Considerations in Compressed SRv6 Deployments and Operations

Presenter : Yisong Liu (China Mobile)

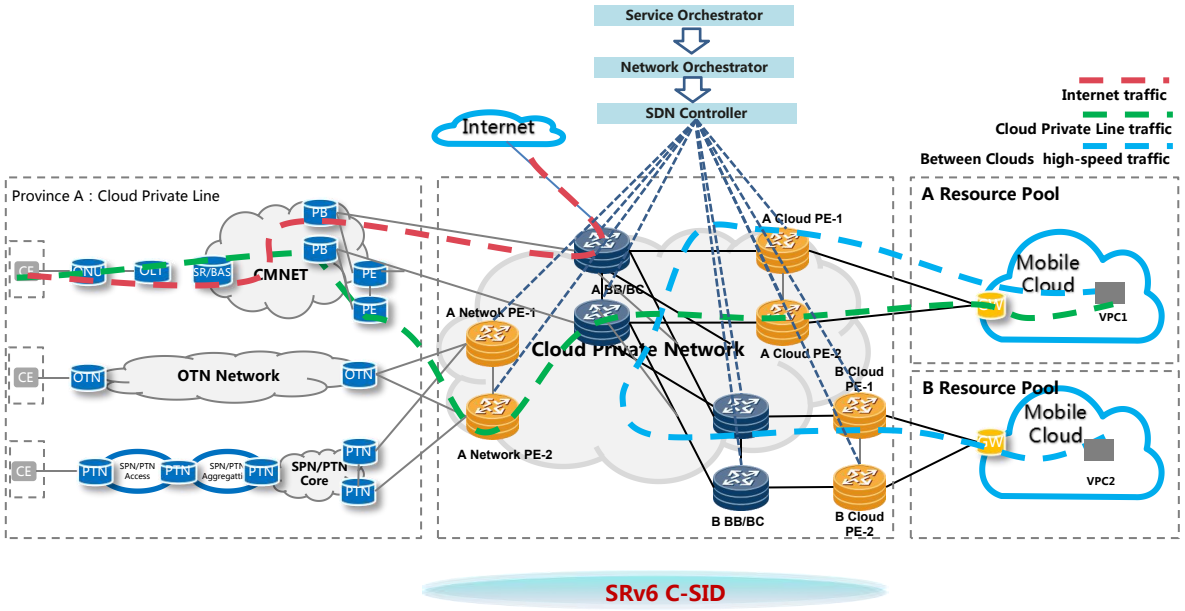
IETF-118 SRv6 Operations Side Meeting, November 2023

Agenda

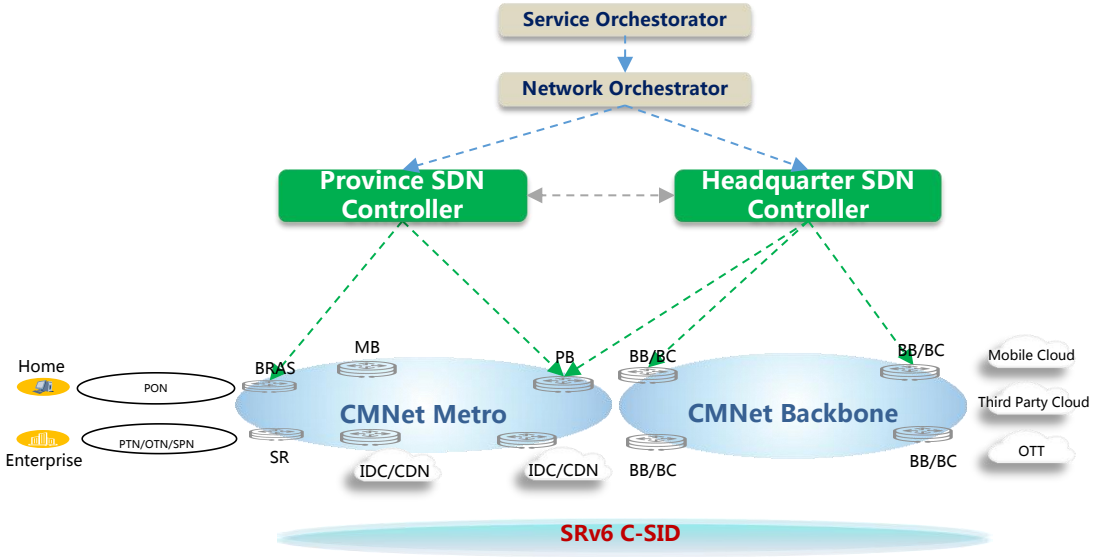
- SRv6 C-SID Deployment Status in China Mobile
- Multi-vendor Interoperation Management
- Inter-AS E2E Deployment
- Protection and Failure Detection Deployment
- Compressed SRv6 SID Planning
- Security Considerations for Deployment

