Implementing Lawful Intercept

Implementing Lawful Intercept

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Lawful Intercept	Release 24.2.1	You can now enable Lawful Intercept (LI) by installing and activating the LI package to enable service providers to perform surveillance on an individual (or target) as authorized by a judicial or administrative order and share the communication intercepts with law enforcement agencies. This feature is supported on Cisco 8800 series routers that have the 88-LC1-36EH line card installed.

Cisco lawful intercept is based on RFC3924 architecture and SNMPv3 provisioning architecture. SNMPv3 addresses the requirements to authenticate data origin and ensure that the connection from the router to the Mediation Device (MD) is secure. This ensures that unauthorized parties cannot forge an intercept target.

Lawful intercept offers these capabilities:

- 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
- IPv4 and IPv6 user datagram protocol (UDP) encapsulation to the MD
- Replication and forwarding of intercepted packets to the MD

Prerequisites for Implementing Lawful Intercept

Lawful intercept implementation requires that these prerequisites are met:

- The router is used as content Intercept Access Point (IAP) router in lawful interception operation.
- **Provisioned Router—**The router must be already provisioned.

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

- **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 interface) 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.
- 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.
- 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 and Usage Guidelines for Implementing Lawful Intercept

The following restrictions are applicable for Lawful Intercept:

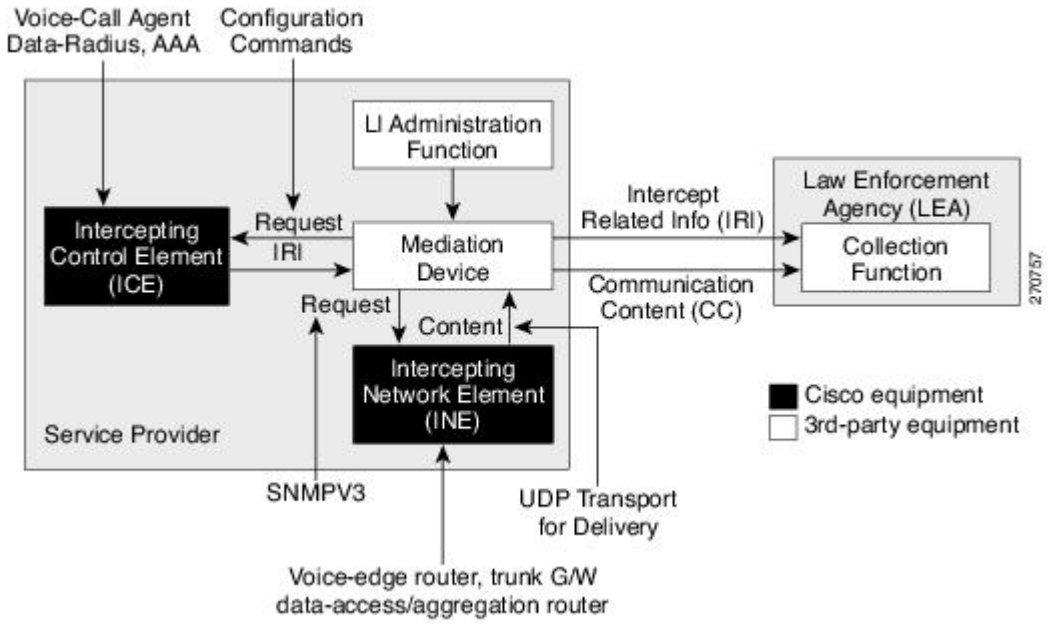
- Lawful intercept is supported only to match pure IP over Ethernet packets.
- Only 512 MDs, 1024 IPv4 and 512 IPv6 TAPs are supported.
- One Tap-to-multiple MDs is not supported.
- After the route processor reload or fail-over, the MD and Tap configuration must be re-provisioned.

- Both IPv4 and IPv6 MD are supported.
- The path to the MD must have the ARP resolved. Any other traffic or protocol will trigger ARP.
- MD next-hop must have ARP resolved. Any other traffic or protocol will trigger ARP.
- Lawful Intercept Stats is not supported.
- Even though the original packets can be fragmented, the LI packets cannot be fragmented. The MTU of the egress interface to the MD must be large enough to support the size of the packets captured.
- LI supports L3 TAPs for L3 interface types, including physical and bundle interfaces.
- Lawful intercept does not provide support for these features on the router:
  - IPv4/IPv6 multicast tapping
  - Per interface tapping
  - Tagged packet tapping
  - Replicating a single tap to multiple MDs
  - Tapping L2 flows and SRv6 traffic
  - RTP encapsulation
  - Lawful Intercept and SPAN on the same interface

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



Note

- The router will be used as content Intercept Access Point (IAP) router, or the Intercepting Network Element (INE) in lawful interception operation.
- The Intercepting Control Element (ICE) could be either a Cisco equipment or a third party equipment.

