Setting Up the PowerKEY CableCARD and M-Card Modules on the DNCS

For System Releases 2.5/3.5 and 4.0

Please Read

Important

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

Notices

Trademark Acknowledgements

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

CableCARD, M-Card, OpenCable, CableLabs and DOCSIS are trademarks or registered 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

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

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

Contents

About This Guide v

Introduction v
Purpose v
Scope v
Audience v
Related Publications vi
Document Version vi

Chapter 1 Set Up the PowerKEY CableCARD or M-Card Module 1

PowerKEY CableCARD and M-Card Modules Supported 2
Configure the DNCS for CableCARD and M-Card Support 4
Introduction 4
Process Overview 4
Before You Begin 4
Loading the EMM CD 5
Setting Up the DNCS for OpenCable Compliance 5
Configuring the CableCARD Server on the DNCS 12
Configuring the Emergency Alert System (EAS) to Properly Function with the CableCARD and M-Card Modules 14
Verifying Installation of the CableCARD or M-Card Module 15

Chapter 2 Manage the CableCARD and M-Card Modules 17

Configure Copy Protection Authorization on the DNCS 18
CableCARD and M-Card Module and Host Copy Protection Binding 18
Editing the CableCARD or M-Card Module and Host in the DNCS 20
Maintain the Host Certification Revocation List 21
Returning CableCARD or M-Card Modules from Service 23
Unbind Copy Protection for CableCARD or M-Card Module and Host 23
Removing Conditional Access Services from the CableCARD and M-Card Modules 24
Deleting the CableCARD or M-Card Module and Associated Host 26

Chapter 3 Identify Error Handling Conditions 27

Identifying Error Handling Conditions 28
Introduction 28
Error Conditions 28

Chapter 4 Customer Information 43

About This Guide

Introduction

The PowerKEY CableCARD module and the PowerKEY Multi-Stream CableCARD module (M-Card) are Cisco's unique hardware modules developed to provide subscribers with controlled conditional access to secure, digital content. Whether paired with a digital cable-ready TV, a digital set-top, or any other host device, the PowerKEY CableCARD or M-Card module must receive an initial configuration in order to function properly.

Purpose

This guide provides instructions for setting up and configuring the PowerKEY CableCARD and PowerKEY Multi-Stream CableCARD (M-Card) modules and the CableCARD Server on the Digital Network Control System (DNCS). This guide also provides procedures for configuring the emergency alert system (EAS) to properly function with the PowerKEY CableCARD and M-Card modules. In addition, this guide also includes a brief overview on how to verify that the PowerKEY CableCARD and M-Card modules are setup and configured correctly.

Scope

The contents of this guide apply to sites that are running DNCS System Releases (SR) 2.5/3.5 or 4.0 and one or more of the following PowerKEY CableCARD or M-Card modules:

- PKM600 PowerKEY CableCARD Module
- PKM800 PowerKEY Multi-Stream CableCARD Module (M-Card)
- PKM802 PowerKEY Multi-Stream CableCARD Module (M-Card)

Audience

This publication is written for Digital Broadband Delivery System (DBDS) operators and engineers, DNCS operators and engineers, Cisco field engineers, and Cisco Services engineers who are setting up (configuring) the PowerKEY CableCARD module.

Related Publications

You may find the following publications useful as resources when you implement the procedures in this document. Check the copyright date on your resources to assure that you have the most current version. The publish dates for the following documents are valid as of this printing. However, some of these documents may have since been revised:

- *Best Practices for Using Single-Stream PowerKEY CableCARD Modules* (part number 4015091, published September 2006)
- *System Release 2.5 Release Notes* (part number 749253, published October 2005)
- *System Release 3.5 Release Notes* (part number 4001159, published October 2005)
- *System Release 4.0 Release Notes* (part number 4001703, published February 2006)
- *Procedure to Enable DNCS to Support New mmi Screen for M-Card™* (part number 736123, expected publish date: late 2006)
- *The PowerKEY CableCARD Module Installation Instructions, Model PKM800* (part number 745460, expected publish date: late 2006)
- *Explorer® Digital Home Communications Terminal Staging Guide* (part number 734375, published September 2006)
- *Enabling Content Protection for Broadcast Programming* (part number 4005893, published September 2005)
- *Downloading New Client Application Platform Software Installation Instructions* (part number 4003052, published September 2005 [revision expected: late 2006])
- *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377, published June 2005)
- *PowerKEY CableCARD Module Installation Instructions, Model PKM600* (part number 736104, published December 2003)

Document Version

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

Description	See Topic
Added descriptions for configuring M-Card modules	Throughout document
Added descriptions of PKM800 and PKM802 M-Card modules	***PowerKEY CableCARD and M-Card Modules Supported*** (on page 2)

1

Set Up the PowerKEY CableCARD or M-Card Module

Introduction

This chapter provides procedures to set up the PowerKEY CableCARD module and the PowerKEY Multi-Stream (M-Card) module to function properly on a DNCS running SR 2.5/3.5 or 4.0.

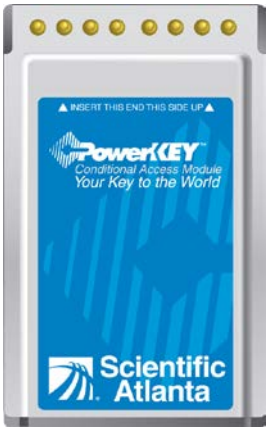
In This Chapter

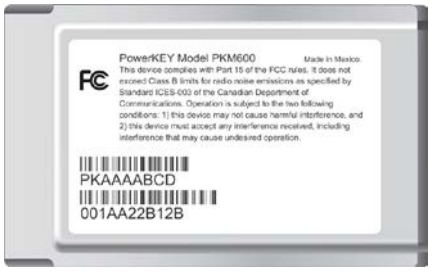
- PowerKEY CableCARD and M-Card Modules Supported 2
- Configure the DNCS for CableCARD and M-Card Support..... 4

PowerKEY CableCARD and M-Card Modules Supported

The following illustrations show the front and back views of the PowerKEY CableCARD and M-Card modules supported by this document.

PKM600 PowerKEY CableCARD Module





PKM800 PowerKEY M-Card Module (teal background)

PKM802 PowerKEY M-Card Module (white background)

Configure the DNCS for CableCARD and M-Card Support

Introduction

In order for the PowerKEY CableCARD or M-Card modules to function properly, you must initially configure the DNCS. The following steps summarize the process. Detailed steps appear later in this section.

Process Overview

If you have not set up your DNCS to configure CableCARD or M-Card modules, you need to complete the following stages. Otherwise, go to ***Before You Begin*** (on page 4).

Important! Stages 3 and 4 only apply to SR 4.0 SP1 and earlier.

1. Load the EMM CD (or download the EMMs from the Cisco FTP site) and confirm that the correct CableCARD or M-Card module types exist.

   Note: Refer to the *Explorer® Digital Home Communications Terminal Staging Guide* for more information.
2. Set up the DNCS for OpenCable compliance.
3. Create an mmi.txt and a gfc.txt file on the DNCS.
4. Make the mmi.txt and gfc.txt files available on the BFS Data Carousel.
5. Configure the CableCARD server on the DNCS.
6. Configure EAS to properly function with the CableCARD and M-Card modules.
7. Verify the setup of the CableCARD and M-Card modules on the DNCS.

Before You Begin

You need to obtain the EMM keys for the PowerKEY CableCARD and/or M-Card modules that you intend to provision on the DNCS at this time. If your EMM CDs or files have been lost or misplaced, contact Cisco Services.

Loading the EMM CD

The EMM CD or the EMM file you obtained from the Customer Self-Service Web site includes one or more of the following types:

- **Type 600 Revision 10**
- **Type 800 Revision 11**
- **Type 800 Revision 12**
- **Type 802 Revision 11**
- **Type 802 Revision 12**

After the EMM files are installed, the DNCS includes this type information in the UN-Config message, allowing the CableCARD and M-Card modules (upon start up) to configure automatically to the network to which they are attached.

Important! Before configuring the system for the CableCARD or M-Card module, load the EMM CD or the EMM file using the instructions described in the *Explorer® Digital Home Communications Terminal Staging Guide*. Then confirm that the correct DHCT type (see previous list) exists in the DHCT type list.

Note: After the CableCARD and M-Card EMM keys are installed on the DNCS, verify that the type and revision that appear in the DHCT Provisioning Type list for the CableCARD and M-Card modules are the same type and revision that appear on the labels attached to the shipping container.

