



Explorer Digital Home Communications Terminal Staging Guide

Please Read

Important

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

Notices

Trademark Acknowledgements

- Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks.
- CableCARD is a trademark of Cable Television Laboratories, Inc.
- "Dolby" and the double-D symbol are trademarks of Dolby Laboratories.
- Other third party trademarks mentioned are the property of their respective owners.
- The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

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

Copyright

© 2000-2002, 2006, 2009, 2012 Cisco and/or its affiliates. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

About This Guide	vii
The Staging Process	1
Overview	2
What Knowledge and Skills Do You Need?	3
Download Methods	4
Install EMMs.....	5
Staging Preparations	9
Overview	10
Verify DNCS System Configuration Settings	11
Set Up Environment Variables.....	12
Create EMM Directories	14
Set Up Default Packages for Instastaging.....	15
Set Up Service Disconnect	17
Set Up the Staging Defaults.....	18
Install Software.....	19
Billing System Preparation	20
Optimize Your System Performance for Downloads and Staging	21
Overview	22
Recommendations to Improve Your Staging and Software Download Performance ..	23
Recommendations to Improve Your Data Carousel Rate	34
Staging Area Considerations	45
Minimum Network Requirements	46
QAM Requirements.....	47
QPSK Requirements	49
CMTS Requirements.....	50
Ventilation and Handling	51
CableCARD Module Requirements	52
Obtain and Load EMM Data	53
Obtain EMM Data	54
FTP Download Option	55
Mail or Shipping Service Option	56

Copy the EMM File.....	58
Send the EMM File to the DNCS Using FTP.....	59
Extract the EMM File.....	60
Copy the TOC File.....	61
Load EMM Data.....	62
How to Stage DHCTs	67
Overview.....	68
DHCT Staging Flowchart.....	69
Staging DHCTs with Services.....	70
Staging DHCTs For Instastaging.....	71
Verify the PowerKEY Information.....	72
Verifying the Staging Process.....	75
How to Stage CableCARD Modules	77
Overview.....	78
Setting Up the DNCS for CableCARD Module Staging.....	79
Staging CableCARD Modules.....	80
Verify CableCARD Module Staging.....	85
Returning DHCTs and CableCARD Modules to Service	87
Check for Stranded IPPV Events and Clear NVM.....	88
Returning CableCARD Modules to Service.....	92
Troubleshooting	93
Staging Failures.....	94
DHCT Errors.....	95
Send Instant Hits.....	99
OS and ResApp Downloads.....	101
PowerKEY/EA Issues.....	104
Customer Information	109
Appendix A Download LED Indicators	111
Overview.....	112
LED Indicators Displayed During an OSM Download.....	113
LED Indicators Displayed During a CVT Download.....	116
DHCTs with Three LED Indicators.....	119
DHCTs with Single LED Indicators.....	122
POWER LED Indicators Displayed on DHCTs.....	125

Appendix B Button Sequence for DHCT Functions	129
Button Sequences	130
E940 Forced Download Button	131
Appendix C Setting Up Multiple Bootloader Carousels	133
Overview	134
Determine Available Bandwidth for Multiple Bootloaders.....	136
Setting Up Multiple Bootloader Carousels	140
Adding a Bootloader Source to the DNCS	142
Setting Up DHCTs to Download Images from a Specific Bootloader Carousel	144
Appendix D Adding an HDD Test Server to the BFS	147
Overview	148
Adding an HDD Test Server to the BFS	150
Registering the HDD Test Server with the BFS	154
Placing the HDD Performance Specification File on the HDD Test Server.....	156
Appendix E Format the Hard Drive Without Clearing NVM	157
Formatting the Hard Drive.....	158
Appendix F Staging Out-Of-Band Bridges	159
Overview	160
Set Up Staging Bridges.....	162
Appendix G Staging Toolkit	165
Overview	166
Remote Controls.....	167
Activating the Staging Toolkit for DHCTs with Alphanumeric LEDs	168
Activating the Staging Toolkit for DHCTs with Single or Triple LEDs.....	169
Index	171

About This Guide

Introduction

This guide provides procedures for staging Explorer® Digital Home Communications Terminals (DHCTs) and CableCARD™ modules for use in the Digital Broadband Delivery System (DBDS).

Scope

This guide provides an overview of the staging process, all the steps you must take to prepare your site for staging DHCTs, staging procedures and the most common staging processes, and presents the best practices based on our experience. This guide also includes common troubleshooting steps.

Notes:

- This guide does not include procedures for installing client release software. Refer to *Downloading New Client Application Platform Installation Instructions* (part number 4003052) for information regarding installing client release software.
- This guide does not include procedures for staging Separable Security Host with CableCARD™ module (SSC) DHCTs. Refer to one of the following guides (based on the Digital Network Control System (DNCS) system release you are using) for information regarding staging SSC DHCTs:
 - *Separable Security Host Staging Guide for System Release 4.2.1 and Earlier* (part number 736107)
 - *Separable Security Host Staging Guide for System Release 4.3 and Later* (part number 4024836)
- See *Related Publications* for information on obtaining the documents mentioned above.

Audience

This guide is written for staging area personnel responsible for staging DHCTs, DHCT installation personnel, and system operators of the DNCS.

Document Version

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

Title	Title
Added a chapter that contains information on optimizing your system performance	<i>Optimize Your System Performance for Downloads and Staging</i> (on page 21)
Added information on improving the speed and performance of CVT downloads for DHCTs	<i>Recommended Frequencies for Improved CVT Download Performance</i> (on page 47)
Fixed a typographical error in the procedure for extracting the EMM file	<i>Extracting the EMM File</i> (on page 60)
Updated LED behavior during download for three-LED DHCTs	<i>DHCTs with Three LED Indicators</i> (on page 119)
Updated LED behavior during download for single-LED DHCTs	<i>DHCTs with Single LED Indicators</i> (on page 122)
Added an appendix that explains how to set up multiple bootloader carousels (SR 4.3 and later only)	<i>Setting Up Multiple Bootloader Carousels</i> (on page 133)
Added an appendix that explains how to set up the HDD test on the DNCS for DVRs	<i>Adding an HDD Test Server to the BFS</i> (on page 147)

1

The Staging Process

Introduction

Staging is the process that prepares a DHCT or CableCARD module to operate correctly on a cable service provider's network. When a DHCT/CableCard is properly staged, it has all of the software and the authorization information that it needs to display programming and other data in the subscriber's home.

This chapter provides an overview of the methods for downloading client release software and for installing authorization Entitlement Management Messages (EMMs).

In This Chapter

■ Overview	2
■ What Knowledge and Skills Do You Need?	3
■ Download Methods	4
■ Install EMMs.....	5

Overview

Devices (DHCTs and CableCARD modules) that require staging include the following:

- Brand new units
- Field-return units: Devices that have been removed from the subscriber's home and returned to the service provider
- Return Material Authorization (RMA) units: Devices that the service provider has received back from factory repair

Staging involves two main tasks:

- Installing the current operating system (OS) onto the DHCT.
- Installing authorization Entitlement Management Messages (EMMs) onto the DHCT.

What Knowledge and Skills Do You Need?

Before you stage DHCTs and CableCARD modules, you must be familiar with the basic operation of the devices and the features that are available to subscribers.

Overall Staging Knowledge

Before you stage devices, you should be familiar with these processes:

- Operation of the DNCS (particularly DHCT and CableCARD module loading and activation)
- Configuration of your cable headend system
- Knowledge of basic UNIX commands
- Knowledge of compressed file formats, such as TAR and GZIP files
- Knowledge of File Transfer Protocol (FTP) and the ability to FTP files to and from your DNCS

For more information, refer to *Related Publications* (on page viii).

DHCT Staging Knowledge

To stage the DHCTs, you should become familiar with the following features of the DHCT:

- Front and back panels of the Explorer DHCT
- Explorer DHCT diagnostic screens
- Configuration settings that define the operating characteristics for DHCTs
- Remote control operation
- LED indicators that indicate DHCT status
- Staging toolkit operation

Staging involves two main tasks:

- Installing the current operating system (OS) onto the DHCT.
- Installing authorization Entitlement Management Messages (EMMs) onto the DHCT.

Download Methods

There are two methods for installing client release software to devices in a DBDS environment:

- Code Version Table (CVT) download (for newer DHCTs and CableCARD modules).
- Operating System Manager (OSM) download (for older DHCTs).

CVT Download Method

The CVT is a table that contains information about download channel and information to map application platform software versions to specific devices.

The DNCS sends the CVT to all QAMs in the network. The QAMs then send the CVT to the devices once every second. The DNCS also sends CVT through the DAVIC (QPSK) or DOCSIS out-of-band forward data channel once every 10 minutes.

The CVT method is the only download method available for newer DHCTs and for all CableCARD modules.

OSM Staging Method (for Older DHCTs Only)

In the OSM staging method, the DHCT receives System Information (SI) and a type-specific user-to-network configuration (Unconfig) message, which includes a table of contents (TOC) file, from the DNCS.

The DHCT reads the contents of the TOC file and compares the checksums of the currently installed image files against the file information in the TOC file. If the checksum of either file does not match, the DHCT installs the new software as needed.

The OSM staging method is the only download method available for older DHCTs and the following specific DHCT/OS combinations:

- All Explorer 2000, 2010, 2100 (rev 2.0 and 2.1), and 3100 (rev 2.0 and 2.1) DHCTs in your network must use the OSM download method.
- The following Explorer DHCT revisions cannot use the CVT download method on networks where the BFS QAM is at a harmonically related carrier (HRC) frequency:
 - Explorer 2100 rev 2.2 and 2.3 DHCTs
 - Explorer 3100 rev 2.4, 2.5, and 2.6 DHCTs

Note: These DHCTs can use the CVT download method on systems using either a standard (STD) frequency plan or an incrementally related-carrier (IRC) plan.

Install EMMs

There are four methods for installing authorization Entitlement Management Messages (EMMs) into DHCTs or CableCARD modules. This section describes each of those methods and describes how to prepare your system to perform each method. The following list provides the methods for installing authorization EMMs:

- ModifyDhctConfiguration
- DhctInstantHit
- Fast Refresh List
- Instastaging

This section explains each of these methods. After you read this section, you should work with your billing system provider to determine which of these methods you should use.

ModifyDhctConfiguration

The ModifyDhctConfiguration method (modDhctCfg) enables all PowerKEY® configuration parameters of the device or, in the case of a field-return unit, authorizes the device for default services. The first time you stage a device and place it into an active inventory status on your billing system, the ModifyDhctConfiguration transaction is automatically sent to the device.

The first time the DNCS receives a request to perform the ModifyDhctConfiguration transaction for a new device (or for RMA units, if EMMs are installed as described later in this guide), the DNCS transmits at least 33 EMMs *twice*. After that, each time the system initiates the ModifyDhctConfiguration transaction, only the Service Authorization EMMs (typically 4 EMMs) are transmitted.

Before a ModifyDHCTConfiguration is initiated from the billing system, you must complete one or both of the following processes:

- DHCT – Connect the DHCT to AC power and let it finish loading software (at which point it displays either a clock or Brick mode status).
- CableCARD module (for testing) – Install the CableCARD module in a host and let it finish loading software. The staging process for CableCARD modules does not require them to receive EMMs initially. See *How to Stage CableCARD Modules* (on page 77) for more information.

DhctInstantHit

The DhctInstantHit transaction, sometimes called an “instant hit,” initiates the transmission of all existing EMMs to the device. The DNCS and some billing systems can send an instant hit. During a DhctInstantHit, the DNCS transmits the EMMs for the device.

You should send a DhctInstantHit if the ModifyDhctConfiguration transaction was started before the device was ready to receive the EMMs (for example, the device had not finished downloading software).

Using an instant hit to send EMMs to the device is only effective when the staging EMMs are present on the DNCS. In most cases, this means that the device must be installed and ready to receive EMMs within 30 days of the EMMs being built as a result of the ModifyDHCTConfiguration transaction (the "EMM window").

Note: The number of days for the EMM window is configurable in the DNCS; 30 days is the default value.

If you do not send the EMMs within the 30-day window, you will need to use the ModifyDHCTConfig transaction to rebuild the staging EMMs. See *ModifyDhctConfiguration* (on page 5) for more information.

Fast Refresh List

The Fast Refresh List is a queue of EMMs that a data carousel within the BFS distributes. A data carousel transports data from the BFS server to the device. Every 5 minutes, the DNCS searches for devices that have the following settings and adds them to the Fast Refresh List:

- Fast Refresh List enabled
- Admin Status set either to In Service Two Way or In Service One Way (set by the ModifyDhctAdminStatus transaction)

During the staging process, the billing system sends the ModifyDhctConfiguration transaction to the DNCS to add a DHCT to the Fast Refresh List. When the DNCS rebuilds the Fast Refresh List, the data carousel continuously sends PowerKEY information to the new DHCTs.

If a DHCT boots and an Entitlement Agent (EA) is not present, the DHCT tunes to the inband QAM data channel and attempts for 5 minutes to receive its PowerKEY information. The 5-minute tuner lockout begins after the DHCT receives its SI and BFS data. The Fast Refresh List has been rebuilt with the PowerKEY information for the DHCT, the DHCT receives its information during this time.

EMMs remain on the Fast Refresh List for 48 hours unless you send a ModifyDhctConfiguration transaction to remove the DHCTs from the Fast Refresh List.

Fast Refresh List Requirements

To use the Fast Refresh List, your system must support SR 2.2 or later. The capacity of the Fast Refresh List for SR 2.2 or later is 1,000 DHCTs.

Note: You should work with your billing department to determine the number of DHCTs on the list, or manually clear the list if you need to stage more DHCTs in a 48-hour period than the Fast Refresh List capacity for your system release.

Instastaging

The instastaging process simplifies EMM installation by automatically sending a hit to a two-way device when the device boots into two-way mode.

To use instastaging, you must meet the following requirements:

- You must be using System Release (SR) 2.5/3.5 or SR 3.3, or later.
- Your billing system must be configured to assign an Out-Of-Service status to devices when they are placed in inventory.
- Your DNCS must be configured to support instastaging.
- The device must be able to boot into two-way mode.
- If you are using CableCARD modules, they must be installed in a two-way host.

2

Staging Preparations

Introduction

This chapter provides procedures that system operators must complete to prepare the DBDS for staging devices.

In This Chapter

■ Overview	10
■ Verify DNCS System Configuration Settings	11
■ Set Up Environment Variables.....	12
■ Create EMM Directories	14
■ Set Up Default Packages for Instastaging	15
■ Set Up Service Disconnect	17
■ Set Up the Staging Defaults.....	18
■ Install Software.....	19
■ Billing System Preparation	20

Overview

Before system personnel can begin to stage devices, there are some tasks that the system operator must perform. The following tasks prepare your DBDS to stage devices:

- Verify your DNCS system configuration settings
- Setting the environment variables (if your site plans to use instant hit, Fast Refresh List, or Instastaging)
- Preparing directories to store and extract EMM and EMM log files
- Set up default packages (if you are using Instastaging)
- Creating a Service Disconnect Avoidance package and enabling service disconnect mode (if your site uses service disconnect mode)
- Setting default configurations for staged DHCTs
- Install the necessary software
- Assuring that your billing system is configured to do the following:
 - Assign at least one package
 - Put the device in service one-way or two-way
 - Enable Digital Interactive Service (DIS)

Note: Refer to your billing system documentation to determine the best method for configuring your billing status to support staging.

Verify DNCS System Configuration Settings

We recommend that you **do not change** the default DHCT and network signaling parameters in the DSM-CC portion of the DNCS System Configuration window when you stage DHCTs.

Note: For more information on the DNCS System Configuration window and the recommended parameter settings for that window, refer to the *Digital Network Control System Online Help* for your system release.

Verify Current DNCS System Configuration Settings (DAVIC Systems)

Verifying Current DNCS System Configuration Settings (DAVIC)

Follow these steps to verify your current DNCS system configuration settings.

- 1 From the Administrative Console on the DNCS, select **System Provisioning**.
- 2 In the System Management area of the DNCS Administrative Console, select **DHCT Mgr**. The DHCT Manager window opens with the DHCT Manager Modes tab in the forefront.
- 3 Is DHCT Registration set to **Administrative Gateway**?
 - If **yes**, go to step 4.
 - If **no**, change the DHCT Registration setting to **Administrative Gateway**, then go to step 5.
- 4 Is IP Address Assignment set to **Override**?
 - If **yes**, go to step 5.
 - If **no**, change the IP Address Assignment setting to **Override**, then to go step 5.
- 5 Click **Save**. The system saves your settings and the DHCT Manager window closes.
- 6 Go to *Billing System Preparation* (on page 20).

Verify Current DNCS System Configuration Settings (DOCSIS Systems)

If your system uses DOCSIS, refer to *DOCSIS in a DBDS Environment* (part number 4000358) to verify your DNCS system configuration.

Set Up Environment Variables

Before you can stage devices, you must first set the environment variables for your DNCS in the `/export/home/dncls/.profile` file. Setting the environment variables lets you configure your system to support a staging option. If you are using the instant hit method, the Fast Refresh List method, or instastaging to stage devices, you must set the environment variables properly. Otherwise, the DNCS will not operate as expected.

Note: The default staging configuration supports the DHCTModifyConfiguration transaction and does not need you to set an environmental variable.

Setting Environment Variables for Instant Hit

Note: You should be familiar with using the UNIX vi editor before attempting this procedure.

- 1 Use the UNIX vi text editor to open the `/export/home/dncls/.profile` file.
- 2 Does the `.profile` file contain the `export CAM_STAGE_INSTANT_HIT=1` line?
 - If **yes**, close the file; you are finished with this procedure.
 - If **no**, go to step 3.
- 3 Use the editor to add the following command to any blank line in the file:
`export CAM_STAGE_INSTANT_HIT =1`
- 4 Save and close the file.

Setting Environment Variables for Fast Refresh Table

Note: You should be familiar with using the UNIX vi editor before attempting this procedure.

- 1 Use the UNIX vi text editor to open the `/export/home/dncls/.profile` file.
- 2 Does the `.profile` file contain the `export CAM_ENABLE_FAST_REFRESH=1` line?
 - If **yes**, close the file; you are finished with this procedure.
 - If **no**, go to step 3.
- 3 Use the editor to add the following command to any blank line in the file:
`export CAM_ENABLE_FAST_REFRESH=1`
- 4 Save and close the file.

Setting Environment Variables for Instastaging

Note: You should be familiar with using the UNIX vi editor before attempting this procedure.

- 1 Use the UNIX vi text editor to open the `/export/home/dncs/.profile` file.
- 2 Does the `.profile` file contain the `HCTM_PROVISIONING_APP=1; export HCTM_PROVISIONING_APP` line?
 - If **yes**, close the file; you are finished with this procedure.
 - If **no**, go to step 3.
- 3 Use the editor to add the following two lines to any blank line in the file:


```
####Setting the flag for Instastaging####
HCTM_PROVISIONING_APP=1; export HCTM_PROVISIONING_APP
```
- 4 Save and close the file.

Enabling Environment Variables

After you set the staging environment variables on the DNCS, you must enable the environment variables by stopping and restarting the `camAm` process.



CAUTION:

Do not perform this procedure if pay-per-view (PPV) events are scheduled to begin in 15 to 20 minutes. Subscribers might experience black screens or be unable to purchase events.

Complete these steps to enable the environment variables on the DNCS.

- 1 On the DNCS Administrative Console Status window, click **Control** in the **DNCS** section. The DNCS Control window displays.
- 2 Highlight the **camAm** process.
- 3 Click the **Process menu** and select **Stop Process**. A confirmation window appears.
- 4 Click **Yes**. When the DNCS stops the `camAm` process, it turns the green status indicator to red.
- 5 On the DNCS Administrative Console Status window, click **Control** in the **DNCS** section. The DNCS Control window displays.
- 6 Highlight the **camAm** process.
- 7 Click the **Process menu** and select **Start Process**. A confirmation window appears.
- 8 Click **Yes**. The DNCS starts the `camAm` process and turns its red status indicator to green.

Create EMM Directories

Creating an EMM File Directory

You must create a directory for storing and extracting the EMM files if you are downloading the files using FTP.

Note: You do not need to create this directory if you are loading the EMM files from a CD.

Follow these instructions to create the `/dvs/dncs/emmcads` directory.

- 1 Open an xterm window on the DNCS.
- 2 Type **`mkdir /dvs/dncs/emmcads`** and press **Enter**. The system creates the `/dvs/dncs/emmcads` directory.
- 3 Do not close the xterm window.

Creating an EMM Log Directory

You must create a directory for storing the EMM log files that result from loading the EMM images files onto the DNCS.

Follow these instructions to create the `/dvs/dncs/emmlogs` directory.

- 1 In the open xterm window, type **`mkdir /dvs/dncs/emmlogs`** and press **Enter**. The system creates the `/dvs/dncs/emmlogs` directory.
- 2 Type **`exit`** and press **Enter** to close the xterm window.

Set Up Default Packages for Instastaging

To use the default staging packages instastaging method, you must use the DNCS to identify the packages that comprise your default level of services.

Note: See *Staging DHCTs For Instastaging* (on page 71) for more information on the process of staging DHCTs using instastaging.

When the DHCT boots into two-way mode for the first time, the DNCS sends all of the EMMs and package authorizations for the default packages, and the subscriber begins to receive the default services.

When the DHCT is added to the subscriber's account, it is upgraded or downgraded to receive only the requested services.

Setting Default Packages

If you are using default staging packages, you must define or identify the default packages that each DHCT receives when it is installed. You can follow one of the following procedures:

- Create a new default package and provision it.
- Choose an existing package.

Notes:

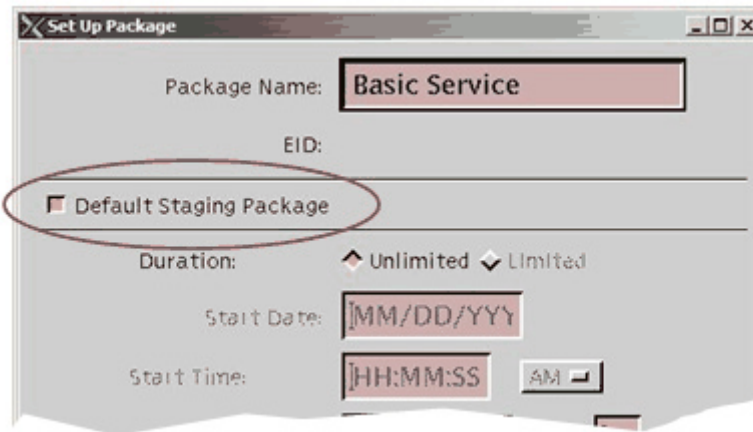
- You can specify multiple default packages.
- If your site uses Service Disconnect feature (Brick mode), be sure that the default staging option is selected for the brick mode package.

Creating a New Default Package

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the **System Provisioning** tab.
- 3 Click **Package**. The Package List window opens.
- 4 Click **File** and select **New**. The Set Up Package window opens.
- 5 Click in the **Package Name** field and type the name you will use to identify this package. You can use up to 20 alphanumeric characters.

Note: In most cases, the package name does not need to follow the package naming convention that your billing system uses. However, if you use this package for any other purpose in addition to instastaging DHCTs, the name should follow the billing system naming conventions. Contact your billing system vendor if you are not sure of their rules for naming packages. Refer to your billing system documentation for instructions and specific information.

- 6 Select the **Default Staging Package** box.



- 7 Add the necessary segments and packages. Refer to the *DNCS Online Help* for more information.
- 8 Click **Save**.

Results:

- The DNCS saves the package information in the DNCS database and closes the Set Up Package window.
- The Package List updates to include the new package.
- An asterisk (*) appears next to this package, indicating that it is a default staging package.

Identifying Existing Packages as Default Packages

Note: If your site uses SARA, you must identify the following packages as default packages:

- The brick mode package (if used), even if you have created a new default package.
 - Some third-party applications use EIDs as part of the SAM URL. If you want the DHCT to receive any of these applications, you must identify them as default packages.
- 1 On the DNCS Administrative Console, click the **DNCS** tab.
 - 2 Click the **System Provisioning** tab.
 - 3 Click **Package**. The Package List window opens.
 - 4 Double-click the name of the package that you want to identify as a default staging package.
 - 5 Select the **Default Staging Package** box.
 - 6 Click **Save**. In the Package List window, an asterisk (*) appears, indicating that this package is a default staging package.

Set Up Service Disconnect

The Service Disconnect feature (also called *Brick mode*) lets you disable a DHCT. When a DHCT is in a service disconnect mode, the subscriber cannot view cable services.

If you want to use the Service Disconnect feature at your site, you must create a Service Disconnect Avoidance package before you enable service disconnect. When you enable the service disconnect mode, the DHCT resident application checks every minute to make sure that the DHCT is authorized for the Service Disconnect Avoidance package. If the DHCT is not authorized, the following actions occur:

- The DHCT goes into a service disconnect mode.
- A barker appears on the subscriber's TV screen.
- All remote keys and front panel keys are locked out.
- The LED screen displays the service disconnect indicator [- - -].

Note: For DHCTs with only POWER LED indicators, the **POWER** LED blinks eight times, pauses, and repeats for Service Disconnect Mode).

For more information on the Service Disconnect feature, refer to *Enhancing Your Subscribers' Experience: SARA Configurable Options* (part number 4002178).

Set Up the Staging Defaults

The next task that you must perform is to set up all of the staging options that will be installed onto each DHCT. These options define the default operating parameters of the DHCT and include such options as:

- The RF output channel (3 or 4).
- The screen language and color scheme for SARA screens.
- The default Personal Identification Number (PIN) for Parental Control and PPV purchases.
- The audio compression range and digital audio output (Dolby™ Digital or two-channel digital).

