Cable Duplicate MAC Address Reject for the Cisco CMTS Router

First Published: February 14, 2008

Last Updated: November 29, 2010

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

The Cable Duplicate MAC Address Reject feature is a DOCSIS 1.1-compliant 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 router with the same HFC interface MAC address. The cloned cable modem may be DOCSIS 1.0 or later, and may be semi-compliant or non-compliant with portions of the DOCSIS specifications.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Cable Duplicate MAC Address Reject

The Cable Duplicate MAC Address Reject feature entails the following behaviors and prerequisites on the DOCSIS-compliant network:

- The Cisco CMTS router requires that the legitimate cable modem is Baseline Privacy Interface Plus (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 router gives priority to any cable modem that registers to the Cisco CMTS router in any of the following four states:

  - online(pt)
  - online(pk)
  - online(ptd)
  - online(pkd)

The Cisco CMTS router 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.

Table 1: Hardware Compatibility Matrix for Cable Duplicate MAC Address Reject, on page 3 shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for Cable Duplicate MAC Address Reject

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR10-MC5X20 Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [1]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [2]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

[1] Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

[2] Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

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 router remains

unchanged. The Cisco CMTS router 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, the Cisco CMTS router 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 router.

Information About Cable Duplicate MAC Address Reject

The Cable Duplicate MAC Address Reject feature is enabled by default on the Cisco CMTS router, and has no associated configuration commands. This feature creates a new log message, which appears in the system log by default.

This document also describes the following security features that are associated with the Cable Duplicate MAC Address Reject feature:

Early Authentication and Encryption

The Early Authentication and Encryption (EAE) feature enables the Cisco CMTS router to authenticate DOCSIS 3.0 cable modems immediately after completion of the ranging process, and encrypt all of the registration packets including DHCP and TFTP traffic. This security feature, compatible only with DOCSIS 3.0 cable modems, was introduced in Cisco IOS Release 12.2(33)SCC to help multiple service operators (MSOs) prevent theft of service.

This feature is enabled only for cable modems that initialize on a downstream channel on which the Cisco CMTS router is transmitting MAC Domain Descriptor (MDD) messages. The Cisco CMTS router uses TLV type 6 in the MDD MAC message to signal EAE to a cable modem. If this feature is enabled, only the authenticated cable modems are allowed to continue their initialization process and subsequently admitted to the network. The early authentication and encryption process involves the following:

- Authentication of the cable modem (that is the BPI+ authorization exchanges) after the ranging process.

- Traffic encryption key (TEK) exchanges for the cable modem primary Security Association Identifier (SAID).

- Encryption of IP provisioning traffic and Multipart Registration Request (REG-REQ-MP) messages during cable modem initialization.

Note When Early Authentication and Encryption is enabled, BPI will revert back to DES-56 even if the hardware supports AES-128.

EAE Enforcement Policies

The Cisco CMTS router supports the following EAE enforcement policies:

- No EAE enforcement (Policy 1)—EAE is disabled and the Cisco CMTS router cannot enforce EAE on any cable modem.

- Ranging-based EAE enforcement (Policy 2)—EAE is enforced on all DOCSIS 3.0 cable modems that range with a B-INIT-RNG-REQ MAC message.

- Capability-based EAE enforcement (Policy 3)—EAE is enforced on all DOCSIS 3.0 cable modems that range with a B-INIT-RNG-REQ MAC message in which the EAE capability flag is set using the .

- Total EAE enforcement (Policy 4)—EAE is enforced on all cable modems irrespective of the EAE capability flag status.

The EAE enforcement policies are mutually exclusive. By default, EAE is disabled on the Cisco CMTS router.

EAE Exclusion

You can exclude cable modems from EAE enforcement using the **cable privacy eae-exclude** command in the global configuration mode. Cable modems in the EAE exclusion list are always exempted from EAE enforcement. You can remove cable modems from the exclusion list using the no form of the **cable privacy eae-exclude** command.

BPI+ Security and Cloned Cable Modems

The BPI+ Security and Cloned Cable Modems feature prioritizes cable modems that are online with 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 does not experience service disruption, even if a non-compliant cable modem with the same HFC MAC address attempt to register.

The cloned cable modem detection function requires that a cable modem use DOCSIS 1.1 or a later version and should be provisioned with BPI+ enabled. That is, one BPI+ type, length, value (TLV) must be included in the DOCSIS configuration file. All DOCSIS 1.0, DOCSIS 1.1, and later 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 router.

