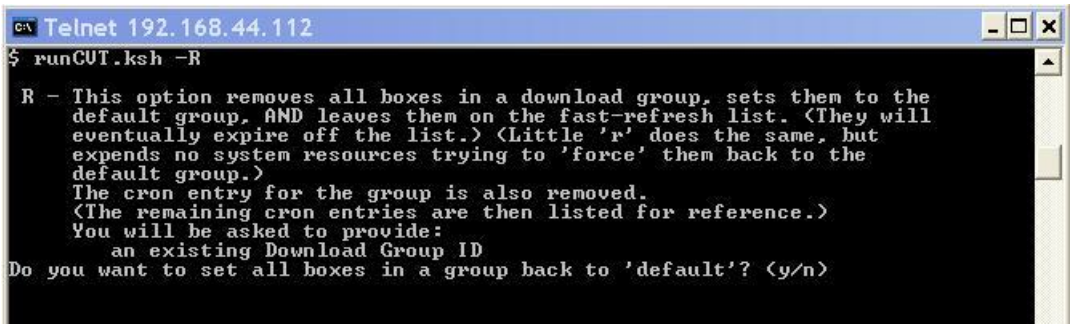
Removing DHCTs from a Download Group and Setting Them to the Default Group

In this procedure, you will use the *-R* option of the runCVT utility to remove all DHCTs from a download group. These DHCTs will then be placed into the default download group and placed on a fast refresh list to download default code.

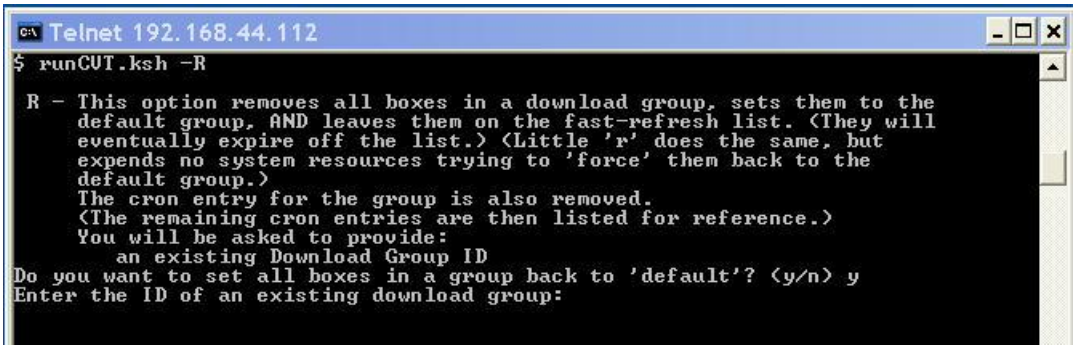
1 If necessary, open an xterm window on the DNCS.

2 Type **runCVT.ksh -R** and then press **Enter**. The system displays a message that describes the actions of the *-R* option, and seeks confirmation of your intent to remove the DHCTs from the download group.

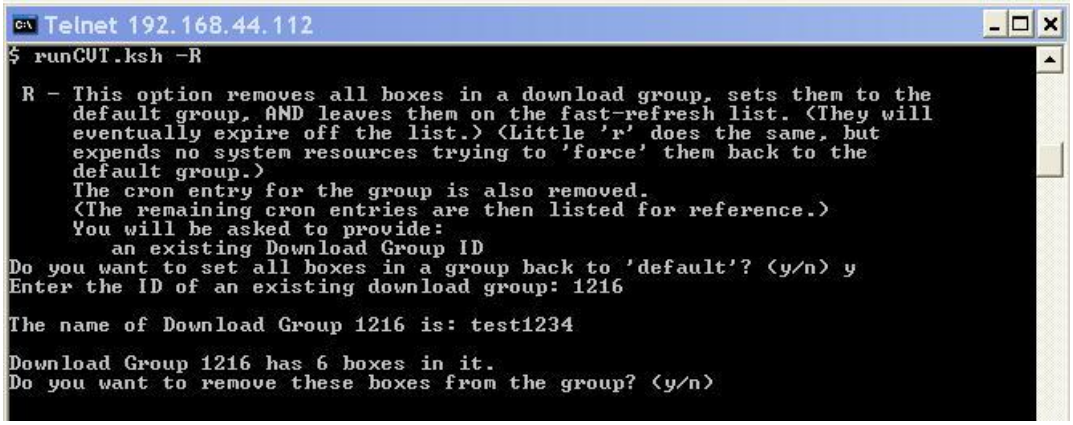
Important: Be sure to read the message thoroughly.



3 Type **y** and then press **Enter**. The message updates to prompt you for the ID number of the download group.



4 Type the ID number of the appropriate download group and then press **Enter**. The message updates to seek confirmation of your intent to remove the DHCTs from the download group.



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

Test a Download Group to See if DHCTs Are Being Fast-Refreshed

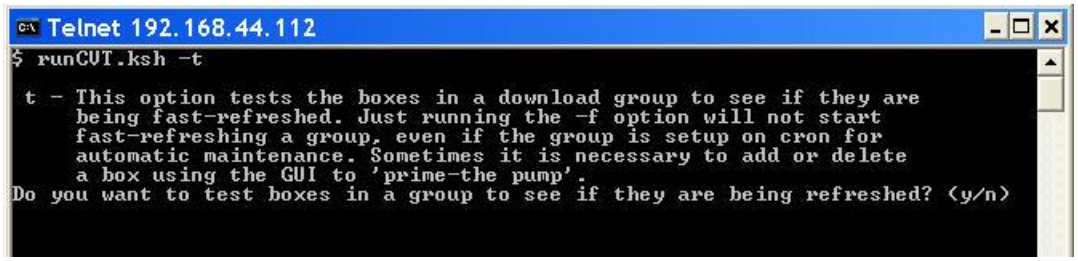
You can use the *-t* option of the runCVT utility to test a download group to see if DHCTs in that group are being fast-refreshed. If the system displays a message that states that DHCTs in a download group are not being fast-refreshed, wait 2 minutes and run the runCVT utility with the *-t* option again.

If, following your second attempt to run the runCVT with the *-t* option, the system still states that DHCTs in a download group are not being fast-refreshed, you will need to add or delete a DHCT to/from the download group using the DNCS GUI to initiate the fast refresh.

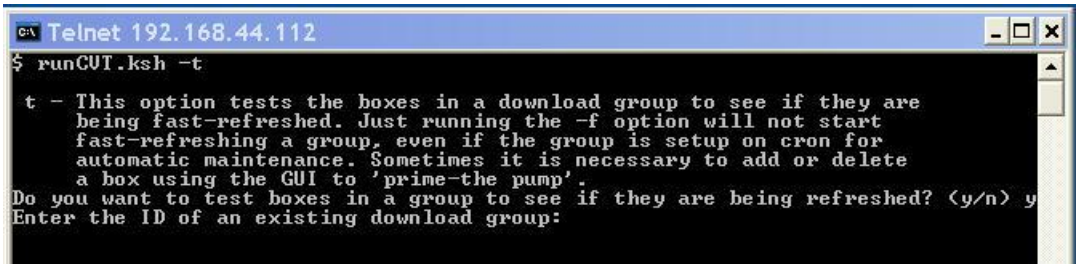
Testing a Download Group to See if DHCTs Are Being Fast-Refreshed

Follow these instructions to use the *-t* option of the runCVT utility to see if DHCTs in a download group are being fast-refreshed.

1. If necessary, open an xterm window on the DNCS.
2. Type **runCVT.ksh -t** and then press **Enter**. A message appears that explains that using the *-f* option of the runCVT utility to start a fast-refresh of a download group will not always work; sometimes DHCTs have to be manually added or deleted from a download group through use of the DNCS GUI. The message then seeks confirmation of your intent to test a download group to see if DHCTs are being fast refreshed.



3. Type **y** and then press **Enter**. The message updates to prompt for the ID of the download group.



4 Type the ID number of the download group, and then press **Enter**. The message updates to either confirm that DHCTs in the download group are on the fast refresh list, or else it prompts you to add or delete a DHCT from the DNCS GUI in order to initiate the fast-refresh action.

16

Synchronize Channel Map, Service Group, and VOD Data with the ncdsGen Utility

Introduction

The Network Configuration Discovery Service (NCDS) server provides a storage location for channel map, service group, and VOD information for your video system. The ncdsGen utility was developed in order to provide a mechanism for synchronizing this data between the NCDS server and the DNCS.

The ncdsGen utility can be configured to either post its collected data to the NCDS, or the NCDS can query the ncdsGen script for the necessary data. The ncdsGen script formats the required data in an XML format.

This chapter provides instructions for running the ncdsGen utility. Running this utility keeps the channel map, service group, and VOD QAM information in sync between the NCDS and the DNCS.

When to Run the ncdsGen Utility

System operators should run the ncdsGen utility whenever they make a change to a channel map or whenever they update VOD information. The ncdsGen utility will propagate and upload the DNCS changes to the NCDS server.

In This Chapter

Run the ncdsGen Utility

The ncdsGen utility uploads the DNCS channel maps and VOD information to the NCDS server.

You can use the following methods to run the utility:

- Push the information from the DNCS to the NCDS server
  Note: The ncdsPush utility, a utility within ncdsGen, triggers ncdsGen to generate the xml files; ncdsPush then transfers those xml files to the appropriate server.
- Poll the DNCS for the information for the NCDS server to fetch
  Note: The ncdsPoll utility, a utility within ncdsGen, is responsible for the polling action.

Pushing the Information to the NCDS Server

To push the information from the DNCS to the NCDS server, complete the following steps.

1 Type the following command to push the information to the NCDS server.

```
./ncdsPush -v http://< ipaddress:port >
```

Note: Use the IP address and port of the NCDS server.

2 To verify that the script has run, look for output similar to the following:

```
./ncdsPush -v http://10.191.11.102:7091
Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-
ControllerAdd.xml
Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-
InputManifest.xml
Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-Input-
CHM.xml
Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-Input-
DSG.xml
Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-Input-
OOB.xml
Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-Input-
VOD.xml
```

Example of ncdsPush in a crontab File

The following instructions show how to use ncdsPush in the crontab file of the DNCS. In this example, ncdsPush is configured to run every weekday at 1:00 am.

