



# Setting Up PowerKEY CableCARD and M-Card Modules on the DNCS For System Release 2.7.1/3.7.1/4.2.1



# Please Read

## Important

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

# Notices

## Trademark Acknowledgements

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

CableLabs and DOCSIS are registered trademarks of Cable Television Laboratories, Inc.

CableCARD, M-Card, OpenCable, and tru2way 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. (1009R)

## Publication Disclaimer

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

## Copyright

© 2008, 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
What's New for CableCARD and M-Card Modules in SR	
2.7.1/3.7.1/4.2.1 .....	vi
Audience .....	vi
Related Publications .....	vii
Document Version .....	vii

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

PowerKEY CableCARD and M-Card Modules Supported .....	2
Configure the DNCS for CableCARD and M-Card Support.....	3
Introduction.....	3
Process Overview.....	3
Before You Begin.....	3
Loading the EMM CD .....	4
Setting Up the DNCS for tru2way (OpenCable) Compliance .....	4
Understand Binding Types .....	7
Configuring the CableCARD Server on the DNCS.....	10
Configuring the MMI Screen for M-Card Modules and Two-Way	
Hosts.....	14
Configuring the Emergency Alert System (EAS) to Properly Function	
with the CableCARD and M-Card Modules.....	17
Verifying Installation of the CableCARD or M-Card Module .....	19

## Chapter 2 Manage the CableCARD and M-Card Modules 21

Configure Copy Protection Authorization on the DNCS .....	22
CableCARD and M-Card Module and Host Copy Protection Binding .....	22
Editing the CableCARD or M-Card Module and Host in the DNCS.....	26
Maintain the Host Certification Revocation List .....	27
Return CableCARD or M-Card Modules from Service .....	29
Removing Conditional Access Services from the CableCARD and	
M-Card Modules.....	29

**Chapter 3 Identify Error Handling Conditions 31**

Identifying Error Handling Conditions ..... 32

    Introduction..... 32

    Error Conditions ..... 32

**Chapter 4 Customer Information 47**

# About This Guide

## Introduction

The PowerKEY® CableCARD™ module and the PowerKEY Multi-Stream CableCARD module (M-Card™) are unique hardware modules developed to provide subscribers with controlled conditional access to secure, digital content. Whether paired with an SSC (Separable Security Host with CableCARD module) Digital Home Communications Terminal (DHCT), 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 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 Release (SR) 2.7.1/3.7.1/4.2.1 or later, and one or more of the following PowerKEY CableCARD or M-Card modules:

- PKM600 PowerKEY Single-Stream CableCARD Module
- PKM800 and/or PKM802 PowerKEY Multi-Stream CableCARD Module (M-Card)

## What's New for CableCARD and M-Card Modules in SR 2.7.1/3.7.1/4.2.1

SR 2.7.1/3.7.1/4.2.1 includes the following new features:

- New CableCARD GUIs on the DNCS
- Out-of-band system information (SI) now carries a Daylight Saving Time (DST) descriptor for cable hosts with CableCARD or M-Card modules.

In earlier system releases, every DHCT received the default hub DST rule regardless of the hub to which they were associated. Beginning with SR 2.7.1/3.7.1/4.2.1, users can define specific DST rules for each hub that distributes DST rules out-of-band (OOB). Every CableCARD Host that receives DST rules out-of-band will be able to receive a specific DST rule that is tailored for its hub.

**Important:** This feature does not affect DST rules that are distributed by Program and System Information Protocol (PSIP). It also does not affect legacy DHCTs that do not include CableCARD modules. In these situations, DHCTs will continue to receive the DST rule for the default hub.

Users must create a DST rule to define the start and end dates for DST and assign the DST rule to a hub, just as they did in earlier system releases.

The SCTE 65 requirements mandate support for DST descriptors for OOB system information (SI). The DNCS implements support for this feature by populating the OOB SI daylight saving time (DST) descriptor based on the hub DST zone.

## Audience

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



## Related Publications

You may find the following publications useful as resources when you implement the procedures in this document.

- *Best Practices for Using Single-Stream PowerKEY CableCARD Modules* (part number 4015091)
- *Best Practices for Using Multi-Stream CableCARD Modules* (part number 4005658)
- *DNCS Online Help, (PC), 4.2.1.0* (part number 4017651)\*
- *Downloading New Client Application Platform Installation Instructions* (part number 4003052)
- *Enabling Content Protection for Broadcast Programming Configuration Guide* (part number 4005893)
- *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375)
- *The PowerKEY CableCARD Module Installation Instructions, Model PKM600* (part number 736104)
- *The PowerKEY CableCARD Module Installation Instructions, Models PKM800 and PKM802* (part number 745460)
- *Recommendations for Data Carousel Rate Management* (part number 716377)
- *Separable Security Host Staging Guide* (part number 736107)
- *System Release 2.7.1 Release Notes* (part number 4001524)
- *System Release 3.7.1 Release Notes* (part number 4001525)
- *System Release 4.2.1 Release Notes* (part number 4002179)

\* The *DNCS Online Help, (UNIX), 4.2.1.0* should already be installed on our DNCS. The PC version is a separate CD that allows you to view the same online Help on a PC separate from the DNCS workstation.

## Document Version

This is the first release of this guide.



# 1

---

## Set Up the CableCARD or M-Card Module

### Introduction

This chapter provides procedures to set up the CableCARD module and the M-Card module to function properly on a DNCS running SR 2.7.1/3.7.1/4.2.1.

### In This Chapter

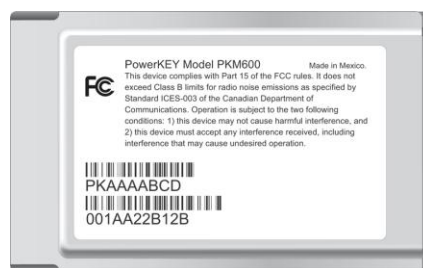
- PowerKEY CableCARD and M-Card Modules Supported ..... 2
- Configure the DNCS for CableCARD and M-Card Support..... 3

## PowerKEY CableCARD and M-Card Modules Supported

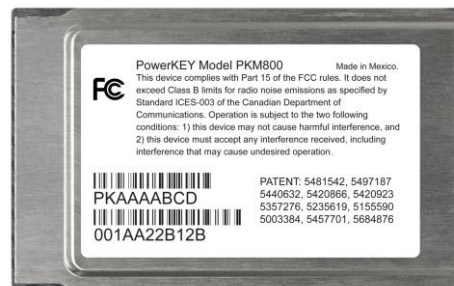
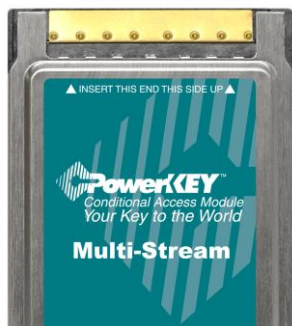
The following illustrations show the front and back views of the PowerKEY CableCARD and M-Card modules described in this document.

