Cisco CMTS Troubleshooting and Network Management Features Configuration Guide

First Published: February 14, 2008

Last Modified: January 28, 2016

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-27613-03

CONTENTS

CHAPTER 1

Automatic ROMMON Upgrade For Cable Interface Line Cards

First Published: June 20, 2011

Automatic ROM Monitor (ROMMON) Upgrade feature enables the Cisco uBR10012 cable interface line cards to automatically update the ROMMON image whenever a newer version is available. This document provides information about the Automatic ROMMON Upgrade feature and configuration.

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 Automatic ROMMON Upgrade

Table 1: Cable Hardware Compatibility Matrix for Automatic ROMMON Upgrade for Cable Interface Line Cards, on page 2 shows the hardware compatibility prerequisites for the Automatic ROMMON Upgrade feature.

Table 1: Cable Hardware Compatibility Matrix for Automatic ROMMON Upgrade for Cable Interface Line Cards

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 router	Cisco IOS Release 12.2(33)SCF and later releases • PRE2 • PRE4	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR10-MC5X20H • Cisco UBR-MC20X20V • Cisco uBR-MC3GX60V[1]

[1] Cisco uBR-MC3GX60V cable interface line card is compatible with Performance Routing Engine 4 (PRE4).

Information About Automatic ROMMON Upgrade

The Cisco IOS Release 12.2(33)SCF introduces the Automatic ROMMON Upgrade feature, which enables the cable interface line cards (CLCs) to automatically upgrade the ROMMON image whenever a newer version is available.

The ROMMON is a bootstrap program that initializes the hardware and boots up the Cisco IOS software when the Cisco CMTS (or CLC) is powered on or rebooted. It is an integral part of the CLC firmware, which provides basic services such as CPU initialization, memory mapping, and image relocation.

Two types of ROMMON images exist on CLCs:

- Primary ROMMON image—This is the original image shipped with the system. This is a read-only image that cannot be erased or altered in the field. In case the secondary ROMMON image gets corrupted during upgrade, the primary ROMMON image is used to boot up the CLC.
- Secondary ROMMON image—This is a field upgradeable image which has the latest software version. This image is upgraded by the Automatic ROMMON Upgrade feature.

The ROMMON image may require updates due to feature additions or enhancements. The Automatic ROMMON Upgrade feature enables the CLC to upgrade the secondary ROMMON image without user intervention. The user is informed about the upgrade status through error or warning messages. For more information on the upgrade status, see Verifying Automatic ROMMON Upgrade on a Cable Interface Line Card, on page 5.

Automatic upgrade of the secondary ROMMON image is performed only when the new image version is higher than the current secondary ROMMON image version. For example, if the secondary ROMMON image version is 160, then the ROMMON image upgrade will be performed only if the new image version is 161 or above.

New ROMMON versions are backward compatible. The updated ROMMON image can be used with the older Cisco IOS Release versions. If, for any reasons, older ROMMON version needs to be used, it is possible to downgrade the ROMMON image using the Automatic ROMMON Upgrade feature with few configuration changes.

To downgrade the ROMMON image, the following conditions must be met:

- The Cisco IOS Release version must support Automatic ROMMON Upgrade feature.
- Automatic ROMMON image downgrade must be enabled. See Enabling Automatic ROMMON Downgrade on Cable Interface Line Cards, on page 4.
- The current ROMMON version should be higher than the downgrade version.

Note The updated ROMMON image may contain critical bug fixes and feature enhancements. It is recommended that the ROMMON image is not downgraded, unless it is necessary.

By default, the automatic ROMMON image upgrade and downgrade are disabled for all CLCs. Use the cable linecard auto-rommon-upgrade command to configure automatic ROMMON image upgrade on CLCs. Use cable linecard auto-rommon-downgrade command to configure automatic ROMMON image downgrade on CLCs.

Note Effective with Cisco IOS Release 12.2(33)SCF1, the automatic ROMMON image upgrade is enabled by default.

How to Configure Automatic ROMMON Upgrade on Cable Interface Line Cards

This section describes the following configuration procedures:

Enabling Automatic ROMMON Upgrade on Cable Interface Line Cards

This procedure describes how to enable or disable automatic upgrade of ROMMON images on CLCs.

Note The automatic ROMMON upgrade is disabled by default on all CLCs. To perform automatic ROMMON upgrade on the cable interface line cards, use the cable linecard auto-rommon-upgrade command to enable automatic ROMMON image upgrade on all the line cards and then reload the line cards.

Note Effective with Cisco IOS Release 12.2(33)SCF1, the automatic ROMMON image upgrade is enabled by default.

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 linecard auto-rommon-upgrade **Example:** `Router(config)# cable linecard auto-rommon-upgrade`	Enables automatic ROMMON image upgrade on all CLCs. **Note** Use the no form of this command to disable automatic ROMMON image upgrade on CLC.
Step 4	end **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Examples to Enable Automatic ROMMON Image Upgrade

The following example shows how to enable automatic ROMMON image upgrade on all CLCs:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable linecard auto-rommon-upgrade
Router(config)# end
```

Enabling Automatic ROMMON Downgrade on Cable Interface Line Cards

This procedure describes how to enable or disable automatic downgrade of ROMMON images on CLCs.

Note The automatic ROMMON downgrade is disabled by default on all CLCs, and we recommend that you do not change this default behavior.

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 linecard auto-rommon-downgrade **Example:** `Router(config)# cable linecard auto-rommon-downgrade`	Enables automatic ROMMON image downgrade on all CLCs. **Note** Use the no form of this command to disable automatic ROMMON image downgrade on CLC.
Step 4	end **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Examples for Automatic ROMMON Image Downgrade

The following example shows how to enable automatic ROMMON image downgrade on all CLCs:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable linecard auto-rommon-downgrade
Router(config)# end
```

Verifying Automatic ROMMON Upgrade on a Cable Interface Line Card

On successful automatic ROMMON upgrade (or downgrade), the following two messages are observed in system logs:

- %UBR10KCLC-6-ROMMON_UPDATE_START
- %UBR10KCLC-6-ROMMON_UPDATE_DONE

For more information on these system messages, see the Cisco IOS CMTS Cable System Messages Guide at the following URL:

http://www.cisco.com/en/US/docs/cable/cmts/system/message/uberrmes.html

Troubleshooting Automatic ROMMON Upgrade failures

If automatic ROMMON image upgrade (or downgrade) fails, system error messages indicating one of the following reasons are observed in the system logs:

- ROMMON update disabled—Line card ROMMON update is temporarily disabled due to a limit on unsuccessful attempts. The card may not have the latest firmware
- ROMMON version error—Line card ROMMON version error. The line card may not have the latest version.
- ROMMON update error—Line card ROMMON update error. The line card ROMMON update can fail due to any one of the following reasons:
  - Failure to erase old firmware on the line card.
  - Failure to program new firmware.
  - Line card not responding.
  - Line card timeout.
  - Memory related failure.

If any of these syslog error messages are observed, wait for 10 minutes and then try to reload the CLC. For more information on how to reload a CLC, see:

http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_installation_guides_list.html

If the problem persists collect the output of the show tech-support command. Contact your Cisco technical support representative and provide the representative with the gathered information.

For more information on the exact system error messages observed during ROMMON upgrade (or downgrade) failure, see the Cisco IOS CMTS Cable System Messages Guide at the following URL:

http://www.cisco.com/en/US/docs/cable/cmts/system/message/uberrmes.html

Additional References

Related Documents

Related Topic	Document Title
Cisco CMTS command reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco CMTS System Messages Guide	Cisco IOS CMTS Cable System Messages Guide http://www.cisco.com/en/US/docs/cable/cmts/system/message/uberrmes.html

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

Feature Information for Automatic ROMMON Upgrade

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 Automatic ROMMON Upgrade for Cable Interface Line Card

Feature Name	Releases	Feature Information
Automatic ROMMON Upgrade for Cable Interface Line Cards	12.2(33)SCF	This feature enables the Cisco uBR10012 cable interface line cards to automatically perform ROMMON image upgrade or downgrade. The following commands were introduced: • **cable linecard auto-rommon-upgrade** • **cable linecard auto-rommon-downgrade**

CHAPTER 2

Cable IPC Statistics Collection Tool

First Published: November 16, 2009

Last Updated: November 29, 2010

The Cable Interprocess Communication (IPC) Statistics Collection tool provides debugging information about all CMTS related IPC messages. You can use this tool to analyze the IPC traffic in a cable communications 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 the Cable IPC Statistics Collection Tool

The table shows the hardware compatibility prerequisites for the Cable IPC Statistics Collection tool.

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

Table 3: Hardware Compatibility Matrix for Cable IPC Statistics Collection Tool

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)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 [2]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 • 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 [3]
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

2 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.
3 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 the Cable IPC Statistics Collection Tool

The Cable IPC Statistics Collection tool has the following restrictions:

- Does not support the line cards running LCDOS images.
- Does not support checkpoint messages between the primary route processor (RP) and secondary RP on the Cisco UBR10012 router.

Information About the Cable IPC Statistics Collection Tool

The Cable IPC Statistics Collection tool monitors IPC messages between cable interface line cards and the RP in a cable communications network. The IPC messages include configuration commands, responses to the configuration commands, and other events that a cable interface line card reports to the RP.

The tool provides the following message statistics:

- Send and receive message counts and byte counts.
- Wait time between request sent and response received for blocked request messages.
- Process time used by the message handler for received request messages.

The tool provides the following queue statistics:

- Queue size.
- Wait time from a message that is enqueued to a message that is dequeued.
- Enqueue and dequeue message counts.
- Queue flush message counts.

Note To save system memory and keep the normal operation performance, the Cable IPC Statistics Collection tool is disabled by default. You can enable the tool using the cable ipc-stats command in global configuration mode. When you enable the tool, a new database memory buffer is allocated, and the API functions start updating the statistics database. When you disable the tool, the allocated memory is freed. We recommend that you enable this tool only when it is necessary as the tool consumes considerable amount of CPU memory while running on a Cisco CMTS router. The actual memory usage varies based on how many messages are defined in a particular Cisco IOS image.

How to Enable the Cable IPC Statistics Collection Tool

This section contains the following procedures:

Enabling the Cable IPC Statistics Collection Tool

The cable ipc-stats command is synchronized to all cable interface line cards from the active RP. You do not have to use this command on cable interface line cards separately.

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 ipc-stats** **Example:** `Router(config)# cable ipc-stats`	Enables the Cable IPC Statistics Collection tool on a Cisco CMTS router.

Verifying IPC Statistics

To verify IPC statistics, use the **show cable ipc-stats** command as shown in the following example:

```
Router# show cable ipc-stats
ubr10k2apatil#show cable ipc-stats
--- TIME ---
Start: 03:27:29 PDT Fri Oct 9 2009
End  : 03:28:22 PDT Fri Oct 9 2009
Total: 0 days 00 hrs 00 mins 53 secs (53 seconds)
size : 1407648 bytes
--- CR10K MSG ---
entity app      io    s/s reqid idx:    pkts      bytes lastEvt totalDur maxDur lastMax
                                                        (sec)   (msec)   (msec) (sec)
rp-lc c10k     TxReq 1/0 10241   1:       1         24      17
 rp-lc c10k     TxReq 1/0    10  14:      11        704       0
 rp-lc c10k     TxReq 2/1    10  14:      10        640       4
 rp-lc c10k     TxReq 3/0    10  14:      10        640       4
 rp-lc c10k     TxReq 3/1    10  14:      11        704       0
 rp-lc c10k     TxReq 4/0    10  14:      10        640       3
 rp-lc c10k     TxReq 6/0 10252   2:      10       9376      13
 rp-lc c10k     TxReq 6/0    10  14:      11        704       0
 rp-lc c10k     TxReq 6/1 10252   2:       1         88      53
 rp-lc c10k     TxReq 6/1    10  14:      11        704       0
 rp-lc c10k     TxReq 7/0 10252   2:       7        696       5
 rp-lc c10k     TxReq 7/0    10  14:      11        704       1
 rp-lc c10k     RxRsp 1/0 10241   1:       1          4      17        0      0 17
 rp-lc c10k     RxReq 1/0 10241   1:      60      21816       0        0      0 0
 rp-lc c10k     RxReq 1/0    10  14:      11        704       0        0      0 0
```

```
 rp-lc c10k     RxReq 2/1 10241   1:      26      13468       1        0      0 1
 rp-lc c10k     RxReq 2/1    10  14:      10        640       4        0      0 4
 rp-lc c10k     RxReq 3/0 10241   1:      20       1340       5        0      0 5
 rp-lc c10k     RxReq 3/0    10  14:      10        640       4        0      0 4
 rp-lc c10k     RxReq 3/1    10  14:      11        704       0        0      0 0
 rp-lc c10k     RxReq 4/0 10241   1:      20       1340       9        0      0 9
 rp-lc c10k     RxReq 4/0    10  14:      10        640       3        0      0 3
 rp-lc c10k     RxReq 6/0 10252   2:      13      27080       0        0      0 0
 rp-lc c10k     RxReq 6/0    10  14:      11        748       0        0      0 0
 rp-lc c10k     RxReq 6/1 10252   2:       1         68      25        0      0 25
 rp-lc c10k     RxReq 6/1    10  14:      11        748       0        0      0 0
 rp-lc c10k     RxReq 7/0 10252   2:      11      24548       3        0      0 3
 rp-lc c10k     RxReq 7/0    10  14:      11        748       1        0      0 1
 rp-lc pnego    TxReq 6/0    14   6:       3        363      13
 rp-lc pnego    TxReq 6/1    14   6:       1         30      53
 rp-lc pnego    TxReq 7/0    14   6:       2         62      13
 rp-lc plfm     RxReq 6/0    24  17:       1         12      37        0      0 37
 rp-lc plfm     RxReq 6/0    27  20:      11       1144       0        0      0 0
 rp-lc plfm     RxReq 6/0    28  21:     484      19360       0        0      0 0
 rp-lc plfm     RxReq 6/1    24  17:       1         12      25        0      0 25
 rp-lc plfm     RxReq 7/0    24  17:       1         12      45        0      0 45
 rp-lc plfm     RxReq 7/0    27  20:      10       1040       3        0      0 3
 rp-lc plfm     RxReq 7/0    28  21:     440      17600       3        0      0 3
 rp-lc docsis   TxReq 7/0   118 110:      10         80       5
 rp-lc hccp     TxReq 6/0     8   8:       8       8416      13
 rp-lc hccp     RxReq 6/0     2   2:       1         28      13        0      0 13
--- CR10K TXQ ---
 TXQ_6_0
 enQ: 10 pkts  max Q size 9 at 13 sec ago
 deQ: 10 pkts  max delay 24 msec at 13 sec ago
   delay between (  0,  10) msec:        6 pkts
   delay between ( 10,  20) msec:        3 pkts
   delay between ( 20,  30) msec:        1 pkts
   delay between (  0,   1) sec :       10 pkts
 flush: 0 ptks  0 times
 TXQ_6_1
 enQ: 1 pkts  max Q size 1 at 53 sec ago
 deQ: 1 pkts  max delay 0 msec at 53 sec ago
   delay between (  0,  10) msec:        1 pkts
   delay between (  0,   1) sec :        1 pkts
 flush: 0 ptks  0 times
 TXQ_7_0
 enQ: 7 pkts  max Q size 1 at 5 sec ago
 deQ: 7 pkts  max delay 48 msec at 13 sec ago
   delay between (  0,  10) msec:        1 pkts
   delay between ( 10,  20) msec:        5 pkts
   delay between ( 40,  50) msec:        1 pkts
   delay between (  0,   1) sec :        7 pkts
 flush: 0 ptks  0 times
--- CR10K WATERMARK ---
--- CR10K RXQ ---
 c10k rxq
 enQ: 236 pkts  max Q size 3 at 5 sec ago
 deQ: 236 pkts  max delay 4 msec at 35 sec ago
   delay between (  0,  10) msec:      236 pkts
   delay between (  0,   1) sec :      236 pkts
 flush: 0 ptks  0 times
 cr10k LP rxq
 enQ: 25 pkts  max Q size 1 at 0 sec ago
 deQ: 25 pkts  max delay 0 msec at 0 sec ago
   delay between (  0,  10) msec:       25 pkts
   delay between (  0,   1) sec :       25 pkts
 flush: 0 ptks  0 times
```

Note When you run the show cable ipc-stats command, a separate shadow database buffer is allocated, and the contents of the active database are copied to the shadow database to display the IPC statistics. This ensures that all the statistics are frozen at the same time for easy comparison and analysis. To clear the active database, use the clear cable ipc-stats command in privileged EXEC mode. This command resets all the statistics in the active database to zero.

Configuration Example for the Cable IPC Statistics Collection Tool

The following example shows how to configure the Cable IPC Statistics Collection Tool on a Cisco CMTS router:

```
Router# configure terminal
Router(config)# cable ipc-stats
```

Additional References

The following sections provide references related to the Cable IPC Statistics Collection tool feature.

Related Documents

Related Topic	Document Title
Commands on the Cisco CMTS (universal broadband) routers	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
IPC messages	*Cisco IOS CMTS Cable System Messages Guide* http://www.cisco.com/en/US/docs/cable/cmts/system/message/uberrmes.html

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

Feature Information for the Cable IPC Statistics Collection Tool

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 4: Feature Information for the Cable IPC Statistics Collection Tool

Feature Name	Releases	Feature Information
Cable IPC Statistics Collection tool	12.2(33)SCC	The Cable IPC Statistics Collection tool provides debugging information about all IPC messages. The following sections provide information about this feature: The following commands were introduced: • **cable ipc-stats** • **clear cable ipc-stats** • **show cable ipc-stats**

CHAPTER 3

Cisco CMTS Static CPE Override

First Published: February 14, 2008

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 commands and guidelines for using the Cisco CMTS Static CPE Override feature. This feature enables service technicians to override Dynamic Host Configuration Protocol (DHCP) settings on a subscriber's Customer Premise Equipment (CPE) devices. This feature is used for troubleshooting purposes and to assign static IP addresses at a customer's facility while retaining full and uninterrupted support from the Cisco CMTS.

The cable submgmt default command enables Multiple Service Operators (MSOs) to override network DHCP settings in the Cisco Cable Modem Termination System (CMTS) when performing troubleshooting with a laptop computer from end user facilities.

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 CMTS Static CPE Override

- Cisco IOS software release 12.3(9a)BC or a later BC train release
- A laptop computer
- Ethernet connection cabling
- Remote console access to the Cisco CMTS

Restrictions for CMTS Static CPE Override

Cisco CMTS Static CPE Override is disabled by default, and is enabled with the cable submgmt default command. This feature has the following intentional restrictions:

- This feature supports additional CPE devices with additional MAC addresses to share the IP address and service ID (SID) with the original CPE device. However, CPE devices are limited to 1024 and beyond that, are not supported nor allowed.
- The original CPE device (with the original MAC address and SID) is not allowed behind a different cable modem with the original IP address. If this restriction were not in place, the original cable modem (with the original IP address and SID) would experience interrupted service.
- The original CPE device (with the original MAC and IP address) is not allowed to support a second SID or IP address through a second cable modem.

The impact of this restriction is as follows:

- ◦ A field technician's laptop is allowed to assume an existing IP address and service ID (SID) behind a cable modem on-site.
- At the end of an on-site service session, the CPE device must reclaim its IP address again via DHCP. If this does not occur, the Cisco CMTS presumes that the technician's laptop remains behind the previous cable modem, and the Static CPE override feature will not be available for a future on-site session at another location.

You can override this state with either of the following two methods:

- ◦ Clear the technician's CPE device information from the host routing tables on the Cisco CMTS.
  ◦ Ensure that at the end of an on-site troubleshooting session, the original CPE device reclaims its IP address using DHCP. The technician's (temporary) CPE entry is automatically deleted.

Information About CMTS Static CPE Override

One typical scenario in which DHCP is used with the Cisco CMTS and CPE devices would include the following:

- A CPE device is configured with a dynamic IP address via DHCP from the Cisco CMTS.
- A CPE MAC address is configured behind the cable modem with a service ID (SID) assigned to the IP address.

In this scenario, the cable submgmt default command can be used on the Cisco CMTS to accomplish the following (temporary) changes between the CPE devices and the Cisco CMTS:

- The original CPE device continues to receive service, but is assigned a static IP address from the Cisco CMTS.
- This static IP address overrides the DHCP IP address without first clearing the DHCP CPE device from the CMTS routing tables.
- The original CPE device automatically changes from dhcp cpe to static cpe in the CMTS host routing tables, and the CPE device continues to receive service with the same SID.
- Additional CPE devices can now share the same IP address and SID as the original CPE device.

How to Configure Cisco CMTS Static CPE Override

This section contains the following procedures for the Cisco CMTS Static CPE Override feature:

Enabling and Using Cisco CMTS Static CPE Override

Perform the following steps to enable Cisco CMTS Static CPE Override, and to enable network access of a second CPE device behind a subscriber's cable modem at the customer facility.

Before You Begin

This procedure requires that the field technician already have connected and started a laptop computer at the customer facilities, is connected through the customer's cable modem, and has accessed the Cisco CMTS with remote router console.

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# config t`	Enters global configuration mode.
Step 3	cable submgmt default active **Example:** `Router(config)# cable submgmt default active`	Enables the Cisco CMTS Static CPE Override feature behind the subscriber's cable modem. Additional CPE devices (with additional MAC addresses) are supported behind the subscriber's cable modem, and they inherit the subscriber's current SID settings. **Note** The subscriber's CPE device changes from dhcp cpe to static CPE in the CMTS host table.
Step 4	cable submgmt default filter-group cm (downstream | upstream) **Example:** `Router(config)# cable submgmt default filter group cm downstream`	Enables one or more temporary CPE devices behind a subscriber's cable modem to operate within the cable modem's downstream or upstream filter group.
Step 5	cable submgmt default filter-group cpe {downstream | upstream} **Example:** `Router(config)# cable submgmt default filter-group cpe upstream`	Enables one or more temporary CPE devices behind a subscriber's cable modem to operate within the subscriber's CPE downstream or upstream filter group.
Step 6	cable submgmt default learnable **Example:** `Router(config)# cable submgmt default learnable`	Enables one or more temporary CPE devices behind a subscriber's cable modem to learn and operate within the routing table defined on the Cisco CMTS.
Step 7	cable submgmt default max-cpe n **Example:** `Router(config)# cable submgmt default max-cpe 1024`	Sets the maximum number of CPE devices to be allowed behind a subscriber's cable modem. • n—The number of allowable CPE devices in addition to the subscriber's CPE device(s), with a range from 0 to 1024 devices. Each device inherits the SID settings as defined by the subscriber's current SID.
Step 8	interface slot/[subslot]/port **Example:** `Router(config)# interface 8/1/0`	Enters interface configuration mode for the specified interface. The subslot is required syntax for the Cisco uBR10012 router, but is not used for the Cisco uBR7246VXR or Cisco uBR7100 series routers.

	Command or Action	Purpose
Step 9	(no) ip address ip-address mask [secondary] **Example:** `Router(config-if)# ip address 131.108.1.27 255.255.255.0`	Sets a primary or secondary IP address for a CPE device, use the ip address command in interface configuration mode. To remove an IP address or disable IP processing, use the no form of this command. ip address ip-address mask [secondary] no ip address ip-address mask [secondary] • ip-address—Static IP address for the CPE device. • mask—Mask for the associated IP subnet. • secondary—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
Step 10	Conduct on-site CPE troubleshooting, as required.	For additional troubleshooting guidelines, refer to the Troubleshooting Tips, on page 55.
Step 11	Ctrl-Z **Example:** `Router(config-if)# Ctrl^z`	As required, return to global configuration mode.

Step 12	Do one of the following:
	
	• no cable submgmt default
	•
	• clear cable host
	
	Example:
	
	`Router(config)# cable submgmt default`
	
	Example:
	
	`Router(config)# clear cable host`
		Disables Static CPE override, and returns the on-site CPE device(s) and cable modem to their original DHCP state (dynamic IP address with associated SID).
		
		To clear the CPE cable modem host from the Cisco router's internal address tables, use the clear cable host command in privileged EXEC mode.
		
		clear cable host {ip-address | mac-address}
		
		• ip-address—IP address for the device to be cleared.
		• mac-address—MAC address for the device to be cleared.
		
		For additional command information, refer to the clear cable command in the Cisco Broadband Cable Command Reference Guide on Cisco.com.

Step 13	exit **Example:** `Router(config)# exit`	Returns the prompt to privileged EXEC mode.
Step 14	**quit**	Proper Telnet reconnection to the Cisco router requires proper disconnect during the current Telnet session. Common Telnet disconnect methods are as follows: • Press Ctrl+Break. • Press Ctrl+].

	Command or Action	Purpose
		• Type quit or send break. Another Telnet disconnect method is as follows: Press Ctrl+Shift 6 6 x. For additional Telnet break sequences, refer to the document Standard Break Key Sequence Combinations During Password Recovery on Cisco.com.
Step 15	Type disc 1 from the router command-line interface.	

Examples

The command in the following example enables Cisco CMTS Static CPE Override in the field, enabling more or more additional CPE devices to be added behind a subscriber's cable modem:

```
Router(config)# cable submgmt default active
```

The command in the following example configures the Cisco CMTS to accept a temporary CPE device which inherits and filters by the subscriber's default downstream cable modem group:

```
Router(config)# cable submgmt default filter-group cm downstream
```

The command in the following example configures the Cisco CMTS to accept a temporary CPE device, and to update the temporary CPE device with the current routing table from the Cisco CMTS:

```
Router(config)# cable submgmt default learnable
```

The command in the following example configures the Cisco CMTS to accept a maximum of five temporary CPE devices behind a subscriber's cable modem:

```
Router(config)# cable submgmt default max-cpe 5
```

Troubleshooting with Cisco CMTS Static CPE Override

When Cisco CMTS Static CPE Override has been enabled at the subscriber's facilities, troubleshooting depends on the service or network needs of the situation. For additional information about troubleshooting the Cisco CMTS or customer CPE devices, refer to the Additional References, on page 22.

Additional References

The following sections provide references related to CPE troubleshooting with the Cisco CMTS.

Related Documents

Related Topic	Document Title
Cisco CMTS command reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
CPE troubleshooting information	• *Cisco TAC Technical Notes for the Cisco CMTS:* http://www.cisco.com/c/en/us/tech/broadband-cable/cable-modem-termination-systems-cmts/tech-tech-notes-list.html • *Removing Cable Modem and CPE Entries from the Cisco CMTS, TAC Document ID 4663* http://www.cisco.com/c/en/us/support/docs/broadband-cable/cable-modems/4663-cm-cpe-entries-removed.html • *Troubleshooting Slow Performance in Cable Modem Networks, TAC Document ID 12551:* http://www.cisco.com/c/en/us/support/docs/broadband-cable/cable-modems/12551-troubleshooting-slow-perf.html • Troubleshooting uBR Cable Modems Not Coming Online, TAC Document ID 16510 http://www.cisco.com/c/en/us/support/docs/broadband-cable/cable-modems/16510-troubleshooting-cm-online.html
DHCP configuration information	• "DHCP, ToD, and TFTP Services for the Cisco CMTS" in the Cisco Cable Modem Termination System Feature Guide: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_dhcp.htm

Standards

Standards	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported 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://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 CMTS Static CPE Override

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 Phrase Based on Module Title

Feature Name	Releases	Feature Information
Cisco CMTS Static CPE Override	12.2(33)S	The following command is introduced or modified in the feature or features documented in this module. • **cable submgmt default**

CHAPTER 4

Control Point Discovery on the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: December 17, 2008

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 Control Point Discovery (CPD) feature. This feature, along with Network Layer Signaling (NLS), enables automatic discovery of any control point associated with an end point.

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 Control Point Discovery

The Control Point Discovery feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. The table shows the hardware compatibility prerequisites for this feature.

Table 6: Control Point Discovery Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • PRE-2	Cisco IOS Release 12.2(33)SCA • Cisco uBR10-MC5X20S/U/H
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1	Cisco IOS Release 12.2(33)SCA • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

Restrictions for Control Point Discovery

- The CPD feature does not sync any dynamic CPD/NLS related data between the route processors (RPs). After sending a NLS challenge to the controller, the new active PRE will ignore the NLS response as a result of any RP switchover.
- The CPEs become inaccessible for a small duration during line card switchovers. During this interval, any CPD request received on CMTS will be responded to as if the endpoint is not connected or as if the control relationship is not supported.
- The CPD functionality is restricted to default VPN table id (0).
- Only manual configuration of NLS authentication pass phrase would be supported for CPD/NLS security.
- For NLS authentication, HMAC SHA1 (no configuration option) is used with MAC length truncated to 96 bits.

Information About Control Point Discovery

To configure the Control Point Discovery feature, you should understand the following concepts:

Control Points

Control points are points in a network that can be used to apply certain functions and controls for a media stream. In a cable environment, the control points are Cable Modem Termination Systems (CMTS) and devices that utilizes these control points are referred to as CPD Requestors (or controllers).

Cable CPD Requestors include the following:

- Call Management Server (CMS)
- Policy Server (PS)
- Mediation Device for Lawful Intercept (MD)

Network Layer Signaling (NLS)

Network Layer Signaling (NSL) is an on-path request protocol used to carry topology discovery and other requests in support of various applications. In the CPD feature, NLS is used to transport CPD messages.

NLS for CPD

NLS is used to transport CPD messages. The CPD data is carried under an application payload of the NLS and contains a NLS header with flow id. The NLS flow id is used during NLS authentication to uniquely identify the CPD requests and responses for an end point of interest.

NLS Flags

All NLS headers contain bitwise flags. The CMTS expects the following NLS flag settings for CPD applications:

- HOP-BY-HOP = 0
- BUILD-ROUTE = 0
- TEARDOWN = 0
- BIDIRECTOINAL = 0
- AX_CHALLANGE = 0/1
- AX_RESPONSE = 0/1

Note Any requests with flags other then AX flags, set to one will be rejected with an error indicating a poorly formed message.

NLS TLVs

The following NLS TLVs are supported for all CPD applications:

- APPLICATION_PAYLOAD
- IPV4_ERROR_CODE
- IPV6_ERROR_CODE
- AGID
- A_CHALLENGE
- A_RESPONSE
- B_CHALLENGE
- B_RESPONSE
- AUTHENTICATION
- ECHO

The following NLS TLVs are not supported for CPD applications:

- NAT_ADDRESS
- TIMEOUT
- IPV4_HOP
- IPV6_HOP

Control Point Discovery

The control point discovery feature allows CPD Requestors to determine the control point IP address between the CPD Requestor and the media endpoint.

Using Networking Layer Signaling (NLS), the control point discovery feature sends a CPD message towards the end point (MTA). The edge/aggregation device (CMTS), located between the requestor and the endpoint, will respond to the message with its IP address.

Note For Lawful Intercept, it is important that the endpoint does not receive the CPD message. In this instance, the CMTS responds to the message without forwarding it to its destination.

CPD Protocol Hierarchy

CPD messages are sent over the NLS.

The CPD Protocol Hierarchy is as follows:

1. CPD
2. NLS

3 UDP
4 IP

Note Since NLS is implemented on the UDP protocol, there is a potential of message loss. If messages are lost, the controller will re-send the CPD request in any such event.

Control Relationship

A control relationship between a control point and a controller is identified as a function on a media flow that passes through a control point. A control relationship is uniquely defined by a control relationship type (CR TYPE) and control relationship ID (CR ID). The CR ID is provisioned on CMTS as well as the controller.

The table lists the supported CR TYPEs and corresponding pre-defined CR IDs

Table 7: Supported Control Relationship Types and Corresponding Control Relationship IDs

Control Relationship Type	Pre-Defined Corresponding Control Relationship ID
CR TYPE = 1 (Lawful Intercept)	CR ID = 1: CMTS
	CR ID = 2: Aggregation router or switch in front of CMTS
	CR ID = 3: Aggregation router or switch in front of Media Services
	CR ID = 4: Media Gateway
	CR ID = 5: Conference Server
	CR ID = 6: Other
CR TYPE = 2 (DQoS)	CR ID = 1: CMTS
CR TYPE = 3 (PCMM)	CR ID = 1: CMTS

How to Configure CPD

Enabling CPD Functionality

To enable the CPD functionality, use the cpd command in global configuration mode. The CPD message authentication is determined by NLS configuration.

Before You Begin

The CPD message authentication is determined by NLS 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	**cpd** **Example:** `Router (config)# cpd`	Enables CPD functionality • Us the “no” form of this command to disable CPD functionality.
Step 4	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples for CPD Enable

The following example shows the cpd enabled on a router:

```
Router (config)# cpd
```

Configuring Control Relationship Identifier

To configure a Control relationship identifier (CR ID) for CMTS, use the cpd cr-id command. When CPD request comes with a wild-card CR ID, the CMTS will respond with this configured value.

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	**cpd cr-id** **Example:** `Router (config)# cpd cr-id 100`	Configures a control relationship identifier (CR ID) for CMTS.
Step 4	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the cpd cr-id command configured with a cr-id number of 100 on a router.

```
Router (config)# cpd cr-id 100
```

Enabling NLS Functionality

To enable the NLS functionality, use the nls command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**nls** **Example:** `Router (config)# nls`	Enables NLS functionality. • NLS authentication is optional. • It is recommended that NLS message authentication be enabled at all times.
Step 4	**debug nls** **Example:** `Router# debug nls`	Enables NLS debug functionality.
Step 5	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the nls command enbaled on a router.

```
Router (config)# nls
```

Configuring Authorization Group Identifier and Authentication Key

The Authorization Group Identifier (AG ID) and corresponding authorization key are provisioned on CMTS, as well as on controller/CPD requester.

To configure the Authorization Group Identifier and Authentication Key, use the nls ag-id command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

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	**nls ag-id** **Example:** `Router (config)# nls ag-id 100 auth-key 20`	Configures the Authorization Group Identifier and Authentication Key.
Step 4	**debug nls** **Example:** `Router (config)# debug nls`	Enables NLS debug functionality.
Step 5	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the nls ag-id command with an Authorization Group ID of 100 and Authentication Key of 20.

```
Router (config)# nls ag-id 100 auth-key 20
```

Configuring NLS Response Timeout

The NLS response timeout governs the time CMTS will wait for getting a response for a NLS authentication request.

To configure the NLS response timeout, use the nls ag-id command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

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	**nls resp-timeout** **Example:** `Router (config)# nls resp-timeout 60`	Configures the NLS response time.
Step 4	**debug nls** **Example:** `Router (config)# debug nls`	Enables NLS debug functionality.
Step 5	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the nls resp-timeout command with a response timeout setting of 60 seconds.

```
Router (config)# nls resp-timeout 60
```

Additional References

The following sections provide references related to the CPD feature.

Related Documents

Related Topic	Document Title
CMTS features	• *Cisco IOS CMTS Cable Software Configuration Guide* • Managed Broadband Access Using MPLS VPNs for Cable Multiservice Operators • Transparent LAN Service over Cable • Troubleshooting the System

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Standards

Standard	Title
Internet Draft, Network Layer Signaling: Transport Layer	Internet Draft, Network Layer Signaling: Transport Layer (IETF draft-shore-nls-tl-05.txt)
PacketCable™ Control Point Discovery Interface Specification	PacketCable™ Control Point Discovery Interface Specification (PKT-SP-CPD-I02-061013)

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 Control Point Discovery

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 8: Feature Information for Control Point Discovery

Feature Name	Releases	Feature Information
Control Point Discovery	12.3(21a)BC3	The control point discovery feature allows CPD Requestors to determine the control point IP address between the CPD Requestor and the media endpoint. The following commands were introduced or modified by this feature: • **cpd** • **cpd cr-id** • **debug cpd** • **debug nls** • **nls** • **nls ag-id auth-key** • **nls resp-timeout** • **show cpd** • **show nls** • **show nls ag-id** • **show nls flow**
Control Point Discovery	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 5

Flap List Troubleshooting for the Cisco CMTS

First Published: February 14, 2008

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 how to configure and use the Flap List Troubleshooting feature on the Cisco Cable Modem Termination System (CMTS) routers. The flap list is a patented tool for the Cisco CMTS routers to diagnose potential problems with a particular cable modem or with a particular cable interface. The flap list tracks "flapping" cable modems, which are cable modems that have intermittent connectivity problems. Excessive flapping could indicate a problem with a particular cable modem or with the upstream or downstream portion of the cable plant.

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 Flap List Troubleshooting

- To configure and access the flap list using SNMP commands, you must be using an SNMPv3 manager and have configured the Cisco CMTS router for SNMP operations.