1 As dncs user in an xterm window on the DNCS, type **crontab -e** and then press **Enter**. The crontab file opens for editing.

2 Add an entry (on one line), similar to the following, to the crontab file:

```
0 1 * * 1,2,3,4,5 [ -f /dvs/dncs/bin/dncsSetup ] && (.
/dvs/dncs/bin/dncsSetup ;
/dvs/dncs/Utilities/ncdsGen/ncdsPush -v "[URL]" ) >
/dev/null
```

Example:

```
0 1 * * 1,2,3,4,5 [ -f /dvs/dncs/bin/dncsSetup ] && (.
/dvs/dncs/bin/dncsSetup ;
/dvs/dncs/Utilities/ncdsGen/ncdsPush -v
"http://10.252.194.37:7091" ) > /dev/null
```

3 Save and close the crontab file.

Supported Option for the ncdsGen Utility

The ncdsGen and ncdsPush utilities supports the *-i* option. This option allows the user to specify an optional controller ID to be embedded in the ControllerID attribute of the InputManifest.xml file. The controller ID represents the ID of the controller that synchronizes data between the NCDS and the DNCS, and is linked to all of the configuration information gathered from the input manifest file.

Example: The following example illustrates the use of the *-i* option with the ncdsGen utility.

```
ncdsPush  -i  112  -v  http://< ipaddress:port >
```

Note: Use the IP address and port of the NCDS server.

Polling for the Information

To poll the DNCS for the information to be fetched for the NCDS server, complete the following steps.

1 Type the following command to poll the DNCS for the information:

```
./ncdsPoll.cgi
```

2 To verify that the script has run, look for output similar to the following:

```
/dvs/dncs/bin/ncdsGen/htdocs/ncdsPoll
-rw-r--r--   1 dncs     dncs           0 Oct 25 14:09
ncdsGen.out
-rw-r--r--   1 dncs     dncs           0 Oct 25 14:09
ncdsGen.err
-rw-r--r--   1 dncs     dncs        6083 Oct 25 14:09
ncdsGen-Input-CHM.xml
-rw-r--r--   1 dncs     dncs         600 Oct 25 14:09
ncdsGen-Input-DSG.xml
-rw-r--r--   1 dncs     dncs         684 Oct 25 14:09
ncdsGen-Input-OOB.xml
-rw-r--r--   1 dncs     dncs        4245 Oct 25 14:09
ncdsGen-Input-VOD.xml
-rw-r--r--   1 dncs     dncs         714 Oct 25 14:09
ncdsGen-InputManifest.xml
```

3 For instruction on transferring the xml files to the NCDS server, contact TVWorks, the vendor supplying the NCDS server.

17

Monitor DHCT Sign-on Activity with the signonCount Utility

Introduction

When DHCTs download new software for the operating system and resident application, they lose the contents of their volatile memory. After the download, DHCTs sign back on to the network and their network configuration data is reloaded. The signonCount utility is useful in monitoring the rate at which DHCTs sign on to the network.

Because some DHCTs make repeated attempts to sign on to the network before they are successful, too many sign-on attempts by DHCTs contribute to network congestion. The signonCount utility can help system operators quickly identify those DHCTs that are having trouble signing on, and the utility can then be used to facilitate the DHCT sign-on process.

In This Chapter

When to Use the signonCount Utility

The signonCount utility enables system operators and engineers to monitor the rate at which DHCTs sign on to the network. This monitoring is required in the following circumstances:

- When DHCTs download new software-DHCTs lose the contents of their volatile memory when the DHCT downloads new software for the operating system and resident application. DHCTs reconnect to the network after the download, and the memory that contained information about the DHCT network connection (IP address, transmit timing and level) is re-loaded. For systems that are forced to rapidly load DHCT software, the signonCount utility is useful in determining when to trigger the next group of DHCTs to load code.
- When the QPSK modulator and demodulator software is upgraded-In this case, the signonCount utility is used in the following two situations:
  - The first situation is to determine if the system is healthy enough to be upgraded. If it is not, the signonCount utility also provides a secondary mode of operation that can dramatically improve the health of the system prior to moving forward with the upgrade.
  - The second situation is to use the signonCount utility to provide more meaningful guidance regarding when you can move forward with upgrading the next QPSK modulator. Previous upgrade guides instructed you either to wait a little while between upgrading units or to monitor the log file, but they offered no real tools to help in this effort.

Two Modes of Operation

You can run the signonCount utility in two modes: **Fix Mode Off** and **Fix Mode On**.

Both modes help system operators monitor the rate at which DHCTs are trying to sign on to the network. When run in *Fix Mode Off* mode, the utility takes no corrective action regarding DHCTs that are having difficulty signing on. When run in *Fix Mode On* mode, however, the utility reboots those DHCTs that have tried to sign on more than three times during a 10-minute period.

Note: By forcing DHCTs that are having trouble signing on to reboot, the memory in the DHCT is refreshed and the sign-on process is made easier.

Important: By default, the utility runs in Fix Mode Off mode. Because the utility interacts with the database when run in Fix Mode On mode, our engineers recommend that you contact Cisco Services before switching modes.

Review the signonCount Utility Help Window

Before you use the signonCount utility on your system, we recommend that you review the information on the utility's help window. The information on the help window may supplement the information and procedures in this chapter.

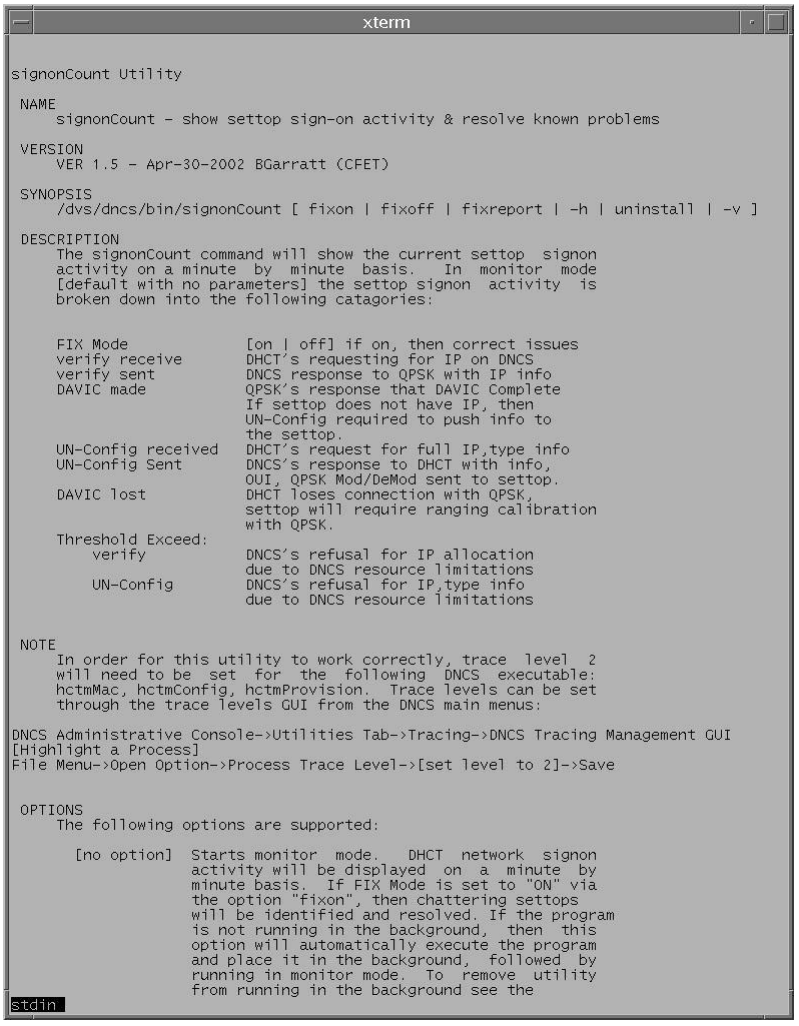
Reviewing the signonCount Utility Help Window

Follow these instructions to review the signonCount utility help window.

1 Open an xterm window on the DNCS and then maximize the window.

Note: The help window for the signonCount utility is large.

2 Type **signonCount -h** and then press **Enter**. The help window for the signonCount utility appears.



3 Press the **Spacebar** as often as necessary to page through the help window.

DNCS Tracing Levels

The signonCount utility's help window indicates that for the utility to operate properly, the tracing levels (also known as logging levels) of three DNCS processes need to be set to a certain level. Refer to ***Set DNCS Tracing or Logging Levels*** (on page 229) for instructions on setting the three DNCS processes to their required tracing or logging levels.

Set DNCS Tracing or Logging Levels

Before you can begin using the signonCount utility, you need to set the tracing or logging levels of three DNCS processes. By setting the tracing or logging levels for these processes, you ensure that the DNCS captures the maximum level of detail for these processes.

Note: The processes are hctmConfig, hctmMac, and hctmProvision.

The procedure you use to set the tracing or logging levels depends upon the version of system software running on the DNCS. Select one of the following options:

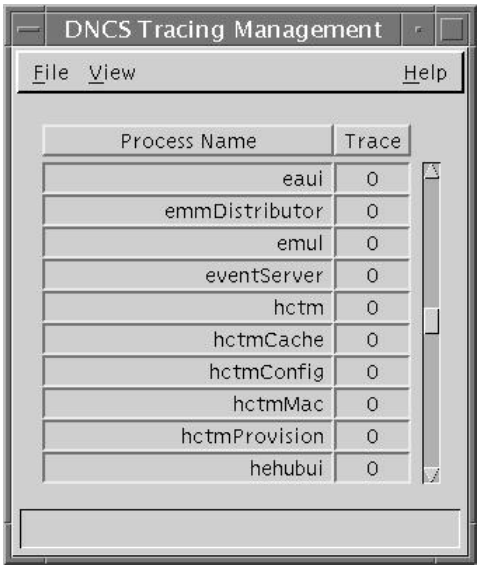
- For system software earlier than SR 4.3, go to ***Setting the DNCS Tracing Levels*** (on page 229).
- For SR 4.3, go to ***Setting the DNCS Logging Levels*** (on page 200).

