Implementing Lawful Intercept

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Lawful Intercept on Cisco NC57 line cards	Release 7.6.1	Lawful intercept is a process that requires 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. You can now activate and deactivate the lawful intercept package on routers that have Cisco NC57 line cards installed and operate in the native mode.

Lawful intercept is the lawfully authorized interception and monitoring of communications of an intercept subject. 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 .

For more information about activating and deactivating the Lawful Intercept package, see the Installing Lawful Intercept (LI) Package, on page 5 section.

Information About Lawful Intercept Implementation

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 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.
- **QoS Peering—** QoS peering must be enabled on the router for Lawful Intercept to work.

Note The Lawful Intercept feature has no intersection with the QoS feature on the router. Enabling the QoS peering profile with **hw-module profile qos ingress-model peering** command on all the required line cards, allows QoS and Lawful intercept to allocate hardware resources.

- 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 for Implementing Lawful Intercept

The following restrictions are applicable for Lawful Intercept:

- 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) shall not yield more than 16 unique source IPs. Note that when configuring the MD, if the value 0 is passed in for the cTap2MediationSrcInterface field, it will be resolved into a source IP address, which is the egress IP to the MD destination.
- Lawful intercept is supported only to match pure IP over Ethernet packets.
- Only 250 MDs and 500 Taps of IPv4 and IPv6 each 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.
- Only IPv4 MD is 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.
- In Cisco IOS XR Release 6.3.x, QoS peering must be enabled for QoS to work.

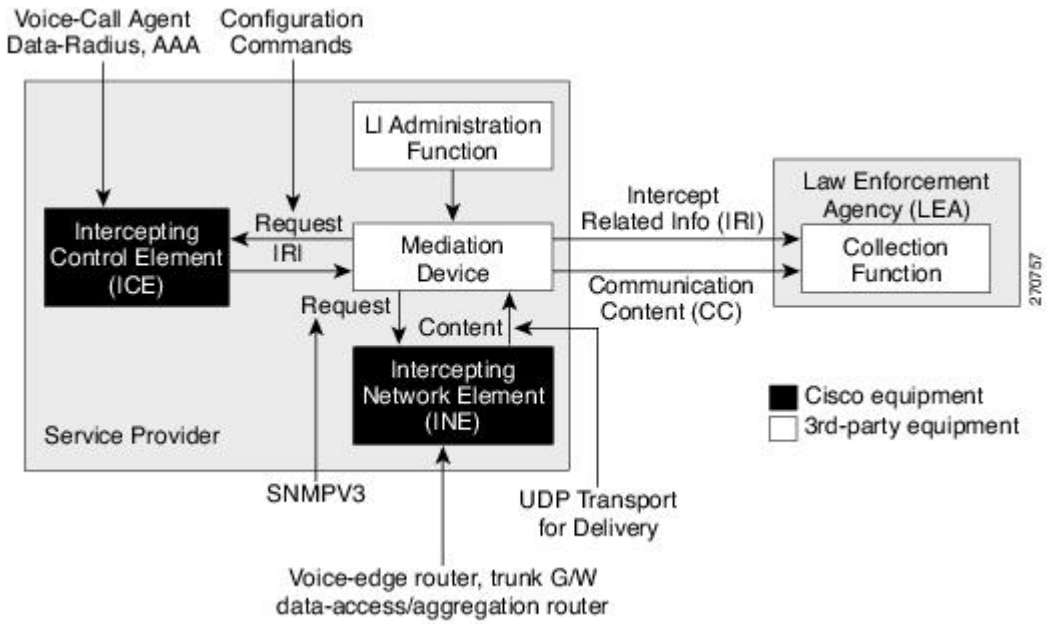
  In Cisco IOS XR Release 6.5.x and later, QoS peering is not required.
- Lawful Intercept has no intersection with the GRE Tunnel feature, except that they allocate hardware resources (16 unique egress IP addresses) from the same pool. In the normal case, the egress interface for the LI packets is decided by the forwarding algorithm. No resource is needed from that unique address pool. However, if the Lawful Intercept configuration mandates that the Lawful Intercept packets have to egress through a certain interface (the cTap2MediationSrcInterface field in the MD configuration), then the forwarding module must be configured so that the packets go out through that interface. In that case, a resource must be allocated from the unique address pool. If GRE uses up all resources, then LI does not work.
- 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.
- Lawful intercept does not provide support for these features on the router:
  - IPv4/IPv6 multicast tapping
  - IPv6 MD encapsulation

- 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

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 .

