Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

First Published: 2020-09-30

Americas Headquarters

C O N T E N T S

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

iii

CHAPTER 2 **Lawful Intercept Architecture** **27**

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

iv

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

v

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

vi

CHAPTER 7 **Subscriber Management Packet Filtering Extension for DOCSIS 2.0** **97**

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

vii

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

viii

Dynamic Shared Secret

This document describes the Dynamic Shared Secret feature, which enables service providers to provide higher levels of security for their Data-over-Cable Service Interface Specifications (DOCSIS) cable networks. This feature uses randomized, single-use shared secrets to verify the DOCSIS configuration files that are downloaded to each cable modem.

The Dynamic Shared Secret feature automatically creates a unique DOCSIS shared secret on a per-modem basis, creating a one-time use DOCSIS configuration file that is valid only for the current session. This ensures that a DOCSIS configuration file that has been downloaded for one cable modem can never be used by any other modem, nor can the same modem reuse this configuration file at a later time.

This patented feature is designed to guarantee that all registered modems use only the quality of service (QoS) parameters that have been specified by the DOCSIS provisioning system for a particular modem at the time of its registration. This feature is an accepted DOCSIS standard.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

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

Contents

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

1

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note

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

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Prerequisites for Dynamic Shared Secret

The configuration of Dynamic Shared Secret feature is supported on the Cisco CMTS routers.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

2

Following is a list of other important prerequisites for the Dynamic Shared Secret feature:

- The Cisco CMTS must be running Cisco IOS-XE 3.15.0S or later.

- The Dynamic Shared Secret feature supports an external provisioning server.

- A cable modem must be able to register with the Cisco CMTS before enabling the Dynamic Shared Secret feature.

- For full security, DOCSIS configuration files should have filenames that are at least 5 or more characters in length.

- For best performance during the provisioning of cable modems, we recommend using Cisco Network Registrar Release 3.5 or later.

Note   When the Dynamic Shared Secret feature is enabled using its default configuration, a cable modem diagnostic webpage shows a scrambled name for its DOCSIS configuration file. This filename changes randomly each time that the cable modem registers with the CMTS. To change the default behavior, use the **nocrypt** option with the **cable dynamic-secret** command.

Restrictions for Dynamic Shared Secret

General Restrictions for Dynamic Shared Secret

- Shared-secret and secondary-shared-secret cannot be configured with Dynamic Shared Secret feature.

- If you configure the Dynamic Shared Secret feature on a primary cable interface, you should also configure the feature on all of the corresponding subordinate cable interfaces.

- The Dynamic Shared Secret feature ensures that each cable modem registering with the CMTS can use only the DOCSIS configuration file that is specified by the service provider's authorized Dynamic Host Configuration Protocol (DHCP) and TFTP servers, using the DOCSIS-specified procedures.

- The Dynamic Shared Secret feature does not affect cable modems that are already online and provisioned. If a cable modem is online, you must reset it, so that it reregisters, before it complies with the Dynamic Shared Secret feature.

- The DMIC lock mode uses the following behavior during a switchover event in HCCP N+1 Redundancy. All cable modems which were previously in lock mode are taken offline during a switchover event, and the prior state of locked modems is lost. If previously locked modems remain non-compliant, they will return to LOCK mode after three failed registration attempts. If the modems have become DOCSIS compliant, they will return online in the normal fashion. Refer to the SNMP Support, on page 9 for additional information about DMIC lock mode.

- If a Broadband Access Center for Cable (BACC) provisioning server is being used, the Device Provisioning Engine (DPE) TFTP server verifies that the IP address of the TFTP client matches the expected DOCSIS cable modem IP Address. If a match is not found, the request is dropped. This functionality is incompatible with the CMTS DMIC feature. Use the no tftp verify-ip command on all BACC DPE servers to disable the verification of the requestor IP address on dynamic configuration TFTP requests. Refer to the Cisco

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

3

Broadband Access Centre DPE CLI Reference in the http://www.cisco.com/c/en/us/td/docs/net_mgmt/broadband_access_center_for_cable/4-0/command/reference/DPECLIRef40.html for additional information.

Cable Modem Restrictions for Dynamic Shared Secret

DHCP Restriction for Incognito Server and Thomson Cable Modems

The Dynamic Host Configuration Protocol (DHCP) passes configuration information to DHCP hosts on a TCP/IP network. Configuration parameters and other control information are stored in the options field of the DHCP message.

When using DMIC with the Incognito DHCP server, the Incognito server must be re-configured so that the following two options are *not* sent in the DHCP message:

- *option 66* —This option is used to identify a TFTP server when the sname field in the DHCP header has been used for DHCP options. Option 66 is a variable-length field in the Options field of a DHCP message described as "an option used to identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options" as per RFC 2132.
- *sname field* —The sname field is a 64-octet field in the header of a DHCP message described as "optional server host name, null terminated string," as per RFC2131. A DHCP server inserts this option if the returned parameters exceed the usual space allotted for options. If this option is present, the client interprets the specified additional fields after it concludes interpretation of the standard option fields.

Note It is not compliant with DOCSIS to include both of these options in the DHCP message.

The problematic packet capture below is a DHCP offer in which both sname and option 66 are set (in this respective sequence):

```
0000  00 30 19 47 8f 00 00 d0 b7 aa 95 50 08 00 45 00
0010  01 4a 8f 50 00 00 80 11 46 30 ac 10 02 01 ac 10
0020  0a 01 00 43 00 43 01 36 0c 75 02 01 06 00 b0 a0
0030  25 01 00 00 00 00 00 00 00 00 ac 10 0a 53 00 00
0040  00 00 ac 10 0a 01 00 10 95 25 a0 b0 00 00 00 00
0050  00 00 00 00 00 00 5b 31 37 32 2e 31 36 2e 32 2e
(sname option immediately above)
0060  31 5d 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090  00 00 00 00 00 00 64 65 66 61 75 6c 74 2e 63 66
00a0  67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110  00 00 00 00 00 00 63 82 53 63 35 01 02 36 04 ac
0120  10 02 01 33 04 00 06 94 0d 01 04 ff ff ff 00 02
0130  04 ff ff b9 b0 03 08 ac 10 02 fe ac 10 0a 01 04
0140  04 ac 10 02 01 07 04 ac 10 02 01 42 0a 31 37 32
(option 66 immediately above)
0150  2e 31 36 2e 32 2e 31 ff
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

4

When using DMIC with Incognito DHCP servers and Thomson cable modems, you must prevent both options from being sent in the DHCP offer. Use one of the following workaround methods to achieve this:

- Change the Incognito DHCP server so that it does not include the sname option as described above.
- Change the cable modem code so that sname is not prioritized above option 66, as in the problematic packet capture shown in the example above.
- Migrate to a compliant DHCP and TFTP server such as CNR. This also offers significantly higher performance.

Refer to these resources for additional DOCSIS DHCP information, or optional DHCP MAC exclusion:

- *DHCP Options and BOOTP Vendor Extensions, RFC 2132*

http://www.ietf.org/rfc/rfc2132.txt

- *Filtering Cable DHCP Lease Queries on Cisco CMTS Routers*

http://www.cisco.com/en/US/docs/cable/cmts/feature/cblsrcvy.html

DOCSIS Compliance

- Cable modems are assumed to be DOCSIS-compliant. If a cable modem is not fully DOCSIS-compliant, it could trigger a CMTS Message Integrity Check (MIC) failure during registration in rare circumstances. Under normal operations, however, it can be assumed that cable modems that fail the CMTS MIC check from the Dynamic Shared Secret feature are either not DOCSIS-compliant, or they might have been hacked by the end user to circumvent DOCSIS security features.

Some of the cable modems with the following OUIs have been identified as having problems with the Dynamic Shared Secret feature, depending on the hardware and software revisions:

- - 00.01.03
    - 00.E0.6F
    - 00.02.B2

These particular cable modems can remain stuck in the init(o) MAC state and cannot come online until the Dynamic Shared Secret feature is disabled. If this problem occurs, Cisco recommends upgrading the cable modem's software to a fully compliant software revision.

Alternatively, these cable modems may be excluded from the *dynamic* secret function using the following command in global configuration mode:

cable dynamic-secret exclude

Excluding cable modems means that if a violator chooses to modify their cable modem to use one of the excluded OUIs, then the system is no longer protected. Refer to the #unique_16.

Tip   To help providers to identify non-DOCSIS compliant modems in their network, the Dynamic Shared Secret feature supports a "mark-only" option. When operating in the mark-only mode, cable modems might be able to successfully obtain higher classes of service than are provisioned, but these cable modems will be marked as miscreant in the **show cable modem** displays (with **!online**, for example). Such cable modems also display with the **show cable modem rogue** command. Service providers may decide whether those cable modems must be upgraded to DOCSIS-compliant software, or whether the end users have hacked the cable modems for a theft-of-service attack.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

5

The following example illustrates output from a Cisco CMTS that is configured with the **cable dynamic-secret mark** command with miscreant cable modems installed. These cable modems may briefly show up as "reject(m)" for up to three registration cycles before achieving the **!online** status.

```
Router# show cable modem rogue
                                    Spoof TFTP
MAC Address     Vendor      Interface  Count Dnld Dynamic Secret
000f.0000.0133 00.0F.00    C4/0/U1    3     Yes  905B740F906B48870B3A9C5E441CDC67
000f.0000.0130 00.0F.00    C4/0/U1    3     Yes  051AEA93062A984F55B7AAC979D10901
000f.0000.0132 00.0F.00    C4/0/U2    3     Yes  FEDC1A6DA5C92B17B23AFD2BBFBAD9E1
vxr#scm | inc 000f
000f.0000.0133 4.174.4.101    C4/0/U1  !online      1    -7.00 2816    0   N
000f.0000.0130 4.174.4.89     C4/0/U1  !online      2    -6.50 2819    0   N
000f.0000.0132 4.174.4.90     C4/0/U2  !online      18   -7.00 2819    0   N
```

TFTP Restrictions

- Cable modems can become stuck in the TFTP transfer state (this is indicated as init(o) by the **show cable modem** command) in the following situation:

  - The Dynamic Shared Secret feature is enabled on the cable interface, using the **cable dynamic-secret** command. This feature applies if the cable modem is a miscreant cable modem, or if the cable modem is a DOCSIS 1.0 cable modem running early DOCSIS 1.0 firmware that has not yet been updated. This feature also applies if the TFTP server is unable to provide the cable modem's TFTP configuration file to the Cisco CMTS. This is the case, for example, when using BACC and not configuring the system to permit a TFTP request from a non-matching source IP address. The **debug cable dynamic-secret** command also shows this failure.
  - A large number of cable modems are registering at the same time. Some or all of those cable modems could also be downloading the DOCSIS configuration file using multiple TFTP transfers that use multiple TFTP ports on the Cisco CMTS router, and the TFTP server is unable to keep up with the rate of TFTP requests generated by the system. Some TFTP servers may be limited to the number of concurrent TFTP get requests initiated by the same source IP address per unit time, or simply unable to handle the rate of new modem registrations before cable dynamic-secret is configured. The **debug cable dynamic-secret** command shows failure to receive some files in this situation.

This situation of stuck cable modems can result in the TFTP server running out of available ports, resulting in the cable modems failing the TFTP download stage. To prevent this situation from happening, temporarily disable the Dynamic Shared Secret feature on the cable interface or reduce the size of the DOCSIS configuration file.

Information About Dynamic Shared Secret

The DOCSIS specifications require that cable modems download, from an authorized TFTP server, a DOCSIS configuration file that specifies the quality of service (QoS) and other parameters for the network session. Theft-of-service attempts frequently attempt to intercept, modify, or substitute the authorized DOCSIS configuration file, or to download the file from a local TFTP server.

To prevent theft-of-service attempts, the DOCSIS specification allows service providers to use a shared secret password to calculate the CMTS Message Integrity Check (MIC) field that is attached to all DOCSIS configuration files. The CMTS MIC is an MD5 digest that is calculated over the DOCSIS Type/Length/Value (TLV) fields that are specified in the configuration file, and if a shared secret is being used, it is used in the MD5 calculation as well.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

6

The cable modem must include its calculation of the CMTS MIC in its registration request, along with the contents of the DOCSIS configuration file. If a user modifies any of the fields in the DOCSIS configuration file, or uses a different shared secret value, the CMTS cannot verify the CMTS MIC when the cable modem registers. The CMTS does not allow the cable modem to register, and marks it as being in the "reject(m)" state to indicate a CMTS MIC failure.

Users, however, have used various techniques to circumvent these security checks, so that they can obtain configuration files that provide premium services, and then to use those files to provide themselves with higher classes of services. Service providers have responded by changing the shared secret, implementing DOCSIS time stamps, and using modem-specific configuration files, but this has meant creating DOCSIS configuration files for every cable modem on the network. Plus, these responses would have to be repeated whenever a shared secret has been discovered.

The Dynamic Shared Secret feature prevents these types of attacks by implementing a dynamically generated shared secret that is unique for each cable modem on the network. In addition, the dynamic shared secrets are valid only for the current session and cannot be reused, which removes the threat of "replay attacks," as well as the reuse of modified and substituted DOCSIS configuration files.

Modes of Operation

The Dynamic Shared Secret feature can operate in three different modes, depending on what action should be taken for cable modems that fail the CMTS MIC verification check:

- Marking Mode—When using the **mark** option, the CMTS allows cable modems to come online even if they fail the CMTS MIC validity check. However, the CMTS also prints a warning message on the console and marks the cable modem in the **show cable modem** command with an exclamation point (!), so that this situation can be investigated.
- Locking Mode—When the **lock** option is used, the CMTS assigns a restrictive QoS configuration to CMs that fail the MIC validity check twice in a row. You can specify a particular QoS profile to be used for locked cable modems, or the CMTS defaults to special QoS profile that limits the downstream and upstream service flows to a maximum rate of 10 kbps.

If a customer resets their CM, the CM will reregister but still uses the restricted QoS profile. A locked CM continues with the restricted QoS profile until it goes offline and remains offline for at least 24 hours, at which point it is allowed to reregister with a valid DOCSIS configuration file. A system operator can manually clear the lock on a CM by using the **clear cable modem lock** command.

This option frustrates users who are repeatedly registering with the CMTS in an attempt to guess the shared secret, or to determine the details of the Dynamic Shared Secret security system.

- Reject Mode—In the reject mode, the CMTS refuses to allow CMs to come online if they fail the CMTS MIC validity check. These cable modems are identified in the **show cable modem** displays with a MAC state of "reject(m)" (bad MIC value). After a short timeout period, the CM attempts to reregister with the CMTS. The CM must register with a valid DOCSIS configuration file before being allowed to come online. When it does come online, the CMTS also prints a warning message on the console and marks the cable modem in the **show cable modem** command with an exclamation point (!), so that this situation can be investigated.

Note To account for possible network problems, such as loss of packets and congestion, the Cisco CMTS will allow a cable modem to attempt to register twice before marking it as having failed the Dynamic Shared Secret authentication checks.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

7

Operation of the Dynamic Shared Secret

The Dynamic Shared Secret feature automatically creates a unique DOCSIS shared secret on a per-modem basis, creating a one-time use DOCSIS configuration file that is valid only for the current session. This ensures that a DOCSIS configuration file that has been downloaded for one cable modem can never be used by any other modem, nor can the same modem reuse this configuration file at a later time.

This patent pending feature is designed to guarantee that all registered modems are using only the QOS parameters that have been specified by the DOCSIS provisioning system for that particular modem at the time of its registration.

When a DOCSIS-compliant cable modem registers with the CMTS, it sends a DHCP request, and the DHCP server sends a DHCP response that contains the name of the DOCSIS configuration file that the cable modem should download from the specified TFTP server. The cable modem downloads the DOCSIS configuration file and uses its parameters to register with the CMTS

When the Dynamic Shared Secret feature is enabled, the CMTS performs the following when it receives the DHCP messages:

- The CMTS creates a dynamically generated shared secret.
- In the default configuration, the CMTS takes the name of the DOCSIS configuration file and generates a new, randomized filename. This randomized filename changes every time the cable modem registers, which prevents the caching of DOCSIS configuration files by cable modems that are only semi-compliant with the DOCSIS specifications. You can disable this randomization of the filename by using the **nocrypt** option with the **cable dynamic-secret** command.
- The CMTS changes the IP address of the TFTP server that the cable modem should use to the IP address of the CMTS. This informs the cable modem that it should download its configuration file from the CMTS.
- The CMTS downloads the original DOCSIS configuration file from the originally specified TFTP server so that it can modify the file to use the newly generated dynamic secret.

When the cable modem downloads the DOCSIS configuration file, it receives the modified file from the CMTS. Because this file uses the one-time-use dynamically generated shared secret, the CMTS can verify that the cable modem is using this configuration file when it attempts to register with the CMTS.

Note The Dynamic Shared Secret feature does not support and is incompatible with, the use of the original shared secret or secondary shared secrets that are configured using the **cable shared-secondary-secret** and **cable shared-secret** commands.

Tip Although a user could attempt to circumvent these checks by downloading a DOCSIS configuration file from a local TFTP server, the cable modem would still fail the CMTS MIC verification.

Interaction with Different Commands

The Dynamic Shared Secret feature works together with a number of other commands to ensure network security and integrity:

- **cable shared-secret**—The DOCSIS specification allows service providers to use a shared-secret to ensure that cable modems are using only authorized DOCSIS configuration files.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

8

The Dynamic Shared Secret feature is incompatible with **cable shared-secret**. Do not configure the **cable shared-secret** command when using the Dynamic Shared Secret feature

- **cable shared-secondary-secret**— The Dynamic Shared Secret feature is incompatible with **cable shared-secret**. Do not configure the **cable secondary-shared-secret** command when using the Dynamic Shared Secret feature

Performance Information

The Dynamic Shared Secret feature does not add any additional steps to the cable modem registration process, nor does it add any additional requirements to the current provisioning systems. This feature can have either a small negative or a small positive effect on the performance of the network provisioning system, depending on the following factors:

- The provisioning system (DHCP and TFTP servers) being used
- The number of cable modems that are coming online
- The vendor and software versions of the cable modems
- The number and size of the DOCSIS configuration files

Large-scale testing has shown that the Dynamic Shared Secret feature can affect the time it takes for cable modems to come online from 5% slower to 10% faster. The most significant factor in the performance of the provisioning process is the provisioning system itself. For this reason, Cisco recommends using Cisco Network Registrar (CNR) Release 3.5 or greater, which can provide significant performance improvements over generic DHCP and TFTP servers.

The second-most important factor in the performance of cable modem provisioning is the number and size of the DOCSIS configuration files. The size of the configuration file determines how long it takes to transmit the file to the cable modem, while the number of configuration files can impact how efficiently the system keeps the files in its internal cache, allowing it to reuse identical configuration files for multiple modems.

SNMP Support

Cisco IOS-XE 3.15.0S and later releases add the following SNMP support for the Dynamic Shared Secret feature:

- Adds the following MIB objects to the CISCO-DOCS-EXT-MIB:

    - cdxCmtsCmDMICMode—Sets and shows the configuration of the Dynamic Shared Secret feature for a specific cable modem (not configured, mark, lock, or reject).
    - cdxCmtsCmDMICLockQoS—Specifies the restrictive QoS profile assigned to a cable modem that has failed the Dynamic Shared Secret security checks, when the interface has been configured for lock mode.
    - cdxCmtsCmStatusDMICTable—Lists all cable modems that have failed the Dynamic Shared Secret security checks.

- An SNMP trap (cdxCmtsCmDMICLockNotification) can be sent when a cable modem is locked for failing the Dynamic Shared Secret security checks. The trap can be enabled using the **snmp-server enable traps cable dmic-lock** command.

Note   The DMIC lock mode is disabled during a switchover event in HCCP N+1 Redundancy.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

9

System Error Messages

The following system error messages provide information about cable modems that have failed the CMTS Message Integrity Check (MIC) when the Dynamic Shared Secret feature is enabled.

Message

%CBR-4-CMLOCKED

The cable modem's DOCSIS configuration file did not contain a Message Integrity Check (MIC) value that corresponds with the proper Dynamic Shared Secret that was used to encode it. The CMTS has, therefore, assigned a restrictive quality of service (QoS) configuration to this cable modem to limit its access to the network. The CMTS has also locked the cable modem so that it will remain locked in the restricted QoS configuration until it goes offline for at least 24 hours, at which point it is permitted to reregister and obtain normal service (assuming it is DOCSIS-compliant and using a valid DOCSIS configuration file).

This error message appears when the **cable dynamic-secret lock** command has been applied to a cable interface to enable the Dynamic Shared Secret feature for the DOCSIS configuration files on that cable interface. The cable modem has been allowed to register and come online, but with a QoS configuration that is limited to a maximum rate of 10 kbps for both the upstream and downstream flows. Check to ensure that this cable modem is not running old software that caches the previously used configuration file. Also check for a possible theft-of-service attempt by a user attempting to download a modified DOCSIS configuration file from a local TFTP server. The CM cannot reregister with a different QoS profile until it has been offline for 24 hours, without attempting to register, or you have manually cleared the lock using the **clear cable modem lock** command.

Message

%CBR-4-CMMARKED

The cable modem's DOCSIS configuration file did not contain a Message Integrity Check (MIC) value that corresponds with the proper dynamic shared secret that was used to encode it. The CMTS has allowed this modem to register and come online, but has marked it in the **show cable modem** displays with an exclamation point (!) so that the situation can be investigated.

This error message appears when the **cable dynamic-secret mark** command has been applied to a cable interface to enable the Dynamic Shared Secret feature for the DOCSIS configuration files on that cable interface. Check to ensure that this cable modem is not running old software that caches the previously used configuration file. Also check for a possible theft-of-service attempt by a user attempting to download a modified DOCSIS configuration file from a local TFTP server.

Message

%CBR-4-NOCFGFILE

The CMTS could not obtain the DOCSIS configuration file for this cable modem from the TFTP server. This message occurs when the Dynamic Shared Secret feature is enabled on the cable interface with the **cable dynamic-secret** command.

Verify that the CMTS has network connectivity with the TFTP server, and that the specified DOCSIS configuration file is available on the TFTP server. Check that the DHCP server is correctly configured to send the proper configuration filename in its DHCP response to the cable modem. Also verify that the DOCSIS configuration file is correctly formatted.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

10

This problem could also occur if the TFTP server is offline or is overloaded to the point where it cannot respond promptly to new requests. It might also be seen if the interface between the CMTS and TFTP server is not correctly configured and flaps excessively.

Note This error indicates a problem with the provisioning system outside of the Cisco CMTS. Disabling the Dynamic Shared Secret feature does not clear the fault, nor does it allow cable modems to come online. You must first correct the problem with the provisioning system.

Benefits

The Dynamic Shared Secret feature provides the following benefits to cable service providers and their partners and customers:

Improves Network Security

Service providers do not need to worry about users discovering the shared secret value and using it to modify DOCSIS configuration files to give themselves higher levels of service. Even if a user were to discover the value of a dynamically generated shared secret, the user would not be able to use that shared secret again to register.

The generic TFTP server performance and error handling on the Cisco CMTS routers has been greatly improved to support the high performance that is required for rapidly provisioning cable modems.

Flexibility in Dealing with Possible Theft-of-Service Attempts

Service providers have the option of deciding what response to take when a DOCSIS configuration file fails its CMTS MIC check: mark that cable modem and allow the user online, reject the registration request and refuse to allow the user to come online until a valid DOCSIS configuration file is used, or lock the cable modem in a restricted QoS configuration until the modem remains offline for 24 hours. Locking malicious modems is the most effective deterrent against hackers, because it provides the maximum penalty and minimum reward for any user attempting a theft-of-service attack.

No Changes to Provisioning System Are Needed

Service providers can use the Dynamic Shared Secret feature without changing their provisioning or authentication systems. Existing DOCSIS configuration files can be used unchanged, and you do not need to change any existing shared secrets.

Tip If not already done, the service provider could also install access controls that allow only the CMTS routers to download DOCSIS configuration files from the TFTP servers.

No Changes to Cable Modems Are Needed

The Dynamic Shared Secret feature does not require any end-user changes or any changes to the cable modem configuration. This feature supports any DOCSIS compliant cable modem.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

11

Note   The Dynamic Shared Secret feature does not affect cable modems that are already online and provisioned. Cable modems that are already online when the feature is enabled or disabled remain online.

Simplifies Network Management

Service providers do not have to continually update the shared secrets on a cable interface whenever the files providing premium services become widely available. Instead, providers can use the same shared secret on a cable interface for significant periods of time, trusting in the Dynamic Shared Secret feature to provide unique, single-use shared secrets for each cable modem.

In addition, service providers do not have to manage unique DOCSIS configuration files for each cable modem. The same configuration file can be used for all users in the same service class, without affecting network security.

Related Features

The following features can be used with the Dynamic Shared Secret feature to enhance the overall security of the cable network.

- Baseline Privacy Interface Plus (BPI+) Authorization and Encryption—Provides a secure link between the cable modem and CMTS, preventing users from intercepting or modifying packets that are transmitted over the cable interface. BPI+ also provides for secure authorization of cable modems, using X.509 digital certificates, as well as a secure software download capability that ensures that software upgrades are not spoofed, intercepted, or altered.

How to Configure the Dynamic Shared Secret Feature

The following sections describe how to enable and configure the Dynamic Shared Secret feature, to disable the feature, to manually clear a lock on a cable modem, or dynamically upgrade firmware on the cable modems.

Note   All procedures begin and end at the privileged EXEC prompt ("Router#").

Enabling and Configuring the Dynamic Shared Secret Feature

This section describes how to enable and configure the Dynamic Shared Secret feature on a cable interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# `**`configure terminal`**	Enters global configuration mode.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

12

	Command or Action	**Purpose**
	Example: `Router(config)#`	
Step 2	**cable qos permission create** **Example:** `Router(config)# `**`cable qos permission create`** **Example:** `Router(config)#`	(Optional) If you are using the **lock** option in Step 6, and if you are not specifying a specific QoS profile to be used, you must allow cable modems to create their own QoS profiles.
Step 3	**cable qos permission update** **Example:** `Router(config)# `**`cable qos permission update`** **Example:** `Router(config)#`	(Optional) If you are using the **lock** option in Step 6, and if you are not specifying a specific QoS profile to be used, you must allow cable modems to update their own QoS profiles.
Step 4	**snmp-server enable traps cable dmic-lock** **Example:** `Router(config)# `**`snmp-server enable traps cable`** **`dmic-lock`** **Example:** `Router(config)#`	(Optional) Enables the sending of SNMP traps when a cable modem fails a dynamic shared-secret security check.
Step 5	**interface cable** *interface* **Example:** `Router(config)# `**`interface cable 3/0`** **Example:** `Router(config-if)#`	Enters interface configuration mode for the specified cable interface.
Step 6	**cable dynamic-secret** {**lock** [*lock-qos*] | **mark** | **reject**} [**nocrypt** **Example:** `Router(config-if)# `**`cable dynamic-secret lock`** **Example:** `Router(config-if)# `**`cable dynamic-secret lock 90`** **Example:**	Enables the Dynamic Shared Secret feature on the cable interface and configures it for the appropriate option: • **nocrypt**—(Optional) The Cisco CMTS does not encrypt the filenames of DOCSIS configuration files, but sends the files to CMs using their original names. • **lock**—Cable modems that fail the MIC verification are allowed online with a restrictive QoS profile. The cable modems must remain offline for 24 hours to be able to reregister with a different QoS profile.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

13

	Command or Action	Purpose
	``
Router(config-if)# cable dynamic-secret mark
```
**Example:**
```
Router(config-if)# cable dynamic-secret reject
```
**Example:**
```
Router(config-if)#
``` | • *lock-qos* —(Optional) Specifies the QoS profile that should be assigned to locked cable modems. The valid range is 1 to 256, and the profile must have already been created. If not specified, locked cable modems are assigned a QoS profile that limits service flows to 10 kbps (requires Step 2 and Step 3).
• **mark**—Cable modems that fail the MIC verification are allowed online but are marked in the **show cable modem** displays so that the situation can be investigated.
• **reject**—Cable modems that fail the MIC verification are not allowed to register.

