

IPSec for BGP Enabled Service over SRv6

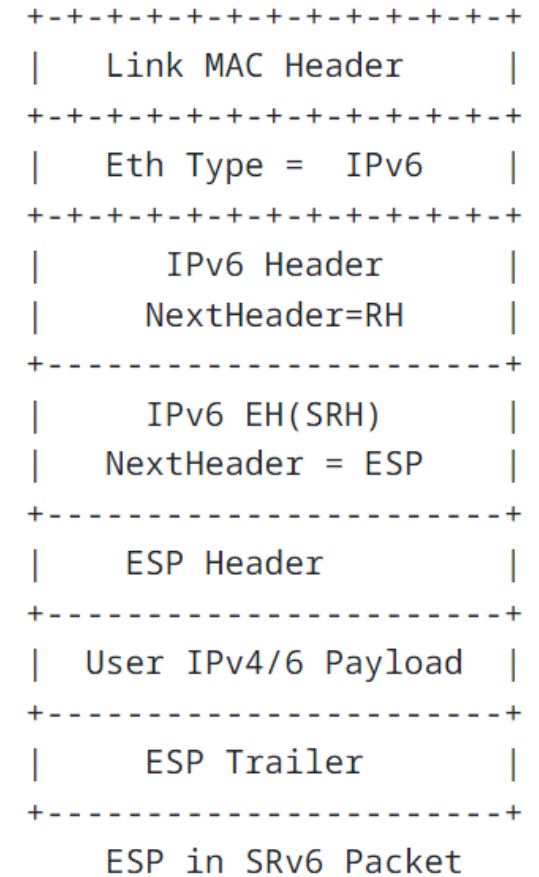
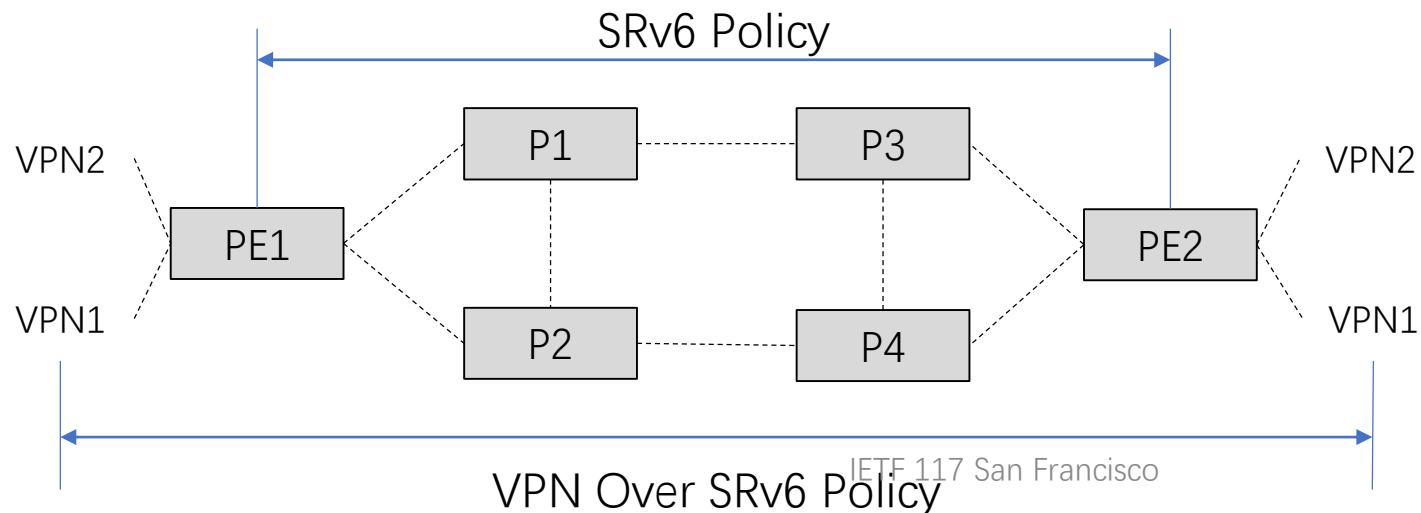
Haibo Wang/Linda Dunbar/Cheng Sheng/**Hang Shi**

