Cisco CMTS Security and Cable Monitoring Features Configuration Guide

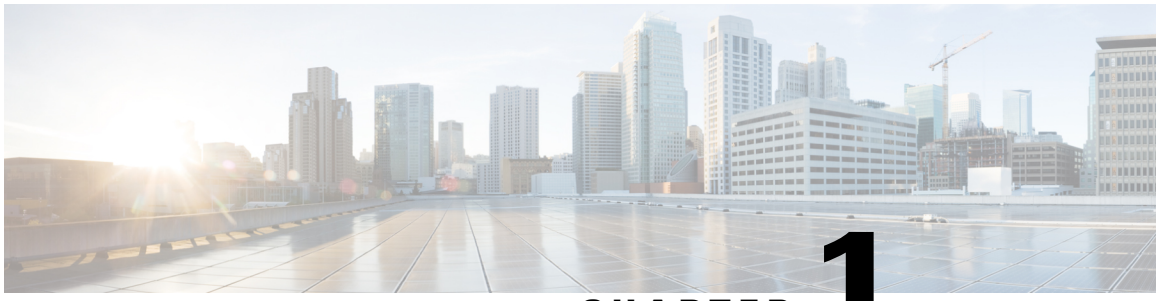
First Published: 2008-02-14

Last Modified: 2012-12-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27612-02

CONTENTS



CHAPTER 1

Cable ARP Filtering

First Published: February 14, 2008

Last Updated: February 9, 2009

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

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 documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Content

Prerequisites for Cable ARP Filtering

The Cable ARP Filtering feature is supported on the Cisco CMTS routers in Cisco IOS software release trains 12.3BC and 12.2SC. Table 1: Cable ARP Filtering Hardware Compatibility Matrix, on page 2 shows the hardware compatibility prerequisites for this.

Table 1: Cable ARP Filtering Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR10-MC5X20S/U[1] **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V[2] **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V 2
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 Cisco IOS Release 12.2(33)SCB • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V 2
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 Cisco IOS Release 12.2(33)SCB • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V 2

1 Supports only DOCSIS 2.0 and IPv6 cable modems.
2 Supports only DOCSIS 3.0 and IPv6 cable modems.

Restrictions for Cable ARP Filtering

Cisco uBR7100 Series Restrictions

- The Cable ARP Filtering feature is not supported on the Cisco uBR7100 series universal broadband routers.

Cisco uBR10012 Router Restrictions

- The Cisco uBR10012 router maintains ARP filtering statistics on the Performance Routing Engine (PRE) module. Statistics are viewed with the **show cable arp-filter** command for a specified interface. When a switchover event occurs, as in RPR+ Redundancy, these ARP filtering statistics are reset to zero.

Cisco uBR10012 PRE modules support the Route Processor Redundancy Plus (RPR+) feature in several Cisco IOS releases. Refer to the following document for additional information:

Route Processor Redundancy Plus for the Cisco uBR10012 Universal Broadband Router

http://www.cisco.com/en/US/docs/cable/cmts/feature/u10krprp.html

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

PXF ARP Filter Restrictions

- The PXF microcode must be enhanced to provide the rate limiting functionality for ARP filtering in PXF.
- ARP filtering in PXF is only supported on the Performance Routing Engine 2 (PRE2) and later versions. For more information, refer to the ARP Filtering in PXF, on page 5.
- The ARP Filter in PXF 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.

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 master and slave 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.

ARP Filtering in PXF

Cisco Release 12.3(17a)BC introduces a PXF component to the ARP filter feature. When enabled, this PXF component 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 PXF is only supported on the PRE2 and later versions, and is enabled by default.

Filtering ARP Traffic in PXF

When ARP traffic in PXF 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 PXF 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 PXF 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 PXF ARP Filter indefinitely.

The PXF 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 PXF.

Because of possible mac address hash collisions, ARP offenders that cannot be programmed into the PXF ARP rate limiter will still be filtered in PXF 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 PXF. Therefore, there will never be an unusual ARP packet source that will NOT be filtered in PXF. False ARP packets with invalid operation codes will be filtered as if they are an ARP Reply.

Note ARP filtering in PXF is only supported on the PRE2 and later versions.

PXF Divert-Rate-Limit

Diverted packets sent from the forwarding processor (FP) to the route processor (RP), via the FP-to-RP interface, may encounter congestion when packets requiring diversion arrive at the FP at a faster rate than they can be transmitted to the RP. When congestion occurs, valid packets in the FP-to-RP queues will be dropped. This situation can be deliberately caused by attacks directed at the CMTS or inadvertently by faulty external hardware.

PXF Divert-Rate-Limit identifies packet streams that will cause congestion of the FP-to-RP interface. Packets in the stream are dropped according to the configured rate-limiting parameters. Rate-limiting occurs before the packets are placed in the FP-to-RP queues, preventing valid packets in other streams from being dropped.

The following diverted packets will be rate-limited:

- fwd-glean—Packets that hit a glean adjacency in the Forwarding Information Base (FIB).
- rpf-glean—Packets that hit a glean adjacency during the Reverse Path Forwarding (RPF) check.

Packets that pass rate-limiting are diverted as they normally would be. Packets that fail rate-limiting are dropped.

Rate-limiting is implemented by a token-bucket algorithm. The token-bucket algorithm requires two variables: rate and limit. Both the rate and limit are configurable via the CLI. The rate is the average number of packets-per-second that pass the rate-limiting code. The limit can be thought of as the number of packets that will pass during an initial burst of packets.

Note The Divert-Rate-Limit feature is always on and cannot be turned off. Using the no form of the configuration CLI returns the rate-limiting parameters to their default values. During a PXF and CPU switchover or reload, the configuration is retained, but not the statistics. Therefore, after switchover, the statistics shown by the show pxf cpu statistics drl command will show zero.

fwd-glean

IP packets that hit a glean adjacency in the FIB are diverted. There are three requirements:

- RPF-check has passed (if required).
- SV-check has passed (if required).
- Forward adjacency is glean.

Packets are rate-limited based on the destination IP address. A hash on the destination IP address is used to create an index that stores state information for rate-limiting. In the event of a hash collision, the pre-existing state information will be used and updated. The table that stores state information is large enough to make collisions rare.

rpf-glean

The RPF feature is modified to divert packets that hit a glean adjacency during the RPF check. A new divert_code will be created for this type of diverted packet. Currently, these packets are dropped.

There are four requirements:

- SV-check has passed (if required).
- RPF is enabled.
- The packet is from a non-load-balanced interface.
- RPF-adjacency is glean.

Packets are rate-limited based on the source IP address. A hash on the source IP address is used to create an index that stores state information for rate-limiting. In the event of a hash collision, the pre-existing state information will be updated. The table that stores state information is large enough to make collisions rare.

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
  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 10).

Enabling ARP Filtering

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *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:** `Router(config-if)# cable arp filter reply-accept 2 2`	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 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. Master and slave 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

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:

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.

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.

The following example shows the ARP packet counters being cleared:

```
Router# show cable arp cable 3/0

ARP Filter statistics for Cable3/0:
  Replies Rcvd: 3278 total. 84 unfiltered, 3194 filtered
  Requests Sent For IP: 941 total. 30 unfiltered, 911 filtered
  Requests Forwarded: 941 total. 37 unfiltered, 904 filtered
Router# show cable arp cable 3/0 replies-filtered 1
Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
2    0006.2854.71e7 50.3.72.2       1815           0                    3194
Router# show cable arp cable 3/0 requests-filtered 1
Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
2    0006.2854.71e7 50.3.72.2       1815           0                    3194


Router# clear counter cable 3/0

Clear "show interface" counters on this interface [confirm] y

22:38:45.875: %CLEAR-5-COUNTERS: Clear counter on interface Cable3/0 by console



Router# show cable arp cable 3/0

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 cable 3/0 replies-filtered 1
```

```
Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered

Router# show cable arp cable 3/0 requests-filtered 1

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
```

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

Identifying ARP Offenders in PXF

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

The following example shows a list of ARP offenders being generated:

```
Router# show cable arp-filter ?

  Bundle  Cable Virtual bundle interface
  Cable   CMTS interface
uBR-15#sho cable arp-filter Bundle1 ?
  ip-requests-filtered  Show modems with arp request for IP packet filter count
                        at or above x
  replies-filtered      Show modems with arp reply filter count at or above x
  requests-filtered     Show modems with arp request filter count at or above x
  |                     Output modifiers
  <cr>
```

The following is a sample output from the CLI:

```
Router# show cable arp-filter Bundle1 requests-filtered 40
Interface Cable5/0/0 - none
Interface Cable6/0/2
Sid  MAC Address    IP Address      Req-Filtered Req-For-IP-Filtered Rep-Filtered
4    0007.0e03.9cad 50.3.81.15      46           0                   0
Interface Cable7/0/0 - none
```

PRE2 Outputs in PXF

When the PXF ARP Filter feature is enabled, the PRE2 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 PXF-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 “PXF.” On the PRE2, it is expected that 99.9% of Pro fields will show “PXF.”

The following is a sample output for an ARP request on a PRE2 in PXF:

```
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   PXF 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  PXF 5122
7    -              -               0006.2854.72d7 50.3.81.11      SID -    PXF 961205
Interface Cable7/0/0 - none
```

This sample output demonstrates the following:

- SID 4 shows a CPE filtered in PXF. 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 PXF-filtered packets.
- SID 5 shows a CPE filtered on the RP. This is extremely unusual and only occurs when the maximum number of PXF-filterable entities has been reached.
- SID 6 shows a modem filtered in PXF (CPE MAC or CPE IP are not shown).
- SID 7 shows ARP packets from an “unknown” source MAC address filtered by SID in PXF.

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 PXF, with Access Control Lists (ACLs) used to defeat IP-based scanning traffic, and the IP punt rate limiting feature for PRE2 used to decrease the punt rate for such traffic. The ARP Filter can still be used to perform analysis of these IP traffic streams.

PRE1 and Cisco 7246 Outputs in PXF

When the PXF ARP Filter is enabled, the PRE1 and Cisco 7246 output for the show commands is simplified to exclude all columns that do not apply.

The following is a sample output for an ARP request on a PRE1 or 7246 in PXF:

```
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 REQs
4    00d0.b75a.822a 50.3.81.56      0007.0e03.9cad 50.3.81.15      MAC 5058
5    00b0.d07c.e51d 50.3.81.57      0007.0e03.1f59 50.3.81.13      MAC 64000
6    -              -               0006.2854.7347 50.3.81.4       MAC 5122
7    -              -               0006.2854.72d7 50.3.81.11      SID 961205
Interface Cable7/0/0 - none
```

Configuring PXF Divert-Rate-Limit

Use the following procedure to configure Divert-Rate-Limit packet streams to identify potential congestion of the FP-to-RP interface.

DETAILED STEPS

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

Step 3	Do one of the following:
	• service divert-rate-limit divert-code rate limit
	
	Example:
	
	`Router(config)# service divert-rate-limit fib-rp-glean 10 limit 20`
	
	Example:
	
	`Router(config)# service divert-rate-limit fib-rpf-glean 10 limit 20`
		Configures the Divert-Rate-Limit for the following packets:
		• fwd-glean—Packets that hit a glean adjacency in the FIB.
		• rpf-glean—Packets that hit a glean adjacency during the RPF check.
		
		The rate is the average number of packets-per-second that pass the rate-limiting code. The minimum rate is 1 packet-per-second and the maximum rate is 255 packets-per-second. The default rate is 20 packets-per-second.
		The minimum limit is 4 packets and the maximum limit is 255 packets. The default limit is 5 packets.
		Note Using the no form of the service divert-rate-limit command will reset the rate and limit to the default values.

