System Security Configuration Guide, Cisco IOS XE 17 (Cisco ASR 900 Series)

What is Lawful Intercept? 2

Lawful Intercept Topology 2

Prerequisites for Implementing Lawful Intercept 3

Restrictions for Implementing Lawful Intercept 3

Benefits of Lawful Intercept 5

Configure the Lawful Intercept SNMP Server Configuration 5

Scale or Performance Values 6

Revised: December 11, 2020

What is Lawful Intercept?

The Lawful Intercept (LI) feature provides electronic surveillance as authorized by a judicial or administrative order for service provider routers. The surveillance is performed using wiretaps to intercept Voice-over-Internet protocol (VoIP) or data traffic going through the edge routers. The Law Enforcement Agency (LEA) delivers a request for a wiretap to the target's service provider, which is responsible for intercepting data communication using IP sessions.

This document explains the LI architecture, describes the components of the LI feature, and provides instructions for setting up the LI feature on a Cisco router.

Cisco lawful intercept is based on RFC 3924 architecture and SNMPv3 provisioning architecture. SNMPv3 addresses the requirements to authenticate the origin of the data 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.

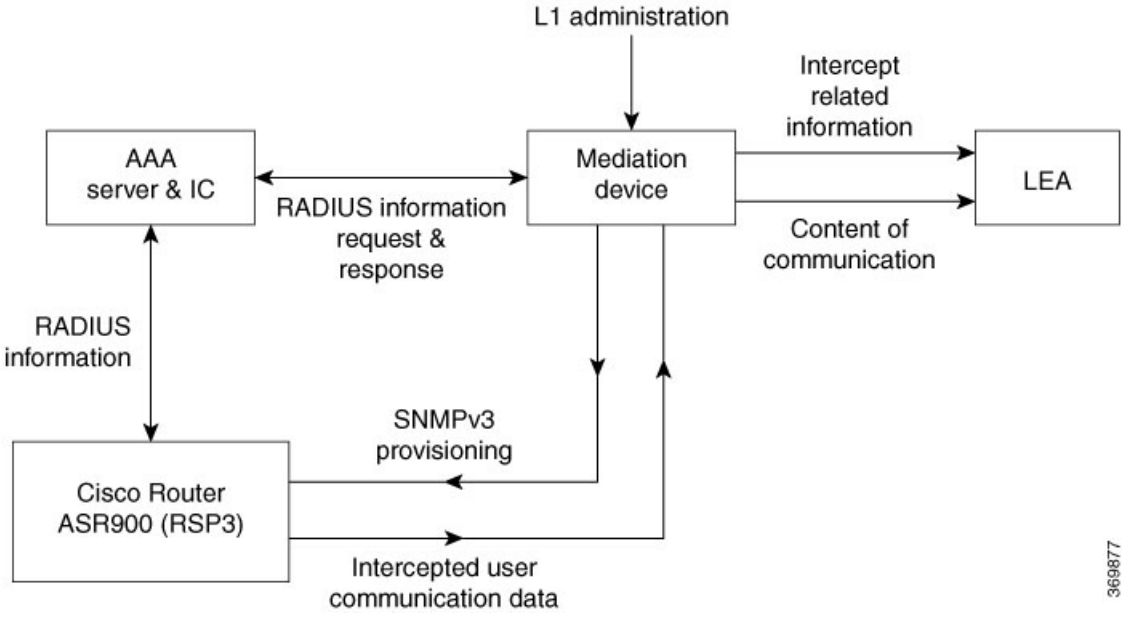
Lawful intercept offers these capabilities:

- SNMPv3 lawful intercept provisioning interface.
- Lawful intercept MIB: CISCO-TAP2-MIB, version 2.
- Lawful Intercept MIB for IP: CISCO-IP-TAP-MIB. This MIB manages the Cisco intercept feature for IP and is used along with CISCO-TAP2-MIB to intercept IP traffic.
- IPv4 user datagram protocol (UDP) encapsulation to the mediation device.
- Replication and forwarding of intercepted packets to the mediaton device.

Lawful Intercept Topology

This figure shows intercept access points and interfaces in a lawful intercept topology.

