QPSK (Release E14)

Release Notes and Installation Instructions

Please Read

Important

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

Notices

Trademark Acknowledgements

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

Third party trademarks mentioned are the property of their respective owners.

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

Publication Disclaimer

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

Copyright

Contents

About This Guide

Introduction

These upgrade and installation instructions provide you with the following information:

- An overview of what's new in the Quadrature Phase-Shift Keying (QPSK) E14 software upgrade for the Model D9482 QPSK Modulator
- Guidelines that define how and when to monitor Explorer® Digital Home Communications Terminals (DHCTs) sign-on rates
- A description of the optional QPSK range extension features, which allow DHCTs to sign on to the system and operate at extended distances from the headend

Who Should Upgrade to QPSK E14 Software?

The significant reduction in reboots with QPSK C81 code can keep a new DHCT from getting an IP address until another DHCT released its connection to the QPSK modulator. Replacing C81 with E14 fixes this issue.

For users of SR 2.7/3.7/4.2, additional features are incorporated in QPSK E14 as described in ***What's Different?*** (on page 2).

The E14 version of QPSK modulator software was tested and verified with System Release (SR) 2.7, 3.7, 4.2.

If you have any questions regarding the compatibility of QPSK E14 with your current system release, call Cisco Services before installing the QPSK E14 software.

Audience

These instructions are written for headend technicians using the Model D9482 QPSK Modulator with either the Cisco Resident Application (SARA) or a third-party resident application.

These instructions are also written for Cisco Services engineers and cable service provider personnel qualified in the following skills required to complete the upgrade process successfully:

- Working knowledge of UNIX vi editor or the text editor on your system
- Recognizing differences between system errors currently seen on your Digital Broadband Delivery System (DBDS) network and new DBDS network errors
- Troubleshooting for basic system errors
- Stopping and starting system components
- Backing up file systems and databases
- Working knowledge of Sun hardware and Sun Disksuite software

  Note: The Sun Disksuite software is necessary for the disk mirroring procedure.
- Working knowledge of Solaris
- Working knowledge of script languages

Document Version

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

Description	See Topic
Updated procedures to check for multiple config files	***Checking for Multiple Config Files*** (on page 8)

1

Introducing QPSK E14

Introduction

This chapter describes the changes and enhancements that are included with QPSK E14 and outlines the known issues that are still outstanding.

In This Chapter

What's Different?

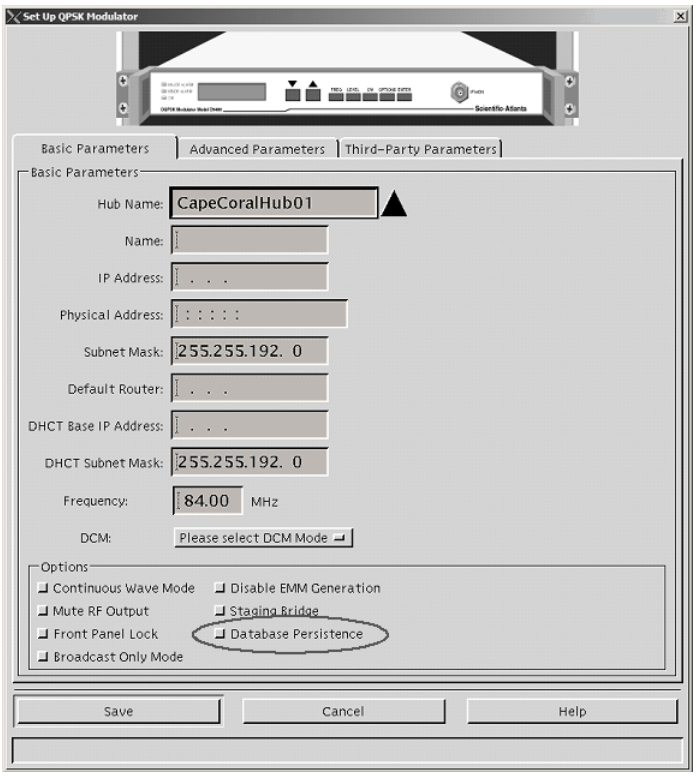
QPSK Enhancements

QPSK software release E14 introduces a new feature called *QPSK database persistence*. When this feature is activated, a QPSK that has spontaneously reset or is manually reset quickly (powered down for only a few seconds) will attempt to recover its database of signed-on DHCT information from its RAM. If the recovered data is valid, then DHCTs do not need to sign back onto the QPSK modulator after the reset, and the DHCTs' operational status in the DNCS remains unchanged. If the database cannot be recovered, the QPSK modulator instructs the DNCS to set the operational status to "unknown" for all DHCTs on that QKSK modulator, and the DNCS will instruct all the DHCTs on the QPSK to sign back on to the network.

Note: After the QPSK is reset, the database recovery process takes 5 minutes for the QPSK to provision and attempt to recover the database. Any DHCTs that are signed on will not be able to communicate with the DNCS for approximately 30 seconds during the reboot, and unsigned DHCTs will not be able to sign on for another 5 minutes after the power-up.

The DHCT does not store its IP address in non-volatile memory. The DNCS must be utilized to reassign an IP address to the DHCT. Therefore, database persistence does not affect the rate at which DHCTs sign on after they are rebooted either due to a power outage or a software download.

To set up a QPSK modulator to use database persistence, select **Database Persistence** in the **Set Up QPSK Modulator** window.



To support this feature, QPSK software version E14 or later must be installed on the QPSK modulator, and the DBDS must be operating at SR 2.7/3.7/4.2 or later (CR 58150).

Important: The QPSK does *not* hold data in its memory indefinitely. If the QPSK is powered down for more than a few seconds, it may not be able to recover its database of sign-on DHCT information.

Note: This feature is called *Database Persistence* in the DNCS GUI. However, it is not true persistence because the data does not persist indefinitely.

Adding and Splitting QPSK Modulators

The process for splitting hubs is different with QPSK E14 installed on your system and with QPSK database persistence turned on. Refer to one of the following documents, depending on the system release installed on your system.

SR 2.2 Service Pack 3 and Earlier

Adding and Splitting QPSK Modulators for System Release 2.2 Service Pack 3 and Earlier (part number 4004456, published April 2005)

SR 2.5/3.5/4.0

Adding and Splitting QPSK Modulators for System Releases 2.5, 3.5, and 4.0 (part number 4002549, published September 2005)

SR 2.7/3.7/4.2

Adding and Splitting QPSK Modulators for System Releases 2.7/3.7 or SR 4.2 (part number 4015109, expected publish date: early 2007)

CRs Corrected in QPSK E14

CR 49349: QPSK stops signing on new DHCTs unless a signed DHCT is released

An issue with QPSK C81 and earlier releases can cause an "artificial sign-on limit," an arbitrary sign-on limit for DHCTs, much less than the advertised 16000. In this condition, the QPSK sets a dynamically reducing limit to the number of DHCTs it can sign on and hence allocate IP addresses. When this limit becomes less than the DHCTs signed on to the QPSK, a new DHCT will not get an IP address unless another DHCT is released.

This "artificial sign-on limit" takes months to exhibit. Due to a significant reduction in reboots with C81, this error became more prominent on that release. Replacing C81 with QPSK E14 fixes this issue.

CR 50664: Possible modulator code download condition

In QPSK C81, QPSK modulators would occasionally lock up if new modulator code was downloaded due to unintentional reboot during a period of high traffic. In this situation, the workaround was to revert to the older code from the DNCS, wait 15 minutes, and then intentionally reboot the modulator to download the new code. This issue has been corrected with QPSK E14.

CR 54139: QPSK modulator Ethernet driver RX can freeze

In earlier releases, the QPSK modulator's Ethernet MAC RX process could freeze. If this occurred, the out-of-band path was cut off, and the modulator needed to be rebooted. CR 54139 adds functionality to keep the Ethernet MAC RX process from freezing.

