Implementing Lawful Intercept

Lawful intercept is the process by which law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications, authorized by judicial or administrative order. Service providers worldwide are legally required to assist law enforcement agencies in conducting electronic surveillance in both circuit-switched and packet-mode networks.

Only authorized service provider personnel are permitted to process and configure lawfully authorized intercept orders. Network administrators and technicians are prohibited from obtaining knowledge of lawfully authorized intercept orders, or intercepts in progress. Error messages or program messages for intercepts installed in the router are not displayed on the console.

Lawful Intercept is not a part of the Cisco IOS XR software by default. You have to install it separately by installing and activating **asr9k-li-px.pie** .

Feature History for Implementing Lawful Intercept

Release	Modification
Release 4.1.0	This feature was introduced.
Release 4.2.0	High Availability support for Lawful Intercept was added. Support for IPv6 Lawful Intercept was added.
Release 4.3.2	Lawful Intercept is available as a separate package. It is no longer a part of the Cisco IOS XR software.
Release 7.0.1	Overlapping tap functionality is made available on Cisco ASR 9000 4th Generation QSFP28 based dense 100GE line cards (A9K-8X100GE-X-TR, A9K-16X100GE-TR, A9K-32X100GE-TR and A99-16x100-X-SE) as well.

- Prerequisites for Implementing Lawful Intercept, on page 2
- Restrictions for Implementing Lawful Intercept, on page 3
- Information About Lawful Intercept Implementation, on page 4
- Intercepting IPv4 and IPv6 Packets, on page 8
- High Availability for Lawful Intercept, on page 10
- Installing Lawful Intercept (LI) Package, on page 11
- How to Configure SNMPv3 Access for Lawful Intercept, on page 16
- Configuration Example for Inband Management Plane Feature Enablement, on page 21
- Additional References, on page 21

Prerequisites for Implementing Lawful Intercept

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Lawful intercept implementation also requires that these prerequisites are met:

- Cisco ASR 9000 Series Aggregation Services Router will be used as content Intercept Access Point (IAP) router in lawful interception operation.
- **Provisioned router—**The router must be already provisioned. For more information, see *Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*.

Tip For the purpose of lawful intercept taps, provisioning a loopback interface has advantages over other interface types.

- **Understanding of SNMP Server commands in Cisco IOS XR software—**Simple Network Management Protocol, version 3 (SNMP v3), which is the basis for lawful intercept enablement, is configured using commands described in the module *SNMP Server Commands* in *System Management Command Reference for Cisco ASR 9000 Series Routers*. To implement lawful intercept, you must understand how the SNMP server functions. For this reason, carefully review the information described in the module *Implementing SNMP* in *System Management Configuration Guide for Cisco ASR 9000 Series Routers*.
- **Lawful intercept must be explicitly disabled—**It is automatically enabled on a provisioned router. However, you should not disable LI if there is an active tap in progress, because this deletes the tap.
- **Management plane configured to enable SNMPv3—**Allows the management plane to accept SNMP commands, so that the commands go to the interface (preferably, a loopback) on the router. This allows the mediation device (MD) to communicate with a physical interface.
- **VACM views enabled for SNMP server—**View-based access control model (VACM) views must be enabled on the router.
- **Provisioned MD—**For detailed information, see the vendor documentation associated with your MD. For a list of MD equipment suppliers preferred by Cisco, see http://www.cisco.com/en/US/tech/tk583/tk799/tsd_technology_support_protocol_home.html.
- **VoIP surveillance-specific requirements**
  - **Lawful-intercept-enabled call agent—**A lawful-intercept-enabled call agent must support interfaces for communications with the MD, for the target of interest to provide signaling information to the MD. The MD extracts source and destination IP addresses and Real-Time Protocol (RTP) port numbers from the Session Description Protocol (SDP) signaling information for the target of interest. It uses these to form an SNMPv3 SET, which is sent to the router acting as the content IAP to provision the intercept for the target of interest.

    The MD uses the CISCO-TAP2-MIB to set up communications between the router acting as the content IAP, and the MD.

    The MD uses the CISCO-IP-TAP-MIB to set up the filter for the IP addresses and port numbers to be intercepted and derived from the SDP.

- Routers to be used for calls by the target number must be provisioned for this purpose through the MD.
- The MD that has been provisioned with the target number to be intercepted.

- **Data session surveillance-specific requirements**
  - Routers to be used by the data target that have been provisioned for this purpose through the MD.
  - **The MD that has been provisioned with the user login ID, mac address of the user CPE device, or the DSLAM physical location ID—**The IP address is the binding that is most frequently used to identify the target in the network. However, alternative forms of information that uniquely identify the target in the network might be used in some network architectures. Such alternatives include the MAC address and the acct-session-id.

- The MD can be located anywhere in the network but must be reachable from the content IAP router, which is being used to intercept the target. MD should be reachable ONLY from global routing table and NOT from VRF routing table.

