CHAPTER 2

Configuring Lawful Intercept Support

This chapter describes how to configure lawful intercept (LI). This is necessary to ensure that unauthorized users cannot perform lawful intercepts or access information related to intercepts.

This chapter contains the following sections:

Prerequisites

To configure support for lawful intercept, the following prerequisites must be met:

- You must be logged in to the router with the highest access level (level 15). To log in with level-15 access, enter the **enable** command and specify the highest-level password defined for the router.
- You must issue commands in global configuration mode at the command-line interface (CLI).
- (Optional) It might be helpful to use a loopback interface for the interface through which the router communicates with the mediation device.

Security Considerations

Consider the following security issues as you configure the router for lawful intercept:

- SNMP notifications for lawful intercept must be sent to User Datagram Protocol (UDP) port 161 on the mediation device, not port 162 (which is the Simple Network Management Protocol (SNMP) default). See the "Enabling SNMP Notifications for Lawful Intercept" section on page 2-10 for instructions.

- 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 router. 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
  CISCO-802-TAP-MIB
  CISCO-USER-CONNECTION-TAP-MIB
  SNMP-COMMUNITY-MIB
  SNMP-USM-MIB
  SNMP-VACM-MIB

See the following section ("Configuration Guidelines and Limitations") for additional considerations. Also see the "Prerequisites" section on page 2-1.

Configuration Guidelines and Limitations

This section and the sections that follow describe the general limitations and configuration guidelines for lawful intercept, Cisco 7600-specific guidelines, and per-subscriber guidelines.

- To maintain router performance, lawful intercept is limited to no more than 0.2% of active calls. For example, if the router is handling 4000 calls, 8 of those calls can be intercepted.

  Note In Release 12.2(33)SRC and later releases, the Route Processor Lawful Interface feature supports up to 50 calls, and the Accelerated Lawful Intercept feature supports up to 500 calls.

- The CISCO-IP-TAP-MIB supports the virtual routing and forwarding (VRF) OID citapStreamVRF.

  Note In Releases 12.2(33)SRC and later releases, citapStreamVRF is supported for per-VRF lawful intercept.

- The Cisco 7600 router supports two types of lawful intercept: regular and broadband (per-subscriber). Broadband wiretaps are executed on access subinterfaces and regular wiretaps are executed on all other types of interfaces. The router determines which type of wiretap to execute based on the interface that the target's traffic is using.
- Lawful intercept uses security TCAM, and shares the TCAM resources with other features like RACL. On the edge, where routing is symmetrical, **ifIndex** should be specified for non-access (regular, non-broadband) interfaces.
- Effective with Cisco IOS Release 15.1(3)S4, in RP based LI, taps on the same stream with different port range is accepted. Note that this is accepted only for RP based LI, not for SIP-400 LI.

General Configuration Guidelines

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 FastEthernet0/0/0 interface 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 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.

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 router.

- 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.
- CISCO-802-TAP-MIB—Required for wiretaps on Layer 2 streams. Supported for interface tapping broadband lawful intercept only.
- The CISCO-IP-TAB-MIB imposes limitations on the following features:
  - Optimized access control list (ACL) logging (OAL) and VLAN access control list (VACL) capturing do not work.
  - IDS can not capture traffic on its own, but is only able to capture traffic that has been intercepted by lawful intercept.
- The CISCO-TAP-MIB **citapStreamInterface** -1 is implemented as 0. That means, TAP will be active on every interfaces and this will adversely affect the TCAM utilization.

Cisco 7600 Configuration Guidelines and Limitations

Following is a list of configuration guidelines for regular lawful intercept on Cisco 7600 series routers.

- These guidelines apply to lawful intercept processing on all non-access (subscriber) subinterfaces. For a list of guidelines that apply to wiretaps on individual subscribers, see the "Broadband (Per-Subscriber) Configuration Guidelines and Limitations" section on page 2-4. For guidelines that apply to wiretaps on VPN traffic, see the "Per-VRF Lawful Intercept Configuration Guidelines and Limitations" section on page 2-5.

- Lawful intercept requires a Route Switch Processor 720 (RSP720), a Supervisor Engine 720 (Sup720), or a Supervisor Engine 32 (Sup32) (supports PFC3A, PFC3B, PFC3BXL, PFC3C, and PFC3CXL). In Cisco IOS Release 12.2SRC and later releases, the RSP720-10GE is also supported.