For more information and procedures to set up these staging defaults, refer to *Enhancing Your Subscribers' Experience: SARA Configurable Options* (part number 4002178).

DVR, DVD, and Multi-Room Device Considerations

DHCTs with DVRs or DVDs require additional configuration steps before you can begin staging them. If you do not follow these additional steps, subscribers will not be able to access DVR, DVD, or multi-room functions.

For more information on these additional configuration steps, refer to *DVR Configuration Guide* (part number 4011411).

Install Software

Install the Application Platform Release

The next task that you must complete before you can stage DHCTs or CableCARD modules is to install the current application platform software onto the DNCS.

Application platform software consists of the OS and ResApp software. The device must have both of these components to function properly.

When the software is installed on the DNCS, the staging process then delivers the software to the devices. Refer to *Downloading New Client Application Platform Software Installation Instructions*.

Install the Current Resource File

If you are using the CVT download method to load the application platform software onto devices, you need to make sure that you are using the most current resource file (**settop.res**). This resource file contains information used by the CVT configuration interface on the DNCS to validate the software for both DHCTs and CableCARD modules to prevent loading the wrong software onto a device.

Refer to *Downloading New Client Application Platform Installation Instructions* (part number 4003052) for more information about acquiring and installing the most current resource files.

Install the OS Check Table (OSM Only)

If you are using the OSM download method to stage DHCTs, you must install the OS check table.

Refer to *Downloading New Client Application Platform Software Installation Instructions* for more information.

Billing System Preparation

Your billing system must be set up with the following parameters when the DHCT is scanned during staging:

- Admin Status—Set to either **One-Way** or **Two-Way**.
- DIS—Set to **enabled**.
- IPPV credit limit—Set to a **non-zero** value.
- Package—At least one package must be sent.

Refer to your billing system documentation to determine the best method for configuring your billing status to support staging.

3

Optimize Your System Performance for Downloads and Staging

Introduction

Before you stage DHCTs or download software to DHCTs, it is very important that your system is in the best condition possible. This chapter includes recommendations for settings and procedures for changing settings that affect the performance of your system.

In This Chapter

- Overview 22
- Recommendations to Improve Your Staging and Software Download Performance 23
- Recommendations to Improve Your Data Carousel Rate 34

Overview

Before you stage devices on your system, it is imperative that you have a healthy system. If you do not have a healthy system, the installation process could fail and disrupt service to your subscribers. We strongly recommend that you follow the procedures in this chapter to maximize your DBDS efficiency before you begin staging DHCTs.

This chapter includes the steps you need to take to perform the following procedures:

- Removing unnecessary files from your BFS
- Verifying the DNCS settings for the CableCARD server
- Turning off inband system information
- Configuring a default download image
- Deleting unused DHCT types
- Deleting unused DHCT software
- Cleaning up the ResApp directory
- Verifying and cleaning up the download directory
- Changing the data carousel rates

This chapter also includes the recommended frequencies for CVT downloads. Using the frequencies in this chapter vastly improves the speed and performance of the initial staging process.

How Do I Manage the Files on My System?

It is important to keep only the currently active client code loaded on your DNCS.

When you upgrade, you should have both the old version of code and the new version loaded onto your system at the same time (while you test the new code). This is encouraged and does not pose a significant problem; it should not increase download times significantly.

After you test a new release and configure all devices to use the new software, we recommend that you aggressively manage your system to keep unused and unneeded files off your system. Following the procedures for loading software that are included in this guide will help you keep unneeded files off of your system.

Recommendations to Improve Your Staging and Software Download Performance

DNCS Settings for the CableCARD Server

The parameters required for configuring the CableCARD server on the DNCS vary with each System Release. Refer to the following tables for the recommended parameters related to the release that is running on your system.

SR 2.5/3.5 and 4.0 and SR 2.5/3.5/4.0 SP3

Note: For detailed information about the fields within the DNCS GUI, refer to *Setting Up the PowerKEY CableCARD and M-Card Modules on the DNCS For System Releases 2.5/3.5 and 4.0* (part number 4011765).

Field	Recommended Value
IP Address of Server Running the CCardServer Process (typically this is the IP Address on the DNCS that connects to the QPSKs)	Autobinding on: 10.253.0.1 Autobinding off: 0.0.0.0 Important: If you do not use the default IP address for your CableCARD server, check your network map, the /etc/hosts file for the dnscatm entry, or with your network administrator for the correct IP address.
Port Number	Autobinding on: 13830 Autobinding off: 0
Authorization Time-out Period (hours)	2 Important: <ul style="list-style-type: none"> ■ We recommend that you set this value to 2. ■ Negative values are not permitted in this field. ■ If you define a value greater than 2, be aware of the following issues: <ul style="list-style-type: none"> – The podData file can contain no more than 1500 entries. During staging, the CableCARD module/host pair is added to the podData file for the length of time indicated by this field. When this time has expired, the pod/host pair is removed from the file. – If you attempt to exceed 1500 entries during the time-out period that you have defined, the CableCARD module/host pairs will be unable to bind.

Chapter 3 Optimize Your System Performance for Downloads and Staging

Field	Recommended Value
De-Authorization Time-out Period (days)	30 Important: We recommend that you set this value to 30. If this value is too large, it could interfere with the total number of authorization entries that can be added to the podData file and could also interfere with the binding of the CableCARD module/host pairs.
MaxKeySessionPeriod*	10 Important: We recommend that you set this value to 10. Defining a rate less than 10 requires a large number of unnecessary calculations on the CableCARD module. Defining a rate greater than 20 does not coincide with best security practices.
RF Output (channel)	Value is based on the site's individual preference. Typically, if the site uses channel 3 for DHCTs, it should also use channel 3 for CableCARD host devices.
Card Authorization Phone Number	Phone number that subscribers should call when they need assistance. You can enter up to 20 alphanumeric characters (including spaces) in this field.

*MaxKeySessionPeriod is measured in decaseconds for S-Mode boxes and minutes for M-Mode boxes. For more information see <http://www.opencable.com/>

SR 2.7/3.7 and 4.2 and SR 2.7/3.7/4.2 SP0.2 or SP2

Note: For detailed information about the fields within the DNCS GUI, refer to *Setting Up PowerKEY CableCARD and M-Card Modules on the DNCS for System Releases 2.7/3.7 and 4.2* (part number 4014667). Sites running SR 2.7/3.7/4.2 SPs should refer to *Setting Up PowerKEY CableCARD and M-Card Modules on the DNCS For System Releases 2.7/3.7 and SR 4.2 Service Pack 2* (part number 4017453).

Field	Recommended Value
IP Address of Server Running the CCardServer Process (typically this is the IP Address on the DNCS that connects to the QPSKs)	Autobinding on: 10.253.0.1 Autobinding off: 0.0.0.0 Important: If you do not use the default IP address for your CableCARD server, check your network map, the /etc/hosts file for the dnscsatm entry, or with your network administrator for the correct IP address.
Port Number	Autobinding on: 13830 Autobinding off: 0

Recommendations to Improve Your Staging and Software Download Performance

Field	Recommended Value
Authorization Time-out Period (hours)	<p>2</p> <p>Important:</p> <ul style="list-style-type: none"> ■ We recommend that you set this value to 2. ■ Negative values are not permitted in this field. ■ If you define a value greater than 2, be aware of the following issues: <ul style="list-style-type: none"> – The podData file can contain no more than 1500 entries. During staging, the CableCARD module/host pair is added to the podData file for the length of time indicated by this field. When this time has expired, the pod/host pair is removed from the file. – If you attempt to exceed 1500 entries during the time-out period that you have defined, the CableCARD module/host pairs will be unable to bind.
De-Authorization Time-out Period (days)	<p>30</p> <p>Important: We recommend that you set this value to 30. If this value is too large, it could interfere with the total number of authorization entries that can be added to the podData file and could also interfere with the binding of the CableCARD module/host pairs.</p>
MaxKeySessionPeriod*	<p>10</p> <p>Important: We recommend that you set this value to 10. Defining a rate less than 10 requires a large number of unnecessary calculations on the CableCARD module. Defining a rate greater than 20 does not coincide with best security practices.</p>
RF Output (channel)	<p>Value is based on the site's individual preference. Typically, if the site uses channel 3 for DHCTs, it should also use channel 3 for CableCARD host devices</p>
Card Authorization Phone Number	<p>Phone number that subscribers should call when they need assistance. You can enter up to 20 alphanumeric characters (including spaces) in this field.</p>

*MaxKeySessionPeriod is measured in decaseconds for S-Mode boxes and minutes for M-Mode boxes. For more information see <http://www.opencable.com/>

Chapter 3 Optimize Your System Performance for Downloads and Staging

The following fields apply to SR 4.2 and later, only. These fields are displayed in **Set CableCARD MMI Copy Protection** on the DNCS GUI screen.

Field	Recommended Value
Display MMI for bi-directional device (SR 4.2 and later, only)	Autobinding on: inactivated (checkmark not displayed)
	Autobinding off: activated (checkmark displayed)
Bidirectional timeout (SR 4.2 and later, only)	Autobinding on: 180 (3 minutes)
	Autobinding off: 0

SR 2.8/3.8 and 4.3 and Later

Field	Recommended Value
IP Address of Server Running the CCardServer Process (typically this is the IP Address on the DNCS that connects to the QPSKs)	Autobinding on: 10.253.0.1
	Autobinding off: 0.0.0.0 Important: If you do not use the default IP address for your CableCARD server, check your network map, the /etc/hosts file for the dnccsatm entry, or with your network administrator for the correct IP address.
Port Number	Autobinding on: 13830
	Autobinding off: 0
Authorization Time-out Period (hours)	2 Important: Negative values are not permitted in this field. If you define a value greater than 2, be aware of the following issues: <ul style="list-style-type: none"> ■ The podData file can contain no more than 1500 entries. During staging, the CableCARD module/host pair is added to the podData file for the length of time indicated by this field. When this time has expired, the pod/host pair is removed from the file. ■ If you attempt to exceed 1500 entries during the time-out period that you have defined, the CableCARD module/host pairs will be unable to bind.
De-Authorization Time-out Period (days)	30 Important: If this value is too large, it could interfere with the total number of authorization entries that can be added to the podData file and could also interfere with the binding of the CableCARD module/host pairs.

Recommendations to Improve Your Staging and Software Download Performance

Field	Recommended Value
MaxKeySessionPeriod (decaseconds for SMode) (minutes for MMode)	SMode: 10 (decaseconds) MMode: 10 (minutes)
Maximum Host Change Count Allowed	Any number; default = 99 (unlimited) The maximum number of times that a CableCARD module is allowed to autobind with a different host. When the CableCARD exceeds this limit, it is no longer allowed to autobind with a different host. The default number, 99, allows an unlimited number of autobindings.
RF Output (channel)	Value is based on the site's individual preference. Typically, if the site uses channel 3 for DHCTs, it should also use channel 3 for CableCARD host devices
Card Authorization Phone Number	Phone number that subscribers should call when they need assistance. You can enter up to 20 alphanumeric characters (including spaces) in this field.
Maximum Bindings Within Authorization Time-Out Period	1500 The maximum number of SCC hosts and CableCARD modules that you can bind during a staging period (defined by the Authorization Time-Out Period). This value cannot be changed from the Server Configuration window. You must use the modCCardStagingLimit script to modify this value. For more information, refer to <i>Change the CableCARD Module Staging Limit</i> (part number 4020737).

The following fields are displayed in the DNCS GUI's **Set CableCARD MMI Copy Protection** screen.

Field	Recommended Value
Display MMI for bi-directional device	Autobinding on: inactivated (checkmark not displayed) Autobinding off: activated (checkmark displayed)
Bidirectional timeout	Autobinding on: 180 (3 minutes) Autobinding off: 0

Turn Off Inband SI

System information (SI) is tuning data sent to CableCARD modules. The default configuration in the DNCS is to send SI as both inband and out-of-band data. This configuration is due to the way in which previous versions of DHCT software operated, and it has not been a requirement in recent years. At this time, we recommend that sites only send SI out-of-band. This helps stabilize the CableCARD download environment.

Note: Refer to *Recommendation for Setting System Information to Out-of-Band* (part number 738143) for procedures to turn off inband SI.

Configuring a Default Download Image

We recommend having the same image on all of your deployed CableCARD modules and downloading that same image onto both new and factory repaired CableCARD modules. This recommendation creates a consistent environment for all cards in your system.

Using group-based downloads will limit which cards use a particular version of code. For this reason, if you choose to implement group-based downloads, we recommend configuring a download that sends the most current CableCARD software (for example, CableCARD software release 1.1.x) to the default CableCARD group.

Important: If you are running CableCARD software that precedes software release 1.1 and you are using an OSM download method, do not send any download-related UN-Config messages to the CableCARD hardware type list. For details, refer to the *Best Practices for Using Multi-Stream CableCARD Modules Operation and Maintenance Guide* (part number 4005658). To obtain a copy of this document, see Related Publications in the *Preface* (on page vii).

Sending the most current CableCARD software to the default group achieves the following results:

- Eliminates the need to use CVT groups for CableCARD downloads
- Provides a standard release with the most recent version of code on all CableCARD modules

Delete Unused DHCT Types

If you have previously deleted unused DHCT Types from your network, then you can skip this section and go to *Running the listOSM Utility and Removing Unneeded Files* (on page 30). If you have not previously deleted unused DHCT types from the network, you need to complete this procedure before going to *Running the listOSM Utility and Removing Unneeded Files* (on page 30).

Deleting Unused DHCT Types

Complete the following steps to delete unused DHCT types from the DNCS database.

- 1 On the DNCS Administrative Console, select the **DNCS** tab.
- 2 From the DNCS Administrative Console, select one of the following tabs:
 - For SR 2.7/3.7/4.2 and later, click the **Network Element Provisioning** tab.
 - For SR 2.5/3.5/4.0 and earlier, click the **Element Provisioning** tab.
- 3 Click **Type**. The DHCT Type List window opens, listing the DHCT type, revision, OUI, and name.
- 4 Look at each entry in the list. Is the entry used in your system?
 - If **yes**, there is no need to delete this entry. Look at the next entry.
 - If **no**, or if you are not certain, go to step 5.
- 5 From the drop-down menu at the top of the DHCT Type List window, click **File > Delete**. The following message appears:
Are you sure you want to delete the current item?
- 6 Click **Yes**.
- 7 Did an **Unspecified Error** message appear?
 - If **yes**, the selected DHCT type is used in your system and you cannot delete it.
 - If **no**, the selected DHCT type is not used in your system, and the DNCS deletes it from the database.
- 8 Repeat steps 4 through 7 for each DHCT type in the DHCT Type List.
- 9 From the drop-down menu at the top of the DHCT Type List window, click **File > Close**. The DHCT Type List closes.
- 10 Go to *Running the listOSM Utility and Removing Unneeded Files* (on page 30).

Running the listOSM Utility and Removing Unneeded Files

The listOSM utility determines which DHCT models are currently using the OSM download method and reports the unused files in the OS list.

Running the listOSM Utility and Removing Unneeded Files

- 1 Are you using the OSM download method for any DHCTs in your network?
 - If **yes** or if you are **unsure**, go to step 2.
 - If **no**, go to *Running the listCVT Utility and Removing Unneeded Files* (on page 31).
- 2 Open an xterm window on the DNCS.
- 3 Type **listOSM -v** and press **Enter**. This command provides you the version of listOSM utility that is currently on your network.
- 4 Compare the version number of the listOSM utility on your DNCS with the version number listed in the ROM to Model Matrix in the *Downloading New Client Application Platform Installation Instructions* (part number 4003052).
 - If the version number is equal to or greater than the one listed in the matrix, go to step 5.
 - If the version number is less than the one listed in the matrix, contact Cisco Services to receive the latest utility.
- 5 Type one of the following, based on the system release you have installed:
 - For SR 4.2.1 and earlier, type **cd /export/home/dncs/doctor** and press **Enter**.
 - For SR 4.3 and later, type **cd /dvs/dncs/Utilities/doctor** and press **Enter**.

Note: Be sure to type a space between **cd** and **/**.

Result: The current directory is now the doctor directory.
- 6 Type **listOSM > preosm** and press **Enter**.
- 7 Type **more preosm** and press **Enter**. This command lets you view the file and verify the current download configuration for each DHCT type active in the network.
- 8 Does the report indicate that there are unused files?
 - If **yes**, go to step 9.
 - If **no**, go to *Running the listCVT Utility and Removing Unneeded Files* (on page 31).
- 9 On the DNCS Administrative Console, select the **DNCS** tab and then select one of the following tabs based on the system release you have installed:
 - For SR 2.5/3.5/4.0 and earlier, select the **Element Provisioning** tab.
 - For SR 2.7/3.7/4.2 and later, select the **Home Element Provisioning** tab.
- 10 Click **OS**. The DHCT OS List window opens.

- 11 Highlight a DHCT software file that is unused in the network, click **File > Delete**.
Important: Do not delete files with different naming formats such as .rle, .res, or .dat. These files are used by other functions such as logos and configuration files.
Note: The DHCT software files typically have file extensions of .ver, _0, and _1.
- 12 Repeat step 11 for each software file that is unused in the network. After you have deleted all of the unused software files, go to *Running the listCVT Utility and Removing Unneeded Files* (on page 31).

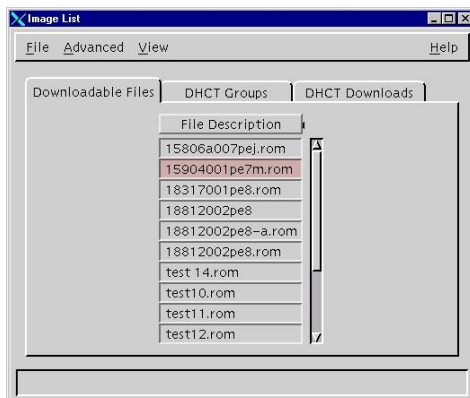
Running the listCVT Utility and Removing Unneeded Files

The listCVT utility determines which DHCT models are currently using the CVT download method and reports unused files on the image list.

- 1 Open an xterm window on the DNCS.
- 2 Type **listCVT -v** and press **Enter**. This command provides the version of listCVT utility that is currently on your network.
- 3 Compare the version number of the listCVT utility on your DNCS with the version number listed in the ROM to Model Matrix in the *Downloading New Client Application Platform Installation Instructions* (part number 4003052).
 - If the version number is same as or later than the one listed in the matrix, go to step 4.
 - If the version number is earlier than the one listed in the matrix, contact Cisco Services to receive the latest utility.
- 4 Type one of the following, based on the system release you have installed:
 - For SR 4.2.1 and earlier, type **cd /export/home/dncs/doctor** and press **Enter**.
 - For SR 4.3 and later, type **cd /dvs/dncs/Utilities/doctor** and press **Enter**.**Note:** Be sure to type a space between **cd** and **/**.
Result: The current directory is now the doctor directory.
- 5 Type **listCVT > precvt** and press **Enter**.
- 6 Type **more precvt** and press **Enter**. This command enables you to view the file and verify the current download configuration for each DHCT type that is active in the network.
- 7 Does the report indicate that there are unused files?
 - If **yes**, go to step 8.
 - If **no**, you have completed this procedure.
- 8 On the DNCS Administrative Console, select the **DNCS** tab and then select one of the following tabs based on the system release you have installed:
 - For SR 2.5/3.5/4.0 and earlier, select the **Element Provisioning** tab.
 - For SR 2.7/3.7/4.2 and later, select the **Home Element Provisioning** tab.

Chapter 3 Optimize Your System Performance for Downloads and Staging

- 9 Click **Image**. The Image List window opens.
- 10 Click the **Downloadable Files** tab.



- 11 Highlight a software file that is unused in the network, click **File > Delete**.

Notes:

- The DHCT software files have file extensions of **.rom** (for 4250-series DHCTs) or **.disk** (for 8300-series DHCTs).
- If a download is associated to a group, the operator should delete the download on the **DHCT Downloads** tab, then delete the image from the **Download Files** tab.

- 12 Repeat step 11 for each file that is unused in the network until all unused software files are deleted.

Clean Up the ResApp Directory

This section provides instructions to clean up the resapp directory.

Important: This procedure is optional, but we recommend that you clean up the directory. The fewer files that are in the directory, the easier the remaining installation procedures. Refer to *How Do I Manage the Files on My System?* (on page 22) for more information.

Cleaning Up the ResApp Directory

- 1 Open an xterm window on the DNCS.
 - 2 Log on to the DNCS as root.
 - 3 Type **cd /dvs/resapp** and press **Enter**.
- Note:** Be sure to type a space between **cd** and **/**.
- 4 Type **ls** and press **Enter**.
 - 5 Delete the software files for the previous versions of software.

Example: Type **rm *1.52*** and press **Enter**.

Important: The CVT download process makes copies of the files currently in use; therefore, deleting files from this directory has no system impact.

- 6 Go to *Verify the Download Directory* (on page 33).

Verify the Download Directory

Before you download the client application software from the FTP server, you must verify that the `/export/home/dncls/download` directory exists on your DNCS. If it does not, you need to create that directory.

Follow these instructions to verify the existence of the download directory on your DNCS and to create it if it does not exist.

- 1 Open an xterm window on the DNCS.
- 2 Log on to the DNCS as root.
- 3 Type `cd /export/home/dncls/download` and press **Enter**.
Note: Type a space between `cd` and `/`.
- 4 Does the `/export/home/dncls/download` directory exist on your DNCS?
 - If **yes**, you are finished with this procedure. Go to *Clean Up the Download Directory* (on page 33).
 - If **no**, go to step 5.
- 5 Type `mkdir /export/home/dncls/download` and press **Enter**.
Note: Type a space between `mkdir` and the `/`.
- 6 Type `cd /export/home/dncls/download` and press **Enter**.
Note: Type a space between `cd` and `/`.
- 7 Go to *Clean Up the Download Directory* (on page 33).

Clean Up the Download Directory

This section provides instructions to clean up the download directory (`/export/home/dncls/download`).

Important: Perform the steps in this section so that the only files left in your directory after your FTP download are those you need for the software update.

Cleaning Up the Download Directory

- 1 Open an xterm window on the DNCS.
- 2 Log on to the DNCS as root.
- 3 Type `cd /export/home/dncls/download` and press **Enter**.
Note: Be sure to type a space between `cd` and `/`.
- 4 Type `ls` and press **Enter**.
- 5 Type `rmi -rf [filename]` for each file listed in the directory.
Note: Do not type the brackets `[]` in the command.
- 6 Confirm the file deletion by typing **yes** and pressing **Enter**.
- 7 Repeat steps 5 and 6 for each file in the directory.

Recommendations to Improve Your Data Carousel Rate

Operators of our DBDS have flexibility in managing both the content and the performance characteristics of their data carousels. This chapter provides background information and recommendations for managing inband and out-of-band data carousel rates on the DNCS. It also provides a procedure for verifying data carousel rate settings and changing them, if necessary.

Note: The terms *data carousels* and *data pumps* are sometimes used interchangeably.

SARA Data Carousel Rate Settings

The following table lists the default data carousel rate settings for systems that use SARA. The footnote numbers are explained on the following page. Also, refer to *General Notes About the SARA Data Carousel Rate Settings* (on page 37) for more general information about the SARA carousels and source IDs.

Source ID	Data Carousel	Data Rate (Mbps)	Block Size (Bytes)	Indication Interval (ms)	Enabled/Run (see note 1)
0	System Carousel	0.01	1024	200	x
1	Out-of-Band	0.05 See note 6	1024	200	x
2	Inband	1.00	4000	100	x
3	CAM OOB	0.01	1024	200	x
4	CAM IB	1.00	4000	100	See note 2
5	IPG OOB	0.05	1024	200	x
6	IPG1 IB	1.00	4000	100	x
7	PPV OOB	0.01	1024	200	x
8	PPV IB	1.00	4000	100	x
9	SAM	0.05	1024	200	x
10	IPG2 IB	1.00	4000	100	x
11	podData	0.03	1024	200	x
12	IPG3 IB	1.00	4000	100	x
14	IPG4 IB	1.00	4000	100	x
16	IPG5 IB	1.00	4000	100	x
18	IPG6 IB	1.00	4000	100	x
20	IPG7 IB	1.00	4000	100	x
21	MMM OOB	0.10	1024	200	x

Recommendations to Improve Your Data Carousel Rate

Source ID	Data Carousel	Data Rate (Mbps)	Block Size (Bytes)	Indication Interval (ms)	Enabled/Run (see note 1)
22	PPV IB2	1.00	4000	100	x
24	SGM IB1	1.00	4000	100	See note 4
26	SGM IB2	1.00	4000	100	See note 4
28	SGM IB3	1.00	4000	100	See note 4
30	SGM IB4	1.00	4000	100	See note 4
32	SGM IB5	1.00	4000	100	See note 4
199	bootloader	3.00	4000	100	See note 3
	Default IB Total:	14			See note 5
	Default OOB Total	0.310			

Specific Notes About the SARA Data Carousel Rate Settings

Each item in the following list pertains to the corresponding footnote number in the preceding table.

- The **Enabled/Run** column pertains to the **Sources** field on the Set Up BFS Source window on systems supporting SR 2.5/3.5/4.0 and later software. After an inband source is disabled, the session for that source is torn down (if active), and the session will not be restored until the BFS source is re-enabled. Also, note that the data pumps for inband and out-of-band sources will not restart until the BFS source is re-enabled.

