Lawful Intercept Architecture

Last Updated: January 18, 2012

The Lawful Intercept (LI) feature supports service providers in meeting the requirements of law enforcement agencies to provide the ability to intercept Voice-over-Internet protocol (VoIP) or data traffic going through the edge routers (or other network locations). This document explains LI architecture, including Cisco Service Independent Intercept architecture and PacketCable Lawful Intercept architecture. It also describes the components of the LI feature and provides instructions on how to configure the LI feature in your system.

- Finding Feature Information, page 1
- Prerequisites for Lawful Intercept, page 1
- Restrictions for Lawful Intercept, page 2
- Information About Lawful Intercept, page 2
- How to Configure Lawful Intercept, page 6
- Configuration Examples for Lawful Intercept, page 14
- Additional References, page 16
- Feature Information for Lawful Intercept, page 17

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Lawful Intercept

Access to the Cisco LI 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.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Communication with Mediation Device

For the router to communicate with the mediation device to execute a lawful intercept, the following configuration requirements must be met:

- The mediation device must have an administrative function (AF) and an administrative function provisioning interface (AFPI).
- You must add the mediation device to the Simple Network Management Protocol (SNMP) user group that has access to the CISCO-TAP2-MIB view.

Use the **snmp-server user** command, specifying the mediation device username and password, to add the mediation device to an SNMP user group, then use the **snmp-server group** command to associate the group with a view that includes the CISCO-TAP2-MIB and one or more optional MIBS, such as CISCO-IP-TAP-MIB.

When you add the mediation device as a CISCO-TAP2-MIB user, you can include the mediation device authorization password if you want. The password must be at least eight characters in length.

- The time of day on both the router and the mediation device must be set to the same value.

To synchronize the time settings, ensure that Network Time Protocol (NTP) is running on both the router and mediation device.

- The security level on both the router and the mediation device must be set to identical values. The minimum security level required for the LI feature is “auth”.

If encryption of SMNP messages is required (optional), set the security level to “priv”.

Restrictions for Lawful Intercept

General Restrictions

- To maintain router performance, LI is limited to no more than .25% of traffic. For example, if the router is handling 10 Gbps, then the average tap rate is 25 Mbps. If the average packet size is 200 b, then the packet-per-second rate would be 16 kpps.
- There is no command-line interface (CLI) available to configure LI on the router. All error messages are sent to the mediation device as SNMP notifications. All intercepts are provisioned using SNMPv3 only.

Cisco ASR 1000 Series Routers

- Cisco ASR 1000 series routers do not support the interception of IP packets from Asynchronous Transfer Mode (ATM) Permanent Virtual Circuits (PVCs).

Information About Lawful Intercept

- Introduction to Lawful Intercept, page 3
- Cisco Service Independent Intercept Architecture, page 3
- PacketCable Lawful Intercept Architecture, page 3
- CISCO ASR 1000 Series Routers, page 4
- VRF Aware LI, page 4

- LI of IP Packets on ATM Interfaces, page 5
- IPv6 Based Lawful Intercepts, page 5
- Lawful Intercept MIBs, page 6

Introduction to Lawful Intercept

LI is the process by which law enforcement agencies (LEAs) conduct electronic surveillance as authorized by judicial or administrative order. Increasingly, legislation is being adopted and regulations are being enforced that require service providers (SPs) and ISPs to implement their networks to explicitly support authorized electronic surveillance. The types of SPs or ISPs that are subject to LI mandates vary greatly from country to country. LI compliance in the United States is specified by the Communications Assistance for Law Enforcement Act (CALEA), and accredited by the Commission on Accreditation for Law Enforcement Agencies.

Cisco supports two architectures for LI: PacketCable and Service Independent Intercept. The LI components by themselves do not ensure customer compliance with applicable regulations but rather provide tools that can be used by SPs and ISPs to construct an LI-compliant network.