Setting Up the DNCS for OpenCable Compliance

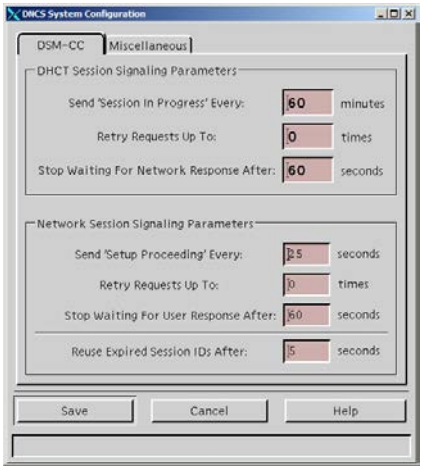
Setting up the DNCS for the OpenCable Compliance industry standard allows the secure and removable CableCARD and M-Card modules to be both available and portable to set-tops and other hosts. This section contains procedures to set up the DNCS for OpenCable compliance.

Configure Your Site for OpenCable Compliance

Complete these steps to configure the site you are upgrading for OpenCable Compliance.

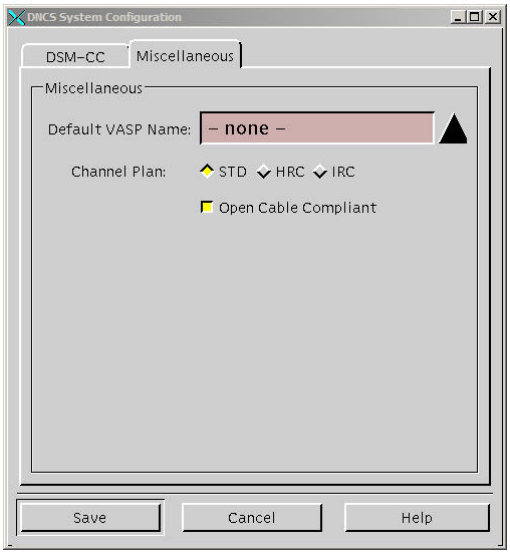
1. From the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **System Provisioning** tab.

3 Click **DNCS System**. The DNCS System Configuration window opens



4 Select the **Miscellaneous** tab.

5 Select the **OpenCable Compliant** option. A yellow highlight appears in the OpenCable Compliant field.



6 Click **Save**. The OpenCable Compliance Warning message appears.

7 Click **OK** to close the OpenCable Compliance Warning message.

8 Click **Close** on the DNCS System Configuration window. The DNCS System Configuration window closes.

9 Go to ***Stopping and Restarting the siManager Process*** (on page 7).

Stopping and Restarting the siManager Process

The System Information Manager (siManager) generates SI tables. The SI tables provide service information to CableCARD modules and hosts, M-Card modules and hosts, set-top CableCARD hosts, and set-top M-Card hosts. To finish updating your system in order to support OpenCable, you must stop and restart (bounce) the siManager process by completing the following steps:

Important! This process will temporarily inhibit DHCTs from booting; however, DHCTs that are already operational will not be impacted.

1 From the DNCS section of the DNCS Administrative Console Status window, click **Control**. The DNCS Control window opens.

2 From the list of processes, select **siManager**.

3 Click **Process** and select **Stop Process**. A confirmation window opens.

4 Click **Yes** to confirm that you want to stop the siManager process. The indicator next to siManager turns red to identify that the process is stopped.

5 With the siManager process selected, click **Process** and select **Start Process**.

Results:

- The indicator next to the siManager process changes to yellow and then green to indicate that the process is active and running.
- Several other processes may also turn yellow while siManager is stopped. This does not indicate a problem.
- The SI tables are updated on the system.

Creating an mmi.txt and a gfc.txt File

The mmi.txt and gfc.txt files are provided by the DNCS and are utilized by the CableCARD or M-Card modules and the host. The contents of each file include the following data:

- **mmi.txt file**—Contains the telephone number of the cable service provider that the subscriber will call to configure the CableCARD or M-Card module at card installation
- **gfc.txt file**—Contains data that tells the host to output programming to either channel 3 or 4

If the mmi.txt and gfc.txt files do not exist on the DNCS, create them using the instructions in the following two sections: **Creating the mmi.txt File** and **Creating the gfc.txt File**.

Important! The mmi.txt and gfc.txt files must exist on the BFS for the CableCARD and the M-Card modules to function properly.

Creating the mmi.txt File

1 From the DNCS Administrative Console, click the **DNCS** tab.
2 Click the **Utilities** tab. The Utilities frame opens.
3 Click **xterm** from the **System Utilities** section of the screen. An xterm window opens.
4 Type **cd /export/home/dncs** at the prompt.
5 Type **ls –l** and press **Enter** to see a list of files in this directory.
6 Does the directory include a file called mmi.txt?
   - If **yes**, you do not need to create the file. Go to ***Creating the gfc.txt File*** (on page 9).
   - If **no**, you need to create the mmi.txt file. Go to step 7.
7 Type the following command: **vi mmi.txt** and press **Enter**. The vi editor opens.
8 Type **i**, where i represents the Insert command.

9 Type the phone number representing your customer service center in the following format:

Ph#: (770) 555-1212

10 Press the **Esc** key to exit from the insert mode.

11 Type the following command: **:wq!** and press **Enter**. The system saves the mmi.txt file and the vi editor closes.

12 Type **more mmi.txt** at the command prompt. The contents of the mmi.txt file display on the next line of the xterm window.

Example: $ **more mmi.txt**
Ph#: (770) 555-1212

Creating the gfc.txt File

1 If necessary, complete steps 1 through 3 from the previous procedure, **Creating the mmi.txt File**, to open an xterm window.

2 Type **ls –l** and press **Enter** to see a list of files in this directory.

3 Does the directory include a file called gfc.txt?

- If **yes**, you do not need to create the file.
- If **no**, you need to create the gfc.txt file. Go to step 4.

4 Type the following command: **vi gfc.txt** and press **Enter**. The vi editor opens.

5 Type **i**, where i represents the Insert command.

6 Type **F01:03 01** and press **Enter**, where 03 is the output channel for the DHCT host.

Note: Type **F01:04 01** if the output is on channel 4.

7 Press the **Esc** key to exit the insert mode.

8 Type the following command: **:wq!** and press **Enter**. The system saves the gfc.txt file and the vi editor closes.

9 Type **more gfc.txt** at the command prompt. The contents of the gfc.txt file display on the next line of the xterm window.

Example: $ **more gfc.txt**
F01:03 01

Adding the mmi.txt and gfc.txt Files to the POD_Data BFS Server

To allow the CableCARD and M-Card modules to have access to the mmi.txt and gfc.txt files, link each file to the POD_Data BFS server. To do so, complete the following steps.

1 From the Application Interface Modules tab, click **BFS Client**.

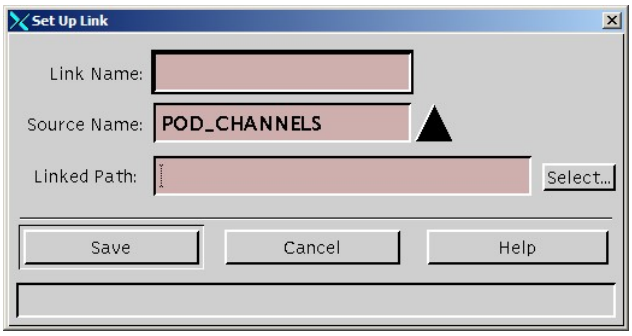
2 Double-click the server (POD_Data) to list the contents of the server and determine if the mmi.txt and gfc.txt links exist.

3 Are the mmi.txt and gfc.txt links present as valid links?

- If **yes**, go to ***Configuring the CableCARD Server on the DNCS*** (on page 12).
- If **no**, delete any invalid mmi.txt and gfc.txt links (orange link icon), if they exist, and then go to step 4.

Note: Valid links are indicated with a gray icon.

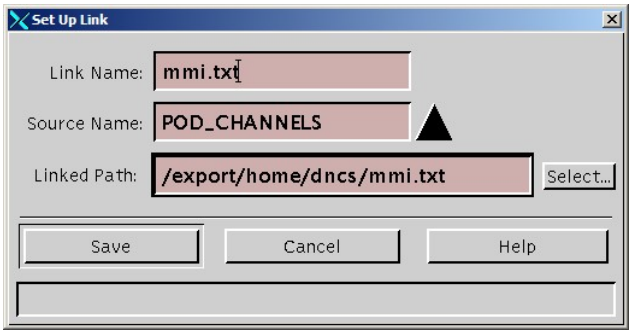
4 Select the **POD_Data** server, click **File**, and then select **New Link**. A window similar to the following window opens.