Configuration

```
Router# install add source tftp://223.255.254.252/auto/tftp-sjc-users/username/
Router# install activate
Router# install commit
```

Verification

```
Router# show install active
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv0
 Active Packages: 2



Node 0/0/CPU0 [LC]
  Boot Partition: xr_lcp_lv0
  Active Packages: 2
```

Deactivating the LI RPM

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

To uninstall the Lawful Intercept package, deactivate as shown in the following steps:

Configuration

```
Router# install deactivate
Router# install commit
Router# install remove
Router# show install committed
```

Lawful Intercept Enablement with Consent-Token

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
LI Enablement with Consent-Token	Release 7.5.1	This feature enables users to optionally gate the Lawful Intercept (LI) enablement on their routers with network vendor's consent, using a consent-token. It also provides an optional package to disable the LI feature for the first time on their routers. This feature is in compliance with the latest ANSSI (*Agence nationale de la sécurité des systèmes d'information*) security standards. Prior to this release, there was no gating for LI enablement on routers. The associated command is: • request consent-token

LI enablement with consent-token is an optional feature for users who want to comply with the latest ANSSI standards, which states that users require the network vendor's consent for enabling LI on their routers.

After you install and activate the LI package as mentioned in the section Installing and Activating the LI Package, on page 5, follow the steps below:

- Step 1: Disable LI feature on the router.
- Step 2: Enable LI feature with consent-token.

Step 1: Disable LI feature on the router:

You can either disable LI with consent-token or with the optional LI-control package:

- **Disable LI with Consent-Token:**

  The following steps show how to disable LI with consent-token:

1. Generate a challenge string to disable LI, by executing the command **request consent-token generate-challenge lawful-intercept disable** on the router.

```
Router# request consent-token generate-challenge lawful-intercept disable

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Challenge string:
pAoP8QAAAQYBAAQAAAAFAgAEAAAABQMACAAAAAAAAAAABAAQFAf7N2FWTaq3Du+bixEyUQUA
BAAA//8GAAxJT1MtWFItU1ctQ1QHAAxJT1MtWFItU1ctQ1QIAAdOQzU1LVJQCQALRk9DMjMxNTRNWVk=
```

2. Send the challenge-string to the network vendor offline. The network vendor uses Signing Servers to validate the challenge-string. And then sends the response-string back to you.
3. In the router console, enter the command **request consent-token accept-response lawful-intercept disable**. When prompted, enter the response string in the router console.

```
Router# request consent-token accept-response lawful-intercept disable
************************************************************
Please enter challenge response string for node location node0_RP0_CPU0
************************************************************
JkVs2AAAAQYBAAQAAAAFAgAEAAAABQMBYm9vZnY3ZUIraXpiY01ESWw1eGZ4TUlJbnZ4MUVQU2VN
VjJsL21uZFlLMXRpeUg5cGNHd1B5VEZHWk53YUVrZmoNCnZHdWpBaU1tNWtUb2VNM2ZYUURYeW5
LQVdnRVZvMXpveitkMlVvNm1xaXBMTlpwZ3YxSWpMdUZyY3VDb3R0bSsNClByRUp2WEZBd3ArUFJrT
042cW4vc3BPWm9JNjFDY2RZSW1Lc1VJOUpRbHNMdExxOZE9FZk1DaW80OEQrdUZTa1cNClhLbWhkN
Ek0bE5IaFplSDlaUVdLVmlYTWIwdDhNemhmR0dRTzFzRVlHaWNtZVhJWnoxaEZ4N1BVb1NVdFFIbjAN
CktaK0hFZ0YxaUU3YzVPdTV0bEJ4MmVHWjVxcWJ6YnBjVmFVTWxQZCtlRTEvWHlzYVAzL01kZTZYTDZ
GSVhlN2ENClc1Zzg0ZE1kbWNSRCtZSUZ3Vk5yeWc9PQ==

+--------------------------------------+
   Node location: node0_RP0_CPU0
+--------------------------------------+
Error code: 0
```

An output of **Error code: 0** means the router has disabled LI functionality successfully.

- **Disable LI with LI-control package:**

  This method is especially useful for a bulk disable of LI on multiple routers as it helps in avoiding multiple challenge-response requests. This package disables LI only for the first time on the router.

  Install and activate the LI-control package ncs5500-lictrl-1.0.0.0-r<*release-number*>.x86_64.rpm, as shown.

```
Router# install add source
tftp://223.255.254.252/auto/tftp-sjc-users/username/ncs5500-lictrl-1.0.0.0-r751.x86_64.rpm
Router# install activate ncs5500-lictrl-1.0.0.0-r751.x86_64.rpm
Router# install commit
```

  After its activation, the LI-control package gates the enablement of LI feature and disables any subsequent LI operations. It blocks the addition of any new MD or taps until the network vendor provides an offline consent. You can re-enable LI only through a consent-token process.

