Service Independent Intercept on the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: July 11, 2012

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

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

- Intercepts for voice traffic in PacketCable environments

- IPv4 intercepts for SII using SNMPv3

- CLI for MAC intercepts

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

Finding Feature Information

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

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

Contents

Prerequisites for Service Independent Intercept

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

Note SII intercepts are supported only on cable bundle interfaces.

This table shows the hardware compatibility prerequisites for this feature.

Table 1: Service Independent Intercept on the Cisco CMTS Routers Hardware Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2[1] Cisco IOS Release 12.2(33)SCB and later • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later releases • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [2]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [3]

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

[1] PRE = Performance Routing Engine

[2] Cisco uBR-MC3GX60V cable interface line card is compatible only with PRE4.

[3] Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2

Restrictions for Service Independent Intercept

- IPv6 addressing for IP intercepts is supported on the Cisco uBR10012 router from Cisco IOS Release 12.2(33)SCG onwards.

- Mediation device (MD) must be reachable through the global IP routing table. Support for an MD inside an Multiprotocol Label Switching (MPLS)/VPN is not supported.

- SII information cannot be displayed using CLI. Intercept content from SII will not appear in the **show pxf cable** commands. Other intercept information outside of SII content (for PacketCable and through the CLI intercept) is shown.

- Cisco uBR10012 router has the following MIB object restrictions:

  ◦ When a PRE switchover occurs, the SII configuration is lost. An SNMP trap is generated for this event. The SII must be configured after a PRE switchover.

  ◦ cTap2MediationDestAddressType—IPv6 is not supported.

  ◦ cTapMediationRtcpPort—Not supported.

  ◦ cTapMediationRetransmitType—Not supported.

  ◦ cTapMediationTransport—UDP only.

  ◦ cTapStreamIpInterface—Only if interface supported is cable.

  ◦ cTapStreamIpAddrType—Supported on IPv6 from Cisco IOS Release 12.2(33)SCG onwards.

  ◦ cTapStreamIpDestinationLength—Must be 32 (no subnets are supported) or 0. The address length and port range restrictions are only for IPv4. There is no restriction for IPv6.

  ◦ cTapStreamIpFlowId—Supported on IPv6 from Cisco IOS Release 12.2(33)SCG onwards.

  ◦ cTapStreamIpDestL4PortMin—Must match DestL4PortMax or have a value of 0.

- cTapStreamIpDestL4PortMax—Must match DestL4PortMin or have a value of 65535.

- cTapStreamIpSourceL4PortMin—Must match SourceL4PortMin or have a value of 0.

- cTapStreamIpSourceL4PortMax—Must match SourceL4PortMax or have a value of 65535.

- Maximum number of IP intercepts allowed is 800.

- Maximum number of MAC intercepts allowed is 400.

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

Information About Service Independent Intercept

SII has the following benefits:

- Does not affect subscriber services on the router.

- Can neither be detected by the target, nor tapped.

- Allows Law Enforcement Agencies (LEAs) to perform lawful intercepts without the knowledge of service providers.

- Uses Simple Network Management Protocol version 3 (SNMPv3) and security features like the View-based Access Control Model (SNMP-VACM-MIB) and User-based Security Model (SNMP-USM-MIB) to restrict access to lawful intercept information and components.

- Supports intercepts of Layer 2, Layer 3, and Layer 4 traffic.

- Supports Layer 2 intercepts for upstream and downstream traffic.

- Hides information about lawful intercepts from all but the most privileged users.

- Provides two secure interfaces for performing an intercept—one for setting up the wiretap and one for sending the intercepted traffic to the MD.

- Coexists with Packet Intercept (PI). To support PI in a PacketCable environment for voice intercepts, you must enable PacketCable operation must be enabled on the Cisco CMTS and other related PacketCable configurations must be implemented as required. For more information about PacketCable and lawful intercept, see the PacketCable and PacketCable Multimedia for the Cisco CMTS Routers and Lawful Intercept Architecture feature guides.

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

Lawful Intercept

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

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

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

- Telephone Industry Association (TIA) specification J-STD-025

- Packet Cable Electronic Surveillance Specification (PKT-SP-ESP-101-991229)

Packet Intercept

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

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

Service Independent Intercept

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

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

Service Independent Intercept Tap in Routed Subnets

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

```
ip address <ip-address> <subnet-mask> or ip address <ip-address> <subnet-mask> secondary
```
For example: ip address 80.32.0.1 255.255.255.0

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

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

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

For more information, see the Provisioning Taps on IP addresses Learned from the CPE Router, on page 21.

