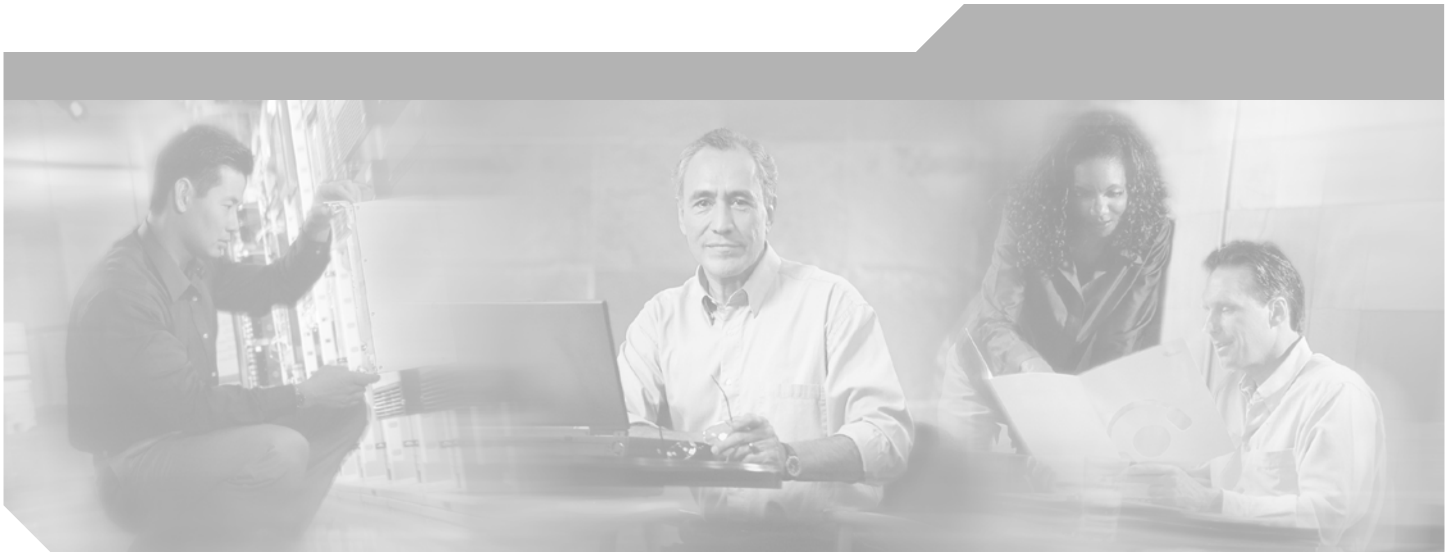

Cisco 10000 Series Router Lawful Intercept Configuration Guide

Software Release 12.2(31)SB2
Version 3.0
November 2006

Corporate 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: 408 526-4100

Text Part Number: OL-3426-03

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.

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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0609R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Lawful Intercept Configuration Guide

CONTENTS

About This Guide

This guide describes the implementation of the lawful intercept feature on the 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)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 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. 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**.
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

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide,* go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Lawful Intercept Overview

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

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 ID 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 Cisco's lawful intercept solution, contact your Cisco account representative.

Feature History for Lawful Intercept

Cisco IOS Release	Description
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(28)SB2	This feature was integrated in Cisco IOS Release 12.2(28)SB2.
Release 12.2(31)SB2	This feature was enhanced to include the CISCO-USER-CONNECTION-TAP-MIB and integrated into Cisco IOS Release 12.2(31)SB2.

Refer to Table 2-1 on page 2-22 for details on lawful intercept capabilities by Cisco IOS release.

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.
- In Cisco IOS Release 12.2(31)SB2 and later releases, intercept taps are supported on the following PPPo*X* sessions using Layer 2 RADIUS-based taps:
  - PPPoA
  - PPPoE
  - PPPoEoA
  - PPPoEoVLAN
  - PPPoEoQinQ

- In Cisco IOS Release 12.2(31)SB2 and later releases, lawful intercepts are supported when Routed Bridged Encapsulation (RBE) is configured on the router (RFC 1483).

