Separable Security Host Staging Guide for System Release 4.3 and Later

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 Acknowledgment

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**.

CableCARD and M-Card are trademarks of Cable Television Laboratories, Inc.

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

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Publication Disclaimer

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

Copyright

Contents

About This Guide

Introduction

This guide provides procedures for staging the following items in the Digital Broadband Delivery System (DBDS):

- Separable Security Host with CableCARD™ module (SSC) Digital Home Communications Terminals (DHCTs)
- CableCARD modules

Notes:

- DHCTs and CableCARD modules are sometimes referred to in this document as *devices*.
- This document only addresses staging for SSC DHCTs and stand-alone CableCARD modules using System Release (SR) 4.3 and later.
  - For information on staging SSC DHCTs and stand-alone CableCARD modules using SR 4.2.1 and earlier, refer to *Separable Security Host Staging Guide for System Release 4.2.1 and Earlier* (part number 736107) (see **Related Publications**, later in this section).
  - For information on staging non-CableCARD DHCTs, refer to the *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) (see **Related Publications**, later in this section).
- This document is mainly concerned with systems that use SARA; however, many of the procedures and troubleshooting tips are applicable to systems using Axiom. Those procedures specifically SARA-related are noted as such.

An SSC DHCT includes the functionality of the stand-alone DHCT, but adds the convenience of a factory-installed PowerKEY® Multi-Stream CableCARD module (or M-Card™). The M-Card module is mounted in the rear of the DHCT and is secured with a cover plate to deter tampering. A label provides the bar codes for the serial number and MAC address of the M-Card module is also provided on the rear panel of the DHCT.

Important: Before staging SSC DHCTs, you must make sure that you do not enable Digital Interactive Services (DIS) or any other options on the Secure Services tab in the Set Up DHCT screen. If you do enable these options, you will provision the DHCTs when you batch load the EMMs, which prevents combo binding from working correctly and might prevent the DHCTs from properly staging. See ***Batch Loading EMM Files and Disabling DIS*** (on page 11) for more information.

Scope

This document provides the procedures to properly stage SSC DHCTs with System Release (SR) 4.3 and later. If your system uses SR 4.2.1 or earlier, refer to the *Separable Security Host Staging Guide for System Release 4.2.1 and Earlier* (part number 736107).

This document is an addendum to the *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375).

Before you begin to stage DHCTs, follow the recommendations in the first five chapters of the *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) regarding the staging process, staging preparations, staging area considerations, obtaining and loading EMM data, and staging non-SSC DHCTs. Also, make sure to follow the recommendations in ***Optimize Your System Performance for Downloads and Staging*** (on page 41) to improve the speed and performance of the initial staging process.

Audience

This guide is written for staging area personnel responsible for staging SSC DHCTs and CableCARD modules, DHCT/CableCARD module installation personnel, and system operators of the Digital Network Control System (DNCS).

Document Version

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

Description	See Topic
Added new error codes for CDL as defined in OCAP host specification and in the host MIB	***CDL Error Codes*** (on page 157)
Added new CableCARD module validation status codes from the CableCARD module copy protection specification	***CableCARD Module Validation Status Codes*** (on page 163)
Added new host-CableCARD module interface errors as defined in the CCIF specification	***Host - CableCARD Module Interface Errors*** (on page 167)

1

Staging Preparation

Introduction

This chapter provides an overview of the information and processes you need before you begin to stage SSC DHCTs.

In This Chapter

Before You Begin

Overview

Before you begin to stage DHCTs, follow the recommendations in the first five chapters of the *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) regarding the staging process, staging preparations, staging area considerations, obtaining and loading EMM data, and staging non-SSC DHCTs. Also, make sure to follow the recommendations in ***Optimize Your System Performance for Downloads and Staging*** (on page 41) to improve the speed and performance of the initial staging process.

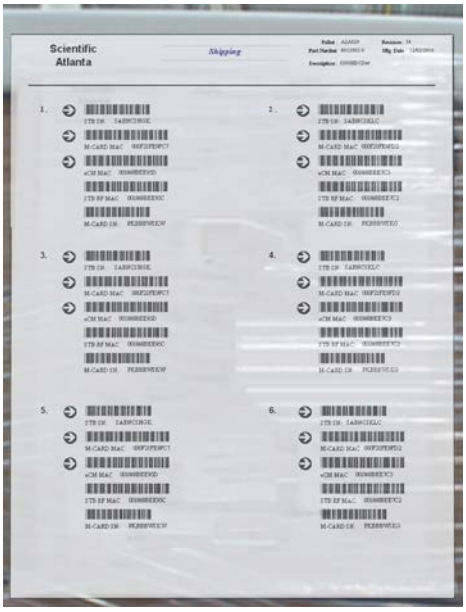
Important:

- If you are upgrading your DNCS at the same time as adding SSC DHCTs to your system, you must make sure that you upgrade your DNCS before you load the tar file for the SSC DHCTs. Refer to *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) for more information on tar files.
- Before staging SSC DHCTs, you must make sure that you do not enable Digital Interactive Services (DIS) or any other options on the Secure Services tab in the Set Up DHCT screen. If you do enable these options, you will provision the DHCTs when you batch load the EMMs, which prevents combo binding from working correctly and might prevent the DHCTs from properly staging. See ***Batch Loading EMM Files and Disabling DIS*** (on page 11) for more information.
- Service providers should make every effort to ensure that the SSC combination (of the DHCT and the CableCARD module or M-Card module) remains together. If this combination is separated, the convenience of having the combination is lost, and you must either implement manual processes to redeploy either unit or return the DHCT to us for repair.

Packaging Labels

SSC Pallet Inventory Bar Code Sheet

We ship SSC DHCTs on carton pallets. There are sheets containing the master pallet inventory bar codes affixed to the side of the pallets.



These inventory sheets contain the following information about the SSC DHCTs and their paired M-Card modules on the pallet:

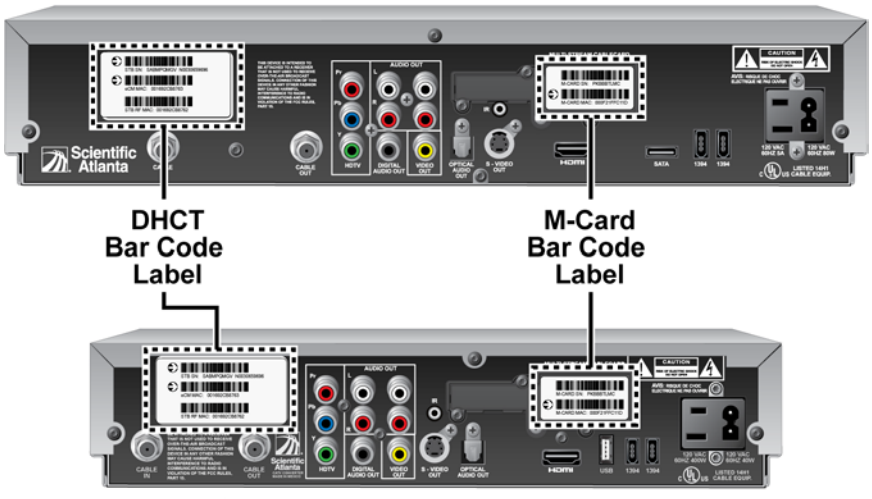
- DHCT serial number (STB SN)
- M-Card MAC address (M-CARD MAC)
- DHCT embedded cable modem MAC address (eCM MAC)
- DHCT RF MAC address (STB RF MAC)
- M-Card serial number (M-CARD SN)

Example: The arrows on the following bar code label point out the bar codes that are typically scanned for inventory and activation purposes.

DHCT Rear Panel Bar Code Labels

The SSC DHCT has two bar code labels located on the rear panel. The bar code labels contain information about the DHCT and its paired M-Card module.

Explorer® 8300HDC Label Locations



Explorer® 4250HDC Label Locations T13058

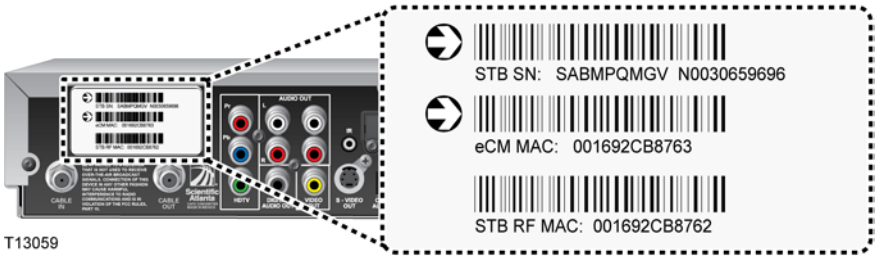
DHCT Bar Code Label

The DHCT label contains the following information for the DHCT:

- Serial number (STB SN)
- eCM MAC address (eCM MAC)
- RF MAC address (STB RF MAC)

These labels are valid for SSC DHCTs and stand-alone DHCTs (those without paired M-Card modules pre-installed).

Example: The arrows on the following bar code label point out the bar codes that are typically scanned for inventory and activation purposes.



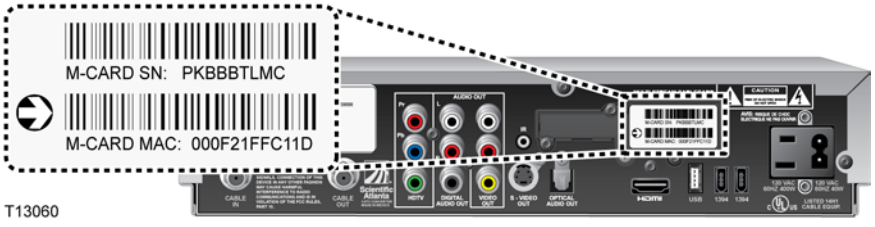
T13059

M-Card Bar Code Label on SSC DHCTs

The M-Card label contains the following information for the paired M-Card module:

- Serial number (M-CARD SN)
- MAC address (M-CARD MAC)

Example: During the staging process, scan the M-CARD MAC bar code into your billing system to activate a "hit," which allows the M-Card module to download the required EMMs.



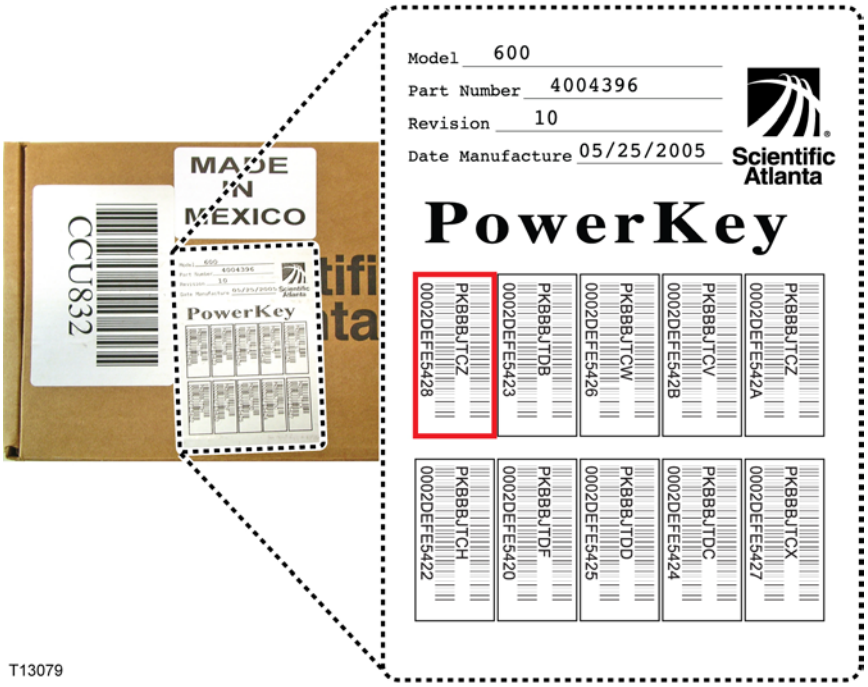
T13060

Shipping Carton Cutouts

The shipping cartons for the SSC DHCTs have the cardboard cut away from the rear panel area so that you can scan both the DHCT and M-Card bar code labels without removing the DHCT from the carton.

CableCARD Module Shipment Bar Codes

Shipping cartons containing CableCARD modules (M-Card modules) from us have a master label on the exterior containing two bar codes for each CableCARD module in the shipment. These bar codes correspond to the MAC address and serial number for the CableCARD modules in the shipment.

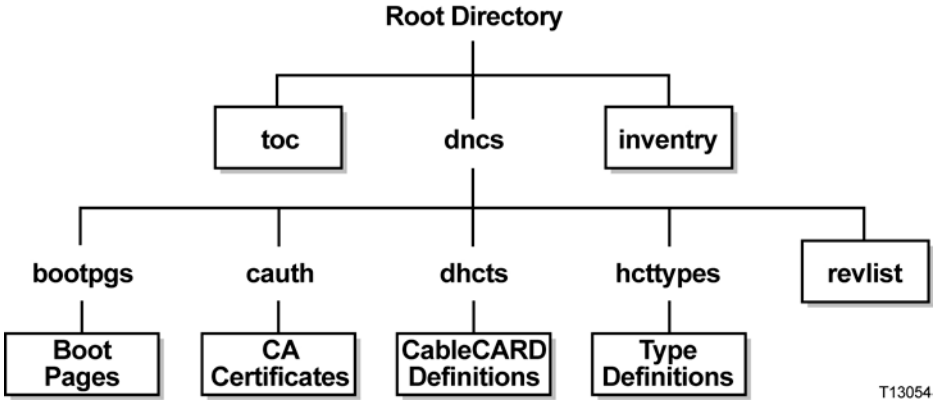


The bar codes are removable from the master list so that you can place them over the CableCARD slot on the DHCT after installing the CableCARD module to deter tampering.

Note: These bar codes are for staging non-SSC DHCTs and stand-alone CableCARD modules, not for SSC DHCTs.

Files Required for Staging

This section describes the files that are created and distributed with every shipment of PowerKEY CableCARD modules and SSC DHCTs. The files are distributed in directories as shown in the following illustration.



Note: The file names follow the MS-DOS "8 plus 3" naming convention.

The following descriptions refer to the files and directories relative to the root directory of the distribution tree. For example, */toc* refers to the file named toc in the root directory of the distribution tree.

The following two files and one directory reside beneath the root of the distribution file tree, and they are discussed in detail in this section:

- **toc:** Table of Contents file
- **inventry:** Inventory file
- **dncs:** DNCS directory

Notes:

- Refer to the *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) for more information on loading the EMMs.
- Refer to your billing system documentation for instructions and specific information for loading files into your billing system.

TOC File

Note: The TOC file does not include information on the paired SSC DHCTs. That information is contained in the inventory file.

When you load the EMMs into the DNCS for a shipment of SSC DHCTs or M-Card modules, a table of contents file (TOC file) is created and is available to your billing system. The **/toc** file contains the serial numbers, the MAC addresses, and the type (model and hardware revision) of all non-SSC DHCTs and CableCARD modules in the shipment.

The TOC file contains the following C structure:

```
struct dhct {
      char SerialNumber[10],       // ASCII
      char MacAddress[18],         // ASCII
      unsigned short Type_Type,
      unsigned short Type_Rev,
      char Type_Oui[3],            // this is binary data
      char fill2;                  // pad to 4-byte boundary
}
```

The serial number is formatted as **PKxxxxxxx**, where xxxxxxx represents a BASE-20 number starting at BBBBBBB. The MAC address takes the traditional UNIX syntax for a printed Ethernet address (**aa:bb:cc:dd:ee:ff**) where **a** through **f** are hexadecimal digits. All ASCII strings are NULL (0x0) terminated.

The Type_Type, Type_Rev, and Type_Oui fields communicate the type of device included in the shipment (SSC DHCTs excluded). These fields use the same values as those supplied in a BOSS DhctType descriptor. The OUI field is three binary bytes rather than a set of ASCII characters.

Inventory File

The inventory file (**/inventry**) describes the pairing of the M-Card modules and the DHCTs (also referred to as *hosts*) in an SSC configuration. The inventory file is produced for all shipments of M-Card modules, host DHCTs, or SSC combinations and is delivered in addition to the TOC file.

Notes:

- If your shipment of DHCTs also contains stand-alone DHCTs, the inventory file is still created; however, the **CaModule** fields contain the values for the stand-alone DHCTs rather than the values for the paired M-Card modules.
- The inventory file must be loaded into your billing system before you stage SSC DHCTs.

Inventory File Format

The inventory file (**/inventry**) contains the following C structure:

```
struct dhct {
      char HctSerialNumber[10],          //ASCII
      char HctHostMacAddress[18],        //ASCII
      char HctCmMacAddress[18],          //ASCII
      char HctHostId[14],                //ASCII
      unsigned short HctType_Type,
      unsigned short HctType_Rev,
      char HctType_Oui[3],               //this is binary data
      char CaModuleSerialNumber[10],     //ASCII
      char CaModuleMacAddress[18],       //ASCII
      char CaModuleId[14],               //ASCII
      unsigned short CaModuleType_Type,
      unsigned short CaModuleType_Rev,
      char CaModuleType_Oui[3]           //this is binary data
}
```

The serial number fields are formatted as **SAxxxxxxx** (for DHCTs) or **PKxxxxxxx** (for CableCARD modules), where xxxxxxx represents a BASE-20 number starting at BBBBBBB.

The MAC address fields are formatted using the traditional UNIX syntax for a printed Ethernet address (**aa:bb:cc:dd:ee:ff**) where **a** through **f** are hexadecimal digits. All ASCII strings are NULL (0x0) terminated.

The Type_Type, Type_Rev, and Type_Oui fields communicate the type of device included in the shipment (SSC DHCTs excluded). These fields use the same values as those supplied in a BOSS DhctType descriptor. The OUI field is three binary bytes rather than a set of ASCII characters.

dncs Directory

The **/dncs** directory contains the following directories that include information needed by the DNCS:

- **/dncs/cauth** contains the key certificates required for Key Certification Authorities that have certified DHCT public keys. This directory includes the certificates for all the Certification Authorities that created the certificates carried in the records in the **/dncs/dhcts** directory. It might also include certificates for other Certification Authorities.
- **/dncs/dhcts** contains records for the DHCTs and the CableCARD modules. Each file contains the records for one DHCT or one CableCARD module, and each record corresponds exactly with the DHCTs and the CableCARD modules represented in the **/toc** file.

  Note: The dhcts directory does not include information on the paired SSC DHCTs. That information is contained in the inventory file.
- **/dncs/hcttypes** contains the Type definitions for all DHCTs and CableCARD modules in the shipment. When the DNCS installs a batch of DHCTs or CableCARD modules, it first checks for the prior installation of the types listed in the **/dncs/hcttypes** directory. Then, the DNCS only installs the types listed in the directory that have not been previously installed. Each file in this directory contains the records for one DHCT or one CableCARD module, and each record corresponds exactly with the DHCTs and the CableCARD modules represented in the **/toc** file.
- **/dncs/bootpgs** contains bootterm pages.
- **/dncs/revlist** contains the certification revocation list.

Note: The DNCS uses the files in the **/dncs** directory to register devices in the network, which must be performed before these devices can be authorized to receive secure services. These files are typically not used by billing systems.

EMM Files

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.

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.

Obtaining EMM Files

There are three options for obtaining the EMM data from us:

- FTP download
- EMM CD received by mail or shipping service
- Customer Self-Service Serial Number Tracking Application

Refer to the *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) for more information on obtaining and loading EMM files.

Batch Loading EMM Files and Disabling DIS

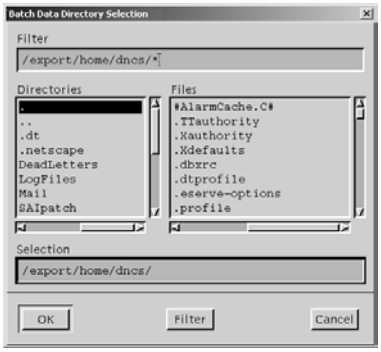
If you batch load EMM files, you must make sure that you do not enable Digital Interactive Services (DIS) or any other options on the Set Up DHCT screen, Secure Services tab. If you do enable these options, you will provision the DHCTs when you bulk load the EMMs, which prevents combo binding from working correctly.

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.

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

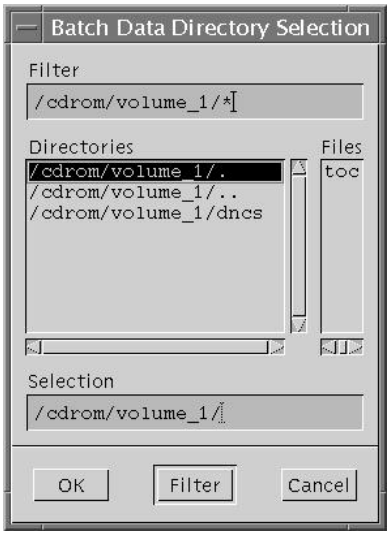
     Note: The DNCS GUI might launch when the system mounts the CD.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, select the **DNCS** tab.
3. Select the **Home Element Provisioning** tab.
4. Click **DHCT** to open the DHCT Provisioning window.
5. Click **New > Batch Install**.
6. Click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



7 Search for the TOC file by replacing the existing **export/home/dncs** filter in the Filter field with one the following options:

- If you are loading EMMs from a CD, replace the export/home/dncs filter with **/cdrom/cdrom0/*** and press **Enter**.
- If you obtained EMMs through FTP, replace the export/home/dncs filter with the path you recorded when you extracted the EMM files. Refer to *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) for more information.

8 In the Directories panel, double-click **volume_1**. The Batch Data Directory Selection window refreshes and lists the **TOC** file.

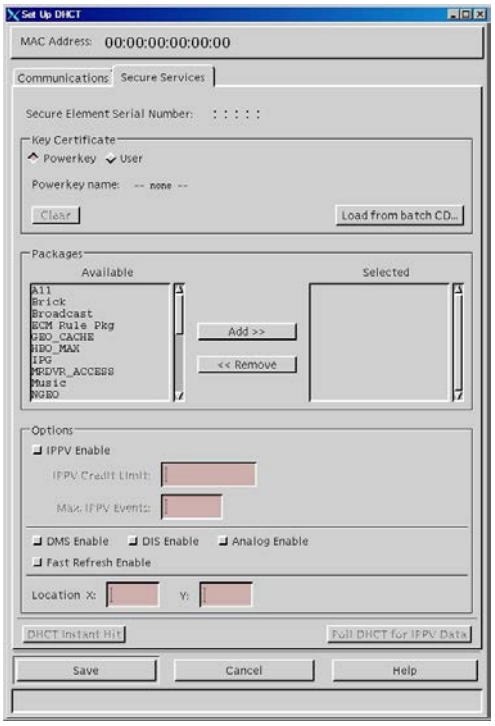


Note: The volume_1 directory may contain additional characters.

Example: volume_1#3

9 Locate the **TOC** file, verify that **TOC** is *not* highlighted, and then click **OK**. The Set Up DHCT window opens.

