



Service Independent Intercept on the Cisco CMTS Routers

First Published: February 14, 2008, Cisco IOS Release 12.2(33)SCA

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

In other Cisco IOS Releases prior to 12.2(33)SCA on the Cable Modem Termination System (CMTS) routers, LI capability includes the following support:

- Intercepts for voice traffic in PacketCable environments
- IP intercepts for SII using SNMPv3
- Command-line interface (CLI) for MAC intercepts

SII extends this LI capability in Cisco IOS Release 12.2(33)SCA by adding support for customer premise equipment (CPE)-based and cable modem (CM)-based MAC intercepts using SNMPv3. SII is designed to provide data intercepts via SNMPv3, while PacketCable intercepts are designed for voice IP intercepts using a COPS interface.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Service Independent Intercept](#)” section on page 379.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for Service Independent Intercept on the Cisco CMTS Routers, page 362](#)
- [Restrictions for Service Independent Intercept, page 362](#)
- [Information About Service Independent Intercept, page 363](#)
- [How to Perform SNMPv3 Provisioning for Service Independent Intercept, page 369](#)
- [Additional References, page 377](#)
- [Feature Information for Service Independent Intercept, page 379](#)

Prerequisites for Service Independent Intercept on the Cisco CMTS Routers

- SII intercepts are supported only on virtual bundle interfaces.
- You understand SNMPv3 configuration before configuring SII, and SNMPv3 is configured on the router.

Table 1 shows the hardware compatibility prerequisites for this feature.

Table 1 *Service Independent Intercept on 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)SCA <ul style="list-style-type: none"> • PRE-2 	Cisco IOS Release 12.2(33)SCA <ul style="list-style-type: none"> • Cisco uBR10-MC5X20S/U/H
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA <ul style="list-style-type: none"> • NPE-G1 • NPE-G2 	Cisco IOS Release 12.2(33)SCA <ul style="list-style-type: none"> • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA <ul style="list-style-type: none"> • NPE-G1 	Cisco IOS Release 12.2(33)SCA <ul style="list-style-type: none"> • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X

Restrictions for Service Independent Intercept

- IPv6 addressing for IP intercepts is not supported.
- The mediation device(MD) must be reachable via the global IP routing table. Support for a MD inside an MPLS/VPN is not supported.
- You cannot display information about intercepts gathered with SII using the command-line interface (CLI). Intercept content from SII will not appear in the **show pxf cable** commands. Other intercept information outside of SII content (for PacketCable and via CLI intercept) is shown.

- The Cisco uBR10012 router has the following MIB object restrictions:
 - When a Performance Routing Engine (PRE) switchover occurs, the SII configuration is lost. You must reconfigure SII after a PRE switchover.
 - cTapMediationDestAddressType—IPv6 is not supported
 - cTapMediationRtcpPort—Not supported
 - cTapMediationRetransmitType—Not supported
 - cTapMediationTransport—UDP only
 - cTapStreamIpInterface—Only if interface supported is cable
 - cTapStreamIpAddrType—IPv6 is not supported
 - cTapStreamIpDestinationLength—Must be 32 (no subnets are supported)
 - cTapStreamIpFlowId—Not supported (for IPv6 only)
 - cTapStreamIpDestL4PortMin—Must match DestL4PortMax or have a value of 0
 - cTapStreamIpDestL4PortMax—Must match DestL4PortMin or have a value of 65535
 - cTapStreamIpSourceL4PortMin—Must match SourceL4PortMin or have a value of 0
 - cTapStreamIpSourceL4PortMax—Must match SourceL4PortMax or have a value of 65535

Information About Service Independent Intercept

SII has the following benefits:

- Does not affect subscriber services on the router.
- Cannot be detected by the target.
- Allows LEAs to perform lawful intercepts without the knowledge of service providers.
- Uses Simple Network Management Protocol Version 3 (SNMPv3) and security features like the View-based Access Control Model (SNMP-VACM-MIB) and User-based Security Model (SNMP-USM-MIB) to restrict access to lawful intercept information and components.
- Supports intercepts of Layer 3 and Layer 2 traffic.
- Supports Layer 2 intercepts for upstream and downstream traffic.
- Hides information about lawful intercepts from all but the most privileged users. An administrator must set up access rights to enable privileged users to access lawful intercept information.
- Provides two secure interfaces for performing an intercept: one for setting up the wiretap and one for sending the intercepted traffic to the mediation device (MD).
- Coexists with Packet Intercept (PI). To support Packet Intercept (PI) in a PacketCable environment for voice intercepts, you must enable PacketCable operation on the CMTS and perform any other related PacketCable configurations as required. For more information about PacketCable, see the [“Related Documents” section on page 377](#).