Known Issues

There are no known issues at the time of this release.

2

Upgrading the QPSK Software

Introduction

This chapter includes procedures to determine your current version of QPSK software and describes how to upgrade to QPSK E14.

In This Chapter

Verify the Current Software Version on the DNCS

Introduction

Before attempting to upgrade to QPSK E14, verify the number of configuration files in use and what QPSK software version is associated with each configuration file.

On occasion, for testing purposes, the configuration file for a test device or a set of test devices is changed to a non-standard value (for example qpsk111.config instead of qpsk.config). If your site has been involved in this type of testing (and you are now ready to use the released code again), you should update the configuration file setting for your test units to reflect the default values.

Note: The default configuration file for the QPSK is **/tftpboot/qpsk.config**.

Failure to correct a unit from using a unique configuration will result in the unit remaining in the uniquely-specified configuration. Specifically, it will not load the new code and it will continue to load the code specified in the unique configuration file.

In extremely rare cases, the configuration file may have been specified in or may need to be specified in the /etc/bootptab file. In the event that a headend device fails to load the code you intended it to receive, you should check to see if a unique file was specified either through the DNCS GUI or in the /etc/bootptab file before contacting Cisco Services for assistance.

Checking for Multiple Config Files

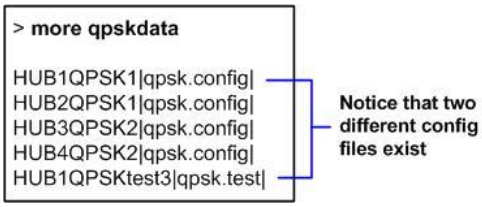
1. From the DNCS Administrative Console, click **Utilities** and click **xterm**. The xterm window opens.
2. Type **dbaccess dncsdb <<%** and press **Enter**.
3. Type **unload to qpskdata select qmod_name, configfile from davic_qpsk;** and press **Enter**.
4. Type % and press **Enter**. A result, similar to the following output, appears.

```
Database selected.

5 row(s) unloaded.

Database closed.
```

5 Type **more qpskdata** and press **Enter**. A result, similar to the following output, appears.



6 Did more than one config file appear?

- If **yes**, keep the xterm window open and go to step 7.
- If **no**, go to ***Checking the Software Version Associated with the config File*** (on page 9).

7 Do you need to continue to run different versions of QPSK software on some QPSKs in your network?

- If **yes**, refer to ***Load Multiple Versions of QPSK Code*** (on page 41).
- If **no**, go to step 8.

8 Update the QPSKs to use the same config file by performing the following steps:

a From the DNCS Administrative Console, click **Element Provisioning** and click **QPSK**. The QPSK List window opens.

b Select the QPSK, click **File** and select **Open**. The Set Up QPSK window opens.

c Click **Advanced Parameters** and modify the configuration file, as needed.

9 Go to ***Checking the Software Version Associated with the config File*** (on page 9).

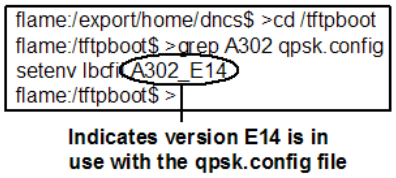
Checking the Software Version Associated with the config File

1 From the xterm window, type **cd /tftpboot** and press **Enter**. The tftpboot directory becomes the working directory.

2 For each unique config file identified in ***Checking for Multiple config Files*** (on page 8), type **grep Appl <config file name>** and press **Enter**.

Example: grep Appl qpsk.config

Result: A result, similar to the following output, appears.



3 Is the proper version of software installed?

- If **yes**, type **exit** and press **Enter**. You do not need to upgrade the QPSK software.
- If **no**, go to ***The Upgrade Process*** (on page 10).

The Upgrade Process

Introduction

This section provides a timeline for each stage of the QPSK E14 upgrade and installation process. Read this section carefully; some of these procedures are not addressed in system release installation instructions.

Is Service Impacted During the Upgrade?

The service impact to subscribers will vary based on the applications installed on your system and how the applications react to a loss of both the forward and reverse QPSK data paths. For a subscriber not actively using an interactive application, the outage will most likely go unnoticed.

When the QPSK starts to load new software, all of the DHCTs will lose IP connectivity and the two-way mode. Depending on the system, these DHCTs may take a few minutes to several hours to reconnect. The DHCTs will be unable to use interactive services until they receive a new IP address.

Taking Advantage of the VLSM Feature

To take advantage of variable-length subnet masks (VLSM), you must have SR 2.x/3.x or later installed. SR 2.x/3.x and later utilize the Solaris 8 operating system (OS) that includes full support for VLSM. To optimize network configuration and to take advantage of VLSM network technology, Cisco recommends that you modify all applicable network configuration files on both the Digital Network Control System (DNCS) and the Application Server when upgrading to SR 2.x/3.x or later.

How Much Time is Required to Install the New QPSK Software?

The initial monitoring of the system and installing the QPSK E14 software requires approximately 2 hours. When installation is complete, continue to monitor the DHCT sign-on traffic for several hours. The following table provides a description and approximate time required for each stage of the QPSK E14 upgrade and installation process.

Stage	Description	Time Required	Refer to
1	Monitor the available DNCS disk space. If the percentage of used disk space exceeds 80 percent, the DNCS is at risk of becoming full, which would cause the DNCS to stop abruptly.	5 minutes	***Monitor the DNCS Disk Space*** (on page 12)

Stage	Description	Time Required	Refer to
2	Monitor the DHCT sign-on rates using the data produced by the signonCount utility. Review the signonCount utility Help window for an understanding of the procedure.	30 - 60 minutes	***Monitor DHCT Sign-on Rates*** (on page 13)
3	Set the DNCS tracing levels to trace the maximum level of sign-on activity.	5 minutes	***Set DNCS Tracing Levels*** (on page 15)
4	Display and interpret the data produced by the signonCount utility so you can take appropriate action.	30 - 60 minutes	***What to Look for in the signonCount Data*** (on page 18)
5	Obtain the software either by ordering the software CD or by connecting to an FTP server maintained by Cisco Services.	5 minutes	***Obtain the Software*** (on page 22)
6	Install the QPSK E14 software onto the DNCS.	15 minutes	***Install QPSK Software onto the DNCS*** (on page 24)
7	Reset a QPSK modulator. Allow the new QPSK E14 software to download to the QPSK modulator. Verify that the software successfully downloaded to the QPSK modulator. Monitor DHCTs as they reconnect to the system.	15 minutes per unit, average	The following sections in this guide: ■ ***Download Software to the QPSK Modulators*** (on page 26) ■ ***Continue to Monitor the DHCT Sign-On Traffic*** (on page 35)
8	After downloading the QPSK E14 software to all modulators, continue to monitor the DHCT sign-on traffic for 10 to 48 hours. **Note:** You do not need to watch the sign-on traffic continuously for 10 to 48 hours. You should check occasionally during this time to ensure that the total number of responding DHCTs is returning to the pre-upgrade level.	10 - 48 hours	***Continue to Monitor the DHCT Sign-On Traffic*** (on page 35)

Monitor the DNCS Disk Space

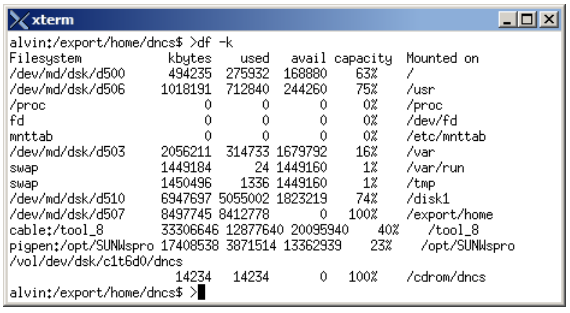
Introduction

The utilities used in monitoring the system while you are loading new software require that you enable the process tracing for some DNCS functions. This tracing may result in a significant increase in the size of the dncsLog file. If allowed to grow unchecked, the dncsLog file could, in rare cases, fill the hard disk and as a result cause the DNCS to stop functioning.