Note   Repeat Step 5 and Step 6 for each cable interface to be configured. |
| **Step 7** | **end**<br>**Example:**<br>```
Router(config-if)# end
```<br>**Example:**<br>```
Router#
``` | Exits interface configuration mode and returns to privileged EXEC mode. |

What to do next

Note   If you configure the Dynamic Shared Secret feature on any interface in a cable interface bundle, you should configure it on all interfaces in that same bundle.

Disabling the Dynamic Shared Secret on a Cable Interface

This section describes how to disable the Dynamic Shared Secret feature on a cable interface. The cable modem continues to be validated against any shared secret or secondary shared secrets that have been defined on the cable interface.

Procedure

	Command or Action	Purpose
| **Step 1** | **configure terminal**<br>**Example:**<br>```
Router# configure terminal
```<br>**Example:** | Enters global configuration mode. |

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

14

	Command or Action	Purpose
	```Router(config)#```	

Step 2	**interface cable** *interface*
	
	Example:
	
	```Router(config)# interface cable 3/0```
	
	Example:
	
	```Router(config-if)#```
		Enters interface configuration mode for the specified cable interface.

Step 3	**no cable dynamic-secret**
	
	Example:
	
	```Router(config-if)# no cable dynamic-secret```
	
	Example:
	
	```Router(config-if)#```
		Disables the Dynamic Shared Secret feature on the cable interface.
		
		Note Repeat Step 2 and Step 3 for each cable interface to be configured.

Step 4	**end**
	
	Example:
	
	```Router(config-if)# end```
	
	Example:
	
	```Router#```
		Exits interface configuration mode and returns to privileged EXEC mode.

Excluding Cable Modems from the Dynamic Shared Secret Feature

This section describes how to exclude one or more cable modems from being processed by the Dynamic Shared Secret feature. The cable modem continues to be validated against any shared secret or secondary shared secrets that have been defined on the cable interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** ```Router# configure terminal```	Enters global configuration mode.
Step 2	**cable dynamic-secret exclude** {**oui** *oui-id* | **modem** *mac-address*} **Example:** ```Router(config)# cable dynamic-secret exclude oui 00.01.B4```	Excludes one or more cable modems from being processed by the Dynamic Shared Secret security checks, on the basis of their MAC addresses or OUI values: • **modem** *mac-address*—Specifies the hardware (MAC) address of one specific and individual cable modem

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

15

Command or Action	Purpose
Router(config)# **cable dynamic-secret exclude modem 00d0.45ba.b34b**	to be excluded from the Dynamic Shared Secret feature. (You cannot specify a multicast MAC address.)
	• **oui** *oui-id*—Specifies the organization unique identifier (OUI) of a vendor, so that a group of cable modems from this vendor are excluded from the Dynamic Shared Secret feature. The OUI should be specified as three hexadecimal bytes separated by either periods or colons.
	Note Repeat this command for each cable modem MAC address or OUI vendor to be excluded.

Step 3	**exit** **Example:** Router(config)# **exit**	Exits the interface configuration mode and returns to privileged EXEC mode.

Clearing the Lock on One or More Cable Modems

This section describes how to manually clear the lock on one or more cable modems. This forces the cable modems to reinitialize, and the cable modems must reregister with a valid DOCSIS configuration file before being allowed online. If you do not manually clear the lock (using the **clear cable modem lock** command), the cable modem is locked in its current restricted QoS profile and cannot reregister with a different profile until it has been offline for at least 24 hours.

Procedure

	Command or Action	Purpose
Step 1	**clear cable modem** {*mac-addr*	*ip-addr*	**all**	**oui***string*	**reject**} **lock** **Example:** Router# **clear cable modem 0001.0203.0405 lock** **Example:** Router# **clear cable modem all lock** **Example:** Router# **clear cable modem oui 00.00.0C lock** **Example:**	Clears the lock for the cable modems, which can be identified as follows: • *mac-addr* —Specifies the MAC address for one particular cable modem to be cleared. • *ip-addr* —Specifies the IP address for one particular cable modem to be cleared. • **all**—Clears the locks on all locked cable modems. • **oui** *string* —Clears the locks on all cable modems with a vendor ID that matches the specified Organizational Unique Identifier (OUI) string. • **reject**—Clears the locks on all cable modems that are currently in the reject state (which would occur if a locked cable modem went offline and attempted to reregister before 24 hours had elapsed).

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

16

Command or Action	Purpose
`Router#`	

What to do next

🔍

Tip   A cable modem can also be unlocked by manually deleting the cable modem from all CMTS internal databases, using the **clear cable modem delete** command.

Upgrading Firmware on the Cable Modems

This section describes how to upgrade firmware on cable modems by dynamically inserting the correct TLV values in the DOCSIS configuration file that is downloaded by the cable modem. The DOCSIS configuration file contains the following TLV values:

- Software Upgrade Filename (TLV 9)—Specifies the filename of the firmware.
- Upgrade IPv4 TFTP Server (TLV21)—Specifies the IPv4 address of the TFTP server from where the modem downloads the DOCSIS configuration file.
- Upgrade IPv6 TFTP Server (TLV58)—Specifies the IPv6 address of the TFTP server from where the modem downloads the DOCSIS configuration file.

✏️

Note   The TFTP server addresses are inserted only when the software upgrade filename (TLV9) is specified and when the TFTP server address (TLV21/TLV58) is either not specified or set to 0.

Before you begin

The Dynamic Shared Secret feature must be enabled first before you can upgrade the firmware on cable modems. See Enabling and Configuring the Dynamic Shared Secret Feature, on page 12 for more information.

✏️

Note   The command to enable or disable the Dynamic Shared Secret feature is available at the MAC domain level. However, the command to upgrade the firmware on cable modems is available at the global level.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# `**`configure terminal`** **Example:**	Enters the global configuration mode.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

17

	Command or Action	Purpose
	`Router(config)#`	
Step 2	cable dynamic-secret tftp insert-upgrade-server **Example:** `Router(config)# `**`cable dynamic-secret tftp`** **`insert-upgrade-server`**	Dynamically inserts the specific IPv4 or IPv6 TLV values in the DOCSIS configuration file to complete firmware upgrade on cable modems.
Step 3	**end** **Example:** `Router(config)# `**`end`** **Example:** `Router#`	Exits the configuration mode and returns to the privileged EXEC mode.

What to do next

Note   If you configure the Dynamic Shared Secret feature on an interface in a cable interface bundle, you should configure it on all the interfaces of that bundle.

How to Monitor the Dynamic Shared Secret Feature

This section describes the following procedures you can use to monitor and display information about the Dynamic Shared Secret feature:

Displaying Marked Cable Modems

When you configure a cable interface with the **cable dynamic-secret mark** command, cable modems that fail the dynamically generated CMTS MIC verification are allowed online, but are marked with an exclamation point (!) in the MAC state column in the **show cable modem** display. The exclamation point is also used to identify cable modems that were initially rejected, using the **cable dynamic-secret reject** command, but then reregistered using a valid DOCSIS configuration file.

For example, the following example shows that four cable modems are marked as having failed the CMTS MIC verification, but that they have been allowed online:

```
Router# show cable modems

MAC Address      IP Address      I/F        MAC        Prim RxPwr  Timing  Num BPI
                                            State      Sid  (db)   Offset  CPE Enb
0010.9507.01db 144.205.151.130 C5/1/0/U5 online(pt)  1    0.25    938    1    N
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

18

```
0080.37b8.e99b 144.205.151.131 C5/1/0/U5 online       2    -0.25   1268  0    N
0002.fdfa.12ef 144.205.151.232 C6/1/0/U0 online(pt)   13   -0.25   1920  1    N
0002.fdfa.137d 144.205.151.160 C6/1/0/U0 !online      16   -0.50   1920  1    N
0003.e38f.e9ab 144.205.151.237 C6/1/0/U0 !online       3   -0.50   1926  1    N
0003.e3a6.8173 144.205.151.179 C6/1/1/U2 offline       4    0.50   1929  0    N
0003.e3a6.8195 144.205.151.219 C6/1/1/U2 !online(pt)  22   -0.50   1929  1    N
0006.28dc.37fd 144.205.151.244 C6/1/1/U2 online(pt)   61    0.00   1925  2    N
0006.28e9.81c9 144.205.151.138 C6/1/1/U2 online(pt)    2    0.75   1925  1    N
0006.28f9.8bbd 144.205.151.134 C6/1/1/U2 online       25   -0.25   1924  1    N
0006.28f9.9d19 144.205.151.144 C6/1/1/U2 online(pt)   28    0.25   1924  1    N
0010.7bed.9b6d 144.205.151.228 C6/1/1/U2 online(pt)   59    0.25   1554  1    N
0002.fdfa.12db 144.205.151.234 C7/0/0/U0 online       15   -0.75   1914  1    N
0002.fdfa.138d 144.205.151.140 C7/0/0/U5 online        4    0.00   1917  1    N
0003.e38f.e85b 144.205.151.214 C7/0/0/U5 !online      17    0.25   1919  1    N
0003.e38f.f4cb 144.205.151.238 C7/0/0/U5 online(pt)   16    0.00  !2750  1    N
0003.e3a6.7fd9 144.205.151.151 C7/0/0/U0 online        1    0.25   1922  0    N
0020.4005.3f06 144.205.151.145 C7/0/0/U0 online(pt)    2    0.00   1901  1    N
0020.4006.b010 144.205.151.164 C7/0/0/U5 online(pt)    3    0.00   1901  1    N
0050.7302.3d83 144.205.151.240 C7/0/0/U0 online(pt)   18   -0.25   1543  1    N
00b0.6478.ae8d 144.205.151.254 C7/0/0/U5 online(pt)   44    0.25   1920  21   N
00d0.bad3.c0cd 144.205.151.149 C7/0/0/U5 online       19    0.25   1543  1    N
00d0.bad3.c0cf 144.205.151.194 C7/0/0/U0 online       13    0.00   1546  1    N
00d0.bad3.c0d5 144.205.151.133 C7/0/0/U0 online       12    0.50   1546  1    N
Router#
```

You can also use the **show cable modem rogue** command to display only those cable modems that have been rejected for failing the dynamic shared-secret authentication checks:

```
Router# show cable modem rogue
                                    Spoof TFTP
MAC Address     Vendor    Interface  Count Dnld Dynamic Secret
AAAA.7b43.aa7f Vendor1   C4/0/U5      2   Yes  45494DC933F8F47A398F69EE6361B017
AAAA.7b43.aa7f Vendor1   C4/0/U5      2   Yes  D47BCBB5494E9936D51CB0EB66EF0B0A
BBBB.7b43.aa7f Vendor2   C4/0/U5      2   No   8EB196423170B26684BF6730C099D271
AAAA.7b43.aa7f Vendor1   C4/0/U5      2   No   DF8FE30203010001A326302430120603
BBBB.7b43.aa7f Vendor2   C4/0/U5      2   No   300E0603551D0F0101FF040403020106
AAAA.7b43.aa7f Vendor1   C4/0/U5      2   Yes  820101002D1A264CE212A1BB6C1728B3
DDDD.7b43.aa7f Vendor4   C4/0/U5      2   Yes  7935B694DCA90BC624AC92A519C214B9
AAAA.7b43.aa7f Vendor1   C4/0/U5      2   No   3AB096D00D56ECD07D9B7AB662451CFF
Router#
```

Displaying the Current Dynamic Secrets

In , the **verbose** option for the **show cable modem** command displays the dynamically generated shared secret (a 16-byte hexadecimal value) that was used in the cable modem's previous registration cycle. The display also shows if the cable modem failed the dynamic shared-secret check or did not download the DOCSIS configuration file from the TFTP server. If a cable modem is offline, its dynamic secret is shown as all zeros.

For example, the following example shows a typical display for a single cable modem that failed the dynamic shared-secret check:

```
Router# show cable modem 00c0.73ee.bbaa verbose

MAC Address                     : 00c0.73ee.bbaa
IP Address                      : 3.18.1.6
Prim Sid                        : 2
QoS Profile Index               : 6
Interface                       : C3/0/U0
Upstream Power                  : 0.00 dBmV (SNR = 26.92 dBmV)
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

19

```
Downstream Power                      : 0.00 dBmV (SNR = ----- dBmV)
Timing Offset                         :  2812
Initial Timing Offset                 : 2812
Received Power                        :  0.00
MAC Version                           : DOC1.0
Provisioned Mode                      : DOC1.0
Capabilities                          : {Frag=N, Concat=N, PHS=N, Priv=BPI}
Sid/Said Limit                        : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support            : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support            : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs                     : 0(Max CPE IPs = 1)
CFG Max-CPE                           : 1
Flaps                                 : 26(Feb 14 02:35:39)
Errors                                : 0 CRCs, 0 HCSes
Stn Mtn Failures                      : 6 aborts, 0 exhausted
Total US Flows                        : 1(1 active)
Total DS Flows                        : 1(1 active)
Total US Data                         : 0 packets, 0 bytes
Total US Throughput                   : 0 bits/sec, 0 packets/sec
Total DS Data                         : 0 packets, 0 bytes
Total DS Throughput                   : 0 bits/sec, 0 packets/sec
Active Classifiers                    : 0 (Max = NO LIMIT)
Dynamic Secret                        : A3D1028F36EBD54FDCC2F74719664D3F
Router#
```

The following example shows a typical display for a single cable modem that is currently offline (the Dynamic Secret field shows all zeros):

```
Router# show cable modem 00C0.6914.8601 verbose

MAC Address                           : 00C0.6914.8601
IP Address                            : 10.212.192.119
Prim Sid                              : 6231
QoS Profile Index                     : 2
Interface                             : C5/1/0/U3
Upstream Power                        : 0.00 dBmV (SNR = 30.19 dBmV)
Downstream Power                      : 0.00 dBmV (SNR = ----- dBmV)
Timing Offset                         : 1831
Initial Timing Offset                 : 1831
Received Power                        : !-2.25
MAC Version                           : DOC1.0
Provisioned Mode                      : DOC1.0
Capabilities                          : {Frag=N, Concat=Y, PHS=N, Priv=BPI}
Sid/Said Limit                        : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support            : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support            : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs                     : 4(Max CPE IPs = 4)
CFG Max-CPE                           : 4
Flaps                                 : 20638(Feb 10 16:04:10)
Errors                                : 0 CRCs, 0 HCSes
Stn Mtn Failures                      : 108 aborts, 161 exhausted
Total US Flows                        : 1(1 active)
Total DS Flows                        : 1(1 active)
Total US Data                         : 236222 packets, 146630868 bytes
Total US Throughput                   : 0 bits/sec, 0 packets/sec
Total DS Data                         : 9 packets, 1114 bytes
Total DS Throughput                   : 0 bits/sec, 0 packets/sec
Active Classifiers                    : 0 (Max = NO LIMIT)
Dynamic Secret                        : 00000000000000000000000000000000
Router#
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

20

Note　The Dynamic Secret field shown above is all zeros ("00000000000000000000000000000000"), which indicates that this cable modem is offline.

You can also use the following command to display all the dynamically generated shared secrets that are in use:

```
Router# show cable modem verbose | include Dynamic Secret

Dynamic Secret                     : 43433036434644344643303841313237
Dynamic Secret                     : 308203E0308202C8A003020102021058
Dynamic Secret                     : 0D06092A864886F70D01010505003081
Dynamic Secret                     : 3037060355040A133044617461204F76
Dynamic Secret                     : 20496E74657266616365205370656369
Dynamic Secret                     : 00000000000000000000000000000000
Dynamic Secret                     : 040B130C4361626C65204D6F64656D73
Dynamic Secret                     : 53204361626C65204D6F64656D20526F
Dynamic Secret                     : 7574686F72697479301E170D30313032
Dynamic Secret                     : 313233353935395A308197310B300906
Dynamic Secret                     : 0A133044617461204F76657220436162
Dynamic Secret                     : 6661636520537065636966696963617469
Dynamic Secret                     : 626C65204D6F64656D73313630340603
Dynamic Secret                     : 65204D6F64656D20526F6F7420436572
Dynamic Secret                     : 747930820122300D06092A864886F70D
Dynamic Secret                     : 010100C0EF369D7BDAB0A938E6ED29C3
Dynamic Secret                     : DA398BF619A11B3C0F64912D133CFFB6
Dynamic Secret                     : FFAD6CE01590ABF5A1A0F50AC05221F2
Dynamic Secret                     : 73504BCA8278D41CAD50D9849B56552D
Dynamic Secret                     : 05F4655F2981E031EB76C90F9B3100D1
Dynamic Secret                     : F4CB0BF4A13EA9512FDE4A2A219C27E9
Dynamic Secret                     : D47BCBB5494E9936D51CB0EB66EF0B0A
Dynamic Secret                     : 8EB196423170B26684BF6730C099D271
Dynamic Secret                     : DF8FE30203010001A3263024301 20603
Dynamic Secret                     : 300E0603551D0F0101FF040403020106
Dynamic Secret                     : 820101002D1A264CE212A1BB6C1728B3
Dynamic Secret                     : 7935B694DCA90BC624AC92A519C214B9
Dynamic Secret                     : 3AB096D00D56ECD07D9B7AB662451CFF
Dynamic Secret                     : 92E68CFD8783D58557E3994F23A8140F
Dynamic Secret                     : 225A3B01DB67AF0C3637A765E1E7C329
Dynamic Secret                     : 2BB1E6221B6D5596F3D6F506804C995E
Dynamic Secret                     : 45494DC933F8F47A398F69EE6361B017
Router#
```

Troubleshooting Cable Modems with Dynamic Shared Secret

If a cable modem is being marked as having violated the dynamic shared secret, you can enable the following debugs to get more information about the sequence of events that is occurring:

- **debug cable mac-address** *cm-mac-addr* **verbose**—Enables detailed debugging for the cable modem with the specific MAC address.
- **debug cable tlv**—Displays the contents of Type/Length/Value messages that are sent during the registration process.
- **debug cable dynamic-secret**—Displays debugging messages about dynamic shared secret operation.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

21

- **debug tftp server events**—Displays debugging messages for the major events that occur with the Cisco CMTS router's onboard TFTP server.
- **debug tftp server packets**—Displays a packet dump for the DOCSIS configuration files that the TFTP server downloads to a cable modem.

🔍

Tip For more information about these debug commands, see the *Cisco CMTS Debugging Commands* chapter in the Cisco Broadband Cable Command Reference Guide, at the following URL:
http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

In addition, examine the messages in the router's log buffer for any helpful information. Use the **show logging** command to display the contents of the router's logging buffer to display these messages. You can limit the output to a specific hour and minute by using the **begin** output modifier. For example, to display only those messages that were recorded at 12:10, give the following command:

```
Router# show logging | begin 12:10
```

✏️

Note The exact format for the **begin** output modifier depends on the timestamp you are using for your logging buffer.

Configuration Examples for Dynamic Shared Secret

This section lists a typical configuration for the Dynamic Shared Secret feature.

✏️

Note These configurations also show a shared secret and secondary secret being configured on the cable interface. This is optional but highly recommended, because it adds an additional layer of security during the registration of cable modems.

Mark Configuration: Example

The following excerpt from a configuration for the cable interface on a Cisco CMTS router configures the cable interface so that cable modems that fail the CMTS MIC check are allowed to come online, but are marked with an exclamation point (!) in the **show cable modem** displays, so that the situation can be investigated further.

```
interface cable c5/1/0
 cable dynamic-secret mark
 ...
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

22

Lock Configuration: Example

The following excerpt from a configuration for the cable interface on a Cisco CMTS router configures the cable interface so that cable modems that fail the CMTS MIC check are allowed to come online, but are locked into a restrictive QoS configuration that limits the upstream and downstream service flows to a maximum rate of 10 kbps. A locked cable modem remains locked into the restrictive QoS configuration until the modem has remained offline for more than 24 hours, or until you have manually cleared it using the **clear cable modem lock** command.

```
cable qos permission create
cable qos permission update
...
interface cable c3/0
 cable dynamic-secret lock
 ...
```

✎
Note   If you use the **lock** option without specifying a specific QoS profile, you must allow cable modems to create and update QoS profiles, using the **cable qos permission** command. If you do not do this and continue to use the **lock** option without specifying a particular QoS profile, locked cable modems will not be allowed to register until the lock clears or expires.

The following example is the same except that it specifies that the locked cable modem should be assigned QoS profile 90. The cable modem remains locked with this QoS profile until the modem has remained offline for more than 24 hours, or until you have manually cleared it using the **clear cable modem lock** command. Because a specific QoS profile is specified, you do not need to use the **cable qos permission** command.

```
interface cable c3/0
 cable dynamic-secret lock 90
 ...
```

✎
Note   When a locked modem is cleared, it is automatically reset so that it reregisters with the CMTS. It is allowed online with the requested QoS parameters if it registers with a valid DOCSIS configuration that passes the Dynamic Shared Secret checks. However, the modem is locked again if it violates the DOCSIS specifications again.

Reject Configuration: Example

The following excerpt from a configuration for the cable interface on a Cisco CMTS configures the cable interface so that cable modems that fail the CMTS MIC check are rejected and not allowed to register. The cable modem must reregister using a DOCSIS configuration file with a CMTS MIC that matches one of the shared secret or secondary secret values. When it does come online, the CMTS also prints a warning message on the console and marks the cable modem in the **show cable modem** command with an exclamation point (!), so that this situation can be investigated.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

23

```
interface cable c3/0
 cable dynamic-secret reject
 ...
```

Disabled Configuration: Example

The following excerpt from a configuration for the cable interface on a Cisco uBR7100 series router disables the Dynamic Shared Secret feature. In this configuration, the CMTS uses the shared secret and secondary shared secret values unchanged when verifying the CMTS MIC value for each DOCSIS configuration file.

```
interface cable c1/0
 no cable dynamic-secret
 ...
```

Additional References

For additional information related to Dynamic Shared Secret, refer to the following references:

Standards

Standards[1]	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1

[1] Not all supported standards are listed.

MIBs

MIBs[2]	MIBs Link
No new or modified MIB objects are supported by the Dynamic Shared Secret feature. • CISCO-DOCS-EXT-MIB—Includes attributes to configure the Dynamic Shared Secret feature and to generate traps when a cable modem fails the shared-secret security checks.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

[2] Not all supported MIBs are listed.

RFCs

RFCs[3]	Title
RFC 2233	DOCSIS OSSI Objects Support
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

24

[3] Not all supported RFCs are listed.

Feature Information for Dynamic Shared Secret

Use Cisco Feature Navigator to find information about the 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 the https://cfnng.cisco.com/ link. An account on the Cisco.com page is not required.

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

Table 2: Feature Information for Downstream Interface Configuration

Feature Name	Releases	Feature Information
Dynamic shared secret	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on theCisco cBR Series Converged Broadband Router.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

25

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

26

CHAPTER 2

Lawful Intercept Architecture

The Lawful Intercept (LI) feature supports service providers in meeting the requirements of law enforcement agencies to provide the ability to intercept Voice-over-Internet protocol (VoIP) or data traffic going through the edge routers. This document explains LI architecture, including Cisco Service Independent Intercept architecture and PacketCable Lawful Intercept architecture. It also describes the components of the LI feature and provides instructions on how to configure the LI feature in your system.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

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

Contents

Hardware Compatibility Matrix for the Cisco cBR Series Routers

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

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

27

Table 3: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Prerequisites for Lawful Intercept

Access to the Cisco LI MIB view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

Communication with Mediation Device

For the router to communicate with the mediation device to execute a lawful intercept, the following configuration requirements must be met:

• The domain name for both the router and the mediation device must be registered in the Domain Name System (DNS).

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

28

In DNS, the router IP address is typically the address of the TenGigabitEthernet5/1/0 or TenGigabitEthernet4/1/0 interface (depending on the slot in which the Supervisor is installed) on the router.

- The mediation device must have an access function (AF) and an access function provisioning interface (AFPI).

- You must add the mediation device to the Simple Network Management Protocol (SNMP) user group that has access to the CISCO-TAP2-MIB view. Specify the username of the mediation device as the user to add to the group.

When you add the mediation device as a CISCO-TAP2-MIB user, you can include the mediation device's authorization password if you want. The password must be at least eight characters in length.

Restrictions for Lawful Intercept

General Restrictions

There is no command-line interface (CLI) available to configure LI on the router. All error messages are sent to the mediation device as SNMP notifications. All intercepts are provisioned using SNMPv3 only.

Lawful Intercept does not support SUP HA. LI configuration needs to be reapplied after SUP switchover. An SNMP trap will be generated for this event.

Lawful Intercept MIBs

Only the mediation device and users who need to know about lawful intercepts are allowed to access the LI MIBs.

Due to its sensitive nature, the Cisco LI MIBs are only available in software images that support the LI feature. These MIBs are not accessible through the Network Management Software MIBs Support page (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml).

SNMP Notifications

SNMP notifications for LI must be sent to User Datagram Protocol (UDP) port 161 on the mediation device, not port 162 (which is the SNMP default).

Information About Lawful Intercept

Introduction to Lawful Intercept

LI is the process by which law enforcement agencies (LEAs) conduct electronic surveillance as authorized by judicial or administrative order. Increasingly, legislation is being adopted and regulations are being enforced that require service providers (SPs) and Internet service providers (ISPs) to implement their networks to explicitly support authorized electronic surveillance. The types of SPs or ISPs that are subject to LI mandates vary greatly from country to country. LI compliance in the United States is specified by the Commission on Accreditation for Law Enforcement Agencies (CALEA).

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

29

Cisco supports two architectures for LI: PacketCable and Service Independent Intercept. The LI components by themselves do not ensure customer compliance with applicable regulations but rather provide tools that can be used by SPs and ISPs to construct an LI-compliant network.

Cisco Service Independent Intercept Architecture

The Cisco Service Independent Intercept Architecture Version 3.0 document describes implementation of LI for VoIP networks using the Cisco BTS 10200 Softswitch call agent, version 5.0, in a non-PacketCable network. Packet Cable Event Message specification version 1.5-I01 is used to deliver the call identifying information along with version 2.0 of the Cisco Tap MIB for call content.

The Cisco Service Independent Intercept Architecture Version 2.0 document describes implementation of LI for VoIP networks using the Cisco BTS 10200 Softswitch call agent, versions 4.4 and 4.5, in a non-PacketCable network. Although not a PacketCable network, PacketCable Event Messages Specification version I08 is still used to deliver call identifying information, along with version 1.0 or version 2.0 of the Cisco Tap MIB for call content. The *Cisco Service Independent Intercept Architecture Version 2.0* document adds additional functionality for doing data intercepts by both IP address and session ID, which are both supported in version 2.0 of the Cisco Tap MIB (CISCO-TAP2-MIB).

The Cisco Service Independent Intercept Architecture Version 1.0 document describes implementation of LI for VoIP networks that are using the Cisco BTS 10200 Softswitch call agent, versions 3.5 and 4.1, in a non-PacketCable network. Although not a PacketCable network, PacketCable Event Message Specification version I03 is still used to deliver call identifying information, along with version 1.0 of the Cisco Tap MIB (CISCO-TAP-MIB) for call content. Simple data intercepts by IP address are also discussed.

PacketCable Lawful Intercept Architecture

The *PacketCable Lawful Intercept Architecture for BTS Version 5.0* document describes the implementation of LI for VoIP using Cisco BTS 10200 Softswitch call agent, version 5.0, in a PacketCable network that conforms to PacketCable Event Messages Specification version 1.5-I01.

The *PacketCable Lawful Intercept Architecture for BTS Versions 4.4 and 4.5* document describes the implementation of LI for VoIP using Cisco BTS 10200 Softswitch call agent, versions 4.4 and 4.5, in a PacketCable network that conforms to PacketCable Event Messages Specification version I08.

The PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1 document describes the implementation of LI for voice over IP (VoIP) using Cisco Broadband Telephony Softswitch (BTS) 10200 Softswitch call agent, versions 3.5 and 4.1, in a PacketCable network that conforms to PacketCable Event Message Specification version I03.

The *PacketCable Control Point Discovery Interface Specification* document defines an IP-based protocol that can be used to discover a control point for a given IP address. The control point is the place where Quality of Service (QoS) operations, LI content tapping operations, or other operations may be performed.

Note The Cisco cBR router does not support PacketCable Communications Assistance for Law Enforcement Act (CALEA).

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

30

Cisco cBR Series Routers

TheCisco cBR series router support two types of LI: regular and broadband (per-subscriber). Regular wiretaps are executed on access subinterfaces and physical interfaces. Wiretaps are not required, and are not executed, on internal interfaces. The router determines which type of wiretap to execute based on the interface that the target's traffic is using.

LI on the Cisco cBR series routers can intercept traffic based on a combination of one or more of the following fields:

- Destination IP address and mask (IPv4 or IPv6 address)

- Destination port or destination port range

- Source IP address and mask (IPv4 or IPv6 address)

- Source port or source port range

- Protocol ID

- Type of Service (TOS)

- Virtual routing and forwarding (VRF) name, which is translated to a *vrf-tableid* value within the router.

- Subscriber (user) connection ID

- Cable modem

- MAC address

The LI implementation on the Cisco cBR series routers is provisioned using SNMP3 and supports the following functionality:

- Interception of communication content. The router duplicates each intercepted packet and then places the copy of the packet within a UDP-header encapsulated packet (with a configured CCCid). The router sends the encapsulated packet to the LI mediation device. Even if multiple lawful intercepts are configured on the same data flow, only one copy of the packet is sent to the mediation device. If necessary, the mediation device can duplicate the packet for each LEA.

- Interception of IPv4, IPv4 multicast, IPv6, and IPv6 multicast flows.

- Maximum interception time—The maximum value of **cTap2MediationTimeout** is 260640 minutes or 181 days from the current time. The minimum value for **cTap2MediationTimeout** is 1 minute from the current time.