Before you configure SII on the Cisco CMTS, you should understand the following concepts:

- [Lawful Intercept, page 364](#)
- [Packet Intercept, page 364](#)
- [Service Independent Intercept, page 364](#)
- [Network Components Used for Lawful Intercept, page 364](#)

- [Lawful Intercept Processing, page 365](#)
- [SNMPv3 Interface, page 366](#)

Lawful Intercept

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

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

The Lawful Intercept feature supports the Communications Assistance for Law Enforcement Act (CALEA), which describes how service providers in the United States must support lawful intercept. Currently, lawful intercept is defined by the following standards:

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

Packet Intercept

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

For more information about PacketCable Lawful Intercept, PacketCable configuration on the CMTS, and COPS support on the CMTS, see the "[Related Documents](#)" section on [page 377](#).

Service Independent Intercept

SII describes a standard Cisco architecture that provides LI capabilities using an SNMPv3 interface.

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

Network Components Used for Lawful Intercept

The following network components are used for lawful intercepts:

- [Mediation Device, page 365](#)
- [Intercept Access Point, page 365](#)

- [Collection Function, page 365](#)

Mediation Device

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

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



Note

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

Intercept Access Point

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

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



Note

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

Collection Function

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

Lawful Intercept Processing

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

In a PacketCable environment, there is not currently any standard method for setting up a tap for voice traffic. SII provides a standard way for setting up data taps by either an IP or MAC address. SII includes two ways of setting a MAC-based tap:

- On CPE—Only intercepts traffic whose source or destination match the MAC address of the CPE device.
- On CM—Intercepts all of the traffic behind the CM, including the CM traffic itself. This form of intercept might generate a lot of traffic to the mediation device.

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

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



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

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



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

4. When the lawful intercept expires, the router stops intercepting the target's traffic.

SNMPv3 Interface

SII in Cisco IOS Release 12.2(33)SCA supports the following MIBs in SNMPv3:

- CISCO-TAP2-MIB
- CISCO-IP-TAP-MIB
- CISCO-802-TAP-MIB

For a link to the Cisco IOS MIB tools, see the [“MIBs” section on page 377](#).

CISCO-TAP2-MIB

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

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

[Table 2](#) lists the tables and objects in the CISCO-TAP2-MIB. For more information, refer to the MIB documentation.

Table 2 CISCO-TAP2-MIB Tables and Objects

Object	Description
cTap2MediationTable	Lists the Mediation Devices with which the intercepting device communicates.
cTap2StreamTable	Lists the traffic streams to be intercepted. Consists of generic fields that are independent of the type of intercept.
cTap2DebugTable	Contains Lawful Intercept debug messages generated by the implementing device.
cTap2MediationNewIndex	Contains a value which may be used as an index value for a new cTap2Mediation Entry.
cTap2MediationCapabilities	Displays the device capabilities for certain fields in the Mediation Device table. This may be dependent on hardware or software capabilities.
cTap2DebugAge	Contains the duration in minutes for which an entry in cTap2DebugTable is maintained by the implementing device. The entry is deleted once this duration is reached.
cTap2DebugMaxEntries	Contains the maximum number of debug messages maintained at one time by the implementing device. When this limit is reached, the most recent message replaces the oldest message.

Table 3 lists the notifications in the CISCO-TAP2-MIB. For more information, refer to the MIB documentation.

Table 3 CISCO-TAP2-MIB Notifications

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

CISCO-IP-TAP-MIB

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



Note

The Cisco CMTS routers currently only support IPv4 IP intercepts.

Table 4 lists the tables and objects in the MIB. For more information, refer to the MIB documentation.

Table 4 CISCO-IP-TAP-MIB Tables and Objects

Object	Description
citapStreamTable	Lists the IP streams to be intercepted.
citapStreamCapabilities	Displays the type of intercept streams that can be configured on this type of device.

CISCO-802-TAP-MIB

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

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

[Table 5](#) lists the tables and objects in the MIB. For more information, refer to the MIB documentation.

Table 5 *CISCO-802-TAP-MIB Tables and Objects*

Object	Description
c802tapStreamTable	Lists the IEEE 802 data streams to be intercepted.
c802tapStreamCapabilities	Displays the types of intercept streams that can be configured on this device. This may be dependent on hardware or software capabilities.

