# Lawful Intercept Architecture

The Lawful Intercept (LI) feature supports service providers in meeting the requirements of law enforcement agencies to provide the ability to intercept Voice-over-Internet protocol (VoIP) or data traffic going through the edge routers. This document explains LI architecture, including Cisco Service Independent Intercept architecture and PacketCable Lawful Intercept architecture. It also describes the components of the LI feature and provides instructions on how to configure the LI feature in your system.

### 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

# Hardware Compatibility Matrix for Cisco cBR Series Routers

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

***Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers***

| Cisco CMTS Platform | Processor Engine | Interface Cards |
|---|---|---|
| Cisco cBR-8 Converged Broadband Router | **Cisco IOS-XE Release 3.15.0S and Later Releases**<br>Cisco cBR-8 Supervisor:<br>• PID—CBR-CCAP-SUP-160G<br>• PID—CBR-CCAP-SUP-60G[1]<br>• PID—CBR-SUP-8X10G-PIC | **Cisco IOS-XE Release 3.15.0S and Later Releases**<br>Cisco cBR-8 CCAP Line Cards:<br>• PID—CBR-LC-8D30-16U30<br>• PID—CBR-LC-8D31-16U30<br>• PID—CBR-RF-PIC<br>• PID—CBR-RF-PROT-PIC<br>Cisco cBR-8 Downstream PHY Modules:<br>• PID—CBR-D30-DS-MOD<br>• PID—CBR-D31-DS-MOD<br>Cisco cBR-8 Upstream PHY Modules:<br>• PID—CBR-D30-US-MOD |

1 Effective with Cisco IOS-XE Release 3.17.0S, CBR-CCAP-SUP-60G supports 8 cable line cards. The total traffic rate is limited to 60Gbps, the total number of downstream service flow is limited to 72268, and downstream unicast low-latency flow does not count against the limits.

# Prerequisites for Lawful Intercept

Access to the Cisco LI MIB view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

### Communication with Mediation Device

For the router to communicate with the mediation device to execute a lawful intercept, the following configuration requirements must be met:

- The domain name for both the router and the mediation device must be registered in the Domain Name System (DNS).

In DNS, the router IP address is typically the address of the TenGigabitEthernet5/1/0 or TenGigabitEthernet4/1/0 interface (depending on the slot in which the Supervisor is installed) on 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 Simple Network Management Protocol (SNMP) user group that has access to the CISCO-TAP2-MIB view. 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 for Lawful Intercept

### General Restrictions

There is no command-line interface (CLI) available to configure LI on the router. All error messages are sent to the mediation device as SNMP notifications. All intercepts are provisioned using SNMPv3 only.

### Lawful Intercept MIBs

Only the mediation device and users who need to know about lawful intercepts are allowed to access the LI MIBs.

Due to its sensitive nature, the Cisco LI MIBs are only available in software images that support the LI feature. These MIBs are not accessible through the Network Management Software MIBs Support page ( http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml ).

### SNMP Notifications

SNMP notifications for LI must be sent to User Datagram Protocol (UDP) port 161 on the mediation device, not port 162 (which is the SNMP default). For more information, see the Enabling SNMP Notifications for Lawful Intercept, on page 9.

# Information About Lawful Intercept

## Introduction to Lawful Intercept

LI is the process by which law enforcement agencies (LEAs) conduct electronic surveillance as authorized by judicial or administrative order. Increasingly, legislation is being adopted and regulations are being enforced that require service providers (SPs) and Internet service providers (ISPs) to implement their networks to explicitly support authorized electronic surveillance. The types of SPs or ISPs that are subject to LI mandates vary greatly from country to country. LI compliance in the United States is specified by the Commission on Accreditation for Law Enforcement Agencies (CALEA).

Cisco supports two architectures for LI: PacketCable and Service Independent Intercept. The LI components by themselves do not ensure customer compliance with applicable regulations but rather provide tools that can be used by SPs and ISPs to construct an LI-compliant network.