LI includes two ways of setting a MAC-based tap:

- On CPE—Only intercepts traffic whose source or destination match the MAC address of the CPE device.

- On CM—Intercepts all of the traffic behind the CM, including the CM traffic itself. This form of intercept might generate a lot of traffic to the mediation device.

VRF Aware LI

VRF Aware LI is the ability to provision a LI wiretap on IPv4 data in a particular Virtual Private Network (VPN). This feature allows a LEA to lawfully intercept targeted data within that VPN. Only IPv4 data within that VPN is subject to the VRF-based LI tap.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

31

VRF Aware LI is available for the following types of traffic:

- ip2ip

- ip2tag (IP to MPLS)

- tag2ip (MPLS to IP)

To provision a VPN-based IPv4 tap, the LI administrative function (running on the mediation device) uses the CISCO-IP-TAP-MIB to identify the name of the VRF table that the targeted VPN uses. The VRF name is used to select the VPN interfaces on which to enable LI in order to execute the tap.

The router determines which traffic to intercept and which mediation device to send the intercepted packets based on the VRF name (along with the source and destination address, source and destination port, and protocol).

Note When using the Cisco-IP-TAP-MIB, if the VRF name is not specified in the stream entry, the global IP routing table is used by default.

Lawful Intercept- Redundant Mediation Devices

The Cisco cBR Series Converged Broadband Routers supports replicating Lawful Intercept (LI) packets to multiple Mediation Devices (MDs). To use this feature, multiple identical taps are configured. The Cisco cBR Series Converged Broadband Routers support up to two identical taps to replicate to two MDs. Only MAC- and CM-taps are supported with multiple MDs.

For a sample SNMP configuration command set to configure two identical taps to tap to two MDs, see Example: Configuring Lawful Intercept- Redundant Mediation Devices, on page 38.

Lawful Intercept MIBs

Due to its sensitive nature, the Cisco LI MIBs are only available in software images that support the LI feature. These MIBs are not accessible through the Network Management Software MIBs Support page (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml).

Restricting Access to the Lawful Intercept MIBs

Only the mediation device and users who need to know about lawful intercepts should be allowed to access the LI MIBs. To restrict access to these MIBs, you must:

1. Create a view that includes the Cisco LI MIBs.

2. Create an SNMP user group that has read-and-write access to the view. Only users assigned to this user group can access information in the MIBs.

3. Add users to the Cisco LI user groups to define who can access the MIBs and any information related to lawful intercepts. Be sure to add the mediation device as a user in this group; otherwise, the router cannot perform lawful intercepts.

For more information, see the Creating a Restricted SNMP View of Lawful Intercept MIBs module.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

32

Note	Access to the Cisco LI MIB view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

Service Independent Intercept

Cisco developed the Service Independent Intercept (SII) architecture in response to requirements that support lawful intercept for service provider customers. The SII architecture offers well-defined, open interfaces between the Cisco equipment acting as the content Intercept Access Point (IAP) and the mediation device. The modular nature of the SII architecture allows the service provider to choose the most appropriate mediation device to meet specific network requirements and regional, standards-based requirements for the interface to the law enforcement collection function.

The mediation device uses SNMPv3 to instruct the call connect (CC) IAP to replicate the CC and send the content to the mediation device. The CC IAP can be either an edge router or a trunking gateway for voice, and either an edge router or an access server for data.

Note	The Cisco cBR router does not support encryption of lawful intercept traffic.

To increase the security and to mitigate any SNMPv3 vulnerability, the following task is required:

Restricting Access to Trusted Hosts (without Encryption)

SNMPv3 provides support for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine the security mechanism employed when handling an SNMP packet.

Additionally, the SNMP Support for the Named Access Lists feature adds support for standard named access control lists (ACLs) to several SNMP commands.

To configure a new SNMP group or a table that maps SNMP users to SNMP views, use the **snmp-server group** command in global configuration mode.

```
access-list my-list permit ip host 10.10.10.1
snmp-server group my-group v3 auth access my-list
```

In this example, the access list named **my-list** allows SNMP traffic only from 10.10.10.1. This access list is then applied to the SNMP group called **my-group**.

How to Configure Lawful Intercept

Although there are no direct user commands to provision lawful intercept on the router, you do need to perform some configuration tasks, such as providing access to LI MIBs, and setting up SNMP notifications. This section describes how to perform the required tasks:

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

33

Creating a Restricted SNMP View of Lawful Intercept MIBs

To create and assign users to an SNMP view that includes the Cisco lawful intercept MIBs, perform the steps in this section.

Before you begin

- You must issue the commands in global configuration mode with level-15 access rights.

- SNMPv3 must be configured on the device.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView ciscoTap2MIB included`	Creates an SNMP view that includes the CISCO-TAP2-MIB (where *exampleView* is the name of the view to create for the MIB). - This MIB is required for both regular and broadband lawful intercept.
Step 4	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView ciscoIpTapMIB included`	Adds the CISCO-IP-TAP-MIB to the SNMP view.
Step 5	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView cisco802TapMIB included`	Adds the CISCO-802-TAP-MIB to the SNMP view.
Step 6	**snmp-server group** *group-name* **v3 noauth read** *view-name* **write** *view-name* **Example:** `Device(config)# snmp-server group exampleGroup v3 noauth read exampleView write exampleView`	Creates an SNMP user group that has access to the LI MIB view and defines the group's access rights to the view.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

34

	Command or Action	Purpose
Step 7	**snmp-server user** *user-name group-name* **v3 auth md5** *auth-password* **Example:** `Device(config)# snmp-server user exampleUser exampleGroup v3 auth md5 examplePassword`	Adds users to the specified user group.
Step 8	**end** **Example:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Where to Go Next

The mediation device can now access the lawful intercept MIBs and issue SNMP **set** and **get** requests to configure and run lawful intercepts on the router. To configure the router to send SNMP notification to the mediation device, see the Enabling SNMP Notifications for Lawful Intercept.

Enabling SNMP Notifications for Lawful Intercept

SNMP automatically generates notifications for lawful intercept events. To configure the router to send lawful intercept notifications to the mediation device, perform the steps in this section.

Before you begin

- You must issue the commands in global configuration mode with level-15 access rights.

- SNMPv3 must be configured on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *ip-address* **community-string udp-port** *port notification-type*
4. **snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart** *and* **snmp-server enable traps rf**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. - Enter your password if prompted.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

35

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** *ip-address* **community-string udp-port** *port notification-type* **Example:** `Device(config)# snmp-server 10.2.2.1 community-string udp-port 161 udp`	Specifies the IP address of the mediation device and the password-like community-string that is sent with a notification request. • For lawful intercept, the **udp-port** must be 161 and not 162 (the SNMP default).

Step 4	**snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart** *and* **snmp-server enable traps rf**
	
	Example:
	
	`Device(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`
	`Device(config)# snmp-server enable traps rf`
		Configures the router to send RFC 1157 notifications to the mediation device.
		
		These notifications indicate authentication failures, link status (up or down), and router restarts.

Step 5	**end** **Example:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Disabling SNMP Notifications

To disable SNMP notifications on the router, perform the steps in this section.

Note To disable lawful intercept notifications, use SNMPv3 to set the CISCO-TAP2-MIB object cTap2MediationNotificationEnable to false(2). To reenable lawful intercept notifications through SNMPv3, reset the object to true(1).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no snmp-server enable traps**
4. **end**

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

36

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**no snmp-server enable traps** **Example:** Device(config)# no snmp-server enable traps	Disables all SNMP notification types that are available on your system.
Step 4	**end** **Example:** Device(config)# end	Exits the current configuration mode and returns to privileged EXEC mode.

Provisioning a MAC Intercept for Cable Modems Using SNMPv3

1. Configure the c802tapStreamInterface object.
2. Set the following bit flags in the c802tapStreamFields object:

   - dstMacAddress (bit 1)
   - srcMacAddress (bit 2)
   - cmMacAddress (bit 6)—The cmMacAddress bit field is newly introduced for cable modem support and determines whether the intercept is a CPE-based or CM-based intercept.

3. Configure the following objects with the same CM MAC address value:

   - c802tapStreamDestinationAddress
   - c802tapStreamSourceAddress

Provisioning a MAC Intercept for a CPE Device Using SNMPv3

1. Configure the c802tapStreamInterface object.
2. Set the following bit flags in the c802tapStreamFields object:

   - dstMacAddress (bit 1)
   - srcMacAddress (bit 2)

3. Configure the following objects with the same CPE MAC address value:

   - c802tapStreamDestinationAddress

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

37

- c802tapStreamSourceAddress

Configuration Examples for Lawful Intercept

Example: Enabling Mediation Device Access Lawful Intercept MIBs

The following example shows how to enable the mediation device to access the lawful intercept MIBs. It creates an SNMP view (tapV) that includes four LI MIBs (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, CISCO-802-TAP-MIB, and CISCO-USER-CONNECTION-TAP-MIB). It also creates a user group that has read, write, and notify access to MIBs in the tapV view.

```
snmp-server view tapV ciscoTap2MIB included
snmp-server view tapV ciscoIpTapMIB included
snmp-server view tapV cisco802TapMIB included
snmp-server view tapV ciscoUserConnectionTapMIB included
snmp-server group tapGrp v3 noauth read tapV write tapV notify tapV
snmp-server user MDuser tapGrp v3 auth md5 MDpasswd
snmp-server engineID local 1234
```

Example: Configuring Lawful Intercept- Redundant Mediation Devices

Lawful Intercept is configured using SNMPv3. The following example shows SNMP configuration command set to configure two identical taps to tap two MDs:

- Setup MD1:

```
setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
cTap2MediationStatus.1 -i 4 \
cTap2MediationDestAddressType.1 -i 1 \
cTap2MediationTimeout.1 -o 07:E0:04:01:B:15:1A:0 \
cTap2MediationTransport.1 -i 1 \
cTap2MediationSrcInterface.1 -i 0 \
cTap2MediationDestAddress.1 -o 0a:0a:00:35 \
cTap2MediationDestPort.1 -g 63
```

- Setup CM tap:

```
setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
c802tapStreamStatus.1.2 -i 4 \
c802tapStreamFields.1.2 -o 62 \
c802tapStreamInterface.1.2 -i -1 \
c802tapStreamDestinationAddress.1.2 -o "c8 fb 26 a5 55 98" \
c802tapStreamSourceAddress.1.2 -o "c8 fb 26 a5 55 98"

setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
cTap2StreamStatus.1.2 -i 5 \
cTap2StreamType.1.2 -i 2 \
cTap2StreamInterceptEnable.1.2 -i 1 \
cTap2StreamStatus.1.2 -i 4
```

- Setup MD2:

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

38

```
setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
cTap2MediationStatus.2 -i 4 \
cTap2MediationDestAddressType.2 -i 1 \
cTap2MediationTimeout.2 -o 07:E0:03:03:7:15:1A:0 \
cTap2MediationTransport.2 -i 1 \
cTap2MediationSrcInterface.2 -i 0 \
cTap2MediationDestAddress.2 -o 0a:0a:00:06 \
cTap2MediationDestPort.2 -g 63
```

- Setup CM tap:

```
setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
c802tapStreamStatus.2.2 -i 4 \
c802tapStreamFields.2.2 -o 62 \
c802tapStreamInterface.2.2 -i -1 \
c802tapStreamDestinationAddress.2.2 -o "c8 fb 26 a5 55 98" \
c802tapStreamSourceAddress.2.2 -o "c8 fb 26 a5 55 98"

setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
cTap2StreamStatus.2.2 -i 5 \
cTap2StreamType.2.2 -i 2 \
cTap2StreamInterceptEnable.2.2 -i 1 \
cTap2StreamStatus.2.2 -i 4
```

- Get tapped packets count:

```
getmany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
cTap2StreamInterceptedPackets
```

Additional References

Related Documents

Related Topic	Document Title
Configuring SNMP Support	*Configuring SNMP Support*
Security commands	*Cisco IOS Security Command Reference*

Standards and RFCs

Standard/RFC	Title
PacketCable™ Control Point Discovery Interface Specification	*PacketCable ™ Control Point Discovery Interface Specification* (PKT-SP-CPD-I02-061013)
RFC-3924	*Cisco Architecture for Lawful Intercept in IP Networks*

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

39

MIBs

MIB	MIBs Link
• CISCO-TAP2-MIB • CISCO-IP-TAP-MIB • CISCO-802-TAP-MIB • CISCO-USER-CONNECTION-TAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Lawful Intercept

Use Cisco Feature Navigator to find information about the 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 the https://cfnng.cisco.com/ link. An account on the Cisco.com page is not required.

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

Table 4: Feature Information for Lawful Intercept

Feature Name	Releases	Feature Information
Lawful intercept - Redundant mediation devices	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on theCisco cBR Series Converged Broadband Routers.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

40

C H A P T E R 3

Cable Monitoring Feature for Cisco cBR Series Routers

After you configure cable monitoring, the router forwards copies of selected packets on the cable interface to an external LAN analyzer attached to another interface on the Cisco CMTS router. This command can help in troubleshooting network and application problems.

Note This feature does not monitor traffic for the purpose of preventing denial-of-service attacks and other types of network attacks. Even after configuring the cable monitoring feature, the traffic continues to its original destination, and only copies of the selected packets are forwarded to the CALEA server or LAN analyzer.

Note This feature doesn't support line card high availability (LCHA).

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

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

Contents

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

41

Overview of Cable Monitor Command for cBR

The **cable monitor** command sends copies of packets for specific types of traffic that is sent over a particular cable interface to a LAN analyzer, for use in troubleshooting network problems. This command can select packets to be forwarded using one or more of the following parameters:

- Either incoming or outbound packets

- Packets that match a specific MAC address (source and destination)

- Packets with a specific Service ID (SID)

Packets can also be timestamped to aid in troubleshooting. The packets are then forwarded out of the specified 10 Gigabit Ethernet port to the LAN analyzer for additional analysis.

The figure below illustrates a LAN packet analyzer attached to a Fast Ethernet port in a DOCSIS two-way configuration.

Figure 1: LAN Packet Analyzer in a DOCSIS Two-Way Configuration

> **Note** The WAN port used for cable monitoring should be exclusively used by the LAN packet analyzer.

Configuring Cable Monitoring for cBR Routers

To enable the cable traffic monitoring feature on a particular cable interface, use the following procedure, starting in privileged EXEC mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable monitor**

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

42

4. **sniff card <slot num> <ds/us> <sniff point> <filter> dest cmon-tunnel <cmon-tunnel num>**
5. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	
	`Router> enable`
	
	Example:
	
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	
	`Router# configure terminal`
	
	Example:
	
	`Router(config)#`
		Enters global configuration mode.

Step 3	**cable monitor**
	
	Example:
	
	`Router(config)# cable monitor`
	
	Example:
	
	`Router(config-cable-monitor)#`
		Enters cable monitor configuration mode.

Step 4	**sniff card <slot num> <ds/us> <sniff point> <filter> dest cmon-tunnel <cmon-tunnel num>**
	
	Example:
	
	Downstream traffic: For each channel
	
	`Router(config-cable-monitor)sniff card 3 outbound docsis integrated-Cable 3/0/0:0 dest cmon-tunnel 3`
	
	Example:
	
	Downstream traffic: For each wideband channel
	
	`Router(config-cable-monitor)sniff card 3 outbound pre-docsis wideband-Cable 3/0/0:0 dest cmon-tunnel 3`
	
	Example:
	
	Downstream traffic: For each MAC address
	
	`Router(config-cable-monitor)sniff card 3 outbound docsis mac-address 0100.5e01.0101 dest cmon-tunnel 3`
	
	Example:
	
	Upstream traffic: For each channel
		Configures the card to forward the sniffed packets.
		
		• **slot number**—Slot number of the line card
		
		• **ds/us**—Downstream or upstream
		
		• **sniff point**—Sniff point in downstream or upstream FPGA (field-programmable gate array)
		
		• **filter**—Packet type filter
		
		• **dest cmon-tunnel**—Cable monitor tunnel for captured packets
		
		• **cmon-tunnel num**—Cable monitor tunnel number for capture packets

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

43

Command or Action	Purpose

`Router(config-cable-monitor)# sniff card 3 incoming`
 	
`post-docsis upstream-cable 3/0/0 us-channel 0 dest`
`cmon-tunnel 3`
 	
Example:
 	
Upstream traffic: For each MAC address (cable modem or CPE)
 	
`Router(config-cable-monitor)#sniff card 3 incoming`
 	
`post-docsis mac-address e448.c70c.9c27 dest`
`cmon-tunnel 3`
 	
Example:
 	
Upstream traffic: For MD/SID
 	
`Router(config-cable-monitor)#sniff card 3 incoming`
 	
`post-docsis cable 3/0/0 sid 12 upstream 0 dest`
`cmon-tunnel 3`	

Step 5   **end**
 	
Example:
 	
`Router(config)# end`
 	
Example:
 	
`Router#`
	Exits global configuration mode.

What to do next

You can capture and forward the sniffed packets to an external server or a local hard disk. For more details, see .

Capturing Sniffed Packets

To forward the captured traffic to an external server, you should configure a tunnel. The external server might not be directly connected and can be away from CMTS.

To capture sniffed packets, you can follow one of these procedures:

- Capture output packets using an external host
- Capture packets by locating the hard disk

Capturing Sniffed Packets on an External Host

To forward the captured traffic to an external server, you should configure a tunnel. The external server might not be directly connected and can be away from CMTS.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

44

SUMMARY STEPS

1. **configure terminal**
2. **interface cmon-tunnel number**
3. **tunnel destination IP address**, **tunnel source IP address**
4. **end**

DETAILED STEPS

	Command or Action	**Purpose**

Step 1	**configure terminal**
	
	Example:
	
	`Router# configure terminal`
	
	Example:
	
	`Router(config)#`
		Enters global configuration mode.

Step 2	**interface cmon-tunnel number**
	
	Example:
	
	`Router(config)# interface CMON-Tunnel 3`
	`Router(config-if)#`
		Enters the interface cmon-tunnel mode to capture sniffed packets.

Step 3	**tunnel destination IP address**, **tunnel source IP address**
	
	Example:
	
	`Router(config-if)#tunnel destination 10.10.21.11`
	`Router(config-if)#tunnel source 10.10.21.1`
		Configures destination IP address and the source IP address for an external host to capture output packets.

Step 4	**end**
	
	Example:
	
	`Router(config)# end`
	
	Example:
	
	`Router#`
		Exits global configuration mode.

Capturing Sniffed Packets on a Local Hard Drive

To forward the captured traffic to a local hard disk, use the following procedure.

