Configuring Lawful Intercept

- Prerequisites for Lawful Intercept, on page 1
- Restrictions for Lawful Intercept, on page 1
- Information About Lawful Intercept, on page 2
- How to Configure Lawful Intercept, on page 9
- Configuration Examples for Lawful Intercept, on page 12
- Feature History for Lawful Intercept, on page 13

Prerequisites for Lawful Intercept

- You must be running images that support secure shell (SSH). Lawful intercept is not supported on images that do not support SSH.
- The switch you are logged into must have the highest access level (L15). To log in with L15 access, enter the **enable** command and specify the highest-level password defined for the switch.
- The time of day on the switch and the mediation device (supplied by a third-party vendor) connected to the network must be must be synchronized; also, configure Network Time Protocol (NTP) on both the switch and the mediation device.
- (Optional) It might be helpful to use a loopback interface for the switch to communicate with the mediation device. If you do not use a loopback interface, you must configure the mediation device with multiple physical interfaces on the switch to handle network failures.

Restrictions for Lawful Intercept

- Intercept or tap can be configured using only SNMP. Also, configuring interface-specific intercept is not allowed.
- The CISCO-IP-TAP-MIB does not support the virtual routing and forwarding (VRF) OID citapStreamVRF.
- IPv4 multicast, IPv6 unicast, and IPv6 multicast flows are not supported. Only IPv4 unicast traffic is supported.
- Lawful Intercept is not supported on Layer 2 interfaces. However, lawful intercept can intercept traffic on VLANs that run over a Layer 2 interface.

- Lawful Intercept is not supported in packets that are encapsulated within other packets, for example, tunneled packets or Q-in-Q packets.
- Lawful Intercept is not supported for Layer 2 taps.
- Lawful Intercept is not supported in packets that are subject to Layer 3 or Layer 4 rewrite, for example, Network Address Translation (NAT) or TCP reflexive.

Information About Lawful Intercept

Overview of Lawful Intercept

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

Surveillance is performed through the use of wiretaps on traditional telecommunications and internet services in voice, data, and multiservice networks. The law enforcement agencies deliver a request for a wiretap to the target's service provider who is responsible for intercepting data communication to and from the individual. The service provider uses the target's IP address to determine which of its edge devices handles the target's traffic (data communication). The service provider then intercepts the target's traffic as it passes through the device, and sends a copy of the intercepted traffic to the LEA without the target's knowledge.

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

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

For information about the Cisco lawful intercept solution, contact your Cisco account representative.

Note The Lawful Intercept feature supports the interception of IPv4 protocol as defined by the citapStreamprotocol object in the CISCO-IP-TAB-MIB that includes voice and date interception.

Benefits of Lawful Intercept

- Allows multiple LEAs to run a lawful intercept on the same target without each other's knowledge.
- Does not affect subscriber services on the device.
- Supports wiretaps in both the input and output direction.
- Supports wiretaps of Layer 1 and Layer 3 traffic. Layer 2 traffic is supported as IP traffic over VLANs.
- Supports Layer 3 physical interfaces or Switch Virtual Interfaces (SVI).
- Supports wiretaps of individual subscribers that share a single physical interface.

- Cannot be detected by the target. Neither the network administrator nor the calling party is aware that packets are being copied or that the call is being tapped.
- Uses Simple Network Management Protocol Version 3 (SNMPv3) and security features such as the View-based Access Control Model (SNMP-VACM-MIB) and the User-based Security Model (SNMP-USM-MIB) to restrict access to lawful intercept information and components.
- Hides information about lawful intercepts from all but the most privileged users. An administrator must set up access rights to enable privileged users to access lawful intercept information.
- Provides two secure interfaces for performing an intercept; one for setting up the wiretap and one for sending the intercepted traffic to the LEA.

CALEA for Voice

The Communications Assistance for Law Enforcement Act (CALEA) for Voice feature allows the lawful interception of voice conversations that are running on VoIP. Although the devices are not voice gateway devices, VoIP packets traverse the devices at the edge of the service provider network.

When an approved government agency determines that a telephone conversation is interesting, CALEA for Voice copies the IP packets comprising the conversation and sends the duplicate packets to the appropriate monitoring device for further analysis.

