CHAPTER 4

Cable Monitor and Intercept Features for the Cisco CMTS

Revised: November 10, 2008, OL-1467-08

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

Feature Specifications for Cable Monitor and Intercept, Support

Feature History	
Release	**Modification**
12.0(6)SC, 12.1(2)EC	The **cable intercept** command was introduced for the Cisco uBR7200 series routers.
12.1(3a)EC	The **cable monitor** command was introduced for Cisco uBR7200 series routers.
12.1(5)EC	Support for both commands was added for the Cisco uBR7100 series routers.
12.1(11b)EC	The **cable intercept** command was enhanced to allow the data collector to be more than two hops from the Cisco CMTS.
12.1(4)CX	The **sid** option was added to the **cable monitor** command for DOCSIS 1.1 support.
12.2(4)BC1	Support for these above commands was added to the Release 12.2 BC train for the Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 universal broadband routers. However, this release does not support JIB-based cable interface line cards (such as the Cisco MC28X/U, Cisco MC16X/U, and Cisco MC520S/U).
12.3(13a)BC	Support for Service Independent Intercept (SII) was added by means of CISCO-TAP-MIB for SNMPv3. Feature support for the Cisco MC28X/U, Cisco MC16X/U, and Cisco MC520S/U cable interface line cards added to Cisco uBR7200 series and Cisco uBR10012 routers.
12.3(17a)BC	• Access Control Lists are supported on the Cisco uBR-MC5X20U/D and Cisco uBR-MC28U cable interface line cards. • Unconditional downstream sniffing enables downstream packets to be monitored, either for MAC or data packets. This enhancement supports both DOCSIS and Ethernet packet encapsulation.
12.2(33)SCB	Support for the Ten Gigabit Ethernet interface type was added to the **cable monitor** command.

Supported Platforms
Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 universal broadband routers

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Prerequisites

Cable Monitor and Intercept

- The Cisco CMTS must be running Cisco IOS Release 12.1(3a)EC and later 12.1 EC releases, or Cisco 12.2(4)BC or later 12.2 BC releases.

Restrictions for Cable Monitor and Intercept

- The **cable intercept** command by itself does not fulfill the PacketCable requirements for Lawful Intercept capability. To meet these requirements, PacketCable operations must also be enabled and configured on the Cisco CMTS router (see the documents in the "Additional References" section on page 4-15 for instructions on enabling PacketCable).
- The WAN interface on which packets are forwarded when using the **cable monitor** command should be used exclusively by the LAN analyzer. This interface must be an Ethernet, Fast Ethernet, Gigabit Ethernet, or Ten Gigabit Ethernet interface.
- Intercepted data from the **cable intercept** command is sent to a user-specified User Datagram Port (UDP) at a user-specified IP address. The data collector at that IP address must have exclusive use of the specified UDP port.
- The interception of customer traffic is governed by local laws and the service level agreements (SLA) with those customers. Consult the proper legal authorities before intercepting and monitoring third-party traffic. Also see the documents on CALEA and Lawful Intercept in the "Additional References" section on page 4-15.

Information About Cable Monitor and Intercept

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

- **cable intercept**—Forwards copies of the traffic to and from a specific MAC address to a server at a specific IP address and UDP port. This command can be used to respond to CALEA requests from law enforcement for traffic concerning a specific user.
- **cable monitor**—Forwards copies of selected packets on the cable interface to an external LAN analyzer attached to another interface on the Cisco CMTS router. This command can help in troubleshooting network and application problems.

See the following sections for more information about these commands.

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

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

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

Overview of the cable intercept Command

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

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

This command can be used to comply with the United States Federal Communications Assistance for Law Enforcement Act (CALEA) and other Lawful Intercept requirements for voice communications. For specifics on CALEA Lawful Intercept, see the *PacketCable Electronic Surveillance Specification*, as listed in the "Additional References" section on page 4-15.