Restrictions for Flap List Troubleshooting

- The Cisco CMTS should be running the latest Cisco IOS Release 12.1 EC or Cisco IOS Release 12.2 EC, or later, release.
- The Flap List Troubleshooting feature can be used only with two-way cable modems. The flap-list does not support telco-return cable modems or set-top boxes.

Note Since the cable flap list was originally developed, polling mechanisms have been enhanced to have an increased rate of 1/sec when polls are missed. Cable modems can go offline faster than the frequency hop period, which can cause the frequency to stay fixed while cable modems go offline. To compensate for this, reduce the hop period to 10 seconds.

Information About Flap List Troubleshooting

This section describes the following information about the Flap List Troubleshooting feature:

Feature Overview

The Flap List Troubleshooting is a patented tool that is incorporated in the Cisco IOS software for the Cisco Cable Modem Termination System (CMTS) routers. The flap list tracks “flapping” cable modems, which are cable modems that have intermittent connectivity problems. A flapping cable modem can indicate either a problem with that particular cable modem, or it could indicate an RF noise problem with the upstream or downstream portion of the cable plant.

The flap-list feature supports any cable modem that conforms to the Data-over-Cable Service Interface Specifications (DOCSIS) because it does use any special messaging to poll cable modems or to request any special information from them. Instead, this feature monitors the normal registration and station maintenance activity that is already performed over a DOCSIS cable network.

This allows the Cisco CMTS to collect the flap-list data without generating additional packet overhead and without impacting network throughput and performance. It also means that although the Flap List Troubleshooting feature is a proprietary feature for Cisco CMTS routers, it is compatible with all DOCSIS-compliant cable modems. In addition, unlike other monitoring methods that use the Simple Network Management Protocol (SNMP), the flap list uses zero bandwidth.

Information in the Flap List

The Flap List Troubleshooting feature tracks the following situations:

- Reinsertions—A reinsertion occurs when the cable modem re-registers more frequently than the user-specified insertion time. A pattern of reinsertions can indicate either potential problems in the downstream or that the cable modem is being improperly provisioned.
- Hits and Misses—A hit occurs when a cable modem successfully responds to the station maintenance messages (MAC-layer "keepalive" messages) that the Cisco CMTS sends out to conform to the DOCSIS standard. A miss occurs when the cable modem does not respond to the request within the user-specified timeout period. A pattern of misses can indicate a potential problem in either the downstream or upstream path, or that a problem can be occurring in the registration process.
- Power Adjustments—DOCSIS cable modems can adjust their upstream transmission power levels to adjust to unstable cable plant signal levels, up to a maximum allowable power level. Repeated power adjustments usually indicate a problem with an amplifier in the upstream return path.

The flap-list feature is automatically enabled, but to use the flap list effectively, the cable system administrator should also typically do the following:

- Set up a script to periodically poll the flap list, for example, every 15 minutes.
- Examine the resulting data and perform trend analysis to identify cable modems that are consistently in the flap list.
- Query the billing and administrative database for cable modem MAC address-to-street address translation and generate a report. The reports can be given to the customer service department or the cable plant's operations and maintenance department. Using these reports, maintenance personnel can quickly discern how characteristic patterns of flapping cable modems, street addresses, and flap statistics indicate which amplifier or feeder lines are faulty. The reports also help to quickly discern whether problems exist in your downstream or upstream path and whether the problem is ingress noise or equipment related.

The flap list provides a quick way to quickly diagnose a number of possible problems. For example, if a subscriber reports a problem, but the flap list for the cable interface that is providing services to them shows little or no flap-list activity, the cable technician can assume that the Cisco CMTS and cable plant are communicating reliably. The problem, therefore, is probably in the subscriber's computer equipment or in the local connection to the cable modem.

Similarly, a cable technician can use the pattern of reinsertions, hits and misses, and power adjustments to quickly troubleshoot the following types of problems:

- If a subscriber's cable modem shows a lot of flap-list activity, it is having some kind of communication problem. Either the cable modem's hardware is faulty, its installation is faulty, the coaxial cable being used is faulty, or some portion of the cable plant that services this cable modem is faulty.
- Focus on the top 10 percent of cable modems that are most active in the flap list, since these are the most likely to indicate consistent and pervasive plant or equipment problems that will continue to disrupt communication with the headend.
- Cable modems with more than 50 power adjustments per day have a suspect upstream path.
- Cable modems with approximately the same number of hits and misses and with a lot of insertions have a suspect downstream path (for example, low level into the cable modem).

- All cable modems incrementing the insertion at the same time indicates a problem with the provisioning servers.
- Cable modems with high cyclic redundancy check (CRC) errors have bad upstream paths or in-home wiring problems.
- Correlating cable modems on the same physical upstream port with similar flap-list statistics can quickly resolve outside plant problems to a particular node or geography.

In addition, the cable network administrators can use the flap list to collect quality control and upstream performance data. Typically, the network operations center (NOC) saves the flap list to a database on a local computer on a daily basis, providing the ability to generate reports that track upstream performance and installation quality control, as well as to provide trend reports on cable plant problems.

Tip The system supports automatic power adjustments. The show cable flap-list and show cable modem commands indicate when the headend cable router has detected an unstable return path for a particular modem and has compensated with a power adjustment. An asterisk (*) appears in the power-adjustment field for a modem when a power adjustment has been made; an exclamation point (!) appears when the modem has reached its maximum power-transmit level and cannot increase its power level any further.

Cisco Cable Manager and Cisco Broadband Troubleshooter

The Flap List Troubleshooting feature is supported by Cisco Cable Manager (CCM), Release 2.0 or later, which is a UNIX-based software suite that manages routers and DOCSIS-compliant cable modems, generates performance reports, troubleshoots connectivity problems, views the network graphically, and edits DOCSIS configuration files. You can access the CCM locally from the CCM server console or remotely from a UNIX workstation or a PC.

The Flap List Troubleshooting feature also works together with the Cisco Broadband Troubleshooter (CBT), which is a graphical-based application to manage and diagnose problems on the hybrid fiber-coaxial (HFC) network. Radio frequency (RF) technicians can quickly isolate plant and provisioning problems and characterize upstream and downstream trouble patterns, including analyzing flapping modems.

Benefits

The Flap List Troubleshooting feature is a proactive way to manage and troubleshoot problems on an HFC network. Its use of passive monitoring is more scalable and efficient than techniques that send special messages to cable modems or that regularly poll the cable modems using Simple Network Management Protocol (SNMP) commands. Because it uses mechanisms that already exist in a DOCSIS network, it can be used with any DOCSIS-certified cable modem or set-top box.

The flap list provides a cable technician with both real-time and historical cable health statistics for quick, accurate problem isolation and network diagnosis. Using the flap list, a cable technician is able to do the following:

- Quickly learn how to characterize trouble patterns in the hybrid fiber-coaxial (HFC) network.
- Determine which amplifier or feeder line is faulty.
- Distinguish an upstream path problem from a downstream one.

- Isolate an ingress noise problem from a plant equipment problem.

How to Configure Flap List Troubleshooting

This section describes how to configure the flap list operation on the Cisco CMTS. You can use either the command-line interface (CLI) commands or Simple Network Management Protocol (SNMP) commands to configure the flap list, to remove a cable modem from the list, or to clear the flap-list counters.

Configuring Flap List Operation Using the CLI (optional)

To configure the operation of the flap list, use the following procedure, beginning in EXEC mode. This procedure is optional, unless you want to change the default values for the flap list.

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 flap-list insertion-time** *seconds* **Example:** `Router(config)# cable flap-list insertion-time 3600`	(Optional) Specifies the minimum insertion (registration) time interval in seconds. Any cable modem that makes a registration request more frequently than this period of time is placed in the flap list.
Step 4	**cable flap-list power-adjust threshold** *db* **Example:** `Router(config)# cable flap-list power-adjust threshold 5`	(Optional) Specifies the minimum power adjustment, in dB, that constitutes a flap-list event. **Note** A threshold of less than 2 dB can cause excessive flap-list event recording. If you need to change this parameter from its default, Cisco recommends setting it to 3 dB or higher.
Step 5	**cable flap-list miss-threshold** *misses* **Example:** `Router(config)# cable flap-list`	(Optional) Specifies the number of MAC-layer station maintenance (keepalive) messages that can be missed in succession before the CMTS places the cable modem in the flap list. **Note** A high miss rate indicates potential plant problems, such as intermittent upstream problems, fiber laser clipping, or common-path distortion.

	Command or Action	Purpose
	`miss-threshold 10`	
Step 6	**cable flap-list aging** *minutes* **Example:** `Router(config)# cable flap-list aging 20160`	(Optional) Specifies how long, in minutes, the Cisco CMTS should keep information for cable modems in the flap list.
Step 7	**cable flap-list size** *number* **Example:** `Router(config)# cable flap-list size 4000`	Specifies the maximum number of cable modems that can be kept in the flap list. **Tip** To avoid wasting processor memory, do not set this value beyond the actual number of cable modems being serviced by the Cisco CMTS.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Clearing the Flap List and Counters Using the CLI (optional)

To clear one or more cable modems from the flap list, or to clear the flap list counters for one or more cable modems (while still keeping the modems in the flap list), use the following procedure, beginning in EXEC mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear cable flap-list** *mac-addr* | **all**} [**save-counters**] **Example:** `Router# clear cable flap-list 0102.0304.0506 save-counters`	Clears one or all cable modems from the flap list.

	Command or Action	Purpose
	Example: `Router# clear cable flap-list 000C.0102.0304`	

Step 3	**clear cable modem** {*mac-addr* | *ip-addr* | [**cable** *interface*] **all** | **oui***string* | **reject**} } **counters**
	Example:
	`Router# clear cable modem 172.12.23.45 counters`
	Example:
	`Router# clear cable modem oui Cisco counters`
	Example:
	`Router# clear cable modem reject counters`
	Example:
	`Router# clear cable modem c4/0 counters`
	Example:
		Sets the flap-list counters to zero for one or more CMs.

Enabling or Disabling Power Adjustment Using the CLI (optional)

The Cisco CMTS can automatically monitor a cable modem's power adjustments and determine whether a particular cable modem requires a chance in the power adjustment method. To enable a cable interface to make automatic power adjustments, and to set the frequency threshold for when those adjustments are made, use the following procedure, beginning in EXEC mode.

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *x/y* **Example:** `Router(config)# interface cable 4/0`	Enters cable interface configuration mode for the specified cable interface.

Step 4	**cable upstream** *n* **power-adjust** {**continue** *pwr-level* | **noise** *perc-pwr-adj* | **threshold value**}
	
	Example:
	
	`Router(config-if)# cable upstream 0 power-adjust threshold 2`
	
	Example:
	
	`Router(config-if)# cable upstream 0 power-adjust noise 50`
		Enables automatic power adjustment on an upstream port for this cable interface.
		
		Note Repeat 4 for each upstream port on the cable interface.

Step 5	**cable upstream** *n* **freq-adj averaging** *percent* **Example:** `Router(config-if)# cable upstream 0 freq-adj averaging 50`	Specifies the percentage of frequency adjustment packets needed to change the adjustment method from the regular power-adjustment method to the automatic power adjustment method.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

What to Do Next

Caution The default settings are adequate for system operation. Amplitude averaging is an automatic procedure. In general, Cisco does not recommend that you adjust values. Cisco does recommend, however, that you clean up your cable plant should you encounter flapping cable modems.

Note In some instances, you might adjust certain values for the **cable upstream power-adjust** command: If CMs cannot complete ranging because they have reached maximum power levels, increase the **continue** *pwr-level* parameter beyond the default value of 2 dB. Values larger than 10 dB on "C" versions of cable interface line cards, or 5 dB on FPGA versions, are not recommended. If the flap list shows CMs with a large number of power adjustments, but the CMs are not detected as "noisy," decrease the **noise** *perc-pwr-adj* value. If too many CMs are unnecessarily detected as "noisy," increase the percentage.

Configuring Flap List Operation Using SNMP (optional)

To configure the Flap List Troubleshooting feature on the Cisco CMTS using SNMP, set the appropriate cssFlapObjects attributes in the CISCO-CABLE-SPECTRUM-MIB. the table lists each of the configurable attributes:

Table 9: Flap-List Configuration Attributes

Attribute	Type	Range	Description
ccsFlapListMaxSize	Integer32	1 to 65536[4]	The maximum number of modems that a flap list can support per line card. The default is 100.[5]
ccsFlapListCurrentSize	Integer32	1 to 65536	The current number of modems in the flap list.[6]
ccsFlapAging	Integer32	1 to 86400	The flap entry aging threshold in minutes. The default is 10080 minutes (180 hours or 7 days).
ccsFlapInsertionTime	Integer32	60 to 86400	The worst-case insertion time, in seconds. If a cable modem has not completed the registration stage within this interval, the cable modem is inserted into the flap list. The default value is 90 seconds.

Attribute	Type	Range	Description
ccsFlapPowerAdjustThreshold	Integer32	1 to 10	When the power of the modem is adjusted beyond the power adjust threshold, the modem is inserted into the flap list.
ccsFlapMissThreshold	Unsigned32	1 to 12	When a cable modem does not acknowledge this number of consecutive MAC-layer station maintenance (keepalive) messages, the cable modem is placed in the flap list.

[4] The allowable range when using SNMP for these parameters is 1 to 65536 (a 32-bit value), but the valid operational range is 1 to 8191.
[5] This value is the same as set by the **cable flap-list size** command and is applied only to the command output. The flap list entries displayed via SNMP are not affected by this.
[6] The number of SNMP entries is the same as this value. The number of the CLI entries depends on the value set by **ccsFlapListMaxSize**.

Note **ccsFlapListMaxSize** controls the display of the flap list per downstream cable interface. As long as the number of flap list entries per line card does not exceed 8191, these entries will be stored in the system, and will not be displayed via CLI.

ccsFlapListCurrentSize reflects the number of flap list entries of all the line cards that in the system, regardless of their visibility to the CLI.

Clearing the Flap List and Counters Using SNMP (optional)

To remove a cable modem from the flap list or to clear one or all of the flap-list counters, set the appropriate cssFlapObjects attributes in the CISCO-CABLE-SPECTRUM-MIB. the table lists the attributes that clear the SNMP counters.

Table 10: Attributes to Clear the Flap List

Attribute	Type	Description
ccsFlapResetAll	Boolean	Setting this object to True (1) resets all flap-list counters to zero.
ccsFlapClearAll	Boolean	Setting this object to True (1) removes all cable modems from the flap list, and destroys all entries in the ccsFlapTable. If a modem keeps flapping, the modem is added again into the flap list as a new entry.

Note The ccsFlapLastClearTime attribute contains the date and time that the entries in the ccsFlapTable table were last cleared.

How to Monitor and Troubleshoot Using Flap Lists

Displaying the Flap List Using the show cable flap-list Command

To display the current contents of the flap list, use the show cable flap-list command in privileged EXEC mode. This command has the following syntax:

- **show cable flap-list—**Displays the complete flap list.
- **show cable flap-list sort-interface—**Displays the complete flap list sorted by cable interface.
- **show cable flap-list cable** *interface* **upstream** *port***—**Displays the flap list for a specific cable interface, or for a specific upstream port on that cable interface.

To change the way the output is sorted, add one of the following optional keywords:

- **sort-flap—**Sorts the output by the number of times that the cable modem has flapped.
- **sort-time—**Sorts the output by the most recent time that the cable modem flapped.

The following example shows typical output of the **show cable flap-list** command.

```
Router# show cable flap-list
Mac Addr       CableIF Ins    Hit   Miss    CRC  P-Adj   Flap    Time
0010.9500.461f C1/0 U1 56  18857    887      0      1    116 Jun 1  14:09:12
0010.9500.446e C1/0 U1 38  18686   2935      0      1     80 Jun 2  19:03:57
0010.9500.38ec C1/0 U2 63  18932   1040      0      8    138 Jun 2  23:50:53
0010.9500.4474 C1/0 U2 65  18913   1053      0      3    137 Jun 2  09:30:09
0010.9500.4672 C1/0 U2 56  18990   2327      0      6    124 Jun 2  10:44:14
0010.9500.38f0 C1/0 U2 50  18964   2083      0      5    111 Jun 2  20:46:56
0010.9500.e8cb C1/0 U2  0   6537    183      0      1      5 Jun 2  22:35:48
0010.9500.38f6 C1/0 U3 50  19016   2511      0      2    104 Jun 2  07:46:31
0010.9500.4671 C1/0 U3 43  18755   3212      1      1     89 Jun 1  19:36:20
0010.9500.38eb C1/0 U0 57  36133   1608      0      6    126 Jun 2  20:04:58
0010.9500.3ce2 C1/0 U0 44  35315   1907      0      4     99 Jun 2  16:42:47
0010.9500.e8d0 C1/0 U2  0  13213    246      0      1      5 Jun 3  04:15:30
0010.9500.4674 C1/0 U2 56  36037   2379      0      4    121 Jun 3  00:34:12
0010.9500.4677 C1/0 U2 40  35781   2381      0      4     91 Jun 2  12:14:38
0010.9500.4614 C1/0 U2 40  21810   2362      0    502    586 Jun 2  21:43:02
0010.9500.3be9 C1/0 U2 63  22862    969      0      0    128 Jun 1  14:09:03
0010.9500.4609 C1/0 U2 55  22723   2127      0      0    112 Jun 1  14:08:02
0010.9500.3cb8 C1/0 U2 49  22607   1378      0      0    102 Jun 1  14:08:58
0010.9500.460d C1/0 U3 46  22477   2967      0      2     96 Jun 2  17:03:48
0010.9500.3cba C1/0 U3 39  22343   3058      0      0     81 Jun 1  14:13:16
0010.9500.3cb4 C1/0 U3 38  22238   2936      0      0     79 Jun 1  14:09:26
0010.9500.4612 C1/0 U3 38  22306   2928      0      0     79 Jun 1  14:09:29
Router#
```

Displaying the Flap List Using the show cable modem flap Command

To display the contents of the flap list for a specific cable modem, use the **show cable modem flap** command in privileged EXEC mode. This command has the following syntax:

- **show cable modem** [*ip-address* | *mac-address*] **flap—**Displays the flap list for a specific cable modem, as identified by its IP address or MAC address.
- **show cable modem cable***interface* [**upstream** *port*] **flap—**Displays the flap list for all cable modems on a specific cable interface.

Note The **show cable modem flap** command displays information similar to that shown by the **show cable flap-list** command, except it displays this information on a per-modem basis.

The following example shows sample output for the **show cable modem flap** command for a particular cable modem:

```
Router# show cable modem 0010.7bb3.fcd1 flap
MAC Address    I/F       Ins   Hit   Miss  CRC   P-Adj   Flap  Time
0010.7bb3.fcd1 C5/0/U5   0     36278 92    0     369     372   Jun 1  13:05:23 (18000msec)
```

The following example shows sample output for the **show cable modem flap** command for all cable modems on a specific cable interface:

```
Router# show cable modem cable 6/0/0 flap
MAC Address    I/F           Ins   Hit   Miss  CRC   P-Adj   Flap  Time
0025.2e34.4386 C6/0/0/U0     0     46778 3980  0      0      0     (14212 msec)
0025.2e2f.d4b6 C6/0/0/U0     0     48002 1899  0      0      0     (18000 msec)
0025.2e2f.d4de C6/0/0/U0     0     48098 1889  0      0      0     (19552 msec)
0023.bee1.e96b C6/0/0/U0     0     46658 4351  0      0      0     (22432 msec)
0025.2e2f.d4d8 C6/0/0/U0     0     21979 781   0      0      0     ( -- )
0025.2e2f.d48c C6/0/0/U0     0     48048 1835  0      0      0     ( -- )
0025.2e2f.d490 C6/0/0/U0     0     48029 1819  0      0      0     ( -- )
```

Displaying the Flap List Using SNMP

To display the contents of the flap list using SNMP, query the ccsFlapTable table in the CISCO-CABLE-SPECTRUM-MIB. This table contains an entry for each cable modem. the table briefly describes each attribute in this table.

Table 11: cssFlapTable Attributes

Attribute	Type	Description
cssFlapMacAddr	MacAddress	MAC address of the cable modem's cable interface. Identifies a flap-list entry for a flapping cable modem.
ccsFlapUpstreamIfIndex	InterfaceIndex	Upstream being used by the flapping cable modem.

Attribute	Type	Description
ccsFlapDownstreamIfIndex	InterfaceIndex	Downstream being used by the flapping cable modem.
ccsFlapLastFlapTime	DateAndTime	Time stamp for the last time the cable modem flapped.
ccsFlapCreateTime	DateAndTime	Time stamp that this entry was added to the table.
ccsFlapRowStatus	RowStatus	Control attribute for the status of this entry.
ccsFlapInsertionFailNum	Unsigned32	Number of times the CM comes up and inserts itself into the network. This counter is increased when the time between initial link establishment and a reestablishment was less than the threshold parameter configured using the **cable flap-list insertion-time** command or ccsFlapInsertionTime attribute. When the cable modem cannot finish registration within the insertion time (ccsFlapInsertionTime), it resends the Initial Maintenance packet. When the CMTS receives the packet sooner than expected, the CMTS increments this counter.
ccsFlapHitNum	Unsigned32	Number of times the CM responds to MAC-layer station maintenance (keepalive) messages. (The minimum hit rate is once per 30 seconds.)
ccsFlapMissNum	Unsigned32	Number of times the CM misses and does not respond to a MAC-layer station maintenance (keepalive) message. An 8 percent miss rate is normal for the Cisco cable interface line cards. If the CMTS misses a ranging request within 25 msec, then the miss number is incremented.
ccsFlapCrcErrorNum	Unsigned32	Number of times the CMTS upstream receiver flagged a packet with a CRC error. A high value indicates that the cable upstream may have a high noise level. The modem may not be flapping yet, but this could become a possible problem.

Attribute	Type	Description
ccsFlapPowerAdjustmentNum	Unsigned32	Number of times the cable modem upstream transmit power is adjusted during station maintenance. When the adjustment is greater than the power-adjustment threshold, the number is incremented.
ccsFlapTotalNum	Unsigned32	Number of times a modem has flapped, which is the sum of the following: • When ccsFlapInsertionFailNum is increased • When the CMTS receives a miss followed by a hit • When ccsFlapPowerAdjustmentNum is increased
ccsFlapResetNow	Boolean	Setting this object to True (1) resets all flap-list counters to zero.
ccsFlapLastResetTime	DateAndTime	Time stamp for when all the counters for this particular entry were reset to zero.

Displaying Flap-List Information for Specific Cable Modems

To use SNMP requests to display flap-list information for a specific cable modem, use the cable modem's MAC address as the index to retrieve entries from the ccsFlapTable. Use the following procedure to retrieve flap-list entries for a particular cable modem.

Step 1 Convert the cable modem's MAC address into a dotted decimal string. For example, the MAC address 000C.64ff.eb95 would become 0.12.100.255.235.149.

Step 2 Use the dotted decimal version of the MAC address as the instance for requesting information from the ccsFlapTable. For example, to retrieve the ccsFlapHits, ccsFlapMisses, and ccsFlapPowerAdjustments values for this cable modem, you would make an SNMP request for the following objects:

- ccsFlapHits.0.12.100.255.235.149
- ccsFlapMisses.0.12.100.255.235.149
- ccsFlapPowerAdjustments.0.12.100.255.235.149

Example

Assume that you want to retrieve the same flap-list information as the **show cable flap-list** command for a cable modem with the MAC address of 000C.64ff.eb95:

```
Router# show cable flap-list
MAC Address     Upstream     Ins   Hit   Miss  CRC   P-Adj Flap  Time
000C.64ff.eb95  Cable3/0/U4  3314  55605 50460 0    *42175 47533 Jan 27 02:49:10
Router#
```

Use an SNMP tool to retrieve the ccsFlapTable and filter it by the decimal MAC address. For example, using the standard Unix **getone** command, you would give the following command:

```
csh% getmany -v2c 192.168.100.121 public ccsFlapTable | grep 0.12.100.255.235.149

ccsFlapUpstreamIfIndex.0.12.100.255.235.149 = 15
ccsFlapDownstreamIfIndex.0.12.100.255.235.149 = 17
ccsFlapInsertionFails.0.12.100.255.235.149 = 3315
ccsFlapHits.0.12.100.255.235.149 = 55608
ccsFlapMisses.0.12.100.255.235.149 = 50460
ccsFlapCrcErrors.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustments.0.12.100.255.235.149 = 42175
ccsFlapTotal.0.12.100.255.235.149 = 47534
ccsFlapLastFlapTime.0.12.100.255.235.149 = 07 d4  01 1b   02 33  1a 00
ccsFlapCreateTime.0.12.100.255.235.149 = 07 d4  01 16   03 23  22 00
ccsFlapRowStatus.0.12.100.255.235.149 = active(1)
ccsFlapInsertionFailNum.0.12.100.255.235.149 = 3315
ccsFlapHitNum.0.12.100.255.235.149 = 55608
ccsFlapMissNum.0.12.100.255.235.149 = 50460
ccsFlapCrcErrorNum.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustmentNum.0.12.100.255.235.149 = 42175
ccsFlapTotalNum.0.12.100.255.235.149 = 47534
ccsFlapResetNow.0.12.100.255.235.149 = false(2)
ccsFlapLastResetTime.0.12.100.255.235.149 = 07 d4  01 16   03 20  18 00
csh%
```

To request just one particular value, use the decimal MAC address as the instance for that object:

```
csh% getone -v2c 172.22.85.7 public ccsFlapMisses.0.12.100.255.235.149

ccsFlapMisses.0.12.100.255.235.149 = 50736
csh %
```

Troubleshooting Suggestions

This section provides tips on how to interpret the flap-list counters, as well as how to determine the optimum power level for a flapping cable modem.

Troubleshooting Tips

This section includes suggestions on how to interpret different network conditions based on the flap-list statistics:

- Condition 1: Low miss or hit ratio (< 2 percent for a Cisco uBR-MC16 card), low insertion, low P-Adj, low flap counter, and old time stamp. Analysis: This exhibits an optimal network situation.
- Condition 2: High ratio of misses over hits (> 10 percent). Analysis: Hit and miss analysis should be done after the Ins count stops incrementing. In general, if the hit and miss counts are about the same

order of magnitude, the upstream can be experiencing noise. If the miss count is greater, then the modem is probably dropping out frequently and not completing registration. The upstream or downstream might not be stable enough for reliable link establishment. Very low hits and miss counters and high insertion counters indicate provisioning problems.

- Condition 3: Relatively high power-adjustment counter. Analysis: Indicates that the power-adjustment threshold is probably set at default value of 2 dB. The modem transmitter step size is 1.5 dB, but the headend can command 0.25 dB step sizes. Tuning your power threshold to 6 dB is recommended to decrease irrelevant entries in the flap list. The power-adjustment threshold can be set using cable flap power threshold <0-10 dB> in the Cisco IOS global configuration mode. A properly operating HFC network with short amplifier cascades can use a 2 to 3 dB threshold.
- Condition 4: High P-Adj and CRC errors. Analysis: This condition can indicate that the fiber node is clipping the upstream return laser. Evaluate the modems with the highest CRC count first. If the modems are not going offline (Ins = 0), this is not noticed by subscribers. However, they could receive slower service due to dropped IP packets in the upstream. This condition also results in input errors on the Cisco CMTS router cable interface.
- Condition 5: High insertion rate. Analysis: If link reestablishment happens too frequently, the modem is usually having a registration problem. This is indicated by a high Ins counter, which tracks the Flap counter.

Performing Amplitude Averaging

The CMTS uses an averaging algorithm to determine the optimum power level for a cable modem with low carrier-to-noise ratio that is making excessive power adjustments—known as flapping. To avoid dropping flapping cable modems, the CMTS averages a configurable number of RNG-REQ messages before it makes power adjustments. By compensating for a potentially unstable return path, the CMTS maintains connectivity with affected cable modems. You can interpret these power adjustments, however, as indicating unstable return path connections.

The **show cable flap-list** and **show cable modem** commands are expanded to indicate to which paths the CMTS is making power adjustments and which modems have reached maximum transmit power settings. These conditions indicate unstable paths that should be serviced.

The following example shows the output of the **show cable flap-list** command:

```
Router# show cable flap-list
MAC Address     Upstream     Ins   Hit   Miss  CRC   P-Adj Flap  Time
 0010.7bb3.fd19  Cable1/0/U1  0     2792  281   0    *45    58    Jul 27 16:54:50
 0010.7bb3.fcfc  Cable1/0/U1  0     19    4     0    !43    43    Jul 27 16:55:01
 0010.7bb3.fcdd  Cable1/0/U1  0     19    4     0    *3     3     Jul 27 16:55:01
```

The asterisk (*) indicates that the CMTS is using the power-adjustment method on this modem. An exclamation point (!) indicates that the modem has reached maximum transmit power.

Output of the **show cable modem** command appears below:

```
Router# show cable modem
 Interface   Prim Online     Timing Rec    QoS CPE IP address      MAC address
             Sid  State      Offset Power
 Cable1/0/U0 1    online     2257    0.00  3   0   10.30.128.142   0090.8330.0217
 Cable1/0/U0 2    online     2262  *-0.50  3   0   10.30.128.145   0090.8330.020f
 Cable1/0/U0 3    online     2260    0.25  3   0   10.30.128.146   0090.8330.0211
 Cable1/0/U0 4    online     2256   *0.75  3   0   10.30.128.143   0090.8330.0216
 Cable1/0/U0 5    online     2265   *0.50  3   0   10.30.128.140   0090.8330.0214
 Cable1/0/U0 6    online     2256    0.00  3   0   10.30.128.141   0090.8330.0215
 Cable1/0/U0 7    online     4138  !-1.00  3   1   10.30.128.182   0050.7366.124d
```

```
Cable1/0/U0 8    online     4142  !-3.25  3   1   10.30.128.164   0050.7366.1245
Cable1/0/U0 9    online     4141  !-3.00  3   1   10.30.128.185   0050.7366.17e3
Cable1/0/U0 10   online     4142  !-2.75  3   0   10.30.128.181   0050.7366.17ab
Cable1/0/U0 11   online     4142  !-3.25  3   1   10.30.128.169   0050.7366.17ef
```

Similar to the **show cable flap-list** command display, the * symbol in the **show cable modem** command output indicates that the CMTS is using the power-adjustment method on this CM. The ! symbol indicates that the CM has reached maximum transmit power.

Using Other Related Commands

The following related Cisco IOS commands can be used to do maintenance on or display information about a cable modem.

- The following clears the counters for a cable modem (or all cable modems) in the station maintenance list:

```
clear cable modem {mac-addr | ip-addr | all} counters
```

- The following displays the QoS, modem status, In and Out octets, IP and MAC addresses per SID:

```
show int cable slot/port sid
```

- The following drops the modem's RF link by removing a modem from the keepalive polling list. This forces the modem to reset. Note the warning below.

```
clear cable-modem {mac-addr | ip-addr | all} reset
```

Tip The **clear cable-modem** *all* **reset** command causes all modems to go offline and disrupt service for your users. It is best used in a test or nonproduction environment.

- The following uses a MAC-layer ping to determine if the cable modem is online. It uses smaller data units on the wire than a standard IP ping, resulting in lower overhead. This command works even if the IP layer in the modem is down or has not completed registration:

```
ping DOCSIS cable-modem mac-addr | IP address
```

- The following displays the timing offset, receive power, and QoS values by cable interface, SID, and MAC address:

```
show cable modem [ip-address | MAC-address]
```

- The following displays the current allocation table and frequency assignments:

```
show cable spectrum-group [spectrum group number]
```

- The following displays maximum, average, and minimum percent of online time and offline time for a given SID on a given cable router interface:

```
show int slot/port sid connectivity
```

- The following command displays input and output rates, input errors, CRC, frames, overruns, underruns, collisions, interface resets. High input errors in the CMTS retrieved from this query suggest noisy upstream. In older versions of the chassis, loose midplane and line card screws caused a similar problem:

```
show interface slot/downstream-port
```

- The following command displays upstream packet discards, errors, error-free packets, correctable and uncorrectable errors, noise, and micro-reflection statistics.

```
show interface slot/downstream-port upstream
```

Configuration Examples for Flap List Troubleshooting

The following excerpt from a configuration file shows a typical flap-list configuration:

```
!
cable flap-list insertion-time 120
cable flap-list power-adjust threshold 3
cable flap-list miss-threshold 4
cable flap-list aging 8
cable flap-list size 8191
...
```

Additional References

For additional information related to the Flap List Troubleshooting feature, refer to the following references:

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco CMTS Cable Command Reference
Cisco Broadband Troubleshooter	http://www.cisco.com/c/en/us/support/cloud-systems-management/broadband-troubleshooter/tsd-products-support-series-home.html

Standards

Standards[7]	Title
ANSI/SCTE 22-1 2012 (formerly SP-RFI-C01-011119)	Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface (RFI)
SP-RFIv1.1-I08-020301	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification
SP-BPI+-I08-020301	DOCSIS Baseline Privacy Interface Plus Specification

7 Not all supported standards are listed.

MIBs

MIBs[8]	MIBs Link
CISCO-CABLE-SPECTRUM-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

8 Not all supported MIBs are listed.

RFCs

Description	Link
No new or modified RFCs are supported by this feature.	To locate and download Request for Comments (RFCs) and Internet Drafts, see the Internet Engineering Task Force (IETF) web site at the following URL: http://www.ietf.org/index.html

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 Flap List Troubleshooting

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 Flap List Troubleshooting

Releases	Feature Information
Release 11.3 NA	This feature was introduced on the Cisco uBR7200 series routers.
Release 12.0(4)XA	The *days* parameter was removed from the **cable flap-list aging** command.
Release 12.0(7)XR, 12.1(2)EC	The output of **show cable flap-list** command was enhanced to show when the Cisco uBR7200 series router has detected an unstable return path for a particular CM and has made an automated power adjustment.
Release 12.1(5)EC	This feature was supported on the Cisco uBR7100 series routers.
Release 12.1(7)CX	The ccsFlapClearAll attribute was added to the ccsFlapTable table in the CISCO-CABLE-SPECTRUM-MIB MIB.
12.2(4)BC1	This feature was supported on the Release 12.2 BC train for all Cisco CMTS platforms. The **show cable modem flap** command was also introduced to display flap-list information for individual cable modems.
Supported Platforms	
Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 universal broadband routers.	

CHAPTER 6

IPDR Streaming Protocol on the Cisco CMTS Routers

First Published: December 17, 2008

Last Updated: July 11, 2012

The Cisco universal broadband router supports the Internet Protocol Detail Record (IPDR) streaming protocol feature that provides high volume data exported from the network equipment to mediation systems such as the Operations Support Systems (OSS) or Business Support Systems (BSS). IPDR provides information about IP-based service usage and other activities that are used by OSS and BSS. This protocol provides a mechanism to collect data from various network elements or equipment using a push model as opposed to the conventional Simple Network Management Protocol (SNMP) polling mechanism.

Based on the DOCSIS 3.0 specifications, the IPDR feature optimizes time and resource efficiency in the transfer of large amounts of performance metrics to the management systems. DOCSIS 3.0 introduces five management features or the FCAPS model. FCAPS represents Fault, Configuration, Accounting, Performance and Security.

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 IPDR Streaming Protocol

The table shows the hardware compatibility prerequisites for the IPDR streaming protocol.

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

Table 13: Cable Hardware Compatibility Matrix for the IPDR Streaming Protocol

Cisco CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCB and later • PRE2 • PRE4 • 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 [9]
Cisco uBR7246VXR Universal Broadband Routers	Cisco IOS Release 12.2(33)SCD and later • Network Processing Engine G2 (NPE-G2)	Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [10]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCD and later • NPE-G2	Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

9 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.
10 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 Configuring IPDR Streaming Protocol

- An IPDR exporter can be connected to many collectors, but it will only send data to the highest priority operating collector at any given time.
- Each IPDR session can be associated to one active (zero) or more standby collector with priority.

Information About IPDR Streaming Protocol

IPDR Streaming Protocol is designed to address the need for a reliable, fast, efficient, and flexible export process of high volume data records such as billing, performance and diagnostic data.

The IPDR/SP process communicates with IPDR collectors. The IPDR streaming protocol supports multiple IPDR sessions. The architecture supports primary and secondary collectors for failover purposes. At any time, data is sent to only one collector. If the exporter to primary collector connection fails due to any reason, the data is sent to the secondary collector. Depending on the network configuration, you can have only one primary collector for each session, while for different sessions, you can have different primary collectors. For example, there may be a billing collector, a diagnostic collector, and so on.