Setting the DNCS Tracing Levels

Follow these instructions to set the tracing levels of the hctmConfig, hctmMac, and hctmProvision processes to level 2.

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

2 Click **Tracing**. The DNCS Tracing Management window opens.



3 Scroll down until the **hctmConfig**, **hctmMac**, and **hctmProvision** processes come into view.

4 Are the tracing levels for all three of these processes already set to 2?

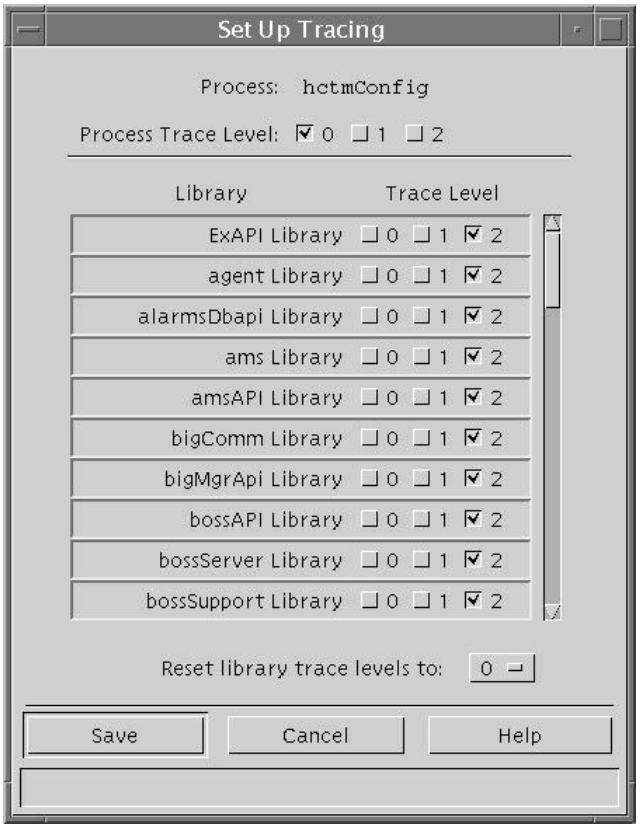
- If **yes**, you have no need to complete the rest of this procedure; continue with *The signonCount Utility Interface* (on page 233).
- If **no**, go to step 5 to begin setting the tracing levels.

Note: The **Trace** column lists the current tracing level.

Example: In the example in step 2, the tracing levels are all set to **0**.

5 Double-click one of the processes. The Set Up Tracing window opens.

Example: Double-click **hctmConfig**.



6 Follow these instructions to configure the Set Up Tracing window.

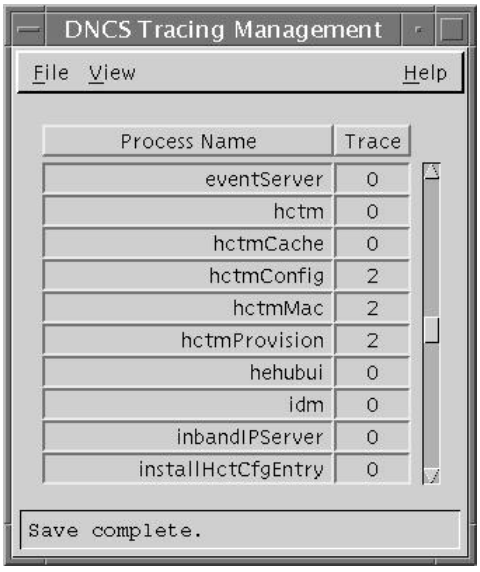
a In the **Process Trace Level** field, select **2**.

b Click **Save**.

Results:

- The DNCS Tracing Management window updates with the new tracing level.
- The Set Up Tracing window closes.

7 Repeat steps 5 and 6 for the **hctmMac** and **hctmProvision** processes (if necessary) to update the tracing level to 2.



Example: When you are finished, the DNCS Tracing Management window should look similar to this example.

Note: The example shows the tracing levels for the hctmConfig, hctmMac, and hctmProvision utilities set to level 2.

8 Click **File** and select **Close** to close the DNCS Tracing Management window.

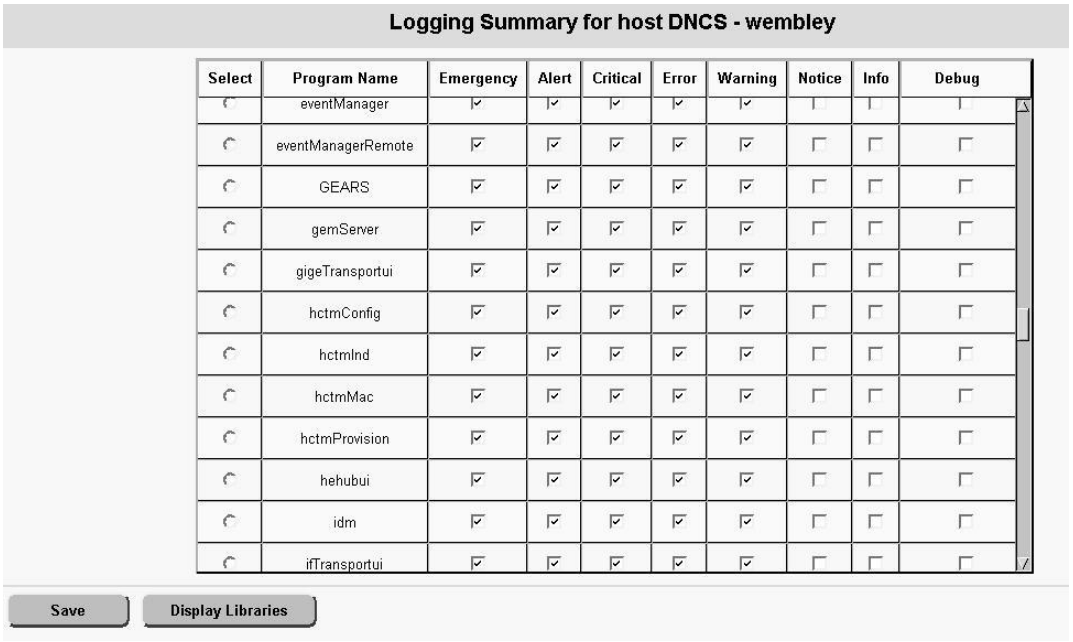
Setting the DNCS Logging Levels

Follow these instructions to set the logging levels of the hctmConfig, hctmMac, and hctmProvision processes.

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

2 Click **Logging**. The Logging Summary for host DNCS window opens.

3 Scroll down until the **hctmConfig**, **hctmMac**, and **hctmProvision** processes come into view.



4 Click to place a check mark in the **Notice**, **Info**, and **Debug** boxes for the **hctmConfig**, **hctmMac**, and **hctmProvision** processes.

5 Click **Save**.

6 Close the Logging Summary for host DNCS window.

The signonCount Utility Interface

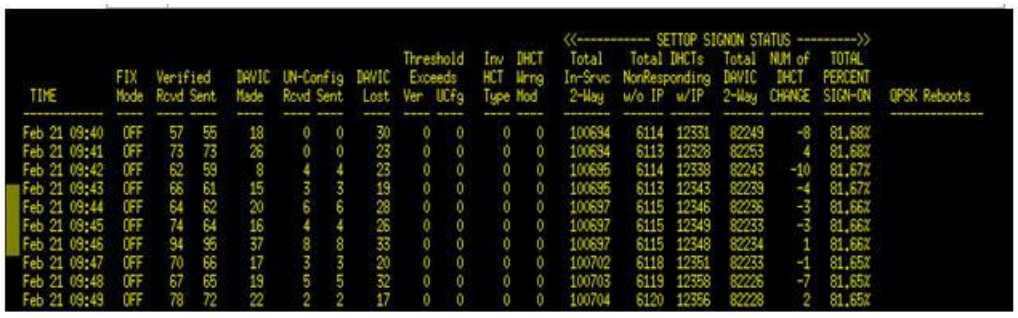
The information in this section provides instructions on how to open the interface of the signonCount utility, as well as providing an explanation of the fields displayed on the interface.

Displaying the signonCount Interface

Follow these steps to display the interface of the signonCount utility.

1. If necessary, open an xterm window on the DNCS.
2. Click and drag the edges of the xterm window to maximize the screen width.

   Note: The signonCount utility fills the width of the screen with data.
3. Type **signonCount** and then press **Enter**. The signonCount utility interface opens.