Notes:

- When you disable (or stop) a source, you free up its associated bandwidth.
 - For systems using SR 4.3 and later, the parameter has changed from "enable/disable" to "run/stop".
- Follow these guidelines to configure the Data Rate for the **CAM IB** data carousel:
 - If your site uses the camFastRefresh feature, set the Data Rate for the CAM IB data carousel to 1.0 Mbps and enable (or run) the source.
 - If your site does not use the camFastRefresh feature, follow these guidelines:
 - For SR 2.5/3.5/4.0 and later software, disable (or stop) the source.
 - For system software earlier than SR 2.5/3.5/4.0, set the Data Rate for the CAM IB data carousel to 0.50 Mbps.
 - For system releases prior to SR 2.5/3.5/4.0, the bootloader carousel is managed by the OSM process and is not visible on the BFS user interface. The 3.00 Mbps data rate of the bootloader carousel, however, must be considered as part of the total inband data carousel rate.

Note: For SR 2.5/3.5/4.0 and later, the bootloader carousel is managed by the bfsServer process and is visible on the BFS user interface.

Chapter 3 Optimize Your System Performance for Downloads and Staging

- 4 SGM IB carousels are added to the default carousels when Switched Digital Video (SDV) is enabled on the system. These carousels provide the mini-carousel discovery files to the SDV client to determine the mini-carousel frequencies available. This method of mini-carousel discovery is used only by SARA SDV clients.

In addition, SARA SDV client software supports an alternate means of obtaining its mini-carousel, which does not require downloading the mini-carousel discovery file. If the SDV client does not require the mini-carousel discovery file, then all SGM IB carousels should be disabled/stopped. If the SARA SDV client uses the mini-carousel discovery file method, then you will enable these carousels based on the number of SDV-enabled service groups are defined on the system.

Each SGM IB carousel supports a maximum of 476 SDV-enabled service groups. Refer to the DNCS release notes for your system release for more details on enabling these carousels.

- 5 The BFS IB total includes CAM IB, but does not include any SGM IB carousels.
- 6 The servicegroupmap.dat file is distributed using the OOB carousel. With systems expanding the number of service groups and/or number of QAMs per service group, the default recommendation may need to be increased for better service group discovery. The following table provides some guidelines on when to increase this rate.

Number of Service Groups	Number of QAMs per Service Group	Recommended Rate
< 400	16	50 Kbps
< 800	8	50 Kbps
400 – 800	16	100 Kbps
800 – 1600	8	100 Kbps
800 – 1200	16	150 Kbps
1600 – 2400	8	150 Kbps

Note: 150 Kbps is the maximum recommended rate for the OOB carousel to ensure sufficient QPSK downstream bandwidth for other OOB messaging.

For systems that surpass the above number of service groups and QAM combinations, DNCS SR 4.2.1.30 (and later) allows you to select the number of QAMs that are included in the servicegroupmap file. The following table provides our rate recommendations, assuming that each service group is limited to 3 QAM carriers in the servicegroupmap file.

Number of Service Groups	Number of QAMs per Service Group	Recommended Rate
< 2000	3	50 Kbps
2000 – 4000	3	100 Kbps
4000 – 6000	3	150 Kbps

General Notes About the SARA Data Carousel Rate Settings

Note these general points about the data in the SARA Data Carousel Rate Settings table:

- The rows highlighted in gray represent inband data carousels.
- The rows without the gray highlighting represent out-of-band (OOB) data carousels.
- We recommend that you use even-numbered source IDs for inband carousels and odd-numbered source IDs for OOB carousels.

General Guidelines for Configuring Data Carousels

Introduction

This section contains general guidelines for configuring the Broadcast File Server (BFS), as well as for managing inband and out-of-band data carousels.

BFS Performance Recommendations

When setting your inband and out-of-band data carousel rates, consider the following points as they pertain to the configuration of your BFS:

- The presence of third-party applications does not require that you configure one data carousel per application. You may assign multiple files to the same carousel, as long as you consider the specific performance requirements of the network. The more files you assign to a given data carousel, the longer it will take for the files to transfer to the set-top.
- You can redistribute existing application files among the data carousels as you add new application files to your system. Consider the specific transfer speed requirements of the files when deciding whether to redistribute the application files.
- Do not use any system default data carousels for third-party application files. We reserve default carousels for system files only. Consider carousels that are set up automatically by the DNCS and have a source ID of less than 200 to be default carousels.

VPI / VCI Pairing

Note: This discussion of VPI/VCI pairing pertains only to sites that use a BFS BIG and does not pertain to sites that use an ASI/HMUX card. The Direct ASI implementation does not use ATM.

We recommend that you map at least 20 VPI/VCI pairs in your Asynchronous Transfer Mode (ATM) switch for inband data when initially configuring the system. The DNCS port on the ATM switch uses VPI/VCI permanent virtual circuits (PVCs) 0/256 through 0/275. These PVCs must be mapped to VPI/VCI pairs $x/256$ through $x/275$ respectively, (where x represents any available VPI) on the Broadband Integrated Gateway (BIG) port of the ATM switch. There is one VPI/VCI PVC for each inband data carousel for up to 20 inband carousels.

If you plan to support more than 20 inband data carousels, you need additional PVCs on the ATM switch. Begin configuring your additional PVCs at 0/276.

The BIG ATM module has no awareness of the VPI. Hence, the ATM switch can map the incoming DNCS PVCs to any VPI on the outgoing BIG PVCs. For simplicity, we recommend that you use VPI of 0.

Change the Data Carousel Rates for an SR 2.5/3.5 and Later System

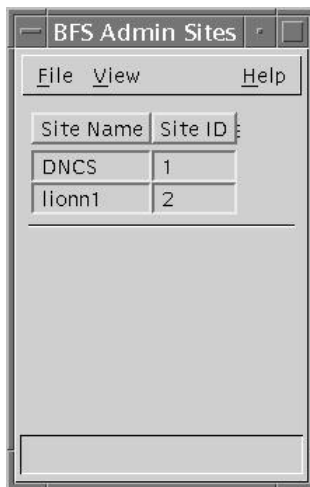
The instructions in this section guide you through the steps of editing the data carousel rates (and related fields) on a system that supports SR 2.5/3.5/4.0 or later system software.

Note: To edit the data carousel rates on a DBDS using a prior release, refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377).

Changing the Data Carousel Rates for the bootloader

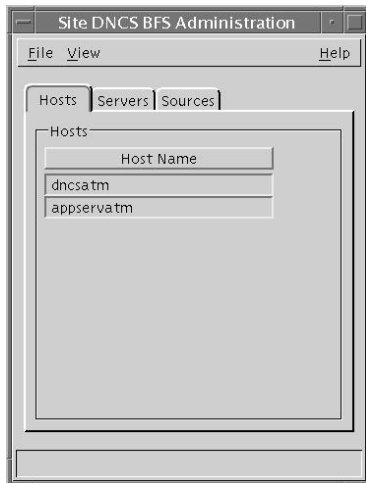
Follow these instructions to change the data carousel rates.

- 1 From the DNCS Administrative Console, select the **Application Interface Modules** tab.
- 2 Click **BFS Admin**. The BFS Admin Sites window opens.



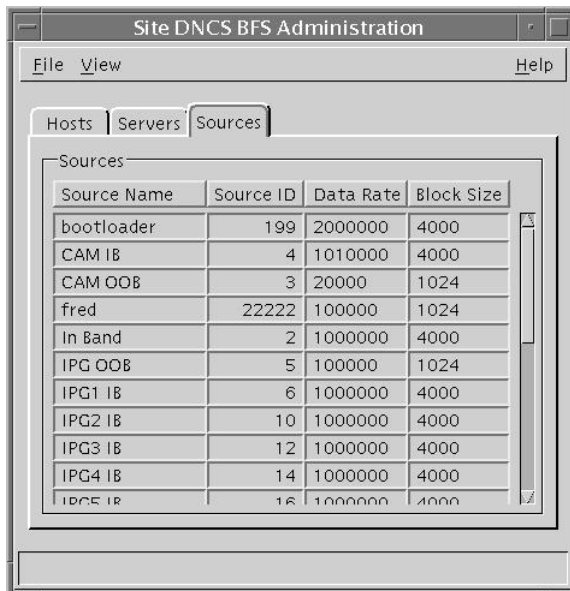
Note: The system used in this example supports the Regional Control System (RCS) feature that uses the DNCS to manage several remote headends. The lionn1 site (shown in this example) is a remote headend. Your system may support more remote headends or might not support the RCS feature at all.

- 3 Double-click the DNCS site. The Site <DNCS> BFS Administration window opens.



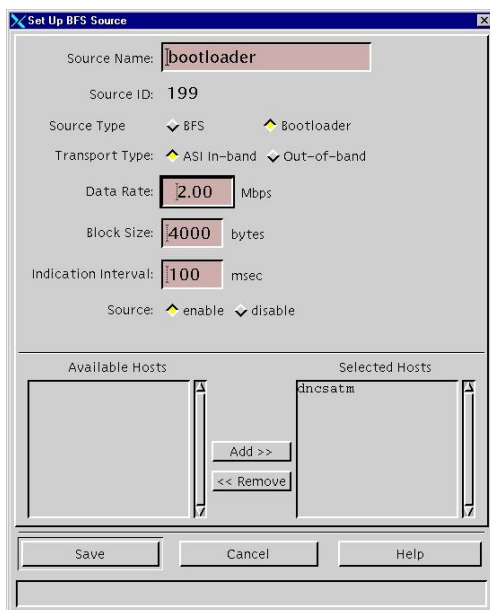
Note: The name of this window will vary, based on the site you select.

- 4 Click the **Sources** tab. The window updates to display a list of BFS source names and associated configuration data.

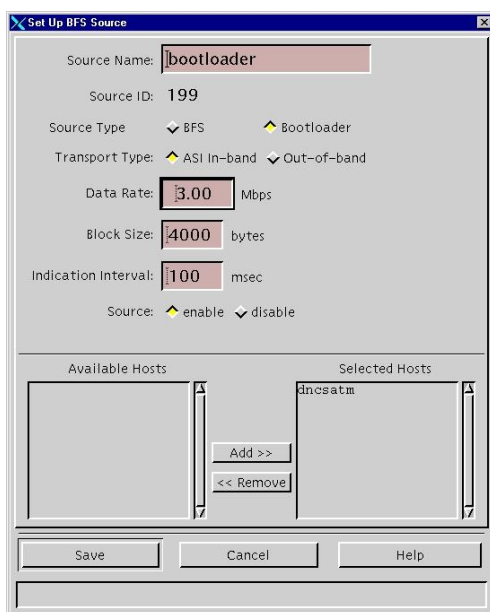


Chapter 3 Optimize Your System Performance for Downloads and Staging

- 5 Double-click the bootloader source. The Set Up BFS Source window for the bootloader opens.



- 6 Set the **Data Rate** to 3.00 Mbps.



- 7 Click **Save**.

Results:

- The Set Up BFS Source window closes.
- The DNCS saves the new settings.
- The BFS automatically repopulates the data carousel. During this period, the carousel may be down for a few minutes.

Note: The staging process could be affected when you change data rates. The download interruption is brief, as the session restarts in a few minutes.

Recommendations to Improve Your Data Carousel Rate

- 8 After examining and changing (if necessary) the carousel data for each source on the DNCS site, go back to step 3 and repeat this procedure for each of the remote sites supported by the system.
- 9 After you have changed all the data carousel rates, click **File> Close** on the Site <Site Name> BFS Administration window.

4

Staging Area Considerations

Introduction

This chapter lists suggested specifications to use for staging DHCTs and describes other network and equipment requirements for the staging area.

In This Chapter

■ Minimum Network Requirements	46
■ QAM Requirements.....	47
■ QPSK Requirements	49
■ CMTS Requirements	50
■ Ventilation and Handling.....	51
■ CableCARD Module Requirements	52

Minimum Network Requirements

The staging area must be connected to a DBDS network that provides a signal from at least one QAM connected to a Broadband Integrated Gateway (BIG) and a single QPSK or CMTS.

QAM Requirements

QAM Forward Path Levels

The following table provides the QAM staging area RF requirements that can be checked from Page 5 of the DHCT diagnostic screens.

Item	Modulation Rate	QAM Level
Current QAM: Level	64 QAM	-20 to +14 dBmV
	256 QAM	-14 to +14 dBmV
Current QAM: S/N	64 QAM	> 27 dB*
	256 QAM	> 31 dB*

* Relative to QAM power

The following table provides the QAM staging area RF requirements that can be checked using the procedures in the *NCTA Recommended Practices for Measurements on Cable Television Systems*.

Item	Modulation Rate	QAM Level
Analog/Digital Difference at DHCT	64 QAM	6 to 10 dB down**
	256 QAM	3 to 6 db down**
Amplitude Response of 6 MHz Channel	64 QAM	< 5 dB
	256 QAM	< 5dB
CTB, CSO, CM	64 QAM	< -50 dB**
	256 QAM	< -53 dB**

** NCTA method relative to analog

Recommended Frequencies for Improved CVT Download Performance

During the CVT download process, the DHCT scans a set of recommended frequencies. If the DHCT does not initially find the recommended frequency, it then searches all frequencies.

This section provides the recommended download frequencies for the following frequency plans:

- Standard frequency (STD)
- Incrementally related carrier (IRC)
- Harmonically related carrier (HRC)

Chapter 4 Staging Area Considerations

Using the frequencies in this appendix vastly improves the speed and performance of the initial staging process.

After a DHCT has been successfully downloaded using the CVT download method, the DHCT retains the frequency of the carousel for subsequent downloads and, therefore, does not search for the frequency again.

What Are the Recommended Frequencies?

We strongly recommend that you configure at least one QAM modulator to use one of the recommended frequencies shown in the following table.

Channel	HRC Frequencies	IRC and STD Frequencies
36	295.75 MHz	297.0 MHz
61	445.75 MHz	447.0 MHz
77	541.75 MHz	543.0 MHz
79	553.75 MHz	555.0 MHz
101	655.75 MHz	657.0 MHz

Important:

- These are the channels and frequencies that the DHCT checks first during staging. If you use other frequencies, then the DHCT is forced to scan all possible frequencies until it finds the correct frequency.
- Although additional scanning increases the time needed to download software, the CVT download method operates at all STD, IRC, and HRC frequencies.
- Because the CVT information is loaded into all QAMs, or those selected as staging bridges, the selected QAM does not need to be the QAM used to carry the BFS sessions. You may select from any of the QAMs configured in your network.

QPSK Requirements

QPSK Recommendations

The RF requirements for the QPSK modulator are as follows:

- The available spectrum of 1 MHz must be within the range of 70 MHz to 130 MHz.
- The selected spectrum must be free of ingress, spurious, and spillover signals from other services.
- The center frequency can be set at 0.25 MHz increments starting with 70 MHz.

QPSK Forward and Reverse Path Levels

The following table provides QPSK signal level requirements that can be checked on page 5 of the DHCT diagnostic screens.

Item	Forward Path Levels
Current FDC: Level	-16 to +15 dBmV
Current FDC: S/N	> 21 dB

The following table provides QPSK signal level requirements that can be checked using procedures in the *NCTA Recommended Practices for Measurements on Cable Television Systems*.

Item	Forward Path Levels	Reverse Path Levels
Analog/Digital Ratio at DHCT	< 10 dB	Not applicable
Amplitude Response in 1 MHz	< 1 dB	< 1 dB
Delay Response in 1 MHz	< 100 ns	<100 ns

CMTS Requirements

CMTS Forward and Reverse Path Levels

RF Downstream (Forward Path)

Item	Value
Frequency Range	88 MHz to 860 MHz
Demodulation	<ul style="list-style-type: none"> ■ 64 QAM ■ 256 QAM
Maximum Data Rate	<ul style="list-style-type: none"> ■ 30 Mbps for 64 QAM ■ 43 Mbps for 256 QAM
Carrier-to-Noise Ratio	> 35 dB
Bandwidth	6 MHz
Operating Level Range	-15 dBmV to +15 dBmV

RF Upstream (Reverse Path)

Item	Value
Frequency Range	5 MHz to 42 MHz
Modulation	<ul style="list-style-type: none"> ■ 16 QAM ■ 64 QAM
Maximum Data Rate	<ul style="list-style-type: none"> ■ 10.2 Mbps for 16 QAM ■ 30.0 Mbps for A-TDMA and SCDMA
Carrier-to-Interference plus Ingress Ratio	> 25 dB
Bandwidth	200 kHz to 6.4 MHz

Ventilation and Handling

DHCTs can overheat if not ventilated properly. Make sure that each DHCT receives proper ventilation. Do not stack more than four DHCTs on top of each other in the same rack. If the DHCTs contain DVRs, do not stack more than two DHCTs on top of each other in the same rack.

**CAUTION:**

Avoid damage to the hard disk drive! The DVR contains an internal hard disk drive. You should take extra care to handle this unit gently. Do not move the unit while it is connected to a power source.

After staging the DVR, wait 15 seconds after power is removed before handling the DVR and removing it from the staging rack.

Do not stand the DVR on its front faceplate while connecting cables to the back panel. Pressing down on the rear panel does not distribute all of the weight across the Explorer frame; rather it localizes the pressure onto the navigation buttons. The force can damage the underlying button supports, which renders the buttons unusable.

CableCARD Module Requirements

CableCARD Hosts

The specifications for CableCARD hosts are determined by the host manufacturers. However, the levels appropriate for staging DHCTs should be sufficient to stage CableCARD modules.

Important: Avoid damage to CableCARD hosts! The card slot in most CableCARD hosts is intended for infrequent use. For more information on handling and installing CableCARD modules, refer to *Best Practices for Using Single-Stream PowerKEY CableCARD Modules* (part number 4015091).

5

Obtain and Load EMM Data

Introduction

This chapter contains procedures that DNCS operators and staging area personnel must complete before they stage devices.

After preparing the DNCS for staging, the DNCS operator must load the Entitlement Management Message (EMM) data onto the DNCS. EMMs are encrypted packets of information that carry default PowerKEY information and service authorizations for DHCTs and CableCARD modules. EMMs let the devices use secure services.

In This Chapter

■ Obtain EMM Data.....	54
■ FTP Download Option.....	55
■ Mail or Shipping Service Option	56
■ Copy the EMM File.....	58
■ Send the EMM File to the DNCS Using FTP.....	59
■ Extract the EMM File.....	60
■ Copy the TOC File	61
■ Load EMM Data.....	62

Obtain EMM Data

To load the EMM data onto the DNCS, you must obtain the two initial EMMs for each device from us. When you order devices from us, you must specify how you want the EMMs for those devices delivered. We can deliver those EMMs to you in one of the following ways:

- Using our secure FTP site—The fastest and most economical way to receive the EMMs. See *FTP Download Option* (on page 55) for more information.
- Using the mail or another shipping service option—We send you a CD containing the EMMs for all devices in the shipment. See *Mail or Shipping Service Option* (on page 56) for more information.

FTP Download Option

You can use FTP to obtain the EMM data from us when you order your DHCTs or CableCARD modules.

If you choose to load EMMs through the FTP site, we will notify you by e-mail whenever new EMMs are available. The e-mail includes a secure link directly to the FTP server. You can click on the link in the e-mail to start downloading EMMs immediately.

Downloading the EMM File

- 1 From the e-mail message, click the link that references your EMM file on the FTP server. A window opens on your PC that lets you specify the directory on your PC where you want to save the EMM file.

Note: The exact method you use to save the downloaded EMM file varies based upon the e-mail software you use on your PC.

- 2 Click on the link in the e-mail that references your EMM file on the Cisco FTP server.
- 3 Save the EMM file in the directory on your PC you choose.

Example: You might choose to save the file in the /temp directory.

- 4 Choose one of the following procedures:
 - To use a CD recorder to copy the EMM TAR file to a CD, go to *Copying the EMM File to a CD* (on page 58).
 - To use a network connection between your PC and the DNCS to FTP the EMM TAR file to the DNCS, go to *Send the EMM File to the DNCS Using FTP* (on page 59).

Mail or Shipping Service Option

You can request that we mail or ship an EMM CD to you when you order your DHCTs or CableCARD modules.

Copy the EMM File

After you download the EMM file, and before you load the EMMs onto the DNCS, you must first copy the EMM file to a CD. This section provides procedures for copying the EMM file to a CD before loading the file onto the DNCS.

Copying the EMM File to a CD

Important: Be sure you know how to use your CD recorder to copy files before starting this procedure.

- 1 Insert a blank CD into the CD recorder of your PC.
- 2 Copy the EMM file from the directory where you saved it on your PC to the CD.
Note: If necessary, refer to the user's guide that accompanied your CD recorder for detailed instructions for copying files.
- 3 Eject the CD.

Copying the EMM File to the DNCS

- 1 Insert the CD into the CD-ROM drive of your DNCS and the system mounts the CD to `/cdrom/cdrom0`.
- 2 Open an xterm window on the DNCS.
Note: We recommend that you store your EMM file in the `/dvs/dnscs/emmcads` directory on the DNCS. If necessary, see *Create EMM Directories* (on page 14) for additional information.
- 3 Type `cd /dvs/dnscs/emmcads` and press **Enter**.
- 4 Type `cp /cdrom/cdrom0/* .` and press **Enter**. The system copies the EMM TAR file on the CD to the `/dvs/dnscs/emmcads` directory on the DNCS.
Important: After typing `/cdrom/cdrom0/` be sure to type the `*` followed by a space and a period (`.`).
- 5 When the system has finished copying the EMM tar file, type `eject cd` and press **Enter** to eject the CD.

Send the EMM File to the DNCS Using FTP

After downloading the EMM file from the FTP server to your PC, you can use FTP to send the EMM file to the DNCS.

Note: Do this only if you have a network connection between your PC and your DNCS.

Sending the EMM File to the DNCS Using FTP

Follow these steps to FTP the EMM file to the DNCS.

Important: You must know the IP address of your DNCS to complete this procedure.

- 1 Initiate an FTP connection to the DNCS.
- 2 Navigate to the `/dvs/dncls/emmclds` directory on the DNCS.
- 3 Send the file to the DNCS.
- 4 Go to *Extract the EMM File* (on page 60).

Extract the EMM File

If you have properly followed the instructions in this section, the EMM TAR file has been copied to the `/dvs/dnscs/emmcads` directory on your DNCS. Extract the individual components of your EMM TAR file to a directory on the DNCS. Record the path and directory here:

Extracting the EMM File

Follow these steps to extract the EMM file on your DNCS.

- 1 Open an xterm window on the DNCS.
- 2 Type `cd /dvs/dnscs/emmcads` and press **Enter**. The `/dvs/dnscs/emmcads` directory becomes the working directory.
- 3 Type `tar xvf [EMM file name]` and press **Enter**.

Example: If your EMM file is named `0090387249drtvh.tar`, as indicated in previous examples, you would type the following:

```
tar xvf 0090387249drtvh.tar.
```

Results:

- The system creates a subdirectory in the `emmcads` directory. The name of the subdirectory is the name of the EMM file without the TAR extension and a COMPLETE suffix.

Example: `OL00272729-COMPLETE`

- Within this subdirectory is the following directory and file:
 - A **dnscs** subdirectory that contains the EMM data in directories and files that the DNCS uses when you load the EMM data.
 - The **TOC** file.

Important: If any of these are missing, contact Cisco Services.

- 4 Go to *Copy the TOC File* (on page 61).

Copy the TOC File

You need to supply your billing system vendor with the TOC file that you extracted from the EMM file. To do this, you need to copy the TOC file to a floppy disk or CD and install it on your billing system. Refer to your billing system documentation for instructions and specific information.

Load EMM Data

After you obtain your EMM files, you must load the EMMs onto the DNCS. This section provides procedures for loading EMM data into the DNCS database.

During this procedure, two directories on your DNCS are used. Those directories are as follows:

- `/dvs/dncls/tmp/emmclds`—Stores the downloaded EMM CD images
- `/dvs/dncls/tmp/emmcldlogs`—Stores the log files created during the loading of EMMs

Important: When you load the EMM files, make sure that you do *not* provision any DHCTs. Enabling any options on the Secure Services tab in the Set Up DHCT screen causes the DNCS to provision the DHCTs.

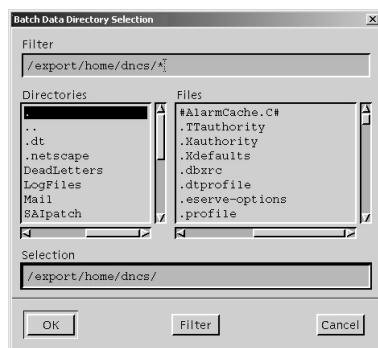
If you do provision DHCTs when you load EMMs, combo binding will not work correctly.

Loading EMM Data

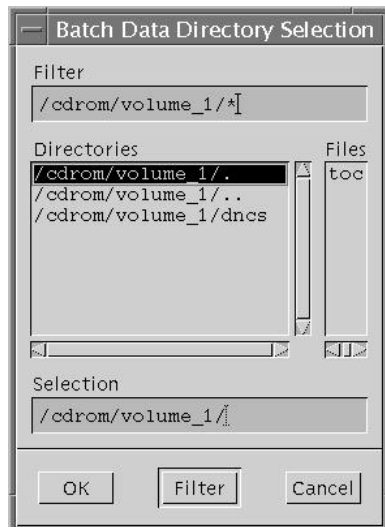
Follow these steps to load EMM data into the DNCS database.

- 1 Are you loading EMM data from CD?
 - If **yes**, make sure that the EMM CD is placed in the CD ROM drive of the DNCS.

Note: The DNCS GUI might launch when the system mounts the CD.
 - If **no**, go to step 2.
- 2 On the DNCS Administrative Console, click the **DNCS** tab and select the **Element Provisioning tab**.
- 3 Click **DHCT** to open the DHCT Provisioning window.
- 4 Select **New** and choose **Batch Install**.
- 5 Click **Select**. The Batch Data Directory Selection window opens.