SUMMARY STEPS

1. **configure terminal**
2. **interface cmon-tunnel number**
3. **mode buffer**
4. **end**
5. **show platform software interface fp active name-string CMON-Tunnel number**
6. **test platform hardware qfp active feature docsis cmon-copy 3 QFP_ID**

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

45

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Router#**configure CMON-Tunnel 3** **Example:** Router(config)#	Enters global configuration mode.
Step 2	**interface cmon-tunnel number** **Example:** Router(config)#**interface CMON-Tunnel 3** Router(config-if)#	Enters the interface cmon-tunnel mode.
Step 3	**mode buffer** **Example:** Router(config-if)#**mode buffer**	Enables mode buffer in the cmon-tunnel to capture packets by locating the hard disk.
Step 4	**end** **Example:** Router(config-if)#**end** Router#	Exits global configuration mode.
Step 5	**show platform software interface fp active name-string CMON-Tunnel number** **Example:** Router# **show platform software interface fp active name-string CMON-Tunnel3** Name: CMON-Tunnel3, ID: 131074, <mark>QFP ID: 11745</mark>, Schedules: 0 Type: CABLE-MONITOR, State: enabled, SNMP ID: 0, MTU: 0 IP Address: 0.0.0.0 IPV6 Address: :: Flags: unknown ICMP Flags: unreachables, no-redirects, no-info-reply, no-mask-reply ICMP6 Flags: unreachables, no-redirects SMI enabled on protocol(s): UNKNOWN Authenticated-user: FRR linkdown ID: 65535 Monitor Type: 0, Instance ID: 3, Mode: 3 Monitor Tunnel Source: 0.0.0.0, Destination: 0.0.0.0 vNet Name: , vNet Tag: 0, vNet Extra Information: 0 Dirty: unknown AOM dependency sanity check: PASS AOM Obj ID: 24094	Gets the QFP ID.
Step 6	**test platform hardware qfp active feature docsis cmon-copy 3 QFP_ID**	Uses the QFP ID to copy the buffer to the harddisk.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

46

Command or Action	Purpose
Example: ``` Router# test platform hardware qfp active feature docsis cmon-copy 3 11745 Router #dir harddisk:	in CMON 50 -rw- 24 Mar 5 2020 12:33:42 +02:00 CMON_3_20200305-123342.pcap ```	

Cable Monitor Packet Struct

The cable monitor packet struct is described as follows:

- For post-docsis and pre-docsis sniffer points: Internal Header (16 Bytes) + Ethernet Header

- For docsis sniffer point: Internal Header (16 Bytes) + Docsis Header + Ethernet Header

If **remove-jib** is configured under CMON-Tunnel interface, the packets will not contain Internal Header.

Feature Information for Cable Monitoring

Use Cisco Feature Navigator to find information about the 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 the https://cfnng.cisco.com/ link. An account on the Cisco.com page is not required.

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

Table 5: Feature Information for Cable Monitoring

Feature Name	Releases	Feature Information
Cable Monitoring	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on theCisco cBR Series Converged Broadband Routers.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

47

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

48

Source-Based Rate Limit

The Source-Based Rate Limit (SBRL) feature prevents congestion of packets on the forwarding processor (FP) to the Route Processor (RP) interface, which can be caused by denial of service (DoS) attacks directed at the Cisco CMTS or by faulty hardware.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

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

Contents

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

49

Hardware Compatibility Matrix for the Cisco cBR Series Routers

✎

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

Table 6: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Prerequisites for Source-Based Rate Limit

• You must configure Control-Plane Policing (CoPP) for WAN-side SBRL.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

50

Restrictions for Source-Based Rate Limit

- WAN-IP and Subscriber MAC address entities are identified using a hash, and hash collisions can occur between two (or more) entities.

- On the WAN-side there is no special processing for hash collisions. Sources that hash-collide are rate-limited as if they are the same source.

- The QOS group 99 is reserved for SBRL and cannot be used for other class maps.

Information About Source-Based Rate Limit

Source-Based Rate Limit (SBRL) feature operates on the punt path in CPP. SBRL identifies and rate-limits the packet streams that can overload the punt path or RP.

Punted packets are sent from the FP to the RP through the FP-to-RP queues. Denial of service (DoS) can occur when:

- The FP-to-RP queues are congested

- The RP cannot process punted packets fast enough

In both cases, the valid punted packets are not processed properly. These situations can be caused deliberately by DoS attacks or by faulty external hardware.

Packet streams identified by SBRL are rate-limited according to configured parameters. Rate-limiting occurs in CPP before the packets reach the FP-to-RP queues. This protects the RP, and also allows other valid punted packets to reach the RP.

SBRL has a separate configuration for the WAN-side and the subscriber-side. WAN-side SBRL is disabled by default. Subscriber-side SBRL has default settings.

WAN-Side Source-Based Rate Limit

WAN-side SBRL uses Control Plane Policing (CoPP). CoPP specifies the WAN-side packet streams that are directed for SBRL. Both trusted and untrusted sites can be specified using CoPP. Using CoPP, you can specify unlimited trusted sites. Access control list (ACL) is used to specify the trusted sites.

Subscriber-Side Source-Based Rate Limit

All subscriber-side punts are processed by subscriber-side SBRL. Note that the CoPP processes all punted packets, but there is no dependency between CoPP and subscriber-side SBRL.

How to Configure Source-Based Rate Limit

This section contains the following:

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

51

Configuring WAN-Side Source-Based Rate Limit

You must enable WAN-side SBRL in two parts:

1. Configure Control Plane Policing (CoPP) to specify which packets are subject to SBRL.

2. Configure WAN-side SBRL to set the rate-limiting parameters for the specified punt-causes.

In the CoPP policy map, the special action **set qos-group 99** denotes that the packets matching a particular class are subject to WAN-side SBRL. This means that the QOS group 99 is globally reserved for SBRL, and must not be used in other policy-maps.

Packets matching a class without **set qos-group 99** bypass WAN-side SBRL. This means that CoPP is also used to specify trusted traffic streams that are not subject to WAN-side SBRL.

All punted packets are subject to CoPP. So, you must ensure that subscriber-side traffic does not match a trusted class.

WAN-side SBRL identifies traffic streams by hashing the punt cause, VRF index, and source IP address. This value is used as the index for rate-limiting. The router does not perform special processing for hash collisions, so hash-colliding streams are treated as if they are from the same stream.

By default, WAN-side SBRL is disabled.

Restrictions

- All the punted packets are subject to CoPP and punt-policing.

This section contains the following:

Configuring Control Plane Policing

Punted packets matching the trusted class bypass WAN-side SBRL. The rest of the WAN-side punts are sent to WAN-side SBRL.

Note The following example shows a simple trusted class.

Procedure

	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	**access-list** *access-list-number* **permit** *protocol* {**any** | **host** {*address* | *name*}} {**any** | **host** {*address* | *name*}} **tos** *tos*	Configures an access list for filtering frames by protocol type.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

52

	Command or Action	Purpose
	Example: Router(config)# **access-list 130 permit ip 192.168.1.10 0.0.0.0 192.168.1.11 0.0.0.0 tos 4**	**Note** Since all the punted packets are subject to CoPP, you must ensure that subscriber-side traffic does not match a trusted class.
Step 4	**class-map** *class-map-name* **Example:** Router(config)# **class-map match-all sbrl_v4_trusted**	Creates a class-map and enters QoS class-map configuration mode.
Step 5	**match access-group** *access-list-index* **Example:** Router(config-cmap)# **match access-group 130**	Specifies access groups to apply to an identity policy. The range of is from 1 to 2799.
Step 6	**exit** **Example:** Router(config-cmap)# **exit**	Exits QoS class-map configuration mode and returns to global configuration mode.
Step 7	**policy-map** *policy-map-name* **Example:** Router(config)# **policy-map copp_policy**	Specifies a service policy and enters QoS policy-map configuration mode.
Step 8	**class** *class-map-name* **Example:** Router(config)# **class sbrl_v4_trusted**	Enters QoS policy-map class configuration mode.
Step 9	**police rate** *units* **pps conform-action** *action* **exceed-action** *action* **Example:** Router(config-pmap-c)# **police rate 1000 pps conform-action transmit exceed-action transmit**	Polices traffic destined for the control plane at a specified rate. **Note** The rate is irrelevant if both the configured actions are **transmit**.
Step 10	**exit** **Example:** Router(config-pmap-c)# **exit**	Exits policy-map class police configuration mode
Step 11	**class class-default** **Example:** Router(config-pmap)# **class class-default**	Specifies the action to take on the packets that do not match any other class in the policy map.
Step 12	**set qos-group 99** **Example:** Router(config-pmap-c)# **set qos-group 99**	Enables WAN-side SBRL for the packets that match this class.
Step 13	**exit** **Example:**	Exits policy-map class configuration mode

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

53

	Command or Action	Purpose
	`Router(config-pmap-c)# exit`	
Step 14	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode
Step 15	**control-plane** [**host** | **transit** | **cef-exception**] **Example:** `Router(config)# control-plane`	Associates or modifies attributes (such as a service policy) that are associated with the control plane of the router and enters control plane configuration mode.
Step 16	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-cp)# service-policy input copp_policy`	Attaches a policy map to a control plane.
Step 17	**end** **Example:** `Router(config-cp)# end`	Exits control plane configuration mode and returns to privileged EXEC mode.

Enabling WAN-Side Source-Based Rate Limit

Procedure

	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	**platform punt-sbrl wan punt-cause** *punt-cause* **rate-per-1-sec** *rate* **Example:** `Router(config)# platform punt-sbrl wan punt-cause 10 rate-per-1-sec 4`	Configures WAN-side rate limit. • **punt-cause** *punt-cause*—Specifies the punt-cause value in number 1 to 107 or string. • **rate-per-1-sec** *rate*—Specifies the rate in packets per second. The range is from 1 to 256, specified in powers-of-2.

Configuring WAN-Side Quarantine

The WAN-side quarantine extends the WAN-side SBRL configuration. When a traffic stream enters quarantine, all punted packets in the stream are dropped for the configured period.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

54

Procedure

	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	**platform punt-sbrl wan punt-cause** *punt-cause* **rate-per-1-sec** *rate* **quarantine-time** *time* **burst-factor** *burst-factor* **Example:** Router(config)# **platform punt-sbrl wan punt-cause 10 rate-per-1-sec 4 quarantine-time 10 burst-factor 500**	Configures quarantine for the WAN-side packet stream. • **punt-cause** *punt-cause*—Specifies the punt-cause value in number 1 to 107 or string. • **rate-per-1-sec** *rate*—Specifies the rate limit in packets per second. The range is from 1 to 256, specified in powers-of-2. • **quarantine-time** *time*—Specifies the quarantine time, in minutes. The range is from 1 to 60. • **burst-factor** *burst-factor*—Specifies the burst-factor, in number of packets. The range is from 50 to 1000.

Example

When (*burst-factor* x *rate*) packets arrive at a rate faster than *rate*, the packet stream enters quarantine.

For example, during a DoS attack, when the following occurs:

- Punted packets from a WAN-side source are arrive at 100 packets per second.

- WAN-side SBRL is configured with a rate of 4 packets per second, quarantine time of 10 minutes, and burst-factor of 500 packets.

The packet rate is significantly higher than the configured rate. Therefore, when 2000 (4 x 500) packets have arrived, the packet stream enters into quarantine. Quarantine is activated at 20 seconds (2000 packets per 100 packets per second), and all punted packets from the stream are dropped for 10 minutes. After 10 minutes, the quarantine is deactivated.

The quarantine calculations restart immediately. So, if the scanning attack is continuous, quarantine is reactivated after the next 20 seconds.

Configuring Subscriber-Side Source-Based Rate Limit

Restrictions

- All punted packets are subject to CoPP and punt-policing.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

55

- The ARP-filter handles the subscriber-side ARP packets. ARP packets are not processed by subscriber-side SBRL.

- The maximum rate is 255. Due to this, the configured rate of 256 from 16.8.X will not transfer properly. A new command must be entered to transfer the configuration.

Subscriber-MAC address SBRL identifies traffic streams by hashing the punt cause and the source MAC address. The hash value is used as the index for rate-limiting. Hash-collision detection is performed so that all traffic streams are processed separately.

Default settings for subscriber-side SBRL are listed in this topic. Using the 'no' configuration returns the rate to the default value.

Rate-limiting is performed using a 2-color token-bucket algorithm. The rate is specified in packets-per-4-seconds, in the range [1, 255]. This translates to a packets-per-second rate in the range [0.25, ~64]. The optional bucket-size is specified in packets, in the range [1, 255]. If not specified, then bucket-size is set equal to rate.

The "no-drop" keyword disables rate-limiting for the specified punt-cause.

There is an optional quarantine configuration. When a traffic stream enters quarantine, all punted packets in the stream are dropped for the configured period. A traffic stream enters quarantine when (burst-factor x rate) packets arrive at a rate faster than rate. An example would be that of a faulty cable modem that continuously sends DHCPv6 solicits.

- DHCPv6 solicits from the faulty cable modem arrive at 100 packets/second, and are all punted.

- Subscriber-side SBRL is configured with a rate-per-4-sec of 8 (i.e. 2 packets-per-sec), quarantine time of 10 minutes, and burst-factor of 500 packets.

The traffic stream rate is higher than the configured rate. Therefore, when approximately 1000 (2 x 500) packets have arrived, the traffic stream enters quarantine. The quarantine happens after about 10 seconds (1000 packets at 100 packets per second), and all punted packets from the stream are dropped for 10 minutes. After 10 minutes, the quarantine is deactivated. The quarantine calculations restart immediately, so if the traffic stream remains continuous, quarantine is reactivated after the next 10 seconds.

1. **enable**

   ```
   Router> enable
   ```

   Enables privileged EXEC mode. Enter your password, if prompted.

2. **configure terminal**

   ```
   Router# configure terminal
   ```

   Enters global configuration mode.

3. **platform punt-sbrl subscriber punt-cause***punt-cause***rate-per-4-sec** *rate* [**bucket-size***bucket-size*] [**quarantine-time***time***burst-factor***burst-factor*]

   Configures subscriber-MAC address SBRL.

   - **punt-cause** *punt-cause* - Specifies the punt cause.

   - **rate-per-4-sec** *rate* - Specifies the rate in packets per 4-seconds. The range is from 1 to 255.

   - **bucket-size***bucket-size* – Specifies the bucket-size in packets. The range is from 1 to 255. If bucket-size is not entered, the bucket-size is set equal to the rate.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

56

- **quarantine-time** *time*– Specifies the quarantine time, in minutes. The range is from 1 to 60.

- **burst-factor** *burst-factor*– Specifies the burst-factor, in number of packets. The range is from 50 to 1000.

Configuring Source-Based Rate Limit Ping-Bypass

Follow the steps below to configure source-based rate limit ping-bypass.

Procedure

	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	**platform punt-sbrl ping-bypass** **Example:** Router(config)# **platform punt-sbrl ping-bypass**	Configures source-based rate limit ping-bypass.

Configuring Punt Policing

The punt policer aggregates all packets (both subscriber-side and WAN-side) with the specified punt cause, and rate-limits them according to the configured parameters.

Procedure

	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	**platform punt-policer** {**cable-snmp** | *punt-cause* }*punt-rate* [**high**] **Example:** Router(config)# platform punt-policer 1 10	Configures punt policing. - *punt-cause*—Specifies the punt cause value. - **cable-snmp**—This is the punt-cause assigned to SNMP packets destined to the CMTS.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

57

Command or Action	Purpose
	• *punt-rate*—Specifies the rate in packets/second. The range is from 10 to 300000.
	• **high**—(Optional) Specifies that the punt policing is performed only for high priority traffic.

Verifying the Source-Based Rate Limit Configuration

- **show cable dp sbrl config**—Displays the SBRL configuration, including default settings. This is equivalent to **show running-config all | include punt-sbrl**.

  Following is a sample output of the command:

  ```
  Router# show cable dp sbrl config
  platform punt-sbrl wan punt-cause for-us-data rate-per-1-sec 8
  platform punt-sbrl wan punt-cause glean-adj rate-per-1-sec 4 quarantine-time 10
  burst-factor 1000
  platform punt-sbrl subscriber punt-cause for-us-data rate-per-4-sec 32 bucket-size 32
  platform punt-sbrl subscriber punt-cause for-us-ctrl rate-per-4-sec 8 bucket-size 8
  platform punt-sbrl subscriber punt-cause cable-l3-mobility rate-per-4-sec 16 bucket-size
   16
  platform punt-sbrl subscriber punt-cause sv-match-unknown rate-per-4-sec 4 bucket-size
   4
  platform punt-sbrl subscriber punt-cause cable-pre-reg rate-per-4-sec 8 bucket-size 8
  platform punt-sbrl subscriber punt-cause cbl-dhcpv6-solicit rate-per-4-sec 8 bucket-size
   8
  platform punt-sbrl subscriber punt-cause cbl-dhcpv6-req rate-per-4-sec 8 bucket-size 8
  platform punt-sbrl subscriber punt-cause cbl-dhcpv6-sub rate-per-4-sec 8 bucket-size 8
  platform punt-sbrl subscriber punt-cause cbl-dhcpv4-sub rate-per-4-sec 8 bucket-size 8
  platform punt-sbrl subscriber punt-cause cbl-dhcpv4-disc-req rate-per-4-sec 8 bucket-size
   8
  ```

- **show access-lists** —Displays the access list information for verifying CoPP configuration.

  Following is a sample output of the command:

  ```
  Router# show access-lists

  Extended IP access list 120
      10 permit ip any any dscp af31
      20 permit ip any any dscp cs2
      30 permit ip any any dscp af21
      40 permit ip 68.86.0.0 0.1.255.255 any
  IPv6 access list TRUSTEDV6
      permit ipv6 2001:558::/32 any sequence 10
  ```

- **show policy-map** *policy-map-name*—Displays the information for the policy map.

  Following is a sample output of the command:

  ```
  Router# show policy-map copp_policy

    Policy Map copp_policy
      Class sbrl_trusted
       police rate 1000 pps
         conform-action transmit
         exceed-action transmit
  ```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

58

```
          Class class-default
            set qos-group 99
```

- **show policy-map control-plane**—Displays the control plane policy map information.

  Following is a sample output of the command:

```
Router# show policy-map control-plane

 Control Plane

  Service-policy input: copp_policy

    Class-map: sbrl_trusted (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group 120
      Match: access-group name TRUSTEDV6
      police:
          rate 1000 pps, burst 244 packets
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          transmit
        conformed 0 pps, exceeded 0 pps

    Class-map: class-default (match-any)
      28 packets, 4364 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      QoS Set
        qos-group 99
          Marker statistics: Disabled
```

- **show platform hardware qfp active infrastructure punt sbrl**—Displays the SBRL statistics.

