Requirements for supporting Customer RSVP and RSVP-TE over a BGP/MPLS IP-VPN

draft-kumaki-l3vpn-e2e-rsvp-te-reqts-06.txt

Kenji Kumaki KDDI R&D Labs, Editor
Raymond Zhang BT
Yuji Kamite NTT Communications

Motivation

- Customers expect to run triple play services through BGP/MPLS VPNs
  - As a result, their requirements for end-to-end QoS of applications are increasing.
  - Depending on applications (e.g. voice, video, bandwidth-guaranteed data pipe, etc.),
    - An end-to-end native RSVP path is required.
      - It may be used to provide for QoS guarantees.
    - An end-to-end MPLS TE LSP is also required.
      - It may be used to guarantee bandwidth.
  - Have the following two advantages to provide the above services in BGP/MPLS VPNs
    - Customers can use both private and global addresses as they desire.
    - Service providers can provide these services while protecting confidentiality from customers.

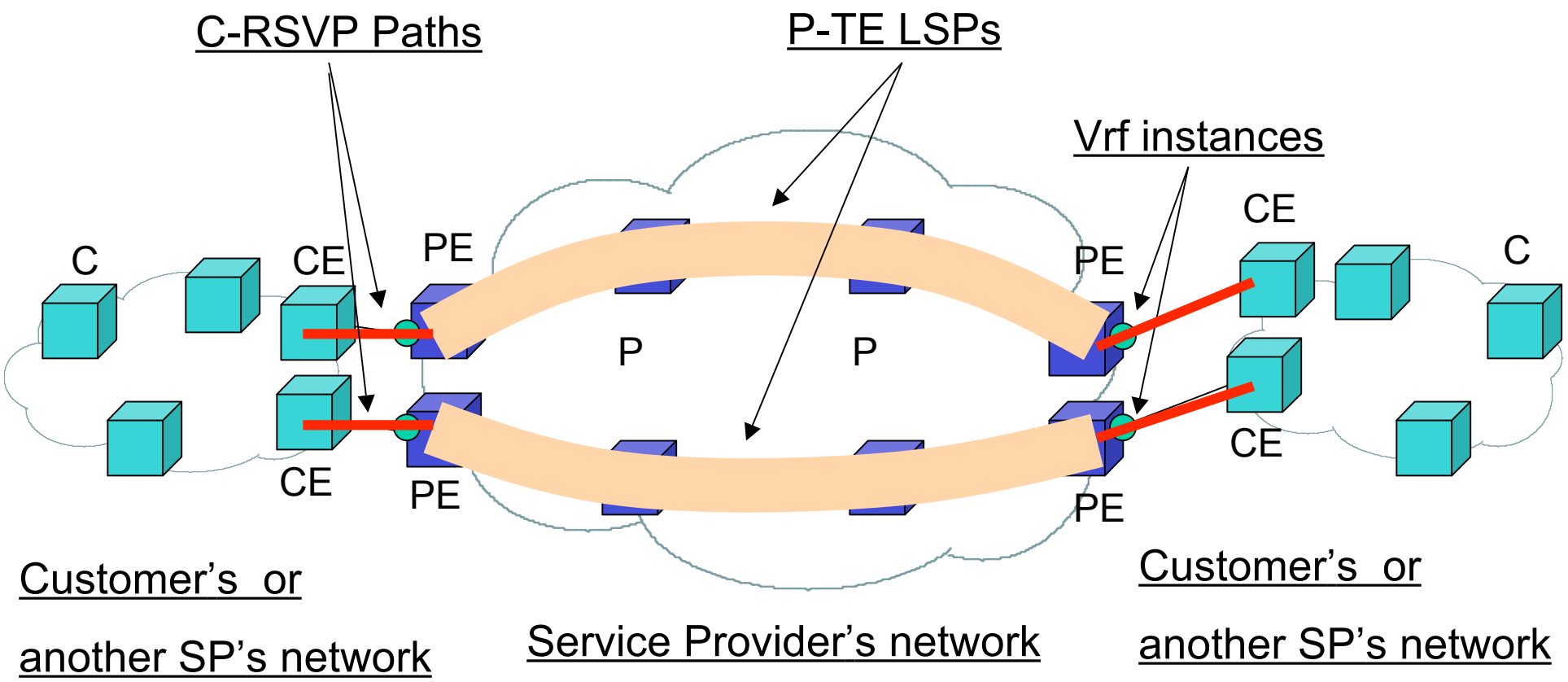
Problem Statement

- C-RSVP path model (data packets among CEs are forwarded by "native IP packets ")
  - When service providers offer a C-RSVP path between CEs over BGP/MPLS VPNs, the CE requests an end-to-end C-RSVP path with bandwidth reservation of X to the remote CE. However, if a C-RSVP signaling is to send within VPN, the service provider network will face scalability issues.
  - Service providers can not provide a C-RSVP path over vrf instance as defined in RFC4364. The current BGP/MPLS IP-VPN architecture also does not support an RSVP instance running in the context of a vrf to process RSVP messages and integrated services (int-serv).