5 Type **mmi.txt** in the **Link Name** text box.

6 Ensure that **POD_CHANNELS** appears in the **Source Name** field. If it does not appear in this field, select it from the Source Name list.

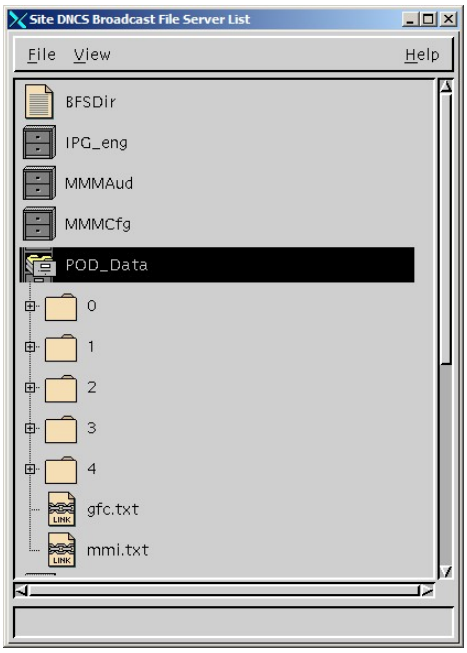
7 Click **Select** adjacent to the **Linked Path** field to locate and select the mmi.txt file created in the procedure ***Creating the mmi.txt File*** (on page 8).



8 Click **Save** to add an mmi.txt link to the POD_Data BFS server.

9 Repeat steps 4 through 8 to add the gfc.txt file to the POD_Data BFS server.

10 After linking both files to the POD_Data BFS server, refresh the BFS Server List window by clicking **View** and selecting **Refresh**. The BFS Server List window updates.



11 Are the mmi.txt and the gfc.txt files listed as links?

- If **yes**, go to step 12.
- If **no**, review the previous steps to link the files to the POD_Data BFS server, or contact Cisco Services.

12 Boot up a DHCT. Do all third-party applications and other DHCT functions work as expected?

- If **yes**, go to ***Configuring the CableCARD Server on the DNCS*** (on page 12).
- If **no**, contact Cisco Services.

Editing the mmi.txt and the gfc.txt Files

Complete the following steps to edit the mmi.txt and gfc.txt files after they are linked to the BFS server.

1 From the Application Interface Modules tab, click **BFS Client**.

2 Double-click the **POD_Data** to list the contents of the server and then delete the BFS POD_Data mmi.txt and/or the gfc.txt links.

3 Use a text editor to edit and save the mmi.txt or the gfc.txt files.

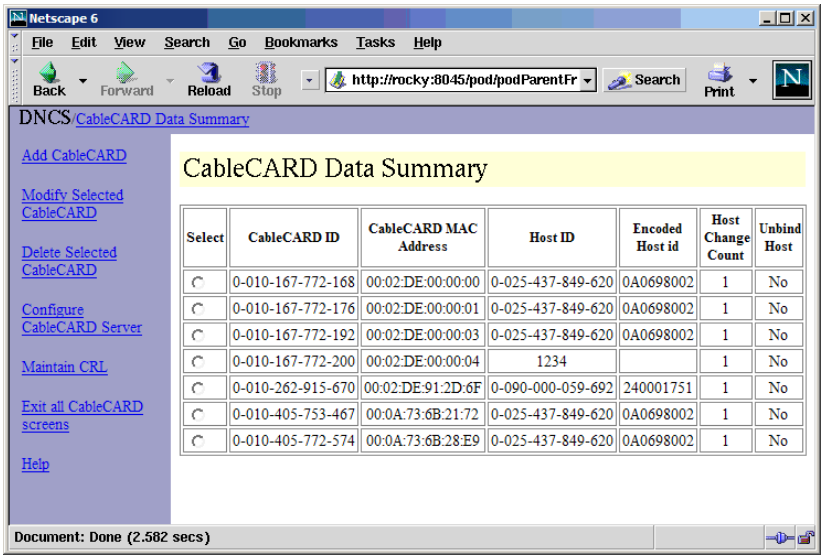
4 Re-link the mmi.txt or the gfc.txt file to the BFS POD_DATA server as shown in the previous procedure ***Adding the mmi.txt and gfc.txt Files to the POD_Data BFS Server*** (on page 9).

Configuring the CableCARD Server on the DNCS

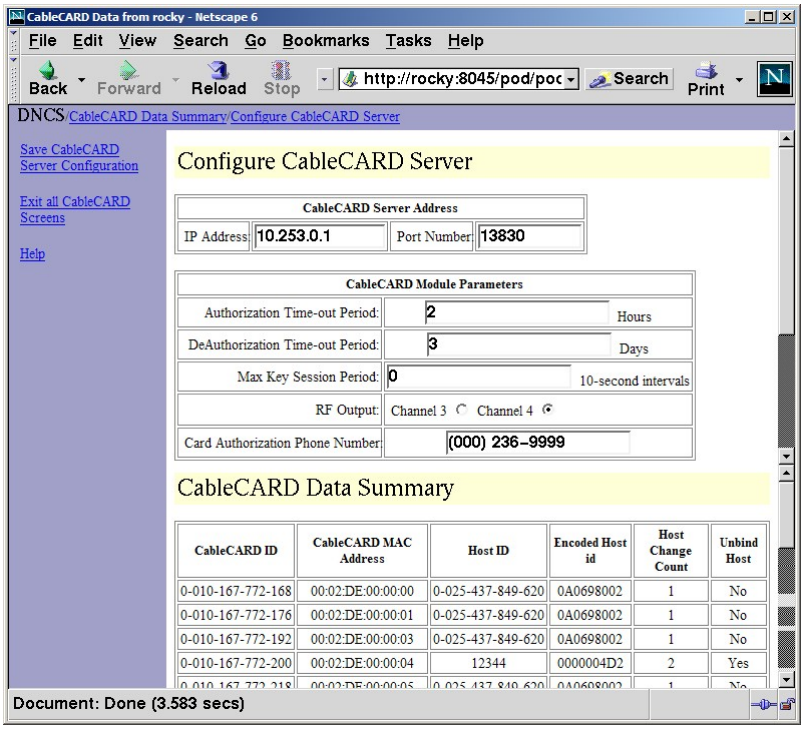
Configuring the CableCARD server enables the DNCS to send information from the DNCS to the CableCARD and M-Card modules. To activate the CableCARD Server on the DNCS, complete these steps.

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

2 Select the **Element Provisioning** tab and then click **CableCARD**. The CableCARD Data Summary screen opens in a Web browser.



3 Click **Configure CableCARD Server**. The CableCARD Data Summary screen updates to display the Configure CableCARD Server portion of the screen.



4 Type the following information into the appropriate fields within the Configure CableCARD Server screen.

- **IP Address**—The IP address of the server that is running the CCardServer process (for example, the DNCS). Typically this is the IP Address on the DNCS that connects to the QPSKs. For example, **10.253.0.1**.
- **Port Number**—The port number on the DNCS that the CableCARD server monitors for incoming CableCARD requests. Type the desired port number in the Port Number field.

  Note: The DNCS has reserved port **13830** for CableCARD and M-Card modules.
- **Authorization Time-out Period**—The time (in hours) that the CableCARD/host pair authorization data is broadcast using the CableCARD BFS file after copy protection authorization is granted from the DNCS. Suggested value for this field is **2**.
- **DeAuthorization Time-out Period**: The time period (in days) that a CableCARD/host pair deauthorization data is broadcast using the CableCARD BFS file after the copy protection deauthorization is saved using the DNCS. Suggested value for this field is **30**.

  Max Key Session Period—The rate at which copy protection keys are refreshed. These keys are copy protected and exchanged between the CableCARD or M-Card modules and the host. The suggested value for this field is **10**.

  Notes:

  – Any CableCARD or M-Card module in single-stream mode uses this entry number as *decaseconds* (multiply by 10). For example, a setting of 1 would equal 100 seconds—(1=10 seconds x 10 = 100 seconds).

  – Any M-Card module in multi-stream mode uses this number as *minutes*. For example, a setting of 10 would equal 10 minutes.

