Implementing Lawful Intercept

Lawful intercept is the process by which law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications, authorized by judicial or administrative order. Service providers worldwide are legally required to assist law enforcement agencies in conducting electronic surveillance in both circuit-switched and packet-mode networks.

Only authorized service provider personnel are permitted to process and configure lawfully authorized intercept orders. Network administrators and technicians are prohibited from obtaining knowledge of lawfully authorized intercept orders, or intercepts in progress. Error messages or program messages for intercepts installed in the router are not displayed on the console.

Feature History for Implementing Lawful Intercept

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.8.0</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Release 4.0.1</td>
<td>Support for Lawful Intercept IPv6 on CRS-MSC-40G and CRS-FP-40 line cards was added. Information on intercepting IPv6 packets, lawful intercept filters, intercepting 6VPE and 6PE packets, IPv6 MD encapsulation, and per tap drop counter support was added.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>High Availability support for Lawful Intercept was added.</td>
</tr>
</tbody>
</table>

- Prerequisites for Implementing Lawful Intercept, page 2
- Restrictions for Implementing Lawful Intercept, page 3
- Information About Lawful Intercept Implementation, page 3
- Intercepting IPv6 Packets, page 6
- How to Configure SNMP v3 Access for Lawful Intercept on the Router, page 8
- Configuration Example for Inband Management Plane Feature Enablement, page 12
- Additional References, page 12
Prerequisites for Implementing Lawful Intercept

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Lawful intercept implementation also requires that these prerequisites are met:

- **Provisioned router**—The router must be already provisioned. For more information, see *Cisco IOS XR Getting Started Guide for the Cisco CRS Router*.

  **Tip** For the purpose of lawful intercept taps, provisioning a loopback interface has advantages over other interface types.

- **Understanding of SNMP Server commands in Cisco IOS XR software**—Simple Network Management Protocol, version 3 (SNMP v3), which is the basis for lawful intercept enablement, is configured using commands described in the module *SNMP Server Commands* in *Cisco IOS XR System Management Command Reference for the Cisco CRS Router*. To implement lawful intercept, you must understand how the SNMP server functions. For this reason, carefully review the information described in the module *Implementing SNMP* in *Cisco IOS XR System Management Configuration Guide for the Cisco CRS Router*.

- **Lawful intercept must be explicitly disabled**—It is automatically enabled on a provisioned router. However, you should not disable LI if there is an active tap in progress, because this deletes the tap.

- **Management plane configured to enable SNMPv3**—Allows the management plane to accept SNMP commands, so that the commands go to the interface (preferably, a loopback) on the router. This allows the mediation device (MD) to communicate with a physical interface.

- **VACM views enabled for SNMP server**—View-based access control model (VACM) views must be enabled on the router.

- **Provisioned MD**—For detailed information, see the vendor documentation associated with your MD. For a list of MD equipment suppliers preferred by Cisco, see http://www.cisco.com/en/US/tech/tk583/tk799/tsd_technology_support_protocol_home.html.

- **VoIP surveillance-specific requirements**
  - **Lawful-intercept-enabled call agent**—A lawful-intercept-enabled call agent must support interfaces for communications with the MD, for the target of interest to provide signaling information to the MD. The MD extracts source and destination IP addresses and Real-Time Protocol (RTP) port numbers from the Session Description Protocol (SDP) signaling information for the target of interest. It uses these to form an SNMPv3 SET, which is sent to the router acting as the content IAP to provision the intercept for the target of interest.

  The MD uses the CISCO-TAP2-MIB to set up communications between the router acting as the content IAP, and the MD.

  The MD uses the CISCO-IP-TAP-MIB to set up the filter for the IP addresses and port numbers to be intercepted and derived from the SDP.

  - Routers to be used for calls by the target number must be provisioned for this purpose through the MD.
The MD that has been provisioned with the target number to be intercepted.

- **Data session surveillance-specific requirements**
  
  - Routers to be used by the data target that have been provisioned for this purpose through the MD.
  
  - **The MD that has been provisioned with the user login ID, mac address of the user CPE device, or the DSLAM physical location ID**—The IP address is the binding that is most frequently used to identify the target in the network. However, alternative forms of information that uniquely identify the target in the network might be used in some network architectures. Such alternatives include the MAC address and the acct-session-id.