Note IPDR exporter refers to the Cable Modem Termination System (CMTS) and the IPDR collector refers to the network equipment.

Data Collection Methodologies

IPDR is the data generated or collected for various performance related metrics such as billing information, diagnostics, network topology, signal quality monitoring, and other management data. These data are based on the FCAPS model (Fault, Configuration, Accounting, Performance and Security.)

The IPDR client application communicates with the IPDR exporter using the IPDR_GET_SESSIONS message to identify the streams provided by the exporter, and the exporter sends responses to the client using the IPDR_GET_SESSIONS_RESPONSE message. This data collection method is based on the *Operations Support System Interface Specification* (CM-SP-OSSIv3.0-I13-101008).

Beginning with Cisco IOS Release 12.2(33)SCE, the IPDR_GET_SESSIONS_RESPONSE message includes the SessionBlock.reserved attribute to identify the IPDR session ID. This attribute helps the Cisco CMTS router define an IPDR session ID for each data collection mechanism supported for each IPDR service definition. This attribute was not used in Cisco IOS Releases earlier to Cisco IOS Release 12.2(33)SCE.

Note You must use a Cisco CMTS router running Cisco IOS Release 12.2(33)SCE or later, if your IPDR client application looks for the SessionBlock.reserved attribute in the IPDR_GET_SESSIONS_RESPONSE message.

The IPDR feature defines methods for the collectors or network elements to collect data from the CMTS. Below is the list of collection methodologies:

Time Interval Session: In this method, the CMTS follows a schedule-based session to stream data at a periodic time interval. A time interval is the time gap between two adjacent sessions' start messages. This method is

managed by the CMTS in controlling the start and stop operation of a session. The time interval session terminates after the CMTS exports the records.

Note During the course of a one-time interval when the CMTS is streaming records, if another time interval is expected, the CMTS will ignore the new time interval and continue exporting the data until the previous time interval ends.

Event-based Session: In this method, the CMTS can export records at any time, when the session is open. In other words, this method works on an open-ended session.

Ad-hoc Session: In this method, the CMTS creates a session, allows data streaming, and closes the session when the data export is complete or when a closing command is generated.

A new session is created by issuing the **ipdr session** command. After, the CMTS receives the FLOW_START message from the collector, the CMTS exporter sends a SESSION_START message to start exporting the IPDR data from the collector. After all data is transported, the exporter receives a ACK message from the collector, and then sends a SESSION_STOP message to the collector. This method is known as the Ad-hoc session.

IPDR Access Control List

The IPDR streaming protocol in Cisco uBR10012 router is enhanced to improve the security of the IPDR collector function. This enhancement prevents the validation and authentication of the fake IPDR collectors, thus preventing billing theft.

This enhancement is optional and may be enabled or disabled. To enable the IPDR Access Control List enhancement, use the **ipdr authorization** command. Effective with Cisco IOS Release 12.2(33)SCI2, only the IPDR collectors on the CMTS network side are authorized based on the authorization procedure.

The **ipdr collector** command is enhanced to configure a NAT address for an IPDR collector that operates from a NAT router. For authorization of such IPDR collectors, the NAT address is also configured for the IPDR collectors using the **nat-address** keyword.

Restrictions

The following restrictions are applicable when the IPDR Access Control List enhancement is enabled:

- Effective with Cisco IOS Release 12.2(33)SCI2, the IPDR collectors on the CMTS bundle side are blocked. This block is irrespective of whether the **ipdr authorization** is enabled or not.
- An IPDR collector that operates from within a NAT router, the NAT address parameter may be configured for that IPDR collector.
- For authentication:
  - If the IPDR collector operates from within a NAT router, then the NAT address of the IPDR collector must match the NAT address of the listed IPDR collector. The IP address of the IPDR collector also must match the IP address of the listed IPDR collector.
  - If the IPDR collector does not operate from within a NAT router, only the IP address of the IPDR collector must match the IP address of the listed IPDR collector.

How to Configure IPDR Streaming Protocol

This section describes the configuration tasks that are performed when using the IPDR streaming protocol feature on the Cisco CMTS platforms.

Note Use no ipdr command to remove the IPDR configuration.

Configuring the IPDR Session

To enable the CMTS application to add a session to the IPDR exporter, use the ipdr session command in global configuration mode.

Use the no form of the command to remove the IPDR session.

Note

- The session ID must be unique.
- To remove an active session, you must deactivate it before removing it.

>

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	ipdr session session_id session_name session_descr **Example:** `Router(config)# ipdr session 1 samis_sxn test`	Enables the CMTS application to add a session to the IPDR exporter.

Configuring the IPDR Type

To configure the IPDR session type, use the ipdr type command in global configuration mode. The IPDR session types that can be defined using this command are event type, time-interval type, and the ad hoc type.

Use the no form of the command to reset the session type to the default "event" type.

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	ipdr type session_id [ad-hoc | event | time-interval value] **Example:** `Router(config)# ipdr type 1 time-interval 15`	Enables the CMTS application to configure an IPDR session type.

What to Do Next

Note Once the IPDR session type is configured, only the templates supported by this IPDR type are allowed be associated with it. Also, the console provides information about those templates that are not supported by this IPDR session type when the type is changed.

Configuring the IPDR Collector

To configure the IPDR collector details, use the ipdr collector command in global configuration mode. The port number is used when an exporter creates an active connection.

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	**ipdr collector** **Example:** `Router(config)# ipdr collector federal 192.168.6.5`	Enables the CMTS application to configure an IPDR collector and authenticate the IPDR protocol. **Note** Configure the NAT address in case of an IPDR collector that is operating in a NAT enabled network.

Configuring the IPDR Associate

To associate the collector with a session, use the ipdr associate command in global configuration mode.

Before You Begin

- You must deactivate the session before configuring the associate.

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	**ipdr associate session_id collector_name priority** **Example:** `Router(config)# ipdr associate 1 federal 1`	Associates the collector with a session.

Configuring the IPDR Template

To add an IPDR template to the IPDR session, use the ipdr template command in global configuration mode. The template list can be viewed by entering a "?" at the command prompt.

Note

- You can add only the system-supported templates.

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	**ipdr template session_id template_name** **Example:** `Router(config)# ipdr template 1 SAMIS`	Adds an IPDR template to the IPDR session.

Configuring the IPDR Exporter

Starting with Cisco IOS Release 12.2(33)SCG, IPDR exporter parameters such as keepalive timer count, the maximum number of unacknowledged records, and unacknowledged timeout interval value can be configured using the following commands.

- **ipdr exporter keepalive—**Sets the keepalive timer count value on the IPDR Exporter.
- **ipdr exporter max-unacked—**Sets the maximum number of unacknowledged records on the IPDR Exporter.
- **ipdr exporter ack-timeout—**Sets the time interval for acknowledged records on the IPDR Exporter.

Note Starting Cisco IOS Release 12.2(33)SCE, the default value for DataAckTimeInterval is 60 seconds and the default value for DataAckSequenceInterval is 200 seconds.

You can set the values for the IPDR parameters to customize exporter for the collectors used in the facility. However, these commands are optional, so if not configured, the default values of the commands are used when **ipdr exporter start** command is executed.

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	**ipdr exporter keepalive** *time_interval* **Example:** `Router(config)# ipdr exporter keepalive 300`	(Optional) Sets the keepalive timer count for the IPDR Exporter. The valid range is from 5 to 300 seconds. The default value is 300.
Step 4	**ipdr exporter max-unacked** *records* **Example:** `Router(config)# ipdr exporter max-unacked 200`	(Optional) Sets the number of maximum unacknowledged records on the IPDR Exporter. The valid range is from 5 to 200 records. The default value is 200.
Step 5	**ipdr exporter ack-timeout** *time_interval* **Example:** `Router(config)# ipdr exporter ack-timeout 60`	(Optional) Sets the acknowledged records timeout interval on the IPDR Exporter. The valid range is from 5 to 60 seconds. The default value is 60.

	Command or Action	Purpose
Step 6	ipdr exporter start **Example:** `Router(config)# ipdr exporter start`	Enables the CMTS application to start the IPDR exporter process to connect the exporter and the collector.

Configuration Examples for IPDR Streaming Protocol

Example: Configuring the IPDR Session

The following example shows how to configure the IPDR session.

```
Router> enable
Router# configure terminal
Router(config)# ipdr session 1 test no_descr
```

Example: Configuring the IPDR Type

The following example shows how to configure the IPDR “time-interval” session type for a time interval of 15 minutes.

```
Router> enable
Router# configure terminal
Router(config)# ipdr type 1 time-interval 15
```

Example: Configuring the IPDR Collector

The following example shows how to configure the IPDR collector.

```
Router> enable
Router# configure terminal
Router(config)# ipdr collector federal 209.165.200.225
```

Example for Configuring the IPDR Collector with NAT Address

Effective with Cisco IOS Release 12.2(33)SCI2, this example shows the **nat-address** keyword used to configure the NAT address for an IPDR collector:

```
Router(config)#ipdr collector federal 192.0.2.225 nat-address 192.0.2.51
```

Example: Configuring the IPDR Associate

The following example shows how to associate the collector with a session.

```
Router> enable
Router# configure terminal
Router(config)# ipdr associate 1 federal 1
```

Example: Configuring the IPDR Template

The following example shows how to add an IPDR template to the IPDR session.

```
Router> enable
Router# configure terminal
Router(config)# ipdr template 1 SAMIS-TYPE1
```

Example: Configuring the IPDR Exporter

The following example shows how to configure the IPDR exporter process to connect the exporter and the collector.

```
Router> enable
Router# configure terminal
Router(config)# ipdr exporter keepalive 300
Router(config)# ipdr exporter max-unacked 200
Router(config)# ipdr exporter ack_timeout 60
Router(config)# ipdr exporter start
```

Example: Configuring the IPDR Authorization

The following example shows how to configure the IPDR authorization.

```
Router> enable
Router# configure terminal
Router(config)# ipdr authorization
```

Verifying IPDR Streaming Protocol

This section describes the commands used for verification of the IPDR streaming protocol feature on the Cisco CMTS platforms.

Verifying the IPDR Collector

The **show ipdr collector** command displays the collector information, message statistics, and event for all the sessions that are associated with the collector.

The following example shows the sample output for the **show ipdr collector** command.

```
Router# show ipdr collector federal
```

```
Collector Name: federal, IP: 192.0.2.0, Port: 0
2001-07-05T19:28:22 Collector in session 1 Statistics:
 Transmitted 12658 Acknowledged 12658 Enqueued 12658 Lost 0
 Last Event: Event Id 1 IPDR_EVENT_SERVER_CONNECTED - INCOMING
Router(config)#
```

Verifying IPDR exporter

The **show ipdr exporter** command displays information about the IPDR Exporter state as listed below.

- started
- not started
- not initialized

The following example shows the sample output for the **show ipdr exporter** command:

```
Router# show ipdr exporter
IPDR exporter is started.
Current parameters:
        KeepAliveInterval   :300
        AckTimeInterval     :60
        AckSequenceInterval :200
Router#
```

Verifying IPDR session

The **show ipdr session** command displays the session details such as the session ID, description, and the session state for all sessions as well as for a specific session.

The following example shows the sample output for the **all** keyword for the **show ipdr session** command.

```
Router# show ipdr session all
Session ID: 1, Name: utilsta, Descr: test, Started: False
```

The following example shows the sample output for the **session_id** keyword for the **show ipdr session** command.

```
Router# show ipdr session 1
Session ID: 1, Name: utilsta, Descr: test, Started: False
2001-07-05T19:36:28 Statistics:
Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
queuedOutstanding 0 queuedUnacknowledged 0
1 Collectors in the session:
Name: federal, IPAddr: 192.0.2.0, Port: 0, Priority: 1
```

Verifying IPDR Session Collector

The **show ipdr session collector** command displays the details of a collector that is associated with a specific session. Because there can be multiple collectors associated to a session, this command is used to show a specific session-collector pair.

The following example shows the sample output for the **show ipdr session collector** command.

```
Router# show ipdr session 1 collector federal
Session ID: 1, Name: utilsta, Descr: test, Started: False
Collecotr Name: federal, IP: 192.0.2.0, Port: 0
2001-07-05T19:38:02 Collector in session 1 Statistics:
 Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
 Last Event: Event Id 0 WRONG_EVENT_ID
```

Verifying IPDR Session Template

The **show ipdr session template** command displays the list of all active templates supported by a specific session.

The following example shows the sample output for the **show ipdr session template** command.

```
Router# show ipdr session 1 template
Template ID: 2, Name:
http://www.cablelabs.com/namespaces/DOCSIS/3.0/xsd/ipdr/DOCSIS-CMTS-CMSERVICE-FLOW-TYPE,
Type: DOCSIS-Type, KeyNumber: 22
Session 1 has totally 1 templates.
```

Additional References

The following sections provide references related to configuring the IPDR streaming protocol feature.

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 uBR10012 Universal Broadband Router Documentation	*Cisco uBR10012 Universal Broadband Router Hardware Installation Guide* http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/guide/hig.html *Cisco uBR10012 Universal Broadband Router Software Configuration Guide* 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

Related Topic	Document Title
IPDR/SP 2.1	IPDR/SP Protocol Specification Version 2.1 http://www.ipdr.org

Standards

Standard	Title
DOCSIS 3.0 OSSI	Data-Over-Cable Service Interface Specifications DOCSIS 3.0 Operations Support System Interface Specification CM-SP-OSSIv3.0-I13-101008 http://www.cablelabs.com

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1014 XDR	XDR: External Data Representation Standard

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 IPDR Streaming Protocol

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 14: Feature Information for IPDR Streaming Protocol

Feature Name	Releases	Feature Information
IPDR Streaming Protocol	12.2(33)SCB	The Cisco universal broadband router supports the IPDR streaming protocol feature that enables efficient and reliable delivery of high volume data records from the service elements to any systems, such as mediation systems and BSS/OSS. The following sections provide information about this feature:
Data Collection Methodologies and DOCSIS 3.0 IPDR Schema	12.2(33)SCD2	This feature was introduced in this release. The following sections provide information about this feature: The following command was introduced: ipdr type
IPDR Exporter parameters such as keepalive timer value, maximum unacknowledged records, and acknowledged records timer value can be configured using the CLI.	12.2(33)SCG	The following commands were introduced: • **ipdr exporter keepalive** • **ipdr exporter max-unacked** • **ipdr exporter ack-timeout**

Feature Name	Releases	Feature Information
IPDR Access Control List	12.2(33)SCI2	This feature was introduced in this release. The following command was introduced: **ipdr authorization** The following command was modified: **ipdr collector**

CHAPTER 7

GOLD Health Monitoring for the Cisco UBR10012 Universal Broadband Router

First Published: November 16, 2009

Last Updated: November 29, 2010

Generic Online Diagnostic (GOLD) is a health monitoring feature implemented on the Cisco UBR10012 Universal Broadband Router in the Cisco IOS Release 12.2(33)SCC. The GOLD functionality is developed to provide online diagnostic capabilities that run at bootup, in the background on a periodic basis, or based on demand from the CLI.

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 GOLD

The table shows the hardware and software 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 15: GOLD Support for the Cisco CMTS Routers Hardware and Software 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)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 [11]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 • 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 [12]
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

11 Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.
12 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 GOLD feature

- GOLD test cases are designed on a per chip or per interface level and are not expected to monitor at a per modem or per service flow level.
- GOLD diagnostic test cases supported in the Cisco IOS Release 12.2(33)SCC are as follows:
  - Low Latency Queue (LLQ) Drop Monitor Test: Implemented on 5x20 cable line card (CLC) (Test520LLQDrops), 20x20 CLC (Test2020LLQDrops), and Modena (TestModenaLLQDrops).
  - Guardian Index Leak Test: Implemented only on 5x20 Guardian LC (TestBlazeIndexLeak).
  - CLC Memory Leak Test: Implemented on 5x20 and 20x20 LC (TestMemLeaks).

Information About GOLD

The following sections provide details of the GOLD feature:

Limitations of Existing Logging Mechanism

To provide high-availability for a router without any downtime it is imperative to analyze the stability of a system. The primary method of discovering the cause of system failure is system messages. However, there are certain system failures that do not send notifications. It is difficult to understand the cause of these system failures, as the existing logging mechanism fails to notify or maintain a log of these failures.

Understanding the Importance of GOLD Functionality

As there are certain system failures that do not send any notification or keep a log of failure, it is essential to address these limitations. The GOLD feature has been designed specifically to provide error detection by polling for errors for those system modules that do not have any notification mechanism. GOLD has been implemented on the Cisco UBR10012 router to actively poll for system errors. Online diagnostics is one of the requirements for high availability (HA). HA is a a set of quality standards that seeks to limit the impact of equipment failures on the network. A key part of HA is detecting system failures and taking corrective actions while the system is running in a live network.

Understanding the GOLD Feature

The GOLD feature is primarily used to poll for system errors targeted for those components, which do not send a notification upon failure. Although the infrastructure can be used to poll for both hardware and system errors, the main scope is to poll for status and error registers on physical hardware device. The Cisco UBR10012 Router uses a distributed GOLD implementation. In this model, the core Cisco IOS GOLD subsystem is linked on both the route processor (RP) and the cable line cards.

Diagnostic tests can be registered either as local tests which run on the RP or as proxy tests which run on the line cards. When a proxy test is requested on the RP, a command is sent using Inter-Process Communication (IPC) to the line card to instruct it to run the test locally. The results are then returned to the RP using IPC. Tests are specified by card type on a per slot/subslot basis. Diagnostic tests can be run either on bootup, periodically (triggered by a timer), or on demand from the CLI. GOLD feature is managed through a range of commands which are mainly used to provide on-demand diagnostic tests, schedule tests at particular intervals, monitor the system health on periodic basis and to view the diagnostic test results.

Configuring Online Diagnostics

The following sections describe how to configure various types of diagnostics and view test reports:

Configuring the Bootup Diagnostics Level

You can configure the bootup diagnostics level as minimal or complete or you can bypass the bootup diagnostics entirely. Enter the **complete** keyword to run all bootup diagnostic tests and the **minimal** keyword to run minimal tests such as loopback. Enter the **no** form of the command to bypass all diagnostic tests. The default bootup diagnostics level is minimal.

Note None of the currently implemented tests on the Cisco UBR 10012 Router are bootup tests.

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	Router(config)# **diagnostic bootup level {minimal | complete}** **Example:** `Router(config)#` **diagnostic bootup level complete**	Configures the bootup diagnostic level.

Configuring On-Demand Diagnostics

You can run the on-demand diagnostic tests from the CLI. You can set the execution action to either stop or continue the test when a failure is detected or to stop the test after a specific number of failures occur by using the failure count setting. You can configure a test to run multiple times using the iteration setting.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**diagnostic ondemand {iteration** *iteration_count* } | {**action-on-error {continue | stop**}[*error_count*]} **Example:** `Router#` **diagnostic ondemand iteration 3**	Configures on-demand diagnostic tests to run, how many times to run (iterations), and what action to take when errors are found.
Step 3	**diagnostic start** {**bay** *slot/bay* | **slot** *slot-no*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive**} • **diagnostic start** {**subslot** *slot/sub-slot*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive | per-port** [**port** {num | *port#-range* | **all**}]} **Example:** `Router# diagnostic start bay 1/0 test 5`	Starts the on-demand diagnostic test on the specified bay, slot, or subslot.
Step 4	**diagnostic stop** {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/sub-slot*} **Example:** `Router# diagnostic stop bay 1/0`	Stops the diagnostic test running on the specified bay, slot, or subslot.

Scheduling Diagnostics

You can schedule online diagnostics to run at a designated time of day or on a daily, weekly, or monthly basis. You can schedule tests to run only once or to repeat at an interval. Use the **no** form of this command to remove the scheduling.

To schedule online diagnostics, perform this task:

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	**diagnostic schedule** {**bay** *slot/bay* | **slot** *slot-no* } **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive**} {**daily** *hh:mm* | **on** *mm dd year hh:mm* | **weekly** *day-of-week hh:mm* } **Example:** **diagnostic schedule** {**subslot** *slot/sub-slot*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive** | **per-port** {**daily** *hh*:*mm* | **on** *mm dd year hh:mm* | **weekly** *day-of-week hh:mm* | **port** {{*num* | *port#range* | **all**}{**daily** *hh*:*mm* | **on** *mm dd year hh:mm* | **weekly** *day-of-week hh:mm*}}}} **Example:** `Router(config)#` **diagnostic schedule bay 1/0 test 1 on september 2 2009 12:00** **Example:** `Router(config)#` **diagnostic schedule slot 1 test complete daily 08:00**	This example shows how to schedule the diagnostic testing on a specific date and time for a specific bay: This example shows how to schedule the diagnostic testing to occur daily at a certain time for a specific slot: Schedules on-demand diagnostic tests for a specific date and time, how many times to run (iterations), and what action to take when errors are found.

Configuring Health-Monitoring Diagnostics

You can configure health-monitoring diagnostic testing while the system is connected to a live network. You can configure the execution interval for each health monitoring test, whether or not to generate a system message upon test failure, or to enable or disable an individual test. Use the **no** form of this command to disable testing.

Note Before enabling the diagnostic monitor test, you first need to set the interval to run the diagnostic test. An error message is displayed if the interval is not configured before enabling the monitoring.

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	**diagnostic monitor interval** {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/sub-slot*} **test** {*test-id* | *test-id-range* | **all**} {*hh:mm:ss*} {*milliseconds*} {*number-of-days* **Example:** `Router(config)#` **diagnostic monitor interval bay 1/0 test 2 06:00:00 100 10**	Configures the health-monitoring interval of the specified tests. The **no** form of this command will change the interval to the default interval, or zero.

Step 4	**diagnostic monitor** {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/sub-slot*} **test** {*test-id* | *test-id-range* | **all**}
	
	Example:
	
	`The following example shows a sample output of an error message displayed when monitoring is enabled before configuring the test interval:`
	
	Example:
	
	`Router(config)#` **diagnostic monitor bay 1/0 test 2**
	
	`Aug 12 18:04:56.280: %DIAG-3-MONITOR_INTERVAL_ZERO: Bay 1/0: Monitoring interval is 0. Cannot enable monitoring for Test #2`
		Enables or disables health-monitoring diagnostic tests.

Step 5	**diagnostic monitor syslog** **Example:** `Router(config)#` **diagnostic monitor syslog**	Enables the generation of a system logging messages when a health-monitoring test fails.
Step 6	**diagnostic monitor threshold** {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/sub-slot* } **test** {*test-id* | *test-id-range* | **all**} {**failure count** *no-of-allowed-failures* }	Configures the failure threshold value for the bay, slot, or subslot.

	Command or Action	Purpose
	Example: `Router(config)#` **diagnostic monitor threshold bay 1/0 test 2 failure count 10**	

Displaying Online Diagnostic Tests and Test Results

You can display the online diagnostic tests that are configured and check the results of the tests using the **show** commands.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show diagnostic content all** | bay *slot/bay* | slot *slot-no* | subslot *slot/subslot* **Example:** `Router#` **show diagnostic content bay 1/0**	Displays the online diagnostics tests and test attributes that are configured.
Step 3	**show diagnostic result** [[**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/subslot*] {**detail** | **test** {*test-id* | *test-id-range* | **all**}} | **all** **Example:** `Router#` **show diagnostic result all**	Displays the diagnostic test results (pass, fail, or untested) for a bay, slot, or subslot.
Step 4	**show diagnostic schedule all** | **bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/subslot*] **Example:** `Router#` **show diagnostic schedule slot 1**	Displays the current scheduled diagnostic tasks.
Step 5	**show diagnostic events** [**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/sub-slot* | **event-type** {*error* | *info* | *warning*}] **Example:** `Router#` **show diagnostic events subslot 5/0**	Displays the diagnostic event log details for the specified bay, slot, or subslot.

Supported GOLD Tests on Cisco UBR10012 Router

This section discusses the GOLD test cases that have been implemented on Cisco UBR10012 Router in the Cisco IOS Release 12.2(33)SCC. This section contains the following topics:

Low Latency Queue (LLQ) Drop Test

To support the low latency requirements of voice calls the UBR10012 Router uses per interface absolute priority queues. Verifying the drops in the queue is a cumbersome manual process. Because of this, the periodic LLQ Drop test has been implemented to monitor all low latency queues on the box for drops. The test is a non-proxy test case that runs on the RP.

For the specified slot/subslot or slot/bay pair, the test will walk all associated forwarding interfaces legacy, modular, integrated, and wideband and look for drops on the interface low latency queue (if one exists). If drops are found, the test case reports a failure to the GOLD infrastructure and log a system log message with pertinent information.

Note The LLQ Drop test runs on demand with a default period of one (1) hour. It can be configured to run as often as every one minute.

The table provides details regarding the supported hardware, test names, and criteria for displaying the test results.

Table 16: Hardware Support Matrix for LLQ Drop Test

Supported Line Card and SPA	Test Name	Criteria To Display Result
5x20 line card	Test520LLQDrops	For 5x20 line cards, the test returns per port results with a port corresponding to a downstream interface.
20x20 line card	Test2020LLQDrops	For 20x20 line cards, the test returns per port results with a port corresponding to a controller.
Modena SPA	TestModenaLLQDrops	On Modena SPA, the test returns global results.

Guardian Index Leak Test

For remote downstreams using SPAs, the Guardian maintains stat indices for remote service flows, PHS indices for voice flows on NB modems and BPI indices for encrypted modems. The index associations are maintained on the host mac-domain. There could be cases where the service flow has been destroyed or the

cable modem has been kicked offline and the corresponding indices have not been de-allocated on the guardian. Any index leaks arising out of corner cases or race conditions would cause the index table to run out of indices which would then prevent any new modems to come online or new service flows to be created.

Periodic GOLD test (TestBlazeIndexLeak) has been introduced for 5x20 line cards to catch these index leaks early. TestBlazeIndexLeak test is a proxy test which runs on the linecard per slot or subslot. The number of Blaze indices are compared on each mac-domain host with the indices allocated by the guardian. If inconsistencies are found, error message is reported on the line card, with the mac-domain host inconsistencies. The error message displays the allocating guardian, the host line card on which the test fails and the margin observed.

Note The TestBlazeIndexLeak test runs on demand with a default period of eight (8) hours.

The table provides details regarding the supported hardware, test names, and criteria for displaying the test results.

Table 17: Hardware Support Matrix for Guardian Index Leak Test

Supported Line Card and SPA	Test Name	Criteria To Display Result
5x20 line card	TestBlazeIndexLeak	For 5x20 line cards, the test returns per port results with a port corresponding to a downstream interface.

Memory Leak Test

As part of health monitoring tests, GOLD test case for detecting memory leaks in IOS have been added. The programmed approach covers potential leaks in IO Buffers and Processor Heap Memory. Most of the approaches to detect memory leak, require human analysis or tool based post-processing of outputs from various show commands. The Memory Leak Test adds a programmatic implementation inside IOS code itself to detect and signal any 'sizeable levels of IOS memory leaks' occurring over-time. The TestMemLeaks test case is automatically kick-started by GOLD on both PRE and CLC. One hour after card bootup, the test starts sampling free-memory data every 2 minutes in the background and then after every two hours it generates Leak test results for GOLD.

Test Result Behavior: The GOLD TestMemLeak failures are persistent failures, i.e. if the test fails due to a leak detected during a two hour window, the test fails from here on till card reboot, even if no new leaks were detected during ongoing two-hour sampling window.

Memory: The TestMemLeaks test adds some fixed-size static data-structures that take less than 10KB of fixed memory. To run per-RU-IO-buffer leak test, dynamic List is also allocated to get per-RU-stats, and these list elements are all freed before the test is over.

The Memory Resource Monitoring test case added as TestMemLeaks currently covers the following two approaches:

- Free Memory Trending, on page 87
- I/O Memory Buffer Hold Accounting, on page 87

Free Memory Trending

Aggregate level memory leaks can be detected using Free Memory Trending. Free memory trending requires system to get baseline usage numbers after one hour of system boot-up, and collect free memory samples every few minutes. Apply the free memory trending approach after you have enough samples. Periodically keep a watch on trend of free, lowest and largest block levels, by performing:

- Leak Trending check: Size of the Lowest Free Memory, Current Free Memory. Compare these samples to previous values and if all these parameters indicate a gradually leaking memory, and signal it as a test failure. If the following conditions are significantly found to be true, the logic alarms leaking memory.
  - FreeBytes of next sample are lower than FreeBytes of previous sample, AND
  - Lowest free in this sample is within 10KB bytes of freeBytes; AND
  - If lowest free in this sample is lesser than lowest block of previous sample
  - If such conditions are found to be true for more than 25% of periodically collected samples, LeakTrend is assumed.
- Lower Threshold Check: Compare the free memory threshold to total memory on the card.

If the above two checks fail, a red flag is raised as an error message that memory on the box has been gradually leaking.

- If Largest Free is less than 1 MB (min. buffer size level for safe allocation) i.e. even if Largest free memory is above risk thresholds but if 'Lowest Sized buffer' reaches dangerous levels (like 1MB), then the logic signals memory leak error.

I/O Memory Buffer Hold Accounting

This section discusses, how I/O memory buffer leak scan algorithm works. To detect I/O memory leaks, besides the free-memory trending approach, the buffer life span analysis approach is also considered, where old buffers stored for more than a specified threshold of time are considered leaking. The command **show buffers leak resource** user displays a detailed summary of buffers that are older than a minute in the system, on a per Resource-User basis.

Note The TestMemLeaks test runs on demand with a default period of two (2) hours.

The table provides details regarding the supported hardware, test names, and criteria for displaying the test results.

Table 18: Hardware Support Matrix for Memory Leak Detection

Supported Line Card and SPA	Test Name	Criteria To Display Result
5x20 line card	TestMemLeaks	Poll, collect, and compare samples of Processor Memory Leak and I/O Memory Buffer leak.

Supported Line Card and SPA	Test Name	Criteria To Display Result
20x20 line card	TestMemLeaks	Poll, collect, and compare samples of Processor Memory Leak and I/O Memory Buffer leak.

How to Manage Diagnostic Tests

This section describes how to manage the diagnostic tests. The following GOLD commands are used to to manage the ondemand and periodic diagnostic tests:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**diagnostic ondemand** **Example:** `Router# diagnostic ondemand iteration 50`	Configures the ondemand diagnostic parameters such as iteration-count and action-on-error. These parameters signify the number of times the test is run and the execution action when a failure is detected. These parameters are used when the command **diagnostic start** is executed. In the given example, the iteration count to the same ondemand diagnostic test again is configured as 50. **Note** By default, iteration-count is 1, action-on-error is continue, and error count is 0.
Step 2	**show diagnostic ondemand settings** **Example:** `Router# show diagnostic ondemand settings`	Displays the ondemand diagnostic settings configured using the command **diagnostic ondemand**.
Step 3	**diagnostic start** {**bay** *slot/bay* | **slot** *slot-no*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive**} **Example:** `Router# diagnostic start bay 1/0 test 1 all`	Starts an ondemand diagnostic test. • **bay** *slot/bay*—Indicates the card slot and bay number where the diagnostic test is executed. The bay keyword is used to refer a SPA on the router. The valid range for the slot number is from 1 to 8 and 0 to 3 for the bay number. • **slot** *slot-no*—Indicates the slot number of the full-height line card where the diagnostic test is executed. The slot keyword is used to refer a full-height line card on the router. The valid range for slot is from 1 to 8. • **subslot** *slot/sub-slot*—Indicates the slot and subslot number of half-height line card where the diagnostic test is executed. The subslot keyword is used to refer a half-height line card on the router. The valid range for the slot number is from 1 to 8 and 0 to 1 for the subslot number. • **test**— Specifies a test to run. • *test-id*—Identification number for the test to run.

	Command or Action	Purpose
		• *test-id-range*—Range of identification numbers for tests to run. • **minimal**—Runs minimal bootup diagnostic tests. • **complete**—Runs complete bootup diagnostic tests. • **non-disruptive**—Runs the non disruptive health-monitoring tests. • **all**—Runs all diagnostic tests.
Step 4	**show diagnostic content** **Example:** `Router# show diagnostic content`	Displays the registered tests, attributes, and the configured interval at which the test runs. **Note** To view the registered test details for a specific SPA, full-height line card, or half-height line-card, use the keywords bay, slot, or subslot.
Step 5	**show diagnostic result** **Example:** `Router# show diagnostic result`	Displays the diagnostic test results for a SPA, full-height line card, or half-height line card.
Step 6	**show diagnostic events** **Example:** `Router# show diagnostic events`	Displays the diagnostic event log details for all the SPAs, full-height line card, and half-height line cards installed on the Cisco UBR10012 Router.
Step 7	**diagnostic stop** {**bay** *slot/bay* | **slot** *slot-no*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive**} **Example:** `Router# diagnostic stop bay 1/0 all`	Stops the ondemand diagnostic test.
Step 8	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 9	**diagnostic bootup level** {**minimal** | **complete**} **Example:** `Router(config)# diagnostic bootup level complete`	Configures the bootup diagnostic level. • **minimal**—Specifies minimal diagnostics. • **complete**—Specifies complete diagnostics.
Step 10	**show diagnostic bootup level** **Example:** `Router# show diagnostic bootup`	Displays the configured bootup diagnostic level.
Step 11	**diagnostic event-log size** *size*	Modifies the diagnostic event log size dynamically.

	Command or Action	Purpose
	Example: `Router(config)# diagnostic event log size 10000`	• *size*—Diagnostic event-log sizes. The valid values range from 1 to 10000 entries.
Step 12	**diagnostic monitor interval** {**bay** *slot/bay* | **slot** *slot-no*} | **subslot** *slot/subslot*} **test** {*test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds days* **Example:** `Router(config)# diagnostic monitor interval bay 1/0 test 2 06:00:00 100 20`	Configures the health monitoring diagnostic test interval to rerun the tests. • *hh:mm:ss*—Hours, minutes, and seconds interval configured to run the test again. • *milliseconds*—Number of milliseconds between tests. • *days*—Number of days between tests. The valid range is from 0 to 20.
Step 13	**diagnostic schedule module** {module-number | slot/subslot} **test** {*test-id* | **all** | **complete** | **minimal** | **non-disruptive** | **per-port**} **Example:** `Router(config)# diagnostic schedule slot 1 test complete daily 08:00`	Schedules the online diagnostic test to run at a designated time, or on daily, weekly or monthly basis. • *module-number*—Specifies the module number. • *per-port*—Selects the per-port test suite.
Step 14	**show diagnostic schedule** **Example:** `Router# show diagnostic schedule`	Displays the current scheduled diagnostic tests.

Configuration Examples for GOLD Feature

The following example shows a sample output of the test configuration, test attributes, and the supported coverage test levels for each test and for each bay/slot/subslot:

```
Slot 1: 2jacket-1
  Diagnostics test suite attributes:
    M/C/* - Minimal bootup level test / Complete bootup level test / NA
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      X/* - Not a health monitoring test / NA
      F/* - Fixed monitoring interval test / NA
      E/* - Always enabled monitoring test / NA
      A/I - Monitoring is active / Monitoring is inactive
                                                              Test Interval
  ID   Test Name                                       Attributes      day hh:mm:ss.
  ==== ============================================ ============    =============
    1) TestJacketSample -------------------------> ***N****I       not configured  n/a
       Bay 1/0: 2jacket-1
```

```
          Diagnostics test suite attributes:
            M/C/* - Minimal bootup level test / Complete bootup level test / NA
              B/* - Basic ondemand test / NA
            P/V/* - Per port test / Per device test / NA
            D/N/* - Disruptive test / Non-disruptive test / NA
              S/* - Only applicable to standby unit / NA
              X/* - Not a health monitoring test / NA
              F/* - Fixed monitoring interval test / NA
              E/* - Always enabled monitoring test / NA
              A/I - Monitoring is active / Monitoring is inactive
                                                                          Test
 Interval
          ID   Test Name                                     Attributes      day
hh:mm:ss.
          ==== ============================================ ============    ====
=========
           1) TestModenaSample -------------------------> ***N****I       not configured
  n/a
          2) TestModenaLLQDrops ------------------------> ***N****A       000 01:00:00.00
 1
```

Additional References

For additional information related to health monitoring, see the following references:

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
System Event Archive (SEA)	SEA feature for the Cisco UBR10012 Router

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
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://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

Feature Information for GOLD 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 19: Feature Information for GOLD for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Generic Online Diagnostic (GOLD) subsystem support for the Cisco CMTS Routers	12.2(33)SCC	GOLD is a health monitoring feature implemented to run diagnostic tests and poll for system components, which do not generated errors. This feature was introduced for the MC5x20, MC20x20 cable line cards, Modena SPA, Jacket cards, PRE2, and PRE4 route processors. The following commands are new or modified: • **diagnostic start** • **diagnostic stop** • **diagnostic ondemand** • **show diagnostic bootup** • **show diagnostic content** • **show diagnostic description** • **show diagnostic events** • **show diagnostic ondemand** • **show diagnostic result** • **show diagnostic schedule** • **diagnostic bootup** • **diagnostic event-log** • **diagnostic monitor** • **diagnostic schedule**

CHAPTER 8

Managing Cable Modems on the Hybrid Fiber-Coaxial Network

After you have completed upstream and downstream configuration you have additional options to manage how your CMs operate in the hybrid fiber-coaxial (HFC) network. You can set the following CM functions:

Section	Purpose
t_Activating_CM_Authentication_1041780.xml#con_1041780	Configures the Cisco uBR10000 series CMTS to require all CMs to return a known text string to register with the CMTS and gain access to the network.
t_Activating_CM_Authentication_1039189.xml#con_1039189	Configures the Cisco uBR10000 series CMTS to require all CMs to return a known text string to register with the CMTS and gain access to the network.
t_Activating_CM_Insertion_Interval_1039220.xml#con_1039220	Limits the amount of time that a CM requests a channel for the first time from the Cisco uBR10012 router. (A CM's initial channel request is known as insertion.)
t_Activating_CM_Upstream_Address_Verification_1039314.xml#con_1039314	Ensures that only CMs that have received DHCP leases through the Cisco uBR10000 series CMTS can access the HFC network.
r_Clearing_CM_Counters_1039366.xml#con_1039366	Clears the counters for the CMs in the station maintenance list.
r_Clearing_CM_Reset_1039411.xml#con_1039411	Removes one or more CMs from the station maintenance list and resets the cable modem (or all CMs) on the network.
t_Configuring_CM_Registration_Timeout_1039439.xml#con_1039439	Specifies the registration timeout interval for CMs connected to the Cisco uBR10012 router.