  – A setting of 0 (zero) means that the Max Key Session Period *never* refreshes.
- **RF Output**—Defines the channel over which the host delivers digital services. Suggested channel choice for this field is **Channel 3**.

  Note: Because this parameter is not supported in this release, go to ***Creating the gfc.txt File*** (on page 9) for instructions to set the RF output.
- **Card Authorization Phone Number**—Instructions that are displayed on a subscriber's television screen immediately after they install the CableCARD module and power on their television. Type the telephone number of the service provider who can verify that the CableCARD module was authorized.

  Note: Because this parameter is not supported in this release, go to ***Creating the mmi.txt File*** (on page 8) for instructions to define the message.

5 Click **Save CableCARD Server Configuration** on the left side of the screen to save these parameters. The CableCARD Data Summary screen appears in the forefront.

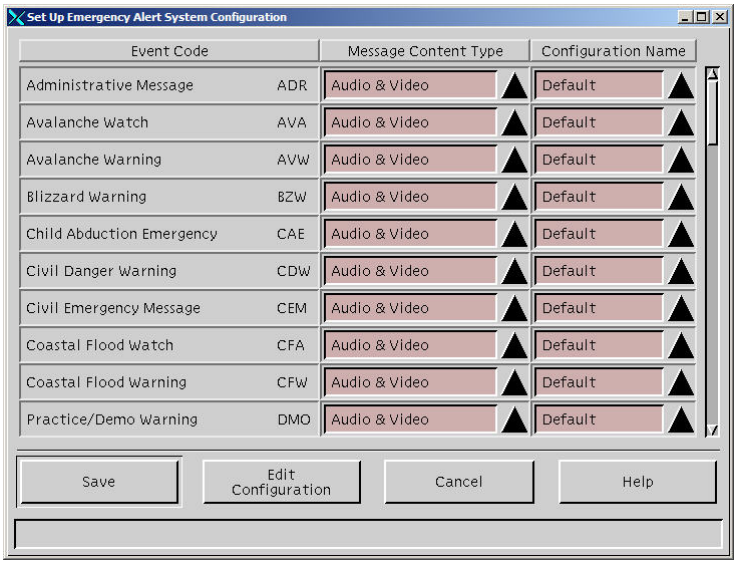
6 If you are finished, click **Exit All CableCARD Screens** to close the CableCARD window.

Configuring the Emergency Alert System (EAS) to Properly Function with the CableCARD and M-Card Modules

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

2 Click the **System Provisioning** tab.

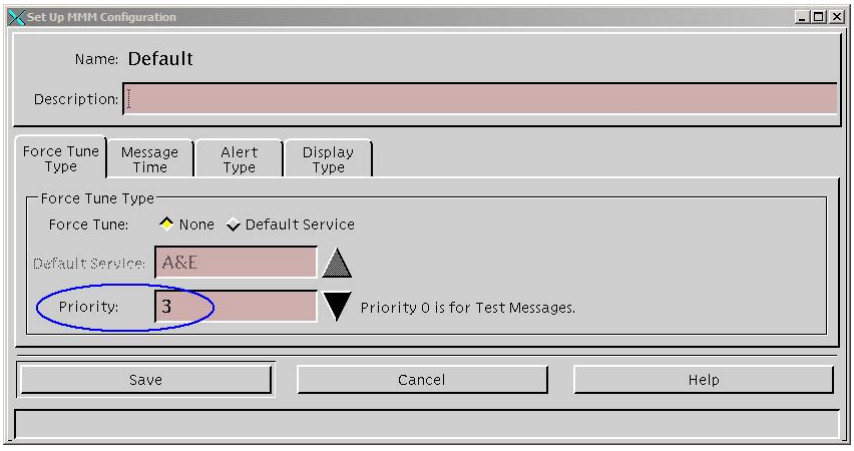
3 Click **EAS Config** to view the Set Up Emergency Alert System Configuration window.



4 Select the row containing the first unique configuration name that you are using, and click **Edit Configuration** to view the Set Up MMM Configuration window.

Note: You can also double-click the event code to access this screen.

5 Verify that the **Priority** field contains a non-zero value.

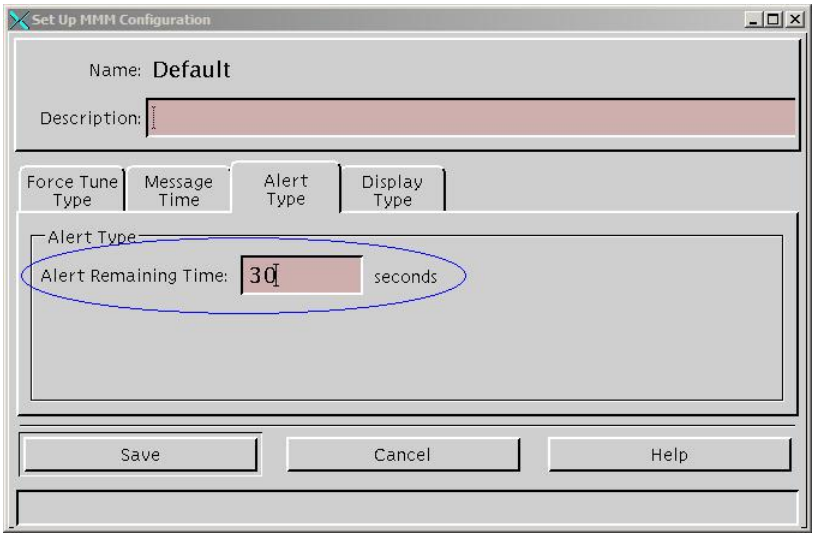


6 Is the Priority value zero?

- If **yes**, click the Priority arrow and select a non-zero value (for example, 3). Then go to step 7.
- If **no**, go to step 7.

7 Click the **Alert Type** tab to verify that the Alert Remaining Time field is a non-zero value.

Note: The value in the Alert Remaining Time field defines the duration of EAS messages on OpenCable hosts (with and without CableCARD modules).



8 Is the Alert Remaining Time set to zero?

- If **yes**, enter a value (in seconds) greater than zero. Then go to step 9.

  Note: Cisco recommends that you type **30** for this field.
- If **no**, go to step 9.

9 Click **Save** and click **Close**.

10 Repeat steps 3 through 9 for each unique configuration you have in use.

11 From the Set Up Emergency Alert System Configuration window, click **Close**.

12 Test the EAS alert functionality to verify that it is working properly.

Note: Cisco recommends that you test the EAS alert functionality each week.

Verifying Installation of the CableCARD or M-Card Module

1 Insert the CableCARD or M-Card module into the CableCARD module slot on the host device at your headend.

2 If your host is a device with RF output, tune the TV to the channel (3 or 4) that you selected in the Configure CableCARD Server Window.

Note: If the host device is a television set, tune to any channel.

3 Verify that the message displayed on the television screen includes the telephone number that is in the CableCARD Server Configuration user interface.

Notes:

- This message appears automatically on one-way hosts within a few minutes after inserting the CableCARD or M-Card module.
- Two-way hosts may not present this message automatically. However, you can obtain the information the message displays from the CableCARD diagnostic screens.

4 Is all of the displayed information correct?

- If **yes**, the CableCARD or M-Card module is configured correctly.
- If **no**, remove and reinsert the CableCARD or M-Card module. If the displayed information is still incorrect, contact your service provider for assistance.

5 After the CableCARD or M-Card module has been in the host device for several minutes, verify that the host displays the correct channel map for the hub to which the host device is connected.

Notes:

- If no packages containing encrypted programs have been assigned to this CableCARD or M-Card module, then only analog and clear digital programs will be viewable on the host device.
- If packages containing encrypted programs have been selected for the CableCARD or M-Card module, then encrypted programs should be viewable. If the encrypted programs are also copy protected, then the CableCARD or M-Card module and the respective host must be granted Copy Protection authorization *prior* to viewing the copy-protected programs.

2

Manage the CableCARD and M-Card Modules

Introduction

This chapter describes how to bind the CableCARD and M-Card modules to a host using the DNCS, enable Conditional Access (CA) and Copy Protection Authorization, and manage the host certificate revocation list (CRL) whenever device certificates are revoked by CableLabs. This chapter also explains how to remove services from a CableCARD or M-Card module when it is returned by a subscriber.

In This Chapter

- Configure Copy Protection Authorization on the DNCS 18
- Maintain the Host Certification Revocation List 21
- Returning CableCARD or M-Card Modules from Service 23

Configure Copy Protection Authorization on the DNCS

Each CableCARD and M-Card module must be paired with a host device in the DNCS database before the host device can present copy protected secure digital content. Prior to configuring Copy Protection Authorization, you must configure PowerKEY Conditional Access Authorization.