Restrictions for Implementing Lawful Intercept

The following restrictions are applicable for Lawful Intercept:

- If lawful intercept is set up separately for two inter-communicating hosts with two different mediation devices, then by default, only the ingress traffic on the ASR 9000 router from one of the hosts is intercepted. You can configure the **overlap-tap enable** command to separately intercept the ASR 9000 ingress as well as egress traffic for both the mediation devices.
- Lawful intercept does not provide support for these features on Cisco ASR 9000 Series Router:
  - IPv6 multicast tapping
  - IPv4 multicast tapping
  - Per tap drop counter
  - IPv6 intercept on gigabit ethernet LCs
  - IPv6 MD encapsulation
  - Per layer 3 interface tapping

Note Per layer 2 interface tapping is supported.

  - Replicating a single tap to multiple MDs
  - Tapping of tag packets
  - Tapping L2 flows
  - RTP encapsulation
  - Encryption and integrity checking of replication device

- GRE encapsulation
- MPLS encapsulation

Note Per tap drop counter support is available only for ASR9000-SIP-700 line card, and not for ethernet line cards.

- Lawful intercept is applied only on ingress traffic.

  Traffic is intercepted, when it arrives as pure IP in the following scenarios:

  - For label imposition direction
  - When it arrives from the core after PHP action.

  Traffic is not intercepted in the following criteria:

  - When it arrives from the core as MPLS encapsulated (with VPN label) for the label disposition direction.
  - For GRE encapsulated packets.

- Lawful intercept traffic cannot be transmitted over the management interface.

Information About Lawful Intercept Implementation

Cisco lawful intercept is based on service-independent intercept (SII) architecture and SNMPv3 provisioning architecture. SNMPv3 addresses the requirements to authenticate data origin and ensure that the connection from the router to the MD is secure. This ensures that unauthorized parties cannot forge an intercept target.

Lawful intercept offers these capabilities:

- Voice-over IP (VoIP) and data session intercept provisioning from the MD using SNMPv3
- Delivery of intercepted VoIP and data session data to the MD
- SNMPv3 lawful intercept provisioning interface
- Lawful intercept MIB: CISCO-TAP2-MIB, version 2
- CISCO-IP-TAP-MIB manages the Cisco intercept feature for IP and is used along with CISCO-TAP2-MIB to intercept IP traffic.
- User datagram protocol (UDP) encapsulation to the MD
- Replication and forwarding of intercepted packets to the MD
- Voice-over IP (VoIP) call intercept, based on any rules configured for received packets.
- Voice-over IP (VoIP) intercept with LI-enabled call agent
- Data session call intercept based on IP address

Interception Mode

The lawful intercept has two interception modes:

- **Global LI:** The taps are installed on all the line cards in the ingress direction. With the global tap, the traffic for the target can be intercepted regardless of ingress point. Only the tap that has wild cards in the interface field is supported.
- **Interface LI:** Taps each packet that is entering or leaving an interface without any additional filters.

Overlapping Taps

Traffic interception can be configured for two inter-communicating intercepted hosts using overlapping taps.

For example, consider two taps, one configured for all traffic from source address A and another for all traffic going to destination address B. When a packet arrives with source address A and destination address B, the packet is tapped by TAP1 in ingress and TAP2 in egress, and copies will be generated and forwarded to both mediation devices. Overlapping taps can be enabled using **overlap-tap enable** command in Global configuration mode.

From Cisco IOS XR Software Release 7.0.1 and later, the Lawful Intercept overlapping tap functionality is available on Cisco ASR 9000 4th Generation QSFP28 based dense 100GE line cards (A9K-8X100GE-X-TR, A9K-16X100GE-TR, A9K-32X100GE-TR and A99-16x100-X-SE) as well.

Provisioning for VoIP Calls

Lawful Intercept provisioning for VoIP occurs in these ways:

- Security and authentication occurs because users define this through SNMPv3.
- The MD provisions lawful intercept information using SNMPv3.
- Network management occurs through standard MIBs.

Call Interception

VoIP calls are intercepted in this manner:

- The MD uses configuration commands to configure the intercept on the call control entity.
- The call control entity sends intercept-related information about the target to the MD.
- The MD initiates call content intercept requests to the content IAP router or trunk gateway through SNMPv3.
- The content IAP router or trunk gateway intercepts the call content, replicates it, and sends it to the MD in Packet Cable Electronic Surveillance UDP format. Specifically, the original packet starting at the first byte of the IP header is prefixed with a four-byte CCCID supplied by the MD in TAP2-MIB. It is then put into a UDP frame with the destination address and port of the MD.
- After replicated VoIP packets are sent to the MD, the MD then forwards a copy to a law-enforcement-agency-owned collection function, using a recognized standard.

Provisioning for Data Sessions

Provisioning for data sessions occurs in a similar way to the way it does for lawful intercept for VoIP calls. (See Provisioning for VoIP Calls, on page 5.)

