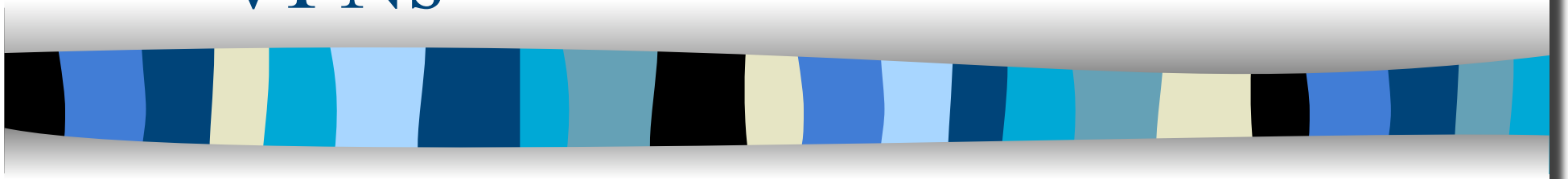
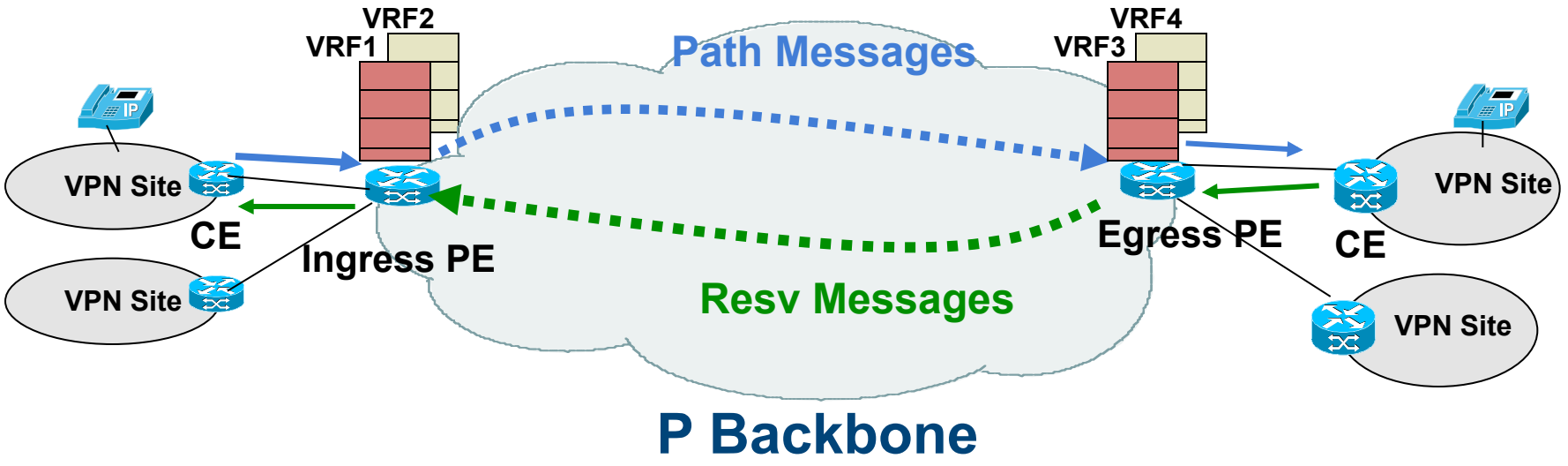
Support for RSVP in Layer 3 VPNs



draft-ietf-tsvwg-rsvp-l3vpn-01.txt

Bruce Davie
François le Faucheur
Ashok Narayanan
Cisco Systems

Model of operation



- Path messages sent by data senders
- Receivers send Resv messages
  - forwarded back up the path to senders
- Neither Paths nor Resvs are processed in P routers

Changes from -00 to -01

- Clarified and simplified methods of controlling redistribution of PE addresses (next slide)
- Recommend use of VPN_IPv4 HOP in all cases
- Wrote a thorough IANA considerations section
- Editorial cleanup, nits

Redistribution of PE addresses

- Ingress PEs need to send RSVP messages to egress PEs and vice versa
- In some inter-AS cases, this requires advertisement of VPN-v4 addresses for PEs across ASBRs
- Operators can either
  - Create VRFs for just control traffic, use addresses from these VRFs in RSVP HOP objects
  - Use addresses from customer VRFs, ensuring Customer A's addresses are not used for Customer B (A≠B)
- We removed (ineffective) community approach from this version of draft