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

Note: Refer to the *Setting Up PowerKEY Conditional Access*, the *Overview of Setting Up Secure Services*, and the *Authorizing a DHCT for Service* sections of the *DNCS Online Help* for additional details for adding services and configuring PowerKEY Conditional Access and Copy Protection Authorization on your system.

CableCARD and M-Card Module and Host Copy Protection Binding

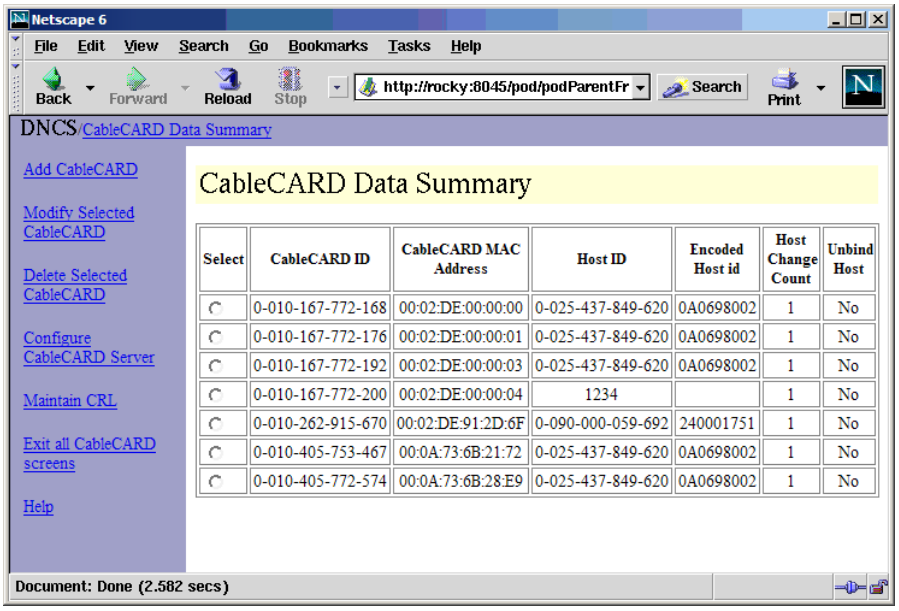
The CableCARD or M-Card module and host must be added to the DNCS to ensure copy protection authorization. The following methods are available:

- Adding the CableCARD or M-Card module to the DNCS through the CableCARD interface on the DNCS.
- Autobinding is available for two-way hosts if the following conditions are met:
  - The CableCARD Key Certificates are installed.
  - The host is not on the certificate revocation list (CRL).
- Using the billing system interface. Contact your billing vendor to see if they support this option.

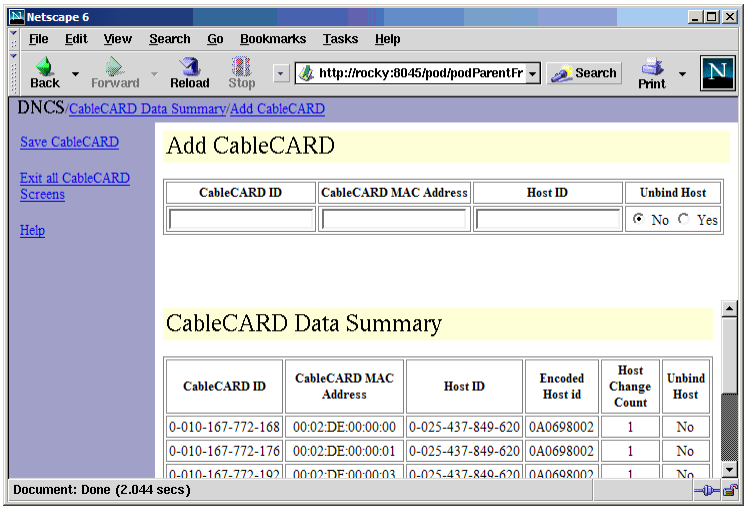
Adding the CableCARD or M-Card Module to the DNCS

To add the CableCARD or M-Card module to the DNCS through the CableCARD interface on the DNCS, complete the following steps.

1 On the DNCS Administrative Console, click the **Element Provisioning** tab, and then click **CableCARD**. The CableCARD Data Summary window opens.



2 Click **Add CableCARD**.



3 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 or M-Card module.

4 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, but all values entered into this field are converted to uppercase letters.

5 For further details, refer to the *DNCS Online Help* for specific steps to add a CableCARD or M-Card module to the DNCS.

Important! After saving the CableCARD or M-Card module on the DNCS, copy protection information should be displayed on the host within a few minutes. If it is not, contact Cisco Services for assistance.

6 If you are finished, click **Exit All CableCARD Screens** to close the CableCARD window.

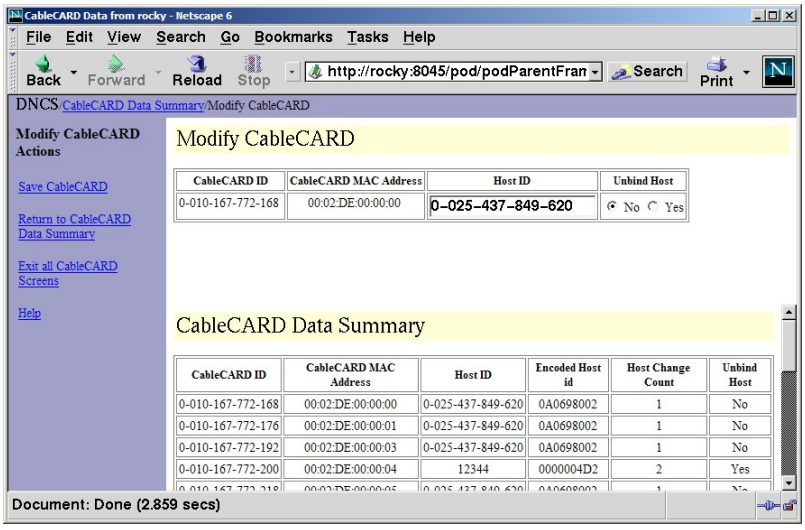
Editing the CableCARD or M-Card Module and Host in the DNCS

After adding and saving the CableCARD or M-Card module and its associated host device on the DNCS, you can modify the host ID information and change whether or not the host is bound to the CableCARD or M-Card module, in order to authorize or deauthorize the host for copy-protected content.

See ***Deleting the CableCARD or M-Card Module and Associated Host*** (on page 26) if you need to modify the CableCARD or M-Card module ID. If you need to modify a parameter other than the CableCARD or M-Card module ID, use the following procedure.

1 From the CableCARD Data Summary window, click the corresponding circle in the **Select** column to choose the CableCARD or M-Card module and host device that you want to modify.

2 Click **Modify Selected CableCARD** from the left side of the window. The Modify CableCARD window opens.



3 Refer to the *DNCS Online Help* for specific steps to modify the CableCARD or M-Card module in the DNCS regarding the Host ID or the unbind host status of the CableCARD or M-Card module.

4 If you are finished, click **Exit All CableCARD Screens** to close the Modify CableCARD window.

Maintain the Host Certification Revocation List

Maintaining the host certificate revocation list (CRL) is based on the CRL list generated and distributed to you by CableLabs. This list identifies device certificates that were revoked by CableLabs.

When a host device is revoked, you can add it to the CRL list, which indicates that this host device is no longer authorized to receive copy-protected content. If you have a CableCARD module or an M-Card module associated with this host device, the host device can still receive "copy freely" digital content.

Important! In order to add a host device to the CRL, it must appear on the CRL list generated and controlled by CableLabs.

