



CHAPTER 1

Lawful Intercept Overview

This chapter provides information about lawful intercept and contains the following sections:

- [Information About Lawful Intercept, page 1-1](#)
- [Network Components Used for Lawful Intercept, page 1-2](#)
- [Lawful Intercept Processing, page 1-4](#)
- [Lawful Intercept MIBs, page 1-5](#)



Caution

This guide does not address legal obligations for the implementation of lawful intercept. As a service provider, you are responsible to ensure that your network complies with applicable lawful intercept statutes and regulations. We recommend that you seek legal advice to determine your obligations.

Information About Lawful Intercept

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

The surveillance is performed through the use of wiretaps on traditional telecommunications and Internet services in voice, data, and multiservice networks. The LEA delivers a request for a wiretap to the target's service provider, who is responsible for intercepting data communication to and from the individual. The service provider uses the target's IP address to determine which of its edge Catalyst 6500 series switches handles the target's traffic (data communication). The service provider then intercepts the target's traffic as it passes through the Catalyst 6500 series switch, 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.

DRAFT -- CISCO CONFIDENTIAL**Note**

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

Benefits of Lawful Intercept

Lawful intercept has the following benefits:

- Allows multiple LEAs to run a lawful intercept on the same target without each other's knowledge.
- Does not affect subscriber services on the Catalyst 6500 series switch.
- 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 wiretaps of individual subscribers that share a single physical interface.
- Cannot be detected by the target. Neither the network administrator nor the calling parties 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 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 Voice over IP (VoIP). Although the Catalyst 6500 series switches are not voice gateway devices, VoIP packets traverse the Catalyst 6500 series switches 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.

Network Components Used for Lawful Intercept

The following network components are used for lawful intercepts:

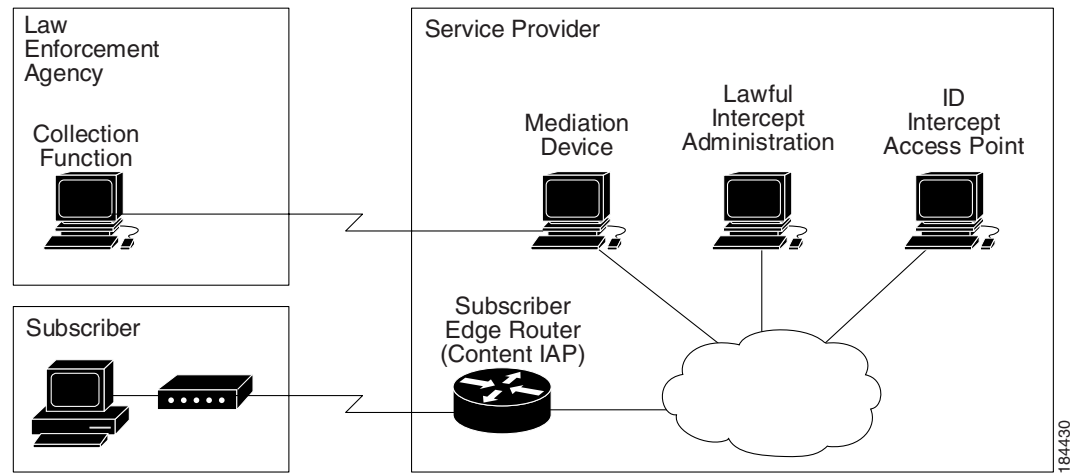
- [Mediation Device](#)
- [Lawful Intercept Administration](#)
- [Intercept Access Point](#)
- [Content Intercept Access Point](#)

For information about lawful intercept processing, see the [“Lawful Intercept Processing”](#) section on page 1-4.

DRAFT -- CISCO CONFIDENTIAL

Figure 1-1 provides an overview of the lawful intercept model.

Figure 1-1 **Lawful Intercept Overview**



Mediation Device

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

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



Note

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

Lawful Intercept Administration

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

DRAFT -- CISCO CONFIDENTIAL

Intercept Access Point

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

- Identification (ID) IAP—A device, such as an authentication, authorization, and accounting (AAA) server, that provides intercept-related information (IRI) for the intercept (for example, the target's username and system IP address) or call agents for voice over IP. The IRI helps the service provider determine which content IAP (Catalyst 6500 series switch) the target's traffic passes through.
- Content IAP—A device, such as a Catalyst 6500 series switch, 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 Catalyst 6500 series switch 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. IP option header is not supported.

**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.

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 requirement and forwards it to law enforcement agency (LEA).

Lawful Intercept Processing

After acquiring a court order or warrant to perform surveillance, the LEA delivers a surveillance request to the target's service provider. 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 (Catalyst 6500 series switch) the target's traffic passes through.
2. After identifying the Catalyst 6500 series switch that handles the target's traffic, the administration function sends SNMPv3 **get** and **set** requests to the Catalyst 6500 series switch'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.

DRAFT -- CISCO CONFIDENTIAL

3. During the lawful intercept, the Catalyst 6500 series switch:
 - a. Examines incoming and outgoing traffic and intercepts any traffic that matches the specifications of the lawful intercept request.
 - b. Creates a copy of the intercepted traffic and forwards the original traffic to its destination so the target does not suspect anything.
 - c. Encapsulates the intercepted traffic in UDP packets and forwards the packets to the mediation device without the target's knowledge.



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

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 Catalyst 6500 series switch 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.

5. When the lawful intercept expires, the Catalyst 6500 series switch stops intercepting the target's traffic.

Lawful Intercept MIBs

To perform lawful intercept, the Catalyst 6500 series switch uses these MIBs, which are described in the following sections:

- [CISCO-TAP2-MIB](#)—Used for lawful intercept processing.
- [CISCO-IP-TAP-MIB](#)—Used for intercepting Layer 3 (IPv4) traffic.

CISCO-TAP2-MIB

The CISCO-TAP2-MIB contains SNMP management objects that control lawful intercepts on the Catalyst 6500 series switch. The mediation device uses the MIB to configure and run lawful intercepts on targets whose traffic passes through the Catalyst 6500 series switch.

The CISCO-TAP2-MIB contains several tables that provide information for lawful intercepts that are running on the Catalyst 6500 series switch:

- **cTap2MediationTable**—Contains information about each mediation device that is currently running a lawful intercept on the Catalyst 6500 series switch. Each table entry provides information that the Catalyst 6500 series switch 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).

DRAFT -- CISCO CONFIDENTIAL

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 the MIB itself.

CISCO-TAP2-MIB Processing

The administration function (running on the mediation device) issues SNMPv3 **set** and **get** requests to the Catalyst 6500 series switch'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 Catalyst 6500 series switch 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 Catalyst 6500 series switch 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 Catalyst 6500 series switch. This MIB is an extension to the CISCO-TAP2-MIB.

You can use the CISCO-IP-TAP-MIB to configure lawful intercept on the Catalyst 6500 series switch 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 target and the second stream is for the RTP packets to target using the specific source and destination IP addresses and ports specified in SDP information used to setup RTP stream.