

Lawful Intercept for cnBNG

- Lawful Intercept for cnBNG, on page 1
- How cnBNG LI works, on page 2
- Configure LI for cnBNG subscriber session, on page 4
- Redundancy Handling, on page 4
- Call flow for LI provisioning, on page 5
- Packet format, on page 6

Lawful Intercept for cnBNG

Lawful intercept (LI) is a surveillance framework that enables law enforcement agencies (LEAs) to conduct electronic surveillance as authorized by a judicial or administrative order.

The cnBNG LI feature is a lawful intercept capability that

- identifies the target subscriber session
- specifies the mediation device destination to which the target subscriber's traffic is copied, and
- ensures that duplicated subscriber traffic is sent to the mediation device without changing the subscriber's normal forwarding behavior.

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Lawful Intercept for cnBNG	Release 2021.01.0	Enables service providers to meet lawful intercept compliance requirements while maintaining normal subscriber traffic forwarding.RADIUS-driven support identifies target PPPoE and IPoE subscriber sessions and replicates their traffic to an authorized mediation device in the default or a nondefault VRF.

cnBNG supports LI as a RADIUS-driven subscriber control function for both PPPoE and IPoE subscribers. The LI workflow is initiated and controlled exclusively through AAA/RADIUS signaling, and is not supported through cnBNG-local configuration or northbound management APIs.

RADIUS-driven LI for cnBNG subscriber sessions

Service providers require a secure, automated method to replicate traffic from specific PPPoE or IPoE subscriber sessions to an authorized Mediation Device (MD) for lawful interception.

The challenge without native LI integration:

- The network cannot dynamically identify or target subscriber sessions via AAA.
- Operators must rely on manual, device-specific traffic mirroring, which is operationally complex and lacks standardized intercept identifiers.
- Interception cannot be centrally managed; the RADIUS server cannot dynamically start or stop monitoring for active sessions.
- The user plane lacks the necessary MD destination and LI parameters to facilitate automated traffic delivery.

cnBNG supports RADIUS-based Lawful Intercept, enabling centralized control over traffic replication. By utilizing `Access-Accept` or `CoA-Request` packets, the RADIUS server dynamically pushes LI parameters—including MD destination, port, and intercept identifiers—directly to the network access server (NAS) or L2TP access concentrator (LAC).

