Lawful Intercept Architecture

The Lawful Intercept (LI) feature supports service providers in meeting the requirements of law enforcement agencies (LEA) to provide electronic surveillance as authorized by a judicial or administrative order. The surveillance is performed using wiretaps to intercept Voice-over-Internet protocol (VoIP) or data traffic going through the edge routers. 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 using IP sessions.

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.

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

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 does not support SUP HA. LI configuration needs to be reapplied after SUP switchover. An SNMP trap will be generated for this event.

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).

Information About Lawful Intercept

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 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 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 and tunnel interfaces. Regular wiretaps are executed on access subinterfaces, tunnel interfaces, 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 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.

RADIUS-Based Lawful Intercept

A RADIUS-based lawful intercept solution enables intercept requests to be sent (through Access-Accept packets or Change of Authorizationt (CoA)-Request packets) to the network access server (NAS) or to the Layer 2 Tunnel Protocol access concentrator (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.

Intercept requests are initiated by the mediation device via SNMPv3 messages, and all traffic data going to or from a given IP address is passed to a mediation device. Interception based on IP addresses prevents a session from being tapped until an IP address has been assigned to the session.

The RADIUS-based lawful intercept feature provides High Availability (HA) support for LI for the following modes:

- Access-Accept based LI for the new session
- CoA based LI for existing session

The RADIUS-based LI HA supports only the RADIUS based provisioning. The SNMP-based provisioning is not supported.

Intercept Operation

How Intercept Requests Work Within Access-Accept Packets

When an intercept target begins to establish a connection, an Access-Request packet is sent to the RADIUS server. The RADIUS server responds with an Access-Accept packet containing the four RADIUS attributes.

The NAS or the LAC receives the LI-Action attribute with the value 1, allowing the NAS or LAC to duplicate the traffic data at the start of the new session and forward the duplicated data to the mediation device that was specified through the attributes, MD-IP-Address and MD-Port-Number.

Note If the NAS or LAC cannot start intercepting traffic data for a new session, the session does not get established.

If accounting is enabled (through the **aaa accounting network** command and the **aaa accounting send stop-record authentication failure** command), an Accounting-Stop packet must be sent with the Acct-Termination-Cause attribute (49) set to 15, which means that service is not available.

How Intercept Requests Work Within CoA-Request Packets

After a session has been established for the intercept target, CoA-Request packets can be used for the following tasks:

- Starting the interception of an existing session. The LI-Action attribute is set to 1.
- Stopping the interception of an existing session. The LI-Action attribute is set to 0.
- Issuing a dummy intercept request. The LI-Action attribute is set to 2. The NAS or LAC should not perform any session interception; instead, it searches the session on the basis of the Acct-Session-ID attribute value that was specified in the CoA-Request packets. If a session is found, the NAS or LAC sends a CoA acknowledgment (ACK) response to the RADIUS server. If a session is not found, the NAS or LAC issues a “session not found” error message.

In each case, the RADIUS server must send CoA-Request packets with the identified attributes and the Acct-Session-ID attribute. Each of these attributes must be in the packet.

The Acct-Session-ID attribute identifies the session that will be intercepted. The Acct-Session-ID attribute can be obtained from either the Access-Request packet or the Accounting-Stop packet.

When a session is being tapped and the session terminates, the tap stops. The session does not start when the subscriber logs back in unless the Access-Accept indicates a start tap or a CoA-Request is sent to start the session.

Note The frequency of CoA-Request packets should not exceed a rate of one request every 10 minutes.

Service Independent Intercept (SII)

Cisco developed the Service Independent Intercept (SII) architecture in response to requirements that support lawful intercept for service provider customers. The SII architecture offers well-defined, open interfaces between the Cisco equipment acting as the content Intercept Access Point (IAP) and the mediation device. The modular nature of the SII architecture allows the service provider to choose the most appropriate mediation device to meet specific network requirements and regional, standards-based requirements for the interface to the law enforcement collection function.