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

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

Overview of the cable monitor Command

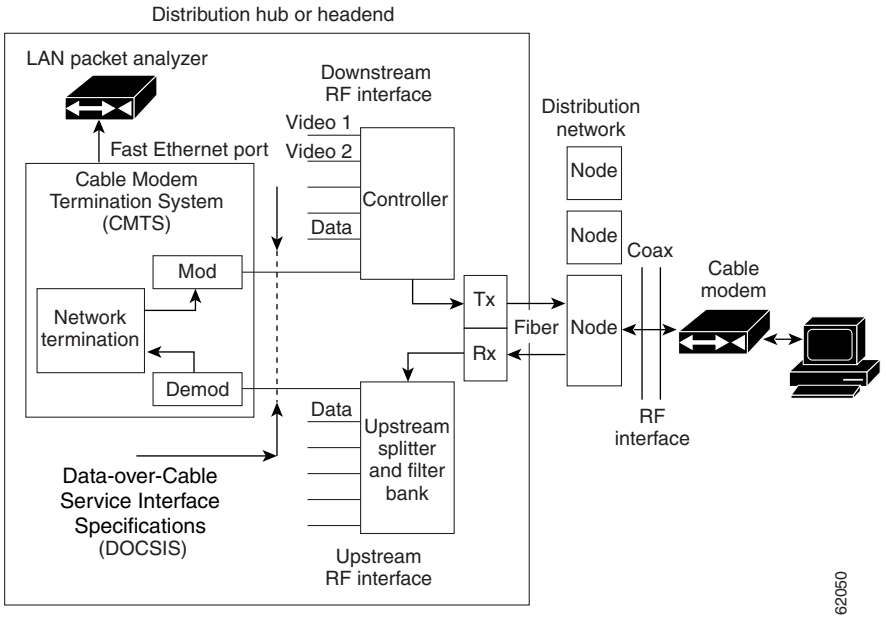
The **cable monitor** command sends copies of packets for specific types of traffic that is sent over a particular cable interface to a LAN analyzer, for use in troubleshooting network problems. This command can select packets to be forwarded using one or more of the following parameters:

- Either incoming or outbound packets
- Packets that match an IP access list
- Packets that match a specific MAC address (source and destination)
- Packets with a specific Service ID (SID)
- When monitoring a specific SID, select only specific DOCSIS MAC-layer packet types (dynamic service packets, MAP grant packets, and MAP request packets)

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

Figure 4-1 illustrates a LAN packet analyzer attached to a Fast Ethernet port in a DOCSIS two-way configuration.

Figure 4-1 LAN Packet Analyzer in a DOCSIS Two-Way Configuration



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

Tip When you are using the **cable monitor** command, and are including the DOCSIS header along with the Ethernet frame, it is possible that the total size of the forwarded packet could exceed the maximum allowable size for an Ethernet frame (1500 bytes), if the original Ethernet frame is at or near 1500 bytes. This is because the **cable monitor** command adds the DOCSIS header to the existing Ethernet frame. If this happens, the console displays a system message similar to the following:

```
%LINK-4-TOOBIG:Interface Ethernet2/0, Output packet size of 1518 bytes too big
```

This error message is typically accompanied by a traceback display. Both the error message and traceback are informational only and can be ignored. They do not indicate a traffic flow problem with the cable modem being monitored.

Overview of CISCO-TAP-MIB

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

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

Table 4-1 lists the objects in the MIB, as well as restrictions for the Cisco uBR10012 CMTS other than those listed in the MIB itself.

Table 4-1 CISCO-TAP-MIB Objects and Restrictions

Object	Restrictions for Cisco uBR10012
cTapMediationDestAddressType	Only IPv4 is supported (ITD restriction)
cTapMediationDestAddress	
cTapMediationDestPort	
cTapMediationSrcInterface	
cTapMediationRtcpPort	Not supported (ITD restriction[1])
cTapMediationDscp	
cTapMediationDataType	
cTapMediationRetransmitType	Not supported (ITD restriction)
cTapMediationTimeout	
cTapMediationTransport	UDP only (ITD restriction)
cTapMediationNotificationEnable	
cTapMediationStatus	
cTapMediationCapabilities	