How cnBNG LI works

Summary

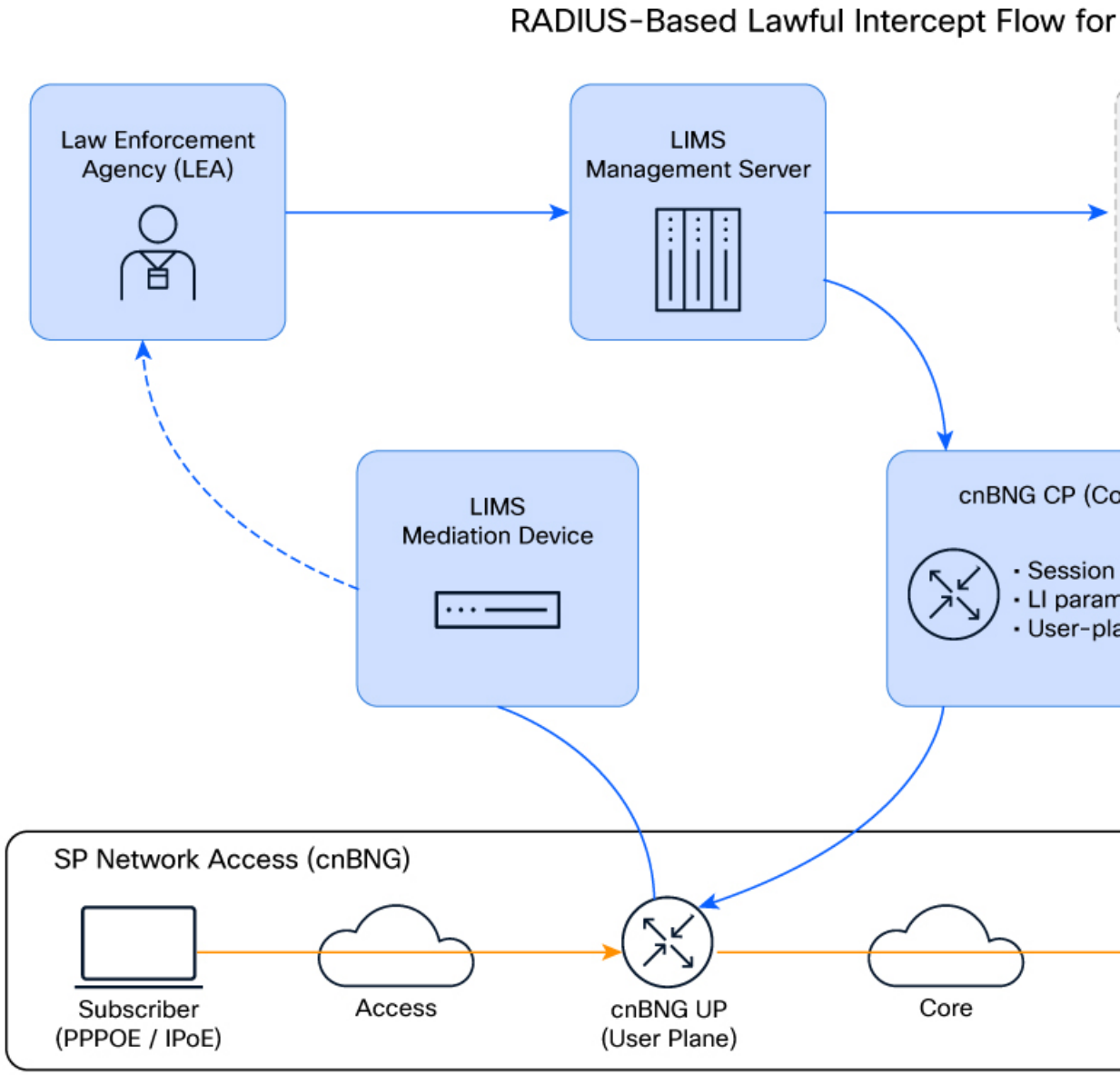
The key components involved in the cnBNG LI process are:

- RADIUS server: Provides LI Cisco VSA attributes via Access-Accept or CoA-Request messages.
- cnBNG: Acts as the LI control input; it parses LI parameters and transparently forwards them to the user-plane.
- cnBNG user-plane: Executes the actual subscriber traffic duplication and mediation-device delivery.
- Mediation device: Receives the duplicated subscriber traffic.

The process involves identifying the target subscriber session, conveying the mediation device destination, and ensuring the replicated copy is sent without altering the subscriber's normal forwarding behavior.

Workflow

Figure 1: Radius-Based LI flow



These stages describe how the cnBNG LI process works.

1. RADIUS attribute reception: The RADIUS server sends LI Cisco VSAs in either an Access-Accept packet (for new sessions) or a CoA-Request packet (for existing sessions).

   The cnBNG parses these attributes as LI service parameters.

   - md-ip-addr / md-ipv6-addr: Specifies the MD address.
   - md-port: Specifies the MD UDP destination port.
   - md-dscp: Specifies the DSCP value for replicated traffic.

- intercept-id: Identifies the intercepted subscriber traffic.
- li-action: Starts (1), stops (0), or validates (2) the intercept.

