CHAPTER 1

Lawful Intercept Overview

This chapter provides information about Lawful Intercept (LI) and contains the following information:

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 or session to determine which of its edge routers handles the target's traffic (data communication). The service provider then intercepts the target's traffic as it passes through the router, 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 a Cisco lawful intercept solution, contact your Cisco account representative.

Feature History for Lawful Intercept

Cisco IOS Release	Description
Release 12.2(31)SB12	The Lawful Intercept for MLP feature was added on Cisco 10000 series router for PRE2 and PRE3.
Release 12.3(7)XI	This feature was integrated in Cisco IOS Release 12.3(7)XI and implemented on the Cisco 10000 series router for the PRE2.
Release 12.2(28)SB	This feature was enhanced to support RADIUS-based lawful intercept and the CISCO-TAP2-MIB replaces the CISCO-TAP-MIB.
Release 12.2(31)SB2	This feature was enhanced to include the CISCO-USER-CONNECTION-TAP-MIB.

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 router.
- Cannot be detected by the target.
- Allows LEAs to perform lawful intercepts without the knowledge of service providers.
- Uses Simple Network Management Protocol Version 3 (SNMPv3) and security features like the View-based Access Control Model (SNMP-VACM-MIB) and User-based Security Model (SNMP-USM-MIB) to restrict access to lawful intercept information and components.
- 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 mediation device.
- The Cisco 10000 series router supports intercept taps on the following PPPo*X* sessions:
  - PPPoA
  - PPPoE
  - PPPoEoA
  - PPPoEoVLAN
  - PPPoEoQinQ
- In Cisco 10000 series router, IPv4 Lawful Intercept support the traffic for the following MLP bundle interfaces:
  - MLP over Serial
  - MLP over Single VC ATM
  - MLP over Multi VC ATM
  - MLP over FR

Note IPv6 tapping on Multilink bundle interfaces is not supported. Interception of Multicast traffic over Multilink bundle interfaces is also not supported.

- In Cisco IOS Release 12.2(31)SB2 and later releases, the router supports lawful intercepts with Routed Bridged Encapsulation (RBE) configured on the router (RFC 1483).

Restrictions for Lawful Intercept

Lawful Intercept has the following restriction:

- Lawful Intercept is not supported on Network Management Ethernet (FastEthernet0/0/0) interfaces on the Cisco 10000 series router.
- Lawful Intercept tapping for traffic belonging to IP sessions is not supported on the Cisco 10000 series router.

Interception Using Layer 2 and Layer 3 Taps

The Lawful Intercept feature supports Layer 2 and Layer 3 taps as the following describes:

- Layer 2 taps—Session-based taps that intercept all traffic to and from the session regardless of its Layer 3 content. Layer 2 taps are configured using SNMP version 3 provisioning and RADIUS-based lawful intercepts, and use the CISCO-TAP2-MIB and CISCO-USER-CONNECTION-TAP-MIB.
- Layer 3 taps—Intercepts at the IP layer that are accessible using SNMPv3 provisioning. Layer 3 taps use the CISCO-TAP2-MIB and CISCO-IP-TAP-MIB.

For additional information on Layer 2 and Layer 3 taps, see Table 2-2 on page 2-5.

Initiating SNMPv3 Provisioning Lawful Intercept Requests

SNMPv3 provisioning lawful intercept requests are initiated by the mediation device using SNMPv3 messages, and all traffic data traveling to or from an IP address or session is passed to a mediation device. SNMPv3 provisioning uses the following lawful intercept MIBs:

- CISCO-TAP2-MIB
- CISCO-IP-TAP-MIB
- CISCO-USER-CONNECTION-TAP-MIB

Note For SNMPv3 to provision lawful intercept requests, ensure that session-based taps are done on the LAC.

Lawful Intercept for MLP

The Cisco 10000 series router is a content intercept access point (IAP) in the network. The Lawful Intercept (LI) for MLP feature gives support for Lawful Interception of subscriber traffic over an MLP bundle interface. The support for LI on MLP bundles is restricted only to IPv4 traffic interception.