10 Click the **Secure Services** tab on the Set Up DHCT window.



11 Is **DIS Enable** selected?

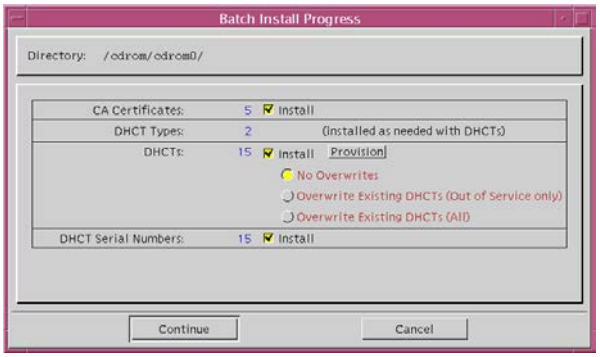
- If **yes**, click the **DIS Enable** option to disable the DIS Enable option.
- If **no**, the DIS Enable option is already off.

12 Are any other options enabled on this screen?

- If **yes**, click the option to disable the option, then click **Save**.
- If **no**, click **Save** to return to the Batch Install Progress window.

Important: If **any** options are enabled on this screen, the DHCTs might not be able to stage correctly.

13 Click **Continue** to open the Batch Install Progress window.



14 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)**.

15 On the Batch Install Progress window, click **Continue**. A window displays the status of the install process.

16 After the **Batch Install is Complete** message appears, click **Close** on the Batch Install Progress window.

17 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.

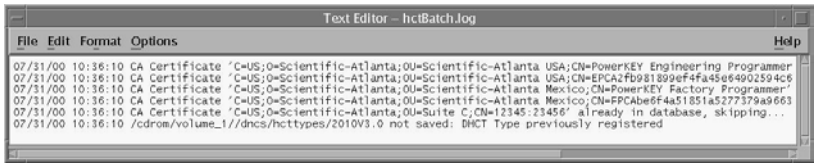
b Click the **Programs** option from the Workspace Menu window.

c From the Personal Applications menu, select the **Text Editor** option.

d Click **File > Open**. The Open a File window opens.

e Enter **/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.

18 Click **File > Copy to File**. The Text Editor – Copy to File window opens.

19 Enter a unique log file name for each EMM CD in the **Enter file name** field. The naming convention of the file name is typically as follows:

/dvs/dncs/tmp/emmcdlogs/<deliverynumber>.log

Example: Enter **/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

20 Click **OK**. The system saves the log file with the new name.

21 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 the procedure, go to step 22 of this procedure.
- If **no**, go to step 22.

22 On the Text Editor window, click **File > Close**.

23 Are you loading EMM data from a CD?

- If **yes**, open an xterm window, enter **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 24.

24 Repeat this procedure for each additional EMM CD.

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** (for DHCTs) or **Two-Way** (for CableCARD modules).
- 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.

Transactions Required for Staging

This section discusses the Business Operations Support System (BOSS) and Business Applications Support System (BASS) transactions required to successfully use SSC DHCTs in your DBDS.

The following billing system interface changes are required for your billing system for SSC DHCTs:

- BOSS and BASS transactions must be directed to the MAC address of the CableCARD module, not to the MAC address of the host.
- VOD session setup messages for session-based encryption must include the MAC address of the CableCARD module.
- The initial billing record, created by your VOD server or your billing messaging system, must use the MAC address of the CableCARD module as the identifier.
- Session response messages are directed to the Source IP Address obtained from the session setup message; typically, this is the IP address of the host.

BOSS Transactions for Staging SSC DHCTs

Use the following BOSS transactions to provision an M-Card for network operation and conditional access:

- **ModifyDhctAdminStatus**—Controls whether an M-Card module is allowed to perform interactive operations and (optionally) sets up the billing ID for the M-Card module.
- **ModifyDhctConfiguration**—Authorizes an M-Card module for subscription video services and applications. Also defines the IPPV credit parameters for the M-Card modules.

BASS Transactions for Staging SSC DHCTs

BASS transactions control the behavior of the resident application operating on a host device and are required when staging SSC DHCTs. Use the following BASS transactions to provision the paired M-Card during the staging process:

- **SetPin**—Defines the Parental Control blocking PIN and/or the IPPV access PIN
- **ResetClientNvm**—Re-initializes all SARA user parameters (favorite channels, parental control, timers, etc.) in the host DHCT and reformats the hard drive in a host DHCT DVR

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 ***Decide Binding Type*** (on page 19).

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.

Decide Binding Type

Binding is a DNCS function that matches the MAC address of the CableCARD to the host ID of the host. You must bind a CableCARD module to its host before the CableCARD module can receive "high-value" copy-protected services (services with copy protection settings of either *copy one generation* or *copy never*).

Important:

- Until you bind the SSC DHCT and the CableCARD module, the DHCT will not be able to display high-value, copy-protected services—even if the DHCT is authorized to receive these services.
- Services that are copy protected with the copy protection setting of *copy freely* can be viewed by an unbound host.

You can choose to use one of the following copy protection binding methods:

- **Combo-binding** occurs when the SSC DHCT downloads EMMs during staging. Sending the EMMs to the SSC DHCT starts a process that adds the CableCARD module/host pair to a file on the BFS. After the pair is added to the file, the SSC DHCT receives the podData file that authorizes the CableCARD module and the DHCT to be bound.
- **Autobinding** matches a CableCARD module and host when the CableCARD module is inserted into the host and the host goes into two-way mode. Autobinding is available for two-way hosts only if all of the following conditions are met:
  - The DNCS is set up for autobinding.
  - The CableCARD module and host can be staged in a one-way or two-way environment.

    Note: To use autobinding, the CableCARD module and host must be bound in a two-way environment to view high value content. Once bound, they can be used in a one-way environment.
  - The host is not on the certificate revocation list (CRL).
  - The Host Change Count for the CableCARD module has not exceeded the Max Host Change Count Allowed setting.
- **Manual binding** allows binding of the CableCARD module and host DHCT from either the DNCS or billing system. From the DNCS, the CableCARD module ID and host ID are added to the DNCS through the CableCARD interface on the DNCS. From the billing system, binding occurs from the billing system interface using the **RegisterHost** command. Contact your billing vendor to see if they support this option.

- **Billing system binding** is binding DHCTs from the billing system interface using the **RegisterHost** command. Contact your billing vendor to see if they support this option.

This section provides a description for each option and contains procedures for autobinding and for manually binding the CableCARD module and host.

Combo-Binding

Combo-binding is a process that the SSC DHCT and CableCARD module pair go through after the CableCARD module downloads its EMMs. The process is as follows.

1. The SSC DHCT and its paired CableCARD module exchange keys to authenticate each other.
2. The DNCS sends the pairing information (as a file named podData) to the BFS. The podData file contains two lists: an authorized list and an unauthorized list. Each list contains information on the SSC DHCT and its paired CableCARD module.

   Note: The DNCS populates its database with the SSC pairing information from the inventory file during the batch load process.
3. The CableCARD module reads the pairing information from the file. If the CableCARD module finds its SSC pairing in the authorized list, it authorizes the binding between it and the SSC host. If it finds its SSC pairing in the unauthorized list, or if it does not find its SSC pairing in either list, it does not authorize the binding.

You do not need to turn combo-binding "on." It is an automatic process available for SSC DHCTs as long as you load the correct DHCT types, have the correct EMMs, and have System Release 4.3 or later.

Autobinding

Autobinding is a process that allows the CableCARD module to bind to a two-way host. The procedure is as follows.

1. When the CableCARD module is inserted into a two-way host, the host and the CableCARD module exchange keys to authenticate each other.
2. After the keys are verified and the host goes into two-way mode, the CableCARD module sends an upstream message to the DNCS that includes the CableCARD ID and the Host ID.
3. The DNCS looks up the Host ID in the CRL. Based on the information in the CRL, the DNCS takes one of the following actions:
   - If the host is in the list, the DNCS does not allow the CableCARD module to bind to the host.
   - If the host is not in the list, the DNCS continues with the next step.

4 The DNCS looks up the CableCARD module/Host in its database to determine if a Host Bound value has been defined for this pair. Based on this information, the DNCS takes one of the following actions:

- If the pair is in the list, and the Host Bound value is **Yes**, the DNCS allows binding for this CableCARD/host pair.
- If the pair is in the list, and the Host Bound value is **No**, the DNCS does not allow binding for this CableCARD module/host pair.
- If the CableCARD module is in the list with a different host, the DNCS continues with step 5.
- If the pair is not in the list, the DNCS checks the Maximum Host Change Count Allowed value (as defined on the CableCARD Server Configuration screen), and takes one of the following actions:
  - If the value is equal to zero (0), the DNCS does not allow binding for this CableCARD module/host pair.

    Note: Setting the Maximum Host Change Count Allowed value to zero disables autobinding.
  - If the value is not equal to zero, the DNCS allows binding for this CableCARD module/host pair.

5 The DNCS checks the Host Change Count value for the CableCARD module and compares it to the CableCARD server's Maximum Host Change Count Allowed value. Based on the values of these two fields, the DNCS takes one of the following actions:

- If the Host Change Count value for the CableCARD module is a smaller value than the Maximum Host Change Count Allowed value, the DNCS allows binding for this CableCARD module/host pair, and increments the Host Change Count by one.
- If the Host Change Count value for the CableCARD module is equal to or larger than the Maximum Host Change Count Allowed value, the DNCS does not allow binding for this CableCARD module/host pair.

Note: If the Maximum Host Change Count Allowed value is 99, the DNCS allows the CableCARD module to bind to different hosts an unlimited number of times.

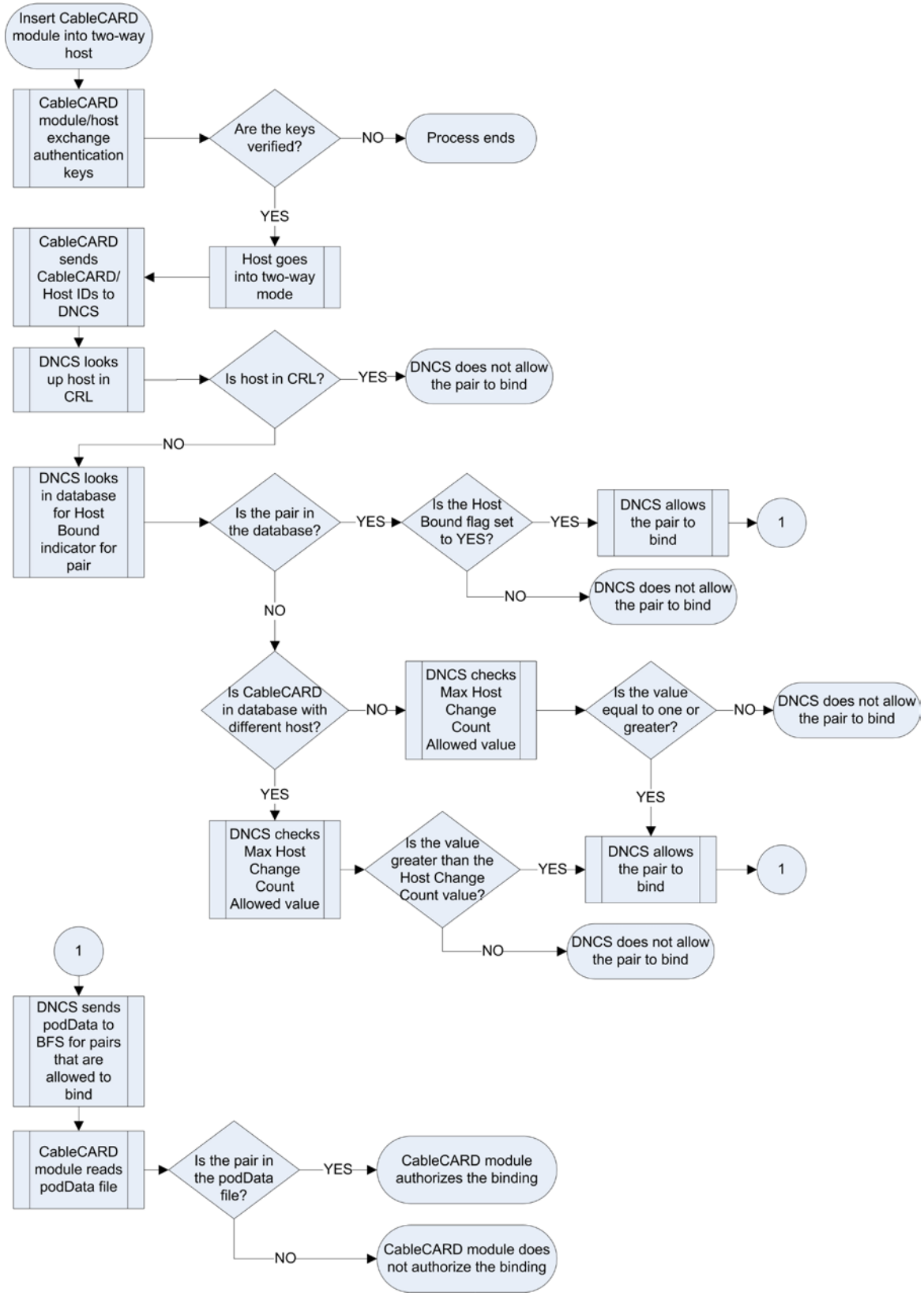
6 The DNCS sends the podData file containing the binding permissions to the BFS for those pairs that are allowed to bind (based on the above criteria).

Note: The CableCARD module/host pairs denied binding are not placed in the podData file.

7 The CableCARD module reads the podData file on the BFS.

- If the CableCARD module finds its pairing in the podData file, the CableCARD module authorizes the binding between itself and the host.
- If the CableCARD module does not find its pairing in the podData file, the CableCARD module does not authorize the binding.

Autobinding Flowchart

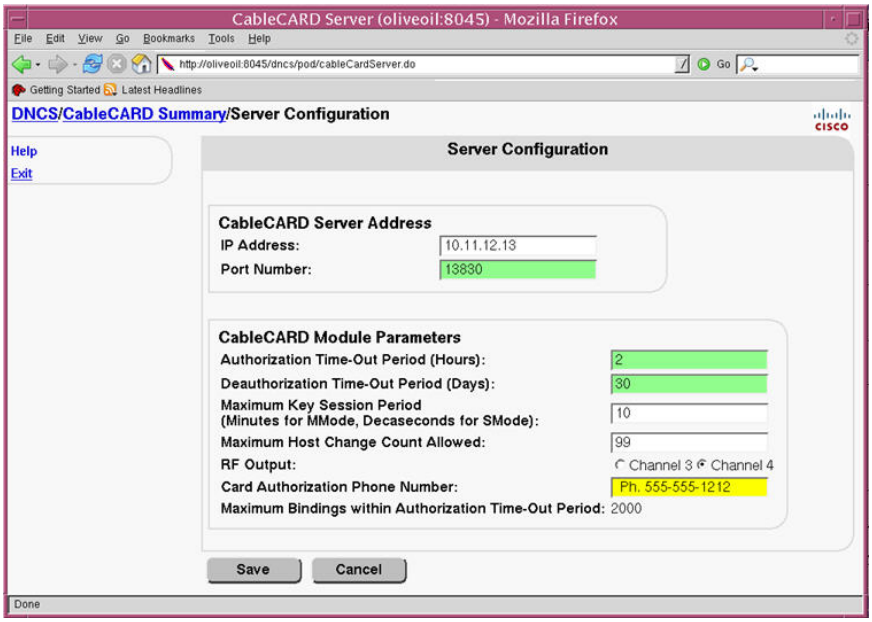


Setting Up the DNCS for Autobinding

1 On the DNCS Administrative Console, select the **Home Element Provisioning** tab.

2 Click **CableCARD**. The CableCARD Summary screen opens showing the CableCARD filter.

3 Click **Server Configuration**. The Server Configuration screen opens.



4 Enter the following information into the appropriate fields within the Configure CableCARD Server screen:

- **IP Address**—Enter the IP address of the server that is running the CableCARD Server. In most cases, the CableCARD Server runs on the DNCS. If this is the case for your system, type **10.253.0.1** in this field.

  Important: If you do not use the default IP address for your CableCARD server, check your network map, the /etc/hosts file for the **dncsatm** entry, or with your network administrator for the correct IP address.

  Note: If you do not want to use autobinding for CableCARD modules, enter **0.0.0.0** in this field.

- **Port Number**—Enter the port number on the DNCS that the CableCARD server will monitor for incoming CableCARD module requests. The port number is **13830**.

  Note: If you do not want to use autobinding for CableCARD modules, enter **0** in this field.

- **Authorization Time-out Period**—Enter the length of time (in hours) the Host-CableCARD pair is kept in the file on the BFS. We recommend that you enter **2** in this field.

Notes:

- Negative values are not permitted in this field.
- If you define a value greater than 2, be aware of the following issues:
  - The podData file on the BFS can contain no more than 1500 entries. During staging, a pod (CableCARD)/host pair is added to the podData file for the amount of time defined in this field. When the Authorization Time-out Period is reached, 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, pod/host pairs will not be able to bind.

- **Deauthorization Time-Out Period**—Enter the length of time (in days) the Authorization message is kept in the file on the BFS. Enter **30** in this field.
- **Max Key Session Period**—Enter the rate that the copy protection key should change. The rate referenced depends on the communications mode of the CableCARD module, as determined by the host's capabilities:
  - **Multistream Mode (MMode):** The field represents minutes. Therefore, entering a **1** in this field causes the copy protection key to change every minute. Enter **10** in this field.
  - **Singlestream Mode (SMode):** The field represents decaseconds. Therefore, entering a **1** in this field causes the copy protection key to change every 10 seconds. Enter **10** in this field.

  Important: Defining a rate less than 1 minute (for MMode) or 10 decaseconds (for SMode) requires a large number of unnecessary calculations on the CableCARD. Defining a rate greater than X minutes (for MMode) or 20 decaseconds (for SMode) does not coincide with best security practices.
- **Maximum Host Change Count Allowed**—Enter the maximum number of times that a CableCARD module is allowed to autobind with a different host. When a module exceeds this limit, it is no longer allowed to autobind with a different host.

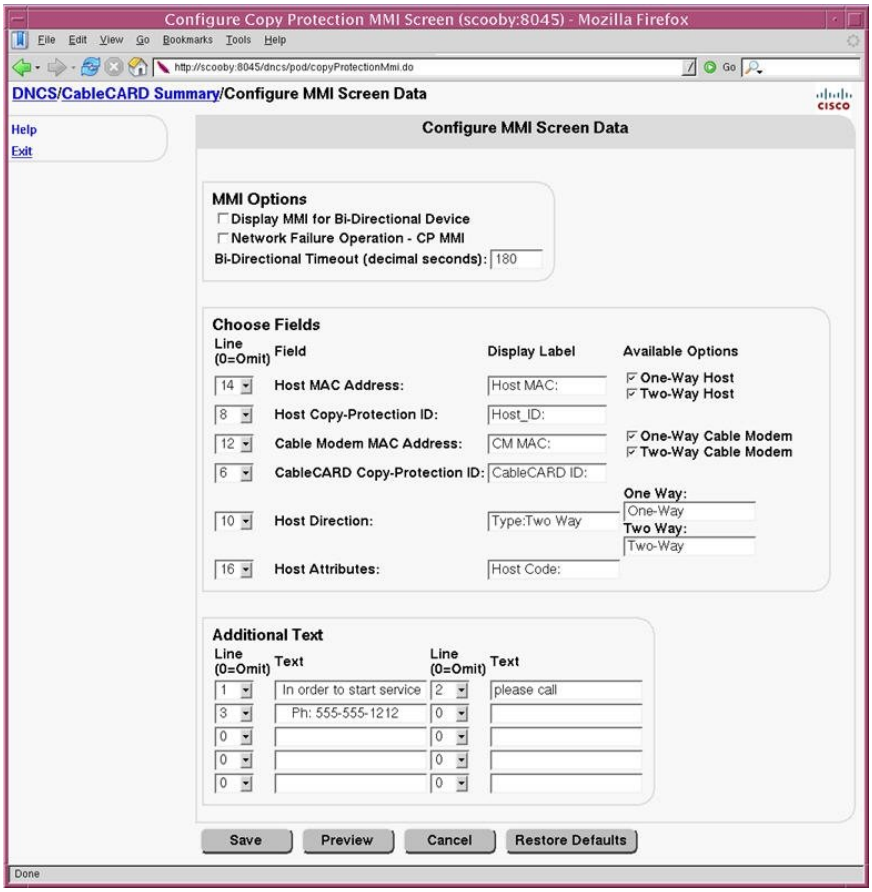
  Note: The default setting of 99 allows an unlimited number of autobindings.
- **RF Output**—Select the channel to which the CableCARD module outputs video. Typically, you should select the same channel that the DHCTs use for the CableCARD modules.
- **Card Authorization Phone Number**—Enter the telephone number that subscribers call to verify that their CableCARD module was authorized. You can enter up to 20 alphanumeric characters, including spaces, in this field.
- **Maximum Bindings Within Authorization Time-Out Period**—Enter the maximum number of CableCARD modules and DHCTs that can bind during a staging period. We recommend that you set this field to the maximum setting of **1500**.

Note: This value cannot be changed from the Server Configuration window. To change this value, you must use the modCCardStagingLimit script. For assistance using this script, refer to *Change the CableCARD Module Staging Limit* (part number 4020737).

5 Click **Save** to save these parameters.

6 Click the **CableCARD Summary** link at the top of the page. The CableCARD Summary screen opens.

7 Click **MMI Screen Format**. The Configure MMI Screen Data screen opens.



8 Make sure that the **Display MMI for Bi-Directional Device** is **not activated** (that a checkmark **does not** display in the box).

9 Select the **Network Failure Operation - Display CP MMI** option you prefer:

- **Unchecked** (disabled, default): The host always uses the value in the **Bidirectional Timeout** field to determine when to display the MMI CP screen.
- **Checked** (enabled): The host displays the MMI CP screen if no network boot occurs.

10 Click in the **Bidirectional Timeout (decimal seconds)** and enter the number of seconds the two-way CableCARD host waits to displays the CP MMI screen after the host determines that it cannot connect to the DNCS or receive a response from the DNCS.

Note: We recommend that you set the Bidirectional timeout to **180** seconds (3 minutes).

11 Click **Save**.

12 Click **Exit** to close the CableCARD Data Summary screen.

Turning Off Autobinding

1 On the DNCS Administrative Console, select the **DNCS** tab.

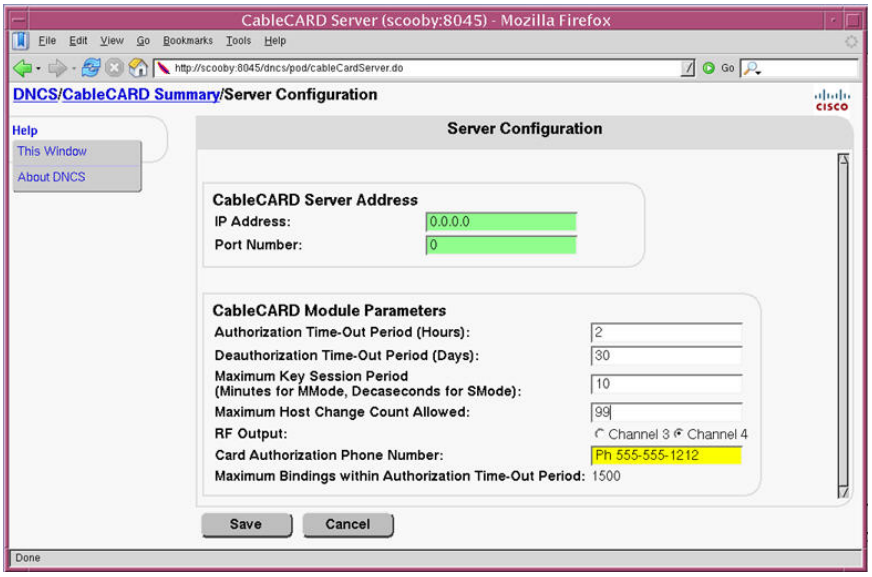
2 Select the **Home Element Provisioning** tab.

