L3DL
Layer 3 Discovery & Liveness
draft-ietf-lsvr-l3dl-06

LSVR WG
2020.07.30

randy@psg.com, sra@hactrn.net, keyur@arrcus.com
Primary Goal

Layer 3 Topology Discovery and Liveless for LSVR / BGP-SPF
Just a Reminder
This is NOT a Routing Protocol

Discovers the Layer 3 Addresses on a PointToPoint Link
Jörg Ott did a Very Helpful Transport Directorate Early Review
You Read the Draft

Then why did you not report the bugs Rob did yesterday?
06 Published
No Significant Change
We have Two Implementations
One Python3 (LSOE)
One in Golang
L3DL-Signing

Layer 3 Discovery and Liveness Signing

draft-ietf-lsvr-l3dl-signing

LSVR WG

2020.07.30

randy@psg.com, sra@hactrn.net, keyur@arrcus.com
OPEN PDU

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

PDU Type = 1 Payload Length

Nonce

LLEI Length My LLEI

AttrCount

Attribute List...

Auth Type Key Length

Key...

Serial Number

Sig Type Signature Length Signature ...
PDU Sender Signing

• The Key in the OPEN PDU SHOULD be the public key of an asymmetric key pair.
• The sender signs with the private key, of course.
• The device sending the OPEN may use one key for all links, a different key for each link, or some aggregation(s) thereof.
Trust on First Use (TOFU)

• The OPEN key is generated on the sending device
• It is believed without question by the receiver
• Used to verify all subsequent PDUs from the same sender with the same Key Type.
PKI-Based Keying

- An enrollment step is performed.
- The public key is put into a certificate, which is signed by the operational environment's trust anchor.
- The relying party can be confident that the public key is under control of the identified L3DL protocol entity.
Do Not Be Afraid
This is NOT X.509

• These need not be X.509 certificates
• X.509 is much more complicated than we need
• They are just signatures of one key (the session key supplied in the Key field of the OPEN PDU) by another key (the trust anchor)
• Every device must have TA burned in
The two methods are indistinguishable.

The key provided in the OPEN PDU is used to verify the signatures of subsequent PDUs.

The difference that PKI-based keys may be verified against the trust anchor when the OPEN PDU is received.
The Choice of Which Keying is Left to the Operator
WG Last Call was Requested
Datatracker does not show WGLC
L3DL-ULPC
Upper Layer Protocol Configuration
draft-ietf-lsvr-l3dl-ulpc-00
LSVR WG
2020.07.30
randy@psg.com, sra@hactrn.net, keyur@arrcus.com
**L3DL PDU for ULPC**

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

```
+----------------------------------------------------------------------------------+
<table>
<thead>
<tr>
<th>Type = 9</th>
<th>Payload Length</th>
<th></th>
</tr>
</thead>
</table>
+-------------------------+----------------+------------------------------------------------|
| ULPC Type | AttrCount |                                    |
+-------------------------+----------------+------------------------------------------------|
| Attribute List ... | Sig Type | Signature Len |                                    |
+-------------------------+----------------+------------------------------------------------|
| Signature ... |                |                                      |
+----------------------------------------------------------------------------------+
```
Provide the \textbf{minimal set of configuration parameters} for BGP OPEN to succeed
Not to replace or conflict with data exchanged by BGP OPEN
Multiple sources of truth are a recipe for complexity and pain
ULPC for BGP

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Attr Type = 1 | Attr Len = 48 | My ASN ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Attr Type = 2 | Attr Len = 56 | My IPv4 Peering Address ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|
Prefix Len |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Attr Type = 4 | Attr Len | BGP Authentication Data ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Yes, there is one for IPv6 😊
Requested WGLC DataTracker does not show it
And For Dessert
An Ops Hack
(not a draft)
At Layer 3
With L3DL