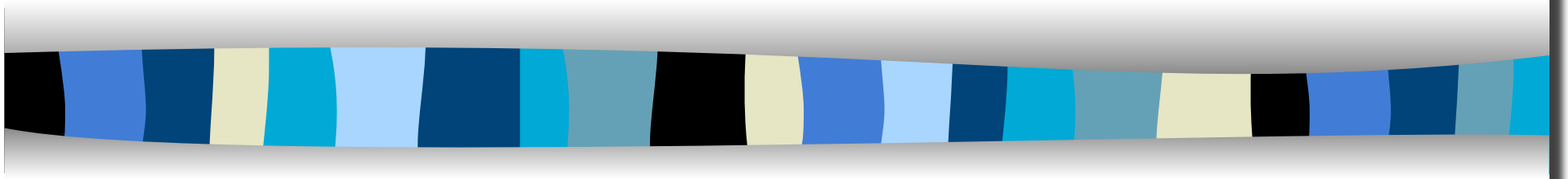
VPN-IPv4 HOP

- Rather than using IPv4 HOP sometimes and VPN-IPv4 HOP at others, PEs SHOULD use VPN-IPv4 always
  - Simplifies operations, reduces chances of errors

Summary

- Admission control on PE-CE links would be useful
- Small set of new mechanisms makes RSVP work in VRF context and avoids use of router alert in provider backbone
  - Put VPN-IPv4 addresses in Path and Resv messages to enable correct VRF to be identified
  - Address Path messages directly to egress PE or ASBR
- Admission control over backbone is optional, leverages existing techniques (RFC 4804)
- No change to RFC4364 (MPLS/BGP VPN) protocols or operations
- Draft has been stable for 3 IETF meetings, now ready for last call, IOHO

Backup



VPN-IPv4 HOP

- Is now a “SHOULD” in all cases
- Why not “MUST”?
  - Not required in certain cases (e.g. single AS, and some inter-AS)
  - Imposes some operational constraints on address assignment

Why not address CE-CE RSVP-TE in this draft?

- CE-CE RSVP for CAC stands on its own without TE
- Requirements for TE are quite extensive
  - See `draft-kumaki-l3vpn-e2e-rsvp-te-reqts-06.txt`
- Meeting those requirements requires considerable work (next slide)
- TE work could certainly build on current draft, but see no reason to delay current draft while designing solutions to all the TE issues

Issues for CE-CE RSVP-TE

- CEs and SPs are in different ASes, making this an inter-AS TE scenario, but one in which CE addresses are not unique
  - Perhaps existing techniques (PCE, loose-hop, etc) can be applied, but details (e.g. PCE with non-unique addresses) would need to be worked out
- Not clear how a CE gets to pick its egress PE (e.g. to support FRR scenario I in draft-kumaki) nor how it can get diverse paths to another CE for FRR support
- LSP hierarchy seems required for scalability; not clear how RFC 4206 (LSP Hierarchy) interacts with L3 VPNs
- Carrier's Carrier would also seem to impose new requirements for LSP hierarchy - details not worked out

Overview of Proposed Solution

- New SESSION, SENDER_TEMPLATE, FILTER_SPEC, HOP types in Path, Resv etc. use VPN-IPv4/6 addresses
  - enable PEs to identify appropriate VRF context during RSVP processing
  - enable any two PEs to exchange messages
  - appear only in PE-PE messages, not outside provider's backbone (except inter-AS options B and C)
- Control-plane approach to direct Path messages to egress PE for processing, avoiding need for Router Alert handling in data plane
- RSVP over TE tunnels as per RFC 4804 if admission control over provider backbone required

Problem Overview (1)

- Admission control may be desired on CE⇔PE links of layer 3 VPNs (RFC4364)
- Running RSVP across these links presents several issues:
  - Need to associate RSVP messages (which contain C addresses) with appropriate VRF context when they arrive at PE across backbone
    - customer address spaces may overlap
  - Need to intercept Path messages at egress PE but Router Alert IP option may not be visible/ accessible
- NB: Focus on admission control, not TE
  - TE has enough differences to warrant new draft

Problem Overview (2)

- May also wish to perform admission control for e2e flows in backbone
  - Clearly need some sort of aggregation for scalability and to avoid installation of per-customer state in P routers
  - Similar to other RSVP aggregation scenarios (e.g. RFC 3175, RFC 4804)
- Need to support Inter-AS operation