Section	Purpose
t_Configuring_Dynamic_Contention_Algorithms_1039463.xml#con_1039463	Configures the algorithms that control the capacity of the contention subchannel and how efficiently a given contention subchannel capacity is used.
t_Configuring_the_Dynamic_Map_Advance_Algorithm_1039513.xml#con_1039513	Enhances the upstream throughput from a CM connected to the Cisco uBR10000 series CMTS. The system employs a new algorithm that automatically tunes the lookahead time in MAC allocation and management messages (MAPs), based on several input parameters for the corresponding upstream channel.
t_Configuring_Maximum_Hosts_Attached_to_a_CM_1039542.xml#con_1039542	Specifies the maximum number of hosts that can be attached to a subscriber's CM.
t_Configuring_Per-Modem_Filters_1039559.xml#task_1039559	Provides instructions to configure the Cisco uBR10012 router to filter incoming packets from individual hosts or cable interfaces based on the source Media Access Controller (MAC) or Internet Protocol (IP) address.
t_Configuring_Sync_Message_Interval_1039622.xml#con_1039622	Specifies the sync message interval between successive sync message transmissions from the Cisco uBR10000 series CMTS.

Note Cisco recommends using default values for most commands. The default values for the commands used in these configuration steps are, in most cases, adequate to configure the Cisco uBR10012 router.

Note For information about setting rate limiting on CMs, refer to these sections in Chapter 3:

- t_Setting_Downstream_Traffic_Shaping_1061062.xml#con_1061062
- t_Setting_Upstream_Traffic_Shaping_1055032.xml#task_1055032

Content

Activating CM Authentication

The Cisco uBR10012 router can be configured to require all CMs to return a known text string to register with the CMTS and gain access to the network. The text string can be from 1 to 80 characters in length. To activate CM authentication, use the following command from cable interface configuration mode.

To configure authentication and data privacy parameters, use the cable shared-secret command in cable interface configuration mode. To disable authentication during the CM registration phase, use the no form of this command.

cable shared-secret [**0** | **7**] *authentication-key*

no cable shared-secret

0	(Optional) Specifies that an unencrypted message will follow.
7	(Optional) Specifies that an encrypted message will follow.
authentication-key	Text string is a shared secret string. When you enable the service password-encryption option, the password is stored in encrypted form. The text string is a 64-character authentication key.

The following example shows how to activate CM authentication using 3344912349988...sf as the shared secret key and indicating that an encrypted message follows:

```
Router(config-if)# cable shared-secret 7 3344912349988cisco@xapowenaspasdpuy230jhm...sf
```

Verify CM Authentication

To verify whether CM authentication is activated or deactivated, enter the command **more system:running-config** and look for the cable interface configuration information. If CM authentication is deactivated, it appears in this output as no cable secret-shared.

Activating CM Insertion Interval

When a CM is ready to transmit data, it requests a channel from the Cisco uBR10012 router. You can limit the amount of time that a CM requests a channel for the first time from the Cisco uBR10012 router. A CM's initial channel request is known as insertion. The valid range is 100 to 2000 milliseconds.

To activate the CM insertion interval, use the following command in cable interface configuration mode.

Command	Purpose
cable insertion-interval milliseconds	Sets the insertion interval in milliseconds.

Validating CM Insertion Interval

To verify that a CM insertion interval has been set, enter the command **more system:running-config** command, and look for the cable interface configuration information, as shown in this command output excerpt:

```
Router# more system:running-config
Building configuration...
Current configuration:
!
interface Cable5/0/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
 cable insertion-interval 2000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
!
```

Troubleshooting CM Insertion Interval

If you are having trouble, make sure that you entered the correct slot and port numbers when you typed the command.

Activating CM Authentication

The Cisco uBR10000 series CMTS can be configured to require all CMs to return a known text string to register with the CMTS and gain access to the network. The text string can be from 1 to 80 characters in length. The default setting is "on" (CM authentication is activated).

To activate CM authentication, use the following command in cable interface configuration mode:

Command	Purpose
cable shared-secret [0|7] authorization-key **no cable shared-secret**	Enables CM authentication: • **0** specifies an unencrypted authentication key. • **7** specifies an encrypted authentication key. Disables CM authentication.

Tip Be sure that you enter the correct slot and port number in cable interface configuration mode. Verify that the CM is using baseline privacy interface (BPI) and that it is assigned to a quality of service (QoS) with privacy active. Verify that the cable interface configuration file contains a matching key.

Verifying CM Authentication

To verify if CM authentication has been activated or deactivated, enter the command more system:running-config and look for the cable interface configuration information. If CM authentication has been activated, it does not appear in this output. If CM authentication has been deactivated, it appears in this output as “ no cable secret-shared ,” as shown in this command output excerpt:

```
Router# more system:running-config
Building configuration...
Current configuration:
!
interface Cable5/0/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
  no cable secret-shared
  cable insertion-interval 150000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
!
```

Troubleshooting CM Authentication

If you are having trouble, make sure that you entered the correct slot and port numbers when you entered cable interface configuration mode.

For additional troubleshooting information, refer to Chapter 6, “Troubleshooting the System.”

Activating CM Upstream Address Verification

CM upstream address verification ensures that only CMs that have received Dynamic Host Configuration Protocol (DHCP) leases through the Cisco uBR10012 router can access the HFC network. The Cisco uBR10012 router discards all packets received from or for hosts that have not received Dynamic Host Configuration Protocol (DHCP)-assigned addresses. The default setting is "off" (CM upstream address verification is deactivated).

To activate or deactivate CM upstream verification, use the following command in the cable interface configuration mode:

Command	Purpose
cable source-verify [dhcp]	Activates CM upstream verification. The **dhcp** option specifies that queries be sent to verify unknown IP addresses in upstream data packets.
no cable source-verify	Returns to the default upstream verification state.

Verifying CM Upstream Address Verification

To verify that CM upstream verification has been activated or deactivated, enter the command **more system:running-config** and look for the **no cable source-verify** notation in the cable interface configuration information. If CM upstream verification has been deactivated, it does not appear in this output. If CM upstream verification has been activated, it appears in this output as **cable source-verify**, as shown in this command output excerpt:

```
Router# more system:running-config
Building configuration...
Current configuration:
!
interface Cable5/0/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
  cable source-verify
  cable insertion-interval 2000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
!
```

Tip Be sure that you enter the correct slot and port number when you enter the cable interface configuration mode.

Note If the Cisco uBR10012 router is reloaded or the Address Resolution Protocol (ARP) table is cleared, all hosts on the network are forced to release and renew their IP addresses. Some systems might require restarting if the IP protocol stack is unable to renew using a broadcast IP address.

Clearing CM Counters

To clear the counters for the CMs in the station maintenance list, use one of the following commands in cable interface configuration mode.

Command	Purpose
clear cable modem *mac-addr* **counters**	Clears the counters in the station maintenance list for the CM with a specific MAC address.
clear cable modem *ip-addr* **counters**	Clears the counters in the station maintenance list for the CM with a specific IP address.
clear cable modem all counters	Clears the counters in the station maintenance list for all CMs.

Verifying Clear CM Counters

To determine if the counters in the station maintenance list are cleared, enter one of the following commands. The station maintenance list counter is 0.

Command	Purpose
show cable modem *ip-address*	Displays the status of a CM identified by its IP address.
show cable modem *mac-address*	Displays the status of a CM identified by its MAC address.
show cable modem *interface-address*	Displays the status of all CMs on a particular upstream.

Clearing CM Reset

To remove one or more CMs from the station maintenance list and reset the cable modem (or all CMs) on the network, use one of the following commands in cable interface configuration mode.

Command	Purpose
`clear cable modem mac-addr reset`	Removes the CM with a specific MAC address from the station maintenance list and resets it.
`clear cable modem ip-addr  reset`	Removes the CM with a specific IP address from the station maintenance list and resets it.
`clear cable modem all reset`	Removes all CMs from the station maintenance list and resets them.

Verifying Clear CM Reset

To determine if the **clear cable modem reset** command has removed a CM from the station maintenance list and forced it to start a reset sequence, enter the **show cable modem** command.

Tip Be sure that you entered the correct CM IP address or MAC address when you typed the **clear cable modem reset** command. It might take up to 30 seconds for the CM to start the reset sequence.

Note The **clear cable modem reset** command is useful if a Simple Network Management Protocol (SNMP) manager is not available, or if the CM is unable to obtain an IP address or respond to SNMP messages.

Configuring CM Registration Timeout

By default, registered CMs that have no upstream activity for three minutes are timed out and disconnected from the Cisco uBR10012 router. This timeout interval can be decreased to 2 minutes or increased up to 60 minutes.

To specify the registration timeout interval for CMs connected to the Cisco uBR10012 router, use the following command in cable interface configuration mode.

Command	Purpose
`cable registration-timeout` *`n`*	Specifies the maximum number of minutes allowed to elapse with no upstream activity before terminating the connection. Valid range is from 2 to 60 minutes. Default = 3 minutes.

Configuring Dynamic Contention Algorithms (Cable Insertion Interval, Range, and Data Backoff)

The Cisco uBR10000 series software includes the following algorithms that control the capacity of the contention subchannel and control the efficient use of a given contention subchannel capacity:

- Algorithm that dynamically controls the rate of upstream contention slots—initial ranging and bandwidth requests.
- Algorithm that varies the backoff parameters that CMs use. Backoff variation falls within each of the initial ranging and bandwidth request upstream contention subchannels.

In high contention mode, the Cisco uBR10000 series MAC scheduler uses collision statistics and sustains a high frequency of initial ranging slots until it detects a steady ranging state. The CMTS dynamically varies the frequency of initial ranging slots using the data grant utilization on the upstream channels. The CMTS trades upstream bandwidth between data grants and initial ranging slots. The CMTS autodetects a high collision state and switches to low insertion interval mode after a steady state is achieved where few collisions occur.

The CMTS is careful when monitoring the ranging channel health to revert to a steady state. In steady state mode, data grants—grant utilization—receive preference over initial ranging slots.

Although the binary exponential backoff algorithm operates in a distributed fashion at different CMs, the CMTS provides centralized control for the backoff algorithm. To achieve this, it remotely monitors traffic load—the backlog developing on the contention channel—and then varies the backoff start and end specified in the MAPs for that upstream channel. This ensures that colliding CMs are properly randomized in time.

The following cable interface commands are available to configure the dynamic contention algorithms:

```
[no] cable insertion-interval [automatic [Imin [Imax]]] | [msecs]
[no] cable upstream port num range-backoff [automatic] | [start end]
[no] cable upstream port num data-backoff [automatic] | [start end]
```

cable insertion-interval Command Examples

To deviate from system defaults when modifying the dynamic contention algorithm, use one of the **cable insertion-interval** command in cable interface configuration mode. For more information on the command, see cable insertion-interval command.

Tip System defaults are to have dynamic ranging interval enabled, dynamic ranging backoff enabled, and fixed data backoffs for each upstream of a cable interface.

The default automatic insertion interval setting enables the Cisco automatic initial ranging period algorithm, where lower and upper default values of 60 msecs and 480 msecs are used. The default **automatic range-backoff** setting enables the dynamic backoff algorithm.

Configuring the Dynamic Map Advance Algorithm

A Cisco CMTS administrator can enhance the upstream throughput from a CM connected to the Cisco uBR10000 series CMTS. The system employs a new algorithm that automatically tunes the lookahead time in MAPs, based on several input parameters for the corresponding upstream channel. The use of dynamic and optimal lookahead time in MAPs significantly improves the per-modem upstream throughput.

Caution Only a trained Cisco CMTS administrator should adjust these values.

To configure the dynamic map advance algorithm, use the following command in cable interface configuration mode.

Command	Purpose
`cable map-advance dynamic [n]|static`	Specifies a value to enhance the upstream throughput from a CM connected to the Cisco uBR10012 router. The *n* argument provides the safety factor for the dynamic map advance algorithm. This argument is specified in usecs and controls the amount of extra lookahead time in MAPs to account for inaccuracies of the measurement system and software latencies. The default value is 1000 usecs. You can vary this value from 500 to 1500 usecs. This argument is a delta value added to the dynamic **map-advance** setting that the algorithm computes. Using larger safety factors increases the run-time lookahead in MAPs, but reduces the upstream performance. Use the static keyword for the cable map-advance command. The Cisco uBR10012 router uses a fixed lookahead time in MAPs, regardless of the real propagation delay of the farthest CM on the network. This fixed lookahead time is computed based on the worst-case parameters, such as farthest DOCSIS propagation delay for the CMs.

Caution If you are adjusting the dynamic map-advance algorithm, do not reduce the safety factor below the default value of 1000 usecs in a production network, until you are confident that the reduced safety factor suffices for your deployment. The default value is chosen to be a safe operating point for the algorithm.

Configuring Maximum Hosts Attached to a CM

To specify the maximum number of hosts that can be attached to a subscriber's CM, use the following command in cable interface configuration mode.

Command	Purpose
`cable max-hosts n` `no cable max-hosts`	Specifies the maximum number of hosts that can be attached to a CM on this interface. Valid range is from 0 to 255 hosts. Default = 0. Resets the allowable number of hosts attached to a CM to the default value of 0 hosts.

Configuring Per-Modem Filters

You can configure the Cisco uBR10012 router to filter incoming packets from individual hosts or cable interfaces based on the source Media Access Controller (MAC) or Internet Protocol (IP) address. Definition of filters follows standard Cisco IOS configuration practices for access lists and groups.

Note Configuring per modem or host filters is supported in Cisco IOS Release 12.0(5)T1 or higher, as well as in Cisco IOS Release 12.0(6)SC or higher.

To configure per modem filters, use the following commands in cable interface configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cable** {**modem** | **host** | **device**} {*macaddr ipaddr* | } **access group** *acl*	Configure access lists to be specified on a per-interface and per-direction basis. The packets received from cable interfaces and/or individual hosts are filtered based on the cable interface or the host the packets are received from. Use modem if the device is a CM. Use host if the device is a CPE device attached to a CM. Define the filter to be applied to the device and a given address. The macaddr specifies the CM's or CPE device's unique MAC address. Use the ipaddr option to specify the CM or CPE device's current IP address. Use the acl option to assign the CM or CPE device to an access list. This defines the per-CM or per-host filter requirements implemented at the CMTS, rather than at the CM. Access list numbers are 1 to 99 for fast IP access lists, 100 to 199 for show extended IP access lists. **Note** Access list numbers of 700 to 799 do not apply.

What to Do Next

Caution The system applies filters after the CM registers with the CMTS. Filter definitions are not saved across system reboots and must be applied each time a CM registers.

The software supports traps to alert CMTS administrators on CMs going offline or back online. A typical registration and login procedure is shown below:

1. The CM registers with the Cisco uBR10000 series.
2. The Cisco uBR10000 series sends traps to management systems in use for the network.
3. The management system sets per modem filters using SNMP or rsh.
4. The user logs in at the server.
5. The login server obtains required modem and CPE information from the Cisco uBR10000 series.
6. The login server sets per-CPE filter in the Cisco uBR10000 series. The per-CPE filter overrides the per modem filter settings.
7. If the CM goes offline for a brief period of time, filters defined using the Cisco uBR10000 series remain active. If a CM stays offline for more than 24 hours, filter settings are reset.
8. If the user logs out or the login server detects that the user is not online, the login server sets default filters for the CM or the CPE device.

Configuring Sync Message Interval

To specify the sync message interval between successive sync message transmissions from the Cisco uBR10012 router, use the following command in cable interface configuration mode.

Command	Purpose
`cable sync-interval msec` **`no cable sync-interval`**	Specifies the interval in milliseconds between successive sync message transmissions from the Cisco uBR10000 series CMTS. Valid values are from 1 to 200 msec. Default = 10 msec. Returns the sync message interval to its default value of 10 msec.

Verifying Sync Message Interval

To determine if a sync message interval is configured, enter the **show running-config** command and look for the cable interface configuration information. If the sync message interval is deactivated or reset to its default value, the no sync interval command line appears in the output.

CHAPTER 9

Maximum CPE and Host Parameters for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: July 23, 2013

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 how to use different methods to control subscriber access that are allowed by the Data-over-Cable Service Interface Specifications (DOCSIS) for use on cable networks.

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 Maximum CPE and Host Parameters for the Cisco CMTS Routers

The Maximum CPE and Host Parameters for the Cisco CMTS Routers feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SC. The table shows the hardware compatibility prerequisites for this feature.

Table 20: Maximum CPE and Host Parameters 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 • PRE-2 Cisco IOS Release 12.2(33)SCB and later • PRE-4 Cisco IOS Release 12.2(33)SCH and later • PRE-5	Cisco IOS Release 12.2(33)SCA • 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-MC3GX60V1
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X
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

Information About the MAX CPE and Host Parameters

The DOCSIS specification includes a number of provisions to allow service providers to control the number of subscribers who can access the network through any particular cable modem.

The following are the parameters that controls the number of CPE that can access the network:

Note In addition, the DOCSIS configuration file contains a Network Access parameter that specifies whether the CPE devices behind the cable modem can access the cable network. If the Network Access parameter is set to Disabled, no CPE devices behind a cable modem are able to access the network.

Tip Also, the Cisco CMTS lists offline cable modems in its internal database for 24 hours. The CMTS does not reset the CPE counts for these offline cable modems until the 24 hour period expires and the cable modems come back online. If the cable modems come back online before the 24 hour period expires, the CMTS continues to use the existing CPE counts.

All of these methods are similar in purpose, but they are configured differently and have a different impact on cable modems and their CPE devices.

The cable modem enforces the MAX CPE and MAC CPE IP values, and the CMTS enforces the MAX Host value. Because CPE devices can come online and offline at any time, it is important to understand how these different parameters interact, and how the cable modem and CMTS enforce them.

Note The MAX CPE parameter provides Layer 2 control of CPE devices. The MAX CPE IP parameter provides Layer 3 control of CPE devices. The two methods are complimentary but not otherwise related.

MAX CPE

The MAX CPE is a required parameter and used to control the number of CPE devices that can access the network during the current session. In DOCSIS 1.0 cable networks, the MAX CPE parameter is the primary means of controlling the number of CPE devices that can connect to the cable network using any particular cable modem. This parameter is configured in the DOCSIS configuration file (TLV 18). If this parameter is not specified in the DOCSIS configuration file, it defaults to a value of 1.

Note In DOCSIS 1.1 cable networks, the CMTS ignores the MAX CPE parameter that is specified in the DOCSIS configuration file, and uses the MAX CPE IP, on page 110 parameter instead.

Each time a new CPE device attempts to connect to the cable network, the cable modem logs the hardware (MAC) address. If the cable modem has not reached the MAX CPE number of MAC addresses, the new CPE device is allowed to access the network. If the cable modem has reached the MAX CPE limit, it drops the traffic from any additional CPE devices.

By default, the cable modem learns new MAC addresses on a first-come, first-served basis. You can also preconfigure the allowable MAC addresses for CPE devices by entering those MAC addresses in the DOCSIS configuration file (TLV 14). These cable modem gives these preconfigured MAC addresses preference in connecting to the network.

The DOCSIS specification does not allow cable modems to age out MAC addresses, so a MAC address stays in the log table of the cable modem until the cable modem is reset. You should therefore think of this parameter as specifying the maximum number of CPE devices that can connect during any particular session, instead of the maximum number of CPE devices that can simultaneously connect to the cable network.

For example, if you set MAX CPE to 2, a customer could use their cable modem to connect a maximum of two CPE devices (two MAC addresses) to the cable network. A customer could choose to connect two PCs simultaneously to their cable modem and use both to access the network.

However, if the customer then disconnected these PCs and connected two new PCs, the cable modem would not allow the new PCs to come online, because they would be the third and fourth MAC addresses that are connected to the cable modem. The customer would have to reset the cable modem before being able to use the new PCs.

Note The MAX CPE value, if present, must be a positive integer in DOCSIS 1.0 configuration files. This parameter can be zero in DOCSIS 1.1 configuration files, but if so, the cable modem uses a MAX CPE value of 1. If the MAX CPE parameter is not present in either type of DOCSIS configuration file, it defaults to 1.

MAX CPE IP

The MAX CPE IP parameter is applicable only in DOCSIS 1.1 cable networks and is an optional parameter. This parameter specifies whether the cable modem should perform IP address filtering on the CPE devices. If so, this attribute also specifies the maximum number of simultaneous IP addresses that are permitted behind the modem at any one time.

The MAX CPE IP parameter is configured in the DOCSIS configuration file (TLV 35), or by using SNMP commands to set the docsDevCpeIpMax attribute (in DOCS-CABLE-DEVICE-MIB) for the cable modem. By default, this parameter is not enabled and the Cisco CMTS does not actively manage CPE devices, unless you enable the use of the MAX CPE IP parameter by using the **cable submgmt default active** command.

Note In DOCSIS 1.1 networks, the CMTS ignores the MAX-CPE value (TLV 18) from the DOCSIS configuration file and uses the MAX CPE IP value instead.

If this feature is enabled, the cable modem learns the allowable IP addresses the first time that the CPE device sends an IP packet out into the network. The IP addresses are added to the docsDevFilterCpeTable table. This address table is cleared automatically when the cable modem is reset or powered off, or you can manually clear the IP address table by setting the docsSubMgtCpeControlReset attribute in the appropriate table entry for this cable modem.

In DOCSIS 1.1 networks, the MAX CPE IP parameter can be configured as follows:

- If MAX CPE IP is set to –1, the cable modem does not filter any IP packets on the basis of their IP addresses, and CPE IP addresses are not added to the modem's CPE address table
- If MAX CPE IP is set to 0, the cable modem does not filter any IP packets on the basis of the IP addresses. However, the source IP addresses are still entered into the modem's CPE address table.
- If MAX CPE IP is set to a positive integer, it specifies the maximum number of IP addresses that can be entered into the modem's CPE address table. The modem compares the source IP address for packets it receives from CPE devices to the addresses in this table. If a match is found, the packet is processed; otherwise, the packet is dropped.

Tip In Cisco IOS Release 12.2(8)BC1, a similar address filtering mechanism exists on the CMTS. See the description of the docsSubMgtCpeControlMaxCpeIp attribute in the DOCS-SUBMGT-MIB MIB for details.

The CMTS uses the MAX CPE IP value as part of its own filtering process, but the two filters operate independently on the cable modem and CMTS.

MAX CPE IPv6

The MAX CPE IPv6 parameter is an optional parameter and specifies the maximum number of simultaneous IPv6 addresses that are permitted for a cable modem at any time.

The MAX CPE IPv6 parameter is configured in the DOCSIS 3.0 configuration file (TLV 63), or by using the SNMP commands to set the docsSubmgt3BaseCpeMaxIpv6PrefixDef attribute (in DOCS-SUBMGT3-MIB) for the cable modem. By default, this parameter is not enabled and the Cisco CMTS does not actively manage CPE devices, unless the use of the MAX CPE IPv6 parameter is enabled by using the **cable submgmt default active** command.

When the MAX CPE IPv6 feature is enabled, the cable modem learns the allowable IPv6 addresses the first time that the CPE device sends an IPv6 packet out into the network. The IPv6 addresses are added to the IPv6 address table. The address table is cleared automatically when the cable modem is reset or powered off.

In DOCSIS 3.0 networks, the MAX CPE IPv6 parameter can be configured as follows:

- If MAX CPE IPv6 is set to 0, the cable modem filters any IPv6 packets on the basis of the IPv6 addresses. All the source IPv6 addresses are not entered into the CPE address table of the cable modem.
- If MAX CPE IPv6 parameter is set to a positive integer, the parameter specifies the maximum number of IPv6 addresses that can be entered into the CPE address table of the cable modem. The modem compares the source IPv6 address for packets it receives from CPE devices to the addresses in this table. If a match is found, the packet is processed; otherwise the Cisco CMTS ignores the DHCPv6 packets from the CPE.

MAX Host

The MAX Host parameter is an optional parameter and is configured on the Cisco CMTS and specifies the maximum number of CPE devices (MAC addresses) that the CMTS will allow to have network access. You can control this parameter for individual cable modems, for all cable modems on a particular cable interface, or for all cable modems on the Cisco CMTS, depending on the CLI command being used:

- **cable modem max-hosts—**Configures MAX Host for a particular cable modem.
- **cable max-hosts—**Configures MAX Host for all cable modems on a particular cable interface.
- **cable modem max-cpe—**Configures MAX Host for all cable modems on the Cisco CMTS. You can use the **unlimited** keyword to specify that the Cisco CMTS should not enforce a MAX Host limit for cable modems.

When this is enabled, the Cisco CMTS learns a MAC address the first time that the CPE device accesses the cable network. After the Cisco CMTS has logged the maximum number of MAC addresses specified by a MAX Host parameter, it drops all traffic from CPE devices that have any other MAC address.

Tip In DOCSIS 1.1 cable networks, when both the MAX CPE IP and MAX Host parameters are configured, the Cisco CMTS uses the lesser value to determine the maximum number of CPE devices that are allowed behind each cable modem.

Note The entire MAX Host address table is cleared whenever the Cisco TS is reset. You can also clear an entry for a particular CPE device using the **clear cable host** command.

Specifying MAX Host and MAX CPE Values

Typically, you would set the MAX Host parameter to a number that is greater than the value for the MAX CPE of the cable modem or MAX CPE IP parameter. This would allow customers to switch between multiple computers, without requiring them to reboot their cable modem, and without requiring any action on the part of the service provider's network administrators.

For example, if you set MAX CPE or MAX CPE IP to a value of 2 for a cable modem, then you could set the MAX Host parameter to a value of 4. This would enable the cable modem to connect four different CPE devices to the cable network, but only two of them could be online simultaneously.

However, if you set the MAX Host parameter to a number smaller than the value of MAX CPE or MAX CPE IP in the DOCSIS configuration file, then the MAX CPE or MAX CPE IP value always takes precedence. For example, if the MAX CPE value is 2 and the MAX Host value is *1* , both the cable modem and CMTS allow up to two CPE devices to pass traffic for that cable modem.

Specifying an Unlimited Value for Max Host

The **cable modem max-cpe** command, which affects all cable modems on the CMTS, supports the **unlimited** keyword, which specifies that the CMTS should not enforce any limit on CPE devices. When you configure the CMTS with the unlimited **keyword**, this setting, you are allowing cable modems to support any number of CPE devices.

Do not use the **unlimited** option without also specifying the proper value for MAX CPE in the DOCSIS configuration file, so that each cable modem can control the maximum number of CPE devices it supports. In addition, to prevent users from requesting an unlimited number of IP address, be sure to configure the DHCP servers so that they control how many IP addresses are assigned to the CPE devices behind each cable modem.

Interoperation of the Maximum CPE Parameters

The different methods of CPE control can all be active simultaneously. They can interact with one another but do not conflict with one another. The table lists each method and compares their characteristics.

Table 21: Comparison of the Different Max CPE and Max Host Control Mechanisms

Method	Configuration Method	Function	Can Be Changed By...
Methods that are configured on the cable modem:			
Network Access Control	DOCSIS Configuration File	Prevents all network access for CPE devices	Reset of cable modem
MAX CPE	DOCSIS Configuration File	Limits MAC addresses (Layer 2 control)	Reset of cable modem
MAX CPE IP	DOCSIS Configuration File SNMP Set Command	Limits IP addresses (Layer 3 control)	SNMP Set Command
Methods that are configured on the CMTS: [13]			
MAX CPE IP (the CMTS uses this value if MAX CPE IP is not specified in the DOCSIS configuration file)	DOCSIS Configuration File CLI Command SNMP Set Command	Limits IP addresses (Layer 3 control)	CLI Command SNMP Set Command
MAX Host Parameters			
MAX Host for one cable modem (**cable modem max-hosts**)	CLI Commands	Limits CPE devices for one particular cable modem	New CLI Command
MAX Host for a cable interface (**cable max-hosts**)		Limits CPE devices for all cable modems on a particular cable interface	
MAX Host for a CMTS (**cable modem max-cpe**)		Limits CPE devices for all cable modems on a Cisco CMTS	

13 In Cisco IOS Release 12.2(4)BC1 and later releases, the Cisco CMTS does not actively manage CPE devices unless this has been enabled using the cable submgmt default active command.

The table lists the MAX CPE parameters in order of priority. For example, the Network Access Control and MAX CPE parameters interact as follows:

- If the Network Access Control field for a cable modem is set to Disabled, none of that modem's CPE devices will be able to access the network, regardless of how the other parameters are set.
- If Network Access Control is Enabled and MAX CPE is set to 1 for a cable modem, then a maximum of one CPE device will be able to access the network, no matter how the remaining parameters are configured.

The table also lists the MAX Host parameters in order of more specific to less specific, where the more specific override the settings of the less specific. For example, if you use the **cable modem max-cpe** command to set

the MAX Host value for all CMs to 2, you can still use the **cable modem max-hosts** command to give a particular CM a MAX Host value of 8.

In addition, the MAX CPE IP and MAX Host parameters interact as follows:

- When both the MAX CPE IP parameter and the MAX Host parameter for a specific cable modem are specified, the CMTS uses the value specified for MAX Host for that particular modem.
- When both the MAX CPE IP parameter and the MAX Host parameter for a cable interface are specified, the CMTS uses the larger value of the two.
- When both the MAX CPE IP parameter and the MAX Host parameter for the CMTS are specified, the CMTS uses the smaller value of the two.

Tip The Cisco CMTS keeps inactive cable modems listed in its internal database for 24 hours. The CMTS does not reset the CPE counts for these offline cable modems until the 24 hour period expires and the cable modems come back online. If the cable modems come back online before the 24 hours expires, the CMTS continues to use the existing CPE counts.

Possible Conflicts Between Parameters

The recommended procedure for disconnecting one PC from a cable modem and reconnecting a new one is the following:

1. The user first releases the IP address assigned to the PC. The user can do this either by using a utility such as winipcfg, or by shutting down the PC.
2. The user disconnects the old PC and reconnects the new PC to the cable modem.
3. The user reboots the cable modem so as to clear out its MAX CPE values.
4. After the cable modem has come online, the user boots the new PC so that it can obtain the correct IP address and come online.

This procedure allows the MAX CPE value on the cable modem to stay synchronized with the MAX Host value on the CMTS. Problems can occur in the following situations:

- If the user does not release the IP address from the old PC before connecting a new one, the CMTS is not informed that the new PC is replacing the old one, and therefore counts both PCs when calculating the Host value. If the new value exceeds the MAX Host value, the CMTS does not allow the new PC to come online. The service provider has to issue the **clear cable host** command to remove the old PC from the MAX Host table, so as to allow the new PC to come online.
- If the user does not reboot the cable modem after disconnecting the old PC, the cable modem retains the old PC's MAC address and continues to count it when calculating the CPE value. If the new value exceeds the MAX CPE value, the cable modem does not allow the new PC to come online. The user has to reboot the cable modem before the new PC comes online.
- If the user booted their PC before turning on the cable modem or before connecting the Ethernet cable to the cable modem. In this case, the operating system typically assigns a static private IP address (such as 169.254.232.199, which is the default Windows IP address). When the cable modem then boots or is connected to the PC, it logs the PC's private IP address as one of the allowable IP addresses. So, if MAX CPE IP is set to 1, the PC will not be allowed access to the Internet. You must reboot the cable modem to clear its IP address tables, and allow the PC to acquire an IP address from the DHCP server. (To avoid this problem, set the docsDevCpeIpMax attribute for the cable modem to –1 in the DOCSIS

configuration file. CableLabs has proposed –1 as the new default, but this change has not yet been given final approval or been implemented in current software releases.)

To reduce service-impacting problems when users replace PCs without following the above guidelines, service providers can configure the MAX Host parameter for a value greater than the MAX CPE value. This allows users to replace a limited number PCs without releasing the IP address and still be able to come online. (Users should continue to reboot the cable modem, however, because that is the only way to clear their internal CPE counter.)

For example, if you configure MAX CPE for a cable modem at 2, and MAX Host at 4, the user can connect any two PCs to the cable modem at any one time. The user can then replace both PCs with new PCs, reboot the cable modem, and have both PCs come online.

The CMTS CPE table for this cable modem lists all four PCs, and the user can switch between them at will, as long as the user reboots the cable modem after each switch. The user, however, is not allowed to bring a fifth PC online until one of the previous PCs has been cleared from the CMTS, using the **clear cable host** command.

Note The cable modem always enforces the MAX CPE parameter, regardless of the setting of the other parameters.

Summary of CPE Address Control

In DOCSIS 1.1 cable networks, CPE address control is done as part of the following process, which also includes Layer 2 and Layer 3 filtering:

1. MAC address filtering—Packets are filtered on the basis of the MAC address for the CPE device. The filter is controlled by the MAX CPE parameter, as set in the DOCSIS configuration file.
2. Logical Link Control (LLC) filtering—Packets are filtered on the basis of the protocol for the packets. The filter is controlled by the docsDevFilterLLCTable table on the cable modem.
3. CPE IP address filtering—Packets are filtered on the basis of the IP address for the CPE device, as controlled by the MAX CPE IP value, as well as the docsDevCpeIpMax attribute and the docsDevFilterCpeTable table on the CMTS.
4. Access list filtering—Packets are filtered on the basis of access lists. IP filtering is controlled by the docsDevFilterIpTable table, and SNMP access filters are controlled by the docsDevNmAccessTable table.
5. MAX Host control—The CMTS allows access for CPE devices on the basis of the MAX Host parameters.

Tip This document does not describe the LLC and access list filtering. For more information about these filters, see the DOCS-CABLE-DEVICE-MIB MIB for more information on the SNMP attributes and tables that are listed above.

Benefits

- CMTS flexibility allows multiple service operator provisioners, service providers, and other users to synchronize between the CMTS and the cable modem the maximum number of permitted CPE devices that can be connected behind a cable modem.

- Changes can be made by using CLI commands or by using SNMP commands.

How to Configure the MAX CPE and Host Parameters

To reset the maximum number of permitted CPE devices recognized by the CMTS, use one of the following configuration commands. All procedures are optional, depending on the requirements.

Note The CMTS assigns the MAX Host value to a cable modem at the time that the cable modem registers with the CMTS. Changing any of the MAX Host commands affects only cable modems that register after the change.

