IPsec-Protected Virtual Links for PPVPNs

draft-duffy-ppvpn-ipsec-vlink-00.txt

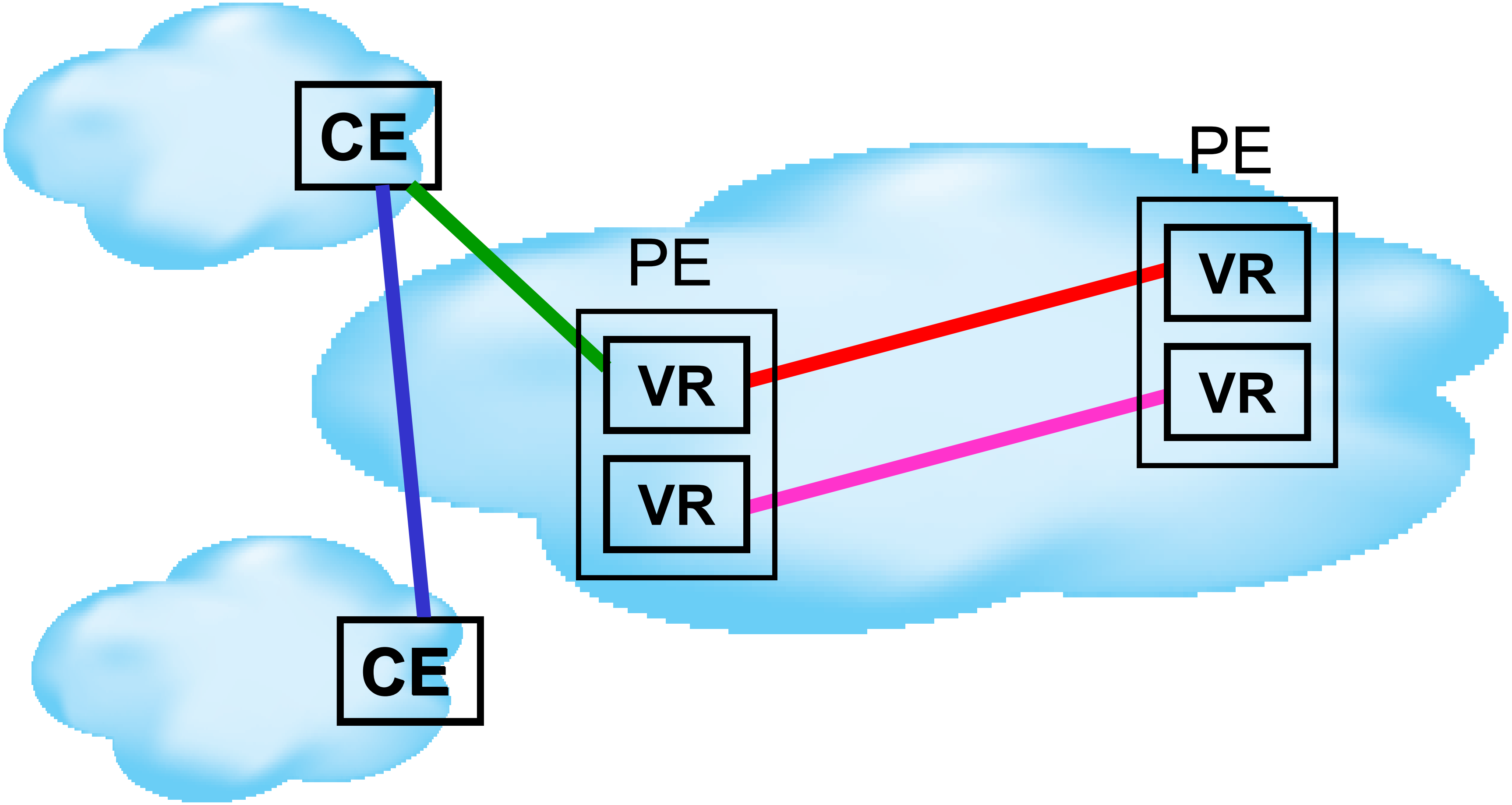
Mark Duffy

Quarry Technologies

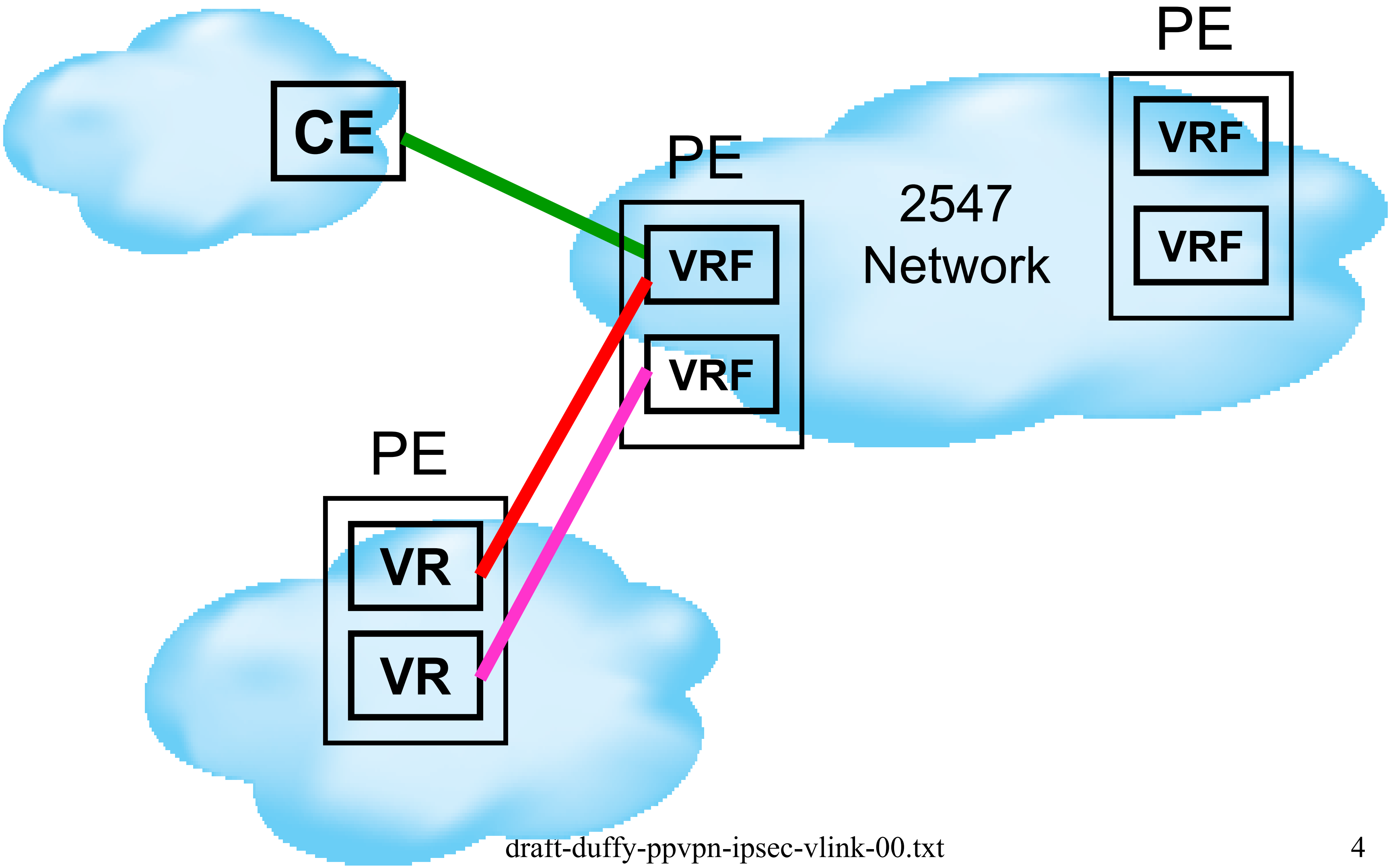
What is a Virtual Link?

- Point-point data link implemented over an IP network using tunneling
- Terminates within each tunnel endpoint device as an IP interface
- Endpoints may form routing adjacencies and forward (by BMP) packets over the virtual link

Scenarios – CE and VR



Scenarios -- 2547



Some Requirements

- Multi-context support (multiple virtual links between a given pair of systems)
  - Bind virtual link to the correct context
  - Distinguish one virtual link from another
- IPsec protection available
- IPsec optional (with reasonable granularity)
- Interoperability between PE and CE

Why Do We Need to Do This?

- Efforts in the IETF to date don’t address the multi-context needs of the network based case

- Existing proposals either require the use of IPsec, or provide poor granularity in selecting its use

Issues

- How does IPsec policy (SPD) fit into a picture where forwarding decisions are made by BMP?

- How should the desired context (e.g. VPN-ID) be conveyed when a tunnel is established?

Some Approaches

- IPsec tunnel mode SA = virtual link
- IP-in-IP tunnel with IPsec transport mode
  - 1 tunnel and n SAs, or n tunnels and n SAs
- GRE tunnel with IPsec transport mode
- MPLS-in-IP with IPsec transport mode
- L2TP with IPsec transport mode

Applicability to PPVPN

- Virtual link is essential to VR-based L3 VPN, and useful for CE-based and 2547
- WG charter calls for "…appropriate mandatory-to-implement technologies … to ensure adequate security and privacy of user data..."

Without a standard, interoperability will suffer!

Next Steps

- Need discussion on the list and input from interested parties
- Select one or two approaches
- Progress approach(es) as WG item

draft-duffy-ppvpn-ipsec-vlink-00.txt