History

- Rev00 was published on October 2018 and presented at IETF 103 in Bangkok
- Rev01 was published on March 2019 and presented at IETF 104 in Prague
- Rev02 was published on July 2019
- Rev03 was published on July 2020
Background & Solution Overview

- Secure control channel between each PE and the RR (e.g., using existing scheme such as IKv2)
  - Setup BGP session over this secure tunnel
- Use this secured BGP channel for P2MP signaling to establish P2P IPsec SAs for user traffic
  - No need for P2P signaling to establish P2P SA
  - Reducing # of msg exchanges from O(N^2) to O(N)
Solution Overview (2)

- When a PE device first comes up and wants to setup an IPsec SA between itself and each of the interested remote PEs, it generates a DH pair for each of its intended IPsec SA using an algorithm defined in the IKEv2 Diffie-Hellman Group Transform IDs [IKEv2-IANA].

- The originating PE distributes DH public value along with a nonce (using IPsec Tunnel TLV in Tunnel Encapsulation Attribute) to other remote PEs via the RR.

- Each receiving PE uses this DH public number and the corresponding nonce in creation of IPsec SA pair to the originating PE.
Changes

- **Rev01**
  - Added the requirements for setting up an IPsec tunnel between a pair of ASs between ingress and egress PEs
  - Added a new section on “Inheritance of Security Policy”
  - Modified IPsec Tunnel Attribute sub-TLVs for better optimization

- **Rev02**
  - Added sections on Zero Touch Bring-up (ZTB), Configuration Management, Orchestration, and Signaling

- **Rev03**
  - Refresh
Granularity of IPSec Tunnels for different VPNs

<table>
<thead>
<tr>
<th>Functionality</th>
<th>EVPN</th>
<th>IP-VPN</th>
<th>MVPN</th>
<th>VPLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>per tenant</td>
<td>IMET (or new)</td>
<td>lpbk (or new)</td>
<td>I-PMSI</td>
<td>N/A</td>
</tr>
<tr>
<td>per subnet</td>
<td>IMET</td>
<td>N/A</td>
<td>N/A</td>
<td>VPLS AD</td>
</tr>
<tr>
<td>per IP</td>
<td>EVPN RT2/RT5</td>
<td>VPN IP rt</td>
<td>*,G or S,G</td>
<td>N/A</td>
</tr>
<tr>
<td>per MAC</td>
<td>EVPN RT2</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Next Step

- Has been around for about 2 years
- It has been stable for over a year
- It is ready for WG adoption call
THANK YOU!