This cloned cable modem detection function mandates that a cable modem provisioned with BPI+ and DOCSIS 1.1 QoS must register with BPI+ and not use BPI. The commonly available non-DOCSIS-compliant cable modems contain an option to force registration in BPI as opposed to BPI+ mode even when DOCSIS 1.1 QoS and BPI+ are specified in the DOCSIS configuration file.

Logging of Cloned Cable Modems

Cloned cable modems are detected and tracked with system logging. The Logging of Cloned Cable Modem feature is enabled by default. 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. By default, cloned cable modem messages are placed in the cable logger, cable layer2events logging. If you disable this feature using the no form of the **cable logging layer2events** command in global configuration mode, then the cloned cable modem messages are placed in the system log (syslog).

A cloned 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 router suppresses clone detected messages for approximately 3 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 router.

DOCSIS 3.0 BPI+ Policy Enforcement

The DOCSIS 3.0 BPI+ Policy Enforcement feature was introduced in Cisco IOS Release 12.2(33)SCD5 to prevent cable modem MAC address cloning and theft of service. This feature enables a Cisco CMTS router to validate the MAC address of each cable modem. To enforce BPI+ on cable modems, you must configure one of the following enforcement policies per MAC domain on the router:

- 1.1 Style Configuration File Parameters and Capability (Policy 1)—The Cisco CMTS router enforces BPI+ on cable modems that register with a DOCSIS 1.1 configuration file with parameters indicating BPI+ is enabled with or without TLV 29. To configure this policy, the privacy support modem capability TLV (type 5.6) in the DOCSIS configuration file must be set to BPI+ support. This policy forces BPI+ on a cable modem that is BPI+ capable and provisioned with DOCSIS1.1 configuration file. A cable modem that signals these capabilities during registration is blocked from accessing the network until the modem completes BPI+ negotiation.

- 1.1 Style Configuration File Parameters (Policy 2)—The Cisco CMTS router enforces BPI+ on cable modems that register with a DOCSIS 1.1 configuration file with parameters indicating BPI+ is enabled with or without TLV 29. A cable modem that registers with this type of configuration file is blocked from accessing the network until the modem completes BPI+ negotiation.

- 1.1 Style Configuration File (Policy 3)—The Cisco CMTS router enforces BPI+ on cable modems that register with a DOCSIS 1.1 configuration file. This means that if you provision a DOCSIS 1.1 configuration file with security disabled (privacy flag is not present in the configuration file), all DOCSIS 1.1 and 2.0 cable modems are blocked from accessing the network. Only the DOCSIS 3.0 cable modems that have security enabled implicitly will pass this check if the privacy flag is not present in the configuration file.

- Total enforcement (Policy 4)—The Cisco CMTS router enforces BPI+ on all cable modems. This means that all cable modems that do not run BPI+ are blocked from accessing the network.

Note You can configure only one enforcement policy at a time per MAC domain. If you configure one policy after another, the latest policy supersedes the already existing policy. For example, if you want Policy 2 to take over Policy 1, you can directly configure the former without disabling the latter.

These enforcement policies are implemented based on CableLabs Security Specification, CM-SP-SECv3.0-I13-100611. You can configure these enforcement policies using the **cable privacy bpi-plus-policy** command in cable interface configuration mode. The cable modems that do not comply with the configured policy can still come online but they cannot access the DOCSIS network and some dual stack cable modems may not get both the IPv4 and IPv6 addresses.

Policies 1, 2, and 3 support a mixed network of DOCSIS 1.0 (including DOCSIS Set-top Gateway), DOCSIS 1.1, and later cable modems. Policy 4 is the most effective configuration for preventing cable modem MAC address cloning as this policy enforces BPI+ on all cable modems. Policy 4 blocks all DOCSIS 1.0 cable modems as they do not register in BPI+ mode. Therefore, if Policy 4 is used, you must upgrade all authorized DOCSIS 1.0 cable modems or remove them from the network.

Note   The **cable privacy bpi-plus-policy** command replaced t**he cable privacy bpi-plus-enforce c**ommand in Cisco IOS Relase12.2(33)SCD5. If you upgrade from an earlier Cisco IOS Release to Cisco IOS Release 12.2(33)SCD5 and later, the existing BPI+ enforcement configuration is disabled by default during the upgrade. You must reconfigure the BPI+ enforcement policy using the **cable privacy bpi-plus-policy** command.