Table 4-1 CISCO-TAP-MIB Objects and Restrictions (continued)

Object	Restrictions for Cisco uBR10012
cTapStreamCapabilities	
cTapStreamIpInterface	Only if interface is cable
cTapStreamIpAddrType	IPv4 only
cTapStreamIpDestinationAddress	
cTapStreamIpDestinationLength	Must be 32 (no subnets)
cTapStreamIpSourceAddress	
cTapStreamIpSourceLength	
cTapStreamIpTosByte	
cTapStreamIpTosByteMask	
cTapStreamIpFlowId	Not supported (IPv6 only)
cTapStreamIpProtocol	
cTapStreamIpDestL4PortMin	Must match …DestL4PortMax, or zero
cTapStreamIpDestL4PortMax	Must match …DestL4PortMin, or 65535
cTapStreamIpSourceL4PortMin	Must match …SourceL4PortMin, or zero
cTapStreamIpSourceL4PortMax	Must match …SourceL4PortMax, or 65535
cTapStreamIpInterceptEnable	
cTapStreamIpInterceptedPackets	
cTapStreamIpInterceptDrops	
cTapStreamIpStatus	

1. This means the restriction is across all Cisco platforms, not just Cisco CMTS platforms.

Benefits

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

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

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

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

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

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

How to Configure Cable Intercept and Monitoring Features

See the following sections to enable and configure the cable intercept and monitoring features.

Configuring the Cable Intercept Feature

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **cable intercept** *mac-address ip-address udp-port*
5. **exit**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

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

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

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

	Command or Action	Purpose

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

Step 5	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.

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

Configuring the Cable Monitor Feature

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **cable monitor** [**incoming** | **outbound**] [**timestamp**]
   interface *interface* {**access-list** {*name* | *number*} | **mac-address** *address* | **sid** *sid-number*}
   [**packet-type** {**data docsis** | **data ethernet** | [**mac type** *type*] }]
5. **exit**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

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

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

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

	Command or Action	Purpose

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

	Note Repeat Step 4 for each type of packet or MAC address to be monitored.	

Step 5	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.

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

Monitoring the Cable Intercept and Monitor Features

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

- Displaying Information About Intercepted Traffic, page 4-11
- Displaying Information About Monitored Traffic, page 4-11

Displaying Information About Intercepted Traffic

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

```
Router# show interface c6/0 intercept

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

Router#
```

Displaying Information About Monitored Traffic

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

```
Router# show interface cable 1/0 monitor

US/ Time Outbound  Flow     Flow Type      Flow  Packet MAC   MAC       Encap
DS  Stmp Interface Type     Identifier     Extn. Type   Extn. Type      Type
all  yes   Et1/0   mac-addr 0050.5462.008c yes   data   no     -        Ethernet
us   yes   Et1/0   acc-list 300            no     -     no     -          -
us   no    Et1/0   sid      2              yes   mac    yes   map-grant   -
all  no    Et1/0   acc-list rrr            no      -    no     -          -
all  no    Et1/0   mac-addr 0042.b013.008c yes   data   no     -        Ethernet
all  no    Et1/0   upstream 0              yes   data   no     -        docsis

Router#
```

Configuration Examples

The following examples illustrate sample configurations of the **cable intercept** and **cable monitor** commands and features on the Cisco CMTS:

Cable Intercept Examples

Cable Intercept Configuration Example

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

```
!
interface Cable3/0
 cable intercept 0003.e3fa.5e11 172.18.73.189 9999
...
```

Cable Monitor Examples

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

Cable Monitor Configuration Example (MAC Address)

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

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

Cable Monitor Configuration Example (Ethernet, MAC-Layer, and DOCSIS-Data Packets)

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

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

Cable Monitor DOCSIS Data Packets Example

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

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

The relevant DOCSIS bytes are the following:

- Byte 0x16—Control Field. A value of 03 indicates an unnumbered information frame.
- Byte 0x17—Version of the MAC management protocol. A value of 1 indicates a DOCSIS 1.0 message and a value of 2 indicates DOCSIS 1.1 message.
- Byte 0x18—MAC message type. In this example, a value of 04 indicates a Ranging Request (RNG-REQ) message.