Cisco Service Independent Intercept Architecture

The *Cisco Service Independent Intercept Architecture Version 3.0* document describes implementation of LI for VoIP networks using the Cisco Broadband Telephony Softswitch (BTS) 10200 Softswitch call agent, version 5.0, in a non-PacketCable network. Packet Cable Event Message specification version 1.5-I01 is used to deliver the call identifying information along with version 2.0 of the Cisco Tap MIB for call content.

The *Cisco Service Independent Intercept Architecture Version 2.0* document describes implementation of LI for VoIP networks using the Cisco BTS 10200 Softswitch call agent, versions 4.4 and 4.5, in a non-PacketCable network. Although not a PacketCable network, PacketCable Event Messages Specification version I08 is still used to deliver call identifying information, along with version 1.0 or version 2.0 of the Cisco Tap MIB for call content. The *Cisco Service Independent Intercept Architecture Version 2.0* document adds additional functionality for doing data intercepts by both IP address and session ID, which are both supported in version 2.0 of the Cisco Tap MIB (CISCO-TAP2-MIB).

The *Cisco Service Independent Intercept Architecture Version 1.0* document describes implementation of LI for VoIP networks that are using the Cisco BTS 10200 Softswitch call agent, versions 3.5 and 4.1, in a non-PacketCable network. Although not a PacketCable network, PacketCable Event Message Specification version I03 is still used to deliver call identifying information, along with version 1.0 of the Cisco Tap MIB (CISCO-TAP-MIB) for call content. Simple data intercepts by IP address are also discussed.

PacketCable Lawful Intercept Architecture

The P*acketCable Lawful Intercept Architecture for BTS Version 5.0* document describes the implementation of LI for VoIP using Cisco BTS 10200 Softswitch call agent, version 5.0, in a PacketCable network that conforms to PacketCable Event Messages Specification version 1.5-I01.

The *PacketCable Lawful Intercept Architecture for BTS Versions 4.4 and 4.5* document describes the implementation of LI for VoIP using Cisco BTS 10200 Softswitch call agent, versions 4.4 and 4.5, in a PacketCable network that conforms to PacketCable Event Messages Specification version I08.

The *PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1* document describes the implementation of LI for VoIP using Cisco BTS 10200 Softswitch call agent, versions 3.5 and 4.1, in a PacketCable network that conforms to PacketCable Event Message Specification version I03.

The *PacketCable Control Point Discovery Interface Specification* document defines an IP-based protocol that can be used to discover a control point for a given IP address. The control point is the place where Quality of Service (QoS) operations, LI content tapping operations, or other operations may be performed.

CISCO ASR 1000 Series Routers

The Cisco ASR 1000 series routers support two types of LI: regular and broadband (per-subscriber). Broadband wiretaps are executed on access subinterfaces. Regular wiretaps are executed on access subinterfaces and physical interfaces. Wiretaps are not required, and are not executed, on internal interfaces. The router determines which type of wiretap to execute based on the interface that the target's traffic is using.

LI on the Cisco ASR 1000 series routers can intercept traffic based on a combination of one or more of the following fields:

- Destination IP address and mask (IPv4 or IPv6 address)
- Destination port or destination port range
- Source IP address and mask (IPv4 or IPv6 address)
- Source port or source port range
- Protocol ID
- Type of Service (TOS)
- Virtual routing and forwarding (VRF) name, which is translated to a *vrf-tableid* value within the router.
- Subscriber (user) connection ID

The LI implementation on the Cisco ASR 1000 series routers is provisioned using SNMP3 and supports the following functionality:

- Interception of communication content. The router duplicates each intercepted packet and then places the copy of the packet within a UDP-header encapsulated packet (with a configured CCCid). The router sends the encapsulated packet to the LI mediation device. Even if multiple lawful intercepts are configured on the same data flow, only one copy of the packet is sent to the mediation device. If necessary, the mediation device can duplicate the packet for each LEA.
- Interception of IPv4 and IPv6 flows.
- Interception of IPv4 and IPv6 multicast flows, where the target is the source of the multicast traffic.

VRF Aware LI

VRF Aware LI is the ability to provision a LI wiretap on IPv4 data in a particular Virtual Private Network (VPN). This feature allows a LEA to lawfully intercept targeted data within that VPN. Only IPv4 data within that VPN is subject to the VRF-based LI tap.