# Cisco Service Independent Intercept Architecture

The Cisco Service Independent Intercept Architecture Version 3.0 document describes implementation of LI for VoIP networks using the Cisco BTS 10200 Softswitch call agent, version 5.0, in a non-PacketCable network. Packet Cable Event Message specification version 1.5-I01 is used to deliver the call identifying information along with version 2.0 of the Cisco Tap MIB for call content.

The Cisco Service Independent Intercept Architecture Version 2.0 document describes implementation of LI for VoIP networks using the Cisco BTS 10200 Softswitch call agent, versions 4.4 and 4.5, in a non-PacketCable network. Although not a PacketCable network, PacketCable Event Messages Specification version I08 is still used to deliver call identifying information, along with version 1.0 or version 2.0 of the Cisco Tap MIB for call content. The *Cisco Service Independent Intercept Architecture Version 2.0* document adds additional functionality for doing data intercepts by both IP address and session ID, which are both supported in version 2.0 of the Cisco Tap MIB (CISCO-TAP2-MIB).

The Cisco Service Independent Intercept Architecture Version 1.0 document describes implementation of LI for VoIP networks that are using the Cisco BTS 10200 Softswitch call agent, versions 3.5 and 4.1, in a non-PacketCable network. Although not a PacketCable network, PacketCable Event Message Specification version I03 is still used to deliver call identifying information, along with version 1.0 of the Cisco Tap MIB (CISCO-TAP-MIB) for call content. Simple data intercepts by IP address are also discussed.

# PacketCable Lawful Intercept Architecture

The *PacketCable Lawful Intercept Architecture for BTS Version 5.0* document describes the implementation of LI for VoIP using Cisco BTS 10200 Softswitch call agent, version 5.0, in a PacketCable network that conforms to PacketCable Event Messages Specification version 1.5-I01.

The *PacketCable Lawful Intercept Architecture for BTS Versions 4.4 and 4.5* document describes the implementation of LI for VoIP using Cisco BTS 10200 Softswitch call agent, versions 4.4 and 4.5, in a PacketCable network that conforms to PacketCable Event Messages Specification version I08.

The PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1 document describes the implementation of LI for voice over IP (VoIP) using Cisco Broadband Telephony Softswitch (BTS) 10200 Softswitch call agent, versions 3.5 and 4.1, in a PacketCable network that conforms to PacketCable Event Message Specification version I03.

The *PacketCable Control Point Discovery Interface Specification* document defines an IP-based protocol that can be used to discover a control point for a given IP address. The control point is the place where Quality of Service (QoS) operations, LI content tapping operations, or other operations may be performed.

**Note** The Cisco cBR router does not support PacketCable Communications Assistance for Law Enforcement Act (CALEA).

# Cisco cBR Series Routers

TheCisco cBR series router support two types of LI: regular and broadband (per-subscriber). Regular wiretaps are executed on access subinterfaces and physical interfaces. Wiretaps are not required, and are not executed, on internal interfaces. The router determines which type of wiretap to execute based on the interface that the target's traffic is using.

LI on the Cisco cBR series routers can intercept traffic based on a combination of one or more of the following fields:

- Destination IP address and mask (IPv4 or IPv6 address)
- Destination port or destination port range
- Source IP address and mask (IPv4 or IPv6 address)
- Source port or source port range
- Protocol ID
- Type of Service (TOS)
- Virtual routing and forwarding (VRF) name, which is translated to a *vrf-tableid* value within the router.
- Subscriber (user) connection ID
- Cable modem
- MAC address

The LI implementation on the Cisco cBR series routers is provisioned using SNMP3 and supports the following functionality:

- Interception of communication content. The router duplicates each intercepted packet and then places the copy of the packet within a UDP-header encapsulated packet (with a configured CCCid). The router sends the encapsulated packet to the LI mediation device. Even if multiple lawful intercepts are configured on the same data flow, only one copy of the packet is sent to the mediation device. If necessary, the mediation device can duplicate the packet for each LEA.
- Interception of IPv4, IPv4 multicast, IPv6, and IPv6 multicast flows.

LI 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.

# VRF Aware LI

VRF Aware LI is the ability to provision a LI wiretap on IPv4 data in a particular Virtual Private Network (VPN). This feature allows a LEA to lawfully intercept targeted data within that VPN. Only IPv4 data within that VPN is subject to the VRF-based LI tap.