The procedures in this section describe how to monitor the DNCS disk space that is presently available. The procedures also indicate when to call Cisco Services to take action should the system start to run low on storage space. Use these monitoring procedures each time you are directed to check available disk space.

Monitoring Available Disk Space

1 From an xterm window, type **df -k** and press **Enter**. A list of DNCS files and disk space appears in the xterm window.



2 Locate **/var** in the **Mounted On** column, and locate the **percentage** that relates to /var in the **Capacity** column.

3 Is the capacity of used disk space in /var less than 80 percent?

- If **yes**, it is safe to set the tracing levels for DNCS processes. But first, go to ***Monitor DHCT Sign-on Rates*** (on page 13) to understand how the signonCount utility can facilitate the DHCT sign-on process.
- If **no**, call Cisco Services for assistance in freeing up space.

Monitor DHCT Sign-on Rates

Introduction

When DHCTs download new software for the operating system and resident application, they lose the contents of their volatile memory. After the download, DHCTs sign back on to the network and their network configuration data is reloaded. The signonCount utility is useful in monitoring the rate at which DHCTs sign on to the network.

Because some DHCTs make repeated attempts to sign on to the network before they are successful, too many sign-on attempts by DHCTs contribute to network congestion. The signonCount utility can help system operators quickly identify those DHCTs that are having trouble signing on, and the utility can then be used to facilitate the DHCT sign-on process.

When to Use the signonCount Utility

The signonCount utility enables system operators and Cisco engineers to monitor the rate at which DHCTs sign on to the network. This monitoring is required in the following circumstances:

- When the QPSK modulator and demodulator software is upgraded—In this case, the signonCount utility is used in the following two situations:
  - The first situation is to determine if the system is healthy enough to be upgraded. If it is not, the signonCount utility also provides a secondary mode of operation that can dramatically improve the health of the system prior to moving forward with the upgrade.
  - The second situation is to use the signonCount utility to provide more meaningful guidance regarding when you can move forward with upgrading the next QPSK modulator. Previous upgrade guides instructed you either to wait a little while between upgrading units or to monitor the log file, but they offered no real tools to help in this effort.
- 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.

Two Modes of Operation

You can run the signonCount utility in two modes: **Fix Mode Off** and **Fix Mode On**. Both modes help system operators monitor the rate at which DHCTs are trying to sign on to the network:

- When run in *Fix Mode Off*, the utility takes no corrective action regarding DHCTs that are having difficulty signing on.
- When run in *Fix Mode On*, however, the utility reboots those DHCTs that have tried to sign on more than three times during a 10-minute period.

Note: By forcing DHCTs that are having trouble signing on to reboot, the memory in the DHCT is refreshed and the sign-on process is made easier.

Important: By default, the utility runs in Fix Mode Off. Because the utility interacts with the database when run in Fix Mode On, Cisco recommends that you contact Cisco Services before switching modes.

Accessing the signonCount Help Window

The DNCS provides an online help window for the signonCount utility. The information in the help window may supplement the information and procedures in these instructions.

Note: If the signonCount utility is not currently installed on your system, call Cisco Services for assistance.

To access the signonCount utility help window, complete the following instructions.

1. Open an xterm window on the DNCS and then maximize the window.
2. Type **signonCount -h** and press **Enter**. The help window for the signonCount utility opens.
3. Press the **Spacebar** as often as necessary to page through the help window.

Set DNCS Tracing Levels

Introduction

Before you begin using the signonCount utility, you need to set the tracing levels of three DNCS processes to level 2. By setting the tracing levels for these processes to level 2, you ensure that the DNCS captures the maximum level of detail for these processes. The three DNCS processes are:

- hctmConfig
- hctmMac
- hctmProvision

CAUTION:

Activating the tracing process as described in this section could cause the dncslog file to grow large enough to fill the hard disk. If this is allowed to happen, the DNCS will stop functioning. While gathering data, carefully monitor the disk usage.

Once you begin the tracing process, do not leave the DNCS unattended. The disk space capacity must be closely monitored because it can change rapidly.

If the disk space capacity approaches or exceeds 80 percent, call Cisco Services immediately.

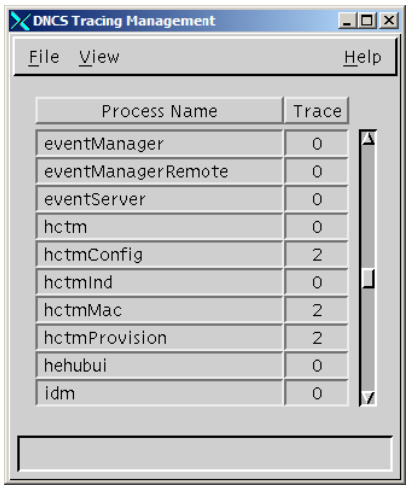
Setting the DNCS Tracing Levels

To set the tracing levels of the hctmConfig, hctmMac, and hctmProvision processes to level 2, complete the following instructions.

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

2 Click **Tracing**. The DNCS Tracing Management window opens.

3 Scroll until the hctmConfig, hctmMac, and hctmProvision processes come into view.



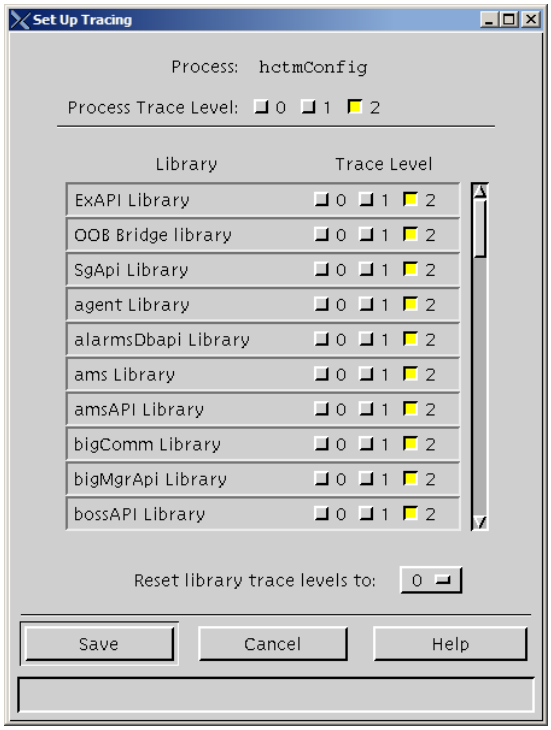
4 Are the tracing levels, in the Trace column, for all three of these processes already set to 2?

- If **yes**, go to ***What to Look for in the signonCount Data*** (on page 18).
- If **no**, go to step 5 to begin setting the tracing levels.

5 Double-click one of the processes. The Set Up Tracing window opens.

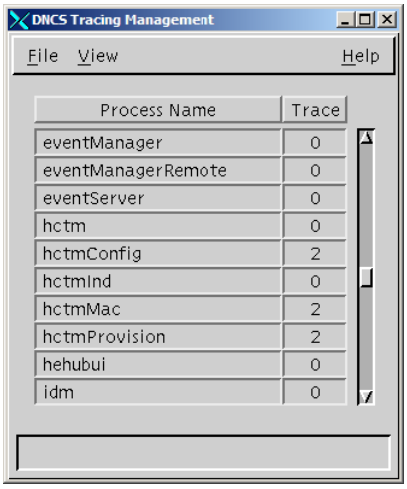
Example: Double-click **hctmConfig**.

6 Select **2** in the **Process Trace Level** field and then click **Save**. The DNCS Tracing Management window updates with the new tracing level, and the Set Up Tracing window closes.