**Note:** These illustrations may vary slightly in appearance from the actual product.

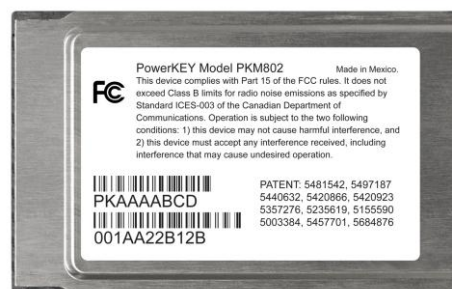
### PKM600 PowerKEY CableCARD Module (blue background)



### 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 CableCARD or M-Card modules to function properly, you must initially configure the DNCS. The following steps summarize the configuration process. (Detailed configuration 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 3).

- 1 Load the EMM CD (or download the EMMs from our 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* (part number 734375) or the *Separable Security Host Staging Guide* (part number 736107) for more information.
- 2 Set up the DNCS for tru2way™ (formerly called OpenCable™) compliance.
- 3 Understand the binding methods offered by the DNCS.
- 4 Configure the CableCARD server on the DNCS.
- 5 Configure the MMI Screen for M-Card modules and two-way hosts.
- 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 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, you can obtain the EMM keys through our Customer Self-Service website.

**Note:** Refer to the *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375) for detailed instructions for obtaining and loading EMMs using the Customer Self-Service website.

## Loading the EMM CD

The EMM CD or the EMM file you obtained from the Customer Self-Service website includes one or more of the following CableCARD or M-Card module 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* (part number 734375). Then confirm that the correct CableCARD or M-Card module 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 tru2way (OpenCable) Compliance

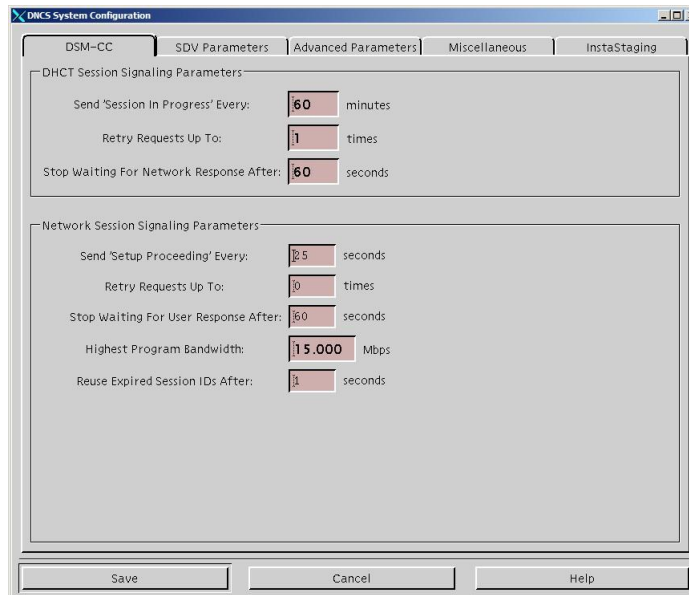
Setting up the DNCS for the tru2way (OpenCable) compliance industry standard allows the secure and removable CableCARD and M-Card modules to be both available and portable to set-tops and other hosts. This section contains procedures to set up the DNCS for tru2way (OpenCable) compliance.

### Configure Your Site for tru2way (OpenCable) Compliance

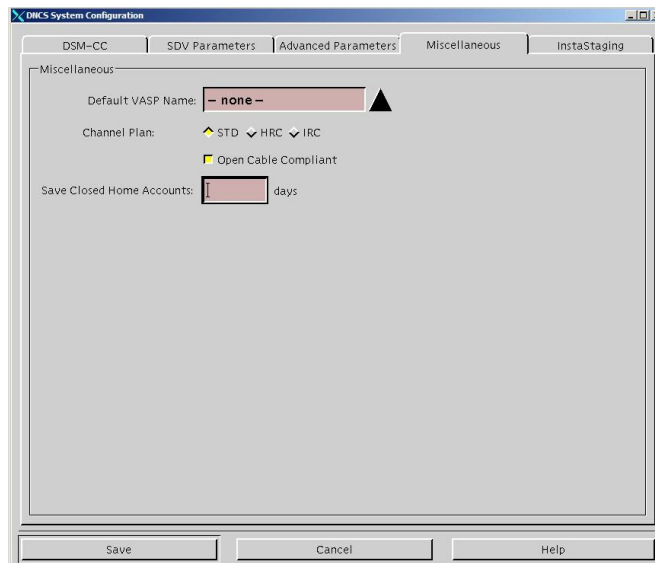
Complete these steps to configure the site you are upgrading for tru2way (OpenCable) compliance.

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

- 3 In the System Management area, click **Sys Config**. The DNCS System Configuration window opens



- 4 Select the **Miscellaneous** tab.
- 5 Select the **Open Cable Compliant** option. A yellow highlight appears in the Open Cable Compliant field.



- 6 Click **Save**. The Open Cable Compliance Warning message appears.



- 7 Click **OK** to close the Open Cable Compliance Warning message.

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

- Click **Close** on the DNCS System Configuration window. The DNCS System Configuration window closes.
- Go to *Stopping and Restarting the siManager Process* (on page 6).

### Stopping and Restarting the siManager Process

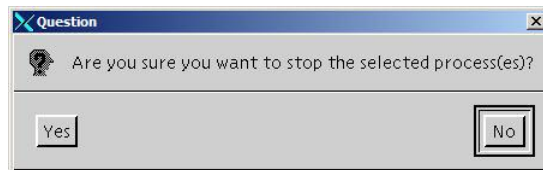
The System Information Manager (siManager) generates SI tables. The SI tables provide service information to CableCARD modules and hosts, M-Card modules and hosts, set-top CableCARD hosts, and set-top M-Card hosts. To finish updating your system in order to support tru2way (OpenCable) technology, you 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.

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



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

## Understand Binding Types

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

**Important:**

- Until you bind the host and the CableCARD or M-Card module, the host will not be able to display "high-value" copy-protected services—even if the CableCARD or M-Card 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 if conditional access is authorized.

The following copy protection binding methods are available on your system:

- **Autobinding** matches a CableCARD or M-Card module and host when the CableCARD or M-Card module is inserted into a host that supports two-way communications. Autobinding will be supported if all of the following conditions are met:

- The DNCS is configured to support autobinding.
- The host supports two-way communications.
- The CableCARD or M-Card module obtains an IP address.

**Note:** To support autobinding, the CableCARD or M-Card module and host must be bound in a two-way environment. Once bound, they may be operated in a one-way environment to view high-value content.

- The host is not on the certificate revocation list (CRL).
- If autobinding with a different host, then the CableCARD or M-Card's host change count should not equal or exceed the system's Max Host Change Count Allowed setting.

