DBDS Utilities Version 8.1.5

User Guide and Release Notes

Please Read

Important

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

Notices

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.

Documentation Copyright Notice

Information in this document is subject to change without notice. No part of this document may be reproduced in any form without the express written permission of Cisco Systems, Inc.

Copyright

Contents

About This Guide

Purpose

The EC Utilities packages contain utility programs that you can use to manage and troubleshoot Cisco's Digital Broadband Delivery System (DBDS). This guide contains instructions to operate the various software utilities contained in the EC utilities packages.

Scope

The utilities described in this guide pertain to systems running System Release (SR) 9.0.

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.

Document Version

This is the first formal release of this document.

Read These Important Recommendations About the EC Utilities

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

- Many of the utilities described in this guide interact with the Explorer Controller (EC) database. Make sure that you have a current database backup before running any of the utilities described in this guide. Refer to the ***Backup and Restore User Guide for EC 9.0 and DTACS 5.2*** for instructions on how to back up the database.
- We strongly recommend that you run the Doctor Report at least once a day. Instructions for running the Doctor Report are in Analyze System Configuration With the Doctor Report.
- We strongly recommend that you run the checkDB script at least once a month. Instructions for running the checkDB script are in ***Identify and Correct Database Problems With the checkDB Script*** (on page 31).

Accessing the root and dncs User Accounts

Important:

- Role-Based Access Control (RBAC) is not supported in SR 9.0. Please follow the steps below to switch between different user accounts.
- The **ecadmin** user is used in examples for all Cisco DBDS documents pertaining to EC 8.0 or later.
- Commands run as **root** user are shown with a **#** symbol.

  Example:

  ```
  [root@ecnextx9 ~]#
  ```

- Commands run as an **admin**, **dncs**, or any **Administrator** user are shown with a **$** symbol.

  Example:

  ```
  [admin@ecnextx9 ~]$
  [ecadmin@ecnextx9 ~]$
  [dncs@ecnextx9 ~]$
  ```

Once the EC application installation is complete, you can only log in with the **admin** user account.

The ***admin*** account is created by default during the installation, and is granted privileges to access the root user account, as root login is not permitted. These privileges allow the admin user to execute root commands by preceding the command with "sudo". For example, if you want to modify a network configuration file, the command will resemble the following:

Example: Executing a root command as admin user:

```
[admin@ecnextx9 ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens192
```

As **admin** user, you can also change to the root user account by entering the following command.

Important: For any procedure in this guide that states "As root user", you must be logged into a terminal window as admin user and switch to the root user.

Command Syntax: Changing to root user:

```
[admin@ecnextx9 ~]$ sudo –i
```

Any ***Administrator*** account that you create using the useradmin script (see the next section) has privileges to log into the EC from a terminal window. Administrator accounts do not have privileges to access the root user account, but should be used to access the dncs user account.

Important: Do not access the dncs user account using the root user account.

To switch to the **dncs** user, type the following command from the terminal window where you are logged in as an Administrative user.

Important: For any procedure that states "As dncs user", you need to execute this command from the terminal window where you are logged in with your Administrator account.

Command Syntax: Changing to the dncs user:

```
[ecadmin@ecnextx9 ~]$ sudo su – dncs
```

Note: Throughout all Cisco DBDS documentation, the **ecadmin** user is used as an example for SR 8.0 systems or later.

Overview:

Terminal Window Logged in as:	Use Account to change to:	Command to execute:
admin	root	sudo -i
[Administrator] **Example:** ecadmin	dncs	sudo su - dncs

1

Release Note

Introduction

The EC Utilities include a series of utility programs that you can use to manage and troubleshoot the Digital Broadband Delivery System (DBDS).

This document lists and describes the implemented bug reports (BRs) associated with this version of the EC Utilities.

See the ***Overview of EC Utilities*** (on page 2) for a brief description of the utilities that comprise this version of the EC Utilities.

This release note is written for system operators of the DBDS who deploy EC Utilities on the sites that they manage. Field service and support engineers who help system operators manage their sites may also find the information in this document useful.

In This Chapter

Introducing Explorer Controller Utilities

This section includes a list of the system releases with which the EC Utilities is compatible, and provides a short description of the utilities that make up EC Utilities.

System Release Compatibility

This version of the EC Utilities (CSCOecutils 8.1.5) is compatible with SR 9.0.

The EC Utilities consists of these software packages:

- CSCOec-utilities (version 9.0.12)
- CSCOecutils (version 8.1.5)

Overview of EC Utilities

The following list contains the utility programs that comprise this version of the EC Utilities. See the details of each utility later in this document for a detailed description of each utility, as well as instructions on how to run each utility.

- ***bfsInfo.ksh*** — Generates the BFS summary report that details the files and file sizes in each BFS carousel.
- ***chanlineupinfo*** — Generates a list of channel lineups.
- ***checkDB.sh*** — Identifies and corrects DHCT records in the database that do not contain serial numbers, required corresponding records in other tables, or that have Entitlement Management Messages (EMMs) ready to expire.
- ***checkdbinfo.sh*** — Allows you to find the type of database (primary, secondary, or standard), and if database replication is on or off.
- ***chkSamUrl*** — Deletes unused SAM URLs from the EC, thereby reducing the size of the bulk.tbl file.
- ***convertIP*** — Converts an IP address from dotted-decimal notation to decimal format and vice versa.
- ***cvtChecker*** — Logs into all the specified devices and reports back the CVT version found on the devices.
- ***dhctStatus*** — Monitors two-way communications between DHCTs and the headend.
- ***doctor*** — Compiles a report on system configuration.
- ***getCCdata.ksh*** — Reports on CableCARD™-related errors and data.
- ***getEASdata.ksh*** — Troubleshoots the DBDS Emergency Alert System (EAS).

- ***listTftpConfigs.ksh*** — Lists configuration data for DBDS devices.
- ***mvsrcid.sh*** — Converts EC source IDs to TV Guide source IDs.

  Note: You must run mvsrcid.sh as **root** user.
- ***ncdsGen*** — Helps synchronize channel maps, service groups, and VOD data.
- ***nonsaradupqha.sh*** — Replicates an existing SARA QAM ports-to-Hub association to a NEW association between the same SARA QAM ports and a NEW NON-SARA hub.

  Note: You must run nonsaradupqha.sh as **root** user.
- ***podDataChk*** — Allows for the examination of the podData file
- ***qtail*—** Uses the Linux *tail* utility to monitor log files of EC processes in real time. When the limit of a specfic log file is reached, the qtail utility automatically starts monitoring the new log file.
- ***runCVTGroup*** — Provides a mechanism for managing download groups.
- ***sesstail*** — Similar to qtail, but monitors the dsm process log files video-on-demand (VOD) session-related activities).
- ***setDbOptCron*** — Allows you to configure the dbOptimizer utility to delete old EMMs based upon selectable options.
- ***setuptail*** — Tracks session setup successes, failures, and error types.
- ***signonCount*** — Monitors DHCT sign-on activity.

Bug Search Tool

The Bug Search Tool is an online tool that allows registered users to search for bugs by release or by a bug number.

To log on to the Bug Search Tool, go to **https://tools.cisco.com/bugsearch** and log on with your user name and password. The Bug Search Tool page opens.

Note: If you have not set up an account on www.cisco.com, click **Register Now** and follow the on-screen instructions to register.

Search for Bugs in This Release

1. From the **Product** dropdown list box, select **Series/Model**.
2. In the adjacent text box, type **DBDS Utilities**. Then choose DBDS Utilities from the list that appears. (Do not press Enter.)
3. In the **Releases** field, type the value for the release, (for example, 9.0) and press **Enter**. The Bug Search Tool displays the list of bugs for this release. You can use the filters to restrict the bugs that you want to view.
4. If you want to view a specific bug, enter the ID of the bug that you want to view in the **Search For** field and press **Enter**.

2

Analyze System Configuration with the Doctor Report

Introduction

The Doctor utility (commonly referred to as the Doctor Report) is one of the most important tools you can use to evaluate the configuration and operation of the EC.

Output from the Doctor Report appears on the screen of the EC 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
- EC disk partition utilization
- Status of EC 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
- Common configuration errors that may lead to problems later

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

In This Chapter

Specify the Output Directory

Specify the DOC_OUTPUT_DIR Parameter

Note: When the DOC_OUTPUT_DIR environment variable is not defined, the Doctor Report output is written to the default path, /dvs/dncs/Utilities/doctor. To customize the Doctor Report path, the ENV DOC_OUTPUT_DIR variable needs to be defined in the .profile file for command line execution, as well as in the dncsSetup file for crontab execution.

Important: You will need to complete this procedure once. There is no need to perform this procedure each time you run the Doctor Report. However, you will need to repeat this procedure should you ever change the output directory of the Doctor Report.

The examples that follow describe how to direct Doctor Report output to the /home/dncs directory.

The .profile File

1. As the **root** user, open the dncs user's **.profile** file with a text editor.
2. Add the following entry to the **.profile** file:
   ```
   export DOC_OUTPUT_DIR=/home/dncs
   ```
3. Save and close the file.
4. As **dncs** user, activate the change by bouncing the **.profile** file.
   ```
   [dncs@ecnextx9 ~]$ . .profile
   ```

The dncsSetup File

1. As **root** user, open the **/dvs/dncs/bin/dncsSetup** file in a text editor.
2. Add the following entry to the **dncsSetup** file:
   ```
   export DOC_OUTPUT_DIR=/home/dncs
   ```
3. Save and close the file.
4. Activate the change by sourcing the **dncsSetup** file.
   ```
   [root@ecnextx9 ~]# . /dvs/dncs/bin/dncsSetup
   ```

Run the Doctor Report

Running the Doctor Report

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

1 As **dncs** user, type the following command and press **Enter**. The system generates a list of parameters that you can use to run the Doctor Report.

```
[dncs@ecnextx9 ~]$ doctor -h
```

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

2 To generate a complete Doctor Report, type the following command and press **Enter**.

```
[dncs@ecnextx9 ~]$ doctor -av
```

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 based upon an environment variable (DOC_OUTPUT_DIR =) set in the .profile file.

Example: The system saves the report with a name similar to `report_26224.180905_1145.doc`, where `26224` refers to the PID.

Notes:

- Depending upon the size of your system and/or the communication states of various network elements, 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.

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 accompanied 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 you 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:

- Contact Cisco Services whenever an unexpected or new error appears in the Doctor Report output or if defined thresholds are about to be reached.
- 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 Non-Cisco Application Server Sites

Due to their unique implementation, sites that use a non-Cisco Application Server may see application server-related errors in their Doctor Report.

Ignore these errors; these errors are normal for these sites. The fields in the Doctor Report that are affected by non-Cisco Application Servers are noted in this section by the words **No Cisco application server**.

System Name

The System Name field appears at the top of the Doctor Report. This field identifies the system by its hostname and displays the operational mode of the system.

All CSCO Installed Package Information

The data in the **All CSCO 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

No Cisco application server: Ignore any application server-related errors at these sites.

EC Info

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

EC Uptime

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

Note: To determine how long the EC 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 EC processes are reset.

Linux Uptime

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

Processor Sockets

The data in the Processor Sockets field contains the model and version for each CPU processor, including its location tag within the virtual server.

Disk Info

The Disk Info field displays configuration information for the server from a virtual disk point of reference.

EC Disk Partition Utilization

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

Important: We 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.

Basic System Performance Stats

There are five 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 top utility to examine the top 30 active processes on the system.

As used in the Doctor Report (`top -b -n1 | head -n 30`), the output of the top command is sorted according to CPU and the head utility prints the top 30 entries.

Memory Usage

The Memory Usage field uses the free utility to examine the free and used memory on the EC.

As used in the Doctor Report (`free -h`), the free utility displays the total amount of free and used physical and swap memory in the system, as well as the buffers and caches used by the kernel.

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.

All values in the output are rates listed as percentages, unless specifically noted.

As used in the Doctor Report (`mpstat -P ALL 5 5`), the mpstat utility collects processor statistics in five-second intervals and produces five reports.

Virtual Memory Stats

The Virtual Memory Stats field uses the vmstat utility to report information about processes, memory, paging, block IO, traps, and CPU activity.

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

Disk Stats

The Disk Stats field uses the iostat utility to iteratively examine statistics and input/output statistics for devices, partitions, and network file systems.

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 -xmz -p 5 5), the utility produces extended statistics and displays names in per-partition format and in per-device format. Data is displayed in MB/second terms. The utility collects statistics every five seconds and issues five separate reports.

Database Tablespace Report

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

- **Database Summary** — Provides information and usage per database installed in Informix.
- **Dbspace Summary** — Provides usage information for each database space installed in Informix.

  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.
- **Extent Summary** — provides information on database tables that have more than 30 extents, and of those that it reports on, only shows those with a next extent size larger than 500MB.

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 Backup Check

This field reports on the presence of a backup that was initialized by a cron job to automatically back up the EC 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 backs up the database and keyfiles is a shell script called DBKF.cron.sh. It is located in the /opt/cisco/backup directory. If desired, you can set up a cronjob to configure your system for automated database and key files backups.

Check for clearDbSessions Activity

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

EC Load Average

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

Important: We recommend that your EC load average remain under 2.0.

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

AppServ Logging Levels at DEBUG or higher

The Application Server allows you to configure the level of detail reported by various system processes. The data in the Appserv Logging Levels at DEBUG or higher field lists all Application Server logging levels that are loglevel debug or higher.

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.

EC Logging Levels at DEBUG or higher

The EC Logging Levels at Debug or higher field lists all EC processes and the level of logging activity that is associated with each process, at logging levels of DEBUG or higher.

System operators can set logging levels for the EC processes by clicking the **Navigation** icon,  , and then selecting **Utilities > Logging** from the Explorer Controller Administrative Console.

EC Processes

The data in the EC Processes field lists all the EC 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 **Info**

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

- Check the EC for core files.

  Note: The ***Recent EC Corefiles (last 2 days)*** (on page 15) field lists recent EC core files.

- If the EC 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.

No Cisco application server: Ignore any application server-related errors at these sites.

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 send the core file to them for analysis.

Use the **appControl** utility to restart the stopped process(s).

Recent EC Corefiles (last 2 days)

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

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

Important: Call Cisco Services if the Recent EC Corefiles (last 2 days) section lists any core files. Cisco Services may request that you send the core file 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.

No Cisco application server: Ignore any application server-related errors at these sites.

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 send the core file to them for analysis.

DNS Check

The data in the DNS Check field reports whether the Domain Name Service (DNS) is running on the EC.

- The system lists **OK** when the DNS is not running
- The system lists **Info** when the DNS is running

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.

- If a SARA Application Server exists on the system and has a valid SAM service ID, the message **OK: All force tune service ids are valid SAM services** displays. Otherwise, an error message displays.
- If a SARA Application Server does not exist on the system and if a non-SAM service EAS force-tune is not enabled, the **CISCO App Server not installed or**

not available message displays.

- If a SARA Application Server does not exist on the system and if a non-SAM service EAS force-tune is enabled, then the force-tune source ID is validated. If it is valid, the message **OK: All force tune ids are valid** displays. Otherwise, an error message displays.

EC License Check

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

- EAS FIPS Code Filtering
- DOCSIS DHCT Support
- Enhanced VOD Session Throughput
- VOD Session Encryption
- Distributed DNCS
- Open Cable Applications Platform (OCAP)

Note: 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.

If the bulk.tbl file grows too large, DHCTs may reboot and display a black screen.

EC File Size Check

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

If all files are under 50 MB, the following message appears:

```
OK: All files under 50M.
```

Last Logging Time Stamp for Selected Processes

The Last Logging Time Stamp for Selected Processes field reports the current time and the timestamp associated with the last time the emmDistributor and camAuditor processes wrote to their respective logfiles.

You can compare the timestamps with the current time to determine whether the emmDistributor and camAuditor processes are running properly.

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

DHCT Status Summary

The data in the DHCT Status Summary field provides a summary of all DHCTs in the database.

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).

The system also reports the number of DHCTs in the database of type NULL.

Note: A DHCT of type NULL represents a DHCT that has no record in the database, but has attempted to sign onto the system.

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

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 before the start of a cycle
- 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 uses to calculate the expected cycle duration. Additionally, a summary of the allocation of bridges (and associated DHCT population numbers) to emmDistributor threads also displays.

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.

Localization (Zip +4) Info

This field lists all the localization groups and the bridges they contain. The Group Key is the Zip+4 code for the group.

Localization groups are required to distribute EMMs efficiently, especially for one-way STBs. Mapping is done from the Web UI and the Doctor Report reports the present configuration.

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 EC.

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.

Active Elements

The data in the Active Elements field reports the number of active QAMs (QAMs, MQAMs, GQAMs, GoQAMs, IFGoQAMs, GQIQAMs, Table Based QAMs), QPSK modulators and demodulators, Netcrypts, vDCMs, Hubs, Headends, Channel Maps, Service Groups, PCGs and CMTSs on the EC.

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 and CMTS bridge in the system.

In addition, under the Node Set Name/HCT Count subheading, the field lists all of the defined node sets on the system and the number of DHCTs assigned to each node set.

Offline QAMs

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

Offline PCGs

The data in the Offline PCGs field lists any PCG listed in the database as offline.

Offline vDCMs

The data in the Offline vDCMs field lists any vDCM listed in the database as offline.

Online QAMs with null keycertificates Check

This field identifies those QAM modulators that have an Admin status of Online, but do not have key certificates.

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 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 EC:

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 EC.

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 EC user interface to create one.

Maximum Session Oid Created

Use this field to verify the session OID in the session table. A warning message displays if it reaches 1,879,048,192, which is 87 percent of the maximum allowable value (2,147,483,647).

If the maximum allowable value is reached, no more session setups can occur.

Active Subscription Packages

The data in the Active Subscriber Packages field lists the number of active subscriber packages and the maximum session OID configured on the EC.

List of Stranded Segments

The data in the List of Stranded Segments field lists the segments that are exist in the database but are not present in the EC Web UI.

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 EC .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 the logLvl 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 and the IP address of that QAM modulator.

Notes:

- 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.
- This field is not applicable if the SI_INSERT_RATE=0 (when SI is being transmitted out-of-band).

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.

Duplicate QAM Frequencies Within Hubs

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

Netcrypt Information

The Netcrypt Information field provides data concerning the Netcrypt Bulk Encryptor.

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.

Post Upgrade Checks (POC)

The data in the POC field verifies if a dncseth entry exists in the /etc/hosts file.

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.

No Cisco application server: Ignore any application server-related errors at these sites.

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.

No Cisco application server: Ignore any application server-related errors at these sites.

Important: Resolve discrepancies by using the EC 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.

No Cisco application server: Ignore any application server-related errors at these sites.

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.

No Cisco application server: Ignore any application server-related errors at these sites.

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 results in a **phoneactivetime** of zero, which leads to a false PPV base time.

No Cisco application server: Ignore any application server-related errors at these sites.

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.

EUT updates should occur when the EC has IPPV events that are beginning and ending. EUT updates indicate that the camPsm process on the EC is functioning properly. If there are no IPPV events, it is normal for there to be no EUT update.

The EUT file updates when subscription packages change.

EUT Package EIDs and ECMs Check

The data in this field verifies that each source is receiving the proper number of entitlement control messages (ECMs).

GBAM Delivery

Assuming that logLvl **camPsm.cam + DE** has been executed, 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, and 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 EC 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.

No Cisco Application Server: Sites that do not use the Cisco Application Server are likely to see SARA- or Vantage-related BFS sessions disabled. This is normal.

BFS Database Metadata and File System Check

The BFS Database Metadata and File System Check field shows available BFS cabinets (also known as, BFS carousels), their links, files, directories, and subdirectories for all available sites.

Miscellaneous BFS Check

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

- No more than one data Carousel 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 is not in SI and the DHCT is 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 700-716377-01), or your appropriate upgrade installation instructions, for assistance in setting data rates.
- Rovi sites, or sites running interactive applications (VOD, games, and so on), may generate data rate errors. Refer to the previously mentioned document for assistance in setting data rates.

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 onto the site of your content provider. You may have network issues preventing the IPG Collector from running.

No Cisco Application Server: Ignore any application server-related errors at these sites.

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.

No Cisco application server: Ignore any application server-related errors at these sites.

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. 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.

CVT Multicast

There are four sections of the Doctor report for monitoring the multicast CVT feature:

- CVT status
- QAM CVT Mode - Lists the QAMs in InsertPacket and PID Route mode
- Multicast CVT Bandwidth Config - Shows the bandwidth allowed for multicast CVT
- Multicast CVT PID Route Information and Status - Shows:
  - QAM Names used in multicast CVT
  - QAM Types
  - Route Types
  - Output Ports
  - Multicast IP
  - PID used
  - Bandwidth
  - Status

Ping All Active Elements

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

- All active QAM-family modulators
- All active QPSK modulators (Ethernet and RF)
- TED device
- Netcrypt server
- Interactive session server
- All active PCGs

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.

Special Use Cases for the Doctor Report

One-to-One Relationship Between DHCTs and Serial Numbers

The Doctor Report includes the –*x* option (doctor -x). Through the –*x* option, you can confirm that each DHCT is in the system with a single serial number. If errors are found, they are listed.

If you detect errors, work with Cisco Services to address them.

Check for Quarantined Modulators

The Doctor Report includes the –*q* option (doctor -q). Through the –*q* option, you can ping the QAM, MQAM, GQAM, and GoQAM modulators and test the remote procedure call (RPC) connection between the modulators and the EC.