- The MD can be located anywhere in the network but must be reachable from the content IAP router, which is being used to intercept the target. MD should be reachable ONLY from global routing table and NOT from VRF routing table.

### Restrictions for Implementing Lawful Intercept

Lawful intercept does not provide support for these features on Cisco CRS Router:

- IPv6 multicast tapping
- Per interface tapping
- Replicating a single tap to multiple MDs
- Tapping basic mpls packets
- Tapping L2 flows
- RTP encapsulation

### Information About Lawful Intercept Implementation

Cisco lawful intercept is based on service-independent intercept (SII) architecture and SNMPv3 provisioning architecture. SNMPv3 addresses the requirements to authenticate data origin and ensure that the connection from the router to the MD is secure. This ensures that unauthorized parties cannot forge an intercept target.

Lawful intercept offers these capabilities:

- Voice-over IP (VoIP) and data session intercept provisioning from the MD using SNMPv3
- Delivery of intercepted VoIP and data session data to the MD
- SNMPv3 lawful intercept provisioning interface
- Lawful intercept MIB: CISCO-TAP2-MIB, version 2
- CISCO-IP-TAP-MIB manages the Cisco intercept feature for IP and is used along with CISCO-TAP2-MIB to intercept IP traffic.
- User datagram protocol (UDP) encapsulation to the MD
- IPv6 MD encapsulation for modular services card and forwarding processor card (CRS-MSC-40G and CRS-FP-40)
• Replication and forwarding of intercepted packets to the MD
• Per tap drop counter support
• Voice-over IP (VoIP) call intercept, based on any rules configured for received packets.
• Voice-over IP (VoIP) intercept with LI-enabled call agent
• Data session call intercept based on IP address

Provisioning for VoIP Calls

Lawful Intercept provisioning for VoIP occurs in these ways:

• Security and authentication occurs because users define this through SNMPv3.
• The MD provisions lawful intercept information using SNMPv3.
• Network management occurs through standard MIBs.

Call Interception

VoIP calls are intercepted in this manner:

• The MD uses configuration commands to configure the intercept on the call control entity.
• The call control entity sends intercept-related information about the target to the MD.
• The MD initiates call content intercept requests to the content IAP router or trunk gateway through SNMPv3.
• The content IAP router or trunk gateway intercepts the call content, replicates it, and sends it to the MD in Packet Cable Electronic Surveillance UDP format. Specifically, the original packet starting at the first byte of the IP header is prefixed with a four-byte CCCID supplied by the MD in TAP2-MIB. It is then put into a UDP frame with the destination address and port of the MD.
• After replicated VoIP packets are sent to the MD, the MD then forwards a copy to a law-enforcement-agency-owned collection function, using a recognized standard.

Provisioning for Data Sessions

Provisioning for data sessions occurs in a similar way to the way it does for lawful intercept for VoIP calls. (See Provisioning for VoIP Calls, page 4.)

Data Interception

Data are intercepted in this manner:

• If a lawful intercept-enabled authentication or accounting server is not available, a sniffer device can be used to detect the presence of the target in the network.
  ◦ The MD uses configuration commands to configure the intercept on the sniffer.
• The sniffer device sends intercept-related information about the target to the MD.
• The MD initiates communication content intercept requests to the content IAP router using SNMPv3.
• The content IAP router intercepts the communication content, replicates it, and sends it to the MD in UDP format.
• Intercepted data sessions are sent from the MD to the collection function of the law enforcement agency, using a supported delivery standard for lawful intercept.

**Information About the MD**
The MD performs these tasks:
• Activates the intercept at the authorized time and removes it when the authorized time period elapses.
• Periodically audits the elements in the network to ensure that:
  ◦ only authorized intercepts are in place.
  ◦ all authorized intercepts are in place.

**Lawful Intercept Topology**
This figure shows intercept access points and interfaces in a lawful intercept topology for both voice and data interception.

*Figure 1: Lawful Intercept Topology for Both Voice and Data Interception*
Scale or Performance Improvement

The new enhancement in terms of scalability and performance for lawful intercept support on Cisco CRS Router modular services cards and forwarding processor cards (CRS-MSC-40G, CRS-FP-40) are:

- Increase in IPv4 lawful intercept tap limit from 250 taps to 1000 taps.
- IPv4 and IPv6 combined tap limit is 2000 taps, 1000 taps each for IPv4 and IPv6.
- Enhancement of interception rate to 100 Mbps per slot.