- **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.
- **Manual binding** allows binding of the CableCARD module and host from either the DNCS or from the billing system. From the DNCS, the CableCARD module ID and host ID are added 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.

This section provides a description for each option.

### Autobinding

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

- 1 When the CableCARD or M-Card module is inserted into a two-way host, the host and the CableCARD or M-Card module exchange keys to authenticate each other.
- 2 The CableCARD or M-Card module initiates the UNConfig process to obtain an IP address. After the keys are verified and the CableCARD or M-Card module obtains an IP address, the CableCARD or M-Card module sends an upstream message to the DNCS that includes the CableCARD or M-Card 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 or M-Card module to bind to the host.
  - If the host is not in the list, the DNCS updates the podData file which grants permission for the CableCARD or M-Card module to bind to the host.
- 4 The DNCS updates the podData file.
- 5 The CableCARD or M-Card reads the podData file on the BFS. Based on the information in the file, the CableCARD or M-Card module takes one of the following actions:
  - If the CableCARD or M-Card module finds its pairing in the authorized list, the CableCARD or M-Card module authorizes the binding between itself and the host.
  - If the CableCARD or M-Card module finds its pairing in the unauthorized list, or if it does not find its pairing in either list, the CableCARD or M-Card module does not authorize the binding.

### Combo-Binding

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

**Note:** The DNCS populates its database with the SSC pairing information from the inventory file during the batch load process.

- 1 The SSC DHCT and its paired CableCARD or M-Card module exchange keys to authenticate each other.
- 2 The DNCS sends the pairing information (as a file named podData) to the BFS when EMMs are sent to the CableCARD or M-Card module for the first time. 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 or M-Card module.
- 3 The CableCARD or M-Card module reads the pairing information from the file. If the CableCARD or M-Card 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.

### Important:

- 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 are running SR 2.7/3.7/4.2 Service Pack 0.2 or later.
- The host/pair will only be in the file as long as the authorization timeout value indicates.

**Note:** For additional details about binding types, refer to the *Separable Security Host Staging Guide* (part number 736107).

### Manual Binding

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

## 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.

**Important:** This procedure also configures the DNCS for autobinding. To disable autobinding, go to *Disabling Autobinding* (on page 16).

**Note:** For additional details on configuring CableCARD and M-Card modules, refer to the *Separable Security Host Staging Guide* (part number 736107) or to the *DNCS Online Help*.

- 1 From the DNCS Administrative Console, select the **DNCS** tab.
- 2 Select the **Home Element Provisioning** tab and then click **CableCARD**. The Define CableCARD Filter screen opens in a Web browser.

Filter	Value
CableCARD ID:	<input type="text"/>
CableCARD MAC:	<input type="text"/>
Host ID:	<input type="text"/>
Host MAC:	<input type="text"/>

- 3 Click **Configure CableCARD Server**. The Define CableCARD Filter screen updates to display the Configure CableCARD Server 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 Server 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 correct port number in the Port Number field. The suggested port for this field is **13830**.
- **Authorization Time-out Period:** The time (in hours) that the CableCARD/host pair authorization data is broadcast via the podData BFS file after copy protection authorization is granted from the DNCS.

**Important:**

- We recommend that you set this value to **2**.
- Negative values are not permitted in this field.
- If you define a value greater than 2, be aware of the following issues:
  - The podData file can contain no more than 1,500 entries. During staging a CableCARD/host pair is added to the podData file for the amount of time defined in this field. When the Authorization Timeout Period is reached, the CableCARD/host pair is removed from the file.
  - If you attempt to exceed 1,500 entries during the timeout period you have defined, then CableCARD/host pairs will be unable to CP bind.

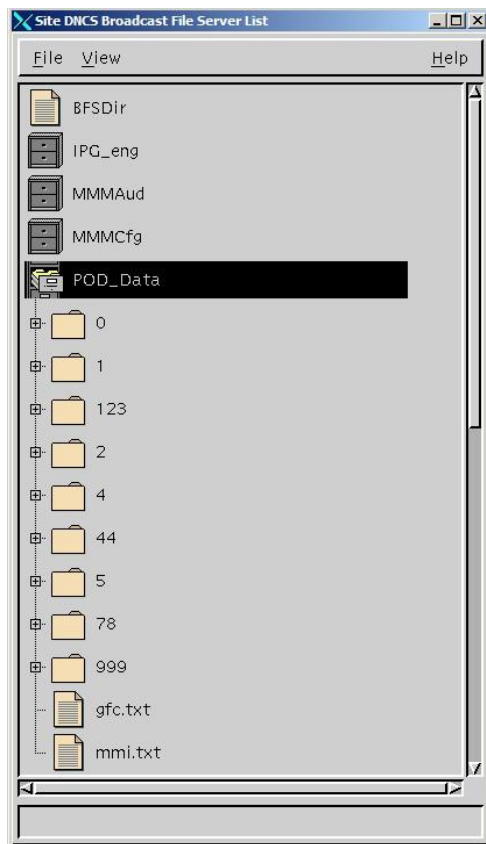
- **DeAuthorization Time-out Period:** The time period (in days) that the CableCARD/host pair deauthorization data is broadcast via the CableCARD BFS file after the copy protection deauthorization is saved using the DNCS.  
**Important:** We recommend that you set this value to **30**. If this value is too large, it could interfere with the total number of authorization entries that can be added to the podData file and could also interfere with the CP binding of CableCARD/host pairs.
- **Max Key Session Period:** The rate at which copy protection keys are refreshed for the CableCARD and M-Card modules. These keys are copy protected and exchanged between the CableCARD module and the host.  
For CableCARD and M-Card modules operating in single-stream mode, typing 1 (one) equals a 10 second time period. For M-Card modules operating in multi-stream mode, the units for this value represent minutes. For example, typing 1 equals a 1 minute (60 second) time period.  
**Important:** We recommend that you set this value to **10**. Defining a rate less than 10 requires a large number of unnecessary calculations on the CableCARD. Defining a rate greater than 20 does not coincide with best security practices.  
**Note:** A setting of **0** (zero) indicates that the copy protection keys never refresh.
- **Maximum Host Change Count Allowed:** The maximum number of times that a CableCARD or M-Card module is allowed to autobind with a different host. When a module's Host Change Count equals this limit, it will no longer be allowed to autobind with a different host. You can enter a value in the range of **0** (zero) to **99**.  
**Important:** This feature is *not* supported in this release.
- **RF Output:** The channel over which the SSC DHCT Host delivers its RF output signal (for example, the Cable Out port will use this channel for its output signal). Suggested channel choice for this field is **Channel 3**.

- **Card Authorization Phone Number:** The phone number that is 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 provider who can verify that the CableCARD module was authorized.