Using RADIUS to Request Lawful Intercepts

A RADIUS-based lawful intercept solution enables intercept requests to be sent to the NAS or to the LAC from the RADIUS server using Access-Accept packets or CoA-Request packets. All traffic data going to or from a PPP or L2TP session is passed to a mediation device.

An advantage of RADIUS-based lawful intercept is the synchronicity of the solution—the tap is set with Access-Accept packets so that all target traffic is intercepted.

Intercepting Conversations Using 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 Cisco 10000 series router is not a voice gateway device, VoIP packets traverse the router at the edge of the service provider's network. CALEA for Voice is one component of a complete lawful intercept solution, consisting of external monitoring and third-party management devices.

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. Neither the network administrator nor the calling parties is aware that packets are being copied or that the call is being snooped.

Note On a PRE2, CALEA for Voice supports Layer 3 tap functionality, including 32 concurrent taps and 6.1 Mbps (of any traffic) maximum rate without detection.

Network Components Used for Lawful Intercept

The following network components are used for lawful intercepts:

- Mediation Device, page 1-4
- Intercept Access Point, page 1-5
- Collection Program, page 1-5

For information about lawful intercept processing, see the "Lawful Intercept Processing" section on page 1-5.

Mediation Device

A mediation device (supplied by a third-party vendor) manages 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 makes a copy of the intercepted traffic for each LEA. The mediation device is also responsible for restarting any lawful intercepts that are disrupted due to a failure.

Intercept Access Point

An intercept access point (IAP) is a device that provides information for the lawful intercept. The following are two types of IAPs you can use:

- 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). The IRI helps the service provider determine which content IAP (router) the target's traffic passes through.
- Content IAP—A device, such as a Cisco 10000 series router, 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 router continues to forward traffic to its destination to ensure that the wiretap is undetected.
  - Creates a copy of the intercepted traffic, encapsulates it in User Datagram Protocol (UDP) packets, and forwards the packets to the mediation device without the target's knowledge.

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

Collection Program

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

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 admin 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 admin 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 admin function contacts the ID IAP for *intercept related information* (IRI), such as the target's user name and the IP address of their system, to determine which content IAP (router) the target's traffic passes through.
2. After identifying the router that handles the target's traffic, the admin function issues SNMPv3 **get** and **set** requests to the router's MIBs to set up and activate the lawful intercept. The router's MIBs include the CISCO-TAP2-MIB and CISCO-IP-TAP-MIB, and CISCO-USER-CONNECTION-TAP-MIB.

3. During the lawful intercept, the router:
   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.

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

Note When there are multiple lawful intercepts, packet count is based on the mediation device entry and not on individual data streams. For example, lawful intercept is tapping two streams and 1000 packets are sent on each stream. The medication device receives 2000 packets and the packet count for each stream is 2000. When non-hardware tapped packets are routed using the route processor (RP), packet count is according to the stream.

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

CISCO-TAP2-MIB

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

CISCO-TAP2-MIB Contents

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

- cTap2MediationTable—Contains information about each mediation device that is currently running a lawful intercept on the router. Each table entry provides information that the router 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 table also contains counts of the number of packets that were intercepted, and counts of dropped packets which should have been intercepted, but were not.
- cTap2DebugTable—Contains debug information for troubleshooting lawful intercept errors.

The MIB also contains several SNMP notifications for lawful intercept events. For detailed descriptions of MIB objects, see the MIB.

CISCO-TAP2-MIB Processing

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

1. Creates a cTap2MediationTable entry to define how the router 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 router intercepts traffic in the stream until the intercept expires (cTap2MediationTimeout).

CISCO-TAP2-MIB Extension MIB

The CISCO-TAP2-MIB includes the following extension MIBs:

- CISCO-IP-TAP-MIB—intercepts based on IP addresses
- CISCO-USER-CONNECTION-TAP-MIB—RADIUS-based user connection intercepts

Related Information

For additional information on lawful intercept, contact your Cisco account representative.