VRF Aware LI is available for the following types of traffic:

- ip2ip
- ip2tag (IP to MPLS)
- tag2ip (MPLS to IP)

To provision a VPN-based IPv4 tap, the LI administrative function (running on the mediation device) uses the CISCO-IP-TAP-MIB to identify the name of the VRF table that the targeted VPN uses. The VRF name is used to select the VPN interfaces on which to enable LI in order to execute the tap.

The router determines which traffic to intercept and which mediation device to send the intercepted packets based on the VRF name (along with the source and destination address, source and destination port, and protocol).

Note When using the Cisco-IP-TAP-MIB, if the VRF name is not specified in the stream entry, the global IP routing table is used by default.

LI of IP Packets on ATM Interfaces

The Lawful Intercept feature enables you to configure the system so that IP packets that are sent and received on ATM interfaces are intercepted based on the PVC information, such as the Virtual Path Identifier (VPI) or Virtual Channel Identifier (VCI). If you specify an interface when configuring the system, then all IP traffic on the given interface corresponding to the VPI or VCI on the ATM PVC is intercepted. If you do not specify an interface when configuring the system, then IP traffic corresponding to the ATM PVC on all interfaces is intercepted.

LI of IP traffic on ATM interfaces is available for the following interfaces and encapsulation types:

- ATM interface
- ATM multipoint interface
- ATM subinterface point-to-point
- PPP over ATM (PPPoA) encapsulation
- PPP over Ethernet over ATM (PPPoEoA) encapsulation

To provision an IP traffic tap on an ATM interface, the LI administrative function (running on the mediation device) uses the CISCO-IP-TAP-MIB to specify the VPI and VCI information for ATM PVCs. This information is used to select the interfaces on which to enable LI in order to execute the tap.

The router determines which traffic to intercept and to which mediation device to send the intercepted packets based on the VPI and VCI information.

When an ATM interface tap is provisioned, the system creates an IP_STREAM entry type, that stores all tap information (such as the PVC information and interface). The LI feature intercepts packets at the IP layer. If the interface is an ATM interface, LI extracts the PVC information from the packet and matches it against the provisioned streams. If an interface is specified when configuring the system, LI also matches the packet information against the interface. For each matching stream, the LI module sends a copy of the packet to the corresponding mediation device.

IPv6 Based Lawful Intercepts

To configure IPv6 based lawful intercepts, the system identifies either the source or destination address as the target address and then determines if a less specific route to the target address exists. If a less specific route to the target address exists, the system identifies the list of interfaces that can used to reach the target address and applies the intercepts to those interfaces only.

The system automatically detects route changes and reapplies intercepts on any changed routes.

The system uses the IPv6 stream details specified by the **snmp set** command to identify the target address, using the following criteria:

- If the source address prefix length is 0, the destination address is chosen as the target address. Likewise, if the destination address prefix length is 0, the source address is chosen as the target address.

- If neither the source address nor destination address prefix length is 0, the address with the longer prefix length is chosen as the target address.
- If the prefix lengths of the source address and destination address are equal, then the system determines which network is close to the Content IAP (CIAP) by doing a longest match lookup on the prefix in the IPv6 routing table. The system chooses the location (source or destination) with the longer prefix as the target.

Lawful Intercept MIBs

Due to its sensitive nature, the Cisco LI MIBs are only available in software images that support the LI 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, page 6

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 LI MIBs. To restrict access to these MIBs, you must:

1. Create a view that includes the Cisco LI 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 LI 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.

For more information, see the Creating a Restricted SNMP View of Lawful Intercept MIBs module.

Note Access to the Cisco LI 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.

How to Configure Lawful Intercept

Although there are no direct user commands to provision lawful intercept on the router, you do need to perform some configuration tasks, such as providing access to LI MIBs, setting up SNMP notifications, and enabling the LI RADIUS session feature. This section describes how to perform the following tasks:

- Creating a Restricted SNMP View of Lawful Intercept MIBs, page 6
- Enabling SNMP Notifications for Lawful Intercept, page 9
- Disabling SNMP Notifications, page 10
- Enabling RADIUS Session Intercepts, page 11

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 steps in this section.