3 Click **CableCARD**. The CableCARD Filter screen opens.

4 Click **Configure CableCARD Server**. The Configure CableCARD Server screen opens.

5 Enter the following information into the appropriate fields within the Configure CableCARD Server screen:

- **IP Address**—Type all zeros for the IP Address: **0.0.0.0**
- **Port Number**—Type a zero for the Port Number: **0**



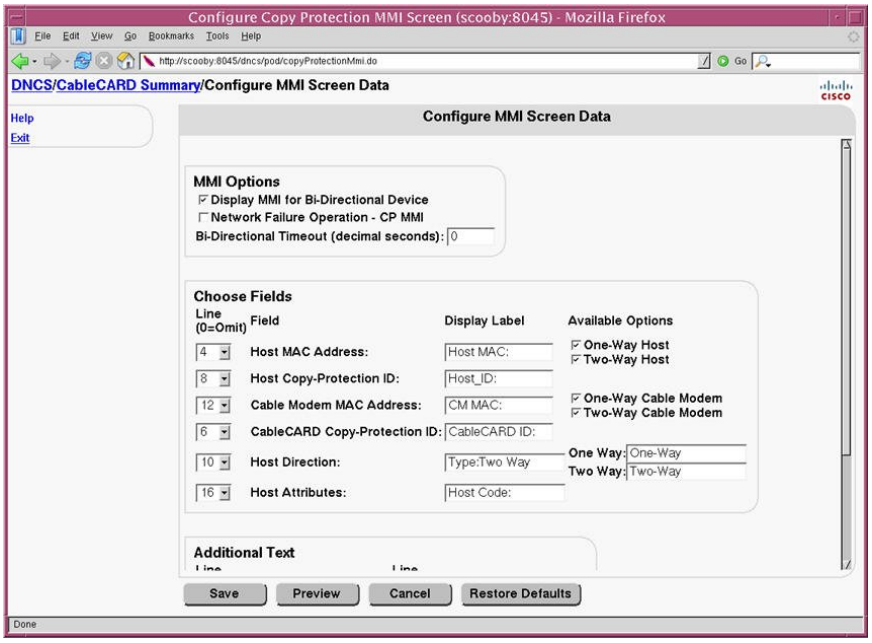
6 Click **Save** to save these parameters.

7 Click the **CableCARD Summary** link at the top of the page. The CableCARD Summary screen opens.

8 Click **MMI Screen Format**. The Configure Copy Protection MMI Screen opens.

9 Make sure that the **Display MMI for Bi-Directional Device** is **activated** (that a checkmark displays in the box).

10 Click in the **Bidirectional Timeout (decimal seconds)** and type a **0** (zero).



11 Click **Save**.

12 Click **Exit** to close the CableCARD Data Summary screen.

Manual Binding

Manual binding is the process of manually adding the CableCARD module ID and host ID to the DNCS through the CableCARD interface on the DNCS so that the CableCARD module can receive "high-value" copy-protected services (services with copy protection settings of either *record once* or *record never*).

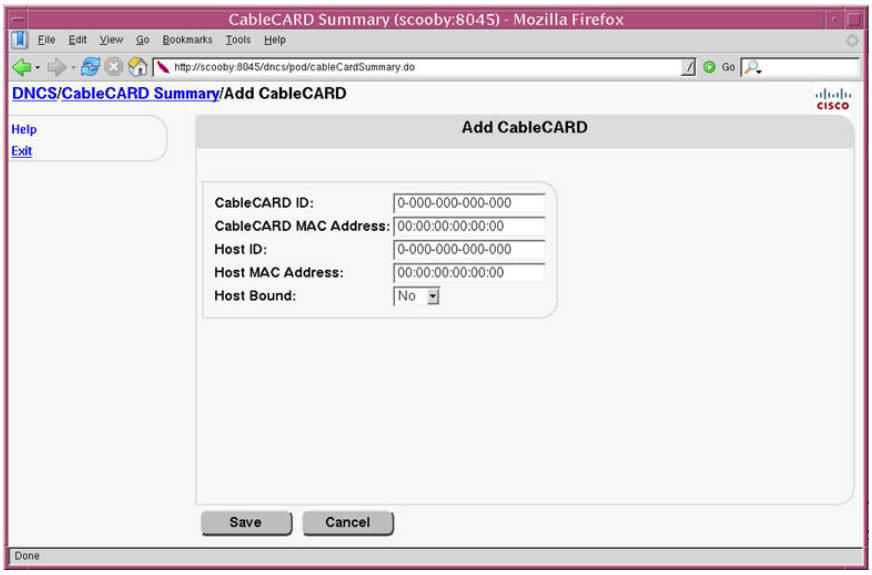
Manually Binding a CableCARD Module and Host

1 On the DNCS Administrative Console, select the **DNCS** tab.

2 Select the **Home Element Provisioning** tab.

3 Click **CableCard**. The CableCARD Summary screen opens showing the CableCARD filter.

4 Click **Add**. The Add CableCARD screen opens.



5 Use the CableCARD diagnostic screens to locate the CableCARD ID, MAC Address, and Host ID, or you can record the IDs that display on the host screen after you insert the CableCARD module into a host.

6 Enter the CableCARD ID or the CableCARD MAC Address, and then enter the Host ID in the appropriate fields.

Notes:

- Entering *both* the CableCARD ID *and* the CableCARD MAC Address is not necessary. Entering either one is sufficient.
- The CableCARD MAC Address field is *not* case-sensitive; however, all values entered into this field are converted to uppercase letters.

7 Select **Yes** in the Host Bound column to allow the module and host set-top to bind.

8 Click **Save** to save the configuration and bind the CableCARD module to the host.

Important: After saving the CableCARD module on the DNCS, copy protected content should be displayed on the host within a few minutes. If it is not, contact Cisco® Services for assistance.

9 If you are finished, click **Exit** to close the Add CableCARD window.

Add DHCT Types to the DNCS

Important: This procedure is only necessary if you added DHCT types to the DNCS before you upgraded to SR 4.3. Otherwise, you can skip this step.

Adding a DHCT type to the DNCS allows the DHCT type to be associated with the correct client software. This allows the DNCS to send the software to the associated DHCTs using the CVT download method.

When you batch install the EMM files for SSC DHCTs, only the M-Card modules in the SSC pair are added to the DNCS as a DHCT type. Because of this, you must add any new model of SSC DHCT (such as the 4250C or the 8300HDC) to the DNCS manually.

Note: The 4240, 4250C, and 4250HDC SSC DHCT types display as *Explorer 4300* DHCTs.

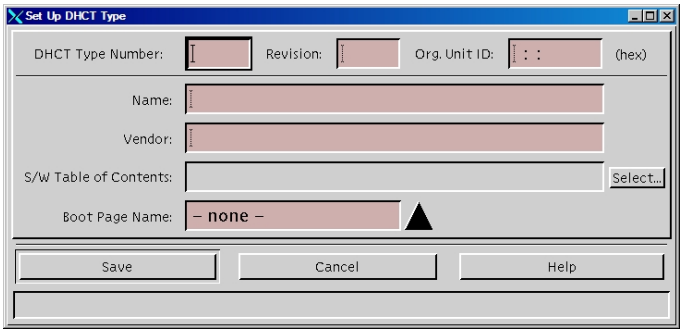
Important: You still need to download the client software to the DHCTs using the default group, unless you manually add each DHCT to the DNCS database. See ***Add DHCTs to the DNCS Database*** (on page 31) for more information.

1 On the DNCS Administrative Console, select the **DNCS** tab.

2 Select the **Home Element Provisioning** tab.

3 Click **Type**. The DHCT Type List screen opens.

4 Click **File > New**. The Set Up DHCT Type window opens.



5 Enter information in the following fields on the Set Up DHCT Type window:

- **DHCT Type Number**—Enter the type number (for example, **8300**)
- **Revision**—Type the revision number of the DHCT type (for example, for 3.1. you would type **31**; do not type the periods)
- **Org. Unit ID**—Type **00:02:DE**
- **Name**—Type a descriptive name for the DHCT type (for example, **8300HDC SSC DHCT rev. 3.1**)
- **Vendor**—Type **Cisco**

- **S/W Table of Contents**—Click **Select** to browse to the correct toc file for this DHCT type (leave blank if you are using bootloader)
- **Boot Page Name**—Click the arrow to select the boot page associated with this DHCT type, if appropriate (leave blank if you are using bootloader)

6 Click **Save**. The Set Up DHCT Type window closes and the new DHCT type displays on the DHCT Type List screen.

Setting Up Download Groups

To stage SSC DHCTs in groups other than the default group, you must manually add the SSC DHCTs to the DNCS database. See ***Add DHCTs to the DNCS Database*** (on page 31) for more information.

Then, if the download group does not already exist, you must create the CVT download group for the SSC DHCT and add the SSC DHCTs to that group. See ***Create CVT Download Groups*** (on page 32) for more information.

Or, if the download group already exists, you must add the SSC DHCTs to the group. See ***Add the SSC DHCTs to Existing CVT Download Groups*** (on page 33) or ***Add CableCARD Modules to Existing CVT Groups*** (on page 35) for more information.

Add DHCTs to the DNCS Database

Important: This procedure is only necessary if you added DHCTs to the DNCS before you upgraded to SR 4.3. Otherwise, you can skip this step.

To use a download group other than the default group, your first step is to manually add the SSC DHCTs to the DNCS database. The following procedure details the steps you must take add the DHCTs to the database.

Adding DHCTs to the DNCS Database

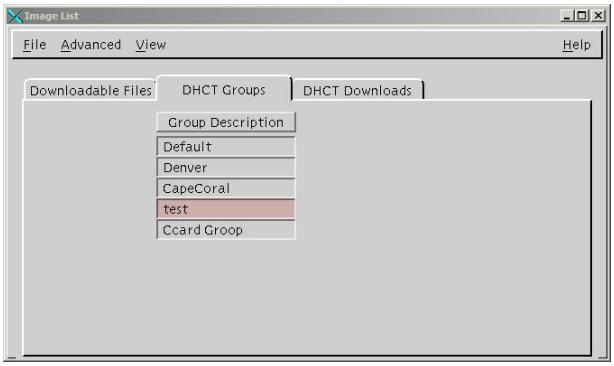
1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning screen opens.
4. Select the **New** option.
5. Type the MAC address for the DHCT you are adding in the **By MAC Address** field.
6. Click **Continue**. The Set Up DHCT window opens.
7. Select the **DHCT Type** of the DHCT you are adding.
8. Enter the **DHCT Serial Number** of the DHCT you are adding.
9. Click the arrow next to **Admin Status** and select **In Service One Way**.
10. Click **Save**.
11. Repeat steps 4 through 9 for every SSC DHCT you need to add to the database.
12. Your next step is to add the SSC DHCTs to the download group. Do you need to create the download group for the SSC DHCTs?
    - If **yes**, go to ***Create CVT Download Groups*** (on page 32).
    - If **no**, go to ***Add the SSC DHCTs to Existing CVT Download Groups*** (on page 33).

Create CVT Download Groups

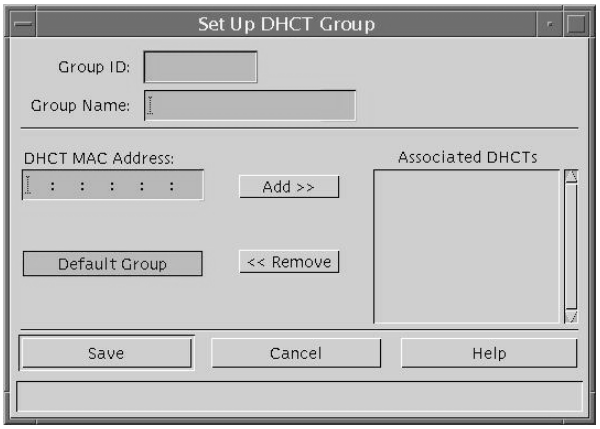
If your download group does not yet exist, follow these steps to create the download group and to add the SSC DHCTs to that group. If your download group already exists, follow the steps in ***Add the SSC DHCTs to Existing CVT Download Groups*** (on page 33).

Creating CVT Download Groups

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **DHCT Groups** tab. The DHCT Groups tab opens.



5. Click **File > New**. The Set Up DHCT Group window opens.



6. Configure the fields on the Set Up DHCT Group window as follows:
   - **Group ID**—Type a unique group identification number (other than zero).
   - **Group Name**—Type a meaningful name for the group.

     Example: SSC_Download_Group
   - **DHCT MAC Address**—Type the MAC address of a DHCT that you want to include in the new group.
7. Click **Add**. The MAC Address of the DHCT moves to the Associated DHCTs column.

8 Repeat steps 6 and 7 for each DHCT you want to add to the group.

9 Click **Save**. The new group appears in the list of group descriptions on the DHCT Groups tab.

Notes:

- The DHCT should be connected to the network within 2 hours of creating or adding it to a test group. If the device is not connected within 2 hours, then the device does not receive a group assignment until the DNCS database cycles through all in-service devices at a rate of approximately one device per second. Depending on the number of devices in your system, this process could take a significant amount of time.
- If the device has an Administrative State of Out of Service, the CVT Group ID message will not be sent by the PassThru process to that device. To check the Administrative State of the device, see ***DHCT and CableCARD Module Administrative Status*** (on page 38).

10 Confirm that the DHCT was successfully placed into the test group by displaying the DHCT diagnostic screens and looking at the **Group ID** field. This group ID should match the Group ID field displayed on the Set Up a DHCT Group window on the DNCS.

Note: The Group ID on the DHCT is in hexadecimal format. The Group ID on the DNCS is in decimal format. You might need to convert the Group ID to verify this step.

11 Do the Group ID values on the diagnostic screen and DNCS match?

- If **yes**, go to ***Staging SSC DHCTs*** (on page 75).
- If **no**, contact Cisco Services.

Add the SSC DHCTs to Existing CVT Download Groups

If your download group already exists, follow these steps to add the SSC DHCTs to the group. If your download group does not already exist, follow the steps in ***Create CVT Download Groups*** (on page 32).

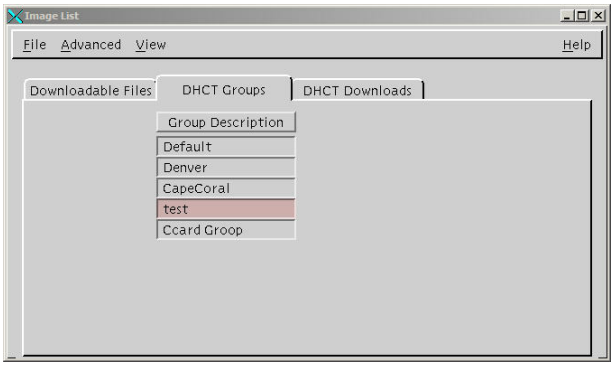
Adding SSC DHCTs to Existing CVT Download Groups

1 On the DNCS Administrative Console, select the **DNCS** tab.

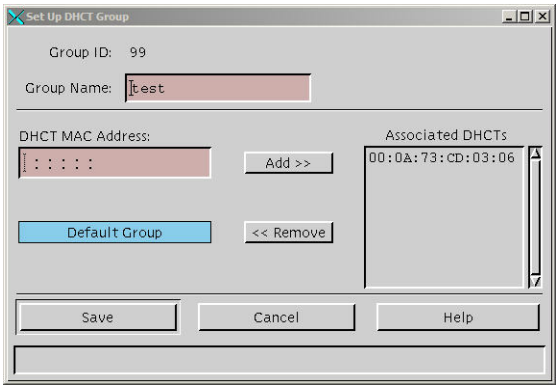
2 Select the **Home Element Provisioning** tab.

3 Click **Image**. The Image List window opens.

4 Click the **DHCT Groups** tab. The DHCT Groups tab opens.



5 Double-click the group you want to which you want to add SSC DHCTs. The Set Up DHCT Group window for the group opens.



6 Type the **DHCT MAC address** of a DHCT that you want to include in the new group.

7 Click **Add**. The MAC Address of the DHCT moves to the Associated DHCTs column.

8 Repeat steps 6 and 7 for each DHCT you want to add to the group.

9 When you are finished adding SSC DHCTs to the group, click **Save**.

Notes:

- The DHCT should be connected to the network within 2 hours of creating or adding it to a test group. If the device is not connected within 2 hours, then the device does not receive a group assignment until the DNCS database cycles through all in-service devices at a rate of approximately one device per second. Depending on the number of devices in your system, this process could take a significant amount of time.
- If the device has an Administrative State of Out of Service, the CVT Group ID message will not be sent by the PassThru process to that device. To check the Administrative State of the device, see ***DHCT and CableCARD Module Administrative Status*** (on page 38).

10 Confirm that the DHCT was successfully placed into the test group by displaying the DHCT diagnostic screens and looking at the **Group ID** field. This group ID should match the Group ID field displayed on the Set Up a DHCT Group window on the DNCS.

Note: The Group ID on the DHCT is in hexadecimal format. The Group ID on the DNCS is in decimal format. You might need to convert the Group ID to verify this step.

11 Do the Group ID values on the diagnostic screen and DNCS match?

- If **yes**, go to ***Staging SSC DHCTs*** (on page 75).
- If **no**, contact Cisco Services.

Add CableCARD Modules to Existing CVT Groups

If your download group already exists, follow these steps to add standalone CableCARD modules to the group. If your download group does not already exist, follow the steps in ***Create CVT Download Groups*** (on page 32).

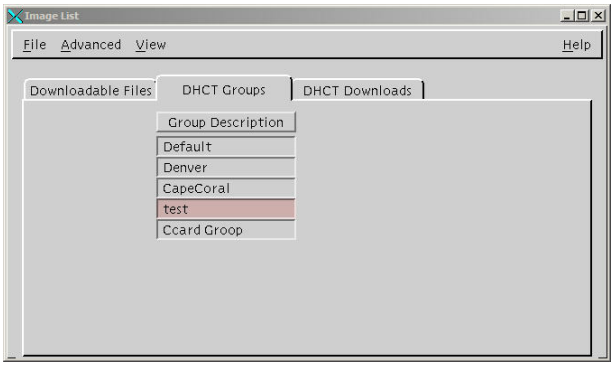
Adding CableCARD Modules to Existing CVT Download Groups

1 On the DNCS Administrative Console, select the **DNCS** tab.

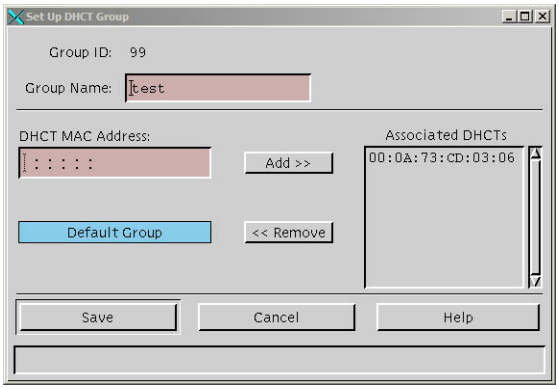
2 Select the **Home Element Provisioning** tab.

3 Click **Image**. The Image List window opens.

4 Click the **DHCT Groups** tab. The DHCT Groups tab opens.



5 Double-click the group to which you want to add the standalone CableCARD modules. The Set Up DHCT Group window for the group opens.



6 Type the **DHCT MAC address** of a CableCARD module that you want to include in the new group.

7 Click **Add**. The MAC Address of the CableCARD module moves to the Associated DHCTs column.

8 Repeat steps 6 and 7 for each CableCARD module you want to add to the group.

9 When you are finished adding CableCARD modules to the group, click **Save**.

Notes:

- The CableCARD module should be connected to the network within 2 hours of creating or adding it to a test group. If the CableCARD module is not connected within 2 hours, then the CableCARD module does not receive a group assignment until the DNCS database cycles through all in-service devices at a rate of approximately one device per second. Depending on the number of devices in your system, this process could take a significant amount of time.
- If the CableCARD module has an Administrative State of Out of Service, the CVT Group ID message will not be sent by the PassThru process to that CableCARD module. To check the Administrative State of the CableCARD module, see ***DHCT and CableCARD Module Administrative Status*** (on page 38).

10 Confirm that the CableCARD module was successfully placed into the test group by displaying the CableCARD module diagnostic screens and looking at the **Group ID** field. This group ID should match the Group ID field displayed on the Set Up a DHCT Group window on the DNCS.

Note: The Group ID on the CableCARD module is in hexadecimal format. The Group ID on the DNCS is in decimal format. You might need to convert the Group ID to verify this step.

11 Do the Group ID values on the diagnostic screen and DNCS match?

- If **yes**, go to ***Verify CableCARD Connectivity*** (on page 36).
- If **no**, contact Cisco Services.

Verify CableCARD Connectivity

Before you add a CableCARD module to a CVT group, you need to verify that the connectivity state on the DNCS matches the connectivity state of the CableCARD module.

Verifying CableCARD Connectivity

1 On the DNCS Administrative Console, select the **DNCS** tab.

2 Select the **Home Element Provisioning** tab.

3 Click **DHCT**. The DHCT Provisioning window opens.

4 Type the **MAC address** of the CableCARD module you are checking and click **Continue**. The Set Up DHCT screen opens.

5 Verify the **Administrative Status** of the CableCARD module.

Note: The Administrative Status will display one of the following values for the CableCARD module:

- Out of Service
- In Service One Way
- In Service Two Way
- Deployed

6 Does the Administrative Status show the CableCARD module as being **In Service Two Way**?

- If **yes**, continue with step 7.
- If **no**, you are finished with this procedure.

7 Is an IP address assigned to the CableCARD module?

- If **yes**, go to step 8.
- If **no**, change the Administrative Status of the CableCARD module to **In Service One Way**.

8 Open an xterm window on the DNCS.

9 Type **ping [CableCARD IP address]** and press **Enter**.

Note: Do not type the brackets **[ ]** in the command.

10 Does the CableCARD module respond to the ping command?

- If **yes**, go to step 11.
- If **no**, change the Administrative Status of the CableCARD module to **In Service One Way**.

11 Open the diagnostic screens on the CableCARD module host.

12 Find the IP address of the CableCARD module.

13 Does it match the IP address listed on the DNCS (in step 7)?

- If **yes**, you have finished this procedure.
- If **no**, reboot the host and verify that the IP address matches the IP address listed on the DNCS.

DHCT and CableCARD Module Administrative Status

This section explains the different possible administrative states a device could be assigned, and also explains how to verify the Administrative Status of a device.