7 Repeat steps 5 and 6 to update the tracing level to 2 for the other two processes (if necessary).

8 When you are finished, the DNCS Tracing Management window should look like the following example. The tracing levels for the hctmConfig, hctmMac, and hctmProvision utilities are set to level 2.



9 Click **File** and select **Close** to close the DNCS Tracing Management window.

10 Go to ***What to Look for in the signonCount Data*** (on page 18).

What to Look for in the signonCount Data

Introduction

This section provides instructions on how to display the signonCount utility interface, provides an explanation of each field of the interface, and states which fields you should focus on first.

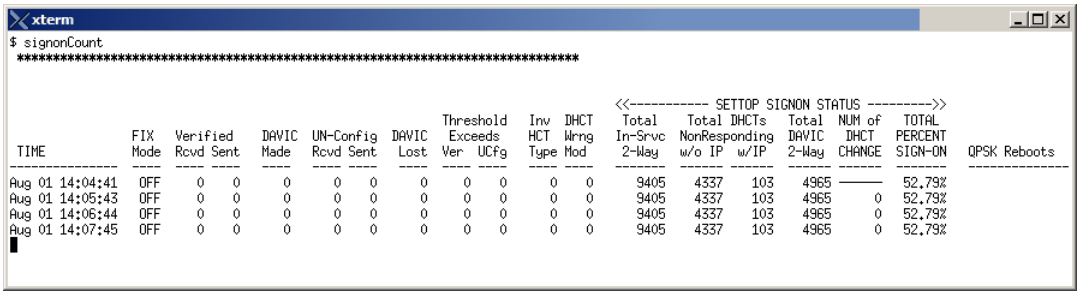
Displaying the signonCount Interface

To display the interface of the signonCount utility, complete the following instructions.

1. Open an xterm window on the DNCS.
2. Click and drag the edges of the xterm window to maximize the screen width. The signonCount utility fills the width of the screen with data.
3. Type **signonCount** and press **Enter**. The signonCount utility interface opens.
4. Look at the following example of the signonCount utility interface; then, go to ***Understanding the signonCount Utility Data Fields*** (on page 18).

signonCount Utility Example

The signonCount utility interface is similar to the following example.



Understanding the signonCount Utility Data Fields

This section provides an explanation of the meaning associated with each field of the signonCount utility.

TIME	The system polls the communication link between the QPSK modulators and the DNCS every minute and records the date and time.
FIX Mode	This field reveals whether the signonCount utility is configured to correct DHCT sign-on problems (Fix Mode On) or whether the utility is running in information-only mode (Fix Mode Off). **Important:** Do not change modes unless you have been instructed to do so by Cisco Services engineers. **Note:** By default, the utility runs in Fix Mode Off.
Verified Rcvd	The QPSK modulator reports the number of DHCTs that have made sign-on requests.
Verified Sent	The DNCS has responded to this number of DHCTs.
DAVIC Made	The QPSK modulator reports the number of DHCTs that have connected to the QPSK modulator and are waiting for UN-Config information.
UN-Config Rcvd	This number of DHCTs is requesting a UN-Config message from the DNCS. The UN-Config message contains information, like an IP address, that allows DHCTs to sign on to the network.
UN-Config Sent	The DNCS has sent this number of UN-Config messages to DHCTs, allowing the DHCTs to sign on to the network. At this point, the DHCTs are physically in two-way mode and have completed the sign-on process.
DAVIC Lost	This field indicates the number of DHCTs that have lost the communication link with the QPSK modulator. The QPSK modulator then sends a message to DHCTs that have lost the communication link. The message requests that the DHCTs recalibrate themselves with the modulator so the entire sign-on process can begin again.
Threshold Exceeds Ver	The DNCS reports the number of DHCTs that simultaneously attempt to verify their configuration in excess of what the system queues allow. The numbers in this column should be zero.

Threshold Exceeds UCfg	The DNCS reports the number of DHCTs that simultaneously attempt to sign on to the system in excess of what the system queues allow. The numbers in this column should be zero.
Inv HCT Type	This field represents the number of DHCTs reporting a DHCT type that does not match the values presently in the database.
IHCT Wrng Mod	This field represents the number of DHCTs that have responded through a QPSK modulator that differs from the modulator through which the DHCT responded in the past. Numbers in this column typically represent DHCTs that have been moved from one subscriber's home to another without having gone through the correct process.
Total In-Srvc 2-Way	The utility reports the number of DHCTs listed in the database with a status of In-Service 2-Way. These DHCTs should be capable of two-way communication.
w/o IP	This field represents the number of two-way DHCTs that have never connected to the network to receive an IP Address. These DHCTs should be capable of two-way communication, but they are listed as non-responders.
w/IP	This field represents the number of DHCTs that have connected at least once to the network and have an IP address, but they are presently not responding.
Total DAVIC 2-Way	This field represents the number of DHCTs that have physically signed on to the network with two-way communication ability.
NUM of DHCT Change	This field represents the number of DHCTs with two-way capability that have been added to or removed from the database during the last minute. Substantial numbers in this column usually indicate staging activity.
TOTAL PERCENT SIGN-ON	The DNCS reports the percentage of DHCTs with two-way capability that are signed on to your network.
QPSK Reboots	In the event that a QPSK modulator reboots, the name and ID of the modulator is listed in this column.

Concentrate on Three Fields

Allow the system to gather signonCount data for several minutes and then examine the numbers in the following fields:

- **Verified Rcvd** (Verified Received)
- **Verified Sent**
- **DAVIC Made**

These fields track the number of sign-on requests made by DHCTs (Verified Rcvd and Verified Sent), as well as the number of sign-on requests that were successful (DAVIC Made). Ideally, the numbers in the three fields should be equal.

When to Call Cisco Services for Assistance

If you notice that the numbers in the DAVIC Made column are regularly becoming less than 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. Contact Cisco Services. Cisco Services engineers may log in to your system and examine the logfiles associated with the hctmConfig, hctmMac, and hctmProvision processes. Additionally, Cisco Services engineers may instruct you to run the signonCount utility in Fix Mode On.

Important: Do not run the utility in Fix Mode On unless you have been instructed to do so by Cisco Services engineers.

If the TOTAL PERCENTAGE SIGN-ON number is less than 85 percent, contact Cisco Services. There are a number of possible reasons for low sign-on percentages. Most are easily remedied; however, they must be looked at on a case-by-case basis.

Important: If your system is not currently operating in a typical manner, do not proceed with this upgrade. Instead, call Cisco Services.

Obtain the Software

Introduction

There are two ways to obtain the QPSK E14 software from Cisco. You can order the software CD or you can download the software by connecting to an FTP server maintained by Cisco Services. This section provides instructions for downloading the software from the Cisco FTP Server.

Downloading the QPSK Software from an FTP Server onto the DNCS

Access to the FTP server requires current FTP server site access information. Because many sites do not allow an open Internet connection to the DNCS for security reasons, the following procedure provides generic instructions to access the FTP server and download the software.

This procedure also assumes the software is in a TAR file format. The TAR file is a compressed image format that is the typical format of a software image released on CD. If you have any questions about this process, contact Cisco Services.

Accessing the FTP Server

Complete the following steps to access the FTP server.

1. Open an xterm window on the DNCS, if necessary.
2. Type **su root** and press **Enter** to log on as root user. The password prompt appears.
3. Type the root password and press **Enter**.
4. Do you have a directory created for downloaded files?
   - If **yes**, go to step 5.
   - If **no**, follow this procedure to create a directory.
     a. Type **mkdir /export/home/dncs/download/QPSK** and press **Enter**.
     b. Type **cd /export/home/dncs/download/QPSK** and press **Enter**.
     c. Go to step 7.
5. Clear the current contents of the download directory. First type **pwd** to confirm you are in the correct directory; then, type **rm -rfi ***.
6. You will be prompted to delete each file in the directory. Press **y** to delete each file.