Data Interception

Data are intercepted in this manner:

- If a lawful intercept-enabled authentication or accounting server is not available, a sniffer device can be used to detect the presence of the target in the network.
  - The MD uses configuration commands to configure the intercept on the sniffer.
  - The sniffer device sends intercept-related information about the target to the MD.
- The MD initiates communication content intercept requests to the content IAP router using SNMPv3.
- The content IAP router intercepts the communication content, replicates it, and sends it to the MD in UDP format.
- Intercepted data sessions are sent from the MD to the collection function of the law enforcement agency, using a supported delivery standard for lawful intercept.

Information About the MD

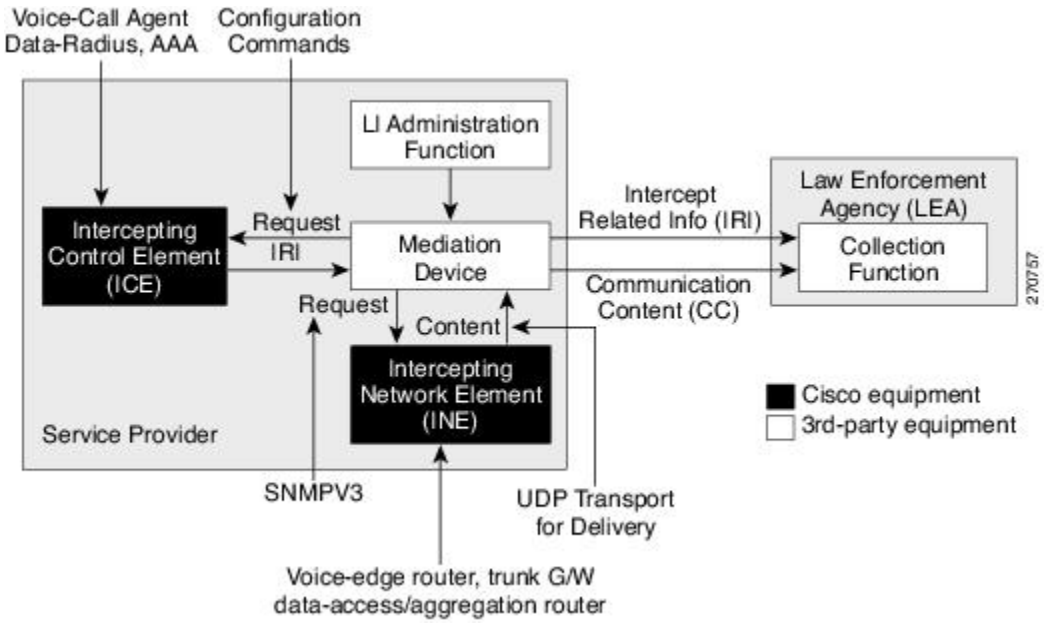
The MD performs these tasks:

- Activates the intercept at the authorized time and removes it when the authorized time period elapses.
- Periodically audits the elements in the network to ensure that:
  - *only* authorized intercepts are in place.
  - *all* authorized intercepts are in place.

Lawful Intercept Topology

This figure shows intercept access points and interfaces in a lawful intercept topology for both voice and data interception.

Figure 1: Lawful Intercept Topology for Both Voice and Data Interception



Layer 2 Lawful Intercept

You can configure SNMP-based lawful intercept on a layer 2 interface. This intercepts all traffic passing through the particular interface.

Scale or Performance Improvement

New enhancements introduced on the Cisco ASR 9000 Series Router in terms of scalability and performance for lawful intercept are:

- IPv4 lawful intercept tap limit is 1000 taps per IPv4 except for the A9K-8x100G-LB-SE and A9K-8x100G-LB-TR line cards. These line cards have a tap limit of 2000 taps per IPv4.
- IPv6 lawful intercept tap limit is 1000 taps per IPv6.
- Interception rate is:
  - 50 Mbps per network processor (NP) for ASR9000-SIP-700 line card.
  - 100 Mbps for Gigabit Ethernet line cards.
  - 500 Mbps for Modular Weapon-X line cards.
  - 1000 Mbps for 100GE line cards.
- Support upto 512 MDs.

Intercepting IPv4 and IPv6 Packets

This section provides details for intercepting IPv4 and IPv6 packets supported on the Cisco ASR 9000 Series Router.

Lawful Intercept Filters

The filters used for classifying a tap are:

- IP address type
- Destination address
- Destination mask
- Source address
- Source mask
- ToS (Type of Service) and ToS mask
- Protocol
- Destination port with range
- Source port with range
- VRF (VPN Routing and Forwarding)
- Flow ID

Intercepting Packets Based on Flow ID (Applies to IPv6 only)

To further extend filteration criteria for IPv6 packets, an additional support to intercept IPv6 packets based on flow ID has been introduced on the Cisco ASR 9000 Series Router. All IPv6 packets are intercepted based on the fields in the IPv6 header which comprises numerous fields defined in IPv6 Header Field Details table:

Note The field length or payload length is not used for intercepting packets.

