



CHAPTER 2

Cable Duplicate MAC Address Reject for the Cisco CMTS

Revised: February 5, 2007, OL-1467-08

Cisco IOS Release 12.3(21)BC introduces a DOCSIS 1.1-compliant and above security enhancement that helps to eliminate denial-of-service (DOS) attacks that are caused by cloned cable modems. A clone is presumed to be one of two physical cable modems on the same Cisco CMTS chassis with the same HFC interface MAC address. The cloned cable modem may be DOCSIS 1.0 or greater, and may be semi-compliant or non-compliant with portions of the DOCSIS specifications.

This feature is enabled by default on the Cisco CMTS, and has no associated command-line interface (CLI) configuration commands. This feature creates a new log message. By default, this message appears in the syslog, but may be moved into the cable layer2 event log using the configuration command **cable logging layer2events**.

This document describes the Cloned Cable Modem Security Detection feature, introduces the **cable privacy bpi-plus-enforce** command, and cites additional commands and supporting documentation on Cisco.com and the Internet.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Additional Information](#)” section on page 2-9.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Cable Duplicate MAC Address Reject](#)
- [Restrictions for Cable Duplicate MAC Address Reject](#)
- [Information About Cable Duplicate MAC Address Reject](#)
- [Enforcing DOCSIS BPI+ Compliance with Layer 2 Logging on the Cisco CMTS](#)
- [System Messages Supporting Cable Duplicate MAC Address Reject](#)
- [Command Reference](#)
- [Additional Information](#)

Prerequisites for Cable Duplicate MAC Address Reject

This feature entails the following behaviors and prerequisites on the DOCSIS-compliant network:

- The Cisco CMTS requires that the legitimate cable modem is DOCSIS 1.1 BPI+ compliant, meaning that it can come to one of the following four online states when provisioned with a DOCSIS configuration file containing at least one BPI+ related type/length value (TLV). For brevity, this document refers to these states as online(p_).
- The Cisco CMTS gives priority to any cable modem that registers to the Cisco CMTS in any of the following four states:
 - online(pt)
 - online(pk)
 - online(ptd)
 - online(pkd)

The Cisco CMTS drops registration requests from another device that purports to use the same MAC address as an already operational modem that is in one of these four states.

Restrictions for Cable Duplicate MAC Address Reject

- If the cable modem is not provisioned to use DOCSIS BPI+, as characterized by not coming online with the above initialization states of online(p_), then the existing behavior of the Cisco CMTS remains unchanged. The Cisco CMTS does not attempt to distinguish between two cable modems if the provisioning system does not provide a DOCSIS configuration file specifying BPI+ be enabled.
- When this feature is enabled on the Cisco CMTS, the Cisco CMTS issues security breach notice in a log message in the cable logging layer2events log, or the generic log if the **cable logging layer2events** command is not configured on the Cisco CMTS.

Information About Cable Duplicate MAC Address Reject

This section explores DOCSIS BPI+ security in relation to cloned cable modems, and the behavior of this feature in networks involving compliant and non-compliant cable modems.

- [BPI+ Security and Cloned Cable Modems](#)
- [Logging of Cloned Cable Modems](#)

BPI+ Security and Cloned Cable Modems

This feature prioritizes cable modems that are online with Baseline Privacy Interface Plus (BPI+) security over new cable modem registration requests that use the same cable modem MAC address. As a result, the legitimate cable modem with BPI+ security certificates that match the HFC MAC address do not experience service disruption, even should a non-compliant cable modem with the same HFC MAC address attempt to register.

The detection function requires that a cable modem use DOCSIS 1.1 or higher, and be provisioned with BPI+ enabled. That is, one BPI+ TLV must be included in the DOCSIS configuration file. All DOCSIS 1.0 and DOCSIS 1.1 or greater cable modems that are provisioned without DOCSIS BPI+ enabled continue to use the legacy DOCSIS behavior, and experience a DOS attack when a cloned cable modem appears on the Cisco CMTS.

Cisco IOS Release 12.3(21)BC also introduces the **cable privacy bpi-plus-enforce** command, which is required for complete security using the Cloned Cable Modem Detection feature. This command mandates that a cable modem provisioned with BPI+ and DOCSIS 1.1 QOS must register with BPI+ and not use BPI. Commonly available non-DOCSIS-compliant cable modems contain an option to force registration in BPI as opposed to BPI+ mode even with DOCSIS 1.1 QOS and BPI+ specified in the DOCSIS configuration file.