Sites using VOD and SDV should run this check daily. Modulators that are quarantined or listed as offline should be investigated and the problems that caused them to be quarantined should be addressed.

Clean Up Old Doctor Reports

The Doctor Report includes the –*c* option (doctor -c). The system generates and stores a new Doctor Report each time the utility is run. Over time, these stored reports can fill the hard drive. Running the Doctor Report with the -c option, followed by the number of files you want to keep, removes old reports.

Example: Keeps 100 existing report.

```
[dncs@berlin3 doctor]$ doctor -c100
```

3

Identify and Correct Database Problems with the checkDB Script

Introduction

The checkDB script identifies and corrects various potential problems in the EC 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 EC 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 EC 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 EC database.

- DHCTs with a status of in-service that have EMMs ready to expire.

  Note: The checkDB.sh script prompts you to either restage or delete DHCTs with EMMs ready to expire.

- Sites are likely to experience a problem due to the EC 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

Make sure that you have a current backup of your EC 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 EC 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 34) 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 to delete DHCT, CableCARD modules, and CableCARD host 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 completely deletes these device records from the EC database. It deletes a single record or all records in a list containing MAC addresses in a text file.

The logic in the deleteDhct utility is very good at finding all database rows in all the different tables that contain or used to contain records for the specified device(s).

The deleteDhct utility deletes orphaned 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 EC database for possible error conditions:

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

You can run the checkDB script in three possible modes:

- **Default mode (with no options) –** Generate a detailed report listing possible error conditions in the database. In default mode, the script does not correct any error conditions it finds. The script merely generates a report listing potential error conditions.
- **Fix mode –** Automatically delete certain orphaned records from the database. 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: We recommend that you run the script with no options before running the script with one of the "fix" mode options.
- **-v option –** 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.

1 As **root** user, type the following command and press **Enter** to make the /dvs/dncs/tmp your working directory:

```
[root@ecnextx9 ~]# cd /dvs/dncs/Utilities
```

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

```
[root@ecnextx9 Utilities]# checkDB.sh
```

Note: This command creates output files in the /home/dncs directory.

Output at end of script:

```
The complete output file is checkDB.180322_1649.txt
The output for check1 is found in checkDB.check1.mac.180322_1649.txt
The output for check2 is found in checkDB.check2.SN.180322_1649.txt
The output for check3 is found in checkDB.check3.KEY.180322_1649.txt
The output for check4 is found in checkDB.check4.SM.180322_1649.txt
The output for check5 is found in checkDB.check5.S_sn.180322_1649.txt
The output for check6 is found in checkDB.check6.SAP.180322_1649.txt
The output for check7 is found in checkDB.check7.SPA.180322_1649.txt
The output for check8 is found in checkDB.check8.CERT.180322_1649.txt
The output for check9 is found in checkDB.check9.emm.180322_1649.txt
The output for check11 is found in checkDB.check11.OLD.180322_1649.txt
The output for check12 is found in checkDB.check12.expEMM.180322_1649.txt
The output for check14 is found in checkDB.check14.sSN.180322_1649.txt
```

3 Type the following command and press **Enter** to view the complete output.

Command Syntax:

```
less checkDB.[DATE_TIME].txt
```

Example:

```
[root@ecnextx9 Utilities]# less checkDB.180108_1142.txt
```

4 Refer to ***Sample Logfile*** (on page 35) and ***Analysis of Logfile*** (on page 39) as you examine the logfile created by the checkDB script.

Notes:

- Press the **spacebar** to page through the output file.
- Press **Q** to close the output file when you are finished.

Sample Logfile

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.

Example Output:

```
Working directory is /dvs/appserv

Database is appdb (localhostdbserver)

Working directory is /dvs/dncs

Database is dncsdb

checkDB.sh script starts

------------------------

# Fri Mar 23 09:20:52 EDT 2018

# The total number of rows in hct_profile  =     14.

# The total number of rows in secure_micro =      0.

# Highest eu_eid used for subscription pkgs=      7.

# DHCT Registration is set to 'Open Registration'.

#########################################################################

# Check 1: Boxes with no Serial Number (missing rows in pdsernummap)

#

Wait while a list of MAC addresses without SNs is generated.
```

```
# There are 4 MAC addresses with No DHCT Serial Number
# Rows defining SN/MAC should be added for these boxes in 'pdsernummap'
00:0F:21:A6:60:34
00:0F:21:A8:C8:14
00:21:BE:1D:97:1C
00:1A:C3:20:86:0E
################################################################################
# Check 2: list of SN/MACs that should NOT be in pdsernummap
#
Wait for a list of SN/MACs that should NOT be in pdsernummap
# There are 0 SN/MAC matches that should be deleted from 'pdsernummap'
################################################################################
# Check 3: Boxes with no KeyCertificate (missing rows in pdkeycertificate)
#
Wait for list of Boxes with no KeyCertificate
# There are 4 boxes with no 'pdkeycertificate'
# These boxes are essentially 'dead'
# They can not be activated because they have no certificate
# (Verify and use the 'deleteDhct' utility to delete these.)
00:0F:21:A6:60:34
00:0F:21:A8:C8:14
00:21:BE:1D:97:1C
00:1A:C3:20:86:0E
################################################################################
# Check 4: List of secure_micro rows orphaned by macaddr
#
Wait for list of secure_micro rows orphaned by macaddr
# There are 0 secure_micro rows with mac_addr not in 'hct_profile'
################################################################################
# Check 5: List of secure_micro rows with SMSN not in hct_profile
#
Generating list of secure_micro rows with SMSN not in hct_profile
# There are 0 secure_micro MACs with sm_serial_num not in 'hct_profile'
################################################################################
# Check 6: List of sm_auth_profile rows with no secure_micro parent
#
Wait for list of sm_auth_profile rows with no secure_micro parent
```

```
# There are 0 sm_auth_profile rows with no secure_micro parent
################################################################################
# Check 7: List of SMSNs from sm_pkg_auth with no sm_auth_profile
#
Listing SMSNs from sm_pkg_auth with no sm_auth_profile counterpart
# There are 0 sm_pkg_auth SMSNs with no sm_auth_profile counterpart.
################################################################################
# Check 8: Count of KeyCertificates with no parent DHCT or QAM
#
Wait for count of KeyCertificates with no parent DHCT or QAM
# There are no orphaned rows in 'pdkeycertificate'.
################################################################################
# Check 9: List of EMMs with no parent hct_profile row
#
Generating a list of EMMs with no parent hct_profile row
# There are 0 boxes having EMMs with MAC address not in 'hct_profile'
################################################################################
# Check 10: Check for orphaned authorizations
#
Wait while I check for orphaned authorizations
# No orphaned authorizations exist...
################################################################################
# Check 11: List of 90-day old Boxes still not fully staged
#
Wait for list of 90-day old Boxes still not fully staged.
# There are 0 boxes with no 'secure_micro', but with very-old EMMs.
################################################################################
# Check 12: List of Boxes with expiring EMMs today or within 4 days from today
#
Wait for List of Boxes with expiring EMMs today or within 4 days from today.
# There are 0 'In-Service' boxes with 'almost-expired' EMMs.
################################################################################
# Check 13: Check for hctt 'oui', 'id', and 'revision' parameters
#
Checking the hctt 'oui', 'id', and 'revision' parameters.
# 4 boxes have NULL in the hctt_oiu, _id, or _revision parameters!
```

```
# 28 percent is MORE than should be tolerated!!
##########################################################################
# Check 14: List of MAC addresses with null hct_se_serial_num
#
Wait while a list of MAC addresses with null hct_se_serial_num is generated.
# There are 4 boxes with no secure serial number
# All STBs having these MAC addresses should be deleted
# (Verify and use the 'deleteDhct' utility to delete these.)
00:0F:21:A6:60:34
00:0F:21:A8:C8:14
00:21:BE:1D:97:1C
00:21:BE:1D:97:1C
00:1A:C3:20:86:0E
The complete output file is checkDB.180323_0920.txt
The output for check1 is found in checkDB.check1.mac.180323_0920.txt
The output for check2 is found in checkDB.check2.SN.180323_0920.txt
The output for check3 is found in checkDB.check3.KEY.180323_0920.txt
The output for check4 is found in checkDB.check4.SM.180323_0920.txt
The output for check5 is found in checkDB.check5.S_sn.180323_0920.txt
The output for check6 is found in checkDB.check6.SAP.180323_0920.txt
The output for check7 is found in checkDB.check7.SPA.180323_0920.txt
The output for check8 is found in checkDB.check8.CERT.180323_0920.txt
The output for check9 is found in checkDB.check9.emm.180323_0920.txt
The output for check11 is found in checkDB.check11.OLD.180323_0920.txt
The output for check12 is found in checkDB.check12.expEMM.180323_0920.txt
The output for check14 is found in checkDB.check14.eSN.180323_0920.txt
```

Analysis of Logfile

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

Section of Log File	Analysis
checkDB.sh script starts	■ Indicates how many records exist in the hct_profile and secure_micro tables in the database. ■ 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 ■ Reports the registration configuration. – Options are Open Registration and Administrative Gateway. – We recommend Administrative Gateway to prevent set-tops from being added to your system without your knowledge.
Check 1: Boxes with no Serial Numbers (missing row in pdsernummap)	This check identifies 4 set-tops that are in the pdsernummap database table without serial numbers. ■ Identifies the total number of MAC addresses not having a DHCT serial number. ■ Lists the actual MAC addresses not having a DHCT serial number. ■ Contact Cisco Services if your logfile indicates that you have set-tops in the database without serial numbers. Cisco Services will retrieve the list from your system and will insert the correct serial numbers into your database.
Check 2: list of SN/MACs that should NOT be in pdsernummap	This check lists the SN/MACs (Serial Numbers/MAC addresses) in the pdsernummap database table, but without a required corresponding entry in the hct_profile table. The checkDB script concludes that these are orphaned records and recommends that they be deleted.

Section of Log File	Analysis
Check 3: Boxes with no KeyCertificate (missing rows in pdkeycertificate)	This check lists the MAC addresses associated with 4 set-tops that do not have a key certificate in the pdkeycertificate entry; thus these set-tops cannot be activated. These set-tops should be deleted using the deleteDhct utility.
Check 4: List of secure_micro rows orphaned by macaddr	This check reports that there are no entries in the secure_micro table of set-tops that have MAC addresses but do not have a corresponding entry in the hct_profile table.
Check 5: List of secure_micro rows with SMSN not in hct_profile	This check reports that there are no entries in the secure_micro table of set-tops that have no SMSN (secure micro serial number) entries in the hct_profile table.
Check 6: List of sm_auth_profile rows with no secure_micro parent	This check 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.
Check 7: List of SMSNs from sm_pkg_auth with no sm_auth_profile	This check 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.
Check 8: Count of KeyCertificates with no parent DHCT or QAM	This check indicates that there are no pdkeycertificates without a parent DCHT or QAM. If records were present, they should be deleted from the pdkeycertificate table. Delete the records listed by oidval in the checkDB.check8.[date_PID].txt file. **Important**: ■ Use caution not to delete the seven starter keys. ■ Do not delete certificates for QAMs with encrypted sessions.
Check 9: List of EMMs with no parent hct_profile row	This check reports that there are no set-tops having EMMs with a MAC address that are not in the hct_profile table.
Check 10: Check for orphaned authorizations	This check indicates that there are no orphaned authorization records in the database.

Section of Log File	Analysis
Check 11: List of 90-day old Boxes still not fully staged	This check indicates that there are no 90-day old set-tops with very old EMMs in the secure_micro table.
Check 12: List of Boxes with expiring EMMs today or within 4 days from today	This check states that there are 0 'In-Service' boxes with 'almost-expired' EMMs.
Check 13: Check for hctt 'oui', 'id', and 'revision' parameters	These lines indicate that there are 4 set-top 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 set-tops with NULL values in the previously mentioned fields exceeds 1 percent of the set-tops in the hct_profile table, the checkDB script notifies you.
Check 14: List of MAC addresses with null hct_se_serial_num	This check lists 4 set-tops, by MAC address, that do not have an hct_se_serial_num entry. These set-tops should be deleted.
Output file names for logs	Identifies the filename for the complete log file as well as the filename for each specific database check.

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.

Important: Before running the checkDB script with the **-f** or **-F** options, make sure that you have a current database backup.

1 As **root** user, type the following command to change to the **/dvs/dncs/Utilities** directory:

```
[root@ecnextx9 ~]# cd /dvs/dncs/Utilities
```

2 Enter the following command to source the environment.

```
[root@ecnextx9 Utilities]# . /dvs/dncs/bin/dncsSetup
```

3 Choose one of the following options:

- Type the following command to run the checkDB script with the **-f** option.

```
[root@ecnextx9 Utilities]# checkDB.sh -f
```

- Type the following command to run the checkDB script with the *-F* option.

```
[root@ecnextx9 Utilities]# checkDB.sh -F
```

4 Review the log files created by the script.

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, you can use the *-F* option 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

1 Open a terminal window on the EC.

2 Type the following command and 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.

```
[root@ecnextx9 Utilities]# checkDB.sh -v
```

Example Output:

```
checkDB.sh script starts
------------------------
This is 'checkDB.sh', version : 8.1.5
```

4

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 EC 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 EC.

One of the conditions of the EC that the Doctor Report monitors is the size of the bulk.tbl file. If 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, you should run the chkSamUrl utility. The chkSamUrl utility allows you to delete unused SAM URLs from the EC, reducing 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 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" *
*********************************************************
```

To Learn More About the chkSamUrl Utility

Follow these instructions to access the help screen:

1 As **dncs** user, type the following command to display the help screen for the **chkSamUrl** utility.

```
[dncs@ecnextx9 Utilities]$ chkSamUrl -h
```

2 Press the **spacebar** to page through the output.

Running the chkSamUrl Utility

Complete the following instructions to run the chkSamUrl utility in order to delete unused SAM URLs from the system:

1 As **dncs** user, type the following command to run the chkSamUrl utility.

```
[dncs@ecnextx9 Utilities]$ chkSamUrl -r
```

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.

Example Output:

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
 Removing unused SAM URLs from the database
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
 - List current database stats:
SAM URL bulk table:     /dvs/dvsFiles/SAM/bulk.tbl
Last Updated:           Jan 19 19:26
Size:                   1661
Used URL Entries:       14
Unused URL Entries:     1
Do you wish to continue with removal of unused SAM URLs? [y/n]:
```

2 When prompted to continue, type **y**. The chkSamUrl script runs to completion.

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

Example Output:

```
 - 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-----. 1 dncs dncs  1726 Jan 19 19:27 /tmp/applicationurl.unl
-rw-r-----. 1 dncs dncs 40125 Jan 19 19:27 /tmp/displaychannels.unl
-rw-r-----. 1 dncs dncs 85469 Jan 19 19:27 /tmp/samservices.unl

 - Now removing unused SAM URL entries from the database
Database selected.
1 row(s) deleted.
Database closed.

 - List updated  database stats:
SAM URL bulk table:     /dvs/dvsFiles/SAM/bulk.tbl
Last Updated:           Jan 19 19:26
Size:                   1661
Used URL Entries:       14
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.
################################################################
```

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

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

- If **yes**, go to the next step.
- If **no** and the **bulk.tbl** file size is greater than 45 KB, contact Cisco Services.
- If **no** and the **bulk.tbl** file size is less than 45 KB, go to the next section.

5 From the EC Web UI, click the **Navigation** menu,  , and then click **App Interface Modules > SAM Service**. The SAM Service List window appears.

6 Use the filter to display SAM services.

7 Select a SAM Service and click **Edit**.

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, as **dncs** user in the terminal window, type the following command. The output lists the updates of the current file size and available space in the bulk.tbl file.

```
[dncs@ecnextx9 Utilities]$ chkSamUrl -l
```

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 3.

Important: If the new bulk.tbl file size is not smaller than the file size recorded in Step 3, call Cisco Services

11 Go to the next section.

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 EC Web UI, click the **Navigation** menu,  , and then click **App Interface Modules > SAM Service**. The SAM Service List window appears.

2 Select the service you want to update and click **Edit**. The Edit SAM Service window opens.

3 Record the URL that you are about to edit _____, and edit the URL as needed (for example, to change the application version number in the URL).

4 Click **Save**. You are returned to the SAM Service List window.

5 Is the SAM URL that you modified used by multiple services?

- If **yes**, repeat Steps 2 through 4 for each of those services and then go to the next step.
- If **no**, go to the next step.

6 Select the SAM service that you selected in Step 2, and click **Edit**. The Edit SAM Service window opens.

7 From the **Application URL** line, click the **Select** button. The Application URL Selection window appears.

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 3, and then click **Delete URL**. A confirmation window appears.

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

5

Retrieve CableCARD Data with the getCCdata Utility

Introduction

The getCCdata utility reports errors and retrieves 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 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

About the getCCdata Utility

Output From the getCCdata Utility

The getCCdata utility generates output to the screen of the EC, and to two files that are stored in the /tmp directory of the EC.

Output generated to the screen tends to roll quickly off the screen; output recorded in files stored on the EC can be examined at your convenience.

Output from the getCCdata utility is divided into two parts.

1. The first part lists any errors uncovered during examination of the CableCARD-related components of the network.
2. The second part provides supporting data for the first part.

Errors uncovered by the getCCdata utility are clearly marked. If the report reveals the presence of an error, you can 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 EC.

- 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 is a troubleshooting tool. We encourage you to run the getCCdata utility daily (similar to the Doctor Report) and focus on data that has changed from day to day.

Cisco Services can help you troubleshoot or interpret the data revealed by the getCCdata utility.

Run the getCCdata Utility

1 As **dncs** user, enter the following command to set the environment variable.

```
[dncs@ecnextx9 Utilities]$ . /dvs/dncs/bin/dncsSetup
```

2 Type the following command and press **Enter:**

```
[dncs@ecnextx9 Utilities]$ getCCdata.ksh
```

The utility runs (this takes a couple of minutes on most systems) and the following menu appears:

```
-------------------
getCCdata
-------------------

1 - Report CableCard Errors
2 - Show CableCard Data
3 - Both 1 & 2

-------------------
Select an Action or
enter q to quit.
-------------------
```

3 Enter one of the following menu options and press **Enter**:

- **1 - Report CableCard Errors** — the utility performs a check for system errors related to CableCARDs.
- **2 - Show CableCard Data** — the utility returns data related to CableCARDs.
- **3 - Both 1 & 2** — the utility performs a check for system errors related to CableCARDs and returns data related to CableCARDs.

Result: The system returns the following output.

```
          CableCardData.out.180109_0924.doc
               getCCdata.ksh v8.1.5
               EC Version:  9.0.12

Enter a MAC address, using capital letters with colons, or hit enter to
continue.
```

4 Perform one of the following tasks:

- Press **Enter** to perform checks on all CableCARDs.
- Type the **MAC address** for a specific CableCARD using upper-case letters and colons.

  Example:

  ```
  00:01:5E:0D:FE:D8
  ```

Result: The data is retrieved and saved to a file in the /tmp directory.

5 When prompted, enter another value to run a report against another CableCARD(s) or enter **q** to exit the script.

Example:

```
00:01:5E:0D:FE:D8
```

6 When prompted, enter another value to run a report against another DHCT with a CableCARD or enter **q** to exit the script.

Sample Output from the getCCdata Utility

Sample Logfile

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.