Understanding DHCT and CableCARD Module Status

The DNCS database maintains four administrative statuses for DHCTs and CableCARD modules (collectively known as *devices*). These statuses are described in the following list:

- **In service, two-way**—Devices with a status of **in service two-way** support communication between the headend and the device, as well as return communication. Devices need two-way communication capability to take full advantage of interactive services.

  Example: Examples of interactive services include impulse pay-per-view (IPPV), video-on-demand (VOD), and anything on-demand (xOD).

- **In service, one-way**—Devices with a status of **in service one-way** support communication from the headend to the device, only. These devices are considered to be in broadcast-only mode and have no two-way services assigned to them.

- **Out of service**—Devices that are new and have not yet been staged or installed in subscribers' homes have a status in the database of **out-of-service**. Devices with a status of out-of-service cannot sign on to the network.

  Note: Devices set to an Administrative Status of Out of Service do not receive PassThru messages, such as Group ID assignment messages.

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

Note: Not all billing vendors support the deployed administrative status.

Verify the Administrative Status of a DHCT or CableCARD Module

Follow this procedure to verify the administrative status of a device.

1. From the Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. Enter one of the following for the device you want to check:
   - MAC address
   - IP Address
   - Serial Number
5. Click **Continue**. The Set Up DHCT window opens.
6. On the **Communications** tab, the Administrative State of the device is listed about halfway down the screen. It will display one of the following values:
   - Out of Service
   - In Service One Way
   - In Service Two Way
   - Deployed

2

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

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 SSC 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 (by running the listCVT utility)
- Cleaning up the ResApp directory
- Verifying and cleaning up the download directory
- Adding multiple bootloader carousels
- Changing the data carousel rates
- Calculating and changing (if necessary) the OOB CVT message cycle time

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 following tables list the recommended parameters related to DNCS SR 4.3.

Note: For settings related to earlier System Releases, refer to one of the following documents:

- *Separable Security Host Staging Guide for System Release 4.2.1 and Earlier* (part number 736107)
- *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375)

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 **dncsatm** 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: ■ 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.

Field	Recommended Value
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.
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 *Change the CableCARD Module Staging Limit* (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

Maximum Host Change Count Allowed

The Maximum Host Change Count Allowed field determines 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 DNCS allows auto-binding of Multistream CableCARDs (M-Cards) with two-way Host devices. In SR 4.3, you can limit the number of autobinding requests (from different hosts) that are honored. If the counter reaches the maximum value configured for the system, autobinding requests are rejected by the DNCS and the Copy Protection (CP) MMI screen is displayed.

The Maximum Host Change Count Allowed field on the CableCARD Server page defines this maximum number. The following values can be used in this field:

- 0 = Autobinding is not used.
- 1 - 98 = The valid range for the count
- 99 = An unlimited number of auto-bindings is allowed (default setting)

Resetting the Binding Counter

What happens when an M-Card module reaches its maximum number of autobindings and needs to be reset? For example, if you have an M-Card that you need to re-deploy into a different subscriber's home?

You need to reset the binding counter for this M-Card module by sending a BOSS **RegisterHost** transaction from the billing system to the valid Host_ID associated with the M-Card module.

The BOSS RegisterHost transaction can reset the counter even if the M-Card module is not physically installed in a Host device. For example, you can use a "dummy" Host_ID to reset the counter maintained by the DNCS when preparing to reissue a previously deployed M-Card module. In this case, you must include the CableCARD_ID of the M-Card module in the RegisterHost transaction along with a valid Host_ID.

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, see Avoid Sending Download-related UN-Config Messages.

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 48). 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 48).

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 then select the **Home Element Provisioning** tab.
2. Click **Type**. The DHCT Type List window opens, listing the DHCT type, revision, OUI, and name.
3. 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 to see if that entry is used in your system.
   - If **no**, or if you are not certain, go to step 4.
4. 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?
5. Click **Yes**.
6. 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.
7. Repeat this procedure from step 6 for each DHCT type in the DHCT Type List.
8. From the drop-down menu at the top of the DHCT Type List window, click **File > Close**. The DHCT Type List closes.

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 49).
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 **cd /dvs/dncs/Utilities/doctor** and press **Enter**. The current directory is now the doctor directory.

   Note: Be sure to type a space between **cd** and **/**.
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 is 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 49).
9. On the DNCS Administrative Console, select the **DNCS** tab.
10. Select the **Home Element Provisioning** tab.
11. Click **OS**. The DHCT OS List window opens.
12. 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.

13 Repeat step 12 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 49).

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.

Running the listCVT Utility and Removing Unneeded Files

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 equal to or greater than the one listed in the matrix, go to step 4.
- If the version number is less than the one listed in the matrix, contact Cisco Services to receive the latest utility.

4 Type **cd /dvs/dncs/Utilities/doctor** and press **Enter**. The current directory is now the doctor directory.

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

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.

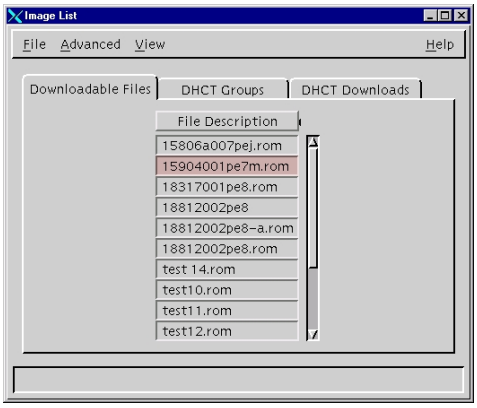
7 Does the report indicate that there are unused files?

- If **yes**, go to step 8.
- If **no**, go to step 13.

8 On the DNCS Administrative Console, select the **DNCS** tab and then select the **Home Element Provisioning** tab.

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**.

Note: The DHCT software files have file extensions of **.rom** (for 4250-series DHCTs) or **.disk** (for 8300-series DHCTs).

12 Repeat step 11 for each file that is unused in the network. After all of the unused software files are deleted, go to step 13.

13 Go to ***Clean Up the ResApp Directory*** (on page 50).

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 42) 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 51).

Verify the Download Directory

Before you download the client application software from the FTP server, you must verify that the /export/home/dncs/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/dncs/download** and press **Enter**.

   Note: Type a space between cd and /.
4. Does the **/export/home/dncs/download** directory exist on your DNCS?
   - If **yes**, you are finished with this procedure. Go to ***Clean Up the Download Directory*** (on page 51).
   - If **no**, go to step 5.
5. Type **mkdir /export/home/dncs/download** and press **Enter**.

   Note: Type a space between **mkdir** and the **/**.
6. Type **cd /export/home/dncs/download** and press **Enter**.

   Note: Type a space between **cd** and **/**.
7. Go to ***Clean Up the Download Directory*** (on page 51).

Clean Up the Download Directory

This section provides instructions to clean up the download directory (/export/home/dncs/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/dncs/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.

Multiple Bootloader Carousels

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 55) 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.

Set Up Multiple Bootloader Carousels

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

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 55).
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 ***Add a Bootloader Source to the DNCS*** (on page 59).

   - **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 ***Set Up DHCTs to Download Images from a Specific Bootloader Carousel*** (on page 60).

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.

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 56).
- If your system uses a BFS BIG, go to ***Determining Available Bandwidth for BFS BIG Systems*** (on page 57).

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:

```
Total Available Bandwidth - Bandwidth in Use = 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 Mbps
     ```
   - **256-QAM:** If your total inband carousel bandwidth in use is 14 Mbps, the available bandwidth is 23 Mbps.

     ```
     37 - 14 = 23 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 ***Add a Bootloader Source to the DNCS*** (on page 59).
   - 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:

```
Total Available Bandwidth - Bandwidth in Use = 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 Mbps
     ```
   - **256-QAM:** From the examples above, the available bandwidth is 21 Mbps.

     ```
     36 - 15 = 21 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 58).
- 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 ***Add a Bootloader Source to the DNCS*** (on page 59).
- If **no**, add more VCIs to the switch. Then, go to ***Add a Bootloader Source to the DNCS*** (on page 59).

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

Add 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.

Set 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.

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.

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 65) 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

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.

1 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".

2 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.

3 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.

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.

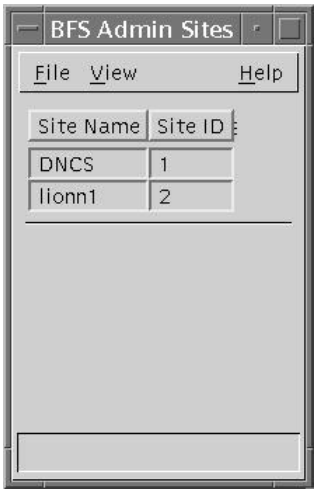
Note: To edit the data carousel rates on a DBDS using a prior release, refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377).

Changing the Data Carousel Rates for the bootloader

Follow these instructions to change the data carousel rates.

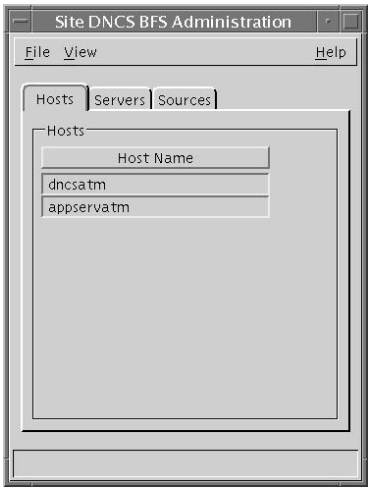
1 From the DNCS Administrative Console, select the **Application Interface Modules** tab.

2 Click **BFS Admin.** The BFS Admin Sites window opens.



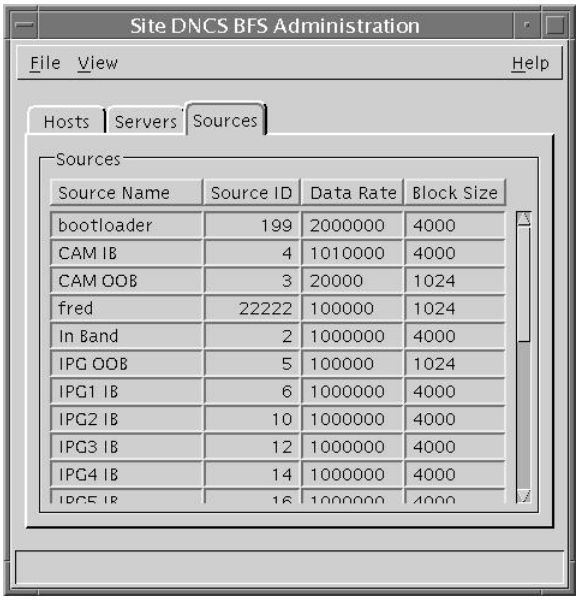
Note: The system used in this example supports the Regional Control System (RCS) feature that uses the DNCS to manage several remote headends. The lionn1 site (shown in this example) is a remote headend. Your system may support more remote headends or might not support the RCS feature at all.

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

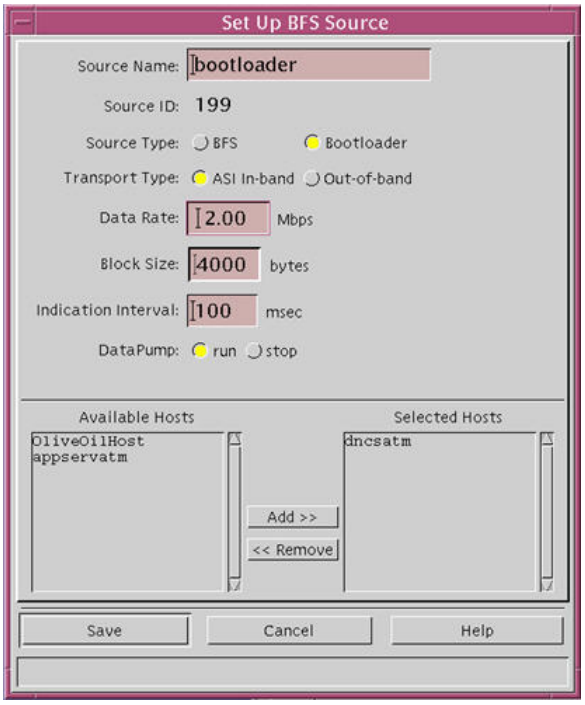


Note: The name of this window will vary, based on the site you select.

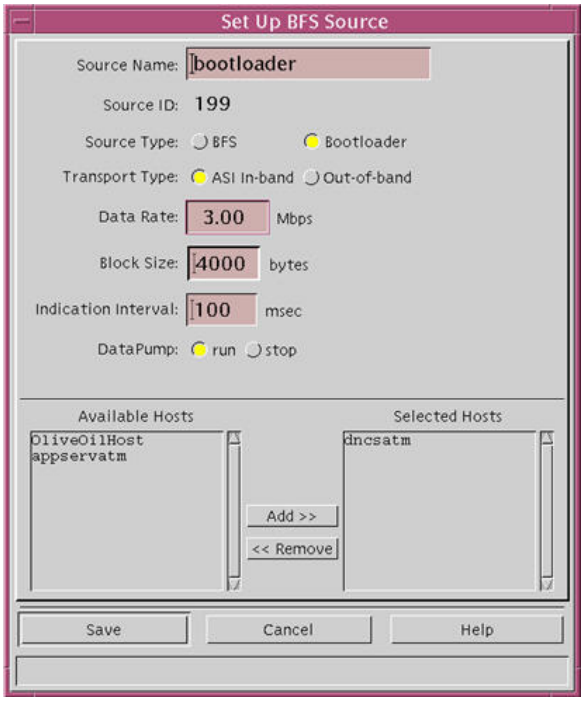
4 Click the **Sources** tab. The window updates to display a list of BFS source names and associated configuration data.



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.

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.

Calculate and Change the OOB CVT Message Cycle Time

This section describes how you can determine and change the out-of-band CVT message cycle time for your system.

Important: Only use this procedure if you are using bootloader version 1.21 or earlier.

Calculate the OOB CVT Message Cycle Time

We have determined that the optimal cycle time for transmission of OOB CVT messages is one-half the cycle time of the bootloader carousel plus one minute.

Adjusting the cycle time of the CVT messages allows you to decrease the staging times for CableCARD modules.

Calculating the Optimum OOB CVT Message Cycle Time

Important: The procedures contained in this document should be repeated whenever you add or remove files from your bootloader carousel.

The optimal cycle time for transmission of OOB CVT messages is one-half the cycle time of the bootloader carousel plus 1 minute (in seconds), or ((bootloader/ 2) + 60).

Follow these steps to calculate the optimum CVT message cycle time for your system:

1. Generate a Doctor report.
2. In the Doctor report, locate the section with the heading **BFS Carousel and OSM Sessions Status**.
3. Locate the bootloader entry (or entries) and obtain the bootloader cycle time from ACCT column. The time is listed in minutes:seconds.

   Example:

```
BFS Carousel and OSM Sessions Status

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

Reporting for site DNCS

                              =Datarate=  =KBytes=   =Intrvl= =Enabled=  =ACCT=

OK:         IB  s( 199) up  3.00 Mbps   10810.000  100      Yes        4:48
bootloader
```

Notes:

- If you have multiple bootloaders, apply this procedure to the bootloader that contains the CableCARD module images.
- If the CableCARD module images are split across mutliple bootloaders, apply this procedure to the bootloader with the largest ACCT value.

Important: If the OOB CVT message cycle time is greater than 3 times the bootloader cycle time, you do not need to change the OOB CVT cycle time.

4 Convert the number to seconds.

Example: 4:48 is equal to 288 seconds.

5 Calculate the optimal cycle time for insertion of OOB CVT messages by dividing the number in half and adding sixty seconds.

Example: (288 seconds/2) + 60 seconds = 204 seconds.

Change Your OOB CVT Message Cycle Time

The process to change your OOB CVT message cycle time is as follows:

1 Add an environmental variable to your DNCS .profile file.

2 Bounce the OSM process.

This process is described in detail in the remaining pages of this document.

Adding the OOB CVT Environment Variable to the .profile File

The first step in the process is to add the **OSM_RF_CVT_PASSTHRU_SECONDS** variable to your .profile file on the DNCS.

Before you begin, you need the OOB CVT message cycle time that you found in ***Calculating the Optimum OOB CVT Message Cycle Time*** (on page 71).

1 Open an xterm window on the DNCS.

2 Type **cd /export/home/dncs** and press **Enter**. The /export/home/dncs directory becomes the working directory.

3 Open the .profile file in a UNIX text editor.

4 Add the following line to the end of the .profile file:

export OSM_RF_CVT_PASSTHRU_SECONDS=[OOB CVT message cycle time in seconds]

Note: Do not include the brackets **[ ]** in the variable.

Example: If your calculated OOB CVT message cycle time is 204 seconds, you would type the following:

export OSM_RF_CVT_PASSTHRU_SECONDS=204

5 Save the file and close the text editor.

6 Log out of the DNCS.

7 Log back into the DNCS.

8 In an xterm window, type **. ./.profile** to source the environment variable. Be sure to type a space between the first two periods.

9 Type **env | grep OSM** and press **Enter**. The system displays the environmental variables associated with the OSM process.

10 Is the OSM_RF_CVT_PASSTHRU_SECONDS included in the list and is the setting correct?

- If **yes**, you are finished with this procedure. Go to ***Bouncing the OSM Process*** (on page 73).
- If **no**, repeat this process from step 3.

Bouncing the OSM Process

After you have added the environment variable to the .profile file, you must bounce (stop and restart) the OSM process.

1 If the DNCS Control window is not already open, click the **Control** button in the DNCS area of the DNCS Administrative Console Status window.

Result: The DNCS Control window opens.

2 From the list of processes, click **osm**.

3 Click **Process > Stop Process**. A confirmation message appears.

4 Click **Yes** to stop the OSM process. This causes the indicator next to OSM to turn red.

5 From the list of processes, click **osm**.

6 Click **Process > Start Process**. The indicator next to osm turns green when the osm process has successfully restarted.

7 Go to ***Test the Updated OOB CVT Message Cycle Time*** (on page 74).

Test the Updated OOB CVT Message Cycle Time

We highly recommend that you test the change to your OOB CVT message cycle time to ensure optimum performance. Complete the following procedure to test the updated OOB CVT message cycle time.

1. Force a group of SSC DHCTs to download code (restage the SSC DHCTs - both the host and the CableCARD module).

   Notes:

   - Make sure that you are downloading the correct code for the SSC DHCT models you are staging.
   - Follow your site's procedures to force the download, or see *Downloading New Client Application Platform Installation Instructions* (part number 4003052) for instructions on how to force an SSC DHCT to download code.

2. Did the SSC DHCTs download the code correctly?

   - If **yes**, you are finished with this procedure.
   - If **no**, follow these steps:
     - Verify that you have the correct code version available for the SSC DHCTs.
     - Verify that you are using the correct OOB CVT message cycle time. Follow the procedure in ***Calculating the Optimum OOB CVT Message Cycle Time*** (on page 71) again.
     - Contact Cisco Services.

3

Staging SSC DHCTs

Introduction

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

In This Chapter

Overview

Staging SSC DHCTs consists of two processes. First, the host DHCT downloads the required software. Then, the M-Card module paired with the DHCT begins its download.

Important:

- These procedures assume that you have followed the recommendations in the first several chapters of the *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) regarding the staging process, staging preparations, staging area considerations, obtaining and loading EMM data, and staging DHCTs and CableCARD modules.
- Before staging SSC DHCTs, you must make sure that you do not enable Digital Interactive Services (DIS) or any other options on the Secure Services tab in the Set Up DHCT screen. If you do enable these options, you will provision the DHCTs when you batch load the EMMs, which prevents combo binding from working correctly and might prevent the DHCTs from properly staging. See ***Batch Loading EMM Files and Disabling DIS*** (on page 11) for more information.

The SSC Staging Process

1. The DHCT downloads its operating system. This occurs immediately when the DHCT is connected to the network. The software downloaded is specified for each DHCT model and revision combination. When the download is complete, the operating system code is written to the flash memory of the DHCT and the DHCT reboots.
2. The hard disk drive (HDD) of DVR-equipped DHCTs is initialized. After the first reboot, the DHCT performs HDD initialization. When this initialization is complete, the DHCT reboots.

   Note: This step is only applicable to DHCTs with DVRs, such as the Explorer 8300 series.
3. The inserted CableCARD module downloads its operating system. This occurs after a delay while the CableCARD module hunts for and identifies the correct download frequency. When the download is complete, the operating system code is written to the flash memory of the CableCARD module and the DHCT reboots.
4. The staging area sends a ModifyDhctConfig message through the billing system to the DNCS. The DNCS sends out the EMMs. The CableCARD downloads its EMMs.
5. The ModifyDhctConfig message also initiates the DNCS to place a bindAuth record on the BFS carousel. When the DHCT receives the message the binding process occurs.

6 Binding can occur automatically (if your system uses combo binding or autobinding) or it must be performed manually (if your system uses neither of these options). The availability of these binding options is dependent upon the type of DBDS connection that you use, as the following table shows.

Type of CableCARD/Host Combination	Connection Required	Binding Required
CableCARD module, inserted into subscriber's host	One-way	Manual
CableCARD module, inserted into subscriber's host	Two-way	Auto or Manual
SSC combination	Two-way	Combo, Auto, or Manual
SSC combination	One-way	Combo or Manual

How Long Does it Take?

The time it takes to completely stage an SSC DHCT and its paired CableCARD module depends on many factors, such as the overall BFS carousel download rate and the amount of software loaded on the carousel. The slower your overall download rate and the more software loaded on the carousel, the longer it will take to stage the SSC DHCT (and any other DHCT, for that matter).

It is important to keep only the currently active client code loaded on your DNCS. 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 of your BFS. Follow the procedures in ***Optimize Your System Performance for Downloads and Staging*** (on page 41) to keep unused and unneeded files off of your system.

In a typical DBDS, the complete SSC DHCT staging cycle includes the time it takes to perform the following functions:

- Download the software to the DHCT and to the CableCARD module.
- Write the downloaded software to the flash memories of the DHCT and the CableCARD module.
- Perform HDD-related operations (DVR-equipped DHCTs only).
- Reboot (standard DHCTs reboot 2 times during the process; DVR-equipped DHCTs reboot as many as 3 times during the process).

How Does the Download Affect the System?

Until you actually download the software across your system, there is no performance impact to your subscribers. After the system-wide download is started, any device being upgraded is unavailable while downloading the software. Therefore, we recommend that you perform Phase Three of these procedures during a maintenance window.

In addition to the outage caused by loading the software, two-way hosts and DHCTs will have to re-establish their network connections. This can cause interactive services to be temporarily unavailable after a software download.

Staging SSC DHCTs with Services

Follow these steps to stage new or RMA SSC DHCTs.

1. Scan the paired M-Card modules 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 and reboots. The DHCT LED displays one of the following states:
   - Brick mode (if used)
   - Clock (if brick mode is not used)
6. Connect the CABLE OUT port on each DHCT to a TV monitor so that you can monitor the staging of the CableCARD module.
7. After a few minutes, the CableCARD modules begin to download the required software from the DNCS.
8. Wait for the DHCTs to reboot and to indicate that the download is complete (the DHCT displays the clock).
9. 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 (clock or Brick mode).
10. At this time, binding should occur. Are you using manual binding?
    - If **yes**, follow the procedure in ***Manual Binding*** (on page 27) to bind the host DHCT and the CableCARD module.
    - If **no**, you are using either combo binding or autobinding. The binding process should proceed automatically.
11. Verify authorized channels.
12. Verify DVR functionality (if applicable) using the **LIST** key.
13. Does your business process require inventory DHCTs to be authorized for service?
    - If **yes**, go to step 14.
    - 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 14.