**Important:**

- You can enter up to 20 alphanumeric characters (including spaces and punctuation) in this field.
- The phone number shown is an example only. Type the telephone number that is unique to your system.

**Note:** The mmi.txt and gfc.txt files no longer need to be created manually. They are automatically created and attached to the BFS as shown in the following example.



- 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 MMI Screen for M-Card Modules and Two-Way Hosts

The Set CableCARD MMI Copy Protection screen allows you to customize the information that is presented in the CableCARD Man-Machine Interface Copy Protection (MMI CP) screen by any host containing M-Card modules. The conditions under which two-way hosts display this screen are defined on this screen as well.

The main purpose of the MMI CP screen is to prompt subscribers to call and authorize their M-Card module. Information about the M-Card module and host along with any other information that is useful in verifying correct M-Card installation may be displayed in this screen. Any changes saved in this screen are saved in a file that is linked on the BFS Client as **POD\_Data/0/CPDefinition.tblo**.

If this file is not linked to the BFS, then the M-Card module will use the phone number in the mmi.txt file to present the original MMI screen format.

The Set CableCARD MMI Copy Protection (CP) screen allows you to make the following changes to the MMI Copy Protection (CP) screen that M-Card hosts display to subscribers:

- Create a customized message that the M-Card host displays to prompt subscribers to telephone for M-Card authorization.
- Configure the MMI CP screen to display information that is useful in verifying correct M-Card installation.
- Define the conditions under which the M-Card in a two-way host displays the MMI CP screen.
- Disable autobinding

This section describes how to display the Set CableCARD MMI Copy Protection screen so that you can view its settings and determine if they meet the needs of your system.



The following illustration is an example of the CableCARD MMI Copy Protection screen.

**Note:** Refer to the *DNCS Online Help* for a detailed description of the fields in the Set CableCARD MMI Copy Protection screen.

**Set CableCARD MMI Copy Protection**

**MMI Options**

☒ Display MMI for bi-directional device    ☐ Network failure operation -- Display CP MMI

Bidirectional timeout (decimal seconds): 180

**Choose Display Fields**

Line (0 = omit)	Field	Display Label	Available Options
14	Host MAC Address	Host MAC:	<input type="checkbox"/> One-way host <input checked="" type="checkbox"/> Two-way host
8	Host Copy Protection ID	Host ID:	
12	Cable Modem MAC Address	CM MAC:	<input type="checkbox"/> One-way Cable Modem <input checked="" type="checkbox"/> Two-way Cable Modem
6	CableCARD Copy Protection ID	CableCARD ID:	
10	Host Direction	Type:	One-way: One-Way Two-way: Two-Way
16	Host Attributes	Host Code:	

**Additional text -- indicate line number**

Line	Text	Line	Text
1	In order to start service for	2	this device please call
3	Ph: 808 -625 -8100	0	

Complete the following steps to display the Set CableCARD MMI Copy Protection screen.

**Important:** This procedure also configures the DNCS for autobinding. To disable autobinding go to *Disabling Autobinding* (on page 16).

- 1 Is the CableCARD Data Summary screen open?
  - If **yes**, go to step 5.
  - If **no**, go to step 2.
- 2 On the DNCS Administrative Console, click the **DNCS** tab.
- 3 Click the **Home Element Provisioning** tab.
- 4 Click **CableCARD**. The CableCARD Data Summary screen opens.
- 5 Click **MMI Screen Format**. The Set CableCARD MMI Copy Protection screen opens.
- 6 Refer to the *DNCS Online Help* for additional details on configuring the Set CableCARD MMI Copy Protection screen.

### Notes on MMI Options

The MMI Options section of the Set CableCARD MMI Copy Protection screen requires special attention. The following table illustrates the results of the selections you make in the MMI Options section.

Display MMI for bi-directional device	Bidirectional timeout (decimal setting)	Autobinding Enabled?	MMI screen displays on TV?
Checked	Set to zero (0)	No	Yes
Not checked	N/A	Yes	No
Checked	Set to a number that is > zero (0) <b>Note:</b> We recommend that this number be set to 180 seconds.	Yes (Attempts to autobind for the length of the Bidirectional timeout setting)	Yes (After the Bidirectional timeout period expires if CP authorization has not been received by the CableCARD or M-Card module)

**Note:** To disable autobinding, go to *Disabling Autobinding* (on page 16).

### Disabling Autobinding

- 1 Open the **Configure CableCARD Server** screen.
- 2 In the appropriate fields within the **Configure CableCARD Server** screen, complete the following steps.
  - a Change the CableCARD Server **IP Address** to all zeros (0.0.0.0).
  - b Change the CableCARD Server **Port Number** to zero (0).
  - c Click **Save CableCARD Server Configuration** on the left side of the screen to save these parameters.
- 3 Open the Set CableCARD MMI Screen Copy Protection Screen and complete the following steps.
  - a Check the **Display MMI for bi-directional device** box in the upper left section of the Set CableCARD MMI Copy Protection screen.
  - b Enter a **zero (0)** in the **Bidirectional timeout (decimal seconds)** box.
- 4 Click **Save**.

## 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.

Event Code	Message Content Type	Configuration Name
Administrative Message	ADR	Audio & Video
Avalanche Watch	AVA	Audio & Video
Avalanche Warning	AVW	Audio & Video
Blizzard Warning	BZW	Audio & Video
Child Abduction Emergency	CAE	Audio & Video
Civil Danger Warning	CDW	Audio & Video
Civil Emergency Message	CEM	Audio & Video
Coastal Flood Watch	CFA	Audio & Video
Coastal Flood Warning	CFW	Audio & Video
Practice/Demo Warning	DMO	Audio & Video

Buttons: Save, Edit Configuration, Cancel, Help

- 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.

Name: Default

Description:

Force Tune Type | Message Time | Alert Type | Display Type

Force Tune Type

Force Tune: None Default Service

Default Service: A&E

Priority: 3

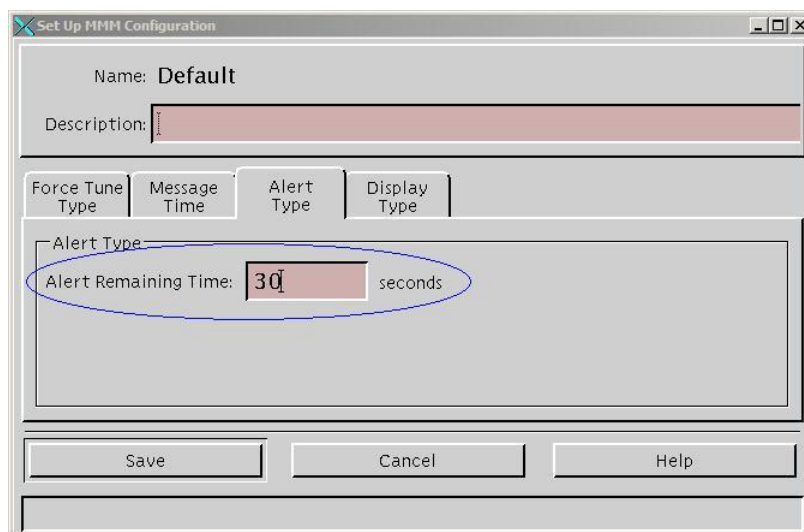
Priority 0 is for Test Messages.