IPv6 Address Packet Intercept

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

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

- IPv6 Taps—Matches all IPv6 packets.

- 6PE Taps—Supports IPv6 Provider Edge (6PE) deaggregation. However, disposition packets are not supported.

- 6VPE Taps—Matches all IPv6 packets in the virtual routing and forwarding (VRF) context. Disposition packets are not supported.

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

- Supports up to 1000 IPv6 taps.

- Supports IPv4 and MAC taps.

- Supports up to 4000 mediation devices.

- Intercepts and forwards up to 100,000 packets per second.

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

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

MPLS and VPN Support

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

Compatibility with Other Taps

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

Network Components Used for Lawful Intercept

Mediation Device

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

- Provides the interface used to set up and provision the lawful intercept.

- Generates requests to other network devices to set up and run the lawful intercept.

- Converts the intercepted traffic into the format required by the LEA (which can vary from country to country) and sends a copy of the traffic to the LEA without the knowledge of the target.

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

Intercept Access Point

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

- Identification (ID) IAP—A device, such as an authentication, authorization, and accounting (AAA) server, that provides intercept related information (IRI) for the intercept (for example, the username of the target and system IP address). The IRI helps the service provider determine which content IAP (router) the traffic of the target passes through.

- Content IAP—A device, such as a Cisco CMTS router, through which the traffic of the target passes through. The content IAP:

   ◦ Intercepts traffic to and from the target for the length of time specified in the court order. The router continues to forward traffic to its destination to ensure that the wiretap is undetected.

   ◦ Creates a copy of the intercepted traffic, encapsulates it in UDP packets, and forwards the packets to the mediation device without the knowledge of the target.

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

Collection Function

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

Lawful Intercept Processing

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

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

- On CPE—Only intercepts traffic whose source or destination match the MAC address of the CPE device.

- On CM—Intercepts all of the traffic behind the CM, including the CM traffic itself. This form of intercept might generate a lot of traffic to the mediation device.

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

- The admin function at the service provider contacts the ID IAP for the IRI, such as the username of the target and the IP address of their system, to determine which content IAP (router) the traffic of the target passes through.

- After identifying the router that handles the traffic of the target, the admin function issues SNMPv3 **get** and **set** requests to the router MIBs to set up and activates the lawful intercept. The router MIBs include the CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, and CISCO-802-TAP-MIB.

- During the lawful intercept, the router:

  - Examines incoming and outgoing traffic and intercepts any traffic that matches the specifications of the lawful intercept request.

  - Creates a copy of the intercepted traffic and forwards the original traffic to its destination so the target does not suspect anything.

  - Encapsulates the intercepted traffic in UDP packets and forwards the packets to the mediation device without the knowledge of the target.

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

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

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

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

SNMPv3 Interface

SII supports the following MIBs in SNMPv3:

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

CISCO-TAP2-MIB

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

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

Table 2: CISCO-TAP2-MIB Tables and Objects

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

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

Table 3: CISCO-TAP2-MIB Notifications , on page 10 lists the notifications in the CISCO-TAP2-MIB. For more information, see 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 object that identifies the actual intercept stream type is included in this notification.
ciscoTap2MediationTimedOut	Sent when an intercept is autonomously removed by an intercepting device, such as due to the time specified in the cTap2MediationTimeout object.
ciscoTap2MediationDebug	Sent when there is intervention needed due to events related to entries configured in the cTap2MediationTable object.
ciscoTap2StreamDebug	Sent when there is intervention needed due to events related to entries in the cTap2StreamTable object.
ciscoTap2Switchover	Sent when there is a redundant (standby) route processor available on the intercepting device and the current active processor is going down causing the standby to takeover.

CISCO-IP-TAP-MIB

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

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

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

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

CISCO-802-TAP-MIB

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

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

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

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

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

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

How to Perform SNMPv3 Provisioning for Service Independent Intercept

This section includes the following procedures:

Prerequisites for SNMPv3 Provisioning

- Ensure you are logged in to the router with the highest access level (level-15). To log in with level-15 access, enter the **enable** command and specify the highest-level password defined for the router.

- Ensure that the mediation device has an access function (AF) and an access function provisioning interface (AFPI).

