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

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

- You must be running images that support secure shell (SSH), for example, the image s72033-adventerprisek9-mz. Lawful intercept is not supported on images that do not support SSH.
- You must be logged in to the Catalyst 6500 series switch 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 Catalyst 6500 series switch.
- You must issue commands in global configuration mode at the command-line interface (CLI). You can configure lawful intercept globally on all interfaces or on a specific interface.
- Lawful intercept is supported on Catalyst 6500 series switches configured with a Supervisor Engine 720 or the Supervisor Engine 720-10GE (supports PFC3A, PFC3B, PFC3BXL, PFC3C, and PFC3CXL).
- The time of day on the Catalyst 6500 series switches and the mediation device must be synchronized; we suggest that you use Network Time Protocol (NTP) on both the Catalyst 6500 series switches and the mediation device.
- (Optional) It might be helpful to use a loopback interface for the interface through which the Catalyst 6500 series switch communicates with the mediation device. If you do not use a loopback interface, you must configure the mediation device with multiple physical interfaces on the Catalyst 6500 series switch to handle network failures.

Security Considerations

Consider the following security issues as you configure the Catalyst 6500 series switch 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 2-7 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 Catalyst 6500 series switch. 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

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, Catalyst 6500 series switch-specific guidelines, and per-subscriber guidelines.

- If the network administrator expects lawful intercept to be deployed at a node, you should not configure optimized ACL logging (OAL), VLAN access control list (VACL) capture, and Intrusion Detection System (IDS) at the node. Deploying lawful intercept at the node causes unpredictable behavior in OAL, VACL capture, and IDS.
- To maintain Catalyst 6500 series switch performance, lawful intercept is limited to no more than 0.2% of active calls. For example, if the Catalyst 6500 series switch is handling 4000 calls, 8 of those calls can be intercepted.
- The CISCO-IP-TAP-MIB does not support the virtual routing and forwarding (VRF) OID citapStreamVRF.
- Captured traffic is rate limited to protect the CPU usage at the route processor. The rate limit is 8500 pps.
- The interface index is used during provisioning to select the index to enable lawful intercept on only; when set to 0, lawful intercept is applied to all interfaces.

General Configuration Guidelines

For the Catalyst 6500 series switch to communicate with the mediation device to execute a lawful intercept, the following configuration requirements must be met:

- (Optional) The domain name for both the Catalyst 6500 series switch and the mediation device may be registered in the Domain Name System (DNS).

  In DNS, the Catalyst 6500 series switch IP address is typically the address of the FastEthernet0/0/0 interface on the Catalyst 6500 series switch.
- The mediation device must have an access function (AF).
- 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 include the mediation device's authorization password. 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 Catalyst 6500 series switch.

- 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.

    The feature starts 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 only.

Configuration Guidelines and Limitations

The following is a list of configuration guidelines for lawful intercept on Catalyst 6500 series switches. This list applies to lawful intercept processing on all non-access (subscriber) subinterfaces.

- Requires a Supervisor Engine 720 or a Supervisor Engine 720-10GE (supports PFC3A, PFC3B, PFC3BXL, PFC3C, and PFC3CXL).

Note We recommend that you dedicate an interface for lawful intercept processing. For example, you should not configure the interface to perform processor-intensive tasks such as QoS or routing.

- 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 if the egress side is MPLS and the ingress side is IPv4.
- IPv4 multicast, IPv6 unicast, and IPv6 multicast flows are not supported.
- Not supported on Layer 2 interfaces. However, lawful intercept can intercept traffic on VLANs that run over the Layer 2 interface.
- Not supported for packets that are encapsulated within other packets (for example, tunneled packets or Q-in-Q packets).
- Not supported for Q-in-Q packets. There is no support for Layer 2 taps for lawful intercept.
- 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 direction, the Catalyst 6500 series switch 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). In the egress direction, packets are not replicated if they are dropped (for example, by ACL).
- Lawful intercept ACLs are applied internally to both the ingress and the egress directions of an interface.
- To intercept traffic from a specific user, a typical configuration consists of two flows, one for each direction.
- 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 LEAs are using a single mediation device and each is executing a wiretap on the same target, the Catalyst 6500 series switch 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 Catalyst 6500 series switch 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

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 Catalyst 6500 series switch 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 Catalyst 6500 series switch. To access the MIB, users must have level-15 access rights on the Catalyst 6500 series switch.

Configuring SNMPv3

To perform the following procedures, SNMPv3 must be configured on the Catalyst 6500 series switch. 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

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

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/ffun_r.html

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 2-6.

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 Catalyst 6500 series switch. For instructions, see the documents listed in the "Configuring SNMPv3" section on page 2-5.

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 streams (where *view_name* is the name of the view you created in Step 2).

```
Router(config)# snmp-server view view_name ciscoIpTapMIB 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 Catalyst 6500 series switch 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 Catalyst 6500 series switch.

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 Catalyst 6500 series switch.

For instructions on how to configure the Catalyst 6500 series switch to send SNMP notifications to the mediation device, see the "Enabling SNMP Notifications for Lawful Intercept" section on page 2-7.

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
```

1. Create a view (tapV) that includes the appropriate lawful intercept MIBs (CISCO-TAP2-MIB and the 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 (for example, 123400000000000000000000) to the Catalyst 6500 series switch 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 Catalyst 6500 series switch 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 Catalyst 6500 series switch to send RFC 1157 notifications to the mediation device. These notifications indicate authentication failures, link status (up or down), and system 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 Catalyst 6500 series switch 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 by entering 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 reenable lawful intercept notifications through SNMPv3, reset the object to true(1).