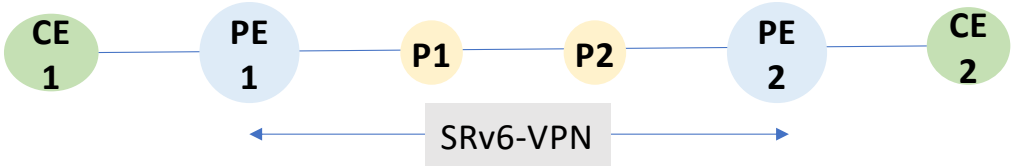
ICMP Error Handling in SRv6 based VPN Networks

draft-ali-6man-srv6-vpn-icmp-error-handling-00

Zafar Ali - Cisco Systems
K. Szarkowicz - HPE
S. Joy – Cisco Systems

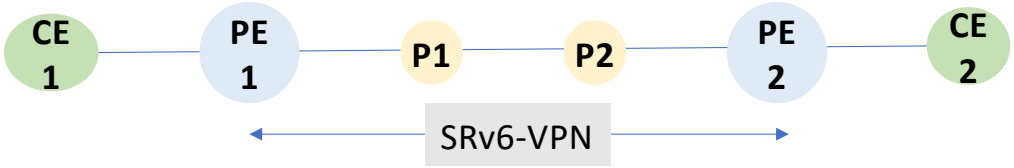
IETF123

Remind



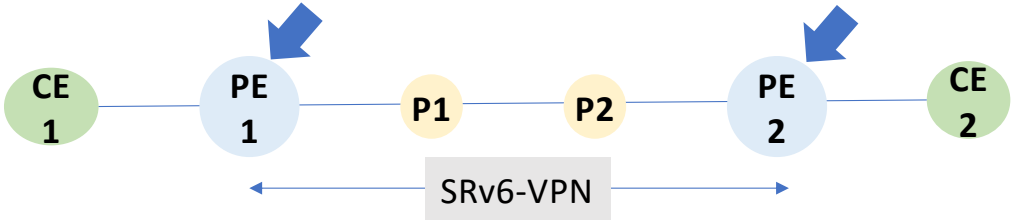
- [RFC9259] explains how the existing mechanisms for ICMP error handling for SRv6 VPNs.
- [RFC9259] does not describe a mechanism for a CE-to-CE traceroute when the provider network deploys Uniform Model [RFC3443].

Problem Statement and Scope



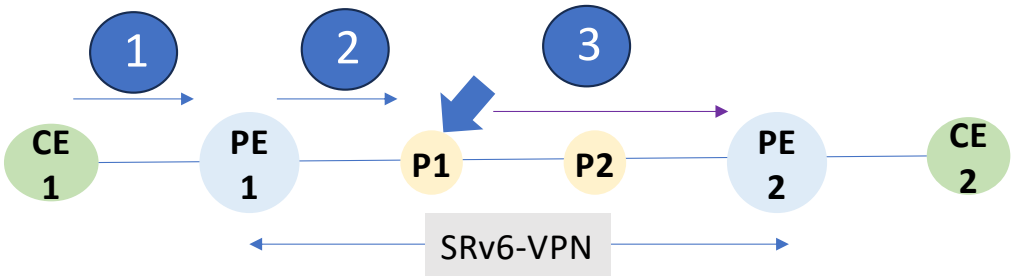
- Handling ICMP errors in SRv6-VPN where the provider network deploys Uniform Model [RFC3443]
  - Nodes that the customer packet traverses visible to nodes outside the provider core
- The draft uses CE-to-CE Traceroute in SRv6-VPN as an “example”
- CEs can be running IPv6 or IPv4 data plane

Uniform Model



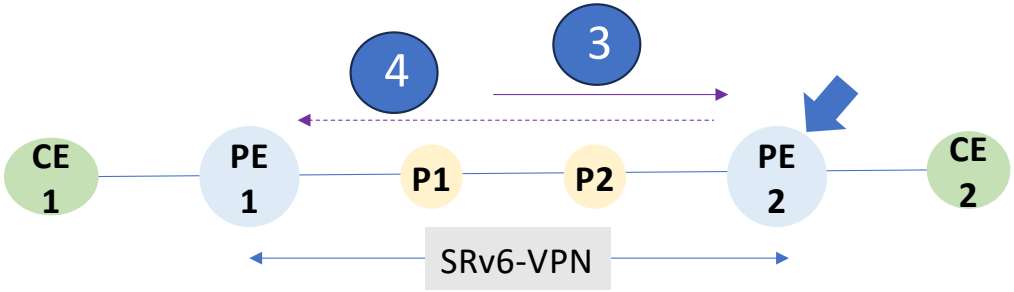
- Uniform Model [RFC3443]
  - @ SRv6 PE node:
    - Time-to-live (TTL) or hop-limit (HL) fields propagated during the SRv6 encapsulation of the customer packet

ICMP Error Handling procedures @ SRv6 P node



1. CE1 sends a traceroute with HL or TTL set to 2.
2. IPv6 packet Hop-Limit expires at P1
3. SRv6 capable P node sends (tunnels) the ICMP error towards the end of SRv6 cloud using VPN SID of the egress PE
   - VPN SID of the egress PE is obtained from the invoking packet
   - Note: This is similar to handling such cases in MPLS network where message is sent (tunneled) to end of the LSP

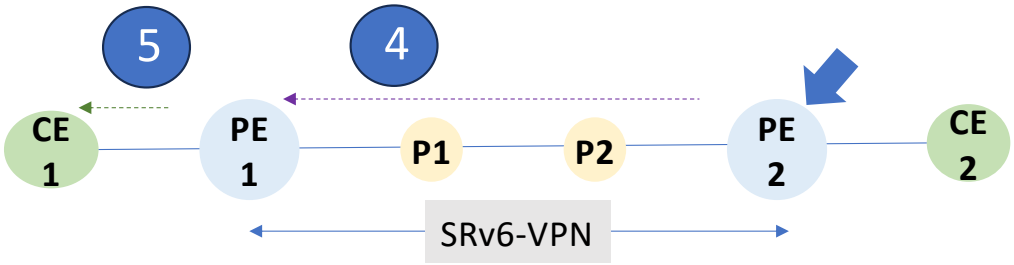
ICMP Error Handling procedures @ SRv6 Egress PE node



3. Once the packet reaches the egress PE, ICMP error packet is decapsulated

4. Subsequent forwarding table lookup on ICMP packet DA results in the ICMP packet being forwarded to ingress PE using the VPN SID of the Ingress PE

ICMP Error Handling procedures @ SRv6 Ingress PE node



4. The ingress PE decapsulates the packet
5. The ingress PE send it to the intended CE
   - CE nodes can be IPv6 or IPv4 nodes

Next Steps

- Would like to request working group adoption