- You must issue the commands in global configuration mode with level-15 access rights.
- SNMPv3 must be configured on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server view** *view-name MIB-name* **included**
4. **snmp-server view** *view-name MIB-name* **included**
5. **snmp-server view** *view-name MIB-name* **included**
6. **snmp-server view** *view-name MIB-name* **included**
7. **snmp-server view** *view-name MIB-name* **included**
8. **snmp-server group** *group-name* **v3 auth read** *view-name* **write** *view-name*
9. **snmp-server user** *user-name group-name* **v3 auth md5** *auth-password*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server view** *view-name MIB-name* **included** **Example:** `Router(config)# snmp-server view exampleView ciscoTap2MIB included`	Creates an SNMP view that includes the CISCO-TAP2-MIB (where *exampleView*is the name of the view to create for the MIB). • This MIB is required for both regular and broadband lawful intercept.
Step 4	**snmp-server view** *view-name MIB-name* **included** **Example:** `Router(config)# snmp-server view exampleView ciscoIpTapMIB included`	Adds the CISCO-IP-TAP-MIB to the SNMP view.

	Command or Action	Purpose
Step 5	**snmp-server view** *view-name MIB-name* **included** **Example:** `Router(config)# snmp-server view exampleView cisco802TapMIB included`	Adds the CISCO-802-TAP-MIB to the SNMP view.
Step 6	**snmp-server view** *view-name MIB-name* **included** **Example:** `Router(config)# snmp-server view exampleView ciscoUserConnectionTapMIB included`	Adds the CISCO-USER-CONNECTION-TAP-MIB to the SNMP view.
Step 7	**snmp-server view** *view-name MIB-name* **included** **Example:** `Router(config)# snmp-server view exampleView ciscoMobilityTapMIB included`	Adds the CISCO-MOBILITY-TAP-MIB to the SNMP view.
Step 8	**snmp-server group** *group-name* **v3 auth read** *view-name* **write** *view-name* **Example:** `Router(config)# snmp-server group exampleGroup v3 auth read exampleView write exampleView`	Creates an SNMP user group that has access to the LI MIB view and defines the group's access rights to the view.
Step 9	**snmp-server user** *user-name group-name* **v3 auth md5** *auth-password* **Example:** `Router(config)# snmp-server user exampleUser exampleGroup v3 auth md5 examplePassword`	Adds users to the specified user group.
Step 10	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

- Where to Go Next, page 8

Where to Go Next

The mediation device can now access the lawful intercept MIBs and issue SNMP **set** and **get** requests to configure and run lawful intercepts on the router. To configure the router to send SNMP notification to the mediation device, see the Enabling SNMP Notifications for Lawful Intercept.

Enabling SNMP Notifications for Lawful Intercept

SNMP automatically generates notifications for lawful intercept events. To configure the router to send lawful intercept notifications to the mediation device, perform the steps in this section.

- You must issue the commands in global configuration mode with level-15 access rights.
- SNMPv3 must be configured on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *ip-address* **community-string udp-port** *port notification-type*
4. **snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** *ip-address* **community-string udp-port** *port notification-type* **Example:** `Router(config)# snmp-server host 10.2.2.1 community-string udp-port 161 udp`	Specifies the IP address of the mediation device and the password-like community-string that is sent with a notification request. • For lawful intercept, the **udp-port** must be 161 and not 162 (the SNMP default).

	Command or Action	Purpose
Step 4	**snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart** **Example:** `Router(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`	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.
Step 5	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Disabling SNMP Notifications

To disable SNMP notifications on the router, perform the steps in this section.