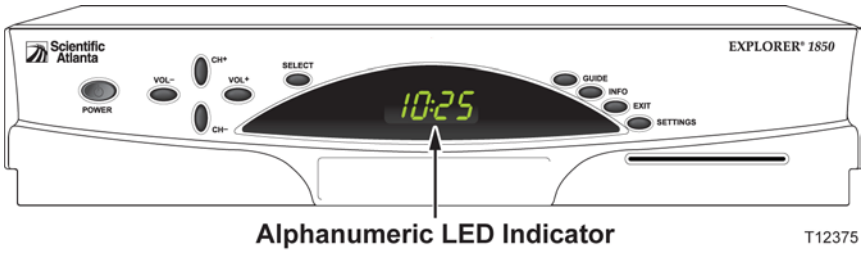
14 Disconnect the DHCTs and either return them as staged inventory to your warehouse or give them to technicians to install at the subscribers' locations.

Note: Some sites reverse steps 13 and 14 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 the DHCT 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.

LED Indicators Displayed During a Software Download

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.



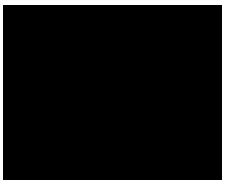
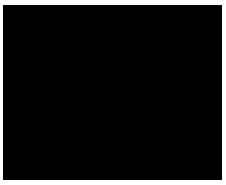
SSC DHCT Download

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.

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.

Stage	Alphanumeric LED Indicator	TV Monitor	Description
2		 or 	The rotating border appears when the DHCT boots into the OS.
3			**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			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.
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. The [000] indicates the QAM frequency.
6			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 		CLr and PR.00 indicate that the second part of the OS is installed into flash memory. Programs upper memory area with ResApp.

Stage	Alphanumeric LED Indicator	TV Monitor	Description
8			The wave appears after the DHCT resets to boot into the OS and the newly downloaded ResApp.
9		 or 	The rotating border appears when the DHCT resets and boots into the OS.
10			The LED is clear when the OS has started the ResApp. The DHCT is in an Off state.
11	 then  or 		If the Service Disconnect mode is activated, the DHCT displays the CableCARD module check then the Service Disconnect mode indicator. If the Service Disconnect mode is not activated, the DHCT displays the time.

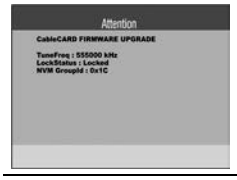
SSC CableCARD Module Download

The DHCT pauses before it launches the CableCARD staging process. The table in this section describes the screen displays during the CableCARD staging process.

Important: The alphanumeric LED indicators in the table in this section display only if you have installed software that includes one of the following numbers in the rom name:

- **0802** (or later) — 4250HDC
- **0902** (or later) — 8300HDC

If you are using an earlier release than those listed above, you must connect a TV monitor to the DHCT to monitor the CableCARD module download.

Stage	Alphanumeric LED Indicator	TV Monitor	Description
1	 and then 		The CableCARD module is preparing to start its download.
2	repeatedly through stage 8		This screen appears while the CableCARD module searches for the frequency of a QAM with a valid CVT table for that CableCARD module.
3			This screen appears after the CableCARD module has searched for, found, and locked in the frequency of a QAM with a valid CVT table for that CableCARD module.
4			The download progress is displayed as a percentage. This screen updates once every minute or so.
5			After the CableCARD module download is complete, the screen indicates that the OS is erasing the existing flash memory of the CableCARD module.
6			After the CableCARD module download is complete, the screen indicates that the OS is being installed into flash memory of the CableCARD module.

Stage	Alphanumeric LED Indicator	TV Monitor	Description
7			When the memory flashing is complete, this screen appears.
8			The DHCT (or host) will now reboot.
9	 and then 		The DHCT (or host) reboots.
10	 or 	 or 	The DHCT (or host) displays the Service Disconnect mode indicator (if activated). If the Service Disconnect mode is not activated, the DHCT (or host) displays the time.

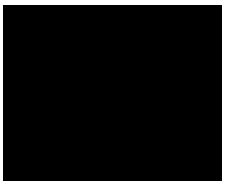
DHCTs with Three LED Indicators

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.

SSC DHCT Download

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.

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.

SSC CableCARD Module Download

The DHCT reboots and pauses before it launches the CableCARD staging process. The table in this section describes the screen displays during the CableCARD staging process.

Stage	LED Indicators	TV Monitor	Description
1	Two quick blinks, pause, repeats through stage 8		The CableCARD module is preparing to start its download.
2			This screen appears while the CableCARD module searches for the frequency of a QAM with a valid CVT table for that CableCARD module.
3			This screen appears after the CableCARD module has searched for, found, and locked in the frequency of a QAM with a valid CVT table for that CableCARD module.
4			The download progress is displayed as a percentage. This screen updates once every minute or so.
5			After the CableCARD module download is complete, the screen indicates that the OS is erasing the existing flash memory of the CableCARD module.

Stage	LED Indicators	TV Monitor	Description
6			After the CableCARD module download is complete, the screen indicates that the OS is being installed into flash memory of the CableCARD module.
7			When the memory flashing is complete, this screen appears.
8			The DHCT (or host) will now reboot.
9	The left LED blinks, the middle LED blinks, the right LED blinks and stays lit.		The DHCT (or host) reboots.
10	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.	 or 	The DHCT (or host) is in either Service Disconnect mode or standard mode.

DHCTs with Only POWER LED Indicators

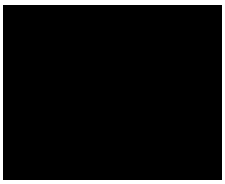
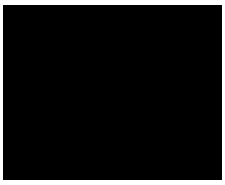
DHCTs with only POWER LED indicators display the codes associated with downloading, installing, and booting into the SARA as a series of flashing lights using the POWER LED indicator light on the front panel.

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

SSC DHCT Download

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.

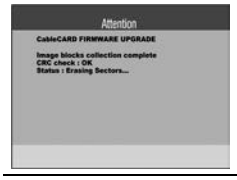
Stage	POWER LED Indicator	TV Monitor	Description
4	The light blinks once every half-second.		If the DHCT cannot acquire the CVT through a known good QAM frequency, it scans the recommended QAM frequencies. The LED displays FR.00 through FR.09 as the DHCT checks each of the ten recommended QAM frequencies. Go to stage 6 of this table.
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	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.

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

SSC CableCARD Module Download

The DHCT reboots and pauses before it launches the CableCARD staging process. The table in this section describes the screen displays during the CableCARD staging process.

Important: The POWER LED indicators in the following table will only display if you are using software version EXP2.1.0.0501 or later. Older versions of software will not display any indication during the CableCARD module download. If you are using an older version of code, you must connect a TV monitor to the DHCT to monitor the CableCARD module download.

Stage	POWER LED Indicator	TV Monitor	Description
1	Two quick blinks, pause, repeats through stage 8		The CableCARD module is preparing to start its download.
2			This screen appears while the CableCARD module searches for the frequency of a QAM with a valid CVT table for that CableCARD module.
3			This screen appears after the CableCARD module has searched for, found, and locked in the frequency of a QAM with a valid CVT table for that CableCARD module.
4			The download progress is displayed as a percentage. This screen updates once every minute or so.
5			After the CableCARD module download is complete, the screen indicates that the OS is erasing the existing flash memory of the CableCARD module.
6			After the CableCARD module download is complete, the screen indicates that the OS is being installed into flash memory of the CableCARD module.

Stage	POWER LED Indicator	TV Monitor	Description
7			When the memory flashing is complete, this screen appears.
8			The DHCT (or host) will now reboot.
9			The DHCT (or host) reboots.
10	For Service Disconnect (brick) mode, the light blinks eight times, pauses for half a second, and repeats. For normal operation, the light blinks four times, pauses, then repeats only once.	 or 	The DHCT (or host) 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.

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 185) 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 185) 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 185) 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.

Verifying the Staging Process

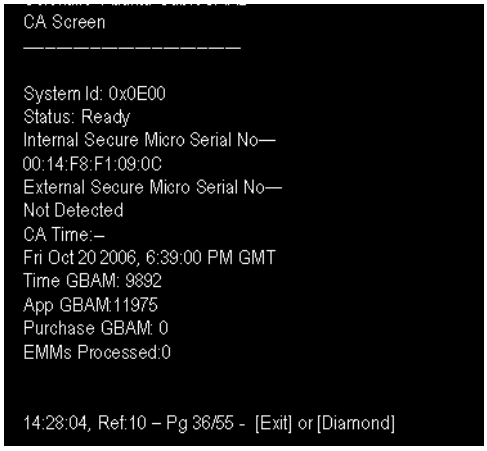
After the staging process is complete, use the following checklist to check each SSC DHCT and confirm that the staging process was correctly completed.

- ☐ **1** Verify that the correct current time appears on the front panel LED (if equipped with front-panel alphanumeric LEDs).
- ☐ **2** Verify that the SSC DHCT is receiving audio and video on the following channels:
  - Digital channels
  - Premium (copy-protected) channels (this determines whether the SSC DHCT and its paired CableCARD module have been bound)
- ☐ **3** Verify that the IPG channel banner is available on the bottom of the screen.
- ☐ **4** View the CableCARD diagnostic screens and verify that the ENTITLEMENT AGENTS / ISE[1] field displays **0x0000001**.
- ☐ **5** View 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 SSC DHCTs, use the Staging Toolkit to verify the following settings:
  - The Boot Status Indicator displays **111**.
  - All personal settings have been cleared and current site defaults are set.
  - There are no stranded IPPV events.

  Note: Refer to the **Returning DHCTs and CableCARD Modules to Service** chapter in the *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) for more information.

Verifying SSC DHCT Staging

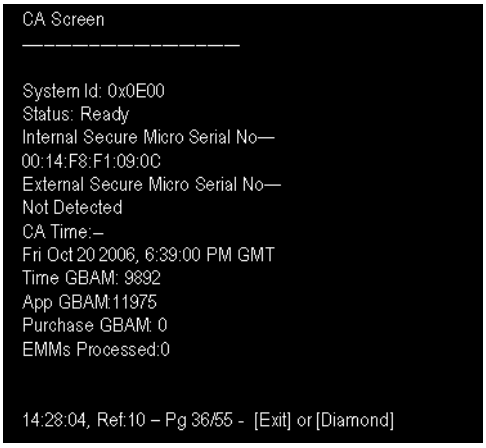
1 Display the first CA screen to verify the number of EMM messages received and validated by the CableCARD module. There should be at least 33 EMMs received and validated. If the number of EMMs processes is 0 (zero), the CableCARD module has yet to receive the EMM messages.



An example of the first CA screen from a CableCARD module, showing that the number of EMMs processes is **0**

2 Check the status of the conditional access for the CableCARD module. The CA status (Status) will be in one of the following states:

- **Ready**—Desired value; PowerKEY CA launched successfully
- **Not Ready-No CA Strm**—CA stream is not available
- **Not Ready-No Time GBAM**—CA stream is available but waiting for Time GBAMs
- **Not Staged**—CableCARD module is not provisioned in the headend
- **N/A**—Initialization or an internal problem while attempting to receive the status



An example of a CA screen showing the CableCARD conditional access status as **Ready** (Status: Ready)

Verify Binding Using the Staging Toolkit

Note: This section is for SARA systems only.

You can verify the host/CableCARD module binding process using the staging toolkit.

Verifying Binding Using the Staging Toolkit

Notes:

- You must have DVR 1.5.3.p3302/SARA_1.90.05.a109 or later to use this feature.
- This feature is only available on DHCTs with full display, alphanumeric LEDs.

1 Activate the staging toolkit using the instructions found in ***Staging Toolkit*** (on page 185).

2 Once you have activated the staging toolkit, press **5** to verify the status of the binding process between the host and the CableCARD module.

The following table shows the LED indicators and what these indicators mean.

LED Display	Description	Notes
	Error obtaining binding status	The toolkit could not identify the binding status.
	CableCARD module is busy with binding authentication process	The CableCARD module is in process of binding with the host. Wait a few minutes to see if they bind correctly.
	Not bound for CableCARD module reasons	Binding failed due to an error on the CableCARD module.
	Not bound, Host Certificate Invalid	Binding failed because the host was found on the CRL.
	Not bound, failed to verify Host Signature	Binding failed because the host signature was not verified.
	Not bound, failed to match AuthKey from Host Device	Binding failed because the Authorization Key on the host device did not match the Authorization Key on the CableCARD module.
	Binding Failed, other reasons	Binding failed due to other, unspecified errors.
	Validated, validation message received, authenticated, and the IDs match those in the current binding	Binding was successful.

	Not Validated, Binding Authorization Complete, Validation message not received yet	Binding has not completed, the host/CableCARD module pair is waiting on the Validation message to finalize the binding.
	Not Validated, validation revoked	Binding failed because the Validation message returned an invalid value.
 to 	Reserved	Reserved for future use.

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).

Moving an SSC DHCT to Another DNCS

There may be times when you need to move an SSC DHCT to another DNCS. At the new site, you need to download the correct EMM data for the SSC DHCT from the customer website. Refer to the *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) for more information on obtaining and loading EMM data into your DNCS.

4

Staging CableCARD Modules

Introduction

This chapter describes how to stage stand-alone CableCARD modules.

In This Chapter

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.

Partial Staging of CableCARD Modules

Unlike DHCTs, CableCARD modules should *not* be provisioned for services during the staging process. During staging, they should *only* be downloaded with software. For detailed steps about the staging procedure, see ***Manually Staging CableCARD Modules*** (on page 106).

Staging EMMs should *only* be sent when the module is installed in a host. Staging entitlement management messages (EMMs) should not be sent during the staging process unless each module is going to be individually, fully staged in a host.

Note: If you generate EMMs for CableCARD modules and the modules do not receive them within 30 days, the database optimizer deletes the EMMs from the DNCS. When the module is installed in a host after the 30-day time period, staged EMMs will not be sent. The modify DHCT config utility (modDhctCfg) can be used to address this condition (modDhctCfg -s [MAC]). Refer to the appropriate *DBDS Utilities Installation Instructions and DNCS Utilities Guide* for details.

Manually Staging CableCARD Modules

The first step in staging CableCARD modules is to load the EMM CD (or download the EMMs from our FTP site) and confirm that the correct CableCARD module type exists. Refer to *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) for more information.

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

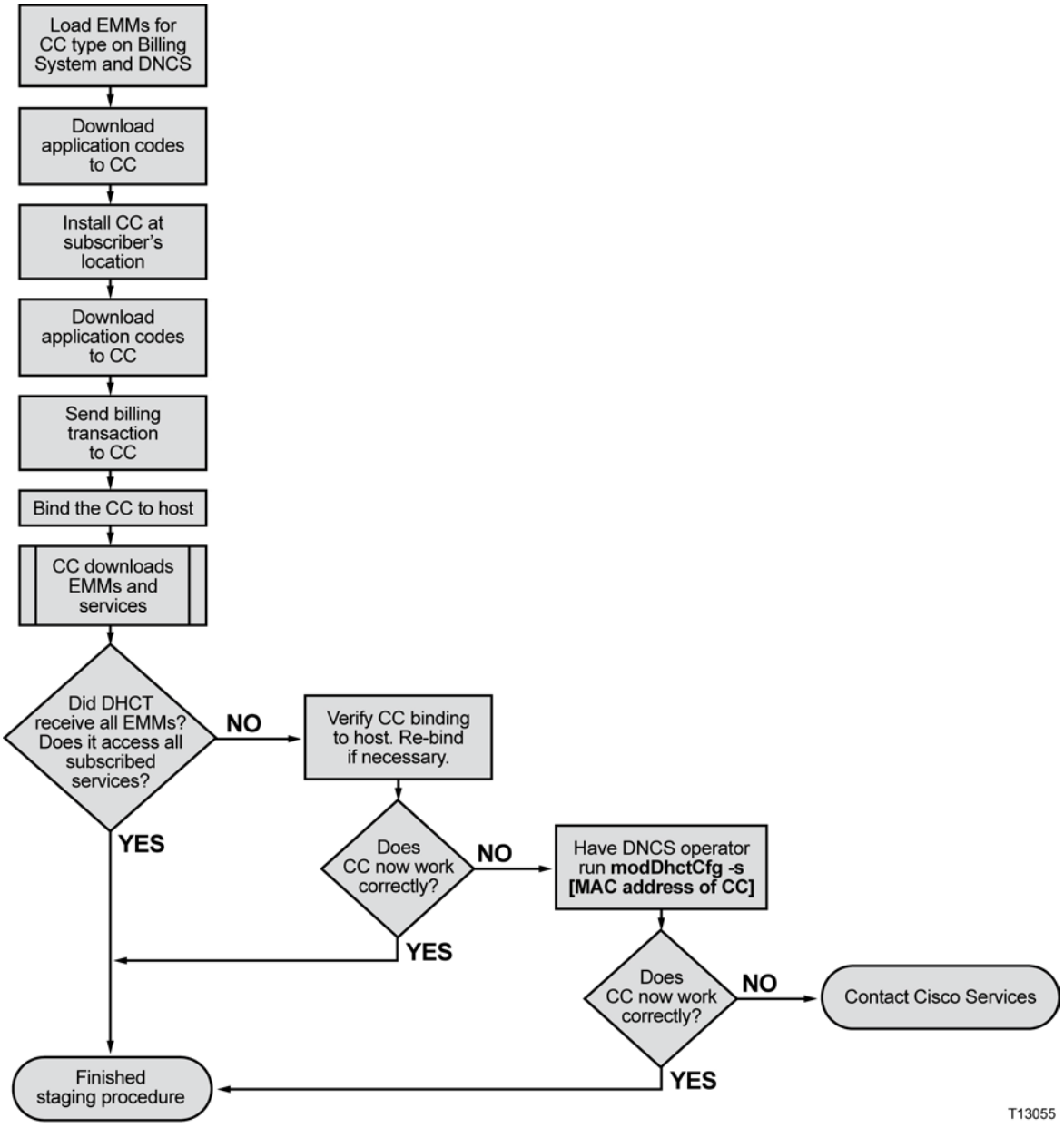
- If **yes**, go to ***Stage CableCARD Modules with No Billing Action*** (on page 106).
- If **no**, go to ***Stage CableCARD Modules with Billing Action*** (on page 108).

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 108).

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.

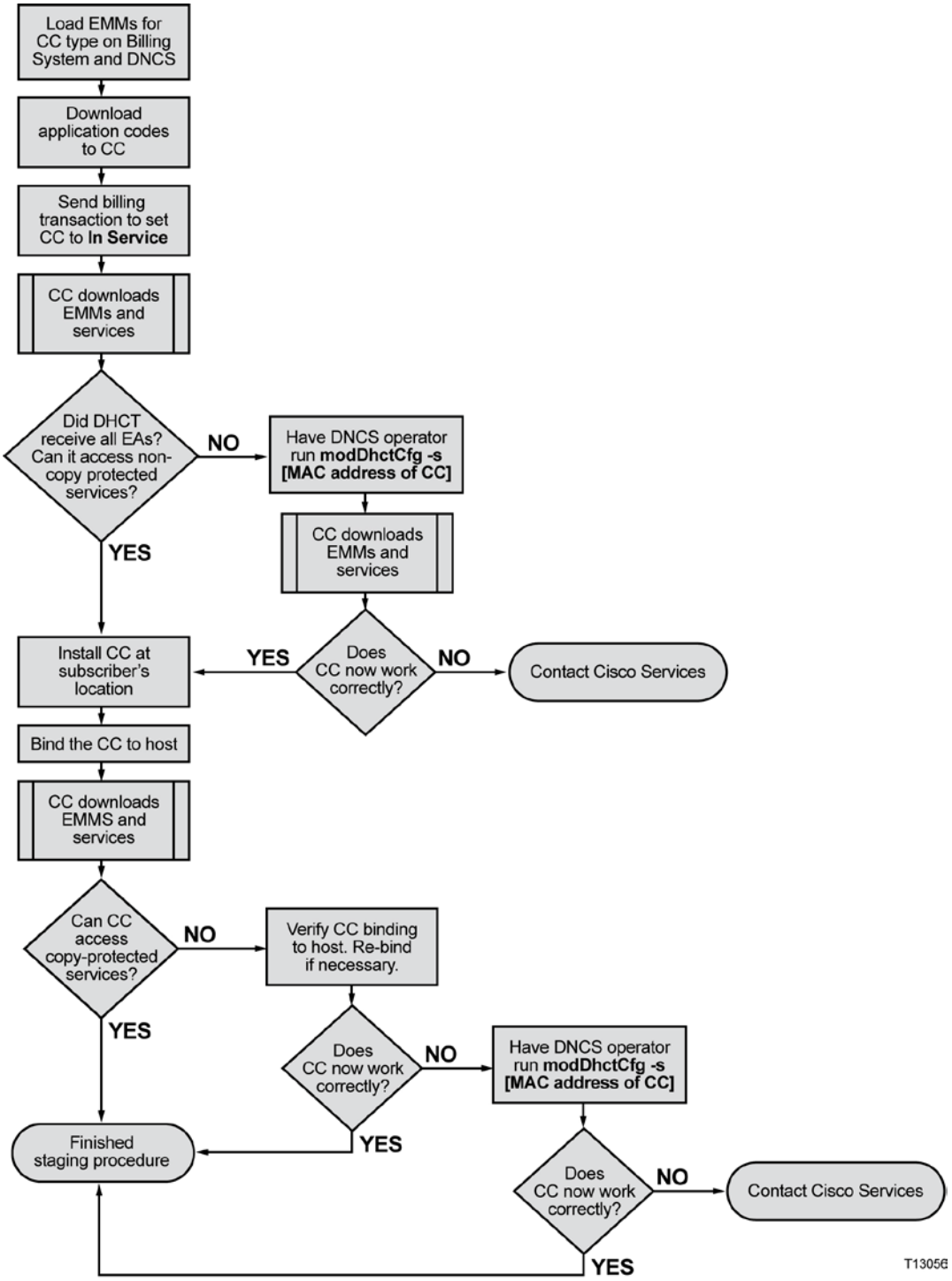
1. Download the application code to the CableCARD module.
2. Is the CableCARD module going directly to a subscriber's location?
   - If **yes**, go to step 3.
   - If **no**, store the CableCARD module for future use.
3. At the subscriber's location, insert the CableCARD module into the subscriber's 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 106).

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

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

5

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 137) for contact information.