  Following is a sample output of the command:

```
Router# show platform hardware qfp active infrastructure punt sbrl

SBRL statistics

Subscriber MAC-addr
  drop-cnt    evict-cnt   quar  MAC-Address       ID  punt-cause

-----------------------------------------------------------------------------------------------
     10000        10000     0  0010.88a3.0456   101  cable-l3-mobility

WAN-IPv4
 drop-cnt    evict-cnt   quar  VRF   cause  IP-address
--------------------------------------------------------
    456788       456788     0    0    050  1.2.0.66

WAN-IPv6
 drop-cnt    evict-cnt   quar  VRF   cause  IP-address
----------------------------------------------------------------------------
    129334       129334     1    0    011  3046:1829:fefb::ddd1
       965          965     0    0    011  2001:420:2c7f:fc01::3

. . .
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

59

Note The value of *quar* is either 0 or 1. The value 1 indicates that quarantine is activated. The *quar* value is updated only when a packet from the source is dropped. If a source enters quarantine, and then stops sending packets, the *quar* value remains 1. However, the *drop-cnt* does not increment.

Note The SBRL statistics algorithm stores the data for the worst offenders. Sources that drop only a few packets are displayed in the table initially, but may be overwritten if the *drop-cnt* does not increase continuously. The *evict-cnt* increases in tandem with *drop-cnt*, but begins to decrease when a source is no longer being actively rate-limited. When the *evict-cnt* drops below 10, the record may be overwritten.

- **show platform hardware qfp active infrastructure punt statistics type global-drop**—Displays the global punt policer statistics.

  Following is a sample output of the command:

```
Router# show platform hardware qfp active infrastructure punt statistics type global-drop

Global Drop Statistics

  Number of global drop counters = 22

  Counter ID  Drop Counter Name                          Packets
  -------------------------------------------------------------------
  000         INVALID_COUNTER_SELECTED                   0
  001         INIT_PUNT_INVALID_PUNT_MODE                0
  002         INIT_PUNT_INVALID_PUNT_CAUSE               0
  003         INIT_PUNT_INVALID_INJECT_CAUSE             0
  004         INIT_PUNT_MISSING_FEATURE_HDR_CALLBACK     0
  005         INIT_PUNT_EXT_PATH_VECTOR_REQUIRED         0
  006         INIT_PUNT_EXT_PATH_VECTOR_NOT_SUPPORTED    0
  007         INIT_INJ_INVALID_INJECT_CAUSE              0
  008         INIT_INJ_MISSING_FEATURE_HDR_CALLBACK      0
  009         PUNT_INVALID_PUNT_CAUSE                    0
  010         PUNT_INVALID_COMMON_HDR_VERSION            0
  011         PUNT_INVALID_PLATFORM_HDR_VERSION          0
  012         PUNT_PATH_NOT_INITIALIZED                  0
  013         PUNT_GPM_ALLOC_FAILURE                     0
  014         PUNT_TRANSITION_FAILURE                    0
  015         PUNT_DELAYED_PUNT_PKT_SB_NOT_IN_USE        0
  016         PUNT_CAUSE_GLOBAL_POLICER                  0
  017         INJ_INVALID_INJECT_CAUSE                   0
  018         INJ_INVALID_COMMON_HDR_VERSION             0
  019         INJ_INVALID_PLATFORM_HDR_VERSION           0
  020         INJ_INVALID_PAL_HDR_FORMAT                 0
  021         PUNT_GPM_TX_LEN_EXCEED                     0
```

- **show platform hardware qfp active infrastructure punt summary** [**threshold** *threshold-value*]—Displays the punt path rate-limiting summary.

  Following is a sample output of the command:

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

60

```
Router# show platform hardware qfp active infrastructure punt summary

Punt Path Rate-Limiting summary statistics

Subscriber-side
ID   punt cause          CPP punt     CoPP  ARPfilt/SBRL    per-cause      global
------------------------------------------------------------------------------
017  IPv6 Bad hop limit       22         0             0            0           0
050  IPv6 packet              13         0             0            0           0
080  CM not online           335         0             0            0           0


WAN-side
ID   punt cause          CPP punt     CoPP       SBRL    per-cause      global
------------------------------------------------------------------------------
017 IPv6 Bad hop limit       471         0          0            0           0
018 IPV6 Hop-by-hop Options 29901        0          0         1430           0
024 Glean adjacency          111         0          0            0           0
025 Mcast PIM signaling       19         0          0            0           0
050 IPv6 packet               11         0          0            0           0
```

- **show platform software punt-policer**—Displays the punt policer configuration and statistics.

  Following is a sample output of the command:

```
Router# show platform software punt-policer

Per Punt-Cause Policer Configuration and Packet Counters

Punt                            Configured (pps) Conform Packets   Dropped Packets
Cause Description               Normal   High    Normal     High   Normal     High
------------------------------------------------------------------------------
  2   IPv4 Options              4000     3000    0          0      0          0
  3   Layer2 control and legacy 40000    10000   16038      0      0          0
  4   PPP Control               2000     1000    0          0      0          0
  5   CLNS IS-IS Control        2000     1000    0          0      0          0
  6   HDLC keepalives           2000     1000    0          0      0          0
  7   ARP request or response   2000     1000    0          49165  0          0
  8   Reverse ARP request or re... 2000  1000    0          0      0          0
  9   Frame-relay LMI Control   2000     1000    0          0      0          0
 10   Incomplete adjacency      2000     1000    0          0      0          0
 11   For-us data               40000    5000    279977     0      0          0
 12   Mcast Directly Connected ... 2000  1000    0          0      0          0
 . . .
```

- **show platform hardware qfp active infrastructure punt policer summary**—Displays the punt policer summary.

  Following is a sample output of the command:

```
Router# show platform hardware qfp active infrastructure punt policer summary

QFP Punt Policer Config Summary


    Policer  Rate    PeakRate  ConformBurst  ExceedBurst  Scaling
    Handle   (pps)   (pps)     (pps)         (pps)        Factor
    ------------------------------------------------------------------
    001      300000  0         2288          2288         0
    002      4000    0         4000          0            0
    003      3000    0         3000          0            0
    004      40000   0         40000         0            0
    005      10000   0         10000         0            0
    006      2000    0         2000          0            0
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

61

```
007      1000     0        1000        0           0
008      2000     0        2000        0           0
009      1000     0        1000        0           0
010      2000     0        2000        0           0
011      1000     0        1000        0           0
012      2000     0        2000        0           0
013      1000     0        1000        0           0
014      2000     0        2000        0           0
  . . .
```

Configuration Example for Source-Based Rate Limit

Example: WAN-Side SBRL Configuration

```
access-list 120 permit ip any any dscp af31
access-list 120 permit ip any any dscp cs2
access-list 120 permit ip any any dscp af21
access-list 120 permit ip 192.168.1.10 0.1.255.255 any

ipv6 access-list TRUSTEDV6
  permit ipv6 any any dscp af31
  permit ipv6 any any dscp cs2
  permit ipv6 any any dscp af21
  permit ipv6 2001:558::/32 any


class-map match-all sbrl_trusted_v4
  match access-group 120

class-map match-all sbrl_trusted_v6
  match access-group name TRUSTEDV6


policy-map copp_policy
  ! IPv4 trusted:
  !   Specified rate is irrelevant.
  !   No special action; these packets bypass WAN-side SBRL.
  class sbrl_trusted_v4
    police rate 1000 pps conform transmit exceed transmit
  ! IPv6 trusted:
  !   Specified rate is irrelevant.
  !   No special action; these packets bypass WAN-side SBRL.
  class sbrl_trusted_v6
    police rate 1000 pps conform transmit exceed transmit

  ! add other classes here, if necessary

  ! Special action to activate WAN-side SBRL for this class.
  class class-default
    set qos-group 99


control-plane
  service-policy input copp_policy


platform punt-sbrl wan punt-cause for-us-data rate-per-1-sec 4
platform punt-sbrl wan punt-cause glean-adj rate-per-1-sec 4 quarantine-time 10 burst-factor
 1000
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

62

Example: Subscriber-Side SBRL Configuration

```
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-solicit rate-per-4-sec 2 bucket-size 8
platform punt-sbrl subscriber punt-cause sv-match-unknown rate-per-4-sec 4 bucket-size 10
quarantine-time 5 burst-factor 500
```

Default SBRL Configuration

Because of the dependency on CoPP, WAN-side SBRL is disabled by default. There is no default WAN-side SBRL configuration.

Subscriber-side SBRL has the following default settings:

```
platform punt-sbrl subscriber punt-cause for-us-data rate-per-4-sec 32 bucket-size 32
platform punt-sbrl subscriber punt-cause for-us-ctrl rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cable-l3-mobility rate-per-4-sec 16 bucket-size 16
platform punt-sbrl subscriber punt-cause sv-match-unknown rate-per-4-sec 4 bucket-size 4
platform punt-sbrl subscriber punt-cause cable-pre-reg rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-solicit rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-req rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-sub rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv4-disc-req rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv4-sub rate-per-4-sec 8 bucket-size 8
```

Conversion of SBRL Subscriber-side Configuration from 16.8.x to 16.9.x

In 16.9.x, several new punt-causes were added for DHCP packets on the subscriber-side. This means that the recommended configuration for 16.8.x does not match up with the default configuration in 16.9.x.

In 16.8.x, the cable-dhcp punt-cause is used by both subscriber-side and WAN-side DHCP punts. In 16.9.x, new punt-causes were added on the subscriber-side for DHCP packets, with the result that the cable-dhcp punt-cause is used ONLY for WAN-side DHCP punts. This means that configuring a rate for cable-dhcp on the subscriber-side is meaningless. The chart below shows the DHCP-related punt-causes for 16.8.x and 16.9.x. In 16.9.x, all the subscriber-side DHCP punt-causes have default SBRL settings.

Table 7: 16.8.x

punt-cause	Origin	Description
cbl-dhcpv6-solicit	sub	DHCPv6 solicit
cbl-dhcpv6-req	sub	DHCPv6 request
cable-dhcp	sub/WAN	all other DHCP packets

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

63

Source-Based Rate Limit

Conversion of Divert Rate Limit Configuration on the Cisco uBR10012 Router to SBRL Configuration on the Cisco cBR Series Routers

Table 8: 16.9.x

punt-cause	Origin	Description
cbl-dhcpv6-solicit	sub	DHCPv6 solicit
cbl-dhcpv6-req	sub	DHCPv6 request
cbl-dhcpv6-sub	sub	all other (sub-side) DHCPv6 packets
cbl-dhcpv4-disc-req	sub	DHCPv4 discover & request
cbl-dhcpv4-sub	sub	all other (sub-side) DHCPv4 packets
cable-dhcp	WAN	all (WAN-side) DHCP packets

•

Conversion of Divert Rate Limit Configuration on the Cisco uBR10012 Router to SBRL Configuration on the Cisco cBR Series Routers

Divert Rate Limit Configuration on the Cisco uBR10012 Router

The following is a sample Divert Rate Limit (DRL) configuration on the Cisco uBR10012 router:

```
service divert-rate-limit ip fib_rp_glean rate 4 limit 4
service divert-rate-limit ip fib_rp_dest rate 4 limit 4
service divert-rate-limit ip fib_rp_punt rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_dest rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_punt rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_glean rate 4 limit 4
service divert-rate-limit ipv6 icmpv6 rate 4 limit 4

service divert-rate-limit trusted-site 0.0.0.0 0.0.0.0 tos 0x68 mask 0xFF
service divert-rate-limit trusted-site 0.0.0.0 0.0.0.0 tos 0x40 mask 0xFF
service divert-rate-limit trusted-site 68.86.0.0 255.254.0.0 tos 0x0 mask 0x0
service divert-rate-limit trusted-site 0.0.0.0 0.0.0.0 tos 0x48 mask 0xFF
service divert-rate-limit trusted-site-ipv6 ::/0 traffic-class 0x40 mask 0xFF
service divert-rate-limit trusted-site-ipv6 ::/0 traffic-class 0x48 mask 0xFF
service divert-rate-limit trusted-site-ipv6 ::/0 traffic-class 0x68 mask 0xFF
service divert-rate-limit trusted-site-ipv6 2001:558::/32 traffic-class 0x0 mask 0x0

interface Cablex/y/z
    cable divert-rate-limit rate 4 limit 30
```

In Cisco IOS Release 12.2(33)SCH2, the **divert-rate-limit max-rate wan** command was introduced on the Cisco uBR10012 router. This configuration limits the aggregate rate of diverted packets on the WAN-side, on a per-divert-code basis. The following is the recommended best-practice configuration for the **divert-rate-limit max-rate wan** command:

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

64

Source-Based Rate Limit

Conversion of Divert Rate Limit Configuration on the Cisco uBR10012 Router to SBRL Configuration on the Cisco cBR Series Routers

```
service divert-rate-limit max-rate wan fib_rp_glean rate 5000
service divert-rate-limit max-rate wan fib_rp_punt rate 5000
service divert-rate-limit max-rate wan fib_rp_dest rate 40000

service divert-rate-limit max-rate wan ipv6_fib_glean rate 5000
service divert-rate-limit max-rate wan ipv6_fib_punt rate 5000
service divert-rate-limit max-rate wan ipv6_fib_dest rate 40000
```

SBRL Configuration on the Cisco cBR Series Routers

The DRL functionality is called as Source-Based Rate Limit (SBRL) on the Cisco cBR Series Routers. The punt-path has three layers of protection:

CoPP

CoPP is used to specify the trusted sites and activate WAN-side SBRL. However, since CoPP applies to all punted packets, you must ensure that cable-side punts do not match the trusted sites.

The following is a sample CoPP configuration, which is equivalent to the configuration on the Cisco uBR10012 router:

```
access-list 120 permit ip any any dscp af31
access-list 120 permit ip any any dscp cs2
access-list 120 permit ip any any dscp af21
access-list 120 permit ip 68.86.0.0 0.1.255.255 any

ipv6 access-list TRUSTEDV6
   permit ipv6 any any dscp af31
   permit ipv6 any any dscp cs2
   permit ipv6 any any dscp af21
   permit ipv6 2001:558::/32 any

class-map match-all sbrl_trusted_v4
   match access-group 120

class-map match-all sbrl_trusted_v6
   match access-group name TRUSTEDV6

policy-map copp_policy
   class sbrl_trusted_v4
     police rate 1000 pps conform transmit exceed transmit
   class sbrl_trusted_v6
     police rate 1000 pps conform transmit exceed transmit
   class class-default
     set qos-group 99

control-plane
   service-policy input copp_policy
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

65

Source-Based Rate Limit

Conversion of Divert Rate Limit Configuration on the Cisco uBR10012 Router to SBRL Configuration on the Cisco cBR Series Routers

Note
- The **set qos-group 99** command activates SBRL for the specified class.

- The police rate for **sbrl_trusted_v***x* is irrelevant, as both actions are set to **transmit**.

- You can add other trusted sites, as necessary.

SBRL

The following subscriber-side SBRL configuration is recommended. This configuration covers the expected subscriber-side punt-causes.

```
platform punt-sbrl subscriber punt-cause for-us-data rate-per-4-sec 32
platform punt-sbrl subscriber punt-cause for-us-ctrl rate-per-4-sec 8
platform punt-sbrl subscriber punt-cause sv-match-unknown rate-per-4-sec 4
platform punt-sbrl subscriber punt-cause cable-pre-reg rate-per-4-sec 8
platform punt-sbrl subscriber punt-cause cable-dhcp rate-per-4-sec 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-solicit rate-per-4-sec 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-req rate-per-4-sec 8
```

The recommended subscriber-side SBRL configuration is the default configuration. All expected subscriber-side punt-causes have default settings.

For WAN-side SBRL, the Cisco cBR Series routers do not have separate IPv4 and IPv6 configurations as the punt causes are shared between IPv4 and IPv6. The *limit* cannot be configured as the hardware policer is used. Therefore, we recommend that you configure a higher *rate* initially. In the following sample configuration, *glean-adj* and *for-us-data* correspond to **x_rp_glean** and **x_rp_dest**, respectively on the Cisco uBR 10012 router.

```
platform punt-sbrl wan punt-cause for-us-data rate 8
platform punt-sbrl wan punt-cause glean-adj rate 8
```

Note
- The *fib-punt* punt cause is used in the Cisco uBR10012 router for packets destined to the management Ethernet. This punt cause is not used on the Cisco cBR Series routers.

- The Cisco cBR Series routers do not have an equivalent punt cause for ICMPV6. In the Cisco uBR10012 routers, ICMPv6 packets must be processed by the Route Processor to generate the checksum. In the Cisco cBR Series routers, ICMPv6 is processed in the control-plane. However, ICMPv6 punts can be identified and rate-limited (in aggregate) using CoPP.

Punt Policer

The punt policer operates on all punt causes and is fully configurable. The punt policer is not divided into WAN-side and subscriber-side. All packets with a given punt cause are aggregated and rate-limited as configured.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

66

Following are the default settings (best-practice configuration) for the punt policer on the Cisco cBR Series routers:

```
punt-cause                      LO      HI

CPP_PUNT_CAUSE_GLEAN_ADJ        2000    5000
CPP_PUNT_CAUSE_FOR_US           40000   5000
```

Note
- The equivalent punt cause for *fib-glean* (on the Cisco uBR10012 router) is *GLEAN_ADJ/HI* on the Cisco cBR Series routers.

- The equivalent punt cause for *fib-dest* (on the Cisco uBR10012 router) is *FOR_US/LO* on the Cisco cBR Series routers.

Additional References

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Source-Based Rate Limit

Use Cisco Feature Navigator to find information about the 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 the https://cfnng.cisco.com/ link. An account on the Cisco.com page is not required.

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

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

67

Table 9: Feature Information for Source-Based Rate Limit

Feature Name	Releases	Feature Information
Source-based rate limit	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on theCisco cBR Series Converged Broadband Routers.
Source-based rate limit	Cisco IOS XE Gibraltar 16.12.1z1	A new punt cause **cable-snmp** was added to rate-limit the SNMP packets destined to the CMTS.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

68

Cable Duplicate MAC Address Reject

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 that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

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

Contents

Hardware Compatibility Matrix for the Cisco cBR Series Routers

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

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

69

Table 10: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

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)

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

70

- 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.

Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 2 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.

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 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.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

71

- 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.

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

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

72

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 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

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

73

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.

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.

Procedure

	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.
Step 4	**cable privacy eae-policy** {**capability-enforcement** | **disable-enforcement** | **ranging-enforcement** | **total-enforcement**} **Example:**	Specifies EAE enforcement policies on DOCSIS 3.0 cable modems.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

74

	Command or Action	Purpose
	Router(config-if)# **cable privacy eae-policy total-enforcement**	
Step 5	**end** **Example:** Router(config)# **end**	Returns to privileged EXEC mode.

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.

Procedure

	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.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x ■

■ **75**

	Command or Action	Purpose
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.

