Lawful Intercept Architecture

First Published: October 31, 2005
Last Updated: August 16, 2010

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. 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.

Before Cisco IOS XE Release 2.5, PPP sessions were tapped based on the accounting session. Circuit-ID based tapping was introduced in Cisco IOS XE Release 2.5.

In Cisco IOS XE Release 2.6, a user session is tapped based on the unique PPP over Ethernet (PPPoE) circuit ID tag. This circuit ID tag serves as a unique parameter for the PPPoE user session on the device. The tapped user session is provisioned through SNMP, and user session data packets and RADIUS authentication data packets are tapped.

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 for Lawful Intercept" section on page 18.

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

Contents

- Prerequisites for Lawful Intercept, page 2
- Restrictions for Lawful Intercept, page 2
- Information About Lawful Intercept, page 3

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

- How to Configure Lawful Intercept, page 6
- Configuration Examples for Lawful Intercept, page 15
- Additional References, page 16
- Feature Information for Lawful Intercept, page 18

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.

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 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 Simple Network Management Protocol (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.

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.

Lawful Intercept MIBs

Only the mediation device and users who need to know about lawful intercepts are allowed to access the LI 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).

SNMP Notifications

SNMP notifications for LI must be sent to User Datagram Protocol (UDP) port 161 on the mediation device, not port 162 (which is the SNMP default). For more information, see the "Enabling SNMP Notifications for Lawful Intercept" section on page 8.

Information About Lawful Intercept

- Introduction to Lawful Intercept, page 3
- Cisco Service Independent Intercept Architecture, page 3
- PacketCable Lawful Intercept Architecture, page 4

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 Internet service providers (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 Commission on Accreditation for Law Enforcement Agencies (CALEA).

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 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 *PacketCable 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 voice over IP (VoIP) using Cisco Broadband Telephony Softswitch (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 Aggregation Services 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:

- RADIUS session intercepts, which can occur in one of the following ways:
  - Interception through Access-Accept packets allows interception to start at the beginning of a session.
  - Interception through CoA-Request packets enables the router to start or stop interception during a session.

- 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, IPv4 multicast, IPv6, and IPv6 multicast flows.

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.

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

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" section on page 6.

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 8
- Disabling SNMP Notifications, page 9
- Enabling RADIUS Session Intercepts, page 10
- Configuring Circuit ID Based Tapping, page 13

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.

Prerequisites

- 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 group** *group-name* ***v*3 noauth read** *view-name* **write** *view-name*
7. **snmp-server user** *user-name group-name* ***v*3 auth md5** *auth-password*

8. **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.
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 group** *group-name* **v3 noauth read** *view-name* **write** *view-name* Example: `Router(config)# snmp-server group exampleGroup v3 noauth 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 7	**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 8	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

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" section on page 8.

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.

Prerequisites

- 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 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).
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.
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** *keyword*
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).
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.

	Command or Action	Purpose
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.

Step 12	**domain** {**delimiter** *character* | **stripping** [**right-to-left**]}
	
	Example:
	`Router(config-locsvr-da-radius)# domain stripping right-to-left`
	`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.

	Command or Action	Purpose
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.

Configuring Circuit ID Based Tapping

To configure circuit ID based tapping of user session data packets and RADIUS authentication data packets on the router, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber access pppoe unique-key circuit-id**
4. **end**
5. **show pppoe session all**
6. **show idmgr session key circuit-id** *circuit-id*

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	**subscriber access pppoe unique-key circuit-id**
	
	`Example:`
	`Router(config)#subscriber access pppoe unique-key circuit-id`
		Specifies a unique circuit ID tag for a PPPoE user session to be tapped on the router.

Step 4	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show pppoe session all** **Example:** `Router# show pppoe session all`	Displays the circuit-id tag in the PPPoE session, which is used in the next step to verify the user session.

Step 6	**show idmgr session key circuit-id** *circuit-id*
	
	Example:
	`Router# show idmgr session key circuit-id Ethernet4/0.100:PPPoE-Tag-1`
	
	`session-handle = AA000007`
	`aaa-unique-id = 0000000E`
	`circuit-id-tag = Ethernet4/0.100:PPPoE-Tag-1`
	`interface = nas-port:0.0.0.0:0/1/1/100`
	`authen-status = authen`
	`username = user1@cisco.com`
	`addr = 106.1.1.3`
	`session-guid = 650101020000000E`
	`The session hdl AA000007 in the record is valid`
	`The session hdl AA000007 in the record is valid`
	`No service record found`
		Verifies the user session information in the ID Manager (IDMGR) database by specifying the unique circuit ID tag.

Configuration Examples for Lawful Intercept

The following examples are provided to show how to configure 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 four LI MIBs (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, CISCO-802-TAP-MIB, and CISCO-USER-CONNECTION-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 view tapV ciscoUserConnectionTapMIB included
snmp-server group tapGrp v3 noauth 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 an Ethernet PPP connection over Ethernet (PPPoE) 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 PPPoE-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 PPPoE-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-TAP2-MIB • CISCO-IP-TAP-MIB • CISCO-802-TAP-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

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 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.

Table 1 Feature Information for Lawful Intercept

Feature Name	Releases	Feature Information
Lawful Intercept	Cisco IOS XE Release 2.4	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 Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
VRF Aware LI (Lawful Intercept)	Cisco IOS XE Release 2.4	VRF Aware LI is the ability to provision a LI wiretap on IPv4 data in a particular Virtual Private Network (VPN). The following sections provide information about this feature: • VRF Aware LI, page 5 In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
RADIUS-based Lawful Intercept	Cisco IOS XE Release 2.4	The LI implementation is provisioned using SNMP3 and supports RADIUS session intercepts. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following sections provide information about this feature: • CISCO ASR 1000 Series Routers, page 4 • Enabling RADIUS Session Intercepts, page 10 • Example: Enabling RADIUS Session Lawful Intercept, page 15

Table 1 Feature Information for Lawful Intercept (continued)

Feature Name	Releases	Feature Information
Circuit ID based tapping of PPP session for Lawful Intercept.	Cisco IOS XE Release 2.5	In Cisco IOS XE Release 2.5, circuit ID based tapping of a PPP session is introduced. Circuit ID based tapping works only if the tap is provisioned after the user session is active. It is assumed in this instance that the user session is uniquely identified by a circuit ID tag.
Circuit ID based tapping for Lawful Intercept	Cisco IOS XE Release 2.6	In Cisco IOS XE Release 2.6, pre-provisioning of circuit-ID based tapping of a PPP session is introduced. If the tap is provisioned before a user session is active, then the tap is effective whenever the user session becomes active. Also, corresponding RADIUS authentication and accounting packets are tapped. It is assumed in this instance that the user session is uniquely identified by a circuit ID tag.