7 Log on to the Cisco FTP server.

Notes:

- The address of the server is **ftp.sciatl.com** or **192.133.243.133**.

  Note: The address for the Cisco FTP server is subject to change. If you are unable to reach the FTP server, please contact Cisco Services for the latest address.

- The username is **anonymous**.
- The password is the email address of the person logging in.

8 Choose one of the following options to navigate to the directory in which the file is located:

- If you are *outside* of Cisco's firewall, type **cd /pub/scicare/RELEASED/QPSK**
- If you are *inside* of Cisco's firewall, type **cd /external_pub/scicare/RELEASED/QPSK**

9 Type **bin** and press **Enter**. The system sets the ftp transfer mode to binary.

10 Type **hash** and press **Enter**. The system configures itself to display hash marks that show file-transfer progress.

11 Type **prompt** and press **Enter**. The system indicates that interactive mode is off.

12 Type **mget** * and press **Enter**. The system begins copying the file (or files) from the FTP site to the current directory on your DNCS.

13 Type **bye** and press **Enter** to log out of the Cisco FTP server.

14 Type **ls** and press **Enter**. Type the lower case of the letter L in this entry.

15 Verify the file was successfully downloaded to the DNCS from the FTP server.

16 Type **/usr/local/bin/gzip -d QPSKE14.tar.gz** and press **Enter**.

17 Type **tar xvf QPSKE14.tar** and press **Enter**. The system extracts the files.

18 Go to ***Install QPSK Software onto the DNCS*** (on page 24).

Install QPSK Software onto the DNCS

Introduction

This section provides instructions for installing the QPSK E14 version of software. You can install the software from either the Cisco FTP Server or from a CD.

Before You Begin

Locate and have available the CD with software version of QPSK currently installed on your system. In the unlikely event that you need to roll back to the current version of QPSK software, you will need to have that CD available.

Read Me

Please read all instructions before beginning the upgrade process. If you are uncomfortable with any of the procedures presented in these instructions, contact Cisco Services for assistance.

Backing Up the Current QPSK Configuration File

Before installing the new QPSK software, make a backup file of the qpsk.config file currently installed on the DNCS by completing the following steps.

1. From an xterm window on the DNCS, log in as a **root** user.
2. Type **cd /tftpboot** and press **Enter** to change the directory.
3. Type **cp -p qpsk.config qpsk.config.old** and press **Enter** to make a backup copy of the current file.

Installing the New QPSK Software

Complete the following steps to install the QPSK E14 software onto the DNCS.

1. Choose one of the following options:
   - If you are installing the software from a CD, insert the CD labeled **QPSK Mod/Demod E14** into the CD-ROM drive of the DNCS. The system automatically mounts the CD to /cdrom/cdrom0 within 30 seconds.
   - If you are installing the software from the FTP site, go to step 3.
2. Type **df -n** and press **Enter**. A list of the mounted file systems appears.

   Note: The presence of /cdrom in the output confirms that the system correctly mounted the CD.
3. Depending on the location of the QPSK software, use one of the following commands to switch to the correct install directory:

- If installing from a CD, type **cd /cdrom/cdrom0** and press **Enter**.
- If installing from an FTP server, type **cd /export/home/download/QPSK** and press **Enter**.

4 Type **./usr/sbin/install_pkg** and press **Enter**. (Be sure to include a . [period] at the beginning of the entry.) A confirmation message appears.

5 Type **y** and press **Enter** to start the installation. The QPSK software installs.

6 Depending on the location of the QPSK software, use one of the following commands to switch to the correct install directory:

- If installing from a CD, type **cd/; eject cdrom** and press **Enter**. The CD ejects.
- If installing from an FTP server, type **rm -rf SAIqpsk *tar** and press **Enter**.

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

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

9 Go to ***Download Software to the QPSK Modulators*** (on page 26).

Download Software to the QPSK Modulators

Introduction

After installing the QPSK E14 software on the DNCS, your next step is to upgrade the QPSK modulators.

When you reset a QPSK modulator, the DNCS downloads the new QPSK software to the QPSK modulator and, if needed, to the QPSK demodulator(s). Follow the instructions in this section to download the QPSK E14software to the QPSK modulators.

Important: Cisco recommends that when you are downloading software to the QPSKs, begin with a test hub or a QPSK with the smallest DHCT population, so that you can confirm the system configuration without affecting subscribers.

Perform the procedures in this section for each QPSK being upgraded.

Downloading Software to Local QPSK Modulators

If your QPSK modulators are located nearby, complete the following steps to download the new software to the QPSK modulators.

Important: The following procedure contains steps that are time-sensitive. Read all of the procedure before beginning so that you are prepared to leave the modulator powered off for the proper amount of time. Failure to do so can affect whether or not database information persists.

1. Power off the QPSK modulator and any associated demodulators.
2. Do you want the information in the database to persist?
   - If **yes**, wait a few seconds, and power on the modulator *only*.
   - If **no**, wait at least 5 minutes, and then power on the modulator *only*.
   - If your system release does not support database persistence, or if database persistence is not turned on for this modulator, wait a few seconds, and power on the modulator *only*.
3. Wait until the power-on self-test sequence is completed and the LCD shows the power-on self test information. This process may take up to 10 minutes.
4. Press the **Status** button on the front panel of the QPSK modulator until the LCD displays **STATUS: Software Version**.

5 Does the LCD display include **A302_E14** on the bottom line?

- If **yes**, the software downloaded successfully. Power on the demodulators, and go to ***Continue to Monitor the DHCT Sign-On Traffic*** (on page 35).
- If **no**, go to the Set Up QPSK Modulator window on the DNCS administrative console and verify that the modulator is set to use qpsk.config. Also, make sure that there is no entry for this unit in the bootptab file. Then repeat this procedure. If the software does not download after the second attempt, call Cisco Services.

Downloading Software to Remote QPSK Modulators

If your QPSK modulators are *not* located nearby, complete the following steps to download the new software to the QPSK modulators.

1 In an xterm window on the DNCS, type **cd /dvs/dncs/tmp** and press **Enter**.

2 Type **ls -ltr boot*** and press **Enter**. The window displays a list of files in the current directory whose filename begins with boot.

3 Look through the list of files and find the most recent file named **bootpd.###**.

Notes:

- The ### extension is a 3-digit number that identifies each bootpd file. Whenever a file reaches its maximum size, the DNCS creates a new bootpd file with the next extension. For example, when the bootpd.005 file is full, the DNCS creates bootpd.006.
- When the bootpd.999 file is full, the DNCS creates a new file called bootpd.000 and overwrites the old bootpd.000 file. The most recent file in the list will have the most recent timestamp.

4 Using the name of the most recent bootpd.### file, type **tail -f bootpd.### | awk '/qpsk/'** and press **Enter**.

Note: If the most recent file is bootpd.065, type tail -f bootpd.065 | awk '/qpsk/'.

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

6 Select the **Element Provisioning** tab.

7 Click **QPSK/CMTS**. The QPSK List window opens.

8 From the QPSK List window, highlight the device you are upgrading.

9 Do you want the information in the database to persist?

- If **yes**, select **File** and choose **Reset**. A confirmation message appears.
- If **no**, select **File** and choose **Reset And Clear DB**. A confirmation message appears.
- If your system release does not support database persistence, or if database persistence is not turned on for this modulator, select **File** and choose **Reset**. A confirmation message appears.