Configuring the Maximum Number of CPE Devices on the Cisco CMTS

To configure the maximum number of CPE devices per cable modem, use the following procedure:

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 modem max-cpe** [*number* | **unlimited**] **Example:** `Router(config)# cable modem max-cpe 8`	Sets the value of the MAX CPE parameter on the Cisco CMTS for all cable interfaces. If *number* is smaller than the MAX CPE value in the DOCSIS configuration file of the cable modem, this command overrides the configuration file value. If *number* is larger than the cpe-max value in the DOCSIS configuration file of the cable modem or or is set to **unlimited**, the value set in the configuration file takes precedence. **Note** If the value in the configuration file is zero and **no cable modem max-cpe** is configured, then no CPE device is able to obtain an IP address.
Step 4	**cable submgmt default active** **Example:** `Router(config)# cable submgmt`	Specifies that the CMTS should actively manage CPE devices. The default is the **no** version of this command, so that the CMTS does not actively manage CPE devices.

	Command or Action	Purpose
	`default active`	**Note** This command is required before the Cisco CMTS manages the CPE devices when running a Cisco IOS Release 12.2 BC software image.
Step 5	**cable submgmt default max-cpe** *cpe-num* **Example:** `Router(config)# cable submgmt default max-cpe 4`	(Optional) Specifies the default value for the MAX-CPE parameter that the CMTS should use when the cable modem does not specify a MAX-CPE value in its DOCSIS configuration file.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

What to Do Next

Note Use of the **cable modem max-cpe unlimited** command can open a security hole in the system by enabling denial of service attacks. It could allow a single user to obtain a large number of IP addresses, and thereby cause the entire network to go down after this single user has reserved all available IP addresses.

Configuring the Maximum Number of Hosts for a Cable Interface

Complete these steps to configure maximum number of hosts for 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	**interface cable** *x/y* **Example:** `Router(config)# interface cable 4/0`	Enters cable interface configuration mode for the specified cable interface:
Step 4	**cable max-hosts** *number* **Example:** `Router(config-if)# cable max-hosts 10`	Specifies the maximum number of hosts that each cable modem on this cable interface can support.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring the Maximum Number of Hosts for a Particular Cable Modem

Complete these steps to configure the maximum number of hosts for a particular cable modem:

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**cable modem** {*mac-addr* | *ip-addr* } **max-hosts** {*number* | **default**} **Example:** `Router# cable modem 000C.0102.0304 max-hosts 8`	Specifies the maximum number of hosts allowed behind this particular cable modem.

Configuring the Maximum Number of IPv6 addresses for a Cable Modem on the Cisco CMTS

Complete these steps to configure the maximum number of IPv6 addresses for a cable modem in Cisco CMTS:

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 modem v6-max-cpe-prefix** [n] **Example:** `Router(config)# cable modem v6-max-cpe-prefix 10`	Specifies the maximum number of IPv6 addresses for a cable modem on the Cisco CMTS for all cable interfaces.
Step 4	**cable submgmt default active** **Example:** `Router(config)#cable submgmt default`	Specifies that the CMTS should actively manage CPE devices. The default is the **no** form of this command, so that the CMTS does not actively manage CPE devices. **Note** This command is required before the Cisco CMTS manages CPE devices when running a Cisco IOS Release 12.2 BC software image.
Step 5	**exit** **Example:** `Router(config)#exit`	Exits global configuration mode.

Configuration Examples for the MAX CPE and Host Parameters

The following example shows how to allow the CMTS to recognize a maximum of four CPE devices attached to online cable modems for a CMTS:

```
cable modem max-cpe 4
```

The following example shows how to set the maximum CPE devices recognized by the CMTS for a cable interface to 15:

```
cable max-hosts 15
```

The following example shows how to allow the CMTS to recognize a maximum of 30 attached CPE devices for a specific cable modem of IP address 172.172.172.12:

```
cable modem 172.172.172.12 max-hosts 30
```

Configuration Examples

To display the current configuration and status of a cable interface, use the **show running-config** command in privileged EXEC mode. The following is sample output that shows that the CMTS permits up to five CPE devices to use the specified cable interface to pass traffic.

```
interface Cable3/0
 ip address 192.168.1.1 255.255.255.0 secondary
 ip address 10.1.1.1 255.255.255.0
 load-interval 30
 no keepalive
 cable max-hosts 5
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 507000000
 cable upstream 0 frequency 27008000
 cable upstream 0 power-level 0
 cable upstream 0 minislot-size 32
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 29008000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot-size 4
 no cable upstream 1 shutdown
 cable dhcp-giaddr policy
 cable helper-address 172.17.110.131
end
```

You can also use the **more system:running-config** command to verify the maximum number of permitted CPE devices for a cable interface.

```
CMTS01# more system:running-config
Building configuration...
Current configuration:
!
interface Cable6/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
 cable max-hosts 4
 cable insertion-interval 2000
```

```
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
```

You can use the **show cable modem detail** command to list information on each CPE device permitted for a cable modem. The command displays the max cpe value as configured in the DOCSIS configuration file for the cable modem, and in parentheses the value of *n* configured in the **cable modem max-cpe** command, if different. See the following sample output where the CMTS is configured for max-cpe equal to four and then max-cpe equal to unlimited:

```
test-cmts# show cable modem detail

Interface         SID MAC address   Max CPE Concatenation Rx SNR
Cable4/0/U0 1      0001.9659.47bb    1      yes           37.37
Cable4/0/U0 2      0001.9659.47ab    1      yes           33.70
Cable4/0/U0 3      0001.9659.47bf    1      yes           30.67
Cable4/0/U0 4      0001.9659.3ef7    1      yes           28.84
Cable4/0/U0 5      0001.9659.47eb    1      yes           30.89
test-cmts# conf t
Enter configuration commands, one per line. End with CNTL/Z.
test-cmts(config)# cable modem max-cpe ?
<1-255> Number
unlimited Max CPE not enforced
test-cmts(config)# cable modem max-cpe 4
test-cmts(config)# end
test-cmts#
00:05:11: %SYS-5-CONFIG_I: Configured from console by console
test-cmts# show cable modem detail
Interface        SID MAC address   Max CPE Concatenation Rx SNR
Cable4/0/U0 1      0001.9659.47bb .1 (4)        yes       37.00
Cable4/0/U0 2      0001.9659.47ab .1 (4)        yes       33.54
Cable4/0/U0 3      0001.9659.47bf .1 (4)        yes       30.70
Cable4/0/U0 4      0001.9659.3ef7 .1 (4)        yes       29.00
Cable4/0/U0 5      0001.9659.47eb .1 (4)        yes       30.92
test-cmts# conf t
Enter configuration commands, one per line. End with CNTL/Z.
test-cmts(config)# cable modem max
test-cmts(config)# cable modem max-cpe ?
<1-255> Number
unlimited Max CPE not enforced
test-cmts(config)# cable modem max-cpe unli
test-cmts(config)# cable modem max-cpe unlimited
test-cmts(config)# ^Z

test-cmts#
00:06:06: %SYS-5-CONFIG_I: Configured from console by console
test-cmts# show cable modem detail
Interface      SID MAC address      Max CPE Concatenation Rx SNR
Cable4/0/U0 1      0001.9659.47bb   1 (ul)      yes          36.64
Cable4/0/U0 2      0001.9659.47ab   1 (ul)      yes          33.26
Cable4/0/U0 3      0001.9659.47bf   1 (ul)      yes          30.73
Cable4/0/U0 4      0001.9659.3ef7   1 (ul)      yes          29.15
Cable4/0/U0 5      0001.9659.47eb   1 (ul)      yes          30.95
```

Additional References

For additional information related to configuring the MAX CPE and Host parameters on the Cisco CMTS, refer to the following references:

Related Documents

Related Topic	Document Title
Cisco CMTS Commands	Cisco CMTS Cable Command Reference
Interaction of MAX CPE Parameters	Using the max-cpe Command in the DOCSIS and CMTS

Standards

Standards[14]	Title
SP-RFIv1.1-I08-020301	*Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification , version 1.1* (http://www.cablelabs.com/cablemodem/)

14 Not all supported standards are listed.

MIBs

MIBs[15]	MIBs Link
DOCS-CABLE-DEVICE-MIB DOCS-SUBMGT-MIB DOCS-SUBMGT3-MIB	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

15 Not all supported MIBs are listed.

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 Maximum CPE and Host Parameters 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 22: Feature Information for Maximum CPE and Host Parameters for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.0(6)SC	This feature was introduced on the Cisco uBR7200 series universal broadband routers.
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.0(10)SC	The **cable modem max-cpe** command was introduced for the Cisco uBR7200 series universal broadband routers.
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.1(2)EC1	This feature was integrated into Cisco IOS Release 12.1(2)EC1.
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.1(5)EC	Support was added for the Cisco uBR7100 series universal broadband routers.
Maximum CPE and Host Parameters for the Cisco CMTS Routers	12.2(4)BC1	This feature was integrated into Cisco IOS Release 12.2(4)BC1 on the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 universal broadband routers.
Maximum CPE and Host Parameters for the Cisco CMTS Routers	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.

Feature Name	Releases	Feature Information
TLV63 Support	12.2(33)SCH1	The **cable modem v6-max-cpe-prefix** command was introduced to limit the maximum number of IPv6 addresses per cable modem for the Cisco uBR10012 and Cisco uBR7200 series universal broadband routers.

CHAPTER 10

Power and Thermal Monitoring on the Cisco CMTS Routers

First Published: May 10, 2010

The power and thermal monitoring feature provides monitoring options for the thermal and power consumption of the Cisco UBR-MC20X20V cable interface line card.

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 Power and Thermal Monitoring

The table shows the hardware compatibility prerequisites for this feature.

Table 23: Power and Thermal Monitoring for the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCD2 and later • PRE4	Cisco IOS Release 12.2(33)SCD2 and later • Cisco UBR-MC20X20V[16]

16 The Cisco UBR-MC20X20V cable interface line card has three variants: Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D. The Cisco UBR-MC20X20V-0D line card supports 20 upstreams and zero (no) downstreams. The Cisco UBR-MC20X20V-5D line card supports 20 upstreams and 5 downstreams, and the Cisco UBR-MC20X20V-20D line card supports 20 upstreams and 20 downstreams.

Note Any reference to the Cisco UBR-MC20X20V cable interface line card used in this document is also applicable to its three variants—Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D.

- The Cisco UBR10012 universal broadband router must be running Cisco IOS 12.2(33)SCD2 release or later.

Restrictions for Power and Thermal Monitoring

The Power and Thermal Monitoring feature has the following restrictions and limitations:

- The power and thermal monitoring facility is enabled by default and you cannot disable it.
- The thermal thresholds are predefined and you cannot configure or modify them.

Information About Power and Thermal Monitoring

The power and thermal monitoring feature provides monitoring options for the thermal and power consumption of the Cisco UBR-MC20X20V cable interface line card. The power and thermal monitoring facility monitors the line card at several different points (See Table 24: Thermal Thresholds for the Cisco UBR-MC20X20V Line Card) to see whether it is overheating or drawing too much power.

The monitoring facility triggers an alert when the operational thresholds are exceeded. Alerts are in the form of syslog messages, alarms, and SNMP traps. Syslog messages are generated when the temperature sensors cross their respective thermal threshold levels. Alarms and SNMP traps are generated only when the inlet sensors cross their thresholds. In addition to the alerts, the power consumption of the line card is checked periodically by the monitoring facility.

The following sections describe the Power and Thermal Monitoring feature in more detail:

Thermal Monitoring

The thermal monitoring facility uses temperature sensors, placed at several different points in the line card, to monitor the thermal threshold levels. Each temperature sensor is monitored against the thermal threshold levels that are specific to the sensor.

The table shows the sensors monitored and their corresponding thresholds.

Note The thermal thresholds shown in the table are predefined and you cannot configure or modify them.

Table 24: Thermal Thresholds for the Cisco UBR-MC20X20V Line Card

Sensor	Minor Threshold (in Celsius)	Major Threshold (in Celsius)	Critical Threshold (in Celsius)
Nickel 10G	82	87	92
CPU	73	78	83
Inlet	68	73	78
Remora	82	87	92
Coldplay	75	80	85
Waxbill	92	97	102
Fauna	82	87	92
Flora	80	85	90
Toucan FPGA A	94	97	100
Toucan FPGA B	94	97	100
Toucan FPGA C	94	97	100

The Cisco UBR-MC20X20V cable interface line card thermal monitoring has three levels of monitoring thresholds: Minor, Major, and Critical. The table shows the thresholding states and their corresponding descriptions.

Table 25: Thresholding States for the Cisco UBR-MC20X20V Line Card

State	Description
Minor	The temperature sensor moves to minor state when the sensor readings stay constant for 2 minutes between minor and major (>= minor and < major) thresholds.
Major	The temperature sensor moves to major state when the sensor readings stay constant for 2 minutes between major and critical (>= major and < critical) thresholds.
Critical	The temperature sensor moves to critical state when the sensor readings stay above the critical (>= critical) threshold.

The temperature sensors are monitored every 2 minutes, with a soaking interval (A soaking interval defines how long a condition must persist before an alarm is declared.) of 2 minutes for minor and major events; there is no soaking interval for critical events.

The following alerts are generated on the Cisco UBR-MC20X20V cable interface line card:

- A syslog error message is generated when a thermal threshold is broken. The syslog error message contains sensor name, reading, threshold state, value, event timestamp, and card power level.
- Alarms and SNMP traps are generated when the inlet sensor crosses its threshold.

Note A high availability (HA) switchover is not initiated for the Cisco UBR-MC20X20V cable interface line card when the temperature sensors cross the critical threshold.

The temperature history of the router is maintained for an hour, with timestamp. It can be viewed using the show environment command. The show environment command displays the PRE temperature, fan status, power supply details, and the thermal and power status of the line card. The slot/subslot option of the show environment command helps to identify the location of the line card.

The thermal monitoring data is exclusive to the Cisco UBR-MC20X20V cable interface line card. When the line card is reset or removed, the outstanding temperature alarm is cleared. However, you can still view the temperature history of the line card that was maintained by the OBFL feature using the show logging onboard slotindex temperature command.

In the event of a line card crash, the temperature history of the line card is viewable from the crashinfo file. The crashinfo file contains the temperature history of the line card for the last one hour before the crash. The data is displayed using the show logging onboard command. See the Onboard Failure Logging feature guide for more details.

A PRE switchover does not impact the monitoring functionality of the line card. All the outstanding temperature threshold alarms are retained.

Power Monitoring

The following power monitoring options are implemented on the Cisco UBR-MC20X20V cable interface line card:

- The power consumption is monitored every 2 minutes.
- The power consumption history of the line card is maintained for an hour, with timestamp. You can view it using the show environment command.

The power consumption history of the line card is not maintained after an OIR; the history is erased and it cannot be retrieved. However, in case of a line card crash, the power consumption history of the line card is available from the crash log file for the last one hour before the crash. The syslog error message also captures the line card power consumption details at the time of the thermal threshold breach.

Alerts

The thermal and power monitoring feature triggers an alert when the operational thresholds are exceeded.

The Cisco uBR10012 universal broadband router uses the following types of alerts:

- Alarms
- SNMP Traps
- Syslog Messages

Alarms

The monitoring facility triggers an alarm when the inlet sensor of the Cisco UBR-MC20X20V cable interface line card breaches a predefined thermal threshold. The temperature status of the line card is maintained by the RP in Cisco uBR10012 universal broadband router. When the temperature varies, the line card passes the information to the RP to fire an alarm and SNMP trap. The RP clears the current outstanding temperature alarm and generates a new alarm. You can view these alarms using the show facility alarm status command.

SNMP Traps

SNMP traps are generated when the inlet temperature sensor of the Cisco UBR-MC20X20V cable interface line card has a status change among normal, minor, major or critical. You can view the SNMP traps through the SNMP manager. To disable SNMP traps, use the no form of the snmp-server enable traps envmon [temperature] command.

The following MIBs are used to generate SNMP traps when the line card crosses thermal thresholds:

- ciscoEnvMonTempStatusChangeNotif: This SNMP trap is generated when the inlet temperature status changes among normal, minor, major or critical.
- ciscoEnvMonTemperatureNotification: This SNMP trap is generated when the inlet temperature status changes from normal to minor, major or critical.

The following is a sample SNMP trap output from SNMP Manager:

```
Received SNMPv2c Trap:
Community: public
From: 10.11.0.17
mib_2.1.3.0 = 500023
internet.6.3.1.1.4.1.0 = ciscoEnvMonTempStatusChangeNotif
ciscoEnvMonTemperatureStatusDescr.6 = Inlet SubSlot 6/1
ciscoEnvMonTemperatureStatusValue.6 = 70
ciscoEnvMonTemperatureState.6 = warning(2)
Received SNMPv2c Trap:
Community: public
From: 10.11.0.17
mib_2.1.3.0 = 500023
internet.6.3.1.1.4.1.0 = ciscoEnvMonTemperatureNotification
ciscoEnvMonTemperatureStatusDescr.6 = Inlet SubSlot 6/1
ciscoEnvMonTemperatureStatusValue.6 = 70
ciscoEnvMonTemperatureState.6 = warning(2)
```

Syslog Messages

Syslog error messages are generated when the temperature sensor of the Cisco UBR-MC20X20V cable interface line card crosses a thermal threshold. The syslog error message also contains the power consumption level of the line card during the time of thermal threshold crossover event.

The following is a sample syslog error message output:

```
SLOT 6/1: Apr  6 19:08:02.584: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: CPU temperature MINOR
limit (73 degC) exceeded at temperature 74 degC and power 172.217 watts
SLOT 6/1: Apr  6 19:50:02.652: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Nickel 10G temperature
 MINOR limit (82 degC) exceeded at temperature 83 degC and power 172.897 watts
SLOT 6/1: Apr  6 19:50:04.152: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Waxbill temperature
MINOR limit (92 degC) exceeded at temperature 93 degC and power 172.897 watts
SLOT 6/1: Apr  6 19:58:04.168: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Remora temperature MINOR
 limit (82 degC) exceeded at temperature 83 degC and power 172.217 watts
SLOT 6/1: Apr  6 19:58:05.668: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Coldplay temperature
MINOR limit (75 degC) exceeded at temperature 75 degC and power 172.217 watts
SLOT 6/1: Apr  6 19:58:07.168: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Fauna temperature MINOR
 limit (82 degC) exceeded at temperature 83 degC and power 172.217 watts
SLOT 6/1: Apr  6 19:58:08.668: %CLCENVM-6-TEMPTHRESHOLDEXCEED: 6/1: Flora temperature MINOR
 limit (80 degC) exceeded at temperature 81 degC and power 172.217 watts
```

How to Configure Power and Thermal Monitoring

This section contains the following procedure:

Power and Thermal Monitoring Configuration

The power and thermal monitoring facility for the Cisco UBR-MC20X20V cable interface line card is enabled by default and you cannot disable it. However, you can disable the facility alarms using the no form of the facility-alarm command. Similarly, you can use the no form of the snmp-server enable traps envmon [temperature] command to disable SNMP traps.

Monitoring Power and Thermal Information

To monitor the Power and Thermal Monitoring facility, use the following procedures:

Viewing Thermal and Power Information

To view information about the power and thermal monitoring of the Cisco UBR-MC20X20 cable interface line card, use the **show environment** command in privileged EXEC mode.

For a complete description of the command, see the Cisco IOS Cable Command Reference Guide on Cisco.com.

Example

The following example shows a typical display for the **show environment** command.

```
Router# show environment subslot 7/0
-----------------------------------------------------------------------
TEMPERATURE/POWER INFORMATION
-----------------------------------------------------------------------
Number of Temperature Sensors : 11
Sampling frequency            : 2 minutes
-----------------------------------------------------------------------
Sensor       | ID | Current     | Minor | Major | Critical | Alarm     |
             |    | Temperature |       Threshold          | Condition |
             |    |     0C      |          0C              |           |
-----------------------------------------------------------------------
Nickel 10G     1       48          82    87      92        Normal
Inlet #1       2       36          68    73      78        Normal
CPU            3       44          73    78      83        Normal
Remora         4       48          82    87      92        Normal
Coldplay       5       40          75    80      85        Normal
Waxbill        6       53          92    97      102       Normal
Fauna          7       46          82    87      92        Normal
Flora          8       47          80    85      90        Normal
Toucan FPGA A  9       45          94    97      100       Normal
Toucan FPGA B  10      36          94    97      100       Normal
Toucan FPGA C  11      47          94    97      100       Normal
-----------------------------------------------------------------------
Power: 168.813 watts
-----------------------------------------------------------------------
-------------------------------------------------------------------------------------------
       Time Stamp       |  Power  |  Sensor Temperature 0C
MM/DD/YYYY HH:MM:SS     |  watts  |  1    2    3    4    5    6    7    8    9   10   11
-------------------------------------------------------------------------------------------
09/30/2009 10:24:26       168.813    48   36   44   48   40   53   46   47  45   36   47
09/30/2009 10:22:26       168.813    48   36   44   48   40   53   46   47  45   36   47
09/30/2009 10:20:26       168.813    48   36   44   47   40   53   46   47  45   36   47
09/30/2009 10:18:26       168.813    48   36   44   47   40   53   46   47  45   36   47
09/30/2009 10:16:26       168.813    47   36   44   47   40   53   46   47  45   36   47
09/30/2009 10:14:26       168.813    47   36   44   47   40   53   46   47  45   36   47
09/30/2009 10:12:26       168.813    47   36   44   46   40   52   45   47  45   36   47
09/30/2009 10:10:26       168.813    47   35   44   45   39   51   45   47  45   36   47
09/30/2009 10:08:26       168.132    46   35   44   43   38   50   43   47  45   36   47
-------------------------------------------------------------------------------------------
```

Viewing Thermal and Power Monitoring Alarms

To view the power and thermal monitoring alarms of the Cisco UBR-MC20X20 cable interface line card, use the show facility-alarm status command in privileged EXEC mode.

For a complete description of the command, see the Cisco IOS Cable Command Reference Guide on Cisco.com.

Example

The following example shows a typical display for the **show facility-alarm status** command.

```
Router# show facility-alarm status
Thresholds:
Intake minor 45 major 54 critical 67
Outlet minor 48 major 58 critical 85
System Totals  Critical: 1  Major: 1  Minor: 1
Source              Severity      ACO        Description [Index]
------              --------      ---        -------------------
chassis             MINOR         NORMAL     Subslot 7/0 Inlet temperature limit
chassis             MAJOR         NORMAL     Subslot 7/1 Inlet temperature limit
chassis             CRITICAL      NORMAL     Subslot 8/0 Inlet temperature limit
```

Additional References

The following sections provide references related to the Power and Thermal Monitoring feature.

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
Onboard Failure Logging	Onboard Failure Logging
Cisco Cisco UBR-MC20X20V Cable Interface Line Card Hardware Installation Guide	Cisco UBR-MC20X20V Cable Interface Line Card Hardware Installation Guide

Standards

Standards	Title
None	—

MIBs

MIBs[17]	MIBs Link
• CISCO-ENVMON-MIB	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

17 Not all supported MIBs are listed.

RFCs

RFCs	Title
None	—

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 Power and Thermal Monitoring 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 26: Feature Information for Power and Thermal Monitoring on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Power and Thermal Monitoring	12.2(33)SCD2	The Power and Thermal Monitoring feature was introduced for the Cisco UBR-MC20X20V line card. The following section provides information about this feature: The following command was modified: • **show environment**

CHAPTER 11

PXF Divert Rate Limit Enhancement on the Cisco CMTS Routers

First Published: December 18, 2008

Last Updated: January 28, 2016

This document describes the Parallel eXpress Forwarding (PXF) Divert Rate Limit (DRL) Enhancement on the Cisco Cable Modem Termination System (CMTS). This feature prevents congestion of packets on the forwarding processor (FP) or the PXF processor to the Route Processor (RP) interface, which can be caused by denial of service (DoS) attacks directed at the CMTS or by faulty hardware.

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 PXF DRL Enhancement

The PXF DRL Enhancement feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.2(33)SCB. The table shows the Cisco CMTS 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 27: PXF DRL Enhancement Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later** • PRE2	**Cisco IOS Release 12.2(33)SCB 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 [18]

[18] Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.

Restrictions for PXF DRL Enhancement

- DRL cannot be configured on a cable bundle interface.
- The trusted-site list can contain a maximum of four sites.
- WAN-IP entities are identified using a hash, and hash collisions can occur between two (or more) entities.
- The DRL feature is always on; it cannot be turned off.
- The PXF DRL Enhancement feature is not applicable to Address Resolution Protocol (ARP) packets arriving from a cable interface. These packets are rate limited by the ARP filter feature.

Information About PXF DRL Enhancement

The PXF DRL Enhancement feature prevents congestion of the FP-to-RP interface by identifying and rate-limiting entities that would otherwise cause congestion.

Diverted packets are sent from the forwarding processor to the Route Processor through the FP-to-RP interface. This interface gets congested when packets (that require diversion) arrive at the FP at a faster rate than they can be transmitted to the RP. When the interface gets congested, valid packets in the FP-to-RP queues are tail-dropped. This situation can be caused deliberately by DoS attacks directed at the CMTS, or by faulty external hardware.

The PXF DRL Enhancement feature identifies packet streams that cause congestion on the FP-to-RP interface. Packets in the stream are then dropped according to the configured rate-limiting parameters. Rate-limiting occurs before the packets are placed in the FP-to-RP queues, thereby allowing other valid packets to reach the RP.

The PXF DRL Enhancement feature applies to both cable and WAN interfaces.

Even if the DRL (per source based divert rate limit) is configured on the WAN interface, sometimes the RP gets overloaded due to Distributed Dos (DDos) attack. The DDos attack is seen when the following occurs:

- When the packets are being pointed to the CMTS directly.
- When the packets are being pointed to a CPE. If the CPE goes down and all traffic gets punted to PRE.

Effective with Cisco IOS Release 12.2(33)SCH3, when the DDos occurs and the flooding packets have one of the support divert codes, the DRL Max-Rate Per Divert-Code on WAN Interface can be configured to reduce the CPU utilization.

PXF DRL Enhancement on a Cable Interface

The PXF DRL Enhancement feature applies to upstream packets from a cable interface. In cable, the entities must be rate-limited on a deterministic basis. Because certain entities (for example, VoIP calls) must be able to divert packets successfully, a probabilistic model cannot be used. As a result, the Media Access Control (MAC)-domain and service identifier (SID) identifies the subscribers. DRL aggregates and limits all diverted traffic originating from a subscriber.

PXF DRL Enhancement on a WAN Interface

The PXF DRL Enhancement feature applies to packets from a non-cable interface (typically a Gigabit Ethernet line card.) WAN-side entities cannot be rate-limited on a deterministic basis due to the large number of entities that can exist. Therefore, a probabilistic model (that is, a hash) is used to identify packet streams. This means that not all entities will be uniquely identified.

IP packet streams are identified and rate-limited by a hash of the source IP address, the fib-root (for example, the VPN routing and forwarding [VRF] name), and the divert code. Non-IP packet streams are not expected on the WAN interface, and are therefore rate-limited on a divert code basis.

A WAN-side “trusted-site” list can be maintained, with a maximum of four trusted sites. Each entry in the “trusted-site” list contains an IP address and mask, an IP type of service (ToS) value and mask, and a VRF name. Packets matching a trusted site will not be subject to rate-limiting. In addition, packets from trusted sites will not affect the rate-limiting of packets from other entities.

How to Configure PXF DRL Enhancement on the Cisco CMTS Routers

This section describes the following required and optional procedures:

Configuring US Cable Divert-Rate-Limit

The cable side DRL is configured on the physical cable interface. It cannot be configured on a cable bundle interface. To configure cable DRL, use the **cable divert-rate-limit** 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** *interface* **Example:** `Router(config)# interface C5/0/0`	Enters interface configuration mode for the specified interface. • **interface—**Specifies the name of the physical Cable interface.
Step 4	**cable divert-rate-limit rate** *rate* **limit** *limit* **Example:** `Router(config-if)#` **cable divert-rate-limit rate 1 limit 4**	Specifies the DRL rate and limit. • **rate—**Specifies the divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second. The default rate is 2000 packets per second. • **limit—**Specifies the number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets. The default limit is 2000 packets.
Step 5	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN IPv4 Rate and Limit

To configure DRL for WAN-side IPv4 packet streams, use the **service divert-rate-limit ip** 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	**service divert-rate-limit ip** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)#` **service divert-rate-limit ip fib-rp-glean rate 1 limit 4**	Specifies the DRL rate and limit for the WAN interface. • **divert-code—**Specifies the applicable divert code. • **rate—**Specifies the divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second. For WAN-IP packets, the default rate is 4000 packets per second. • **limit—**Specifies the number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets. For WAN-IP packets, the default limit is 4000 packets.
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN IPv6 Rate and Limit

To configure DRL for WAN-side IPv6 packet streams, use the **service divert-rate-limit ipv6** command.

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	**service divert-rate-limit ipv6** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)# service divert-rate-limit ipv6 ipv6_rp_glean rate 20 limit 10`	Specifies the DRL rate and limit for the WAN interface. • *divert-code*—Applicable divert code. Refer to the list of divert codes in Cisco IOS CMTS Cable Command Reference • **rate**—Divert rate in packets per second. The minimum rate is 1 packet per second and the maximum rate is 65535 packets per second. For WAN-IP packets, the default rate is 4000 packets per second. • **limit**—Number of packets to be diverted in an initial burst of packets. The minimum limit is 4 packets and the maximum limit is 4194 packets. For WAN-IP packets, the default limit is 4000 packets.
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN Non-IP Rate and Limit

To configure DRL for WAN-side non-IP packet streams, use the **service divert-rate-limit non-ip** 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.

	Command or Action	Purpose
Step 3	**service divert-rate-limit non-ip** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)#` **service divert-rate-limit non-ip cgmp rate 1 limit 4** **Example:**	Specifies the DRL rate and limit for the WAN interface. • **divert-code—**Applicable divert code. • **rate—**Divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second. For WAN non-IP packets, the default rate is 2000 packets per second. • **limit—**Number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets. For WAN non-IP packets, the default limit is 2000 packets.
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an IPv4 Trusted Site

Each entry in the IPv4 trusted-site list contains a source IP address and mask, an IP ToS value and mask, and a VRF name. The IPv4 “trusted-site” list applies only to WAN-side IPv4 packets. A maximum of four IPv4 trusted sites can be configured.

To configure a trusted-site list, use the **service divert-rate-limit trusted-site** 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	**service divert-rate-limit trusted-site** *source-ip ip-mask* **tos** *tos-value* **mask** *tos-mask* **Example:**	Adds entries to the IPv4 trusted-site list using the specified parameters. **Note** If no VRF name is specified, the trusted site applies to all VRF and the global Internet.

	Command or Action	Purpose
	Example: **service divert-rate-limit trusted-site** *source-ip ip-mask* **tos** *tos-value* **mask** *tos-mask* **global** **Example:** **Example:** **service divert-rate-limit trusted-site** *source-ip ip-mask* **tos** *tos-value* **mask** *tos-mask* **vrf** *vrf-name* **Example:** `Router(config)#` **service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255** **Example:** **tos 0xD0 mask 0xF3** **Example:** **Example:** `Router(config)#` **service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255** **Example:** **tos 0xD0 mask 0xF3 global** **Example:** **Example:** `Router(config)#` **service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255** **Example:** **tos 0xD0 mask 0xF3 vrf name1**	• **source-ip—**Specifies the source IP address that should be matched. • **ip-mask—**Specifies the mask to apply to the source IP address of the packet before testing if it matches. There are no restrictions on the mask-ip-address value. • **tos tos-value—**Specifies the ToS value of the trusted site. There are no restrictions on the tos-value value. • **mask tos-mask—**Specifies the mask to apply to the IP ToS value and the trusted-site tos value before testing whether it matches. There are no restrictions on the tos-mask value. • **global—**Specifies that the trusted-site is applicable to the global internet, but not to other VRF names. • **vrf vrf-name—**Specifies the VPN routing and forwarding (VRF) name that applies to this trusted site. **Note** Only four entries are allowed in the IPv4 trusted site list.
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an IPv6 Trusted Site

Each entry in the IPv6 'trusted site' list contains a 128-bit source IP address & mask, an 8-bit traffic-class value & mask, and a VRF name. The IPv6 trusted-site list applies only to WAN-side IPv6 packets. A maximum of four IPv6 trusted site can be configured.

To configure a IPv6 trusted-site list, use the service divert-rate-limit trusted-site-ipv6 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	**service divert-rate-limit trusted-site-ipv6** *ip-address traffic-class tc_value mask tc-mask* **Example:** **Example:** **service divert-rate-limit trusted-site-ipv6** *ip-address traffic-class tc_value mask tc-mask* **global** **Example:** **Example:** **service divert-rate-limit trusted-site-ipv6** *ip-address traffic-class tc_value mask tc-mask* **vrf** *vrf-name* **Example:** `Router(config)#service divert-rate-limit trusted-site-ipv6 2001:420:3800:800:21F:29FF::1/128 traffic-class 0x3 mask 0xFF global`	Adds IPv6-specific entries to the trusted-site list using the specified parameters. **Note** If no VRF name is specified, the trusted site applies to all VRF and the global Internet. • ip-address/prefix-length—The source IPv6 address/ prefix-length that should be matched. • traffic-class tc_value—The 8-bit traffic-class of the trusted site. There are no restrictions on the tc_value. • mask tc-mask—The mask to apply to the packet traffic-class and the trusted-site tc_value before testing if it matches. • **global**—The trusted-site is applicable to the global internet, but not to other VRF names. • **vrf vrf-name**—VPN routing and forwarding (VRF) name that applies to this trusted site. **Note** Only four entries are allowed in the trusted site list.

	Command or Action	Purpose
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring DRL Max-Rate Per Divert-Code on WAN Interface

Effective with Cisco IOS Release 12.2(33)SCH3, per-divert-code rate limit can be configured on the WAN interface to reduce the CPU utilization.

The DRL Max-Rate Per Divert-Code on WAN Interface can be configured, when the DDos occurs and the flooding packets have one of the support divert codes.

This procedure provides information to configure per-divert-code rate limit on the WAN interface.

Before You Begin

Before you configure the service divert-rate-limit max-rate command, it is recommended to configure the source based DRL first.

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	**service divert-rate-limit max-rate wan** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)# service divert-rate-limit max-rate wan fib_rp_dest rate 5000 limit 100`	Specifies the DRL rate and limit for the WAN interface per divert-code. • **divert-code**—Specifies the applicable divert code. ◦ fib_rp_dest— IPv4 packets targeting to CMTS. ◦ fib_rp_glean—FIB glean adjacency used for IPv4 adjacency resolving. ◦ fib_rp_punt—FIB punt adjacency used for IPv4 adjacency resolving. ◦ ipv6_rp_dest—IPv4 packets targeting to CMTS. ◦ ipv6_rp_glean—IPv6 receive adjacency used for IPv4 adjacency resolving. ◦ ipv6_rp_punt—IPv6 punt adjacency used for IPv4 adjacency resolving.

	Command or Action	Purpose
		Starting from Cisco IOS Release 12.2(33)SCJ, the following divert codes were supported: ◦ mfib_224_0_0_x—The Packet whose destination IP is 224.0.0.x. ◦ icmpv6—IPv6 ICMP ◦ mfib_igmp—IGMP protocol packet ◦ ipv6_nd_na_mcast—IPv6 ND NA (multicast) ◦ ipv6_nd_na_ucast—IPv6 ND NA (unicast) ◦ ipv6_nd_ns_mcast—IPv6 ND NS (multicast) ◦ ipv6_nd_ns_ucast—IPv6 ND NS (unicast) ◦ ipv6_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IPV6 header. ◦ ipv6_src_linklocal—IPv6 SRC LinkLocal ◦ fib_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IP header. • **rate**—Specifies the divert rate in packets/sec. The range is from 1 to 65535. The default value is 4194. • **limit**—Specifies the limit for the number of packets that will be diverted in an initial burst of packets. The range is from 4 to 4194.The default value is 4194.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring DRL Max-Rate Per Divert-Code on Upstream Cable Interface

Effective with Cisco IOS Release 12.2(33)SCJ, per-divert-code rate limit can be configured on the upstream cable interface to reduce the CPU utilization.

The DRL Max-Rate Per Divert-Code on upstream cable interface can be configured, when the DDos occurs and the flooding packets have one of the support divert codes.

This procedure provides information to configure per-divert-code rate limit on the upstream cable interface.

Before You Begin

Before you configure the service divert-rate-limit max-rate command, it is recommended to configure the source based DRL first.