Table 1: IPv6 Header Field Details

IPv6 Field Name	Field Description	Field Length
Version	IPv6 version number.	4 bits
Traffic Class	Internet traffic priority delivery value.	8 bits
Flow ID (Flow Label)	Used for specifying special router handling from source to destination(s) for a sequence of packets.	20 bits

IPv6 Field Name	Field Description	Field Length
Payload Length	Specifies the length of the data in the packet. When cleared to zero, the option is a hop-by-hop Jumbo payload.	16 bits unassigned
Next Header	Specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.	8 bits
Hop Limit	For each router that forwards the packet, the hop limit is decremented by 1. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header that was originally intended to be used as a time based hop limit.	8 bits unsigned
Source Address	The IPv6 address of the sending node.	16 bytes
Destination Address	The IPv6 address of the destination node.	16 bytes

The flow ID or flow label is a 20 bit field in the IPv6 packet header that is used to discriminate traffic flows. Each flow has a unique flow ID. The filteration criteria to intercept packets matching a particular flow ID is defined in the tap configuration file. From the line card, the intercepted mapped flow IDs are sent to the next hop, specified in the MD configuration file. The intercepted packets are replicated and sent to the MD fom the line card.

Intercepting VRF (6VPE) and 6PE Packets

This section provides information about intercepting VRF aware packets and 6PE packets. Before describing how it works, a basic understanding of 6VPE networks is discussed.

The MPLS VPN model is a true peer VPN model. It enforces traffic separations by assigning unique VPN route forwarding (VRF) tables to each customer's VPN at the provider content IAP router. Thus, users in a specific VPN cannot view traffic outside their VPN.

Cisco ASR 9000 Series Router supports intercepting IPv6 packets of the specified VRF ID for 6VPE. To distiguish traffic on VPN, VRFs are defined containing a specific VRF ID. The filter criteria to tap a particular VRF ID is specified in the tap. IPv6 packets are intercepted with the VRF context on both scenarios: imposition (ip2mpls) and disposition (mpls2ip).

The 6PE packets carry IPv6 packets over VPN. The packets do not have a VRF ID. Only IP traffic is intercepted; no MPLS based intercepts are supported. The IPv6 traffic is intercepted at the content IAP of the MPLS cloud at imposition (ip2mpls) and at disposition (mpls2ip).

Intercepting IPv6 packets is also performed for ip2tag and tag2ip packets. Ip2tag packets are those which are converted from IPv6 to Tagging (IPv6 to MPLS), and tag2ip packects are those which are converted from Tagging to IPv6 (MPLS to IPv6) at the provider content IAP router.

Encapsulation Type Supported for Intercepted Packets

Intercepted packets mapping the tap are replicated, encapsulated, and then sent to the MD. IPv4 and IPv6 packets are encapsulated using UDP (User Datagram Protocol) encapsulation. The replicated packets are forwarded to MD using UDP as the content delivery protocol. Only IPv4 MD encapsulation is supported.

The intercepted packet gets a new UDP header and IPv4 header. Information for IPv4 header is derived from MD configuration. Apart from the IP and UDP headers, a 4 byte channel identifier (CCCID) is also inserted

after the UDP header in the packet. After adding the MD encapsulation, if the packet size is above the MTU, the egress LC CPU fragments the packet. Moreover, there is a possibility that the packet tapped is already a fragment. Each tap is associated with only one MD. Cisco ASR 9000 Series Router does not support forwarding replicated packets to multiple MDs.

Note Encapsulation types, such as RTP and RTP-NOR, are not supported.

Per Tap Drop Counter Support

Cisco ASR 9000 Series Router line cards provide SNMP server as an interface to export each tap forwarded to MD packet and drop counts. Any intercepted packets that are dropped prior to getting forwarded to the MD due to policer action are counted and reported. The drops due to policer action are the only drops that are counted under per tap drop counters. If a lawful intercept filter is modified, the packet counts are reset to 0.

Note Per tap drop counter support is available only for ASR9000-SIP-700 line card, and not for ethernet line cards.

High Availability for Lawful Intercept

High availability for lawful intercept provides operational continuity of the TAP flows and provisioned MD tables to reduce loss of information due to route processor fail over (RPFO).

To achieve continuous interception of a stream, when RP fail over is detected; MDs are required to re-provision all the rows relating to CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, and CISCO-USER-CONNECTION-TAP-MIB to synchronize database view across RP and MD.

Note The high availability for lawful intercept is enabled by default from Release 4.2.0 onwards.

Preserving TAP and MD Tables during RP Fail Over

At any point in time, MD has the responsibility to detect the loss of the taps via SNMP configuration process.

After RPFO is completed, MD should re-provision all the entries in the stream tables, MD tables, and IP taps with the same values they had before fail over. As long as an entry is re-provisioned in time, existing taps will continue to flow without any loss.

