



Cisco 10000 Series Router Lawful Intercept Configuration Guide

May 2008

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-3426-05

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Cisco 10000 Series Router Lawful Intercept Configuration Guide
Copyright © 2004-2009 Cisco Systems, Inc. All rights reserved.



CONTENTS

About This Guide v

Guide Revision History -v

Audience -v

Organization -v

Document Conventions -vi

CHAPTER 1

Lawful Intercept Overview 1-1

Information About Lawful Intercept 1-1

Feature History for Lawful Intercept 1-2

Benefits of Lawful Intercept 1-2

Interception Using Layer 2 and Layer 3 Taps 1-3

Initiating SNMPv3 Provisioning Lawful Intercept Requests 1-3

Lawful Intercept for MLP 1-3

Using RADIUS to Request Lawful Intercepts 1-4

Intercepting Conversations Using CALEA for Voice 1-4

Network Components Used for Lawful Intercept 1-4

Mediation Device 1-4

Intercept Access Point 1-5

Collection Program 1-5

Lawful Intercept Processing 1-5

CISCO-TAP2-MIB 1-6

Related Information 1-7

CHAPTER 2

Configuring Lawful Intercept Support 2-1

Prerequisites for Lawful Intercept 2-1

Security Considerations 2-1

Restrictions and Limitations 2-2

Configuration Notes 2-3

Accessing the Lawful Intercept MIBs 2-3

Restricting Access to the Lawful Intercept MIBs 2-3

Configuring SNMPv3 2-4

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

Configuration Example 2-5

Enabling SNMP Notifications for Lawful Intercept 2-5
Disabling SNMP Notifications 2-6

INDEX



About This Guide

This guide describes the implementation of the lawful intercept feature on a Cisco 10000 series router. 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.

Guide Revision History

Cisco IOS Release	Part Number	Publication Date	Description
Release 12.2(31)SB12	OL-3426-05	May 2008	Added the Lawful Intercept for MLP feature.
Release 12.2(31)SB2	OL-3426-04	March, 2008	Updated Lawful Intercept restrictions.
Release 12.2(31)SB2	OL-3426-03	November, 2006	Added new MIB support information.
Release 12.2(28)SB2	OL-3426-02	June, 2006	Added history tables and configuration information.
Release 12.3(7)XI	OL-3426-01	2004	Initial release

Audience

This guide is intended for system administrators who must configure a 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. This chapter also describes the CISCO-TAP2-MIB, which is 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.

- Index

Document Conventions

In this guide, command descriptions use these conventions:

boldface font	Commands, user entry, and keywords appear in bold .
<i>italic font</i>	Arguments for which you supply values and new terms appear in <i>italics</i> .
[]	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 <code>screen font</code> .
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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Lawful Intercept Overview

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

- [Information About Lawful Intercept, page 1-1](#)
- [CISCO-TAP2-MIB, page 1-6](#)
- [Related Information, page 1-7](#)



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 PPPoX 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).

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.



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, page 2-1](#)
- [Security Considerations, page 2-1](#)
- [Restrictions and Limitations, page 2-2](#)
- [Configuration Notes, page 2-3](#)
- [Accessing the Lawful Intercept MIBs, page 2-3](#)
- [Configuring SNMPv3, page 2-4](#)
- [Enabling SNMP Notifications for Lawful Intercept, page 2-5](#)

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/fc014.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)`.



## INDEX

---

### A

- access, restricting CISCO-TAP2-MIB [2-3](#)
- access setup, example [2-5](#)
- activating lawful intercept [1-7](#)
- admin function (mediation device) [1-7](#)

---

### C

- CALEA, See Communications Assistance for Law Enforcement Act (CALEA)
- CISCO-TAP2-MIB
  - accessing [2-3](#)
  - overview [1-7](#)
  - restricting access to [2-3, 2-4](#)
- collection function [1-5](#)
- Communications Assistance for Law Enforcement Act
  - CALEA for voice [1-4](#)
  - lawful intercept [1-1](#)
- configuring
  - lawful intercept [2-4, 2-5, 2-6](#)
  - SNMP [2-4](#)
- content IAP [1-5](#)
- cTap2MediationDebug notification [2-5](#)
- cTap2MediationNewIndex object [1-7](#)
- cTap2MediationTable [1-7](#)
- cTap2MediationTimedOut notification [2-5](#)
- cTap2MIBActive notification [2-5](#)
- cTap2StreamDebug notification [2-5](#)
- cTap2StreamIpTable [1-7](#)
- cTap2Switchover notification [2-5](#)

---

### D

- DNS, See Domain Name System
- Domain Name System [2-3](#)

---

### E

- electronic traffic, monitoring [1-5](#)
- enabling
  - lawful intercept [1-7](#)
  - SNMP notifications [2-5](#)

---

### G

- get requests [1-7](#)

---

### I

- ID IAP [1-5](#)
- intercept access point (IAP) [1-5](#)
- intercept related information (IRI) [1-5](#)

---

### L

- Law Enforcement Agency (LEA) [1-1](#)
- lawful intercept
  - admin function [1-7](#)
  - collection function [1-5](#)
  - configuring [2-4, 2-5, 2-6](#)
  - enabling [1-7](#)
  - IAP [1-5](#)
  - IPv4 [1-3](#)
  - IPv6 [1-2](#)

IRI [1-5](#)  
 LI on MLP [1-3](#)  
 mediation device [1-4](#)  
 overview [1-1, 1-2](#)  
 prerequisites [2-1](#)  
 processing [1-5, 1-6](#)  
 security considerations [2-1](#)  
 SNMP notifications [2-5](#)

Layer 3, taps [1-4](#)

---

## M

mediation device

admin function [1-7](#)  
 description [1-4](#)

MIBs

CISCO-TAP2-MIB [1-7, 2-3](#)  
 SNMP-COMMUNITY-MIB [2-2](#)  
 SNMP-USM-MIB [1-2, 2-2](#)  
 SNMP-VACM-MIB [1-2, 2-2](#)

monitoring electronic traffic [1-5](#)

---

## N

notifications, See SNMP notifications

---

## P

prerequisites for lawful intercept [2-1](#)  
 privileged users [2-1](#)

---

## R

RADIUS-based lawful intercept [1-4](#)  
 rate, maximum without detection [1-4](#)  
 restricting CISCO-TAP2-MIB access [2-3](#)  
 CISCO-TAP2-MIB [2-4](#)

---

## S

security considerations [2-1](#)  
 set requests [1-7](#)  
 setting up lawful intercept [1-5](#)

SNMP

configuring [2-4](#)  
 default view [2-2](#)  
 get and set requests [1-7](#)  
 get requests [1-7](#)  
 notifications [2-1, 2-5](#)  
 set requests [1-7](#)

SNMP-COMMUNITY-MIB [2-2](#)

SNMP-USM-MIB [1-2, 2-2](#)

SNMP-VACM-MIB [1-2, 2-2](#)

standards, lawful intercept [1-1](#)

surveillance [1-5](#)

---

## T

taps, concurrent [1-4](#)  
 traps, see SNMP notifications

---

## U

UDP port for SNMP notifications [2-5](#)

---

## W

wiretaps [1-1](#)