  Note Lawful intercept can intercept traffic at a rate of 6000 packets per second (pps) without affecting the packet forwarding rate. This intercept rate includes all active intercepts and assumes that packets are 150 to 200 bytes long. If the intercept rate exceeds 6000 pps, the packet forwarding rate will decrease slightly because lawful intercept is processor intensive.

- Lawful intercept is supported for IPv4 unicast traffic only. In addition, for traffic to be intercepted, the traffic must be IPv4 on both the ingress and egress interfaces. For example, lawful intercept cannot intercept traffic based on the Multiprotocol Label Switching (MPLS) tag.
- IPv4 multicast, IPv6 unicast, and IPv6 multicast flows are not supported.
- Lawful intercept is not supported on Layer 2 interfaces. However, lawful intercept can intercept traffic on VLANs that run over the Layer 2 interface if the VLAN interface is a Layer 3 interface and traffic is routed by the VLAN interface.
- Lawful intercept is not supported for packets that are encapsulated within other packets (for example, tunneled packets or Q-in-Q packets).
- Lawful intercept is not supported for packets that are subject to Layer 3 or Layer 4 rewrite (for example, Network Address Translation [NAT] or TCP reflexive).
- In the ingress or egress direction, the router intercepts and replicates packets even if the packets are later dropped (for example, due to rate limiting or an ACL deny statement), up to the drop-packet rate-limiter setting (default is 100 pps).
- 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 (LEAs) are using a single mediation device and each is executing a wiretap on the same target, the router sends a single packet to the mediation device. It is up to the mediation device to duplicate the packet for each LEA.
- Lawful intercept on the Cisco 7600 router 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
  - Interface index (Used only during provisioning to select the index to enable lawful intercept on. Not used to identify the target of a lawful intercept tap.)

Broadband (Per-Subscriber) Configuration Guidelines and Limitations

Broadband lawful intercept supports wiretaps on individual subscribers. Following are the guidelines to configure lawful intercept to support wiretaps for individual subscribers:

- Hardware and software requirements:

  - Cisco IOS Release 12.2SRB or later.
  - Cisco 7600 SIP-400 with Gigabit Ethernet (GE) Shared Port Adapters (SPAs), which support individual subscribers configured as access subinterfaces. Lawful intercept is supported on up to ten GE ports, using any combination of 2-port and 5-port GE SPAs.

Note Lawful intercept can also be executed on Cisco 7600 SIP-400 GE interfaces that are not configured as access subinterfaces.

- Per-subscriber wiretaps are supported for both IPv4 and IEEE 802 streams. To enable support for both types of streams, you must add the CISCO-IP-TAP-MIB and CISCO-802-TAP-MIB to the lawful intercept SNMP view.
- Up to 20 intercepts can be active at a time without affecting the router packet forwarding rate. In addition, up to 200 intercepts can be configured simultaneously, but in a disabled state. If the intercept rate exceeds this rate, the packet forwarding rate will decrease slightly because lawful intercept is processor intensive.
- Lawful intercept processing is performed in the egress direction after security ACLs and Quality of Service (QoS) features have been applied to the subscriber traffic. This way, lawful intercept does not replicate traffic that was dropped by these features. In the ingress direction, lawful intercept is performed before security ACLs and QoS features have been applied.
- Stateful SwitchOver (SSO) and NonStop Forwarding (NSF) are not supported for wiretaps. When a switchover occurs between the active and standby supervisor engines, information about active wiretaps is deleted.
- Statistics for subscriber wiretaps are maintained by the Cisco 7600 SIP-400.
- After online insertion and removal (OIR), all wiretap counters are cleared.

Per-VRF Lawful Intercept Configuration Guidelines and Limitations

Per-VRF lawful intercept is the ability to provision a lawful intercept wiretap on IPv4 data in a particular VPN. This allows a Law Enforcement Agency to lawfully intercept targeted data within that VPN. Only IPv4 data within that VPN is subject to the VRF-based LI tap.

Note Per-VRF lawful intercept is available in Cisco IOS Release 12.2SRC and later releases.

Per-VRF LI is available for the following types of traffic:

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

Note MPLS is supported only in Release 12.2(33)SRC and later releases.

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 virtual routing and forwarding (VRF) table that the targeted VPN uses. The VRF name is used to select the VPN interfaces to enable LI on 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.