The following restrictions are listed for re-provisioning MD and tap tables with respect to behavior of SNMP operation on citapStreamEntry, cTap2StreamEntry, cTap2MediationEntry MIB objects:

- After RPFO, table rows that are not re-provisioned, shall return NO_SUCH_INSTANCE value as result of SNMP Get operation.

- Entire row in the table must be created in a single configuration step, with exactly same values as before RPFO, and with the rowStatus as CreateAndGo. Only exception is the cTap2MediationTimeout object, that should reflect valid future time.

Replay Timer

The replay timer is an internal timeout that provides enough time for MD to re-provision tap entries while maintaining existing tap flows. It resets and starts on the active RP when RPFO takes place. The replay timer is a factor of number of LI entries in router with a minimum value of 10 minutes.

After replay timeout, interception stops on taps that are not re-provisioned.

Note In case high availability is not required, MD waits for entries to age out after fail over. MD cannot change an entry before replay timer expiry. It can either reinstall taps as is, and then modify; or wait for it to age out.

Installing Lawful Intercept (LI) Package

As LI is not a part of the Cisco IOS XR image by default, you need to install it separately.

Installing and Activating the LI Package

The Package Installation Envelope (PIE) files, are installable software files with the .pie extension. PIE files are used to copy one or more software components onto the router. A PIE may contain a single component, a group of components (called a package), or a set of packages (called a composite package).

Use the **show install committed** command in EXEC mode to verify the committed software packages.

To install the Lawful Intercept (LI) package, you must install and activate the **asr9k-li-px.pie**

For more information about installing PIEs, refer to *Upgrading and Managing Cisco IOS XR Software section* of the *System Management Configuration Guide for Cisco ASR 9000 Series Routers*.

SUMMARY STEPS

1. **admin**
2. **install add** *tftp://<IP address of tftp server>/<location of pie on server>*
3. **install activate** *device:package*
4. **install commit**
5. **exit**
6. **show install committed**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RSP0/CPU0:router# admin`	Enters administration EXEC mode.
Step 2	**install add** *tftp://<IP address of tftp server>/<location of pie on server>* **Example:** `RP/0/RSP0/CPU0:router(admin)# install add tftp://172.201.11.140/auto/tftp-users1/`**`asr9k-li-px.pie`**	Copies the contents of a package installation envelope (PIE) file to a storage device.
Step 3	**install activate** *device:package* **Example:** `RP/0/RSP0/CPU0:router(admin)# install activate disk0:asr9k-li-px.pie`	Activates the respective package and adds more functionality to the existing software.
Step 4	**install commit** **Example:** `RP/0/RSP0/CPU0:router(admin)# install commit`	Saves the active software set to be persistent across designated system controller (DSC) reloads.
Step 5	**exit** **Example:** `RP/0/RSP0/CPU0:router(admin)# exit`	Exits from the admin mode.
Step 6	**show install committed** **Example:** `RP/0/RSP0/CPU0:router# show install committed`	Shows the list of the committed software packages.

Deactivating the LI PIE

To uninstall the Lawful Intercept package, deactivate asr9k-li-px.pie as shown in the following steps:

Note You might experience interface or protocol flaps while uninstalling or deactivating the LI PIE. Hence, we recommend you to perform this activity during a maintenance window.

SUMMARY STEPS

1. **admin**
2. **install deactivate** *device:package*

3. **install commit**
4. **install remove** *device:package*
5. **exit**
6. **show install committed**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RSP0/CPU0:router# admin`	Enters administration EXEC mode.
Step 2	**install deactivate** *device:package* **Example:** `RP/0/RSP0/CPU0:router(admin)# install deactivate disk0:asr9k-li-px.pie`	Activates the respective package and adds more functionality to the existing software.
Step 3	**install commit** **Example:** `RP/0/RSP0/CPU0:router(admin)# install commit`	Saves the active software set to be persistent across designated system controller (DSC) reloads.
Step 4	**install remove** *device:package* **Example:** `RP/0/RSP0/CPU0:router(admin)# install remove disk0:asr9k-li-px.pie`	Saves the active software set to be persistent across designated system controller (DSC) reloads.
Step 5	**exit** **Example:** `RP/0/RSP0/CPU0:router(admin)# exit`	Exits from the admin mode.
Step 6	**show install committed** **Example:** `RP/0/RSP0/CPU0:router# show install committed`	Shows the list of the committed software packages.

Upgrade and Downgrade Scenarios for the Lawful Intercept package

This section describes the possible upgrade and downgrade scenarios with respect to the Lawful Intercept (LI) package.

This example configuration demonstrates how to upgrade or downgrade the Cisco IOS XR software with or without the LI package. Suppose you have two versions of software images, V1 and V2. If you want to upgrade or downgrade from V1 to V2 without the LI package, you need to perform the following steps for the upgrade or the downgrade procedure:

Note Ensure that you use Turbo Boot to load the image for the downgrade process.