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	**service divert-rate-limit max-rate us-cable** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)# service divert-rate-limit max-rate us-cable fib_rp_dest rate 5000 limit 100`	Specifies the DRL rate and limit for the upstream cable interface per divert-code. • **divert-code**—Specifies the applicable divert code. ◦ mfib_224_0_0_x—The Packet whose destination IP is 224.0.0.x. ◦ icmpv6—IPv6 ICMP ◦ mfib_igmp—IGMP protocol packet ◦ ipv6_nd_na_mcast—IPv6 ND NA (multicast) ◦ ipv6_nd_na_ucast—IPv6 ND NA (unicast) ◦ ipv6_nd_ns_mcast—IPv6 ND NS (multicast) ◦ ipv6_nd_ns_ucast—IPv6 ND NS (unicast) ◦ fib_rp_dest— IPv4 packets targeting to CMTS. ◦ fib_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IP header. ◦ fib_rp_glean—FIB glean adjacency used for IPv4 adjacency resolving. ◦ fib_rp_punt—FIB punt adjacency used for IPv4 adjacency resolving. ◦ src_ver_leasequery_req—Divert to RP due to zero MD and sid value and need to send lease query to DHCP server for those packets. ◦ src_ver_unknown_ip_addr—Divert to RP due to zero MD and sid value and no adjacency information for source IP address of those packets. ◦ ipv6_rp_dest—IPv4 packets targeting to CMTS. ◦ ipv6_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IPV6 header. ◦ ipv6_rp_glean—IPv6 receive adjacency used for IPv4 adjacency resolving. ◦ ipv6_rp_punt—IPv6 punt adjacency used for IPv4 adjacency resolving. ◦ ipv6_src_linklocal—IPv6 SRC LinkLocal ◦ ipv6_src_ver_mac_req—Divert to RP due to zero MD and sid value.

	Command or Action	Purpose
		• **rate**—Specifies the divert rate in packets/sec. The range is from 1 to 65535. The default value is 4194. • **limit**—Specifies the limit for the number of packets that will be diverted in an initial burst of packets. The range is from 4 to 4194.The default value is 4194.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying US Cable Dropped Packets

To view and verify the number of upstream cable packets that are dropped from the CMTS, use the show pxf cpu statistics drl us-cable command as shown in the following examples:

```
Router# show pxf cpu statistics drl us-cable
Divert-Rate-Limit US-cable statistics
   dropped   identifier
       361   interface: Cable6/0/1   SID: 28
      2457   interface: Cable6/0/0   SID: 1
Router# show pxf cpu statistics drl us-cable threshold 400
Divert-Rate-Limit US-cable statistics :: threshold = 400
   dropped   identifier
      2457   interface: Cable6/0/0   SID: 1
Router#
```

Verifying WAN IPv4 Dropped Packets

To verify drop counters for WAN-IPv4 packets, use the show pxf cpu statistics drl ipv4 commands as shown in the following examples:

```
Router# show pxf cpu statistics drl ipv4
Divert-Rate-Limit WAN-IPv4 statistics
   dropped   identifier
       460   11.12.13.10  VRF: global  divert_code: fib_rp_dest
       150   11.12.13.10  VRF: global  divert_code: fib_limited_broadcast
Router#
Router# show pxf cpu statistics drl ipv4 threshold 400
Divert-Rate-Limit WAN-IPv4 statistics :: threshold = 400
   dropped   identifier
       460   11.12.13.10  VRF: global  divert_code: fib_rp_dest
```

Verifying WAN IPv6 Dropped Packets

To verify drop counters for WAN-IPv6 packets, use the show pxf cpu statistics drl ipv6 commands as shown in the following examples:

```
Router# show pxf cpu statistics drl ipv6
Divert-Rate-Limit WAN-IPv6 statistics
   dropped   identifier
       460   10FA:6604:8136:6502::/64  VRF: global  divert_code: ipv6_rp_dest
       150   10FA:6604:8136:6502::/64  VRF: global  divert_code: ipv6_rp_punt
Router#
Router# show pxf cpu statistics drl ipv6 threshold 400
Divert-Rate-Limit Cable/WAN-IP statistics :: threshold = 400
   dropped   identifier
       460   10FA:6604:8136:6502::/64  VRF: global  divert_code: ipv6_rp_dest
Router#
```

Verifying WAN Non-IP Dropped Packets

To verify drop counters for WAN non-IP packets, use the **show pxf cpu statistics drl non-ip or** show pxf cpu statistics drl non-ip threshold commands as shown in the following examples:

```
Router# show pxf cpu statistics drl non-ip
Divert-Rate-Limit WAN-non-IP statistics
   dropped divert_code
         5 cdp
        17 cgmp
Router# show pxf cpu statistics drl non-ip threshold 10
Divert-Rate-Limit WAN-non-IP statistics :: threshold = 10
   dropped divert_code
        17 cgmp
```

Verifying the Trusted-Site List

To verify the trusted-site configuration, use the **show pxf cpu drl trusted-sites** command as shown in the following example:

```
Router# show pxf cpu drl trusted-sites
Divert-Rate-Limit IPv4 Trusted-Site list
 IP-addr          IP-addr mask     ToS   ToS mask  VRF
 60.0.1.0         255.255.255.0    0x18  0xF8      blue
 50.0.1.0         255.255.255.240  0x01  0xFF      <all>
 50.0.0.0         255.255.255.0    0x18  0xF8      <global internet>
Divert-Rate-Limit IPv6 Trusted-Site list
 5436:6AB4:2344::1/128  tc 0xA3  tc_mask 0xFF  VRF <all>
Router#
```

Verifying WAN DRL Max-Rate Dropped Packets

To verify drop counters for the DRL max-rate on the WAN interface, use the **show pxf cpu statistics drlmax-rate** command as shown in the following examples:

```
Router#show pxf cpu  statistics drl max-rate wan threshold 1
dropped   divert_code
      2617    cable_filter_us
```

Verifying US Cable DRL Max-Rate Dropped Packets

To verify drop counters for the DRL max-rate on the US cable interface, use the **show pxf cpu statistics drlmax-rate** command as shown in the following examples:

```
Router#show pxf cpu statistics drl max-rate us-cable
Load for five secs: 44%/4%; one minute: 45%; five minutes: 28%
Time source is hardware calendar, 16:52:36.953 CST Thu Dec 17 2015

Divert-Rate-Limit max-rate US-cable statistics
   dropped   divert_code
 No max-rate US-cable drops.
```

Clearing Statistics

Use **clear** commands to do the tasks listed in the table:

Command	Description
clear pxf statistics drl all	To clear all the entries in all the DRL statistics table
clear pxf statistics drl us-cable	To clear all the entries in the US-cable statistics table
clear pxf statistics drl ipv4	To clear all the entries in the WAN IPv4 statistics table
clear pxf statistics drl ipv6	To clear all the entries in the WAN IPv4 statistics table
clear pxf statistics drl non-ip	To clear all the entries in the WAN non-IP statistics table
clear pxf statistics drl max-rate	Clears the DRL max-rate statistics on the WAN interface

Note Starting from Cisco IOS Release 12.2(33)SCJ, only the **clear pxf statistics drl all** command is supported.

Configuration Examples for PXF DRL Enhancement

This section provides the following configuration examples:

Example: Configuring Cable Divert Rate Limit

The following example shows how to configure a cable DRL.

```
Router(config)# interface C5/0/0
Router(config-if)#cable divert-rate-limit rate 1 limit 4
```

Example: Configuring WAN IPv4 Rate and Limit

The following example shows how to configure a WAN-IPv4 rate and limit.

```
service divert-rate-limit
service divert-rate-limit ip
service divert-rate-limit ip fib_rp_glean
service divert-rate-limit ip fib_rp_glean rate
service divert-rate-limit ip fib_rp_glean rate 65530
service divert-rate-limit ip fib_rp_glean rate 65530 limit
service divert-rate-limit ip fib_rp_glean rate 65530 limit 4194
```

Example: Configuring WAN IPv6 Rate and Limit

The following example shows how to configure a WAN-IPv6 rate and limit.

```
service divert-rate-limit
service divert-rate-limit ipv6
service divert-rate-limit ipv6 ipv6_rp_glean
service divert-rate-limit ipv6 ipv6_rp_glean rate
service divert-rate-limit ipv6 ipv6_rp_glean rate 20
service divert-rate-limit ipv6 ipv6_rp_glean rate 20 limit
service divert-rate-limit ipv6 ipv6_rp_glean rate 20 limit 10
```

Example: Configuring WAN Non-IP Rate and Limit

The following example shows how to configure a WAN Non-IP rate and limit.

```
service divert-rate-limit
service divert-rate-limit non-ip
service divert-rate-limit non-ip cgmp
service divert-rate-limit non-ip cgmp rate
service divert-rate-limit non-ip cgmp rate 65535
service divert-rate-limit non-ip cgmp rate 65535 limit
service divert-rate-limit non-ip cgmp rate 65535 limit 4100
```

Example: Configuring an IPv4 Trusted Site

The following example shows how to configure an IPv4 trusted site.

```
service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255
  tos 0xD0 mask 0xF3
```

Example: Configuring an IPv6 Trusted Site

The following example shows how to configure a IPv6 trusted site.

```
service divert-rate-limit trusted-site-ipv6 2001:420:3800:800:21F:29FF::1/128 traffic-class
 0x3 mask 0xFF global
```

Example: Configuring DRL Max-Rate Per Divert-Code on WAN Interface

The following example shows how to configure DRL max-rate per divert-code on WAN interface

```
Router> enable
Router# configure terminal
Router(config)# service  divert-rate-limit max-rate wan fib_rp_dest rate 5000 limit 100
Router(config)# end
```

Example: Configuring DRL Max-Rate Per Divert-Code on US Cable Interface

The following example shows how to configure DRL max-rate per divert-code on upstream cable interface.

```
Router> enable
Router# configure terminal
Router(config)# service divert-rate-limit max-rate us-cable fib_rp_dest rate 5000 limit 100
Router(config)# end
```

Additional References

The following sections provide references related to the PXF Divert Rate Limit Enhancement feature.

Related Documents

Related Topic	Document Title
CMTS cable commands	Cisco IOS CMTS Cable Command Reference
Cable ARP Filtering	Cisco IOS CMTS Cable Software Configuration Guide

Standards

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

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

Feature Information for PXF DRL Enhancement

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 28: Feature Information for PXF DRL Enhancement

Feature Name	Releases	Feature Information
PXF DRL Enhancement on the Cisco CMTS Routers	12.2(33)SCB	The PXF DRL Enhancement feature prevents congestion of the FP-to-RP interface by identifying and rate-limiting entities that would otherwise cause congestion. The following sections provide information about this feature: The following commands were introduced or modified: cable divert-rate-limit, • **service serviceip** • **service servicenon-ip** • **service divert-rate-limit trusted-site** • **clear pxf statistics drl cable-wan-ip** • **show pxf cpu statistics**, **show pxf cpu drl-trusted-sites**

Feature Name	Releases	Feature Information
PxF Accelerated for IPv6 Forwarding	12.2(33)SCE	The PXF Accelerated for IPv6 Forwarding feature for the Cisco uBR10000 series router includes support for the following IPv6 features: • IPv6 Security and QoS ACLs • IPv6 over IPv4 Tunnels • IPv6 Packet Filter Groups • IPv6 QoS Classifiers • ToS Overwrite for IPv6 • IPv6 Source Verify • IPv6 Packet Intercept • IPv6 SAV The following commands were introduced: service divert-rate-limit trusted-site-ipv6, **service divert-rate-limit ipv6,** show pxf cpu statistics drl us-cable, show pxf cpu statistics drl ipv6, show pxf cpu statistics drl ipv4, and **show pxf cpu statistics drl non-ip**.
DDoS attack solution	12.2(33)SCH3	The DDOS attack solution feature helps reduce the CPU utilization when the DDos occurs. The following commands were introduced: • **service divert-rate-limit max-rate** • **clear pxf statistics drl max-rate** • **show pxf cpu statistics drlmax-rate**

Feature Name	Releases	Feature Information
IPv6 DRL Punt Codes	12.2(33)SCJ	The feature applies rate limit to traffic from upstream cable. The following commands were introduced: • **service divert-rate-limit max-rate us-cable** • **show pfx cpu statistics drl max-rate us-cable** • **clear pfx statistics drl all**

CHAPTER 12

Resolving Common Image Installation Problems

Note The information in this document is based on Cisco IOS Release 11.2 and later releases.

This appendix is designed to assist you with problems that may develop while you are installing Cisco IOS software images using a TFTP or remote copy protocol (rcp) server application. For rcp applications, substitute rcp for TFTP in the instructions.

Contents

Before You Begin

Caution Do not save anything while you are in boot mode. Avoid using the saving commands (write mem or copy run start), and respond **no** to any prompt suggesting that you save your current configuration. If you save while you are in this mode, your configuration can be partially or completely erased.

Resolving Default Gateway Issues

Determine the Default Gateway for the Router

The default gateway is always the next hop that any packet will have to cross to reach the workstation where you have the TFTP server or Telnet session source, or both. The traceroute command shows the IP address of the default gateway in the first line of the output:

Example

```
Router> traceroute 172.17.247.195
Type escape sequence to abort.
Tracing the route to 172.17.247.195
1 10.200.40.1 4 msec 4 msec 4 msec
2 172.17.247.195 4 msec *  0 msec
Router>
```

Adding the Default Gateway in the Configuration

To add the default gateway, type the **ip default-gateway** command in the global configuration mode.

```
ip default-gateway [ip address]
```

ip address	The IP address of the router.

Verifying the TFTP Server and Router are in the Same Network

You will need to compare the IP addresses and masks of the TFTP server and the Ethernet interface of the router.

Example 1

The TFTP server IP address is 172.17.247.195 and the mask is 255.255.0.0. The interface Ethernet 0 of the router IP address is 172.17.3.192 and the mask is 255.255.0.0. In this example, the TFTP server and this interface of the router are in the same network, so a default gateway is not required.

Example 2

The TFTP server IP address is 172.17.247.195 and the mask is 255.255.0.0. The interface Ethernet 0 of the router IP address is 172.10.3.192 and the mask is 255.255.0.0. In this example, they are on different IP networks so it is necessary to configure a default gateway on the router.

Determining the IP Address and Mask on the Router

Look for the IP address command under the interface Ethernet statement in your configuration.

Example

```
Router> en
Password:
Router# show run
Building configuration...
Current configuration:
!
version 11.3
```

```
service timestamps debug uptime
..................
interface Ethernet0
ip address 172.17.3.192 255.255.0.0
```

Determining the IP Address of the TFTP Server on Windows 95

Step 1 From the toolbar, select Start and then Run.

Step 2 Type winipcfg and then click OK to display the IP configuration dialog box.

Determining the IP Address of the TFTP Server on a UNIX Workstation

Step 1 Enter the command netstat -in. The IP addresses of the interfaces on your station appear.

Step 2 Select the IP address for the interface that goes into the router network.

Troubleshooting Problems During Software Transfer

Resolving Error Message Text checksum verification failure During the Copy

If you have seen many "." instead of "!" during the copy, you may see a message similar to the following example:

```
COPY: Text checksum verification failure
TFTP from 172.17.247.195 failed/aborted
Verifying checksum... invalid (expected 0x62B7,
computed 0x60B9)
```

If you enter a show flash command, you may see something similar to the following example:

```
Router# show flash
PCMCIA flash directory:
File Length Name/status
1 3437967 c1600-sy-mz.120-8.0.2.T
2 3489036 c1600-y-l.112-19.P1
3 290304 c1600-y-l.112-18.P [invalid checksum]
```

In both cases, a checksum failure indicates that the file has not been properly copied into the memory and you need to copy it again. First, verify that the file you copied to the TFTP server is the same size as the original file. (Be aware that the size is listed in bytes in the router and is sometimes listed in kilobytes in TFTP servers.) If the network is very busy, you may also see this behavior; try the copy again when the network is not so loaded, or establish a direct Ethernet connection between the TFTP server and the router to download the file.

Resolving Error Message "error opening tftp"

This is an example of the error message:

```
Router# copy tftp flash
Address or name of remote host [172.17.0.5]?
Source filename [rsp-dsv-mz.112-19.P1.bin]?
Destination filename [rsp-dsv-mz.112-19.P1.bin]?
Accessing tftp://172.17.0.5/rsp-dsv-mz.112-19.P1.bin...
%Error opening tftp://172.17.0.5/rsp-dsv-mz.112-19.P1.bin (No such file or directory)
```

If you receive this message, verify that the file is in the root directory of the TFTP server, and check to see if you entered the correct filename. Some easily mistaken letters are I (capital i), l (small L) and 1 (one).

Resolving Display of Timeout Error Messages

Step 1 Verify that the TFTP server is open on your PC.

Step 2 Make sure that the file is in the root directory (from the menu bar, select **View**>**Options**).

Resolving Error Message "Can't open file"

Verify that the TFTP server is running on your PC. Verify that you have copied the exact filename. Some easily mistaken letters are I (capital i), l (small L) and 1 (one).

Instructions for Run-from-RAM Installations

Step 1 To copy a system image from one device to another, use the copy command in global configuration mode.

Example:

```
copy tftp ?
```

Step 2 Refer to the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 for additional information about the copy command. Methods vary according to different platforms.

What to Do Next

The three most common forms of the copy command for this purpose are as follows:

```
copy tftp flash
copy rcp flash
copy slot0: slot1:
```

The following example provides an illustration of the copy slot0: slot1 command:

```
router# show slot0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------
name
1 .D unknown 5E8B84E6 209D8 11 2392 Jan 22 2000 00:22:42
flashconfig
2 .. image 5E7BAE19 B623C4 22 11802988 Jan 22 2000 00:23:18
rsp-jsv-mz.1
20-8.0.2.T
router# show slot1:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------
name
1 .. unknown 6A2B4BA7 6FA9E0 20 7186784 Jul 30 1999 15:05:19
rsp-jv-mz.11 1-26.CC1
2 .. config 631F0D8B 6FB1EC 6 1929 Oct 19 1999 06:15:49
config
     3 .. config 631F0D8B 6FB9F8 7 1929 Oct 19 1999 06:16:03
     config1
router# copy slot0: slot1:
Source filename []? rsp-jsv-mz.120-8.0.2.T
Destination [slot1]?
CCCCCCCCCCCCCCCCCCCC
2392 bytes copied in 0.300 secs
```

Instructions Before Reloading

Step 1 Verify that the new Cisco IOS software image has been stored properly. Use the show flash command to make sure that the file has been saved, that the size is correct, and that you do not have an invalid checksum message.
If the file does not appear, or if it appears followed by "[invalid checksum]", or if the size does not correspond to the file size on the tftp server, you must start the installation again. Be aware that the size is listed in bytes in the router and is sometimes listed in kilobytes in TFTP servers.

Step 2 Verify that the boot system commands are in the right order in the configuration. The router stores and executes the boot system commands in the order in which you enter them in the configuration file. If a boot system command entry in the list specifies an invalid device or filename, the router skips that entry.

What to Do Next

This is an example of boot system commands defined in the configuration file:

```
Router> en
Password:
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)# boot system flash c1600-y-l.112-18.P
Router(config)# boot system flash
```

Troubleshooting Problems by Verifying the Software Image

Resolving the show version Command not Displaying Proper Image

If the show version command output does not display the Cisco IOS image that you just loaded, perform these steps:

Step 1 Verify that the new Cisco IOS software image has been stored properly. Use the show flash command to make sure that the file has been saved, that the size is correct, and that you do not have an invalid checksum message.
If the file does not appear, or if it appears followed by "[invalid checksum]", or if the size does not correspond to the file size on the tftp server, you need to start the installation again. Be aware that the size is listed in bytes in the router and is sometimes listed in kbytes in TFTP servers.

Step 2 Verify that the boot system commands are in the right order in the configuration. The router stores and executes the boot system commands in the order in which you enter them in the configuration file. If a boot system command entry in the list specifies an invalid device or filename, the router skips that entry.

Resolving the Rxboot Prompt (Router(boot)) Displaying After Reload

Step 1 Verify that the new Cisco IOS software image has been stored properly. Use the show flash command to make sure that the file has been saved, that the size is correct, and that you do not have an invalid checksum message.
If the file does not appear, or if it appears followed by "[invalid checksum]", or if the size does not correspond to the file size on the tftp server, you need to start the installation again. Be aware that the size is listed in bytes in the router and is sometimes listed in kbytes in TFTP servers.

Step 2 Verify that the boot system commands are in the right order in the configuration. The router stores and executes the boot system commands in the order in which you enter them in the configuration file. If a boot system command entry in the list specifies an invalid device or filename, the router skips that entry.

Step 3 Verify that the config register value is correct. The last digit should be a 2. You can check this with the show version command. If the value is not correct, you need to restore a valid value and reload the image.

CHAPTER 13

SEA Health Monitoring for the Cisco UBR10012 Routers

First Published: November 16, 2009

Last Updated: November 16, 2009

Maintaining a log of major and critical events and alarms helps the system administrator in identifying and resolving the problems from further occurrence. There are various other methods for reproducing the problems but these methods have limitations. The System Event Archive (SEA) is a health monitoring feature. It maintains a log of major and critical events and alarms of the system that helps identify and resolve problems from occurring later. The SEA feature maintains a log of hardware and software events and alarms in the sea_log.dat file. These generated events can be analyzed and copied to the sea_log.dat file at the specified location. The Cisco IOS Release 12.2(33)SCC introduces the SEA feature for Cisco Universal Broadband Router 10012.

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 SEA

The table shows the hardware and software compatibility prerequisites for this feature.

Table 29: SEA Support for the Cisco CMTS Routers Hardware and Software Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards or Jacket Cards	SIP/SPA
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)SCA and later** • Cisco uBR10-MC5X20S/U[19] **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V[20] **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V 2	• Cisco Wideband SPA 2

19 Supports DOCSIS 2.0 and IPv6 cable modems.
20 Supports DOCSIS 3.0 and IPv6 cable modems.

Restrictions for SEA

- SEA event log feature only supports PCMCIA ATA disk or Compact flash disk in adapter for PRE2.
- Due to a limitation (reference CDETS ID: CSCsz77977) for performing Online-Insertion-Removal (OIR) of the disk on PRE2, the following actions are recommended before performing an OIR of the disk on PRE2:
- Disable SEA logging using **no logging system** command, before performing an OIR of disk on PRE2.
- Enable SEA logging using **logging system** command, after performing OIR of disk on PRE2.
- Use different disk for SEA logging and for storing Cisco IOS image. For example, if disk0: is used to store IOS image and is referenced in boot system command, use disk1: for storing SEA logging.
- For PRE4, keep the SEA storage on boot flash: (which is the default disk).

Information About SEA

The following sections provide the details of the SEA feature:

Importance of System Health Monitoring

Keeping a regular check of health of a system is essential. To provide high-availability for a router without any downtime it is imperative to analyze the stability of a system. The stability of a system is determined by system log messages and debug traces. If any of the log messages are ignored for a significant time, it can bring a system down. Essentially, the system log messages help in analyzing the root cause of the generated event. To prevent downtime, the root cause of the problem can be identified and resolved.

Limitations of Existing Logging Mechanisms

The primary method of discovering the cause of system failure is system messages. When system messages do not provide the information needed to determine the cause of a failure, you can enable debug traces and attempt to recreate the failure. However, there are several situations in which neither of the above methods provides an optimum solution. Following are the limitations of the existing logging mechanism:

- Reviewing a large number of system messages can be an inefficient method of determining the cause of a failure.
- Debug trace is usually not configured by default.
- You cannot recreate the failure while using debug trace.
- Using debug trace is not an option if the switch on which the failure has occurred is part of your critical network.
- The problem is not reproducible when debug trace is enabled due to change in timings.
- If the system is part of a critical network, it is not advisable to recreate or debug the issue.
- Unless the problem is reproduced, the exact root cause of the system failure is not known.

Understanding the System Event Archive

The SEA feature addresses the shortcomings of the existing logging mechanism. The SEA feature can help debug issues without reproducing the problem. The SEA runs on the route processor (RP). SEA allows each CPU to report major and abnormal events to the RP using the out-of-band interface and log it into the non-volatile storage using the time-stamp. The RP logs its own events to the boot flash disk. The RP receives event messages from the cable line card and jacket card over IPC, and logs them to the boot flash.

Logging Location

By default, the SEA feature is enabled and events are stored in the log file ‘sea_log.dat’ with the timestamp. The events are stored in sea_log.dat along with the timestamp. The SEA feature requires either PCMCIA ATA Flash or Compact Flash disk for storage. By default, on PRE2 the SEA creates the log file on disk0:. The SEA command enables changing the location (disk) of the sea_log.dat file using the **logging system disk** *name* command. The size of the sea_log.dat file is 32 MB or 10% of the disk size or at least 448KB. The sea_log.dat file stores the most recent event messages in the log file in a circular fashion.

Note SEA feature does not automatically search for a disk if the default disk or explicitly configured disk is not inserted.

Managing SEA

This section describes how to manage the system event archive. The following SEA commands are used to manage the SEA functionality.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**logging system** **Example:** `Router(config)# logging system`	Enables the SEA logging feature. By default, the SEA feature is enabled. **Note** To disable the SEA logging feature, use the **no logging system** command.
Step 2	**logging system disk disk1:** **Example:** `Router(config)# logging system disk disk1:`	Changes the disk location on PRE2 or PRE4 for storing the SEA log messages. **Note** By default, SEA log messages are stored on disk0: for PRE2 and on boot flash: for PRE4.
Step 3	**show logging system** **Example:** `Router# show logging system`	Displays the latest SEA log messages stored in the sea_log.dat file.
Step 4	**show logging system disk** **Example:** `Router# show logging system disk`	Displays the disk used to store the sea_log.dat file.
Step 5	**copy logging system target** *filename* **Example:** `Router# copy logging system target filename`	Copies the sea_log.dat file to the destination file system.
Step 6	**clear logging system** **Example:** `Router# clear logging system`	Clears the events stored in the sea_log.dat file.
Step 7	**logging cmts sea** **Example:** `Router#config t`	Enables logging of system log messages to SEA.

	Command or Action	Purpose
	Example: `Router(config)# logging cmts sea`	

Step 8	**logging cmts sea syslog-level warnings**
	Example:
	`Router# config t`
	Example:
	`Router(config)# logging cmts sea syslog-level warning`
		Configures the level of system log messages inclusive of and above the configured level to be stored in sea_log.dat file. The example shows the configuration to store system log messages with severity 'warning' and above to be stored in the sea_log.dat file.

Probable Scenarios and Useful SEA Commands

The table discusses the various scenarios and how to use the SEA commands for managing the event logs.

Table 30: Possible Scenarios and Useful SEA Commands

Possible Scenarios	Command Used	Explanation
To check whether SEA feature is enabled.	`Router# dir disk0:` `23 -rw-  6710888 May 16 2009 06:03:36 +00:00 sea_log.dat`	By default, SEA is enabled and the command is not shown under the "show running. To check the log file location, execute the **dir [diskname]** command from EXEC command mode. **Note** On PRE2, the default location to store the SEA log message is disk0:.
To check the latest SEA log messages.	`Router# show logging system`	To check the latest SEA log messages, execute the **show logging system** command from EXEC mode. The SEA log messages are stored with the actual time-stamp, slot/sub-slot number, name of software generating the system event, and the event message. **Tip** The sea_log.dat file is created as soon as the first SEA log message is stored in the file.
To check the current location to store the sea_log.dat file.	`Router# show logging system disk` `SEA log disk: disk0:`	If you are unsure of the disk currently storing the SEA event log messages, execute the **show logging system disk** command. As shown in the example, it displays the SEA log disk currently used to store the sea_log.dat file.
To check the last 'n' number of SEA event log messages.	`Router# show logging system last 5`	The system administrator can also check the desired number of last messages stored in the sea_log.dat file. Use the **show logging system last** *5* command to view the last 5 messages stored in the log file. **Tip** The valid range to display the last number of SEA messages is 1 to 10,000.
To change the location of the sea_log.dat file to a different disk.	`Router(config)# logging system disk disk1:` `You are configuring a different disk from the current log disk.`	To change the location of the sea_log.dat file execute the command **logging system disk diskname** from global configuration mode. **Note** After changing the disk, the new event log information is logged to the new location (in this example disk1:) and the log event information before the change disk is available at the old location (in this case disk0:).

Possible Scenarios	Command Used	Explanation

Copying the SEA event log messages to a target file.	`Router# copy logging system rcp`
	`Address or name of remote host []? 192.0.2.1`
	`Destination username [Router]? username1`
	`Destination filename [sea_log.dat]? /auto/tftpboot-users/username1/sea_log.dat`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
		The advantage of SEA feature is that you can copy and back up SEA event log messages at specific target file locations. Use the **copy logging system target** *filename* command to copy the sea contents to the desired location.
		Note Copying the SEA event log file is useful when there is less disk space available on the disk or the disk is almost full.

To clear the SEA event log messages stored on the disk.	`Router# clear logging system`
	`Clear logging system operation will take a while.`
	`Do you want to continue? [no]: yes`
		After taking a back up of SEA event log messages, you can clear the event log details stored at the default location using the **clear logging system** command.
		Note Before clearing the event log messages, it is recommended to take a back up of the SEA event log messages to a target file system.

Configuring a different disk to store the sea_log.dat file without the disk being present, provides an error message.	`Router(config)# logging system disk disk1:` `disk1: does not exist in the system`	Before changing the location of the disk, check if the target disk is present on PRE2 or PRE4. If the disk is not present then the **logging system disk disk1:** command, generates an error message. **Note** SEA will not automatically search for the disk, if the default disk is not inserted.
Configuring bootflash: as the disk to store log messages on PRE2, provides an error message.	`Router(config)# logging system disk bootflash:` `bootflash: is not allowed`	The supported disk to store the sea_log.dat file is either PCMCIA ATA flash disk or Compact Flash disk in PCMCIA jacket. If bootflash: is configured to store the log messages on PRE2 using the logging system disk bootflash: command, it generates an error message. In the example, a linear flash disk is configured to store the SEA log messages, hence an error message is shown. **Note** The SEA event log messages cannot be stored on a linear flash disk.
Changing the level of system log event messages inclusive of and above 'warning' level to be stored in the sea_log.dat file.	`Router(config)# logging cmts sea syslog-level warning`	

Possible Scenarios	Command Used	Explanation
		By default, the system log event message to be stored in the log file is enabled with the severity-level of system log messages being set to 'errors'. Use the **logging cmts sea syslog-level warning** command to configure the system log event messages inclusive of and above 'warning' level to be stored in the sea_log.dat file.

Additional References

For additional information related to health monitoring, see the following references:

Related Documents

Related Topic	Document Title
CMTS commands	Cisco IOS CMTS Cable Command Reference
Generic Online Diagnostics (GOLD)	GOLD feature for the Cisco UBR10012 Universal Broadband Router

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
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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

Feature Information for SEA 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 31: Feature Information for System Event Archive (SEA) for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
System Event Archive (SEA) Support for the Cisco CMTS Routers	12.2(33)SCC	The System Event Archive (SEA) is a health monitoring feature that maintains a log of major and critical events and alarms of the system that helps identify and resolve problems from occurring later. This feature was introduced for the PRE2 and PRE4 route processors. The following commands are new or modified: • **logging system** • **show logging system** • **copy logging system** • **clear logging system** • **logging cmts sea** [**syslog-level** [**level**]]

CHAPTER 14

Usage-Based Billing for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: May 10, 2010

Note Cisco IOS Release 12.2(33)SCA and later releases integrate 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 Usage-based Billing feature for the Cisco Cable Modem Termination System (CMTS) routers, which provides subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format. The SAMIS format is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

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 Usage-based Billing

The usage-based billing feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and Cisco IOS Release 12.2SC.

Table 32: Usage-based Billing Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Line Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.3(21)BC and later releases • PRE-1 • PRE-2 Cisco IOS Release 12.2(33)SCA and later releases • PRE-2 Cisco IOS Release 12.2(33)SCB and later releases • PRE-4	Cisco IOS Release 12.3(21)BC and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco uBR-MC20X20V
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.3(21)BC and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCA and later releases • NPE-G2 Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.3(21)BC and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCA and later releases • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V[21]

CMTS Platform	Processor Engine	Cable Line Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.3(21)BC and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCA and later releases • NPE-G1 Cisco IOS Release 12.2(33)SCD and later releases • NPE-G2	Cisco IOS Release 12.3(21)BC and later releases • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCA and later releases • 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 releases • Cisco uBR-MC88V

[21] 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.

The Usage-based Billing feature has the following prerequisites:

- Cable modems must be compliant with DOCSIS 1.0 or DOCSIS 2.0 in Cisco IOS Release 12.2(33)SCA, OSSI version 3.0 in Cisco IOS Release 12.2(33)SCB and DOCSIS 3.0 in Cisco IOS Release 12.2(33)SCC and later releases.
- The Cisco CMTS router must be running Cisco IOS Release 12.2(33)SCA or later releases.
- Cable modems that are being monitored should use a DOCSIS configuration file that defines upstream and downstream primary service flows using Service Class Naming (SCN [TLV 24/25, subTLV 4]). If dynamically-created service flows are to be monitored, they should also be created with SCN names.
- When the feature is operating in File mode, an external billing server must log into the Cisco CMTS to copy the billing records to the external server, using either Secure Copy (SCP) or Trivial File Transfer Protocol (TFTP). The Cisco CMTS cannot operate as a FTP or secure FTP (SFTP) server.
- When the feature is operating in Streaming mode in non-secure mode, an external billing server must be configured to receive the billing records at a configurable TCP port.
- When the feature is operating in Streaming mode in secure mode, the following are required:
  - The external billing server must be configured to receive the billing records at a configurable TCP port using a secure socket layer (SSL) connection.

Tip Several third-party solutions for SSL support on the billing application server are available http://www.openssl.org/index.html .

- ◦ A Certificate Authority (CA) must be configured and available to provide the required digital certificates to the billing application and Cisco CMTS router. The CA can be a public CA, such as Verisign, or a server on your private management network that is running software such as the Cisco Provisioning Center (CPC).

- To use the **full-records** keyword, the Cisco CMTS router must be running the Cisco IOS Release SCC4, Cisco IOS Release SCD2, or later releases.
- To use the **flow-aggregate** keyword for ipdr/ipdr-d3 the Cisco CMTS router must be running the Cisco IOS Release SCC4, Cisco IOS Release SCD2, or later releases.

When **flow-aggregate** is enabled, the service flows are combined into one record per cable modem:

- ◦ ServiceClassName element always returns a null value in IPDR records, even when service flows on the cable modem have a valid service class name.
  - ◦ ServiceIdentifier element always returns a zero value.

Restrictions for Usage-based Billing

The Usage-based Billing feature has the following restrictions and limitations:

- SNMP commands can be used to display or modify the Usage-based Billing configuration, and SNMP traps can be used to notify the billing application system when a billing record is available. However, SNMP commands cannot be used to retrieve billing records.
- Enabling IPDR mode through SNMP is not supported.
- Cisco IOS Release 12.3(9a)BC and Cisco IOS Release 12.2(33)SC do not support Usage-based Billing with 1:N or Route Processor Redundancy (RPR):
  - ◦ When HCCP N+1 switchover events occur to a protect cable interface, usage-based billing is suspended until the system returns to the working cable interface.
  - ◦ On the Cisco uBR10012 router, when the system switches over to the secondary PRE1 module, usage-based billing is suspended unless you have also preconfigured the usage-based billing on the secondary PRE1 module.

- The **ipdr template** command allows the user to add an IPDR template to the desired session (based on session ID) on the Cisco CMTS. Only the system-supported templates can be added. The system-supported templates list can be viewed by entering "?" at the command prompt.

The **cable sflog** command specifies the logging mechanism for deleted SNMP service flows. For those items that meet its criteria, are stored on the cable line card side (these items can be also be queried by the docsQosServiceFlowLogTable, docsQos3ServiceFlowLogTable, and docsIetfQosServiceFlowLogTable MIBs). The other items are stored on the route processor (RP) side of the sflog file.

During a line card switchover, the items in the line card side are lost. Similarly, during a PRE switchover, those items in the RP side of the sflog file are lost.

If the user uses the SAMIS file destination, a PRE switchover also reinitializes that output file

- Billing records do not include information about multicast service flows and traffic counters.

- The packet counters displayed by CLI commands are reset to zero whenever the Cisco CMTS router is rebooted. The packet counters displayed by SNMP commands are not retained across router reloads, and SNMP MIB counters cannot be preserved during reloads. These counters are 64-bit values and could roll over to zero during periods of heavy usage.
- When configuring cable metering in the usage-based billing File Mode, the source-interface cannot be specified immediately after using the cable metering filesystem command. Once the cable metering filesystem command is used, the cable metering file will write to the bootflash. Until this operation is complete, no cable metering configuration will be allowed. After the file write operation is complete, the source-interface command (cable metering source-interface) can then be configured; and the metering file in the bootflash would need to be removed so that billing packets have the source-interface's IP address.