In This Chapter

Overview

The procedures in this chapter are specific to troubleshooting SSC DHCTs. Other issues may arise that are related to either the installed CableCARD module or the DHCT itself. Refer to the following documents for more information on these other issues:

- *Best Practices for Using Multi-Stream CableCARD Modules Operation and Maintenance Guide* (part number 4005658)
- *Downloading New Client Application Platform Installation Instructions* (part number 4003052)
- *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375)
- *Explorer*® Digital Home Communications Terminal Troubleshooting Guide (part number 717867)
- *M-Card and S-Card Diagnostic Screens on a TV Host: A Reference Guide* (part number 4015203)
- *Understanding Diagnostic Screens for the Explorer DHCTs Application Guide* (part number 749244)

Most of the procedures and troubleshooting information is in reference to the SARA software. For information on troubleshooting the Axiom software, see the following appendices and documents:

- ***CDL Error Codes*** (on page 157)
- ***CableCARD Module Validation Status Codes*** (on page 163)
- ***Host - CableCARD Module Interface Errors*** (on page 167)
- *Troubleshooting Guide for Axiom Software Stacks* (part number 4036280)
- *Understanding Diagnostic Screens for 8200, 85xx, and 45xx DHCTs in an Axiom tru2way Environment Application Guide* (part number 4011047)

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 137) for information on returning products to us for repair.

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.
- If you must return a DHCT to us for repair, always use a repair tag to properly identify the problem. You can fill out and submit a repair tag (RMA form) on the customer self-service website. See ***Customer Information*** (on page 137) for instructions to access the customer self-service website.

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 the SSC DHCT will not completely stage, verify that you can access the CableCARD module diagnostic screens. If you cannot access these screens, there is a problem in the communication between the CableCARD module and the host DHCT.

If you stage an SSC DHCT and the CableCARD module 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 an SSC DHCT module and the EMM count does not meet the required number, you should send an instant hit to the paired CableCARD module. See ***Send Instant Hits*** (on page 126) 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 CableCARD module. 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 CableCARD module. If the numbers do not match, return the DHCT to us for repair.
- The DHCT is on the Fast Refresh List (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 CableCARD module]

  This command resets the CableCARD module 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 the ISE errors continually increment, ask the DNCS operator to verify that the DNCS MAC address and the Secure Micro Address match the CableCARD module. Then, ask the DNCS operator to run the **modDhctCfg -s [MAC address of the CableCARD module]** command. If this does not work, contact Cisco Services to obtain new EMMs for the SSC DHCT and try to stage the SSC DHCT again.

DHCT Errors Solutions Table

The following table lists some common symptoms, the corresponding LED display, and possible solutions to the problem. These symptoms and solutions are for DHCTs with full display, alphanumeric LEDs. For DHCTs with single- or triple-LEDs, see ***DHCT Errors Solutions Table for Single- and Triple-LED DHCTs*** (on page 121).

Note: If you must return a DHCT to us for repair, see ***Return Products for Repair*** (on page **Error! Bookmark not defined.**) for information.

Symptom	Possible Solution
DHCT displays the following symptoms: ■ No display ■ **POWER** button does not work	**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: ■ No display ■ **POWER** button works	**1** Follow these steps: **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.

Symptom	Possible Solution
DHCT will not stage	**1** Can you access any of the CableCARD module diagnostic screens? **a** If **yes**, continue with step 2. **b** If **no**, there is a problem in the communication between the CableCARD module and its host DHCT. Contact Cisco Services. **2** Does the diagnostic screen for the host DHCT display the CableCARD RF MAC address (rather than the DHCT RF MAC address)? **a** If **yes**, follow these steps: **i** Verify that the DHCT is connected to a known good RF cable. **ii** Verify that the DHCT is in the correct download group on the DNCS. **iii** If these do not remedy the problem, contact Cisco Services. **b** If **no**, there is a problem in the communication between the CableCARD module and its host DHCT. Contact Cisco Services.
DHCT displays one of the following constantly: ■ **br.xx** ■ **er.xx** ■ **xxxx**	**1** Reboot the DHCT by following these steps: **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: **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	Possible Solution
DHCT will not download, stays in hunt mode, displaying the following constantly: ■ **h.xxx**	**1** Connect the DHCT to a known good RF cable. **2** Power cycle the DHCT. **3** Force a download by following these steps: **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** Have the DNCS operator confirm that the hardware type on the DHCT label is associated with the correct ROM version file on the DNCS. Compare to a known good DHCT of the same type. **5** 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**	**1** Force a download by following these steps: **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 DNCS 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	**1** Power cycle the DHCT. **2** Reformat the hard drive using the Staging Toolkit by following these steps: **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	Possible Solution
DHCT stuck, displaying the following constantly: ■ **dIAG**	**1** Force a download by following these steps: **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 (SARA only), displaying the following constantly: ■ **– – – –** (four dashes)	**1** Follow these steps: **a** Confirm that the CableCARD module MAC address matches the billing MAC address and that the CableCARD module is authorized for service. **b** Ask the DNCS operator to correct any mis-match and send a hit to the CableCARD module. **2** See ***PowerKEY/EA Issues*** (on page 131) 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: – **S2. Stays in Brick Mode (– – – –)** – **S1. No EMMs/ISE/EA**
Front panel LED displays  for 1 second before the DHCT reboots	■ 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: ■ **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).**
Card Status on CableCARD Information diagnostic screen shows **Reset**	**1** Power cycle the DHCT. **2** Contact Cisco Services.

Symptom	Possible Solution
Tuner, QAM, or FDC levels are less than range on the Status Summary, Current FDC, Current RDC, or Current QAM diagnostic pages	**1** Connect the DHCT to a known good RF cable. **2** Power cycle the DHCT. **3** Connect a good DHCT of the same type to confirm that you have a good network connection.
ITFS, WDIDE, AVFS shows **Not Ready** or **Not Initiated** on the DVR Status diagnostic page	**1** Power cycle the DHCT. **2** Reformat the hard drive using the Staging Toolkit by following these steps: **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.

DHCT Errors Solutions Table for Single- and Triple-LED DHCTs

The following table lists the single- and/or triple-LED display, the equivalent alphanumeric LED display (if appropriate) and possible solutions to the problem. These symptoms and solutions are for DHCTs with one or three LEDs. For DHCTs with full display, alphanumeric LEDs, see ***DHCT Errors Solutions Table*** (on page 117).

Note: If you must return a DHCT to us for repair, see ***Return Products for Repair*** (on page **Error! Bookmark not defined.**) for information.

Symptom	Equivalent	Possible Solution
POWER LED blinks on for one second, off for one second, repeats (continuously)	**cA.rd/dn.Ld** - CableCARD module download error	**1** Check the RF levels at the download frequency. If necessary, adjust the levels. **2** Verify that the image is on the BFS. If not, contact the DNCS operator to troubleshoot. **3** If these steps do not work, return the DHCT to us for repair. Mark the repair tag with D11. CableCARD Download Incomplete.

Symptom	Equivalent	Possible Solution
DHCT displays the following symptoms: ■ No display ■ **POWER** button does not work (POWER LED on or off)	N/A	**1** Follow these steps: **a** Connect the DHCT AC input to a known good AC source. **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 F1. No Power / Dead.
DHCT displays the following symptoms: ■ No display ■ **POWER** button works	N/A	**1** Follow these steps: **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.

Symptom	Equivalent	Possible Solution
POWER LED is on for two seconds, off for two seconds, repeats (continuously)	**Br.xx** - OS trap	**1** Reboot the DHCT by following these steps: **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: **a** Unplug the DHCT power cord from the power receptacle. **b** Plug the DHCT power cord into the power receptacle while pressing and holding the **POWER** button until either the POWER LED (on single-LED DHCTs) or the REMOTE LED (on triple-LED DHCTs) begins blinking. **c** Press the POWER button again so the LED blinks faster. In a few seconds, the DHCT will begin downloading code. **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	Equivalent	Possible Solution
DHCT blinks 8 times quickly, pauses, repeats (continuously) [SARA only]	**– – – –** (four dashes, stuck in Brick mode)	**1** Follow these steps: **a** Confirm that the CableCARD module MAC address matches the billing MAC address and that the CableCARD module is authorized for service. **b** Ask the DNCS operator to correct any mis-match and send a hit to the DHCT and CableCARD module. **2** See ***PowerKEY/EA Issues*** (on page 131) 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: – **S2. Stays in Brick Mode (– – – –)** – **S3. Invalid Sub Expire Date** – **S1. No EMMs/ISE/EA**
Single-LED DHCT: POWER LED blinks once every half-second (continuously) **Triple-LED DHCT:** LEDs blink twice, rotate left, repeats (continously)	**h.xxx** - DHCT will not download, stays in hunt mode	**1** Connect the DHCT to a known good RF cable. **2** Power cycle the DHCT. **3** Force a download by following these steps: **a** Unplug the DHCT power cord from the power receptacle. **b** Plug the DHCT power cord into the power receptacle while pressing and holding the **POWER** button until either the POWER LED (on single-LED DHCTs) or the REMOTE LED (on triple-LED DHCTs) begins blinking. **c** Press the POWER button again so the LED blinks faster. In a few seconds, the DHCT will begin downloading code. **4** Have the DNCS operator confirm that the hardware type on the DHCT label is associated with the correct ROM version file on the DNCS. Compare to a known good DHCT of the same type. **5** If these steps do not work, return the DHCT to us for repair. Mark the repair tag with D6. DHCT in Hunt Mode (hXXX).

Symptom	Equivalent	Possible Solution
Single-LED DHCT: POWER LED blinks twice, pauses, repeats (continuously) **Triple-LED DHCT:** LEDs blink three times, rotate left, repeats (continously)	**r.xxx** - DHCT will not download, stays in hunt mode	**1** Force a download by following these steps: **a** Unplug the DHCT power cord from the power receptacle. **b** Plug the DHCT power cord into the power receptacle while pressing and holding the **POWER** button until either the POWER LED (on single-LED DHCTs) or the REMOTE LED (on triple-LED DHCTs) begins blinking. **c** Press the POWER button again so the LED blinks faster. In a few seconds, the DHCT will begin downloading code. **2** If a known good DHCT of the same type and revision does not download, contact your DNCS 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	N/A	**1** Power cycle the DHCT. **2** If these steps do not work, return the DHCT to us for repair. Mark the repair tag with D5. Constantly Resets / Reboots.

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 CableCARD modules.

Sending an Instant Hit to a CableCARD Module

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
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.

OS and ResApp Downloads

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

Note: If you must return a DHCT to us for repair, see ***Return Products for Repair*** (on page **Error! Bookmark not defined.**) for information.

Symptom	Possible Solution
Monitor displays the MMI screen, **combo binding only**	**1** Ask the DNCS operator to confirm that the CableCARD ID and the Host ID are present in the DNCS GUI. If not, ask the DNCS operator to enter the IDs to bind the CableCARD module to the host. **2** Unbind the CableCARD module from the host. Rebind the CableCARD module to the host. **3** If these do not remedy the problem, contact Cisco Services.
Monitor displays the MMI screen, **auto binding only**	**1** Is the IP address for the CableCARD module present on the IP Service diagnostic screen? – If **yes**, verify that the RF levels for the QPSK are within the acceptable limits. – If **no**, access the DNCS GUI and verify and/or correct the following settings: ▪ Admin Status for the CableCARD module is set to In Service Two Way (DHCT Provisioning window) ▪ Autobinding is enabled. See ***Setting Up the DNCS for Autobinding*** (on page 23) for more information. **2** If these do not remedy the problem, contact Cisco Services.
Monitor displays the MMI screen, **manual binding only**	**1** Ask the DNCS operator to enter the CableCARD module ID and the host ID into the DNCS GUI to bind the CableCARD module to the host. **2** Unbind the CableCARD module from the host. Rebind the CableCARD module to the host.
SARA blue screen (SARA only)	**1** Follow these steps: **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.

Symptom	Possible Solution
CableCARD firmware upgrade screen shows that the QAM is not locked on frequency	1 Verify that the QAM is powered on. 2 If the QAM is on, verify that the QAM levels are within the acceptable limits. 3 Have the DNCS operator confirm that the hardware type on the DHCT label is associated with the correct ROM version file on the DNCS. Compare to a known good DHCT of the same type. 4 If these do not remedy the problem, contact Cisco Services.
CableCARD firmware upgrade screen shows that download not complete	1 Verify the RF levels at the download frequency. Adjust if necessary. 2 Remove the ROM image from the BFS then reload the image back onto the BFS. 3 If these do not remedy the problem, contact Cisco Services.
Monitor displays the following: ■ **Video Recorder Not Ready**	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 (SARA only): ■ **Disk Trouble - Problems with the program storage disk**	1 Power cycle the DHCT. 2 Reformat the hard drive using the Staging Toolkit by following these steps: **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
Monitor displays the following (SARA only): ■ **Disk Trouble - Unrecoverable Write Error**	**1** Power cycle the DHCT. **2** Reformat the hard drive using the Staging Toolkit by following these steps: **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.
Monitor displays the following: ■ Video macroblocking ■ Tiling or freezing ■ Snowy, grainy video	**1** Follow these steps: **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: – **V2. Macroblocking/Tiling/Freezing** – **V4. Poor/No Color** – **V5. Snowy/Grainy/Noisy Picture**
No video	**1** Follow these steps: **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 (SARA only). **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.

Symptom	Possible Solution
DHCT does not show premium channels, but does show other channels	**1** Follow these steps: **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 ***PowerKEY/EA Issues*** (on page 131) 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.
DHCT shows some copy-protected channels, but not all copy-protected channels it is authorized to receive	The CableCARD module and the host are not bound (the host can still receive copy-protected channels that are designated *copy freely* without being bound) or the CableCARD module did not receive its total allotment of EMMs. **1** Ask the DNCS operator to enter the IDs to bind the CableCARD module to the host. **2** Unbind the CableCARD module from the host. Rebind the CableCARD module to the host. **3** Ask the DNCS operator to perform a **modDhctCfg -s [MAC address of the module]** on the CableCARD module. **4** If these steps do not work, return the DHCT to us for repair. Mark the repair tag with S5. No Premium Channels.
Front panel LED displays  for 1 second before the DHCT reboots	■ 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: ■ **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.

Note: If you must return a DHCT to us for repair, see ***Return Products for Repair*** (on page **Error! Bookmark not defined.**) for information.

Symptom	Type of DHCT	Possible Solution
No Entitlement Agent (EMMs)	Unstaged	**1** Does the CableCARD module's MAC address match the MAC address recorded in the billing system? – **If yes**, follow these steps: **i** Confirm that the actual MAC address for the module matches the MAC address recorded in the DNCS. **ii** Confirm that the Secure Micro Address for the module matches the Secure Micro Address recorded in the DNCS. **iii** Ask the DNCS operator to perform a **modDhctCfg -s [MAC address of the module]** on the CableCARD module. **iv** Stage the CableCARD module again. – **If no**, follow these steps: **i** Ask the DNCS operator to correct any existing mis-matches. **ii** Stage the CableCARD module again. **iii** Go to step 2 if these actions do not remedy the situation. **2** Follow these steps: **a** Take the SSC DHCT out of service. **b** Try to stage the SSC DHCT again. **3** Follow these steps: **a** Delete the SSC DHCT from the DNCS. **b** Contact us to have new EMMs built. **c** Try to stage the SSC 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	Type of DHCT	Possible Solution
Sub Expire shows expired or past date	Deployed	**1** Follow these steps: **a** Confirm that the CableCARD module is authorized for service in the billing system. **b** Confirm that the CableCARD module is authorized for service in the DNCS. **c** Send an instant hit to the CableCARD module. **d** Stage the CableCARD module again. **2** Follow these steps: **a** Ask the DNCS operator to perform a **modDhctCfg -s [MAC address of the module]** on the CableCARD module. **b** Stage the CableCARD module 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	Unstaged or Deployed	**1** Follow these steps: **a** Confirm that the CableCARD module is authorized for service in the billing system. **b** Confirm that the CableCARD module is authorized for service in the DNCS. **c** Send an instant hit to the CableCARD module. **d** Stage the CableCARD module again. **2** Follow these steps: **a** Ask the DNCS operator to perform a **modDhctCfg -s [MAC address of the module]** on the CableCARD module. **b** Stage the CableCARD module 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	Type of DHCT	Possible Solution
No Incoming EMMs	Unstaged	**1** Does the DNCS have the EMMs loaded for the CableCARD module? **a** If **yes**, follow these steps: **i** Ask the DNCS operator to perform a **modDhctCfg -s [MAC address of the module]** on the CableCARD module. **ii** Stage the CableCARD module again. **b** If **no**, contact us to get the correct EMMs. **2** Does the CableCARD module's MAC address match the MAC address recorded in the billing system? – **If yes**, follow these steps: **i** Confirm that the actual MAC address for the module matches the MAC address recorded in the DNCS. **ii** Confirm that the Secure Micro Address for the module matches the Secure Micro Address recorded in the DNCS. **iii** Ask the DNCS operator to perform a **modDhctCfg -s [MAC address of the module]** on the CableCARD module. **iv** Stage the CableCARD module again. – **If no**, follow these steps: **i** Ask the DNCS operator to correct any existing mismatches. **ii** Stage the CableCARD module again. **iii** Go to step 3 if these actions do not remedy the situation. **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	Deployed	**1** Follow these steps: **a** Confirm that the DHCT boots into two-way mode (that it has an IP address listed on the diagnostic screens, if applicable). **b** Ask the DNCS operator to send an instant hit to the CableCARD module. **c** Stage the CableCARD module 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	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	Unstaged	**1** Do the MAC addresses and Secure Micro for the CableCARD module match what is recorded in the DNCS? – If **yes**, follow these steps: **i** Ask the DNCS operator to perform a **modDhctCfg -s [MAC address of the module]** on the CableCARD module. **ii** Stage the CableCARD module again. – If **no**, continue with step 2. **2** Follow these steps: **a** Delete the SSC DHCT from the DNCS. **b** Contact us to have new EMMs built. **c** Try to stage the SSC 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.**

CableCARD Module Errors

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).

Troubleshooting CableCARD Modules

Issue	Probable Cause	What to Do
Black screen appears on channels during tuning	No EMMs; EMMs do not increment to 33 (or to the number that your site requires) and/or the PowerKEY status is not Ready	1 Verify that the CableCARD module has Key certificates (DHCT > by MAC Address > Open > Service Element). 2 Verify that the CableCARD module has packages and DMS is enabled. 3 Ask the DNCS operator to send an instant hit to the CableCARD module. 4 If the instant hit does not work, re-stage the CableCARD module (xterm window: type **modDhctCfg —s <mac address>**). **Note:** If the file does not update, contact Cisco Services.
Freezing or black screen on channels	Card not bound to host or No EMMs; CP Auth Received does not appear in the CP Auth Status of the SA CableCARD CP Info diagnostic screen	1 Verify that the CableCARD ID and the Host ID are present in the DNCS GUI. If not, have the DNCS operator enter the IDs to bind the CableCARD module to the host. 2 Verify that the following file has an updated time stamp (xterm window: type **ls -l /dvs/dvsFiles/CCardServer/PodData**). 3 Reboot the DHCT by following these steps: **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. **d** Turn the DHCT power on.

Issue	Probable Cause	What to Do
Channels are skipped during tuning	Channel map has not completely updated or You are not authorized to receive the skipped channels (SARA only)	Reset or reboot the CableCARD module using one of the following methods: – Reset through the host device – Reboot (power off and then on) the host
Barker displays that the CableCARD module is invalid	An unsupported or failed CableCARD module has been inserted into the host	**1** Power cycle the DHCT. **2** Replace the CableCARD module with a known good module.
DVR-equipped host does not play back content	The host does not have a CableCARD module installed (SARA only)	**1** Insert a CableCARD module into the host. **2** Reset or reboot the CableCARD module using one of the following methods: – Reset through the host device – Reboot (power off and then on) the host
Host reboots when CableCARD module is inserted	This is normal behavior	No action is required.

6

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

Bootloader LED Error Codes

Introduction

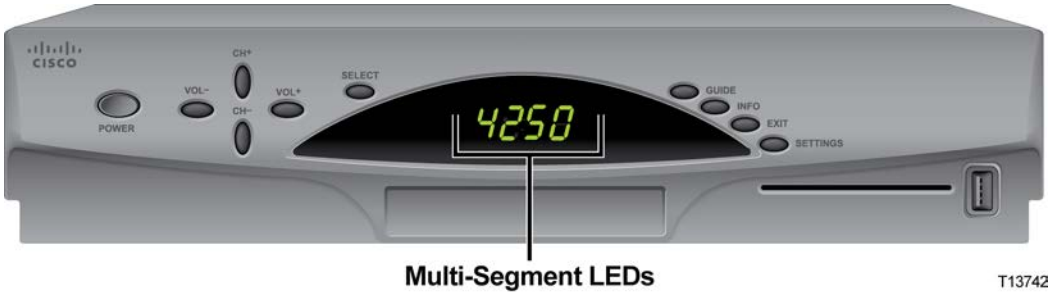
This appendix discusses how the error codes that might display on the DHCT. These error codes include those that display on multi-segment-LED, three-LED, and single-LED DHCTs. This appendix also includes a section on how to read the error codes and what the error codes indicate.

In This Document

Bootloader Error Codes for Multi-Segment-LED DHCTs

Low-level bootloader error codes on the multi-segment-LED set-top display if there is an error condition detected by the bootloader when the set-top boots, or when it loads or installs software.

The set-top displays the error code using the multi-segment LEDs on the face of the set-top.



Error Codes

The following table contains the bootHi error codes that might display on the DHCT.

LED Message	Error Indication
Addr	■ Image won't fit in flash memory. Displayed by BSTRAP.IMG (c51 command and either xA2, xA3, xA3p, or xG2 protocols). ■ RAM load address is not in RAM. Displayed by BSTRAP.IMG (c54 command with "a" option and either xA2, xA3, xA3p, or xG2 protocols). Try a different address with the "a" option. ■ RAM offset to start address is too large. Displayed by BSTRAP.IMG (c54 command with "s" option and either xA2, xA3, xA3p, or xG2 protocols). Try a different offset with the "s" option.
AuLd	The bootloader or the universal bootstrap is waiting for the host (PC) to respond to its attempt to initiate a download over the serial port. Typically, this means that the host was not ready (the PC-side (XLD) was not started first). Displayed by bootloader or BSTRAP.IMG.
br.2A	The ASIC in the DHCT could not be identified. Press the POWER key to initiate a soft reset. Displayed by BSTRAP.IMG (xA2, xA3, xA3p, or xG2 protocols). The universal bootstrap can identify Mercury, BIP2, QBIP, QBIPE, Laurasia, Titan, Pangea, and Atlas ASICs.