Requirements and Limitations

The same limitations and restrictions that apply to normal lawful intercept also apply to per-VRF LI. In addition, the following requirements and limitations exist for per-VRF LI:

- Lawful intercept supports up to 1000 VRFs or interfaces.
- To determine which VRF to use for a VPN-based tap, the router performs recirculation using the ACL ternary content addressable memory (TCAM). To accommodate recirculation, the following hardware resources are required:
  - Two internal VLANs per VRF (one for ingress traffic and one for egress).
  - An internal VLAN is required for each interface where a VPN-based tap is being executed if the interface has ingress features whose adjacency results might conflict those of LI. See the next section for a list of features that use ACL TCAM recirculation.

  Note The above internal VLANs are taken from the total number of internal VLANs available per router (4096), which limits the number of VPN-based LI taps that the router can execute at a time.
- When an interface that belongs to a VPN is configured for per-VRF LI, policy-based routing (PBR), or ingress Web Cache Communication Protocol (WCCP) ACL TCAM entries that use adjacency results will be set to the LI recirculation adjacency. While the adjacency results are rewritten, traffic flow might be temporarily interrupted.
- Recirculation can sometimes result in a VPN-based LI tap intercepting traffic that ends up being dropped by the router.
- If a VPN-based tap is executed on a pair of ingress and egress interfaces that both belong to the same VPN, any IP-to-IP traffic passing through the interfaces will be intercepted twice. This results in duplicate packets being sent to the mediation device.

Interaction with Other Features

Because per-VRF LI uses redirection adjacency results to determine the ingress ACL result, there might be potential conflicts with other features that also use adjacency results. The following IP ACL features currently use recirculation adjacency results:

- DHCP snooping
- IP recirculation
- PBR
- Reverse path forwarding (RPF)
- Server load balancing (SLB)
- WCCP

Using the Cisco 7600 SIP-400 as Lawful Intercept Service Module

The Cisco 7600 SIP-400 can be used to implement the same LI functionality as is performed by the route processor on the Cisco 7600 series router. With the SIP-400 in the chassis, the intercept packet processing is off-loaded from the route processor to the SIP-400, and the route processor no longer looks for LI packets.

This feature is implemented by specifying a list of SIP-400 modules that can be used for LI processing. When lawful intercept is initiated, the first SIP-400 on the list is used. If the currently active module becomes inactive, the list is scanned again to find a new active module to use. If no SIP-400 modules are active, the route processor assumes the LI functionality. When a listed SIP-400 again becomes active, the LI function automatically reverts to the SIP-400.

Configuration Guidelines and Restrictions

The following are guidelines and limitations related to using the Cisco 7600 SIP-400 as a lawful intercept device:

- Router provisioning to enable LI is accomplished, as usual, through SNMPv3.
- The SIP-400 may or may not have interfaces installed.
  - If there are interfaces installed in the SIP-400, the additional traffic generated by the LI feature may affect traffic flow through the SIP-400.
  - If there are no interfaces installed, the SIP-400 acts only as an LI service module.
  - If there is more than one SIP-400 in the chassis, only one SIP-400 can be configured as a service module.
- During a SIP-400 online insertion and removal, the route processor handles the LI traffic until the SIP-400 is replaced in the chassis.
- Intercepted packets are treated as high-priority packets.
- The SIP-400 supports up to 500 taps.
- The SIP-400 supports only UDP as the content delivery protocol.
- Only routed packets (IPv4 unicast and multicast traffic) are supported. Intercept of IPv6 packets is not supported.
- VLAN-based intercept is not supported.

Selecting the SIP-400

To select the list of SIP-400s to use as lawful intercept modules, perform the following tasks in global configuration mode:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# li-slot slot-list slot1, slot2, ... rate value`	Selects the location of the SIP-400 modules to be used as LI devices. **rate** *value* valid range is 1000 to 1000000 pps.
Step 3	`Router(config)# show li slot`	Verifies the location of all SIP-400 modules to be used.

Accessing the Lawful Intercept MIBs

Due to its sensitive nature, the Cisco lawful intercept MIBs are only available in software images that support the lawful intercept 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 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 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.

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 router. To access the MIB, users must have level-15 access rights on the router.

Configuring SNMPv3

To perform the following procedures, SNMPv3 must be configured on the router. For information about how to configure SNMPv3, and for detailed information about the commands described in the sections that follow, see the following Cisco documents:

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Part 3: System Management, "Configuring SNMP Support" section, available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm

- *Cisco IOS Configuration Fundamentals and Network Management Command Reference*, available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/cfr_1g11.htm

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 following procedure at the CLI, in global configuration mode with level-15 access rights. For command examples, see the "Configuration Example" section on page 2-10.

Note The command syntax in the following steps includes only those keywords required to perform each task. For details on command syntax, see the documents listed in the previous section ("Configuring SNMPv3").

