Cable Monitoring Feature for Cisco cBR Series Routers

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

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

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

Finding Feature Information

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

Contents

Overview of Cable Monitor Command for cBR

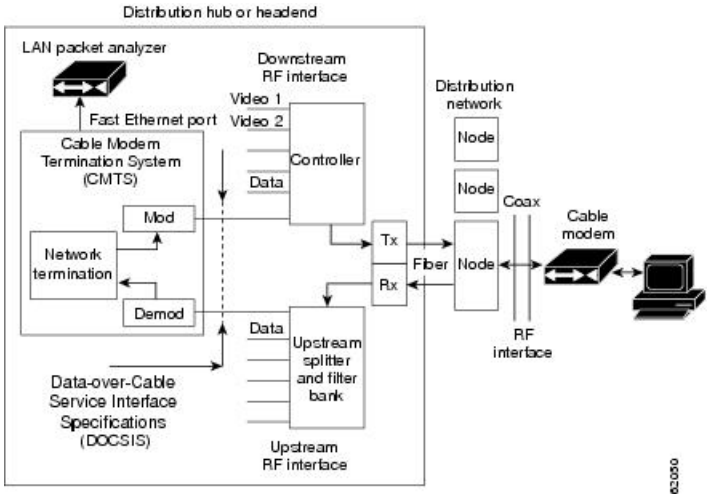
The **cable monitor** command sends copies of packets for specific types of traffic that is sent over a particular cable interface to a LAN analyzer, for use in troubleshooting network problems. This command can select packets to be forwarded using one or more of the following parameters:

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

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

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

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



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

Configuring Cable Monitoring for cBR Routers

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

SUMMARY STEPS

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

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

DETAILED STEPS

	Command or Action	Purpose

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

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

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

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

	Command or Action	Purpose

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

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

What to do next

You can capture and forward the sniffed packets to an external server or a local hard disk. For more details, see Capturing Sniffed Packets, on page 4.

Capturing Sniffed Packets

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

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

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

Capturing Sniffed Packets on an External Host

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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

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

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

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

Capturing Sniffed Packets on a Local Hard Drive

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`Router#configure CMON-Tunnel 3`
	Example:
	`Router(config)#`
		Enters global configuration mode.

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

Step 3	**mode buffer** **Example:** `Router(config-if)#mode buffer`	Enables mode buffer in the cmon-tunnel to capture packets by locating the hard disk.

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

Step 5	**show platform software interface fp active name-string CMON-Tunnel number**
	Example:
	`Router# show platform software interface fp active name-string CMON-Tunnel3`
	`Name: CMON-Tunnel3, ID: 131074, QFP ID: 11745,`
	`Schedules: 0`
	`Type: CABLE-MONITOR, State: enabled, SNMP ID: 0,`
	`MTU: 0`
	`IP Address: 0.0.0.0`
	`IPV6 Address: ::`
	`Flags: unknown`
	`ICMP Flags: unreachables, no-redirects,`
	`no-info-reply, no-mask-reply`
	`ICMP6 Flags: unreachables, no-redirects`
	`SMI enabled on protocol(s): UNKNOWN`
	`Authenticated-user:`
	`FRR linkdown ID: 65535`
	`Monitor Type: 0, Instance ID: 3, Mode: 3`
	`Monitor Tunnel Source: 0.0.0.0, Destination:`
	`0.0.0.0`
	`vNet Name: , vNet Tag: 0, vNet Extra Information: 0`
	`Dirty: unknown`
	`AOM dependency sanity check: PASS`
	`AOM Obj ID: 24094`
		Gets the QFP ID.

Step 6	**test platform hardware qfp active feature docsis cmon-copy 3 QFP_ID**	Uses the QFP ID to copy the buffer to the harddisk.

	Command or Action	Purpose

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

Cable Monitor Packet Struct

The cable monitor packet struct is described as follows:

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

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

Feature Information for Cable Monitoring

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

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

Table 1: Feature Information for Cable Monitoring

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