- Ensure that you have added the mediation device to the SNMP user group that has access to the CISCO-TAP2-MIB view, using the **snmp-server user** command. Specify the username of the mediation device as the user to add to the group.

- Ensure that when you add the mediation device as a CISCO-TAP2-MIB user, the authorization password of the mediation device must be at least eight characters in length.

Restrictions to SNMPv3 Provisioning

- The only users who should be allowed to access the Lawful Intercept MIBs are the mediation device and system administrators who need to know about lawful intercepts on the router. In addition, these users must have authPriv or authNoPriv access rights to access the SII MIBs. Users with NoAuthNoPriv access cannot access the Lawful Intercept MIBs.

- You cannot use the SNMP-VACM-MIB to create a view that includes the Lawful Intercept MIBs.

- The default SNMP view excludes the following MIBs:

  - CISCO-TAP2-MIB

  - CISCO-IP-TAP-MIB

  - SNMP-COMMUNITY-MIB

  - SNMP-USM-MIB

  - SNMP-VACM-MIB

- The Cisco CMTS router does not display log messages about SII taps; therefore, you can only see configuration errors by using SNMP traps.

- The Cisco CMTS router does not display any details about SII taps in **show pxf cable** commands. A line in the output of the **show pxf cable** command displays the number of SII taps, but not their content.

- The Cisco CMTS router supports IPv6 addressing for IP taps only from Cisco IOS Release 12.2(33)SCG onwards.

Accessing the Lawful Intercept MIBs

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

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

- Cisco uBR7246VXR router—ubr7200-k9pu2-mz

- Cisco uBR10012 router—ubr10k2-k9p6u2-mz

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

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

　　　　　　　　　　• Cisco uBR10012 router with PRE4—ubr10k4-k9p6u2-mz

　　　　　　　　　　• Cisco uBR7246VXR router with NPE-G1—ubr7200-ik9su2-mz

　　　　　　　　　　• Cisco uBR7246VXR router with NPE-G2—ubr7200p-jk9su2-mz

Restricting Access to the Lawful Intercept MIBs

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

- Create a view that includes the Cisco LI MIBs.

- Create an SNMP user group that has read and write access to the view. Only users assigned to this user group can access information in the MIBs.

- Add users to the Cisco LI user groups to define who can access the MIBs and any information related to lawful intercepts. Be sure to add the mediation device as a user in this group; otherwise, the router cannot perform lawful intercepts.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal**	Enters global configuration mode.
Step 3	**snmp-server view***view-name**oid-tree***included** **Example:** Router(config)# **snmp-server view tapView ciscoIpTapMIB included**	Creates or updates a view entry. - **view** *view-name*—Label for the view record that you are updating or creating. The name is used to reference the record. - *oid-tree*—Object identifier of the ASN.1 subtree. - **included**—Type of view. Repeat this step as needed to include other MIBs in the view.
Step 4	**snmp-server group***groupname***v3noauthread***readview***write***writeview***notify***notifyview*	Configures a new SNMPv3 group. - *groupname*—SNMP server group name.

Command or Action	Purpose
Example: Router(config)# **snmp-server group tapGroup v3 noauth read tapView write tapView notify tapView**	• **v3**—The most secure of the possible security models. • **noauth**—Specifies no authentication of a packet. • **read**—The option that allows you to specify a read view. • *readview*—A string (not to exceed 64 characters) that is the name of the view that enables you only to view the contents of the agent. • **write**—The option that allows you to specify a write view. • *writeview*—A string (not to exceed 64 characters) that is the name of the view that enables you to enter data and configure the contents of the agent. • **notify**—The option that allows you to specify a notify view. • *notifyview*—A string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.
Step 5 **snmp-server user** *usernamegroupname***v3authmd5***auth-password* **Example:** Router(config)# **snmp-server user tapuser tapGroup v3 auth md5 cisco**	Configures a new user to an SNMPv3 group • *username*—The name of the user on the host that connects to the agent. • *groupname*—The name of the group to which the user is associated. • **v3**—The most secure of the possible security models. • **auth**—Initiates an authentication level setting session • **md5**—The HMAC-MD5-96 authentication level. • *auth-password*—A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
Step 6 **exit** **Example:** Router(config)# **exit**	Exits global configuration mode.

Verifying the SNMP Configuration

Use the following commands to verify the configuration of SNMP:

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

Provisioning the Cable Interface Using SNMPv3

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

  • CISCO-802-TAP-MIB—Configure the c802tapStreamInterface object.