Buttons: Save, Cancel, Help

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

- 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 tru2way (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:** We recommend 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:** We recommend that you test the EAS alert functionality each week.

## Verifying Installation of the CableCARD or M-Card Module

- 1 Connect your SSC DHCT device to the headend, or insert a CableCARD or M-Card module into the CableCARD module slot on a 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.
- 3 Verify that the MMI message displayed on the television screen includes the telephone number that is in the CableCARD Server Configuration user interface.

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

**Important:** If the CableCARD or M-Card module is already bound to the host, the MMI message will not appear on the TV.

### Notes:

- This message appears automatically on one-way hosts within a few minutes after inserting the CableCARD or M-Card module into the host.
  - This message appears automatically on two-way hosts within a few minutes after inserting the M-Card module into the host if the **Display MMI for bi-directional device** option is selected in the Set CableCARD MMI Copy Protection screen.
  - This message contains the information defined in the MMI CP screen for hosts with M-Card modules
  - This message contains the phone number defined in the CableCARD Server Configuration screen for hosts with CableCARD modules
- 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, 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 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 ..... 22
- Maintain the Host Certification Revocation List ..... 27
- Return CableCARD or M-Card Modules from Service ..... 29

## 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 (also known as "Manual" binding)
- Autobinding will be supported if all of the following conditions are met:
  - The DNCS is configured to support autobinding.
  - The host supports two-way communications.
  - The CableCARD or M-Card module obtains an IP address.

**Note:** To support autobinding, the CableCARD or M-Card module and host must be bound in a two-way environment. Once bound, they may be operated in a one-way environment to view high-value content.

- The host is not on the certificate revocation list (CRL).
  - If autobinding with a different host, then the CableCARD or M-Card's host change count should not equal or exceed the system's Max Host Change Count Allowed setting.
- Using the billing system interface. Contact your billing vendor to see if they support this option
- Combo-binding during staging of our set-tops that contain M-Card modules



## Adding a CableCARD or M-Card Module to the DNCS

- 1 On the DNCS Administrative Console, click the **Home Element Provisioning** tab, and then click **CableCARD**. The Define CableCARD Filter window opens.

CableCARD Data from flame - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://flame:8045/pod/podParentFrame.jsp?actionRequested=cableCardFilter

DNCS/CableCARD Filter

Scientific Atlanta

[New CableCARD](#)

[Open CableCARD](#)

[Configure CableCARD Server](#)

[Maintain CRL](#)

[MMI Screen Format](#)

[Exit all CableCARD Screens](#)

[Help](#)

## Define CableCard Filter

Filter	Value
CableCARD ID:	<input type="text"/>
CableCARD MAC:	<input type="text"/>
Host ID:	<input type="text"/>
Host MAC:	<input type="text"/>

Done

- 2** Click **New CableCARD** and the Add CableCARD window opens.

CableCARD Data from flame - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://flame:8045/pod/podParentFrame.jsp?serverName=%3C?=%20serverNameAndPort%20%: /

DNCS/CableCARD Filter/Add CableCARD

Scientific Atlanta

Save CableCARD

Exit all CableCARD Screens

Help

## Add CableCARD

CableCARD ID	CableCARD MAC Address	Active Time	Host Change Count
<input type="text"/>	<input type="text"/>		
Host MAC Address	Host ID	Encoded Host ID	Host Bound
<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> Yes <input type="radio"/> No	

Done

- 3 Write down the following information from the CableCARD diagnostic screens.

■ Host ID Diagnostic Screen

```
In order to start service for
this device, please contact
customer service at
Ph #(888) 123-4567

CableCARD(tm): 0-010-334-695-847
Host ID: 0-025-437-849-620
Host Type: Two-Way
Authorization: Received
```

CableCARD ID (labeled as CableCARD (tm) on the screen)\_\_\_\_\_

Host ID\_\_\_\_\_

■ Diagnostics

```
----- Diagnostics -----
-----
H/W Model: 0802 Ver: 0012
MAC addr: 00:0F:21:FF:22:FA
SL.No.: PKBBBQZRR, Mode: MMODE
Boot Time
Wed Apr 25 2007, 2:58:59 PM GMT
Current Time
Wed Apr 25 2007, 3:07:13 PM GMT
Free Memory: 670 kB
Bldr Ver: 121
OS Ver: 01.01.10P2
Build Time: Apr 16 2007, 11:34:17
Current Resource Status:3C1F3FBF
BFS: Received, Hub ID: 2

Next: CPU Channel, Generic Diags
```

CableCARD MAC Address\_\_\_\_\_

- 4 Choose and type either the CableCARD ID or the CableCARD MAC address into a field.

**Important:**

- 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 Type the Host ID number into the Host ID field.
- 6 When you are finished making changes, click **Save CableCARD**. The system saves the new information in the DNCS database and closes the Modify CableCARD window.
- 7 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.

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

- 8 When you are finished, click **Exit All CableCARD Screens** to close the 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.

**Important:** If you need to modify a parameter *other than* the CableCARD or M-Card host ID or the bind status, (for example, the CableCARD MAC Address or ID contains a typographical error), then you must delete the CableCARD or M-Card module using the **Delete Selected CableCARD** link on the CableCARD Data Summary screen and then re-enter the CableCARD or M-Card information.

**Note:** You will need at least *one* of the following device IDs or MAC address to complete this procedure.

- CableCARD ID
- CableCARD MAC address
- Host ID
- Host MAC address

For additional details on editing the CableCARD or M-Card module and its associated host device on the DNCS, refer to the *DNCS Online Help*.

## Maintain the Host Certification Revocation List

The Maintain CRL window allows you to keep track of the host devices that CableLabs has placed on its Certification Revocation List (CRL). Whenever CableLabs sends you a CRL, enter the hosts listed on the CableLabs CRL in the Maintain CRL window. By adding the hosts to the Maintain CRL window, you keep a comprehensive list of all host devices that CableLabs has identified should have their ability to decrypt copy-protected content revoked. In order to ensure that these devices cannot decrypt copy-protected content, you must unbind the module and host. Until the module and host are unbound, the module will remain authorized to decrypt copy-protected content.

If you have a CableCARD or an M-Card module associated with this host device (as shown when you select the **Show CableCARDS with Revoked Hosts** link), then the binding status of this host/pair should be manually updated in the CableCARD Data Summary table to "Host Bound = No" in order to revoke CPAuthorization. Note that a CableCARD/Host pair will continue to receive *copy freely* encrypted digital content even after CP Authorization has been revoked; therefore, it is recommended that this CableCARD or M-Card module's services be removed as described in the next section.