Note 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).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no snmp-server enable traps**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no snmp-server enable traps** **Example:** `Router(config)# no snmp-server enable traps`	Disables all SNMP notification types that are available on your system.
Step 4	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Enabling RADIUS Session Intercepts

There are no user CLI commands available to provision the mediation device or taps. However, to enable the intercepts through the CISCO-TAP-MIB you must configure the system to make the account-session-id value available to the mediation device. To enable RADIUS session intercepts on the router, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa intercept**
4. **aaa authentication ppp default group radius**
5. **aaa accounting delay-start all**
6. **aaa accounting send stop-record authentication failure**
7. **aaa accounting network default start-stop group radius**
8. **radius-server attribute 44 include-in-access-req**
9. **radius-server host** *host-name*
10. **aaa server radius dynamic-author**
11. **client** *ip-address*
12. **domain** {**delimiter** *character*| **stripping [right-to-left]**}
13. **server-key** *word*
14. **port** *port-number*
15. **exit**
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa intercept** **Example:** `Router(config)# aaa intercept`	Enables lawful intercept on the router. • Associate this command with a high administrative security to ensure that unauthorized users cannot stop intercepts if this command is removed.
Step 4	**aaa authentication ppp default group radius** **Example:** `Router(config)# aaa authentication ppp default group radius`	Specifies the authentication method to use on the serial interfaces that are running Point-to-Point protocol (PPP). **Note** This command is required because tap information resides only on the RADIUS server. You can authenticate with locally configured information, but you cannot specify a tap with locally configured information.
Step 5	**aaa accounting delay-start all** **Example:** `Router(config)# aaa accounting delay-start all`	Delays the generation of accounting start records until the user IP address is established. Specifying the **all** keyword ensures that the delay applies to all VRF and non-VRF users. **Note** This command is required so that the mediation device can see the IP address assigned to the target.
Step 6	**aaa accounting send stop-record authentication failure** **Example:** `Router(config)# aaa accounting send stop-record authentication failure`	(Optional) Generates accounting stop records for users who fail to authenticate while logging into or during session negotiation. **Note** If a lawful intercept action of 1 does not start the tap, the stop record contains Acct-Termination-Cause, attribute 49, set to 15 (Service Unavailable).

	Command or Action	Purpose
Step 7	**aaa accounting network default start-stop group radius** **Example:** `Router(config)# aaa accounting network default start-stop group radius`	(Optional) Enables accounting for all network-related service requests. **Note** This command is required only to determine the reason why a tap did not start.
Step 8	**radius-server attribute 44 include-in-access-req** **Example:** `Router(config)# radius-server attribute 44 include-in-access-req`	(Optional) Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication). **Note** Enter this command to obtain attribute 44 from the Access-Request packet. Otherwise you will have to wait for the accounting packets to be received before you can determine the value of attribute 44.
Step 9	**radius-server host** *host-name* **Example:** `Router(config)# radius-server host host1`	(Optional) Specifies the RADIUS server host.
Step 10	**aaa server radius dynamic-author** **Example:** `Router(config)# aaa server radius dynamic-author`	Configures a device as an Authentication, Authorization, and Accounting (AAA) server to facilitate interaction with an external policy server and enters dynamic authorization local server configuration mode. **Note** This is an optional command if taps are always started with a session starts. The command is required if CoA-Requests are used to start and stop taps in existing sessions.
Step 11	**client** *ip-address* **Example:** `Router(config-locsvr-da-radius)# client 10.0.0.2`	(Optional) Specifies a RADIUS client from which the device will accept CoA-Request packets.

	Command or Action	Purpose

Step 12	**domain** {**delimiter** *character*| **stripping [right-to-left]**}
	
	Example:
	`Router(config-locsvr-da-radius)# domain stripping right-to-left`
	
	Example:
	`Router(config-locsvr-da-radius)# domain delimiter @`
		(Optional) Configures username domain options for the RADIUS application.
		• The **delimiter** keyword specifies the domain delimiter. One of the following options can be specified for the *character* argument: **@**, /, **$**, **%**, \, **#** or **-**
		• The **stripping** keyword compares the incoming username with the names oriented to the left of the **@** domain delimiter.
		• The **right-to-left** keyword terminates the string at the first delimiter going from right to left.