CLr_	Displays while the flash sectors are being erased, before programming. The received image's CRC was valid, and flash programming will begin soon.
dala	"Data move" save error. Either the NVM copy is too big to save (greater than 256 KB), the CRC of the data is invalid, or there is no data to save because a "data move" has not been done on this DHCT. Displayed by BSTRAP.IMG (xA2, xA3, xA3p, or xG2 protocols with "d" option). Try again without the "d" option.
donE	Displayed by the BSTRAP.IMG when the upload is complete. Reset the DHCT to re-gain control of it.
Er.00	■ MIPS bootloaders: Clock initialization error. The bootloader is unable to initialize a system PLL. ■ SPARC bootloaders: Ethernet link initialization failed. Either the Ethernet option board is not in the DHCT, is not properly seated in the connector, or the board is defective. Displayed by BSTRAP.IMG (xA2, xA3, xA3p, or xG2 protocols).
Er.01	■ MIPS bootloaders: Error loading the "BootHi" portion of the bootloader. ■ SPARC bootloaders: Transfer error during download. XLD has retransmitted the same packet 3 times, but the DHCT cannot validate the packet. Check all serial or Ethernet connections and try again. Displayed by BSTRAP.IMG (xA2, xA3, xA3p, or xG2 protocols).
Er.02	■ MIPS bootloaders: A memory test of the RAM reserved for the "Boothi" portion of the bootloader failed. ■ SPARC bootloaders: The image would not fit in NVM or the image CVC failed. Displayed by BSTRAP.IMG (xA2, xA3, xA3p, or xG2 protocols).
Er.03	Signature error.
Er.05	During an upload of memory contents to the PC, the PC failed to acknowledge that it received a data packet from the DHCT within the 3-second timeout limit. Correct the problem on the PC, reset the DHCT, and try again. Displayed by BSTRAP.IMG (c55 command with xA2, xA3, xA3p, or xG2 protocols).
Er.06	Transfer error during upload. The DHCT has transmitted the packet 3 times, but XLD cannot validate the packet. Check all connections and try again. Displayed by BSTRAP.IMG (c55 command with xA2, xA3, xA3p, or xG2 protocols).
Er.07	■ Disk access not supported. The DHCT does not support transfers to disk because its disk drive is either missing or not connected. Displayed by BSTRAP.IMG (c57 command with xA2, xA3, xA3p, or xG2 protocols). ■ Command not supported. Only RAM-resident or disk-based bootloaders support this command. Displayed by BSTRAP.IMG or BSTR60.IMG.

Er.20	Transfer error during download. XLD has transmitted the packet 3 times, but the DHCT cannot validate the packet. Check all serial or Ethernet/USB connections and try again. Displayed by BSTRAP.IMG (c57 command with xA2, xA3, xA3p, or xG2 protocols).
Er.21	Invalid transfer parameters. The protocol (xA2, xa3p, or xG2) might have been omitted, and the command line is telling the disk-based bootloader to write to flash (which it cannot do). Specify the appropriate 2-step download protocol and try again. This error might also indicate that the cable connecting the serial ports has poor electrical contact. Verify that the connectors are properly plugged in and that there is no damage to the connection socket.
Er.22	The transfer failed because the disk-based bootloader could not verify the CRC of the entire received image. Check all serial or Ethernet/USB connections and try again.
Er.23	■ Invalid address. Choose a different address and try again. Displayed by the disk-based bootloader if the request was for a RAM download (c53 or c54) using an address ("a" option) that is too low or too high (either below RAM or in the area reserved for the bootloader, or high enough that there is not enough room for the image to fit in RAM). ■ Wrong BSTRAP. In some DHCTs, you will see this error if you omit the eBSTR60.IMG option on the XLD command line. Add this option to the XLD command and try again.
Er.24	Invalid start offset. Choose a different offset and try again. Displayed by disk-based bootloader if the request was for a RAM download with an offset ("s" option), but the offset places the code start outside the image.
Er.25	Invalid NVM record. Displayed by the disk-based bootloader if an NVM download was requested (c52 command) but one of the records in the file is invalid.
Er.26	Unsupported image type. Displayed by the disk-based bootloader when the c57 command is used and the value specified by the "s" option is not between 0 and 3: ■ 0 = OS/SARA ■ 1 = Monitor ■ 2 = DIAGs ■ 3 = OS/SARA Change the "s" option and try again.

Er.27	Image overflow. The image is too large to fit into the area reserved for that image type. This is typically caused by choosing the wrong image type ("s" option): ■ 0 = OS/SARA (60 MB) ■ 1 = Monitor (1 MB) ■ 2 = DIAG (3 MB) ■ 3 = OS/SARA (60 MB) Change the "s" option and try again.
Er.30	Image length wrong. Displayed by the disk-based bootloader when the image length specified in the signature block is different from the real length of the received image.
Er.31	Invalid CRC. Displayed by the disk-based bootloader when the CRC in the signature block cannot be verified.
Er.32	Incoherent signature. Displayed by the disk-based bootloader when the offset to code start is outside the image, or when other signature values are incorrect.
Er.33	Expanded image CRC error. Displayed by the disk-based bootloader when a compressed image is expanded and its CRC cannot be verified.
Er.34	Expansion overrun. Displayed by the disk-based bootloader when the expanded image overflows available memory.
Er.35	Expansion stop-code failure. Displayed by the disk-based bootloader if the stop-code was not found at the end of the compressed image during expansion.
Er.3F	Bootloader replacement error. Displayed by the upgradable, RAM-based bootloaders when the new image is too large, or when the CRC is incorrect.
Er.41	Bootloader tuner communication error.
Er.45	TUA6130 detection error. The DHCT's NVM HwChipVersion indicates the presence of a TUA6130 tuner, but it was not found.
Er.50	Disk not detected. The DHCT is supposed to have a disk drive, but it did not respond during DHCT initialization. Displayed by the disk-based bootloader.
Er.51	Disk not responding. The disk drive was found during initialization, but it is not responding to commands. Displayed by the disk-based bootloader.
Er.52	Disk timeout. The disk drive did not finish the commanded operation in the allotted time period.
Er.53	Error reported from disk. Operation finished with an error reported by the disk drive controller.
Er.54	DMA error during disk write. The DMA operation did not finish during the write operation.
Er.55	DMA error during disk read. The DMA operation did not finish during the read operation.
Er.56	Uncorrectable data errors have been reported from the disk drive.

Er.57	Disk read failure. The bootloader has received uncorrectable errors from the disk drive. To recover, the bootloader attempts to overwrite the bad sectors. This overwrite process was successful.
Er.58	Disk operation aborted.
Er.59	An error has been reported from the SATA PHY layer.
Er.5A	Disk addressing error.
Er.60	Basic disk storage format has been established.
Er.61	The bootloader attempted to format the disk, but it was not successful.
Er.62	The bootloader could not find a valid image in the bootable image list.
Er.63	One or more images in the bootable image list has an invalid header.
Er.64	The selected image is not bootable.
Er.65	Storage unavailable for Boot or Save operations.
Er.66	Image invalidated due to Seven-strikes.
Er.6F	Invalid module number.
Er.74	Tuner failure, invalid LO1 status.
Er.80	Failed to initialize USB hardware. Displayed by Zstrap and Cstrap.
Er.91	Error programming NAND flash. You might receive this error if bad blocks have reduced NAND storage to the point that there is not enough memory for the image.
Er.FL	■ Unrecognized flash type. Displayed by BSTRAP.IMG (xA2, xA3, xA3p, or xG2 protocols). ■ Option board flash not found (if running from the main board flash), or flash type not recognized. If you are running from the main board flash, make sure that the Ethernet option board is properly installed. Displayed by BSTRAP.IMG ("f" option with xA2, xA3, xA3p, or xG2 protocols).
EfL-	The universal bootstrap (BSTRAP.IMG) is initializing the Ethernet interface. If this remains on the LED display indefinitely, there is a problem with the interface. Try using USB or serial interfaces instead. Displayed by BSTRAP.IMG.
EfLd	The universal bootstrap (BSTRAP.IMG) is waiting for the host (PC) to respond to its attempt to initiate a download over the Ethernet interface. This might indicate a cabling problem or that the XLD terminated prematurely. Displayed by BSTRAP.IMG.
L	The hardware loader (Laruasia, Pangea, or Atlas) is downloading from the main board serial port. Wait until you see this indicator on the display before starting XLD to perform a 3-step load (xA3 or xA3p protocols).

L-	The hardware loader (Laruasia, Pangea, or Atlas) is executing the image downloaded into RAM from the main board serial port. Typically, if you see this, there is a problem with the serial port, the cabling, or the XLD has aborted. Try again.
L--	The hardware loader (Laruasia, Pangea, or Atlas) is executing the image downloaded into RAM from the main board serial port. Typically, if you see this, there is a problem with the downloaded image.
L.000	The first download packet has been received from the serial, USB, or Ethernet port.
L.xxx	As the download progresses, the numbers (xxx) increase sequentially.
Ldbc	The hardware loader (Laruasia, Pangea, or Atlas) is waiting for the host (PC) to respond to its attempt to initiate a download over the serial port. Displayed by the small loader (Laurasia or Pangea/Atlas version) that is loaded and executed by the hardware loader (xA3 or xA3p protocols).
Pr.xx	Displays while the image is programming into flash. The numbers (xx) increase sequentially and represent each 16 kB section that is programmed. Above 4 MB, a dot is added.
lFr_	The universal bootstrap (BSTRAP.IMG) is attempting to replace a NAGRA bootloader using either the data ("d") or forced data ("d!") option, and the image does exactly fill the space reserved for it. The bootloader for NAGRA must always be in whole-sector format.
u.000	The first packet has been sent over the serial port. Displayed by BSTRAP.IMG.
u.xxx	As the upload progresses, the numbers (xxx) increase sequentially. Displayed by BSTRAP.IMG.
USb-	The universal bootstrap (BSTRAP.IMG) is initializing the USB interface. If this remains on the LED display indefinitely, there is a problem with the USB interface. Try the serial interface instead. Displayed by BSTRAP.IMG.
USbL	The universal bootstrap (BSTRAP.IMG) is waiting for the host (PC) to respond to its attempt to initiate a download over the USB interface. Typically, there is a cabling problem. Displayed by BSTRAP.IMG.

Bootloader Error Codes for Three-LED DHCTs

Low-level bootloader error codes on the three-LED DHCT display if there is an error condition detected by the bootloader when the DHCT boots, or when it loads or installs software.

The DHCT displays the error code for a little over a second and as many as 10 times. Before the DHCT displays the error code, all three LEDs are off.

All off [error code] [error code] [error code] [repeats up to 10 times] All off

Reading Bootloader Error Codes on the Three-LED DHCT

Error codes are displayed by the 3-LED DHCTs as a series of bright and dim illuminations, which correspond to the ones and zeros of a digital code. The bright illuminations represent 1 (or 'on') digits, and the dim illuminations represent 0 (or 'off') digits. The LEDs are on the face of the DHCT.

Important: Some DHCTs have 4 LEDs; however, the error codes will also use this 3-LED illumination pattern.

Each code represents a subset of a binary code. The binary code has an arbitrary zero (0) added before the most-significant digit to round the code to 9 bits (3 codes with 3 bits each). Ignore the first zero in the code.

Example:

The LEDs display the following codes:

Left LED	Middle LED	Right LED	Code
dim	dim	dim	~~0~~00
bright	dim	bright	101
dim	dim	bright	001

This LED pattern represents a code of 000 101 001. Removing the leading 0 results in the binary code of **0010 1001**, a hexadecimal value of **0x29**.

Example:

The LEDs display the following code:

All off, [(1 dim, 1 dim, 1 dim) (1 bright, 1 bright, 1 dim) (1 dim, 1 dim, 1 dim)], all off, [repeats up to 10 times].

This LED pattern (between the brackets [ ] in the example above) represents a code of 000 110 000. Removing the leading 0 results in a binary code of **0011 0000**, a hexadecimal value of **0x30**). You refer to the error codes in this document and see that this error indicates that the image length is incorrect.

BootLo Error Codes

The following table contains the bootLo error codes that might display on the DHCT.

Important: The bootLo error codes are 2-byte codes that display on only one LED.

Illuminations	Codes	Binary	Hex	Error Indication
dim, dim	00	00	0x00	One of the clock initializations failed.
dim, bright	01	01	0x01	Loading bootHi failure.
bright, dim	10	10	0x10	bootHi load memory failure.
bright, bright	11	11	0x11	bootHi security check failure.

BootHi Error Codes

The following table contains the bootHi error codes that might display on the DHCT.

Illuminations (left - middle - right)			Codes	Binary	Hex	Error Indication
dim	dim	dim	~~0~~00	0010 0000	0x20	Failed reception after the maximum retries.
bright	dim	dim	100			
dim	dim	dim	000			
dim	dim	dim	~~0~~00	0010 0001	0x21	Transfer parameters are incorrect.
bright	dim	dim	100			
dim	dim	bright	001			
dim	dim	dim	~~0~~00	0010 0010	0x22	CRC on the received image is incorrect.
bright	dim	dim	100			
dim	bright	dim	010			

dim	dim	dim	000	0010 0011	0x23	Wrong address (overflow/underflow).
bright	dim	dim	100			
dim	bright	bright	011			
dim	dim	dim	000	0010 0100	0x24	Start offset error.
bright	dim	dim	100			
bright	dim	dim	100			
dim	dim	dim	000	0010 0111	0x27	Overflow - Image is too long.
bright	dim	dim	100			
bright	bright	bright	111			
dim	dim	dim	000	0011 0000	0x30	Image length wrong.
bright	bright	dim	110			
dim	dim	dim	000			
dim	dim	dim	000	0011 0001	0x31	CRC in signature failed.
bright	bright	dim	110			
dim	dim	bright	001			
dim	dim	dim	000	0011 0010	0x32	Signature values wrong.
bright	bright	dim	110			
dim	bright	dim	010			
dim	dim	dim	000	0011 0011	0x33	Image does not pass verification.
bright	bright	dim	110			
dim	bright	bright	011			
dim	dim	dim	000	0011 1111	0x3F	Bootloader replacement verification failed.
bright	bright	bright	111			
bright	bright	bright	111			
dim	dim	bright	001	0100 0001	0x41	Failed communication with tuner.
dim	dim	dim	000			
dim	dim	bright	001			
dim	dim	bright	001	0100 0101	0x45	QPSK receiver expected but not found.
dim	dim	dim	000			
bright	dim	bright	101			
dim	dim	bright	001	0101 0000	0x50	Disk not detected.
dim	bright	dim	010			
dim	dim	dim	000			

dim	dim	bright	001	0101 0001	0x51	Disk not responding (during initialization).
dim	bright	dim	010			
dim	dim	bright	001			
dim	dim	bright	001	0101 0010	0x52	Timed out waiting for finish.
dim	bright	dim	010			
dim	bright	dim	010			
dim	dim	bright	001	0101 0011	0x53	Error reported from disk.
dim	bright	dim	010			
dim	bright	bright	011			
dim	dim	bright	001	0101 0100	0x54	DMA error during disk write.
dim	bright	dim	010			
bright	dim	dim	100			
dim	dim	bright	001	0101 0101	0x55	DMA error during disk read.
dim	bright	dim	010			
bright	dim	bright	101			
dim	dim	bright	001	0101 0110	0x56	Uncorrectable data.
dim	bright	dim	010			
bright	bright	dim	110			
dim	dim	bright	001	0101 0111	0x57	Read fail, data corrected (overwrite).
dim	bright	dim	010			
bright	bright	bright	111			
dim	dim	bright	001	0101 1000	0x58	Operation aborted.
dim	bright	bright	011			
dim	dim	dim	000			
dim	dim	bright	001	0101 1001	0x59	PHY error.
dim	bright	bright	011			
dim	dim	bright	001			
dim	dim	bright	001	0101 1010	0x5A	Disk addressing error.
dim	bright	bright	011			
dim	bright	dim	010			
dim	dim	bright	001	0110 0000	0x60	Basic storage format established.
bright	dim	dim	100			
dim	dim	dim	000			

dim	dim	bright	~~0~~01	0110 0001	0x61	Reformat failed.
bright	dim	dim	100			
dim	dim	bright	001			
dim	dim	bright	~~0~~01	0110 0010	0x62	Invalid image list.
bright	dim	dim	100			
dim	bright	dim	010			
dim	dim	bright	~~0~~01	0110 0011	0x63	Failed check of one of module headers.
bright	dim	dim	100			
dim	bright	bright	011			
dim	dim	bright	~~0~~01	0110 0100	0x64	Boot image load failure.
bright	dim	dim	100			
bright	dim	dim	100			
dim	dim	bright	~~0~~01	0110 0101	0x65	Storage unavailable for boot/save.
bright	dim	dim	100			
bright	dim	bright	101			
dim	dim	bright	~~0~~01	0110 0110	0x66	Image invalidated due to 7-strike ovf.
bright	dim	dim	100			
bright	bright	dim	110			
dim	dim	bright	~~0~~01	0110 0111	0x67	File name too long.
bright	dim	dim	100			
bright	bright	bright	111			
dim	dim	bright	~~0~~01	0110 1111	0x6F	Invalid module number.
bright	dim	bright	101			
bright	bright	bright	111			
dim	dim	bright	~~0~~01	0111 0100	0x74	Invalid LO1 status in ForceLock().
bright	bright	dim	110			
bright	dim	dim	100			
dim	dim	bright	~~0~~01	0111 0101	0x75	LO1 could not be forced to lock.
bright	bright	dim	110			
bright	dim	bright	101			
dim	dim	bright	~~0~~01	0111 0110	0x76	LO2 is not locked.
bright	bright	dim	110			
bright	bright	dim	110			

dim	dim	bright	001	0111 0111	0x77	Tuning/decode script error.
bright	bright	dim	110			
bright	bright	bright	111			
dim	dim	bright	001	0111 1000	0x78	Wrong parameter passed to script process.
bright	bright	bright	111			
dim	dim	dim	000			
dim	bright	dim	010	1000 0000	0x80	USB hardware initialization failure.
dim	dim	dim	000			
dim	dim	dim	000			
dim	bright	dim	010	1001 0001	0x91	Error accessing NAND flash.
dim	bright	dim	010			
dim	dim	bright	001			

LxLoader Error Codes

The following table contains the LxLoader error codes that might display on the DHCT.

Illuminations (left - middle - right)			Codes	Binary	Hex	Error Indication
dim	bright	dim	010	1010 0000	0xA0	Error loading image.
bright	dim	dim	100			
dim	dim	dim	000			
dim	bright	dim	010	1010 0001	0xA1	Error loading image.
bright	dim	dim	100			
dim	dim	bright	001			

Bootloader Error Codes for Single-LED DHCTs

Low-level bootloader error codes on the single-LED DHCT display if there is an error condition detected by the bootloader when the DHCT boots, or when it loads or installs software.

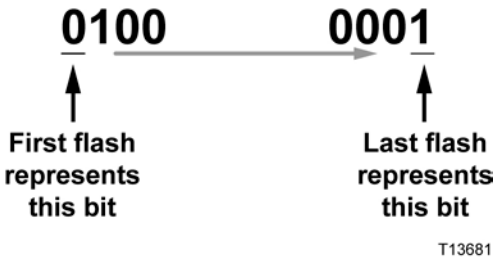
The DHCT displays the error code between a series of 4 illuminations. Before the DHCT displays the error code, it will blink 4 times, then display the error code, then blink 4 times, etc.

4 blinks, [error code] 4 blinks, [error code] 4 blinks, etc.

Note: The error code can display as many as 10 times.

Reading Bootloader Error Codes on the Single-LED DHCT

Error codes are displayed by the DHCT LED as a series of bright and dim illuminations, which correspond to the ones and zeros of a binary code. The bright illuminations represent 1 (or 'on') digits, and the dim illuminations represent 0 (or 'off') digits. The binary code is displayed by the DHCT from left (most-significant bit) to right (least-significant bit).



The LED is located on the face of the DHCT.

Example: The binary code **0100 0001**, representing a hexadecimal value of 0x41, is read as one dim illumination followed by one bright illumination, followed by five dim illuminations, and finally one bright illumination.

Important: You might not be able to distinguish a 'space' between consecutive dim or bright illuminations. However, the relative time for each illumination is the same. Therefore, two illuminations take twice as long to display as a single illumination.

Example: The DHCT displays the following code:

4 blinks, [2 dim, 2 bright, 4 dim], 4 blinks, [2 dim, 2 bright, 4 dim], 4 blinks, etc.

This blinking pattern (between the brackets [ ] in the example above) represents a binary code of **0011 0000** (hex **0x60**). You refer to the error codes in this document and see that this error indicates that the image length is incorrect.

BootLo Error Codes

The following table contains the bootLo error codes that might display on the DHCT.

Important: The bootLo error codes are 2-byte codes.

Illuminations	Codes	Binary	Hex	Error Indication
dim, dim	00	00	0x00	One of the clock initializations failed.
dim, bright	01	01	0x01	Loading bootHi failure.
bright, dim	10	10	0x10	bootHi load memory failure.
bright, bright	11	11	0x11	bootHi security check failure.

BootHi Error Codes

The following table contains the bootHi error codes that might display on the DHCT.

Illuminations	Binary	Hex	Error Indication
2 dim, 1 bright, 5 dim	0010 0000	0x20	Failed reception after the maximum retries.
2 dim, 1 bright, 4 dim, 1 bright	0010 0001	0x21	Transfer parameters are incorrect.
2 dim, 1 bright, 3 dim, 1 bright, 1 dim	0010 0010	0x22	CRC on the received image is incorrect.
2 dim, 1 bright, 3 dim, 2 bright	0010 0011	0x23	Wrong address (overflow/underflow).
2 dim, 1 bright, 2 dim, 1 bright, 2 dim	0010 0100	0x24	Start offset error.
2 dim, 1 bright, 2 dim, 3 bright	0010 0111	0x27	Overflow - Image is too long.
2 dim, 2 bright, 4 dim	0011 0000	0x30	Image length wrong.
2 dim, 2 bright, 3 dim, 1 bright	0011 0001	0x31	CRC in signature failed.
2 dim, 2 bright, 2 dim, 1 bright, 1 dim	0011 0010	0x32	Signature values wrong.

Illuminations	Binary	Hex	Error Indication
2 dim, 2 bright, 2 dim, 2 bright	0011 0011	0x33	Image does not pass verification.
2 dim, 5 bright, 1 dim	0011 1110	0x3E	Bootloader repl. - duplicate found.
2 dim, 6 bright	0011 1111	0x3F	Bootloader replacement verification failed.
1 dim, 1 bright, 5 dim, 1 bright	0100 0001	0x41	Failed communication with tuner.
1 dim, 1 bright, 3 dim, 1 bright, 1 dim, 1 bright	0100 0101	0x45	QPSK receiver expected but not found.
1 dim, 2 bright, 3 dim, 1 bright, 1 dim	0110 0010	0x62	Invalid image list.
1 dim, 2 bright, 3 dim, 2 bright	0110 0011	0x63	Failed check of one of module headers.
1 dim, 2 bright, 2 dim, 1 bright, 2 dim	0110 0100	0x64	Boot image load failure.
1 dim, 2 bright, 2 dim, 1 bright, 1 dim, 1 bright	0110 0101	0x65	Storage unavailable for boot/save.
1 dim, 2 bright, 2 dim, 2 bright, 1 dim	0110 0110	0x66	Image invalidated due to 7-strike ovf.
1 dim, 2 bright, 2 dim, 3 bright	0110 0111	0x67	File name too long.
1 dim, 2 bright, 1 dim, 4 bright	0110 1111	0x6F	Invalid module number.
1 dim, 3 bright, 1 dim, 1 bright, 2 dim	0111 0100	0x74	Invalid LO1 status in ForceLock().
1 dim, 3 bright, 1 dim, 1 bright, 1 dim, 1 bright	0111 0101	0x75	LO1 could not be forced to lock.
1 dim, 3 bright, 1 dim, 2 bright, 1 dim	0111 0110	0x76	LO2 is not locked.
1 dim, 3 bright, 1 dim, 3 bright	0111 0111	0x77	Tuning/decode script error.
1 dim, 4 bright, 3 dim	0111 1000	0x78	Wrong parameter passed to script process.
1 bright, 7 dim	1000 0000	0x80	USB hardware initialization failure.
1 bright, 2 dim, 1 bright, 3 dim, 1 bright	1001 0001	0x91	Error accessing NAND flash.