SRv6 C-SID Deployment in China Mobile

Cloud Private Network



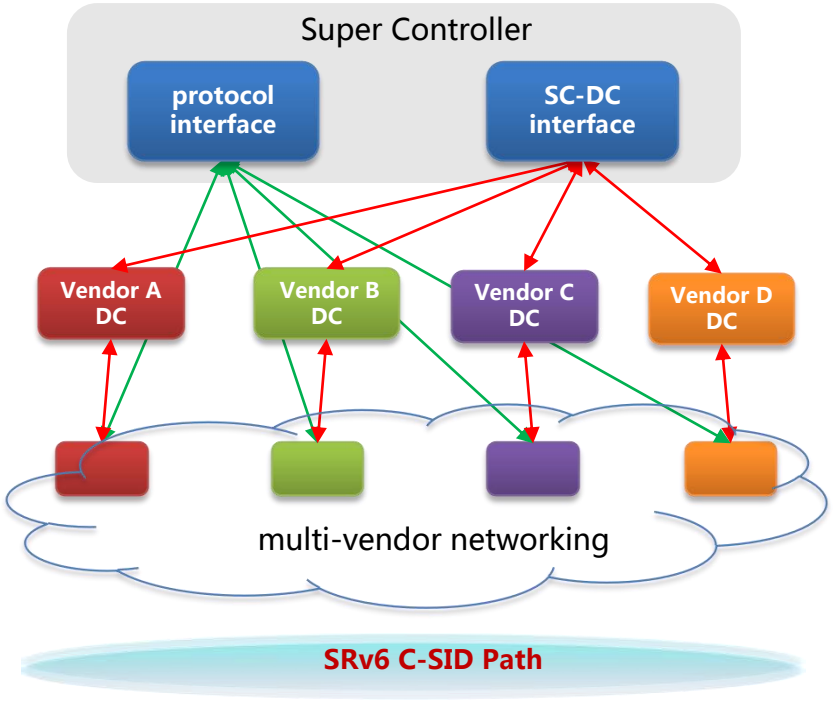
CMNet

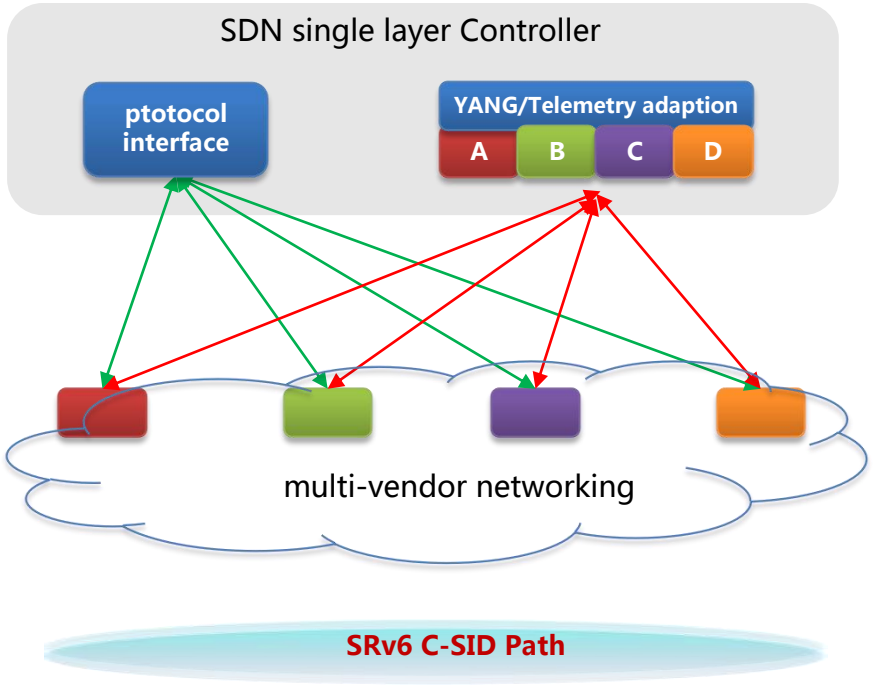


- China Mobile deployed SRv6 C-SID in Cloud Private Network
- Beyond 800+ nodes in Cloud Backbone Network
- Single AS and Single layer SDN Controller to distribute SRv6 C-SID