  • CISCO-IP-TAP-MIB—Configure the citapStreamInterface object.

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

Provisioning IP Intercepts Using SNMPv3

1 Configure objects in the CISCO-TAP2-MIB:

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

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

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

1 Set the cTap2StreamInterceptEnable object bit.

Note   IP intercepts also have interface OIDs. For more information, see the Provisioning the Cable Interface Using SNMPv3, on page 18.

Provisioning IPv6 Taps Using SNMPv3

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

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

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

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

Restrictions for IPv6 Address Packet Intercept

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

- The IPv6 address tap through SNMP MIB is supported only on the Cisco uBR10012 series routers.

- The IPv6 address tap provision is not supported on the Cisco uBR7200 series routers. Any SNMP request on these routers will fail.

- The IPv6 packet intercept can be performed at the Cisco uBR7200 series routers only by setting up the MAC tap.

- The Cisco CMTS router does not support IPv6 multicast address tap on cable interfaces.

- The Cisco CMTS router supports only IPv4 MD encapsulation.

- The MPLS/VPN supports imposition and deaggregation.

- The IPv4 or IPv6 packets within an L2VPN or AToM will not be tapped.

- The IPv6 taps are supported only on cable interfaces.

- The IPv6 packet will be tapped only once.

- The IPv6 packets that come in as fragments without L4 fields are intercepted.

To provision the cable interface using SNMPv3, see Provisioning the Cable Interface Using SNMPv3, on page 18.

The IPv6 packet can also be tapped per CPE and per CM MAC address. For more details, see the Provisioning MAC Intercepts Using SNMPv3, on page 19.

Provisioning MAC Intercepts Using SNMPv3

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

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

Prerequisites for Provisioning MAC Intercepts using SNMPv3

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

- Set the CM bit only if you want to configure a CM-based tap.

- The destination (dstMACAddress) and source MAC address (srcMacAddress) bits must both be set.

- The values of the destination (c802tapStreamDestinationAddress) and source address (c802tapStreamSourceAddress) objects must have identical values.

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

Restrictions to Provisioning MAC Intercepts using SNMPv3

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

You can provision the following MAC intercepts using SNMPv3:

Provisioning a MAC Intercept for Cable Modems Using SNMPv3

1 Configure the c802tapStreamInterface object.
2 Set the following bit flags in the c802tapStreamFields object:

- dstMacAddress (bit 1)

- srcMacAddress (bit 2)

- cmMacAddress (bit 6)—The cmMacAddress bit field is newly introduced for cable modem support and determines whether the intercept is a CPE-based or CM-based intercept.

3 Configure the following objects with the same CM MAC address value:

- c802tapStreamDestinationAddress

- c802tapStreamSourceAddress

Provisioning a MAC Intercept for a CPE Device Using SNMPv3

1 Configure the c802tapStreamInterface object.
2 Set the following bit flags in the c802tapStreamFields object:

- dstMacAddress (bit 1)

- srcMacAddress (bit 2)

3 Configure the following objects with the same CPE MAC address value:

- c802tapStreamDestinationAddress

- c802tapStreamSourceAddress

Provisioning Taps on IP addresses Learned from the CPE Router

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

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

- Routing Information Protocol (RIP)

- RIP2

- Static route

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

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

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

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

Table 6: IP Address Tap , on page 21 and Table 7: MAC Address Tap , on page 22 display the conditions when a tap is successful.

Table 6: IP Address Tap

Source IP[4]	Destination IP	Specified Interface (bundle interface)	IP Subnet – Statically Configured or Learned on any Cable Interface	IP Subnet – Statically Configured or Learned on a Specified Cable Interface	Tap Enable?	Tap Success?
Yes	Yes	No	Yes	—[5]	Yes	Yes
Yes	Wildcard[6]	No	Yes	—	Yes	Yes
Wildcard	Yes	No	Yes	—	Yes	Yes
Wildcard	Wildcard	No	—	—	—	No
Yes	Yes	Yes	X	Yes	Yes	Yes

Source IP[4]	Destination IP	Specified Interface (bundle interface)	IP Subnet – Statically Configured or Learned on any Cable Interface	IP Subnet – Statically Configured or Learned on a Specified Cable Interface	Tap Enable?	Tap Success?
Yes	Wildcard	Yes	X	Yes	Yes	Yes
Wildcard	Yes	Yes	X	Yes	Yes	Yes
Wildcard	Wildcard	Yes	—	—	—	No
X[7]	X	X	No	No	—	No

4 Source IP, Destination IP, and Specified Interface columns are the OIDs from the SNMP.

5 "—" indicates that the item is not available or not applicable.