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

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
```

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 master and slave 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
 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 PXF Default Configuration: Example

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

Related Documents

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

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 826	An Ethernet Address Resolution Protocol (ARP)
RFC 2665	DOCSIS Ethernet MIB Objects Support

RFCs	Title
RFC 2669	Cable Device MIB

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 ARP Filtering on the Cisco Cable Modem Termination System

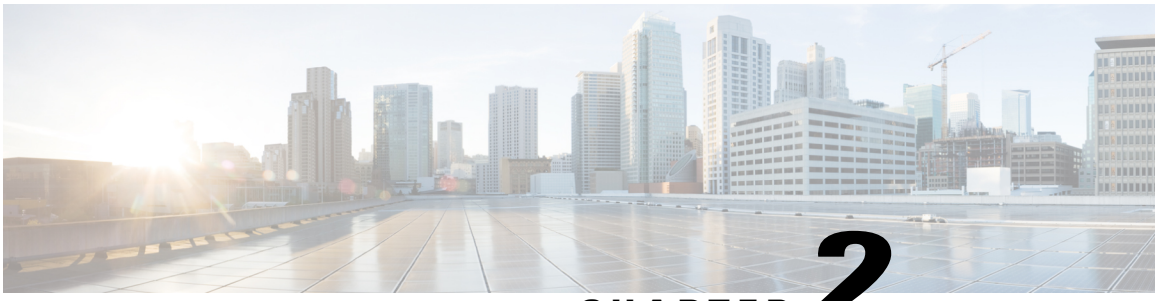
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/.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

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

Table 2: Feature Information for the Cable ARP Filtering Feature

Feature Name	Releases	Feature Information
Cable ARP Filtering	12.2(15)BC2	This feature was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.

Feature Name	Releases	Feature Information
Cable ARP Filtering	12.2(15)BC2b	The **ip-requests-filtered** option was added to the **service divert-rate-limit** command to display the specific Service IDs (SIDs) that are generating or forwarding a minimum number of ARP packets.
Cable ARP Filtering	12.3(9a)BC	Introduced optional syntax for the cable arp filter command, where number and window-size values are optional for reply-accept and request-send settings.
Cable ARP Filtering	12.3(17a)BC	The **show cable arp-filter** command was introduced for the PXF ARP Filter feature. The **service divert-rate-limit** command was introduced. Default settings changed for two commands to result as follows: • **cable arp filter request-send 3 2** • **cable arp filter reply-accept 3 2**
Cable ARP Filtering	12.2(33)SCA	This feature is integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.



CHAPTER 2

Cable Monitor and Intercept Features for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: December 02, 2012

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

The Cable Monitor and Intercept features for Cisco Cable Modem Termination System (CMTS) routers provide a software solution for monitoring and intercepting traffic coming from a cable network. These features give service providers Lawful Intercept capabilities, such as those required by the Communications Assistance for Law Enforcement Act (CALEA).

Finding Feature Information

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

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

Contents

Prerequisites for the Cable Monitor and Intercept Features on the Cisco CMTS Routers

The Cable Monitor and Intercept Features for the Cisco CMTS Routers is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC.

Note The cable monitor and intercept features began support in Cisco IOS Releases prior to 12.2BC; however, several of these releases and hardware have since reached End-of-Life (EOL) and therefore we are showing only some of the latest Cisco IOS software release trains in this hardware compatibility table. For more information about the complete feature history, see the Feature Information for Cable Monitor and Intercept Features for the Cisco CMTS Routers, on page 40.

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

Table 3: Cable Monitor and Intercept for the Cisco CMTS Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [3]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [4]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

3 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

4 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for Cable Monitor and Intercept

- The **cable intercept** command by itself does not fulfill the PacketCable requirements for Lawful Intercept capability. To meet these requirements, PacketCable operations must also be enabled and configured on the Cisco CMTS router (see the documents in the Additional References, on page 38 for instructions on enabling PacketCable).
- For Cisco uBR10012 routers, starting from Cisco IOS Release 12.2(33)SCC, the **cable intercept** command is configured only under bundle interface and for Cisco uBR7200 series routers, **cable intercept** is allowed in Cable interface, however it is recommended to configure in Bundle interface.

Note Starting from Cisco IOS Release 12.2(33)SCH, the **cable intercept** command is not allowed to configure in Cable Interface, both in Cisco uBR7200 series and Cisco uBR10012 routers.

- The WAN interface on which packets are forwarded when using the **cable monitor** command should be used exclusively by the LAN analyzer. This interface must be an Ethernet, Fast Ethernet, Gigabit Ethernet or Ten Gigabit Ethernet interface.

- Intercepted data from the **cable intercept** command is sent to a user-specified User Datagram Port (UDP) at a user-specified IP address. The data collector at that IP address must have exclusive use of the specified UDP port.
- The interception of customer traffic is governed by local laws and the service level agreements (SLA) with those customers. Consult the proper legal authorities before intercepting and monitoring third-party traffic. Also see the documents on CALEA and Lawful Intercept in the Additional References, on page 38.
- The Cable Monitor and Intercept feature does not support monitoring of upstream traffic if upstream channel bonding is configured on a cable interface line card.
- The Cable Monitor feature does not function correctly after a cable line card switchover. To recover from this change in functionality, re-apply the **cable monitor** command.
- The **cable monitor outbound downstream** command can be enabled:
  - only one mac-domain on a line card at a time
  - for one modular-cable or intergrated-cable interface per line card at one time
  - for one wideband-cable interface per line card at one time
- The Cable intercept feature is used to implement lawful intercept to monitor specific data or traffic streams. It is not a management tool. The information related to changes in modem states or CPE states, like DHCP information, cannot be intercepted by cable intercept feature.

Information About Cable Monitor and Intercept

Cisco CMTS routers support the following two complementary commands to intercept traffic being sent or received over a cable interface:

- **cable intercept—**Forwards copies of the traffic to and from a specific MAC address to a server at a specific IP address and UDP port. This command can be used to respond to CALEA requests from law enforcement for traffic concerning a specific user.
- **cable monitor—**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.

See the following sections for more information about these commands.

Note These commands do not monitor or intercept traffic for the purpose of preventing denial-of-service attacks and other types of network attacks. With both of these commands, the traffic continues on to its original destination, and only copies of the selected packets are forwarded to the CALEA server or LAN analyzer.

- Service Independent Intercept (SII), a superset of the existing Packet Intercept (PI) feature, is one of several systems for law enforcement to monitor traffic on the Cisco CMTS. SII differs from other systems in its ability to monitor both non-voice as well as voice traffic. Whereas the current PI feature supports the interception of UDP packets only, SII supports the interception of any legal IP protocol. In addition, because SII uses SNMP (specifically SNMPv3), its use can be hidden from other users of the CMTS.

SII requires two devices: an interception device with which to intercept monitored traffic, and a mediation device (MD) that filters and reads the intercepted traffic. Here the interception device is the Cisco CMTS, and the MD is an SNMP management workstation.

Overview of the cable intercept Command

The **cable intercept** command forwards all traffic to and from a particular MAC address on a specific cable interface to a data collection server at a particular IP address and User Datagram Protocol (UDP) port. This command examines the source and destination MAC addresses of each Ethernet frame that is transmitted over the selected cable interface, and when a match is found, a copy of the frame is encapsulated within a UDP packet and forwarded to the specified server.

Note The MAC address being intercepted is typically the MAC address of a user's CPE device (PC, Voice-over-IP phone, or so forth), not the MAC address of the cable modem.

This command can be used to comply with the United States Federal Communications Assistance for Law Enforcement Act (CALEA) and other Lawful Intercept requirements for voice communications. For specifics on CALEA Lawful Intercept, see the *PacketCable Electronic Surveillance Specification* , as listed in the Additional References, on page 38.

This command requires that the law enforcement agency (LEA) provide a server at the specified IP address with an application that monitors the given UDP port and collects all of the data sent to that port. The choice of this application is up to the LEA. Although this application could be as simple as a packet sniffer, typically the LEA would desire a more complex application that could reconstruct the user's original data or voice traffic.

Note Before Cisco IOS Release 12.1(11b)EC, the destination server had to be within two network hops of the Cisco CMTS router. This restriction was removed in Cisco IOS Release 12.1(11b)EC, 12.2(4)BC1, and all later releases.

Note Starting from Cisco IOS Release 12.2(33)SCC, the cable intercept command is configured under bundle interface.

Overview of the Cable Monitor Command

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:

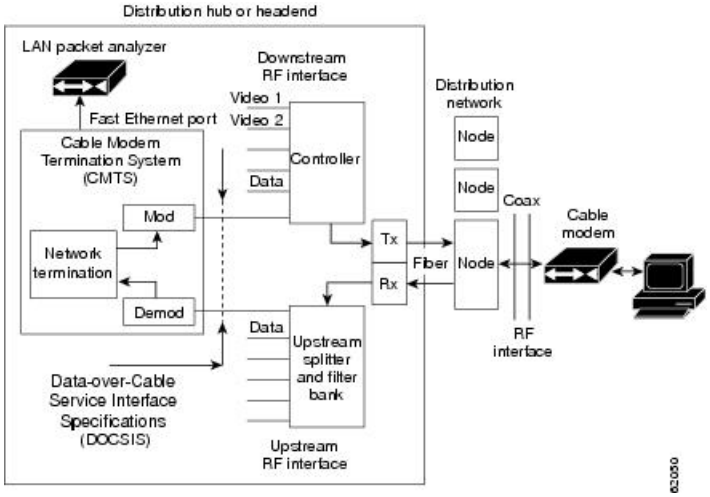
- Either incoming or outbound packets
- Packets that match an IP access list
- Packets that match a specific MAC address (source and destination)
- Packets with a specific Service ID (SID)

- When monitoring a specific SID, select only specific DOCSIS MAC-layer packet types (dynamic service packets, MAP grant packets, and MAP request packets)

In addition, the **cable monitor** command can forward full DOCSIS packets, or it can strip the DOCSIS headers and forward only the Ethernet frames. Packets can also be timestamped to aid in troubleshooting. The packets are then forwarded out of the specified Ethernet or Fast 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.

Tip When you are using the **cable monitor** command, and are including the DOCSIS header along with the Ethernet frame, it is possible that the total size of the forwarded packet could exceed the maximum allowable size for an Ethernet frame (1500 bytes), if the original Ethernet frame is at or near 1500 bytes. This is because the **cable monitor** command adds the DOCSIS header to the existing Ethernet frame. If this happens, the console displays a system message similar to the following: %LINK-4-TOOBIG:Interface Ethernet2/0, Output packet size of 1518 bytes too big This error message is typically accompanied by a traceback display. Both the error message and traceback are informational only and can be ignored. They do not indicate a traffic flow problem with the cable modem being monitored.

Note All cable modems may be captured while specifying the MAC address for a single cable modem for packets received on the upstream (**incoming**) and transmitted on the downstream (**outbound**). This issue occurs while executing the **cable monitor interface mac address** command and the MAC address of a cable modem is specified.

Overview of CISCO-TAP-MIB

There is no user-accessible CLI to support the SII feature. All interaction is implemented by means of SNMPv3, and all configurations, both for taps (SII intercepts) as well as the mediation device, are implemented by means of the CISCO-TAP-MIB.

Note At the time of publication, the Cisco IOS 12.3 BC release train does not support virtual private networks with the SII feature. The CISCO-TAP-MIB does not specify any particular VPN, so this MIB is not assigned to a particular instance of VPN routing/forwarding (VRF).

Table 4: CISCO-TAP-MIB Objects and Restrictions , on page 29 lists the objects in the MIB, as well as restrictions for the Cisco uBR10012 CMTS other than those listed in the MIB itself.

Table 4: CISCO-TAP-MIB Objects and Restrictions

Object	Restrictions for Cisco uBR10012
cTapMediationDestAddressType	Only IPv4 is supported (ITD restriction)
cTapMediationDestAddress	
cTapMediationDestPort	
cTapMediationSrcInterface	
cTapMediationRtcpPort	Not supported (ITD restriction[5])
cTapMediationDscp	
cTapMediationDataType	
cTapMediationRetransmitType	Not supported (ITD restriction)
cTapMediationTimeout	
cTapMediationTransport	UDP only (ITD restriction)
cTapMediationNotificationEnable	
cTapMediationStatus	
cTapMediationCapabilities	
cTapStreamCapabilities	
cTapStreamIpInterface	Only if interface is cable
cTapStreamIpAddrType	IPv4 only

Object	Restrictions for Cisco uBR10012
cTapStreamIpDestinationAddress	
cTapStreamIpDestinationLength	Must be 32 (no subnets)
cTapStreamIpSourceAddress	
cTapStreamIpSourceLength	
cTapStreamIpTosByte	
cTapStreamIpTosByteMask	
cTapStreamIpFlowId	Not supported (IPv6 only)
cTapStreamIpProtocol	
cTapStreamIpDestL4PortMin	Must match ...DestL4PortMax, or zero
cTapStreamIpDestL4PortMax	Must match ...DestL4PortMin, or 65535
cTapStreamIpSourceL4PortMin	Must match ...SourceL4PortMin, or zero
cTapStreamIpSourceL4PortMax	Must match ...SourceL4PortMax, or 65535
cTapStreamIpInterceptEnable	
cTapStreamIpInterceptedPackets	
cTapStreamIpInterceptDrops	
cTapStreamIpStatus	

[5] This means the restriction is across all Cisco platforms, not just Cisco CMTS platforms.

Benefits

The **cable intercept** command helps the CMTS or network administrator to:

- Comply with CALEA requirements for Lawful Intercept.
- Comply with PacketCable requirements for electronic surveillance.

Monitoring upstream and downstream data packets with the **cable monitor** command helps the CMTS or network administrator to:

- Manage network variables and understand network issues that affect application performance and functionality.

- Resolve interoperability problems.

SII, with SNMPv3, helps the CMTS or network administrator, in conjunction with law enforcement, to:

- Monitor both voice and non-voice traffic, unlike with PI.
- Hide the use of SII from other users of the Cisco CMTS.

How to Configure Cable Intercept and Monitoring Features

Configuring the Cable Intercept Feature

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

Note For Cisco uBR10012 router, a maximum of 4095 MAC intercepts can be configured. This includes the MAC intercepts configured using the cable intercept command, and other lawful intercept features (such as SII). The bandwidth used by each MAC intercept is also a deciding factor for the number of MAC intercepts that can be configured. High bandwidth usage by a MAC intercept might reduce the number of MAC intercepts that can be configured.

DETAILED STEPS

	Command or Action	Purpose

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

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

Step 3	Do one of the following:
	• **interface cable** *x /y*
	`Router(config)# interface cable 4/0`
	• **interface bundle** *x*
	`Router(config)# interface bundle 1`
		Enters cable or bundle interface configuration mode for the specified cable or bundle interface.
		Note Starting from Cisco IOS Release 12.2(33)SCC, the cable intercept command is configured under bundle interface.

	Command or Action	Purpose
Step 4	**cable intercept** *mac-address i p-address udp-port* **Example:** `Router(config-if)# cable intercept 000C.0102.0304 10.10.10.45 8132`	Enables cable interception on this cable or bundle interface with the following parameters: • *mac-address* —Specifies the MAC address for traffic that is to be intercepted. Packets with a source or destination MAC address that matches this address are forwarded. Typically, this is the MAC address of the user's CPE device (such as a PC or VoIP phone), not the MAC address of the user's cable modem. • *ip-address*— Specifies the IP address for the data collection server that is to receive copies of the forwarded traffic. • *udp-port*—Specifies the destination UDP port number at the data collection server. The valid range is 0 to 65535 with no default. This port must be unused except by the data collection server at this IP address.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring the Cable Monitor Feature

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

Note When using ACLs with cable monitor and the Cisco uBR10012 router, combine multiple ACLs into one ACL, and then configure cable monitor with the consolidated ACL.

DETAILED STEPS

	Command or Action	Purpose

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

	Command or Action	Purpose

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

Step 3	**interface cable** *x/y*
	
	Example:
	`Router(config)# interface cable 4/0`
	
	Example:
	`Router(config-if)#`
		Enters cable interface configuration mode for the specified cable interface.

Step 4	**cable monitor incoming** | **outbound**] [**timestamp**] **interface** *interface* **access-list** *name* | *number*} | **mac-address** *address* | **sid** *sid-number* [**packet-type** {**data docsis** | **data ethernet** | **mac** [**type** *type*]}]
	
	Example:
	`Router(config-if)# cable monitor interface e1/2 mac-address 0123.4567.89ab packet-type data docsis`
	
	Example:
	`Router(config-if)#`
		Enables cable monitoring on the cable interface with the following parameters:
		• **incoming—**(Optional) Forwards only packets being received on the upstream.
		• **outbound—**(Optional) Forwards only packets being transmitted on the downstream.
		• **timestamp—**(Optional) Appends a four-byte timestamp, in hundredths of a second, to the packets when they are forwarded to the LAN analyzer.
		• **interface** *interface* **—**Specifies the WAN interface on the router to which the LAN analyzer is connected. This interface should be used only by the LAN analyzer. Interface types are Ethernet, Fast Ethernet, Gigabit Ethernet, or Ten Gigabit Ethernet interface.
		
		Identify the packets to be monitored with one of the following:
		• **access-list—**Selects packets that match the specified access list. You can specify the access list by name or by number (1 to 2699).
		• **mac-address—**Specifies the MAC address for packets that should be forwarded.
		• **sid—**Selects packets with the specified service ID (SID). The valid range is 1 to 16384.
		
		You can configure the types of packets to be forwarded with the following options:
		• **packet-type—**(Optional) Selects the type of packet to be forwarded:
		◦ **data docsis—**Forward only data packets as full complete DOCSIS frames.

	Command or Action	Purpose
		◦ **data ethernet—**Forward only data packets by stripping off the DOCSIS header and forwarding only the Ethernet frame. ◦ **mac—**Forwards only the MAC-layer packets. When monitoring a specific SID, you can also optionally specify the **type** option with one of the following MAC-layer message types: **dsa**, **dsc**, **dsd**, **map-grant**, **map-req**. **Note** Repeat Step 4 for each type of packet or MAC address to be monitored.

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

Monitoring the Cable Intercept and Monitor Features

To display information about the operation of the cable intercept and **cable monitor** commands, use the following procedures:

Displaying Information About Intercepted Traffic

To display information about what traffic is being forwarded by the **cable intercept** command, use the **show interface cable intercept** command:

```
Router#  show interface c6/0 intercept

                Destination    Destination
MAC Address     IP Address     UDP Port
00C0.0102.0DEF  10.10.10.131   7512
```

Effective with Cisco IOS Release 12.2(33)SCC, to display information about what traffic is being forwarded by the **cable intercept** command, use the **show interface bundle intercept** command:

```
Router#  show interfaces bundle 1 intercept
                MAC-based intercepts:
Source            Server           Server
MAC Address       IP Address       UDP Port
000c.0102.0304    10.10.10.45      8132
```

Displaying Information About Monitored Traffic

Note Effective with Cisco IOS Release 12.2(33)SCA the **show interface cable monitor** command is replaced by the **show interface cable cable-monitor** command.

To display information about what traffic is being sent to the external LAN analyzer by the **cable monitor** command, use the **show interface cable monitor** command:

```
Router# show interface cable 1/0 monitor
US/ Time Outbound  Flow     Flow Type      Flow  Packet MAC   MAC       Encap
DS  Stmp Interface Type     Identifier     Extn. Type   Extn. Type      Type
all  yes   Et1/0   mac-addr 0050.5462.008c yes   data   no     -        Ethernet
us   yes   Et1/0   acc-list 300            no     -     no     -          -
us   no    Et1/0   sid      2              yes   mac    yes   map-grant   -
all  no    Et1/0   acc-list rrr            no      -    no     -          -
all  no    Et1/0   mac-addr 0042.b013.008c yes   data   no     -        Ethernet
all  no    Et1/0   upstream 0              yes   data   no     -        docsis
The following is sample output from the show interface cable cable-monitor command:
```

Starting with Cisco IOS Release 12.2(33)SCA and later, use the **show interface cable cable-monitor** command to display information about what traffic is being sent to the external LAN analyzer:

```
Router# show interface cable 5/0 cable-monitor
US/ Time Outbound  Flow     Flow Type      Flow  Packet MAC   MAC       Encap
DS  Stmp Interface Type     Identifier     Extn. Type   Extn. Type      Type
us   no    Et1/2   us-port  0              yes   data   no     -        docsis
all  no    Et1/2   acc-list 103            yes   data   no     -        docsis
all  yes   Et1/2   mac-addr 0050.0000.0000 yes   mac    no     -          -
```

Configuration Examples

The following examples illustrate sample configurations of the **cableintercept** and **cablemonitor** commands and features on the Cisco CMTS:

Example: Cable Intercept Configuration

The following sample configuration shows traffic to and from MAC address 0003.e3fa.5e11 being forwarded to a data collection server at the IP address 172.18.73.189 and UDP port 9999:

```
!
interface cable 1/0
 cable monitor timestamp int fe0/0 mac-address 0002.b9ff.8c00 packet-type data ethernet
...
```

Effective from Cisco IOS Release 12.2(33)SCC, the following is the sample configuration showing traffic to and from MAC address 0003.e3fa.5e11 being forwarded to a data collection server at the IP address 172.18.73.189 and UDP port 9999:

```
!
interface bundle 1
```

```
 cable intercept 0003.e3fa.5e11 172.18.73.189 9999
...
```

Cable Monitor Examples

This section contains the following examples that illustrate the Cable Monitor feature on the Cisco CMTS:

Cable Monitor Configuration Example (MAC Address)

The following example of the **cable monitor** command on a Cisco uBR7114 router monitors packets with the MAC address of 0002.b9ff.8c00. Both upstream and downstream packets are forwarded to a LAN analyzer on the router's Fast Ethernet interface (FE0/0).

```
!
interface cable 1/0
 cable monitor timestamp int fe0/0 mac-address 0002.b9ff.8c00 packet-type data ethernet
...
```

Configuration Example for Ethernet, MAC-Layer, and DOCSIS-Data Packets

The following example of the **cable monitor** command monitors Ethernet, MAC-layer, and DOCSIS-data packets with the MAC address of 0003.e3fa.5e8f, adding a timestamp to the packets before forwarding them to the LAN analyzer.