- 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

Multi-vendor Interoperation Management

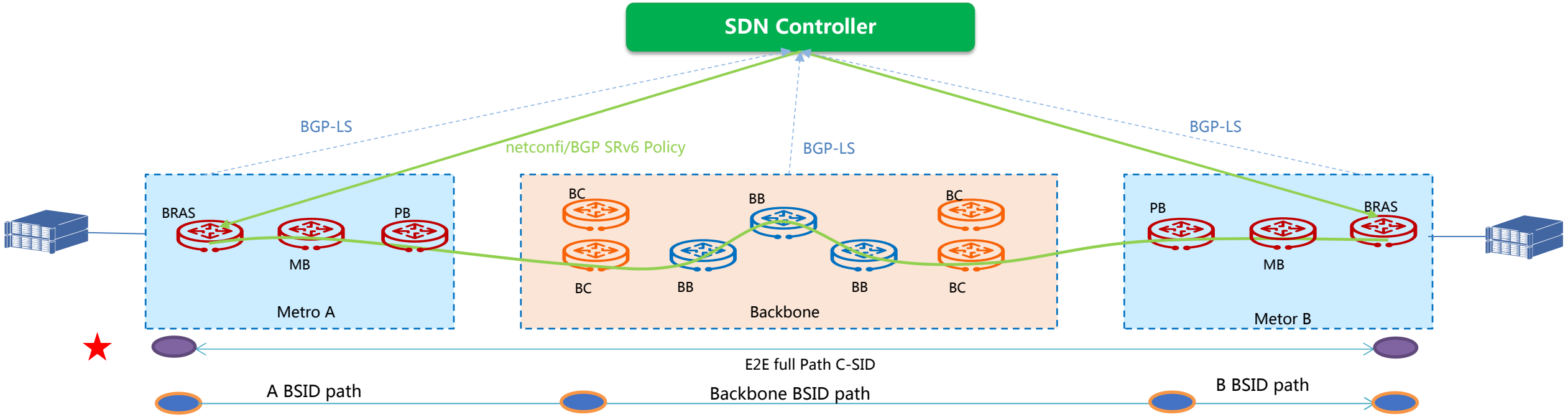




- Each vendor uses own controller deploy own devices
- Operator need to deploy a super controller to manage device controllers of all the vendors
- increasing deployment complexity and failure probability