6 Wildcard is a subnet mask of 0.0.0.0

7 "X" can indicate either Yes or No.

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

Table 7: MAC Address Tap

Source MAC Address	Destination MAC Address	Specified Interface (Cable Interface)	MAC Address Presented at the Cisco CMTS Cable Interface	MAC Address Presented at the Specified Cable Interface	Tap Enable	Tap Success?
Yes	Yes	No	Yes	—[8]	Yes	Yes
Yes	Wildcard[9]	No	Yes	—	—	No*[10]
Wildcard	Yes	No	Yes	—	—	No*
Wildcard	Wildcard	No	—	—	—	No*
Yes	Yes	Yes	X	Yes	Yes	Yes
Yes	Wildcard	Yes	X	Yes	—	No*
Wildcard	Yes	Yes	X	Yes	—	No*
Wildcard	Wildcard	Yes	—	—	—	No
Yes	Yes	X	No	No	No**[11]	Yes**

Source MAC Address	Destination MAC Address	Specified Interface (Cable Interface)	MAC Address Presented at the Cisco CMTS Cable Interface	MAC Address Presented at the Specified Cable Interface	Tap Enable	Tap Success?
Yes	Wildcard	X	X	X	—	No*
Wildcard	Yes	X	X	X	—	No*
X[12]	X	X	No	No	—	No

8   "—" indicates that the item is not available or not applicable.

9   Wildcard is a subnet mask of 0.0.0.0.

10   Both the source and destination MAC addresses must be present.

11   This is a preconfiguration case indicating that the CPE or the CM is not online.

12   "X" can indicate either Yes or No.

Enabling SNMP Notifications for Lawful Intercept

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

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

DETAILED STEPS

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

Step 3	**snmp-server host** *hostname***version3noauth***community-string***udp-port***portnotification-type*
	
	Example:
	
	Router(config)# **snmp-server host 10.10.10.10 version 3 noauth mdpass udp-port 161 snmp**
		Specifies the recipient of an SNMP notification operation.
		
		  • *hostname*—Name or Internet address of the host (the targeted recipient).
		
		  • **version3**—Version of the SNMP used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the priv keyword. If you use the version

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

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

Disabling SNMP Notifications

- To disable all SNMP notifications, use the **no snmp-server enable traps** command.

- To disable lawful intercept notifications, use SNMPv3 to set the CISCO-TAP2-MIB object cTap2MediationNotificationEnable to false(2). To re-enable lawful intercept notifications through SNMPv3, reset the object to true(1).

Configuration Examples for SNMPv3 Provisioning for Service Independent Intercept

```
Router# show running-config | include snmp
snmp-server engineID local 80000009030002000000000
snmp-server group tapGroup v3 noauth read tapView write tapView
snmp-server view tapView ciscoIpTapMIB included
snmp-server view tapView cisco802TapMIB included
snmp-server view tapView ciscoTap2MIB included
snmp-server enable traps tty
snmp-server enable traps alarms informational
snmp-server manager


Router# show snmp user
User name: tapuser
Engine ID: 80000009030002000000000
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: tapGroup
```

Additional References

The following sections provide references related to the SII feature.

Related Documents

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

MIBs

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

Technical Assistance

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

Feature Information for Service Independent Intercept

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

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

Table 8: Feature Information for Service Independent Intercept

Feature Name	Releases	Feature Information
Service Independent Intercept	12.2(33)SCA	SII support is introduced and enhanced using SNMPv3 in Cisco IOS Release 12.2(33)SCA on the Cisco uBR7225VXR, Cisco uBR7246VXR, and Cisco uBR10012 (with PRE2) universal broadband routers.
SII Routed CPE Support	12.2(33)SCF	SII Routed CPE Support feature was introduced.
IPv6 Address Packet Intercept	12.2(33)SCG	The IPv6 Address Packet Intercept feature supports lawful intercept of CMs and CPEs provisioned with IPv6 addresses. The following sections provide information about this feature: • IPv6 Address Packet Intercept, on page 6 • Provisioning IPv6 Taps Using SNMPv3, on page 18