```
!
interface Cable 3/0
 ip address 10.100.100.1 255.255.255.0
 cable monitor timestamp int e2/0 mac-address 0003.e3fa.5e8f packet-type data ethernet
 cable monitor timestamp int e2/0 mac-address 0003.e3fa.5e8f packet-type mac
 cable monitor timestamp int e2/0 mac-address 0003.e3fa.5e8f packet-type data docsis
...
```

Cable Monitor DOCSIS Data Packets Example

This example shows sample DOCSIS packets that have been captured by the **cable monitor** command and forwarded to a LAN analyzer. The hexadecimal dump for the first packet is the following:

```
LLC: ----- LLC Header -----
      LLC:
      LLC: DSAP Address = E2, DSAP IG Bit = 01 (Group Address)
      LLC: SSAP Address = FA, SSAP CR Bit = 00 (Command)
      LLC: I frame, N(R) = 71, N(S) = 47, POLL
      LLC:
DLC: Frame padding= 43 bytes
ADDR  HEX                                                ASCII
0000:c0 00 00 1c ea 1d 00 03 fe e1 a0 54 00 03 e3 fa | ...........T....
0010:5e 8f 00 0a 00 00 03 01 04
 00 00 03 00 00 00 8a | ^.............
0020:4d 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | Mn..............
0030:00 00 00 00 00 00 00 00 00 00 00 00             | ............
```

The relevant DOCSIS bytes are the following:

- Byte 0x16—Control Field. A value of 03 indicates an unnumbered information frame.

- Byte 0x17—Version of the MAC management protocol. A value of 1 indicates a DOCSIS 1.0 message and a value of 2 indicates DOCSIS 1.1 message.
- Byte 0x18—MAC message type. In this example, a value of 04 indicates a Ranging Request (RNG-REQ) message.

The hexadecimal dump of the next packet is the following:

```
LLC: ----- LLC Header -----
      LLC:
      LLC: DSAP Address = FE, DSAP IG Bit = 00 (Individual Address
)
      LLC: SSAP Address = E0, SSAP CR Bit = 01 (Response
)
      LLC: I frame, N(R) = 42, N(S) = 80
      LLC:
DLC: Frame padding= 43 bytes
ADDR  HEX                                                 ASCII
0000:c2 00 00 2b 00 00 00 03 e3 fa 5e 8f 00 03 fe e1 | ...+......^.....
0010:a0 54 00 19 00 00 03 01 05

00 00 03 01 01 04 00 | .T.............
0020:00 00 00 02 01 00 03 02 00 00 05 01 03 00 8a 4d | ..............M
0030:6e 00 00 00 00 00 00 00 00 00 00 00             | n...........
```

This packet has a MAC message type of 05, indicating a Ranging Response (RNG-RSP) message.

Note For complete information on the DOCSIS MAC packet format, see Chapter 6 in the DOCSIS 1.1 specification (see the Additional References, on page 38).

Cable Monitor Timestamped Packets Example

The following example shows how to interpret the four-byte timestamp that is appended to packets that are forwarded by the **cable monitor** command when using the **timestamp** option. The following hexadecimal dump shows the 64-byte contents of the first MAP message packet being examined:

```
  0000(0000): C3
02003A 00000000  01E02F00 0001
0008...:....../.....
  0010(0016): 0D6F4670 00260000  03010300 01380400 .oFp.&.......8..
  0020(0032): 0061A1C1 0061A07C  00030004 FFFC4000 .a...a.|......@.
  0030(0048): 0189401F FFFC4042  0001C043 007EF4EA
 ..@...@B...C.~..
```

The relevant portions of this packet are the following:

- Byte 0—C3 indicates a MAP management message.
- Bytes 08 to 0D—Multicast address that is used to address cable modem when transmitting allocation MAP protocol data units (PDUs).
- Bytes 3C to 3F—Timestamp from the **cable monitor** command in hexadecimal (0x007EF4EA). This value is a 32-bit counter that is incremented every 10 milliseconds.

The following hexadecimal dump shows the second MAP message being forwarded:

```
  0000(0000): C302003A 00000000  01E02F00 00010008 ...:....../.....
  0010(0016): 0D6F4670 00260000  03010300 01380400 .oFp.&.......8..
```

```
  0020(0032): 0061A5AE 0061A469  00030004 FFFC4000 .a...a.i......@.
  0030(0048): 0189401A FFFC403D  0001C03E 007EF4EF
 ..@...@=...>.~..
```

In this example, the timestamp is 0x007EF4EF. Subtracting the two timestamps (0x007EF4EF–0x007EF4EA) produces the time difference between the two MAP messages in hundredths of a second (which in this case is a difference of 5, for a total time difference of 50 milliseconds).

Additional References

The following sections provide references related to the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
CMTS commands	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Common Open Policy Service (COPS)	*COPS Engine Operation on the Cisco CMTS Routers* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_cops_eng_op_ps2209_TSD_Products_Configuration_Guide_Chapter.html
PacketCable configuration	*PacketCable and PacketCable Multimedia for the Cisco CMTS Routers* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm_ps2209_TSD_Products_Configuration_Guide_Chapter.html
Using the LAN analyzer	See the documentation for the LAN analyzer or other network interception software you are using for instructions on decoding DOCSIS MAC frames. **Note** One possible software utility you can use for this purpose is the Ethereal software, which is available for Windows and Unix systems.
CALEA Information	See the Communications Assistance for Law Enforcement Act (CALEA), which was passed by the United States Congress in 1994 and is now sections 1001 to 1010 of the United States Code Title 47 (Telegraphs, Telephones, and Radiotelegraphs). Also see the information on Cisco's web site at the following URL: http://www.cisco.com/wwl/regaffairs/lawful_intercept/index.html
Lawful Intercept technology information	http://www.cisco.com/en/US/tech/tk583/tk799/tsd_technology_support_protocol_home.html http://www.cisco.com/en/US/tech/tk583/tk799/tsd_technology_support_protocol_home.html

Standards

Standards[6]	Title
SP-RFIv1.1-I09-020830	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
PKT-SP-ESP-I01-991229	PacketCable™ Electronic Surveillance Specification

6 Not all standards supported by this release are listed.

MIBs

MIBs[7]	MIBs Link
CISCO-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

7 Not all MIBs supported by this release are listed.

RFCs

Description	Link
No new or modified RFCs are supported by this feature.	http://www.ietf.org/rfc.html

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cable Monitor and Intercept Features for the Cisco CMTS Routers

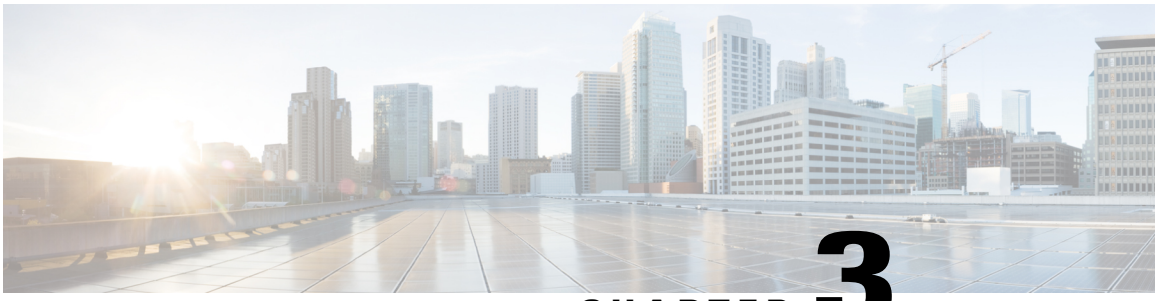
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/.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

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

Table 5: Feature Information for Cable Monitor and Intercept Features for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Cable Intercept Feature	12.0(6)SC, 12.1(2)EC	This feature was introduced for Cisco uBR7200 series routers. The following new command was introduced: • **cable intercept**
Cable Monitor Feature	12.1(3a)EC	The **cable monitor** command was introduced for Cisco uBR7200 series routers.
Cable Monitor and Intercept Features	12.1(5)EC	Support for the **cable intercept** and **cable monitor** commands was added for the Cisco uBR7100 series routers.
Cable Intercept Feature	12.1(11b)EC	The **cable intercept** command was enhanced to allow the data collector to be more than two hops from the Cisco CMTS router.
Cable Monitor and Intercept Features	12.1(4)CX	This feature was integrated into Cisco IOS Release 12.1(4)CX. The **sid** option was added to the **cable monitor** command for DOCSIS 1.1 support.

Feature Name	Releases	Feature Information
Cable Monitor and Intercept Features	12.2(4)BC1	This feature was integrated into Cisco IOS Release 12.2(4)BC1 for the Cisco uBR7100 series, Cisco uBR7200 series, and the Cisco uBR10012 routers. However, this release does not support JIB-based cable interface line cards (such as the Cisco uBR-MC28X/U, Cisco uBR-MC16X/U, and Cisco uBR10-MC520S/U).
Service Independent Intercept	12.3(13a)BC	Support for Service Independent Intercept (SII) was introduced using the CISCO-TAP-MIB for SNMPv3. Feature support for the Cisco uBR-MC28X/U, Cisco uBR-MC16X/U, and Cisco uBR10-MC5X20S/U cable interface line cards was added to Cisco uBR7200 series and Cisco uBR10012 routers.
Cable Monitor and Intercept Features	12.3(17a)BC	• Access Control Lists are supported on the Cisco uBR10-MC5X20U/D and Cisco uBR-MC28U cable interface line cards. • Unconditional downstream sniffing enables downstream packets to be monitored, either for MAC or data packets. This enhancement supports both DOCSIS and Ethernet packet encapsulation.
Cable Monitor and Intercept Features	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR Universal Broadband Router was added.



CHAPTER 3

Cable Duplicate MAC Address Reject for the Cisco CMTS Router

First Published: February 14, 2008

Last Updated: November 29, 2010

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

The Cable Duplicate MAC Address Reject feature is a DOCSIS 1.1-compliant security enhancement that helps to eliminate denial-of-service (DOS) attacks that are caused by cloned cable modems. A clone is presumed to be one of two physical cable modems on the same Cisco CMTS router with the same HFC interface MAC address. The cloned cable modem may be DOCSIS 1.0 or later, and may be semi-compliant or non-compliant with portions of the DOCSIS specifications.

Finding Feature Information

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

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

Contents

Prerequisites for Cable Duplicate MAC Address Reject

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

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

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

Table 6: Hardware Compatibility Matrix for Cable Duplicate MAC Address Reject, on page 45 shows the hardware compatibility prerequisites for this feature.

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

Table 6: Hardware Compatibility Matrix for Cable Duplicate MAC Address Reject

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR10-MC5X20 Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [8]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [9]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

8 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.
9 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for Cable Duplicate MAC Address Reject

- If the cable modem is not provisioned to use DOCSIS BPI+, as characterized by not coming online with the above initialization states of online(p_), then the existing behavior of the Cisco CMTS router remains

unchanged. The Cisco CMTS router does not attempt to distinguish between two cable modems if the provisioning system does not provide a DOCSIS configuration file specifying BPI+ be enabled.

- When this feature is enabled, the Cisco CMTS router issues security breach notice in a log message in the cable logging layer2events log, or the generic log if the **cable logging layer2events** command is not configured on the Cisco CMTS router.

Information About Cable Duplicate MAC Address Reject

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

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

Early Authentication and Encryption

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

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

- Authentication of the cable modem (that is the BPI+ authorization exchanges) after the ranging process.
- Traffic encryption key (TEK) exchanges for the cable modem primary Security Association Identifier (SAID).
- Encryption of IP provisioning traffic and Multipart Registration Request (REG-REQ-MP) messages during cable modem initialization.

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

EAE Enforcement Policies

The Cisco CMTS router supports the following EAE enforcement policies:

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

- Ranging-based EAE enforcement (Policy 2)—EAE is enforced on all DOCSIS 3.0 cable modems that range with a B-INIT-RNG-REQ MAC message.
- Capability-based EAE enforcement (Policy 3)—EAE is enforced on all DOCSIS 3.0 cable modems that range with a B-INIT-RNG-REQ MAC message in which the EAE capability flag is set using the .
- Total EAE enforcement (Policy 4)—EAE is enforced on all cable modems irrespective of the EAE capability flag status.

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

EAE Exclusion

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

BPI+ Security and Cloned Cable Modems

The BPI+ Security and Cloned Cable Modems feature prioritizes cable modems that are online with BPI+ security over new cable modem registration requests that use the same cable modem MAC address. As a result, the legitimate cable modem with BPI+ security certificates that match the HFC MAC address does not experience service disruption, even if a non-compliant cable modem with the same HFC MAC address attempt to register.

The cloned cable modem detection function requires that a cable modem use DOCSIS 1.1 or a later version and should be provisioned with BPI+ enabled. That is, one BPI+ type, length, value (TLV) must be included in the DOCSIS configuration file. All DOCSIS 1.0, DOCSIS 1.1, and later cable modems that are provisioned without DOCSIS BPI+ enabled continue to use the legacy DOCSIS behavior, and experience a DoS attack when a cloned cable modem appears on the Cisco CMTS router.

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

Logging of Cloned Cable Modems

Cloned cable modems are detected and tracked with system logging. The Logging of Cloned Cable Modem feature is enabled by default. Due to the large number of DOCSIS Layer 2 messages typically seen in a production network, a separate log is available to segregate these messages. By default, cloned cable modem messages are placed in the cable logger, cable layer2events logging. If you disable this feature using the no form of the **cable logging layer2events** command in global configuration mode, then the cloned cable modem messages are placed in the system log (syslog).

A cloned cable modem might attempt dozens of registration attempts in a short period of time. In order to suppress the number of log messages generated, the Cisco CMTS router suppresses clone detected messages for approximately 3 minutes under certain conditions.

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

DOCSIS 3.0 BPI+ Policy Enforcement

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

- 1.1 Style Configuration File Parameters and Capability (Policy 1)—The Cisco CMTS router enforces BPI+ on cable modems that register with a DOCSIS 1.1 configuration file with parameters indicating BPI+ is enabled with or without TLV 29. To configure this policy, the privacy support modem capability TLV (type 5.6) in the DOCSIS configuration file must be set to BPI+ support. This policy forces BPI+ on a cable modem that is BPI+ capable and provisioned with DOCSIS1.1 configuration file. A cable modem that signals these capabilities during registration is blocked from accessing the network until the modem completes BPI+ negotiation.
- 1.1 Style Configuration File Parameters (Policy 2)—The Cisco CMTS router enforces BPI+ on cable modems that register with a DOCSIS 1.1 configuration file with parameters indicating BPI+ is enabled with or without TLV 29. A cable modem that registers with this type of configuration file is blocked from accessing the network until the modem completes BPI+ negotiation.
- 1.1 Style Configuration File (Policy 3)—The Cisco CMTS router enforces BPI+ on cable modems that register with a DOCSIS 1.1 configuration file. This means that if you provision a DOCSIS 1.1 configuration file with security disabled (privacy flag is not present in the configuration file), all DOCSIS 1.1 and 2.0 cable modems are blocked from accessing the network. Only the DOCSIS 3.0 cable modems that have security enabled implicitly will pass this check if the privacy flag is not present in the configuration file.
- Total enforcement (Policy 4)—The Cisco CMTS router enforces BPI+ on all cable modems. This means that all cable modems that do not run BPI+ are blocked from accessing the network.

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

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

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

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

BPI+ Policy Enforcement Exclusion

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

How to Configure EAE and BPI+ Enforcement Features

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

Configuring EAE Enforcement Policies

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

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

DETAILED STEPS

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

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

Enforcing DOCSIS BPI+ Compliance on the Cisco CMTS Router

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

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

DETAILED STEPS

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

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

Step 3	**cable privacy bpi-plus-enforce** **Example:** `Router(config)# cable privacy bpi-plus-enforce`	Forces DOCSIS 1.1 or later cable modems to register with DOCSIS BPI+ security certificates, and not use the earlier DOCSIS BPI security.

	Command or Action	Purpose

Step 4	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Returns to privileged EXEC mode.

Step 5	**show cable logging** **Example:** `Router# show cable logging`	Displays whether the Layer 2 Logging feature is enabled, and displays the status of the logging buffer.

Examples enforcing DOCSIS BPI

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

```
SLOT 7/0: Nov 14 12:07:26: %UBR10000-6-CMMOVED: Cable modem 0007.0e03.3e71 has been moved
from interface Cable7/0/1 to interface Cable7/0/0.
Nov 14 12:07:57: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
 access detected at Cable7/0/0 interface
```

For additional information about this feature and supporting system log messages, see the System Messages Supporting Cable Duplicate MAC Address Reject, on page 54.

Configuring BPI+ Enforcement Policies

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

Before You Begin

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

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

DETAILED STEPS

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

Troubleshooting Tips

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

- **debug cable mac-address—**Provides debugging information about a specific cable modem.
- **debug cable bpiatp—**Enables debugging of the BPI handler.

Configuration Example for EAE and BPI+ Enforcement Policies

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

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

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

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

Verifying EAE and BPI+ Enforcement Policies

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

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

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

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

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

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

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

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

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

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

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

What to Do Next

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

System Messages Supporting Cable Duplicate MAC Address Reject

The following example illustrates logged events for the Cloned Cable Modem Detection feature on a Cisco uBR10012 router with PRE2 modules.

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

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

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