Note This cable metering restriction will not be a problem during reload.

- When configuring cable metering in the usage-based billing Streaming Mode, make sure that the loopback interface is accessible from the collector server. Telnetting to the IP address of the loopback interface from the collector server is a good method of testing whether the loopback interface is accessible from the collector server or not.
- To use the **full-records** and **flow-aggregate** keywords, the router must be running the Cisco IOS Release SCC3, or Cisco IOS Release SCD1, or later releases.

Information About Usage-based Billing

Feature Overview

The Usage-based Billing feature provides a standards-based, open application approach to recording and retrieving traffic billing information for DOCSIS networks. When enabled, this feature provides the following billing information about the cable modems and customer premises equipment (CPE) devices that are using the cable network:

- IP and MAC addresses of the cable modem.
- Service flows being used (both upstream and downstream service flows are tracked).
- IP addresses for the CPE devices that are using the cable modem.
- Total number of octets and packets received by the cable modem (downstream) or transmitted by the cable modem (upstream) during the collection period.
- Total number of downstream packets for the cable modem that the CMTS dropped or delayed because they would have exceeded the bandwidth levels allowed by the subscriber's service level agreement (SLA).

Billing records are maintained in a standardized text format that the service provider can easily integrate into their existing billing applications. Service providers can use this information to determine which users might be potential customers for service upgrades, as well as those customers that might be trying to exceed their SLA limits on a regular basis.

Usage-Based Billing and DOCSIS Support on the Cisco CMTS Routers

The usage-based billing feature supports these DOCSIS features on the Cisco CMTS routers:

- DOCSIS 1.0, DOCSIS 2.0, and DOCSIS 3.0 compliant cable modems are supported.
- Best Effort service flows are supported for DOCSIS-compliant cable modems.
- Secondary service flows are supported for DOCSIS-compliant cable modems.
- Dynamic service flows are supported for DOCSIS-compliant cable modems.
- Information about deleted service flows is available only for DOCSIS 1.1 service flows but not for DOCSIS 1.0 service flows.
- Support for terminated service flows must be enabled using the **cable sflog** command in global mode.

Standards

The Usage-based Billing feature is based on several open standards, allowing it to be supported by a wide range of commercial and custom-written billing applications. The following standards provide the major guidelines for writing and using the billing records that the CMTS produces:

- Extensible Markup Language (XML)—A metalanguage that in turn can easily define other markup languages to contain any kind of structured information, such as billing records. An XML-based approach allows the collected billing information to be used by and distributed among many different billing applications from different vendors. It also allows the format to be easily updated and customized to meet the needs of different providers.
- IP Detail Record (IPDR)—An open, vendor-independent standard, defined in the *Network Data Management—Usage (NDM-U) For IP-Based Services* specification, to simplify billing and usage record-keeping for any type of services that can be delivered over an IP-based network. Service providers can use IPDR to create unified billing applications for all of their services, such as DOCSIS or Voice-over-IP, even though those services use different protocols and application servers.
- DOCSIS Operations Support System Interface (OSSI) specification—A DOCSIS specification that defines the requirements for the network management of a DOCSIS network, including a Subscriber Account Management Interface Specification (SAMIS) for a billing record interface. The DOCSIS 2.0 version of this specification states that a CMTS is not required to provide a billing interface, but if the CMTS does provide a billing interface, it must be based on the IPDR/XML standards.

Tip For further information about these standards, see the documents listed in the “Standards” section on page 38 .

IPDR Service Definition Schemas

To standardize the management of objects, service definition schemas are associated with IPDR just as MIBs are associated to SNMP.

For more information, see the OSSI specification document at http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-OSSIv3.0-I02-070223.pdf

The schemas are supported on Cisco IOS Release 12.2(33)SCC4, 12.2(33)SCD2, and later releases.

Table 33: IPDR Schema List for DOCSIS 3.0

Category	Service Definition	Schema Definition	Collection Method
SAMIS	SAMIS-TYPE-1	DOCSIS-SAMIS-TYPE-1_3.5.1-A.1.xsd	time interval, ad-hoc
	SAMIS-TYPE-2	DOCSIS-SAMIS-TYPE-2_3.5.1-A.1.xsd	time interval, ad-hoc
Diagnostic Log Service Definition Schemas	DIAG-LOG-TYPE	DOCSIS-DIAG-LOG-TYPE_3.5.1-A.1.xsd	ad-hoc
	DIAG-LOG-EVENT-TYPE	DOCSIS-DIAG-LOG-EVENT-TYPE_3.5.1-A.1.xsd	event
	DIAG-LOG-DETAIL-TYPE	DOCSIS-DIAG-LOG-DETAIL-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc, event
Spectrum Management	SPECTRUM-MEASUREMENT-TYPE	DOCSIS-SPECTRUM-MEASUREMENT-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc
CMTS CM Registration Status Information	CMTS-CM-REG-STATUS-TYPE	DOCSIS-CMTS-CM-REG-STATUS-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc, event
CMTS CM Upstream Status Information	CMTS-CM-US-STATS-TYPE	DOCSIS-CMTS-CM-US-STATS-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc
CMTS Topology	CMTS-TOPOLOGY-TYPE	DOCSIS-CMTS-TOPOLOGY-TYPE_3.5.1-A.1.xsd	ad-hoc, event
CPE Information	CPE-TYPE	DOCSIS-CPE-TYPE_3.5.1-A.1.xsd	ad-hoc, event
CMTS Utilization Statistics	CMTS-US-UTIL-STATS-TYPE	DOCSIS-CMTS-US-UTIL-STATS-TYPE_3.5.1-A.1.xsd	event
	CMTS-DS-UTIL-STATS-TYPE	DOCSIS-CMTS-DS-UTIL-STATS-TYPE_3.5.1-A.1.xsd	event

The schemas listed in the table are supported by implementing the respective Collectors, which work as SNMP agents to generate these IPDR records according to management information of the system.

DOCSIS SAMIS Service Definitions

SAMIS for DOCSIS 3.0 service definitions are well structured and has two versions—SAMIS-TYPE-1 and SAMIS-TYPE-2 and provide a different level of information details than SAMIS.

DOCSIS 2.0 SAMIS supports only event session (default type) and DOCSIS 3.0 SAMIS TYPE 1 and DOCSIS 3.0 SAMIS TYPE 2 support only interval and ad-hoc sessions.

SAMIS is collected based on configurable time intervals. Each interval is a different document and the Exporter stops and starts a new session for a new interval. The interval starts from the last metering that has either succeeded or failed, unlike the time-interval session that has a fixed starting point and an interval.

Note The SAMIS schema can be configured with the **cable metering ipdr session** command SAMIS-TYPE-1 and SAMIS-TYPE-2 schemas can be configured through the **cable metering ipdr-d3** command. These schemas are mutually exclusive of each other.

Limitation To DOCSIS SAMIS

- Only a schema that is consistent with the **cable metering ipdr| ipdr-d3** command will work. If none of the schemas are consistent, none of them will work.
- Changing the SAMIS IPDR type will abort exporting IPDR data.

DOCSIS Diagnostic Log Service Definitions

This service definition defines the IPDR Streaming using a two-step process:

- SNMP or other configuration management interface, such as the CLI is used to configure the Diagnostic Log.
- IPDR/SP is used to stream the Diagnostic Log instances.

These Diagnostic Log service definition schemas support the following collection methods:

- The Cisco CMTS supports streaming of the DIAG-LOG-TYPE record collections as an ad-hoc session.
- The Cisco CMTS supports streaming of DIAG-LOG-EVENT-TYPE record collections as an event session. For event-based Diagnostic Log records, the Cisco CMTS streams the record when the event is logged in the Diagnostic Log and an IPDR message is transmitted to the Collector.
- The DOCSIS-DIAG-LOG-DETAIL-TYPE supports the following collection methods:
  - Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the diagnostic log, then streams the record to the Collector associated with this session. For time interval based Diagnostic Log records, the Cisco CMTS streams a snapshot of the Diagnostic Log at the scheduled collection time.
  - Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect the diagnostic record and send the data to the Collector.
  - Event—When a diagnostic log record is created, an ipdr message is transmitted to the Collector. For more information, see the Operations Support System Interface (OSSI) Specification.

DOCSIS Spectrum Measurement Service Definition

This service definition schema defines the IPDR schema for the enhanced signal quality monitoring feature.

The DOCSIS-SPECTRUM-MEASUREMENT-TYPE schema supports the following collection methods:

- Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the spectrum information, then streams the records to the Collector.

- Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect the spectrum information and send the data to the Collector.

DOCSIS CMTS CM Registration Status Service Definition

This service definition schema defines the IPDR service definition schema for the CMTS CM Registration Status information.

The DOCSIS-CMTS-CM-REG-STATUS-TYPE schema supports the following collection methods:

- Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the CM status information, then streams the records to the Collector.
- Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect all status information of the cable modems and send the data to the Collector.
- Event—When a cable modem goes from "offline" status to "online" or changes to "offline" from "online" (not including intermediate state changes), the Exporter invokes the application to collect the cable modem status information and sends the data to the Collector. For more information, see the Operations Support System Interface (OSSI) Specification.

DOCSIS CMTS CM Upstream Status Service Definition

This service definition schema define the cable modem registration status objects and upstream status objects from the cable modem and the Cisco CMTS perspective. In the CmtsCmUsEqData IPDR schema field, configure the **cable upstream equalization-coefficient** command under the corresponding MAC domain to enable the feature to have data. For more information on this command, see the Cisco IOS CMTS Cable Command Reference Guide .

The DOCSIS-CMTS-CM-US-STATS-TYPE schema support the following collection methods:

- Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the cable modem upstream status information, then streams the records to the Collector.
- Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect all upstream status information of the cable modem and send the data to the Collector.

DOCSIS CMTS Topology Service Definition

In the case of an event session, the event means a change of the topology.

This service definition schema defines the IPDR service definition schema for the CMTS Topology information.

The DOCSIS-CMTS-TOPOLOGY-TYPE schema supports the following collection methods:

- Ad-hoc—Sends the entire picture of all fiber-nodes.
- Event—Sends only the updated channels status of the fiber nodes.

DOCSIS CPE Service Definition

The DOCSIS-CPE-TYPE schema supports the following collection methods:

- Ad-hoc—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the CPE status information, then transfers the records to the Collector.
- Event—When new CPE is added, the status of the CPE changes (including change in IP address), or a new CPE replaces an old one (in this case, two messages are displaced— removal of the old CPE and addition of the new CPE). For more information, see the Operations Support System Interface (OSSI) Specification.

DOCSIS CMTS Utilization Statistics Service Definition

The CMTS Utilization Statistics mainly focuses on channel utilization. It covers CMTS MAC Domain, channel identifier, and the upstream or downstream utilization attributes and counters.

The DOCSIS-CMTS-US-UTIL-STATS-TYPE schemas defines upstream utilization statistics for a specified upstream logical channel interface for the specified Cisco CMTS. The interval can be configured through Channel Utilization Interval.

The DOCSIS-CMTS-DS-UTIL-STATS-TYPE schema defines downstream utilization statistics for a specified downstream interface for the specified Cisco CMTS. The interval can be configured through Channel Utilization Interval.

For more information, see the IPDR Streaming Protocol on the Cisco CMTS Routers guide at the following URL:

IPDR Streaming Protocol

These schemas support only interval-driven event session for the entire downstream and upstream. The interval is defined in the docsIfCmtsChannelUtilizationInterval MIB and it creates document for every exporting.

Note The UsUtilTotalCntnReqDataMslots, UsUtilUsedCntnReqDataMslots, and UsUtilCollCntnReqDataMslots MIBs are not supported on the Cisco CMTS implementation.

The DsUtilTotalBytes MIB for RF Gateway RF channels is the maximum counter of bytes this RF channel can pass during an interval.

Modes of Operation

The Usage-based Billing feature can operate in three modes:

- File Mode—In file mode, the CMTS collects the billing record information and writes the billing records to a file on a local file system, using a file name that consists of the router's hostname followed by a timestamp of when the file was written. A remote application can then log into the CMTS and transfer the billing record file to an external server where the billing application can access it.

The remote application can use the Secure Copy Protocol (SCP) or the Trivial File Transfer Protocol (TFTP) to transfer the file. After a successful transfer, the remote application then deletes the billing record file, which signals the CMTS that it can create a new file. The remote application can either periodically log into the

CMTS to transfer the billing record file, or it can wait until the CMTS sends an SNMPv2 trap to notify the application that a billing record file is available.

- Streaming Mode—In streaming mode, the CMTS collects the billing record information and then regularly transmits the billing record file to an application on an external server, using either a non-secure TCP connection or a secure sockets layer (SSL) connection. The billing record data collected is streamed in real time; and if streaming is unsuccessful, then the SAMIS data is sent only at the next interval.

If the CMTS fails to establish a successful connection with the external server, it retries the connection between one to three times, depending on the configuration. If the CMTS continues to fail to connect with the external server, the Cisco CMTS sends an SNMPv2 trap to notify the SNMP manager that this failure occurred.

In streaming mode, you can configure the CMTS to transmit the billing record file at regular intervals. Typically, the interval chosen would depend on the number of cable modems and the size of the billing record files that the CMTS produces.

- IPDR Mode—In the IPDR mode, the IPDR export process communicates with IPDR Collectors. The architecture supports multiple Collectors distinguished by priority value for failover purposes. The smaller the number of Collectors, the higher is the priority value. Associating one session to two or more Collectors with the same priority value is regarded as random priority. At any given time, data is sent to only the available highest priority Collector. If the highest priority Collector connection fails due to any reason, the data is sent to the next available highest priority Collector. After a higher priority Collector comes back online, it will fail over again. Depending on the network configuration, you can have different primary Collectors for different IPDR sessions. For example, there may be a billing Collector or a diagnostic Collector.

Billing Record Format

Each billing record is an ASCII text file using XML formatting to encode the billing record objects that are required by the DOCSIS specifications. This file can be read by any billing application that can be configured to parse XML data files.

The table lists the objects that are contained in each billing record that the CMTS generates. This table shows the object's name, as it appears in the billing record, and a description of that object.

Table 34: Billing Record Objects

Object Name	Description
IPDRcreationTime	(Appears in header of billing record) Date and time that the CMTS created the billing created. Cisco uBR10012 router provides UTC timestamps for IPDR timestamping feature. To provide usage records with local time timestamping, use the **cable metering localtime** command. The IPDRcreationTime field in the Billing records shows the localtime timestamp as the time of creation of the record when it is enabled using the **cable metering localtime** command. If the localtime timestamping is not enabled, then the default UTC timestamp (indicated by a Z after the timestamp) is shown as time of creation of the record. For example, when the local time timestamping is enabled, the timestamp in metering output is local time "2015-03-03T16:26:07", otherwise the timestamp is the UTC time "2015-03-03T16:26:07Z" (with a "Z" indicating that the time is UTC).)
serviceClassName	Service Class Name (SCN) identifying the service flow (for example, BronzeDS). **Note** Cisco IOS Release 12.3(9a) and Cisco IOS Release 12.2(33)SC support DOCSIS 1.0 and DOCSIS 1.1 cable modems with the following differences between them: • Because DOCSIS 1.0 cable modems do not have service class names, the SCN field is always blank and the service flow ID (SFID) is the same as the service ID (SID). • For DOCSIS 1.1 cable modems, the value for the SCN field is what is configured and the SFID.
CMmacAddress	MAC Address of the cable modem, expressed as six hexadecimal bytes separated by dashes (for example, 00-00-0C-01-02-03).
CMipAddress	IP address for the cable modem, expressed in dotted decimal notation (for example, 192.168.100.101).
CMdocsisMode	Version of DOCSIS QoS provision that the cable modem is currently using (DOCSIS 1.0 or 1.1).

Object Name	Description
CPEipAddress	IP address for each CPE device that is using this cable modem, expressed in dotted decimal notation. This object is optional and can be suppressed to improve performance by reducing the size of the billing record files.
CMTSipAddress	IP address for the CMTS, expressed in dotted decimal notation.
CMTShostName	Fully qualified hostname for the CMTS (for example, cmts01.cisco.com).
CMTSsysUpTime	Amount of time, in hundredths of a second, since the last initialization of the CMTS management interface, expressed as a 32-bit decimal number (0 to 4,294,967,296).
RecType (SFType renamed to RecType in Cisco IOS Release 12.3(17a)BC)	Type of service flow being described: • **Interim—**the service flow was active throughout the collection period and should be reported as 1. • **Stop—**the service flow was deleted at some point during the collection period and should be reported as 2.
serviceIdentifier	Service flow ID assigned to this service flow by the CMTS, expressed as a decimal number. **Note** For DOCSIS 1.0 cable modems, the SFID field always shows the primary service flow for the upstream or downstream.
serviceDirection	Direction for the service flow (**Downstream** or **Upstream**).
serviceOctetsPassed	Total number of octets received by the cable modem (downstream service flows) or transmitted by the cable modem (upstream service flows) during the collection period, expressed as a 64-bit decimal number.
servicePktsPassed	Total number of packets received by the cable modem (downstream service flows) or transmitted by the cable modem (upstream service flows) during the collection period, expressed as a 64-bit decimal number.

Object Name	Description
SLAdropPkts	(Downstream service flows only) Total number of downstream packets for the cable modem that the CMTS dropped because otherwise they would have exceeded the bandwidth levels allowed by the subscriber's service level agreement (SLA), expressed as a 64-bit decimal number.
SLAdelayPkts	(Downstream service flows only) Total number of packets that the CMTS delayed transmitting on the downstream to the cable modem because otherwise they would have exceeded bandwidth levels allowed by the subscriber's service level agreement (SLA), expressed as a 64-bit decimal number.
CMTScatvIfIndex	The ifIndex of the MAC interface.
CMTScatvIfName	The ifName of the CMTS CATV (MAC) interface associated with this cable modem.
CMTSupIfName	The ifName of the CMTS Upstream interface associated with this cable modem.
CMTSdownIfName	The ifName of the CMTS Downstream interface associated with this cable modem.
CMcpeFqdn	FQDNs for cable modem associated CPEs.
serviceTimeCreated	Timestamp for SF creation (consistent with QoS MIB model).
serviceTimeActive	The active time of the SF in seconds.

Note Because the byte and packet counters are 64-bit values, it is possible for them to wrap around to zero during a billing period. The billing application should use the sysUpTime value along with the counters to determine whether the counters have wrapped since the last billing period. If a counter appears to regress, and if the current sysUpTime indicates this billing cycle is the next scheduled cycle for this particular cable modem, you can assume that the counter has wrapped during the billing cycle.

Note These billing record objects are defined in Appendix B, *IPDR Standards Submission for Cable Data Systems Subscriber Usage Billing Records* , in the *DOCSIS 2.0 OSSI Specification* (SP-OSSIv2.0-IO3-021218).

The following example shows a sample IPDR billing record for a downstream service flow:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="DOCSIS-3.1-B.0.xsd"
docId="C341A679-0000-0000-0000-000BBF54D000"
creationTime="2002-05-25T14:41:29Z"
IPDRRecorderInfo="CMTS01"
version="3.1">
</IPDR>
<IPDR xsi:type="DOCSIS-Type">
<IPDRcreationTime>2003-09-18T16:52:34Z</IPDRcreationTime>
<CMTShostname>R7519-UBR7246.cisco.com</CMTShostname>
<CMTSipAddress>1.8.8.21</CMTSipAddress>
<CMTSsysUpTime>287315    </CMTSsysUpTime>
<CMTScatvIfName>Cable8/0/0</CMTScatvIfName>
<CMTScatvIfIndex>13</CMTScatvIfIndex>
<CMTSupIfName>Ca8/0/0-upstream0</CMTSupIfName>
<CMTSupIfType>129</CMTSupIfType>
<CMTSdownIfName>Ca8/0/0-downstream</CMTSdownIfName>
<CMmacAddress>00-00-39-AB-D4-53</CMmacAddress>
<CMdocsisMode>1.0</CMdocsisMode>
<CMipAddress>3.8.21.3</CMipAddress>
<CPEipAddress></CPEipAddress>
<RecType>1</SFtype>
<serviceIdentifier>3</serviceIdentifier>
<serviceClassName></serviceClassName>
<serviceDirection>2</serviceDirection>
<serviceOctetsPassed>23457</ServiceOctetsPassed>
<servicePktsPassed>223</ServicePktsPassed>
<serviceSlaDropPkts>2</serviceSlaDropPkts>
<serviceSlaDelayPkts>0</serviceSlaDelayPkts>
<serviceTimeCreated>11000</serviceTimeCreated>
<serviceTimeActive>15890</serviceTimeActive>
</IPDR>
</IPDRDoc>
```


The following example shows a sample IPDR billing record for an upstream service flow:

<?xml version="1.0" encoding="UTF-8"?>


```
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="DOCSIS-3.1-B.0.xsd"
docId="docId="C3146152-0000-0000-0000-000BBF7D5800"
creationTime="2003-09-18T16:52:34Z"
IPDRRecorderInfo="CMTS01-UBR7246.cisco.com"
version="3.1">
<IPDR xsi:type=" DOCSIS-Type">
<IPDRcreationTime>2003-09-18T16:52:34Z</IPDRcreationTime>
<CMTShostname>R7519-UBR7246.cisco.com</CMTShostname>
<CMTSipAddress>1.8.8.21</CMTSipAddress>
<CMTSsysUpTime>287315    </CMTSsysUpTime>
<CMTScatvIfName>Cable8/0/0</CMTScatvIfName>
<CMTScatvIfIndex>13</CMTScatvIfIndex>
<CMTSupIfName>Ca8/0/0-upstream0</CMTSupIfName>
<CMTSupIfType>129</CMTSupIfType>
<CMTSdownIfName>Ca8/0/0-downstream</CMTSdownIfName>
<CMmacAddress>00-00-39-18-8A-4D</CMmacAddress>
<CMdocsisMode>1.0</CMdocsisMode>
<CMipAddress>3.8.21.14</CMipAddress>
<CPEipAddress></CPEipAddress>
<RecType>1</SFtype>
<serviceIdentifier>3</serviceIdentifier>
<serviceClassName></serviceClassName>
<serviceDirection>1</serviceDirection>
<serviceOctetsPassed>1404</ServiceOctetsPassed>
<servicePktsPassed>6</ServicePktsPassed>
<serviceSlaDropPkts>0</serviceSlaDropPkts>
<serviceSlaDelayPkts>0</serviceSlaDelayPkts>
<serviceTimeCreated>11000</serviceTimeCreated>
<serviceTimeActive>15890</serviceTimeActive>
</IPDR>
```

```
</IPDRDoc>
```

SNMP Support

Cisco IOS Release 12.3(9a)BC and Cisco IOS Release 12.2(33)SC support the following MIBs that provide SNMPv2 support for the Usage-based Billing feature:

CISCO-CABLE-METERING-MIB

- Supports configuration of the usage-based billing feature using SNMPv2 commands.
- Displays the current usage-based billing configuration using SNMPv2 commands.
- Sends SNMPv2 traps based on the following usage-based billing events:
  - The Cisco CMTS reports that a new billing record is available.
  - The Cisco CMTS reports that a failure occurred in writing the most recent billing record (for example, the disk is full).
  - The Cisco CMTS reports that it could not successfully open a secure SSL connection to stream a billing record to the billing server.

CISCO-CABLE-WIDEBAND-MIB
Sets the polling interval for calculating the utilization of an RF channel by using the **ccwbRFChanUtilInterval** object.

DOCS-QOS-MIB

- Sets the load and utilization of both upstream and downstream physical channels through the **docsIfCmtsChannelUtilizationInterval** object. This information may be used for capacity planning and incident analysis, and may be particularly helpful in provisioning high value QoS.
- Displays information about all service flows (DOCSIS 1.1 service flows only) including multicast service flow is maintained in the **docsQosServiceFlowLogTable** in DOCS-QOS-MIB, **docsIetfQosServiceFlowLogTable** in DOCS-IETF-QOS-MIB, and **docsQos3ServiceFlowLogTable** in DOCS-QOS3-MIB.

To view information about deleted service flows, enable logging of deleted service flows using the **cable sflog** global configuration command.

Benefits

The usage-based billing feature provides the following benefits to cable service providers and their partners and customers:

- Allows service providers to integrate their billing applications for DOCSIS services with their other XML-capable billing applications.
- Standards-based approach that supports existing networks and services, such as DOCSIS and PacketCable, and is easily extensible to support future services as they are supported on the Cisco CMTS.

How to Configure the Usage-based Billing Feature

This section describes the following tasks that are required to implement the Usage-based Billing feature:

Enabling Usage-based Billing Feature File Mode Using CLI Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in file mode, where it writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

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 metering filesystem** *filesys* [**flow-aggregate**] [**cpe-list-suppress**] [**full-records**]
	
	Example:
	`Router(config)# cable metering filesystem harddisk:`
	
	Example:
	`Router(config)#`
		Enables the Usage-based Billing feature for file mode and configures it.
		
		The system will write the billing records on this file system using a file name that contains the hostname of the router followed by a timestamp when the record was written.

Step 4	**snmp-server enable traps cable metering** **Example:** `Router(config)# snmp-server enable traps cable metering`	(Optional) Enables SNMP traps for usage-based billing events. Traps are sent when a new billing record is available, or when the system encountered a failure (such as insufficient disk space) in writing the new billing record.

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

Step 5	**cable sflog max-entry** *number* **entry-duration** *time*
	Example:
	`Router(config)# cable sflog max-entry 2000 entry-duration 7200`
	Example:
	`Router(config)#`
		(Optional) Enables logging for deleted SNMP service flows, which allows the billing feature to include information about deleted service flows.

Step 6	**cable metering source-interface** *interface*
	Example:
	`Router(config)# cable metering source-interface loopback100`
	Example:
	`Router(config)#`
		(Optional) Enables specification of the source-interface for the billing packets, usually a loopback interface.

Step 7	**end**
	Example:
	`Router(config)# end`
	Example:
	`Router#`
		Exits global configuration mode and returns to privileged EXEC mode.

Enabling Usage-based Billing Feature File Mode Using SNMP Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in file mode and writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

To configure the Cisco CMTS for Usage-based Billing feature in file mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB.

In addition, to include information about deleted service flows in the billing records (supported for DOCSIS 1.1 service flows), you must enable the logging of deleted service flows, using the **cable sflog** global configuration command.

Table 35: SNMP Objects to be Configured for File Mode

Object	Type	Description
ccmtrCollectionType	Integer	Enables or disables the Usage-based Billing feature. The valid values are: • 1—none. The Usage-based Billing feature is disabled (default). • 2—local. The Usage-based Billing feature is enabled and configured for file mode. • 3—stream. The Usage-based Billing feature is enabled and configured for streaming mode. Set ccmtrCollectionType to 2 (local) to enable the feature for file mode.
ccmtrCollectionFilesystem	DisplayString	Specifies the file system where the billing record file should be written. This object has a maximum length of 25 characters and must specify a valid file system on the router (such as slot0, disk1, or flash). **Note** The Cisco CMTS writes the billing records to this file system using a file name that consists of the router's hostname followed by a timestamp when the record was written.
ccmtrCollectionCpeList	TruthValue	(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following: • true—CPE information is present (default). • false—CPE information is omitted. **Note** When set to true, a maximum of 5 CPE IP addresses for each cable modem.

Object	Type	Description
ccmtrCollectionAggregate	TruthValue	(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows: • true—All service flow information for each cable modem is aggregated into a single billing record. In this configuration, the service flow ID (SFID) for the billing record is set to 0 and the service class name (SCN) is blank. • false—Information for each cable modem is not aggregated into a single billing record, but instead each service flow is recorded into its own record (default).
ccmtrCollectionSrcIfIndex	TruthValue	(Optional) Specifies the source-interface for the billing packets.

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Step 1 Set the ccmtrCollectionType object to 2, to enable the Usage-based Billing feature and to configure it for file mode:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
ccmtrCollectionType.0 -i 2
workstation#
```

Step 2 Set the ccmtrCollectionFilesystem object to the local file system where the Cisco CMTS should write the billing records:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
```

```
 ccmtrCollectionFilesystem.0 -D disk0:

workstation#
```

Step 3 (Optional) To omit the IP addresses of CPE devices from the billing records, set the ccmtrCollectionCpeList object to 2 (false). The default is to include the CPE information.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionCpeList.0 -i 2
workstation#
```

Step 4 (Optional) To aggregate all service flow information for each cable modem in a single record, set the ccmtrCollectionAggregate object to 1 (true). The default is for each service flow to be written in a separate record:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionAggregate.0 -i 1
workstation#
```

Step 5 (Optional) To specify the source-interface for the billing packets, set the ccmtrtrCollectionSrcIfIndex object to 1 (true). The default is for the billing packets to automatically select a source-interface.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrtrCollectionSrcIfIndex.0 -i 1
workstation#
```

Examples for Enabling Usage Billing using SNMP Mode

The following example shows the Usage-based Billing feature being configured using SNMP commands. The following display shows that a Cisco CMTS router at IP address 10.8.8.21 is configured with the default configuration (the Usage-based Billing feature is disabled):

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmtrCollectionType.0 = none(1)
ccmtrCollectionFilesystem.0 =
ccmtrCollectionCpeList.0 = true(1)
ccmtrCollectionAggregate.0 = false(2)
ccmtrCollectionStatus.0 = 0
ccmtrCollectionDestination.0 =
ccmtrCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmtrCollectionNotifEnable.0 = true(1)
workstation#
```

The following SNMP commands are then given to enable the Usage-based Billing feature and to configure it for file mode:

```
workstation# setany -v2c 10.8.8.21 rw-string ccmtrCollectionType.0 -i 2
```

```
workstation# setany -v2c 10.8.8.21 rw-string
ccmtrCollectionFilesystem
.0 -D disk1:
workstation#
```

These commands add the following line to the router's running configuration file:

```
Router# show running-config | include metering

cable metering filesystem disk1:
Router#
```

The following SNMP display shows the new configuration, after the Cisco CMTS has successfully written a billing record:

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmtrCollectionType.0 = local(2)
ccmtrCollectionFilesystem.0 = disk1:
ccmtrCollectionCpeList.0 = true(1)
ccmtrCollectionAggregate.0 = false(2)
ccmtrCollectionStatus.0 = success(1)
ccmtrCollectionDestination.0 = disk1:UBR7246.cisco.com-20030925-185827
ccmtrCollectionTimestamp.0 = 07 d3  09 19   12 3a  1c 00
ccmtrCollectionNotifEnable.0 = true(1)
workstation#
```

Enabling Usage-based Billing Feature Streaming Mode Using CLI Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in streaming mode, where it regularly transmits the billing records to an external server for use by the billing application.

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.

	Command or Action	Purpose

Step 3	**cable metering destination** *ip-address port* [*ip-address2 port2*] *retries minutes* {**non-secure** | **secure**} [**flow-aggregate**] [**cpe-list-suppress**] [**full-records**]
	
	Example:
	
	`Router(config)# cable metering destination 10.10.21.3 5300 10.10.21.4 5300 2 30 secure`
	
	Example:
	
	`Router(config)#`
		Enables the Usage-based Billing feature for streaming mode and configures it with the following parameters:

Step 4	**snmp-server enable traps cable metering**
	
	Example:
	
	`Router(config)# snmp-server enable traps cable metering`
	
	Example:
	
	`Router(config)#`
		(Optional) Enables SNMP traps for usage-based billing events. Traps are sent when a new billing record is available, or when the system encountered a failure (such as insufficient disk space) in writing the new billing record.

Step 5	**cable sflog max-entry** *number* **entry-duration** *time*
	
	Example:
	
	`Router(config)# cable sflog max-entry 2000 entry-duration 7200`
	
	Example:
	
	`Router(config)#`
		(Optional) Enables logging for deleted SNMP service flows, which allows the billing feature to include information about deleted service flows.

Step 6	**cable metering source-interface** *interface*
	
	Example:
	
	`Router(config)# cable metering source-interface loopback100`
	
	Example:
	
	`Router(config)#`
		(Optional) Enables specification of the source-interface for the billing packets, usually a loopback interface.

Step 7	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router#`	

Enabling Usage-based Billing Feature Streaming Mode Using SNMP Commands

This section describes how to use SNMP commands to enable and configure the Usage-based Billing feature so that it operates in streaming mode, where it regularly transmits the billing records to an external server for use by the billing application.

To configure the Cisco CMTS for Usage-based Billing feature in streaming mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB.

Note In addition, to include information about deleted service flows (DOCSIS 1.1 service flows only) in the billing records, you must enable the logging of deleted service flows, using the **cable sflog** global configuration command. See the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com:

Cisco CMTS Cable Command Reference

Table 36: SNMP Objects to be Configured for Streaming Mode

Object	Type	Description
cdtIpc	Integer	

Object	Type	Description
		Enables or disables the Usage-based Billing feature. The valid values are: • enable(1) - This object is used to enable the Usage-based Billing feature. • disable(2) - This object is used to disable the Usage-based Billing feature. • streaming(3) - This object is used to enable the Usage-based Billing feature in streaming mode. Set to 3

Object	Type	Description
		(stream) to enable the feature for streaming mode.
[illegible]	IpAddress	IP address for the external collection server. This value must be specified

Object	Type	Description
ccmCollectionPort	Unsigned32	TCP port number at the external collection server to which the billing records should be sent. The valid range is 0 to 65535, but you should not specify a port in the reserved range of 0 to 1024. This value must be specified

Note You can configure the ccmCollectionIpAddress and ccmCollectionPort objects twice, to specify a primary collection server and a secondary collection server.

Object	Type	Description
[illegible]	[illegible]	(Optional) Type of IP address being used for the collection server. The only valid value is ipv4, which is the default value.

Object	Type	Description
[illegible]	Unsigned32	(Optional) Specifies how often, in minutes, the billing records are streamed to the external server. The valid range is 2 to 1440 minutes (24 hours), with a default of 30 minutes (We recommend a minimum interval of 30 minutes)

Object	Type	Description
[illegible]	Unsigned32	(Optional) Specifies the number of retry attempts that the CMTS will make to establish a secure connection with the external server before using the secondary server (if configured) and sending an SNMP trap about the failure. The valid range for *n* is 0 to 5, with a default of 0.

Object	Type	Description
Note	The ccmCollectionInterval and ccmCollectionRetries parameters are optional when configuring usage-based billing for streaming mode with SNMP commands, but these parameters are required when configuring the feature with CLI commands.	

Object	Type	Description
[illegible]	TimeTicks	

Object	Type	Description
		(Optional) Specifies whether the Cisco CMTS should use a secure socket layer (SSL) connection when connecting with the billing application on the external server. The valid values are: – 1 = Enable SSL connection. The Cisco CMTS uses a SSL connection to stream billing records to the SNMP server. This is the default value. If the SNMP server does not support SSL, the Cisco CMTS will fallback to using TCP.

Object	Type	Description
		[illegible]

Object	Type	Description
[illegible]	[illegible]	

Object	Type	Description
		(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following: - [illegible] (Indicates that [illegible] IP addresses are [illegible] in the billing records.) - [illegible] (Indicates that [illegible] IP addresses are [illegible] in the billing records.) **Note** When set to

Object	Type	Description
		true, a maximum of 5 CPE IP addresses for each cable modem.

Object	Type	Description
[illegible]	TimeTicks	

Object	Type	Description
		(optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows: • latest: counters will reflect only the most recent cable modem

Object	Type	Description
		This object indicates the usage-based billing mode for IP traffic. If the value of this object is set to 0 and the CMTS is configured for usage-based billing, the CMTS will send DOCSIS-formatted usage-based billing records to the collector.

Object	Type	Description
		[illegible]
[illegible]	[illegible]	(Optional) Specifies the source for the billing packets

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Step 1 Set the ccmCollectionType object to 3, to enable the Usage-based Billing feature and to configure it for streaming mode:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionType.0 -i 3
workstation#
```

Step 2 Set the ccmCollectionIpAddress and ccmCollectionPort objects to the IP address of the external collection server and the TCP port number to which billing records should be sent:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionIpAddress.1 -o '0a 08 06 0b'

workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionPort.1 -g 6789

workstation#
```

Step 3 (Optional) Set the ccmCollectionIpAddress and ccmCollectionPort objects a second time to specify the IP address and TCP port number of a second external collection server to which billing records should be sent, in the case that the Cisco CMTS cannot connect to the primary collection server:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionIpAddress.1 -o '0a 08 06 0c'

workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionPort.1 -g 7000

workstation#
```

Step 4 (Optional) To change any of the other default parameters, set the appropriate objects to the desired values. For example, the following lines configure the Usage-based Billing feature for a non-secure connection, with a collection interval of 45 minutes, and a maximum number of 3 retries.

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionSecure.1 -i 2
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionInterval.1 -i 45
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionRetries.1 -i 3
workstation#
```

Step 5 (Optional) To omit the IP addresses of CPE devices from the billing records, set the ccmCollectionCpeList object to 2 (false). The default is to include the CPE information.