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

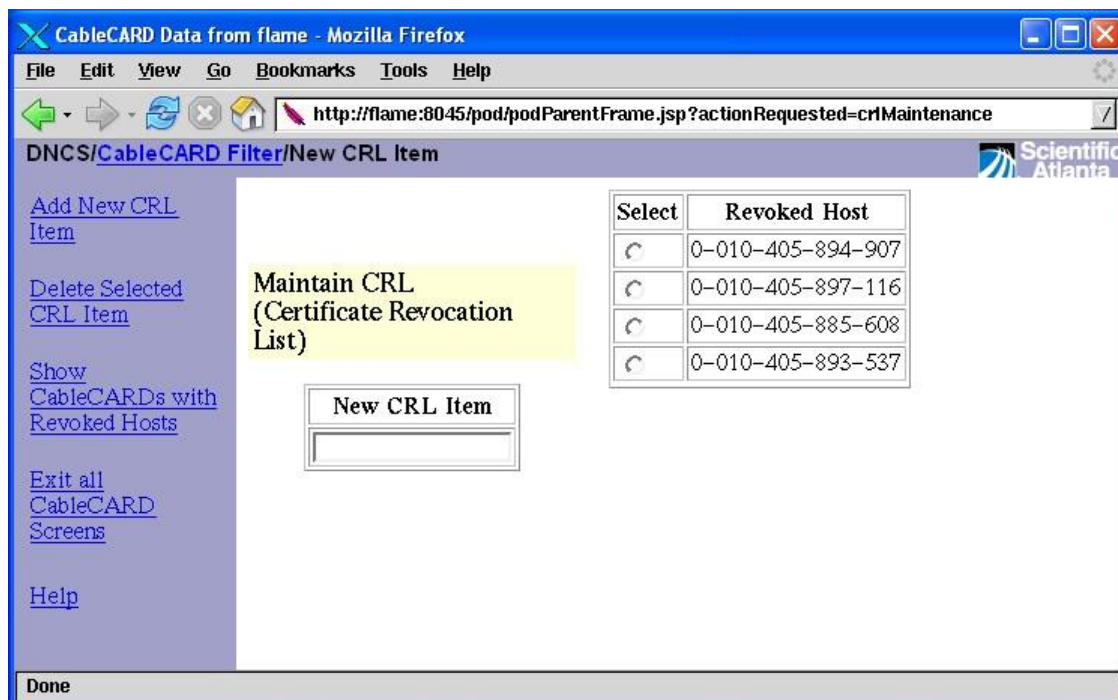
### Notes:

- Adding hosts to the CRL does not automatically change the binding status of the host/pair.
- You can also use this window to see which CableCARD or M-Card modules are associated with the host devices in the CRL.
- If a host device is removed from the CRL list by CableLabs, you can remove it from the CRL list.

### Maintaining the Host CRL

To maintain the host CRL, complete these steps.

- 1 From the Define CableCARD Filter screen, click **Maintain CRL** to view the Maintain CRL window.



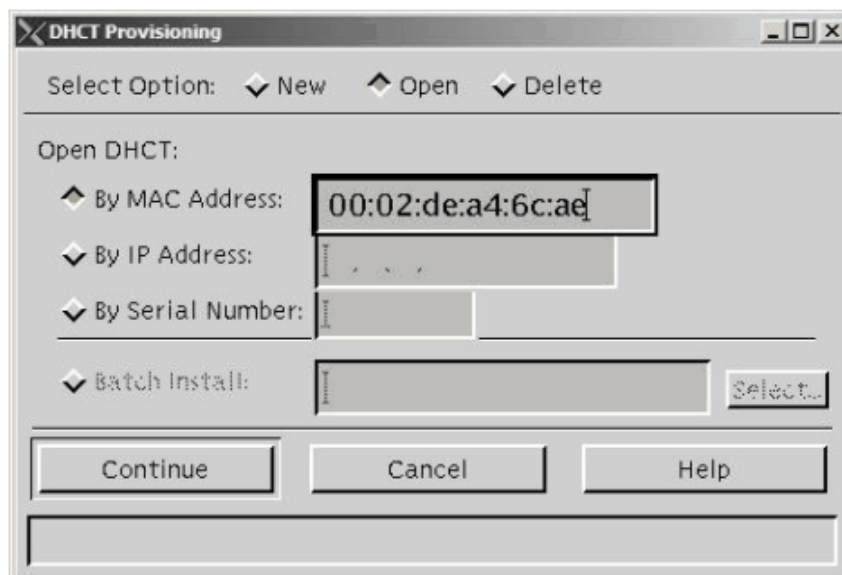
- 2 Perform one of the following functions:
  - Click **Add New CRL Item** to add a new host device to the CRL list.
  - Select a host from the **Revoked Host** list, and click **Delete Selected CRL Item** to remove a host from the CRL list.
  - Click **Show CableCARDs with Revoked Hosts** to see a complete list of hosts on the CRL list.
- 3 Refer to the *DNCS 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 screen.

## Return CableCARD or M-Card Modules from Service

When CableCARD or M-Card modules are taken out of service, you need only to remove the conditional access in order to deauthorize 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 conditional access using the billing system or the DNCS as described in the following procedure.