The mediation device uses SNMPv3 to instruct the call connect (CC) IAP to replicate the CC and send the content to the mediation device. The CC IAP can be either an edge router or a trunking gateway for voice, and either an edge router or an access server for data.

To increase the security and to mitigate any SNMPv3 vulnerability, the following tasks are required:

Restricting Access to Trusted Hosts (without Encryption)

SNMPv3 provides support for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine the security mechanism employed when handling an SNMP packet.

Additionally, the SNMP Support for the Named Access Lists feature adds support for standard named access control lists (ACLs) to several SNMP commands.

To configure a new SNMP group or a table that maps SNMP users to SNMP views, use the **snmp-server group** command in global configuration mode.

```
access-list my-list permit ip host 10.10.10.1
snmp-server group my-group v3 auth access my-list
```

In this example, the access list named **my-list** allows SNMP traffic only from 10.10.10.1. This access list is then applied to the SNMP group called **my-group**.

Encrypting Lawful Intercept Traffic and Restricting Access to Trusted Hosts

Encryption of intercepted traffic between the router (the content Intercept Access Point (IAP)) and the Mediation Device (MD) is highly recommended.

The following configuration is required:

- Configuring encryption in the router and either an encryption client in the MD or a router associated with the MD to decrypt the traffic.
- Restricting access to trusted hosts.
- Configuring the VPN client.

Configuring encryption in the Router

First configure Authentication, Authorization and Accounting (AAA) parameters. The following example shows how to configure the parameters:

```
aaa authentication login userauthen local
username <username> password 0 <password>
```

The following example uses the internal database; however, external authentication servers can also be specified to perform the authentication.

After configuring the AAA parameters, configure the Internet Security Association and Key Management Protocol (ISAKMP) policy and the crypto map. The following example uses pre-shared keys, Diffie-Hellman (DH) group 2 and AES 256 as the encryption protocol for phase 1 (Internet Key Exchange (IKE)). The crypto map is called dynamic-map and the VPN group is called LI-group. Access-list 108 defines the traffic that is allowed to the router (in this case the ip pool is 10.1.1.1 through 10.1.1.254).

```
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
!
crypto isakmp client configuration group LI-group
key <password>
dns 10.10.10.10
wins 10.10.10.20
domain cisco.com
pool ippool
acl 108
!
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
set transform-set myset
!
!
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
interface GigabitEthernet0/3
ip address <IP address of LI-enabled router> 255.255.255.0
crypto map clientmap
!
!
ip local pool ippool 10.1.1.1 10.1.1.254
!
!
access-list 108 permit ip  10.1.1.0 0.0.0.255 host 10.0.24.4 <IP address of LI-enabled
router>
```

Restricting Access to Trusted Hosts (with Encryption)

The following example shows how to create an ACL that allows only the IP pool (10.1.1.0/24) for VPN clients, and assign that ACL to the SNMPv3 group.

```
access-list my-list permit ip 10.1.1.0 0.0.0.255
snmp-server group my-group v3 auth access my-list
```

Configuring the VPN Client

```
See the
 Installing the VPN Client
 document to download and configure the Cisco VPN Client for Solaris. See the
```

```
Cisco VPN Client installation instructions
 document to download and configure the Cisco VPN Client for other operating systems.
```

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 required tasks.

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.

Before you begin

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa intercept**
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 group** *group-name* **v3 noauth read** *view-name* **write** *view-name*
8. **snmp-server user** *user-name group-name* **v3 auth md5** *auth-password*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa intercept** **Example:**	Enables lawful intercept on the device.