Example Output:

```
                  CableCardErrors.out.180119_1939.doc

                        getCCdata.ksh v8.1.5

                      EC Version:  9.0.12

Enter a MAC address, using capital letters with colons, or hit enter to continue.

00:01:5E:0D:FE:D8

*****Check 1: CCardServer running:*****

================================================================================

dncs      3821  1999  0 Mar13 ?    00:00:00 Logger -g -n
/dvs/dncs/tmp/CCardServer

dncs      3824  1999  0 Mar13 ?    00:00:33 /dvs/dncs/bin/CCardServer

*****Check 2: CCardServer log files:*****

================================================================================

-rw-r-----. 1 dncs dncs 3942 Mar 13 16:47 /dvs/dncs/tmp/CCardServer.000

*****Check 3: logLvl setting for applicable processes *****

================================================================================

bfsServer                        +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

CCardServer                      +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

hctmConfig                       +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

hctmInd                          +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

hctmMac                          +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

hctmProvision                    +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

osm                              +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

PassThru                         +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

*****Check 4: tomcat running:*****

================================================================================

error

*****Check 5: apache running:*****

================================================================================
```

```
dncs      1705     1  2 Mar13 ?        05:04:41 /usr/lib/jvm/jre-1.8.0/bin/java
Djava.library.path=/dvs/dncs/lib:/usr/lib64 -
Dorg.apache.tomcat.util.http.Parameters.MAX_COUNT=10000 -DDNCSDB=dncsdb -
Djava.util.prefs.systemRoot=/home/dncs/.java -
Djava.util.prefs.userRoot=/home/dncs/.java/.userPrefs -classpath
/usr/share/tomcat/bin/bootstrap.jar:/usr/share/tomcat/bin/tomcat-
juli.jar:/usr/share/java/commons-daemon.jar -Dcatalina.base=/usr/share/tomcat-
dncs -Dcatalina.home=/usr/share/tomcat -Djava.endorsed.dirs= -
Djava.io.tmpdir=/var/cache/tomcat-dncs/temp -
Djava.util.logging.config.file=/usr/share/tomcat-dncs/conf/logging.properties -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
org.apache.catalina.startup.Bootstrap start

*****Check 6: dbUIServer running:*****

================================================================================

dncs      6969  3887  0 Mar13 ?        00:00:00 Logger -g -
n/dvs/dncs/tmp/dbUIServer

dncs      6970  3887  0 Mar13 ?        00:00:03 dbUIServer 5051 127.0.0.1 884744
1

*****Check 8: loghost in /etc/hosts File*****

================================================================================

*****Check 9: Open Cable Compliant:*****

================================================================================

Scientific-Atlanta|openCableCompliant|0|

*****Check 10: Server Defined on BFS:*****

================================================================================

d4f93a098c570007e4000001|POD_Data|1|0|

d4f93a09aea10007e4000001|podServer|1|0|

*****Check 11: CableCard Data on Carousel:*****

================================================================================

/DNCS/POD_Data

/DNCS/POD_Data/7

/DNCS/POD_Data/7/podchan.tblo

/DNCS/POD_Data/gfc.txt

/DNCS/POD_Data/mmi.txt

/DNCS/camPsm/eut

/DNCS/podServer

/DNCS/podServer/podData

*****Check 12: mmi File on BFS:*****

================================================================================

/DNCS/POD_Data/mmi.txt

*****Check 13: mmi File Contents:*****

================================================================================
```

```
*****Check 14: gfc File on BFS:*****

================================================================================

/DNCS/POD_Data/gfc.txt

*****Check 15: gfc File Contents:*****

================================================================================

*****Check 16: Cable Card on Type List:*****

================================================================================

802|12|734|Explorer 0802 version 1.2|Scientific Atlanta|

803|10|734|Explorer 0803 version 1.0|Scientific Atlanta|

802|11|734|Explorer 0802 version 1.1|Scientific Atlanta|

*****Check 17: Number of Type 600, 800, 801, 802, 803, 805, 908, 928 DHCTs in
hct_profile:*****

================================================================================

*****Check 18: CableCARD Data Summary Count:*****

================================================================================

0.0

*****Check 19: podhostpair table:*****

================================================================================

The podhostpair table data has been redirected to the file podhostpair_table.tmp
in /tmp.

*****Check 20: podcrlhost table:*****

================================================================================

*****Check 21: podcrlpackage table:*****

================================================================================

*****Check 22: podserverconfig table:*****

================================================================================

dd47460e0437007462000001|204.3.1.97||13830||||10|0||7200|2592000|120|1500|43|99||

*****Check 23: pod/CC in msgserverclass table:*****

================================================================================

9|CCardServer|127.0.0.1|1|0|

*****Check 24: Files in podServer:*****

================================================================================

total 16

-rw-r-----. 1 dncs dncs 185 Mar 13 16:46 CPDefinition.tbl

-rw-r-----. 1 dncs dncs   5 Mar 13 16:47 mmi.txt

-rw-r-----. 1 dncs dncs  11 Mar 13 16:47 gfc.txt

-rw-r-----. 1 dncs dncs  60 Mar 13 16:47 podData

*****Check 25: CVT Data:*****
```

```
================================================================================

Model  Rev   OUI  Img#   Grp   Download Group    Image          Mode      DHCTs

-----  ---   ---  -----  ----  ---------------   -------------  -------   -------

*****Check 26: DHCT MAC=00:01:5E:0D:FE:D8 Provisioning Data:*****

================================================================================

podhostpair data:

1.pod_mac_address|2.host_id_field|3.pod_id_field|4.pod_revoked|5.request_cpkey_re
f+|6.active_file_date|7.host_change_count

hct_profile data:

1.hct_mac_address|2.hct_ip_address|3.hct_admin_status|4.hct_oper_status|5.hct_se_
serial_num|6.hct_nsap_address|7.sp_nsap_address|8.hct_qpsk_demod_id|9.offset_minu
tes|10.daylight_savings|11.billingid|12.connectionid|13.hctt_oui|14.hctt_id|15.hc
tt_revision|16.btp_name|17.hct_qpsk_mod_id|18.mykeycert|19.sw_toc_id|20.optimctrl

pdsernummap data:

1.sernum|2.macaddr

secure_micro data:

1.sm_serial_num|2.sm_host_mac_addr|3.sm_host_ip_addr|4.sm_admin_state|5.sm_emm_ex
pire|6.sm_last_auth|7.ea_id

sm_auth_profile data:

1.ap_host_mac_addr|2.ap_host_ip_addr|3.ap_analog|4.ap_dis_enable|5.ap_admin_state
|6.ap_ippv_limit|7.ap_pin|8.ap_dms_enable|9.ap_ippv_req_pin||11.ap_blackout_x|12.
ap_blackout_y|13.ap_ippv_enable|14.emm_id|15.sm_serial_num|16.ea_id|17.ap_fast_re
fresh|18.fast_ref_loc_exp|19.fast_ref_gmt_exp|20.ap_credit_limit

sm_pkg_auth data:

1.pkgauth_type|2.pkg_name|3.emm_id|4.sm_serial_num|5.authmap_id|6.auth_id|7.grp_a
uth_id|8.ea_id|9.eu_eid|10.pkgauth_expire_tm|11.pkgauth_evstrt_tm|12.pkgauth_evnt
_dur|13.pkgauth_adm_state

*****Check 27: CC Check-Alert Remaining Time(ART) Parameter Not Zero:*****

================================================================================

Event   ART    Config Name

EAT     0       Default

NIC     0       Default

NPT     0       Default

RMT     0       Default

RWT     0       Default

*****Check 28: OSM AutoMux Data:*****

================================================================================

osmAutoMux Environment Variables in .profile:

osmAutoMux.cfg file contents:

/dvs/dvsFiles/OSM/osmAutoMux.cfg: No such file or directory
```

```
*****Check 29: NOTE:*****

================================================================================

The location of the output file is /tmp/CableCardData.out.180323_1100.doc.

If you see no issues with the data in this report, then proceed with general EC
troubleshooting, i.e. run doctor etc.

                  CableCardErrors.out.180323_1101.doc

                        getCCdata.ksh v8.1.3

                     EC Version:  9.0.4

*****Check 1: CCardServer running:*****

================================================================================

Yes

*****Check 2: CCardServer log files:*****

================================================================================

Yes:  There are multiple CCardServer log files.

*****Check 3: logLvl setting for applicable processes *****

================================================================================

bfsServer                       +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

CCardServer                     +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

hctmConfig                      +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

hctmInd                         +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

hctmMac                         +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

hctmProvision                   +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

osm                             +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

PassThru                        +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP

*****Check 5: apache running:*****

================================================================================

Yes

*****Check 6: dbUIServer running:*****

================================================================================

Yes

*****Check 8: loghost in /etc/hosts File*****

================================================================================

Error:  There is no entry for loghost in the hosts file.

  This entry depends on network design.

*****Check 9: Open Cable Compliant:*****

================================================================================

Error:  Not Open Cable Compliant
```

```
*****Check 10: Server Defined on BFS:*****

================================================================================

Yes

*****Check 11: CableCard Data on Carousel:*****

================================================================================

Yes

*****Check 12: mmi File on BFS:*****

================================================================================

Yes

*****Check 13: mmi File Contents:*****

================================================================================

Error:  mmi.txt does not exist.

wc: /tmp/cbcdmmicontents3: No such file or directory

rm: cannot remove '/tmp/cbcdmmicontents2': No such file or directory

rm: cannot remove '/tmp/cbcdmmicontents3': No such file or directory

*****Check 14: gfc File on BFS:*****

================================================================================

Yes

*****Check 15: gfc File Contents:*****

================================================================================

Error:  gfc.txt does not exist.

diff: /tmp/cbcdgfccontents3: No such file or directory

diff: /tmp/cbcdgfccontents3: No such file or directory

*****Check 16: Cable Card on Type List:*****

================================================================================

Yes:  There is more than one revision of Type 600, 800, 801, 802, 803, 805, 908,
928 DHCT on the Type List.

*****Check 17: Number of Type 600, 800, 801, 802, 803, 805, 908, 928 DHCTs in
hct_profile:*****

================================================================================

*****Check 18: CableCARD Data Summary Count:*****

================================================================================

0.0

*****Check 19: podhostpair table:*****

================================================================================

The podhostpair table data has been redirected to the file podhostpair_table.tmp
in /tmp.
```

```
*****Check 20: podcrlhost table:*****

================================================================================

0.0

*****Check 21: podcrlpackage table:*****

================================================================================

0.0

*****Check 22: podserverconfig table:*****

================================================================================

Error: IP

*****Check 23: pod/CC in msgserverclass table:*****

================================================================================

Yes

*****Check 24: Files in podServer:*****

================================================================================

Yes

*****Check 25: CVT Data:*****

================================================================================

Yes

*****Check 26: DHCT MAC=00:01:5E:0D:FE:D8 Provisioning Data:*****

================================================================================

03/23/2018
11:01:55.489|29705/29705/0xf702a700|SYSLOG|libloggingApi:LogService.C(214)|Progra
m started tellDhct

# MACaddress        SM_serial_num   admin op OUI Model Rev mod dmod     IP
IPV6

# 00:01:5E:0D:FE:D8 - hct_profile does not exist.

03/23/2018
11:01:55.509|29705/29705/0xf702a700|SYSLOG|libloggingApi:LogService.C(808)|Proces
s 29705 exiting.

*****Check 27: CC Check-Alert Remaining Time(ART) Parameter Not Zero:*****

================================================================================

Error

*****Check 28: OSM AutoMux Data:*****

================================================================================

N/A

*****Check 29: NOTE:*****

================================================================================

The location of the output file is /tmp/CableCardErrors.out.180323_1101.doc.

If you see no issues with the data in this report, then proceed with general EC
troubleshooting, i.e. run doctor etc.
```

6

Troubleshoot the EAS with the getEASdata Utility

Introduction

The Federal Communications Commission (FCC) 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 make sure that their subscribers receive national, state, and local warning messages about emergency conditions.

The getEASdata utility ensures the reliability of your EAS. The utility helps you troubleshoot your EAS by reporting EAS-related errors and retrieving data associated with system components that pertain to the EAS.

Some of the EAS-related data retrieved by the getEASdata utility are:

- 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 /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 EC 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 five minutes of transmitting the EAS message.

Note: Refer to ***Before Running the getEASdata Utility*** (on page 62) for additional system requirements 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 EC is used for EAS functionality.
- The MMMServer debug flag must be checked in the logging Web UI on the EC.

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

  Note: Refer to the online help for your system release for assistance in setting tracing 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 five minutes and less than 15 minutes since you transmitted an EAS message. It sometimes takes up to five 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 the following two reports:

- **EAS Error Report** — highlights errors that the utility discovers in its examination of the EAS configuration.
- **EAS Data Report** — displays EAS configuration data that you can examine to identify the source of the error.

Our engineers recommend that system operators generate each report whenever you run the getEASdata utility, even if the EAS Error Report shows no errors. Examining the 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

1 As **dncs** user, enter the following command to run the **getEASdata** utility. 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.

```
[dncs@ecnextx9 Utilities]$ getEASdata.ksh
--------------------
   getEASdata
--------------------
1  - Report EAS Errors
2  - Show EAS Data
--------------------
Select an Action or
enter q to quit.
--------------------
```

2 Type **1** (for Report EAS Errors) and press **Enter**. The utility displays a confirmation message about several conditions that must be true before you should run the report.

```
------------------------------------------------------------------------------
Execute this selection if:

(a) The debug flag L is set in .profile on the EC.
(b) You have successfully sent EAS messages in the past.
(c) An EAS message was sent from the EAC more than 5 minutes ago.
(d) It is more than 5 minutes and less than 15 minutes
     since the message was sent.
(e) The message has not displayed on the DHCTs.
(f) The DHCT IP is pingable and cmd2000 is enabled in the DHCT.

------------------------------------------------------------------------------

Would you like to continue? y/n
```

3 Type **y** and press **Enter**. You are prompted to enter an IP address of a DHCT that should have received the EAS message or hit.

4 Type the IP address of a DHCT and press **Enter**.

Note: If you fail to provide an IP address, the utility still runs 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 EC.
- The system displays a message that states that the EAS Error Report can also be found in the **/tmp** directory.
- The system redisplays the menu of the getEASdata utility.

5 Type **2** (for Show EAS Data) and press **Enter**.

6 Type the IP address of a test DHCT that did not receive the EAS message and press **Enter** or simply press **Enter** to continue. The following message appears

Results:

- The system runs the EAS Data Report and displays the output to the screen of the EC.
- The system displays a message that states that the EAS Data Report can also be found in the **/tmp** directory.
- The system redisplays the menu of the getEASdata utility

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

8 Go to the next section.

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 terminal windows. By examining the two reports simultaneously, you can better understand the relationship of the reports.

1 As an Administrative user (for example, ecadmin), open two terminal windows.

2 Type the following command in each windows to change to the **/tmp** directory.

```
[ecadmin@ecnextx9 ~]$ cd /tmp
```

3 In one window, type the following command and press **Enter**. The system lists all files in the /tmp directory that begin with EASerrors.

```
[ecadmin@ecnextx9 tmp]$ ls 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 window, type the following command and press **Enter**. The selected EAS Error Report opens in the window using the Linux *less* utility.

Command Syntax:

```
less [EAS Error Report name]
```

Example:

```
[ecadmin@ecnextx9 tmp]$ less EASerrors.out.180323_1207.doc
```

5 In the other window, type the following command and press **Enter**. The system lists all files in the /tmp directory that begin with EASdata.

```
[ecadmin@ecnextx9 tmp]$ ls 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 Type the following command to open the EASdata file. The selected EAS Data Report opens in the window.

Command Syntax:

```
less [EAS Data Report name]
```

Example:

```
[ecadmin@ecnextx9 tmp]$ less EASdata.out.180323_1210.doc
```

7 Go to the next section 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 the next section 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: If needed, call Cisco Services for assistance.

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 EC or the Application Server is incorrect.

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

- 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 /home/dncs/.profile file.

7

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 EC.

Through the listTftpConfigs file, you can examine this data at a glance, without having to access the Web UI for each device.

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 utility examines all network element configuration files in the EC database for the EC. When complete, the utility lists those files to the screen of the EC. Displayed information includes the name and path of the configuration file, the site ID, the name of the network element, and 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, and the IP address that the network element uses to communicate with the various processes associated with the network element.

- *-f* — The utility 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. This option forces the utility to increase the detail in the data it reports.

- *-V* — The utility displays its version number.

- *-c CFGFILE* — Display configuration data and drop point values for the specified configuration file.

- *-n NENAME* — Display configuration data and drop point values for the specified network element.

  Example: QAM1

- *-s SITE* — Display configuration data and drop point values for the specified site.

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 with this option includes the following:

- Name of the configuration file
- Site (local EC 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 As **dncs** user, type the following command to change to the **/dvs/dncs/Utilities** directory.

```
[dncs@ecnextx9 ~]$ cd /dvs/dncs/Utilities
```

2 Enter the following command to run the **listTftpConfigs** script with the **-a** option.

```
[dncs@ecnextx9 Utilities]$ listTftpConfigs.ksh  -a
```

Example Output:

```
Tftp Config DB Report for ALL sites from DB=dncsdb for vodwater8 on Fri Mar 23 14:55:40 EDT 2018
=========================================================================
Config File                   Site(ID)  NE Name/Oid      IP Addr      Mac Addr
===========                   ========  =============    =========    ========
/var/lib/tftpboot/qpsk.config  DNCS(1)   QPSK425007001    142.7.70.1   00:02:DE:83:93:2C
/var/lib/tftpboot/qpsk.config  DNCS(1)   QPSK425099001    142.99.70.1  00:02:00:00:00:01
/var/lib/tftpboot/qpsk.config  DNCS(1)   QPSK425014001    142.14.70.1  00:02:DE:83:A2:5A
/var/lib/tftpboot/qam.config   DNCS(1)   CAQAMB425007001  142.7.0.1    00:00:00:00:00:02
/var/lib/tftpboot/qam.config   DNCS(1)   CAQAMB425014001  142.14.0.1   00:02:DE:81:F5:23
/var/lib/tftpboot/mqam.config  DNCS(1)   MQAMB425007001   142.7.10.1   00:00:00:00:00:03
/var/lib/tftpboot/mqam.config  DNCS(1)   MQAMB425014001   142.14.10.1  00:02:DE:83:3A:E4
/var/lib/tftpboot/gqam.config  DNCS(1)   GQAMB425007001   142.7.20.1   00:02:DE:82:3C:2F
/var/lib/tftpboot/gqam.config  DNCS(1)   GQAMB425007002   142.7.20.2   00:02:DE:82:90:FF
/var/lib/tftpboot/gqam.config  DNCS(1)   GQAMB425099001   142.99.20.1  00:1A:C3:D2:B0:EC
/var/lib/tftpboot/gqam.config  DNCS(1)   GQAMB425099002   142.99.20.2  00:02:DE:82:3C:61
/var/lib/tftpboot/gqam.config  DNCS(1)   GQAMB425099003   142.99.20.3  00:02:DE:82:81:8A
/var/lib/tftpboot/gqam.config  DNCS(1)   GQAMB425099004   142.99.20.4  00:02:DE:82:81:99
/var/lib/tftpboot/gqam.config  DNCS(1)   GQAMB425014001   142.14.20.1  00:02:DE:82:5A:4E
/var/lib/tftpboot/gqam.config  DNCS(1)   GQAMB425014002   142.14.20.2  00:1A:C3:D2:AD:B5
/var/lib/tftpboot/nc.config    DNCS(1)   NETCR425007001   142.7.60.1   00:00:00:00:00:0F
Tftp Config File Report for ALL files for vodwater8 on Fri Mar 23 14:55:41 EDT 2018
=========================================================================
DNCS:/var/lib/tftpboot/gqam.config droppoints:
                      BootCodePath gqam_host_boot_4_6_4.bin
                      ApplCodePath gqam_host_app_4_6_4.bin
                        RFCodePath gqam_rf_26.bin
               InputNPBootCodePath gqam_input_boot_4_6_4.bin
                InputNPAppCodePath gqam_input_app_4_6_4.bin
              OutputNPBootCodePath gqam_output_boot_4_6_4.bin
               OutputNPAppCodePath gqam_output_app_4_6_4.bin
                   RpcServerIpAddr 204.3.1.97
                 AlarmServerIpAddr 204.3.1.97
                  TrapServerIpAddr 127.0.0.1
DNCS:/var/lib/tftpboot/mqam.config droppoints:
                      BootCodePath mqam_boot_1_2_3.bin
                      ApplCodePath mqam_app_2_8_1.bin
                        RFCodePath mqam_rf_23.bin
                   RpcServerIpAddr 204.3.1.97
                 AlarmServerIpAddr 204.3.1.97
DNCS:/var/lib/tftpboot/nc.config droppoints:
                      BootCodePath nc_host_boot_1_4_3.bin
                      ApplCodePath nc_host_app_1_4_3.bin
               InputNPBootCodePath nc_input_boot_1_4_3.bin
                InputNPAppCodePath nc_input_app_1_4_3.bin
              OutputNPBootCodePath nc_output_boot_1_4_3.bin
               OutputNPAppCodePath nc_output_app_1_4_3.bin
                      FpgaCodePath nc_fpga_16_8.bin
                   RpcServerIpAddr 204.3.1.97
                RpcInitialProgNum 805306370
                 AlarmServerIpAddr 204.3.1.97
                  TrapServerIpAddr 127.0.0.1
DNCS:/var/lib/tftpboot/qam.config droppoints:
                      BootCodePath caqam_boot212.bin
                      ApplCodePath caqam_app271.bin
                   RpcServerIpAddr 204.3.1.97
                 AlarmServerIpAddr 204.3.1.97
DNCS:/var/lib/tftpboot/qpsk.config droppoints:
                       qpsk_man_ip 204.3.1.97
                        hct_man_ip 204.3.1.97
                        nms_man_ip 204.3.1.97
                       stat_mgr_ip 204.3.1.97
                           appver app_A62
```

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 As **dncs** user, type the following command and press **Enter**.

Command Syntax:

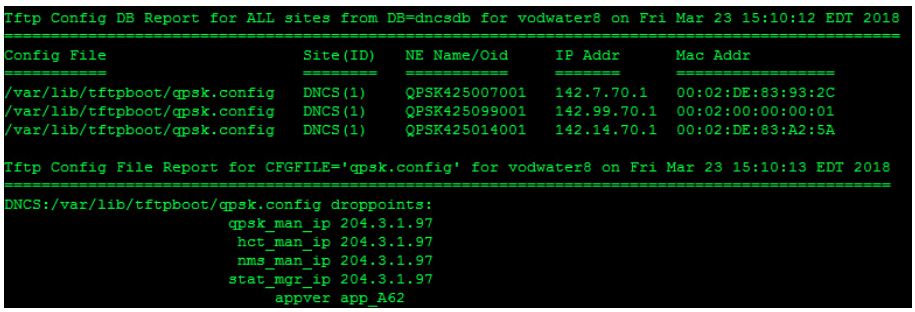
```
listTftpConfigs.ksh  -c [CFGFILE]
```

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

Example:

```
[dncs@ecnextx9 Utilities]$ listTftpConfigs.ksh -c
/var/lib/tftpboot/qpsk.config
```

Example Output:



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 As **dncs** user, type the following command and press **Enter**.