VRF Aware LI is available for the following types of traffic:

- ip2ip
- ip2tag (IP to MPLS)
- tag2ip (MPLS to IP)

To provision a VPN-based IPv4 tap, the LI administrative function (running on the mediation device) uses the CISCO-IP-TAP-MIB to identify the name of the VRF table that the targeted VPN uses. The VRF name is used to select the VPN interfaces on which to enable LI in order to execute the tap.

The router determines which traffic to intercept and which mediation device to send the intercepted packets based on the VRF name (along with the source and destination address, source and destination port, and protocol).

**Note** When using the Cisco-IP-TAP-MIB, if the VRF name is not specified in the stream entry, the global IP routing table is used by default.

# Lawful Intercept MIBs

Due to its sensitive nature, the Cisco LI MIBs are only available in software images that support the LI feature. These MIBs are not accessible through the Network Management Software MIBs Support page ( http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml ).

## 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 LI MIBs. To restrict access to these MIBs, you must:

1. Create a view that includes the Cisco LI MIBs.
2. 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.
3. 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.

For more information, see the Creating a Restricted SNMP View of Lawful Intercept MIBs module.

**Note** Access to the Cisco LI MIB view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

# Service Independent Intercept

Cisco developed the Service Independent Intercept (SII) architecture in response to requirements that support lawful intercept for service provider customers. The SII architecture offers well-defined, open interfaces

between the Cisco equipment acting as the content Intercept Access Point (IAP) and the mediation device. The modular nature of the SII architecture allows the service provider to choose the most appropriate mediation device to meet specific network requirements and regional, standards-based requirements for the interface to the law enforcement collection function.

The mediation device uses SNMPv3 to instruct the call connect (CC) IAP to replicate the CC and send the content to the mediation device. The CC IAP can be either an edge router or a trunking gateway for voice, and either an edge router or an access server for data.

**Note** The Cisco cBR router does not support encryption of lawful intercept traffic.

To increase the security and to mitigate any SNMPv3 vulnerability, the following task is required:

### Restricting Access to Trusted Hosts (without Encryption)

SNMPv3 provides support for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine the security mechanism employed when handling an SNMP packet.

Additionally, the SNMP Support for the Named Access Lists feature adds support for standard named access control lists (ACLs) to several SNMP commands.

To configure a new SNMP group or a table that maps SNMP users to SNMP views, use the **snmp-server group** command in global configuration mode.

```
access-list my-list permit ip host 10.10.10.1
snmp-server group my-group v3 auth access my-list
```

In this example, the access list named **my-list** allows SNMP traffic only from 10.10.10.1. This access list is then applied to the SNMP group called **my-group**.

# How to Configure Lawful Intercept

Although there are no direct user commands to provision lawful intercept on the router, you do need to perform some configuration tasks, such as providing access to LI MIBs, and setting up SNMP notifications. This section describes how to perform the required tasks:

## Creating a Restricted SNMP View of Lawful Intercept MIBs

To create and assign users to an SNMP view that includes the Cisco lawful intercept MIBs, perform the steps in this section.

#### Before You Begin

- You must issue the commands in global configuration mode with level-15 access rights.
- SNMPv3 must be configured on the device.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Device> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server view** *view-name MIB-name* **included**<br><br>**Example:**<br><br>`Device(config)# snmp-server view exampleView ciscoTap2MIB included` | Creates an SNMP view that includes the CISCO-TAP2-MIB (where *exampleView*is the name of the view to create for the MIB).<br><br>• This MIB is required for both regular and broadband lawful intercept. |
| **Step 4** | **snmp-server view** *view-name MIB-name* **included**<br><br>**Example:**<br><br>`Device(config)# snmp-server view exampleView ciscoIpTapMIB included` | Adds the CISCO-IP-TAP-MIB to the SNMP view. |
| **Step 5** | **snmp-server view** *view-name MIB-name* **included**<br><br>**Example:**<br><br>`Device(config)# snmp-server view exampleView cisco802TapMIB included` | Adds the CISCO-802-TAP-MIB to the SNMP view. |
| **Step 6** | **snmp-server group** *group-name* **v3 noauth read** *view-name* **write** *view-name*<br><br>**Example:**<br><br>`Device(config)# snmp-server group exampleGroup v3 noauth read exampleView write exampleView` | Creates an SNMP user group that has access to the LI MIB view and defines the group's access rights to the view. |
| **Step 7** | **snmp-server user** *user-name group-name* **v3 auth md5** *auth-password*<br><br>**Example:**<br><br>`Device(config)# snmp-server user` | Adds users to the specified user group. |

