Catalyst 6500 Series Switches Lawful Intercept Configuration Guide

Cisco IOS Software Release 12.2(33)SXH and later releases

August 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-14149-01

CONTENTS

Preface

This guide describes the implementation of the Lawful Intercept feature on Catalyst 6500 series switches.

Lawful intercept is a process that enables a Law Enforcement Agency (LEA) to perform electronic surveillance on an individual as authorized by a court order. To assist in the surveillance, the service provider intercepts the target's traffic as it passes through one of their routers, and sends a copy of the intercepted traffic to the LEA without the target's knowledge.

Audience

This guide is intended for system administrators who must configure the router to support lawful intercept. This guide may also be useful for application developers who are developing management applications for use with lawful intercept.

Organization

This guide contains the following chapters:

- Chapter 1, "Lawful Intercept Overview," provides background information about lawful intercept and its implementation. It also describes the CISCO-TAP2-MIB and CISCO-IP-TAP-MIB, which are used for lawful intercept. A Management Information Base (MIB) enables the router to be controlled through the Simple Network Management Protocol (SNMP).
- Chapter 2, "Configuring Lawful Intercept Support," provides instructions for configuring the router to support lawful intercept.

Document Conventions

In this guide, command descriptions use these conventions:

boldface font	Commands, user entry, and keywords appear in **bold**.
italic font	Arguments for which you supply values and new terms appear in *italics*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.

Examples use these conventions:

`screen` font	Terminal sessions and information the system displays are in `screen` font.
`bold screen` font	Information you must enter is in **`bold screen`** font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.

Notes and cautions use these conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Lawful Intercept Overview

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

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 switchs 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.

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 date 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

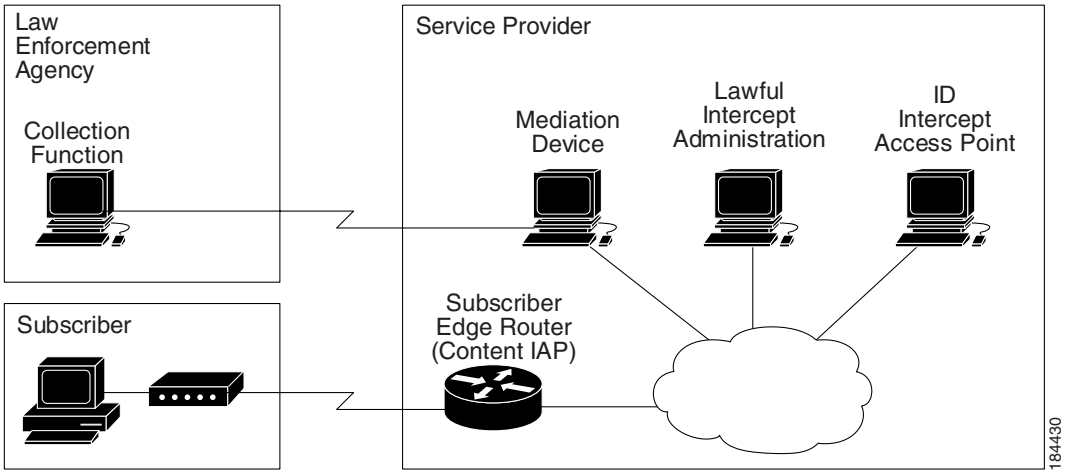
The following network components are used for lawful intercepts:

- 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.

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.

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.

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).

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.

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).

INDEX

L

M

N

P

R

S

T

U

W