10 Click **Yes** on the confirmation message. A message appears stating that the QPSK has received the reset command.

11 In the xterm window, watch the bootpd file for confirmation that the QPSK has rebooted. The confirmation message contains the IP address of the QPSK modulator that you reset and looks like the following example:

```
found 172.20.1.17 (qpsk_172.20.1.17)
Jan 12 09:48:49 bootpd: info(6):   bootfile="/qpsk.config"
Jan 12 09:49:10 bootpd: info(6):   DNCS
QPSK[qpsk_172.20.1.17:ht=ethernet:sm=255.255.192.0:ip=172.20.1
.17:ha=0x0002DE9132E8:vm=rfc1048:gw=10.253.0.254:sa=dncsatm:bf
=qpsk.config:]
```

12 When this confirmation message appears, the QPSK has rebooted. Before downloading the software to the next modulator, go to ***Continue to Monitor the DHCT Sign-On Traffic*** (on page 35).

What Is the QPSK Range Extension Feature?

Introduction

With prior versions of software, the Model D9482 QPSK Modulator was capable of successfully connecting and operating DHCTs within a distance of approximately 128 km round trip (64 km each way when forward and reverse paths are equal).

Note: One kilometer equals 0.621 miles.

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.

The width of the ranging slots limits the maximum distance between DHCTs for successful connection and operation. Because the current modulator software assumes that the closest DHCT is at the same location as the QPSK modulator, an unnecessary limit is placed on the furthest distance that a DHCT can be located from that QPSK modulator.

Some cable service providers would 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 for the Model D9482 QPSK Modulator allows Explorer DHCTs to sign on to the system and operate properly at extended distances from the QPSK modulator. (This feature provides the resolution to CR 6922.)

Using the front panel of the QPSK modulator, you can select one of nine different values of one-way range extension. The front panel displays the extension distance in kilometers.

Note: Though it is not possible to extend the maximum distance between the DHCTs, which must remain within 64 km, it is possible to delay the timing within the modulator such that the distance to all DHCTs can be extended. This software feature allows you to extend the distance to the closest DHCT from 0 km to 248 km, one way, in steps of 31 km.

Distance and Delay

The distance that appears on the front panel of the QPSK modulator is approximate and based on fiber with a propagation velocity of 68 percent of the speed of light in a vacuum.

Note: The modulator has no way of calculating how much coax or fiber is deployed between and to the DHCTs.

If you anticipate that DHCTs will be deployed near the limits of the distance ranges, Cisco recommends that you use delay numbers and translate the numbers to the actual length of fiber and/or coaxial cable deployed.

The delay numbers used in the modulator are as follows:

- With no extension, the modulator can range DHCTs to a distance corresponding to 628 microseconds round trip.
- Each front-panel step of 31 km (one way) corresponds to a round-trip delay extension of 300 microseconds.

Distance Between DHCTs

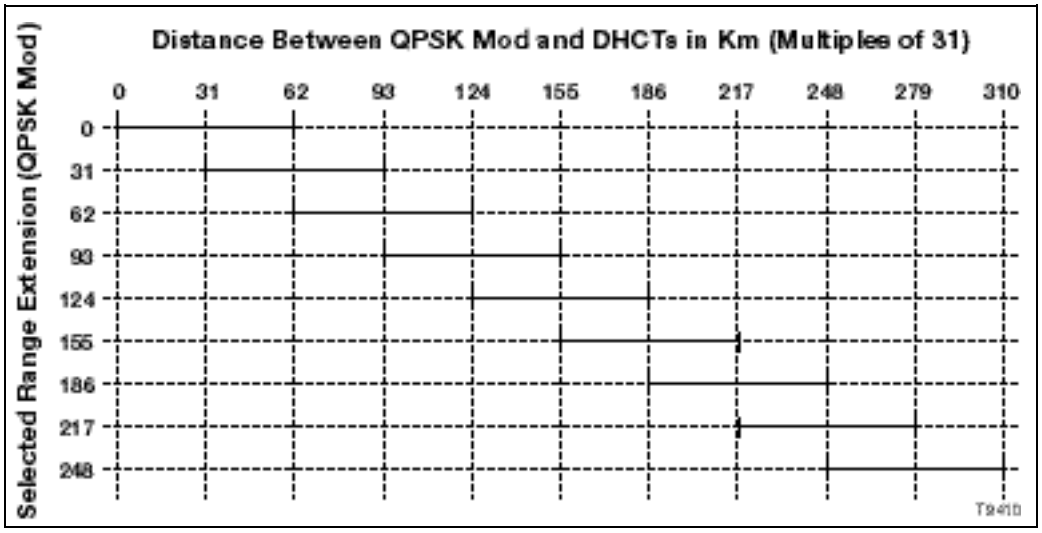
When the range extension mode is activated, the QPSK modulator expects a transmission delay that is equal to or greater than the distance value programmed into the QPSK modulator.

The distance between the closest and the furthest DHCT is still a maximum of 64 km. Thus, the closest a DHCT can be located is the distance programmed on the front panel of the QPSK modulator. The furthest a DHCT can be located from the headend is the sum of the programmed distance plus the 64 km ranging distance.

DHCTs operated outside these bounds may not be able to connect to the system and may also potentially interfere with the transmissions of other DHCTs. The programmed distance applies to all of the demodulators connected to that modulator.

Range Distance Settings Diagram

The following diagram illustrates the correct range distance settings.



Example: With 155 km set on the QPSK, the closest distance you could locate a DHCT to a QPSK modulator is 155 km. The furthest distance you could locate a DHCT to a QPSK modulator is 217 km.

Network Configuration Application Rules

Follow these application rules when configuring the network for the QPSK ranging-distance extension mode.

Rule	Description
1	The QPSK modulator operates normally when no delay value is configured.
2	Only four D9482 QPSK Demodulators can be connected to a QPSK modulator operating in delay mode. These demodulators must be connected to ATM-25 port locations 5, 6, 7, and/or 8. (Ports 1 through 4 may not be used in the range extension mode.) The configuration at the DNCS should reflect this requirement.
3	The programmed delay distance should be less than or equal to the sum of the transport cable to the hub, plus the shortest optical cable distance on any of the attached nodes.
4	The ranging radius is 0 km to 64 km, with 0 km set at the programmed cable length.

Rule	Description
5	Transport distances are in integer multiples of 31 km to a maximum of 248 km.
6	All four demodulators are delayed by the same value programmed in the QPSK modulator.
7	The distance ranges stated in this document are approximate and based on a velocity of propagation in fiber of 68 percent of the speed of light in a vacuum (3 x 108 meters per second). Corrections to the setting of the QPSKs should be made where these distances do not apply, as in coaxial cable.
8	DHCTs closer than the programmed distance value may not range and may interfere with other DHCTs.
9	The delay distances that appear on the front panel of the QPSK are one-way path distances and assume an equal distance path on the forward and reverse connection. It is not necessary for the forward and reverse path to be the same distance as long as the total propagation delay matches the equivalent time delay.
10	It will not be possible to use a co-located DHCT directly connected to the QPSK modem as a test device for QPSK link verification when the ranging extension mode is used. This connection violates rule 8. However, you can test for QPSK link verification with a DHCT directly connected to the QPSK as long as the reverse path is not active.

Activate the Range Extension Feature (Optional)

Introduction

This section provides instructions for changing the modulator-to-node distance settings for the QPSK modulators on your system.

Change the Distance Settings

If the modulator-to-node distance of the QPSK modulators on your system is more than 64 km, complete these steps to change the distance settings.

1 If the hub you are configuring supports existing customers, disconnect the **modulator RF output cable** for 15 minutes. Otherwise, go to step 2.

Note: While the QPSK is disconnected, the DHCTs on the hub are not fully functional.

2 See the ***Range Distance Settings Diagram*** (on page 30) to determine the QPSK range distance settings appropriate for your system setup. Then, complete the following steps to set the modulator-to-node distances.

a On the front panel of the QPSK modulator, press the **Options** button until the Mod-Node Dist option appears.

b Select a value of **optical fiber length** that is less than or equal to the sum of the actual optical cable length used for distribution to the remote hub, plus the minimum optical cable length used in the HFC network from the hub.

c Adjust the setting if the cable propagation velocity factor is not equal to 68 percent of the speed of light in a vacuum.

d Press the **up** and **down** buttons to choose the desired one-way fiber delay and then press **Enter**.

