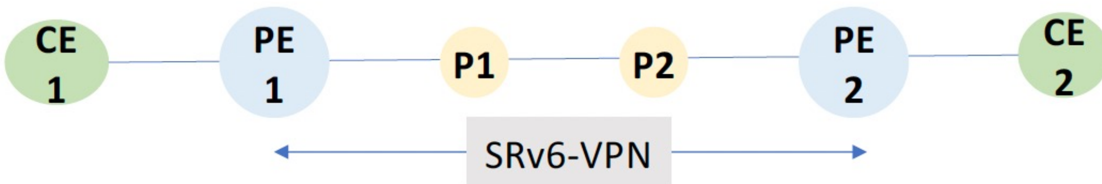
ICMP Error Handling in SRv6 based VPN Networks

draft-ali-6man-srv6-vpn-icmp-error-handling-02

Z. Ali, Cisco Systems
K. Szarkowicz – HPE
M. Manish, Meta
G. Mishra, Verizon
S. Joy - Cisco Systems

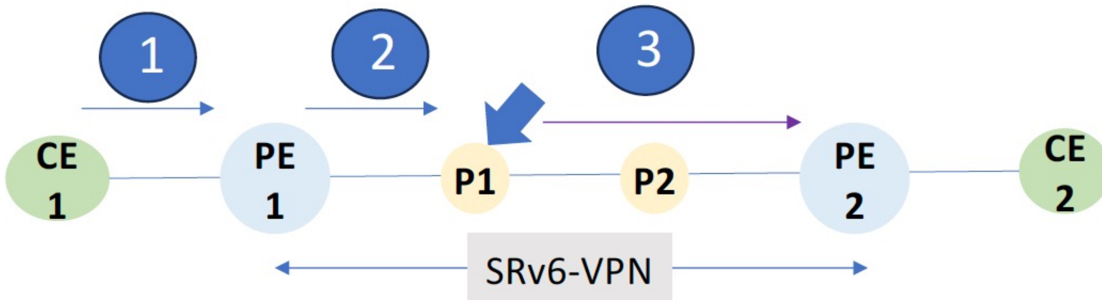
IETF124 6man WG

Problem Statement/ Scope



- Handling ICMP errors (e.g., Time Exceeded) in SRv6-VPN where the provider network deploys Uniform Model [RFC3443]
  - @ SRv6 Ingress PE node: Time-to-live (TTL) or hop-limit (HL) fields propagated during the SRv6 encapsulation of the customer packet
- CEs can be running IPv6 or IPv4 data plane

ICMP Error Handling procedures @ SRv6 P node



1. CE1 sends a traceroute with HL or TTL set to 2
2. PE1 copies the HL or TTL = 1 into the outer IPv6 Header
3. The outer IPv6 header Hop-Limit expires at P1

The draft proposes an Proposes an alternate solution similar to handling such cases in the MPLS network

- ICMP error is sent (tunneled) to Egress PE for forwarding in data plane to the invoking CE.
- VPN SID of the egress PE is copied from the outer IPv6 header

Status and Next Steps

- IETF123
  - The draft was presented at 6man, intarea WGs
  - Addressed all comments received from WGs
- IETF124
  - Based on WG chair's feedback, the draft was presented in Spring WG
  - The draft was also presented at intarea WG
- Next Steps
  - Authors would like to request working group adoption

Thank You!