Configuring AES-128 for non-MTC DOCSIS3.0 Cable Modem

This feature is enabled by default. To disable this feature, follow the steps below:

```
enable
configure terminal
no cable privacy non-mtc-aes128
end
```

Verifying AES-128 for non-MTC DOCSIS3.0 Cable Modem

To verify whether AES-128 is supported for non-MTC DOCSIS3.0 Cable Modem, use **show running-config** command as shown in the example below:

```
Router# show running-config | include cable privacy non-mtc-aes128
no cable privacy non-mtc-aes128
```

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 cBR-8 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
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

76

```
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 cBR-8 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.

To verify which cable modems are excluded from EAE enforcement on the Cisco CMTS router, use the **show cable privacy** command.

To verify BPI+ enforcement policies, use the **show interface cable privacy** command.

> **Note** A character "*" is placed before the online state to identify modems that have not satisfied the bpi-plus-policy.

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 cBR-8 router.

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.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

77

- 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: %CBR-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: %CBR-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: %CBR-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: %CBR-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: %CBR-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: %CBR-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

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 the 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 the https://cfnng.cisco.com/ link. An account on the Cisco.com page is not required.

✎

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

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

78

Table 11: Feature Information for Cable Duplicate MAC Address Reject

Feature Name	Releases	Feature Information
Cable Duplicate MAC Address Reject	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on theCisco cBR Series Converged Broadband Routers.
AES-128 for non-MTC DOCSIS 3.0 Cable Modem	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on theCisco cBR Series Converged Broadband Routers.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

79

Feature Information for Cable Duplicate MAC Address Reject

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

80

CHAPTER 6

Cable ARP Filtering

This document describes the Cable ARP Filtering feature for the Cisco Cable Modem Termination System (CMTS). This feature enables service providers to filter Address Resolution Protocol (ARP) request and reply packets, to prevent a large volume of such packets from interfering with the other traffic on the cable network.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

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

Contents

Hardware Compatibility Matrix for the Cisco cBR Series Routers

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

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

81

Table 12: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Prerequisites for Cable ARP Filtering

No specialequipment or softwareis needed to use the Cable ARP Filtering feature.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

82

Restrictions for Cable ARP Filtering

Cisco cBR-8 Router Restrictions

- The Cisco cBR-8 router maintains ARP filtering statistics on the Supervisor (SUP) module. Statistics are viewed with the **show cable arp-filter** command for a specified interface. When a switchover event occurs, as in SUP Redundancy, these ARP filtering statistics are reset to zero.

- The Cable ARP Filter feature is not configurable per subinterface.

FP ARP Filter Restrictions

- The FP microcode must be enhanced to provide the rate limiting functionality for ARP filtering in FP.
- The ARP Filter in FP feature is not configurable per subinterface.

Information About Cable ARP Filtering

Overview

Theft-of-service and denial-of-service (DNS) attacks have become increasingly common in cable broadband networks. In addition, virus attacks are becoming more common, and users are often unaware that their computers have become infected and are being used to continue the attacks on the network.

One sign that often appears during these attacks is an unusually high volume of Address Resolution Protocol (ARP) packets. The user or virus repeatedly issues ARP requests, trying to find the IP addresses of additional computers that might be vulnerable to attack.

ARP requests are broadcast packets, so they are broadcast to all devices on that particular network segment. In some cases, a router can also forward ARP broadcasts to an ARP proxy for further processing.

This problem is also made worse because some low-end routers commonly used by subscribers for home networks can also incorrectly respond to all ARP requests, which generates even more traffic. Until these customer premises equipment (CPE) devices can be upgraded with firmware that is compliant to the appropriate Request for Comments (RFC) specifications, service providers need to be able to deal with the incorrectly generated or forwarded traffic.

In addition, the Cisco CMTS router automatically monitors ARP traffic and enters the IP addresses found in ARP requests into its own ARP table, in the expectation that a device will eventually be found with that IP address. Unacknowledged IP addresses remain in the router's ARP table for 60 seconds, which means that a large volume of ARP traffic can fill the router's ARP table.

This process can create a large volume of ARP traffic across the network. In some situations, the volume of ARP requests and replies can become so great that it can throttle other traffic and occupy most of the Cisco CMTS router's processing time, hampering efforts by technicians to recover their network.

The router cannot use fast-switching to process ARP packets, but must instead forward them to the route processor (RP). Because of this, processing a large volume of ARP traffic can also prevent the router from handling normal traffic.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

83

Filtering ARP Traffic

To control the volume of ARP traffic on a cable interface, you can configure the **cable arp filter** command to specify how many ARP packets are allowed per Service ID (SID) during a user-specified time period. You can configure separate thresholds for ARP request packets and for ARP reply packets.

When a cable interface is configured to filter ARP packets, it maintains a table of the number of ARP request or reply packets that have been received for each SID. If a SID exceeds the maximum number of packets during the window time period, the Cisco CMTS drops the packets until a new time period begins.

> ✎
> **Note**   If using bundled cable interfaces, the Cable ARP Filtering feature is configured on the primary and subordinate interfaces separately. This allows you to configure the feature only on the particular interfaces that require it. In addition, you can configure the feature with different threshold values, allowing you to customize the feature for each interface's traffic patterns.

Monitoring Filtered ARP Traffic

After ARP filtering has been enabled on a cable interface, you can then use the service **divert-rate-limit** command to display the devices that are generating excessive amounts of ARP traffic. These devices could be generating this traffic for any of the following reasons:

- Cable modems that are running software images that are either not DOCSIS-compliant or that have been hacked to allow theft-of-service attacks.
- CPE devices that are either performing a theft-of-service or denial-of-service attack, or that have been infected with a virus that is searching for other computers that can be infected.
- Routers or other devices that mistakenly reply to or forward all ARP requests.

After identifying the specific devices that are generating this traffic, you can use whatever techniques are allowed by your service level agreements (SLAs) to correct the problem.

Linksys Wireless-Broadband Router (BEFW11S4)

The Linksys Wireless-B Broadband Router, Model number BEFW11S4 version 4 with 1.44.2 firmware, incorrectly sends its own ARP reply packet for every ARP request packet it receives, instead of replying only to the ARP requests that are specifically for itself. Customers with these routers should upgrade the firmware to the latest revision to fix this bug. To upgrade the firmware, go to the download section on the Linksys website.

> ✎
> **Note**   It is extremely important that non-compliant CPE devices be updated to firmware that correctly handles ARP and other broadcast traffic. Even one or two non-compliant devices on a segment can create a significant problem with dropped packets, impacting all of the other customers on that segment.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

84

ARP Filtering in FP

ARP filter feature is performed on SUP FP complex. When enabled, this FP complex filters ARP packets for identified ARP offenders, decreasing the ARP punt rate and RP CPU usage. It also provides the user with clearer separation in ARP filtering by utilizing source MAC addresses instead of SIDs.

The filter logic now filters by source MAC address instead of by SID. Currently, the modem MAC addresses are excluded from having their ARPs filtered, but Multimedia Terminal Adapters (MTAs) and other non-offending CPEs can still (statistically) have ARPs filtered because all ARPs appear to come from the same SID. Therefore, filtering by source MAC address will isolate the filtering to the offensive devices. By doing so, a customer who has Voice-over-IP (VoIP) service via an MTA and an infected CPE will not have MTA issues while being contacted by the service provider in regards to the infected CPE.

ARP offenders will still be allowed to use ARP to avoid complete loss of Internet connectivity through their configured or provisioned gateway address. Because of this, it is expected that the "ARP Input" process will still show a few percentage points of CPU usage, but the net interrupt CPU usage will decrease.

Note ARP filtering in FP is enabled by default on Cisco cBR-8 router.

Filtering ARP Traffic in FP

When ARP traffic in FP is enabled, a lightweight algorithm executing on the RP is used to identify ARP offenders by the source MAC address or the SID. All offending source MAC addresses or SIDs are then programmed by the ARP Filter control module into the FP ucode divert rate limiting module (ARP offenders are still allowed to perform ARP transactions, but only at the configured filtering rate).

Offending source MAC addresses or SIDs are filtered in FP for a minimum of 50 minutes (ten 5-minute intervals with no occurring offenses). Utilizing the existing ARP Filter CLI tools, the cable operator can obtain enough information about the modem and CPE to contact the end user to request the necessary anti-virus software installation or firmware upgrade for the CPE.

Note If the offending device is not "repaired" or shut off, it will remain in the FP ARP Filter indefinitely.

The FP ARP rate limiter is designed to filter a maximum of 16,000 ARP offenders. If this pool of 16,000 filterable entities is exhausted, then the entity is filtered on the RP. The CLI statistics will distinguish mac addresses filtered on the RP verses FP.

Because of possible mac address hash collisions, ARP offenders that cannot be programmed into the FP ARP rate limiter will still be filtered in FP by SID. Since the hash is done by source mac address and SID, such devices can actually moved back to mac address filtering by deleting the associated modem and forcing it back online with a new SID (this merely a possibility and is not expected to be a common practice).

ARP packets with a source mac address that is not "known" to the CMTS as a modem or CPE will be filtered by their SID in FP. Therefore, there will never be an unusual ARP packet source that will NOT be filtered in FP. False ARP packets with invalid operation codes will be filtered as if they are an ARP Reply.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

85

How to Configure Cable ARP Filtering

Use the following procedures to determine whether ARP filtering is required and to configure ARP filtering on one or more cable interfaces.

Monitoring ARP Processing

Use the following steps to monitor how the router is processing ARP traffic and whether the volume of ARP packets is a potential problem.

Step 1 To discover the CPU processes that are running most often, use the **show process cpu sorted** command and look for the ARP Input process:

Example:

```
Router# show process cpu sorted

CPU utilization for five seconds: 99%/28%; one minute: 93%; five minutes: 90%
 PID Runtime(ms)   Invoked     uSecs   5Sec   1Min   5Min TTY Process
  19  139857888  44879804      3116 31.44% 28.84% 28.47%   0 ARP Input
 154   74300964  49856254      1490 20.29% 19.46% 15.78%   0 SNMP ENGINE
  91   70251936   1070352     65635  8.92%  9.62%  9.59%   0 CEF process
  56   17413012  97415887       178  3.01%  3.67%  3.28%   0 C10K BPE IP Enqu
  78   24985008  44343708       563  3.68%  3.47%  3.24%   0 IP Input
  54    6075792   6577800       923  0.90%  0.67%  0.65%   0 CMTS SID mgmt ta
...
```

In this example, the ARP Input process has used 31.44 percent of the CPU for the past five seconds. Total CPU utilization is also at 99 percent, indicating that a major problem exists on the router.

Note As a general rule, the ARP Input process should use no more than one percent of CPU processing time during normal operations. The ARP Input process could use more processing time during certain situations, such as when thousands of cable modems are registering at the same time, but if it uses more than one percent of processing time during normal operations, it probably indicates a problem.

Step 2 To monitor only the ARP processes, use the **show process cpu | include ARP** command:

Example:

```
Router# show process cpu | include ARP

  19  139857888  44879804      3116 31.44% 28.84% 28.47%   0 ARP Input
 110          0         1         0  0.00%  0.00%  0.00%   0 RARP Input
```

Step 3 To monitor the number of ARP packets being processed, use the **show ip traffic** command.

Example:

```
Router# show ip traffic | begin ARP

ARP statistics:
  Rcvd: 11241074 requests, 390880354 replies, 0 reverse, 0 other
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

86

```
     Sent: 22075062 requests, 10047583 replies (2127731 proxy), 0 reverse
```

Repeat this command to see how rapidly the ARP traffic increases.

Step 4   If ARP traffic appears to be excessive, use the **show cable arp-filter** command to display ARP traffic for each cable interface, to identify the interfaces that are generating the majority of the traffic.

Example:

```
Router# show cable arp-filter Cable5/0/0

ARP Filter statistics for Cable5/0/0:
  Rcvd Replies: 177387 total, 0 unfiltered, 0 filtered
  Sent Requests For IP: 68625 total, 0 unfiltered, 0 filtered
  Sent Requests Proxied: 7969175 total, 0 unfiltered, 0 filtered
```

In the above example, the unfiltered and filtered counters show zero, which indicates that ARP filtering has not been enabled on the cable interface. After ARP filtering has been enabled with the **cable arp filter** command, you can identify the specific devices that are generating excessive ARP traffic by using the **service divert-rate-limit** command (see the Identifying the Sources of Major ARP Traffic, on page 88).

Enabling ARP Filtering

Use the following procedure to enable ARP filtering on a particular cable interface.

Procedure

	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** *x/y* **Example:** Router(config)# **interface cable 5/1**	Enters interface configuration mode for the specified cable interface.
Step 4	**cable arp filter reply-accept** *number window-size* **Example:**	Configures the cable interface to accept only the specified *number* of ARP reply packets every *window-size* seconds for each active Service ID (SID) on that interface. The cable

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

87

	Command or Action	Purpose
	Router(config-if)# **cable arp filter reply-accept 2 2**	interface drops ARP reply packets for a SID that would exceed this number. (The default behavior is to accept all ARP reply packets.)
Step 5	**cable arp filter request-send** *number window-size* **Example:** Router(config-if)# **cable arp filter request-send 3 1**	Configures the cable interface to send only the specified *number* of ARP request packets every *window-size* seconds for each active SID on that interface. The cable interface drops ARP requests for a SID that would exceed this number. (The default behavior is to send all ARP request packets.) **Note** Repeat Step 3 through Step 5 to enable ARP filtering on other cable interfaces. Primary and subordinate interfaces in a cable bundle must be configured separately.
Step 6	**end** **Example:** Router(config-if)# **end**	Exits interface configuration mode and returns to privileged EXEC mode.

Identifying the Sources of Major ARP Traffic

After you have begun filtering ARP traffic on a cable interface, use the following procedure to identify the cable modems or CPE devices that are generating or forwarding major amounts of ARP traffic.

Tip The Linksys Wireless-B Broadband Router, Model number BEFW11S4 version 4 with 1.44.2 firmware, has a known problem in which it incorrectly generates an ARP reply for every ARP request packet it receives. See the Linksys Wireless-Broadband Router (BEFW11S4) guide for information on how to resolve this problem.

Step 1 To discover the devices that are responsible for generating or forwarding more ARP requests on a specific cable interface than a specified minimum number of packets, use the **show cable arp-filter requests-filtered** command where *number* is the threshold value for the number of packets being generated:

Example:

```
show cable arp-filter cable interface requests-filtered number
```

For example, to display the devices that have generated more than 100 ARP request packets, enter the following command:

Example:

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 100
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

88

```
Sid   MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
1     0006.2854.72d7 10.3.81.4       12407          0                    0
81    00C0.c726.6b14 10.3.81.31      743            0                    0
```

Step 2   Repeat the **show cable arp-filter** command to show how quickly the devices are generating the ARP packets.

Step 3   To discover the devices that are responsible for generating or forwarding more ARP replies on a specific cable interface than a specified minimum number of packets, use the **show cable arp-filter replies-filtered** command where *number* is the threshold value for the number of packets being generated:

Example:

```
show cable arp-filter cable interface requests-filtered number
```

For example, to display the devices that have generated more than 200 ARP reply packets, enter the following command:

Example:

```
Router# show cable arp-filter cable 5/0/0 replies-filtered 200
```

```
Sid   MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
2     0006.53b6.562f 10.11.81.16     0              0                    2358
191   0100.f31c.990a 10.11.81.6      0              0                    11290
```

Step 4   (Optional) If a particular cable modem is generating or forwarding excessive ARP replies, contact the customer to see if they are using a Linksys Wireless-B Broadband Router, Model number BEFW11S4. If so, this router could be running old firmware that is incorrectly generating excessive ARP packets, and the customer should upgrade their firmware. For more information, see the Linksys Wireless-Broadband Router (BEFW11S4) guide

Step 5   Repeat this command during each filter period (the time period you entered with the **cable arp filter** command) to show how quickly the devices are generating the ARP packets.

Step 6   (Optional) The ARP reply and request packet counters are 16-bit counters, so if a very large number of packets are being generated on an interface, these counters could wrap around to zero in a few hours or even a few minutes. Clearing the ARP counters eliminates stale information from the display and makes it easier to see the worst offenders when you suspect ARP traffic is currently creating a problem on the network.

To eliminate the modems that are not currently triggering the ARP filters and to isolate the worst current offenders, use the **clear counters cable** *interface* command to reset all of the interface counters to zero. Then the **show cable arp-filter** commands clearly identify the SIDs of the modems that are currently forwarding the most ARP traffic.

For example, the following example indicates that a number of modems are forwarding a large enough volume of ARP traffic that they have triggered the ARP packet filters:

Example:

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 10
```

```
Sid   MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
1     0006.2854.72d7 10.3.81.4       8              0                    0
23    0007.0e02.b747 10.3.81.31      32             0                    0
57    0007.0e03.2c51 10.3.81.31      12407          0                    0
...
81    00C0.c726.6b14 10.3.81.31      23             0                    0
```

SID 57 shows the largest number of packets, but it is not immediately apparent if this modem is causing the current problems. After clearing the counters though, the worst offenders are easily seen:

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

89

Example:

```
Router# clear counter cable 5/1/0

Clear show interface counters on this interface [confirm] y

08:17:53.968: %CLEAR-5-COUNTERS: Clear counter on interface Cable5/1/0 by console
Router# show cable arp cable 5/1/0

ARP Filter statistics for Cable3/0:
  Replies Rcvd: 0 total. 0 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 0 total. 0 unfiltered, 0 filtered

Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address     Req-Filtered  Req-For-IP-Filtered  Rep-Filtered
Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address     Req-Filtered  Req-For-IP-Filtered  Rep-Filtered
57   0007.0e03.2c51 10.3.81.31     20            0                    0
81   00C0.c726.6b14 10.3.81.31     12            0                    0
Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address     Req-Filtered  Req-For-IP-Filtered  Rep-Filtered
57   0007.0e03.2c51 10.3.81.31     31            0                    0
81   00C0.c726.6b14 10.3.81.31     18            0                    0
```

Step 7   (Optional) If the Req-For-IP-Filtered column shows the majority of ARP packets, use the **show cable arp-filter ip-requests-filtered** command to display more details about the CPE device that is generating this traffic. Then use the **debug cable mac-address** and **debug cable arp filter** commands to display detailed information about this particular traffic; for example:

Example:

```
Router# show cable arp-filter c5/0/0 ip-requests-filtered 100

Sid  MAC Address    IP Address      Req-Filtered Req-For-IP-Filtered Rep-Filtered
1    0007.0e03.1f59 50.3.81.3       0            37282               0
Router# debug cable mac-address 0007.0e03.1f59

Router# debug cable arp filter

Router#
Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip 50.3.81.13 dip
 50.3.82.173 prot 6 len 46 SrcP 445 DstP 445
Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip 50.3.81.13 dip
 50.3.82.174 prot 6 len 46 SrcP 445 DstP 445
Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip 50.3.81.13 dip
 50.3.82.175 prot 6 len 46 SrcP 445 DstP 445
[additional output omitted]...
```

This example shows that the CPE device at IP address 50.3.81.13 is sending packets to TCP port 445 to every IP address on the 50.3.82.0 subnet, in a possible attempt to find a computer that has Microsoft Windows file-sharing enabled.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

90

Step 8   After determining the specific devices that are generating excessive ARP traffic, you can take whatever action is allowed by your company's service level agreements (SLAs) to correct the problem.

Examples

In this example, two cable interfaces, C5/0/0 and C7/0/0, are joined in the same bundle, which means the interfaces share the same broadcast traffic. Separate devices on each interface are generating excessive ARP traffic:

- The device at MAC address 000C.2854.72D7 on interface C7/0/0 is generating or forwarding a large volume of ARP requests. Typically, this device is a cable modem that is forwarding the ARP requests that are being generated by a CPE device behind the modem. The CPE device could be attempting a theft-of-service or denial-of-service attack, or it could be a computer that has been infected by a virus and is trying to locate other computers that can be infected.
- The device at MAC address 000C.53B6.562F on Cable 5/0/0 is responding to a large number of ARP requests, which could indicate that the device is a router that is running faulty software.

The following commands identify the device on the C7/0/0 interface that is generating the excessive ARP requests:

```
Router# show cable arp-filter c7/0/0

ARP Filter statistics for Cable7/0/0:
  Replies Rcvd: 3 total. 3 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 27906 total. 562 unfiltered, 27344 filtered
Router# show cable arp-filter c7/0/0 requests-filtered 100

Sid  MAC Address    IP Address    Req-Filtered    Req-For-IP-Filtered    Rep-Filtered
1    000C.2854.72d7 50.3.81.4     62974           0                      0
```

The following commands identify the device on the C5/0/0 interface that is generating the excessive ARP replies:

```
Router# show cable arp-filter c5/0/0

ARP Filter statistics for Cable5/0/0:
  Replies Rcvd: 2400 total. 456 unfiltered, 1944 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 26 total. 26 unfiltered, 0 filtered
Router# show cable arp-filter c5/0/0 replies-filtered 100