The hexadecimal dump of the next packet is the following:

```
LLC: ----- LLC Header -----
      LLC:
      LLC: DSAP Address = FE, DSAP IG Bit = 00 (Individual Address)
      LLC: SSAP Address = E0, SSAP CR Bit = 01 (Response)
      LLC: I frame, N(R) = 42, N(S) = 80
      LLC:
DLC: Frame padding= 43 bytes
ADDR  HEX                                                 ASCII
0000:c2 00 00 2b 00 00 00 03 e3 fa 5e 8f 00 03 fe e1 | ...+......^.....
0010:a0 54 00 19 00 00 03 01 05 00 00 03 01 01 04 00 | .T..............
0020:00 00 00 02 01 00 03 02 00 00 05 01 03 00 8a 4d | ...............M
0030:6e 00 00 00 00 00 00 00 00 00 00 00             | n...........
```

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

Note For complete information on the DOCSIS MAC packet format, see Chapter 6 in the DOCSIS 1.1 specification (see the "Additional References" section on page 4-15).

Cable Monitor Timestamped Packets Example

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

```
0000(0000): C302003A 00000000  01E02F00 00010008...:....../.....
0010(0016): 0D6F4670 00260000  03010300 01380400 .oFp.&.......8..
0020(0032): 0061A1C1 0061A07C  00030004 FFFC4000 .a...a.|......@.
0030(0048): 0189401F FFFC4042  0001C043 007EF4EA ..@...@B...C.~..
```

The relevant portions of this packet are the following:

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

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

```
0000(0000): C302003A 00000000  01E02F00 00010008 ...:....../.....
0010(0016): 0D6F4670 00260000  03010300 01380400 .oFp.&.......8..
0020(0032): 0061A5AE 0061A469  00030004 FFFC4000 .a...a.i......@.
0030(0048): 0189401A FFFC403D  0001C03E 007EF4EF ..@...@=...>.~..
```

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

Additional References

For additional information related to the Cable Monitor and Intercept feature, refer to the following references:

Related Documents

Related Topic	Document Title
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference,* at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS Release 12.2 configuration guide	Cisco IOS Release 12.2 Configuration Guides References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html
Cisco IOS Release 12.2 command reference	Cisco IOS Release 12.2 Command References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html
Common Open Policy Service (COPS)	*COPS Engine Operation on the Cisco CMTS* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_cops_eng_op_ps2209_TSD_Products_Configuration_Guide_Chapter.html
PacketCable Configuration	*PacketCable for the Cisco CMTS*, in the Cisco CMTS Feature Guide, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm_ps2209_TSD_Products_Configuration_Guide_Chapter.html
Using the LAN analyzer	See the documentation for the LAN analyzer or other network interception software you are using for instructions on decoding DOCSIS MAC frames. **Note** One possible software utility you can use for this purpose is the Ethereal software, which is available for Windows and Unix systems.
CALEA Information	See the Communications Assistance for Law Enforcement Act (CALEA), which was passed by the United States Congress in 1994 and is now sections 1001 to 1010 of the United States Code Title 47 (Telegraphs, Telephones, and Radiotelegraphs). Also see the information on Cisco's web site at the following URL: http://www.cisco.com/wwl/regaffairs/lawful_intercept/index.html
Lawful Intercept	Lawful Intercept Technical Documentation at the following URL: http://www.cisco.com/en/US/tech/tk583/tk799/tsd_technology_support_protocol_home.html

Standard s

Standards[1]	Title
SP-RFIv1.1-I09-020830	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablelabs.com/cablemodem)
PKT-SP-ESP-I01-991229	PacketCable™ Electronic Surveillance Specification (http://www.cablelabs.com/packetcable)

1. Not all standards supported by this release are listed.

MIBs

MIBs[1]	MIBs Link
CISCO-TAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

1. Not all MIBs supported by this release are listed.

RFCs

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

Technical Assistance

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