```
connection attempt rejected on Cable7/0/0 U1
Dec 5 13:12:37: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
connection attempt rejected on Cable7/0/0 U0
Dec 5 13:18:28: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
connection attempt rejected on Cable7/0/0 U0
Dec  5 13:18:28: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address 0013.7116.e726
 connection attempt rejected o n Cable7/0/0 U0
```

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

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

Additional References

Related Documents

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

Standards

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

RFCs

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

MIBs

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

Technical Assistance

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

Feature Information for Cable Duplicate MAC Address Reject

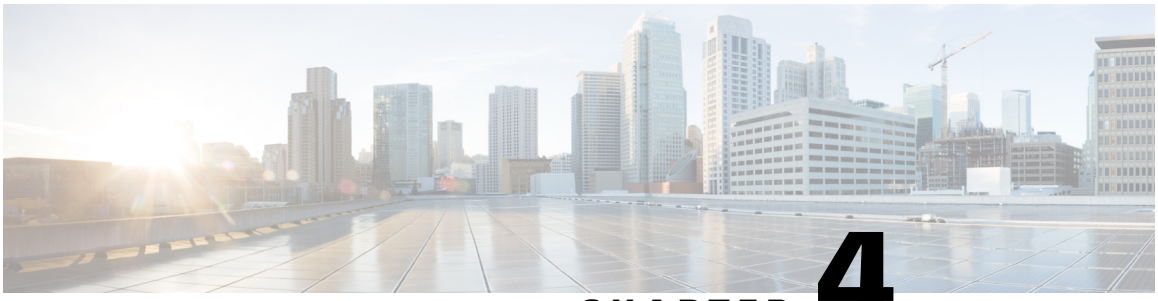
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/.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

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

Table 7: Feature Information for Cable Duplicate MAC Address Reject

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

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



CHAPTER 4

DOCSIS 3.0 CRL and OCSP on the Cisco CMTS Routers

First Published: November 13, 2009

Last Updated: November 29, 2010

Cisco IOS Release 12.2(33)SCC provides support for certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP) in Data-over-Cable Service Interface Specifications (DOCSIS) 3.0 environment on the Cisco CMTS routers enabling you to validate the certificates issued by the certificate authority (CA) for secure transactions.

Finding Feature Information

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

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

Contents

Prerequisites for DOCSIS 3.0 CRL and OCSP

- The cable modems must be DOCSIS 1.1 and above.
- Baseline Privacy Interface Plus (BPI+) must be enabled.
- The system clock on the Cisco uBR10012 universal broadband router should be set to a current date and time to ensure that system logs have the proper timestamp and to ensure that the BPI+ subsystem uses the correct timestamp for verifying cable modem digital certificates.

This table shows the hardware compatibility prerequisites for this feature.

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

Table 8: DOCSIS 3.0 CRL and OCSP Feature Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [10]

10 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

Restrictions for DOCSIS 3.0 CRL and OCSP

The DOCSIS 3.0 CRL and OCSP have the following restrictions and limitations:

- The OCSP responder does not verify the validity of the certificate. It only verifies the revocation status of the certificate.
- When the OCSP status of a certificate is unknown to the CMTS, the certificate is treated as “valid”.
- When the CMTS fails to receive the OCSP or CRL response, the certificate is considered as “valid”.
- You cannot specify more than a single server for each protocol.

Information About DOCSIS 3.0 CRL and OCSP

The following sections describe the DOCSIS 3.0 CRL and OCSP support:

Feature Overview

CRL and OCSP are two methods used to check the revocation status of certificates that the certification authority (CA) issues.

CRL is a single signed file that lists the revocation status of certificates. The status includes the date of certificate revocation, time of CRL file creation, and time of release of the next CRL file.

OCSP is the alternative to the CRL. OCSP checks the certificate status at the external OCSP responder for each individual CA and CM certificate. The OCSP responder signs each response and the CMTS validates it.

Certificate Revocation List

Certificate revocation lists are used to check the revocation status of certificates when using a public key infrastructure (PKI) for maintaining access to servers in a network. When there is an attempt to access the server, the access action (allow or deny) is taken based on the specified CRL entry.

The CMTS retrieves the CRL files using HTTP. The retrieved files are checked with a trusted CA to ascertain the validity of the CRL file. If the CMTS cannot verify the validity of the CRL file, it discards the CRL file.

The CMTS employs the following validation process to check the validity of a CA certificate or CM certificate:

- The CMTS uses the current CRL file and attempts to retrieve the subsequent CRL file as indicated in the next-update value in the current CRL file. If the attempt fails, the CMTS continues to use the existing file and attempts to retrieve the new file at periodic intervals.
- If the next-update value is missing from the current CRL file, the CMTS uses the value configured for the CRL file.

Note The next-update value is contained in the CRL file itself.

For more details on CRL feature, refer to the What Is a CRL? section in Configuring Authorization and Revocation of Certificates in a PKI guide.

Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) is an alternative to Certificate Revocation Lists. It provides timely information regarding the revocation status of a digital certificate. Unlike CRL, OCSP downloads the revocation status for each CA and CM certificate individually. Because of this, any changes to the revocation states are noted quickly, but at the expense of the additional overhead of contacting the server for each certificate.

When the CMTS receives a CA certificate or CM certificate, it sends a status request to an OCSP responder using the OCSP protocol to check the revocation state of the certificate. The OCSP responder sends the

response as “good”, “revoked”, or “unknown” after checking the revocation status of the certificate in its database. The CMTS uses the response from OCSP responder for the certificate validation process.

The CMTS uses the following validation process to check the validity of a CA certificate or cable modem (CM) certificate:

- The CMTS checks the OCSP response for the next-update value. If the next-update value is available, the CMTS acts as an OCSP client and caches the response status of the certificate. Next, the CMTS attempts to retrieve the revocation status of the certificate only after the time indicated in the next-update value.
- If next-update value is not available in the OCSP response, the CMTS does not cache the OCSP revocation status of the certificate and checks for the certificate validity every time a certificate validation is requested. This is a very resource-intensive method as the certificate validity is checked on a regular basis.

The CMTS sends an OCSP request when a CA certificate or CM certificate is obtained. The request is sent only when the CMTS is configured with OCSP responder information and does not posses a valid certificate status in its cache.

The CMTS treats the certificate as “valid” when:

- The CMTS is unable to retrieve the certificate status.
- The status of the certificate is “unknown”.
- The CMTS fails to receive any response from the OCSP responder.

For more details on OCSP feature, refer to the Online Certificate Status Protocol (OCSP) guide.

How to Configure DOCSIS 3.0 CRL and OCSP

This section describes the following tasks that are required to implement DOCSIS 3.0 CRL and OCSP support:

Configuring Trustpoints

This section describes how to configure trustpoints for CRL and OCSP.

Configuring a Trustpoint

This section describes how to configure trustpoints. Use the cable privacy revocation enable command at the global configuration mode to create the trustpoints and add the certificates for revocation checking.

The cable privacy revocation enable command creates the necessary trustpoints for proper DOCSIS operation. Specify the correct CRL Distribution Point and OCSP responder to configure these trustpoints.

Note IOS is based on trustpoints and the certificates configured in the system refer to this trustpoint.

For information on creating trustpoints, see the Configuring Certificates chapter of the Cisco Security Appliance Command Line Configuration Guide .

Note To set the timeout value of CRL or OCSP response time for authorization messages, use the cable privacy revocation timeout command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation enable** **Example:** `Router(config)# cable privacy revocation enable`	Creates the trustpoints and adds the certificates for revocation checking.
Step 4	**cable privacy revocation timeout** **Example:** `Router(config)# cable privacy revocation timeout`	(Optional) Allows the CMTS to set the timeout value of OCSP response time.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to the privileged EXEC mode.

Configuring DOCSIS Trustpoints

The trustpoints for the US (DOCSIS-US-TRUSTPOINT) and EU (DOCSIS-EU-TRUSTPOINT) root certificates are created dynamically and are used to verify all the manufacturer and CM certificates.

For information on creating trustpoints, see the Configuring Trustpoints section of Configuring Certificates chapter of the Cisco Security Appliance Command Line Configuration Guide.

Tip Use the CRL URL and the OCSP URL to add additional trustpoints. CableLabs and ComLabs also provide a public URL that contains DOCSIS root certificates signed for OCSP responses.

Configuring OCSP

Note The server specified using the ocsp url command is used only when the URL is not specified in the certificate.

To allow the CMTS to skip the OCSP response signature check, use the **cable privacy revocation ocsp skip-sig-check** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable privacy revocation ocsp skip-sig-check**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation ocsp skip-sig-check** **Example:** `Router(config)# cable privacy revocation ocsp skip-sig-check`	Allows the CMTS to skip the OCSP response signature check.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring CRL

This section describes how to configure CRL. For information on Configuring CRL, see the Configuring CRLs for a Trustpoint section of Configuring Certificates document.

Note The server specified using the crl query command is used only when the URL is not specified in the certificate.

To allow the CMTS to skip the CRL response signature check, use the cable privacy revocation crl skip-sig-check command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation crl skip-sig-check** **Example:** `Router(config)# cable privacy revocation ocsp skip-sig-check`	Allows the CMTS to skip the CRL response signature check.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Disabling OCSP Nonce

For information on disabling OCSP Nonce, see the Disabling OCSP Nonces section of Configuring PKI Using the IPSec VPN SPA document.

Note This feature is enabled by default in IOS.

Obtaining Certificates

For information on obtaining certificates, see the Obtaining Certificates section of Configuring Certificates document.

Note The trustpoint needs a public or private keypair to sign the OCSP requests. This key should be made known to the OCSP responder to verify the request. However, signing the request is optional and the OCSP responders do not normally check the validity of the requests.

The OCSP method of checking the certificate status for each individual CA and CM certificate in real-time consumes more resources with resultant performance problems. To mitigate performance related problems, you can disable checking of the CM certificates using the **cable privacy revocation skip-cm-cert** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable privacy revocation skip-cm-cert** **Example:** `Router(config)# cable privacy revocation skip-cm-cert`	Allows the CMTS to disable checking of CM certificates.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Monitoring the DOCSIS 3.0 CRL and OCSP

To verify certificate and trustpoint information, perform the following steps:

Verifying Certificates

To display the certificates that are currently used on the CMTS, use the **show crypto pki certificates** command.

Verifying Certificate Revocation Lists

To display the certificate revocation lists that are currently used on the CMTS, use the **show crypto pki crls** command.

For information on verifying certificate revocation lists, see the Configuring Certificate Authorization and Revocation Settings section of the Configuring Authorization and Revocation of Certificates in a PKI document.

Configuration Examples for DOCSIS 3.0 CRL and OCSP

This section lists the following sample configurations for the DOCSIS 3.0 CRL and OCSP feature on a Cisco CMTS router:

Creating Trustpoints Examples

The following sample configuration shows typical example of a router configured to use trustpoints and optionally sets the timeout value for authorization messages:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation enable
Router(config)# cable privacy revocation timeout
Router(config)# end
```

OCSP Configuration Examples

The following sample configuration shows typical example of a router configured to skip the OCSP response signature check:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation ocsp skip-sig-check
Router(config)# end
```

CRL Configuration Examples

The following sample configuration shows typical example of a router configured to skip the CRL response signature check:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation crl skip-sig-check
Router(config)# end
```

Obtaining Certificates Configuration Examples

The following sample configuration shows typical example of a router configured to skip the CM certificate check:

```
Router> enable
Router# configure terminal
Router(config)# cable privacy revocation skip-cm-cert
Router(config)# end
```

Additional References

The following sections provide references related to the DOCSIS 3.0 CRL and OCSP feature.

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
Configuring Certificates	Cisco Security Appliance Command Line Configuration Guide
Security commands	Cisco IOS Security Command Reference
What is OCSP?	Configuring Authorization and Revocation of Certificates in a PKI
CMTS MIBs	Cisco CMTS Universal Broadband Router Series MIB Specifications Guide 12.2SC

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• IF-MIB • DOCS-IF3-MIB • DOCS-SEC-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 For information on MIBs, see http://www.cisco.com/en/US/docs/cable/cmts/mib/12_2sc/reference/guide/ubrmibv5.html Cisco CMTS Universal Broadband Router Series MIB Specifications Guide 12.2SC.

RFCs

RFCs[11]	Title
RFC 3280	Internet X.509 Public Key Infrastructure CRL
RFC 2616	HTTP/1.1
RFC 2560	X.509 Internet Public Key Infrastructure OCSP

11 Not all supported RFCs are listed.

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

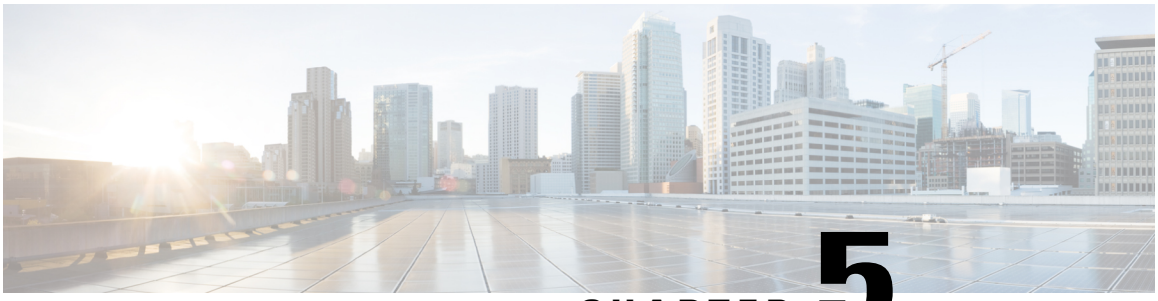
Feature Information for DOCSIS 3.0 CRL and OCSP on the Cisco CMTS Routers

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

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

Table 9: Feature Information for DOCSIS 3.0 CRL and OCSP for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS 3.0 CRL and OCSP on the Cisco CMTS Routers	12.2(33)SCC	This feature was introduced for the Cisco uBR10012 universal broadband router. The following commands are new or modified: • **cable privacy revocation crl skip-sig-check** • **cable privacy revocation enable** • **cable privacy revocation ocsp skip-sig-check** • **cable privacy revocation skip-cm-cert** • **cable privacy revocation timeout**



CHAPTER 5

Dynamic Shared Secret for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: March 31, 2015

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

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 documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Contents

Prerequisites for Dynamic Shared Secret

The configuration of Dynamic Shared Secret feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.2BC and Cisco IOS Release 12.3BC 12.2SC or later releases. Table 10: Configuring Dynamic Shared Secret on the Cisco CMTS Routers Hardware Compatibility Matrix, on page 74 shows the hardware compatibility prerequisites for this feature.

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

Table 10: Configuring Dynamic Shared Secret on the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco cBR-8 Converged Broadband Router	Cisco IOS-XE 3.15.0S	Cisco cBR-8 CCAP line cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • PRE2 Cisco IOS Release 12.2(33)SCC • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [12]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V[13]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

12 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

13 Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

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

- The Cisco CMTS must be running Cisco IOS Release 12.2(15)BC1 or later Cisco IOS Release 12.2 BC or 12.3 BC release.
- The Dynamic Shared Secret feature supports an external provisioning server.
- The Dynamic Shared Secret feature supportsThe Dynamic Shared Secret feature supports the CMTS acting as the TFTP server (using either DOCSIS configuration files stored in Flash memory or using the internal DOCSIS configuration file editor). If you are using the CMTS as the TFTP server, you must also meet the prerequisites given in the Additional References, on page 100.
- A cable modem must be able to register with the Cisco CMTS before enabling the Dynamic Shared Secret feature.
- It is optional, but highly recommended, that you also configure a shared secret on each cable interface, and use that shared secret to create the DOCSIS configuration files for those cable modems. You can also optionally configure up to 16 secondary shared secrets on each cable interface. This is not required to use the Dynamic Shared Secret feature, but it does provide another layer of security, because the CMTS uses the manually configured shared secret to verify the original DOCSIS configuration files that it downloads from the TFTP server.

Note If a manually configured shared secret is configured, it *must* match the shared secret that was used to create the DOCSIS configuration files. If the configuration file cannot be verified against the shared secret (and any secondary shared secrets that might be configured), the CMTS does not allow any cable modems using that configuration file to come online, regardless of the Dynamic Shared Secret configuration.

- It is optional to also configure the **cable tftp-enforce** command on each cable interface to require that cable modems download their DOCSIS configuration files through the CMTS. This identifies, on a per-modem basis, those users who are attempting to bypass the shared secret checks by downloading a DOCSIS configuration file from a local TFTP server.

When the **cable tftp-enforce** command is used with the **cable dynamic-secret** command, the TFTP enforce checks are done before the dynamic shared-secret checks. If a cable modem fails to download a DOCSIS configuration file through the CMTS, it is not allowed to register, regardless of the dynamic shared-secret checks.

- The Dynamic Shared Secret feature is compatible with cable modems that are DOCSIS 1.0-, DOCSIS 1.1-, and DOCSIS 2.0-certified, which are operating in any valid DOCSIS mode.
- 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. (See the Performance Information, on page 83.)