Intercepting IPv6 Packets

This section provides details for intercepting IPv6 packets supported on the Cisco CRS Router.

Lawful Intercept Filters

The filters used for classifying a tap are:

- IP address type (IPv4/IPv6)
- Destination address
- Destination mask
- Source address
- Source mask
- ToS (Type of Service) and ToS mask
- Protocol
- Destination port with range
- Source port with range
- VRF (VPN Routing and Forwarding)
- Flow ID (for IPv6 only)

Intercepting IPv6 Packets Based on Flow ID

To further extend filtration criteria for IPv6 packets, an additional support to intercept IPv6 packets based on flow ID has been introduced on the Cisco CRS Router. All IPv6 packets are intercepted based on the fields in the IPv6 header which comprises numerous fields defined in IPv6 Header Field Details table:

Table 1: IPv6 Header Field Details

<table>
<thead>
<tr>
<th>IPv6 Field Name</th>
<th>Field Description</th>
<th>Field Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>IPv6 version number.</td>
<td>4 bits</td>
</tr>
</tbody>
</table>
### Interception Table

<table>
<thead>
<tr>
<th>IPv6 Field Name</th>
<th>Field Description</th>
<th>Field Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Class</td>
<td>Internet traffic priority delivery value.</td>
<td>8 bits</td>
</tr>
<tr>
<td>Flow ID (Flow Label)</td>
<td>Used for specifying special router handling from source to destination(s) for a sequence of packets.</td>
<td>20 bits</td>
</tr>
<tr>
<td>Payload Length</td>
<td>Specifies the length of the data in the packet. When cleared to zero, the option is a hop-by-hop Jumbo payload.</td>
<td>16 bits unassigned</td>
</tr>
<tr>
<td>Next Header</td>
<td>Specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.</td>
<td>8 bits</td>
</tr>
<tr>
<td>Hop Limit</td>
<td>For each router that forwards the packet, the hop limit is decremented by 1. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header that was originally intended to be used as a time based hop limit.</td>
<td>8 bits unsigned</td>
</tr>
<tr>
<td>Source Address</td>
<td>The IPv6 address of the sending node.</td>
<td>16 bytes</td>
</tr>
<tr>
<td>Destination Address</td>
<td>The IPv6 address of the destination node.</td>
<td>16 bytes</td>
</tr>
</tbody>
</table>

The flow ID or flow label is a 20 bit field in the IPv6 packet header that is used to discriminate traffic flows. Each flow has a unique flow ID. The filteration criteria to intercept packets matching a particular flow ID is defined in the tap configuration file. From the line card, the intercepted mapped flow IDs are sent to the next hop, specified in the MD configuration file. The intercepted packets are replicated and sent to the MD from the line card. The ideal replication rate on MSC-40 is 100 Mbps depending on packet size and features configured on the router.

### Intercepting VRF (6VPE) and 6PE Packets

This section provides information about intercepting VRF aware packets and 6PE packets. Before describing how it works, a basic understanding of 6VPE networks is discussed.

The MPLS VPN model is a true peer VPN model. It enforces traffic separations by assigning unique VPN route forwarding (VRF) tables to each customer's VPN at the provider content IAP router. Thus, users in a specific VPN cannot view traffic outside their VPN.

Cisco CRS Router supports intercepting IPv6 packets of the specified VRF ID for 6VPE. To distinguish traffic on VPN, VRFs are defined containing a specific VRF ID. The filter criteria to tap a particular VRF ID is specified in the tap. IPv6 packets are intercepted with the VRF context on both scenarios: imposition (ip2mpls) and disposition (mpls2ip).

The 6PE packets carry IPv6 packets over VPN. The packets do not have a VRF ID. Only IP traffic is intercepted; no MPLS based intercepts are supported. The IPv6 traffic is intercepted at the content IAP of the MPLS cloud at imposition (ip2mpls) and at disposition (mpls2ip).

Intercepting IPv6 packets is also performed for ip2tag and tag2ip packets. Ip2tag packets are those which are converted from IPv6 to Tagging (IPv6 to MPLS), and tag2ip packets are those which are converted from Tagging to IPv6 (MPLS to IPv6) at the provider content IAP router.
Encapsulation Type Supported for Intercepted Packets

Intercepted packets mapping the tap are replicated, encapsulated, and then sent to the MD. IPv4 and IPv6 packets are encapsulated using UDP (User Datagram Protocol) encapsulation. The replicated packets are forwarded to MD using UDP as the content delivery protocol. Both IPv4 and IPv6 MD encapulations are supported. The encapsulation type (IPv4 or IPv6) depends on the address of MD.