Configuration Guidelines

- To deploy Lawful Intercept at a node, do not configure optimized ACL logging, VLAN access control list (VACL) capture, or Intrusion Detection System (IDS) at the node. Deploying lawful intercept at the node causes unpredictable behavior in optimized ACL logging, VACL capture, and IDS.
- The maximum number of TAPs supported on Catalyst 9500 series switches is 160.
- When provisioning the mediation device, if the interface index passed is zero, the switch selects the best possible interface to reach the mediation device. If the interface index is set to another value, the switch uses that interface index to reach the mediation device.
- (Optional) The domain name for both the device and the mediation device can be registered in the Domain Name System (DNS).
- The mediation device must have an access function.
- You must add the mediation device to the 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 must also include the mediation device’s authorization password.
- The device intercepts and replicates packets even if the packets are later dropped, for example, due to rate limiting or an access control list (ACL) deny statement.
- Lawful intercept ACLs are applied internally to both the ingress and the egress directions of an interface.
- Packets that are subject to hardware rate limiting are processed by lawful intercept as follows:
    - Packets that are dropped by the rate limiter are not intercepted or processed.

- Packets that are passed by the rate limiter are intercepted and processed.

- If multiple law enforcement agencies use a single mediation device and each of these agencies is executing a wiretap on the same target, the device sends a single packet to the mediation device. It is up to the mediation device to duplicate the packet for each law enforcement agency.
- Lawful intercept can intercept IPv4 packets with values that match a combination of one or more of the following fields:
  - Destination IP address and mask
  - Destination port range
  - Source IP address and mask
  - Source port range
  - Protocol ID

Network Components Used for Lawful Intercept

This section describes the network components used for lawful intercept.

Mediation Device

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

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

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

Lawful Intercept Administration

Lawful intercept administration (LIA) provides the authentication interface for lawful intercept or wiretap requests and administration.

Intercept Access Point

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

- Identification (ID) IAP—A device, such as an authentication, authorization, and accounting (AAA) server that provides intercept-related information (IRI) for the intercept (for example, the target's username

and system IP address) or call agents for VoIP. The IRI helps a service provider determine which content IAP (switch) the target's traffic passes through.

- Content IAP—A device that the target's traffic passes through. The content IAP:
  - Intercepts traffic to and from the target for the length of time specified in the court order. The device continues to forward traffic to its destination to ensure that the wiretap is undetected.
  - Creates a copy of the intercepted traffic, encapsulates it in User Datagram Protocol (UDP) packets, and forwards the packets to the mediation device without the target's knowledge. Note that the IP option header is not supported.

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.

Content Intercept Access Point

Content IAP intercepts the interested data stream, duplicates the content, and sends the duplicated content to the mediation device. The mediation device receives the data from the ID IAP and content IAP, converts the information to the required format depending on country-specific requirements and forwards it to the law enforcement agency.

Lawful Intercept Processing

After acquiring a court order or warrant to perform surveillance, the LEA delivers a surveillance request to the target's service provider. Service provider personnel use an administration function that runs on the mediation device to configure a lawful intercept to monitor the target's electronic traffic for a specific period of time (as defined in the court order).

After the intercept is configured, user intervention is no longer required. The administration function communicates with other network devices to set up and execute the lawful intercept. The following sequence of events occurs during a lawful intercept:

1. The administration function contacts the ID IAP for intercept-related information (IRI), such as the target's username and the IP address of the system, to determine which content IAP (switch) the target's traffic passes through.
2. After identifying the device that handles the target's traffic, the administration function sends SNMPv3 get and set requests to the device's Management Information Base (MIB) to set up and activate the lawful intercept. The CISCO-TAP2-MIB is the supported lawful intercept MIB to provide per-subscriber intercepts.
3. During lawful intercept, the device:
   a. Examines incoming and outgoing traffic and intercepts any traffic that matches the specifications of the lawful intercept request.
   b. Creates a copy of the intercepted traffic and forwards the original traffic to its destination so that the target does not suspect anything.
   c. Encapsulates the intercepted traffic in UDP packets, and forwards the packets to the mediation device without the target's knowledge.