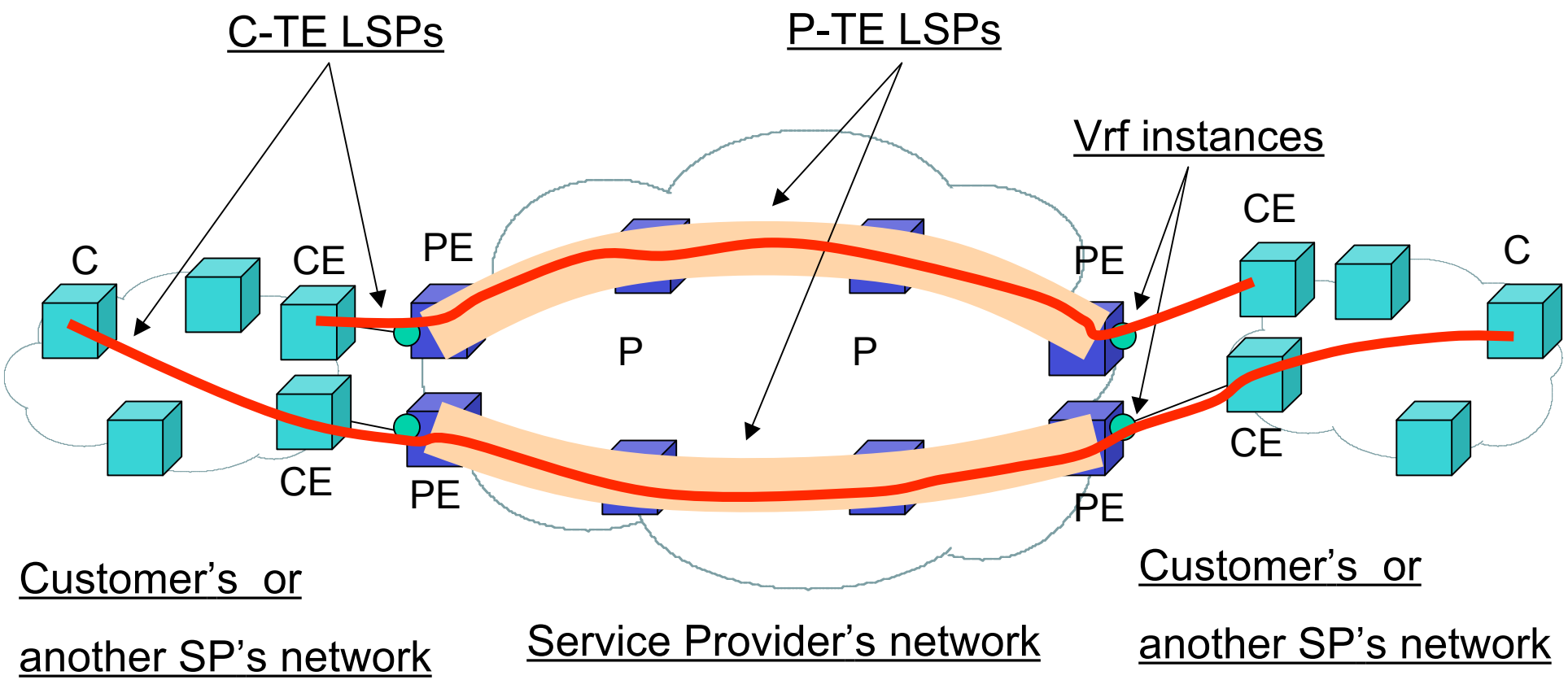
Problem Statement (contd.)

- C-TE LSP model (data packets among CEs are forwarded by "labeled IP packets ")
  - If service providers offer a C-TE LSP from CE to CE over BGP/MPLS VPNs, they require that a MPLS TE LSP from a local CE to a remote CE be established. However, if a C-TE LSP signaling is to send within VPN, the service provider network will face scalability issues.
  - If service providers provide the C-TE LSP over a BGP/MPLS VPN, they can not provide it over vrf instance as defined in RFC4364. The current BGP/MPLS IP-VPN architecture does not support an RSVP-TE instance running in the context of a vrf to process RSVP messages and trigger the establishment of the C-TE LSP over the service provider core network.
- In the models of C-RSVP paths and C-TE LSPs both, the solution must address these scalability concerns.

Reference model (C-RSVP Path Model)



Reference model (C-TE LSP Model)



Application Scenarios

- C-RSVP Path Model
  - RSVP Aggregation over MPLS TE Tunnels
  - RSVP over Non-TE LSP
- C-TE LSP Model
  - Fast recovery over IP-VPN
  - Strict C-TE LSP QoS guarantees
  - Load balancing of CE-to-CE traffic

Detailed Requirements

- Requirements for C-TE LSP Model
  - 11 requirements [See section 6]
- Requirements for C-RSVP Path Model
  - 4 requirements [See section 7]
- Common requirements for two models
  - 6 requirements [See section 8]

Major Changes from -05

- Added new co-author, Yuji Kamite, NTT communications
- Clarified C-RSVP path and C-TE LSP models
- Clarified problem statement in Section 3
- Modified specific requirements for C-TE LSP model in section 6
- Added specific requirements for C-RSVP path model in section 7
- Added common requirements for two models in section 8

Next Steps

- Received a lot of emails for support and comments on L3VPN WG ML
  - Will reflect comments in the next revision
- Request WG to accept this I-D as a WG document