Sid  MAC Address    IP Address    Req-Filtered    Req-For-IP-Filtered    Rep-Filtered
2    000C.53b6.562f 50.3.81.6     0               0                      2097
```

Clearing the Packet Counters

To clear the packet counters on an interface, which includes the ARP packet counters, use the **clear counters cable** *interface* command. You can also clear the packet counters on all interfaces by using the **clear counters** command without any options. This allows you to use the **show cable arp** commands to display only the CPE devices that are currently generating the most traffic.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

91

![Note icon]

Note   The **clear counters** command clears all of the packet counters on an interface, not just the ARP packet counters.

Identifying ARP Offenders in FP

When the FP ARP Filter feature is enabled, use the **show cable arp-filter** *interface* command to generate a list of ARP offenders.

cBR-8 Outputs in FP

When the FP ARP Filter feature is enabled, the cBR-8 output formatting displays the modem and the CPE addresses on a single line, in addition to the following columns:

- M/S—This column shows if packets are being filtered by MAC address or SID. A majority of these columns will show MAC address.
- Rate—This column shows the packet rate for FP-filtered packets in the last 5 minutes monitoring time window. Rate is not calculated for RP-filtered packets.
- Pro—This column will identify the processor that performed the filtering with either "RP" or "FP." On the cBR-8, it is expected that 99.9% of Pro fields will show "FP."

The following is a sample output for an ARP request on a cBR-8 in FP:

```
Router# show cable arp-filter Bundle1 requests-filtered 40
Interface Cable5/0/0 - none
Interface Cable6/0/2
Sid  CPE Mac        CPE IP          Modem MAC       Modem IP        M/S Rate Pro REQS
4    00d0.b75a.822a 50.3.81.56      0007.0e03.9cad 50.3.81.15       MAC -    RP  46
4    00d0.b75a.822a 50.3.81.56      0007.0e03.9cad 50.3.81.15       MAC 25   FP  5012
5    00b0.d07c.e51d 50.3.81.57      0007.0e03.1f59 50.3.81.13       MAC -    RP  64000
6    -              -               0006.2854.7347 50.3.81.4        MAC 101  FP  5122
7    -              -               0006.2854.72d7 50.3.81.11       SID -    FP  961205
Interface Cable7/0/0 - none
```

This sample output demonstrates the following:

- SID 4 shows a CPE filtered in FP. The threshold specified is low enough to show the packets that were filtered on the RP as the offender was being identified. A high enough threshold would not have shown the RP-filtered packets. The ARP packet rate of 25 is shown for FP-filtered packets.
- SID 5 shows a CPE filtered on the RP. This is extremely unusual and only occurs when the maximum number of FP-filterable entities has been reached.
- SID 6 shows a modem filtered in FP (CPE MAC or CPE IP are not shown).
- SID 7 shows ARP packets from an "unknown" source MAC address filtered by SID in FP.

The counts for requests, replies, and requests for IP will no longer be shown on a single line in order to keep the line concise and less than 90 characters in length.

The "REQs" column is now stated as "REPs" in the case of ARP replies. The column will show "REQ-IP" in cases involving ARP requests for IP.

Requests being sent by the CMTS due to encroaching IP packets, "ip-requests-filtered", will still be filtered on the RP and not in FP, with Access Control Lists (ACLs) used to defeat IP-based scanning traffic, and the IP punt rate limiting feature for cBR-8 used to decrease the punt rate for such traffic. The ARP Filter can still be used to perform analysis of these IP traffic streams.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

92

Configuration Examples for Cable ARP Filtering

This section provides the following examples of how to configure the Cable ARP Filtering features:

ARP Filtering Configuration on an Individual Cable Interface: Example

The following example shows a typical configuration of a cable interface that is configured for the Cable ARP Filtering feature:

```
!
interface Cable5/0/0
 ip address 192.168.100.1 255.255.255.0 secondary
 ip address 192.168.110.13 255.255.255.0
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream channel-id 0
 cable upstream 0 frequency 6000000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000 200000
 cable upstream 0 minislot-size 16
 cable upstream 0 modulation-profile 6 7
 no cable upstream 0 shutdown
 cable upstream 1 frequency 26000000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000 200000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 6 7
 no cable upstream 1 shutdown
 cable upstream 2 frequency 15008000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000 200000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 6 7
 cable upstream 2 shutdown
 cable upstream 3 spectrum-group 25
 cable upstream 3 channel-width 3200000 200000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable upstream 4 frequency 21008000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 3200000 200000
 cable upstream 4 minislot-size 16
 cable upstream 4 modulation-profile 1
 no cable upstream 4 shutdown
 cable upstream 5 spectrum-group 25
 cable upstream 5 channel-width 3200000 200000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 1
 cable upstream 5 shutdown
 cable arp filter request-send 4 2
 cable arp filter reply-accept 4 2
end
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

93

ARP Filtering Configuration on Bundled Cable Interfaces: Example

The following example shows a typical configuration of a cable interface bundle that is also using the Cable ARP Filtering feature. Both the primary and subordinate interface are configured separately, allowing you to configure the feature only on the particular interfaces that require it. In addition, you can configure the feature with different threshold values, allowing you to customize the feature for each interface's traffic patterns.

```
!
interface Cable5/0/0
 description Master cable interface
 ip address 10.3.130.1 255.255.255.0 secondary
 ip address 10.3.131.1 255.255.255.0 secondary
 ip address 10.3.132.1 255.255.255.0 secondary
 ip address 10.3.133.1 255.255.255.0 secondary
 ip address 10.3.81.1 255.255.255.0
 ip helper-address 10.14.0.4
 load-interval 30
 cable bundle 1 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 0
 cable upstream 0 frequency 5008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 1
 no cable upstream 0 shutdown
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 1
 cable upstream 1 shutdown
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 1
 cable upstream 2 shutdown
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable arp filter request-send 4 2
 cable arp filter reply-accept 4 2
!
interface Cable7/0/0
 description Slave cable interface--Master is C5/0/0
 no ip address
 cable bundle 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 562000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream 0 connector 0
 cable upstream 0 frequency 5008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

94

```
cable upstream 1 channel-width 1600000
cable upstream 1 minislot-size 4
cable upstream 1 modulation-profile 21
cable upstream 1 shutdown
cable upstream 2 connector 2
cable upstream 2 channel-width 1600000
cable upstream 2 minislot-size 4
cable upstream 2 modulation-profile 21
cable upstream 2 shutdown
cable upstream 3 connector 3
cable upstream 3 channel-width 1600000
cable upstream 3 minislot-size 4
cable upstream 3 modulation-profile 21
cable upstream 3 shutdown
cable arp filter request-send 20 5
cable arp filter reply-accept 20 5
end
```

ARP Filtering in FP Default Configuration: Example

The following example shows the default configuration of a cable interface for the ARP Filtering in FP feature.

```
interface Bundle1
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
end
```

Additional References

The following sections provide references related to the Cable ARP Filtering feature.

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
Source-Based Rate Limit	http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cmts_sec_and_cable_mon_features_cbr/source-based_rate_limit.html
show platform hardware qfp active infrastructure punt summary command	http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref/b_cmts_cable_cmd_ref_chapter_010100.html

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

95

Feature Information for Cable ARP Filtering

Use Cisco Feature Navigator to find information about the 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 the https://cfnng.cisco.com/ link. An account on the Cisco.com page is not required.

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

Table 13: Feature Information for the Cable ARP Filtering Feature

Feature Name	Releases	Feature Information
Cable ARP Filtering	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on theCisco cBR Series Converged Broadband Routers.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

96

C H A P T E R 7

Subscriber Management Packet Filtering Extension for DOCSIS 2.0

The Cisco converged broadband router supports management of data packet filtering based on the subscriber's preferences and criteria. Packet filtering enhances security to the cable network by allowing only the specific packets to flow to the Customer Premise Equipment (CPE) while dropping the unwanted data packets from the cable network.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

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

Contents

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note

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

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

97

Table 14: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Prerequisites for Configuring Subscriber Management Packet Filtering

The software prerequisites for the subscriber management packet filtering feature are:

- The latest software image is loaded and working on the Cable Modem Termination System (CMTS) and the cable modems (CM).
- The configuration information on the main supervisor (SUP) and the standby SUP should be the same before the switchover.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

98

Restriction for Configuring Subscriber Management Packet Filtering

- This feature can define up to 254 filtering groups. The number of filters in each group is 255.

Information About Configuring Subscriber Management Packet Filtering

A filter group specifies what filters are applied to the packets going to or coming from each specific CM or CPE device. It defines the rules or criteria to filter or drop a packet. Every packet that has to be filtered can either be accepted to send or filtered to be dropped. The criteria to filter a packet depends on the subscriber's preferences. The filter group can be applied to different subscriber management groups.

Cable subscriber management can be established using the following configuration methods:

- CMTS router configuration (via CLI)
- SNMP configuration

The process of configuring the subscriber management packet filtering is:

1. The packet filter group defines the action for a packet. The packet can be let to go to the CPE or dropped off the cable network based on the subscriber's packet criteria.
2. The CM sends a registration request to the CMTS. The registration request contains provisioning information that defines the association of a Packet Filtering Group (PFG) with the CM and its subscribers.
3. The specific downstream or upstream PFGs are used to bind the CM, CPE, embedded Multimedia Terminal Adaptor (eMTA), embedded Set-Top Box (eSTB) and embedded portal server (ePS) to a specific PFG.
4. The CMTS identifies the CPE device based on the CPE's DHCP information.

Note   For the filter group to work for CMs, a CM must re-register after the CMTS router is configured.

How to Configure Subscriber Management Packet Filtering

This section describes the configuration tasks that are performed to manage subscriber packet filtering on the Cisco CMTS platforms. You can use the command-line interface (CLI) commands to complete the configuration.

Configuring the Filter Group

This section describes the tasks to configure the packet filter group. Follow the summary steps to complete the configuration.

To create, configure, and activate a DOCSIS filter group that filters packets on the basis of the TCP/IP and UDP/IP headers, use the cable filter group command in global configuration mode.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

99

Procedure

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> **enable** **Example:** Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal** **Example:** Router(config)#	Enters global configuration mode.
Step 3	**cable filter group group-id index index-num [option option-value]** **Example:** Router(config)# **cable filter group 10 index 10 src-ip 10.7.7.7**	Creates, configures, and activates a DOCSIS filter group that filters packets.

Defining the Upstream and Downstream MTA Filter Group

This section describes the configuration tasks to define the upstream and downstream subscriber management filter groups for an embedded Multimedia Terminal Adaptor (eMTA.) Follow the summary steps to complete the configuration.

Procedure

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

100

	Command or Action	Purpose
	Router# **configure terminal**	
Step 3	cable submgmt default filter-group mta {downstream | upstream} group-id **Example:** Router(config)# **cable submgmt default filter-group mta downstream 130**	Defines the upstream and downstream subscriber management filter groups for an MTA.

Defining the Upstream and Downstream STB Filter Group

This section describes the configuration tasks to define the upstream and downstream subscriber management filter groups for a Set-Top Box (STB.) Follow the summary steps to complete the configuration.

Procedure

	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	cable submgmt default filter-group stb {downstream | upstream} group-id **Example:** Router(config)# **cable submgmt default filter-group stb downstream 20**	Defines the upstream and downstream subscriber management filter groups for an STB.

Defining the Upstream and Downstream PS Filter Group

This section describes the configuration tasks to define the upstream and downstream subscriber management filter groups for a Portal Server (PS.) Follow the summary steps to complete the configuration.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x ■

■ **101**

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable** **Example:** Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal** **Example:** Router(config)#	Enters global configuration mode.
Step 3	cable submgmt default filter-group ps {downstream | upstream} group-id **Example:** Router(config)# **cable submgmt default filter-group ps downstream 10**	Defines the upstream and downstream subscriber management filter groups for a portal server.

Configuration Examples for Subscriber Management Packet Filtering

This section describes a sample configuration example for configuring the subscriber management packet filtering.

Configuring the Filter Group: Example

The following example shows configuration of a filter group that drops packets with a source IP address of 10.7.7.7 and a destination IP address of 10.8.8.8, and a source port number of 2000 and a destination port number of 3000. All protocol types and ToS and TCP flag values are matched:

```
Router(config)# cable filter group 10 index 10 src-ip 10.7.7.7
Router(config)# cable filter group 10 index 10 src-mask 255.255.0.0
Router(config)# cable filter group 10 index 10 dest-ip 10.8.8.8
Router(config)# cable filter group 10 index 10 dest-mask 255.255.0.0
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

102

```
Router(config)# cable filter group 10 index 10 ip-proto 256
Router(config)# cable filter group 10 index 10 src-port 2000
Router(config)# cable filter group 10 index 10 dest-port 3000
Router(config)# cable filter group 10 index 10 tcp-flags 0 0
Router(config)# cable filter group 10 index 10 match-action drop
```

Defining the Upstream and Downstream MTA Filter Group: Example

The following example shows configuration of an upstream and downstream MTA filter group.

```
Router# configure terminal
Router(config)# cable submgmt default filter-group mta downstream 10
```

Defining the Upstream and Downstream STB Filter Group: Example

The following example shows configuration of an upstream and downstream STB filter group.

```
Router#configure terminal
Router(config)#cable submgmt default filter-group stb downstream 20
```

Defining the Upstream and Downstream PS Filter Group: Example

The following example shows configuration of an upstream and downstream portal server filter group.

```
Router#configure terminal
Router(config)#cable submgmt default filter-group ps downstream 10
```

Additional References

The following sections provide references related to configuring the subscriber management packet filtering feature.

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

103

FeatureInformationforSubscriberManagementPacketFiltering

Use Cisco Feature Navigator to find information about the 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 the https://cfnng.cisco.com/ link. An account on the Cisco.com page is not required.

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

Table 15: Feature Information for Subscriber Management Packet Filtering

Feature Name	Releases	Feature Information
Subscriber management packet filtering	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on theCisco cBR Series Converged Broadband Router

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

104

CHAPTER **8**

MAC Filtering

This feature enables/disables MAC address filter on the backhaul interface.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

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

Contents

Hardware Compatibility Matrix for the Cisco cBR Series Routers

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

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

105

Table 16: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Information About MAC Filtering

With this feature, only the packet whose destination MAC address is the MAC address of the router interface can be forwarded. It supports 32 unicast filter entries per interface. It is disabled by default.

Note When port-channel is enabled, MAC filtering must be enabled on backhaul interface to take effect.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

106

Note	When both dot1q l2vpn and MAC filtering are enabled on backhaul interface, only 1 unicast filter entry is supported per backhaul interface. The MAC filtering is only supported for non-l2vpn unicast packets.

How to Configure MAC Filtering

This section describes the configuration tasks that are performed to manage MAC filtering. You can use the command-line interface (CLI) commands to complete the configuration.

Configuring MAC Filtering

To configure MAC filtering, follow the steps below:

```
enable
configure terminal
interface tenGigabitEthernet slot/subslot/port
mac-addr-filter
end
```

Verifying MAC Filtering

To verify the MAC filtering configuration on the backhaul interface, use **show running-config interface** command as shown below:

```
Router# show running-config interface tenGigabitEthernet 4/1/0
Building configuration...

Current configuration : 73 bytes
!
interface TenGigabitEthernet4/1/0
 no ip address
 mac-addr-filter
end
```

To verify the MAC filtering status on a specific SUP slot and SUP-PIC bay, use **show platform software iomd** command as shown below:

```
Router# show platform software iomd 4/4 mac-filter
IOMD (Input Output Module Driver) Mac Filter Status


port: 0     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
          Input Drop cnt:                   0      Total Drop cnt:
    0
          Entry Number:    1
    Index      Mode     Action           Entry MAC           Entry MASK           Match
Count
      00     enable      pass     c4:14:3c:16:7c:04     ff:ff:ff:ff:ff:ff
    0
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

107

```
port: 1       promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
              Input Drop cnt:                    0      Total Drop cnt:
     0
              Entry Number:    1
     Index      Mode     Action         Entry MAC          Entry MASK          Match
Count
       00    enable       pass   c4:14:3c:16:7c:05   ff:ff:ff:ff:ff:ff
  1729


port: 2       promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
              Input Drop cnt:                    0      Total Drop cnt:
     0
              Entry Number:    1
     Index      Mode     Action         Entry MAC          Entry MASK          Match
Count
       00    enable       pass   c4:14:3c:16:7c:06   ff:ff:ff:ff:ff:ff
     0


port: 3       promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
              Input Drop cnt:                    0      Total Drop cnt:
     0
              Entry Number:    1
     Index      Mode     Action         Entry MAC          Entry MASK          Match
Count
       00    enable       pass   c4:14:3c:16:7c:07   ff:ff:ff:ff:ff:ff
     0


port: 4       promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
              Input Drop cnt:                    0      Total Drop cnt:
     0
              Entry Number:    1
     Index      Mode     Action         Entry MAC          Entry MASK          Match
Count
       00    enable       pass   c4:14:3c:16:7c:08   ff:ff:ff:ff:ff:ff
     0


port: 5       promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
              Input Drop cnt:                    0      Total Drop cnt:
     0
              Entry Number:    1
     Index      Mode     Action         Entry MAC          Entry MASK          Match
Count
       00    enable       pass   c4:14:3c:16:7c:09   ff:ff:ff:ff:ff:ff
    15


port: 6       promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
              Input Drop cnt:                    0      Total Drop cnt:
     0
              Entry Number:    1
     Index      Mode     Action         Entry MAC          Entry MASK          Match
Count
       00    enable       pass   c4:14:3c:16:7c:0a   ff:ff:ff:ff:ff:ff
     0
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

108

```
port: 7        promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
               Input Drop cnt:                   0      Total Drop cnt:
    0
           Entry Number:   1
   Index      Mode    Action         Entry MAC          Entry MASK          Match
Count
      00    enable      pass    c4:14:3c:16:7c:0b    ff:ff:ff:ff:ff:ff
    0
```

If the MAC filtering is disabled, the output of the **show platform software iomd** command is shown as below:

```
Router# show platform software iomd 4/5 mac-filter
IOMD (Input Output Module Driver) MAC filter Status


port: 0        promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
               Input Drop cnt:                   0      Total Drop cnt:
    0
               Entry Number:   0


port: 1        promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
               Input Drop cnt:                   0      Total Drop cnt:
    0
               Entry Number:   0


port: 2        promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
               Input Drop cnt:                   0      Total Drop cnt:
    0
               Entry Number:   0


port: 3        promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
               Input Drop cnt:                   0      Total Drop cnt:
    0
               Entry Number:   0


port: 4        promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
               Input Drop cnt:                   0      Total Drop cnt:
    0
               Entry Number:   0


port: 5        promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
               Input Drop cnt:                   0      Total Drop cnt:
    0
               Entry Number:   0


port: 6        promiscuous mode:     unicast: enable   multicast: enable     broadcast:
enable
               Input Drop cnt:                   0      Total Drop cnt:
```

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

109

```
            0
                Entry Number:   0


port: 7     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
                Input Drop cnt:                   0     Total Drop cnt:
    0
                Entry Number:   0
```

Configuration Examples for MAC Filtering

This section describes a sample configuration example for configuring the MAC filtering.

```
router> enable
router# configure terminal
router(config)# interface tenGigabitEthernet 4/1/0
router(config-if)# mac-addr-filter
router(config-if)# end
```

Feature Information for MAC Filtering

Use Cisco Feature Navigator to find information about the 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 the https://cfnng.cisco.com/ link. An account on the Cisco.com page is not required.

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

Table 17: Feature Information for MAC Filtering

Feature Name	Releases	Feature Information
MAC Filtering	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.

Cisco cBR Series Converged Broadband Routers Security and Cable Monitoring Configuration Guide for Cisco IOS XE Amsterdam 17.3.x

110