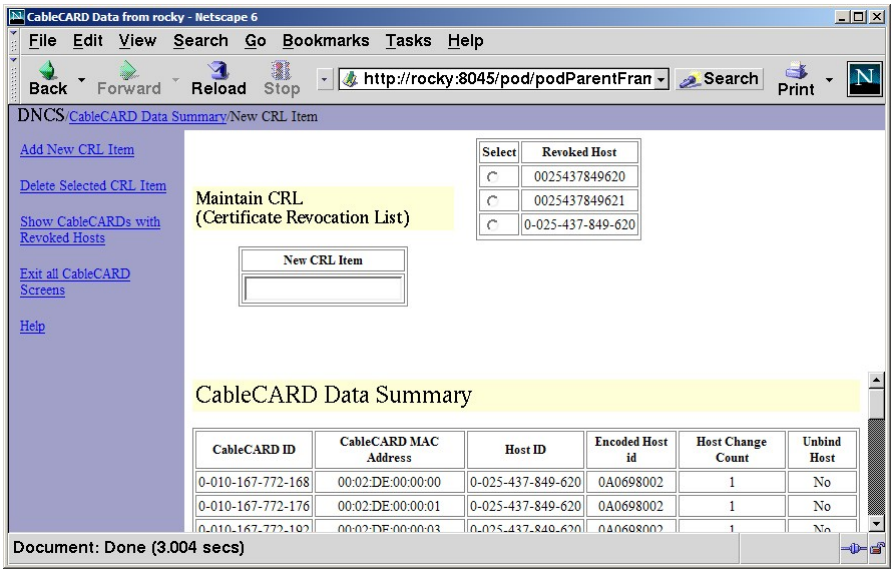
If a host device is removed from the CRL list by CableLabs, you can remove it from the CRL list.

Note: You can also use this window to see which CableCARD or M-Card modules are associated with which host devices on the CRL.

Maintaining the Host CRL

To maintain the host CRL, follow these steps.

1 From the CableCARD Data Summary window, click **Maintain CRL** to view the Maintain CRL window.



2 Perform one of the following functions:

- Click **Add New CRL Item** to add a new host device to the CRL list.
- Select a host from the **Revoked Host** list, and click **Delete Selected CRL Item** to remove a host from the CRL list.
- Click **Show CableCARDs with Revoked Hosts** to see a complete list of hosts on the CRL list.

3 Refer to the online help for specific steps to perform the functions listed in step 2.

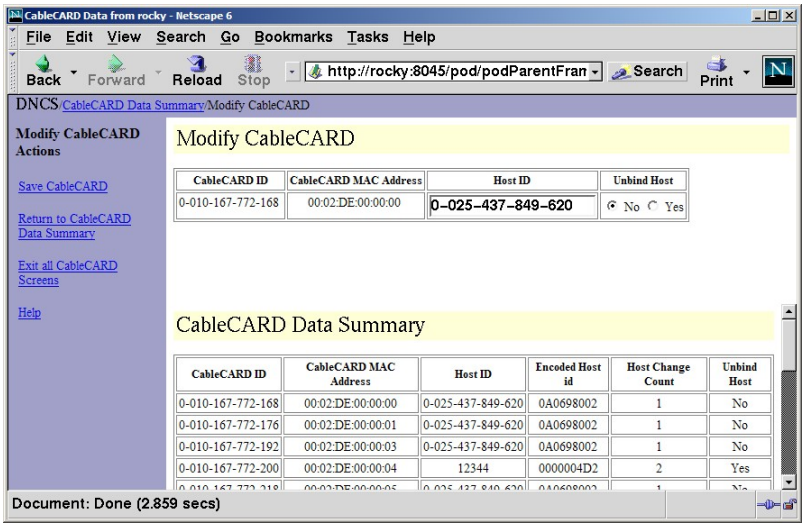
4 If you are finished, click **Exit All CableCARD Screens** to close the CableCARD window.

Returning CableCARD or M-Card Modules from Service

When CableCARD or M-Card modules are taken out of service, you must unbind the CableCARD or M-Card/host copy protection and remove the conditional access in order to disable the services on the CableCARD or M-Card modules. These services may be re-activated when the CableCARD or M-Card module is returned to service. You can remove the copy protection and the conditional access using the billing system or the DNCS as described in the following procedures.

Unbind Copy Protection for CableCARD or M-Card Module and Host

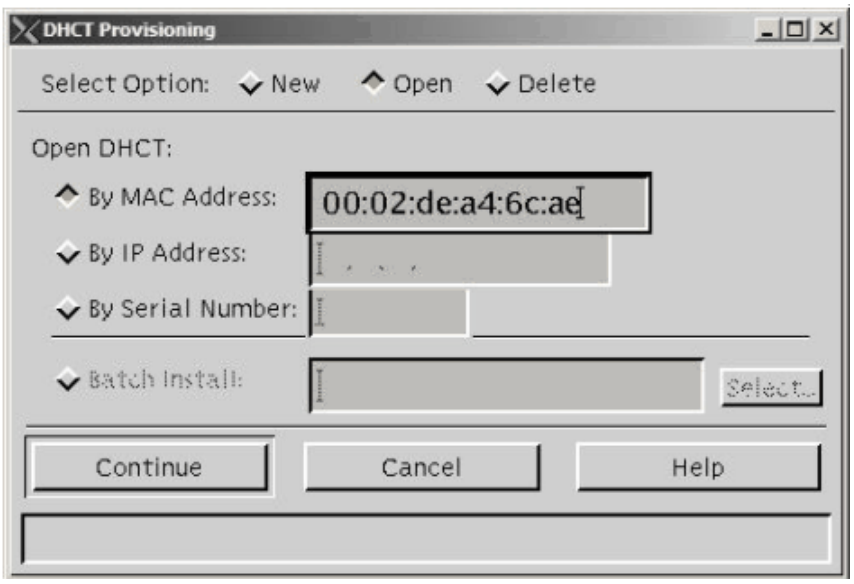
1. From the CableCARD Data Summary window, click the corresponding circle in the **Select** column to choose the CableCARD or M-Card module and host device that you want to unbind.
2. Click **Modify Selected CableCARD** from the left side of the window. The Modify CableCARD window opens.



3. Refer to the online help for specific steps to modify the CableCARD or M-Card module in the DNCS regarding the Host ID or the unbind host status of the CableCARD or M-Card module.
4. If you are finished, click **Exit All CableCARD Screens** to close the Modify CableCARD window.

Removing Conditional Access Services from the CableCARD and M-Card Modules

1 From the DNCS Administrative Console, select the **DNCS** tab, select the **Element Provisioning** tab, and then click **DHCT**. The DHCT Provisioning window opens.



2 Select the **By MAC Address** option and type the MAC Address for the CableCARD or M-Card module.

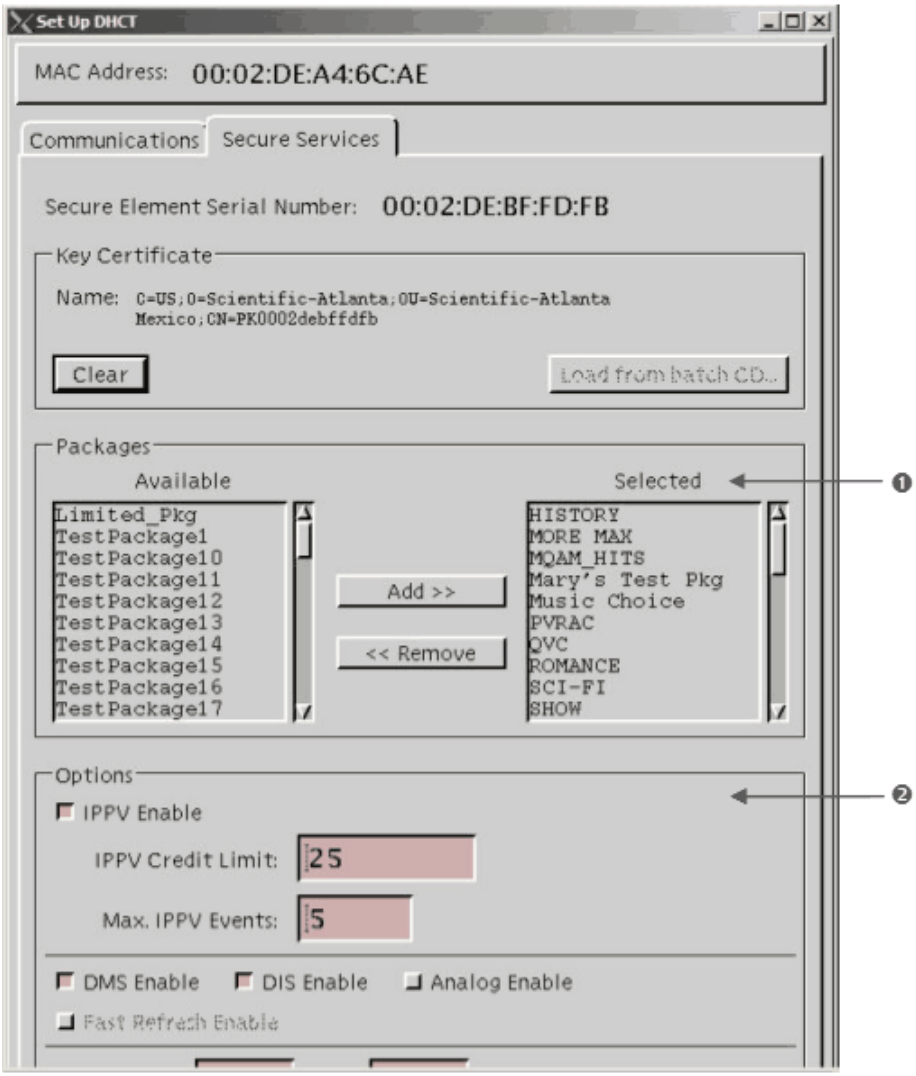
3 Click **Continue**. The Set Up DHCT window opens. A CableCARD or M-Card entry appears in the DHCT Type box.