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 master cable interface, you should also configure the feature on all of the corresponding slave 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, commencing in Cisco IOS Release 12.3(17a)BC. 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 84 for additional information about DMIC lock mode.
- The Cisco uBR7100 series router does not support the Dynamic Shared Secret feature when running in MxU bridging 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 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
```

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.
- Upgrade your installation of Cisco IOS to Release 12.3(9a)BC4 or a later release. These releases can exclude Thomson cable modems from the Cable dynamic secret feature by excluding the OUI setting.

Note The above method is not secure.

- 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_118.

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.

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.
  - The cable modems on that interface are downloading a DOCSIS configuration file that is greater than 4 Kbytes in size. This condition applies when using a Cisco IOS release prior to 12.3(15)BC4.

- 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.

Individual cable modems may react better if they are power cycled after DMIC is enabled or disabled as they have trouble changing the TFTP server IP address for the DOCSIS config file. While this behavior has been indicated for older modems, it has not yet been reproduced consistently in the lab at large scale.

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.

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.

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 affect 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. If these shared secrets are configured, the Cisco CMTS continues to use them to validate the original DOCSIS configuration file that is downloaded from the TFTP server. If the DOCSIS configuration file fails to pass the original or secondary shared secret verification checks, the cable modem is not allowed to register, and the Dynamic Shared Secret feature is not invoked for that particular cable modem.

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.

To identify users who are attempting to use a locally downloaded configuration file, use the **cable tftp-enforce** command.

Interaction with Different Commands

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

- **cable config-file—**This command enables the Cisco CMTS internal DOCSIS configuration file editor, which creates DOCSIS configuration files as part of the router's configuration. The Cisco CMTS can transmit these files to cable modems using its onboard TFTP server. The Dynamic Shared Secret feature can be used together with these DOCSIS configuration files.
- **cable qos permission—**The enforce option with this command allows you to require a cable modem to use a specific, CMTS-provided QoS profile. This command can be used with the Dynamic Shared

Secret feature, but if the dynamic shared-secret lock option is used, the QoS profile specified by the **cable qos permission enforce** command takes precedence over that specified using the **lock** option.

- **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.

  The Dynamic Shared Secret feature enhances this security by providing another layer of security. Cable modems must successfully pass all shared-secret checks to come online.

- **cable shared-secondary-secret—** For flexible network management, the Cisco CMTS allows you to configure additional shared secrets on a cable interface. If a cable modem fails the primary shared-secret checks, the CMTS checks the modem against the secondary shared-secrets. This allows cable providers to regularly change their shared secrets without having to update all cable modems at once. The Dynamic Shared Secret feature works together with this feature, so that if primary and secondary shared-secrets are configured, cable modems must pass at least one of those checks, as well as the dynamic shared-secret checks, before being allowed to come online.

- **cable tftp-enforce—**This command requires that cable modems download a DOCSIS configuration file over the cable interface before being allowed to come online. If a cable modem fails the TFTP-enforce checks, it is not allowed to come online. This command, along with the Dynamic Shared Secret feature, prevents the most comment theft-of-service attacks in which users try to substitute their own configuration files or try to modify the service provider's files.

- **tftp-server—**This command enables the TFTP server that is onboard the Cisco CMTS router, allowing it to deliver DOCSIS configuration files to cable modems. The DOCSIS configuration files can already be saved in the router's Flash memory, or you can create them using the router's internal DOCSIS configuration file editor. The Dynamic Shared Secret feature can be used with both types of DOCSIS configuration files and the onboard TFTP server.

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 Release 12.2(15)BC2 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.

System Error Messages

Cisco IOS Release 12.2(15)BC1 and later releases display the following system error messages to 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.

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.

Message

%UBR7100-4-BADCFGFILE

%UBR7200-4-BADCFGFILE

%UBR10000-4-BADCFGFILE: Modem config file [chars] at [integer]: [chars]

The DOCSIS configuration file for the cable modem failed its CMTS MIC verification, either because the MIC is missing or because the CMTS MIC failed verification with the shared secret or secondary shared secrets that have been configured for the cable interface. This message occurs when the dynamic secret feature is enabled on the cable interface with the **cable dynamic-secret** command.

Verify that the DOCSIS configuration file for the cable modem has been created using the correct shared secret value. Also verify that the DHCP server is specifying the proper configuration file for this cable modem, and that the configuration file on the TFTP server is the correct one.

Use the **show cable modem** command to display the MAC state for this particular cable modem. If the cable modem will remain in the "init(t)" state continually when the Dynamic Shared Secret feature is enabled, check for the following possible problems:

- The shared secret and secondary shared secrets that are configured on the cable interface do not match the ones that were used to create the DOCSIS configuration files. Either reconfigure the cable interface with the correct shared secret, or recreate the DOCSIS configuration files using the correct shared secret.

- The provisioning server is specifying the wrong DOCSIS configuration file for this cable modem.
- The DOCSIS configuration file on the TFTP server is either corrupted or incorrectly named.
- A user has successfully substituted their own DOCSIS configuration file into the service provider's network.
- A cable modem has cached the DOCSIS configuration file, or a user is attempting to reuse a previously generated DOCSIS configuration file. This could also indicate a possible theft-of-service attempt by a user attempting to upload a modified DOCSIS configuration file into the operator's TFTP server.

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.

In addition, if a manually configured shared secret is also used, the CMTS uses it to verify the DOCSIS configuration files that it receives from the TFTP server, providing MD-5 authenticated transactions between the TFTP server and the CMTS. This prevents users from bypassing the Dynamic Shared Secret feature by attempting to spoof the IP address of the provider's TFTP server.

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 1.0, DOCSIS 1.1, or DOCSIS 2.0-compatible cable modem.

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.
- TFTP Server and Internal DOCSIS Configurator File Generator—The Cisco CMTS can act as a TFTP server, providing dynamically generated DOCSIS configuration files to cable modems. The Dynamic Shared Secret feature can be used with the DOCSIS configuration files created by the internal editor and delivered by the CMTS TFTP server.
- Shared Secrets—A shared secret can be manually configured on a cable interface using the **cable shared-secret** command. All cable modems on that interface must use DOCSIS configuration files with a CMTS MIC that has been calculated with that shared secret, before being allowed to come online. When used with the Dynamic Shared Secret feature, the CMTS uses the manually specified shared secret to verify the DOCSIS configuration files it downloads from the TFTP server, before it modifies them with the dynamically generated shared secret.

Tip When using both a manually configured shared secret and the Dynamic Shared Secret feature, when a modem's configuration file fails the manual shared secret verification, the modem remains in the "init(t)" state until it times out and reregisters. If a cable modem seems stuck in the "init(t)" state, it could be a failure of the manual shared secret verification.

- Secondary Shared Secrets—To allow service providers to change the shared secret on a cable interface, without also having to immediately change all the DOCSIS configuration files being used on that

interface, a cable interface can be configured with up to 16 additional shared secrets, using the **cable shared-secondary-secret** command. When a service provider changes the primary shared secret on a cable interface, the service provider can configure the previous shared secret as a secondary secret. This allows cable modems to continue using the previous shared secret until the provider can update the configuration file with the new value.

- TFTP Enforce—To require cable modems to download a DOCSIS configuration file over the cable interface, through the CMTS, use the **cable tftp-enforce** command. This prevents a common theft-of-service attack, in which a user attempts to download a modified DOCSIS configuration file from a local TFTP server.

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.

DETAILED STEPS

	Command or Action	Purpose

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

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.

	Command or Action	Purpose

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:
	`Router(config-if)# cable dynamic-secret mark`
	
	Example:
	`Router(config-if)# cable dynamic-secret reject`
		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.
		• *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.

	Command or Action	Purpose
	Example: `Router(config-if)#`	• **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**
	Example:
	`Router(config-if)# end`
	Example:
	`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.

DETAILED STEPS

	Command or Action	Purpose

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

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

	Command or Action	Purpose
	Example: `Router(config-if)#`	

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.

DETAILED STEPS

	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`
	`Router(config)# cable dynamic-secret exclude modem 00d0.45ba.b34b`
		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 to be excluded from the Dynamic Shared Secret feature. (You cannot specify a multicast MAC address.)

	Command or Action	Purpose
		• **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.

DETAILED STEPS

	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`
		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).

	Command or Action	Purpose
	Example: `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 88 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.

DETAILED STEPS

	Command or Action	Purpose

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

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
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/U5 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 Cisco IOS Release 12.2(15)BC1, 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)
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#
```

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                      : 20496E7465726661636520537065636369
Dynamic Secret                      : 00000000000000000000000000000000
Dynamic Secret                      : 040B130C4361626C65204D6F64656D73
Dynamic Secret                      : 53204361626C65204D6F64656D20526F
Dynamic Secret                      : 7574686F72697479301E170D30313032
Dynamic Secret                      : 313233353935395A308197310B300906
Dynamic Secret                      : 0A133044617461204F76657220436162
Dynamic Secret                      : 666163652053706563696669636174 69
Dynamic Secret                      : 626C65204D6F64656D73313630340603
Dynamic Secret                      : 65204D6F64656D20526F6F7420436572
Dynamic Secret                      : 7479308201223 00D06092A864886F70D
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                      : DF8FE30203010001A326302430120603
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.

- **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
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

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
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

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
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

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.

```
interface cable c3/0
 cable dynamic-secret reject
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

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
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

Additional References

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

Related Documents

Related Topic	Document Title
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS command reference	Cisco IOS Release 12.2 Command References http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html
Configuring DOCSIS 1.1 on the Cisco CMTS	"DOCSIS 1.1 for the Cisco CMTS Routers" in the *Cisco IOS CMTS Cable Software Configuration Guide* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_docsis11.html
Cisco Network Registrar End User Guides	Cisco Network Registrar user guides http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/products_user_guide_list.html

Related Topic	Document Title
Cisco Broadband Access Center DPE CLI Reference, 2.7.1	Cisco Broadband Access Center DPE CLI REference, 2.7.1 http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/2.7.1/command/reference/cli.html

Standards

Standards[14]	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1

14 Not all supported standards are listed.

MIBs

MIBs[15]	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

15 Not all supported MIBs are listed.

RFCs

RFCs[16]	Title
RFC 2233	DOCSIS OSSI Objects Support
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

16 Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Dynamic Shared Secret

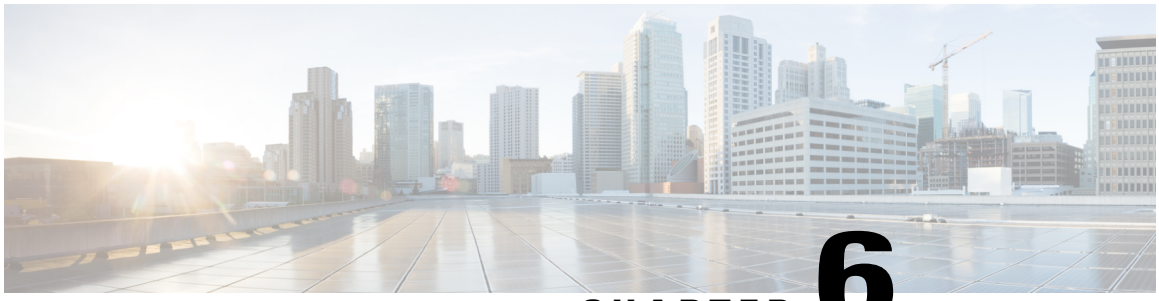
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/.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

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

Table 11: Feature Information for Dynamic Shared Secret

Feature Name	Releases	Feature Information
Dynamic Shared Secret	12.2(15)BC1	This feature was introduced.
Changing Default Behavior of Dynamic Shared Secret	12.2(15)BC1b	Support for the **nocrypt** option was added to the **cable dynamic-secret** command.
SNMP support for the Dynamic Shared Secret	12.2(15)BC2	SNMP support for the Dynamic Shared Secret feature was added to CISCO-DOCS-EXT-MIB, and a new option (**dmic-lock**) was added to the **snmp-server enable traps cable** command.
Excluding Cable Modems from Dynamic Shared Secret	12.3(9a)BC	The **cable dynamic-secret exclude** command was added to allow specific cable modems to be excluded from the Dynamic Shared Secret feature.

Feature Name	Releases	Feature Information
DMIC lock mode	12.3(17a)BC	The DMIC lock mode behavior is revised to support additional security during N+1 Redundancy switchover events. Refer to Restrictions for Dynamic Shared Secret, on page 76 for additional information.
Dynamic Insertion of TFTP Server TLV for CM Firmware Upgrade	12.2(33)SCD2	The cable dynamic-secret tftp insert-upgrade-server command was added to support dynamic insertion of the TFTP server address in the DOCSIS configuration file.



CHAPTER 6

Cable DHCP Leasequery

First Published: February 14, 2008

Last Updated: November 29, 2010

This document describes the Dynamic Host Configuration Protocol (DHCP) Leasequery feature on the Cisco cable modem termination system (CMTS) router.

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

Finding Feature Information

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

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

Contents

• Feature Information for Cable DHCP Leasequery , page 115

Prerequisites for Cable DHCP Leasequery

- The Cisco CMTS router must be running Cisco IOS Release 12.2(15)BC1d or Cisco IOS Release12.2(15)BC2b or Cisco IOS Release 12.2(33)SCA or a later release.
- You must configure a cable interface with the **cable source-verify dhcp** command and the **no cable arp** command before the Cisco CMTS router can enable DHCP Leasequery. Lease queries are sent to the DHCP server or to a configured alternate server.

To divert DHCP Leasequeries to a specific server, you must use the cable **source-verify dhcp server** ipaddress command and the **no cable arp** command before the Cisco CMTS router is enabled for DHCP Leasequery. Only one alternate server may be configured.

- You must configure the **cable ipv6 pd-route** command when IPv6 Customer Premise Equipment (CPE) routers are deployed on the Cisco CMTS router.

Restrictions for Cable DHCP Leasequery

- Leasequeries are sent to the DHCP server unless an alternate server is configured.
- Only one alternate server can be configured.
- Users are responsible for the synchronization of the DHCP server and the configured alternate server.
- If the configured alternate server fails, leasequery requests are *not* returned to the DHCP server.
- Only one IA_IADDR is supported per client. If the leasequery returns multiple results, only the IA_ADDR matching the query is added to the Cisco CMTS subscriber database.
- The Cisco CMTS will not verify the source of the IPv6 link-local address of a CPE.

Information About Cable DHCP Leasequery

Problems can occur, though, when viruses, denial of service (DoS) attacks, and theft-of-service attacks begin scanning a range of IP addresses, in an attempt to find unused addresses. When the Cisco CMTS router is verifying unknown IP addresses, this type of scanning generates a large volume of DHCP leasequeries, which can result in the following problems:

- High CPU utilization on the Cisco CMTS router PRE card.
- High utilization on the DHCP servers, resulting in a slow response time or no response at all.
- Packets can be dropped by the Cisco CMTS router or DHCP server (or configured alternate server).
- Lack of available bandwidth for other customers on the cable interface.

To prevent such a large volume of leasequery requests on cable interfaces, you can enable filtering of these requests on upstream interfaces, downstream interfaces, or both. When the Cable DHCP Leasequery feature is enabled, the Cisco CMTS allows only a certain number of DHCP leasequery requests for each service ID

(SID) on an interface within the configured interval time period. If an SID generates more Leasequeries than the maximum, the router drops the excess number of requests until the next interval period begins.

You can configure both the number of allowable DHCP leasequery requests and the interval time period, so as to match the capabilities of your DHCP server (or configured alternate server) and cable network.

To configure the Cisco CMTS router to send DHCP leasequery requests to the DHCP server, use the **cable source-verify dhcp** and **no cable arp** commands. Unknown IP addresses that are found in packets for customer premises equipment (CPE) devices that use the cable modems on the cable interface are verified. The DHCP server returns a DHCP ACK message with the DHCP relay information and lease information of the CPE device that has been assigned this IP address, if any.

When **cable source-verify dhcp** and **no cable arp** commands are configured, DHCP leasequery is sent for downstream packets to verify unknown IP addresses within the IP address range configured on the cable bundle interface.

For DHCP leasequery to work in the downstream direction, the Cisco Network Registrar (CNR) should be made aware of the DHCP Option 82. This is required to make the CMTS map the CPE IP address to the correct CM. To do this, configure the **ip dhcp relay information option** command on the bundle interface to insert service class relay agent option into the DHCP DISCOVER messages. When the configuration is in place, during DHCP DISCOVER the values of DHCP Option 82 is cached by the CNR and is returned to the CMTS on any subsequent DHCP leasequery for that IP address.

To configure the Cisco CMTS router to divert DHCP leasequery requests to a server other than the DHCP server, use the **cable source-verify dhcp server ipaddress** and **no cable arp** commands.

The Cisco CMTS supports two types of DHCP leasequery implementation, Cisco standard compliant DHCP leasequery and RFC 4388 standard compliant DHCP leasequery. These two standards differ mostly in the identifiers used to query or respond to the DHCP Server. You can choose between these two implementations depending on which standard is supported on your DHCP Server.

Use the **ip dhcp compatibility lease-query client** {**cisco** | **standard**} command to configure the Cisco CMTS in either Cisco mode or RFC 4388 standard mode.

For more information about this command, see the "DHCP Commands" chapters in the *Cisco IOS IP Addressing Services Command Reference* , Release 12.2 at the following URL: http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html.

DHCP MAC Address Exclusion List

The Cisco IOS Release 12.3(13)BC introduces the ability to exclude trusted MAC addresses from the standard DHCP source verification checks, as supported in earlier Cisco IOS releases for the Cisco CMTS. This feature enables packets from trusted MAC addresses to pass when otherwise packets would be rejected with standard DHCP source verification. This feature overrides the cable source-verify command on the Cisco CMTS for the specified MAC address, yet maintains overall support for standard and enabled DHCP source verification processes. This feature is supported on the Performance Routing Engine 1 (PRE1), PRE2, and PRE4 modules on the Cisco uBR10012 router chassis.

To enable packets from trusted source MAC addresses in DHCP to pass without source verification checks, use the cable trust command in global configuration mode. To remove a trusted MAC address from the MAC exclusion list, use the no form of this command. Removing a MAC address from the exclusion list subjects all packets from that source to standard DHCP source verification.

For more information on the cable trust command, see the Cisco IOS CMTS Cable Command Reference Guide .

Unitary DHCPv6 Leasequery

The Cisco IOS Release 12.2(33)SCF1 introduces support for unitary DHCPv6 leasequery protocol (RFC 5007) on the Cisco CMTS routers for upstream IPv6 source verification. This protocol verifies the authenticity of the IPv6 CPE behind a home or small office cable deployment.

If the IPv6 source verification fails on the router and the **cable ipv6 source-verify dhcp** and **no cable nd** commands are configured on the bundle interface or subinterface, the Cisco CMTS triggers a unitary DHCPv6 leasequery to the Cisco Network Registrar (CNR). If a valid leasequery response is received from the CNR, the Cisco CMTS adds the CPE to its subscriber database and allows future traffic for the CPE.

The primary use of the unitary DHCPv6 leasequery protocol on the Cisco CMTS router is to recover lost CPE data including the Prefix Delegation (PD) route. The IPv6 CPE data can be lost from the Cisco CMTS in several ways. For example, PD route loss can occur during a Cisco CMTS reload.

The unitary DHCPv6 leasequery protocol also supports the following:

- DHCPv6 leasequery protocol.
- Rogue client database for failed source-verify clients.
- DHCPv6 leasequery filters.
- DHCPv6 leasequeries to a specific DHCPv6 server.

How to Configure Filtering of Cable DHCP Leasequery Requests

Use the following procedures to configure the filtering of DHCP Leasequery requests on the Cisco CMTS downstreams and upstreams:

Enabling DHCP Leasequery Filtering on Downstreams

Use the following procedure to start filtering DHCP leasequeries on all downstreams of a cable interface.

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**cable source-verify leasequery-filter downstream** *threshold interval* **Example:** `Router(config)# cable source-verify leasequery-filter downstream 5 10`	Enables leasequery filtering on all downstreams on the specified bundle interface, using the specified *threshold* and *interval* values.
Step 4	**end** **Example:** `Router(config)# end`	Exits configuration mode and returns to privileged EXEC mode.

Enabling DHCP Leasequery Filtering on Upstreams

Use the following procedure to start filtering DHCP Leasequeries on all upstreams on a bundle interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface bundle** *bundle-no* **Example:** `Router(config)# interface bundle 1`	Enters interface configuration mode for the specified bundle interface.
Step 4	**cable source-verify leasequery-filter upstream** *threshold interval* **Example:** `Router(config-if)# cable source-verify`	Enables leasequery filtering on all upstreams on the specified bundle interface, using the specified *threshold* and *interval* values. **Note** The **cable source-verify leasequery-filter upstream** command can only be configured under bundle interface.

	Command or Action	Purpose
	`leasequery-filter upstream 2 5`	**Note** Repeat step 3 and step 4 to enable the filtering of DHCP Leasequeries on the upstreams for other bundle interfaces. Master and slave interfaces in a cable bundle must be configured separately.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Unitary DHCPv6 Leasequery Filtering

Use the following procedure to configure the Cisco CMTS router to send Leasequeries to a DHCP server to verify the authenticity of the IPv6 CPE. You can also enable filtering of these requests to prevent large volumes of Leasequery requests on the bundle interfaces. Similarly, the number of allowable Leasequery requests and the interval time period can also be configured.

Note When the leasequery timer expires, only the IPv4 static CPE is automatically removed from the host database.

Before You Begin

- Disable the IPv6 Neighbor Discovery (ND) Gleaning feature using the **no** form of the **cable nd** command in bundle interface configuration mode before configuring the unitary DHCPv6 leasequery protocol. For details on IPv6 ND gleaning, see IPv6 on Cable feature guide.
- Configure the **cable ipv6 source-verify dhcp** command, introduced from Cisco IOS Release 12.2(33)SCF1 onwards, under the Cisco CMTS bundle or bundle subinterface to enable the unitary DHCPv6 leasequery protocol.
- In the cable ipv6 pd-route {enclosing-route | prefix-length} bundle-interface command, enclosing-route | prefix-length parameters should not be the same as IA_PD request and should be configured as a large prefix to include all the pd-route prefix for the downstream lease query.
- Use the **cable ipv6 source-verify dhcp** [**server** *ipv6-address]* command for a single DHCP server.
- *Use the* **cable ipv6 source-verify dhcp command without any keywords** *for multiple DHCP servers.*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface bundle** *bundle-no* **Example:** `Router(config)# interface bundle 1`	Enters interface configuration mode for the specified bundle interface.

Step 4	**cable ipv6 source-verify** or**cable ipv6 source-verify dhcp** [server ipv6-address]
	Example:
	`Router(config-if)# cable ipv6 source-verify`
	`or`
	`Router(config-if)# cable ipv6 source-verify dhcp server 2001:DB8:1::1`
		Enables leasequery filtering on the specified bundle interface and verifies the IP address with multiple DHCPv6 servers. or Enables leasequery filtering on the specified bundle interface and verifies the IP address with a specified DHCPv6 server.

Step 5	**cable ipv6 source-verify leasetimer** *value* **Example:** `Router(config-if)# cable ipv6 source-verify leasetimer 200`	Enables leasequery timer on the specified bundle interface, for the Cisco CMTS to check its internal CPE database for IPv6 addresses whose lease time has expired.
Step 6	**cable ipv6 source-verify leasequery-filter** *threshold interval* **Example:** `Router(config-if)# cable ipv6 source-verify leasetimer 5 10`	Enables filtering of the IPv6 leasequery requests.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling DHCPv6 Leasequery Filtering on Downstreams

Use the following procedure to start filtering DHCP Leasequeries on all downstreams of a cable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable ipv6 source-verify leasequery-filter downstream** *threshold interval* **Example:** `Router(config-if)# cable ipv6 source-verify leasetimer 5 10`	Enables leasequery filtering on all downstreams on the specified bundle interface, using the specified threshold and interval values:
Step 4	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Filtering of DHCP Leasequery

This section provides the following examples on how to configure the DHCP leasequery filtering feature:

Example: DHCP Leasequery Filtering

The following example shows an excerpt from a typical configuration of a bundle interface that is configured for filtering DHCP leasequery requests on both its upstream and downstream interfaces:

Note If an alternate server has been configured to receive leasequery requests, the **cable source-verify dhcp server** *ipaddress command* would display in place of the **cable source-verify dhcp** command below.