How to Perform SNMPv3 Provisioning for Service Independent Intercept

This section includes the following procedures:

- [Prerequisites, page 369](#)
- [Restrictions, page 370](#)
- [Accessing the Lawful Intercept MIBs, page 370](#)
- [Restricting Access to the Lawful Intercept MIBs, page 370](#)
- [Verifying the SNMP Configuration, page 372](#)
- [Provisioning the Cable Interface Using SNMPv3, page 373](#)
- [Provisioning IP Intercepts Using SNMPv3, page 373](#)
- [Provisioning MAC Intercepts Using SNMPv3, page 373](#)
- [Enabling SNMP Notifications for Lawful Intercept, page 374](#)
- [Disabling SNMP Notifications, page 376](#)

Prerequisites

To perform SNMPv3 provisioning for SII, the following prerequisites must be met:

- You must be logged in to the router with the highest access level (level-15). To log in with level-15 access, enter the enable command and specify the highest-level password defined for the router.
- The mediation device must have an access function (AF) and an access function provisioning interface (AFPI).

- You must add the mediation device to the SNMP user group that has access to the CISCO-TAP2-MIB view using the **snmp-server user** command. Specify the username of the mediation device as the user to add to the group.
- When you add the mediation device as a CISCO-TAP2-MIB user, you can include the mediation device's authorization password if you want. The password must be at least eight characters in length.

Restrictions

Consider the following restrictions as you perform SNMPv3 provisioning for SII:

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

Accessing the Lawful Intercept MIBs

Due to its sensitive nature, the Cisco lawful intercept MIBs supported by SII are only available in software images that support the SII and Lawful Intercept features. These MIBs are not accessible through the Network Management Software MIBs Support page (<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.)

The Cisco CMTS routers support LI and SII MIBs using the following images:

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

Restricting Access to the Lawful Intercept MIBs

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

- Create a view that includes the Cisco Lawful Intercept MIBs.

- Create an SNMP user group that has read and write access to the view. Only users assigned to this user group can access information in the MIBs.
- Add users to the Cisco Lawful Intercept user groups to define who can access the MIBs and any information related to lawful intercepts. Be sure to add the mediation device as a user in this group; otherwise, the router cannot perform lawful intercepts.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server view** *view-name oid-tree* {**included** | **excluded**}
4. **snmp-server group** *groupname v3* {**auth** | **noauth** | **priv**} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]
5. **snmp-server user** *username groupname* [**remote** *host* [**udp-port** *port*]] **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>snmp-server view view-name oid-tree {included excluded}</p> <p>Example: Router(config)# snmp-server view tapView ciscoIpTapMIB included</p>	<p>Creates or updates a view entry.</p> <p>Repeat this step as needed to include other MIBs in the view.</p>
Step 4	<p>snmp-server group groupname v3 {auth noauth priv} [read readview] [write writeview] [notify notifyview] [access access-list]</p> <p>Example: Router(config)# snmp-server group tapGroup v3 noauth read tapView write tapView notify tapView</p>	<p>Configures a new SNMPv3 group.</p>
Step 5	<p>snmp-server user username groupname [remote host [udp-port port]] v3 [encrypted] [auth {md5 sha} auth-password] [access access-list]</p> <p>Example: Router(config)# snmp-server user tapuser tapGroup v3 auth md5 cisco</p>	<p>Configures a new user to an SNMPv3 group.</p>

Verifying the SNMP Configuration

Use the following commands to verify the configuration of SNMP:

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

Provisioning the Cable Interface Using SNMPv3

When you provision the cable interface using SNMPv3, complete the following requirements:

- The mediation device must be established first.
- To provision the cable interface for which intercepts should be enabled, you need to configure objects in both the CISCO-802-TAP-MIB and the CISCO-IP-TAP-MIB:
 - CISCO-802-TAP-MIB—Configure the c802tapStreamInterface object.
 - CISCO-IP-TAP-MIB—Configure the citapStreamInterface object.
- The c802tapStreamInterface and citapStreamInterface objects specify the ifIndex of the desired interface. Use a -1, 0, or the address of the cable bundle interface.

Provisioning IP Intercepts Using SNMPv3

Restrictions

To provision an IP intercept using SNMPv3, perform the following tasks in SNMPv3:

1. Configure objects in the CISCO-TAP2-MIB:
Configure the cTap2StreamEntry table object with the cTap2StreamType object configured for IP. This entry is used with the citapStreamEntry table object in the CISCO-IP-TAP-MIB.
2. Configure objects in the CISCO-IP-TAP-MIB:
Configure the ciTapStreamEntry table object that provides the details of the intercept in the CISCO-IP-TAP-MIB. This entry is used with the cTap2StreamEntry table object in the CISCO-TAP2-MIB.
3. Set the cTap2StreamInterceptEnable bit.

Provisioning MAC Intercepts Using SNMPv3

SII in Cisco IOS Release 12.2(33)SCA on the CMTS routers allows you to provision bi-directional MAC intercepts (supports the upstream and downstream path) for a cable modem (CM) or customer premise equipment (CPE) using SNMPv3.

