Challenges of the SRv6 Deployments and Operations

Tianji Jiang / Yisong Liu

China Mobile

IETF-119 SRv6 Operations BoF, March 2024
Agenda

• China Mobile: A gigantic SRv6 network with C-SID Deployment
• The ‘horizontal’ challenge: Multi-vendor interoperability
• The ‘vertical’ challenge:
  • Day-0: The planning of Compressed SRv6 SID
  • Day-1: The deployment of the Inter-AS E2E network
  • Day-2: Achieving the operational excellence with protection & failure detection
China Mobile: SRv6 C-SID Deployment

- China Mobile deployed SRv6 C-SID in Cloud Private Network
- Beyond 800+ nodes in Cloud Backbone Network
- Single AS and Single layer SDN Controller to distribute SRv6 C-SID

- China Mobile deployed SRv6 C-SID in CMNet
- Beyond 10k+ nodes in CMNet backbone and metros
- Multi-AS and unified SDN Controller to distribute E2E SRv6 C-SID path
The ‘Horizontal’ Challenge: Multi-vendor Interoperability

The challenge:
• Each vendor uses its proprietary controller to deploy the brand-name devices
• An operator has to deploy a super controller to manage the versatile device controllers of all the vendors
• increasing deployment complexity and might result in high failure probability

To remedy:
• The deployment of a fully decoupled single-layer controller for various vendors devices
• unified southbound interface and unified control protocol for greatly simplified deployment
The ‘vertical’ challenge: Day-0: Planning of Compressed SRv6 SID

**Compressed SID**

- Allocate separate prefix for SRv6 SID in IPv6 address space, due to the high aggregation of SIDs, boundary devices have simple ACL policy configuration to prevent SID information leakage.

**Uncompressed SID**

- Coexistence of uncompressed and compressed SID in the same locator (C-SID and 128 bits uncompressed SID in the figure as example).

- Allocate network layer IDs in Node ID field based on administrative regions like cities, counties etc., and then continue to assign specific Node IDs in every administrative region.

---

The ’vertical’ challenge: **Day-1: Deployment of Inter-AS E2E Network**

- SDN controller collects the topology and SID information of the entire network by BGP-LS, calculate the inter-AS compressed SRv6 Policy that meets the SLA, and distribute the policy to the headend node.
- SDN Controller distributes VPN configuration by netconf, and inject VPN traffic into the corresponding compressed SRv6 Policy based on color or routing policies.
- Full path compressed SID list better than assigning BSID to every AS, fully utilize compression to improve packet transmission efficiency.
The ‘vertical’ challenge: Day-2: Achieving operational excellence via Protection and Failure Detection

<table>
<thead>
<tr>
<th>Protection</th>
<th>failure point</th>
<th>protection deployment</th>
<th>failure detection deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hot-standby</td>
<td>1&amp;2</td>
<td>• Establish the primary and backup paths (both use C-SID)</td>
<td>• Echo BFD or pathsegment to ensure BFD detection bidirectional paths consistency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Detect failure in the primary path and the head node finish a quick switch</td>
<td>• Adjust the detection time according to the actual situation of the network to prevent network instability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Deploy the SRv6 BE escape mechanism, Used for both primary and backup paths to fail</td>
</tr>
<tr>
<td>VPN FRR</td>
<td>3</td>
<td>• Ingress PE establish C-SID path to both primary and backup egress PEs in advance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Detect failure in the primary egress PE, ingress PE finish a quick switch to backup egress PE by VPN FRR</td>
<td></td>
</tr>
<tr>
<td>TI-LFA</td>
<td>2</td>
<td>• A fast rerouting protection mechanism based on IGP</td>
<td>• BFD detection time is related to transmission distance delay, adjust the detection time according to the actual situation of the network to prevent network instability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Establish a backup path in advance</td>
<td>• If deploying hot standby at the same time, trigger local protection first, set the detection time path BFD is greater than local BFD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Switch quickly from adjacent upstream nodes to the backup path when detect failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Repair list should use C-SID list</td>
<td></td>
</tr>
</tbody>
</table>

In summary, we have to tackle both the ‘horizontal’ challenge (i.e., multi-vendor interoperability) and the ‘vertical’ challenge (i.e., the holistic considerations of day-0 (planning), day-1 (deployment) and day-2 (operations)).

The whole practice involves inevitably different technologies: SRv6 + SDN controller + BGP + IGP + VPN + v6Ops...

There is currently no suitable place in IETF to handle this type of interoperable & managerial challenges in a holistic way...

So, let’s form a WG, i.e., the SRv6-OPs, to get it under control & also share any best practice.
Thanks