Lawful Interception

Version 23.8.1.3, 10 November 2023

Registered Address	Support	Sales
26, Kingston Terrace, Princeton, New Jersey 08540, United States		
		+91 80 4850 5445
http://www.rtbrick.com	support@rtbrick.com	sales@rtbrick.com

Table of Contents

1. Introduction

Lawful Interception (LI) is a legal requirement in most of the countries. It enables the legal authorities to obtain communications network data for analysis or evidence. It is a method of intercepting certain data-streams of end-users in both directions, and tunnel the intercepted traffic to a Mediation Device (MD) with information about direction of capture and reference to the intercepted connection.

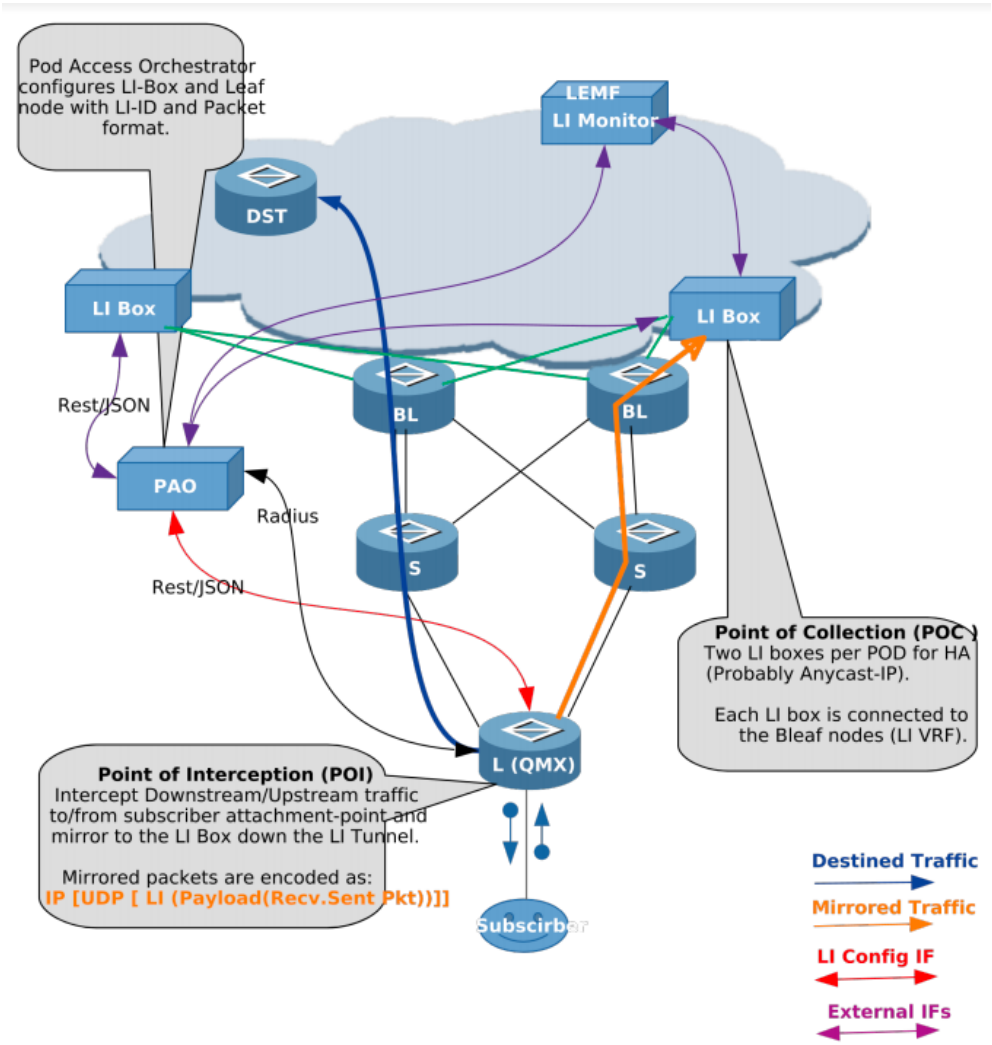
Leaf node is the Point of Interception (POI) and MD is the final Point of Collection (POC).

1.1. Supported Platforms

Not all features are necessarily supported on each hardware platform. Refer to the *Platform Guide* for the features and the sub-features that are or are not supported by each platform.

1.2. Components of Lawful Interception

The figure below shows the different components of the LI solution.



Definitions

L(QMX)

Leaf node in the POD which is connected to subscribers.

S/BL

Spine and Border Leaf in the POD, which can be replaced with just one node.