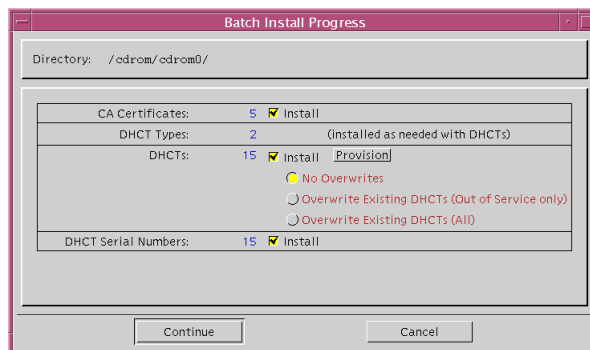
- 6 Search for the TOC file by replacing the existing `/export/home/dnscs` filter in the Filter field with the following text:
 - If you are loading EMMs from CD, replace the `export/home/dnscs` filter with `/cdrom/cdrom0/*` and press **Enter**.
 - If you obtained EMMs through FTP, replace the `export/home/dnscs` filter with the path you recorded in step 6 of *Extracting the EMM File* (on page 60).
- 7 In the Directories panel, highlight and double-click **volume_1**. The Batch Data Directory Selection window refreshes and lists the TOC file.



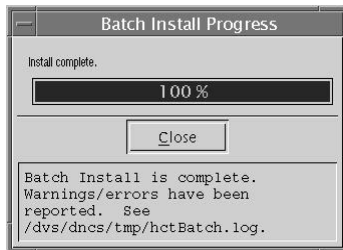
Note: The volume_1 directory may contain additional characters.

Example: volume_1#3

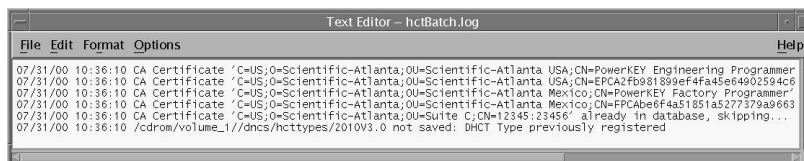
- 8 Locate the **TOC** file, and verify that **TOC** is *not* highlighted. Click **OK**. The DHCT Provisioning window opens.
- 9 Click **Continue** to open the Batch Install Progress window.



- 10 Select one of the following options:
 - If you are loading EMMs for RMA units only, select **Overwrite Existing DHCTs (All)**.
 - If you are loading EMMs for new units only, select **No Overwrites**.
 - If you are loading EMMs for both RMA units and new units, select **Overwrite Existing DHCTs (Out of Service only)**.
- 11 On the Batch Install Progress window, click **Continue**. A window displays the status of the install process.



- 12 After the **Batch Install is Complete** message appears, click **Close** on the Batch Install Progress window.
- 13 From the Solaris toolbar, open the Text Editor to check the hctBatch.log and complete the following steps:
 - a Right-click the background area of the DNCS screen to open the **Workspace Menu** window.
 - b Click the **Programs** option from the Workspace Menu window.
 - c From the Personal Applications menu, select the **Text Editor** option.
 - d From the Text Editor **File** menu, choose **Open**.
 - e On the Text Editor – Open a File window, type **/dvs/dncs/tmp/** in the Enter a Path or folder name field, and press **Enter**.
 - f Scroll through the file list that appears in the Files panel, highlight the **hctBatch.log** file, and click **OK**. The Text Editor displays the contents of the **hctBatch.log** file.



Notes:

- If the DHCT type already exists in the database, the **HctType record with version <type revision> and model <modeltype> already existed in cache** message appears.
- If a DHCT type is not added to the database for any reason, the **HctType record with version <type revision> and model <modeltype> could not be inserted into the database** message appears.

- 14 Select **Copy to File** from the File menu. The Text Editor – Copy to File window opens.
- 15 Type a unique log file name for each EMM CD in the **Enter file name** field. The file name typically follows this naming convention:
/dvs/dncs/tmp/emmcdlogs/<deliverynumber>.log
Example: Type **/dvs/dncs/tmp/emmcdlogs/OL00251237-5618.log** for the file name. **OL00251237-5618** is the delivery number of the EMM CD.
Note: You might want to use the following alternate naming convention on your system:
/dvs/dncs/tmp/emmcdlogs/<deliverynumber>_date_time.log
- 16 Click **OK**. The system saves the log file with the new name.
- 17 Does the DNCS indicate that a new device type was added?
 - If **yes**, you need to make sure a download is configured for the new device type. Refer to *Downloading New Client Application Platform Installation Instructions* (part number 4003052) for more information. When you complete this procedure, go to step 18 of this procedure.
 - If **no**, go to step 18.
- 18 From the **File** menu of the Text Editor window, select **Close**.
- 19 Are you loading EMM data from a CD?
 - If **yes**, open an xterm window and type **eject** and press **Enter** to eject the CD (or, if the GUI is open, you can eject the CD from the GUI).
 - If **no**, go to step 20.
- 20 Repeat steps 1 through 18 for each additional EMM CD.
- 21 Go to *How to Stage DHCTs* (on page 67).

6

How to Stage DHCTs

Introduction

This chapter provides procedures for staging DHCTs and procedures for verifying the staging process.

In This Chapter

■ Overview	68
■ DHCT Staging Flowchart	69
■ Staging DHCTs with Services	70
■ Staging DHCTs For Instastaging	71
■ Verify the PowerKEY Information	72
■ Verifying the Staging Process	75

Overview

This section contains procedures for staging area personnel to stage DHCTs.

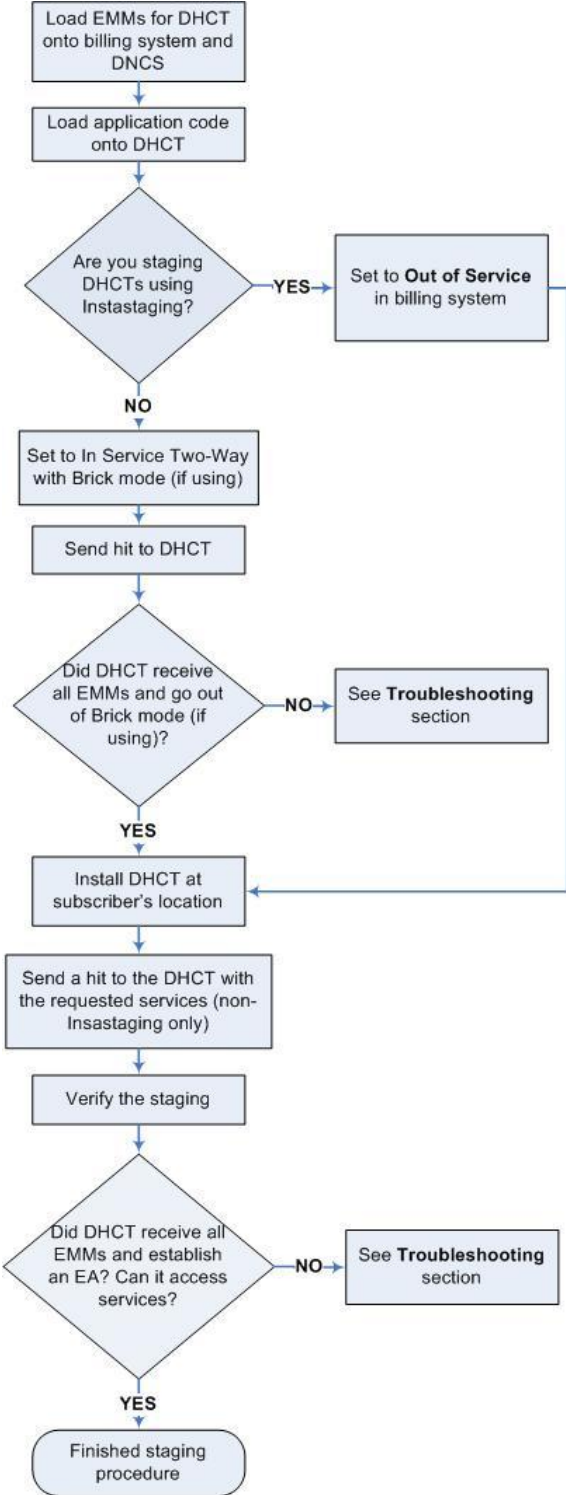
There are two possible outcomes when you stage a DHCT:

- A fully staged DHCT that is set up with the current OS and some level of authorization for services – when DHCTs are staged in this manner, the DHCT only displays services if it is installed within the default EMM timeout period (usually 30 days). After this timeout period, the DHCT will need to receive a hit before it can receive any secure services. See *Staging DHCTs with Services* (on page 70) for more information on fully staging a DHCT.
- An instastaged DHCT that is set up with the current OS and is ready to receive authorization for services when it boots into two-way mode the first time – these DHCTs must be more carefully protected from theft, because they are fully functional as soon as they are installed on a two-way capable cable connection. See *Staging DHCTs For Instastaging* (on page 71) for more information on instastaging DHCTs.

Important: Some billing systems automatically send EMMs to DHCTs when you scan the bar code and/or when you move the DHCT from inventory to a technician's account in the billing system. If your billing system sends EMMs to DHCTs when you scan the bar code, make sure that the DHCTs are connected to an RF signal, have already downloaded software, and currently display either the service disconnect (Brick mode indicator) or the current time before you scan the DHCTs into the billing system.

DHCT Staging Flowchart

The following flowchart illustrates the DHCT staging process.



Staging DHCTs with Services

Follow these steps to stage new or RMA DHCTs.

- 1 Scan the DHCTs into the billing system using the appropriate procedures authorized by your billing system vendor.
Important: Ensure that the billing system operator does not send transactions to the DNCS at this time.
- 2 Unpack the DHCTs you want to stage.
- 3 Place the DHCTs on the staging rack.
- 4 Connect the CABLE IN port to an RF signal.
- 5 Connect the DHCTs to AC power. The DHCT downloads the OS and ResApp software from the DNCS.
- 6 Wait for the DHCTs to indicate that the download is complete (DHCT ready or Brick mode).
- 7 From the billing system, send a "hit" to the DNCS to place the DHCTs in service with at least one package, and, if applicable, authorize DVR capability. Wait for the DHCTs to show the correct indication (DHCT ready or Brick mode).
- 8 Connect the CABLE OUT port on each DHCT to a TV monitor and verify authorized channels.
- 9 Verify DVR functionality (if applicable) using the **LIST** key.
- 10 Does your business process require inventory DHCTs to be authorized for service?
 - If **yes**, go to step 11.
 - If **no**, downgrade (disable) the DHCTs in accordance with your site process, wait for the Brick mode indicator or loss of secure services, and then go to step 11.
- 11 Disconnect the DHCTs and either return them as staged inventory to your warehouse or give them to technicians to install at the subscribers' locations.

Note: Some sites reverse steps 10 and 11 to let the installers see services during the installation before having the DHCT receive a hit with the subscriber's contracted services. If your site does this, the DHCT will only display services if it is installed within the EMM timeout period (by default, 30 days). After the timeout period, the DHCT will need to receive a hit before it can display any secure services.

Staging DHCTs For Instastaging

The instastaging process supports the following two configurations:

- **Subscriber Chooses Services** – the subscriber chooses a group of services before installing the DHCT.
- **Using Default Packages** – the provider assigns a default group of services and adjusts the DHCT to receive subscriber-requested services at a later time.

If you prefer, you can use both methods. Each DHCT stages correctly according to the administrative status it receives (either In-Service Two-Way or Out-Of-Service).

Instastaging DHCTs

Follow these steps to instastage new or RMA DHCTs.

- 1 Unpack the DHCTs you want to stage.
- 2 Place the DHCTs on the staging rack.
- 3 Connect the DHCTs to the RF signal in the staging area.
- 4 Connect the DHCTs to AC power. The DHCT downloads the OS and ResApp software from the DNCS.
- 5 Wait for the DHCTs to indicate that the download is complete (DHCT ready or Brick mode).
- 6 Disconnect the DHCTs from AC power and from the RF signal.
- 7 Scan each DHCT into the billing system. Refer to your billing system documentation for instructions and specific information.
- 8 Place the DHCTs **Out of Service**.
- 9 Return the DHCTs to a secure storage area or give them to subscribers for installation.

Note: These DHCTs must be carefully protected from theft, because they become functional as soon as they are installed on a two-way capable cable connection.

Verify the PowerKEY Information

You can verify the staged PowerKEY information using one of the following methods:

- Staging Toolkit
- Diagnostic screens

Note: If you are verifying POWER LED only DHCTs, you need to use the diagnostic screens.

This section provides detailed procedures for verifying the PowerKEY information using the methods listed above.

Verifying the PowerKEY Information Using the Staging Toolkit

Activating the Staging Toolkit

If you are verifying the PowerKey information on POWER LED only DHCTs, you need to use the procedures in *Verifying the PowerKEY Information Using the Diagnostic Screens* (on page 73).

- 1 Press and hold the **Pause** key on the remote control until the message indicator of the DHCT blinks (approximately 13 seconds).
Note: For POWER LED only DHCTs, the POWER LED blinks four times, pauses, and repeats only once.
- 2 Press one of the following keys:
 - For the 3-function remote controls (models ER-1 and AT2300), press the **PAGE -** key.
 - For the 4-function remote controls (models AT2000 and AT 2400), press the **PREV -** key.
 - For the 4-function PVR/PIP remote controls (model AT8400), press the **PAGE -** key.

Result: The front-panel alphanumeric DHCT LEDs display **E-XX**, where XX is the number of EMMs processed by the DHCT. When XX equals the total number of EMMs (at least 33), the DHCT has received all of its PowerKEY information. The XX varies based on the level of Service Authorizations provisioned for the DHCT.

Note: See *The Staging Toolkit* (on page 165) for more information about monitoring the DHCT status indicators.

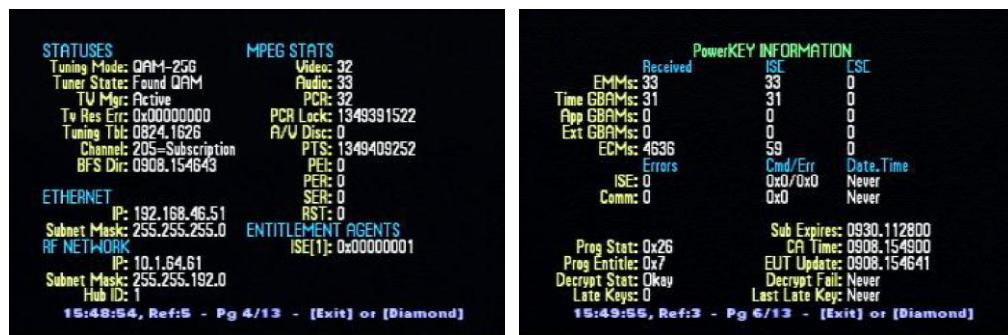
Verifying the PowerKEY Information Using the Diagnostic Screens

- 1 Connect the DHCT to a TV monitor.
- 2 Press and hold the **Pause** key on the remote control until the message indicator of the DHCT blinks (approximately 13 seconds).

Note: For POWER LED only DHCTs, the POWER LED blinks four times, pauses, and repeats only once.
- 3 Press one of the following keys:
 - For the 3-function remote controls (models ER-1 and AT2300), press the **PAGE -** key.
 - For the 4-function remote controls (models AT2000 and AT 2400), press the **PREV -** key.
 - For the 4-function PVR/PIP remote controls (model AT8400), press the **PAGE -** key.
- 4 Using the **PAGE +/NEXT +** or the **Page - /PREV -** keys, go to Page 4 of the diagnostic screens.
- 5 Verify that the ENTITLEMENT AGENTS / ISE(1): field displays **0x0000001**.
- 6 Go to Page 6 of the diagnostic screens and verify the EMMs: / ISE: field displays at least **33**.
- 7 From the same page, verify that the **Sub Expires** field displays the appropriate time stamp (usually 30 days in the future).

Notes:

- The following illustrations are examples of Page 4 and Page 6 of the Explorer diagnostic screens:



- The EMMs: / ISE field will vary based on the level of Service Authorizations provisioned for the DHCT.
- When the DHCT has received all its PowerKEY information, the Time GBAMs: / ISE field will increment, and the ISE error count will no longer increase.
- Refer to *Understanding Diagnostic Screens for the Explorer DHCTs Application Guide* (part number 749244) for more information.

Results:

- The Entitlement Agent displays ISE (1) 0X000000001
 - The Sub Expire date is set to 30 days from today
 - IPPV / VOD / xOD sites are activated (only if you are using them)
 - IPPV cells are not 0 (zero; only if you are using IPPV)
 - VOD cells are not 0 (zero; only if you are using VOD)
- 8 Do the pages display all of the items shown in the results of the preceding step?
- If **yes**, go to step 9.
 - If **no**, send an instant hit to that DHCT using one of the following methods:
 - **Using the billing system.** The billing system has been set up to send the DhctInstantHit command to DHCTs. Refer to your billing system documentation for instructions and specific information.
 - **Using the DNCS.** See *Sending an Instant Hit to a DHCT* (on page 99) for more information.
- 9 Did the instant hit increase the EMM count to the required number?
- If **yes**, you are finished with this procedure.
 - If **no**, go to *DHCT EMM Count Errors* (on page 95) for more information.

Verifying the Staging Process

After the staging process is complete, use the following checklist to check each DHCT and confirm that the staging process was correctly completed.

- 1 Verify that the correct current time appears on the front panel LED (if equipped with front-panel alphanumeric LEDs).
- 2 Verify that the DHCT is receiving audio and video on the following channels:
 - Analog channels (if supported)
 - Digital channels
 - Premium channels
- 3 Verify that the IPG channel banner is available on the bottom of the screen.
- 4 View Page 4 of the diagnostic screens and verify that the ENTITLEMENT AGENTS / ISE[1] field displays **0x0000001**.
- 5 View Page 6 of the diagnostic screens and verify that the date in the SUB EXPIRES field is at least 30 days in the future.
- 6 If you are staging field-return or RMA DHCTs, use the Staging Toolkit to verify the following settings. See *Returning DHCTs and CableCARD Modules to Service* (on page 87) for more information.
 - The Boot Status Indicator displays **111**
 - All personal settings have been cleared and current site defaults are set
 - There are no stranded IPPV events

7

How to Stage CableCARD Modules

Introduction

This chapter provides procedures for staging CableCARD modules and procedures for verifying the staging process.

In This Chapter

- Overview 78
- Setting Up the DNCS for CableCARD Module Staging..... 79
- Staging CableCARD Modules..... 80
- Verify CableCARD Module Staging 85

Overview

To encourage competition in the availability of retail cable devices (hosts) for cable subscribers, the Federal Communications Commission (FCC) has mandated that host devices be available for sale in retail stores.

To comply with this mandate and to help ensure the security of encrypted (secure) digital content, we manufacture the PowerKEY CableCARD Module to work with these host devices. A CableCARD module inserts into a slot on a host device and controls conditional access to secure digital content.

The CableCARD module also unencrypts copy-protected content so that authorized host devices can record this content. The host device, such as a digital cable-ready television, supplies all other basic tuning, navigation, and video display capabilities. If the host device is capable of receiving clear digital content, and the subscriber does not want to receive secure digital content, a CableCARD module is not required. However, a CableCARD module is required if the subscriber wants to receive secure digital content.

A subscriber in a cable system that uses our broadband delivery equipment must use a PowerKEY CableCARD Module. Any host device can be purchased from a retail store or elsewhere, but the CableCARD module must come from the service provider for the subscriber's service area.

The CableCARD module uses the PowerKEY Conditional Access System in the same manner as an Explorer DHCT to decrypt secure digital content. In fact, you authorize CableCARD modules for services in the same way that you authorize Explorer DHCTs.

Host devices with CableCARD modules can receive both inband and out-of-band data. However, host devices without CableCARD modules can receive only inband data.

Setting Up the DNCS for CableCARD Module Staging

For the procedures to set up your DNCS for staging CableCARD modules, refer to one of the following documents:

- *Best Practices for Using Single-Stream PowerKEY CableCARD Modules* (part number 4015091)
- *Setting Up Dual Sources and Hiding Services from One-Way CableCARD Hosts* (part number 4011367)

To improve the staging of CableCARD modules, our engineers have identified the following three best practices:

- Configure a download for a default group of CableCARD modules.
- Avoid sending download-related uncfg messages to CableCARD modules.
- Do not provision CableCARD modules as part of the staging process.

Staging CableCARD Modules

The first step in staging CableCARD modules is to load the EMM CD (or download the EMMs from the Cisco FTP site) and confirm that the correct CableCARD module type exists. See *Obtain and Load EMM Data* (on page 53) for more information.

Does your billing system allow you to set up CableCARD modules with no billing action?

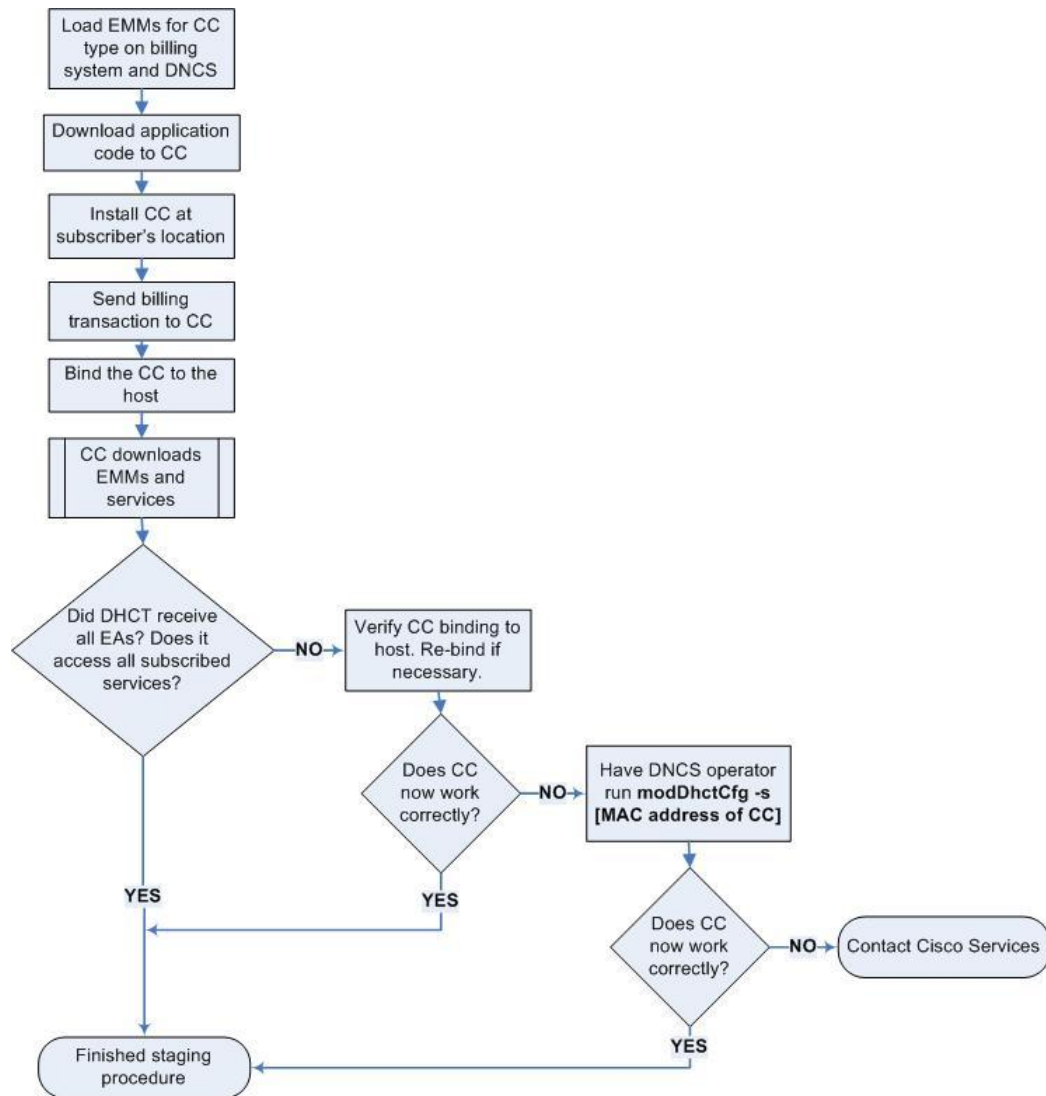
- If **yes**, go to *Stage CableCARD Modules with No Billing Action* (on page 80).
- If **no**, go to *Stage CableCARD Modules with Billing Action* (on page 82).

Stage CableCARD Modules with No Billing Action

If your billing system allows you to set up CableCARD modules with no billing action, you can stage them using the procedures in this section. If your billing system requires a billing action when you stage CableCARD modules, you must use the staging procedures in *Stage CableCARD Modules with Billing Action* (on page 82).

Staging with No Billing Action Process

The following flowchart illustrates the staging process for CableCARD (CC) modules when you can set up your billing system with no billing action.



Staging CableCARD Modules with No Billing Action

Follow these steps only if your billing system allows the status of the CableCARD module to be set with no billing action.