Command Syntax:

```
listTftpConfigs.ksh -n [NENAME]
```

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

Example:

```
[dncs@ecnextx9 Utilities]$ listTftpConfigs.ksh -n
QPSK425007001
```

Example Output:

```
Tftp Config DB Report for ALL sites from DB=dncsdb for vodwater8 on Fri Mar 23 15:16:35 EDT 2018
=================================================================================================
Config File                   Site(ID)   NE Name/Oid       IP Addr         Mac Addr
===========                   ========   ===========       =======         ========
/var/lib/tftpboot/qpsk.config  DNCS(1)    QPSK425007001     142.7.70.1      00:02:DE:83:93:2C

Tftp Config File Report for NENAME='QPSK425007001' for vodwater8 on Fri Mar 23 15:16:37 EDT 2018
=================================================================================================
DNCS:/var/lib/tftpboot/qpsk.config droppoints:
                       qpsk_man_ip 204.3.1.97
                        hct_man_ip 204.3.1.97
                        nms_man_ip 204.3.1.97
                       stat_mgr_ip 204.3.1.97
                           appver app_A62
```

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 As **dncs** user, type the following command and press **Enter**:

Command Syntax:

```
listTftpConfigs.ksh -s [SITE]
```

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

Example:

```
[dncs@ecnextx9 Utilities]$ listTftpConfigs.ksh -s DNCS
```

Example Output:

```
Tftp Config DB Report for Site=DNCS from DB=dncsdb for vodwater8 on Fri Mar 23 15:20:45 EDT 2018
================================================================================================
Config File                   Site(ID)    NE Name/Oid      IP Addr       Mac Addr
===========                   ========    ===========      =======       ========
/var/lib/tftpboot/qpsk.config  DNCS(1)     QPSK425007001    142.7.70.1    00:02:DE:83:93:2C
/var/lib/tftpboot/qpsk.config  DNCS(1)     QPSK425099001    142.99.70.1   00:02:00:00:00:01
/var/lib/tftpboot/qpsk.config  DNCS(1)     QPSK425014001    142.14.70.1   00:02:DE:83:A2:5A
/var/lib/tftpboot/qam.config   DNCS(1)     CAQAMB425007001  142.7.0.1     00:00:00:00:00:02
/var/lib/tftpboot/qam.config   DNCS(1)     CAQAMB425014001  142.14.0.1    00:02:DE:81:F5:23
/var/lib/tftpboot/mqam.config  DNCS(1)     MQAMB425007001   142.7.10.1    00:00:00:00:00:03
/var/lib/tftpboot/mqam.config  DNCS(1)     MQAMB425014001   142.14.10.1   00:02:DE:83:3A:E4
/var/lib/tftpboot/gqam.config  DNCS(1)     GQAMB425007001   142.7.20.1    00:02:DE:82:3C:2F
/var/lib/tftpboot/gqam.config  DNCS(1)     GQAMB425007002   142.7.20.2    00:02:DE:82:90:FF
/var/lib/tftpboot/gqam.config  DNCS(1)     GQAMB425099001   142.99.20.1   00:1A:C3:D2:B0:EC
/var/lib/tftpboot/gqam.config  DNCS(1)     GQAMB425099002   142.99.20.2   00:02:DE:82:3C:61
/var/lib/tftpboot/gqam.config  DNCS(1)     GQAMB425099003   142.99.20.3   00:02:DE:82:81:8A
/var/lib/tftpboot/gqam.config  DNCS(1)     GQAMB425099004   142.99.20.4   00:02:DE:82:81:99
/var/lib/tftpboot/gqam.config  DNCS(1)     GQAMB425014001   142.14.20.1   00:02:DE:82:5A:4E
/var/lib/tftpboot/gqam.config  DNCS(1)     GQAMB425014002   142.14.20.2   00:1A:C3:D2:AD:B5
/var/lib/tftpboot/nc.config    DNCS(1)     NETCR425007001   142.7.60.1    00:00:00:00:00:0F

Tftp Config File Report for SITE='DNCS' for vodwater8 on Fri Mar 23 15:20:46 EDT 2018
================================================================================
DNCS:/var/lib/tftpboot/gqam.config droppoints:
                    BootCodePath gqam_host_boot_4_6_4.bin
                    ApplCodePath gqam_host_app_4_6_4.bin
                      RFCodePath gqam_rf_26.bin
                     BootCodePath gqam_input_h
```

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 EC.

1 As **dncs** user, type the following command to view the version number of the listTvtpConfigs utility.

```
[dncs@ecnextx9 Utilities]$ listTftpConfigs.ksh -V
```

Example Output:

```
listTftpConfigs.ksh: Version :  8.1.5
```

8

Monitor DHCTs with the DHCT Status Reporting Utility

Introduction

The DHCT Status Reporting Utility lets you monitor two-way communications between DHCTs and the headend.

DHCTs without two-way communications are said to be *non-responding*. Subscribers with non-responding DHCTs are unable to participate fully in the interactive features of the DHCT, while you are unable to maximize the revenue potential associated with a DHCT that can establish and maintain two-way communication.

The first section of this chapter, ***Defining Non-Responding DHCTs*** (on page 78), develops the definition of non-responding DHCTs from the point of view of our support engineers, and from your point of view.

Later 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. These include the following models: 85xx/45xx, 86xx/46xx, 87xx/47xx, and 9865.

In This Chapter

Defining Non-Responding DHCTs

The DHCT Status reporting utility helps you minimize the system impact caused by non-responding DHCTs.

We will provide two definitions of non-responding DHCTs, explore some of the reasons DHCTs cannot respond, and describe some of the utilities that are available for you 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 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, and 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.

Some examples of conditions that might exist in a subscriber's home that could cause the subscriber's DHCT to be a non-responder are:

- **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 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.

Return-Path Network Conditions

Some return-path network conditions that might cause a DHCT to become a non-responder are:

- **Laser clipping** — Lasers that assist in return path communications may be calibrated incorrectly, resulting in a distortion of the signal.
- **Excessive splitting of reverse path** — 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.

Notes:

- **Ingress** refers to noise from an external source.
- **Intermodulation** refers to noise generated from within the network.

Hardware Failures on the DBDS Network

Some ecnextx9 network components that could cause DHCTs to become non-responders should the network components fail are:

- **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 onto 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.

Configuration and Management Issues

Some conditions that might exist in the configuration of the ecnextx9 that may cause a DHCT to become a non-responder are:

- **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 EC database may fall out of synchronization with the database of the billing vendor. This loss of synchronization may cause the EC to try to poll DHCTs that are not actually in subscribers' homes.
- **Failure to run the updateOUI utility** — DHCTs that attempt to sign onto the network using an incorrect organizationally unique identifier (OUI) are unsuccessful.
- **Changes in RF plant performance** — Over time, changes in RF plant performance or customer wiring may require the DHCT to increase or decrease its transmit level. Failing to design the return path such that the DHCT has the ability to accommodate these changes (by adjusting the transmit level up or down) can lead to non-responding DHCTs.

What Activities Can Minimize the Non-Responding Condition?

This section summarizes some actions that you can take to reduce the non-responding condition on your 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.
  - Make sure 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 incorrectly calibrated laser 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 onto 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 you 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 tests and analyzes two-way communications between the DHCT and the headend. The DHCT Status Reporting Utility provides you with the following data:

- A current summary of the status of a system's DHCT population
- IP address data:
  - DHCT transmit levels
  - DHCT delay values
  - Currently loaded resident application and operating system

- 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 in homes of subscribers, labs, or ready to be immediately re-issued should have a status of in-service, two-way in the EC.

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 ecnextx9. The DHCT Status Reporting Utility tests and analyzes two-way communications between the DHCT and the headend.

The information in this section tells you how to access the user interface of the DHCT Status reporting utility and how to interpret the data it displays. Later sections provide instructions for running the various features included as part of the DHCT Status reporting utility.

DHCT Status Reporting Utility Interface

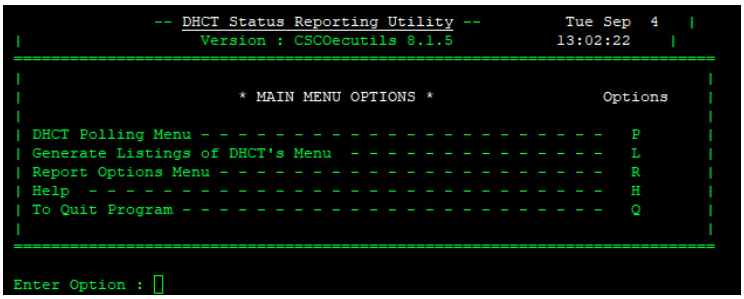
Accessing the Interface

1 As **dncs** user, change to the **/dvs/dncs/Utilities** directory.

```
[dncs@ecnextx9 ~]$ cd /dvs/dncs/Utilities
```

2 Type the following command to initiate the dhctStatus utility. The dhctStatus Main Menu displays.

```
[dncs@ecnextx9 Utilities]$ dhctStatus
```



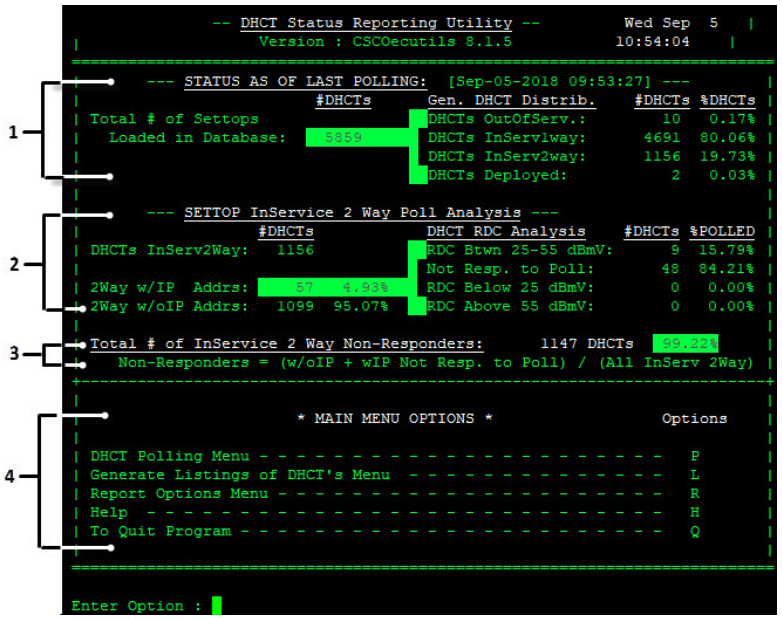
3 Go to the next section.

Understanding the Interface

Introduction

An example of the initial screen of the DHCT Status Reporting Utility is shown 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 document 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, you 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 set-tops (DHCTs) in the EC 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 not yet be staged or installed into subscribers' homes.

- In-service, two-way (**DHCTs InServ2way**) — DHCTs that support communication between the headend and the DHCT, and return communication. DHCTs need two-way communication capability to take full advantage of interactive services.

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

- In-service, one-way (**DHCTs InServ1way**) — DHCTs that 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 probably been staged and may have been installed in 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 that are usually in transit. These DHCTs are not technically out-of-service, but not quite in-service, either. These DHCTs have been staged and will soon be installed in the homes of subscribers. These DHCTs 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 you. Ultimately, your billing system dictates which DHCTs will generate revenue.

Section 2 - SETTOP InService 2 Way Poll 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 InServ 2 Way Poll Analysis** section includes:

- The number of DHCTs with two-way capability *with* an IP address (**2Way w/IP Addrs**) and the number of DHCTs with two-way capability *without* 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 EC 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.

- Higher than 55 dBmV (**RDC Above 55 dBmV**) — DHCTs respond to the poll, but respond at a transmit level higher than the optimum level.

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 InServ 2 Way Poll Analysis** section includes:

- The number of DHCTs with two-way capability *with* an IP address (**2Way w/IP Addrs**) and the number of DHCTs with two-way capability *without* 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 EC 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.
  - Higher than 55 dBmV (**RDC Above 55 dBmV**) — DHCTs respond to the poll, but respond at a transmit level higher than the optimum level.

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 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 Report*** (on page 102).

You can use the information provided by the DHCT Status Reporting Utility to identify modulators or demodulators associated with non-responding DHCTs. You can then take measures to adjust transmit levels so that they conform with our recommendations. This issue is discussed in more detail in ***DHCT Delay Value Report*** (on page 107).

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

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. Later sections in this section 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* (next in this document) for more information.

DHCT Status Reporting Utility Help Option

Displaying the Help Screen for the DHCT Status Reporting Utility

1 From the DHCT Status reporting utility screen, type **H** and then press **Enter**. The Main Menu Help Screen, which lists information that explains the options on the main menu, displays.

2 Read the description of the **P**, **L**, and **R** options and press **Enter** to return to the DHCT Status reporting utility window.

3 Press **Q** to exit the utility.

Note: Refer to later 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, and provides the mechanism for identifying and correcting non-responding issues.

By examining polling data, you can make changes to your system configuration that improve DHCT performance and reduce the number of non-responding DHCTs on a specific QPSK modulator or demodulator.

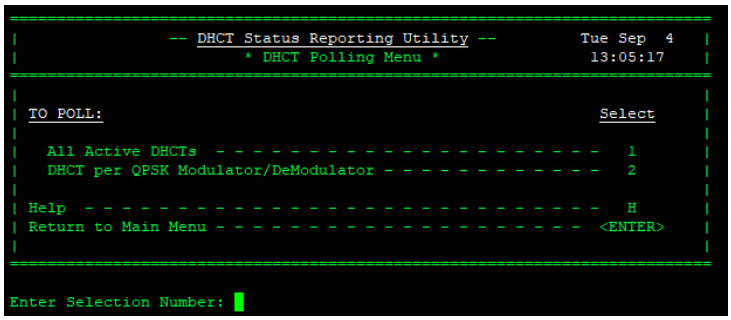
Poll DHCTs

Note: All procedures in this section assume that the DHCT Status reporting utility screen is open on the EC.

If the interface is not open, go to ***Accessing the Interface*** (on page 83).

Polling DHCTs

1 From the DHCT Status reporting utility screen, type **P** and press **Enter**. The DHCT Polling Menu screen opens.



2 Choose one of the following options:

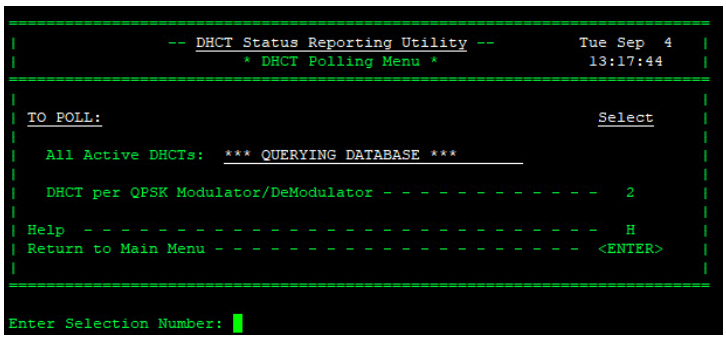
- To poll all active DHCTs on the network, go to *Polling All Active DHCTs*, next in this document.
- To poll DHCTs associated with a specific QPSK modulator or demodulator, go to ***Polling DHCTs per QPSK Modulator or Demodulator*** (on page 91).

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

Polling All Active DHCTs

1 From the DHCT Polling Menu screen, type **1** and press **Enter**. The DHCT Polling Menu screen updates to briefly display a **Querying Database** message in the **To Poll** area 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.

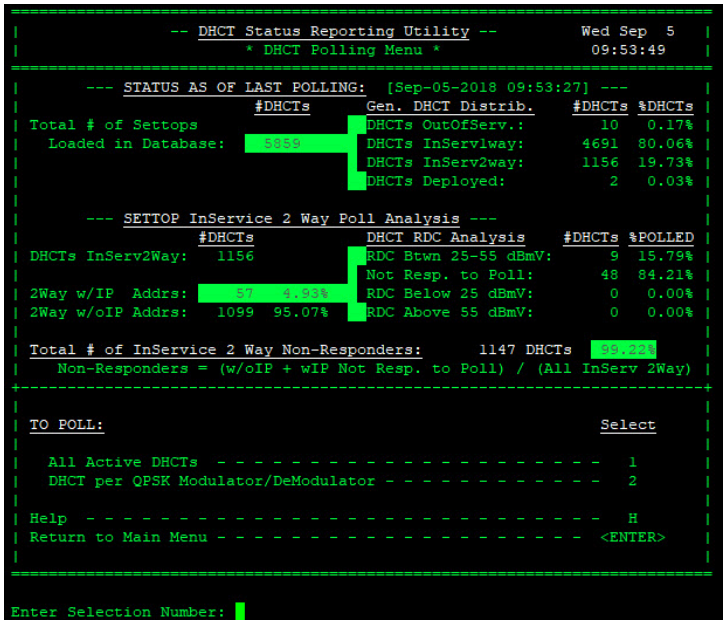


2 Type **U** (for update) and press **Enter**. The Status of Last Polling area of the window updates.

3 Type **all** and 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 you can compare the new data with data from the previous polling operation.
- The screen also displays the estimated poll completion time.
- The estimated completion time does not remain constant as the poll progresses. Type `all` and press **Enter** again to obtain the latest estimate.

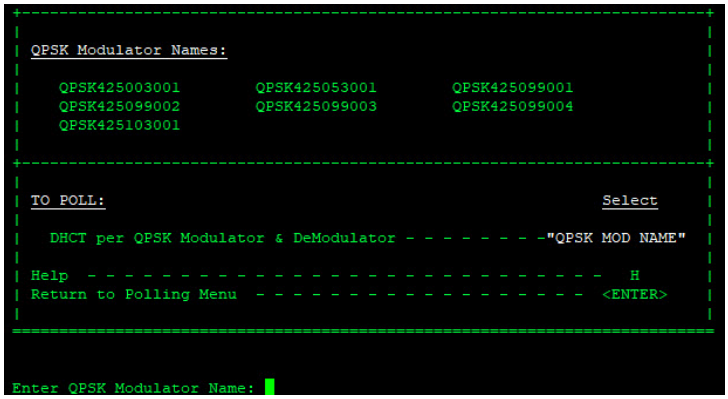


Polling DHCTs per QPSK Modulator or Demodulator

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

Results:

- The DHCT Polling Menu By QPSK Mod/DeMod window opens.
- The screen lists the QPSK modulators on the system.
- The **Enter QPSK Modulator Name** prompt appears.



2 At the prompt, copy and paste the name of a QPSK modulator you want to poll. Then press **Enter**.

Results:

- The DHCT Polling Menu By QPSK Mod/DeMod screen updates to list the QPSK demodulators associated with the selected modulator.
- 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 press **Enter** to poll DHCTs associated with a specific demodulator.

Note: The next two steps and results are based upon polling DHCTs by the 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 EC that tells the EC 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 a terminal window on the EC, type the following command and press **Enter**. The selected directory becomes the working directory.

Command Syntax:

```
cd /dvs/dncs/tmp/dhctStatus2/[DATE]/ALL/GR_REPORTS
```

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

Example: poll conducted on September 5, 2018, type and press **Enter**.

```
[dncs@ecnextx9 Utilities]$ cd
/dvs/dncs/tmp/dhctStatus2/20180905/ALL/GR_REPORTS
```

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

```
[dncs@ecnextx9 Utilities]$ cat NR_ModDeMod.txt
```

Example Output:

```
================================================================================
|                -- DHCT Status Reporting Utility --          Wed Sep  5    |
|                     ** Report Options Menu **                09:53:27     |
|                  - Non-Responder Report by Mod/DeMod -                      |
================================================================================
|       --- STATUS AS OF LAST POLLING:  [Sep-05-2018 09:53:27] ---           |
|                        #DHCTs       Gen. DHCT Distrib.     #DHCTs %DHCTs   |
| Total # of Settops                  DHCTs OutOfServ.:         10   0.17%   |
|   Loaded in Database:    5859       DHCTs InServ1way:       4691  80.06%   |
|                                     DHCTs InServ2way:       1156  19.73%   |
|                                     DHCTs Deployed:            2   0.03%   |
|                                                                             |
|       --- SETTOP InService 2 Way Poll Analysis ---                         |
|                   #DHCTs            DHCT RDC Analysis     #DHCTs %POLLED   |
| DHCTs InServ2Way:   1156            RDC Btwn 25-55 dBmV:       9  15.79%   |
|                                     Not Resp. to Poll:        48  84.21%   |
| 2Way w/IP  Addrs:     57   4.93%    RDC Below 25 dBmV:         0   0.00%   |
| 2Way w/oIP Addrs:   1099  95.07%    RDC Above 55 dBmV:         0   0.00%   |
|                                                                             |
| Total # of InService 2 Way Non-Responders:      1147 DHCTs   99.22%         |
|    Non-Responders = (w/oIP + wIP Not Resp. to Poll) / (All InServ 2Way)     |
+-----------------------------------------------------------------------------+
NOTE -  QPSK Mod/DeMods with a percent NonResponder greater than [20]
will be highlighted in "POLL".

QPSK Mod Name/          QPSK Mod    # of DHCTs   TTL   % DHCTs
DeMod ID                Identif.  Not Respond. DHCTs Not Respond.

 QPSK425003001             1          33        45     73.33%
   DeModID:  1                        33        41     80.49%
   DeModID:  0                         0         4      0.00%

 QPSK425053001             2          13        24     54.17%
   DeModID:  1                        13        24     54.17%

 QPSK425099001             5           0         0      0.00%

 QPSK425099002             6           0         0      0.00%

 QPSK425099003             7           0         0      0.00%

 QPSK425099004             8           0         0      0.00%

 QPSK425103001             3           2         2    100.00%
   DeModID:  1                         2         2    100.00%
```

Note: Refer to *Explanation of Output From Non-Responder Report*, next in this document, for an explanation of some of the findings revealed in this non-responder report.