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

Prerequisites

- When you are provisioning a CM MAC intercept, the CM must be online before the MAC intercept can be configured using SNMPv3.
- Set the CM bit only if you want to configure a CM-based tap.
- The destination (dstMACAddress) and source MAC address (srcMacAddress) bits must both be set.
- The values of the destination (c802tapStreamDestinationAddress) and source address (c802tapStreamSourceAddress) objects must have identical values.

**Note**

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

Restrictions

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

Provisioning a MAC Intercept for Cable Modems Using SNMPv3

To provision a MAC intercept for CMs using SNMPv3, perform the following tasks in SNMPv3:

1. Configure the `c802tapStreamInterface` object.
2. Set the following bit flags in the `c802tapStreamFields` object:
 - `dstMacAddress` (bit 1)
 - `srcMacAddress` (bit 2)
 - `cmMacAddress` (bit 6)—The `cmMacAddress` bit field is newly introduced for cable modem support and determines whether the intercept is a CPE-based or CM-based intercept
3. Configure the following objects with the same CM MAC address value:
 - `c802tapStreamDestinationAddress`
 - `c802tapStreamSourceAddress`

Provisioning a MAC Intercept for a CPE Device Using SNMPv3

To provision a MAC intercept for a CPE device using SNMPv3, perform the following tasks in SNMPv3:

1. Configure the `c802tapStreamInterface` object.
2. Set the following bit flags in the `c802tapStreamFields` object:
 - `dstMacAddress` (bit 1)
 - `srcMacAddress` (bit 2)
3. Configure the following objects with the same CPE MAC address value:
 - `c802tapStreamDestinationAddress`
 - `c802tapStreamSourceAddress`

Enabling SNMP Notifications for Lawful Intercept

SNMP automatically generates notifications for lawful intercept events (see [Table 3 on page 368](#)). This is because the default value of the `cTap2MediationNotificationEnable` object is `true(1)`.

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

Prerequisites

- ~~SNMP notifications for lawful intercept must be sent to UDP port 161 on the mediation device, not port 162 (which is the SNMP default).~~

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version 3** [**auth** | **noauth** | **priv**]] [*community-string*] [**udp-port** *port*] [*notification-type*]
4. **snmp-server enable traps snmp** [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]
5. **snmp-server enable traps** [*notification-type*] [**vrrp**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>snmp-server host {hostname ip-address} [vrf vrf-name] [traps informs] [version 3 [auth noauth priv]] community-string [udp-port port] [notification-type]</p> <p>Example: Router(config)# snmp-server host 10.10.10.10 version 3 noauth mdpass udp-port 161 snmp</p>	<p>Specifies the recipient of an SNMP notification operation.</p>
Step 4	<p>snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]</p> <p>Example: Router(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart</p>	<p>Enables the sending of RFC 1157 SNMP notifications.</p>
Step 5	<p>snmp-server enable traps [notification-type] [vrrp]</p> <p>Example: Router(config)# snmp-server enable traps tty</p>	<p>Enables all SNMP notification types that are available on your system.</p>

Disabling SNMP Notifications

You can disable SNMP notifications on the router as follows:

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

Additional References

The following sections provide references related to the SII feature.

Related Documents

Related Topic	Document Title
SNMP configuration information	<i>Cisco IOS Configuration Fundamentals Configuration Guide, Part 3: Cisco IOS System Management</i> , “Configuring SNMP Support” section at: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fc014.html
SNMP command information	<i>Cisco IOS Network Management Command Reference, Release 12.2SB</i> at: http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html
Cable interface bundling configuration	<i>Cisco IOS CMTS Cable Software Configuration Guide</i> http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/12_2sc/cbl_12_2sc_book.html
PacketCable Lawful Intercept Architecture in Cisco IOS Release 12.2SB	“PacketCable Lawful Intercept Architecture” topic at: http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_siiv2_ps2209_TSD_Products_Configuration_Guide_Chapter.html
PacketCable configuration on the Cisco CMTS	<i>Cisco IOS CMTS Cable Software Configuration Guide</i> http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/12_2sc/cbl_12_2sc_book.html

Standards

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

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> CISCO-TAP2-MIB CISCO-IP-TAP-MIB CISCO-802-TAP-MIB 	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Feature Information for Service Independent Intercept

Table 6 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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



Note

Table 6 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 6 Feature Information for Service Independent Intercept

Feature Name	Releases	Feature Information
Service Independent Intercept	12.2(33)SCA	SII support is introduced and enhanced using SNMPv3 in Cisco IOS Release 12.2(33)SCA on the Cisco uBR7225VXR, Cisco uBR7246VXR and Cisco uBR10012 (with PRE-2) universal broadband routers. There are no new or modified commands.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.