Benefits of Lawful Intercept

Lawful intercept has the following benefits:

- Allows multiple LEAs to run a lawful intercept on the same Router without each other's knowledge.
- Does not affect subscriber services on the router.
- Supports wiretaps in both the input and output direction.
- Supports wiretaps of Layer 3 traffic.
- Cannot be detected by the target.
- Uses Simple Network Management Protocol Version 3 (SNMPv3) and security features such as the View-based Access Control Model (SNMP-VACM-MIB) and User-based Security Model (SNMP-USM-MIB) to restrict access to lawful intercept information and components.
- Hides information about lawful intercepts from all but the most privileged users. An administrator must set up access rights to enable privileged users to access lawful intercept information.

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

To install the optional LI feature, use the following steps to install and activate the LI RPM package. This example shows the procedure and associated sample configurations to install an RPM package.

1. Use SCP (secure copy) to transfer the RPM files to a folder on the router.
2. Start the LI RPM installation.

   Router#**install source** *<location of the RPM package file>* **xr-8000-li xr-li noprompt**

   Example:

   Router#**install source** */harddisk:/li-rpms/optional-rpms-argon* **xr-8000-li xr-li noprompt**

3. To verify the progress of the RPM installation, use the following CLI command:

   Router#**show install request verbose**

   Example: RPM Installation (in progress)

```
Router#show install request verbose
Tue Apr 11 17:59:09.145 UTC

User request: install source file:///harddisk:/li-rpms/optional-rpms-argon xr-8000-li
xr-li
Operation ID: 1.1
State:        In progress since 2023-04-11 17:58:30 UTC

Current activity:    Verify input and download to internal repository if needed
Next activity:       Veto check
Time started:        2023-04-11 17:58:44 UTC
No per-location information.
```

   Example: RPM Installation (complete)

```
Router#show install request verbose
Tue Apr 11 18:00:49.696 UTC

User request: install source file:///harddisk:/li-rpms/optional-rpms-argon xr-8000-li
xr-li
Operation ID: 1.1
State:        Success since 2023-04-11 18:00:46 UTC

Current activity:    Await user input
Time started:        2023-04-11 18:00:46 UTC

The following actions are available:
    install package add
    install package remove
    install package upgrade
    install package downgrade
    install package replace
    install package rollback
```

```
    install replace
    install rollback
    install source
    install commit
    install replace reimage
```

4. To complete the LI package installation, use the following CLI command:

   ```
   Router#install commit
   ```

   Example:

   ```
   Router#install commit
   Tue Apr 11 18:00:55.671 UTC
   Install commit operation 1 has started
   Install operation will continue in the background
   ```

5. To verify the progress of the installation commit, use the following CLI command:

   ```
   Router#show install request verbose
   ```

   Example:

   ```
   Router#show install request verbose
   Tue Apr 11 18:01:10.078 UTC

   User request: install commit
   Operation ID: 1
   State:        In progress since 2023-04-11 18:00:57 UTC

   Current activity:    Commit transaction
   Next activity:       Transaction complete
   Time started:        2023-04-11 18:00:57 UTC

   No per-location information.
   RP/0/RP0/CPU0:ios#show install request verbose
   Tue Apr 11 18:09:57.666 UTC

   User request: install commit
   Operation ID: 1
   State:        Success since 2023-04-11 18:01:36 UTC

   Current activity:    No install operation in progress

   The following actions are available:
       install package add
       install package remove
       install package upgrade
       install package downgrade
       install package replace
       install package rollback
       install replace
       install rollback
       install source
       install replace reimage
   ```

6. To verify the successful installation of the LI package, use the following CLI command:

   ```
   Router#show install active summary
   ```

   Example:

   ```
   Router#show install active summary
   Tue Apr 11 18:12:43.340 UTC
   Active Packages:    XR: 208    All: 1325
   ```

```
Label:             7.11.1.01I
Software Hash:     f73f9988276c2001702066ac8173de2fe5b9501849ca2c98d49f9828b4ab7522

Optional Packages                                                    Version
---------------------------------------------------- --------------------------
xr-8000-l2mcast                                                 7.11.1.01Iv1.0.0-1
xr-8000-li                                                    7.11.1.01Iv1.0.0-1
xr-8000-mcast                                                   7.11.1.01Iv1.0.0-1
xr-8000-netflow                                                 7.11.1.01Iv1.0.0-1
xr-bgp                                                          7.11.1.01Iv1.0.0-1
xr-ipsla                                                        7.11.1.01Iv1.0.0-1
xr-is-is                                                        7.11.1.01Iv1.0.0-1
xr-li                                                         7.11.1.01Iv1.0.0-1
xr-lldp                                                         7.11.1.01Iv1.0.0-1
xr-mcast                                                        7.11.1.01Iv1.0.0-1
xr-mpls-oam                                                     7.11.1.01Iv1.0.0-1
xr-netflow                                                      7.11.1.01Iv1.0.0-1
xr-ops-script-repo                                              7.11.1.01Iv1.0.0-1
xr-ospf                                                         7.11.1.01Iv1.0.0-1
xr-perf-meas                                                    7.11.1.01Iv1.0.0-1
xr-perfmgmt                                                     7.11.1.01Iv1.0.0-1
xr-track                                                        7.11.1.01Iv1.0.0-1
```

Uninstalling the LI Package

To uninstall the LI package, use the following steps:

1. To start the uninstallion, use the following CLI command:

   install package remove xr-8000-li xr-li

   Example:

   ```
   Router#install package remove xr-8000-li xr-li
   Tue Apr 11 18:18:03.732 UTC
   Install remove operation 2.1.1 has started
   Install operation will continue in the background
   ```

2. To verify the progress of the uninstallation, use the following CLI command:

   show install request verbose

   Example: Uninstallation (in progress)

   ```
   Router#show install request verbose
   Tue Apr 11 18:19:08.473 UTC

   User request: install package remove xr-8000-li xr-li
   Operation ID: 2.1.1
   State:        In progress since 2023-04-11 18:18:05 UTC

   Current activity:    Package add or other package operation
   Next activity:       Await user input
   Time started:        2023-04-11 18:18:44 UTC
   Timeout in:          39m 34s
   Locations responded: 0/1

   Location 0/RP0/CPU0:
     Packaging operation stage: Package operations - completed 6/6
     No client notifications waiting
   ```

   Example: Uninstallation (complete)

```
Router#show install request verbose
Tue Apr 11 18:19:56.671 UTC

User request: install package remove xr-8000-li xr-li
Operation ID: 2.1.1
State:        Success since 2023-04-11 18:19:37 UTC

Current activity:    Await user input
Time started:        2023-04-11 18:19:37 UTC

The following actions are available:
    install package add
    install package remove
    install package upgrade
    install package downgrade
    install package abort latest
    install package abort all-since-apply
    install apply restart
    install apply reload
    install replace reimage

Least impactful apply method: install apply restart
```

3. To apply the LI package uninstallation, use the following CLI command:

   install apply restart

   Example:

```
Router#install apply restart
Tue Apr 11 18:20:43.441 UTC
Install apply operation 2.1 has started
Install operation will continue in the background
```

   Example: Apply restart (in progress)

```
Router#show install request verbose
Tue Apr 11 18:22:04.298 UTC

User request: install apply restart
Operation ID: 2.1
State:        In progress since 2023-04-11 18:20:44 UTC

Current activity:    Post-apply operation cleanup
Next activity:       Await user input
Time started:        2023-04-11 18:21:07 UTC

No per-location information.
```

   Example: Apply restart (complete)

```
Router#show install request verbose
Tue Apr 11 18:22:21.102 UTC

User request: install apply restart
Operation ID: 2.1
State:        Success since 2023-04-11 18:22:09 UTC

Current activity:    Await user input
Time started:        2023-04-11 18:22:09 UTC

The following actions are available:
    install package add
    install package remove
    install package upgrade
```

```
install package downgrade
install package replace
install package rollback
install replace
install rollback
install source
install commit
install replace reimage
```

4. To complete the LI package uninstallation, use the following CLI command:

   install commit

   Example:

```
Router#install commit
Tue Apr 11 18:22:55.627 UTC
Install commit operation 2 has started
Install operation will continue in the background
```

5. To verify the LI package uninstallation, use one of the following CLI commands:

   - **show install request verbose**

     Example:

```
Router#show install request verbose
Tue Apr 11 18:23:45.086 UTC

User request: install commit
Operation ID: 2
State:        Success since 2023-04-11 18:23:35 UTC

Current activity:    No install operation in progress

The following actions are available:
    install package add
    install package remove
    install package upgrade
    install package downgrade
    install package replace
    install package rollback
    install replace
    install rollback
    install source
    install replace reimage
```