Note The process of intercepting and duplicating the target's traffic does not add detectable latency in the traffic stream.

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

5. When the lawful intercept expires, the device stops intercepting the target's traffic.

Lawful Intercept MIBs

This section lists the MIBs used for lawful intercept processing.

- CISCO-TAP2-MIB: Used for lawful intercept processing.
- CISCO-IP-TAP-MIB: Used for intercepting Layer 3 (IPv4) traffic.

Due to its sensitive nature, the Cisco lawful intercept MIBs are only available in software images that support the Lawful Intercept feature. To access the Cisco IOS MIB Locator page, go to:

http://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index.

CISCO-TAP2-MIB

The CISCO-TAP2-MIB contains SNMP management objects that control lawful intercepts. The mediation device uses the MIB to configure and run lawful intercepts on targets whose traffic passes through the device.

The CISCO-TAP2-MIB contains several tables that provide information for lawful intercepts that are running on the device:

- cTap2MediationTable: Contains information about each mediation device that is currently running lawful intercept on the device. Each table entry provides information that the device uses to communicate with the mediation device, for example, the device's address, the interfaces to send intercepted traffic over, and the protocol to use to transmit the intercepted traffic.
- cTap2StreamTable: Contains information used to identify the traffic to intercept. Each table entry contains a pointer to a filter that is used to identify the traffic stream associated with the target of a lawful intercept. Traffic that matches the filter is intercepted, copied, and sent to the corresponding mediation device application (cTap2MediationContentId).

  The cTap2StreamTable table also contains counts of the number of packets that were intercepted, and counts of dropped packets that should have been intercepted, but were not.
- cTap2DebugTable: Contains debug information for troubleshooting lawful intercept errors.

The CISCO-TAP2-MIB also contains several SNMP notifications for lawful intercept events. For detailed descriptions of MIB objects, see corresponding MIBs.

CISCO-TAP2-MIB Processing

The administration function (running on the mediation device) issues SNMPv3 set and get requests to the device's CISCO-TAP2-MIB to set up and initiate a lawful intercept. To do this, the administration function performs the following actions:

1. Creates a cTap2MediationTable entry to define how the device is to communicate with the mediation device executing the intercept.

Note The cTap2MediationNewIndex object provides a unique index for the mediation table entry.

2. Creates an entry in the cTap2StreamTable to identify the traffic stream to intercept.
3. Sets cTap2StreamInterceptEnable to true(1) to start the intercept. The device intercepts traffic in the stream until the intercept expires (cTap2MediationTimeout).

CISCO-IP-TAP-MIB

The CISCO-IP-TAP-MIB contains the SNMP management objects to configure and execute lawful intercepts on IPv4 traffic streams that flow through the device. This MIB is an extension of the CISCO-TAP2-MIB.

You can use the CISCO-IP-TAP-MIB to configure lawful intercept on a device to intercept IPv4 packets with values that match a combination of one or more of the following fields:

- Destination IP address and mask
- Destination port range
- Source IP address and mask
- Source port range
- Protocol ID

CISCO-IP-TAP-MIB Processing

When data is intercepted, two streams are created. One stream is for packets that originate from the target IP address to any other IP address using any port. The second stream is created for packets that are routed to the target IP address from any other address using any port. For VoIP, two streams are created, one for RTP packets from the target and the second stream for the RTP packets to target using the specific source and destination IP addresses and ports specified in the SDP information used to set up the RTP stream.

MIB Guidelines

The following Cisco MIBs are used for lawful intercept processing. Include these MIBs in the SNMP view of lawful intercept MIBs to enable the mediation device to configure and execute wiretaps on traffic that flows through the device.

- CISCO-TAP2-MIB: Required for both types of lawful intercepts: regular and broadband.
- CISCO-IP-TAP-MIB: Required for wiretaps on Layer 3 (IPv4) streams. Supported for regular and broadband lawful intercept.