Results:

- The first time you change the modulator-to-node distance setting from 0 (zero) to xx, the QPSK will reboot.
- The modified code is downloaded to the QPSK modulator and demodulator.

3 Reconnect the **cable** to force all DHCTs on the hub to reestablish a DAVIC connection with the appropriate time offsets.

4 Place a DHCT at the closest possible location to where the HFC network transitions from optics to cable; then, boot the DHCT and press the **Power** button.

5 Check the delay time on the DHCT diagnostic screen by choosing one of the following options:

- For sites using Cisco Resident Application (SARA), look at the RF Statistical Information diagnostic screen, and choose one of the following options:
  - If the delay value is *less* than 761, the delay time is correct. Go to step 6.
  - If the delay value is *more* than 761, the DHCT is "too close." Repeat step 2 and lower the modulator-to-node distance. Then, reboot the QPSK modulator.
- For sites using the Pioneer resident application, call Pioneer for assistance in determining the current time delay.

6 Place a DHCT in the location with the maximum possible cable distance from the QPSK.

7 Again, check the delay time in the DHCT diagnostic screen by choosing one of the following options:

- For sites using Cisco Resident Application (SARA), choose one of the following options from the RF Statistical Information diagnostic screen:
  - If the delay values fall within the 134 and 761 microsecond delay-time bound, the programmed delay values are correct.
  - If the delay value is less than 134 microseconds, the overall delay between DHCTs is "too far." Call Cisco Services for assistance.
- For sites using the Pioneer resident application, call Pioneer for assistance in determining the current time delay.

Continue to Monitor the DHCT Sign-On Traffic

Introduction

With the signonCount interface displayed, continue to monitor the signonCount utility output to determine the health of your system before downloading the QPSK E14 software to the next QPSK modulator.

Monitoring the DHCT Sign-On Traffic

To determine when it is safe to download the QPSK E14 software to the next QPSK modulator, complete the following steps.

1 Continue to monitor the DHCT sign-on traffic. Your system is healthy if the following conditions are true:

- The values in the **Verified Rcvd**, **Verified Sent**, and **DAVIC Made** columns are the same.
- The values in the **Un-Config Rcvd** and **Un-Config Sent** fields are approximately one fourth of the values in the **DAVIC Made** column.
- The values in the **Threshold Exceeds Ver** and **Threshold Exceeds UCfg** columns are zero.
- No QPSK modulators have rebooted.

2 Is your system healthy?

- If **yes**, go to step 3.
- If **no**, call Cisco Services. Do not continue with these instructions.

3 Wait approximately 15 minutes before resetting the next QPSK. Then, repeat the procedures in ***Download Software to the QPSK Modulators*** (on page 26) for each QPSK modulator you are upgrading.

Important: After resetting each QPSK modulator, continue to monitor the DHCT sign on traffic. As each QPSK modulator reboots, notice that the values in the signonCount utility interface increases. This is to be expected. Also notice that as DHCTs sign on to the system, the values decrease, and the system returns to its healthy state.

- After downloading the QPSK E14 software, continue to monitor the DHCT sign-on traffic for 10 to 48 hours. It is not necessary to watch the sign-on traffic continuously, but you should check occasionally during this time to ensure that there are no problems.
- In the QPSK Reboots column of the signonCount Interface, you may notice that a QPSK modulator reboots automatically. If this occurs, wait 15 minutes before resetting (rebooting) the next QPSK.

4 When you have completed upgrading all QPSK modulators on your system, select **File** from the QPSK List window, and choose **Close**. The QPSK List window closes. Also, the QPSK E14 software is loaded and the range extension default setting is 0 km.

5 You have completed the QPSK E14 software installation.

3

Customer Information

If You Have Questions

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

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

A

Verify the Install Package Exists on the DNCS

Introduction

For system releases that do not include the pre-packaged install tool, we recommend that you verify whether or not the tool exists on your DNCS; because, the tool is required to load new software onto the DNCS. This appendix provides procedures for checking for the install tool, as well as procedures for retrieving it from the Cisco FTP site.

In This Appendix

Check for the Install Tool on the DNCS

Important! If you are using SR 2.7/3.7/4.2, this procedure is not required because the install tool (install.pkg) is pre-packaged within the software.

Checking for install.pkg on the DNCS

1. From an xterm window, type **cd /usr/sbin** and press **Enter**.
2. Type **ls** and press **Enter**.
3. Is the install.pkg file present on the DNCS?
   - If **yes**, resume your installation procedures.
   - If **no**, go to step 4.
4. Log on to Cisco's FTP server.

   Notes:
   - The address of the server is **ftp.sciatl.com** or **192.133.243.133**.

     Note: The address for the Cisco FTP server is subject to change. If you are unable to reach the FTP server, please contact Cisco Services for the latest address.
   - The username is **anonymous**.
   - The password is the email address of the person logging in.
5. Choose one of the following options to navigate to the directory in which the file is located:
   - If you are *inside* of Cisco's firewall, type **cd /external_pub/scicare/RELEASED/SR2.2Patches**.
   - If you are *outside* of Cisco's firewall, type **cd /pub/scicare/RELEASED/SR2.2Patches**.
6. Type **bin** and press **Enter**. The system sets the ftp transfer mode to binary.
7. Type **hash** and press **Enter**. The system configures itself to display hash marks that show file-transfer progress.
8. Type **get install_pkg** and press **Enter**. The system begins copying files into the /export/home/dncs/download/ directory on your DNCS.
9. Type **get install_pkg README_3.0.1.3p2EP1.txt**. The system begins copying files into the /export/home/dncs/download/ directory on your DNCS.
10. Type **bye** and press **Enter** to log out of Cisco's FTP server.
11. Continue with the installation procedures.

B

Load Multiple Versions of QPSK Code

Introduction

The recommended upgrade process for QPSKs is based on a goal of getting all the units upgraded within a short period of time (typically one day). In some cases a site may choose to upgrade the QPSKs over time or may desire to load a unique version of code onto a single QPSK for extended testing. This appendix describes how to accomplish either of these goals.

In This Appendix

Loading Multiple Versions of QPSK Code

Note: If you need to determine which config files are being used by each QPSK, ***refer to Checking for Multiple Con***fig Files (on page 8) for details. For this procedure, we will assume that qpsk.config is the current configuration file.

1. Go to the /tftpboot directory on the DNCS and rename the current qpsk.config file as **qpsk.current**.
2. Install the new version of QPSK software that you intend to use using ***Install QPSK Software onto the DNCS*** (on page 24).
3. From the /tftpboot directory on the DNCS, rename the new qpsk.config file as **qpsk.new**.
4. From the /tftpboot directory on the DNCS, rename the original backup file (for example, rename qpsk.current to qpsk.config).
5. From the QPSK List window on the DNCS, open the entry for the QPSK that should download the new code.
6. Click the **Advanced Parameters** tab, and change the configuration file name from qpsk.config to **qpsk.new**.
7. Click **Apply**.
8. From the QPSK List window on the DNCS, reset the QPSK to which you want to download the new code.
9. Repeat steps 6 through 8 for each QPSK to which you want to download the new code.
10. When you are ready to load code to all of your QPSKs, perform one of the following approaches:
    - **Preferred Approach**
      i. Go to the /tftpboot directory and rename qpsk.new as **qpsk.config**.
      ii. From the QPSK List window on the DNCS, reset all the QPSKs that are using the qpsk.config file.
      iii. From the QPSK List window on the DNCS, change the configuration file value for all QPSKs that currently use qpsk.new to **qpsk.config**. These units do not need to be reset.
    - **Alternative Approach**
      i. From the QPSK List window, change the configuration file value for all modulators using qpsk.config to use **qpsk.new**.
      ii. Reset the changed QPSKs.