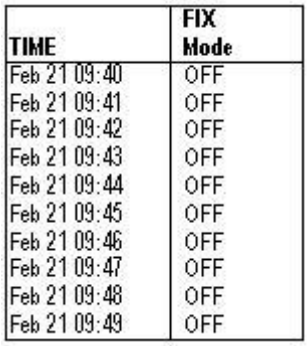
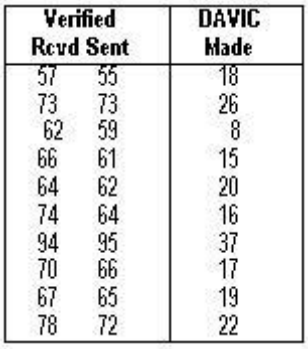


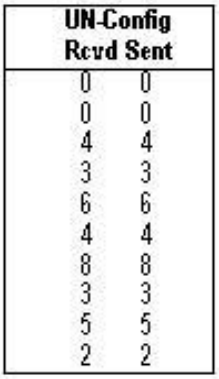
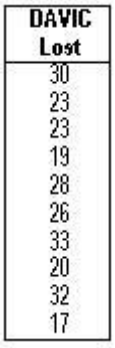
TIME	FIX Mode	Verified Rcvd	Verified Sent	DAVIC Made	UN-Config Rcvd	UN-Config Sent	DAVIC Lost	Threshold Exceeds Ver	Threshold Exceeds UCfg	Inv HCT Type	DHCT Wrng Mod	<<---------- SETTOP SIGNON STATUS ---------->> Total In-Srvc 2-Way	Total DHCTs NonResponding w/o IP	Total DHCTs NonResponding w/IP	Total DAVIC 2-Way	NUM of DHCT CHANGE	TOTAL PERCENT SIGN-ON	QPSK Reboots
Feb 21 09:40	OFF	57	55	18	0	0	30	0	0	0	0	100694	6114	12331	82249	-8	81.68%	
Feb 21 09:41	OFF	73	73	26	0	0	23	0	0	0	0	100694	6113	12328	82253	4	81.68%	
Feb 21 09:42	OFF	62	59	8	4	4	23	0	0	0	0	100695	6114	12338	82243	-10	81.67%	
Feb 21 09:43	OFF	66	61	15	3	3	19	0	0	0	0	100695	6113	12343	82239	-4	81.67%	
Feb 21 09:44	OFF	64	62	20	6	6	28	0	0	0	0	100697	6115	12346	82236	-3	81.66%	
Feb 21 09:45	OFF	74	64	16	4	4	26	0	0	0	0	100697	6115	12349	82233	-3	81.66%	
Feb 21 09:46	OFF	94	95	37	8	8	33	0	0	0	0	100697	6115	12348	82234	1	81.66%	
Feb 21 09:47	OFF	70	66	17	3	3	20	0	0	0	0	100702	6118	12351	82233	-1	81.65%	
Feb 21 09:48	OFF	67	65	19	5	5	32	0	0	0	0	100703	6119	12358	82226	-7	81.65%	
Feb 21 09:49	OFF	78	72	22	2	2	17	0	0	0	0	100704	6120	12356	82228	2	81.65%	

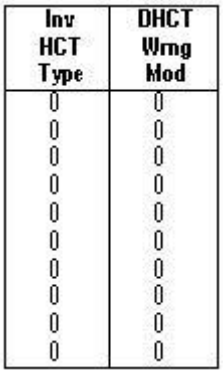
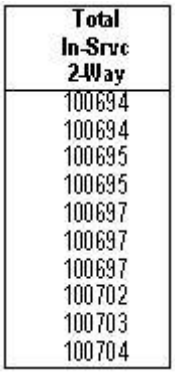
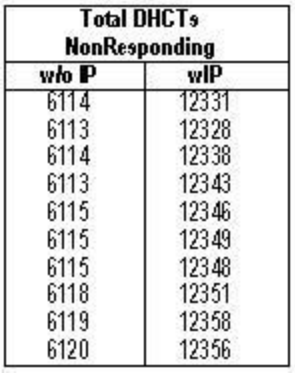
The signonCount Utility Data Fields

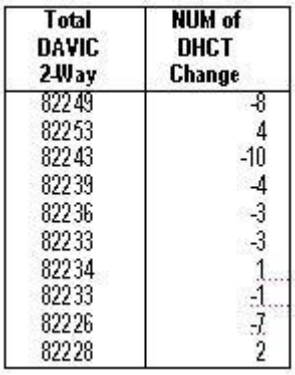
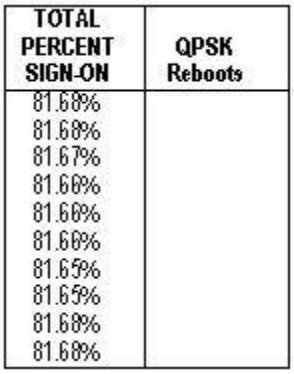
Data Fields

The following tables list the fields included on the interface of the signonCount utility and provide an explanation of the meaning associated with each field.

Columns	Descriptions
 TIME / FIX Mode Feb 21 09:40 OFF Feb 21 09:41 OFF Feb 21 09:42 OFF Feb 21 09:43 OFF Feb 21 09:44 OFF Feb 21 09:45 OFF Feb 21 09:46 OFF Feb 21 09:47 OFF Feb 21 09:48 OFF Feb 21 09:49 OFF	■ **TIME**-The system polls the communication link between the QPSK modulators and the DNCS every minute and records the date and time. ■ **FIX Mode**-This field reveals whether the signonCount utility is configured to automatically correct DHCT sign-on problems (*Fix Mode On*) or whether the utility is running in information-only mode (*Fix Mode Off*). **Note:** By default, the utility runs in Fix Mode Off mode. **Important:** Do not change modes unless you have been instructed to do so by Cisco Services.
 Verified Rcvd / Verified Sent / DAVIC Made 57 55 18 73 73 26 62 59 8 66 61 15 64 62 20 74 64 16 94 95 37 70 66 17 67 65 19 78 72 22	■ **Verified Rcvd**-The QPSK modulator reports the number of DHCTs that have made sign-on requests. ■ **Verified Sent**-The DNCS has allocated this number of DHCT IP addresses based upon the sign-on requests. ■ **DAVIC Made**-The QPSK modulator reports the number of DHCTs that have connected to the QPSK modulator and are waiting for UN-Config information.

Columns	Descriptions
	■ **UN-Config Rcvd**-This number of DHCTs are requesting a UN-Config message from the DNCS. **Note:** The UN-Config message contains information, like an IP address, that allows DHCTs to sign on to the network. ■ **UN-Config Sent**-The DNCS has sent this number of UN-Config messages to DHCTs, allowing the DHCTs to sign on to the network. **Note:** At this point, the DHCTs are physically in two-way mode and have completed the sign-on process.
	■ **DAVIC Lost**-This field indicates the number of DHCTs that have lost the communication link with the QPSK modulator. **Note:** The QPSK modulator then sends a message to DHCTs that have lost the communication link. The message requests that the DHCTs recalibrate themselves with the modulator so the entire sign-on process can begin again.
	■ **Threshold Exceeds Ver**-The DNCS reports the number of DHCTs that simultaneously attempt to verify their configuration in excess of what the system queues allow. ■ **Threshold Exceeds UCfg**-The DNCS reports the number of DHCTs that simultaneously attempt to sign on to the system in excess of what the system queues allow. **Note:** The numbers in the Threshold Exceeds Ver and Threshold Exceeds UCfg columns should theoretically be zero.

Columns	Descriptions
	■ **Inv HCT Type**-This field represents the number of DHCTs in the database with the wrong type, revision, or OUI. ■ **DHCT Wrng Mod**-This field represents the number of DHCTs that have responded through a QPSK modulator that differs from the modulator through which the DHCT responded in the past. **Note:** Numbers in this column typically represent DHCTs that have been moved from one subscriber's home to another without having gone through the correct process.
	■ **Total In-Srvc 2-Way**-The utility reports the number of DHCTs listed in the database with a status of In-Service 2-Way. **Note:** These DHCTs should be capable of two-way communication.
	These fields list the number of DHCTs in the database that should be capable of two-way communication, but they are listed as non-responders. ■ **w/o IP**-This number of non-responding DHCTs do not have an IP address. ■ **wIP**-This number of non-responding DHCTs have an IP address.

Columns	Descriptions
	■ **Total DAVIC 2-Way**-This field represents the number of DHCTs that have physically signed on to the network with two-way communication ability. ■ **NUM of DHCT Change**-This field represents the number of DHCTs with two-way capability that have been added to or removed from the database during the last minute. **Note:** Substantial numbers in the column usually indicate staging activity.
	■ **TOTAL PERCENT SIGN-ON**-The DNCS reports the percentage of DHCTs with two-way capability that are signed on to your network. ■ **QPSK Reboots**-In the event that a QPSK modulator reboots, the name and ID of the modulator is listed in this column.

What to Look For in the signonCount Data

Concentrate on Three Fields

Allow the system to gather signonCount data for several minutes and then examine the numbers in the following fields:

- **Verified Rcvd (Verified Received)**
- **Verified Sent**
- **DAVIC Made**

These fields track the number of sign-on requests made by DHCTs (Verified Rcvd and Verified Sent), as well as the number of sign-on requests that were successful (DAVIC Made). Ideally, the numbers in the three fields should be equal.

If you notice that the numbers in the DAVIC Made column regularly fall more than two or three below the numbers in the Verified Rcvd and Verified Sent columns, your DHCTs may be having trouble signing on and may be contributing to network congestion.

Call Cisco Services

If you notice that the numbers in the DAVIC Made column regularly fall more than two or three below the numbers in the Verified Rcvd and Verified Sent columns, call Cisco Services. Engineers at Cisco Services may log in to your system and examine the logfiles associated with the hctmConfig, hctmMac, and hctmProvision processes. Additionally, they may instruct you to run the signonCount utility in *Fix Mode On* mode.

Important: Do not run the utility in *Fix Mode On* mode unless you have been instructed to do so by Cisco Services.

18

Send Entitlement Permissions with the sendPTEA Utility

Introduction

The sendPTEA utility is used to send entitlement permissions to DHCTs. The sendPTEA utility accepts a formatted text file as an input, and then broadcasts the data in the text file to applicable DHCTs through the PassThruManager process of the DNCS.

In This Chapter

Overview of the sendPTEA Utility

The sendPTEA utility accepts, as its only input, a formatted text file, and then transmits a pass-through, broadcast message to DHCTs by means of the PassThruManager process of the DNCS. The message sent by the sendPTEA utility sets entitlement permissions (permission to run a specific application) for DHCTs. There is no naming convention for the text file; the utility processes only the contents of the file.

Example of the Text File Used by the sendPTEA Utility

The following example is from the readme file that accompanies the sendPTEA utility. This example illustrates how a file to be used with the sendPTEA utility should look.

This example file defines a PTEA message for use with sendPTEA.

!VERSION|3| #Version must be incremented each time this file is changed.

!Global #The First group is always the global group.

DISABLED|C2K|0|

DISABLED|TELN|0| #ENABLED or DISABLED|8 char name|Duration in minutes|

DISABLED|KGDB|0|

DISABLED|GDB|0|

!Group1 #'!' specifies a new group. The name is not read in.