- The CISCO-IP-TAB-MIB imposes limitations on the following features:
  - If one or all of the following features are configured and functioning and lawful intercept is enabled, lawful intercept takes precedence, and the feature behaves as follows:
    - Optimized ACL logging (OAL): Does not function.
    - VLAN access control list (VACL) capturing: Does not function properly.
    - Intrusion detection system (IDS): Does not function properly.

    These features start to function after you disable or unconfigure lawful intercept.
  - IDS cannot capture traffic on its own, but captures traffic that has been intercepted by lawful intercept.

Security Considerations

This section lists the security considerations during lawful intercept.

- SNMP notifications for lawful intercept must be sent to UDP port 161 on the mediation device, not port 162 (which is the SNMP default).
- 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 device. In addition, these users must have authPriv or authNoPriv access rights to access the lawful intercept 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

We recommend that you also see the information provided in #unique_1134 and #unique_1135.

Restricting Access to the Lawful Intercept MIBs

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

1. Create a view that includes the Cisco lawful intercept 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 lawful intercept user groups to define who can access the MIBs along with information, if any, related to lawful intercepts. Be sure to add the mediation device as a user in this group; otherwise, the device cannot perform lawful intercepts.

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

How to Configure Lawful Intercept

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 provided in this section.

Before you begin

- SNMPv3 must be configured on the device.

Note Issue the commands in global configuration mode with level-15 access rights.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server view** *view-name MIB-name* **included** **Example:** `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. This MIB is required for both regular and broadband lawful intercept.
Step 4	**snmp-server view** *view-name MIB-name* **included** **Example:**	Adds the CISCO-IP-TAP-MIB to the SNMP view.

	Command or Action	Purpose
	`Device(config)# snmp-server view exampleView ciscoIpTapMIB included`	
Step 5	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView cisco802TapMIB included`	Adds the CISCO-802-TAP-MIB to the SNMP view.
Step 6	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView ciscoUserConnectionTapMIB included`	Adds the CISCO-USER-CONNECTION-TAP-MIB to the SNMP view.
Step 7	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView ciscoMobilityTapMIB included`	Adds the CISCO-MOBILITY-TAP-MIB to the SNMP view.
Step 8	**snmp-server group** *group-name* **v3 auth read** *view-name* **write** *view-name* **Example:** `Device(config)# snmp-server group exampleGroup v3 auth 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 9	**snmp-server user** *user-name group-name* **v3 auth md5** *auth-password* **Example:** `Device(config)# snmp-server user exampleUser exampleGroup v3 auth md5 examplePassword`	Adds users to the specified user group.
Step 10	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling SNMP Notifications for Lawful Intercept

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

Before you begin

- SNMPv3 must be configured on the device..

Note Issue the commands in global configuration mode with level-15 access rights.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** *ip-address* **community-string udp-port** *port notification-type* **Example:** `Device(config)# snmp-server host 10.2.2.1 community-string udp-port 161 udp`	Specifies the IP address of the mediation device and the password-like community-string that is sent with a notification request. • 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** **Example:** `Device(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`	Configures the device to send RFC 1157 notifications to the mediation device. • These notifications indicate authentication failures, link status (up or down), and device restarts.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Disabling SNMP Notifications

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

Note 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).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no snmp-server enable traps** **Example:** `Device(config)# no snmp-server enable traps`	Disables all SNMP notification types that are available on your system.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

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 three LI MIBs (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, CISCO-802-TAP-MIB). It also creates a user group that has read, write, and notify access to MIBs in the tapV view.

```
Device> enable
Device# configure terminal
Device(config)# snmp-server view tapV ciscoTap2MIB included
Device(config)# snmp-server view tapV ciscoIpTapMIB included
```

```
Device(config)# snmp-server view tapV cisco802TapMIB included
Device(config)# snmp-server group tapGrp v3 auth read tapV write tapV notify tapV
Device(config)# snmp-server user MDuser tapGrp v3 auth md5 MDpasswd
Device(config)# snmp-server engineID local 1234
Device(config)# end
```

Feature History for Lawful Intercept

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.8.1a	Lawful Intercept	The Lawful Intercept feature supports service providers in meeting the requirements of law enforcement agencies to provide electronic surveillance as authorized by a judicial or administrative order. Support for this feature was introduced on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.