2. Subscriber context binding: The cnBNG binds the parsed LI parameters.
3. User-plane programmingThe cnBNG forwards the LI service parameters transparently to the cnBNG UP:
   - For new sessions, parameters are sent in the Session Establishment Request.
   - For existing sessions, parameters are sent in the Session Modification Request

   The duplicating parameters grouped information element (IE) conveys LI parameters within these messages, consisting of these attributes:
   - Destination interface
   - outer header creation
   - BNG LI info
   - BNG LI id

   Note: The cnBNG Duplicating Parameters IE is implemented in accordance with the ETSI 29.244 standard.
4. Traffic interception and duplicationThe user-plane receives the programming. Subscriber traffic is then intercepted and duplicated toward the mediation device.

Configure LI for cnBNG subscriber session

LI for cnBNG subscriber sessions is enabled by default and requires no local configuration. To initiate interception, ensure the following attributes are configured on the RADIUS server:

- md-ip-addr or md-ipv6-addr: Specifies the mediation device (MD) address.
- md-port: Specifies the MD UDP destination port.
- md-dscp: Specifies the DSCP value for replicated traffic.
- intercept-id: Identifies the intercepted subscriber traffic.
- li-action: Starts, stops, or validates the intercept.

Redundancy Handling

- SRG or UP Redundancy: During session establishment, the cnBNG propagates the duplicating parameters to both the active and standby user planes. This ensures that in the event of an SRG switchover, the standby UP is already provisioned with the correct mediation device details, allowing for seamless traffic replication.
- CP Redundancy: CP redundancy has no impact on LI operations, as the session state and LI parameters are synchronized or re-established as part of the standard CP failover process.