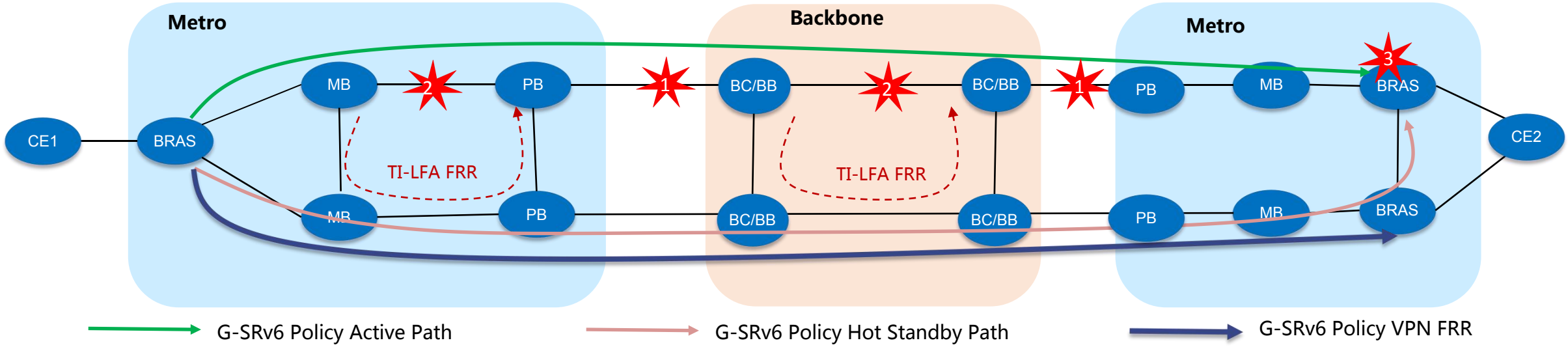
- Fully decoupled single-layer controller deployment for various vendors devices
- unified southbound interface, unified control protocol, greatly simplified deployment

Inter-AS E2E Deployment



- SDN controller collects the topology and SID information of the entire network by BGP-LS, calculate the inter-AS compressed SRv6 Polcy 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 transimission efficiency

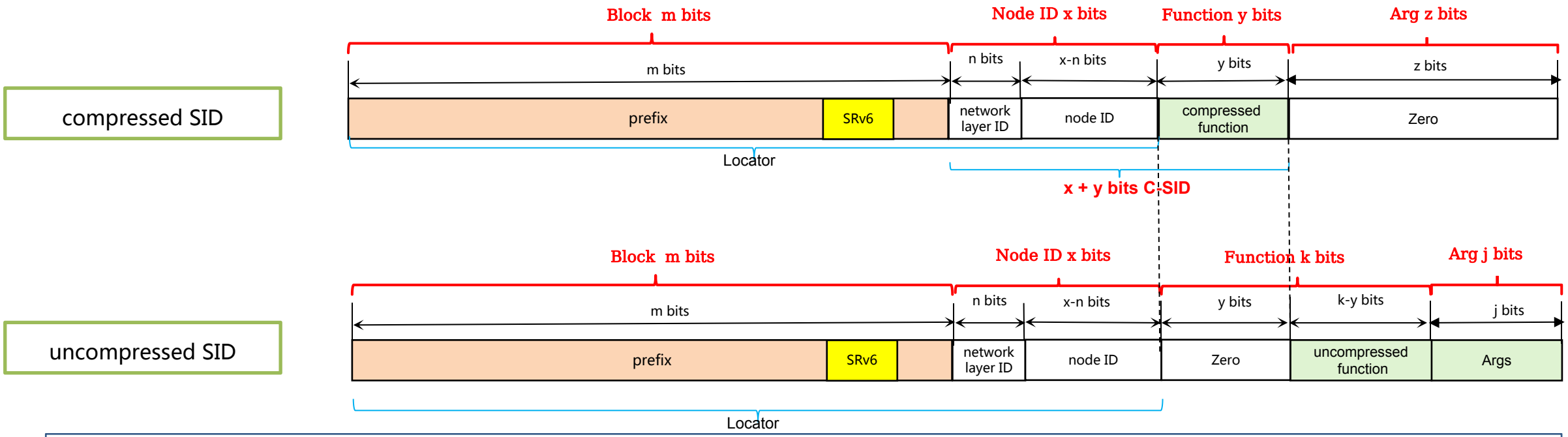
Protection and Failure Detection Deployment



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

detailed information refer to : https://datatracker.ietf.org/doc/draft-liu-rtgwg-sr-protection-considerations/