BPI+ Policy Enforcement Exclusion

You can exclude cable modems (DOCSIS 1.0 and later versions) from BPI+ policy enforcement based on their MAC addresses, using the **cable privacy bpi-plus-exclude** command in global configuration mode. You can exclude a maximum of 30 cable modems per MAC domain.

How to Configure EAE and BPI+ Enforcement Features

This section provides information on how to configure the following BPI+ enforcement features:

Configuring EAE Enforcement Policies

By default, EAE is disabled on the Cisco CMTS router. You can configure EAE enforcement policies using the **cable privacy eae-policy** command in cable interface configuration mode.

Note   EAE enforcement policies are enabled only for the DOCSIS 3.0 cable modems that initialize on a downstream channel.

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** `Router> `**`enable`**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# `**`configure terminal`**	Enters global configuration mode.
Step 3	**interface cable** {*slot*/*cable-interface-index* | *slot*/*subslot*/*cable-interface-index*} **Example:** `Router(config)# `**`interface cable 6/0/1`**	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**cable privacy eae-policy {capability-enforcement | disable-enforcement | ranging-enforcement | total-enforcement}** **Example:** Router(config-if)# **cable privacy eae-policy total-enforcement**	Specifies EAE enforcement policies on DOCSIS 3.0 cable modems.
Step 5	**end** **Example:** Router(config)# **end**	Returns to privileged EXEC mode.

Enforcing DOCSIS BPI+ Compliance on the Cisco CMTS Router

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

Note Beginning with Cisco IOS Release 12.2(33)SCD5, BPI+ enforcement configuration using the cable privacy bpi-plus-enforce command is not supported. In Cisco IOS Release 12.2(33)SCD5 and later, you will have to configure BPI+ enforcement policies using the cable privacy bpi-plus-policy command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. • 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 DOCSIS 1.1 or later cable modems to register with DOCSIS BPI+ security certificates, and not use the earlier DOCSIS BPI security.

	Command or Action	Purpose
Step 4	**exit** **Example:** Router(config)# **exit** Router#	Returns to privileged EXEC mode.
Step 5	**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 enforcing DOCSIS BPI

The following 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
```

For additional information about this feature and supporting system log messages, see the System Messages Supporting Cable Duplicate MAC Address Reject, on page 12.

Configuring BPI+ Enforcement Policies

The BPI+ enforcement policies are configured per MAC domain to prevent cable modem MAC address cloning and theft of service.

Before You Begin

The customer premise equipment (CPE) must use DHCP to acquire IP addresses to access the network, or the statically assigned IP addresses must be managed appropriately.

Note   Only a single enforcement policy can be applied per MAC domain. If you upgrade from an earlier Cisco IOS Release to Cisco IOS Release 12.2(33)SCD5 and later, the existing BPI+ enforcement configuration is disabled by default during the upgrade. You must reconfigure BPI+ enforcement policy using the **cable privacy bpi-plus-policy** command.

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal**	Enters global configuration mode.
Step 3	**interface cable** *{slot/subslot/port |slot/port}* **Example:** Router(config)# **interface cable 5/1/0**	Specifies the cable interface line card on a Cisco CMTS router.
Step 4	**cable privacy bpi-plus-policy {capable-enforcement | d11-enabled-enforcement | d11-enforcement | total-enforcement}** **Example:** Router (config-if)# **cable privacy bpi-plus-policy total-enforcement**	Specifies the BPI+ enforcement policies per MAC domain.
Step 5	**end** **Example:** Router(config-if)# **end**	Returns to Privileged EXEC mode.

Troubleshooting Tips

Use the following debug commands to troubleshoot BPI+ policy enforcement configuration:

  • **debug cable mac-address**—Provides debugging information about a specific cable modem.

  • **debug cable bpiatp**—Enables debugging of the BPI handler.

Configuration Example for EAE and BPI+ Enforcement Policies

The following example shows how to configure an EAE enforcement policy on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface cable 8/1/0
Router (config-if)# cable privacy eae-policy capability-enforcement
Router (config-if)# cable privacy eae-policy ranging-enforcement
Router (config-if)# cable privacy eae-policy total-enforcement
```

The following example shows how to configure a BPI+ enforcement policy at slot/subslot/port 5/1/0 on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface cable 5/1/0
Router (config-if)# cable privacy bpi-plus-policy total-enforcement
```

Verifying EAE and BPI+ Enforcement Policies

Use the following show commands to verify EAE and BPI+ enforcement configurations:

- **show interface cable privacy**
- **show cable privacy**
- **show cable modem access-group**

To verify which EAE policy is configured on the Cisco CMTS router, use the **show interface cable privacy** command as shown in the following example:

```
Router# show interface cable 8/1/0 privacy eae-policy
EAE Configuration
 Policy: EAE Total Enforcement
```

To verify which cable modems are excluded from EAE enforcement on the Cisco CMTS router, use the **show cable privacy** command as shown in the following example:

```
Router# show cable privacy eae-exclude
EAE Exclusion List:
  MAC: 0019.474e.e80c Mask: ffff.ffff.ffff
  MAC: 0025.2eaf.6f26 Mask: ffff.ffff.ffff
```

To verify BPI+ enforcement policies, use the **show interface cable privacy** command as shown in the following example:

```
Router# show interface cable 3/1 privacy all
EAE Configuration
 Policy: EAE Enforcement disabled
KEK Configuration
 KEK lifetime: 604800
 Auth Infos: 0
 Auth Requests: 0, Auth Replies: 0
 Auth Rejects: 0, Auth Invalids: 0
 Packet Buffer Failures: 0
TEK Configuration
```

```
   TEK lifetime: 43200
   TEK Requests: 0, TEK Replies: 0
   TEK Rejects: 0, TEK Invalids: 0
   SAMap Requests: 0, SAMap Replies: 0
   SAMap Rejects: 0
Interface Configuration
 SelfSigned Trust: Untrusted
 Check Cert Validity Periods: True
```

To verify which cable modem is blocked by the Cisco CMTS router, use the show cable modem access-group command as shown in the following example. In this example, two cable modems (0025.2e2d.71fc and 0025.2e2d.7254) that do not comply with BPI+ policy requirements are blocked.

```
Router# show cable modem access-group
MAC Address IP Address Access-group
000e.9bb3.b868 19.19.1.2 N/A
0016.924f.8222 19.19.1.12 N/A
0025.2e2d.71fc 19.19.1.4 CMTS_PKT_FILTER_GROUP_255
0000.caad.109f 19.19.1.3 N/A
0025.2e2d.7254 19.19.1.14 CMTS_PKT_FILTER_GROUP_255
0000.cadb.2f56 19.19.1.6 N/A
0000.cae2.70fb 19.19.1.15 N/A
0000.caad.0da7 19.19.1.7 N/A
0022.ce89.c748 19.19.1.5 N/A
0014.04ba.c958 19.19.1.18 N/A
```

What to Do Next

The Cloned Cable Modem Detection feature relates to multiple BPI+ certificate and DOCSIS 1.1 factors.

System Messages Supporting Cable Duplicate MAC Address Reject

The following example illustrates logged events for the Cloned Cable Modem Detection feature 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# show cable modem 000f.66f9.48b1
MAC Address    IP Address      I/F        MAC        Prim RxPwr  Timing Num BPI
                                          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
```

Additional References

Related Documents

Related Topic	Document Title
DOCSIS 1.1	DOCSIS 1.1 for the Cisco CMTS Routers
Commands on the Cisco CMTS routers	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Standards

Standard	Title
CM-SP-SECv3.0-I13-100611	Data-Over-Cable Service Interface Specifications DOCSIS 3.0 Security Specification

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cable Duplicate MAC Address Reject

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 2: Feature Information for Cable Duplicate MAC Address Reject

Feature Name	Releases	Feature Information
BPI+ Security and Cloned Cable Modems	12.2(33)SCA	This feature prioritizes cable modems that are online with BPI+ security over new cable modem registration requests that use the same cable modem MAC address. The following sections provide information about this feature: The following commands were introduced or modified: • **cable privacy bpi-plus-enforce** • **cable logging layer2events** • **show cable logging** • **show cable modem**
Early Authentication and Encryption (EAE)	12.2(33)SCC	The EAE feature enables the Cisco CMTS router to authenticate cable modems immediately after completion of the ranging process, and encrypt all of the registration packets including DHCP and TFTP traffic. The following sections provide information about this feature: The following commands were introduced or modified: • **cable privacy eae-exclude** • **cable privacy eae-policy** • **show cable privacy** • **show interface cable privacy**

Feature Name	Releases	Feature Information
DOCSIS 3.0 BPI+ Policy Enforcement	12.2(33)SCD5	The DOCSIS 3.0 BPI+ Policy Enforcement feature was introduced in Cisco IOS Release 12.2(33)SCD5 to prevent cable modem MAC address cloning and theft of service. The following commands were introduced or modified: • **cable privacy bpi-plus-policy** • **cable privacy bpi-plus-exclude**