MAC|00:11:22:33:44:55|

MAC|00:18:68:BF:AF:62| #MAC| Network address of a settop|

ENABLED|C2K|1|

ENABLED|TELN|1|

Important Notes About the Text File for the sendPTEA Utility

Note these important points about the text file used by the sendPTEA utility. Refer to the text file in ***Example of the Text File Used by the sendPTEA Utility*** (on page 240) when studying these notes.

- You must increment the version field for each revision of the text file. DHCTs will ignore data in the text file if the file does not contain an updated version number. The version number must be within the 0 to 255 range. Using a version number greater than 255 leads to unpredictable results.
  Example: VERSION|3| #Version must be incremented each time this file is changed.
- DHCTs sometimes fail to retain the data sent by the sendPTEA utility between reboots. Therefore, you may need to transmit a specific version of the data file more than once. DHCTs that have already received that version will ignore it, while DHCTs that have not yet received it will process it.
- An exclamation point (!) declares a group. The entitlement permissions and MAC addresses that follow a group declaration belong to the DHCTs in that group.
- The first group listed in the text file always pertains to the global group, and this group's entitlements are used by all DHCTs.
  Important: The global group *must* be present in any data file used by the sendPTEA utility.
  Example: !Global #The first group is always the global group.
- The actual names of the groups are for the convenience of the operator and are ignored by the utility.
- Declare MAC addresses in the following format:
  MAC|FF:11:22:33:44:55|
  Important: Use capital letters for the higher range of hexadecimal numbers.
- The first field following the declaration of the global group or the list of MAC addresses represents the type of entitlement (enabled or disabled) followed by the name of the entitlement (C2K, TELN, etc.). The last field represents the duration of the entitlement, in minutes.
  Note: A duration of "0" represents no end time.
- Comments are marked by "#". Comments can either begin a line or follow a line, and are ignored by the utility.

Run the sendPTEA Utility

Store the text file that you use for the sendPTEA utility in the /export/home/dncs directory on the DNCS.

Example: Create a directory called PTEA in the /export/home/dncs path (/export/home/dncs/PTEA), and store the text file there.

This example assumes that the text file, stored in the /export/home/dncs/PTEA directory of the DNCS, is called PTEA.msg.

1 From an xterm window on the DNCS, type **cd /dvs/dncs/Utilities** and press **Enter**.

   Important: The sendPTEA utility must always be run from the /dvs/dncs/Utilities directory.

2 Type **sendPTEA.pl /export/home/dncs/PTEA/PTEA.msg** and then press **Enter**. The system runs the sendPTEA utility.

   Result: There are two possible outcomes:

   - If the utility runs successfully, the system displays a hexadecimal dump of the pass-through messages, similar to the following example:

     ```
     PTEA Message
     =>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=>=
     Protocol: 0x11
     Type:     5
     Msg Id:   0x01  (PassThruRequest)
     Tran Id:  1
     Ad Len:   22
     UserId: 2D000000000000000000AFD000100000000000064
     Body Len: 73
     UserId:      2D0000000000000000FFFFFFFF00000000000000
     Msg Type:    0x80BC (unknown)
     Data Length:  49
     Dumping 49 message bytes
         00000000 01 03 01 01 00 00 2A 00 28 02 18 00 02 43 32 4B      ......*.(....C2K
         00000010 20 20 20 20 20 80 01 54 45 4C 4E 20 20 20 20 80      ..TELN    .
         00000020 01 01 10 00 02 00 11 22 33 44 55 00 18 68 BF AF    ......."3DU..h..
         00000030 62                                                 b
     One way, not expecting reply
     ```

     Note: Ignore the *One way, not expecting reply* message; it is a normal part of the output.

- Should the utility fail to run successfully, the system displays a message similar to the following:
  cannot connect to server on 10.253.0.1:13820 using tcp: Connection refused at TestUtil.pm line 80
  Note: The Pass Through process on the DNCS may not be running. Call Cisco Services for assistance, if necessary.

19

Assign the Set-Top Host to a Download Group with the cronCVT Utility

Introduction

The cronCVT utility was developed so that system operators could place the set-top host of a DHCT/embedded CableCARD pair into a download group. This is accomplished by assigning a package to the CableCARD module of the DHCT/CableCARD pair. The package that is assigned to the CableCARD module must already be associated with a download group by means of a configuration file.

The cronCVT utility reads a user-specified configuration file which links a package to a download group. If no configuration file is specified, then the /dvs/dncs/Utilities/croncvt.ini file is used, by default. The configuration file can support up to ten packages and ten download groups when the *-z* option is used.

The S25 feature of the cronCVT utility allows for the transition of CableCARD and legacy STBs to the native iGuide (S25) client.

The cronCVT utility is typically run as a cron entry.

In This Chapter

Display the Help Window of the cronCVT Utility

The Help window is often a good place to start when you are unfamiliar with a utility. To access the Help window of the cronCVT utility, type, from an xterm window, **cronCVT -?** and then press **Enter**. Output similar to the following appears.

```
Usage:
     -c <configfile>  Package to Group Assignment with up to two packages.
                      Add Host to a CVT group per rules specified in the configfile.
        Note: Package to Group Assignment with up to two packages.
        This  switch supports  up to two packages and two CVT group assignments.
        Once it has  been  determined  that  a given CableCard has received PKG1
        or PKG2, the tool  will  assign the  Host that is bound to the CableCard
        to the CVT Group ID GRP1 or GRP2 respectively. Only certain Hardware IDs
        specify  in the  Hardware Id  section  will be  affected.  Once the Host
        assigned to the CVT group GRP1 or GRP2 via package PKG1 or PKG2, removal
        of package PKG1  or PKG2  from  the CableCard  will not  remove the Host
        that is bound to the CableCard from the CVT group GRP1 or GRP2.

     -r <configfile>  Package to Group Assignment with one package.
                      Add Host to a CVT group per rules specified in the configfile.
        Note: Package to Group Assignment with one package.
        This switch supports one  package and  one CVT group assignment. Once it
        has  been  determined that a given CableCard has received PKG1, the tool
        will assign  the  Host that is bound   to the CableCard to the CVT Group
        ID GRP1. Only  certain  Hardware IDs specify  in the Hardware Id Section
        will be affected.  Removal of package PKG1 from  the CableCard will move
        the  Host that is bound to  the CableCard from  CVT group ID GRP1 to the
        Default CVT group.

     -z <configfile>  Package to Group Assignment with multiple packages.
                      Add Host, Embedded STB to a CVT group per rules specified in the configfile.
        Note: Package to Group Assignment with multiple packages.
        This switch supports multiple packages and  multiple  CVT group assignments.
        The tool will  assign  the CableCard  and/or the Host  that is bound  to the
        CableCard  or the  Embedded STB  the  appropriate CVT Group.  Removal of the
        package  from the  CableCard or Embedded STB will NOT move  the CableCard or
        host that is bound to the CableCard or Embedded STB to the Default CVT group.

Example:
Cron entry to schedule cronCVT to run every 5 minutes:
0,5,10,15,20,25,30,35,40,45,50,55 * * * * [ -f /dvs/dncs/bin/dncsSetup ] && (. /dvs/dncs/bin/dncsSetup ; /dvs/dncs/Utilities/cronC
VT -c ) > /dev/null
Note: If the <configfile> is not specified, cronCVT will use /dvs/dncs/Utilities/croncvt.ini
```

Three Options Supported by cronCVT

As the Help window shows, the cronCVT utility supports three options: *-c, -r, and -z*. These options are used to place the CableCARD module or DHCT into specific download groups. The utility links a package with a download group so when that package is assigned to a CableCARD module (through the DNCS or through the billing system), the CableCARD module or DHCT host is placed into the download group.

Note: The *-z* option was developed for Verizon systems; the *-c* and *-r* options pertain mainly to the DBDS.

The -c Option

The *-c* option supports up to two packages and two download group assignments. When a CableCARD module has been assigned PKG1 and/or PKG2, the cronCVT utility assigns the host that is bound to the CableCARD module the group ID GRP1

and/or GRP2.

The *-c* option also supports the S25 Native iGuide stack for existing hardware, and is used for SARA to S25, or S25 to tru2way™ transitions. The configuration file used by the cronCVT utility, when the S25 stack is used, must be dedicated to the S25 stack. Mixed formats are not supported. Hardware IDs are not required in the configuration file when using the S25 Native iGuide stack.

With the *-c* option, removal of the package from the CableCARD module does not change the download group assignment of the CableCARD module or DHCT. Should the user want to place them into a different download group, then the first package must be removed and a second package must be assigned which is associated with a second download group. If both packages are assigned to the CableCARD module, then the CableCARD module or DHCT host is placed into the first download group specified in the configuration file, by default.

The -r Option

The *-r* option supports one package and one download group assignment. When a CableCARD module has been assigned PKG1, the cronCVT utility assigns the host that is bound to the CableCARD module the group ID GRP1.

With the *-r* option, removal of the package from the CableCARD module places the CableCARD module into the default download group.

The -z Option

The *-z* option supports up to ten packages and ten download group assignments. This option was developed for Verizon headends and should be used only by Verizon personnel.

With the *-z* option, if the package is removed from the CableCARD module, the CableCARD module is not removed from the download group. To remove the CableCARD module from the download group, the package not only has to be removed from the module, but another package has to be assigned for it to move to another group. To place the CableCARD module into the default download group, the proper association has to be made in the configuration file similar to the following example:

```
PKG2GRP=<Pkg Name>, 0,0.
```

Group ID 0 always represents the Default group.

The cronCVT Configuration File

Consider the following points about the configuration file used by the cronCVT utility:

- When DBDS Utilities is loaded onto the DNCS, the system automatically places the croncvt.sample.ini file into the /dvs/dncs/Utilities directory of the DNCS. The system operator should then copy this file to croncvt.ini, and then edit the file to suit their system's configuration.
- The croncvt.ini file can be moved to another directory, if desired. However, the path to that directory then needs to be explicitly specified when setting up the crontab file. Likewise, the file can be renamed to suit the system operator, but the new name must be reflected accurately in the crontab file.