1. Ensure that the device has booted with the V1 image. Check the Package Installation Envelope (PIE) files that have been installed in V1.
2. Save all the PIE files that exist in V2 in the Trivial File Transfer Protocol (TFTP) server. Copy the contents of the PIE files from the TFTP server by using the **install add** command in the admin mode.

```
RP/0/RSP0/CPU0:router(admin)# install add tar
tftp://223.255.254.254/install/files/pies.tar
```

3. To activate all the PIE files in V2 at once, run the following commands based on the type of upgrade:

At any point during the upgrade or the downgrade process, you can check the progress by using the **show install request** or the **show issu** command.

Some of the conventions that are followed in describing these scenarios are:

- Release 4.3.1 base image: It is the Cisco IOS XR software for Release 4.3.1 that contains Cisco LI by default.
- Release 4.3.2 base image: It is the Cisco IOS XR software for Release 4.3.2 that does not contain Cisco LI by default.
- Separate LI package: It is the LI package that needs to be installed separately for Release 4.3.2 and higher versions.

Table 2: Upgrade Scenarios

Upgrade From	Upgrade To	Result	Supported
Release 4.3.1 base image	Release 4.3.2 base image	Before the upgrade, the LI has to be configured and provisioned completely. After the upgrade to Release 4.3.2 version without the LI package, you cannot configure or provision LI.	Yes
Release 4.3.1 base image	Release 4.3.2 base image with the separate LI package	The Upgrade will reload the router. After the upgrade process completes, you need to reconfigure LI MDs/TAPs from the SNMP server. Also, all the LI configurations made in the earlier version is accepted.	Yes
Release 4.3.2 base image with the separate LI package	Release 4.3.3 base image with the separate LI package	After the upgrade, the LI configuration is not retained.	Yes

Upgrade From	Upgrade To	Result	Supported
Release 4.3.2 base image with the separate LI package	Release 4.3.3 base image without the separate LI package	This upgrade is not possible as the installation process will not proceed without the LI PIE.	No
Release 4.3.2 base image without the separate LI package	Release 4.3.3 base image with the separate LI package	This upgrade is possible.	Yes
ISSU for Release 4.3.1 base image	Release 4.3.2 with the separate LI package	After this upgrade, to retain the LI configuration, you have to replay the configuration before the replay timeout occurs.	Yes
ISSU for Release 4.3.2 base image with the separate LI package	Release 4.3.3 with the separate LI package	After this upgrade, to retain the LI configuration, you have to replay the configuration before the replay timeout occurs.	Yes

Table 3: Downgrade Scenarios

Downgrade From	Downgrade To	Result	Supported
Release 4.3.2 base image without the separate LI package	Release 4.3.1 base image	After the downgrade, begin the provisioning process of LI.	Yes
Release 4.3.2 base image with the separate LI package	Release 4.3.1 base image	This scenario is not supported.	No
Release 4.3.3 base image with the separate LI package	Release 4.3.2 base image with the separate LI package	After the downgrade, the LI configuration is not retained. You have to provision the LI once again.	Yes
Release 4.3.3 base image with the separate LI package	Release 4.3.2 base image without the LI package	After the downgrade, the LI configuration is lost. You will not be able to provision it after downgrade.	Yes
Release 4.3.3 base image	Release 4.3.2 base image with the separate LI package	The LI configuration is accepted and can be provisioned only after the downgrade.	Yes
ISSU			No

How to Configure SNMPv3 Access for Lawful Intercept

Perform these procedures in the order presented to configure SNMPv3 for the purpose of Lawful Intercept enablement:

Disabling SNMP-based Lawful Intercept

Lawful Intercept is enabled by default on the Cisco ASR 9000 Series Router after installing and activating the **asr9k-li-px.pie**.

- To disable Lawful Intercept, enter the **lawful-intercept disable** command in global configuration mode.
- To re-enable it, use the **no** form of this command.