Example:

```
workstation# setany -v2c
```

```
ip-address rw-community-string
 ccmCollectionCpeList.0 -i 2
workstation#
```

Step 6 (Optional) To aggregate all service flow information for each cable modem in a single record, set the ccmCollectionAggregate object to 1 (true). The default is for each service flow to be written in a separate record:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmCollectionAggregate.0 -i 1
workstation#
```

Step 7 (Optional) To specify the source-interface for the billing packets, set the ccmtrCollectionSrcIfIndex object to 1 (true). The default is for the billing packets to automatically select a source-interface.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionSrcIfIndex.0 -i 1
workstation#
```

Examples for SNMP Commands

The following example shows the Usage-based Billing feature being configured using SNMP commands. The following display shows that a Cisco CMTS router at IP address 10.8.8.21 is configured with the default configuration (the Usage-based Billing feature is disabled):

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmCollectionType.0 = none(1)
ccmCollectionFilesystem.0 =
ccmCollectionCpeList.0 = true(1)
ccmCollectionAggregate.0 = false(2)
ccmCollectionStatus.0 = 0
ccmCollectionDestination.0 =
ccmCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmCollectionNotifEnable.0 = true(1)
workstation#
```

The following SNMP commands are then given to enable the Usage-based Billing feature and to configure it for streaming mode:

```
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionType.0 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionIpAddress.1 -o '0a 08 06 0b'

workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionPort.1 -g 6789

workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionSecure.1 -i 2
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionRetries.1 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionInterval.1 -i 45
workstation#
```

These commands add the following line to the router's running configuration file:

```
Router# show running-config | include metering

cable metering destination 10.8.6.11 6789 3 45 non-secure
Router#
```

The following SNMP display shows the new configuration:

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmCollectionType.0 = stream(3)
ccmCollectionFilesystem.0 =
ccmCollectionIpAddrType.1 = ipv4(1)
ccmCollectionIpAddress.1 = 0a 08  06 0b
ccmCollectionPort.1 = 6789
ccmCollectionInterval.1 = 45
ccmCollectionRetries.1 = 3
ccmCollectionSecure.1 = false(2)
ccmCollectionRowStatus.1 = active(1)
ccmCollectionCpeList.0 = true(1)
ccmCollectionAggregate.0 = false(2)
ccmCollectionStatus.0 = 0
ccmCollectionDestination.0 =
ccmCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmCollectionNotifEnable.0 = true(1)
workstation#
```

Enabling Usage-based Billing Feature File Mode Using CLI Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in file mode, where it writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

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.

	Command or Action	Purpose

Step 3	**cable metering filesystem** *filesys* [**flow-aggregate**] [**cpe-list-suppress**] [**full-records**]
	
	Example:
	
	`Router(config)# cable metering filesystem harddisk:`
	
	Example:
	
	`Router(config)#`
		Enables the Usage-based Billing feature for file mode and configures it.
		
		The system will write the billing records on this file system using a file name that contains the hostname of the router followed by a timestamp when the record was written.

Step 4	**snmp-server enable traps cable metering**
	
	Example:
	
	`Router(config)# snmp-server enable traps cable metering`
	
	Example:
	
	`Router(config)#`
		(Optional) Enables SNMP traps for usage-based billing events. Traps are sent when a new billing record is available, or when the system encountered a failure (such as insufficient disk space) in writing the new billing record.

Step 5	**cable sflog max-entry** *number* **entry-duration** *time*
	
	Example:
	
	`Router(config)# cable sflog max-entry 2000 entry-duration 7200`
	
	Example:
	
	`Router(config)#`
		(Optional) Enables logging for deleted SNMP service flows, which allows the billing feature to include information about deleted service flows.

Step 6	**cable metering source-interface** *interface*
	
	Example:
	
	`Router(config)# cable metering source-interface loopback100`
	
	Example:
	
	`Router(config)#`
		(Optional) Enables specification of the source-interface for the billing packets, usually a loopback interface.

Step 7	**end**
	
	Example:
	
	`Router(config)# end`
	
	Example:
	
	`Router#`
		Exits global configuration mode and returns to privileged EXEC mode.

Enabling Usage-based Billing Feature File Mode Using SNMP Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in file mode and writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

To configure the Cisco CMTS for Usage-based Billing feature in file mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB.

In addition, to include information about deleted service flows in the billing records (supported for DOCSIS 1.1 service flows), you must enable the logging of deleted service flows, using the **cable sflog** global configuration command.

Table 37: SNMP Objects to be Configured for File Mode

Object	Type	Description
ccmtrCollectionType	Integer	Enables or disables the Usage-based Billing feature. The valid values are: • 1—none. The Usage-based Billing feature is disabled (default). • 2—local. The Usage-based Billing feature is enabled and configured for file mode. • 3—stream. The Usage-based Billing feature is enabled and configured for streaming mode. Set ccmtrCollectionType to 2 (local) to enable the feature for file mode.
ccmtrCollectionFilesystem	DisplayString	Specifies the file system where the billing record file should be written. This object has a maximum length of 25 characters and must specify a valid file system on the router (such as slot0, disk1, or flash). **Note** The Cisco CMTS writes the billing records to this file system using a file name that consists of the router's hostname followed by a timestamp when the record was written.

Object	Type	Description
ccmtrCollectionCpeList	TruthValue	(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following: • true—CPE information is present (default). • false—CPE information is omitted. **Note** When set to true, a maximum of 5 CPE IP addresses for each cable modem.
ccmtrCollectionAggregate	TruthValue	(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows: • true—All service flow information for each cable modem is aggregated into a single billing record. In this configuration, the service flow ID (SFID) for the billing record is set to 0 and the service class name (SCN) is blank. • false—Information for each cable modem is not aggregated into a single billing record, but instead each service flow is recorded into its own record (default).
ccmtrCollectionSrcIfIndex	TruthValue	(Optional) Specifies the source-interface for the billing packets.

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Step 1 Set the ccmtrCollectionType object to 2, to enable the Usage-based Billing feature and to configure it for file mode:

Example:

```
workstation# setany -v2c

ip-address rw-community-string

ccmtrCollectionType.0 -i 2

workstation#
```

Step 2 Set the ccmtrCollectionFilesystem object to the local file system where the Cisco CMTS should write the billing records:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionFilesystem.0 -D disk0:

workstation#
```

Step 3 (Optional) To omit the IP addresses of CPE devices from the billing records, set the ccmtrCollectionCpeList object to 2 (false). The default is to include the CPE information.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionCpeList.0 -i 2
workstation#
```

Step 4 (Optional) To aggregate all service flow information for each cable modem in a single record, set the ccmtrCollectionAggregate object to 1 (true). The default is for each service flow to be written in a separate record:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionAggregate.0 -i 1
workstation#
```

Step 5 (Optional) To specify the source-interface for the billing packets, set the ccmtrtrCollectionSrcIfIndex object to 1 (true). The default is for the billing packets to automatically select a source-interface.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
```

```
 ccmtrtrCollectionSrcIfIndex.0 -i 1
workstation#
```

Enabling and Configuring the Secure Copy Protocol (optional)

This section describes how to configure the Cisco CMTS for the Secure Copy Protocol (SCP), which allow an external server to log in to the Cisco CMTS and copy the billing records from the Cisco CMTS to the external server.

Note For instructions on the actual procedure to be used when downloading the billing files from the Cisco CMTS router, see the Retrieving Records from a Cisco CMTS in File Mode, on page 225.

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	**aaa new-model**
	
	Example:
	`Router(config)# aaa new-model`
	
	Example:
	`Router(config)#`
		Enables the Authentication, Authorization, and Accounting (AAA) access control model.

Step 4	**aaa authentication login** {**default** | *list-name* } *method1* [*method2* ...]	Enables AAA access control authentication at login, using the following parameters:

	Command or Action	Purpose

	Example:
	`Router(config)# aaa authentication login default enable`
	Example:
	`Router(config)#`
		Valid methods include **enable**, **line**, and **local**.
		Note This command includes additional options. For details, see the documentation listed in Additional References, on page 240 .

Step 5	**aaa authorization exec** {**default** | *list-name* } *method1* [*method2* ...]
	Example:
	`Router(config)# aaa authorization exec default local`
	Example:
	`Router(config)#`
		Configures the CMTS to allow users to run an EXEC shell and access the CLI to run the Secure Copy commands.
		Valid methods include **local**.
		Note This command includes additional options. For details, see the documentation listed in Additional References, page 38 .

Step 6	**username** *name* **privilege** *level* **password** *encryption-type password*
	Example:
	`Router(config)# username billingapp privilege 15 password 7 billing-password`
	Example:
	`Router(config)#`
		(Optional) Creates a user account for login access and specifies the privilege level and password for that account:
		Note This step is optional but for the purposes of security and management, Cisco recommends creating a unique account for the billing application to use when logging into the CMTS.

Step 7	**ip ssh time-out** *seconds*
	Example:
	`Router(config)# ip ssh time-out 120`
	Example:
	`Router(config)#`
		Enables Secure Shell (SSH) access on the Cisco CMTS, which is required for SCP use. The *seconds* parameter specifies the maximum time allowed for SSH authentication, in seconds, with a valid range of 0 to 120 seconds, with a default of 120 seconds.

Step 8	**ip ssh authentication-retries** *n*
	Example:
	`Router(config)# ip ssh authentication-retries 3`
	Example:
	`Router(config)#`
		Specifies the maximum number of login attempts a user is allowed before the router disconnects the SSH session. The valid range is 1 to 5, with a default of 3 attempts.

	Command or Action	Purpose

Step 9	**ip scp server enable**
	
	Example:
	`Router(config)# ip scp server enable`
	
	Example:
	`Router(config)#`
		Enables SCP access on the Cisco CMTS.

Step 10	**end**
	
	Example:
	`Router(config)# end`
	`Router#`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring the Cisco CMTS for SSL Operation

This section describes the procedures to configure the Cisco CMTS for secure socket layer (SSL) operation, so that the Usage-based Billing feature can use an SSL connection to transfer the billing record files in streaming mode.

Note This procedure is required only when using the **secure** option with the **cable metering destination** command.

Prerequisites for CA

- The billing application server must be configured for SSL operations.
- A Certificate Authority (CA) must be configured to provide the required digital certificates to the billing application and Cisco CMTS router. The CA can be a public CA, such as Verisign, or a server on your private management network that is running software such as the Cisco Provisioning Center (CPC).

SUMMARY STEPS

To prepare the Cisco CMTS router for SSL operation, you must perform the following configuration steps:

- Configuring the router's host name and IP domain name, if not already done.
- Generating an RSA key pair.
- Declaring a Certification Authority.
- Configuring a Root CA (Trusted Root).
- Authenticating the CA.

- Requesting the Certificates.

For the detailed steps in performing these procedures, see the Configuring Certification Authority Interoperability

Retrieving Records from a Cisco CMTS in File Mode

When the Usage-based Billing feature is enabled and configured for File mode, the billing application server must regularly retrieve the billing records from the Cisco CMTS. This is typically done by a script that either logs in to the Cisco CMTS and uses CLI commands to transfer the file, or by a script that uses SNMP commands to transfer the file.

When using CLI commands, the procedure is typically as follows:

1. The billing application server receives an SNMP trap from the Cisco CMTS when a billing record is written. This notification contains the file name of the billing record that should be retrieved.
2. The billing application server starts a custom-written script to retrieve the billing record. This script would do one of the following:
   a. If using CLI commands, the script logs in to the Cisco CMTS using a telnet connection, and then transfers the billing record to the billing application server, using the **copy** CLI command. The transfer can be done using either the Secure Copy Protocol (SCP) or the Trivial File Transfer Protocol (TFTP).

Note You could also use the File Transfer Protocol (FTP) to transfer files from the Cisco CMTS to an external FTP server, but this is not recommended, because the FTP protocol transmits the login username and password in cleartext.

   b. If using SNMP commands, the script sets the ciscoFlashCopyEntry objects in the CISCO-FLASH-MIB to transfer the billing record to the application server, using TFTP.
3. After transferring the billing record, the script deletes it on the Cisco CMTS file system, so that the Cisco CMTS can begin writing a new billing record.

The following sections show examples of how this can be done, using each method.

Tip The following examples are given for illustration only. Typically, these commands would be incorporated in automated scripts that would retrieve the billing records.

Using SCP

To transfer billing records using SCP, you must first enable and configure the router for SCP operation, using the procedure given in the “Enabling and Configuring Secure Copy (optional)” section on page 21 . Then, the application server must log in to the Cisco CMTS and use the **copy** command at the privileged EXEC prompt. The **copy** command needs to specify the location of the billing record on the local filesystem and the destination server for the SCP transfer.

The following example shows a typical session where a billing record on slot0 is transferred to an FTP server with the hostname of billserver.mso-example.com:

```
CMTS01# copy slot0:CMTS01_20030211-155025 scp://billingapp-server.mso-example.com/

Address or name of remote host [billingapp-server.mso-example.com]?
Destination username [billing-app]?
Destination filename [CMTS01_20030211-155025]?
Writing CMTS01_20030211-155025
Password: billing-password

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1403352/1024 bytes]
1403352 bytes copied in 17.204 secs (85631 bytes/sec)
CMTS01# delete slot0:CMTS01_20030211-155025

CMTS01# squeeze slot0:

CMTS01#
```

Note The billing application must delete the billing record after it has been successfully transferred, so that the Cisco CMTS can write the next record. The **squeeze** command frees up the deleted disk space on Flash Memory and old-style PCMCIA cards (bootflash, flash, slot0, slot1). It is not needed on the newer ATA-style PCMCIA cards (disk0, disk1, disk2). However, because the **squeeze** command takes several seconds to complete, it should be given only when insufficient disk space exists for a new billing record. To avoid this problem, Cisco recommends using a 64 MB (or larger) ATA-style PCMCIA memory card, which automatically reclaims disk space for deleted files.

Using TFTP

To transfer billing records using TFTP, you must first configure an external workstation to be a TFTP server. For security, the TFTP server should be isolated from the Internet or any external networks, so that only authorized TFTP clients, such as the Cisco CMTS router, can access the server.

To transfer the billing records, the application server must log in to the Cisco CMTS and use the **copy** command at the privileged EXEC prompt. The **copy** command needs to specify the location of the billing record on the local filesystem and the destination server for the TFTP transfer.

The following example shows a typical session where a billing record on slot0 is transferred to an TFTP server with the hostname of billserver.mso-example.com.

```
Router# copy slot0:CMTS01_20030211-155025 tftp://billingapp-server.mso-example.com/incoming

Address or name of remote host [billingapp-server.mso-example.com]?
Destination username [billing-app]?
Destination filename [CMTS01_20030211-155025]?
Writing CMTS01_20030211-155025
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1102348/1024 bytes]
1102348 bytes copied in 14.716 secs (63631 bytes/sec)
Router# delete slot0:CMTS01_20030211-155025

Router# squeeze slot0:

Router#
```

Note The billing application must delete the billing record after it has been successfully transferred, so that the Cisco CMTS can write the next record. The **squeeze** command frees up the deleted disk space on Flash Memory and old-style PCMCIA cards (bootflash, flash, slot0, slot1). It is not needed on the newer ATA-style PCMCIA cards (disk0, disk1, disk2). However, because the **squeeze** command takes several seconds to complete, it should be given only when insufficient disk space exists for a new billing record. To avoid this problem, Cisco recommends using a 64 MB (or larger) ATA-style PCMCIA memory card, which automatically reclaims disk space for deleted files.

Using SNMP

To transfer billing record file using SNMP commands, you must set a number of objects in the CISCO-FLASH-MIB to transfer the file to a TFTP server. After the file has been successfully transferred, you can then use SNMp commands to delete the billing record file.

Note Before proceeding with these steps, ensure that the TFTP server is properly configured to receive to receive the billing records. At the very least, this means creating a directory that is readable and writable by all users. On some servers, the TFTP server software also requires that you create a file with the same name as the file that is to be received, and this file should also be readable and writable by all users.

To transfer a billing record file to a TFTP server, using SNMP commands, you must set a number of objects in the CISCO-FLASH-MIB.

Table 38: Transferring a File to a TFTP Server Using SNMP Commands

Object	Type	Description
ciscoFlashCopyEntryStatus	RowStatus	Status of this table entry. Typically, this object is first set to 5 (create-and-wait). Then after all other parameters are specified, it is set to Active (1) to execute the command.
ciscoFlashCopyCommand	INTEGER	Type of copy command to be performed. To copy a billing record file to a TFTP server, set this object to 3 (copyFromFlash).
ciscoFlashCopyServerAddress	IpAddress	IP address of the TFTP server. **Note** This parameter defaults to the broadcast address of 255.255.255.255, which means it will transfer the billing record file to the first TFTP server that responds. For security, this object should always be set to the IP address of the authorized TFTP server.

Object	Type	Description
ciscoFlashCopySourceName	DisplayString	Name of the billing record file to be transferred, including the Flash device on which it is stored.
ciscoFlashCopyDestinationName	DisplayString	(Optional) Name for the billing record, including path, on the TFTP server. If not specified, the copy operation defaults to saving the billing record at the top-most directory on the TFTP server, using the original file name. **Note** A file with the destination file name should already exist on the TFTP server. This file should be readable and writable by all users, so that it can be replaced with the billing record file.
ciscoFlashCopyProtocol	INTEGER	(Optional) Specifies the protocol to be used when copying the file. For a TFTP transfer, set this object to 1 (tftp), which is the default.
ciscoFlashCopyNotifyOnCompletion	TruthValue	(Optional) Specifies whether the Cisco CMTS should generate a trap upon the completion of the copy operation. The default is false (no trap is generated).

After transferring the billing records file, you must then set a number of objects in the CISCO-FLASH-MIB to delete the file, so that the Cisco CMTS can begin writing a new file. If the Flash memory is not ATA-compatible, you must also set a number of objects to squeeze the Flash memory to make the deleted space available for new files. Table 39: Deleting a File Using SNMP Commands , on page 228 describes each of these objects, and whether they are required or optional.

Table 39: Deleting a File Using SNMP Commands

Object	Type	Description
ciscoFlashMiscOpCommand	INTEGER	Specifies the operation to be performed: • 3—Delete the file. • 5—Squeeze the Flash memory, so as to recover the deleted space and make it available for new files.

Object	Type	Description
ciscoFlashMiscOpDestinationName	DisplayString	When deleting a file, the name of the file to be deleted, including the name of the file system, up to a maximum of 255 characters. When squeezing a file system, the name of the file system to be squeezed (slot0:, slot1:, flash:, or bootflash:).
ciscoFlashMiscOpEntryStatus	RowStatus	Status of this table entry. Typically, this object is first set to 5 (create-and-wait). Then after all other parameters are specified, it is set to Active (1) to execute the command.
ciscoFlashMiscOpNotifyOnCompletion	TruthValue	(Optional) Specifies whether the Cisco CMTS should generate a trap upon the completion of the operation. The default is false (no trap is generated).

DETAILED STEPS

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Copying the Billing Record File to the TFTP Server

Step 1 The script performing the copy should generate a 32-bit number to be used as the index entry for this copy command. The script can generate this number in any convenient way, so long as the index number is not currently being used for another operation.

Step 2 Create the table entry for the copy command, by using the number that was generated in Step 1 and setting the ciscoFlashCopyEntryStatus object to the create-and-wait state (5):

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 5

workstation#
```

Step 3 Set the ciscoFlashCopyCommand to 3 (copyFromFlash) to specify that the billing record file should be copied from the router's Flash file system:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyCommand
.582
```

```
-i 3
workstatioN#
```

Step 4 Set the ciscoFlashCopyServerAddress object to the IP address of the TFTP server:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyServerAddress
.582

-a "172.20.12.193"

workstatioN#
```

Step 5 Set the ciscoFlashCopySourceName object to the file name, including the device name, of the billing record file to be transferred:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopySourceName
.582
-D
"slot0:CMTS01_20030211-155025
"
workstation#
```

Step 6 (Optional) To specify a specific destination on the TFTP server, set the ciscoFlashCopyDestinationName object to the path name and file name for the billing record file on the TFTP server. (Typically, the path name and file name should already exist on the TFTP server.)

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyDestinationName
.582
-D
"/cmts01-billing/billing-file
"
workstation#
```

Step 7 To execute the command, set the ciscoFlashCopyEntryStatus object to the active state (1):

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 1

workstation#
```

Step 8 Periodically poll the ciscoFlashCopyStatus object until the file transfer completes:

Example:

```
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyOperationSuccess(2)
workstation#
```

If the file transfer fails, the most common status values that are reported by the ciscoFlashCopyStatus object are:

- 3—copyInvalidOperation. This indicates that the operation failed on the TFTP server, typically because the destination file name and path name do not exist on the TFTP server, or they exist but are not writable by all users.
- 5—copyInvalidSourceName. The file name for the billing record, as specified in ciscoFlashCopySourceName does not exist. Verify that you specified the correct device name and that no spaces exist in the file name.
- 6—copyInvalidDestName. The destination path name and file name specified in ciscoFlashCopyDestinationName is not accessible on the TFTP server. This could be because the path name does not exist or is not configured to allow write-access. This error could also occur if a file with the same path name and file name already exists on the TFTP server.
- 7—copyInvalidServerAddress. The IP address of the TFTP server specified in ciscoFlashCopyServerAddress is invalid, or the TFTP server is not responding.
- 14—copyFileTransferError. A network error occurred that prevented the file transfer from completing.

Step 9 After the file transfer has completed successfully, set the ciscoFlashCopyEntryStatus object to 6 (delete) to delete the row entry for this copy command:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 6
workstation#
```

What to Do Next

Deleting the Billing Record File

Using SNMP

After the billing record file has been successfully transferred, use the following procedure to delete the billing record on the Cisco CMTS flash file system, so that the Cisco CMTS can write the new billing record.

Step 1 Generate another random number to be used as an index entry and configure the following objects in the ciscoFlashMiscOpTable:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.31 -i 5

workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpCommand
.31 -i 3
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpDestinationName
.31 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.31 -i 1
```

```
workstation#
```

Step 2 Periodically poll the ciscoFlashMiscOpStatus object until the file transfer completes:

Example:

```
workstation# getmany -v2c ip-address rw-community-string ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.31 = miscOpInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.582 = miscOpOperationSuccess(2)
workstation#
```

Step 3 If the Flash memory system is not ATA-compatible (slot0:, slot1:, flash:, or bootflash:), configure the following objects in the ciscoFlashMiscOpTable to squeeze the Flash file system to recover the deleted file space:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.32
-i 5

workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpCommand
.32 -i 5
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpDestinationName
.32 -D slot0:
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.32
-i 1

workstation#
```

Examples To Transfer Using SNMP

The following SNMP commands transfer a file named CMTS01_20030211-155025 to a TFTP server at the IP address 10.10.31.3. After the file is successfully transferred, the row entry for this copy command is deleted.

```
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyCommand
.582
 -i 3
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyServerAddress
.582
 -a "10.10.31.3"

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopySourceName
.582 -D
"slot0:CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyDestinationName
.582 -D
"/cmts01-billing/CMTS01_20030211-155025
```

```
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 1

workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyOperationSuccess(2)
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 6

workstation#
```

The following commands show a billing record file being deleted on the Cisco CMTS file system, and the deleted file space being recovered by a squeeze operation:

```
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.31 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpCommand
.31 -i 3
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpDestinationName
.31 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.31 -i 1

workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.31 = miscOpInProgress(1)
workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.582 = miscOpOperationSuccess(2)
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.32 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpCommand
.32 -i 5
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpDestinationName
.32 -D slot0:
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.32 -i 1

workstation#
```

Disabling the Usage-based Billing Feature

This section describes how to disable the Usage-based Billing. Giving this command immediately stops the collection of billing information. If a billing record is currently written or being streamed to an external server, the CMTS completes the operation before disabling the usage-based billing feature.

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	**no cable metering**
	
	Example:
	`Router(config)# no cable metering`
	
	Example:
	`Router(config)#`
		Immediately disables the Usage-based Billing feature and stops the collection of billing information.

Step 4	**no snmp-server enable traps cable metering**
	
	Example:
	`Router(config)# no snmp-server enable traps cable metering`
	
	Example:
	`Router(config)#`
		(Optional) Disables SNMP traps for usage-based billing events.

Step 5	**no cable sflog**
	
	Example:
	`Router(config)# no cable sflog`
	
	Example:
	`Router(config)#`
		(Optional) Disables the logging of deleted service flows.

	Command or Action	Purpose

Step 6	**no cable metering source-interface**
	
	Example:
	`Router(config)# no cable metering source-interface`
	
	Example:
	`Router(config)#`
		(Optional) Disables a specified source-interface for the billing packets.

Step 7	**exit**
	
	Example:
	`Router(config)# exit`
	
	Example:
	`Router#`
		Exits global configuration mode.

Configuring Certified SSL Servers for Usage-Based Billing

Cisco IOS Release 12.3(17a)BC introduces support for the Secure Socket Layer (SSL) Server, used with the usage-based billing feature of the Cisco CMTS. Usage-based billing implements the DOCSIS Subscriber Account Management Interface Specification (SAMIS) format.

This new capability enables the configuration of the SSL server between the Cisco CMTS and a collection server. Certificate creation steps and **debug** commands are added or enhanced to support the SSL Server and certificates. This section describes general steps.

Refer also to the "Configuring the Cisco CMTS for SSL Operation" section .

Generating SSL Server Certification

These general steps describe the creation and implementation of certification for the Secure Socket Layer (SSL) Server.

1. Generate the CA key.
2. Set up the open SSL environment, to include directory and sub-directory.
3. Copy files to the appropriate directories.
4. Generate the SSL Server certification request.
5. Grant the SSL Server certification request.
6. Convert the SSL Server certification to DER format.
7. Copy the SSL certification to Bootflash memory (write mem).
8. Start the SSL server.

Configuring and Testing the Cisco CMTS for Certified SSL Server Support

Perform the following steps to configure the Cisco router to support the SSL Server and certification.

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	**ip domain name** *domain* **Example:** `Router(config)# ip domain name Cisco.com`	Defines a default domain name that the Cisco IOS software uses to complete unqualified host names (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. **Note** See the Domain Name System (DNS) document on Cisco.com for additional DNS information.
Step 4	**crypto key generate rsa** **Example:** `Router(config)# crypto key generate rsa`	Generates RSA key pairs.

Step 5	Ctrl-Z
	
	Example:
	`Router(config)# Ctrl-Z`
	
	Example:
	`Router#`
		Returns to privileged EXEC mode.

Step 6	**test cable read certificate** **Example:** `Router# test cable read certificate`	Verifies the certificate is valid and operational on the Cisco CMTS.
Step 7	**show crypto ca certificate** **Example:** `Router# show crypto ca certificate`	Displays the available certificates on the Cisco CMTS.

	Command or Action	Purpose

Step 8	**configure terminal**
	
	Example:
	
	`Router# configure terminal`
	
	Example:
	
	`Router(config)#`
		Enters global configuration mode.

Step 9	**cable metering destination** *ip-addr num-1 num-2 num-3* **secure** **Example:** `Router(config)# cable metering destination 1.7.7.7 6789 0 15 secure`	Defines the destination IP address for cable metering, to be used with the certificate.
Step 10	test cable metering **Example:** `Router# test cable metering`	Tests cable metering in light of the supported SSL server and metering configuration.

Monitoring the Usage-based Billing Feature

To display the most current billing record, use the **show cable metering-status** command. The following example shows typical output when usage-based billing is configured to write the billing records to a local file system:

```
CMTS01# show cable metering-status

destination                         complete-time   flow   cpe     status
                                                   aggr suppress
disk0:R7519-UBR7246-20000308-004428 Jun 12 09:33:05  No     No     success
CMTS01#
```

The following example shows a typical output for the **show cable metering-status** command when usage-based billing is configured to stream the billing records to an external server:

```
Router# show cable metering-status

destination                       complete-time   flow cpe  full status
                                                  aggr supp rec
10.11.37.2 :1234                  Jun 12 09:33:05  No   No  No success
Router#
```

The following example shows a typical output for the **show cable metering-status** command using verbose option:

```
Router# show cable metering-status verbose
```

```
Last export status
Destination : disk0:sunethra10k-20070129-190423
Complete Time : Jan29 19:04:38
Flow Aggregate : No
Full records : No
Cpe list suppression : No
Source interface : FastEthernet0/0/0
Status of last export : success
Current export status : In progress
```

The following example shows a typical output for the **show cable metering-status** command when usage-based billing is configured to use the IPDR Exporter to stream the billing records to an external server:

```
Router# show cable metering-status
destination                 complete-time   flow  cpe   full    status
              aggr  supp  rec
IPDR_Session2               Apr12 16:51:15  No    No    No    success
```

The following example shows a typical output for the verbose form of the **show cable metering-status** command when usage-based billing is configured to use the IPDR Exporter to stream the billing records to an external server:

```
Router# show cable metering-status
 verbose

Last export status
Destination                : IPDR_Session2
Complete Time          : Apr12 16:51:15
Flow Aggregate         : No
Full records                :No
Cpe list suppression   : No
Source interface       : Not defined
Status of last export  : success
```

Note If the **show cable metering-status** command displays the status of a streaming operation as “success” but the records were not received on the billing application server, verify that the Cisco CMTS and server are configured for the same type of communications (non-secure TCP or secure SSL). If the Cisco CMTS is configured for non-secure TCP and the server is configured for secure SSL, the Cisco CMTS transmits the billing record successfully, but the server discards all of the data, because it did not arrive in a secure SSL stream.

Tip The **show cable metering-status** command continues to show the status of the last billing record operation, until that billing record is deleted. If the record is not deleted, no new records are created.

To display information about the state of the IPDR Exporter, use the show ipdr Exporter command. The following example shows typical output:

```
Router#configure terminal
Router#show ipdr exporter
```

IPDR exporter is started.

Configuration Examples for Usage-based Billing

This section lists the following sample configurations for the Usage-based Billing feature:

File Mode Configuration (with Secure Copy)

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in file mode and enabling Secure Copy (SCP) for file transfers.

```
!
cable metering filesystem disk1:
snmp-server enable traps cable metering
...
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
username billingapp level 15 password 7 billing-password
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

Non-Secure Streaming Mode Configuration

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in streaming mode and specifying both a primary and a secondary external server. The data is sent using standard TCP packets, without any security.

```
cable metering destination 10.10.10.171 5321 10.10.10.173 5321 2 30 non-secure
snmp-server enable traps cable metering
```

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in streaming mode and specifying only a primary external server:

```
cable metering destination 10.10.11.181 6789 2 30 non-secure
snmp-server enable traps cable metering
```

Note You must ensure that the billing application server is configured for standard TCP communications. If the billing application server is configured for SSL communications when the Cisco CMTS is configured for standard TCP, the Cisco CMTS is able to send the billing records to the server, but the server discards all of that information because it is not arriving in a secure stream.

Secure Streaming Mode Configuration

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in streaming mode and specifying only a primary external server. Secure socket layer (SSL) TCP connections are used to transmit the data, which requires the configuration of a digital certificate.

```
cable metering destination 10.10.11.181 6789 2 30 secure cpe-list-suppress
snmp-server enable traps cable metering
...
crypto ca trustpoint SSL-CERT
!
crypto ca certificate chain SSL-CERT
 certificate ca 00
  308204A6 3082038E A0030201 02020100 300D0609 2A864886 F70D0101 04050030
  8198310B 30090603 55040613 02555331 13301106 03550408 130A4361 6C69666F
  726E6961 3111300F 06035504 07130853 616E204A 6F736531 1C301A06 0355040A
  13134369 73636F20 53797374 656D732C 20496E63 2E311130 0F060355 040B1308
```

```
  4361626C 65204255 310E300C 06035504 03130553 65656D61 3120301E 06092A86
...
  3E65DBBA 337627E8 589980D6 C8836C7E 3D3C3BC1 F21973BF 7B287D7A 13B16DA2
  02B2B180 C2A125C7 368BDA4C 0B8C81B7 7D5BEFF9 A6618140 1E95D19E BD0A84F5
  B43702AB 39B5E632 87BA36AC A3A8A827 C5BAC0F1 B24B8F4D 55615C49 5B6E4B61
  B15CC48A 8EF566C8 6E449B49 BF8E9165 317C1734 9A48A240 78A356B5 403E9E9B
  88A51F5B 0FE38CC2 F431
  quit
!
```

Note You must ensure that the billing applications server is also configured for SSL communications.

Additional References

Related Documents

Related Topic	Document Title
IPDR Streaming Protocol on the Cisco CMTS Routers	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/c/en/us/td/docs/ios/cable/configuration/guide/12_2sc/Cisco_CMTS_NetworkMgmt_Trblshting/ipdr_feature.html
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/c/en/us/support/ios-nx-os-software/ios-software-releases-12-2-mainline/products-installation-and-configuration-guides-list.html http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-software-releases-12-2-mainline/products-command-reference-list.html
Secure Copy (SCP) Configuration	*Secure Copy* feature module, at the following URL: http://www.cisco.com/en/US/partner/docs/ios/sec_user_services/configuration/guide/sec_secure_copy_external_docbase_0900e4b180de5694_4container_external_docbase_0900e4b181501651.html Cisco IOS Release 12.2 T Command Reference, *Other Security Features, Secure Shell Commands* , at the following URL: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecur_r/srfssh.html

Related Topic	Document Title
Secure Sockets Layer (SSL)	Introduction to Secure Sockets Layer white paper, at the following URL: http://www.cisco.com/c/en/us/tech/security-vpn/secure-socket-layer-ssl/index.html
Information about IPDR	IPDR.org web site, at the following URL: http://www.ipdr.org
IPDR.org Software Reference Libraries	IPDR.org project page, at the following URL: http://sourceforge.net/projects/ipdr/index.html
OSSI Specification	http://www.cablelabs.com/specifications/CM-SP-OSSIv3.0-I13-101008.pdf

Standards

Standards[22]	Title
NDM-U v3.1.1	Network Data Management – Usage (NDM-U) For IP-Based Services, Version 3.1.1 (http://www.ipdr.org)
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)
SP-OSSIv2.0-I09-050812	Data-Over-Cable Service Interface Specifications DOCSIS 2.0 Operations Support System Interface (OSSI) Specification (http://www.cablemodem.com)
XML Schema	Extensible Markup Language (XML) schema (http://www.w3.org)

22 Not all supported standards are listed.

MIBs

MIBs[23]	MIBs Link
CISCO-CABLE-METERING-MIB CISCO-CABLE-WIDEBAND-MIB DOCS-QOS-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

23 Not all supported MIBs are listed.

RFCs

RFCs[24]	Title
RFC 2233	DOCSIS OSSI Objects Support
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

24 Not all supported RFCs are listed.

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 Usage-Based Billing 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.

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

Table 40: Feature Specifications for Usage-based Billing

Feature Name	Release	Feature Information
Usage-based Billing	12.3(9a)BC	This feature was introduced on Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers. Feature support includes the new CISCO-CABLE-METERING-MIB, which contains objects that provide subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format.
Usage-based Billing	12.3(17a)BC	This feature includes additional MIBs that support OSSI specifications as well as enhanced billing reports. For more information about DOCSIS 2.0, see the Cable Labs document Data-Over-Cable Service Interface Specifications DOCSIS 2.0 Operations Support System Interface Specification. Support for Secure Socket Layer (SSL) Servers introduced with certification support.
Usage-based Billing	12.3(21)BC	This feature provides enhancements to specify the source interface for billing packets in the Subscriber Account Management Interface Specification (SAMIS). The cable metering source-interface <interface> command was introduced. Support also includes a new object **ccmtrCollectionSrcIfIndex** in CISCO-CABLE-METERING-MIB.my.
Usage-based Billing	12.2(33)SCB	SAMIS over Internet Protocol Detail Record (IPDR) was introduced.
Usage-based Billing	12.2(33)SCC4 12.2(33)SCD2	Added the **full-records** keyword to the **cable metering** commands. Introduced the **cable util-interval** command.
Usage-based Billing	12.2(33)SCI2	Added the**localtime** keyword in the **cable metering** command to enable local time timestamping in the IPDRcreationTime field in the Billing records.