Explanation of Output From Non-Responder Report

The top portion of the report 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.

The lower section of the report lists the number of non-responding DHCTs assigned to each modulator or demodulator, the total number of DHCTs supported by the modulator or demodulator, and 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: You may want to examine the following conditions to troubleshoot the significant percentage of non-responding DHCTs.

- 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, and a description of the type of data contained in the file.

Note: Type the following command and press **Enter** from the **/dvs/dncs/tmp/dhctStatus2/[DATE]/ALL** directory to view the output.

- ALLDHCTS
- ALLDHCTSmacs_Deployed
- ALLDHCTSmacs_IS1WAY
- ALLDHCTSmacs_IS2WAY
- ALLDHCTSmacs_OutOfService
- DL_MODDEMOD_DATA
- FINAL_RPT
- macTwoWay
- nonResponders
- NR_MODDEMOD_DATA
- NR_TYPEREV_DATA
- pollTwoWay

- pollTwoWay.log
- pollTwoWay_wIP
- pollTwoWay_woIP
- TL_MODDEMOD_DATA

List DHCTs

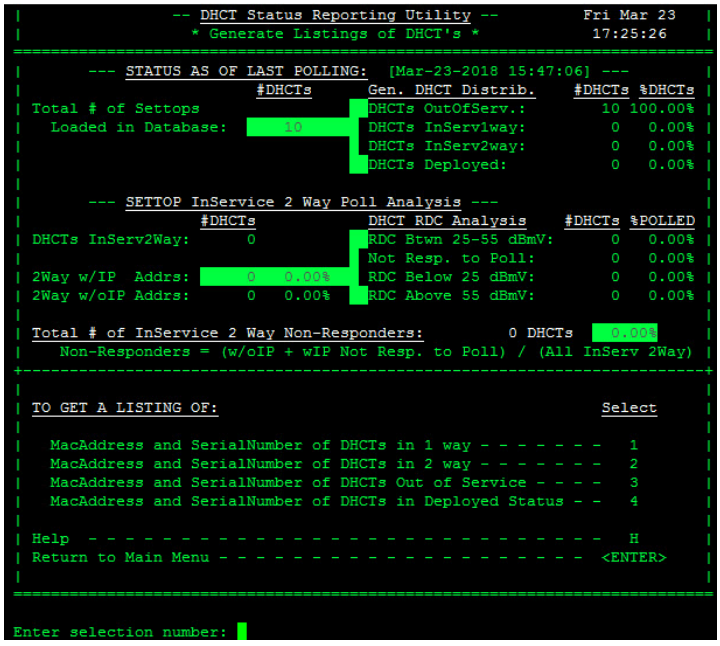
The DHCT Status reporting utility lets you query the database for a listing of MAC addresses and serial numbers of DHCTs with a specific status. The utility can generate a list for DHCTs with the following statuses:

- **DHCTs with a 1-way status** — DHCTs that support communication between the headend and the DHCT.
- **DHCTs with a 2-way status** — DHCTs that support communication between the headend and the DHCT, and return communication between the DHCT and the headend.
- **DHCTs with an Out-of-Service status** — 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** — DHCTs in a transition period. They have been staged and are waiting to be placed 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 EC. Instead, output is written to a file in the **/dvs/dncs/tmp/dhctStatus2/[DATE]/ALL** directory of the EC, where can view it at your convenience.

Generate a Listing of DHCTs

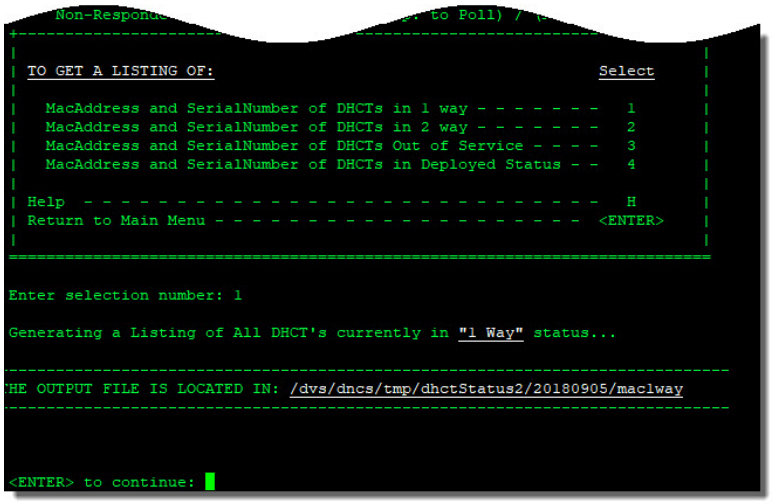
1 From the DHCT Status reporting utility screen, type **L** and press **Enter**. The Generate Listings of DHCTs screen appears.



2 Choose one of the following options:

- To generate a listing of DHCTs with a 1-way status, go to the next step.
- To generate a listing of DHCTs with a 2-way status, go to Step 6.
- To generate a listing of DHCTs with a status of Out-of-Service, go to Step 9.
- To generate a listing of DHCTs with a status of Deployed, go to Step 12.

3 Type **1** and press **Enter** to generate a listing of DHCTs with a one-way status. The system displays a message that indicates the directory location of the output file.



4 Go to the next section for instructions on how to view the contents of the output file generated by the DHCT Status Reporting Utility.

5 Press **Enter** to continue.

6 Type **2** and press **Enter** to generate a listing of DHCTs with a two-way status. The system displays a message that indicates the directory location of the output file.

7 Go to the next section for instructions on how to view the contents of the output file generated by the DHCT Status Reporting Utility.

8 Press **Enter** to continue.

9 Type **3** and press **Enter** to generate a listing of DHCTs with a status of out-of-service. The system displays a message that indicates the directory location of the output file.

10 Go to the next section for instructions on how to view the contents of the output file generated by the DHCT Status Reporting Utility.

11 Press **Enter** to continue.

12 Type **4** and press **Enter** to generate a listing of DHCTs with a status of deployed. The system displays a message that indicates the directory location of the output file.

13 Go to the next section for instructions on how to view the contents of the output file generated by the DHCT Status Reporting Utility.

View the Output Files

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

1 As **dncs** user, enter the following command to go to the directory where the output files are saved.

Command Syntax:

```
cd /dvs/dncs/tmp/dhctStatus2/[DATE]
```

Example:

```
[dncs@ecnextx9 Utilities]$ cd
/dvs/dncs/tmp/dhctStatus2/20180905
```

2 Type the following command and press **Enter** to view a list of DHCTs, by MAC address, in one of the output files.

Command Syntax:

```
less [filename]
```

Example:

```
[dncs@ecnextx9 Utilities]$ less mac1way
```

Notes:

- 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.

The Reporting Option

The DHCT Status reporting utility includes several reports that summarize various types of DHCT polling data.

You 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 and detailed instructions on running the reports.

Description of Reports

DHCT Status Reporting Utility Reports

The DHCT Status reporting utility includes the following reports that you can generate to summarize various DHCT polling data:

- **Non-Responder Reports (NR) —** DHCTs with an IP address that fail to respond to poll requests from the EC 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, you 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 (TL) —** 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, you can quickly spot when network conditions are preventing effective communication between the headend and the DHCTs.
- **DHCT Delay Value Report (DL) —** 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 checks 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, you can spot conditions under which it may be advantageous to configure a QPSK modulator for the QPSK Range Extension Feature.

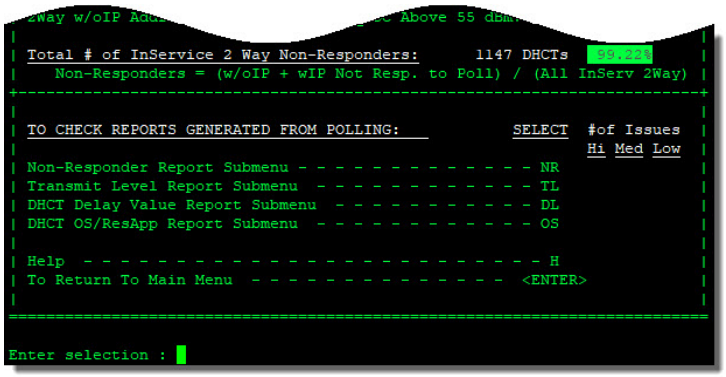
Note: The QPSK Range Extension Feature allows DHCTs to sign on to the system and operate properly at extended distances from the QPSK modulator.

- **DHCT OS/ResApp Report (OS) —** 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

1 From the main menu of the DHCT Status reporting utility, type **R** and press **Enter**. The Report Options Menu screen appears.



2 Type **H** and 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 Press **Enter** to return to the Report Options Menu screen.

4 Choose one of the following options:

- To generate DHCT non-responder reports, go to *Non-Responder Reports*, next in this document.
- To generate a DHCT transmit level report, go to ***DHCT Transmit Level Saturation Report*** (see "***DHCT Transmit Level Report***" on page 102).
- To generate a DHCT delay value report, go to ***DHCT Delay Value Saturation Report*** (on page 107).
- 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 110).

Non-Responder Reports

Generating Non-Responder Reports

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

1 From the main menu of the DHCT Status Reporting Utility, type **NR** and 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 - - - - - - (1)**
- **Non-Responders by DHCT Type/Rev - - - - - - - - - - (2)**

2 Choose one of the following options:

- To generate a Non-Responder Report for DHCTs based upon QPSK modulator and demodulator ID, go to the next step.
- 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** and 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** and 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.

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 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 on these measurements, the QPSK modulator 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 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.

You can use the DHCT Transmit Level Saturation Report to view data pertaining to the transmission levels of DHCTs on the network and 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 (SNR) is a measurement of signal strength relative to background noise. Competing transmissions from other DHCTs on the network tend to increase the background noise, decreasing the SNR.
- 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 Report

1 Maximize the window.

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

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

3 Go to *Understanding the DHCT Transmit Level Saturation Report* (next in this document) for help in interpreting the data displayed in the report.

Understanding the DHCT Transmit Level Report

There are two parts to the DHCT Transmit Level Report:

- A graphical representation of the distribution of the various transmission levels of DHCTs assigned to each QPSK modulator on the system.

  Note: See *Graphical Distribution of DHCT Transmission Levels* (next in this document) for information on interpreting the graphical representation.

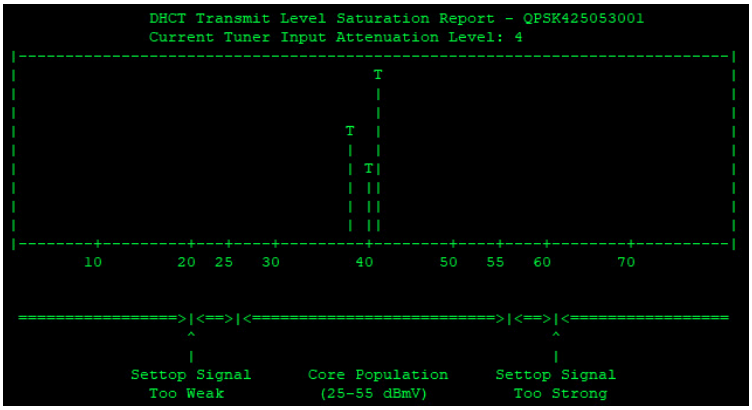
- A numerical analysis of the graphical representation of the various transmission levels of DHCTs assigned to each QPSK modulator on the system.

  Note: Read ***Transmit Level Analysis*** (on page 104) for information on interpreting the numerical analysis.

Graphical Distribution of DHCT Transmit Levels

The first part of the DHCT Transmit Level 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.



We 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 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; all of the DHCTs assigned to this QPSK modulator transmit within our recommended range of 25 to 55 dBmV.

Notice the **Current Tuner Input Attenuation Level** of **4** 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 EC. A Current Tuner Input Attenuation Level of 4 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 Report provides a chart showing the detailed breakdown of the graphical data displayed in the previous topic.

```
                                        Transmit Level Breakdown
QPSK Mod Name      ID  Avg. Md      20db   25db   30db   50db   55db   60db
----------------- --- ----- -- <------+------+------+------+------+------+-------->
QPSK425053001       2 40.22 40      0|     0|     0|     9|     0|     0|     0
 DMod:  1             40.22 40      0|     0|     0|     9|     0|     0|     0
                          <------+------+------+------+------+------+-------->
```

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 QPSK425053001 modulator is configured with one demodulator.

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

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 basically at the midpoint (40 dBmV) of our recommended range of 25 to 55 dBmV.

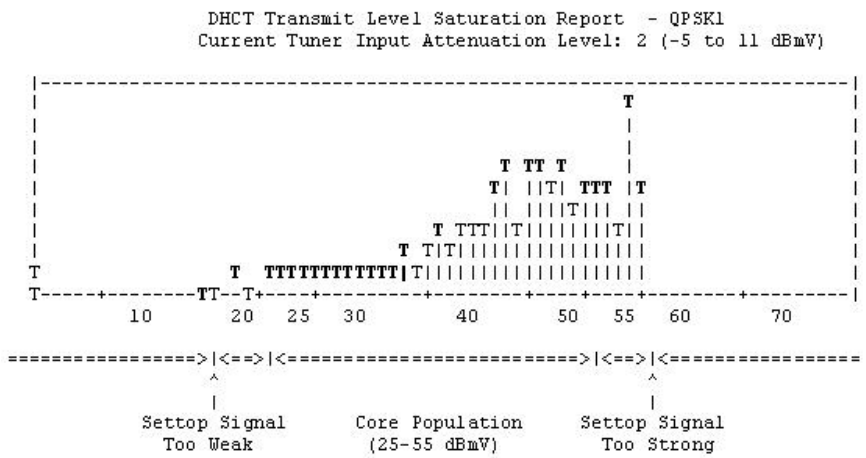
Examples of Systems Needing Recalibration

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*** (next in this document) 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 106) 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.

Also, 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.

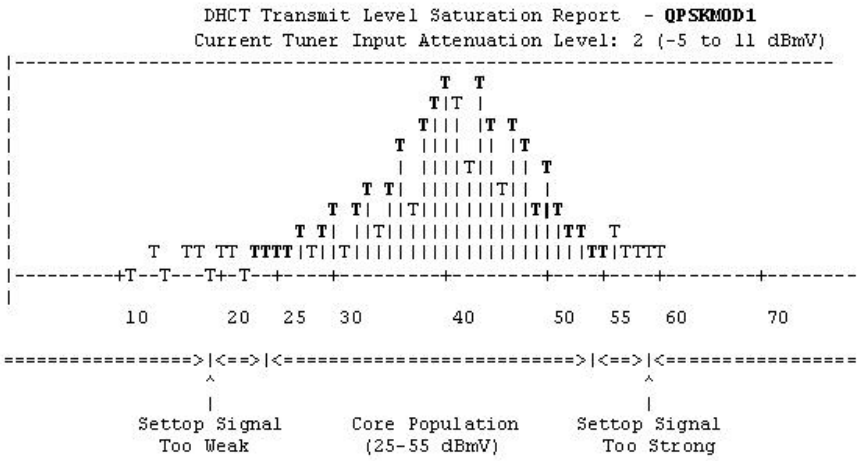
			Transmit Level Breakdown					
QPSK Mod Name	ID	Avg. Md	20db	25db	30db	50db	55db	60db
QPSK1	13	50.90 52	5	7	27	3549	2250	2421	0
DMod: 1		49.50 50	1	1	11	833	362	413	0
DMod: 2		50.97 52	0	3	0	774	531	506	0
DMod: 3		50.20 51	1	2	11	583	357	336	0
DMod: 4		52.41 53	0	1	5	649	525	725	0
DMod: 5		50.99 51	3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

You 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 you 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. You 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
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		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 Report

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

Generating the DHCT Delay Value Report

1 Maximize the window.

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

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

3 Go to *Understanding the DHCT Delay Value Saturation Report* (next in this document) for information on interpreting the data displayed in the report.

Understanding the DHCT Delay Value Saturation Report

There are two parts to the DHCT Delay Value Report:

- A graphical representation of the distribution of the various delay values of DHCTs assigned to each QPSK modulator on the system

  Note: See *Graphical Distribution of DHCT Delay Values* (next in this document) for information on 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

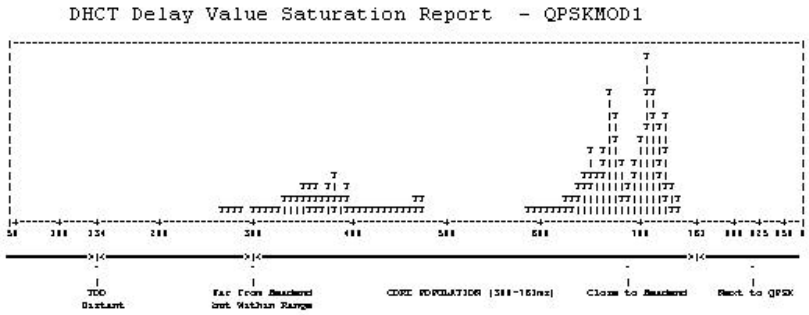
  Note: See ***Delay Value Analysis*** (on page 108) for information on interpreting the numerical analysis.

Graphical Distribution of DHCT Delay Values

The first part of the DHCT Delay Value 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 Report provides a detailed breakdown of the graphical data displayed in Graphical Distribution of DHCT Delay Values, earlier in this section.

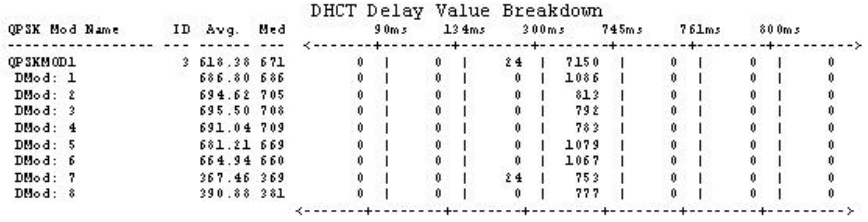
This part of the report contains the following data:

- 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
QPSKMODl	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 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 DHCTs to sign onto 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 ecnextx9 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

1. Maximize the window.

   Note: The data in the DHCT OS and ResApp Evaluation by Set Top Type and Rev Report displays best if the window is maximized.
2. From the main menu of the DHCT Status utility, type **OS** and press **Enter**. The system generates the DHCT OS and ResApp Evaluation by Set Top Type and Rev Report.
3. Press **Enter** as often as required to scroll through the entire report.

9

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

Introduction

The mvsrcid utility allows you to convert existing EC source IDs to TV Guide source IDs, or to update existing TV Guide source IDs.

Using this utility, you can 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

Display the Help Window and Version Number of the mvsrcid Utility

Displaying the Help Window of the mvsrcid Utility

1 As **root** user, type the following command to source the environment.

```
[root@ecnextx9 ~]# . /dvs/dncs/bin/dncsSetup
```

2 Type the following command to display the help window for the **mvsrcid** utility.

```
[root@ecnextx9 Utilities]# mvsrcid.sh -h
```

Output:

```
-------------------------------------------
Tue Jan 23 16:24:34 EST 2018
-------------------------------------------

/mvsrcid.sh Version 8.1.5

NAME
        mvsrcid.sh - allows the ROOT operator to convert existing sourceIDs
on
        the EC 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 responsibility 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 EC), 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.
        -V|v    Print current version of this command.
-------------------------------------------
Tue Jan 23 16:24:34 EST 2018
-------------------------------------------
```

Displaying the Version Number of the mvsrcid Utility

1 Type the following command and press **Enter**. The system displays the version number of the mvsrcid utility.

```
[root@ecnextx9 Utilities]# mvsrcid.sh -v
```

Example output:

```
-------------------------------------------
Tue Jan 23 21:28:31 UTC 2018
-------------------------------------------
./mvsrcid.sh Version 8.1.5
-------------------------------------------
Tue Jan 23 21:28:31 UTC 2018
-------------------------------------------
```

Back Up the Database Tables

The **-b** option of the mvsrcid utility allows you to back up those database tables that are affected by the mvsrcid utility, before the utility generates 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, we 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 let you 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.

1 As **root** user, type the following command to execute the **mvsrcid** utility with the **-b** option.

```
[root@ecnextx9 ~]# mvsrcid.sh -b
```

Example Output:

```
-------------------------------------------
Tue Jan 23 21:34:07 UTC 2018
-------------------------------------------

Database selected.
41 row(s) unloaded.
58 row(s) unloaded.
89 row(s) unloaded.
70 row(s) unloaded.
28 row(s) unloaded.
17 row(s) unloaded.
29 row(s) unloaded.
33 row(s) unloaded.
0 row(s) unloaded.
0 row(s) unloaded.

Database closed.

tar: Removing leading `/' from member names

/dvs/backups/samservices.unl
/dvs/backups/pdsourceident.unl
/dvs/backups/pdsource.unl
/dvs/backups/pdsrcinfo.unl
/dvs/backups/pdsourcesecurity.unl
/dvs/backups/applicationurl.unl
/dvs/backups/pdsegment.unl
/dvs/backups/displaychannels.unl
/dvs/backups/sdv_source.unl
/dvs/backups/pdnonsasource.unl

You just requested the -b option to be executed, which backups all tables
related to converting the existing sources to new sources before the
conversion takes place. The backup file will be located in the /dvs/backup
directory The format of the name of the backup file is:
      srcidbackup_mmddyyyyhhmmss.list:

*** The file /dvs/backups/srcidbackup_01232018213407.tar contains a backup of
the tables that will be changed prior to the conversion ***

-------------------------------------------
Tue Jan 23 21:34:07 UTC 2018
-------------------------------------------
```

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

- The naming convention of the backup file is **srcidbackup_mmddyyyyhhmmss.list** (for example, srcidbackup_01232018213407.tar) and it is saved to the **/dvs/backups/** directory.
- 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.

