CHAPTER 2

Configuring Lawful Intercept Support

This chapter describes how to configure lawful intercept. 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 for Lawful Intercept

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 UDP port 161 on the mediation device, not port 162 (which is the SNMP default). See the "Enabling SNMP Notifications for Lawful Intercept" section on page 2-5 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-USER-CONNECTION-TAP-MIB
  SNMP-COMMUNITY-MIB
  SNMP-USM-MIB
  SNMP-VACM-MIB

For additional information, see the "Restrictions and Limitations" section on page 2-2 and the "Prerequisites for Lawful Intercept" section on page 2-1.

Restrictions and Limitations

- The router does not support L2TP LNS sessions for RADIUS-based lawful intercept.
- To maintain router performance, lawful intercept is limited to no more than .2% of active calls. For example, if the router is handling 4000 calls, 8 of those calls can be intercepted.
- Cisco IOS Release 12.2(31)SB supports virtual routing and forwarding (VRF) aware IP taps using the citapStreamVRF OID in the CISCO-IP-TAP-MIB on the PRE2 and PRE3.
- The PRE1 does not support lawful intercepts.
- Voice and data interception are supported in Cisco IOS Release 12.2(7)XI and later releases.
- The tapping of multicast packets is achieved using Layer 3 intercepts, except where the target identity is the MAC address.
- In Cisco IOS Release 12.2(28)SB, the PXF processes Layer 2 intercepts and the RP processes Layer 3 intercepts.
- In Cisco IOS Release 12.2(31)SB, the PXF processes both PRE2 and PRE3 Layer 3 intercepts.

Table 2-1 describes the lawful intercept capabilities of Cisco IOS software.

Table 2-1 Lawful Intercept Feature Implementation

Cisco IOS Release	Tap Type	Tap Capacity	PRE	MIB	RP/PXF[1]
Release 12.3(7)XI	Layer 3 SNMPv3	Total of 6.4 Mbps for all active taps	PRE2	CISCO-TAP-MIB	RP
Release 12.2(28)SB	Layer 2 RADIUS	4095 concurrent taps	PRE2	CISCO-TAP2-MIB	PXF
	Layer 3 SNMPv3	Total of 6.4 Mbps for all active taps	PRE2		RP
Release 12.2(31)SB	Layer 2 RADIUS	4095 concurrent taps	PRE2, PRE3	CISCO-TAP2-MIB	PXF
	Layer 3 SNMPv3	4095 concurrent taps	PRE2, PRE3		PXF

1. Each intercepted packet is processed by the route processor (RP) or parallel express forwarding (PXF) engine.

Configuration Notes

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.

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-TAP2-MIB and CISCO-IP-TAP-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:

- Creating a Restricted SNMP View that Includes the Lawful Intercept MIBs, page 2-4

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/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html

- "SNMP Commands" in the *Cisco IOS Network Management Command Reference*, available at the following URL:

  http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

Creating a Restricted SNMP View that Includes the 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. After completing this procedure, the mediation device is able to access the Lawful Intercept MIBs, and issue SNMP **set** and **get** requests to configure and run lawful intercepts on the router.

Step 1 Make sure that SNMPv3 is configured on the router. For instructions, see the documents listed in the "Configuring SNMPv3" section on page 2-4

Step 2 Create an SNMP view that includes the CISCO-TAP2-MIB and CISCO-IP-TAP-MIB (where *view_name* is the name of the view to create for the MIB).

```
Router(config)# snmp-server view view_name cTap2MIB included
```

Step 3 Create an SNMP user group that has access to the CISCO-TAP2-MIB and CISCO-IP-TAP-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 4 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 user group; otherwise, the router cannot perform lawful intercepts. Access to the CISCO-TAP2-MIB view should be restricted to the mediation device and to system administrators who need to know about lawful intercepts on the router.

The command syntax in the above procedure includes only those keywords required to perform each task. For information on command syntax, see the documents listed in the "Configuring SNMPv3" section on page 2-4.

For instructions on how to configure the router to send SNMP notifications to the mediation device, go to the "Enabling SNMP Notifications for Lawful Intercept" section on page 2-5.

Configuration Example

The following commands show an example of how to enable the mediation device to access the Lawful Intercept Tap MIBs. Note that the **snmp-server group** command format is for a router with a PRE2 card.

```
Router(config)# snmp-server view tapV cTap2MIB 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 engineid-string
```

1. Create a view (tapV) that includes the CISCO-TAP2-MIB and CISCO-IP-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 to the router for administration purposes. If you do not specify an engine ID, one is automatically generated. Note that 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 2-2). 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 2-2 lists the MIB notifications generated for lawful intercept events.

Table 2-2 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.
cTap2Switchover	A redundant, active route processor (RP) is going into standby mode and the standby is the active RP.

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).