Layer 2 and Layer 3 Taps

The Lawful Intercept feature supports Layer 2 and Layer 3 taps.

- 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 via SNMPv3 provisioning and RADIUS-based lawful intercepts. Layer 2 taps use the CISCO-TAP2-MIB and CISCO-USER-CONNECTION-TAP-MIB.
- Layer 3 taps—Intercepts at the IP layer that are accessible via 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, refer to Table 2-1 on page 2-22.

SNMPv3 Provisioning Lawful Intercept

SNMPv3 provisioning lawful intercept requests are initiated by the mediation device via SNMPv3 messages, and all traffic data going to or from a given 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

RADIUS-Based Lawful Intercept

A RADIUS-based lawful intercept solution enables intercept requests to be sent (via Access-Accept packets or CoA-Request packets) to the NAS or to the LAC from the RADIUS server. All traffic data going to or from a PPP or L2TP session is passed to a mediation device. Another 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.

For more information about RADIUS-Based Lawful Intercept, see the *RADIUS-Based Lawful Intercept, Release 12.2(28)SB feature module* located at the following URL:

http://www.cisco.com/en/US/products/ps6566/products_feature_guide09186a008060de94.html

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 non-Cisco 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 1-16
- Intercept Access Point, page 1-16
- Collection Function, page 1-17

For information about lawful intercept processing, see the "Lawful Intercept Processing" section on page 1-17.

Mediation Device

A mediation device (supplied by 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.

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). 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 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.

Collection Function

The collection function is a program that stores and processes traffic intercepted by the service provider. The program runs on equipment at the 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 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, 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.

   Note 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 mediation 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 MIBs

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.

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 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 2-25 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

See the "Restrictions and Limitations" section on page 2-22 for additional considerations. Also see the "Prerequisites" section on page 2-21.

Restrictions and Limitations

- 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)SB2 supports VRF-aware IP taps using the citapStreamVRF OID in the CISCO-IP-TAP-MIB. VRF-based interception is in the PXF and supported on the PRE2 and PRE3.
- Cisco IOS Release 12.2(28)SB does not support VRF-aware lawful intercept.
- Lawful intercepts are not supported on a PRE1.
- Voice and data interception are supported in Cisco IOS Release 12.2(7)XI and later releases.
- Tapping of multicast packets is achieved using Layer 3 intercepts, except where the target identity is the MAC address.
- Taps are not allowed on subnets that span multiple routes in the route table.

Table 2-1 describes the lawful intercept capabilities by Cisco IOS release.

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 6.4Mbps 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 6.4Mbps for all active taps	PRE2		RP
Release 12.2(31)SB2	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).

In summary, IOS Release 12.2(28)SB Layer 2 intercepts are processed by the PXF and Layer 3 intercepts are processed by the RP. In IOS Release 12.2(31)SB2, both PRE2 and PRE3 Layer 3 intercepts are processed by the PXF.

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 view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

Configuring SNMPv3

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

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

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm
- *Cisco IOS Configuration Fundamentals Command Reference*, Part 3: Cisco IOS System Management Commands, "SNMP Commands" section, available at the following URL:

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

Creating a Restricted SNMP View 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. For command examples, see the "Configuration Example" section on page 2-25.

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 "Configuring SNMPv3" section on page 2-23.

Step 1 Make sure that SNMPv3 is configured on the router. For instructions, see the documents listed in the "Configuring SNMPv3" section on page 2-23

Step 2 Create an SNMP view that includes the CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, and CISCO-USER-CONNECTION-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 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 mediation device is now able to access the Lawful Intercept MIBs, and issue SNMP **set** and **get** requests to configure and run lawful intercepts on the router.

For instructions on how to configure the router to send SNMP notifications to the mediation device, go to the "Enabling SNMP Notifications for Lawful Intercept" section on page 2-25.

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.
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