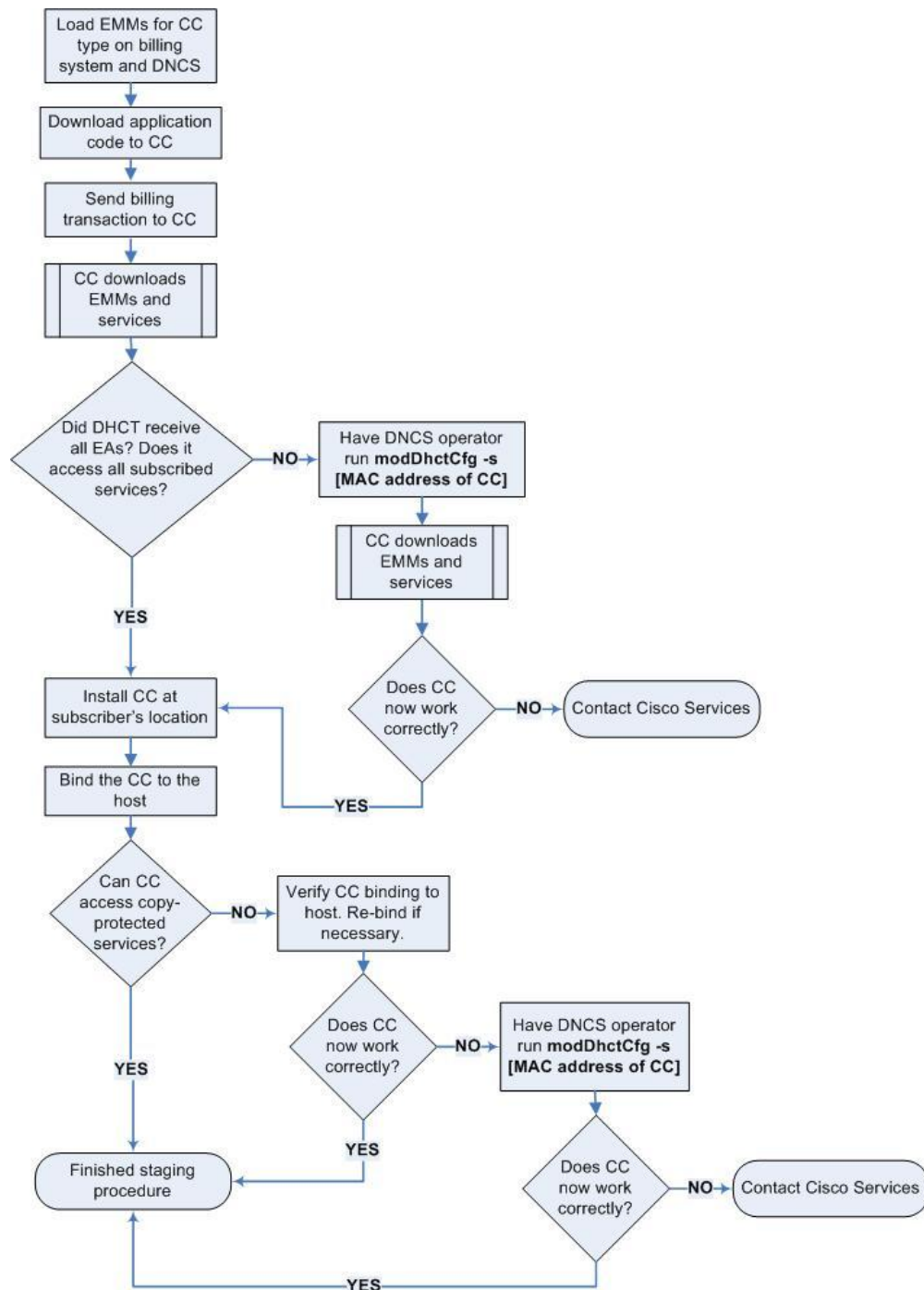
- 1 Download the application code to the CableCARD module.
- 2 Is the CableCARD module going directly to a subscriber's location?
 - If **yes**, go to step 3.
 - If **no**, store the CableCARD module for future use.
- 3 At the subscriber's location, insert the CableCARD module into the subscriber's host.
- 4 Send a billing transaction and bind the CableCARD module to the host. If the CableCARD module came directly to the subscriber's location, it downloads the required EMMs and services at this time.
- 5 Did the CableCARD module receive all the required EMMs and Entitlement Agents (EAs) and does it have access to all subscribed services?
 - If **yes**, you are finished staging the CableCARD module.
 - If **no**, follow these steps:
 - a Verify the binding of the CableCARD module to the host. The diagnostic screen should display "authorization received." If it does not, bind the CableCARD module to the host again.
 - b Ask the DNCS operator to run the following command:
modDhctCfg -s [MAC address of CableCARD module]
Note: Do not type the brackets ([]) in the above command; type the MAC address of the CableCARD module. This command resets the CableCARD module and forces it to download the EMMs and EAs again. Test to see if all required EMMs and EAs are present and that the module can access the copy-protected services.
 - c If these steps do not correct the situation, contact Cisco Services for more information.

Stage CableCARD Modules with Billing Action

If your billing system requires that you set up CableCARD modules with billing actions, you must stage them using the procedures in this section. If your billing system allows you to set up CableCARD modules without billing actions, you should use the staging procedures in *Stage CableCARD Modules with No Billing Action* (on page 80).

Staging with Billing Action Process

The following flowchart illustrates the staging process for CableCARD (CC) modules when you must set up your billing system with billing actions.



Staging CableCARD Modules with Billing Action

Important: Follow these steps only if your billing system requires that the status of the CableCARD module be set with billing action.

- 1 Download the application code to the CableCARD module and send a billing transaction. The CableCARD module downloads the required EMMs, EAs, and services.
- 2 Did the CableCARD module receive all the required EMMs and EAs? Does it have access to all non-copy protected services?
 - If **yes**, go to step 3.
 - If **no**, ask the DNCS operator to run the following command:
modDhctCfg -s [MAC address of CableCARD module]
Note: Do not type the brackets ([]) in the above command. This command resets the CableCARD module and forces it to download the EMMs and EAs again. Test to see if all required EMMs and EAs are present and that the module can access the subscribed services. If not, contact Cisco Services for more information.
- 3 At the subscribers location, insert the CableCARD module into the subscriber's host.
- 4 Send a billing transaction and bind the CableCARD module to the host.
- 5 Can the CableCARD module access the subscribed copy-protected services?
 - If **yes**, you are finished staging the CableCARD module.
 - If **no**, follow these steps:
 - a Verify the binding of the CableCARD module to the host. The diagnostic screen should display "authorization received." If it does not, bind the CableCARD module to the host again.
 - b Ask the DNCS operator to run the following command:
modDhctCfg -s [MAC address of CableCARD module]
Note: Do not type the brackets ([]) in the above command; type the MAC address of the CableCARD module. This command resets the CableCARD module and forces it to download the EMMs and EAs again. Test to see if all required EMMs and EAs are present and that the module can access the copy-protected services.
 - c If these steps do not correct the situation, contact Cisco Services for more information.

Verify CableCARD Module Staging

Verifying the PowerKEY Information

You can verify the PowerKEY information on a staged CableCARD module using the diagnostic screens. See *Verifying the PowerKEY Information Using the Diagnostic Screens* (on page 73) for more information.

After the staging process is complete, use the following checklist to check each CableCARD module and confirm that the staging process was correctly completed.

Verify that the CableCARD module receives audio and video on the following channels:

- 1 Analog channels
- 2 Digital channels
- 3 Premium (high-value, copy-protected) channels (this determines whether the CableCARD module has been bound to its host)
- 4 Music channels

CableCARD Module Errors

CableCARD module errors are set by the HOST-POD Interface Standard (ANSI-SCTE 28 2001), as written and approved by the Society of Cable Communications Engineers (SCTE). Please refer to the standards document located on the Internet for the most current error-handling conditions (<http://www.scte.org/documents/pdf/ANSISCTE282004.pdf>).

8

Returning DHCTs and CableCARD Modules to Service

Introduction

This chapter contains procedures that staging area personnel must perform to stage devices that have already been returned from service (RMA and field-return devices).

These procedures are necessary for a device to be returned successfully to the field.

For DHCTs, these procedures include using the staging toolkit to monitor the staging process and clearing previously stored information from the device.

For CableCARD modules, these procedures include using the billing system to de-authorize the CableCARD module from service.

In This Chapter

- Check for Stranded IPPV Events and Clear NVM..... 88
- Returning CableCARD Modules to Service 92

Check for Stranded IPPV Events and Clear NVM

This section contains procedures to prepare a DHCT for in-home use after it has been returned from a subscriber's home. The procedures necessary for processing field returns are listed as follows:

- 1 If your facility uses the Service Disconnect feature (Brick mode), place the DHCT into Service Disconnect mode.
- 2 Check for stranded IPPV events and request collection of any stranded events from a DHCT in a two-way staging area.
- 3 Activate the Staging Toolkit and clear the Non-Volatile Memory (NVM) menu settings.

Note: Clearing the NVM does not remove stored purchases. You must connect the DHCT to the network and poll it using the DNCS to clear stored purchases.

- 4 Format the hard drive in the DHCT if the DHCT is a Home Entertainment Server with a DVR. For further instructions, see *Format the Hard Drive Without Clearing NVM* (on page 157).

Detailed instructions for these procedures are included in this section.

Placing the DHCT into Service Disconnect Mode

This process assumes that your system is using Service Disconnect Mode. If not, then the DNCS system operator must use one of the following to remove the menu settings for the DHCT:

- A billing transaction that sends a reset client NVM transaction—Refer to your billing system documentation for instructions and specific information.
- The DNCS Addressable Config option—Refer to *Enhancing Your Subscribers' Experience: SARA Configurable Options* (part number 4002178) or your DNCS Online Help for more information.

Complete the following instructions to prepare the DHCT for clearing NVM and checking for stranded PPV events.

- 1 Connect the DHCT in a two-way staging area. Wait until the LED displays the time or before proceeding.

Important: A DHCT will attempt to upgrade its software when you connect the RF cable and turn on the power. If this occurs, let the upgrade complete and wait until the LED displays the time or [- - -] before continuing this procedure.

Note: For POWER LED only DHCTs, the **POWER LED** either blinks four times, pauses, then repeats only once (for normal operation); or the LED blinks eight times, pauses, and repeats (for Service Disconnect Mode [- - -]).

- 2 Send a hit to the DHCT from your billing system to place the DHCT into Service Disconnect mode.

- 3 When the LED displays the time or [- - -] (or, for non-LED DHCTs, blinks eight times, pauses, and repeats), go to *Check for Stranded IPPV Events* (on page 89).

Check for Stranded IPPV Events

This section provides instructions for checking for stranded IPPV events for DHCTs with and without LEDs.

Checking for Stranded IPPV Events on DHCTs with Front-Panel Alphanumeric LED Displays

This procedure is for DHCTs with front-panel alphanumeric displays. If your DHCTs do not have front-panel alphanumeric displays, follow the procedure in *Checking for Stranded IPPV Events on DHCTs with Only POWER LED Indicators* (on page 89).

- 1 Activate the staging toolkit using the procedures described in *Activating the Staging Toolkit* (on page 168). The LED panel on the DHCT displays the EMM ISE count for each DHCT that has been entered into the billing system. Before proceeding, wait for the count to stop. There should be 4 or 5 EMMs.
- 2 Press **4** on the remote control and the LED panel displays the PPV purchase count in the form of **P-XX**.
- 3 Does the LED panel display **P-00**?
 - If **yes**, there are no stranded IPPV events. Press the **Exit** key on the remote. The LED panel displays the [- - -] Service Disconnect Mode indicator. You are finished with this procedure.
 - If **no**, then there are stranded IPPV events in the DHCT. Go to *Clearing Stranded IPPV Events* (on page 90).

Checking for Stranded IPPV Events on DHCTs with Only POWER LED Indicators

Note: This procedure is for DHCTs without front-panel LEDs. If your DHCTs have front-panel alphanumeric LED displays, follow the procedure in *Checking for Stranded IPPV Events on DHCTs with Front-Panel Alphanumeric LED Displays* (on page 89).

- 1 Activate the staging toolkit using the procedures described in *Activating the Staging Toolkit* (on page 168). The POWER light indicator blinks four times, pauses, then blinks four times again. This behavior does not repeat.
- 2 Press **4** on the remote control. The POWER light indicator displays one of the following behaviors:
 - Blinks five times quickly, pauses, then repeats. This indicates there are no stranded IPPV events on the DHCT
 - Blinks five times slowly, pauses, then repeats. This indicates there are stranded IPPV events on the DHCT

- 3 Are there IPPV events on the DHCT (the POWER light indicator blinks five times slowly, pauses, then repeats)?
 - If **yes**, go to *Clearing Stranded IPPV Events* (on page 90).
 - If **no**, press the **Exit** key on the remote. The POWER light indicator displays the Service Disconnect Mode indicator blink pattern (blinks eight times, pauses, then repeats).

Clearing Stranded IPPV Events

If the DHCT contains stranded IPPV events, follow these steps to remove them.

Note: The DHCT should be authorized to receive premium services with the time displayed on the LED.

- 1 If your billing system requires the DHCT to be in the subscriber's account before polling occurs, move the DHCT ID into the subscriber's account.
- 2 Activate the diagnostic screens on the DHCT.

Notes:

- See *The Staging Toolkit* (on page 165) for instructions on accessing the diagnostic screens.
 - Refer to *Understanding Diagnostic Screens for the Explorer DHCTs Application Guide* (part number 749244) for additional information.
- 3 Go to Page 7 of the diagnostic screens. The IPPV Collect field displays the time and date that the DHCT was last polled to collect IPPV purchases and the number of Entitlement IDs that have not yet been collected.
 - 4 Collect the IPPV information using one of the following methods:
 - Send an IPPV Collection hit from your billing system to the DHCT. Refer to your billing system documentation for instructions and specific information.
 - Wait one hour to see if the automatic polling process clears the IPPV events.
 - Send an IPPV Poll from the DNCS. You must provide a list of MAC addresses for each of the DHCTs to the DNCS operator when you request an IPPV Poll.

Results: When the DHCT receives the IPPV poll, the following fields change:

- The PPV Collect field displays the current date and time and displays **EIDs=0**.
 - The FPM Poll field displays the current date and time.
- 5 Verify that the PPV Collect field on each DHCT displays **EIDs=0** after the poll. If not, request another poll.

Important: If the IPPV events will not clear, send the unit to Cisco for repair.

- 6 If you moved the DHCT ID into the subscriber's account in step 2, return the DHCT to the appropriate inventory status.
- 7 Disconnect the DHCT.

Resetting the DHCT to the Default Configuration

This process assumes that your system is using Service Disconnect Mode. Follow these steps to reset the DHCT to the default configuration. This process clears the NVM or SARA menu settings and, for DVR-equipped DHCTs, reformats the hard drive and erases all DVR recordings.

Note: If you are troubleshooting the DHCT and need to only reformat the hard drive without clearing the NVM, go to *Format the Hard Drive Without Clearing NVM* (on page 157).

- 1 Activate the staging toolkit using the procedures described in *Activating the Staging Toolkit* (on page 168). The LED panel on the DHCT displays the EMM ISE count for each DHCT that has been entered into the billing system. Before proceeding, wait for the count to stop. There should be 4 or 5 EMMs.
- 2 Place the DHCT in an inventory status that has no authorization profile.
- 3 After the EMM ISE count stops, press the **Exit** key on the remote control. Each DHCT should be in Service Disconnect mode with [- - -] displaying on the LED panel.

Note: For POWER LED only DHCTs, the **POWER** LED either blinks four times, pauses, then repeats only once (for normal operation); or the LED blinks eight times, pauses, and repeats (for Service Disconnect Mode [- - -]).

- 4 Press and hold the **Pause** key on the remote control for approximately 10 seconds or until the message indicator flashes on the DHCT.
- 5 Press one of the following keys:
 - For 3-function or PVR/PIP remote controls, press the **PAGE -** key.
 - For 4-function remote controls, press the **PREV -** key.
- 6 Press one of the following keys:
 - For 3-function or PVR/PIP remote controls, press the **SETTINGS** key.
 - For 4-function remote controls, press the **SETTINGS MENU** key.

Result: The LED panel displays C-0.

- 7 Enter pin code **728469** to clear the existing DHCT settings. The LED panel on the DHCT displays [C - - -], indicating that all menu settings are clear and PINs disabled.

Important: If you are clearing the settings on a DVR-equipped DHCT, this procedure also reformats the hard drive and reboots the DHCT.

- 8 Press the **Exit** key on the remote control.

Returning CableCARD Modules to Service

When subscribers cancel their CableCARD module services, you must remove services from the CableCARD module they return. After you remove these services, the CableCARD module can no longer view encrypted sources or copy-protected content.

Important: The following procedures are *not* required when you remove services from a CableCARD module returned by a subscriber:

- Deleting the CableCARD module from the DNCS database (the DNCS maintains a record of the CableCARD module in the database).
- Modifying the Host Revoked option within the CableCARD module user interface (this option only defines whether or not the CableCARD module is bound to a host).
- Maintaining the CRL list (the CRL list is provided by CableLabs to identify devices that should not be authorized in the system).

Removing Services from CableCARD Modules

You must use billing system transactions to remove services from CableCARD modules.

Note: It is not required to unbind the CableCARD module from the host. However, if your billing system allows it, you might want to delete the binding from the CableCARD module as a housekeeping procedure.

Refer to your billing system documentation for instructions and specific information.

9

Troubleshooting

Introduction

This chapter provides suggestions for troubleshooting Explorer DHCTs that fail the staging process. It also contains general troubleshooting guidelines.

Suggested solutions are also included; however, in some instances, it may be necessary to contact us. Refer to *Customer Information* (on page 109) for contact information.

In This Chapter

■ Staging Failures.....	94
■ DHCT Errors	95
■ Send Instant Hits.....	99
■ OS and ResApp Downloads.....	101
■ PowerKEY/EA Issues	104

Staging Failures

In the unlikely event that a DHCT fails to stage, the tables in this chapter provide the following troubleshooting information:

- The source of the staging failure including symptoms
- Possible solutions for the failure

Refer to the tables in this chapter to troubleshoot problems before returning a DHCT to us. Identify the problem or symptom and try the possible solutions offered.

If the condition persists, or if the symptom is not identified in this chapter, see *Customer Information* (on page 109) for information.

Note: Refer to *Explorer® Digital Home Communications Terminal Troubleshooting Guide* (part number 717867) for additional information on troubleshooting DHCTs.

General Guidelines

Follow these general guidelines as you troubleshoot DHCTs.

- Compare the performance of a suspected failed DHCT to a known good DHCT of the same type and revision.
- If you are staging HD DHCTs using coaxial cable connected to the TV input, you must use the HD Setup Wizard to make sure that the DHCTs are in SD mode.
- Always make sure that your RF connections are connected correctly before you determine whether the DHCT is defective.
- Make sure that you use the correct download method for your site's frequency plan and for the DHCTs that your subscribers use. See *Download Methods* (on page 4) for more information.
- If you must return a DHCT to us for repair, always use a repair tag to properly identify the problem.

DVR Requirements

Follow these general guidelines when you troubleshoot DHCTs with DVRs:

- Always reformat DVRs before you determine whether the DVR is defective.
- Make sure DVRs are properly packaged before you transport them.
- Avoid excessive temperature extremes when you stage or install DVRs.
- Always make sure that your RF connections are correct before you determine whether the DVR is defective.

DHCT Errors

This section provides a list of suggested solutions for problems with the DHCT.

DHCT EMM Count Errors

If you stage a DHCT and the EMM count is zero, you should take the DHCT out of service then try to stage it again. The DHCT might have an IP address on a different hub and, as a result, the EMMs are being sent to the wrong hub.

If you stage a DHCT and the EMM count does not meet the required number (at least 33), you should send an instant hit to the DHCT. See *Send Instant Hits* (on page 99) for more information.

If the instant hit does not increase the EMM count to the required number, go to the Secure Services tab of the Set Up DHCT screen and confirm the following:

- The Secure Element Serial number on the DNCS matches the ISE number on the DHCT (Page 3 of the diagnostic screens). If the numbers do not match, return the DHCT to us for repair.
- The MAC address on the DNCS matches the RF-MAC number on the DHCT (Page 3 of the diagnostic screens). If the numbers do not match, return the DHCT to us for repair.
- The DHCT is on the FRL in the DNCS. If the DHCT is no longer on the list, add it to the list and recheck the DHCT after 5 minutes.
- Ask the DNCS operator to perform the following command:

modDhctCfg -s [MAC address of the DHCT]

This command resets the DHCT and forces it to download the OS and EMMs again.

Note: If none of these situations apply, you may need to run the deleteDHCT script to delete the DHCT from the DNCS, and then scan it again. Contact Cisco Services for more information.



If you stage a DHCT and the EMM count is correct, but there are ISE errors, ask the DNCS operator to run the **modDhctCfg -s [MAC address of the DHCT]** command. If this does not work, contact Cisco Services to obtain new EMMs for the DHCT and try to stage the DHCT again.

DHCT Errors Solutions Table

The following table lists some common symptoms and the corresponding LED display (if applicable), the corresponding POWER LED indicator (if applicable), and possible solutions to the problem. Some DHCTs do not include front-panel alphanumeric LED indicators. These DHCTs rely on the flashing POWER LED indicators to give you information about their status. These errors, where appropriate, are listed in the POWER LED Indicator column in the following table.

Symptom	POWER LED Indicator	Possible Solution
DHCT displays the following symptoms: <ul style="list-style-type: none"> ■ No display ■ POWER button does not work 	Not available	<ol style="list-style-type: none"> 1 Switch the AC input and power cycle the DHCT. 2 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with F1. No Power/Bad Keypad Button.
DHCT displays the following symptoms: <ul style="list-style-type: none"> ■ No display ■ POWER button works 	Not available	<ol style="list-style-type: none"> 1 Follow these steps: <ol style="list-style-type: none"> a Connect the DHCT to a known good RF cable. b Power cycle the DHCT. c Wait 5 minutes. 2 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with D2. Unable to Connect to Network.
DHCT displays one of the following constantly: <ul style="list-style-type: none"> ■ br.xx ■ er.xx ■ xxxx 	Blinks twice in rapid succession (like a heartbeat), repeats	<ol style="list-style-type: none"> 1 Reboot the DHCT by following these steps: <ol style="list-style-type: none"> a Turn the DHCT power off. b Unplug the DHCT power cord from the power receptacle. c Plug the DHCT power cord into the power receptacle. 2 Turn the DHCT power on. 3 Force a download by following these steps: <ol style="list-style-type: none"> a Unplug the DHCT power cord from the power receptacle. b Plug the DHCT power cord into the power receptacle while pressing the SELECT and POWER buttons at the same time (on the DHCT front panel). 4 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with D7. Error Code (BRXX, ERXX, or XXXX).

Symptom	POWER LED Indicator	Possible Solution
DHCT will not download, stays in hunt mode, displaying the following constantly: ■ h.xxx	Blinks once every half-second	<ol style="list-style-type: none"> 1 Connect the DHCT to a known good RF cable. 2 Power cycle the DHCT. 3 Force a download by following these steps: <ol style="list-style-type: none"> a Unplug the DHCT power cord from the power receptacle. b Plug the DHCT power cord into the power receptacle while pressing the SELECT and POWER buttons at the same time (on the DHCT front panel). 4 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with D6. DHCT in Hunt Mode (hXXX).
DHCT will not download, stays in hunt mode, displaying one the following constantly: ■ r--- ■ r.xxx	Blinks twice, pauses, repeats	<ol style="list-style-type: none"> 1 Force a download by following these steps: <ol style="list-style-type: none"> a Unplug the DHCT power cord from the power receptacle. b Plug the DHCT power cord into the power receptacle while pressing the SELECT and POWER buttons at the same time (on the DHCT front panel). 2 If the known good DHCT of the same type and revision does not download, contact your DPCS operator to resolve the network issue. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with D2. Unable to Connect to Network.
DHCT continuously reboots	Not available	<ol style="list-style-type: none"> 1 Power cycle the DHCT. 2 Reformat the hard drive using the Staging Toolkit by following these steps: <ol style="list-style-type: none"> a Disconnect the DHCT's RF input. b Press PAUSE until the Mail indicator flashes. c Press the PAGE - button. d Press LIST three times. e Reconnect the DHCT's RF input. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with D5. Constantly Resets/Reboots.

Symptom	POWER LED Indicator	Possible Solution
DHCT stuck, displaying the following constantly: <ul style="list-style-type: none"> ■ dIAG 	Not available	<ol style="list-style-type: none"> 1 Force a download by following these steps: <ol style="list-style-type: none"> a Unplug the DHCT power cord from the power receptacle. b Plug the DHCT power cord into the power receptacle while pressing the SELECT and POWER buttons at the same time (on the DHCT front panel). 2 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with D4. Unit Stuck in dIAG.
DHCT stuck in brick mode, displaying the following constantly: <ul style="list-style-type: none"> ■ --- (four dashes) 	Blinks eight times, pauses, repeats	<ol style="list-style-type: none"> 1 Follow these steps: <ol style="list-style-type: none"> a Confirm that the DHCT MAC address matches the billing MAC address and that the DHCT is authorized for service. b Ask the DNCS operator to correct any mis-match and send a hit to the DHCT. 2 See <i>PowerKEY/EA Issues</i> (on page 104) for more information. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with one of the following: <ul style="list-style-type: none"> – S2. Stays in Brick Mode (---) – S1. No EMMs/ISE/EA
Front panel LED displays  for 1 second before the DHCT reboots	Not available	<ul style="list-style-type: none"> ■ The Cyclic Redundancy Check verification on the Bootloader code failed. You might be able to stage the DHCT, but the DHCT might not accept an OS upgrade in the future. ■ Return the DHCT to us for repair. Mark the repair tag with D7. Error Code (BRXX, ERXX, or XXXX).
Front panel LED displays  for 5 seconds before the DHCT reboots	Not available	<p>The test of the internal DRAM failed:</p> <ul style="list-style-type: none"> ■ If the condition was a one-time occurrence, after rebooting the DHCT, the DHCT boots correctly into the OS and resident application. ■ If this problem continues, the DHCT reboots continuously and display this message. Return the DHCT to us for repair. Mark the repair tag with D7. Error Code (BRXX, ERXX, or XXXX).