Step 2: Enable LI feature with consent-token

The following steps show how to enable LI with consent-token:

1. Generate a challenge-string to enable LI, by executing the command **request consent-token generate-challenge lawful-intercept enable** on the router.

```
Router# request consent-token generate-challenge lawful-intercept enable

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Challenge string:
pAoP8QAAAQYBAAQAAAAFAgAEAAAABQMACAAAAAAAAAAABAAQFAf7N2FWTaq3Du+bixEyUQUA
BAAA//8GAAxJT1MtWFItU1ctQ1QHAAxJT1MtWFItU1ctQ1QIAAdOQzU1LVJQCQALRk9DMjMxNTRNWVk=
```

2. Send the challenge-string to the network vendor offline. The network vendor uses Signing Servers to validate the challenge string. And then sends the response-string back to you.
3. On the router console, execute the command **request consent-token accept-response lawful-intercept enable**. When prompted, enter the response string in the router console.

```
Router# request consent-token accept-response lawful-intercept enable
************************************************************
Please enter challenge response string for node location node0_RP0_CPU0
************************************************************
JkVs2AAAAQYBAAQAAAAFAgAEAAAABQMBYm9vZnY3ZUIraXpiY01ESWw1eGZ4TUlJbnZ4MUVQU2VN
VjJsL21uZFlLMXRpeUg5cGNHd1B5VEZHWk53YUVrZmoNCnZHdWpBaU1tNWtUb2VNM2ZYUURYeW5
LQVdnRVZvMXpveitkMlVvNm1xaXBMTlpwZ3YxSWpMdUZyY3VDb3R0bSsNClByRUp2WEZBd3ArUFJrT
042cW4vc3BPWm9JNjFDY2RZSW1Lc1VJOUpRbHNMdExxOZE9FZk1DaW80OEQrdUZTa1cNClhLbWhkN
Ek0bE5IaFplSDlaUVdLVmlYTWIwdDhNemhmR0dRTzFzRVlHaWNtZVhJWnoxaEZ4N1BVb1NVdFFIbjAN
CktaK0hFZ0YxaUU3YzVPdTV0bEJ4MmVHWjVxcWJ6YnBjVmFVTWxQZCtlRTEvWHlzYVAzL01kZTZYTDZ
GSVhlN2ENClc1Zzg0ZE1kbWNSRCtZSUZ3Vk5yeWc9PQ==

+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Error code: 0
```

An output of **Error code: 0** means the router has enabled LI functionality successfully. You can now run LI commands and requests.

4. If needed, you can verify the pending consent-token requests using the following command:

```
Router# show ct requests
+-------------------------------------+
   Node location: node0_RP0_CPU0
+-------------------------------------+
Type:
        Enable LI     >>> Consent-token request to enable LI is awaiting challenge
response
+-------------------------------------+
   Node location: node0_5_CPU0
+-------------------------------------+
No existing Consent Token Requests >>> No consent-token request has been generated
+-------------------------------------+
   Node location: node0_4_CPU0
+-------------------------------------+
No existing Consent Token Requests

+-------------------------------------+
   Node location: node0_RP1_CPU0
+-------------------------------------+
No existing Consent Token Requests
```

Note Once enabled, if you want to disable LI, use the consent-token work-flow.

Restrictions for LI activation with Consent-Token

The following restrictions apply for this feature:

- This feature doesn't remove MDs and taps that you configured before installing the LI-control package **ncs5500-lictrl-1.0.0.0-rxyz.x86_64.rpm**.
- As a best practice, delete all MDs and taps before disabling LI with consent-token.

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 .

- 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 .

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. The lawful intercept is available on line cards where QoS peering is enabled. 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 IPv4 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 500 IPv4 intercepts and 500 IPv6 intercepts are supported.
- The scale decreases, if port ranges are used in the taps.
- The IPv6 entries consume double the memory of the IPv4 entries. Hence, the IPv6 scale will reduce to half of the IPv4 scale.
- A maximum of 250 IPv4 MDs are supported.

Note A maximum of 249 IPv4 MDs are supported on routers that have Cisco NC57 line cards installed and operate in the native mode.

- Interception rate is 1 Gbps best effort per Linecard NPU.

Note Interception rate is 2Gbps on routers that have Cisco NC57 line cards installed and operate in the native mode.

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 address
- Destination mask
- Source address
- Source mask
- ToS (Type of Service) and ToS mask
- L4 Protocol
- Destination port with range
- Source port with range
- VRF (VPN Routing and Forwarding)

Note Flow-id and inteface 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 and IPv6 packets are encapsulated using IPv4 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 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. 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.