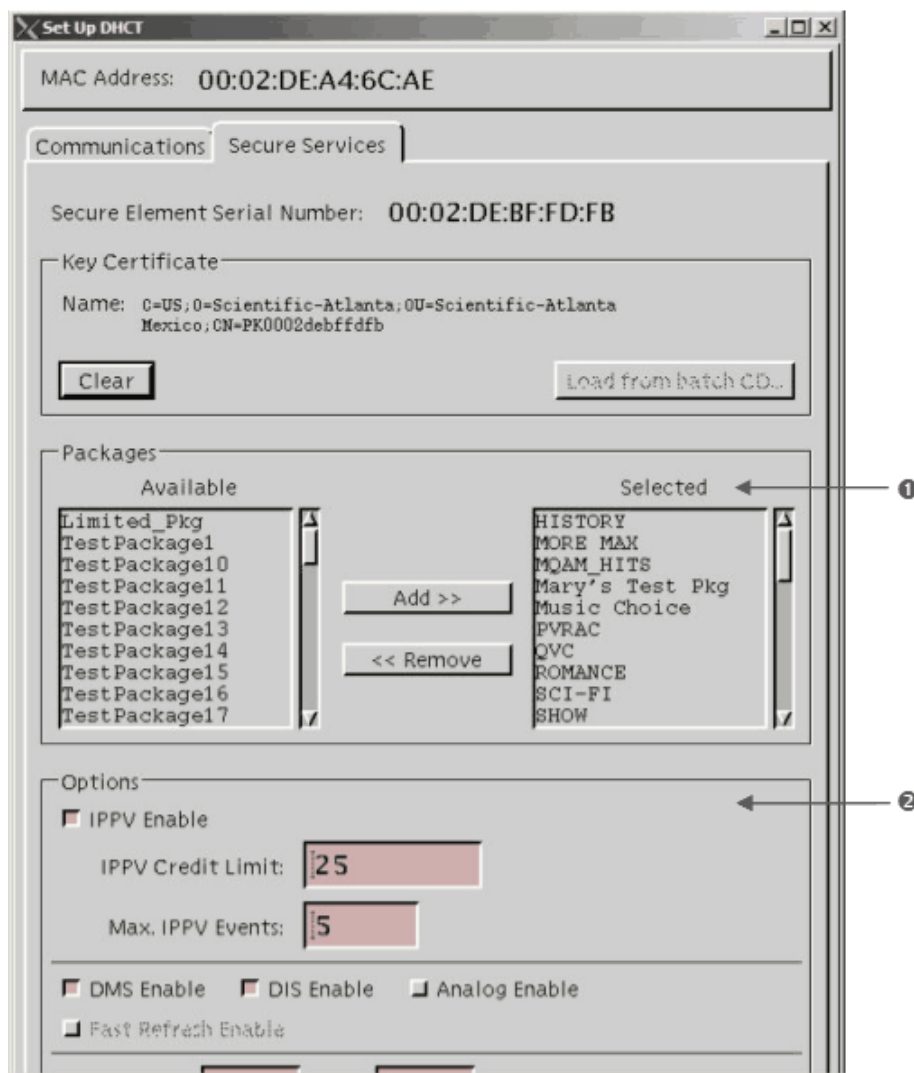
### Removing Conditional Access Services from the CableCARD and M-Card Modules

- 1 From the DNCS Administrative Console, select the **DNCS** tab, select the **Home 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 of 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.



# 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

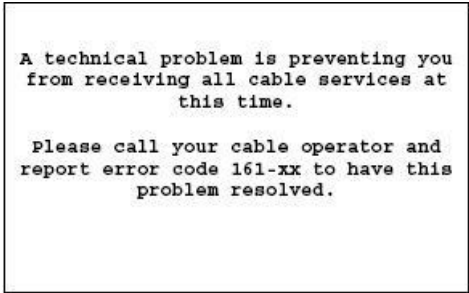
- Identifying Error Handling Conditions..... 32

## 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.



```
A technical problem is preventing you
from receiving all cable services at
this time.

Please call your cable operator and
report error code 161-xx to have this
problem resolved.
```

**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.

## Identifying Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
1	POD READY signal does not go active	POD	Host either: <ul style="list-style-type: none"> <li>■ Reports error message</li> <li>■ Retries PCMCIA resets up to two times and then reports error message</li> <li>■ Reports error, but continues to perform PCMCIA resets</li> </ul>	None	Host reports error to user <sup>1</sup>
2	Host reads incorrect CIS values	POD	Host reports error message	None	Host reports error to user <sup>1</sup>
3	Host writes incorrect TPCE_INDXX value to POD configuration register	Host	None	POD cannot perform any action	Host detects a failure #4 and reports error to user <sup>1</sup>
4	Host sets data channel RS bit, but POD fails to set FR bit within 5 second timeout	POD	Host either: <ul style="list-style-type: none"> <li>■ Reports error message</li> <li>■ Retries PCMCIA resets up to two times and then reports error message</li> <li>■ Reports error and continues to perform PCMCIA resets</li> </ul>	None	Host reports error to user <sup>1</sup>

### Chapter 3 Identify Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
5	Host sets extended channel RS bit, but POD fails to set FR bit within 5 second timeout	POD	Host either: <ul style="list-style-type: none"> <li>■ Reports error message</li> <li>■ Retries PCMCIA resets up to two times and then reports error message</li> <li>■ Reports error and continues to perform PCMCIA resets</li> </ul>	None	Host reports error to user <sup>1</sup>
6	<b>Invalid buffer negotiation</b> – POD data channel (buffer size < 16)	POD	Host either: <ul style="list-style-type: none"> <li>■ Reports error message</li> <li>■ Retries PCMCIA resets up to two times and then reports error message</li> <li>■ Operates with smaller size</li> </ul>	None	Host reports error to user <sup>1</sup>
7	<b>Invalid buffer negotiation</b> – Host data channel (buffer size < 16 or greater than POD data channel buffer size)	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls  <b>Preferred</b> -POD works with host buffer size	Host reports error to user <sup>1</sup>
8	<b>Invalid buffer negotiation</b> – POD extended channel (buffer size < 16)	POD	Host either: <ul style="list-style-type: none"> <li>■ Reports error message</li> <li>■ Retries PCMCIA resets up to two times and then reports error message</li> <li>■ Operates with smaller size</li> </ul>	None	Host reports error to user <sup>1</sup>

## Identifying Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
9	<b>Invalid buffer negotiation</b> – Host extended channel (buffer size < 16 or > POD data channel buffer size)	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls  <b>Preferred</b> -POD works with host buffer size	Host reports error to user <sup>1</sup>
10	POD does not respond to host's open transport request within 5 seconds	POD	Host either: <ul style="list-style-type: none"><li>■ Reports error message</li><li>■ Retries PCMCIA resets up to two times and then reports error message</li><li>■ Reports error and continues to perform PCMCIA resets</li></ul>	None	Host reports error to user <sup>1</sup>
11	Host does not respond to POD request to open resource manager session within 5 seconds	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls	Host reports error to user <sup>1</sup>
12	Host response to open resource manager session response – resource manager non-existent	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls	Host reports error to user <sup>1</sup>
13	Host response to open resource manager session response – resource manager unavailable	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls	Host reports error to user <sup>1</sup>
14	Host response to open resource manager session response – incorrect version of resource manager	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls	Host reports error to user <sup>1</sup>

### Chapter 3 Identify Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
15	Host response to open resource manager session response – resource manager busy	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls	Host reports error to user <sup>1</sup>
16	Host response to open resource manager session. response – invalid status byte	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls	Host reports error to user
17	POD fails to respond to profile_inq within 5 seconds	POD	Host either: <ul style="list-style-type: none"> <li>■ Reports error message</li> <li>■ Retries PCMCIA resets up to two times and then reports error message</li> <li>■ Reports error and continues to perform PCMCIA resets</li> </ul>	None	Host reports error to user <sup>1</sup>
18	Host resource response – no application information resource	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls <b>Preferred</b> -POD continues operation and will not open a session to the application info resource	<b>Minimum</b> -Host reports error to user <b>Preferred</b> -Applications on POD may not operate correctly, including MMI <sup>1</sup>
19	Host resource response – no Host control resource	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls	POD may not be able to do conditional access properly <b>Note:</b> There is a discussion ongoing about DOCSIS-only operations