Send Instant Hits

Sometimes, when you stage a device, one of the following might occur:

- The Entitlement Agent might not display.
- The EMM count may not increment to the required number.
- The Sub Expire date is not set correctly.

In these cases, you might need to send an instant hit to the device. This section provides the procedures for sending instant hits to DHCTs and to CableCARD modules.

Sending an Instant Hit to a DHCT

- 1 From the DNCS Administrative Console, click the **DNCS** tab.
- 2 From the DNCS Administrative Console, select one of the following tabs:
 - For SR 2.7/3.7/4.2 and later, click the **Network Element Provisioning** tab.
 - For SR 2.5/3.5/4.0 and earlier, click the **Element Provisioning** tab.
- 3 Click **DHCT**. The DHCT Provisioning Screen opens.
- 4 On the DHCT Provisioning screen, select **Open**.
- 5 Enter the **MAC Address**, **IP address**, or **serial number** of the DHCT and click **Continue**. The Set Up DHCT screen opens.
- 6 From the Set Up DHCT screen, click the **Secure Services** tab.
- 7 Click **DHCT Instant Hit**.

Sending an Instant Hit to a CableCARD Module

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click one of the following tabs:
 - If you are using SR 4.2 and later, click **Home Element Provisioning**.
 - If you are using SR 4.0 and earlier, click **Element Provisioning**.
- 3 Click **CableCARD**. The CableCARD Data Summary screen opens.
- 4 Select the CableCARD module that you want to hit.
- 5 Click **Modify Selected CableCARD**.
- 6 Click **Save CableCARD**. The DNCS will send an instant hit to the CableCARD module.

DHCTs With Only POWER LED Indicators

DHCTs with only POWER LED indicators display the codes associated with downloading, installing, and booting into the SARA as a series of flashing lights using the POWER LED indicator light on the front panel.



Note: You must stage DHCTs with only POWER LED indicators using the CVT download method.

The information conveyed by the POWER LED indicator is discussed in the following sections of this document:



- **DHCT Errors** (on page 95) – Displays several errors that might occur during staging of the DHCT
- **LED Indicators Displayed During a CVT Download** (on page 116) – Displays the POWER LED indicators during the CVT download
- **POWER LED Indicators Displayed on DHCTs** (on page 125) – Displays the POWER LED error indicators if the CVT download fails

OS and ResApp Downloads

This section provides a list of suggested solutions for problems with the operating system (OS), Guardian mode, or downloading the resident applications (ResApp).

Symptom	Possible Solution
SARA blue screen	<ol style="list-style-type: none"> 1 Follow these steps: <ol style="list-style-type: none"> a Connect the DHCT to a known good RF cable. b Power cycle the DHCT. c Wait for the clock to display. 2 Connect to a known good DHCT of the same type to determine if the problem is a network issue. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with D2. Unable to Connect to Network.
Monitor displays the following: ■ Video Recorder Not Ready	<ol style="list-style-type: none"> 1 Wait 10 minutes then press the LIST button. 2 Power cycle the DHCT. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with R5. Video Recorder Not Ready - Your recording device is being checked.
Monitor displays the following: ■ Disk Trouble - Problems with the program storage disk	<ol style="list-style-type: none"> 1 Power cycle the DHCT. 2 Reformat the hard drive using the Staging Toolkit by following these steps: <ol style="list-style-type: none"> a Disconnect the DHCT's RF input. b Press PAUSE until the Mail indicator flashes. c Press the PAGE - button. d Press LIST three times. e Reconnect the DHCT's RF input. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with R9. Disk Trouble - Program Storage Disk.

Symptom	Possible Solution
<p>Monitor displays the following:</p> <ul style="list-style-type: none"> ■ Disk Trouble - Unrecoverable Write Error 	<ol style="list-style-type: none"> 1 Power cycle the DHCT. 2 Reformat the hard drive using the Staging Toolkit by following these steps: <ol style="list-style-type: none"> a Disconnect the DHCT's RF input. b Press PAUSE until the Mail indicator flashes. c Press the PAGE - button. d Press LIST three times. e Reconnect the DHCT's RF input. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with R4. Disk Trouble - Unrecoverable Write Error.
<p>Monitor displays the following:</p> <ul style="list-style-type: none"> ■ Video macroblocking ■ Tiling or freezing ■ Snowy, grainy video 	<ol style="list-style-type: none"> 1 Follow these steps: <ol style="list-style-type: none"> a Connect to a known good RF cable. b Power cycle the DHCT. c Check the output channel configuration (3 or 4). 2 Verify that the same problem occurs on a known good DHCT of the same type on the same channel and a different channel. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with one of the following: <ul style="list-style-type: none"> – V2. Macroblocking/Tiling/Freezing – V4. Poor/No Color – V5. Snowy/Grainy/Noisy Picture
No video	<ol style="list-style-type: none"> 1 Follow these steps: <ol style="list-style-type: none"> a Check the connections to the DHCT, TV configurations, and other outputs. b For HD DHCTs, use the HD Wizard to make sure the DHCT is in the correct mode. 2 Connect the DHCT to a known good RF cable and power cycle the DHCT. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with V1. No Video.
DHCT does not show premium channels, but does show other channels	<ol style="list-style-type: none"> 1 Follow these steps: <ol style="list-style-type: none"> a Confirm that the DHCT MAC address matches the billing MAC address and that the DHCT is authorized for service. b Ask the DNCS operator to correct any mis-match and send a hit to the DHCT. 2 See <i>PowerKEY/EA Issues</i> (on page 104) for more information. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with S5. No Premium Channels.

Symptom	Possible Solution
Front panel LED displays  for 1 second before the DHCT reboots	<ul style="list-style-type: none"> ■ The Cyclic Redundancy Check verification on the Bootloader code failed. You might be able to stage the DHCT, but the DHCT might not accept an OS upgrade in the future. ■ Return the DHCT to us for repair. Mark the repair tag with D7. Error Code (BRXX, ERXX, or XXXX).
Front panel LED displays  for 5 seconds before the DHCT reboots	The test of the internal DRAM failed: <ul style="list-style-type: none"> ■ If the condition was a one-time occurrence, after rebooting the DHCT, the DHCT boots correctly into the OS and resident application. ■ If this problem continues, the DHCT reboots continuously and display this message. Return the DHCT to us for repair. Mark the repair tag with D7. Error Code (BRXX, ERXX, or XXXX).

PowerKEY/EA Issues

This section provides a list of suggested solutions for problems that result from PowerKEY Conditional Access or EA.

Symptom	Diagnostic Screen	Type of DHCT	Possible Solution
No Entitlement Agent (EMMs)	Page 4	Unstaged	<ol style="list-style-type: none"> 1 Does the DHCT's MAC address match the MAC address recorded in the billing system? <ul style="list-style-type: none"> – If yes, follow these steps: <ol style="list-style-type: none"> i Confirm that the actual MAC address for the DHCT matches the MAC address recorded in the DNCS. ii Confirm that the Secure Micro Address for the DHCT matches the Secure Micro Address recorded in the DNCS. iii Ask the DNCS operator to perform a modDhctCfg -s [MAC address of the DHCT] on the DHCT. iv Stage the DHCT again. – If no, follow these steps: <ol style="list-style-type: none"> i Ask the DNCS operator to correct any existing mismatches. ii Stage the DHCT again. iii Go to step 2 if these actions do not remedy the situation. 2 Follow these steps: <ol style="list-style-type: none"> a Take the DHCT out of service. b Try to stage the DHCT again. 3 Follow these steps: <ol style="list-style-type: none"> a Delete the DHCT from the DNCS. b Contact us to have new EMMs built. c Try to stage the DHCT again using the new EMMs. 4 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with S1. No EMMs/ISE/EA.

Symptom	Diagnostic Screen	Type of DHCT	Possible Solution
Sub Expire shows expired or past date	Page 6	Deployed	<ol style="list-style-type: none"> 1 Follow these steps: <ol style="list-style-type: none"> a Confirm that the DHCT is authorized for service in the billing system. b Confirm that the DHCT is authorized for service in the DNCS. c Send an instant hit to the DHCT. d Stage the DHCT again. 2 Follow these steps: <ol style="list-style-type: none"> a Ask the DNCS operator to perform a modDhctCfg -s [MAC address of the DHCT] on the DHCT. b Stage the DHCT again. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with S3. Invalid Sub Expire Date.
Insufficient number of EMMs (less than the minimum of 33 EMMs)	Page 6	Unstaged or Deployed	<ol style="list-style-type: none"> 1 Follow these steps: <ol style="list-style-type: none"> a Confirm that the DHCT is authorized for service in the billing system. b Confirm that the DHCT is authorized for service in the DNCS. c Send an instant hit to the DHCT. d Stage the DHCT again. 2 Follow these steps: <ol style="list-style-type: none"> a Ask the DNCS operator to perform a modDhctCfg -s [MAC address of the DHCT] on the DHCT. b Stage the DHCT again. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with S1. No EMMs/ISE/EA.

Symptom	Diagnostic Screen	Type of DHCT	Possible Solution
No Incoming EMMs	Page 6	Unstaged	<ol style="list-style-type: none"> 1 Does the DNCS have the EMMs loaded for the DHCT? <ol style="list-style-type: none"> a If yes, follow these steps: <ol style="list-style-type: none"> i Ask the DNCS operator to perform a modDhctCfg -s on the DHCT. ii Stage the DHCT again. b If no, contact us to get the correct EMMs. 2 Does the DHCT's MAC address match the MAC address recorded in the billing system? <ul style="list-style-type: none"> – If yes, follow these steps: <ol style="list-style-type: none"> i Confirm that the actual MAC address for the DHCT matches the MAC address recorded in the DNCS. ii Confirm that the Secure Micro Address for the DHCT matches the Secure Micro Address recorded in the DNCS. iii Ask the DNCS operator to perform a modDhctCfg -s [MAC address of the DHCT] on the DHCT. iv Stage the DHCT again. – If no, follow these steps: <ol style="list-style-type: none"> i Ask the DNCS operator to correct any existing mismatches. ii Stage the DHCT again. iii Go to step 3. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with S1. No EMMs/ISE/EA.
No Incoming EMMs	Page 6	Deployed	<ol style="list-style-type: none"> 1 Follow these steps: <ol style="list-style-type: none"> a Confirm that the DHCT boots into two-way mode (that it has an IP address listed on Page 4 of the diagnostic screens). b Ask the DNCS operator to send an instant hit to the DHCT. c Stage the DHCT again. 2 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with S1. No EMMs/ISE/EA.

Symptom	Diagnostic Screen	Type of DHCT	Possible Solution
ISE errors continually increment when an instant hit is sent to the DHCT from the billing system or from the DNCS	Page 6	Unstaged	<ol style="list-style-type: none"> 1 Do the MAC addresses and Secure Micro for the DHCT match what is recorded in the DNCS? <ul style="list-style-type: none"> – If yes, follow these steps: <ol style="list-style-type: none"> i Ask the DNCS operator to perform a modDhctCfg -s on the DHCT. ii Stage the DHCT again. – If no, continue with step 2. 2 Follow these steps: <ol style="list-style-type: none"> a Delete the DHCT from the DNCS. b Contact us to have new EMMs built. c Try to stage the DHCT again using the new EMMs. 3 If these steps do not work, return the DHCT to us for repair. Mark the repair tag with S1. No EMMs/ISE/EA.

10

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

Download LED Indicators

Introduction

This appendix contains explanations of what the front panel Light-Emitting Diode (LED) displays on the Explorer DHCTs mean. It also contains examples of the front panel LED displays, TV screen sequences, and POWER LED flash codes that might appear during DHCT software downloads.

In This Appendix

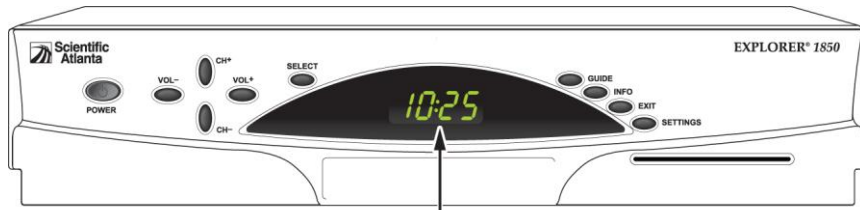
■ Overview	112
■ LED Indicators Displayed During an OSM Download	113
■ LED Indicators Displayed During a CVT Download	116
■ DHCTs with Three LED Indicators	119
■ DHCTs with Single LED Indicators	122
■ POWER LED Indicators Displayed on DHCTs	125

Overview

DHCTs provide feedback during the process of downloading, installing, and booting into the SARA. Where and how this feedback is displayed depends on the type of DHCT you are staging.

DHCTs with Front-Panel Alphanumeric LED Indicators

Explorer DHCTs with front-panel alphanumeric LED indicators display the codes associated with downloading, installing, and booting into the SARA on the front-panel LED indicator.



Alphanumeric LED Indicator

T12375

LED Indicators Displayed During an OSM Download


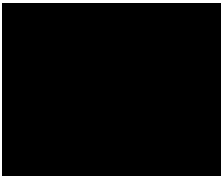




Understanding the LED Indicator Sequence in OSM Downloads

After a DHCT is connected to the RF network and AC power is applied, the Bootloader monitors the download, verification, and installation of the new OS into memory. At the end of the process (which might repeat until the DHCT receives a valid OS download), the DHCT displays one of the following:







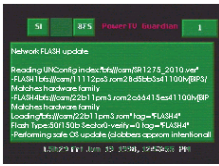











- The Service Disconnect mode (brick mode) indicator (if enabled on your system)
- The clock

The following table shows an example of an OSM download sequence of front panel LED displays that appear after AC power is applied to the DHCT.

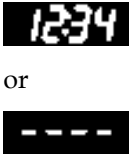

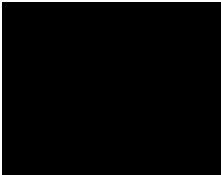
Note: The front-panel alphanumeric LED displays that appear on the Explorer DHCTs may change for each stage of the DHCT software download process. Therefore, in the following table, the LED displays that correspond to certain stages of the download process may be repeated or skipped, as noted in the Description column. In other words, the stages do not always occur in the order shown.

Stage	Alphanumeric LED Indicator	TV Monitor	Description
1.			The “wave” appears each time the DHCT resets. The DHCT is initializing and testing the system. The wave provides a visual cue as to when to press buttons to force auxiliary functions.
2.			The DHCT boots into the OS.
3.			“Dancing dashes” that alternate between the middle [- -] and outside [-] segments appear when the OS runs the Guardian Mode application to receive the upgrade. The image installs from the BFS into internal DRAM.

Appendix A
Download LED Indicators

Stage	Alphanumeric LED Indicator	TV Monitor	Description
4.	 and then 		CLr appears when the current OS image clears. Pr.00 appears when the new received image overwrites it the current OS image.
5.			The rotating border appears when the DHCT boots into the OS.
6.			Dancing dashes appear when Guardian downloads the second part of the image, which contains the ResApp, from BFS to internal DRAM.
7.			The wave indicates that the DHCT resets to execute programming.
8.	 and then 		CLr and PR.00 indicate that the second part of the OS is installed into flash memory. Programs upper memory area with ResApp.
9.			The wave appears after the DHCT resets to boot into the OS and the newly downloaded ResApp.
10.			The rotating border appears when the DHCT resets and boots into the OS.
11.			The LED is clear when the OS has started the ResApp. The DHCT is in an Off state.

LED Indicators Displayed During an OSM Download

Stage	Alphanumeric LED Indicator	TV Monitor	Description
12.	 or 		The DHCT displays the time (normal operation) or the Service Disconnect mode indicator (if activated). The DHCT has received the time from the DNCS.









LED Indicators Displayed During a CVT Download

Understanding the LED Indicator Sequence in CVT Downloads


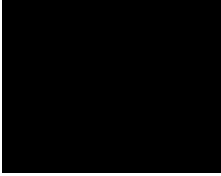

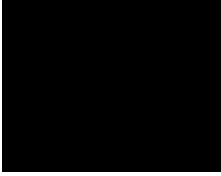


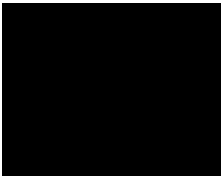





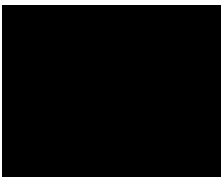

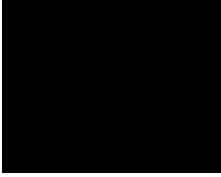
The following table shows an example of a CVT download sequence of front panel LED displays that appear after AC power is applied to the DHCT.

Note: The front-panel alphanumeric LED displays that appear on the Explorer DHCTs may change for each stage of the DHCT software download process. Therefore, in the following table, the LED displays that correspond to certain stages of the download process may be repeated or skipped, as noted in the Description column. In other words, the stages do not always occur in the order shown.



If the DHCT only has a POWER LED indicator, the appropriate blink patterns are listed in the Power LED Indicator column.

Stage	Alphanumeric LED Indicator	POWER LED Indicator	TV Monitor	Description
1.		The light is off.		The “wave” appears each time the DHCT resets. The DHCT is initializing and testing the system. The wave provides a visual cue as to when to press buttons to force auxiliary functions.
2.		Solid on, then off. The light is off as the DHCT boots into the OS.		The rotating border appears when the DHCT boots into the OS.
3.		The light blinks once every half-second.		Fr.LA appears if the DHCT can tune to the last known good frequency in NVM and acquires the CVT. Go to stage 9 of this table.
4.		The light blinks once every half-second.		If the DHCT cannot acquire the CVT through a known good QAM frequency, it scans the recommended QAM frequencies. The LED displays FR.00 through FR.09 as the DHCT checks each of the ten recommended QAM frequencies. Go to stage 6 of this table.

LED Indicators Displayed During a CVT Download

Stage	Alphanumeric LED Indicator	POWER LED Indicator	TV Monitor	Description
5.		The light blinks once every half-second.		If the DHCT cannot acquire the CVT through a recommended QAM frequency, it 'hunts' until it finds the frequency of a QAM with a valid CVT table for that DHCT. The [000] indicates the QAM frequency.
6.		The light blinks twice, pauses, then repeats.		The LED displays r.xxx, where [xxx] indicates the number of packets remaining to be downloaded. This number counts down to zero as the packets are downloaded.
7.	 and then 	The light blinks 3 times, pauses, then repeats.		CLr and PR.00 indicate that the second part of the OS is installed into flash memory. Programs upper memory area with ResApp.
8.		The light is off.		The wave appears after the DHCT resets to boot into the OS and the newly downloaded ResApp.
9.		Solid on, then off. The light is off as the DHCT boots into the OS.		The rotating border appears when the DHCT resets and boots into the OS.
10.		The light is off.		The LED is clear when the OS has started the ResApp. The DHCT is in an Off state. If you use Service Disconnect (brick) mode, go to stage 11 of this table. If you do not use Service Disconnect (brick) mode, go to stage 12 of this table.
11.		For Service Disconnect (brick) mode, the light blinks eight times, pauses for half a second, and repeats.		The DHCT displays the Service Disconnect mode indicator (if activated).

Appendix A
Download LED Indicators

Stage	Alphanumeric LED Indicator	POWER LED Indicator	TV Monitor	Description
12.		For normal operation, the light blinks four times, pauses, then repeats only once.		The DHCT displays the time (normal operation). The DHCT has received the time from the DNCS.

DHCTs with Three LED Indicators


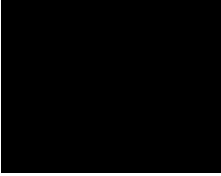
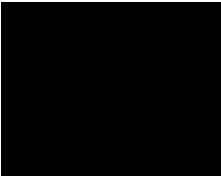




Explorer DHCTs with three front-panel LEDs display the codes associated with downloading, installing, and booting into the SARA as a series of flashing lights using three LEDs on the front panel.

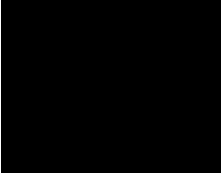


The following table shows an example of a CVT download sequence of front-panel LED displays that appear after AC power is applied to the DHCT.

Stage	LED Indicators	TV Monitor	Description
1	The left LED blinks, the middle LED blinks, the right LED blinks and stays lit.		The “wave” appears each time the DHCT resets. The DHCT is initializing and testing the system. The wave provides a visual cue as to when to press buttons to force auxiliary functions.
2	POWER LED blinks.	 or 	The rotating border appears when the DHCT boots into the OS.
3	LEDs rotate left (through step 5).		This pattern appears if the DHCT can tune to the last known good frequency in NVM and acquires the CVT. Go to stage 9 of this table.
4			If the DHCT cannot acquire the CVT through a known good QAM frequency, it scans the recommended QAM frequencies. Go to stage 6 of this table.

Appendix A
Download LED Indicators

Stage	LED Indicators	TV Monitor	Description
5			If the DHCT cannot acquire the CVT through a recommended QAM frequency, it 'hunts' until it finds the frequency of a QAM with a valid CVT table for that DHCT.
6	During download, the LEDs rotate to the right.		The LED displays this code as it downloads packets.
7	The LEDs rotate left then right, repeat.		This code indicates that the second part of the OS is being installed into flash memory.
8	The LEDs rotate right once, then the right LED stays lit. (Through stage 10.)		This pattern appears after the DHCT resets to boot into the OS and the newly downloaded ResApp.
9		 or 	
10			

Stage	LED Indicators	TV Monitor	Description
11	For Service Disconnect (brick) mode, the left LED blinks eight times, pauses for half a second, and repeats. For normal operation, the left LED blinks four times, pauses, then repeats only once.		The DHCT (or host) is in either Service Disconnect mode or standard mode.

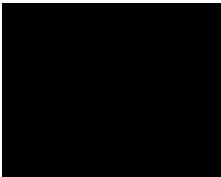



DHCTs with Single LED Indicators





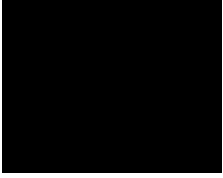
DHCTs with only POWER LED indicators display the codes associated with downloading, installing, and booting into the SARA as a series of flashing lights using the POWER LED indicator light on the front panel.





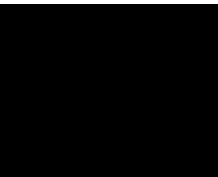
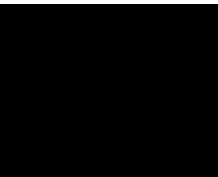
Note: You must stage DHCTs with only POWER LED indicators using the CVT download method.

The following table shows an example of a CVT download sequence of front panel LED displays that appear after AC power is applied to the DHCT.

Stage	POWER LED Indicator	TV Monitor	Description
1	The light is off.		The “wave” appears each time the DHCT resets. The DHCT is initializing and testing the system. The wave provides a visual cue as to when to press buttons to force auxiliary functions.
2	Solid on, then off. The light is off as the DHCT boots into the OS.	 or 	The rotating border appears when the DHCT boots into the OS.
3	The light blinks once every half-second.		Fr.LA appears if the DHCT can tune to the last known good frequency in NVM and acquires the CVT. Go to stage 9 of this table.

Stage	POWER LED Indicator	TV Monitor	Description
4	The light blinks once every half-second.		<p>If the DHCT cannot acquire the CVT through a known good QAM frequency, it scans the recommended QAM frequencies. The LED displays FR.00 through FR.09 as the DHCT checks each of the ten recommended QAM frequencies.</p> <p>Go to stage 6 of this table.</p>
5	The light blinks once every half-second.		<p>If the DHCT cannot acquire the CVT through a recommended QAM frequency, it 'hunts' until it finds the frequency of a QAM with a valid CVT table for that DHCT. The [000] indicates the QAM frequency.</p>
6	The light blinks twice, pauses, then repeats.		<p>The LED displays r.xxx, where [xxx] indicates the number of packets remaining to be downloaded. This number counts down to zero as the packets are downloaded.</p>
7	The light blinks 3 times, pauses, then repeats.		<p>CLr and PR.00 indicate that the second part of the OS is installed into flash memory.</p> <p>Programs upper memory area with ResApp.</p>
8	The light is off.		<p>The wave appears after the DHCT resets to boot into the OS and the newly downloaded ResApp.</p>

Appendix A
Download LED Indicators

Stage	POWER LED Indicator	TV Monitor	Description
9	Solid on, then off. The light is off as the DHCT boots into the OS.	 <p>or</p> 	The rotating border appears when the DHCT resets and boots into the OS.
10	The light is off.		The DHCT reboots.
11	<p>For Service Disconnect (brick) mode, the light blinks eight times, pauses for half a second, and repeats.</p> <p>For normal operation, the light blinks four times, pauses, then repeats only once.</p>		The DHCT is in either Service Disconnect mode or standard mode.

POWER LED Indicators Displayed on DHCTs

Some DHCTs do not include front-panel alphanumeric LED indicators. These DHCTs rely on the flashing POWER LED indicators to give you information about their status.

Understanding the POWER LED Indicators

Blinks Once Every Half-Second

The POWER LED indicator blinks once every half-second. This is equivalent to the **h.nnn** message LED code that appears on the front panel of alphanumeric LED DHCTs.

An h.nnn condition indicates normal behavior for the DHCT. The condition occurs while the DHCT scans the entire frequency spectrum for the presence of a CVT. The DHCT is scanning the QAM frequency spectrum for all of your QAMs.

Blinks 2 Times, Pauses, Repeats

The POWER LED indicator blinks twice, pauses, then repeats. This is equivalent to the **r.xxx** LED code that appears on the front panel of alphanumeric LED DHCTs.

An r.xxx condition indicates that the DHCT may be downloading software. Do not reboot the DHCT. As a CVT download progresses, the hex number decreases sequentially to zero, showing the number of blocks remaining. Block size is configured on the headend.