	Command or Action	Purpose
	`Device(config)# aaa intercept`	• Associate this command with a high administrative security to ensure that unauthorized users cannot stop intercepts if this command is removed. **Note** The **aaa intercept** command is required to set up the wiretap using an IP session.
Step 4	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(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 5	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView ciscoIpTapMIB included`	Adds the CISCO-IP-TAP-MIB to the SNMP view.
Step 6	**snmp-server view** *view-name MIB-name* **included** **Example:** `Device(config)# snmp-server view exampleView cisco802TapMIB included`	Adds the CISCO-802-TAP-MIB to the SNMP view.
Step 7	**snmp-server group** *group-name* **v3 noauth read** *view-name* **write** *view-name* **Example:** `Device(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 8	**snmp-server user** *user-name group-name* **v3 auth md5** *auth-password* **Example:** `Device(config)# snmp-server user exampleUser exampleGroup v3 auth md5 examplePassword`	Adds users to the specified user group.
Step 9	**end** **Example:** `Device(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.

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.

Before you begin

- 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** *and* **snmp-server enable traps rf**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** *ip-address* **community-string udp-port** *port notification-type* **Example:** `Device(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** *and* **snmp-server enable traps rf**	Configures the router to send RFC 1157 notifications to the mediation device.

	Command or Action	Purpose

	Example:
	`Device(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`
	`Device(config)# snmp-server enable traps rf`
		These notifications indicate authentication failures, link status (up or down), and router restarts.

Step 5	**end** **Example:** `Device(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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no snmp-server enable traps** **Example:** `Device(config)# no snmp-server enable traps`	Disables all SNMP notification types that are available on your system.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa intercept**	Enables lawful intercept on the router.

	Command or Action	Purpose
	Example: `Device(config)# aaa intercept`	• 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:** `Device(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:** `Device(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:** `Device(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:** `Device(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:** `Device(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:**	(Optional) Specifies the RADIUS server host.

	Command or Action	Purpose
	`Device(config)# radius-server host host1`	
Step 10	**aaa server radius dynamic-author** **Example:** `Device(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:** `Device(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:
	`Device(config-locsvr-da-radius)# domain stripping right-to-left`
	Example:
	`Device(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:** `Device(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:** `Device(config-locsvr-da-radius)# port 1600`	(Optional) Specifies a RADIUS client from which the device will accept CoA-Request packets.
Step 15	**exit** **Example:** `Device(config-locsvr-da-radius)# exit`	Exits dynamic authorization local server configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 16	**end** **Example:** `Device(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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**subscriber access pppoe unique-key circuit-id** **Example:** `Device(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:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 5	**show pppoe session all** **Example:**	Displays the circuit-id tag in the PPPoE session, which is used in the next step to verify the user session.

	Command or Action	Purpose
	`Device# show pppoe session all`	

Step 6	**show idmgr session key circuit-id** *circuit-id*
	Example:
	`Device# show idmgr session key circuit-id Ethernet4/0.100:PPPoE-Tag-1`
	Example:
	Example:
	`session-handle = AA000007`
	Example:
	`aaa-unique-id = 0000000E`
	Example:
	`circuit-id-tag = Ethernet4/0.100:PPPoE-Tag-1`
	Example:
	`interface = nas-port:0.0.0.0:0/1/1/100`
	Example:
	`authen-status = authen`
	Example:
	`username = user1@cisco.com`
	Example:
	`addr = 106.1.1.3`
	Example:
	`session-guid = 650101020000000E`
	Example:
	`The session hdl AA000007 in the record is valid`
	Example:
	`The session hdl AA000007 in the record is valid`
	Example:
	`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

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.

```
aaa intercept
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

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	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.15S	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. In Cisco IOS XE Release 3.15S, the Lawful Intercept feature was introduced on tunnel interfaces for 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). In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Feature Name	Releases	Feature Information
RADIUS-based Lawful Intercept	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.5S	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. In Cisco IOS XE Release 3.5, High Availability support was added for RADIUS-Based Lawful Intercept.
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.
Non-Lawful Intercept (Non-LI) Images	Cisco IOS XE Release 3.10S	In Cisco IOS XE Release 3.10S, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The Non-LI images will be available from Cisco IOS XE Release 3.10S onwards and will not contain the LI subsystems.