Some examples of the croncvt.ini file follow.

croncvt.ini (with -c)

```
#This is a comment
#you may place as many comments in this file as you want.
#the comment line must begin with an #

#

# Package to Group assignment:
# The tool supports two packages and two CVT groups
# assignment. Once it has been determined that a
# given CableCard has received PKG1 or PKG2,
# the tool will assign the Host that is bound to
# the CableCARD to the CVT Group ID GRP1 or GRP2
# respectively. Only certain Hardware IDs specified
# in the Hardware Id Section will be affected.
#

# First Package and CVT group assignment
PKG1=tru2way
GRP1=7779

# Second Package and CVT group assignment
PKG2=SARA
GRP2=1234

# Hardware IDs (Type,Revision)
#HWID=8300,63
```

```
HWID=4300,43
HWID=5000,10
HWID=8300,63
```

croncvt.ini (with -c and the S25 stack)

Important: When using the *-c* option with the S25 stack, be sure to comment out, or delete, references to the hardware ID (HWID) parameters from this file.

```
#This is a comment
#you may place as many comments in this file as you want.
#the comment line must begin with an #

#
# Package to Group assignment:
# The tool supports two packages and two CVT groups
# assignment. Once it has been determined that a
# given CableCARD has received PKG1 or PKG2,
# the tool will assign the Host that is bound to
# the CableCARD to the CVT Group ID GRP1 or GRP2
# respectively.


# When using the S25 option, comment out or
# delete the HWID parameters from this
# config file.

# First Package and CVT group assignment
S25PKG1=S25
S25GRP1=999

# Second Package and CVT group assignment
S25PKG2=Brick
S25GRP2=999
```

croncvt.ini (with -r)

```
#This is a comment
#you may place as many comments in this file as you want.
#the comment line must begin with an #
#
# Package to Group assignment:
# The tool supports two packages and two CVT groups
# assignment. Once it has been determined that a
# given CableCARD has received PKG1 or PKG2,
# the tool will assign the Host that is bound to
# the CableCARD to the CVT Group ID GRP1 or GRP2
# respectively. Only certain Hardware IDs specified
# in the Hardware Id Section will be affected.
#
# First Package and CVT group assignment
PKG1=tru2way
GRP1=7779


# Second Package and CVT group assignment (Not used with -r)
#PKG2=SARA
#GRP2=1234

# Hardware IDs (Type,Revision)
#HWID=8300,63
HWID=4300,43
HWID=5000,10
HWID=8300,63
```

croncvt.ini (with -z)

```
#This is a comment
#you may place as many comments in this file as you want.
#the comment line must begin with an #

#
PKG2GRP=CleanScreen1,1111
PKG2GRP=CleanScreen2,2222
PKG2GRP=CleanScreen3,3333
```

Examples of the cronCVT Utility in the crontab File

This section provides two examples for adding an entry for the cronCVT utility to the crontab file of the DNCS.

Every Minute

To configure the cronCVT utility to run every minute, follow these instructions.

1. As dncs user in an xterm window, type the following command and then press **Enter**.
   ```
   crontab -l > /tmp/dncs.cron
   ```
2. Open the /tmp/dncs.cron file with a text editor.
3. Add an entry (on one line), similar to the following, to the crontab file:
   ```
   * * * * * [ -f /dvs/dncs/bin/dncsSetup ] && (.
   /dvs/dncs/bin/dncsSetup ; /dvs/dncs/Utilities/cronCVT -z )
   > /dev/null
   ```
4. Save and close the file.
5. Type the following command and then press **Enter**.
   ```
   crontab /tmp/dncs.cron
   ```
6. Type `crontab -l` and then press **Enter** to verify that the entry was added successfully.

Every 10 Minutes

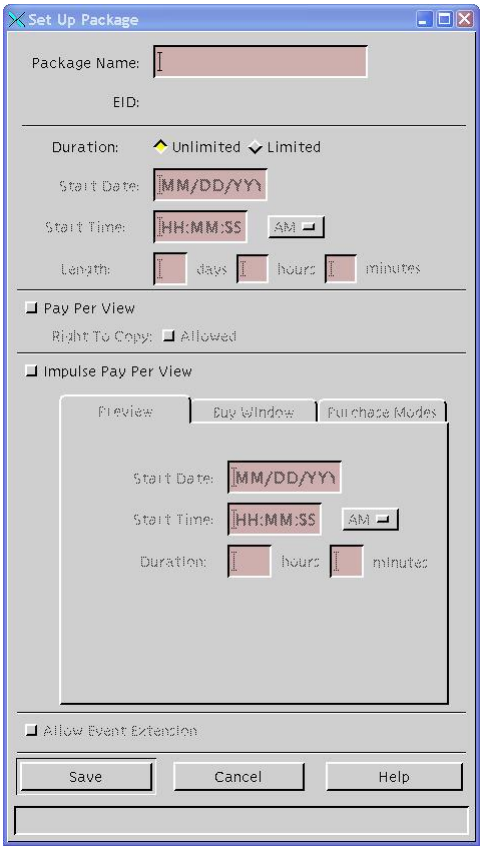
To configure the cronCVT utility to run every 10 minutes, follow these instructions.

1. As dncs user in an xterm window, type the following command and then press **Enter**.
   ```
   crontab -l > /tmp/dncs.cron
   ```
2. Open the /tmp/dncs.cron file with a text editor.
3. Add an entry (on one line), similar to the following, to the crontab file:
   ```
   0,10,20,30,40,50 * * * * [ -f /dvs/dncs/bin/dncsSetup ] &&
   (. /dvs/dncs/bin/dncsSetup ; /dvs/dncs/Utilities/cronCVT -z
   ) > /dev/null
   ```
4. Save and close the file.
5. Type the following command and then press **Enter**.
   ```
   crontab /tmp/dncs.cron
   ```
6. Type `crontab -l` and then press **Enter** to verify that the entry was added successfully.

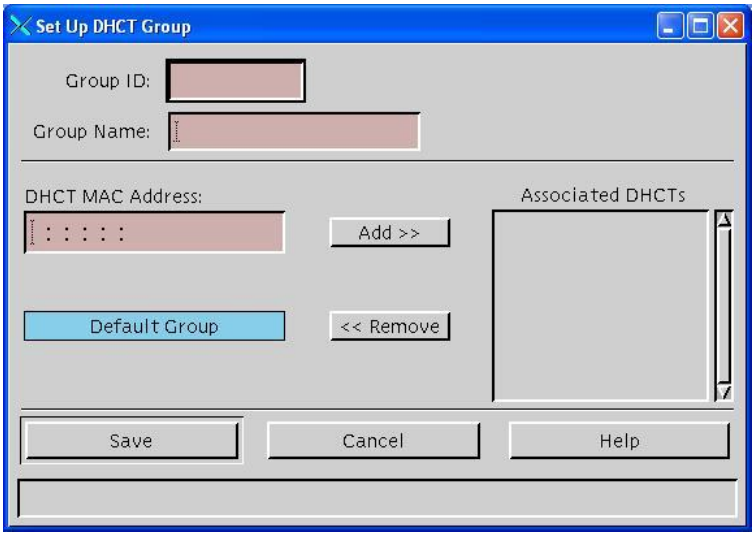
Configure the cronCVT Utility for the DNCS

Follow these general instructions to configure the cronCVT utility to run on the DNCS. These instructions use the *-z* option as an example.

1 Use the Set Up Package window to create a package(s) to use with the cronCVT utility, or you can use an existing package(s).



2 Use the Set Up DHCT Group window to create a group to use with the cronCVT utility, or you can use an existing group.



3 Create a configuration file using the package(s) and CVT download group(s) that you configured in steps 1 and 2. In an xterm window on the DNCS, use a text editor to add entries similar to the following examples to the /dvs/dncs/Utilities/croncvt.ini file:

PKG2GRP=CleanScreen1,1111,9999

PKG2GRP=CleanScreen2,2222,*

PKG2GRP=CleanScreen3,*,3333

Refer to ***The cronCVT Configuration File*** (on page 214) for information regarding the format of the configuration file.

Notes:

- CleanScreen1 is the name of the package, 1111 is the group ID of the download group into which the DHCT's host will be placed, and 9999 is the group ID of the download group into which the DHCT's CableCARD module will be placed.
- CleanScreen2 is the name of the package, 2222 is the group ID of the download group into which the DHCT's host will be placed, and * indicates an empty CableCARD field, meaning the CableCARD module for DHCTs with this package will be left alone with no changes.
- CleanScreen3 is the name of the package, * indicates an empty host field, meaning the host for DHCTs with this package will be left alone with no changes, and 3333 is the group ID of the download group into which the DHCT's CableCARD module will be placed.

Important: The download groups named in this example (1111, 2222, 3333) represent the group ID. They are not the group names.

4 In an xterm window on the DNCS, follow these instructions to add an entry to the crontab file so that the cronCVT utility runs automatically.

a In the dncs role, type the following command and press **Enter**.

```
crontab -l > /tmp/dncs.cron
```

b Open the /tmp/dncs.cron file with a text editor.

c Add an entry similar to the following. The first example configures the cronCVT utility to run every minute, the second example every 10 minutes.

Every Minute

```
* * * * * [ -f /dvs/dncs/bin/dncsSetup ] && (.
/dvs/dncs/bin/dncsSetup ; /dvs/dncs/Utilities/cronCVT -z
) > /dev/null
```

Every 10 Minutes

```
0,10,20,30,40,50 * * * * [ -f /dvs/dncs/bin/dncsSetup ]
&& (. /dvs/dncs/bin/dncsSetup ;
/dvs/dncs/Utilities/cronCVT -z ) > /dev/null
```

d Save and close the file.