The r.xxx message is normal behavior for the DHCT. Do not reboot the set-top unless the message appears constantly.

To clear the r.xxx message, complete the following steps.

- 1 Wait 5 to 20 minutes. The DHCT could be downloading software.
- 2 Did this clear the message?
 - If **yes**, you have corrected the problem.
 - If **no**, follow your company's escalation procedure.

Blinks On for Two Seconds, Off Momentarily, Repeats

The POWER LED indicator blinks on for two seconds, off for two seconds, and repeats. This is equivalent to the **BR.xx** message LED code that appears on the front panel of alphanumeric LED DHCTs.

A BR.xx (where xx is a hexadecimal number) message usually indicates that the DHCT has a software or hardware malfunction that prevented it from properly receiving an instruction to complete a function. This condition is also referred to as an OS trap.

Appendix A Download LED Indicators

For example, an exception may have caused the CPU to trap while the Bootloader's trap table was in effect.

To clear a BR.xx message, complete the following steps.

- 1 Turn off the DHCT and unplug it from the wall outlet or rear panel of the DHCT.
- 2 Plug the DHCT into the wall outlet or rear panel and turn it on.
- 3 Did this clear the error message?
 - If **yes**, you have corrected the problem.
 - If **no**, the DHCT may need to be replaced. Follow your company's replacement procedure.

Blinks 3 Times, Then Pauses

The POWER LED indicator blinks 3 times, pauses, then repeats. This is equivalent to the **PR.xx** LED code that appears on the front panel of alphanumeric LED DHCTs.

This message indicates that the DHCT is receiving new software. This is normal behavior. Do not reboot the DHCT or remove power.

The PR.xx condition can take 15 to 30 minutes to clear if the software download is interrupted.

Important: If you interrupt the DHCT in its download process, the DHCT could be damaged and will have to be replaced. If the DHCT does not update its software after 30 minutes, notify your supervisor or headend manager. The DHCT may have an RF issue or a download issue. Follow your company's escalation procedure.

Blinks 4 Times, Pauses, Repeats Only Once

The POWER LED indicator blinks 4 times, pauses, and repeats only once. This indicates that you have activated the Staging Toolkit.

This is normal behavior and is given so you know when the Staging Toolkit is ready for further instructions. Refer to *Staging Toolkit* (on page 165) for more information.

Blinks 5 Times Slowly, Pauses, Repeats

The POWER LED indicator blinks 5 times slowly, pauses then repeats. This indicates that the DHCT has no stranded IPPV events.

Important: This behavior only appears when you activate the Staging Toolkit and check for stranded IPPV events. Refer to *Staging Toolkit* (on page 165) for more information.

Blinks 5 Times Quickly, Pauses, Repeats

The POWER LED indicator blinks 5 times quickly, pauses, then repeats. This indicates that the DHCT has stranded IPPV events.

Important: This behavior only appears when you activate the Staging Toolkit and check for stranded IPPV events. Refer to *Staging Toolkit* (on page 165) for more information.

Blinks 8 Times, Then Pauses

The POWER LED indicator blinks eight times and then pauses for half a second. This is equivalent to the **four dashes** [- - - -] LED code that appears on the front panel of alphanumeric LED DHCTs.

This message indicates that the DHCT is not authorized for the brick mode avoidance package. In addition, the Service Disconnect Barker message appears on the screen of any TV connected to the DHCT.

If a DHCT has not received the brick mode avoidance package, the DHCT is considered in brick mode. The brick mode avoidance package lets cable service providers authorize services for the DHCT.

The possible causes for this condition are as follows:

- The cable service was disconnected.
- The DHCT needs to receive a hit from the billing system that authorizes services that a subscriber has requested.
- The DHCT is not authorized for the brick mode avoidance package.
- The DHCT timed out while receiving EMMs.

B

Button Sequence for DHCT Functions

Introduction

Our DHCTs have button sequences you can use to force behavior in certain situations. The table in this appendix details several of these button sequences in both the standard (alphanumeric LED-equipped) and POWER LED indicator only DHCTs.

In This Appendix

- Button Sequences 130
- E940 Forced Download Button 131

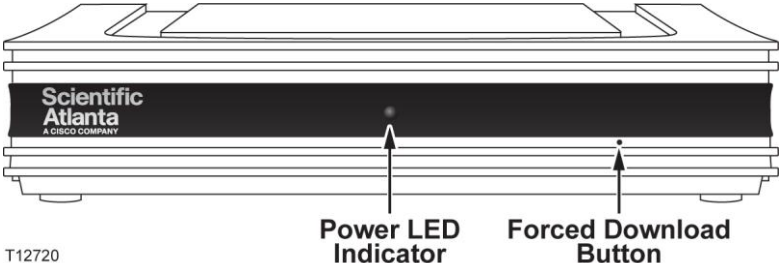
Button Sequences

The following table details the button sequences you can use on DHCTs to force certain behavior.

Function	Alphanumeric LED-Equipped DHCT	POWER LED Indicator Only DHCT	E940 DHCT
Temporarily stop the DHCT from 'hunting'	Press the POWER button during the hunt	Press the POWER button during the hunt	Press the Forced Download button during the hunt
Download software using the main serial port	Press the SELECT and GUIDE buttons at the same time until the download begins	Press and hold the CH+ button until the download begins	Press and hold the Forced Download button until the download begins
Download software using the optional serial port	Press the CH+ and CH- buttons at the same time until the download begins	Not available	Not available
Force a hunt when the DHCT boots	Press the POWER and SELECT buttons at the same time until the hunt begins	Press the CH+ and CH- buttons at the same time until the hunt begins	Press and hold the Forced Download button until the hunt begins
Reboot the DHCT while the OS is booting	Press the INFO , VOL+ , and VOL- buttons at the same time until the DHCT reboots	Press the POWER and CH+ buttons at the same time until the DHCT reboots	Press and hold the Forced Download button until the DHCT reboots

E940 Forced Download Button

The Forced Download button on E940-series DHCTs is located on the front panel of the DHCT.



T12720

C

Setting Up Multiple Bootloader Carousels

Introduction

This appendix examines why it might be beneficial for a site to use more than one bootloader and also gives examples of different ways to configure multiple bootloader carousels.

In This Appendix

- Overview 134
- Determine Available Bandwidth for Multiple Bootloaders..... 136
- Setting Up Multiple Bootloader Carousels 140
- Adding a Bootloader Source to the DNCS 142
- Setting Up DHCTs to Download Images from a Specific Bootloader Carousel 144

Overview

This section discusses the benefits of using multiple bootloader carousels and provides examples of ways you might configure multiple bootloader carousels.

With multiple bootloader carousels, the BFS can send set-top software version images using more than one carousel. This enhancement gives you the flexibility you need to reduce download times and maintain system performance by creating the optimal number of bootloader carousels for your system.

Note: You must have DNCS System Release 4.3 or later to use the multiple bootloader feature.

Why Use Multiple Bootloaders?

Using more than one carousel can help you use the Broadcast File System (BFS) more efficiently. The packet interleave algorithm used by the DNCS allows a 1 MB image (file) to download in the same amount of time as an 8 MB file. In each case, it takes one full revolution of the carousel.

One way to optimize the carousels is to arrange the files so that each carousel is approximately the same size. Another option is to put the images for the new types of devices being staged (M-Card modules and hosts, for example) on one carousel and put the images for all legacy types on another.

We recommend that you place the images of similar devices on their own bootloader (for example, standalone M-Card module images on one bootloader and SSC set-top images on another). That way, you can keep the image sizes and cycle times appropriate for each device type.

Important: When you use more than one carousel, you should make certain that the BFS QAM has enough bandwidth to support a second bootloader carousel. Go to *Determine Available Bandwidth for Multiple Bootloaders* (on page 136) for more information.

Ways to Configure Multiple Bootloader Carousels

Here are a few examples of how you might configure your bootloader carousels:

- Put CableCARD module images on a separate carousel from DHCT images. Because CableCARD module images are smaller, the carousel cycle time is lessened. As a result, the CableCARD modules receive their images quicker.
- Put larger images on one carousel and smaller images on the other carousel. The carousel that carries only the smaller images allows the receiving device (DHCT or CableCARD module) to get the smaller image in less time because it is not impacted by being interleaved with the larger content.
- If you need to send an image out to a device population quickly, you might create one carousel to carry this image.

Note: Faster downloads can sometimes be realized by increasing the data rate for the existing 199 bootloader carousel. Keep in mind that this strategy works only when using DHCTs (set-tops) that support download data rates greater than 10 Mbps.

Determine Available Bandwidth for Multiple Bootloaders

This section provides inband data carousel recommendations and procedures for determining how much bandwidth is currently available on the BFS QAM for bootloader sources.

Why Determine Available Bandwidth?

Determining the amount of unused (or available) bandwidth for inband sources ensures that your system has sufficient bandwidth for additional bootloader carousels. Bootloader carousels require a data rate between 1.00 and 3.00 Mbps.

Example: If your BFS QAM has 4 Mbps of available bandwidth and you want to add two bootloader carousels, each with a data rate of 3 Mbps, you cannot; there is only enough available bandwidth to support one of the carousels.

Note: For assistance selecting a suitable rate for additional bootloader carousels, refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377).

How Much Bandwidth Can My System Support?

Depending on your QAM modulation mode, the sum of your inband carousel rates plus any audio-visual content that is combined on the BFS QAM modulator should not exceed the following totals:

Modulation Type	Direct ASI Bandwidth	BFS BIG Bandwidth
64-QAM modulation	26 Mbps	25 Mbps
256-QAM modulation	37 Mbps	36 Mbps

Determine Available Bandwidth for Your System

To determine the available bandwidth for your system, go to one of the following topics:

- If your system uses ASI, go to *Determining Available Bandwidth for Direct ASI Systems* (on page 137).
- If your system uses a BFS BIG, go to *Determining Available Bandwidth for BFS BIG Systems* (on page 138).

Determining Available Bandwidth for Direct ASI Systems

This section provides procedures for operators with direct ASI to use in determining how much bandwidth is available for inband sources. To determine the amount of bandwidth available for additional bootloader carousels, perform the following calculation:

$$\text{Total Available Bandwidth} - \text{Bandwidth in Use} = \text{Available Bandwidth}$$

Notes:

- The inband data rate for a 64-QAM is 26 Mbps.
- The inband data rate for a 256-QAM is 37 Mbps.

These rates are due to modulation coding and error corrections (real rates are higher).

- 1 Open an xterm window on the DNCS.
- 2 Type one of the following, based on the system release you have installed:
 - For SR 4.2.1 and earlier, type **cd /export/home/dncs/doctor** and press **Enter**.
 - For SR 4.3 and later, type **cd /dvs/dncs/Utilities/doctor** and press **Enter**.

Note: Be sure to type a space between **cd** and **/**.

Result: The current directory is now the doctor directory.

- 3 Type **doctor -bv** and press **Enter**. A table appears that lists the inband and out-of-band data rates on the BFS carousel. The total inband carousel bandwidth in use is displayed in the **Aggregate IB Carousel Datarate** field.
- 4 Subtract the total inband carousel bandwidth in use from the total available bandwidth to determine the unused inband bandwidth on the BFS.

Examples:

- **64-QAM:** If your total inband carousel bandwidth in use is 14 Mbps, the available bandwidth is 12 Mbps.

$$26 - 14 = 12 \text{ Mbps}$$
- **256-QAM:** If your total inband carousel bandwidth in use is 14 Mbps, the available bandwidth is 23 Mbps.

$$37 - 14 = 23 \text{ Mbps}$$

- 5 Compare the amount of unused bandwidth to the amount of bandwidth required for the additional bootloader carousels.
- 6 Is there enough bandwidth to add the new bootloader carousels? (Bootloader carousels require data rates between 1.00 and 3.00 Mbps.)
 - If **yes**, go to *Adding a Bootloader Source to the DNCS* (on page 142).
 - If **no**, refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377) for details on how to increase the bandwidth of your system.

Determining Available Bandwidth for BFS BIG Systems

This section provides procedures for operators with a BFS BIG to use in determining how much bandwidth is available for inband sources. To determine the amount of bandwidth available for additional bootloader carousels, perform the following calculation:

$$\text{Total Available Bandwidth} - \text{Bandwidth in Use} = \text{Available Bandwidth}$$

Notes:

- The inband data rate for a 64-QAM is 25 Mbps.
 - The inband data rate for a 256-QAM is 36 Mbps.
- 1 Open an xterm window on the DNCS.
 - 2 Type one of the following, based on the system release you have installed:
 - For SR 4.2.1 and earlier, type **cd /export/home/dncs/doctor** and press **Enter**.
 - For SR 4.3 and later, type **cd /dvs/dncs/Utilities/doctor** and press **Enter**.

Note: Be sure to type a space between **cd** and **/**.

Result: The current directory is now the doctor directory.

- 3 Type **doctor -bv** and press **Enter**. A table appears and lists the inband and out-of-band data rates on the BFS carousel. The total inband carousel bandwidth in use is displayed in the **Aggregate IB Carousel Datarate** field.
- 4 Add **1 Mbps** to the data rate in the **Aggregate IB Carousel Datarate** field to account for any overhead.

Example: If you have a total inband data rate of 14 Mbps, add 1 Mbps for a total of 15 Mbps in use.

$$14 + 1 = 15$$

- 5 Subtract the total inband carousel bandwidth in use from the total available bandwidth to determine the unused inband bandwidth on the BFS.

Examples:

- **64-QAM:** From the examples above, the available bandwidth is 10 Mbps.
$$25 - 15 = 10 \text{ Mbps}$$
- **256-QAM:** From the examples above, the available bandwidth is 21 Mbps.
$$36 - 15 = 21 \text{ Mbps}$$

- 6 Compare the amount of unused bandwidth to the amount of bandwidth required for the additional bootloader carousels.

- 7 Is there enough bandwidth to add the new bootloader carousels? (Bootloader carousels require data rates between 1.00 and 3.00 Mbps.)
 - If **yes**, go to *Verify a VCI for Inband BFS Sources on BFS BIG Systems* (on page 139).
 - If **no**, refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377) for details on how to increase the bandwidth of your system.

Verify a VCI for Inband BFS Sources on BFS BIG Systems

This section describes how to check the number of BFS sessions on your system to determine whether any unused VCIs are present for the inband BFS carousel.

Notes:

- Your network was initially installed and reserved with 20 Virtual Channel Indicator (VCI) connections (values 256-275) on the ATM switch. The VCIs carry inband BFS information from the DNCS to the BIG. Because you will create a new inband source, you must make sure that one VCI is available for each additional bootloader carousel that you add to the DNCS.
- If you need detailed instructions for this procedure, refer to the manual that came with your ATM switch.

Complete the following steps to determine whether there are enough unused VCIs available for the additional inband BFS carousels.

- 1 Using the manual that came with your ATM switch, check the ATM switch to determine the number of unused VCIs.
- 2 Are there enough VCIs for the new bootloader carousels?
 - If **yes**, go to *Adding a Bootloader Source to the DNCS* (on page 142).
 - If **no**, add more VCIs to the switch. Then, go to *Adding a Bootloader Source to the DNCS* (on page 142).

Note: Having unused VCIs does not present any issues to your system; therefore, we recommend that you create 5 to 10 extra VCIs.

Setting Up Multiple Bootloader Carousels

This section provides an overview of the steps required to set up more than one bootloader carousel and configure DHCTs to use the correct carousel when downloading images.

Note: You must have DNCS System Release 4.3 or later to use the multiple bootloader feature.

- 1 Verify that the BFS QAM has enough bandwidth to support a second bootloader carousel. To make this determination, go to *Determine Available Bandwidth for Multiple Bootloaders* (on page 140).

- 2 Add the new bootloader carousel to the DHCT by adding a bootloader source with the following characteristics to the BFS Administration window.

Note: For assistance adding a bootloader source to the BFS Administration window, go to *Adding a Bootloader Source to the DNCS* (on page 142).

- **Source Name** - Enter a name to describe this source; for example, **Bootloader2**.
- **Source ID** - Ideally, we recommend that you select an even number that is not in use and that is greater than 200 to correspond with our numbering convention.
- **Source Type** - Select **Bootloader**.
- **Transport Type** - Select **ASI In-band**.
- **Data Rate** - The rate depends on several factors, including the DHCT type, the BFS QAM setting, and the available bandwidth. When you make this decision, select a rate between 1.00 and 3.00 Mbps. For assistance, refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377).

Important: When you stage SCC DHCTs, use a data rate of 3.00 Mbps.

- **Block size** - Enter **4000**.
- **Indication Interval** - Enter **100**.
- **DataPump** - Set to **run**.

Note: If your system uses the RCS feature, skip this field.

- **Selected Hosts** - Select the same hosts as the main Bootloader source.

- 3 Configure set-tops to use the correct bootloader carousel when downloading images. For assistance, go to *Setting Up DHCTs to Download Images from a Specific Bootloader Carousel* (on page 148).

Important: When you set up multiple bootloader carousels, send each DHCT image using only one bootloader source. Attempting to send the same DHCT image to two different bootloader sources at the same time will cause the system to display a **Save Failed** error message when saving the image to the second bootloader source.

Adding a Bootloader Source to the DNCS

This section provides instructions for adding a bootloader source to the DNCS. The DNCS uses a default bootloader source (source ID 199); however, you can add bootloader sources to the DNCS. With multiple bootloader carousels, the BFS can send set-top software version images using more than one carousel. This enhancement gives operators the flexibility needed to reduce download times and maintain system performance by creating the optimal number of bootloader carousels for their system.

Important: If you are using our RCS solution, select **All Sites** to add this source to all existing sites as well as all future sites.

Before you begin, determine the data rate for each bootloader carousel. The rate is dependent on several factors, such as the BFS QAM setting and the available bandwidth. When making this decision, select a rate between 1.00 and 3.00 Mbps. For assistance, refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377).

You also need to assign the new bootloader to the same hosts as the original bootloader. Refer to the configuration of the original bootloader and record which hosts it uses.

- 1 On the DNCS Administrative Console, click the **Application Interface Modules** tab.
- 2 Click **BFS Admin**. Depending on your system configuration, the following window opens:
 - If you are using a typical DBDS with no RCS, the BFS Administration window opens. If this window opens, go to step 4.
 - If you are using an RCS, the Please select a site window opens. If this window opens, go to step 3.
- 3 Select **File > All Sites**.
- 4 Click the **Sources** tab.
- 5 Click **File > New**. The Set Up BFS Source window opens.
- 6 Complete the following fields as indicated here:
 - **Source Name** - Enter a name to describe this source; for example, **Bootloader2**.
 - **Source ID** - Ideally, we recommend that you select an even number that is not in use and that is greater than 200 to correspond with our numbering convention.
 - **Source Type** - Select **Bootloader**.
 - **Transport Type** - Select **ASI In-band**.

- **Data Rate** - The rate depends on several factors, including the DHCT type, the BFS QAM setting, and the available bandwidth. When you make this decision, select a rate between 1.00 and 3.00 Mbps. For assistance, refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377).

Important: When you stage SCC DHCTs, use a data rate of 3.00 Mbps.

- **Block size** - Enter **4000**.
- **Indication Interval** - Enter **100**.
- **DataPump** - Set to **run**.

Note: If your system uses the RCS feature, skip this field.

Selected Hosts - Select the same hosts as the main Bootloader source.

- 7 Click **Save**. The system saves the carousel in the DNCS database and closes the Set Up BFS Source window.
- 8 Click the **Servers** tab, and double-click the bootloader server. The Authorize BFS Server window opens for the bootloader server.
- 9 In the **Available Sources** field, select the bootloader source that you just created and then click **Add**. The host you selected moves to the Selected Sources list.
Important: Move only the server that you just created to the Selected Sources list.
- 10 Click **Save**. The system saves this change and closes the Authorize BFS Server window.
- 11 Do you need to add another bootloader source the DNCS?
 - If **yes**, repeat this procedure from step 5.
 - If **no**, you are ready to configure DHCTs to use the correct bootloader carousel when downloading images. Go to *Setting Up DHCTs to Download Images from a Specific Bootloader Carousel* (on page 144).

Setting Up DHCTs to Download Images from a Specific Bootloader Carousel

After you have added a bootloader source to the DNCS, set up DHCTs to download images from a specific bootloader carousel.

Important: When you set up multiple bootloader carousels, send each DHCT image using only one bootloader source. Attempting to send the same DHCT image to two different bootloader sources at the same time will cause the system to display a **Save Failed** error message when saving the image to the second bootloader source.

- 1 On the DNCS Administrative Console, click the **DNCS** tab.
- 2 Click the **Home Element Provisioning** tab.
- 3 Click **Image**. The Image List window opens.
- 4 Click the **DHCT Downloads** tab.
- 5 Click **File > New**. The Set Up DHCT Download window opens.
- 6 Click the **DHCT Type** arrow and select a device that needs to receive the new software.
- 7 Click the **Group** arrow and select the group to which you want to download the image.
- 8 Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.
- 9 Click the **Downloading Schedule** arrow and select the type of download appropriate to your business needs.

Notes:

- A **Normal** download does not begin until the DHCT is turned off.
 - An **Immediate** download occurs in a relatively short period of time, but interrupts watching TV, PPV, VOD, and other services.
 - An **Emergency** download begins instantaneously and no barker opens to the subscriber.
- 10 Click the **Carousel** arrow and select the bootloader carousel that these devices should use to download DHCT images.

Important: When you set up multiple bootloader carousels, send each DHCT image using only one bootloader source. Attempting to send the same DHCT image to two different bootloader sources at the same time will cause the system to display a **Save Failed** error message when saving the image to the second bootloader source.

- 11 Click **Save**. The Association Verification window opens.

Setting Up DHCTs to Download Images from a Specific Bootloader Carousel

- 12 Verify that the information shown is correct, and configure the following fields on the Association Verification window:
 - **Are you SURE you want to do this?** - Type **yes**.
 - **Enter your name** - Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
 - **Password** - Type the password you received from Cisco Services.
- 13 Click **OK**. The association Verification window closes and the Image List window is updated with the newly defined test download schedule. The emergency download begins instantaneously and no barker opens to the subscriber.

D

Adding an HDD Test Server to the BFS

Introduction

This appendix includes the tasks required to set up the BFS to support the HDD test.

Important Note for Multiple-Site (RCS-Enabled) Systems: Manually setting up any BFS server or source must be done for the "AllSites" site only and not for any other individual sites in your system. Otherwise, the server and source will fail.

For more information on the HDD test, refer to the *DVR Configuration Guide* (part number 4011411).

In This Appendix

■ Overview	148
■ Adding an HDD Test Server to the BFS	150
■ Registering the HDD Test Server with the BFS	154
■ Placing the HDD Performance Specification File on the HDD Test Server.....	156

Overview

The following steps summarize the tasks required to set up the BFS to support the HDD test. Experienced users may prefer to follow this summary.

Users who require step-by-step instructions should go to *Adding an HDD Test Server to the BFS* (on page 150).

Important Note for Multiple-Site (RCS-Enabled) Systems: Manually setting up any BFS server or source must be done for the "AllSites" site only and not for any other individual sites in your system. Otherwise, the server and source will fail.

- 1 Add a server with the following characteristics to the **Servers** tab of the **BFS Administration** window.

- Server Name: **hddtest**

Important: This field requires a specific entry. You must enter **hddtest** in lowercase letters in this field. Otherwise, set-tops will not receive the testparam.cfg file.

- Selected Sources: **Out of Band**

Important: Multi-site (RCS-enabled) systems must add the server to only the Site AllSites Administration window. Adding a server to the BFS Administration window of individual sites and to the Site AllSites Administration window causes the server to fail.

Note: To define these characteristics, display the Authorize BFS Server window by following the quick path for your system configuration:

- **Single-site systems:** DNCS Administrative Console > Application Interface Modules tab > BFS Admin > Servers tab > File > New
- **Multi-site systems:** DNCS Administrative Console > Application Interface Modules tab > BFS Admin > File > All Sites > Servers tab > File > New

- 2 Register the server with the BFS Client by adding a server with the following characteristics to the **Broadcast File Server List** window.

- Server Name: **hddtest**
- Mode: **2-way**
- Selected Sources: **Out of Band**

Important: Multi-site (RCS-enabled) systems must add the server to only the All Sites Broadcast File Server List window. Adding a server to the Broadcast File Server window of other individual sites and to the All Sites Broadcast File Server List window prevents the system from setting up a server.

Note: To define these characteristics, display the Set Up Server window by following the quick path for your system configuration:

- **Single-site systems:** DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > New Server
- **Multi-site systems:** DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > All Sites > File > New Server

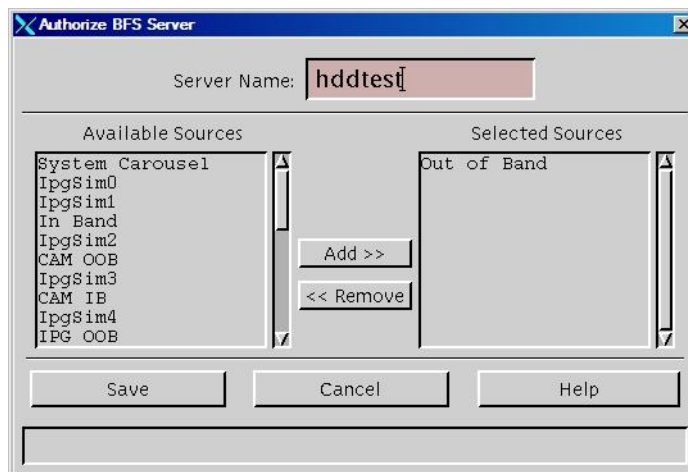
- 3 Add the **testparam.cfg** file to the hddtest server in the BFS Client window.