The intercepted packet gets a new UDP header and IPv4 header. Information for IPv4 header is derived from MD configuration. Apart from the IP and UDP headers, a 4 byte channel identifier (CCCID) is also inserted after the UDP header in the packet. After adding the MD encapsulation, if the packet size is above the MTU, the egress LC CPU fragments the packet. Moreover, there is a possibility that the packet tapped is already a fragment. Each tap is associated with only one MD. Cisco CRS Router does not support forwarding replicated packets to multiple MDs.

Note: Encapsulation types, such as RTP and RTP-NOR, are not supported.

Per Tap Drop Counter Support

Cisco CRS Router line cards provide an interface to export each tap forwarded to MD packet and drop counts. Any intercepted packets that are dropped prior to getting forwarded to the MD due to policer action are counted and reported. The drops due to policer action are the only drops that are counted under per tap drop counters. If a lawful intercept filter is modified, the packet counts are reset to 0.

How to Configure SNMP v3 Access for Lawful Intercept on the Router

Perform these procedures in the order presented to configure Management Plane Protection (MPP) and SNMP for the purpose of lawful intercept enablement:

Disabling Lawful Intercept

Lawful Intercept is enabled by default on each supported router.

- To disable LI, enter the command `lawful-intercept disable` in global configuration mode.
- To reenable it, use the `no` form of this command.

Note: LI should not be disabled if any active taps and MDs are provisioned. Otherwise, it will delete all taps and MDs from the router.
Configuring the Inband Management Plane Protection Feature

Unless you have previously configured MPP to work with another protocol, you do not need to configure the MPP feature to enable the SNMP server to communicate with the MD for the purpose of lawful intercept. Only in such a case, you must specifically configure MPP as an inband interface to allow SNMP commands to be accepted by the router, using a specified interface or all interfaces.

Note
If you have recently migrated to Cisco IOS XR software from Cisco IOS, and you had MPP configured for a given protocol, you still need to perform this task.

For the purpose of lawful intercept, a loopback interface is often the destination of choice for SNMP messages. If you choose this interface type, you must include it in your inband management configuration.

For the configuration procedure, see the section Configuring a Device for Management Plane Protection for an Inband Interface. For an LI-related example of this procedure, see Configuring the Inband Management Plane Protection Feature: Example, page 12.

For a more detailed discussion of the inband management interface, see the Inband Management Interface.

Enabling the Mediation Device to Intercept VoIP and Data Sessions

These SNMP server configuration tasks enable the Cisco SII feature on a router running Cisco IOS XR software by allowing the MD to intercept VoIP or data sessions.

SUMMARY STEPS

1. configure
2. snmp-server view view-name ciscoTap2MIB included
3. snmp-server view view-name ciscoIpTapMIB included
4. snmp-server group group-name v3 auth read view-name write view-name notify view-name
5. snmp-server host ip-address traps version 3 priv username udp-port port-number
6. snmp-server user mduser-id groupname v3 auth md5 md-password
7. Use one of the following commands:
   * end
   * commit
8. show snmp users
9. show snmp group
10. show snmp view
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp-server view</td>
<td>Creates or modifies a view record and includes the CISCO-TAP2-MIB family.</td>
</tr>
<tr>
<td></td>
<td>view-name ciscoTap2MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>included</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>snmp-server view</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TapName ciscoTap2MIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>included</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>snmp-server view</td>
<td>Creates or modifies a view record and includes the CISCO-IP-TAP-MIB family.</td>
</tr>
<tr>
<td></td>
<td>view-name ciscoIpTapMIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>included</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>snmp-server view</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TapName ciscoIpTapMIB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>included</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>snmp-server group</td>
<td>Configures a new SNMP group, or a table that maps SNMP users to SNMP views. This group must have read, write, and notify privileges for the SNMP view.</td>
</tr>
<tr>
<td></td>
<td>group-name v3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>auth read view-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>write view-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>notify view-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>snmp-server group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TapGroup v3 auth read TapView write</td>
<td></td>
</tr>
<tr>
<td></td>
<td>notify TapView</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>snmp-server host</td>
<td>Specifies SNMP trap notifications, the version of SNMP to use, the security level of the notifications, and the recipient (host) of the notifications.</td>
</tr>
<tr>
<td></td>
<td>ip-address traps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>version 3 priv</td>
<td></td>
</tr>
<tr>
<td></td>
<td>username udp-port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port-number</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>snmp-server host</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host 223.255.254.224 traps version 3 priv</td>
<td></td>
</tr>
<tr>
<td></td>
<td>bgreen udp-port 255</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>snmp-server user</td>
<td>Configures the MD user as part of an SNMP group, using the v3 security model and the HMAC MD5 algorithm, which you associate with the MD password.</td>
</tr>
<tr>
<td></td>
<td>mduser-id groupname v3 auth md5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>md-password</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>snmp-server user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mduser-id TapGroup v3 auth md5 mdpassword</td>
<td></td>
</tr>
<tr>
<td></td>
<td>md-password</td>
<td></td>
</tr>
</tbody>
</table>