Call flow for LI provisioning

Figure 2: New subscriber session

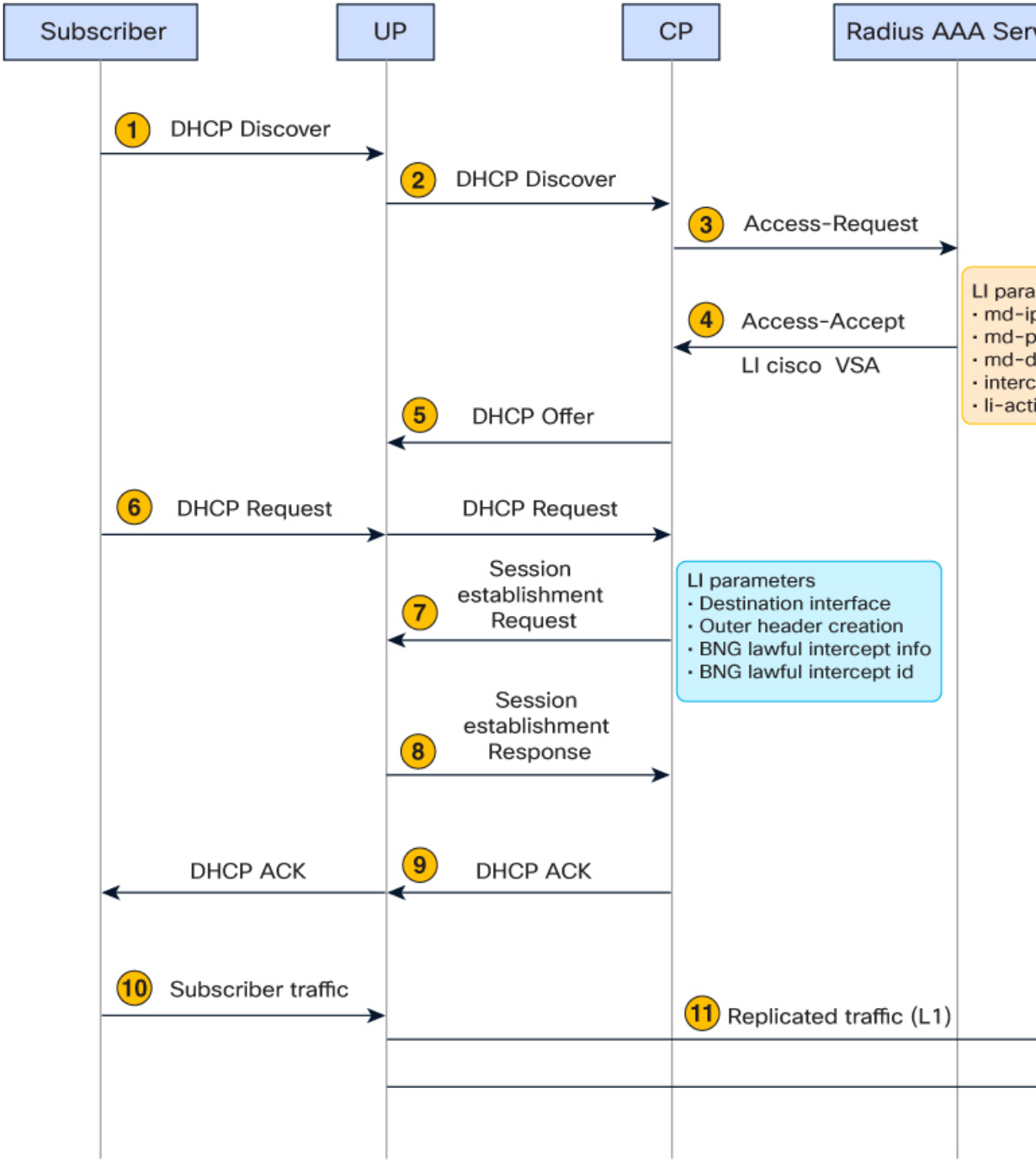
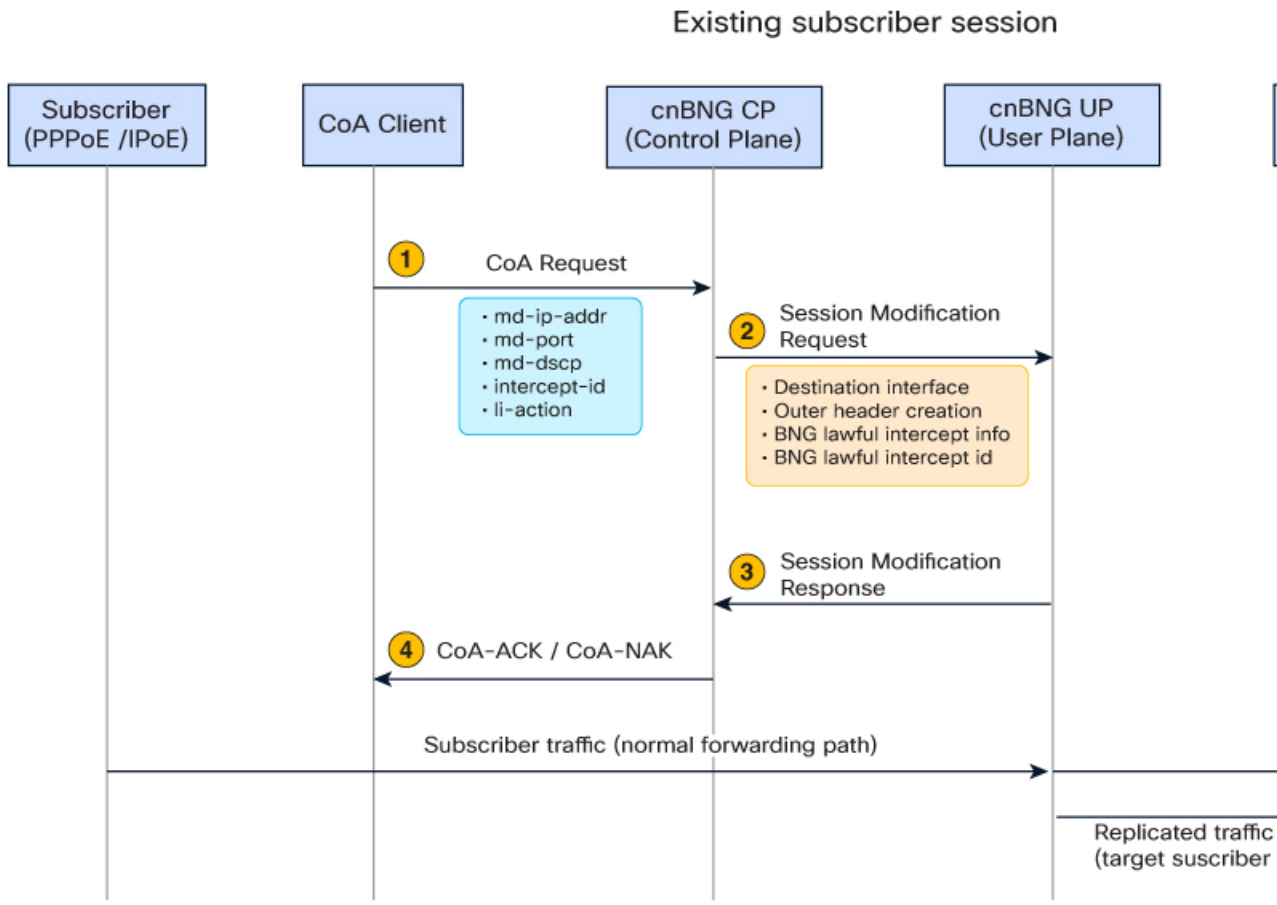