LI Box

Lawful Intercept Box, which communicates to Law Enforcement Agency (LEMF) and relays mirrored traffic. Two LI boxes per POD are connected for redundancy.

PAO

POD Access Orchestrator, which configures the LI Box and network nodes with LI configurations.

DST

Destination node for traffic from subscribers.

Abbreviations

Abbreviation	Definition
LI	Lawful Interception
POI	Point of Interception
POC	Point of Collection
PAO	Pod Access Orchestrator
LIMS	Lawful Interception Management System
VRF	Virtual Routing Instance
LEMF	Lawful Enforcement Monitoring Facility
Leaf	Access node
PPPoE	Point to Point Protocol over Ethernet
L2TP	Layer 2 Tunnelling Protocol
MPLS	Multi Protocol Label Switching

1.3. Guidelines & Limitations

- The unidentified LI traffic is subject to the following limitations when using more than seven UDP ports.
  Currently, there is a restriction on UDP destination ports, which are limited to 7. The IP destination addresses (IP1 through IPn) can utilize any of the seven ports. The distribution of these seven ports is determined by the order in which requests are received, with priority given to those who arrive first.
- All upstream packets, regardless of whether they were dropped or not, are intercepted and mirrored to the LI collection entity.
  The following are some of the reasons that could cause dropped packets, but LI will still intercept and mirror traffic to LI collection.
  - A routing failure occurred. This is unlikely as there is a default route to the spine.
  - The RPF check has failed.
  - The policer was dropped.
  - The ACL/filter was dropped.

This limitation does not apply to downstream packets.

2. LI Encapsulation

Qumran-MX (BCM) supports LI with 32 bits shim header: SHIMoUDPoIPoETH

2.1. Packet Format Encoding

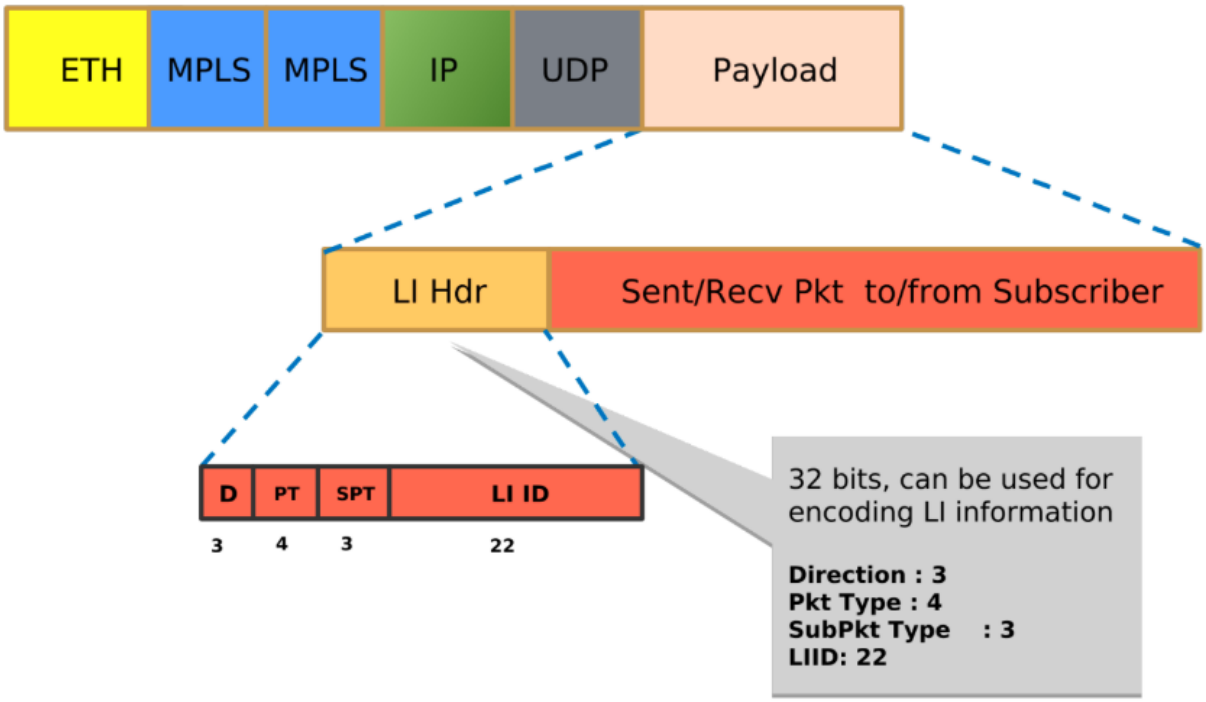


Figure 1. Packet Format Encoding

2.1.1. Payload Direction

Value	Payload Direction
0	Reserved for keepalive mechanism
2	Intercepted data or event was sent to target (downstream)
3	Intercepted data or event was sent from target (upstream)