- The *mduser-id* and *mdpassword* must match that configured on MD. Alternatively, these values must match those in use on the router.
- Passwords must be eight characters or longer to comply with SNMPv3 security minimums.
- Minimum LI security level is *auth*; *noauth* will not work. The LI security level must also match that of the MD.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Choices other than MD5 are available on the router, but the MD values must match. Most MDs default to or support only MD5.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**

Use one of the following commands:

- `end`
- `commit`

**Example:**

```
RP/0/RP0/CPU0:router(config)# end
```

or

```
RP/0/RP0/CPU0:router(config)# commit
```

Saves configuration changes.

- When you issue the `end` command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
```

- Entering `yes` saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering `no` exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering `cancel` leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the `commit` command to save the configuration changes to the running configuration file and remain within the configuration session.

**Step 8**

`show snmp users`

**Example:**

```
RP/0/RP0/CPU0:router# show snmp users
```

Displays information about each SNMP username in the SNMP user table.

**Step 9**

`show snmp group`

**Example:**

```
RP/0/RP0/CPU0:router# show snmp group
```

Displays information about each SNMP group on the network.

**Step 10**

`show snmp view`

**Example:**

```
RP/0/RP0/CPU0:router# show snmp view
```

Displays information about the configured views, including the associated MIB view family name, storage type, and status.
Configuration Example for Inband Management Plane Feature Enablement

This example illustrates how to enable the MPP feature, which is disabled by default, for the purpose of lawful intercept.

Configuring the Inband Management Plane Protection Feature: Example

You must specifically enable management activities, either globally or on a per-inband-port basis, using this procedure. To globally enable inbound MPP, use the keyword `all` with the `interface` command, rather than use a particular interface type and instance ID with it.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)# inband
RP/0/RP0/CPU0:router(config-mpp-inband)# interface loopback0
RP/0/RP0/CPU0:router(config-mpp-inband-Loopback0)# allow snmp
RP/0/RP0/CPU0:router(config-mpp-inband-Loopback0)# commit
RP/0/RP0/CPU0:router(config-mpp-inband-Loopback0)# exit
RP/0/RP0/CPU0:router(config-mpp-inband)# exit
RP/0/RP0/CPU0:router(config-ctr)# exit
RP/0/RP0/CPU0:router# show mgmt-plane inband interface loopback0

interface - Loopback0
  snmp configured - All peers allowed
```

Management Plane Protection - inband interface

Additional References

These sections provide references related to implementing lawful intercept.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawful Intercept commands</td>
<td>Cisco IOS XR System Security Command Reference for the Cisco CRS Router</td>
</tr>
<tr>
<td>Implementing SNMP</td>
<td>Cisco IOS XR System Management Configuration Guide for the Cisco CRS Router</td>
</tr>
<tr>
<td>SNMP Server commands</td>
<td>Cisco IOS XR System Management Command Reference for the Cisco CRS Router</td>
</tr>
</tbody>
</table>
## Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>A modular, open architecture designed for simple implementation that easily interacts with third-party equipment to meet service provider lawful intercept requirements.</td>
<td>See RFC-3924 under RFCs, page 13.</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-TAP2-MIB, version 2</td>
<td>To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
<tr>
<td>• CISCO-IP-TAP-MIB</td>
<td></td>
</tr>
</tbody>
</table>

## RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC-3924</td>
<td>Cisco Architecture for Lawful Intercept in IP Networks</td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>