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

```
crontab /tmp/dncs.cron
```

5 Type `crontab -l` and press **Enter** to verify that the entry was added successfully.

Add Packages to the CableCARD Module

There are two methods you can use to add a package to the CableCARD module:

- Use the **Secure Services** tab of the Set Up DHCT window to manually add the package.
  Note: To access the Set Up DHCT window, select **Home Element Provisioning** from DNCS Administrative Console. Then, click **DHCT**.
- Use the modDhctCfg utility to add the package.
  Usage: `modDhctCfg +p[Package name] [MAC address]`
  Example: `modDhctCfg +pCleanScreen1 00:02:DE:AA:BB:CC`
  Notes:
  - [Package name] is the name of the package to be added.
  - [MAC address] is the MAC address of the CableCARD module.
  - You can replace [MAC address] with the name of a file containing multiple line-delimited MAC addresses to add the package to multiple CableCARD modules.

Should you need to remove a package from the CableCARD module, use the *-p* option with the modDhctCfg utility.

Example: `modDhctCfg -pCleanScreen1 00:02:DE:AA:BB:CC`

Troubleshooting the cronCVT Utility

Should the host fail to properly download code for the correct group, consider these troubleshooting tips:

- Does the /dvs/dncs/tmp/cronCVT.<yyyymm> file contain any errors?
- Is the correct package assigned to the CableCARD module?
- Is the CableCARD module assigned more than one package for download groups?
  Note: It should have only one package assigned.
- Is the cronCVT utility set up as a cron job correctly?
  - It should be set up for the **dncs** user and not the **root** user.
  - How frequently does the cron execute?
    Note: Recommended values are every 1 to 10 minutes.
  - Does the cronCVT utility specify the use of a specific file?
    Note: If not, the /dvs/dncs/Utilities/croncvt.ini file is used by default.
- Is the croncvt.ini file (or other specified file) configured correctly?
  Notes:
  - Is package 1 and group 1 configured?
  - Is the customer using package 2 and group 2?
  - Are the package names spelled correctly with the correct capitalization?
  - Are the Group IDs correct?
  - Are the Hardware types and revisions correct?
  - Is the Host Hardware ID of the device included in the HWID section of the file?

20

Report CVT Download Group Information with the listCVT Utility

Introduction

The listCVT Utility determines which DHCT models are currently using the Code Version Table (CVT) download method and reports upon unused files on the image list. System operators may find the information generated by the listCVT utility useful because it provides a comprehensive report of all DHCT types, revisions, and associated images without requiring that the user navigate a series of GUI and WUI screens.

Note: CVT is a method for staging DHCTs. The CVT is a table that contains information about download channels, as well as information to map client release software versions to specific DHCT types. The Broadcast File Server (BFS) broadcasts this information once per second on every QAM frequency, as well as on the QPSK frequency. If a DHCT does not have valid client release software installed (such as new DHCTs), the DHCT searches QAM frequencies for software download information. When the DHCT finds this information, it can begin to download valid client release software.

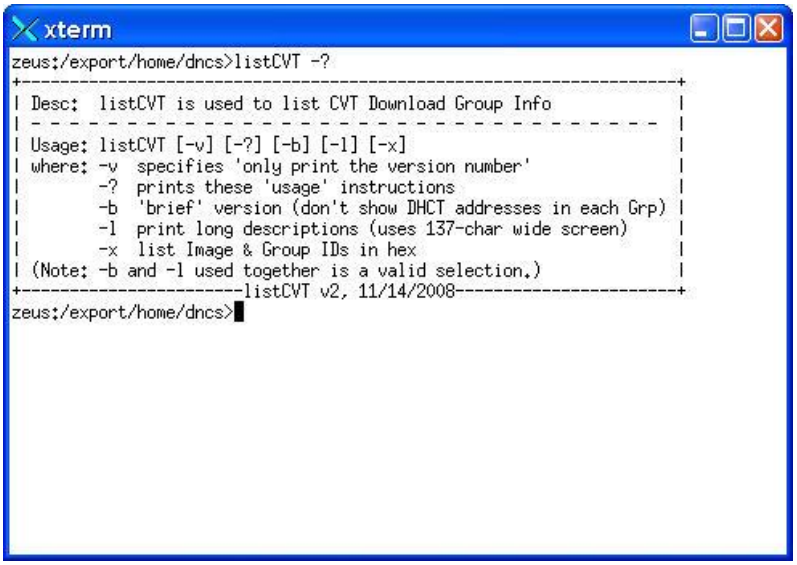
In This Chapter

Display the Help Window for the listCVT Utility

The help window is often a good place to start if you are unfamiliar with a utility. Follow these instructions to display the help window of the listCVT utility.

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

2 Type **listCVT -?** and then press **Enter**. The system displays the valid options for the listCVT utility.



Note: The Help window for the listCVT utility also shows the version of the utility that is loaded onto the DNCS. This example shows that version 2 of the listCVT utility is in use on the DNCS.

Display CVT Download Group Information

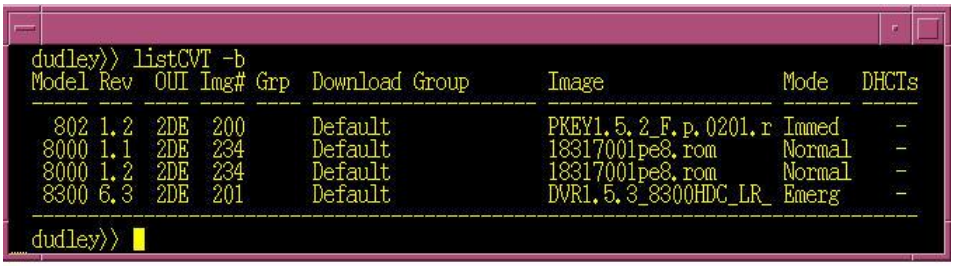
Use the *-b*, *-l*, and *-x* options of the listCVT utility to display information about the system's CVT download groups. The *-b* option displays the data in a brief format. The *-l* option displays longer descriptions. The *-x* option displays image and group IDs in hexadecimal format.

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

2 Choose one of the following options:

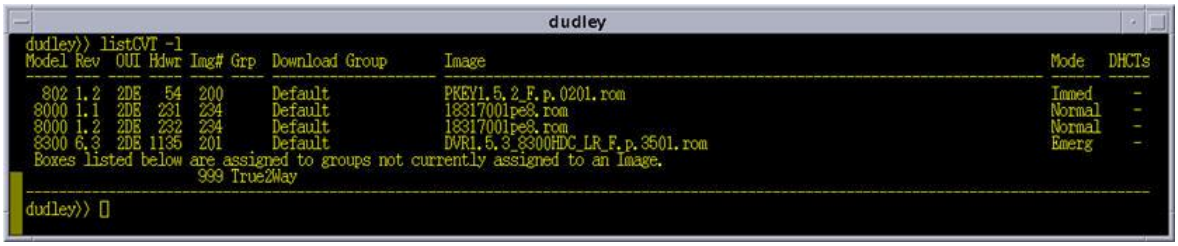
- To display a brief version of CVT download group information, go to step 3.
- To display longer CVT download group descriptions, go to step 4.
- To display image and group IDs in hexadecimal format, go to step 5.

3 To display a brief version of CVT download group information, type **listCVT -b** and then press **Enter**. The system displays CVT download group information in a brief format.



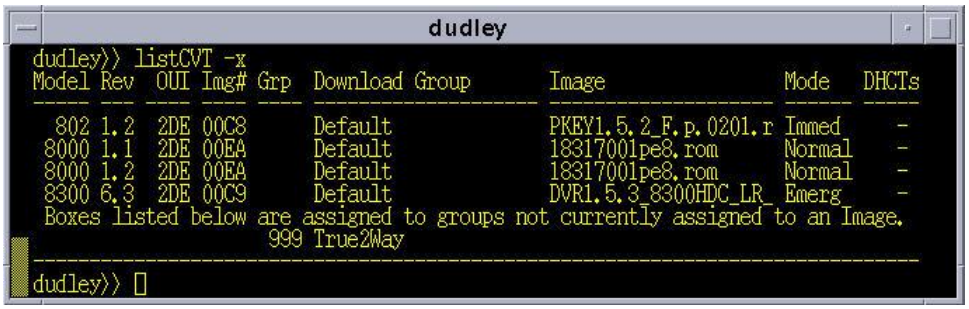
4 To display longer CVT download group descriptions, type **listCVT -l | more** and then press **Enter**.

Note: Pipe the output to the *more* utility so you can review it before it scrolls off the screen. Press the **Spacebar** to scroll through the output.



5 To display image and group IDs in hexadecimal format, type **listCVT -x | more** and then press **Enter**.

Note: Pipe the output to the *more* utility so you can review it before it scrolls off the screen. Press the **Spacebar** to scroll through the output.



21

Display OSM Download Information with the listOSM Utility

Introduction

The listOSM reports on Operating System Manager (OSM) download information.

Note: OSM is a method for staging DHCTs. Under the OSM method, the DHCT receives System Information (SI) and a type-specific user-to-network configuration (UN-Config) message, which includes a table of contents (TOC) file, from the DNCS. The DHCT reads the contents of the TOC file and compares the checksums of the currently loaded image files against the file information in the TOC file.

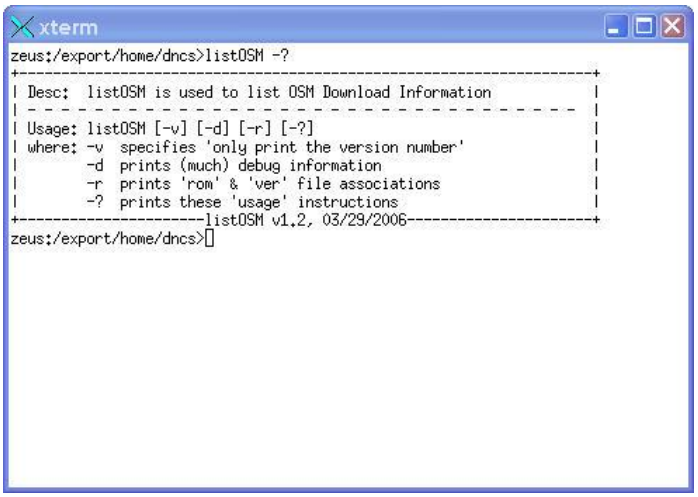
In This Chapter

Display the Help Window for the listOSM Utility

The help window is often a good place to start if you are unfamiliar with a utility. Follow these instructions to display the help window of the listOSM utility.