| | Command or Action | Purpose |
|---|---|---|
| | `exampleUser exampleGroup v3 auth md5 examplePassword` | |
| **Step 8** | **end**<br><br>**Example:**<br><br>`Device(config)# end` | Exits the current configuration mode and returns to privileged EXEC mode. |

### Where to Go Next

The mediation device can now access the lawful intercept MIBs and issue SNMP **set** and **get** requests to configure and run lawful intercepts on the router. To configure the router to send SNMP notification to the mediation device, see the Enabling SNMP Notifications for Lawful Intercept.

## Enabling SNMP Notifications for Lawful Intercept

SNMP automatically generates notifications for lawful intercept events. To configure the router to send lawful intercept notifications to the mediation device, perform the steps in this section.

### Before You Begin

- You must issue the commands in global configuration mode with level-15 access rights.
- SNMPv3 must be configured on the router.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Device> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server host** *ip-address* **community-string udp-port** *port notification-type* | Specifies the IP address of the mediation device and the password-like community-string that is sent with a notification request. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config)# snmp-server 10.2.2.1 community-string udp-port 161 udp` | • For lawful intercept, the **udp-port** must be 161 and not 162 (the SNMP default). |
| **Step 4** | **snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart**<br>**Example:**<br>`Device(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart` | Configures the router to send RFC 1157 notifications to the mediation device.<br>• These notifications indicate authentication failures, link status (up or down), and router restarts. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Exits the current configuration mode and returns to privileged EXEC mode. |

# Disabling SNMP Notifications

To disable SNMP notifications on the router, perform the steps in this section.

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

### Procedure

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **no snmp-server enable traps**<br><br>**Example:**<br><br>`Device(config)# no snmp-server enable traps` | Disables all SNMP notification types that are available on your system. |
| **Step 4** | **end**<br><br>**Example:**<br><br>`Device(config)# end` | Exits the current configuration mode and returns to privileged EXEC mode. |

# 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

# Configuration Examples for Lawful Intercept

## Example: Enabling Mediation Device Access Lawful Intercept MIBs

The following example shows how to enable the mediation device to access the lawful intercept MIBs. It creates an SNMP view (tapV) that includes four LI MIBs (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, CISCO-802-TAP-MIB, and CISCO-USER-CONNECTION-TAP-MIB). It also creates a user group that has read, write, and notify access to MIBs in the tapV view.

```
snmp-server view tapV ciscoTap2MIB included
snmp-server view tapV ciscoIpTapMIB included
snmp-server view tapV cisco802TapMIB included
snmp-server view tapV ciscoUserConnectionTapMIB included
snmp-server group tapGrp v3 noauth read tapV write tapV notify tapV
snmp-server user MDuser tapGrp v3 auth md5 MDpasswd
snmp-server engineID local 1234
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Configuring SNMP Support | *Configuring SNMP Support* |
| Security commands | *Cisco IOS Security Command Reference* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| PacketCable™ Control Point Discovery Interface Specification | *PacketCable ™ Control Point Discovery Interface Specification* (PKT-SP-CPD-I02-061013) |
| RFC-3924 | *Cisco Architecture for Lawful Intercept in IP Networks* |

### MIBs

| MIB | MIBs Link |
|---|---|
| • CISCO-TAP2-MIB<br>• CISCO-IP-TAP-MIB<br>• CISCO-802-TAP-MIB<br>• CISCO-USER-CONNECTION-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:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>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.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature Information for Lawful 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 2: Feature Information for Lawful Intercept*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Service Independent Intercept | Cisco IOS-XE Release 3.15.0S | This feature was introduced on the Cisco cBR Series Converged Broadband Routers. |