2.1.2. Mapping Payload Format

Value	Payload Format
0-3	Reserved (unused)
4	Unknown, Not able to decide the PT
5	IPv4 packet (not used)
6	IPv6 packet (not used)
7	Ethernet Frame (used for Lawful Interception)

2.1.2.1. Sub-payload Format (Type)

The sub-payload formats are:

1. Single VLAN tag
2. Double VLAN tag
3. Untagged

3. Enabling Lawful Interception

- RBFS 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.
- LI can be enabled for both L2TP and PPPoE subscribers.

3.1. RADIUS Lawful Interception

All of the following attributes must be present in RADIUS access-accept or CoA request to control Lawful Interception (LI) via RADIUS. Those attributes are salt encrypted using the algorithm described in RFC 2868 for the Tunnel-Password. This encryption algorithm is defined for RADIUS access-accept messages only. To support CoA requests the request authenticator should be replaced with 16 zero bytes which is common industry standard.

RFC and draft compliance are partial except as specified.

The LI action NOOP can be used to obfuscate lawful interception requests (fake requests) to prevent that just the presence of those attributes indicates that a subscriber is intercepted. LI requests via RADIUS will show up in the same table as requests via REST or HTTP RPC API (secure.lawful.access.1.li_request).

The failed LI activations are not signalled via RADIUS to prevent that just the presence of CoA response NAK shows that LI request is not fake (action NOOP).

VSA 26-50058-140 - RtBrick-LI-Action (salt encrypted integer)

Value	Code	Description
NOOP	0	No action / Ignore LI request
ON	1	Start LI / Add LI request
OFF	2	Stop LI / Delete LI request

VSA 26-50058-141 - RtBrick-LI-Identifier (salt encrypted integer)

Device unique lawful interception identifier (LIID) within the range from 1 to 4194303.

VSA 26-50058-142 - RtBrick-LI-Direction (salt encrypted integer)

Value	Code	Description
INGRESS	1	Ingress mirroring only (from subscriber)
EGRESS	2	Egress mirroring only (to subscriber)
BOTH	3	Bidirectional mirroring (from and to subscriber)

VSA 26-50058-143 - RtBrick-LI-MED-Instance (salt encrypted string)

Routing instance through which the mediation device is reachable.

VSA 26-50058-144 - RtBrick-LI-MED-IP (salt encrypted IPv4 address)

IPv4 address of the mediation device.

VSA 26-50058-145 - RtBrick-LI-MED-Port (salt encrypted integer)

UDP port between 49152 and 65535 set in the mirrored traffic

3.2. RBFS Operational State API

The RBFS Operational State API provides endpoints for enabling and disabling LI on a per-subscriber basis:

- A HTTP POST request to /subscribers/{subscriber_id}/enableLI?id={li_id}&direction={li_direction}&med_ip={med_ip}&med_instance={med_instance}&med_port={med_port} enables LI for the specified subscriber
- A HTTP POST request to /subscribers/{subscriber_id}/disableLI?id={li_id} disable LI for the specified subscriber

The table below lists the request parameters:

Parameter Name	Description
subscriber_id	Subscriber identifier that is generated by RBFS, for example, 72339069014638701.
id	Identifier for Lawful Interception. This is unique Identifier used by mediation device to identify the intercepted subscriber. The range can be between 1 to 4194303.
direction	LI direction. Values are: INGRESS, EGRESS, BOTH.
med_instance	VRF instance through the which the mediation device is reachable.
med_ip	IPv4 address of the mediation device
med_port	UDP port(MD)(49152-65535), mirrored traffic is forwarded

All parameters are mandatory to enable LI.

3.2.1. Request Examples

3.2.1.1. Enabling LI

The example below shows a curl command to enable LI:

```
curl -i -H "Content-Type: application/json" -X POST -d
http://198.51.100.76:19091/api/v1/rbfs/elements/rtbrick/services/opsd/proxy/subscr
ibers/72339069014639042/enableLI?id=66666&direction=BOTH&med_instance=libox&med_ip
=10.0.0.1&med_port=49153
```

3.2.1.2. Disabling LI

The example below shows a curl command to disable LI.

```
curl -i -H "Content-Type: application/json" -X POST -d
http://198.51.100.76:19091/api/v1/rbfs/elements/rtbrick/services/opsd/proxy/subscr
ibers/72339069014639042/disableLI?id=66666
```