Step 13	**server-key** *word* **Example:** `Router(config-locsvr-da-radius)# server-key samplekey`	(Optional) Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 14	**port** *port-number* **Example:** `Router(config-locsvr-da-radius)# port 1600`	(Optional) Specifies a RADIUS client from which the device will accept CoA-Request packets.
Step 15	**exit** **Example:** `Router(config-locsvr-da-radius)# exit`	Exits dynamic authorization local server configuration mode and returns to global configuration mode.
Step 16	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Configuration Examples for Lawful Intercept

- Example Enabling Mediation Device Access Lawful Intercept MIBs, page 15
- Example Enabling RADIUS Session Lawful Intercept, page 15

Example Enabling Mediation Device Access Lawful Intercept MIBs

The following example shows how to enable the mediation device to access the lawful intercept MIBs. It creates an SNMP view (tapV) that includes three LI MIBs (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, CISCO-802-TAP-MIB). It also creates a user group that has read, write, and notify access to MIBs in the tapV view.

```
snmp-server view tapV ciscoTap2MIB included
snmp-server view tapV ciscoIpTapMIB included
snmp-server view tapV cisco802TapMIB included
snmp-server group tapGrp v3 auth read tapV write tapV notify tapV
snmp-server user MDuser tapGrp v3 auth md5 MDpasswd
snmp-server engineID local 1234
```

Example Enabling RADIUS Session Lawful Intercept

The following example shows the configuration of a RADIUS-Based Lawful Intercept solution on a router acting as a network access server (NAS) device employing a PPPoEoA link:

```
aaa new-model
!
aaa intercept
!
aaa group server radius SG
server 10.0.56.17 auth-port 1645 acct-port 1646
!
aaa authentication login LOGIN group SG
aaa authentication ppp default group SG
aaa authorization network default group SG
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group SG
!
aaa server radius dynamic-author
client 10.0.56.17 server-key cisco
!
vpdn enable
!
bba-group pppoe PPPoEoA-TERMINATE
virtual-template 1
!
interface Loopback0
ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet4/1/0
description To RADIUS server
ip address 10.0.56.20 255.255.255.0
duplex auto
!
interface GigabitEthernet4/1/2
description To network
ip address 10.1.1.1 255.255.255.0
duplex auto
!
interface GigabitEthernet5/0/0
description To subscriber
no ip address
!
interface GigabitEthernet5/0/0.10
encapsulation dot1q 10
protocol pppoe group PPPoEoA-TERMINATE
!
interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
!
radius-server attribute 44 include-in-access-req
```

```
radius-server attribute nas-port format d
radius-server host 10.0.56.17 auth-port 1645 acct-port 1646
radius-server key cisco
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring SNMP Support	Configuring SNMP Support
Security Commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
PacketCable™ *Control Point Discovery Interface Specification*	*PacketCable™ Control Point Discovery Interface Specification* (PKT-SP-CPD-I02-061013)

MIBs

MIB	MIBs Link
• CISCO-802-TAP-MIB • CISCO-IP-TAP-MIB • CISCO-MOBILITY-TAP-MIB • CISCO-TAP2-MIB • CISCO-USER-CONNECTION-TAP-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC-2865	*Remote Authentication Dial In User Service (RADIUS)*
RFC-3576	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*
RFC-3924	*Cisco Architecture for Lawful Intercept in IP Networks*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Lawful Intercept

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Lawful Intercept

Feature Name	Releases	Feature Information
Lawful Intercept	12.0(32)S 12.2(31)SB2 12.2(33)SRB 12.2(33)SXH 12.4(22)T 15.0(1)M	The Lawful Intercept (LI) feature supports service providers in meeting the requirements of law enforcement agencies to provide the ability to intercept VoIP or data traffic going through the edge routers. In 12.0(32)S, this feature was introduced. This feature was integrated into Cisco IOS Release 12.2(31)SB2. This feature was integrated into Cisco IOS Release 12.2(33)SRB. This feature was integrated into Cisco IOS Release 12.2(33)SXH. This feature was integrated into Cisco IOS Release 12.4(22)T. In Cisco IOS Release 15.0(1)M, support was added for intercepting IP packets on ATM interfaces and for IPv6 based Lawful Intercepts. For more information, see