  Important: Do NOT use the *-r* option without calling Cisco Services first. 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 are affected 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. Complete the following steps to generate this file.

1 As **root** user, type the following command to generate a file that contains source IDs that need to be converted to TV Guide source IDs.

```
[root@ecnextx9 ~]# mvsrcid.sh -g
```

Example Output:

```
-------------------------------------------
Tue Jan 23 21:49:57 UTC 2018
-------------------------------------------

Database selected.
866 row(s) unloaded.

Database closed.

You just requested the -g option to be executed, which creates a file with
the list of SA-sources that need to be converted. This file will then be
given to TVGuide so they can fill in the corresponding matching TVguide
sourceIDs at the end of the file. The name and content of the generated file
is:

      sasourceids_mmddyyyhhmmss.list:
          SA-shortdescription,SA-longdescription,SA-appid,SA-sourceId,

*** The file sasourceids_01232018214957.list contains the list of sources
that
need to be mapped to TVGuide sources ***

-------------------------------------------
Tue Jan 23 21:49:57 UTC 2018
-------------------------------------------
```

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 (for example, /dvs/dncs/Utilities).
- The file contains the short description, the long description, the application ID, and the current source ID, all separated by commas.

2 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.

3 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 has been edited, either by TV Guide engineers or someone on-site who is familiar with TV Guide source IDs, and returned to the headend. In addition, you have renamed the edited sasourceids_mmddyyyyhhmmss.list file to easily differentiate it from the original sasourceids_mmddyyyyhhmmss.list file.

This section provides procedures to update the database tables.

Note: For purposes of an example in this procedure, assume that the edited and renamed file is called **sasourceids_implemented_01232018214957.list**.

Inspecting the TV Guide Source IDs

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.

1 As **root** user, type the following command to display the data with which the database tables will be updated.

Command Syntax:

```
mvsrcid.sh -i [name of edited file]
```

Note: Substitute the name of the edited sasourceids_mmddyyyyhhmmss.list file for [name of edited file].

Example:

```
[root@ecnextx9 Utilities]# mvsrcid.sh -i
sasourceids_implemented_01232018214957.list
```

Example Output:

```
------------------------------------------------
Tue Jan 23 16:34:34 EST 2018
------------------------------------------------

Database selected.
Temporary table created.
Index created.
Index created.

3 row(s) loaded.

shortd  longd                 appid  sa_sourceid  tvg_sourceid
BET     BET                      20         4103          1066
CSPAN   CSPAN                    27         4105          1999
CNN     Cable News Network       24         4110          1955

3 row(s) retrieved.

Routine created.
Routine executed.
Routine dropped.
```

```
Database closed
*** Please check file sourceconversion_01232018214957.log for results ***
```

2 Inspect the output.

Stopping the cron Jobs on the EC

1 As **admin** user, type the following command to stop the crond service.

```
[admin@ecnextx9 ~]$ sudo systemctl stop crond
```

2 Confirm that the cron jobs have stopped by typing the following command. The output should resemble the following:

```
[admin@ecnextx9 ~]$ systemctl status crond
```

Example Output:

```
Redirecting to /bin/systemctl status crond.service
* crond.service - Command Scheduler
   Loaded: loaded (/usr/lib/systemd/system/crond.service; enabled; vendor
preset: enabled)
   Active: inactive (dead) since Mon 2018-03-26 08:55:12 EDT; 3s ago
 Main PID: 1511 (code=exited, status=0/SUCCESS)

Mar 26 08:00:01 berlin3 CROND[29207]: (root) CMD (/usr/lib64/sa/sa1 1 1)
Mar 26 08:01:01 berlin3 CROND[29247]: (root) CMD (run-parts /etc/cron.hourly)
Mar 26 08:10:01 berlin3 CROND[29649]: (root) CMD (/usr/lib64/sa/sa1 1 1)
Mar 26 08:20:01 berlin3 CROND[30080]: (root) CMD (/usr/lib64/sa/sa1 1 1)
Mar 26 08:30:01 berlin3 CROND[30592]: (root) CMD (/usr/lib64/sa/sa1 1 1)
Mar 26 08:30:01 berlin3 CROND[30593]: (root) CMD ([ -x
/dvs/admin/passwd_check.pl ] && ( /... ))
Mar 26 08:40:01 berlin3 CROND[31076]: (root) CMD (/usr/lib64/sa/sa1 1 1)
Mar 26 08:50:01 berlin3 CROND[31599]: (root) CMD (/usr/lib64/sa/sa1 1 1)
Mar 26 08:55:12 berlin3 systemd[1]: Stopping Command Scheduler...
Mar 26 08:55:12 berlin3 systemd[1]: Stopped Command Scheduler.
Hint: Some lines were ellipsized, use -l to show in full.
```

Stopping the System Processes

1 Close all Web UIs.

2 As **dncs** user, type the following commands to stop the system processes.

```
[dncs@ecnextx9 ~]$ appStop
[dncs@ecnextx9 ~]$ dncsStop
```

3 Type the following command shut down the Initd processes.

```
[dncs@ecnextx9 ~]$ appKill
[dncs@ecnextx9 ~]$ dncsKill
```

4 Type the following command to determine if the processes have stopped. The processes are stopped when there are no EC processes listed in the output.

```
[dncs@ecnextx9 ~]$ pgrep -fl dvs
```

5 If the output from the command in the previous step shows that processes are running, do the following:

a As **admin** user, type the following command to stop the running processes.

Command Syntax:

```
sudo kill [PID1] [PID2] [PID3]....[PIDn]
```

Note: PID is the process ID of a running process(es).

Example:

```
[admin@ecnextx9 ~]$ sudo kill 7069 7287
```

Note: If the kill command is unsuccessful, contact Cisco Services for assistance.

Ensuring No Database Sessions are Active on the EC

1 Close all windows and Web UIs that are open except for a terminal window where you are logged in as the **admin** user.

2 Type the following command and press **Enter**. The system lists running processes that use the tomcat server.

```
[admin@ecnextx9 ~]$ systemctl status tomcat
```

3 Is the tomcat server running?

- If **yes**, type the following command and press **Enter** to stop the tomcat service.

  ```
  [ecadmin@ecnextx9 ~]$ sudo systemctl stop tomcat
  ```

- If **no**, go to Step 5.

4 Type the following command and press **Enter** to confirm that the tomcat server has stopped:

```
[admin@ecnextx9 ~]$ systemctl status tomcat
```

5 Type the following command and press **Enter**. The system lists running UI processes.

```
[admin@ecnextx9 ~]$ ps -ef | grep UI
```

6 Are any UI processes running (**dbUIServer** and **podUIServer**)?

- If **yes**, as **dncs** user, type the following command and press **Enter**:

  ```
  [dncs@ecnextx9 ~]$ /dvs/dncs/bin/stopSOAPServers
  ```

- If **no**, go to Step 9.

7 Type the following command and press **Enter** to confirm that UI processes have stopped:

```
[dncs@ecnextx9 ~]$ ps -ef | grep UI
```

Note: If any Web UI processes are still running, repeat the previous step.

8 Are any **ui** processes running?

- If **yes**, as **admin** user, type the following command and press **Enter** for any console ui process that is still running:

  ```
  [admin@ecnextx9 ~]$ sudo kill [PID]
  ```

  Notes:

  – The PID to kill is in the second column in the output from Step 7.

  – If the kill command is unsuccessful, contact Cisco Services.

- If **no**, go to the next step.

9 As **root** user, enter the following command to source the environment.

```
[root@ecnextx9 ~]#. /dvs/dncs/bin/dncsSetup
```

10 Type the following command and press **Enter**:

```
[root@ecnextx9 ~]# showActiveSessions
```

Result: One of the following messages appears:

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

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

- If **yes**, follow these instructions:

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

  ```
  [root@ecnextx9 ~]# killActiveSessions
  ```

  b Type the following command again and press **Enter**:

  ```
  [root@ecnextx9 ~]# showActiveSessions
  ```

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

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

- If **no**, go to the next step.

12 As **dncs** user, type the following commands and press **Enter**. The system terminates the Initd processes they are still running.

```
[dncs@ecnextx9 ~]$ appKill
[dncs@ecnextx9 ~]$ dncsKill
```

13 Wait a few moments, type the following command and press **Enter**. The system reports whether any Initd processes are still running.

```
[dncs@ecnextx9 ~]$ ps -ef | grep Initd
```

Note: If the either of both of the Initd processes are still running, repeat Step 12.

Terminating the dhctStatus Polling Operation

1. As **dncs** user, type the following command and press **Enter**. The system reveals whether there are any instances of the dhctStatus process running.

   ```
   [dncs@ecnextx9 ~]$ ps -ef |grep dhctStatus
   ```

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

   - If **yes**, go to the next step to shut down the polling operations.
   - If **no**, skip the rest of this procedure and go to the next section.

3. Type the following command and press **Enter** to change to the **/dvs/dncs/Utilities** directory.

   ```
   [dncs@ecnextx9 ~]$ cd /dvs/dncs/Utilities
   ```

4. Enter the following command to display the **dhctStatus** menu.

   ```
   [dncs@ecnextx9 Utilities]$ dhctStatus
   ```

5. To terminate the polling operation, follow these instructions:

   a Type **P** and press **Enter**. The system displays a polling menu.

   b Type **T** and press **Enter**. The system terminates the polling operation.

   c Press **Enter** to return to the main menu.

   d Type **q** and press **Enter** to exit the menu.

6. Type the following command and press **Enter** to determine whether all of the processes have been terminated:

   ```
   [dncs@ecnextx9 Utilities]$ ps -ef | grep dhctStatus
   ```

7. Type the following command and press **Enter** for any process ID displayed in the results from Step 6.

   ```
   [dncs@ecnextx9 Utilities]$ kill [process ID]
   ```

   Notes:

   - The process ID(s) to kill is/are located starting with the second column of the output from Step 6.
   - If the kill command is unsuccessful, contact Cisco Services.

8. Repeat Steps 6 and 7 for any process that is still active.

Removing the signonCount Utility from System Memory

1. Type the following command and press **Enter**. A list of EC processes and process IDs display on the screen.

   ```
   [dncs@ecnextx9 ~]$ ps -ef | grep signonCount
   ```

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

   - If **yes**, continue with the next step.
   - If **no**, skip the rest of this procedure and go to the next section.

3. As **dncs** user, type the following command and press **Enter**:

   ```
   [dncs@ecnextx9 ~]$ signonCount uninstall
   ```

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

4. Type the following command and press **Enter**. A list of EC processes and process IDs display on the screen.

   ```
   [dncs@ecnextx9 ~]$ ps -ef | grep signonCount
   ```

5. To kill any remaining processes, type the following command and press **Enter**:

   ```
   [dncs@ecnextx9 ~]$ pkill signonCount
   ```

6. Type the following command and press **Enter** to ensure all the processes are terminated.

   ```
   [dncs@ecnextx9 ~]$ ps -ef | grep signonCount
   ```

7. Repeat Steps 5 and 6 for any process that continues to be displayed.

   Note: The system should only display the grep process.

Stopping 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 EC, you can now update the database.

1. As **root** user, type the following command to change to the **/dvs/dncs/Utilities** directory.

   ```
   [root@ecnextx9 ~]$ cd /dvs/dncs/Utilities
   ```

2. Type the following command and press **Enter**. The system loads the relevant database tables with TV Guide source IDs.

   Command Syntax:

   ```
   mvsrcid.sh -u [name of edited file]
   ```

   Example:

   ```
   [root@ecnextx9 Utilities]# mvsrcid.sh -u
   sasourceids_implemented_01032018161728.list
   ```

Example Output:

```
------------------------------------------------
Thursday, January 3, 2018  2:16:08 PM EDT
------------------------------------------------

Database selected.
Temporary table created.
Index created.
Index created.

3 row(s) loaded.

shortd  longd                 appid  sa_sourceid  tvg_sourceid
BET     BET                     20         4103          1066
CSPAN   CSPAN                   27         4105          1999
CNN     Cable News Network      24         4110          1955

3 row(s) retrieved.

Routine created.
Routine executed.
Routine dropped.

Database closed

*** Please check file sourceconversion_01032018163158.log for results ***
```

Restarting the cron Jobs on the EC

1. Type the following command to check the current status of the **crond** service.

   ```
   [root@ecnextx9 Utilities]# systemctl status crond
   ```

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 section.
   - If **no**, continue with the next step.
3. Type the following command to start the **crond** jobs.

   ```
   [root@ecnextx9 Utilities]# systemctl start crond
   ```

4. Repeat Step 1 to verify that the **crond** service is running.

   ```
   [root@ecnextx9 Utilities]# systemctl status crond
   ```

Restarting the EC

1. As **dncs** user, type the following commands to restart the Informix database, the SOAPServers, and the EC processes.

   ```
   [dncs@ecnextx9 ~]$ dncsStart
   [dncs@ecnextx9 ~]$ appStart
   ```

2. From a supported Web browser, log into the EC Web UI. The Administrative Console opens.
3. Verify that the processes are all green.
4. If any processes continue to display yellow or red after several minutes, try to restart each individually by selecting the process and clicking **Start**.

`

5 Do all processes display green indicators?

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

A Workaround for Sites Experiencing Lost Video

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

1 From the EC Administrative Console, click the **Navigation** icon, , and select **App Interface Modules > SAM Config**. The SAM Configuration window appears.

2 In the space provided, record the current setting for the **Update Timer**.

Update Timer: _____

3 Change the **Update Timer** to **60** seconds. This change forces the SAM to update faster.

4 Click **Save** and close the SAM Configuration window.

5 Click the **Navigation** icon, , again and select **App Interface Modules > SAM Service**. The SAM Service List window appears.

6 Using the **Filter** feature, display SAM services.

7 Select one of the SAM services and click **Edit**. The Edit SAM Service window opens.

8 Click **Save**. You are returned to the SAM Service List window.

Result: Normal video should now return within 2 or 3 minutes.

9 Close the SAM Service List window.

10 Click the **Navigation** icon, , and select **App Interface Modules > SAM Config**. The SAM Configuration window appears.

11 Using the setting you recorded in Step 2, set the Update Timer setting back to its original value.

12 Click **Save**.

10

Examine the podData File with the podDataChk Utility

Introduction

Using the podDataChk utility, you can examine the contents of the podData file that is stored in the /dvs/dvsFiles/BFS/DNCS/podServer directory.

The podData file contains data that is communicated to CableCARD modules through the BFS carousel, such as CableCARD configuration data, and data that pertains to the authorization and deauthorization of copy protection for CableCARD modules.

The podDataChk utility helps you determine what CableCARD/host (Pod/Host) pairs are included in the podData file, and are transmitted using the BFS carousel.

Because the podData file is limited to 1,500 records, the podDataChk utility helps you monitor the growth of the file. If the podData file grows 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 previously.

Each time the podDataChk utility runs, it generates the /dvs/dvsFiles/BFS/DNCS/podServer/podData.txt file, which contains a complete summary of the data in the podData file. You can then use the LINUX *less* 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 EC. 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

1 As **dncs** user, type one of the following commands to display the help window for the **podDataChk** utility.

```
[dncs@ecnextx9 Utilities]$ podDataChk -?
[dncs@ecnextx9 Utilities]$ poddataChk -h
```

Example Output:

```
 usage: podDataChk [options]
No options: Read <podData> file from the current location and
            write output <podData.txt> file to the current location.
Standard options:
  -c              display the count of records for each section
  -?              show this message
  -h              show this message
  -s              display CCardServer data
  -f <FILE>       use FILE instead of podData file
  -m <POD mac>    display the HOST id for this POD, if found
  -H <host id>    display the POD mac for this Host, if found
```

Count the Records in the podData File

The podDataChk utility sorts the data in the podData file into various categories, or sections:

- **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.
- **Pod/Host Pairs Auth** section — Contains the MAC addresses of CableCARD modules that have active copy protection authorization.
- **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 EC.

The podDataChk utility also generates a detailed summary of the podData file and writes that summary to the /dvs/dvsFiles/BFS/DNCS/podServer/podData.txt file.

1 As **dncs** user, type the following command to make the /dvs/dvsFiles/BFS/DNCS/podServer directory the working directory.

Command Syntax:

```
cd /dvs/dvsFiles/BFS/DNCS/podServer
```

Example:

```
[dncs@ecnextx9 ~]$ cd /dvs/dvsFiles/BFS/DNCS/podServer
```

2 Type the following command to display the record count from all three sections of the **podData** file.

```
[dncs@ecnextx9 podServer]$ podDataChk -c
```

Example Output:

```
processing file <podData> ...
*********************************
Forced key refresh count = 0
Auth count               = 0
Deauth count             = 1
Note: Output file <podData.txt> created. Review for more info.
```

3 Type the following command to view the complete contents of the **podData.txt** file.

```
[dncs@ecnextx9 podServer]$ less podData.txt
```

Example Output:

```
*************** TIMESTAMP SECTION ***************
Time stamp   = 1514992538 (01/03/2018 10:15:38)
File version = 805
************** GLOBAL DATA SECTION **************
Max key session period = 10
Server IP              = 204.25.1.1
Server Port            = 13830
********** POD/HOST PAIRS AUTH SECTION **********
Num of records = 0
********* POD/HOST PAIRS DEAUTH SECTION *********
Num of records = 1
      POD MAC           Host Id
      -------           -------
00:21:BE:2E:25:C5, 0-380-169-302-854
***************** CRC32 SECTION *****************
CRC32 = 402937769
```

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 EC and to the /dvs/dvsFiles/BFS/DNCS/podServer/podData.txt file.

1 As **dncs** user, type the following command to display the configuration data for the CableCARD server.

```
[dncs@ecnextx9 podServer]$ podDataChk -s
```

Example Output:

```
processing file <podData> ...
*******************************
Server IP    = 204.54.1.1
Server Port  = 13830
Note: Output file <podData.txt> created. Review for more info.
```

2 Type the following command to view the complete contents of the **podData.txt** file:

```
[dncs@ecnextx9 podServer]$ less podData.txt
```

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 EC, and to the /dvs/dvsFiles/BFS/DNCS/podServer/podData.txt file.

1 As **dncs** user, type the following command to display the host ID for the specified CableCARD module, provided the CableCARD module/host pair is contained in the podData file.

Command Syntax:

```
podDataChk -m [MAC Address of CableCARD module]
```

Example:

```
[dncs@ecnextx9 podServer]$ podDataChk -m 00:21:BE:2E:25:C5
```

Example Output:

```
processing file <podData> ...
Cable card with MAC <00:21:BE:2E:25:C5> deauthorized to Host = 0-380-169-302-854
Note: Output file <podData.txt> created. Review for more info.
```

2 Type the following command to view the complete contents of the **podData.txt** file:

```
[dncs@ecnextx9 podServer]$ less podData.txt
```

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 EC, and to the /dvs/dvsFiles/BFS/DNCS/podServer/podData.txt file.

1 As **dncs** user, type the following command to display the CableCARD MAC address for the specified host, provided the CableCARD/host pair is contained in the podData file.

Command Syntax:

```
podDataChk -H [Host ID]
```

Example:

```
[dncs@ecnextx9 podServer]$ podDataChk -H 0-380-169-302-854
```

Example Output:

```
Host with ID <0-380-169-302-854> is deauthorized with Cable card =
00:21:BE:2E:25:C5
Note: Output file <podData.txt> created. Review for more info.
```

2 Type the following command to view the complete contents of the **podData.txt** file:

```
[dncs@ecnextx9 podServer]$ less podData.txt
```

11

Monitor the Logfiles of EC Processes with the qtail and sesstail Utilities

Introduction

The logfiles in the /dvs/dncs/tmp directory contain important information about how the EC 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 and the current values of the software parameters and variables coded into the processes.

The qtail and sesstail utilities help you monitor the EC logfiles.

In This Chapter

Design of the qtail and sesstail Utilities and the System Logfiles

Design of the qtail and sesstail Utilities

The LINUX 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 a terminal window on the EC, type **man tail** and press **Enter**.

You can use the tail utility to monitor the logfile of an EC process in real time. The problem 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. No new data can be observed in the logfile monitored by the tail utility.

The qtail utility uses the LINUX tail utility to monitor logfiles of EC 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 EC.

By default, we place a 50,000 line limit on individual logfiles. Each EC 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 EC allows you plenty of time to save a specific logfile for later examination.

The qtail Utility

The qtail utility lets you monitor log activity and automatically switch to the next logfile when the 50,000 line limit has been reached.

The qtail utility monitors 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 LINUX grep utility to search for that pattern.

Running the qtail Utility

1. As **dncs** user, type the following command to change to the **/dvs/dncs/tmp** directory.

   ```
   [dncs@ecnextx9 podServer]$ cd /dvs/dncs/tmp
   ```

2. Choose one of the following options:

   - To use the qtail utility to monitor an entire logfile, go to the next step.
   - To use the qtail utility to display only those lines that contain a particular pattern, go to Step 5.