```
.
.
.
cable source-verify leasequery-filter downstream 5 20
.
.
.
interface bundle 1
.
.
.
 cable source-verify dhcp
 cable source-verify leasequery-filter upstream 1 5
 no cable arp
.
.
```

Example: Unitary DHCPv6 Leasequery Filtering

The following example shows how to display the total number of DHCPv6 leasequery requests that have been filtered on the router in Cisco IOS Release 12.2(33)SCF1:

```
Router# show cable leasequery-filter
IPv4 Lease Query Filter statistics for Unknown Sid
  Requests Sent : 0 total. 0 unfiltered, 0 filtered
IPv6 Lease Query Filter statistics for Unknown Sid
  Requests Sent : 0 total. 0 unfiltered, 0 filtered
```

The following example shows how to display the total number of DHCP leasequery requests that have been filtered on a particular cable interface in Cisco IOS Release 12.2(33)SCF1:

```
Router# show cable leasequery-filter cable 7/0/0

IPv4 Lease Query Filter statistics for Cable7/0/0:
  Requests Sent : 0 total. 0 unfiltered, 0 filtered
IPv6 Lease Query Filter statistics for Cable7/0/0:
  Requests Sent : 0 total. 0 unfiltered, 0 filtered
```

The following example shows how to display a list of cable modems on a cable interface and the number of DHCP leasequery messages filtered per interface in Cisco IOS Release 12.2(33)SCF1:

```
Router# show cable leasequery-filter cable 7/0/0 requests-filtered

Sid  MAC Address    IP Address      Req-Filtered
1    0018.6835.2756 0.0.0.0         0
2    0025.2e2d.7440 0.0.0.0         0
Sid  MAC Address    IP Address          Req-Filtered
1    0018.6835.2756 2001:DB8:1::1       0
2    0025.2e2d.7440 2001:DB8:1::2       0
```

Troubleshooting

The following **debug** commands help you to troubleshoot an improper DHCPv6 leasequery filtering configuration:

- **debug cable ipv6—**Enables debug operation for the IPv6 transactions on a cable interface.
- **debug cable ipv6 db—**Displays debug messages associated with host database transactions.
- **debug cable ipv6 dhcp—**Displays debug messages associated with DHCPv6 transactions.
- **debug cable ipv6 ha—**Displays debug messages associated with High Availability (HA) IPv6 transactions.
- **debug cable ipv6 lq—**Displays debug messages associated with leasequery (LQ) transactions.
- **debug cable ipv6 nd—**Displays debug messages associated with Neighbor Discovery (ND) transactions.
- **debug cable ipv6 source-verify—**Displays debug messages associated with source verification transactions.

For detailed information on these and other debug commands, see the Cisco IOS CMTS Cable Command Reference Guide .

Additional References

The following sections provide references related to the Cable DHCP Leasequery feature.

Related Documents

Related Topic	Document Title
IPv6	IPv6 on Cable
Cisco CMTS Command Reference	Cisco IOS CMTS Cable Command Reference Guide
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/security/command/ reference/fsecur_r.html

Standards

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

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 826	*An Ethernet Address Resolution Protocol (ARP)*
RFC 4388	Dynamic Host Configuration Protocol (DHCP) Leasequery
RFC 5007	Unitary DHCPv6 Leasequery

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

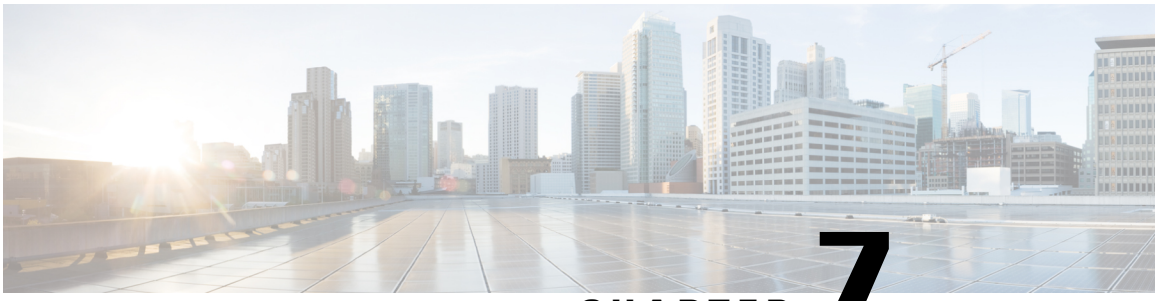
Feature Information for Cable DHCP Leasequery

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

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

Table 12: Feature Information for Cable DHCP Leasequery

Feature Name	Releases	Feature Information
Cable DHCP Leasequery	12.2(15)BC1d, 12.2(15)BC2b	This feature was introduced for the Cisco uBR7100 series, Cisco uBR7246VXR, and Cisco uBR10012 universal broadband routers.
Cable DHCP Leasequery	12.3(13)BC	Added support for the MAC Address Exclusion List for the cable-source verify dhcp command.
Filtering Cable DHCP Leasequery	12.3(17a)BC	Added support for the configurable leasequery server using the cable source-verify dhcp server ipaddress command.
RFC4388 Compliance Cable Leasequery	12.2(33)SCE1	Added support for RFC 4388 compliant DHCP leasequery. The **ip dhcp compatibility lease-query client** {**cisco** | **standard**} command was integrated to this feature.
Unitary DHCPv6 Leasequery protocol (RFC 5007)	12.2(33)SCF1	Added support for RFC 5007 compliant DHCPv6 leasequery protocol. The following sections provide information about this feature: The following commands were introduced or modified: **cable ipv6 source-verify, cable ipv6 source-verify leasequery-filter downstream, show cable leasequery-filter**, and **debug cable ipv6 lq**.



CHAPTER 7

Service Independent Intercept on the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: July 11, 2012

In Cisco IOS Release 12.2(33)SCA, the Service Independent Intercept (SII) feature enhances the current Lawful Intercept (LI) capability for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers using SNMPv3.

In releases prior to Cisco IOS Release 12.2(33)SCA, the Cisco cable modem termination system (CMTS) routers supported these LI capabilities:

- Intercepts for voice traffic in PacketCable environments
- IPv4 intercepts for SII using SNMPv3
- CLI for MAC intercepts

SII extends these LI capabilities in Cisco IOS Release 12.2(33)SCA and later releases by adding support for customer premise equipment (CPE) and cable modem (CM) based MAC intercepts using SNMPv3. SII is designed to provide data intercepts through SNMPv3, while PacketCable intercepts are designed for VoIP intercepts using a Common Open Policy Service (COPS) interface.

Finding Feature Information

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

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

Contents

Prerequisites for Service Independent Intercept

Before configuring SII, an understanding of the SNMPv3 configuration is required. Ensure that SNMPv3 is configured on the router.

Note SII intercepts are supported only on cable bundle interfaces.

This table shows the hardware compatibility prerequisites for this feature.

Table 13: Service Independent Intercept on the Cisco CMTS Routers Hardware Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2[17] Cisco IOS Release 12.2(33)SCB and later • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [18]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [19]

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

17 PRE = Performance Routing Engine

18 Cisco uBR-MC3GX60V cable interface line card is compatible only with PRE4.

19 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2

Restrictions for Service Independent Intercept

- IPv6 addressing for IP intercepts is supported on the Cisco uBR10012 router from Cisco IOS Release 12.2(33)SCG onwards.
- Mediation device (MD) must be reachable through the global IP routing table. Support for an MD inside an Multiprotocol Label Switching (MPLS)/VPN is not supported.
- SII information cannot be displayed using CLI. Intercept content from SII will not appear in the **show pxf cable** commands. Other intercept information outside of SII content (for PacketCable and through the CLI intercept) is shown.
- Cisco uBR10012 router has the following MIB object restrictions:
  - When a PRE switchover occurs, the SII configuration is lost. An SNMP trap is generated for this event. The SII must be configured after a PRE switchover.
  - cTap2MediationDestAddressType—IPv6 is not supported.
  - cTapMediationRtcpPort—Not supported.
  - cTapMediationRetransmitType—Not supported.
  - cTapMediationTransport—UDP only.
  - cTapStreamIpInterface—Only if interface supported is cable.
  - cTapStreamIpAddrType—Supported on IPv6 from Cisco IOS Release 12.2(33)SCG onwards.
  - cTapStreamIpDestinationLength—Must be 32 (no subnets are supported) or 0. The address length and port range restrictions are only for IPv4. There is no restriction for IPv6.
  - cTapStreamIpFlowId—Supported on IPv6 from Cisco IOS Release 12.2(33)SCG onwards.
  - cTapStreamIpDestL4PortMin—Must match DestL4PortMax or have a value of 0.

- cTapStreamIpDestL4PortMax—Must match DestL4PortMin or have a value of 65535.
- cTapStreamIpSourceL4PortMin—Must match SourceL4PortMin or have a value of 0.
- cTapStreamIpSourceL4PortMax—Must match SourceL4PortMax or have a value of 65535.

- Maximum number of IP intercepts allowed is 800.
- Maximum number of MAC intercepts allowed is 400.

Note Performance is measured based on the total bit rate and bandwidth based on the tapped traffic rather than the stream number. For example, one MAC intercept may carry 300 Mbps of traffic while a normal VoIP traffic may be around 80 Kbps.

Information About Service Independent Intercept

SII has the following benefits:

- Does not affect subscriber services on the router.
- Can neither be detected by the target, nor tapped.
- Allows Law Enforcement Agencies (LEAs) to perform lawful intercepts without the knowledge of service providers.
- Uses Simple Network Management Protocol version 3 (SNMPv3) and security features like the View-based Access Control Model (SNMP-VACM-MIB) and User-based Security Model (SNMP-USM-MIB) to restrict access to lawful intercept information and components.
- Supports intercepts of Layer 2, Layer 3, and Layer 4 traffic.
- Supports Layer 2 intercepts for upstream and downstream traffic.
- Hides information about lawful intercepts from all but the most privileged users.
- Provides two secure interfaces for performing an intercept—one for setting up the wiretap and one for sending the intercepted traffic to the MD.
- Coexists with Packet Intercept (PI). To support PI in a PacketCable environment for voice intercepts, you must enable PacketCable operation must be enabled on the Cisco CMTS and other related PacketCable configurations must be implemented as required. For more information about PacketCable and lawful intercept, see the PacketCable and PacketCable Multimedia for the Cisco CMTS Routers and Lawful Intercept Architecture feature guides.

Before configuring SII on the Cisco CMTS, understand the following concepts:

Lawful Intercept

LI is a process that enables a Law Enforcement Agency (LEA) to perform electronic surveillance on an individual (also known as target) as authorized by a judicial or administrative order. To facilitate the lawful intercept process, certain legislation and regulations require SPs and ISPs to implement their networks to explicitly support authorized electronic surveillance.

The surveillance is performed through the use of wiretaps on traditional telecommunications and Internet services in voice, data, and multiservice networks. The LEA delivers a request for a wiretap to the service provider of the target, who is responsible for intercepting data communication to and from the target. The service provider uses the MAC address or session ID of the target to determine which of its edge routers handles the traffic (data communication) of the target. The service provider then intercepts the traffic of the target as it passes through the router, and sends a copy of the intercepted traffic to the LEA without the knowledge of the target.

The LI feature supports the Communications Assistance for Law Enforcement Act (CALEA), which specifies that SP in the United States must support lawful intercept. Currently, LI is defined by the following standards:

- Telephone Industry Association (TIA) specification J-STD-025
- Packet Cable Electronic Surveillance Specification (PKT-SP-ESP-101-991229)

Packet Intercept

PI describes a Cisco CMTS-specific implementation for lawful intercept on Cisco CMTS routers. PI is supported through two interfaces. In a PacketCable environment, PI provides voice intercept capability for IP intercepts using COPS to support CALEA. Using a CLI interface (**cable intercept** command), PI also supports MAC intercepts.

For more information about PacketCable Lawful Intercept, PacketCable configuration on the Cisco CMTS, and COPS support on the Cisco CMTS, see the PacketCable and PacketCable Multimedia for the Cisco CMTS Routers .

Service Independent Intercept

SII describes a standard Cisco architecture (RFC 3924, Cisco Architecture for Lawful Intercept in IP Networks) that provides Layer 1 capabilities using an SNMPv3 interface.

SII supports a different intercept method than PI on the Cisco CMTS router by using SNMPv3 for both MAC and IP intercepts. Although SII is a distinct method from PI, SII can coexist with PI-based intercepts in Cisco IOS Release 12.2(33)SCA and later releases.

Service Independent Intercept Tap in Routed Subnets

In Cisco IOS Release 12.2(33)SCE and earlier releases, it is assumed that the “IP tap” on the Cisco CMTS cable interface is a legal IP address acquired from the Cisco Network Registrar (CNR), which can pass reverse path forwarding (RPF) verification. Based on this assumption, a tapped IP address is defined under the scope of the cable bundle interface subnet, such as:

```
ip address <ip-address> <subnet-mask> or ip address <ip-address> <subnet-mask> secondary
```

For example: ip address 80.32.0.1 255.255.255.0

Cisco IOS Release 12.2(33)SCF and later releases do not have any CNR restrictions.

The source IP address or the destination IP address of a tapped stream is normally learned from a routing protocol or provisioned by a static route. When a CPE acts as a router, the IP route behind the CPE is not allocated by the CNR DHCP. Therefore, the destination IP address is not defined in the bundle interface subnet.

Starting with Cisco IOS Release 12.2(33)SCF, the SII provisioning mode is supported in the route processor and on the Cisco IOS LI.

For more information, see the Provisioning Taps on IP addresses Learned from the CPE Router, on page 137.

IPv6 Address Packet Intercept

The IPv6 Address Packet Intercept feature provides lawful intercept of cable modems and CPEs provisioned with IPv6 addresses. This feature taps all the packets received and sent from the system. The intercepted packets are sent to the MD with the content connection identifier (CCCID) specified by the tapping rule.

The following types of IPv6 taps are supported on the Cisco CMTS router:

- IPv6 Taps—Matches all IPv6 packets.
- 6PE Taps—Supports IPv6 Provider Edge (6PE) deaggregation. However, disposition packets are not supported.
- 6VPE Taps—Matches all IPv6 packets in the virtual routing and forwarding (VRF) context. Disposition packets are not supported.

The IPv6 Address Packet Intercept feature provides these benefits on a Cisco CMTS router:

- Supports up to 1000 IPv6 taps.
- Supports IPv4 and MAC taps.
- Supports up to 4000 mediation devices.
- Intercepts and forwards up to 100,000 packets per second.

In the Cisco CMTS, IPv6 taps can be applied only to the cable interfaces. However, the Cisco CMTS can search for the interface using the IPv6 routing table using the IPv6 source (src) and destination (dst) address tap. A tap request on the cable interface will fail only if the tap requests exceed the maximum number of taps supported on the Cisco CMTS.

A forwarding packet can be tapped at both the input and output interface, and a single packet may be hit by more than one tapping rule. However, the Cisco CMTS will send only one replication of the forwarding packet to the MD. Likewise, both IPv6 address taps and MAC taps can be provisioned. If the packet matches both the taps, the MAC tap will take priority and the packet will be sent only to the MD of the MAC tap.

MPLS and VPN Support

The IPv6 Address Packet Intercept supports MPLS and VPN at the Provider Edge (PE) router. The VRF processes the MPLS and VPN traffic, and interception is performed on the IPv6 packet under VRF.

Compatibility with Other Taps

The SII Access Control List (ACL) tap is compatible with other kinds of tap, such as MAC tapping, CALEA, and hash table based IPv4 tapping. It also coexists with security ACL, quality of service (QoS) ACL, cable filter, overlapping tap, and multiple MDs. However, SII ACL tap will not work with Layer 2 VPN (L2VPN) and Any Transport Over MPLS (AToM) packets.

Network Components Used for Lawful Intercept

Mediation Device

A mediation device (supplied by third-party vendor) handles most of the processing for the lawful intercept. The mediation device:

- Provides the interface used to set up and provision the lawful intercept.
- Generates requests to other network devices to set up and run the lawful intercept.
- Converts the intercepted traffic into the format required by the LEA (which can vary from country to country) and sends a copy of the traffic to the LEA without the knowledge of the target.

Note If multiple LEAs are performing intercepts on the same target, the mediation device must make a copy of the intercepted traffic for each LEA. The mediation device is also responsible for restarting any lawful intercepts that are disrupted due to a failure.

Intercept Access Point

An intercept access point (IAP) is a device that provides information for the lawful intercept. There are two types of IAPs:

- Identification (ID) IAP—A device, such as an authentication, authorization, and accounting (AAA) server, that provides intercept related information (IRI) for the intercept (for example, the username of the target and system IP address). The IRI helps the service provider determine which content IAP (router) the traffic of the target passes through.
- Content IAP—A device, such as a Cisco CMTS router, through which the traffic of the target passes through. The content IAP:
  - Intercepts traffic to and from the target for the length of time specified in the court order. The router continues to forward traffic to its destination to ensure that the wiretap is undetected.
  - Creates a copy of the intercepted traffic, encapsulates it in UDP packets, and forwards the packets to the mediation device without the knowledge of the target.

Note The content IAP sends a single copy of intercepted traffic to the mediation device. If multiple LEAs are performing intercepts on the same target, the mediation device must make a copy of the intercepted traffic for each LEA.

Collection Function

The collection function is a program that stores and processes traffic intercepted by the service provider. The program runs on the equipment at the LEA.

Lawful Intercept Processing

After acquiring a court order or warrant to perform surveillance, the LEA delivers a surveillance request to the service provider of the target. The service provider determines the appropriate router to set up the tap and forwards the intercepted packets to the mediation device, which might be located outside of the premises of the service provider.

There is no standard method in a PacketCable environment for setting up a tap for voice traffic. SII provides a standard way for setting up data taps by either an IP or MAC address. SII 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.

The following sequence of events provides an example of a process that might be used during a sample lawful intercept:

- The admin function at the service provider contacts the ID IAP for the IRI, such as the username of the target and the IP address of their system, to determine which content IAP (router) the traffic of the target passes through.
- After identifying the router that handles the traffic of the target, the admin function issues SNMPv3 **get** and **set** requests to the router MIBs to set up and activates the lawful intercept. The router MIBs include the CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, and CISCO-802-TAP-MIB.
- During the lawful intercept, the router:
  - Examines incoming and outgoing traffic and intercepts any traffic that matches the specifications of the lawful intercept request.
  - Creates a copy of the intercepted traffic and forwards the original traffic to its destination so the target does not suspect anything.
  - Encapsulates the intercepted traffic in UDP packets and forwards the packets to the mediation device without the knowledge of the target.

Note The process of intercepting and duplicating the traffic of the target adds no detectable latency in the traffic stream.

- The mediation device converts the intercepted traffic into the required format and sends it to a collection function running at the LEA. Here, the intercepted traffic is stored and processed.

Note If the router intercepts traffic that is not allowed by the judicial order, the mediation device filters out the excess traffic and sends the LEA only the traffic allowed by the judicial order.

- When the lawful intercept expires, the router stops intercepting the traffic of the target.

SNMPv3 Interface

SII supports the following MIBs in SNMPv3:

- CISCO-TAP2-MIB, on page 125
- CISCO-IP-TAP-MIB, on page 126
- CISCO-802-TAP-MIB, on page 128

For more information on the Cisco IOS MIB tools, see the the MIB Locator page.

CISCO-TAP2-MIB

The CISCO-TAP2-MIB contains SNMP management objects that control lawful intercepts on the router. The mediation device uses the MIB to configure and run lawful intercepts on targets whose traffic passes through the router. The MIB is bundled with Cisco IOS software images that support the Service Independent Intercept feature.

The CISCO-TAP2-MIB works with the CISCO-IP-TAP-MIB and the CISCO-802-TAP-MIB to define specific intercepts.

Table 14: CISCO-TAP2-MIB Tables and Objects

Object	Description
cTap2MediationTable	Lists the MDs with which the intercepting device communicates.
cTap2StreamTable	Lists the traffic streams to be intercepted. Consists of generic fields that are independent of the type of intercept.
cTap2DebugTable	Contains LIt debug messages generated by the implementing device.
cTap2MediationNewIndex	Contains a value which may be used as an index value for a new cTap2Mediation object entry.
cTap2MediationCapabilities	Displays the device capabilities for certain fields in the MD. This may be dependent on hardware or software capabilities.
cTap2DebugAge	Contains the duration in minutes for which an entry in the cTap2DebugTable object is maintained by the implementing device. The entry is deleted when this duration is reached.

Object	Description
cTap2DebugMaxEntries	Contains the maximum number of debug messages maintained at one time by the implementing device. When this limit is reached, the most recent message replaces the oldest message.

Table 15: CISCO-TAP2-MIB Notifications , on page 126 lists the notifications in the CISCO-TAP2-MIB. For more information, see the MIB documentation.

Table 15: CISCO-TAP2-MIB Notifications

Notification	Description
ciscoTap2MIBActive	Sent when an intercepting router or switch is first capable of intercepting a packet corresponding to a configured data stream. The value of the corresponding cTap2StreamType object that identifies the actual intercept stream type is included in this notification.
ciscoTap2MediationTimedOut	Sent when an intercept is autonomously removed by an intercepting device, such as due to the time specified in the cTap2MediationTimeout object.
ciscoTap2MediationDebug	Sent when there is intervention needed due to events related to entries configured in the cTap2MediationTable object.
ciscoTap2StreamDebug	Sent when there is intervention needed due to events related to entries in the cTap2StreamTable object.
ciscoTap2Switchover	Sent when there is a redundant (standby) route processor available on the intercepting device and the current active processor is going down causing the standby to takeover.

CISCO-IP-TAP-MIB

The CISCO-IP-TAP-MIB contains the SNMP management objects to configure and execute lawful intercepts on IP Layer 3 streams. This MIB is used with the CISCO-TAP2-MIB to intercept traffic based on the IP address.

Note The Cisco CMTS routers supports IPv6 IP intercepts only from Cisco IOS Release 12.2(33)SCG onwards.

Table 16: CISCO-IP-TAP-MIB Tables and Objects

Object	Description
citapStreamTable	Lists the IP streams to be intercepted.
citapStreamCapabilities	Displays the type of intercept streams that can be configured on this type of device.
citapStreamInterface	Lists the ifIndex value of the interface over which the traffic to be intercepted is received or transmitted.
citapStreamAddrType	Lists the type of address used in the packet selection.
citapStreamDestinationAddress	Lists the destination address or prefix used in the packet selection. This address is of "type" specified in the citapStreamAddrType.
citapStreamDestinationLength	Lists the length of the destination prefix. A value of zero causes all addresses to match.
citapStreamSourceAddress	Lists the source address used in the packet selection. This address is of "type" specified in the citapStreamAddrType object.
citapStreamSourceLength	Lists the length of the source prefix. A value of zero causes all addresses to match. This prefix length is consistent with the "type" specified in the citapStreamAddrType object.
citapStreamTosByte	Lists the value of the ToS byte when masked with citapStreamTosByteMask object, of traffic to be intercepted. If citapStreamTosByte&(~citapStreamTosByteMask)!=0, the configuration is rejected.
citapStreamTosByteMask	Lists the value of the ToS byte in an IPv4 header. The AND operation is performed on the citapStreamTosByteMask and citapStreamTosByte objects; if the values are equal, the comparison is equal. If the mask is zero and the ToS byte value is zero, the result is to always accept.
citapStreamFlowId	Lists the flow identifier in an IPv6 header. -1 indicates that the flow ID is unused.
citapStreamProtocol	Lists the IP protocol that must be matched against the IPv4 protocol number in the packet. -1 means "any IP protocol".

Object	Description
citapStreamDestL4PortMin	Lists the minimum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or less than the value specified for this entry in the citapStreamDestL4PortMax object.
citapStreamDestL4PortMax	Lists the maximum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or greater than the value specified for this entry in the citapStreamDestL4PortMin object.
citapStreamSourceL4PortMin	Lists the minimum value that the Layer 4 destination port number in the packet must have in order to match. This value must be equal to or less than the value specified for this entry in the citapStreamSourceL4PortMax object.
citapStreamSourceL4PortMax	Lists the maximum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or greater than the value specified for this entry in the citapStreamSourceL4PortMin object.
citapStreamVRF	Lists the name of a VRF table (ASCII string) comprising the routing context of a VPN. The interface or set of interfaces on which the packet may be found should be selected from the set of interfaces in the VRF table. A string length of zero implies that the global routing table must be used for selection of interfaces on which the packet might be found.

CISCO-802-TAP-MIB

The CISCO-802-TAP-MIB contains the SNMP management objects to configure and execute lawful intercepts on Layer 2 streams. This MIB is used with the CISCO-TAP2-MIB to intercept traffic based on the MAC address.

The Cisco CMTS routers in Cisco IOS Release 12.2(33)SCA support MAC-based intercepts for both the cable modem (CM) and the CPE using SNMPv3.

Table 17: CISCO-802-TAP-MIB Tables and Objects

Object	Description
c802tapStreamTable	Lists the IEEE 802 data streams to be intercepted.

Object	Description
c802tapStreamCapabilities	Displays the types of intercept streams that can be configured on this device. This may be dependent on hardware or software capabilities.
citapStreamInterface	Lists the ifIndex value of the interface over which the traffic to be intercepted is received or transmitted.
citapStreamAddrType	Lists the type of address used in the packet selection.
citapStreamDestinationAddress	Lists the destination address or prefix used in the packet selection. This address is of “type” specified in the citapStreamAddrType object.
citapStreamDestinationLength	Lists the length of the destination prefix. A value of zero causes all addresses to match.
citapStreamSourceAddress	Lists the source address used in the packet selection. This address is of “type” specified in the citapStreamAddrType object.
citapStreamSourceLength	Lists the length of the source prefix. A value of zero causes all addresses to match. This prefix length is consistent with the “type” specified in the citapStreamAddrType object.
citapStreamTosByte	Lists the value of the ToS byte when masked with the citapStreamTosByteMask object, of traffic to be intercepted. If citapStreamTosByte&(~citapStreamTosByteMask)!=0, the configuration is rejected.
citapStreamTosByteMask	Lists the value of the ToS byte in an IPv4 header. The AND operation is performed on the citapStreamTosByteMask and citapStreamTosByte objects; if the values are equal, the comparison is equal. If the mask is zero and the ToS byte value is zero, the result is to always accept.
citapStreamFlowId	Lists the flow identifier in an IPv6 header. -1 indicates that the flow ID is unused.
citapStreamProtocol	Lists the IP protocol that must be matched against the IPv4 protocol number in the packet. -1 means “any IP protocol”.

Object	Description
citapStreamDestL4PortMin	Lists the minimum value that the Layer 4 destination port number in the packet must have in order to match. This value must be equal to or less than the value specified for this entry in the citapStreamDestL4PortMax object.
citapStreamDestL4PortMax	Lists the maximum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or greater than the value specified for this entry in the citapStreamDestL4PortMin object.
citapStreamSourceL4PortMin	Lists the minimum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or less than the value specified for this entry in the citapStreamSourceL4PortMax object.
citapStreamSourceL4PortMax	Lists the maximum value that the Layer 4 destination port number in the packet must have in order to match this classifier entry. This value must be equal to or greater than the value specified for this entry in the citapStreamSourceL4PortMin object.
citapStreamVRF	Lists the name of a VRF table (ASCII string) comprising the routing context of a VPN. The interface or set of interfaces on which the packet may be found should be selected from the set of interfaces in the VRF table. A string length of zero implies that the global routing table must be used for selection of interfaces on which the packet might be found.

How to Perform SNMPv3 Provisioning for Service Independent Intercept

This section includes the following procedures:

Prerequisites for SNMPv3 Provisioning

- Ensure you are logged in to the router with the highest access level (level-15). To log in with level-15 access, enter the **enable** command and specify the highest-level password defined for the router.
- Ensure that the mediation device has an access function (AF) and an access function provisioning interface (AFPI).

- Ensure that you have added the mediation device to the SNMP user group that has access to the CISCO-TAP2-MIB view, using the **snmp-server user** command. Specify the username of the mediation device as the user to add to the group.
- Ensure that when you add the mediation device as a CISCO-TAP2-MIB user, the authorization password of the mediation device must be at least eight characters in length.

Restrictions to SNMPv3 Provisioning

- The only users who should be allowed to access the Lawful Intercept MIBs are the mediation device and system administrators who need to know about lawful intercepts on the router. In addition, these users must have authPriv or authNoPriv access rights to access the SII MIBs. Users with NoAuthNoPriv access cannot access the Lawful Intercept MIBs.
- You cannot use the SNMP-VACM-MIB to create a view that includes the Lawful Intercept MIBs.
- The default SNMP view excludes the following MIBs:
  - CISCO-TAP2-MIB
  - CISCO-IP-TAP-MIB
  - SNMP-COMMUNITY-MIB
  - SNMP-USM-MIB
  - SNMP-VACM-MIB
- The Cisco CMTS router does not display log messages about SII taps; therefore, you can only see configuration errors by using SNMP traps.
- The Cisco CMTS router does not display any details about SII taps in **show pxf cable** commands. A line in the output of the **show pxf cable** command displays the number of SII taps, but not their content.
- The Cisco CMTS router supports IPv6 addressing for IP taps only from Cisco IOS Release 12.2(33)SCG onwards.

Accessing the Lawful Intercept MIBs

Due to its sensitive nature, the Cisco lawful intercept MIBs supported by SII are only available in software images that support the SII and Lawful Intercept features. These MIBs are not accessible through the Network Management Software MIBs Support page.

In Cisco IOS Release 12.2(33)SCA and later releases, the Cisco CMTS routers support LI and SII MIBs using the following images:

- Cisco uBR7246VXR router—ubr7200-k9pu2-mz
- Cisco uBR10012 router—ubr10k2-k9p6u2-mz

In Cisco IOS Releases 12.2(33)SCF and later releases, the Cisco CMTS routers support LI and SII MIBs using the following images:

- Cisco uBR10012 router with PRE2—ubr10k2-k9p6u2-mz

- Cisco uBR10012 router with PRE4—ubr10k4-k9p6u2-mz
- Cisco uBR7246VXR router with NPE-G1—ubr7200-ik9su2-mz
- Cisco uBR7246VXR router with NPE-G2—ubr7200p-jk9su2-mz

Restricting Access to the Lawful Intercept MIBs

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

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server view***view-name oid-tree* **included** **Example:** `Router(config)# snmp-server view tapView ciscoIpTapMIB included`	Creates or updates a view entry. • **view** *view-name*—Label for the view record that you are updating or creating. The name is used to reference the record. • *oid-tree*—Object identifier of the ASN.1 subtree. • **included**—Type of view. Repeat this step as needed to include other MIBs in the view.
Step 4	**snmp-server group***groupname* **v3 noauth read***readview* **write***writeview* **notify***notifyview*	Configures a new SNMPv3 group. • *groupname*—SNMP server group name.

	Command or Action	Purpose
	Example: `Router(config)# snmp-server group tapGroup v3 noauth read tapView write tapView notify tapView`	• **v3—**The most secure of the possible security models. • **noauth—**Specifies no authentication of a packet. • **read—**The option that allows you to specify a read view. • *readview***—**A string (not to exceed 64 characters) that is the name of the view that enables you only to view the contents of the agent. • **write—**The option that allows you to specify a write view. • *writeview***—**A string (not to exceed 64 characters) that is the name of the view that enables you to enter data and configure the contents of the agent. • **notify—**The option that allows you to specify a notify view. • *notifyview***—**A string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.
Step 5	**snmp-server user** *username groupname* **v3 auth md5** *auth-password* **Example:** `Router(config)# snmp-server user tapuser tapGroup v3 auth md5 cisco`	Configures a new user to an SNMPv3 group • *username***—**The name of the user on the host that connects to the agent. • *groupname***—**The name of the group to which the user is associated. • **v3—**The most secure of the possible security models. • **auth—**Initiates an authentication level setting session • **md5—**The HMAC-MD5-96 authentication level. • *auth-password***—**A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Verifying the SNMP Configuration

Use the following commands to verify the configuration of SNMP:

Command	Description
show snmp group	Displays the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group.
show snmp user	Displays information about the configured characteristics of SNMP users.
show snmp view	Displays the family name, storage type, and status of an SNMP configuration and associated MIB.

Provisioning the Cable Interface Using SNMPv3

1 Establish the mediation device first.
2 Provision the cable interface for which intercepts should be enabled by configuring objects in both the CISCO-802-TAP-MIB and the CISCO-IP-TAP-MIB:

- CISCO-802-TAP-MIB—Configure the c802tapStreamInterface object.
- CISCO-IP-TAP-MIB—Configure the citapStreamInterface object.

3 Use the c802tapStreamInterface and citapStreamInterface objects to specify the ifIndex of the desired interface. Use a -1, 0, or the address of the cable bundle interface.

Provisioning IP Intercepts Using SNMPv3

1 Configure objects in the CISCO-TAP2-MIB:

Configure the cTap2StreamEntry table object with the cTap2StreamType object configured for IP. This entry is used with the citapStreamEntry table object in the CISCO-IP-TAP-MIB.

1 Configure objects in the CISCO-IP-TAP-MIB:

Configure the ciTapStreamEntry table object that provides the details of the intercept in the CISCO-IP-TAP-MIB. This entry is used with the cTap2StreamEntry table object in the CISCO-TAP2-MIB.

1 Set the cTap2StreamInterceptEnable object bit.

Note IP intercepts also have interface OIDs. For more information, see the Provisioning the Cable Interface Using SNMPv3, on page 134.

Provisioning IPv6 Taps Using SNMPv3

The IPv6 Address Packet Intercept is provisioned through SNMPv3. The MIBs involved in configuring IPv6 address tap are CISCO-IP-TAP-MIB and CISCO-TAP2-MIB. CISCO-IP-TAP-MIB object ID (OID) specifies

the IPv6 packet stream. CISCO-TAP2-MIB OID specifies the MD, as to where and how to send the intercepted packet.

The IPv6 tap request should comply with the CISCO-IP-TAP-MIB and CISCO-TAP2-MIB to provision tap. The Cisco CMTS accepts each tap rule provisioned through SNMPv3 and sends the intercepted packet to the MD with the CCCID specified by the tapping rule.

The basic difference of IPv6 address tap from IPv4 address tap is that you have to specify the IPv6 address type and assign IPv6 address at the source and destination fields. Except the flow identifier, which is not used in IPv4 tap, all the other OIDs used by the IPv6 address tap are the same as of IPv4 address tap.

Restrictions for IPv6 Address Packet Intercept

The IPv6 Address Packet Intercept has the following specific restrictions in addition to the general IPv4 address tapping restrictions.

- The IPv6 address tap through SNMP MIB is supported only on the Cisco uBR10012 series routers.
- The IPv6 address tap provision is not supported on the Cisco uBR7200 series routers. Any SNMP request on these routers will fail.
- The IPv6 packet intercept can be performed at the Cisco uBR7200 series routers only by setting up the MAC tap.
- The Cisco CMTS router does not support IPv6 multicast address tap on cable interfaces.
- The Cisco CMTS router supports only IPv4 MD encapsulation.
- The MPLS/VPN supports imposition and deaggregation.
- The IPv4 or IPv6 packets within an L2VPN or AToM will not be tapped.
- The IPv6 taps are supported only on cable interfaces.
- The IPv6 packet will be tapped only once.
- The IPv6 packets that come in as fragments without L4 fields are intercepted.

To provision the cable interface using SNMPv3, see Provisioning the Cable Interface Using SNMPv3, on page 134.

The IPv6 packet can also be tapped per CPE and per CM MAC address. For more details, see the Provisioning MAC Intercepts Using SNMPv3, on page 135.

Provisioning MAC Intercepts Using SNMPv3

SII in Cisco IOS Release 12.2(33)SCA on the Cisco CMTS routers allows you to provision bidirectional MAC intercepts (supports the upstream and downstream path) for a CM or CPE using SNMPv3.

The cmMacAddress object is used to specify the MAC address of either the CPE device or CM, and therefore is the object that determines the type of MAC intercept used.

Prerequisites for Provisioning MAC Intercepts using SNMPv3

- The CM must be online before the MAC intercept can be configured using SNMPv3.

- Set the CM bit only if you want to configure a CM-based tap.
- The destination (dstMACAddress) and source MAC address (srcMacAddress) bits must both be set.
- The values of the destination (c802tapStreamDestinationAddress) and source address (c802tapStreamSourceAddress) objects must have identical values.

Note If both destination and source MAC bits are not set, or the MAC address values do not match, the tap is rejected.

Restrictions to Provisioning MAC Intercepts using SNMPv3

- SII interface taps are only supported on cable line card bundle interfaces.

You can provision the following MAC intercepts using SNMPv3:

- Provisioning a MAC Intercept for Cable Modems Using SNMPv3, on page 136
- Provisioning a MAC Intercept for a CPE Device Using SNMPv3, on page 136
- Provisioning Taps on IP addresses Learned from the CPE Router, on page 137

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
- c802tapStreamSourceAddress

Provisioning Taps on IP addresses Learned from the CPE Router

Note To provision taps, the IP address must be available to the Cisco CMTS either through a routing protocol or by specifying the interface for the tap.

When a routed CPE is provisioned, the Cisco CMTS checks if the CPE is reachable by using the routing table. The Cisco CMTS can learn the route in the routing table through routing protocols, such as:

- Routing Information Protocol (RIP)
- RIP2
- Static route

The route can also be manually configured on the Cisco CMTS (static route).

Static route can be manually added by executing the **ip route** *destination netmask next-hop* command. For example, ip route 192.168.80.0 255.255.255.0 172.27.184.69 .

Use the **show ip route** command to verify if the static route has been configured. The routing protocol can also be viewed by running the **show ip route** command.

Note Starting with Cisco IOS Release 12.2(33)SCF, SII taps can be configured to an IP address learned from a CPE router.

Table 18: IP Address Tap , on page 137 and Table 19: MAC Address Tap , on page 138 display the conditions when a tap is successful.

Table 18: IP Address Tap

Source IP[20]	Destination IP	Specified Interface (bundle interface)	IP Subnet – Statically Configured or Learned on any Cable Interface	IP Subnet – Statically Configured or Learned on a Specified Cable Interface	Tap Enable?	Tap Success?
Yes	Yes	No	Yes	—[21]	Yes	Yes
Yes	Wildcard[22]	No	Yes	—	Yes	Yes
Wildcard	Yes	No	Yes	—	Yes	Yes
Wildcard	Wildcard	No	—	—	—	No
Yes	Yes	Yes	X	Yes	Yes	Yes

Source IP[20]	Destination IP	Specified Interface (bundle interface)	IP Subnet – Statically Configured or Learned on any Cable Interface	IP Subnet – Statically Configured or Learned on a Specified Cable Interface	Tap Enable?	Tap Success?
Yes	Wildcard	Yes	X	Yes	Yes	Yes
Wildcard	Yes	Yes	X	Yes	Yes	Yes
Wildcard	Wildcard	Yes	—	—	—	No
X[23]	X	X	No	No	—	No

20 Source IP, Destination IP, and Specified Interface columns are the OIDs from the SNMP.
21 "—" indicates that the item is not available or not applicable.
22 Wildcard is a subnet mask of 0.0.0.0
23 "X" can indicate either Yes or No.

Note The IP address presented at the Cisco CMTS Cable interface, Tap Enable, and Tap Success columns refer to the state on the Cisco CMTS.

Table 19: MAC Address Tap

Source MAC Address	Destination MAC Address	Specified Interface (Cable Interface)	MAC Address Presented at the Cisco CMTS Cable Interface	MAC Address Presented at the Specified Cable Interface	Tap Enable	Tap Success?
Yes	Yes	No	Yes	—[24]	Yes	Yes
Yes	Wildcard[25]	No	Yes	—	—	No*[26]
Wildcard	Yes	No	Yes	—	—	No*
Wildcard	Wildcard	No	—	—	—	No*
Yes	Yes	Yes	X	Yes	Yes	Yes
Yes	Wildcard	Yes	X	Yes	—	No*
Wildcard	Yes	Yes	X	Yes	—	No*
Wildcard	Wildcard	Yes	—	—	—	No
Yes	Yes	X	No	No	No**[27]	Yes**

Source MAC Address	Destination MAC Address	Specified Interface (Cable Interface)	MAC Address Presented at the Cisco CMTS Cable Interface	MAC Address Presented at the Specified Cable Interface	Tap Enable	Tap Success?
Yes	Wildcard	X	X	X	—	No*
Wildcard	Yes	X	X	X	—	No*
X[28]	X	X	No	No	—	No

24 "—" indicates that the item is not available or not applicable.
25 Wildcard is a subnet mask of 0.0.0.0.
26 Both the source and destination MAC addresses must be present.
27 This is a preconfiguration case indicating that the CPE or the CM is not online.
28 "X" can indicate either Yes or No.

Enabling SNMP Notifications for Lawful Intercept

SNMP automatically generates notifications for lawful intercept events. This is because the default value of the cTap2MediationNotificationEnable object is true(1).

The **snmp-server enable traps snmp** command configures the router to send RFC 1157 notifications to the mediation device.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** *hostname* **version3noauth** *community-string* **udp-port** *portnotification-type* **Example:** `Router(config)# snmp-server host 10.10.10.10 version 3 noauth mdpass udp-port 161 snmp`	Specifies the recipient of an SNMP notification operation. • *hostname*—Name or Internet address of the host (the targeted recipient). • **version3**—Version of the SNMP used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the priv keyword. If you use the version

	Command or Action	Purpose
		keyword, you should also specify a security level. • **noauth—**The noAuthNoPriv security level. This is the default value. • *community-string***—**Password-like community string sent with the notification operation. • **udp-port—**UDP port of the host to use. The default is 162. • *notification-type***—**Type of notification to be sent to the host. If no type is specified, all notifications are sent.
Step 4	**snmp-server enable traps snmp** [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**] **Example:** `Router(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`	Enables the sending of RFC 1157 SNMP notifications. • **authentication—**(Optional) Controls the sending of SNMP authentication failure notifications. • **linkup—**(Optional) Controls the sending of SNMP linkUp notifications. • **linkdown—**(Optional) Controls the sending of SNMP linkDown notifications. • **coldstart—**(Optional) Controls the sending of SNMP coldStart notifications. • **warmstart—**(Optional) Controls the sending of SNMP warmStart notifications.
Step 5	**snmp-server enable traps** [*notification-type*] [**vrrp**] **Example:** `Router(config)# snmp-server enable traps tty`	Enables all SNMP notification types that are available on your system. • *notification-type***—**(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled (if the **no** form is used). • **vrrp—**(Optional) Specifies the Virtual Router Redundancy Protocol (VRRP).

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Disabling SNMP Notifications

- To disable all SNMP notifications, use the **no snmp-server enable traps** command.
- To disable lawful intercept notifications, use SNMPv3 to set the CISCO-TAP2-MIB object cTap2MediationNotificationEnable to false(2). To re-enable lawful intercept notifications through SNMPv3, reset the object to true(1).

Configuration Examples for SNMPv3 Provisioning for Service Independent Intercept