Adding an HDD Test Server to the BFS

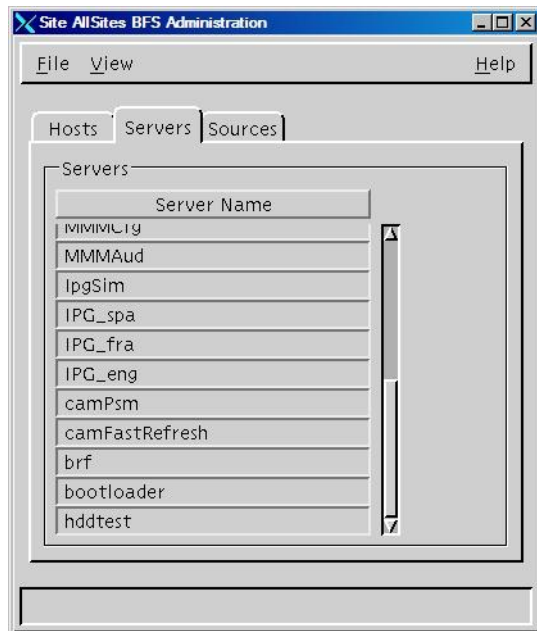
Note: This procedure can be used for systems that support multiple sites (RCS-enabled) or single sites.

- 1 On the DNCS Administrative Console, select the **Application Interface Modules** tab.
- 2 Click **BFS Admin**. Choose one of the following options:
 - **For single-site systems**, the Site DNCS BFS Administration window opens. Click **File > All Sites**.
 - **For multiple-site (RCS-enabled) systems**, the Please Select a Site window opens.
- 3 Select the **Servers** tab.
- 4 Click **File > New**. The Authorize BFS Server window opens.
- 5 Enter the following data into the fields of the Authorize BFS Server window:
 - In the Server Name field, enter **hddtest**.
 - From the Available Sources list, select **Out of Band**.
 - Click **Add**.

Result: The Authorize BFS Server window is configured as shown in the following example.



- 6 Click **Save** to save your changes and close the Authorize BFS Server window. The HDD Test server has been added to the BFS. As a result, the hddtest server shows in the Server Name list, similar to the following example.



- 7 Click **File > Close** to close the window.
- 8 Verify that you set up the HDD test server correctly. Go to *Verify that the HDD Test Server is Successfully Set Up* (on page 156).

Verify That the HDD Test Server Is Successfully Set Up

This section provides instructions for using a local DVR with an HDD that is known to be in good working order to verify that the HDD Test server has been set up successfully. During this process, you are instructed to load the HDD test on a local DVR and then run the HDD test on the DVR. A successful result indicates that the HDD Test server has been set up correctly.

Before You Begin

Before you begin, make certain that the DVR you intend to use meets the following specifications:

- For Explorer 8000, 8010, or 8300 DVRs – DVR 1.5.2-1404 or later is installed on the DVR.
- For Explorer 8300HDC DVRs – DVR 1.5.3 or later is installed on the DVR.
- The DVR is connected to your DBDS network.
- The HDD is known to be in good operating order.


Quick Steps for Experienced Users

The following steps summarize the tasks required to verify that the HDD Test server has been set up successfully. Experienced users may prefer to follow this summary.

Users who require step-by-step instructions should go to *Verifying the Success of the HDD Test Server* (on page 153).

- 1 Reboot a DVR in your headend that meets the following specifications:
 - For Explorer 8000, 8010, or 8300 DVRs – DVR 1.5.2-1404 or later is installed on the DVR.
 - For Explorer 8300HDC DVRs – DVR 1.5.3 or later is installed on the DVR.
 - The DVR is connected to your DBDS network.
 - The HDD is known to be in good operating order.






Result: When the DVR reboots, the SARA client reads the testparam.cfg file, finds the appropriate entry for the DVR type, obtains the HDD performance specifications for the DVR type, and stores this data in nonvolatile memory (NVM).


- 2 Activate the Staging Toolkit, and then press the  key three times to start the HDD test utility. When the HDD test is complete, **PASS** appears in the DVR display to indicate that the HDD meets performance specifications. If PASS does not appear and you are confident that the HDD is in good operating order, contact Cisco Services for assistance troubleshooting the HDD Test server.

Verifying the Success of the HDD Test Server

- 1 Select a DVR in your headend that meets the following specifications:
 - For Explorer 8000, 8010, or 8300 DVRs – DVR 1.5.2-1404 or later is installed on the DVR.
 - For Explorer 8300HDC DVRs – DVR 1.5.3 or later is installed on the DVR.
 - The DVR is connected to your DBDS network.
 - The HDD is known to be in good operating order.
- 2 Reboot the DVR that you selected in step 1. When the DVR reboots, the SARA client does the following:
 - Reads the testparam.cfg file.
 - Finds the appropriate entry for the DVR type.
 - Obtains the HDD performance specifications for the DVR type.
 - Stores this data in nonvolatile memory (NVM).

Note: After the HDD test has been downloaded to the DVR, the HDD test utility can be run without a DBDS network connection.

- 3 Place the remote in Cable mode by pressing the  key on the remote control. The CBL key blinks red when pressing it to indicate that it is in Cable mode.
 - 4 Press and hold the **Pause** key on the remote control until the message indicator () on the DVR blinks.
 - 5 While the message indicator blinks, quickly press the  key to activate the Staging Toolkit.
- Note:** To activate the Staging Toolkit, you must press the  key while the message indicator is blinking. The message indicator blinks for about 13 seconds.
- 6 When the DVR display changes from displaying the time to displaying the EMM count (for example, E-00) the Staging Toolkit is active.
 - 7 Press the **Last**  key three times to start the HDD test utility. The DVR display alternately flashes **hdd** and **diAg** while the HDD test utility runs. The test takes only a few minutes to complete.
 - 8 Does **PASS** appear on the DVR display?

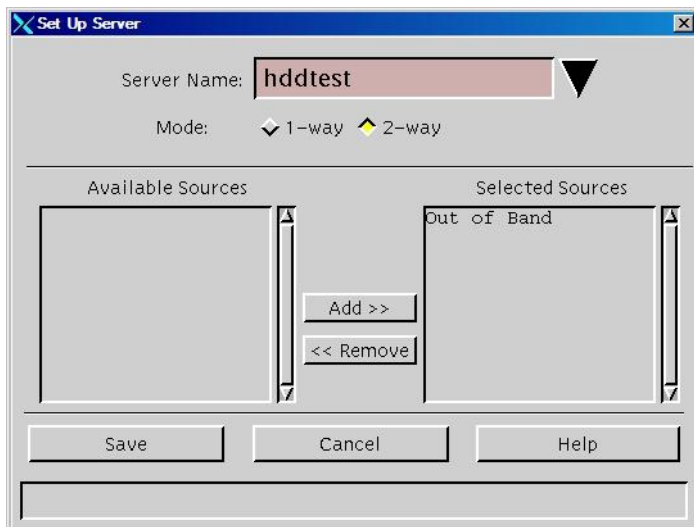
- If **yes**, you have verified the success of the HDD Tests server. Press the  key to exit the HDD test utility. As the utility exits, the front panel LED shows four dashes (----) and the set-top reboots.
- If **no**, the HDD test utility is not functioning as expected. Contact Cisco Services for assistance troubleshooting the HDD test utility.

Registering the HDD Test Server with the BFS

Note: This procedure can be used for systems that support multiple or single sites.

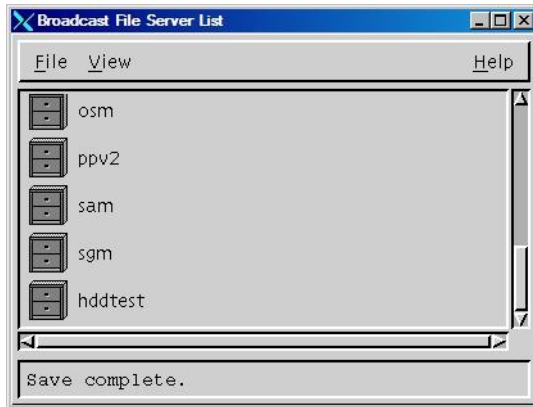
- 1 On the DNCS Administrative Console, select the **Application Interface Modules** tab.
- 2 Click **BFS Client**. Choose one of the following options:
 - For **single-site systems**, the Broadcast File Server List window opens. Click **File > All Sites**.
 - For **multiple-site (RCS-enabled) systems**, the Please Select a Site window opens.
- 3 Click **File > New Server**. The Set Up Server window opens.
- 4 Enter the following data into the fields of the Set Up Server window:
 - Click the Server Name arrow and select **hddtest**.
 - Click the **2-way** Mode option.
 - From the Available Sources list, select **Out of Band**.
 - Click **Add**.

Result: The Set Up Server window is configured as shown in the following example.



Registering the HDD Test Server with the BFS

- 5 Click **Save** to save your changes and close the Set Up Server window. The hddtest server has been registered with the BFS. As a result, the hddtest appears in the Broadcast File Server List, similar to the following example.



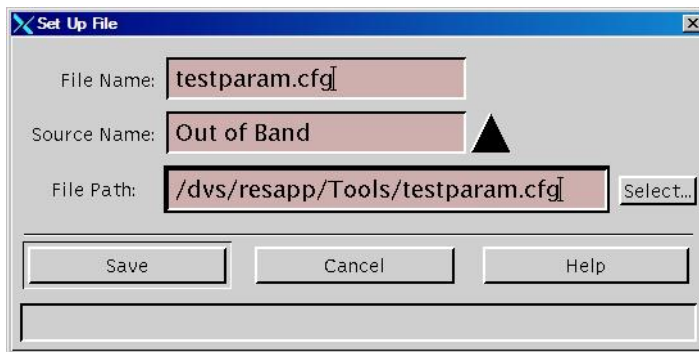
- 6 Finish setting up the BFS to support the HDD Test by placing the HDD Performance Specification file on the HDD Test server. Go to *Placing the HDD Performance Specification File on the HDD Test Server* (on page 156).

Placing the HDD Performance Specification File on the HDD Test Server

Note: This procedure can be used for systems that support multiple or single sites.

- 1 In the Broadcast File Server List window, double-click the **hddtest** server. The hddtest server opens to show its contents.
- 2 Click **File > New File**. The Set Up File window opens.
- 3 Follow these instructions to enter data into the fields of the Set Up File window:
 - Click in the File Name field and type **testparam.cfg**.
 - Click the Source Name arrow and select **Out of Band**.
 - Click in the File Path field and type **/dvs/resapp/Tools/testparam.cfg**.

Result: The Set Up File window is configured as shown in the following example.



- 4 Click **Save** to save your changes and close the Set Up File window. The HDD Performance Specification file is placed on the HDD Test server. As a result, the testparam.cfg file appears beneath the open hddtest server.
- 5 Click **File > Close** to close the Broadcast File Serve List window. You have successfully set up the BFS to support the HDD Test.

E

Format the Hard Drive Without Clearing NVM

Introduction

This appendix provides instructions on formatting the hard drive of a DVR-equipped DHCT without clearing the non-volatile memory (NVM) of the DHCT.

In This Appendix

- Formatting the Hard Drive..... 158

Formatting the Hard Drive

Complete the following instructions to format the hard drive of RMA or field-returned DVRs. Use the DVR/PIP remote control to format the hard drive.

Notes:

- Your remote control must be set to **Cable** mode to complete these instructions.
- Only complete these instructions to manually format DVRs that have stored information such as favorite channels or parental control PINs that you want to keep on the server.

To format the hard drive, complete these steps.

- 1 Make sure that the DVR is plugged into an AC power source.
- 2 Press **Pause** on the remote control until the message indicator (mail light) flashes.
- 3 Press **Page -**.
- 4 Press **List** three times.

Results:

- The DVR automatically reboots.
- The hard drive in the DVR is formatted and all previous recordings are erased.
- The subscriber settings (such as favorite channels and parental control PINs) are retained on the hard drive.

F

Staging Out-Of-Band Bridges

Introduction

This appendix contains information about setting up out-of-band (OOB) bridges for staging DHCTs.

In This Appendix

- Overview 160
- Set Up Staging Bridges 162

Overview

The traditional staging method for DHCTs involves the DNCS sending EMMs to every bridge on the DNCS network when operators stage DHCTs with the reverse plant disabled.

Note: Staging Out-Of-Band Bridges functionality is available beginning with the following System Releases:

- SR 2.7/3.7/4.2
- CV 3.4

What Are Staging Bridges?

Staging bridges are a subset out-of-band (OOB) bridge population of the DBDS that DNCS operators assign the task of DHCT staging. This subset (which can consist of QPSKs, CMTSs, or both) receives all staging message traffic instead of having every QPSK/CMTS in the network receive staging message traffic.

Using staging bridges eliminates the staging communication from being broadcast throughout the entire network (to every QPSK / CMTS hub). Staging bridges reduce the processing load on the DNCS and reduces the amount of network message traffic when you perform staging.

How Do Staging Bridges Work?

The billing system sends staging information to DHCTs through the DNCS using BOSS transactions. These BOSS transactions are also sent for service upgrades, service downgrades, and periodic DHCT refreshes. Previous to SR 2.7/3.7/4.2 and CV3.4, there was no reliable way to distinguish a modify DHCT transaction for a staging hit from a modify DHCT transaction for any other purpose.

Beginning with SR 2.7/3.7/4.2 and CV3.4, we added a flag to the `hct_profile` table which the Conditional Access System (CAM) of the DNCS uses to identify DHCTs that have not been previously staged (identifying DHCTs with no EMMs). When the DHCT receives a modify DHCT transaction, the CAM checks the staging flag of the DHCT.

If the flag is set, the CAM performs the following:

- Assumes that the transaction is not a staging transaction
- If the DHCT is in service one-way, has the DNCS send the EMMs to the entire DHCT population (as in previous SR releases)

If the flag is not set, the CAM performs the following:

- Assumes that the transaction is a staging transaction
- If the DHCT is in service one-way, has the DNCS send the EMMs to only those QPSKs or CMTSs designated as staging bridges
- After a successful completion of the EMM transfer, updates the flag in the DHCT `hct_profile` table to indicate the DHCT has received staging information

Set Up Staging Bridges

You can either set up a QPSK or CMTS as a new staging bridge. You can also designate an existing QPSK or CMTS as a staging bridge.

Setting Up New Staging Bridges

The procedures in this section describe how to add a new hub (QPSK or CMTS) as a staging bridge.

Setting Up a New QPSK Staging Bridge

Follow this procedure to set up a new QPSK staging bridge.

- 1 From the DNCS Administrative Console, click the **Network Element Provisioning** tab.
- 2 Click **QPSK/CMTS**. The QPSK/CMTS list panel displays.
- 3 Click **File > New > QPSK**. The Set Up QPSK Modulator screen displays.
- 4 Enter the information for the new QPSK modulator. Refer to the documentation you received with your QPSK modulator for more information.
- 5 In Options, select the **Staging Bridge** check box.
- 6 Click **Save**. The DNCS adds the QPSK modulator as a staging bridge.

Setting Up a New CMTS Staging Bridge

Follow this procedure to set up a new CMTS staging bridge.

- 1 From the DNCS Administrative Console, click the **Network Element Provisioning** tab.
- 2 Click **QPSK/CMTS**. The QPSK/CMTS list panel displays.
- 3 Click **File** then select **New** then select **CMTS**. The Set Up CMTS screen displays.
- 4 Enter the information for the new CMTS. Refer to the documentation you received with your CMTS for more information.
- 5 In Options, select the **Staging Bridge** check box.
- 6 Click **Save**. The DNCS adds the CMTS as a staging bridge.

Designating an Existing Hub as a Staging Bridge

The procedures in this section describe how to designate an existing hub (QPSK or CMTS) as a staging bridge.

Designating an Existing QPSK as a Staging Bridge

Follow this procedure to designate an existing QPSK as a staging bridge.

- 1 From the DNCS Administrative Console, click the **Network Element Provisioning** tab.
- 2 Click **QPSK/CMTS**. The QPSK/CMTS list panel displays.
- 3 Locate the QPSK modulator you want to designate as a staging bridge in the QPSK/CMTS list.
- 4 Double-click the name of the QPSK modulator.
- 5 In Options, select the **Staging Bridge** check box.
- 6 Click **Save**. The DNCS will use this QPSK modulator as a staging bridge.

Designating an Existing CMTS as a Staging Bridge

Follow this procedure to designate an existing CMTS as a staging bridge.

- 1 From the DNCS Administrative Console, click the **Network Element Provisioning** tab.
- 2 Click **QPSK/CMTS**. The QPSK/CMTS list panel displays.
- 3 Locate the CMTS you want to designate as a staging bridge in the QPSK/CMTS list.
- 4 Double-click the name of the CMTS.
- 5 In Options, select the **Staging Bridge** check box.
- 6 Click **Save**. The DNCS will use this CMTS as a staging bridge.

G

Staging Toolkit

Introduction

This section contains procedures for viewing status information or resetting a DHCT using any of our remote controls.

In This Appendix

- Overview 166
- Remote Controls..... 167
- Activating the Staging Toolkit for DHCTs with Alphanumeric LEDs..... 168
- Activating the Staging Toolkit for DHCTs with Single or Triple LEDs..... 169

Overview

The Staging Toolkit is a set of tools that is built into every Explorer DHCT. These tools let you observe the staging process, view DHCT status indicators, reset non-volatile memory (NVM), and reset DHCTs.

Note: The Staging Toolkit must be enabled in the DNCS before you can use it.

Remote Controls

We offer several different remote control models:

- **Three-function** remote controls let you control a TV, a VCR, and a DHCT. These remote controls include the following models:
 - Model ER1 Remote Control
 - AllTouch® AT2300 Remote Control
- **Four-function** remote controls let you control all of the same devices as the 3-function remote controls, plus a fourth device (such as a stereo receiver or amplifier). These remote controls include the following models:
 - AllTouch 2000 Remote Control
 - AllTouch AT2400 Remote Control
- **DVR/PIP** remote controls let you control four devices, including Digital Video Recorder (DVR) devices, and provide Picture-In-Picture (PIP) functions. These remote controls include the following model:
 - AllTouch 8400 Remote Control

Activating the Staging Toolkit for DHCTs with Alphanumeric LEDs

Note: These instructions are for DHCTs with full-display, alphanumeric LEDs. For instructions for DHCTs with single or triple LEDs, see *Activating the Staging Toolkit for DHCTs with Single or Triple LEDs* (on page 169).

Follow these steps to activate the Staging Toolkit.

- 1 Place the remote control into VOD mode by choosing one of the following options:
 - For 3-function remote controls, switch the **VCR/VOD** key on the remote control to the **VOD** position.
 - For 4-function and PVR/PIP remote controls, press the **CBL** key on the remote control.

- 2 Hold down the **Pause** key on the remote control for a few seconds until the message indicator on the DHCT flashes.

Note: The message indicator continues to flash for approximately 13 seconds after you release the **Pause** key. You must press the **PAGE -** or the **PREV -** key within this period to activate the Staging Toolkit.

- 3 Press one of the following keys to activate the staging toolkit:

- For 3-function and PVR/PIP remote controls, press the **Page -** key.
- For 4-function remote controls, press the **PREV -** key.

Result: The Staging Toolkit activates. The LED on the DHCT changes from displaying the time to displaying the EMM count, for example, E-00. The DHCT is not in diagnostic mode, and the programs still appear on the television monitor.

Note: The EMM count corresponds to the number of Internal Security Element (ISE) EMMs in the DHCT. This number resets to zero every time the DHCT goes through a hard reset (power cycle), which, for example, might occur after one of the following:

- The DHCT receives the Operating System (OS) and Resident Application (ResApp) software.
- The DHCT power cord is unplugged.
- You use a pin to press the hidden reset button of the DHCT.
- You use the Staging Toolkit to reboot the DHCT.

Activating the Staging Toolkit for DHCTs with Single or Triple LEDs

Note: These instructions are for DHCTs with single or triple LEDs. For instructions for DHCTs with full-display, alphanumeric LEDs, see *Activating the Staging Toolkit for DHCTs with Alphanumeric LEDs* (on page 168).

You can activate the staging toolkit using either the remote control or the front panel POWER button.

Activating the Staging Toolkit Using the Remote Control

- 1 On the remote control, press and hold the **PAUSE** button until the POWER LED blinks.
- 2 As the POWER LED blinks, press the **PAGE +** button. The staging toolkit activates and displays the DHCT diagnostic screens.
- 3 To page up and page down within the diagnostic screens, press **PAGE +/PAGE UP/NEXT +** or **PAGE -/PAGE DOWN/NEXT -**, based on the type of remote control you are using.
- 4 To exit the diagnostic screens, press the **EXIT** button on the remote control.

Activating the Staging Toolkit Using the POWER Button

- 1 Press and hold the **POWER** button until the POWER LED on the front panel blinks, then release the POWER button.
- 2 While the LED is blinking, press the **POWER** button a second time. The POWER LED should begin to blink quickly, and the diagnostic pages open.
- 3 To page up and page down within the diagnostic screens, press **PAGE +/PAGE UP/NEXT +** or **PAGE -/PAGE DOWN/NEXT -**, based on the type of remote control you are using.
- 4 To exit the diagnostic screens, press the **EXIT** button on the remote control.

Appendix G
Staging Toolkit

Index

---- (four dashes) • 96, 113, 116, 127

A

application platform release, installing • 19

B

bandwidth, available for multiple bootloader • 136

bootloader, adding multiple • 134

br.xx • 96, 125

button sequences • 130

C

CableCARD module

 CableCARDS, overview • 2, 78

 returning to service • 92

 setting up DNCS for staging • 23, 79

 staging • 78, 80, 82

clearing NVM • 88

clearing stranded PPV events • 90

Clr • 113

CVT download, recommended frequencies for • 47

D

DHCT • 2

 continuously reboots • 96

 DHCT

setting up for multiple bootloader • 144

errors when staging • 95

Forced Download button • 131

LED indicators • 112

no display • 96, 101

No Entitlement Agent • 104

no premium channels • 101

removing settings • 91

snowy video • 101

staging • 68

staging process flowchart • 69

tiling or freezing • 101

video macroblocking • 101

DhctInstantHit • 6

dIAG • 96

DNCS • 11

 install application platform release • 19

 verifying current configuration • 11

document version • vii

download methods • 4

DVR • 18

 format hard drive • 158

 package, create • 18

 requirements, troubleshooting • 94

E

E940 • 130, 131

EA issues • 104

EMMs • 5

 copy the EMM file • 58

 copy TOC file • 61

 create EMM file load log directory • 14

 extract EMM file • 60

 install, overview • 5

 insufficient number • 104

 load EMM data • 62

 no incoming • 104

 none listed • 104

 obtain EMM data • 54

 send file to DNCS • 59

environment variables

Index

- enabling • 13
- setting up • 12
- Er.00 • 96, 101
- Er.01 • 96, 101
- er.xx • 96

F

- Fast Refresh List • 6
- Flowcharts
 - DHCT staging • 69
- Forced Download button • 131
- format hard drive • 158
- forward path levels • 47, 49
- Fr.00 • 116
- Fr.LA • 116
- freezing video • 101
- frequencies, recommended for CVT download • 47
- ftp option for EMM data • 55

H

- h.nnn • 96, 116, 125
- hard drive, formatting • 158
- HDD test server, adding to BFS • 148

I

- instastaging
 - described • 7
 - instastaging
- DHCTs • 71
 - setting environment variables for • 13
- IPPV events • 89
 - checking for stranded • 89
 - clearing stranded events • 90

K

- knowledge needed • 3

L

- LED indicators
 - during CVT download • 116
 - during OSM download • 113
- load EMM data • 62

M

- mail option for EMM data • 56
- minimum network requirements • 46
- ModifyDhctConfiguration • 5
- multiple bootloader, adding • 134

O

- obtain EMM data • 54
- OS downloads • 101

P

- PowerKEY issues • 104
- Pr.xx • 113, 116, 126

Q

- QAM forward path levels • 47
- QPSK recommendations • 49

R

- r--- • 96
- r.xxx • 96, 116, 125
- reformat hard drive • 158
- related publications • vii
- ResApp download • 101
- reverse path levels • 49

S

- SARA blue screen • 101
- service disconnect
 - setting up • 17
 - troubleshooting • 127
- shipping option for EMM data • 56
- skills needed • 3
- staging
 - area considerations • 46
 - button sequences • 130
 - CableCARDS, overview • 2, 78
 - CVT, overview • 4
 - defaults, setting up • 18
 - DHCTs • 68, 70
 - DHCTs, overview • 2
 - failures • 94
 - instastaging • 71
 - instastaging, described • 7
 - LED indicators • 112
 - methods, described • 4
 - minimum network requirements • 46
 - monitoring • 112
 - OSM method, overview • 4
 - preparations • 10
 - process • 2
 - verifying • 75
- staging methods, described • 4
- staging toolkit • 166
- Sub Expire past date • 104

T

- tiling • 101
- TOC file • 61
- toolkit • 166
- troubleshooting
 - BR.xx • 125
 - Brick mode • 127
 - DHCTs • 95
 - EA issues • 104
 - four dashes • 127
 - general guidelines • 94
 - h.nnn • 125
 - OS downloads • 101
 - PowerKEY issues • 104
 - PR.xx • 126
 - r.xxx • 125
 - ResApp downloads • 101
 - snowy video • 101
 - tiling or freezing • 101
 - video macroblocking • 101

V

- ventilation • 51
- verifying staging process • 75
- video macroblocking • 101

W

- wave • 113, 116



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

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

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc. trademarks used in this document.

Product and service availability are subject to change without notice.

©2000, 2002, 2006, 2009, 2012 Cisco and/or its affiliates. All rights reserved.

June 2012 Printed in USA

Part Number 734375 Rev H