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

2 Type **listOSM -?** and then press **Enter**. The system displays the valid options for the listOSM utility.



Note: The Help window also displays the version number of the listOSM utility. This example shows that version 1.2 of the listOSM utility is loaded onto the DNCS.

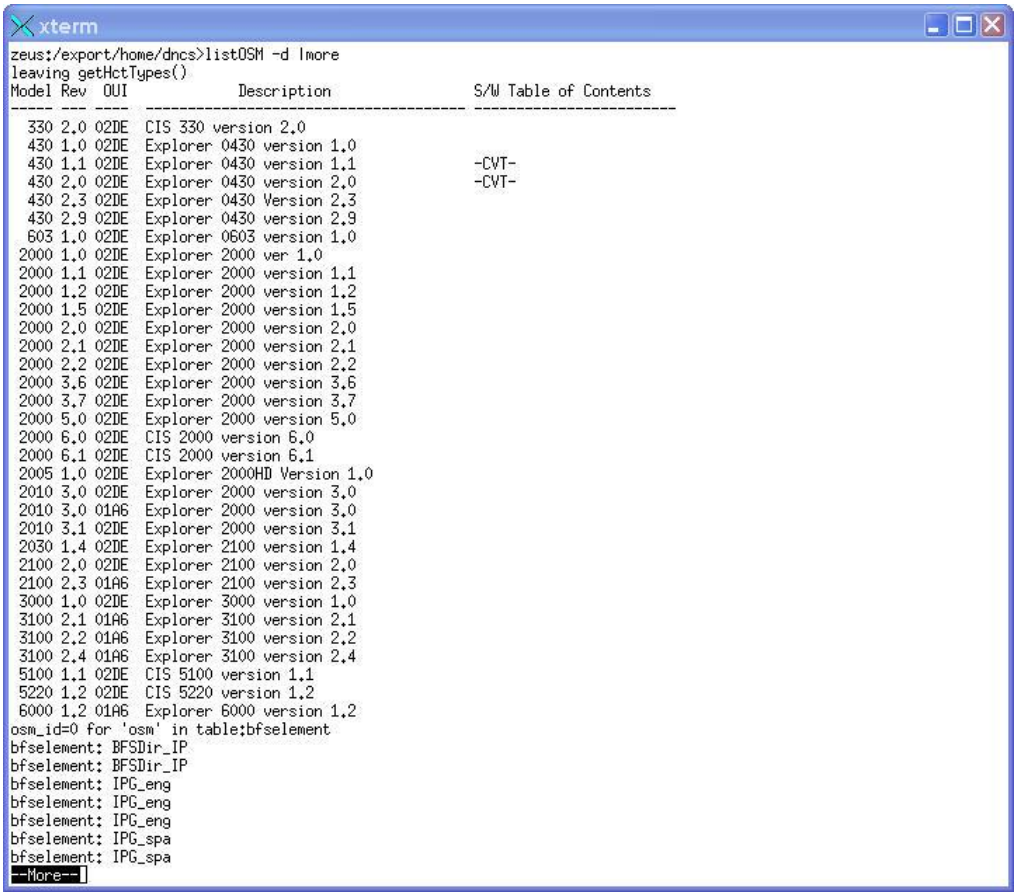
Display OSM Debug Information

The *-d* option of the listOSM utility displays debug information associated with the OSM download method. Because the output can be quite lengthy, pipe it to the *more* utility so that the output does not scroll off of the screen.

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

2 Type **listOSM -d | more** and then press **Enter**. The system displays debug information for the OSM download method.

Note: Press the **Spacebar** to scroll through the output.



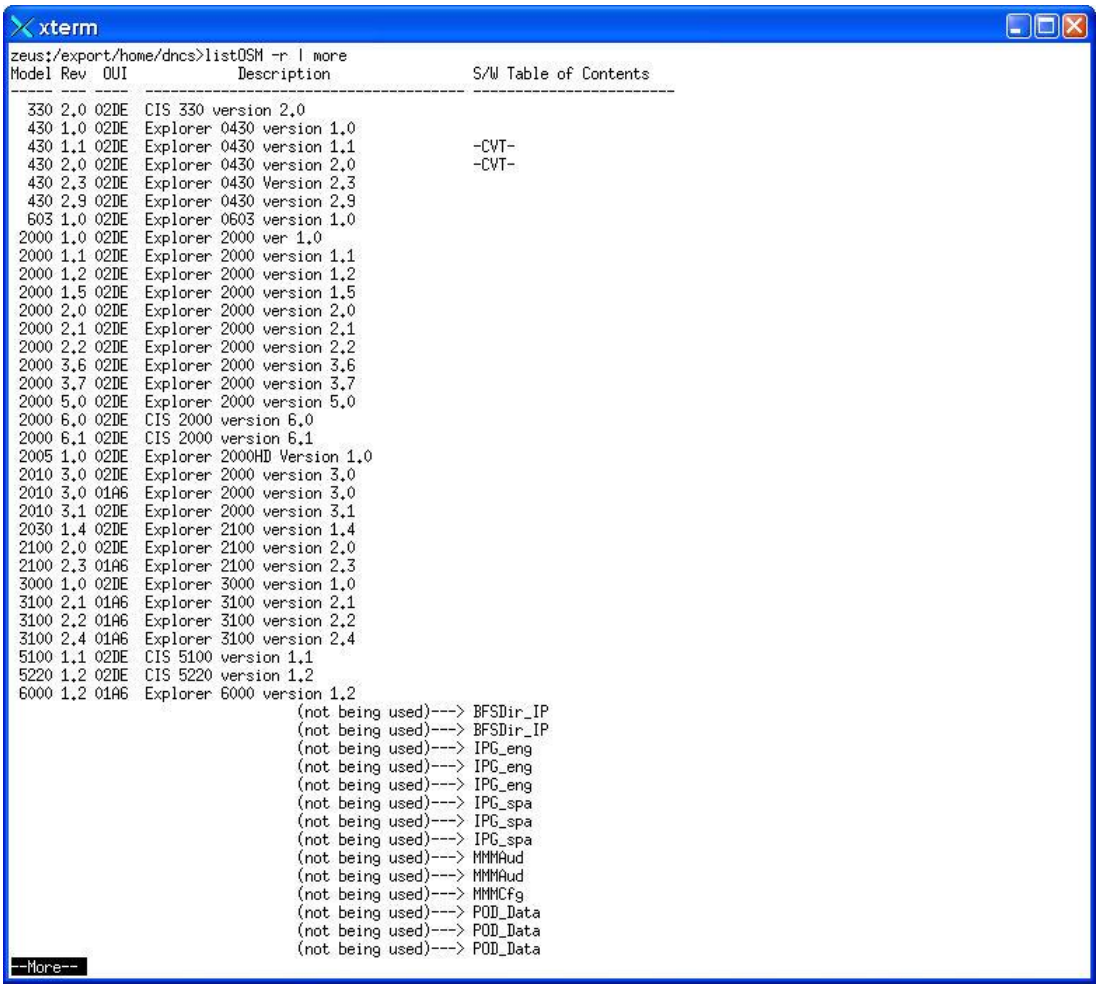
Display *.rom and *.ver File Associations

The *-r* option of the listOSM utility displays the *.rom and *.ver file associations used with the OSM download method. Because the output can be quite lengthy, pipe it to the *more* utility so that the output does not scroll off of the screen.

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

2 Type **listOSM -r | more** and then press **Enter**. The system displays the *.rom and *.ver file associations used with the OSM download method.

Note: Press the **Spacebar** to scroll through the output.



22

Display Data About QAM Devices with the listQam Utility

Introduction

System operators can use the listQam utility to obtain an overview of the QAM devices on the DNCS, especially with respect to service group and Switched Digital Video (SDV) configuration.

In This Chapter

Run the listQam Utility

The listQam utility provides an overview of the configuration of the QAM devices on a system. The output shows the basic parameters for each port, and indicates whether the port is associated with a service group or is enabled for SDV. System operators can use the utility to troubleshoot VOD or SDV issues.

Follow these instructions to run the listQam utility.

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

2 Type **listQam** and then press **Enter**. Output similar to the following appears:

```
scooby:/export/home/dncs$ listQam
QAM_NAME              TYPE                IP   STATUS | FREQ PORT    TSID SRVC_MODE  OUTPUT     |    SGID GNAME         SDV_ENABLED
-----------------------------------------------------+-------------------------------------------+-----------------------------------
BFSQam               CAQAM       172.16.4.100   ONLINE |  603    2      27 BCST       ENABLED    |
EmulGQAM02            GQAM         172.29.0.2   ONLINE |  615    1   20021 SHARED     ENABLED    |
EmulGQAM02            GQAM         172.29.0.2   ONLINE |  621    2   20022 SHARED     ENABLED    |
EmulGQAM02            GQAM         172.29.0.2   ONLINE |  627    3   20023 SHARED     ENABLED    |
EmulGQAM02            GQAM         172.29.0.2   ONLINE |  633    4   20024 SHARED     ENABLED    |
EmulGQAM02            GQAM         172.29.0.2   ONLINE |  615    5   40021 SHARED     ENABLED    |
EmulGQAM02            GQAM         172.29.0.2   ONLINE |  621    6   40022 SHARED     ENABLED    |
EmulGQAM02            GQAM         172.29.0.2   ONLINE |  627    7   40023 SHARED     ENABLED    |
EmulGQAM02            GQAM         172.29.0.2   ONLINE |  633    8   40024 SHARED     ENABLED    |
EmulGQAM03            GQAM         172.29.0.3   ONLINE |  700    1   30011 SHARED     ENABLED    |    9090 EmulVOD               YES
EmulGQAM03            GQAM         172.29.0.3   ONLINE |  706    2   30012 SHARED     ENABLED    |    9090 EmulVOD               YES
```

23

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 4031374 Rev B