BootHi Error Codes

The following table contains the bootHi error codes that might display on the DHCT.

Illuminations	Binary	Hex	Error Indication
2 dim, 1 bright, 5 dim	0010 0000	0x20	Failed reception after the maximum retries.
2 dim, 1 bright, 4 dim, 1 bright	0010 0001	0x21	Transfer parameters are incorrect.
2 dim, 1 bright, 3 dim, 1 bright, 1 dim	0010 0010	0x22	CRC on the received image is incorrect.
2 dim, 1 bright, 3 dim, 2 bright	0010 0011	0x23	Wrong address (overflow/underflow).
2 dim, 1 bright, 2 dim, 1 bright, 2 dim	0010 0100	0x24	Start offset error.
2 dim, 1 bright, 2 dim, 3 bright	0010 0111	0x27	Overflow - Image is too long.
2 dim, 2 bright, 4 dim	0011 0000	0x30	Image length wrong.
2 dim, 2 bright, 3 dim, 1 bright	0011 0001	0x31	CRC in signature failed.
2 dim, 2 bright, 2 dim, 1 bright, 1 dim	0011 0010	0x32	Signature values wrong.
2 dim, 2 bright, 2 dim, 2 bright	0011 0011	0x33	Image does not pass verification.
2 dim, 5 bright, 1 dim	0011 1110	0x3E	Bootloader repl. - duplicate found.
2 dim, 6 bright	0011 1111	0x3F	Bootloader replacement verification failed.
1 dim, 1 bright, 5 dim, 1 bright	0100 0001	0x41	Failed communication with tuner.
1 dim, 1 bright, 3 dim, 1 bright, 1 dim, 1 bright	0100 0101	0x45	QPSK receiver expected but not found.
1 dim, 1 bright, 1 dim, 1 bright, 4 dim	0101 0000	0x50	Disk not detected.
1 dim, 1 bright, 1 dim, 1 bright, 3 dim, 1 bright	0101 0001	0x51	Disk not responding (during initialization).
1 dim, 1 bright, 1 dim, 1 bright, 2 dim, 1 bright, 1 dim	0101 0010	0x52	Timed out waiting for finish.
1 dim, 1 bright, 1 dim, 1 bright, 2 dim, 2 bright	0101 0011	0x53	Error reported from disk.
1 dim, 1 bright, 1 dim, 1 bright, 1 dim, 1 bright, 2 dim	0101 0100	0x54	DMA error during disk write.
1 dim, 1 bright, 1 dim, 1 bright, 1 dim, 1 bright, 1 dim, 1 bright	0101 0101	0x55	DMA error during disk read.

Illuminations	Binary	Hex	Error Indication
1 dim, 1 bright, 1 dim, 1 bright, 1 dim, 2 bright, 1 dim	0101 0110	0x56	Uncorrectable data.
1 dim, 1 bright, 1 dim, 1 bright, 1 dim, 3 bright	0101 0111	0x57	Read fail, data corrected (overwrite).
1 dim, 1 bright, 1 dim, 2 bright, 3 dim	0101 1000	0x58	Operation aborted.
1 dim, 1 bright, 1 dim, 2 bright, 2 dim, 1 bright	0101 1001	0x59	PHY error.
1 dim, 1 bright, 1 dim, 2 bright, 1 dim, 1 bright, 1 dim	0101 1010	0x5A	Disk addressing error.
1 dim, 2 bright, 5 dim	0110 0000	0x60	Basic storage format established.
1 dim, 2 bright, 4 dim, 1 bright	0110 0001	0x61	Reformat failed.
1 dim, 2 bright, 3 dim, 1 bright, 1 dim	0110 0010	0x62	Invalid image list.
1 dim, 2 bright, 3 dim, 2 bright	0110 0011	0x63	Failed check of one of module headers.
1 dim, 2 bright, 2 dim, 1 bright, 2 dim	0110 0100	0x64	Boot image load failure.
1 dim, 2 bright, 2 dim, 1 bright, 1 dim, 1 bright	0110 0101	0x65	Storage unavailable for boot/save.
1 dim, 2 bright, 2 dim, 2 bright, 1 dim	0110 0110	0x66	Image invalidated due to 7-strike ovf.
1 dim, 2 bright, 2 dim, 3 bright	0110 0111	0x67	File name too long.
1 dim, 2 bright, 1 dim, 4 bright	0110 1111	0x6F	Invalid module number.
1 dim, 3 bright, 1 dim, 1 bright, 2 dim	0111 0100	0x74	Invalid LO1 status in ForceLock().
1 dim, 3 bright, 1 dim, 1 bright, 1 dim, 1 bright	0111 0101	0x75	LO1 could not be forced to lock.
1 dim, 3 bright, 1 dim, 2 bright, 1 dim	0111 0110	0x76	LO2 is not locked.
1 dim, 3 bright, 1 dim, 3 bright	0111 0111	0x77	Tuning/decode script error.
1 dim, 4 bright, 3 dim	0111 1000	0x78	Wrong parameter passed to script process.
1 bright, 7 dim	1000 0000	0x80	USB hardware initialization failure.
1 bright, 2 dim, 1 bright, 3 dim, 1 bright	1001 0001	0x91	Error accessing NAND flash.

B

CDL Error Codes

Introduction

This appendix contains a table that covers the CDL error codes as defined in the OCAP host specification and in the host MIB.

In This Appendix

Introduction

The codes in the following table are only supported by the Cisco Axiom middleware and by the Cisco Factory Staging Application.

Note: The OpenCable Common Download functionality supported by the Cisco Factory Staging Application is only available on NGP platforms.

The error codes described in the following table are defined by the CableLabs OpenCable Host CFR2.1 Specification and by the CableLabs OpenCable Host CFR2.X MIB Specification. The CableLabs OpenCable Host CFR2.1 Specification requires that these specific codes be displayed.

CDL Error Codes Table

In this table, the Error Code and Definition are defined by the OCAP host specification. The Cisco Source Component and Cisco Notes are information specific to Cisco.

Error Code	Definition	Cisco Source Component	Cisco Notes
Ed01	No Failure	N/A	N/A
Ed02	Improper code file controls - CVC subject organizationName for manufacturer does not match the Host device manufacturer name	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed03	Improper code file controls - CVC subject organizationName for code cosigning agent does not match the Host device current code cosigning agent.	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed04	Improper code file controls - The manufacturer's PKCS #7 signingTime value is less-than the codeAccessStart value currently held in the Host device	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed05	Improper code file controls - The manufacturer's PKCS #7 signingTime is greater than the CVC validity end time	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed06	Improper code file controls - The manufacturer's CVC validity start time is less-than the cvcAccessStart value currently held in the Host device	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed07	Improper code file controls - The manufacturer's PKCS #7 signingTime value is less-than the CVC validity start time	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed08	Improper code file controls - Missing or improper extendedKeyUsage extension in the manufacturer CVC.	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image

Error Code	Definition	Cisco Source Component	Cisco Notes
Ed09	Improper code file controls - The cosigner's PKCS #7 signingTime value is less-than the codeAccessStart value currently held in the Host device	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed10	Improper code file controls - The cosigner's PKCS #7 signingTime is greater than CVC validity end time	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed11	Improper code file controls - The cosigner's CVC validity start time is less-than the cvcAccessStart value currently held in the Host device	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed12	Improper code file controls - The cosigner's PKCS #7 signingTime value is less-than the CVC validity start time	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed13	Improper code file controls - Missing or improper extended key-usage extension in the cosigner's CVC	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed14	Code file manufacturer CVC validation failure	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed15	Code file manufacturer CVS validation failure	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed16	Code file cosigner CVC validation failure	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image
Ed17	Code file cosigner CVS validation failure	eCM	Triggered after code download when authenticating the downloaded image prior to committing the image

Error Code	Definition	Cisco Source Component	Cisco Notes
Ed18	Improper eCM configuration file CVC format (e.g., missing or improper key usage attribute)	eCM	Triggered before code download when validating the CVCs from eCM config file
Ed19	eCM configuration file CVC validation failure	eCM	Triggered before code download when validating the CVCs from eCM config file
Ed20	Improper SNMP CVC format	eCM	Triggered before code download when validating the CVCs from SNMP
Ed21	CVC subject organizationName for manufacturer does not match the Host devices manufacturer name	eCM	Triggered before code download when validating the CVCs (from SNMP, eCM config file, or CVT). These would not apply to CVT PKCS#7 validation.
Ed22	*Reserved for future use*		
Ed23	The CVC validity start time is less-than or equal-to the corresponding subject's cvcAccessStart value currently held in the Host device	eCM	Triggered before code download when validating the CVCs (from SNMP, eCM config file, or CVT). These would not apply to CVT PKCS#7 validation
Ed24	Missing or improper key usage attribute for CVCs other than the eCM configuration file CVC	eCM	Triggered before code download when validating the CVCs (from SNMP, eCM config file, or CVT). These would not apply to CVT PKCS#7 validation
Ed25	SNMP CVC validation failure	eCM	Triggered before code download when validating the CVCs from SNMP

C

CableCARD Module Validation Status Codes

Introduction

This appendix contains a table that covers the CableCARD module validation status codes as defined in the CableCARD module copy protection specification.

In This Appendix

Introduction

The codes in the following table are only supported by the Cisco Axiom middleware and by the Cisco Factory Staging Application.

Note: The OpenCable Common Download functionality supported by the Cisco Factory Staging Application is only available on NGP platforms.

The error codes described in the following table are defined by the CableLabs CableCARD Copy Protection 2.0 Specification. The CableLabs OpenCable Host CFR2.1 Specification requires that these specific codes be displayed.

CableCARD Module Validation Status Codes Table

In this table, the Status Field and Value are defined by the CableCARD module copy protection specification. The Cisco Source Component and Cisco Notes are information specific to Cisco.

Error Code	Status Field	Value	Cisco Notes
noCA	Card is busy with binding authentication process	0x00	noCA on front panel
CP01	Not bound for Card reasons	0x01	CP01 on front panel
CP02	Not bound, Host Certificate Invalid	0x02	CP02 on front panel
CP03	Not bound, failed to verify Host's $SIGN_H$	0x03	CP03 on front panel
CP04	Not bound, failed to match AuthKey from Host	0x04	CP04 on front panel
CP05	Binding Failed, other reasons	0x05	CP05 on front panel
noCA - noCP	Not Validated, Binding Authentication Complete, Validation message not received yet	0x07	Triggers transition from displaying noCA to noCP on front pannel
noCP - clear	Validated, validation message is received, authenticated, and the IDs match those in the current binding	0x06	Triggers removal of noCP from front panel display
CP08	Not Validated, validation revoked	0x08	CP08 on front panel
	Reserved	0x09 to 0xFF	From looking at CAM code, it appears that the value 0xff will be reported by default if CP_valid_cnf APDU has yet to be received from the card.

D

Host - CableCARD Module Interface Errors

Introduction

This appendix contains a table that covers the Host - CableCARD module interface errors as defined in the CCIF specification.

In This Appendix

Introduction Host CableCARD Interface Errors

The codes in the following table are only supported by the Cisco Axiom middleware and by the Cisco Factory Staging Application.

Note: The OpenCable Common Download functionality supported by the Cisco Factory Staging Application is only available on NGP platforms.

The error codes described in the following table are defined by the CableLabs CableCARD Interface 2.0 Specification. The CableLabs OpenCable Host CFR2.1 Specification requires that these specific codes be displayed.

Host - CableCARD Module Interface Errors Table

In this table, the Status Field and Value are defined by the CableCARD module copy protection specification. The Cisco Source Component and Cisco Notes are information specific to Cisco.

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC00	Unable to communicate with Card	Host	S-Mode M-Mode	Host reports error to user	Host unable to communicate with Card
CC01	Card READY signal does not go active	Card	S-Mode	Host reports error to user	Not applicable – Cisco Host does not support S-Mode
CC02	Host reports error using screen in Figure B–1 - Error Display.	Card	S-Mode	Host reports error to user	Not applicable – Cisco Host does not support S-Mode
CC03	Host writes incorrect TPCE_INDX value to POD configuration register	Host	S-Mode	Host detects as failure #4 and reports error to user	Not applicable – Cisco Host does not support S-Mode
CC04	Host sets command channel RS bit but Card fails to set FR bit within 5-second timeout.	Card	S-Mode	Host reports error to user	Not applicable – Cisco Host does not support S-Mode
CC05	Host sets command channel RS bit and extended channel RS bit but Card fails to set FR bit within 5-second timeout	Card	S-Mode	Host reports error to user	Not applicable – Cisco Host does not support S-Mode
CC06	Invalid buffer negotiation - Card data channel (buffer size < 16)	Card	S-Mode	Host reports error to user	Not applicable – Cisco Host does not support S-Mode

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC07	Invalid buffer negotiation - Host data channel (buffer size < 256 bytes or greater than Card data channel buffer size)	Host	S-Mode	Host reports error to user	Not applicable – Cisco Host does not support S-Mode
CC08	Invalid buffer negotiation – Card extended channel (buffer size < 16)	Card	S-Mode	Host reports error to user	Not applicable – Cisco Host does not support S-Mode
CC09	Invalid buffer negotiation – Host extended channel (buffer size < 256 bytes or greater than Card data channel buffer size)	Host	S-Mode	Host reports error to user	Not applicable – Cisco Host does not support S-Mode
CC10	Card does not respond to Hosts open transport request within 5 seconds	Card	S-Mode	Host reports error to user	Not applicable – Cisco Host does not support S-Mode
CC11	Host does not respond to Card request to open resource manager session within 5 seconds	Host	S-Mode M-Mode	Host reports error to user	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error See also: 26, 32, 39, and 72

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC12	Host response to open resource manager session response – resource manager non-existent.	Host	S-Mode M-Mode	Host reports error to user	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC13	Host response to open resource manager session response – resource manager unavailable	Host	S-Mode M-Mode	Host reports error to user	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC14	Host response to open resource manager session response – incorrect version of resource manager.	Host	S-Mode M-Mode	Host reports error to user	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC15	Host response to open resource manager session response – resource manager busy	Host	S-Mode M-Mode	Host reports error to user	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC16	Host response to open resource manager session response – invalid status byte	Host	S-Mode M-Mode	Host reports error to user	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC17	Card fails to respond to profile_inq within 5 seconds	Card	S-Mode M-Mode	Host reports error to user	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC18	Host resource response – no application information resource.	Host	S-Mode M-Mode	**Minimum** – Host reports error to user. **Preferred** – Applications on the Card may not operate correctly, including MMI	Not applicable Should never happen on Cisco host because resource is always present
CC19	Host resource response – no Host control resource	Host	S-Mode M-Mode	Card may not be able to do conditional access properly	Not applicable Should never happen on Cisco host because resource is always present
CC20	Host resource response – no system time resource	Host	S-Mode M-Mode	Card operations which require system time will not operate	Not applicable Should never happen on Cisco host because resource is always present
CC21	Host resource response – no MMI resource	Host	S-Mode M-Mode	Card cannot utilize MMI for applications or to report error conditions	Not applicable Should never happen on Cisco host because resource is always present
CC22	Host resource response – no low speed communications	Host	S-Mode M-Mode	If OOB reverse path not available, then some applications will be unavailable, and the unit may function as a uni-directional device	Not applicable Should never happen on Cisco host because resource is always present

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC23	Host resource response – no homing resource	Host	S-Mode M-Mode	Card may have some operational problems (i.e., downloading software)	Not applicable Should never happen on Cisco host because resource is always present
CC24	Host resource response – no copy protection resource	Host	S-Mode M-Mode	All CA channels will not be descrambled, only clear channels may be viewed	Not applicable Should never happen on Cisco host because resource is always present
CC25	Host resource response – unknown resource identifier	Host	S-Mode M-Mode	Not a failure condition	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC26	Host fails to respond to open session request within 5 seconds	Host	S-Mode M-Mode	Host reports error to user	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error See also: 11, 32, 39, 72

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC27	Host response to open application info resource session – application info non-existent	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Applications on the Card may not operate correctly, including MMI	
CC28	Host response to open application info resource session – application info unavailable	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Applications on the Card may not operate correctly, including MMI	
CC29	Host response to open application info resource session – incorrect version of application info	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Applications on the Card may not operate correctly, including MMI	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC30	Host response to open application info resource session – application info busy	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Applications on the Card may not operate correctly, including MMI	

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC31	Host response to open application info resource session – invalid status byte	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Applications on the Card may not operate correctly, including MMI	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC32	Card requests to open conditional access session to the Host times out after 5 seconds	Host	S-Mode M-Mode	Host reports error to user	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error See also: 11, 26, 39, 72
CC33	Host response to conditional access resource session – conditional access non-existent	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Scrambled channels are not viewed	
CC34	Host response to conditional access resource session – conditional access unavailable	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Scrambled channels are not viewed	

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC35	Host response to conditional access resource session – incorrect version of conditional access	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Scrambled channels are not viewed	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC36	Host response to conditional access resource session – conditional access busy	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Scrambled channels are not viewed	
CC37	Host response to conditional access resource session – invalid status byte	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Scrambled channels are not viewed	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC38	Card fails to respond to ca_info_inq within 5 seconds.	Card	S-Mode M-Mode	Host reports error to user	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC39	Card requests to open copy protection resource session to the Host times out after 5 seconds	Host	S-Mode M-Mode	All CA channels will not be descrambled, only clear channels may be viewed	Host will not implement
CC40	Host response to open copy protection resource session – copy protection non-existent	Host	S-Mode M-Mode	All CA channels will not be descrambled, only clear channels may be viewed	
CC41	Host response to open copy protection resource session – copy protection unavailable	Host	S-Mode M-Mode	All CA channels will not be descrambled, only clear channels may be viewed	
CC42	Host response to open copy protection resource session – copy protection busy	Host	S-Mode M-Mode	All CA channels will not be descrambled, only clear channels may be viewed	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC43	Host response to open copy protection resource session – invalid status byte	Host	S-Mode M-Mode	All CA channels will not be descrambled, only clear channels may be viewed	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC44	Host does not support the Card's copy protection system	Host/Card incompatibility	S-Mode M-Mode	All CA channels will not be descrambled, only clear channels may be viewed	CP binding error
CC45	Host and Card do not mate	Host/Card incompatibility	S-Mode M-Mode	All CA channels will not be descrambled, only clear channels may be viewed	CP binding error
CC46	Host response to CP_sync – Host busy	Host	S-Mode M-Mode	A copy protected channel will stop being descrambled	CP sync error
CC47	Host response to CP_sync – no CP support	Host	S-Mode M-Mode	A copy protected channel will stop being descrambled	CP sync error
CC48	Host response to CP_sync – invalid status	Host	S-Mode M-Mode	A copy protected channel will stop being descrambled	CP sync error

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC49	Host fails to respond to cp_open_req.	Host	S-Mode M-Mode	A copy protected channel will stop being descrambled	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC50	Invalid Host certificate	Host	S-Mode M-Mode	All CA channels will not be descrambled, only clear channels may be viewed	CP binding error
CC51	Write Error (WE) occurs after completion of any transfer from Host to Card	Card or Host	S-Mode	User may see frozen picture on scrambled channels	Other Error
CC52	Read Error (RE) occurs after completion of any transfer from Card to Host	Card or Host	S-Mode	User may see frozen picture on scrambled channels	Other Error
CC53	Card fails to respond to any request within 5 seconds	Card	S-Mode M-Mode	User MAY see frozen picture on scrambled channels	Other Error
CC54	Invalid session APDU from Host	Host	S-Mode M-Mode	Not a failure condition	Other Error
CC55	Invalid session APDU from Card	Card	S-Mode M-Mode	Not a failure condition	Other Error
CC56	Invalid SPDU tag from Host	Host	S-Mode M-Mode	Not a failure condition	Other Error
CC57	Invalid SPDU tag from Card	Card	S-Mode M-Mode	Not a failure condition	Other Error
CC58	Invalid APDU tag from Host	Host	S-Mode M-Mode	Not a failure condition	Other Error

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC59	Invalid APDU tag from Card	Card	S-Mode M-Mode	Not a failure condition	Other Error
CC60	Transport ID from Host that has not been created and confirmed by Card	Host	S-Mode M-Mode	Not a failure condition	Other Error
CC61	Transport ID from Card that has not been created by Host	Card	S-Mode M-Mode	Not a failure condition	Other Error
CC62	Session ID from Host that has not been created and confirmed by Card	Host	S-Mode M-Mode	Not a failure condition	Other Error
CC63	Session ID from the Card that has not been created by Host	Card	S-Mode M-Mode	Not a failure condition	Other Error
CC64	Incompatible CableCARD device Inserted	Host	M-Mode	Used when an S-CARD in inserted into an M-Host	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC65	Card Resource Limit Reached	Card	M-Mode	Used when the stream, program and/or PID limit has been reached by a user initiated action	

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
■ CC66	When the Card is in M-Mode and the Host sets the ER bit but the Card fails to set the CR bit in the IQB within 5 seconds of RESET going inactive	Card	M-Mode	Host reports error to user	CCIF Init Error
CC67	Host resource response – no Extended Channel resource	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Applications on the Card and/ or Host may not operate correctly	Not applicable Should never happen on Cisco host because resource is always present
CC68	Host resource response – no System Control Resource	Host	S-Mode M-Mode	**Minimum** – Host reports error to user **Preferred** – Common Downloads to the Host may not function properly	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC69	Host resource response – no CARD RES Resource	Host	M-Mode	**Minimum** – Host reports error to user **Preferred** – Interface limits may be reached and the Host may not function properly, and/ or may also display error code 65	Not applicable Should never happen on Cisco host because resource is always present

Error Code	Error Condition	Failure	Card Mode	Comments	Cisco Notes
CC70	Host resource response – no DSG Resource	Host	M-Mode	**Minimum** – Host reports error to user **Preferred** – DSG operations/ messaging to the Card/Host may not function properly.	This condition can arise for DAVIC-only builds, because resource is only included in host's profile for DOCSIS builds
CC71	The M-CARD in M-Mode failed to open a Resource Manager session within 10 seconds after the RESET went inactive	Card	M-Mode	Optional: Host reports error to user when the two PCMCIA resets and the two power cycles do not clear the problem	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error
CC72	Host fails to send profile_inq() APDU within 5 seconds of Resource Manager session being established	Host	S-Mode M-Mode	None	This condition reports one of the following: ■ <blank> ■ Not supported ■ Not applicable ■ CCIF Initialization Error ■ CP binding error ■ CP sync error ■ Other error See also: 11, 26, 32, 39
CC73	Host resource response - no Headend Communication Resource	Host	S-Mode M-Mode	Host reports error to user	Not applicable Should never happen on Cisco host because resource is always present

E

Staging Toolkit

Introduction

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

Note: This appendix is applicable only to systems using SARA.

In This Appendix

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 189).

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 188).

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.

Index

U

V

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

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

Part Number 4024836 Rev D
August 2012 Printed in USA