      Note: Units that were already using qpsk.new as their configuration file do not need to be reset.

C

Roll Back to the Previous Version of QPSK Software

Introduction

This appendix contains instructions for restoring the previous version of QPSK software should you encounter problems after upgrading to QPSK E14. Follow the instructions in this appendix only after Cisco Services directs you to restore the previous version of software.

Important! If after downloading QPSK E14 you encounter problems, contact Cisco Services for assistance. In the event that Cisco directs you to download the previous version of software to QPSKs, follow the procedures in this appendix while working with Cisco Services.

In This Appendix

Restore the Previous Version of QPSK Software

Restoring the Previous QPSK Software Version

Note: To restore the previous QPSK executable files, restore the configuration backup file that you saved in ***Backing Up the Current QPSK Configuration File*** (on page 24).

1. Open an xterm window on the DNCS and log on as the **root** user. The root prompt appears.
2. Type **cd /tftpboot** and press **Enter**. The root prompt appears.
3. Type **pwd** and press **Enter**. The text /tftpboot appears at the prompt. This text indicates you are in the correct directory.
4. Type **cp –p qpsk.config qpsk.config.yyy** and press **Enter**. The configuration file named qpsk.config, which contains QPSK version E14 configuration settings, is saved to a file named qpsk.config.yyy.

   Note: The yyy represents the QPSK software version number you just installed.
5. Type **cp –p qpsk.config.old qpsk.config** and press **Enter.** The configuration file named qpsk.config.old, which contains the previous list of QPSK configuration files, is copied to a configuration file named qpsk.config.
6. Type **ls -l** and press **Enter**. A list of files displays. The files **qpsk.config.old**, **qpsk.config**, and **qpsk.config.bakyyy** appear in the list.

   Note: The "l" used in **ls** and **-l** is a lowercase letter L.
7. Confirm that the date and size of **qpsk.config** matches those of **qpsk.config.old**.
8. Type **exit** and press **Enter**.
9. Download the previous version of software to QPSKs by rebooting the modulators. For detailed procedures, go to ***Download Software to the QPSK Modulators*** (on page 26).

D

Troubleshoot Constant Reboots

After you install new code on a previously functioning QPSK, you may occasionally find that the QPSK will reboot continuously. This appendix contains a procedure to troubleshoot that situation.

In This Appendix

Troubleshooting Constant Reboots

If a previously functioning QPSK continues to reboot after an attempt to install new code, follow these steps to diagnose the situation.

1. Open an xterm window on the DNCS.
2. Type **su** and press **Enter** to switch to the super user mode. When prompted, enter the root password.
3. Type **traceroute [qspk ip address]** and press **Enter**. You should see a message similar to the following:

   Example:

   ```
   traceroute to 172.20.1.1 (172.20.1.1), 30 hops max, 40 byte packets
   1 switch (10.253.0.254) 3.443 ms 3.224 ms 4.279 ms
   2 172.20.1.1 (172.20.1.1) 3.919 ms 0.483 ms 0.584 ms
   ```

   The IP address shown in bold here is the interface that the QPSK traffic is going out from on the DNCS.
4. Type **ifconfig -a** and press **Enter** to determine which interface is on the network carrying the QPSK traffic.

   Note: In this example the interface is ci0.

   Example:

   ```
   lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
   inet 127.0.0.1 netmask ff000000
   hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
   inet 192.168.1.1 netmask ffffff00 broadcast 192.168.1.255
   hme1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
   inet 192.168.2.1 netmask ffffff00 broadcast 192.168.2.255
   ci0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 9180 index 4
   inet 10.253.0.1 netmask ffffc000 broadcast 10.253.63.255
   ether 0:20:48:40:1a:32
   [Sys 2 5.1.523 Lab] $
   ```
5. Type **snoop -d [interface] between [qpsk IP address]** and press **Enter**. This step shows the traffic between the DNCS and the QPSK. The following is an example of normal traffic.

   Example:

   ```
   Using device /dev/ci (promiscuous mode)
   dncsatm -> 172.20.1.1 RPC C XID=1143855649 PROG=805306881 (?) VERS=1
   PROC=1506
   172.20.1.1 -> dncsatm RPC R (#1) XID=1143855649 Success
   172.20.1.1 -> dncsatm RPC C XID=2240127 PROG=805306625 (?) VERS=1 PROC=1001
   dncsatm -> 172.20.1.1 TCP D=1024 S=57455 Ack=128230 Seq=1829802840 Len=0
   Win=24656
   dncsatm -> 172.20.1.1 TCP D=717 S=60909 Ack=192058 Seq=1829995505 Len=0
   Win=36984
   dncsatm -> 172.20.1.1 RPC R (#3) XID=2240127 Success
   172.20.1.1 -> dncsatm TCP D=57455 S=1024 Ack=1829802868 Seq=128230 Len=0
   Win=4096
   ^C# snoop -d ci0 between 172.20.1.1
   Using device /dev/ci (promiscuous mode)
   172.20.1.1 -> dncsatm TFTP Read "/qpsk.config" (octet)
   dncsatm -> 172.20.1.1 TFTP Data block 1 (512 bytes)
   172.20.1.1 -> dncsatm TFTP Ack block 1
   dncsatm -> 172.20.1.1 TFTP Data block 2 (512 bytes)
   172.20.1.1 -> dncsatm TFTP Ack block 2
   ```

```
dncsatm -> 172.20.1.1 TFTP Data block 3 (512 bytes)
172.20.1.1 -> dncsatm TFTP Ack block 3
dncsatm -> 172.20.1.1 TFTP Data block 4 (512 bytes)
172.20.1.1 -> dncsatm TFTP Ack block 4
dncsatm -> 172.20.1.1 TFTP Data block 5 (166 bytes) (last block)
172.20.1.1 -> dncsatm TFTP Ack block 5
172.20.1.1 -> dncsatm PORTMAP C GETPORT prog=805306625 (?) vers=1 proto=TCP
dncsatm -> 172.20.1.1 PORTMAP R GETPORT port=57455
172.20.1.1 -> dncsatm TCP D=57455 S=1024 Syn Seq=192001 Len=0 Win=4096
dncsatm -> 172.20.1.1 TCP D=1024 S=57455 Ack=128230 Seq=1829802868 Len=0
Win=24656
172.20.1.1 -> dncsatm TCP D=57455 S=1024 Rst Seq=128230 Len=0 Win=4096
172.20.1.1 -> dncsatm PORTMAP C GETPORT prog=805306625 (?) vers=1 proto=TCP
dncsatm -> 172.20.1.1 PORTMAP R GETPORT port=57455
172.20.1.1 -> dncsatm TCP D=57455 S=1025 Syn Seq=320001 Len=0 Win=4096
dncsatm -> 172.20.1.1 TCP D=1025 S=57455 Syn Ack=320002 Seq=3671790772 Len=0
Win=24656 Options=<mss 9140>
```

The key things to note in this example are the QPSK read of the qpsk.config file and the TFTP traffic that follows. Following these lines, the QPSK either provisions or attempts to load software (indicated by additional TFTP requests for the various files). The most common failure is a TFTP error due to network traffic or other problems.

TFTP Error Code	Definition
0	Not defined, see error message (if any).
1	File not found.
2	Access violation.
3	Disk full or allocation exceeded.
4	Illegal TFTP operation.
5	Unknown transfer ID.
6	File already exists.
7	No such user.

In most cases, errors are due to one of the following situations:

- An incorrectly performed install of the QPSK code
- An incorrect IP address in the configuration file being used by the QPSK
- Some network layer type of problem

6 If you encounter errors that you cannot resolve, contact Cisco Services.

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

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

June 2012 Printed in USA

Part Number 4013491 Rev C