   - **show install active summary**

     Example:

```
show install active summary
Tue Apr 11 18:24:12.052 UTC
Active Packages:    XR: 206    All: 1323
Label:              7.11.1.01I
Software Hash:     cdef36e9cf22ba3a1c1217d7b05b41a45b7e9ff6e8f30d871a1c52b91bf16047

Optional Packages                                                 Version
----------------------------------------------------- ----------------------------
xr-8000-l2mcast                                                 7.11.1.01Iv1.0.0-1
xr-8000-mcast                                                   7.11.1.01Iv1.0.0-1
xr-8000-netflow                                                 7.11.1.01Iv1.0.0-1
xr-bgp                                                          7.11.1.01Iv1.0.0-1
xr-ipsla                                                        7.11.1.01Iv1.0.0-1
xr-is-is                                                        7.11.1.01Iv1.0.0-1
```

```
xr-lldp                                                    7.11.1.01Iv1.0.0-1
xr-mcast                                                   7.11.1.01Iv1.0.0-1
xr-mpls-oam                                                7.11.1.01Iv1.0.0-1
xr-netflow                                                 7.11.1.01Iv1.0.0-1
xr-ops-script-repo                                         7.11.1.01Iv1.0.0-1
xr-ospf                                                    7.11.1.01Iv1.0.0-1
xr-perf-meas                                               7.11.1.01Iv1.0.0-1
xr-perfmgmt                                                7.11.1.01Iv1.0.0-1
xr-track                                                   7.11.1.01Iv1.0.0-1
```

How to Configure SNMPv3 Access for Lawful Intercept

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

Disabling SNMP-based Lawful Intercept

Lawful Intercept is enabled by default on the router after installing and activating the LI RPM package.

- 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

```
Router# configure
Router(config)# lawful-intercept disable
```

Note The **lawful-intercept disable** command is available on the router, only after installing and activating the LI RPM package.

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.

Example: Configuring the Inband Management Plane Protection Feature

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

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.

```
router# configure
router(config)# control-plane
router(config-ctrl)# management-plane
router(config-mpp)# inband
router(config-mpp-inband)# interface loopback0
router(config-mpp-inband-Loopback0)# allow snmp
router(config-mpp-inband-Loopback0)# commit
router(config-mpp-inband-Loopback0)# exit
router(config-mpp-inband)# exit
router(config-mpp)# exit
router(config-ctr)# exit
router(config)# exit
router# show mgmt-plane inband interface loopback0
Management Plane Protection - inband interface
interface - Loopback0
        snmp configured -
All peers allowed
router(config)# commit
```

Enabling the Lawful Intercept SNMP Server Configuration

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

Configuration

```
router(config)# snmp-server engineID local 00:00:00:09:00:00:00:a1:61:6c:20:56
router(config)# snmp-server host 1.75.55.1 traps version 3 priv user-name udp-port 4444
router(config)# snmp-server user user-name li-group v3 auth md5 clear lab priv des56 clear
 lab
router(config)# snmp-server view li-view ciscoTap2MIB included
router(config)# snmp-server view li-view ciscoIpTapMIB included
router(config)# snmp-server view li-view snmp included
router(config)# snmp-server view li-view ifMIB included
router(config)# snmp-server view li-view 1.3.6.1.6.3.1.1.4.1 included
router(config)# snmp-server group li-group v3 auth read li-view write li-view notify li-view
```

Note SNMP configuration must be removed while deactivating the LI RPM.

Additional Information on Lawful Intercept

Interception Mode

The lawful intercept operates in the **Global LI** mode.

In this mode, 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.

Data Interception

Data are intercepted in this manner:

- 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 either IPv4 or IPv6 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.

Scale or Performance Values

The router support the following scalability and performance values for lawful intercept:

- A maximum of 1024 IPv4 intercepts and 512 IPv6 intercepts are supported.

Intercepting IPv4 and IPv6 Packets

This section provides details for intercepting IPv4 and IPv6 packets supported on the router.

Lawful Intercept Filters

The following filters are supported for classifying a tap:

- IP address type

- Destination IP address
- Destination mask
- Source IP address
- Source mask
- ToS (Type of Service) and ToS mask
- L4 protocol
- L4 destination port with range
- L4 source port with range

Note VRF (VPN Routing and Forwarding), flow-id, and interface filters are not supported.

Encapsulation Type Supported for Intercepted Packets

Intercepted packets mapping the tap are replicated, encapsulated, and then sent to the MD. IPv4 packets are encapsulated using IPv4 UDP encapsulation, while IPv6 packets are encapsulated using IPv6 UDP encapsulation. The replicated packets are forwarded to MD using UDP as the content delivery protocol.

The intercepted packet gets a new UDP header and IPv4 or IPv6 header, depending on the packet type. Information for IP 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. The router does not support forwarding the same replicated packets to multiple MDs.

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

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 and CISCO-IP-TAP-MIB to synchronize database view across RP and MD.

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.