Disabling SNMP-based Lawful Intercept: Example

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# lawful-intercept disable
```

Note The **lawful-intercept disable** command is available on the router, only after installing and activating the **asr9k-li-px.pie**.

All SNMP-based taps are dropped when lawful intercept is disabled.

Configuring the Inband Management Plane Protection Feature

If MPP was not earlier configured to work with another protocol, then ensure that the MPP feature is also not configured to enable the SNMP server to communicate with the mediation device for lawful interception. In such cases, MPP must be configured specifically as an inband interface to allow SNMP commands to be accepted by the router, using a specified interface or all interfaces.

Note Ensure this task is performed, even if you have recently migrated to Cisco IOS XR Software from Cisco IOS, and you had MPP configured for a given protocol.

For lawful intercept, a loopback interface is often the choice for SNMP messages. If you choose this interface type, you must include it in your inband management configuration.

For a more detailed discussion of the inband management interface, see the Inband Management Interface.

Related Tasks

- Configuring a Device for Management Plane Protection for an Inband Interface

Related Examples

- Configuring the Inband Management Plane Protection Feature: Example, on page 21

Enabling the Mediation Device to Intercept VoIP and Data Sessions

The following SNMP server configuration tasks enable the Cisco SII feature on a router running Cisco IOS XR Software by allowing the MD to intercept VoIP or data sessions.

SUMMARY STEPS

1. **configure**
2. **snmp-server view** *view-name* **ciscoTap2MIB included**
3. **snmp-server view** *view-name* **ciscoUserConnectionTapMIB included**
4. **snmp-server group** *group-name* **v3auth read** *view-name* **write** *view-name* **notify** *view-name*
5. **snmp-server host** *ip-address* **traps version 3 auth** *username* **udp-port** *port-number*
6. **snmp-server user** *mduser-id groupname* **v3 auth md5** md-*password*
7. Use the **commit** or **end** command.
8. show snmp users
9. show snmp group
10. show snmp view

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**snmp-server view** *view-name* **ciscoTap2MIB included** **Example:** `RP/0//CPU0:router(config)# snmp-server view TapName ciscoTap2MIB included`	Creates or modifies a view record and includes the CISCO-TAP2-MIB family in the view. The SNMP management objects in the CISCO-TAP2-MIB that controls lawful intercepts are included. This MIB is used by the mediation device to configure and run lawful intercepts on targets sending traffic through the router.
Step 3	**snmp-server view** *view-name* **ciscoUserConnectionTapMIB included** **Example:** `RP/0//CPU0:router(config)# snmp-server view TapName ciscoUserConnectionTapMIB included`	Creates or modifies a view record and includes the CISCO-USER-CONNECTION-TAP-MIB family, to manage the Cisco intercept feature for user connections. This MIB is used along with the CISCO-TAP2-MIB to intercept and filter user traffic.

	Command or Action	Purpose
Step 4	**snmp-server group** *group-name* **v3auth read** *view-name* **write** *view-name* **notify** *view-name* **Example:** `RP/0//CPU0:router(config)# snmp-server group TapGroup v3 auth read TapView write TapView notify TapView`	Configures a new SNMP group that maps SNMP users to SNMP views. This group must have read, write, and notify privileges for the SNMP view.
Step 5	**snmp-server host** *ip-address* **traps version 3 auth** *username* **udp-port** *port-number* **Example:** `RP/0//CPU0:router(config)# snmp-server host 223.255.254.224 traps version 3 auth bgreen udp-port 2555`	Specifies SNMP trap notifications, the version of SNMP to use, the security level of the notifications, and the recipient (host) of the notifications.
Step 6	**snmp-server user** *mduser-id groupname* **v3 auth md5** md-*password* **Example:** `RP/0//CPU0:router(config)# snmp-server mduser-id TapGroup v3 auth md5 mdpassword`	Configures the MD user as part of an SNMP group, using the v3 security model and the HMAC MD5 algorithm, which you associate with the MD password. • The *mduser-id* and *mdpassword* must match that configured on MD. Alternatively, these values must match those in use on the router. • Passwords must be eight characters or longer to comply with SNMPv3 security minimums. • Minimum Lawful Intercept security level is auth; The noauth option will not work, as it indicates noAuthnoPriv security level. The Lawful Intercept security level must also match that of the MD. • Choices other than MD5 are available on the router, but the MD values must match. Most MDs default to or support only MD5.
Step 7	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.
Step 8	show snmp users **Example:**	Displays information about each SNMP username in the SNMP user table.

	Command or Action	Purpose
	`RP/0//CPU0:router# show snmp users`	
Step 9	show snmp group **Example:** `RP/0//CPU0:router# show snmp group`	Displays information about each SNMP group on the network.
Step 10	show snmp view **Example:** `RP/0//CPU0:router# show snmp view`	Displays information about the configured views, including the associated MIB view family name, storage type, and status.

Adding MD and TAP Objects

To keep the MD row in active state, the following objects are mandatory:

- cTap2MediationDestAddressType
- cTap2MediationDestAddress
- cTap2MediationDestPort
- cTap2MediationSrcInteraface
- cTap2MediationTimeout
- cTap2MediationTransport
- cTap2MediationStatus

SUMMARY STEPS

1. Add MD.
2. Add TAP.
3. Activate TAP.

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	Add MD.
	Example:
	`setany -v3 <ip-address> <user>`
	`cTap2MediationDestAddressType.1 <ipv4/ipv6>`
	`cTap2MediationDestAddress.1 <"ip">`
	`cTap2MediationDestPort.1 "1234"`
	`cTap2MediationSrcInterface.1 0`
		Creates an MD for mediation services.
		To delete a MD, run:
		`setany -v3 <ip-address> <user>`
		`cTap2MediationStatus.1 6`
		`cTap2MediationStatus.1 = destroy(6)`

	Command or Action	Purpose

	`cTap2MediationTransport.1 udp`
	`cTap2MediationNotificationEnable.1 true`
	`cTap2MediationTimeout.1 '7 de 6 14 3 4 5 6 2d 1 2'`
	` cTap2MediationStatus.1 createAndGo`
	` cTap2MediationDestAddressType.1 = ipv4(1)`
	` cTap2MediationDestAddress.1 = 46 01  01 02`
	` cTap2MediationDestPort.1 = 1234`
	` cTap2MediationSrcInterface.1 = 0`
	` cTap2MediationTransport.1 = udp(1)`
	` cTap2MediationNotificationEnable.1 = true(1)`
	` cTap2MediationTimeout.1 =`
	`2014-Jun-20,03:04:05.6,-1:2`
	` cTap2MediationStatus.1 = createAndGo(4)`	

Step 2	Add TAP.
	Example:
	`setany -v3 <ip-address> <user>`
	`citapStreamInterface.1.1 0 citapStreamAddrType.1.1`
	` <ipv4/ipv6>`
	`citapStreamSourceAddress.1.1 "5a 1 1 2"`
	`citapStreamSourceLength.1.1 32`
	`citapStreamStatus.1.1 citapStreamInterface.1.1 =`
	`0`
	` citapStreamAddrType.1.1 = ipv4(1)`
	` citapStreamSourceAddress.1.1 = 5a 01  01 02`
	` citapStreamSourceLength.1.1 = 32`
	` citapStreamStatus.1.1 = createAndGo(4)`
		Creates a TAP for stream operation.
		To delete a TAP, run:
		`setany -v3 <ip-address> <user>`
		`citapStreamStatus.1.1 6 cTap2StreamStatus.1.1 6`
		` citapStreamStatus.1.1 = destroy(6)`
		` cTap2StreamStatus.1.1 = destroy(6)`

Step 3	Activate TAP.
	Example:
	`setany -v3 <ip-address> <user> cTap2StreamType.1.1`
	` ip cTap2StreamInterceptEnable.1.1 true`
	`cTap2StreamStatus.1.1 createAndGo`
	` cTap2StreamType.1.1 = ip(1)`
	` cTap2StreamInterceptEnable.1.1 = true(1)`
	` cTap2StreamStatus.1.1 = createAndGo(4)`
	Example:
	To add TAP for L2VPN networks
	`setany -v3 <ip-address> <user>`
	`citapStreamInterface.4.1200 1125`
	`citapStreamStatus.4.1200 createAndGo`
		Activates the TAP for stream operation.

Configuration Example for Inband Management Plane Feature Enablement

This example illustrates how to enable the MPP feature, which is disabled by default, for the purpose of lawful intercept.

Configuring the Inband Management Plane Protection Feature: Example

You must specifically enable management activities, either globally or on a per-inband-port basis, using this procedure. To globally enable inbound MPP, use the keyword **all** with the **interface** command, rather than use a particular interface type and instance ID with it.