3. To monitor an entire logfile, type the following command and press **Enter**. The qtail utility begins monitoring the logfile of the selected process.

   Command Syntax:

   ```
   qtail [process_name]
   ```

   Example: `qtail siMan`

   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 Output:

   ```
   Wed Jan 31 16:14:33 EST 2018
   ***********************
   Tailing /dvs/dncs/tmp/camAuditor.033 ...
   01/31/2018
   10:53:58.489|2355/2355/0xf4faf840|DEBUG|camAuditor:CamuAuditMgr.C(1047)|No
   entries to process : assessing look ahead
   01/31/2018
   10:53:58.489|2355/2355/0xf4faf840|DEBUG|camAuditor:CamuAuditMgr.C(1052)|Curre
   nt last jump process restriction window is 1522102252
   ```

```
01/31/2018
10:53:58.489|2355/2355/0xf4faf840|DEBUG|camAuditor:CamuAuditMgr.C(1053)|Compa
iring with 1522076038
.
.
```

4 Press **Ctrl + c** to exit from the qtail utility.

5 To use the qtail utility to monitor a specific logfile and display only those lines that contain a particular pattern, type the following command and press **Enter**:

Command Syntax:

```
qtail [process_name] <pattern>
```

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. Examples include:
  - Type **qamM** for qamManager
  - Type **siM** for siManager
  - Type **camAu** for camAuditor
- Substitute the pattern you want to find for <pattern>.

Example:

```
[dncs@ecnextx9 tmp]$ qtail camAu timeout
```

Example Output:

```
Wed Jan 31 16:14:55 EST 2018
**********************
Tailing /dvs/dncs/tmp/camAuditor.033 ...
01/31/2018
10:52:58.186|2355/2355/0xf4faf840|DEBUG|camAuditor:CamuAuditMgr.C(485)|_compl
eteAudit setting timeout
01/31/2018 10:52:58.186|2355/2355/0xf4faf840|DEBUG|c
```

6 Press **Ctrl + c** to exit from the qtail utility.

The sesstail Utility

The sesstail utility is similar to the qtail utility, except that it monitors the logfiles of the dsm process for session-related information. Examples of session-related information include session setup 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.

Notes:

- To run the sesstail utility, the dsm log level must be enabled.
- By searching for session-related activity in existing dsm logfiles, you can troubleshoot VOD problems that have already occurred.

Running the sesstail Utility

1. As **dncs** user, choose one of the following options:
   - To monitor the dsm logfiles in real time for session-related activity, go to the next step.
   - To review existing dsm logfiles for session-related activity, go to Step 4.
2. To monitor the dsm logfiles for session-related activity in real time, type `sesstail` and 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.

   ```
   [dncs@ecnextx9 tmp]$ sesstail
   ```

   Example Output:

   ```
    ++++ 00:40:7B:D6:B5:B3/515 ++++
   ClientSessReq:     Jan 03 07:23:50.008
   ServerSessInd:     Jan 03 07:23:50.016
   ServerAddRsrReq:   Jan 03 07:23:50.207
   ServerAddRsrCnf:   Jan 03 07:23:50.270 (response=0)
   ServerSessRsp:     Jan 03 07:23:50.335 (response=0)
   ClientSessCnf:     Jan 03 07:23:50.346 (response=0)
    ++++ 00:40:7B:D6:B5:B3/515 ++++
   ClientRelReq:      Jan 03 07:23:58.683
   ServerRelInd:      Jan 03 07:23:58.687
   ServerRelRsp:      Jan 03 07:23:58.709 (Response=0)
   ClientRelCnf:      Jan 03 07:23:58.713 (Response=0)
   ```

3 Press **Ctrl + c** to exit from the sesstail utility.

4 To review an existing dsm logfile for session-related activity, type the following command and press **Enter**. The selected file opens for review.

Command Syntax:

```
sesstail [filename]
```

Example:

```
[dncs@ecnextx9 tmp]$ sesstail /dvs/dncs/tmp/dsm.000
```

5 Press **Ctrl + c** to exit from the qtail utility.

12

Assign DHCTs to Download Groups with the runCvtGroup Utility

Introduction

When you use the CVT method to download DHCT code, you might want to restrict the download to DHCTs that belong to a specific download group.

Before the release of the runCvtGroup utility, you had to use the EC user interface to assign DHCTs to the download group. The process of assigning DHCTs to the download group was often quite lengthy; you had to type one MAC address at a time.

The runCvtGroup utility expedites the process by which DHCTs are assigned to download groups. You can now prepare a text file that contains one DHCT MAC address per line. The runCvtGroup utility reads that text file and quickly assigns the DHCTs associated with those MAC addresses to the specified download group.

Note: The download group must already exist.

In This Chapter

Run the runCvtGroup Utility

Use these instructions to run the runCvtGroup utility:

1 Do you need to create a download group?

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

2 From the Administrative Console, click the **Navigation** icon, , and then click **Home Element Provisioning > Image**. The Downloadable Files window opens.

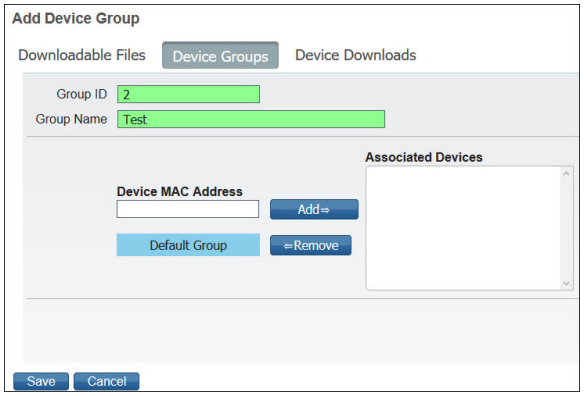
3 Click the **Device Groups** tab.

4 Click **Add**. The Add Device Group window opens.

5 Follow these instructions to configure the device group.

a Type an unused ID value in the **Group ID** field.

b Type a unique name for the group in the **Group Name** field.



c Click **Save**. A Group Save Successful message appears.

6 As **dncs** user in a terminal window, type the following command and press **Enter**. The system assigns the DHCTs in the text file to the specified download group.

Notes:

- See **Guidelines for Preparing the Text File** (next in this document) for instructions on creating the text file to be used with the runCvtGroup utility.
- Substitute the ID of the download group for [group ID].
- Substitute the name of the text file for [filename].
- Separate the filename and the group ID with a comma.

Command Syntax:

```
runCvtGroup -f [filename],[group ID]
```

Example:

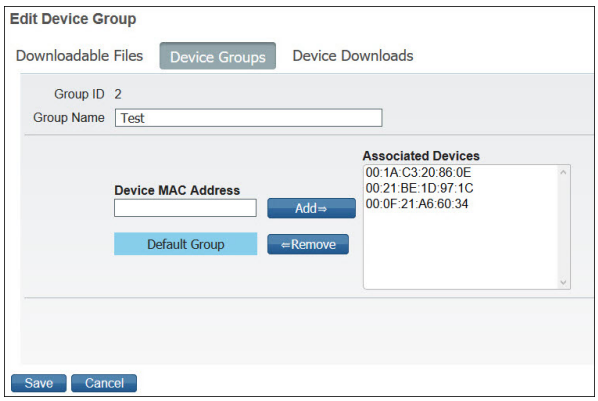
```
[dncs@ecnextx9 ~]$ runCvtGroup -f /tmp/runCvtGroup_03262018,2
```

Example Output:

```
OK    : Successfully assigned 00:1A:C3:20:86:0E to CVT GroupId: 2.
OK    : Successfully assigned 00:21:BE:1D:97:1C to CVT GroupId: 2.
OK    : Successfully assigned 00:0F:21:A6:60:34 to CVT GroupId: 2
```

7 Return to the EC Web UI Device Groups page and select the group you added.

8 Click **Edit**. The MAC addresses you assigned to the group ID in Step 6 are now listed in the Associated Devices area.



Guidelines for Preparing the Text File

- Prepare the file using a standard text editor (for example, vi).
- Prepare the file with one MAC address per line.

  Examples:

  ```
  00:1A:C3:20:86:0E
  00:1A:C3:20:86:0E
  00:21:BE:1D:97:1C
  00:0F:21:A6:60:34
  ```

- Each MAC address must be left-justified on each line of text.
- Save the file using a name that is relevant to the contents of the file. Append the current date to the end of the file name.

  Examples:

  - **tellDhct-in_010218** for a file that was created on January 2, 2018
  - **tellDhctInfo-in_021318** for a file that was created on February 13, 2018

- **For files that you will only use once,** we recommend that you save the file to the /tmp directory on the EC.
- **For files that you may re-use,** we recommend that you create a directory for the file under /export/home.

13

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 provides a mechanism for synchronizing this data between the NCDS server and the EC.

You can configure the ncdsGen utility 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.

Running this utility keeps the channel map, service group, and VOD QAM information in sync between the NCDS and the EC.

When to Run the ncdsGen Utility

You should run the ncdsGen utility whenever you make a change to a channel map or whenever you update VOD information. The ncdsGen utility propagates and uploads the EC changes to the NCDS server.

In This Chapter

About the ncdsGen Utility

The ncdsGen utility uploads the EC channel maps and VOD information to the NCDS server.

You can use the following methods to run the utility:

- Push the information from the EC to the NCDS server.

  Note: The ncdsPush utility, a utility within ncdsGen, triggers the ncdsGen utility to generate the xml files. The ncdsPush utility then transfers those xml files to the appropriate server.

- Poll the EC for the information for the NCDS server to fetch.

  Note: The ncdsPoll utility, a web interface within ncdsGen, is responsible for the polling action.

The ncdsGen Help File

Note: The ncdsPoll utility, a web interface, does not have a help file.

The ncdsGen Utility Help File

1 As **dncs** user, type the following command to change to the **/dvs/dncs/Utilities/ncdsGen** directory.

```
[dncs@ecnextx9 ~]$ cd /dvs/dncs/Utilities/ncdsGen
```

2 Type the following command to generate the help file for the ncdsGen utility.

```
[dncs@ecnextx9 ncdsGen]$ ncdsGen -h
```

Output:

```
Usage:  ncdsGen [-v] [-V] [ -d OUTDIR ] [ -B BASEURL ] [ -i ControllerID ] [-
s] [-h help]

        Generate NCDS Input Documents for posting to the NCDS Server, or
        for placing in a web server's directory so the NCDS Server can
        periodically poll for the data.

        ncdsGen can pull in the /home/dncs/SGFrequencies.dat file to
        create a more efficient method of VOD AutoDiscovery.
        The ncdsGen-Input-VOD.xml file is created with the sort criteria
based on
        the frequencies (in MHz) specified in the SGFrequencies.dat.

        In the SGFrequencies.dat, the frequencies should be format as follow:
        888
        555
        777.25

        -v                increase verbosity
        -V                print version and exit
        -d OUTDIR         generate files in the given OUTDIR (default is ".")
        -B BASEURL        generate files for subsequent "poll", such that the
                          Input Manifest contains URLs based on the BASEURL

        -i ControllerID   (optional) This is the ID value of the controller
                          that making the information available to the NCDS
        -n ControllerName (optional) This is the Name of the controller
                          that making the information available to the NCDS
        -s                (optional) Include the source ID to be used for
                          auto-discovery to the ncdsGen-Input-VOD.xml file.
                          The SourceID will have been associated to the
                          TSID/QAM/Freq in the DNCS via the Source Definition
                          and Session creation.
```

The -i and -s Options

The ncdsGen and ncdsPush utilities both support the **-i** and **-s** options.

- The **-i** option allows you 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 EC, 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.

- The **-s** option allows you to specify an optional source ID that is associated with the Transport Stream ID (TSID) to be used for auto-discovery in the ncdsGen-Input-VOD.xml file. The source ID must previously have been associated with the TSID, as well as the QAM modulator frequency during source definition and session creation.

  Example: The following example illustrates the use of the **-s** option with the ncdsGen utility.

  ```
  ncdsPush -i 112 -s -v http://<ipaddress:port>
  ```

Pushing the Information to the NCDS Server

1 Type the following command to push the information for the NCDS server.

Note: Use the IP address and port of the NCDS server.

Command Syntax:

```
./ncdsPush -v http://<ipaddress:port>
```

Example:

```
[dncs@ecnextx9 ncdsGen]$ ./ncdsPush -v
http://209.165.200.224:7091
```

2 To verify that the script has run, look for output similar to the following:

```
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 EC. In this example, ncdsPush is configured to run every weekday at 1:00 am.

1 As **dncs** user, type the following command to edit the **crontab** file.

```
[dncs@ecnextx9 ncdsGen]$ crontab -e
```

2 Add an entry (on one line), similar to the following, to the **crontab** file.

cron Job Syntax:

```
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
```

Note: These commands are each one continuous line.

3 Save and close the **crontab** file.

Polling for the Information

1. Type the following command to poll the EC.

```
[dncs@ecnextx9 ncdsGen]$ ./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.

14

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 onto the network and their network configuration data is reloaded. The signonCount utility is useful in monitoring the rate at which DHCTs sign onto the network.

Because some DHCTs make repeated attempts to sign onto the network before they are successful, too many sign-on attempts by DHCTs contribute to network congestion.

The signonCount utility can help you quickly identify those DHCTs that are having trouble signing on, and you can use the utility to facilitate the DHCT sign-on process.

In This Chapter

When to Use the signonCount Utility

The signonCount utility allows you 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:
  - 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.
  - 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 you monitor the rate at which DHCTs are trying to sign on to the network.

- **Fix Mode Off —** The utility takes no corrective action regarding DHCTs that are having difficulty signing on.
- **Fix Mode On —** 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, we 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

1 As **dncs** user. enter the following command to view the help window for the **signonCount** utility.

```
[dncs@ecnextx9 Utilities]$ signonCount -h
```

2 Press the **spacebar** to page through the help window.

Set EC Logging Levels

Set EC Logging Levels

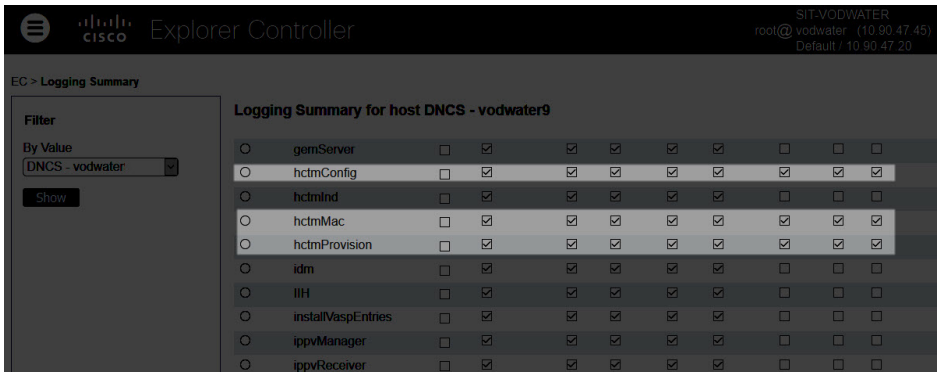
Before you can begin using the signonCount utility, you need to set the logging levels of three EC processes. By setting the logging levels for these processes, you make sure that the EC captures the maximum level of detail for these processes.

Note: The processes are:

- hctmConfig
- hctmMac
- hctmProvision

Setting the EC Logging Levels

1. From the EC Administrative Console, click the **Navigation** icon, , and then click **Utilities > Logging**. The Logging Summary DNCS window opens.
2. Scroll down until the **hctmConfig**, **hctmMac**, and **hctmProvision** processes come into view.
3. Click to place a check mark in the **Notice**, **Info**, and **Debug** checkboxes for the **hctmConfig**, **hctmMac**, and **hctmProvision** processes.



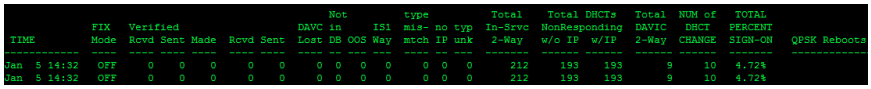
4. Click **Save**.

The signonCount Utility Interface

Displaying the signonCount Interface

1. Maximize your terminal window as the signonCount utility fills the entire screen.
2. As **dncs** user, type **signonCount** and press **Enter**. The signonCount utility interface opens.

   Example Output:



```
                                                 Not          type          Total    Total DHCTs   Total  NUM of   TOTAL
             FIX   Verified                      DAVC in      IS1  mis- no typ In-Srvc  NonResponding DAVIC   DHCT   PERCENT
TIME         Mode  Rcvd Sent Made  Rcvd Sent    Lost DB OOS  Way  mtch IP unk 2-Way   w/o IP  w/IP  2-Way  CHANGE  SIGN-ON   QPSK Reboots
------------ ----- ---- ---- ----  ---- ----    ---- -- ---  ---  ---- -- --- ------- ------- ------ ------ ------- ------- ------------
Jan  5 14:32  OFF    0    0    0     0    0       0  0   0    0     0  0   0     212     193    193      9     10   4.72%
Jan  5 14:32  OFF    0    0    0     0    0       0  0   0    0     0  0   0     212     193    193      9     10   4.72%
```

The signonCount Utility Data Fields

Data Fields

The following tables list the fields included on the interface of the signonCount utility and provides an explanation of the meaning associated with each field.

Header	Column Name	Description
	TIME	The system polls the communication link between the QPSK modulators and the EC 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.
SUCCESSFUL SIGNON DAVIC	Verified Rcvd	The QPSK modulator reports the number of DHCTs that have made sign-on requests.
	Verified Sent	The EC has allocated this number of DHCT IP addresses based upon the sign-on requests.
	Made	The QPSK modulator reports the number of DHCTs that have connected to the QPSK modulator and are waiting for UN-Config information.
SUCCESSFUL SIGNON UNCfg	Rcvd	This number of DHCTs are requesting a UN-Config message from the EC. **Note**: The UN-Config message contains information, like an IP address, that allows DHCTs to sign on to the network.
	Sent	The EC 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.

Header	Column Name	Description
FAILURE to SIGNON DAVIC	DAVC 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.
	Not in DB	The number of DHCTs in the database with the wrong type, revision, or OUI.
	OOS	The number of DHCTs in the database that are out of service (OOS).
	IS1 WAY	The number of DHCTs in the database that are operating in 1-Way mode.
FAILURE to SIGNON UN-Config	type mis-mtch	The number of DHCTs in the database that have incorrect data.
	no IP	The number of DHCTs in the database that do not have an IP address.
	typ unk	The number of DHCTs in the database that have an unknown data in their database record.
DATABASE 2way Signon Status	Total In-Srvc 2-Way	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.
	Total DHCTs Non responding w/o IP	The number of DHCTs in the database that should be capable of two-way communication, but they are listed as non-responding DHCTs not having an IP address.
	Total DHCTs Non responding w/ IP	The number of DHCTs in the database that should be capable of two-way communication, but they are listed as non-responding DHCTs and having an IP address.
	Total DAVIC 2-Way	The number of DHCTs that have physically signed on to the network with two-way communication ability.

Header	Column Name	Description
	NUM of DHCT CHANGE	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 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**
- **Made**

These fields track the number of sign-on requests made by DHCTs (Verified Rcvd and Verified Sent), and the number of sign-on requests that were successful (Made). Ideally, the numbers in the three fields should be equal.

If you notice that the numbers in the 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 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 into 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.

15

Replicate SARA QAM-to-Hub Associations with the nonsaradupqha Utility

Introduction

The purpose of the nonsaradupqha utility is to duplicate an existing SARA QAM port-to-hub association to new, non-SARA hub association. between the same SARA QAM ports and new non-SARA hubs. The utility prompts the operator for the existing SARA hub ID and then duplicates any records associated with that hub ID to a new, operator-supplied, non-SARA hub ID.

The nonsaradupqha.sh script includes options to run in Info Mode (-i option) without performing database updates, as well as in Update Mode (-u option), which makes permanent database updates. After running the script, a list of successful duplicated records, as well as a list of failed duplications are displayed.

In This Chapter

Run the nonsaradupqha Utility

Overview of the nonsaradupqha Utility

The nonsaradupqha utility prompts you for the existing SARA hub ID and duplicates any records associated with that hub ID to a new, non-SARA hub ID.

After running the script, a list of successful duplicated records and a list of failed duplications are provided.