Figure 3: Existing subscriber session



Packet format

Access-Accept message with li Cisco AVP

```
 Subscriber Id: aa11.0000.0001@automation-userplane
      Message: RadiusUdpProxyMsg
      Description: Received Auth/Acct Response Message from UDP-Proxy
      Source: bng.udp-proxy.DC.Local.0
      Destination: bng.radius-ep.DC.Local.0

      PAYLOAD:
        RadiusUdpProxyMsg:
            RadiusUdpProxyMsg:
                SrcIp: 10.1.6.218
                SrcPort: 1812
                DestIp: 10.1.0.58
                DestPort: 16384
                Payload:

Code = AccessAccept
Id = 23
Authenticator = [143 103 48 233 240 179 78 238 166 222 143 157 215 13 172 152]
```

```
Cisco-Vsa_Cisco-AVpair_1 = "intercept-id=abcd3235"
Cisco-Vsa_Cisco-AVpair_1 = "md-ip-addr=20.0.0.xx"
Cisco-Vsa_Cisco-AVpair_1 = "md-port=4546"
Cisco-Vsa_Cisco-AVpair_1 = "md-dscp=7"
Cisco-Vsa_Cisco-AVpair_1 = "li-action=1"
               PayloadLen: 133
               SrcIpv6:
               DestIpv6:
               IsIpv6: false
```

Packet format of CoA-Request

```
Subscriber Id: aa11.0000.0001@automation-userplane-stby
      Timestamp: 2026/10/06 11:22:53.443569
      Message: RadiusUdpProxyCoaMsg
      Description: Received COA/DM Request Message from UDP-Proxy
      Source: bng.udp-proxy.DC.Local.0
      Destination: bng.radius-ep.DC.Local.0
      PAYLOAD:
        RadiusUdpProxyCoaMsg:
            RadiusUdpProxyCoaMsg:
               SrcIp: 10.1.6.218
               SrcPort: 55291
               DestIp: 10.1.0.58
               DestPort: 2000
               Payload:

Code = CoARequest
Id = 8
Authenticator = [197 92 21 13 169 188 0 98 55 89 118 223 25 23 60 84]
Acct-Session-Id = "01000007"
Cisco-Vsa_Cisco-AVpair_1 = "md-ip-addr=192.0.2.10"
Cisco-Vsa_Cisco-AVpair_1 = "li-action=1"
Cisco-Vsa_Cisco-AVpair_1 = "md-port=5000"
Cisco-Vsa_Cisco-AVpair_1 = "intercept-id=a0000312"

               PayloadLen: 127
               SrcIpv6:
               DestIpv6:
               IsIpv6: false
```