Step 1 Make sure that SNMPv3 is configured on the router. For instructions, see the documents listed in the "Configuring SNMPv3" section on page 2-8.

Step 2 Create an SNMP view that includes the CISCO-TAP2-MIB (where *view_name* is the name of the view to create for the MIB). This MIB is required for both regular and broadband lawful intercept.

```
Router(config)# snmp-server view view_name ciscoTap2MIB included
```

Step 3 Add one or both of the following MIBs to the SNMP view to configure support for wiretaps on IPv4 and 802 streams (where *view_name* is the name of the view you created in Step 2).

```
Router(config)# snmp-server view view_name ciscoIpTapMIB included
Router(config)# snmp-server view view_name ciscoTap802MIB included
```

Step 4 Create an SNMP user group (*groupname*) that has access to the lawful intercept MIB view and define the group's access rights to the view.

```
Router(config)# snmp-server group groupname v3 noauth read view_name write view_name
```

Step 5 Add users to the user group you just created (where *username* is the user, *groupname* is the user group, and *auth_password* is the authentication password):

```
Router(config)# snmp-server user username groupname v3 auth md5 auth_password
```

Note Be sure to add the mediation device to the SNMP user group; otherwise, the router cannot perform lawful intercepts. Access to the lawful intercept MIB view should be restricted to the mediation device and to system administrators who need to know about lawful intercepts on the router.

The mediation device is now able to access the lawful intercept MIBs, and issue SNMP **set** and **get** requests to configure and run lawful intercepts on the router.

For instructions on how to configure the router to send SNMP notifications to the mediation device, see the "Enabling SNMP Notifications for Lawful Intercept" section on page 2-10.

Configuration Example

The following commands show an example of how to enable the mediation device to access the lawful intercept MIBs.

```
Router(config)# snmp-server view tapV ciscoTap2MIB included
Router(config)# snmp-server view tapV ciscoIpTapMIB included
Router(config)# snmp-server view tapV ciscoTap802MIB included
Router(config)# snmp-server group tapGrp v3 noauth read tapV write tapV notify tapV
Router(config)# snmp-server user ss8user tapGrp v3 auth md5 ss8passwd
Router(config)# snmp-server engineID local 1234
```

1. Create a view (tapV) that includes the appropriate lawful intercept MIBs (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, CISCO-802-TAP-MIB, and CISCO-USER-CONNECTION-TAP-MIB).
2. Create a user group (tapGrp) that has read, write, and notify access to MIBs in the tapV view.
3. Add the mediation device (ss8user) to the user group, and specify MD5 authentication with a password (ss8passwd).
4. (Optional) Assign a 24-character SNMP engine ID (for example, 123400000000000000000000) to the router for administration purposes. If you do not specify an engine ID, one is automatically generated. Note that you can omit the trailing zeros from the engine ID, as shown in the last line of the example above.

Note Changing an engine ID has consequences for SNMP user passwords and community strings.

Enabling SNMP Notifications for Lawful Intercept

SNMP automatically generates notifications for lawful intercept events (see Table 2-1). This is because the default value of the cTap2MediationNotificationEnable object is true(1).

To configure the router to send lawful intercept notifications to the mediation device, issue the following CLI commands in global-configuration mode with level-15 access rights (where *MD-ip-address* is the IP address of the mediation device and *community-string* is the password-like community string to send with the notification request):

```
Router(config)# snmp-server host MD-ip-address community-string udp-port 161 snmp
Router(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart
warmstart
```

- For lawful intercept, **udp-port** must be 161 and not 162 (the SNMP default).
- The second command configures the router to send RFC 1157 notifications to the mediation device. These notifications indicate authentication failures, link status (up or down), and router restarts.

Table 2-1 lists the SNMP notifications generated for lawful intercept events.

Table 2-1 SNMP Notifications for Lawful Intercept Events

Notification	Meaning
cTap2MIBActive	The router is ready to intercept packets for a traffic stream configured in the CISCO-TAP2-MIB.
cTap2MediationTimedOut	A lawful intercept was terminated (for example, because cTap2MediationTimeout expired).
cTap2MediationDebug	Intervention is required for events related to cTap2MediationTable entries.
cTap2StreamDebug	Intervention is required for events related to cTap2StreamTable entries.

Disabling SNMP Notifications

You can disable SNMP notifications on the router as follows:

- To disable all SNMP notifications, issue the **no snmp-server enable traps** command.
- 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).