4 Click the **Secure Services** tab. The Secure Services window opens.

5 From the **Packages** section, select the first package in the Selected list. Scroll to the bottom of the list, hold down the **Shift** key, and select the last package in the list to highlight all of the packages in the list.

6 Click **Remove**. All the packages move to the Available list.

7 From the **Options** section, select those options that are required by your internal procedures.



Result: In the illustration above, the numbers illustrate the following information:

❶ Packages that must be *removed* from the Selected List.

❷ Options that can be *modified* according to your procedures.

8 Click **Save**.

Results:

- The Set Up DHCT settings are saved.
- All package authorizations are removed from the CableCARD or M-Card module.

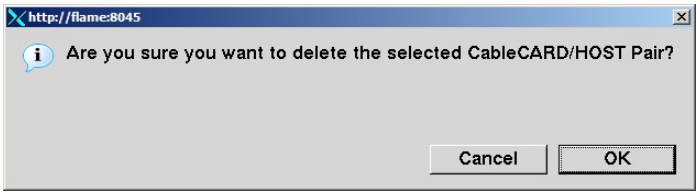
9 Click **Close**. The Set Up DHCT window closes.

Deleting the CableCARD or M-Card Module and Associated Host

Use this procedure to delete the CableCARD module or M-Card from its associated host on the DNCS.

Important! Only perform this procedure if you are removing the CableCARD module or M-Card from service indefinitely, or if you are correcting an incorrect ID for a CableCARD or M-Card or an incorrect MAC address. Otherwise, the Host Change Count information in the CableCARD Data Summary screen for a specific CableCARD or M-Card module will be lost.

1. From the CableCARD Data Summary window, click the corresponding circle in the **Select** column to choose the CableCARD or M-Card module and host device that you want to delete.
2. Click **Delete Selected CableCARD**. A confirmation window similar to the following opens.



3. Click **OK** to delete the CableCARD or M-Card module and host pair, or click **Cancel** to cancel the request.
4. If you are finished, click **Exit All CableCARD Screens** to close the CableCARD window.

3

Identify Error Handling Conditions

Introduction

This section is taken from the **HOST-POD Interface Standard** (ANSI-SCTE 28 2004), as written and approved by the Society of Cable Telecommunications Engineers (SCTE). Please refer to this interface standard document for the most up-to-date error handling conditions. You can access the interface standard document at the following URL:

(http://www.scte.org/documents/pdf/ANSISCTE282004.pdf).

In This Chapter

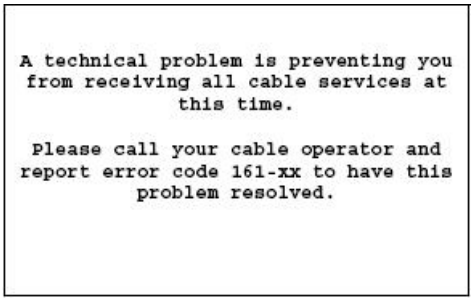
- Identifying Error Handling Conditions..... 28

Identifying Error Handling Conditions

Introduction

When error handling requires action by both the host and the CableCARD or M-Card module, the action by the first is designated with a (1). It is suggested that the CableCARD or M-Card module create a diagnostic user interface that registers with the application information resource to allow it to report any error conditions, especially in a broadcast (one-way) scenario.

In the event that an error occurs, the host displays an error message similar to the following message.



Note: The "xx" after the error code 161 is the item number that failed, as listed in the following table.

Error Conditions

Please refer to the following table to reference each error condition.

Note: A CableCARD or M-Card module reset is defined so that the host shall set the RS bit in the command interface control register. A PCMCIA reset is defined so that the host shall set the RESET signal active on the PCMCIA interface.