```
RP/0//CPU0:router# configure
RP/0//CPU0:router(config)# control-plane
RP/0//CPU0:router(config-ctrl)# management-plane
RP/0//CPU0:router(config-mpp)# inband
RP/0//CPU0:router(config-mpp-inband)# interface loopback0
RP/0//CPU0:router(config-mpp-inband-Loopback0)# allow snmp
RP/0//CPU0:router(config-mpp-inband-Loopback0)# commit
RP/0//CPU0:router(config-mpp-inband-Loopback0)# exit
RP/0//CPU0:router(config-mpp-inband)# exit
RP/0//CPU0:router(config-mpp)# exit
RP/0//CPU0:router(config-ctr)# exit
RP/0//CPU0:router(config)# exit
RP/0//CPU0:router# show mgmt-plane inband interface loopback0

Management Plane Protection - inband interface


interface - Loopback0
        snmp configured -
                All peers allowed
RP/0//CPU0:router(config)# commit
```

Additional References

These sections provide references related to implementing lawful intercept.

Related Documents

Related Topic	Document Title
Lawful Intercept commands	*System Security Command Reference for Cisco ASR 9000 Series Routers*
Implementing SNMP	*System Management Configuration Guide for Cisco ASR 9000 Series Routers*
SNMP Server commands	*System Management Command Reference for Cisco ASR 9000 Series Routers*

Standards

Standards	Title
A modular, open architecture designed for simple implementation that easily interacts with third-party equipment to meet service provider lawful intercept requirements.	See RFC-3924 under RFCs, on page 22.
An application layer protocol that facilitates the exchange of management information between network devices. Part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.	Simple Network Management Protocol Version 3 (SNMPv3)

MIBs

MIBs	MIBs Link
• CISCO-TAP2-MIB, version 2 • CISCO-IP-TAP-MIB	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
RFC-3924	Cisco Architecture for Lawful Intercept in IP Networks

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access more content.	http://www.cisco.com/techsupport