Compressed SRv6 SID Planning



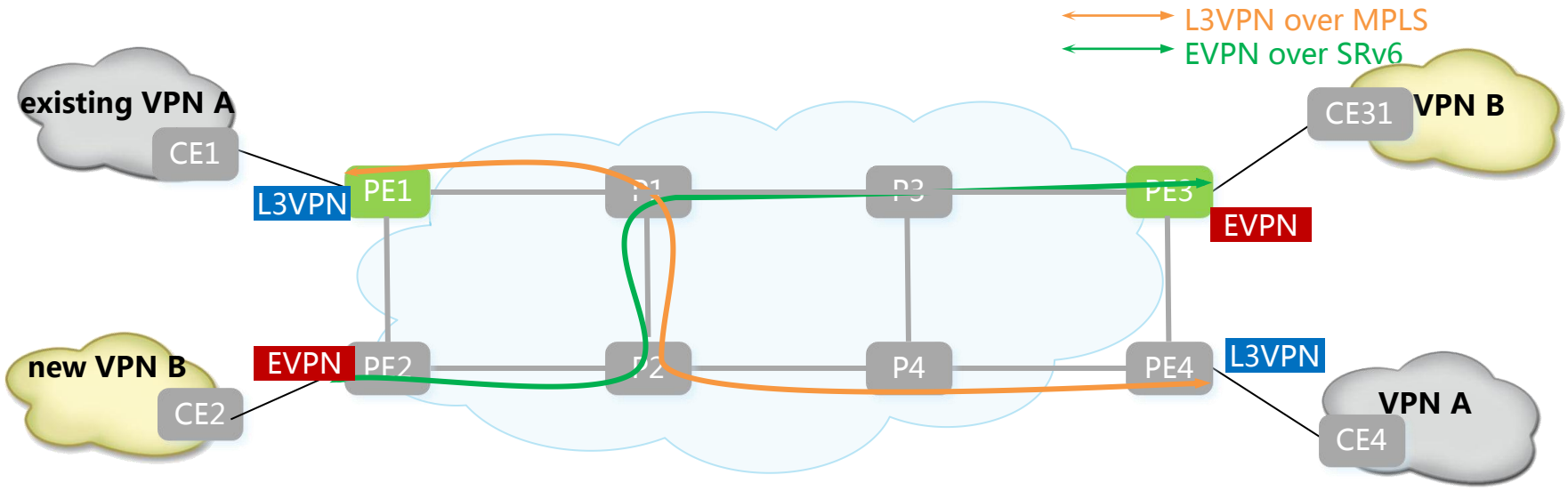
- Allocate separate prefix for SRv6 SID in IPv6 address space, due to the high aggregation of SIDs, boundary devices have simple ACL policy configuration to prevent SID information leakage
- Coexistence of uncompressed and compressed SID in the same locator(C-SID and 128 bits uncompressed SID in the 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

Security Considerations for Deployment

- Source Routing Security
  - ✓ No SRH tampering and spoofing and no SRv6 path information leakage
  - ✓ Reason for Secure Deployment
    - ➢ Separate prefix allocation for SRv6 SID in IPv6 address space as mentioned in compressed SRv6 SID planning
    - ➢ Simple ACL policy configuration on boudaries to prevent SID information leakage
- Control Signaling Distribution Security
  - ✓ No SID information leakage outside the trusted domain via protocol signaling
  - ✓ Reason for Secure Deployment
    - ➢ SID information distributed by the IGP protocol limited to a single IGP area
    - ➢ SID information distributed by the BGP protocol export policies limited to a single AS or multiple ASes within a trusted domain

Thanks

MPLS Evolution towards SRv6



- PE devices need to support both SRv6 EVPN and MPLS VPN
- The current network PE has added the deployment of EVPN address family and IPv6 peer (pre deployment)
- The new and old VPN services on PE devices use different tunnel
- The old L3VPN service will not be upgraded and will continue to be carried by MPLS tunnels.
- The newly created VPN service is hosted by using EVPN SRv6