Logging of Cloned Cable Modems

Cloned Cable Modems are detected and tracked with system logging. Due to the large number of DOCSIS layer 2 messages typically seen in a production network, a separate log is available to segregate these messages. If the **cable logging layer2events** command in global configuration mode is configured, Cloned Cable Modem messages are removed from the system log (syslog), and placed instead in the cable layer2logging.

A clone cable modem might attempt dozens of registration attempts in a short period of time. In order to suppress the number of log messages generated, the Cisco CMTS suppresses clone detected messages for approximately three minutes under certain conditions.

The log message provides the cable interface and MAC address of the cable modem attempting to register when another physical modem with that same MAC address is already in a state of online(P_) elsewhere on the Cisco CMTS.

Enforcing DOCSIS BPI+ Compliance with Layer 2 Logging on the Cisco CMTS

Perform these steps with the **cable privacy bpi-plus-enforce** command for the strongest DOCSIS BPI+ security and best performance of the Cloned Cable Modem Detection feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable privacy bpi-plus-enforce**
4. **cable logging layer2events**
5. **exit**
6. **show cable logging**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	cable privacy bpi-plus-enforce Example: Router(config)# cable privacy bpi-plus-enforce	Forces cable modems provisioned in DOCSIS 1.1 or higher to register with DOCSIS BPI+ security certificates, and not use the earlier DOCSIS BPI security.
Step 4	cable logging layer2events Example: Router# cable logging layer2events	Saves selected DOCSIS events that are specified in the Cisco CMTS MIB Registry to the cable logging buffer (instead of to the general logging buffer). This command supports Cloned Cable Modem Detection in Cisco IOS Release 12.3(21)BC and later releases.
Step 5	exit Example: Router(config)# exit Router#	Returns to Privileged EXEC mode.
Step 6	show cable logging Example: Router# show cable logging	Displays whether the Layer 2 Logging feature is enabled, and displays the status of the logging buffer.

Examples

The following brief example illustrates logging messages that are created with the detection of cloned cable modems. In this example, the clone modem came online just before the legitimate modem, and was taken offline according to the legacy behavior. (The cable modem was not in `online(p_)` state when another modem with the *same* MAC address attempted to come online.)

```
SLOT 7/0: Nov 14 12:07:26: %UBR10000-6-CMMOVED: Cable modem 0007.0e03.3e71 has been moved
from interface Cable7/0/1 to interface Cable7/0/0.
```

```
Nov 14 12:07:57: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
access detected at Cable7/0/0 interface
```

Refer to the [“System Messages Supporting Cable Duplicate MAC Address Reject”](#) section on page 2-5 for additional illustration of this feature and supporting system log messages.

What to Do Next

The Cloned Cable Modem Detection feature on the Cisco CMTS relates to multiple BPI+ certificate and DOCSIS 1.1 factors. Refer to additional information in this document for implementation of the Cloned Cable Modem Detection feature.

System Messages Supporting Cable Duplicate MAC Address Reject

The following example illustrates logged events for the Cloned Cable Modem Detection feature with activity that you may see with Cisco IOS Release 12.3(21)BC. This example uses the system image file `ubr10k2-k9p6u2-mz.12.3(21)BC` on a Cisco uBR10012 router with PRE2 modules.

In the below scenario, there are two cable modems with MAC addresses that have been cloned:

- For MAC address `000f.66f9.48b1`, the legitimate cable modem is on `C5/0/0` upstream 0, and the cloned cable modem is on `C7/0/0`.
- For MAC address `0013.7116.e726`, the legitimate cable modem is on `C7/0/0` upstream 0, and the cloned cable modem is also on the same interface.
- In the below example, the `CMMOVED` message occurred because the cloned cable modem for MAC address `000f.66f9.48b1` came online before the legitimate cable modem.
- There is no `CMMOVED` message for the cable modem on interface `C7/0/0` with MAC address `0013.7116.e726` because the legitimate cable modem came online with state of `online(pt)` before the cloned cable modem attempted to come online.

```
Dec 5 13:08:18: %UBR10000-6-CMMOVED: Cable modem 000f.66f9.48b1 has been moved from
interface Cable7/0/0 to interface C able5/0/0.
Dec 5 13:08:44: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
connection attempt rejected o n Cable7/0/0 U0
Dec 5 13:10:48: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 000f.66f9.48b1
connection attempt rejected on Cable7/0/0 U1
Dec 5 13:12:37: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
connection attempt rejected on Cable7/0/0 U0
Dec 5 13:18:28: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
connection attempt rejected on Cable7/0/0 U0
Dec 5 13:18:28: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
connection attempt rejected o n Cable7/0/0 U0
```