```
Router# show running-config | include snmp
snmp-server engineID local 800000090300020000000000
snmp-server group tapGroup v3 noauth read tapView write tapView
snmp-server view tapView ciscoIpTapMIB included
snmp-server view tapView cisco802TapMIB included
snmp-server view tapView ciscoTap2MIB included
snmp-server enable traps tty
snmp-server enable traps alarms informational
snmp-server manager


Router# show snmp user
User name: tapuser
Engine ID: 800000090300020000000000
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: tapGroup
```

Additional References

The following sections provide references related to the SII feature.

Related Documents

Related Topic	Document Title
SNMP configuration information	*Cisco IOS Configuration Fundamentals Configuration Guide,* Part 3: Cisco IOS System Management, "Configuring SNMP Support" section at: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html
SNMP command information	*Cisco IOS Network Management Command Reference , Release 12.2SB* at: http://www.cisco.com/en/US/docs/ios/netmgmt/command/ reference/nm_book.html
Lawful Intercept Architecture	*Lawful Intercept Architecture* http://www.cisco.com/en/US/docs/ios/sec_user_services/ configuration/guide/sec_lawful_intercept.html
PacketCable	PacketCable and PacketCable Multimedia for the Cisco CMTS Routers http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm.html

MIBs

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

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 Service Independent Intercept

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

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

Table 20: Feature Information for Service Independent Intercept

Feature Name	Releases	Feature Information
Service Independent Intercept	12.2(33)SCA	SII support is introduced and enhanced using SNMPv3 in Cisco IOS Release 12.2(33)SCA on the Cisco uBR7225VXR, Cisco uBR7246VXR, and Cisco uBR10012 (with PRE2) universal broadband routers.
SII Routed CPE Support	12.2(33)SCF	SII Routed CPE Support feature was introduced.
IPv6 Address Packet Intercept	12.2(33)SCG	The IPv6 Address Packet Intercept feature supports lawful intercept of CMs and CPEs provisioned with IPv6 addresses. The following sections provide information about this feature: • IPv6 Address Packet Intercept, on page 122 • Provisioning IPv6 Taps Using SNMPv3, on page 134

CHAPTER 8

Subscriber Management Packet Filtering Extension for DOCSIS 2.0

First Published: December 17, 2008

Last Updated: November 16, 2009

The Cisco universal 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 documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Contents

Prerequisites for Configuring Subscriber Management Packet Filtering

The table shows the hardware compatibility prerequisites for the subscriber management packet filtering feature.

Table 21: Cable Hardware Compatibility Matrix for Subscriber Management Packet Filtering

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB** • PRE2 • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20 Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later Cisco uBR-MC3GX60V [29]

29 Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

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 performance routing engine (PRE) and the standby PRE should be the same before the switchover.

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.

DETAILED STEPS

	Command or Action	Purpose

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

	Command or Action	Purpose

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.

DETAILED STEPS

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

	Command or Action	Purpose
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.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	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.

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 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
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.

Related Documents

Related Topic	Document Title
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference*, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Related Topic	Document Title
Cisco uBR10012 Universal Broadband Router Documentation	*Cisco uBR10012 Universal Broadband Router Hardware Installation Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/guide/hig.html *Cisco uBR10012 Universal Broadband Router Software Configuration Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/configuration/guide/scg.html Cisco uBR10012 Universal Broadband Router Release Notes http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_release_notes_list.html

Standards

Standard	Title
None	

MIBs

MIB	MIBs Link
None	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

RFCs

RFC	Title
None	

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

Command Reference

For information about commands, see the Cisco IOS CMTS Command Reference at http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html . For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the Cisco IOS Master Command List, All Releases, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html .

FeatureInformationforSubscriberManagementPacketFiltering

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

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

Table 22: Feature Information for Subscriber Management Packet Filtering

Feature Name	Releases	Feature Information
Subscriber Management Packet Filtering	12.2(33)SCB	The Cisco universal broadband router supports management of data packet filtering based on the subscriber's preferences and criteria.