Figure 1: Lawful Intercept Topology



Prerequisites for Implementing Lawful Intercept

Lawful intercept implementation requires that these prerequisites are met:

- The mediation device (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 router, which is being used to intercept the target. The MD must be reachable from only the global routing table and not from the VRF routing table.
- You must **disable** these SDM templates for Lawful Intercept to work:

  enable_portchannel_qos_multiple_active

  enable_l3vpn_cm

  enable_egr_l3vpn_cm

Restrictions for Implementing Lawful Intercept

- 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. Lawful Intercept does not support RSP HA.The LI configuration needs to be reapplied after the RSP switchover. An SNMP trap is generated for this event.
- Only the mediation device and the users who need to know about lawful intercepts are allowed to access the LI MIBs.
- The provisioning of the RSP3 module, to enable lawful interception through SNMPv3, is supported for the following MIBs:

    - CISCO-TAP2-MIB
    - CISCO-IP-TAP2-MIB

- SNMP notifications for LI must be sent to **(UDP) port 161** on the mediation device, and not the SNMP default port 162.
- Lawful intercept is supported only to match IPv4 unicast over Ethernet packets.
- LI on the Cisco routers can intercept traffic based on a combination of one or more of the following fields:
    - IPv4 Source address and mask
    - IPv4 Destination address and mask
    - ToS (Type of Service) mask
    - Protocol ID
    - Destination port with range
    - Source port with range
    - VRF aware (IP to IP, IP to MPLS)
- Lawful intercept does not provide support for these features on the Cisco Router:
    - IPv6 multicast tapping
    - Per interface tapping for multiple TAPs
    - MPLS packet tapping
    - Multicast traffic tapping
    - GRE Tunneled traffic tapping
    - Replicating a single tap to multiple MDs
    - Tapping L2 flows
    - RTP encapsulation
    - LI and SPAN on the same interface
    - Intercept on Port-channel interface
- The intercepted packets are encapsulated using only UDP.
- Maximum bandwidth of 1 Gbps for each device is supported for LI intercept.
- In Cisco IOS XE Release 17.1.1, only single TAP per interface is supported. Effective from Cisco IOS XE Release 17.3.1, multiple TAPs per interface are supported.
- The TAP scale is reduced if TCP/UDP port range is specified in the TAP, one tap becomes multiple subtaps, and takes up more hardware resources.
- LI intercept Statistics not supported.
- The path to the MD or MD next-hop must have ARP resolved.

- Maximum of 16 different MD source interfaces is allowed. However, this value depends on the total number of tunnel interfaces with different source addresses on the device.
- Lawful Intercept shares a pool of 16 unique source IP addresses with tunnel-IP.
- The combined configuration of GRE tunnel-IPs and the MDs (the cTap2MediationSrcInterface field) does not yield more than 16 unique source IPs.
- Configuration of LI with Netconf yang model is not supported.
- If there is an ACL matching the LI tap, then ACL fails to work in presence of the LI.
- LI packets cannot be fragmented.
- The modification of MD and TAP is not supported . If there are changes, delete the older MD or TAP and create a new one.

Benefits of Lawful Intercept

Lawful intercept has the following benefits:

- It allows multiple LEAs to run a lawful intercept on the same Router without each other's knowledge.
- It does not affect subscriber services on the router.
- It supports wiretaps in both the input and output direction.
- It supports wiretaps of Layer 3 traffic.
- It cannot be detected by the target.
- It 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.
- It 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.

Configure the Lawful Intercept SNMP Server Configuration

The following SNMP server configuration tasks enable the Cisco LI feature on the Cisco router

Configuration

```
snmp-server group tapGroup v3 auth read tapView write tapView notify tapView
snmp-server view tapView iso included
snmp-server view tapView ciscoIpTapMIB included
snmp-server view tapView ciscoTap2MIB included
snmp-server community tap2Comm view tapView RW
snmp-server community private RW
snmp-server community public RO
snmp-server manager
snmp-server user tapUser tapGroup v3 auth md5 cisco123
```

Note SNMP configuration must be removed while deactivating the LI.

Verification

```
P1#sh snmp user
User name: tapUser
Engine ID: 8000000903007426ACF71912
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: tapGroup
P1#

P1#sh snmp view | in tap
tapView iso - included nonvolatile active
tapView ciscoIpTapMIB - included nonvolatile active
tapView ciscoTap2MIB - included nonvolatile active
P1#
```

Scale or Performance Values

- A maximum of 200 IPv4 MDs/TAPs are supported.

Note The scale decreases if port ranges are used in TAPs.

- Interception rate is 1 Gbps best effort for each Cisco router.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.