The following example of the **show cable modem** command illustrates additional cable modem information for the above scenario involving the specified MAC addresses:

```
Router# scm 000f.66f9.48b1
MAC Address      IP Address      I/F      MAC          Prim RxPwr  Timing Num BPI
                  IP Address      I/F      State        Sid   (dBmv)  Offset
CPE Enb
000f.66f9.48b1  4.222.0.253    C5/0/0/U0 online(pt)   24    0.50   1045    1   Y

Router# scm 0013.7116.e726
MAC Address      IP Address      I/F      MAC          Prim RxPwr  Timing Num BPI
                  IP Address      I/F      State        Sid   (dBmv)  Offset
CPE Enb
0013.7116.e726  4.175.0.18    C7/0/0/U0 online(pt)   4     0.00   1789    0   Y
```

Command Reference

This section describes commands that are introduced or enhanced in Cisco IOS Release 12.3(21) BC in support of the Cloned Cable Modem Detection feature.

cable privacy bpi-plus-enforce

To mandate that a cable modem provisioned in DOCSIS 1.1 or higher must register with DOCSIS Baseline Privacy Interface Plus (BPI+), and not use the earlier DOCSIS BPI, use the **cable privacy bpi-plus-enforce** command in global configuration mode. To remove this configuration, use the **no** form of this command.

cable privacy bpi-plus-enforce

no cable privacy bpi-plus-enforce



Note

Non-DOCSIS-compliant cable modems that are commonly available contain an option to force registration in DOCSIS BPI as opposed to DOCSIS BPI+ mode even in DOCSIS 1.1-provisioned networks.

Syntax Description

No additional keywords or arguments

Defaults

The **cable privacy bpi-plus-enforce** command is not enabled by default, but must be configured for optimal DOCSIS BPI+ security. There is no legitimate reason for a cable modem provisioned with DOCSIS 1.1 QOS to register with DOCSIS 1.0 BPI. Such behavior is not compliant with the DOCSIS 1.1 specification.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(21)BC	This command was introduced to support Cloned Cable Modem Detection for DOCSIS BPI+ on the Cisco uBR10012 and Cisco uBR7246VXR routers.

Usage Guidelines

If the cable modem is not provisioned to use DOCSIS BPI or BPI+ security certificates, as characterized by not coming online with the above initialization states, then the existing behavior of the Cisco CMTS remains unchanged. The Cisco CMTS does not attempt to distinguish between two cable modems if neither is provisioned for BPI+ security.

Because this feature is enabled by default on the Cisco CMTS, the Cisco CMTS issues security breach notice in a log message in the generic system log or syslog if **cable logging layer2events** is not configured on the Cisco CMTS.

Several additional guidelines for the **cable privacy bpi-plus enforce** command and the Cloned Cable Modem Detection feature are described in additional sections of this document.

Examples

The following brief example illustrates logging messages that are created with the detection of cloned cable modems behind the configuration in the above procedure.

```
SLOT 7/0: Nov 14 12:07:26: %UBR10000-6-CMOVED: Cable modem 0007.0e03.3e71 has been moved
from interface Cable7/0/1 to interface Cable7/0/0.
```

```
Nov 14 12:07:57: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
access detected at Cable7/0/0 interface
```

Refer to the [“System Messages Supporting Cable Duplicate MAC Address Reject”](#) section on page 2-5 for additional illustration of this feature and supporting system log messages.

Related Commands

Command	Description
cable logging layer2events	Saves selected (low priority) DOCSIS events that are specified in the Cisco CMTS MIB Registry to the cable logging buffer (instead of to the general logging buffer).
show cable logging	Displays the log of messages about bad IP source addresses or DOCSIS-layer events on the cable interfaces.
show cable modem	Displays information for registered and non-registered cable modems on the Cisco CMTS.

Additional Information

For additional information about BPI+ security, system messages, and DOCSIS 1.1 support, refer to the following documents:

- *Theft of Service—Inevitable?* Cable360.Net's article by Mark Millet of Cisco Systems, Inc.:
<http://www.cable360.net/ct/data/15302.html>
- *DOCSIS 1.1 for the Cisco CMTS*
http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html
- *Cisco Broadband Cable Command Reference Guide*
http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
- *Cisco CMTS System Messages*
<http://www.cisco.com/en/US/docs/cable/cmts/system/message/uberrmes.html>
- *Cisco CMTS MIB Specifications Guide*
<http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html>