## Identifying Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
20	Host resource response – no system time resource	Host	None	<b>Minimum</b> -POD continues operation and will not open a session to the system time resource  <b>Preferred</b> -Same as minimum, but also reports this in its MMI diagnostics application	POD operations that require system time will not operate <sup>1</sup>
21	Host resource response-no MMI resource	Host	None	<b>Minimum</b> -POD continues operation and will not open a session to the MMI resource	POD cannot initialize MMI for applications or to report error conditions <sup>1</sup>
22	Host resource response – no low speed communications	Host	None	<b>Minimum</b> -POD continues operation and will not open a session to the low speed communication resource  <b>Preferred</b> -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	<b>Minimum</b> -POD continues operation and will not open a session to the homing resource  <b>Preferred</b> -Same as minimum, but also reports this in its MMI diagnostic application	POD may have some operational problems (for example, downloading software)

### Chapter 3 Identify Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
24	Host resource response – no copy-protection resource	Host	None	<b>Minimum</b> -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 <sup>1</sup>
25	Host resource response – unknown resource identifier	Host	None	<b>Minimum</b> -POD continues operation	Not a failure condition
26	Host fails to respond to open session request within 5 seconds	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls	Host reports error to user <sup>1</sup>
27	Host response to open application info resource session – application info non-existent	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls <b>Preferred</b> -POD continues operation and will not open a session to the application info resource	<b>Minimum</b> – Host reports error to user <b>Preferred</b> – Applications on POD may not operate correctly, including MMI <sup>1</sup>
28	Host response to open application info resource session – application info unavailable	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls <b>Preferred</b> -POD continues operation and will not open a session to the application info resource	<b>Minimum</b> – Host reports error to user <b>Preferred</b> – Applications on POD may not operate correctly, including MMI <sup>1</sup>



## Identifying Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
29	Host response to open application info resource session – incorrect version of application info	Host	None	<b>Minimum-</b> POD sets IIR flag and stops responding to polls <b>Preferred-</b> POD continues operation and will not open a session to the application info resource	<b>Minimum-</b> Host reports error to user <b>Preferred-</b> Applications on POD may not operate correctly, including MMI <sup>1</sup>
30	Host response to open application info resource session – application info busy	Host	None	<b>Minimum-</b> POD sets IIR flag and stops responding to polls <b>Preferred-</b> POD continues operation and will not open a session to the application info resource	<b>Minimum-</b> Host reports error to user <b>Preferred-</b> Applications on the POD may not operate correctly, including MMI <sup>1</sup>
31	Host response to open application info resource session – invalid status byte	Host	None	<b>Minimum-</b> POD sets IIR flag and stops responding to polls <b>Preferred-</b> POD continues operation and will not open a session to the application info resource	<b>Minimum-</b> Host reports error to user <b>Preferred-</b> Applications on the POD may not operate correctly, including MMI <sup>1</sup>
32	POD module requests to open conditional access session to the Host times-out after 5 seconds	Host	None	<b>Minimum-</b> POD sets IIR flag and stops responding to polls	Host reports error to user <sup>1</sup>

### Chapter 3 Identify Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
33	POD response to conditional access resource session – conditional access non-existent	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls <b>Preferred</b> -POD will not descramble, but will continue other operations and reports this in its MMI diagnostic application	<b>Minimum</b> -Host reports error to user <b>Preferred</b> -Scrambled channels are not viewed <sup>1</sup>
34	POD response to conditional access resource session – conditional access unavailable	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls <b>Preferred</b> -POD will not descramble, but will continue other operations and reports this in its MMI diagnostic application	<b>Minimum</b> -Host reports error to user <b>Preferred</b> -Scrambled channels are not viewed <sup>1</sup>
35	POD response to conditional access resource session – incorrect version of conditional access	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls <b>Preferred</b> -POD will not descramble, but will continue other operations and reports this in its MMI diagnostic application	<b>Minimum</b> -Host reports error to user <b>Preferred</b> -Scrambled channels are not viewed <sup>1</sup>

## Identifying Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
36	POD response to conditional access resource session – conditional access busy	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls <b>Preferred</b> -POD will not descramble, but will continue other operations and reports this in its MMI diagnostic application	<b>Minimum</b> -Host reports error to user <b>Preferred</b> -Scrambled channels are not viewed <sup>1</sup>
37	POD response to conditional access resource session - invalid status byte	Host	None	<b>Minimum</b> -POD sets IIR flag and stops responding to polls <b>Preferred</b> -POD will not descramble, but will continue other operations and reports this in its MMI diagnostic application	<b>Minimum</b> -Host reports error to user <b>Preferred</b> -Scrambled channels are not viewed <sup>1</sup>
38	POD fails to respond to ca_info_inq within 5 seconds	POD	Host either: <ul style="list-style-type: none"> <li>■ Reports error message</li> <li>■ Retry PCMCIA resets up to two times and then reports error message</li> <li>■ Reports error and continues to perform PCMCIA resets</li> </ul>	None	Host reports error to user <sup>1</sup>

### Chapter 3 Identify Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
39	POD module request to open copy-protection resource session to the host times-out after 5 seconds	Host	None	<b>Minimum</b> –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 <sup>1</sup>
40	Host response to open copy-protection resource session – copy protection non-existent	Host	None	<b>Minimum</b> –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 <sup>1</sup>
41	Host response to open copy-protection resource session – copy protection unavailable	Host	None	<b>Minimum</b> –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 <sup>1</sup>

## Identifying Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
42	Host response to open protection resource session-copy-protection busy	Host	None	<b>Minimum</b> - 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 <sup>1</sup>
43	Host response to open copy-protection resource session – invalid status byte	Host	None	<b>Minimum</b> -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 <sup>1</sup>
44	Host does not support POD's copy protection system	Host/POD incompatibility	None	<b>Minimum</b> -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 <sup>1</sup>

### Chapter 3 Identify Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
45	Host and POD do not mate	Host/POD incompatibility	None	<b>Minimum</b> –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 <sup>1</sup>
46	Host response to CP_sync – Host busy	Host	None	<b>Minimum</b> –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	<b>Minimum</b> –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	<b>Minimum</b> –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	<b>Minimum</b> –POD will cease descrambling of copy-protected channels	A copy-protected channel will stop being descrambled
50	Invalid Host certificate	Host	None	<b>Minimum</b> –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 <sup>1</sup>

## Identifying Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
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 <sup>1</sup>
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 <sup>1</sup>
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 <sup>1</sup>
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
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

### Chapter 3 Identify Error Handling Conditions

Error	Error Condition	Failure Mechanism	Host Action	SCTE POD Module Action	Comments
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 reached by a user-initiated action

<sup>1</sup> 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](http://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.

© 2008, 2012 Cisco and/or its affiliates. All rights reserved.

May 2012 Printed in USA

Part Number 4021652 Rev B