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
1	POD READY signal does not go active	POD	Host either: ■ Reports error message ■ Retries PCMCIA resets up to two times and then reports error message ■ Reports error, but continues to perform PCMCIA resets	None	Host reports error to user[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
2	Host reads incorrect CIS values	POD	Host reports error message	None	Host reports error to user
3	Host writes incorrect TPCE_INDX value to POD configuration register	Host	None	POD cannot perform any action	Host detects a failure #4 and reports error to user[1]
4	Host sets data channel RS bit, but POD fails to set FR bit within 5 second timeout	POD	Host either: ■ Reports error message ■ Retries PCMCIA resets up to two times and then reports error message ■ Reports error and continues to perform PCMCIA resets	None	Host reports error to user[1]
5	Host sets extended channel RS bit but POD fails to set FR bit within 5 second timeout	POD	Host either: ■ Reports error message ■ Retries PCMCIA resets up to two times and then reports error message ■ Reports error and continues to perform PCMCIA resets	None	Host reports error to user[1]
6	**Invalid buffer negotiation**– POD data channel (buffer size < 16)	POD	Host either: ■ Reports error message ■ Retries PCMCIA resets up to two times and then reports error message ■ Operates with smaller size	None	Host reports error to user[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
7	**Invalid buffer negotiation–** Host data channel (buffer size < 16 or greater than POD data channel buffer size)	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**-POD works with host buffer size	Host reports error to user[1]
8	**Invalid buffer negotiation–** POD extended channel (buffer size < 16)	POD	Host either: ■ Reports error message ■ Retries PCMCIA resets up to two times and then reports error message ■ Operates with smaller size	None	Host reports error to user[1]
9	**Invalid buffer negotiation–** Host extended channel (buffer size < 16 or > POD data channel buffer size)	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**-POD works with host buffer size	Host reports error to user[1]
10	POD does not respond to host's open transport request within 5 seconds	POD	Host either: ■ Reports error message ■ Retries PCMCIA resets up to two times and then reports error message ■ Reports error and continues to perform PCMCIA resets	None	Host reports error to user[1]
11	Host does not respond to POD request to open resource manager session within 5 seconds	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls	Host reports error to user[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
12	Host response to open resource manager session response – resource manager non-existent	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls	Host reports error to user[1]
13	Host response to open resource manager session response – resource manager unavailable	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls	Host reports error to user[1]
14	Host response to open resource manager session response – incorrect version of resource manager	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls	Host reports error to user[1]
15	Host response to open resource manager session response – resource manager busy	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls	Host reports error to user[1]
16	Host response to open resource manager session. response – invalid status byte	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls	Host reports error to user[1]
17	POD fails to respond to profile_inq within 5 seconds	POD	Host either: ■ Reports error message ■ Retries PCMCIA resets up to two times and then reports error message ■ Reports error and continues to perform PCMCIA resets	None	Host reports error to user[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
18	Host resource response – no application information resource	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**-POD continues operation and will not open a session to the application info resource	**Minimum**–Host reports error to user **Preferred**–Applications on POD may not operate correctly, including MMI[1]
19	Host resource response – no Host control resource	Host	None	**Minimum**–POD sets IIR flag and stops responding to polls	POD may not be able to do conditional access properly **Note**: There is a discussion ongoing about DOCSIS-only operations
20	Host resource response – no system time resource	Host	None	**Minimum**-POD continues operation and will not open a session to the system time resource **Preferred**–Same as minimum, but also reports this in its MMI diagnostics application	POD operations that require system time will not operate[1]
21	Host resource response–no MMI resource	Host	None	**Minimum**-POD continues operation and will not open a session to the MMI resource	POD cannot initialize MMI for applications or to report error conditions[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
22	Host resource response – no low speed communications	Host	None	**Minimum**-POD continues operation and will not open a session to the low speed communication resource **Preferred**-Same as minimum, but also reports this in its MMI diagnostic application	If OOB reverse path not available, then some applications will be unavailable
23	Host resource response – no homing resource	Host	None	**Minimum**-POD continues operation and will not open a session to the homing resource **Preferred**-Same as minimum, but also reports this in its MMI diagnostic application	POD may have some operational problems (for example, downloading software)
24	Host resource response – no copy-protection resource	Host	None	**Minimum**-POD continues operation, disables descrambling of all conditional access channels; it will not open a session to the copy-protection resource, reports to headend if possible, reports error to user, and reports this in its MMI diagnostic application	All CA channels will not be descrambled; only clear channels may be viewed[1]
25	Host resource response – unknown resource identifier	Host	None	**Minimum**-POD continues operation	Not a failure condition
26	Host fails to respond to open session request within 5 seconds	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls	Host reports error to user[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
27	Host response to open application info resource session – application info non-existent	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**-POD continues operation and will not open a session to the application info resource	**Minimum**– Host reports error to user **Preferred**– Applications on POD may not operate correctly, including MMI[1]
28	Host response to open application info resource session – application info unavailable	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**-POD continues operation and will not open a session to the application info resource	**Minimum**– Host reports error to user **Preferred**– Applications on POD may not operate correctly, including MMI[1]
29	Host response to open application info resource session – incorrect version of application info	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**-POD continues operation and will not open a session to the application info resource	**Minimum**– Host reports error to user **Preferred**– Applications on POD may not operate correctly, including MMI[1]
30	Host response to open application info resource session – application info busy	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**-POD continues operation and will not open a session to the application info resource	**Minimum**- Host reports error to user **Preferred**– Applications on the POD may not operate correctly, including MMI[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
31	Host response to open application info resource session – invalid status byte	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**-POD continues operation and will not open a session to the application info resource	**Minimum**-Host reports error to user **Preferred**–Applications on the POD may not operate correctly, including MMI[1]
32	POD module requests to open conditional access session to the Host times-out after 5 seconds	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls	Host reports error to user[1]
33	POD response to conditional access resource session – conditional access non-existent	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**–POD will not descramble, but will continue other operations and reports this in its MMI diagnostic application	**Minimum**–Host reports error to user **Preferred**–Scrambled channels are not viewed[1]
34	POD response to conditional access resource session – conditional access unavailable	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**–POD will not descramble, but will continue other operations and reports this in its MMI diagnostic application	**Minimum**–Host reports error to user **Preferred**–Scrambled channels are not viewed[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
35	POD response to conditional access resource session – incorrect version of conditional access	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**–POD will not descramble, but will continue other operations and reports this in its MMI diagnostic application	**Minimum**–Host reports error to user **Preferred**–Scrambled channels are not viewed[1]
36	POD response to conditional access resource session – conditional access busy	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**–POD will not descramble, but will continue other operations and reports this in its MMI diagnostic application	**Minimum**–Host reports error to user **Preferred**–Scrambled channels are not viewed[1]
37	POD response to conditional access resource session - invalid status byte	Host	None	**Minimum**-POD sets IIR flag and stops responding to polls **Preferred**–POD will not descramble, but will continue other operations and reports this in its MMI diagnostic application	**Minimum**–Host reports error to user **Preferred**–Scrambled channels are not viewed[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
38	POD fails to respond to ca_info_inq within 5 seconds	POD	Host either: ■ Reports error message ■ Retries PCMCIA resets up to two times and then reports error message ■ Reports error and continues to perform PCMCIA resets	None	Host reports error to user[1]
39	POD module request to open copy-protection resource session to the host times-out after 5 seconds	Host	None	**Minimum**–POD continues operation, disables descrambling of all conditional access channels, reports to headend if possible, reports this to user, and reports this in its MMI diagnostic application	All CA channels will not be descrambled; only clear channels may be viewed[1]
40	Host response to open copy-protection resource session – copy protection non-existent	Host	None	**Minimum**–POD continues operation, disables descrambling of all conditional access channels, reports to headend if possible, reports this to user, and reports this in its MMI diagnostic application	All CA channels will not be descrambled; only clear channels may be viewed[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
41	Host response to open copy-protection resource session – copy protection unavailable	Host	None	**Minimum**–POD continues operation, disables descrambling of all conditional access channels, reports to headend if possible, reports this to user, and reports this in its MMI diagnostic application	All CA channels will not be descrambled; only clear channels may be viewed[1]
42	Host response to open protection resource session–copy-protection busy	Host	None	**Minimum**– POD continues operation, disables descrambling of all conditional access channels, reports to headend if possible, reports this to user, and reports this in its MMI diagnostic application	All CA channels will not be descrambled; only clear channels may be viewed[1]
43	Host response to open copy-protection resource session – invalid status byte	Host	None	**Minimum**–POD continues operation, disables descrambling of all conditional access channels, reports to headend if possible, reports this to user, and reports this in its MMI diagnostic application	All CA channels will not be descrambled; only clear channels may be viewed[1]

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
44	Host does not support POD's copy-protection system	Host/POD incompatibility	None	**Minimum–**POD continues operation, disables descrambling of all conditional access channels, reports to headend if possible, reports this to user, and reports this in its MMI diagnostic application	All CA channels will not be descrambled; only clear channels may be viewed[1]
45	Host and POD do not mate	Host/POD incompatibility	None	**Minimum–**POD continues operation, disables descrambling of all conditional access channels, reports to headend if possible, reports this to user, and reports this in its MMI diagnostic application	All CA channels will not be descrambled; only clear channels may be viewed[1]
46	Host response to CP_sync – Host busy	Host	None	**Minimum–**POD will cease descrambling of copy-protected channels	A copy-protected channel will stop being descrambled
47	Host response to CP_sync – no CP support	Host	None	**Minimum–**POD will cease descrambling of copy-protected channels	A copy-protected channel will stop being descrambled
48	Host response to CP_sync – invalid status	Host	None	**Minimum–**POD will cease descrambling of copy-protected channels	A copy-protected channel will stop being descrambled
49	Host fails to respond to cp_open_req	Host	None	**Minimum–**POD will cease descrambling of copy-protected channels	A copy-protected channel will stop being descrambled

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
50	Invalid Host certificate	Host	None	**Minimum**–POD continues operation, disables descrambling of all conditional access channels, reports to headend if possible, reports this to user, and reports this in its MMI diagnostic application	All CA channels will not be descrambled; only clear channels may be viewed[1]
51	Writer Error (WE) occurs after completion of any transfer from Host to POD	POD or Host	Host performs POD reset	None	User may see frozen picture on scrambled channels[1]
52	Read Error (RE) occurs after completion of any transfer from POD to Host	POD or Host	Host performs POD reset	None	User may see frozen picture on scrambled channels[1]
53	POD fails to respond to any request within 5 seconds, other than described by error conditions 17 and 38	POD	Host performs PCMCIA reset up to two times and then reports error using the screen on page ##	None	User may see frozen picture on scrambled channels[1]
54	Invalid session APDU from host	Host	None	No Action	Not a failure condition
55	Invalid session APDU from POD	POD	Host ignores invalid sessions	None	Not a failure condition
56	Invalid SPDU tag from host	Host	None	No Action	Not a failure condition
57	Invalid SPDU tag from POD	POD	Host ignores invalid SPDU tags	None	Not a failure condition
58	Invalid APDU tag from host	Host	None	No Action	Not a failure condition
59	Invalid APDU tag from POD	POD	Host ignores invalid APDU tags	None	Not a failure condition

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
60	Transport ID from host that has not been created and confirmed by POD	Host	None	No Action	Not a failure condition
61	Transport ID from POD that has not been created by host	POD	Host ignores transport IDs that have not been created	None	Not a failure condition
62	Session ID from Host that has not been created and confirmed by POD	Host	None	No Action	Not a failure condition
63	Session ID from POD that has not been created by host	POD	Host ignores session IDs that have not been created	None	Not a failure condition
64	Incompatible POD inserted	Host	Reports error using an on-screen error display	None	Used when a single stream card is inserted into a multi-stream or multi-tuner host
65	Card Resource Limit Reached	Card	Reports error using an on-screen display	None	Used when the stream, program, or PID limit has been reach by a user-initiated action

[1] This condition is detected during certification if the error is caused by an issue with the design of the host or POD module.

4

Customer Information

If You Have Questions

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

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

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

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

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc. trademarks used in this document.
Product and service availability are subject to change without notice.

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

September 2012 Printed in USA

Part Number 78-4011765-01 Rev C