The script generates a log file in the directory in which the script is run that contains the status of each hub-to-port duplication. The log file has the following format: **phdup_01192018053926_forSaraHub_1_ToNONSara_255.log**

To Learn More About the nonsaradupqha Utility

Follow these instructions to access the help screen for the nonsaradupqha utility:

1 As **root** user, enter the following command to source the environment.

```
[root@ecnextx9 ~]# . /dvs/dncs/bin/dncsSetup
```

2 Type the following command to display the help screen for the **nonsaradupqha** utility.

```
[root@ecnextx9 ~]# nonsaradupqha.sh -h
```

Output:

```
-------------------------------------------
Thu Jan 11 11:04:40 EST 2018
-------------------------------------------

/dvs/dncs/Utilities/nonsaradupqha.sh Version 8.1.3

NAME
        nonsaradupqha.sh - allows the ROOT operator to replicate existing
SARA Qam
        ports to Hub associations to a NEW association between the same SARA
        Qam ports and a NEW NON-SARA hub.

SYNOPSIS
        nonsaradupqha.sh [-biruhv ]

DESCRIPTION
        nonsaradupqha.sh primary responsibility is to duplicate a given SARA
        Qam ports to hub association by prompting the operator for the
existing
        SARA hub id, and duplicating any records associated with the given
SARA
        hub id with an operator given NEW NON-SARA hub ID.

        The script has the option to run under INFO MODE without performing
any
        updates to the database by using the -i option, or under UPDATE MODE
        making changes to the database permanent by using the -u option.

        The script will provide a list of successful duplications, and a list
        of failed duplications.

        A log file will be generated in the current directory containing
        the status of each port to hub duplication.   The file will have the
        following format/name:
```

```
                porthublistduplication_mmddyyyyhhmmss.log
OPTIONS
        The following options are supported:
        -i      INFO MODE: prompts the user to enter the SARA hub, and the
                NEW NON-SARA hub ids, and proceed to replicate the existing
                SARA-HUB to port associations with the given NEW-NON-SARA
hubs,
                WITHOUT updating the database.
        -u      UPDATE MODE: prompts the user to enter the SARA hub, and the
                NEW NON-SARA hub ids, and proceed to replicate the existing
                SARA-HUB to port associations with the given NEW-NON-SARA
hubs,
                UPDATING the database.
        -b      Backups the database tables involved in the duplication
before
                they are duplicated.  The backup files are located in the
                /dvs/backups directory and the name of the backup files have
                the following format "pdporthublist_mmddyyyy.tar.
        -r      Restores a backup of the tables prior to the duplication
                the backup files are located in the /dvs/backups directory.
        -H|h    Help.
        -V|v    Print current version of this command.
-------------------------------------------
Thu Jan 11 11:04:40 EST 2018
-------------------------------------------
```

procd Running the nonsaradupqha Utility

Running nonsaradupqha Without Updating the Database

Complete the following steps to execute the nonsaradupqha utility in INFO mode. This results in the replication of the existing SARA-HUB to port associations with the NEW-NON-SARA hubs, ***without*** updating the database.

1 As **root** user, enter the following command to run the **nonsaradupqha** utility in INFO mode. You are prompted to enter a valid hub ID from the list provided in the output.

```
[root@ecnextx9 ~]# nonsaradupqha.sh -i
```

Example Output:

```
-------------------------------------------
Wed Jan 17 21:30:24 UTC 2018
-------------------------------------------
Please enter a valid SARA hub id from the list.
     hub_id hub_name
         18 HUB60_Condor
         20 Test_Hub1
Please enter the SARA hub Id from the list shown above :
```

2 Enter the hub ID for the existing SARA-HUB to port associations and press **Enter**. You are prompted to enter a valid NON-SARA hub ID from the list provided in the output.

```
Please enter a valid NON-SARA hub id from the list.
     hub_id hub_name                mylugid lub_name
         18 HUB60_Condor                  1 Condor_Map
         20 Test_Hub1                     2 Rick_ChMap
Please enter the NON-SARA hub Id from the list shown above :
```

3 Enter a valid NON-SARA hub ID and press **Enter**. The script completes and provides the location for the log file.

Example Output:

```
Will duplicate SARA hub id [18] with NON-SARA hub id [20]
*** Please check file phdup_01172018213024_forSaraHub_18_ToNONSara_20.log for
results ***
-------------------------------------------
Wed Jan 17 21:34:36 UTC 2018
-------------------------------------------
```

4 Review the log file displayed in the output from Step 3.

Backing Up the Database Tables Before Duplicating Them

Complete the following steps to backup the database tables ***before*** executing the nonsaradupqha script with the -u (update) option.

1 As **root** user, enter the following command to backup the appropriate database tables.

```
[root@ecnextx9 ~]# nonsaradupqha.sh -b
```

Example Output:

```
-------------------------------------------
Wed Jan 17 21:17:45 UTC 2018
-------------------------------------------

tar: Removing leading `/' from member names
/dvs/backups/pdporthublist.unl

You just requested the -b option to be executed, which backups all tables
related to duplicating the existing porthublists to new porthublists before
the
duplication takes place.  The backup file will be located in the /dvs/backup
directory.   The format of the name of the backup file is:
      pdporthublist_mmddyyyhhmmss.tar:

*** The file /dvs/backups/pdporthublist_01172018211745.tar contains a backup
of the tables that will be changed prior to the duplication ***
-------------------------------------------
Wed Jan 17 21:17:46 UTC 2018
-------------------------------------------
```

2 Enter the following command to change to the **/dvs/backups** directory.

```
[root@ecnextx9 ~]# cd /dvs/backups
```

3 Enter the following command to verify that the tar file displayed in the output of Step 1 is present in the **/dvs/backups** directory.

```
[root@ecnextx9 ~]# ls -ltr /dvs/backups | grep tar
```

Example Output:

```
-rw-r--r--. 1 root root 10240 Jan 17 21:17 pdporthublist_01172018211745.tar
```

Running nonsaradupqha and Updating the Database

Complete the following steps to execute the nonsaradupqha utility in UPDATE mode. This results in the replication of the existing SARA-HUB to port associations with the NEW-NON-SARA hubs, *while* updating the database.

Note: System processes ***do not*** need to be stopped to execute this procedure.

1 As **root** user, enter the following command to run the **nonsaradupqha** utility in UPDATE mode. You are prompted to enter a valid hub ID from the list provided in the output.

```
[root@ecnextx9 ~]# nonsaradupqha.sh -u
```

Example Output:

```
-------------------------------------------
Wed Jan 17 21:39:10 UTC 2018
-------------------------------------------
Please enter a valid SARA hub id from the list.
     hub_id hub_name
         18 HUB60_Condor
         20 Test_Hub1
Please enter the SARA hub Id from the list shown above :
```

2 Enter the hub ID for the existing SARA-HUB to port associations and press **Enter**. You are prompted to enter a valid NON-SARA hub ID from the list provided in the output.

```
Please enter a valid NON-SARA hub id from the list.
     hub_id hub_name                 mylugid lub_name
         18 HUB60_Condor                   1 Condor_Map
         20 Test_Hub1                      2 Rick_ChMap
Please enter the NON-SARA hub Id from the list shown above :
```

3 Enter a valid NON-SARA hub ID and press **Enter**. You are prompted to continue with the update.

4 Type **y** and press **Enter**. The script performs a backup of the database and then updates the database.

Example Output:

```
tar: Removing leading `/' from member names
/dvs/backups/pdporthublist.unl
You just requested the -b option to be executed, which backups all tables
related to duplicating the existing porthublists to new porthublists before
the duplication takes place.  The backup file will be located in the
/dvs/backup/directory.  The format of the name of the backup file is:
      pdporthublist_mmddyyyyhhmmss.tar:
*** The file /dvs/backups/pdporthublist_01172018213910.tar contains a backup
of the tables that will be changed prior to the duplication ***
```

```
*** Please check file phdup_01172018213910_forSaraHub_18_ToNONSara_20.log for
results ***
-------------------------------------------
Wed Jan 17 21:42:02 UTC 2018
-------------------------------------------
```

5 Review the log file displayed in the output from Step 4.

Restoring the Database Tables

Complete the following steps to restore a backup of the database tables. The backup files are located in the /dvs/backups directory.

Note: System processes ***do not*** need to be stopped to execute this procedure.

1 As **root** user, enter the following command to run the **nonsaradupqha** utility in RESTORE mode. A list of the backup files is displayed.

```
[root@ecnextx9 ~]# nonsaradupqha.sh -r
```

Example Output:

```
-------------------------------------------
Thu Jan 18 15:13:17 UTC 2018
-------------------------------------------
List of backup files.  Please enter just the name of the file (do not include
the path) as in the example below:
        pdporthublist_mmddyyyyhhmmss.tar
-rw-r--r--. 1 root root 10240 Jan 17 21:17
/dvs/backups/pdporthublist_01172018211745.tar
-rw-r--r--. 1 root root 10240 Jan 17 21:42
/dvs/backups/pdporthublist_01172018213910.tar
```

2 When prompted, enter the file name for the backup you want to restore.

Important: Only enter the file name. The absolute path is not required.

Example:

```
Please enter the name: pdporthublist_01172018213910.tar
```

3 When prompted to continue, type **y** and press **Enter**. The tables are restored to the database.

Example Output:

```
dvs/backups/pdporthublist.unl
Database selected.
   BEGIN WORK;
Started transaction.
DELETE FROM pdporthublist;
      LOAD FROM '/dvs/backups/pdporthublist.unl' INSERT INTO pdporthublist;
     COMMIT WORK;
Data committed.
Database closed.
You just executed -r option. All tables were restored from the backup
specified by the file pdporthublist_01172018213910.tar.
-------------------------------------------
Thu Jan 18 15:20:46 UTC 2018
-------------------------------------------
```

16

Convert IP Addresses with the convertIP Utility

Introduction

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

Example: An example of an IP address in dotted-decimal notation is **209.165.201.0**. That very same IP address is stored in the database in decimal format as **3517303040**.

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

Available Options When Running the convertIP Utility

The convertIP utility accepts as an argument either as a single IP address, or from the name of a file containing a list of IP addresses.

In general, use the single IP address when you have only one or two IP addresses to convert. When you have many IP addresses to convert, consider creating a text file that contains the IP addresses that you want to convert.

In This Chapter

Prepare the Text File

Guidelines for Preparing the Text File

Use the following guidelines when preparing the text file:

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

  Note: You can mix formats in the text file.
- We recommend that you save the file in the **/dvs/dncs/tmp** directory.

Preparing the Text File

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

1 As **dncs** user, type the following command to change to the **/dvs/dncs/tmp** directory.

```
[dncs@ecnextx9 ~]$ cd /dvs/dncs/tmp
```

Note: We recommend that you save the file in the /dvs/dncs/tmp directory of the EC.

2 Open a new file in a text editor (for example, ipec9.txt). The file opens for editing.

```
[dncs@ecnextx9 ~]$ vi ipec9.txt
```

3 Insert your list of IP addresses into the file you have just opened.

Note: Use the guidelines in ***Guidelines for Preparing the Text File*** from the previous section.

Example:

```
209.165.201.0
209.165.201.0
3517303040
127.255.255.255
3221424141
172.16.16.4
```

4 Save the file and close the text editor.

Run the convertIP Utility

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

- To convert a single IP address, follow the instructions in ***Converting a Single IP Address*** (on page 169).
- To convert IP addresses listed in a file of IP addresses, follow the instructions in ***Converting a File of IP Addresses*** (on page 169).

Note: The convertIP utility should be run as the **dncs** user.

Converting a Single IP Address

1 As **dncs** user, type the following command to convert a single IP address. The **Enter IP address to convert** message appears.

```
[dncs@ecnextx9 tmp]$ convertIP
```

2 Type the IP address you want to convert to decimal format and press **Enter**. The convertIP utility converts the IP address and displays both the original value and the converted value on the screen of the EC.

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

Examples:

- Decimal - **3517303040**
- Dotted-decimal notation - **127.255.255.255**

Converting a File of IP Addresses

When the convertIP utility runs, it displays each original and converted IP address on the screen of the EC and writes the output to a user-specified file.

Important: You should already have prepared a text file containing IP addresses using the guidelines and directions in ***Preparing the Text File*** (on page 168).

1 As **dncs** user, type the following command to initiate the convertIP script. The **Enter the file name (full path) containing IP addresses to convert** message appears.

```
[dncs@ecnextx9 tmp]$ convertIP -f
```

2 Type the name of the file you prepared (including the full directory path) and press **Enter**. The **Enter the file name (full path) in which to store the converted IP addresses** message appears.

3 Type the name of the file (including the full directory path) where you want to store the file containing the output.

Example:

```
[dncs@ecnextx9 tmp]$ /dvs/dncs/tmp/IP_input_file.txt
```

Results:

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

  Example Output:

```
209.165.201.0
3517303040

209.165.201.0
3517303040

3517303040
127.255.255.255

127.255.255.255
2147483647
3221424141
127.255.255.25

172.16.16.4
2886733828
```

17

Monitor Session Setup with the setuptail Utility

Introduction

This chapter describes the setuptail utility, which is used to monitor session setup.

In This Chapter

The setuptail Utility

The setuptail utility tracks session setup successes, failures, and error types. The setuptail utility runs every minute and displays the following information:

- Session setup and failures for each minute
- Total number of successes since the script was started
- Total number of failures since the script was started
- Cumulative errors by type

Output for the setuptail utility can be directed (piped) to a file, so the output can be examined whenever you want to monitor session setups over a period of time to analyze trends of usage and error rates.

Output Format:

```
<Time> <Success for the minute> <Failures for the minute> <Total successes>
<Total failures> ( <Error type 1 cumulative> <Error type 2 cumulative> …)
```

Example Output:

```
14:35 succ=164 fail=0 totalsucc=46076 totalfail=3342 ( resp18=3342 )
14:36 succ=170 fail=0 totalsucc=46246 totalfail=3342 ( resp18=3342 )
14:37 succ=84 fail=52 totalsucc=46330 totalfail=3394 ( resp6=52 resp18=3342 )
14:38 succ=154 fail=0 totalsucc=46484 totalfail=3394 ( resp6=52 resp18=3342 )
```

Running the setuptail Utility

Complete the following steps to run the setuptail utility.

1 As **dncs** user, type the following command to run the **setuptail** script.

```
[dncs@ecnextx9 Utilities]$ setuptail
```

Example: The following command directs the output to the setuptail.log file.

```
[dncs@ecnextx9 Utilities]$ setuptail >
/home/ecadmin/setuptail.log
```

2 To stop the script, press **Ctrl+C**. You are returned to a command prompt.

18

Generate a BFS Summary Report with the bfsInfo Utility

Overview

The bfsInfo.ksh script generates a BFS summary report that details the files within each BFS carousel and the file sizes of each BFS carousel.

In This Chapter

Run the bfsInfo Utility

Overview of the bfsInfo Utility

The bfsInfo utility does not prompt you for any information. When executed, the following information is retrieved from the database and displayed on the screen.

- BFS Cancel Packet Settings
- Data Pump Summary Information
- Element Summary Information
- Location of the BFS Summary Report

The script generates a BFS Summary Report in the /tmp directory. This log file has the following format: `/tmp/bfsinfo.out.[YYMMDD]_[HHMM].doc`

To Learn More About the bfsInfo Utility

1 As **dncs** user, enter the following command to view the help file for the **bfsInfo.ksh** utility.

```
[dncs@ecnextx9 Utilities]$ bfsInfo.ksh -h
```

Output:

```
Usage: bfsInfo.ksh [-v] [-h] [-?]

The bfsInfo script generates BFS summary report which is useful for isolating
files and file sizes on each BFS carousel

   v = print script name, version and exit
   h = Display the usage and exit
   ? = Display the usage and exit
   with no arguments generates the BFS summary report
```

Generating a BFS Summary Report

Complete the following steps to generate a BFS Summary Report.

1 As **dncs** user, enter the following command to run the **bfsInfo.ksh** utility. The output is generated to the screen and saved to a log file displayed at the end of the output.

```
[dncs@ecnextx9 dncs]$ bfsInfo.ksh
```

2 From the output, open the BFS Summary Report.

Example:

```
[dncs@ecnextx9 dncs]$ less /tmp/bfsinfo.out.180118_1644.doc
```

3 Review the report.

19

Check Database Information with the checkdbinfo Utility

Overview

The checkdbinfo.sh script allows you to find the type of database (primary, secondary, or standard) and whether database replication is on or off.

In This Chapter

Run the checkdbinfo Utility

Overview of the checkdbinfo Utility

The script shows if the database type is standard, primary or secondary, and it also shows whether the database replication is ON or OFF.

- When you run the script without any options, it displays the type and the state of the database.
- When you use the **-t** option, the type is displayed: standard, primary, or secondary.
- When you use the **-r** option, the script displays if the database replication is ON or OFF.

To Learn More About the checkdbinfo.sh Utility

Complete the following steps to view the help file for the checkdbinfo.sh utility.

1 As **dncs** user, enter the following command to display the help file for the **checkdbinfo.sh** utility.

```
[dncs@ecnextx9 ~]$ checkdbinfo.sh -h
```

Output:

```
NAME
        checkdbinfo.sh - allows an operator to find the type of database
        (primary, secondary, or standard), and if database replication is
        on or off.
SYNOPSIS
        checkdbinfo.sh [-TtRrHhVv]
DESCRIPTION
        The script shows if the database type is standard, primary or
        secondary, and it also shows if the database replication is ON or
OFF.
        When the script is run without any options it will display the type,
        and the state of the database.
        When the -t option is used the type will be display: standard,
        primary, or secondary.
        When the -r option is used then the script will display if the
        database replication is ON or OFF.
OPTIONS
        The following options are supported:
        -T|t    Shows if the database type is standard, primary or secondary.
        -R|r    Shows if the database replication is ON or OFF.
        -H|h    Help.
        -V|v    Print current version of this command.
```

2 Press the **Spacebar** to page through the help content.

Checking the Version of the checkdbinfo.sh Utility

1 As **dncs** user, type the following command to view the version of the checkdbinfo utility.

```
[dncs@ecnextx9 Utilities]$ checkdbinfo.sh -v
```

Example Output:

```
/dvs/dncs/Utilities/checkdbinfo.sh Version 8.1.5
```

Note: This example shows that version 8.1.5 is loaded onto the EC.

Checking the Type and State of the Database

1 As **dncs** user, enter the following step to determine the current type and state of the database.

```
[dncs@ecnextx9 ~]$ checkdbinfo.sh
```

Example Output:

```
DB Type: Primary
DB State: Replication is enabled (On).
```

20

Retrieve the System CVT Version with the cvtChecker Utility

Introduction

The cvtChecker utility logs into all the specified devices and reports back the CVT version found on the devices.

The utility (cvtChecker.py) prompts you for authentication and lists the CVT version installed on both the GQAMs (**-g** option) and the GQI-based QAMs (**-r** option).

In This Chapter

Important Notes about the cvtChecker Utility

You can check the **/tmp/cvtChecker.log** utility file for detailed information on execution and errors of the utility.

Notes:

- The **–g** option checks for the cvt version on GQAMs
- The **–r** utility lists Cisco GQI-based QAMs (RFGWs) where packet insert is enabled
- The utility assumes that telnet-capable devices are loaded

Display the Help Window and Version Number of the cvtChecker Utility

Displaying the Help Window of the cvtChecker Utility

The cvtChecker script includes a help window that lets you examine the various options supported by the utility.

1 As **dncs** user, type the following command to view the help file for the **cvtChecker.py** utility. The system displays the help window.

```
[dncs@ecnextx9 ~]$ cvtChecker.py -h
```

Example Output:

```
NAME
    cvtChecker.py - Checks the cvt version on RFGW or GQAM.
SYNPOSIS
    cvtChecker.py - [-h] [-gr] [-v]
DESCRIPTION
    This script will log into all the specified devices and
    report back the CVT version found on the device. It assumes
    that telnet capable GQAM code is loaded.
    ***NOTE*** - This will not check MQAM's or CAQAM's.
OPTIONS
    The following options are supported.
    -h    Help page.
    -g    Will only check CVT's on GQAM's.
    -r    Will only check CVT's on RFGW's.
    -v    Prints script version and exits.
```

2 Review the information.

Displaying the Version Number of the cvtChecker Utility

1 As **dncs** user, type the following command to view the version of the cvtChecker utility.

```
[dncs@ecnextx9 Utilities]$ cvtChecker.py -v
```

Example Output:

```
8.1.5
```

Note: This example shows that version 8.1.5 is loaded onto the EC.

Retrieving the CVT from GQAMs

The **-g** option of the cvtChecker script provides the CVTs on GQAMs.

1 As **dncs** user, enter the following command to run the **cvtChecker** with the **-g** option. The number of GQAMS found is displayed and you are prompted for the username for the GQAM.

```
[dncs@ecnextx9 ~]$ cvtChecker.py -g
```

Example Output:

```
Found GQAMS:  504
Username for GQAM:
```

2 Enter a valid username for the GQAM and press **Enter**. You are prompted for the password for the GQAM.

Example Output:

```
Password for GQAM:
```

3 Enter the password and press **Enter**. The following output displays:

- System CVT version
- CVT CreationTime
- Device Name
- Device Type
- Device Model Name
- IP address
- Memory Address
- Hex Version
- Dec Version
- Ping status
- Telnet status

4 Review the **/tmp/cvtChecker.log** for any errors.

Retrieving the CVT from RFGWs

The **-r** option of the cvtChecker script provides the CVTs on RFGWs.

1 As **dncs** user, enter the following command to run the **cvtChecker** with the **-r** option. The number of RFGWs found is displayed and you are prompted for the username for the RFGW.

```
[dncs@ecnextx9 ~]$ cvtChecker.py -r
```

Example Output:

```
Found possible RFGW'S: 513
Username for RFGW:
```

2 Enter a valid username for the RFGW and press **Enter**. You are prompted for the password for the RFGW.

Example Output:

```
Password for RFGW:
```

3 Enter the password for the RFGW and press **Enter**. The following output displays:

- System CVT version
- CVT Creation Time
- Device Name
- Device Type
- Device Model Name
- IP address
- Memory Address
- Hex Version
- Dec Version
- Ping status
- Telnet status

4 Review the **/tmp/cvtChecker.log** for any errors.

21

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.

Index

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

October 2018