Huawei, Futurewei

IETF 117

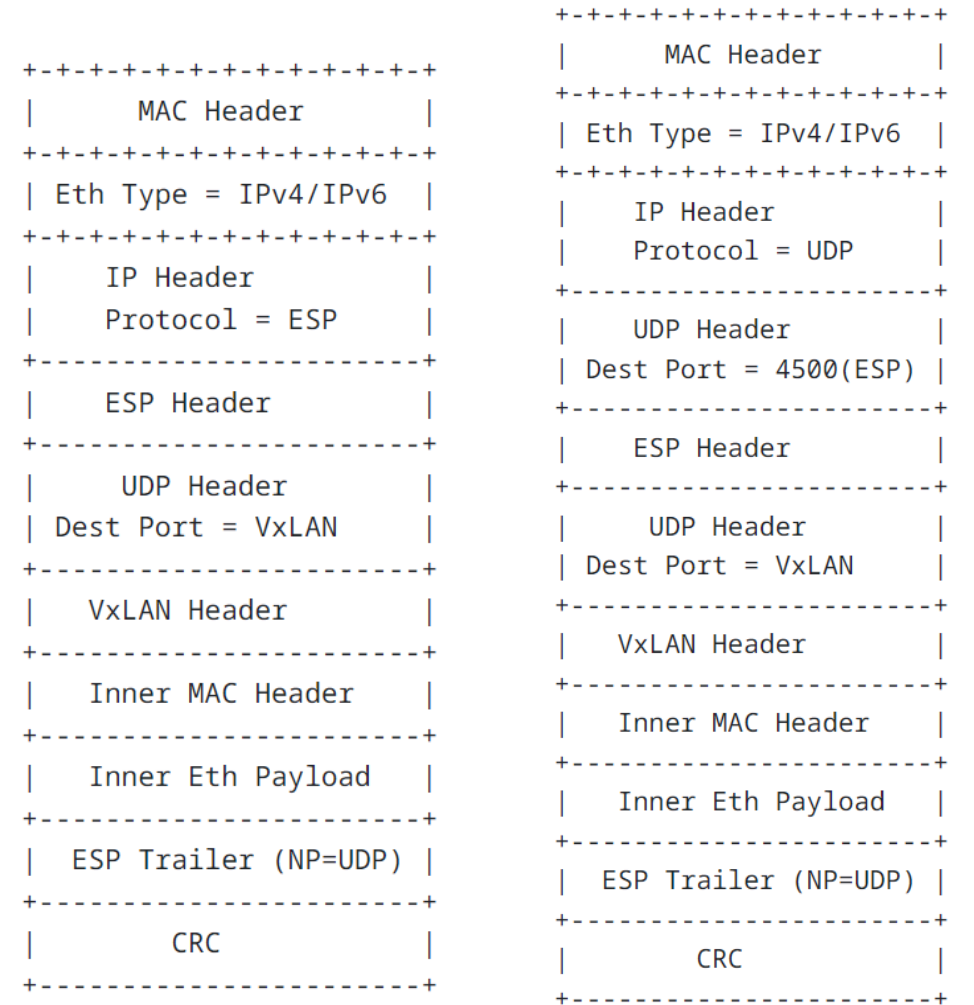
IPSec over SRv6

- Some customers in financial industry build their own backbone network and use SRv6 to orchestrate service.
- Normally, SRv6 domain is considered secure(RFC 8754, RFC 8402, RFC 8986);
- But financial data needs additional security. IPSec is used to encrypted the data end to end in case of any intrusion in the backbone network
- SRH needs to be outside of encryption



Existing BGP extension

- RFC 9012 Tunnel Encapsulation Attribute can be used to indicate the **creation of tunnel** and the encapsulation of tunnel info. See [draft-ietf-idr-sdwan-edge-discovery-10](#)
- [draft-ietf-bess-secure-evpn-00](#) defines extension to convey IPsec info in a service route. It is only for VXLAN-encapsulated service in ESP
 - Tunnel Type = ESP-Transport/ESP-in-UDP Transport
 - Encapsulation Extended Community = NVO

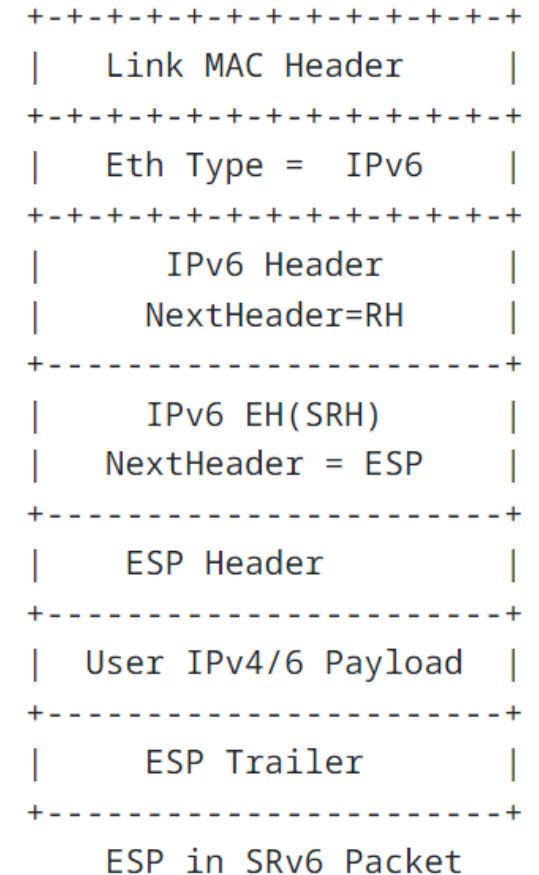


VXLAN in ESP

VXLAN in ESP-in-UDP

New Tunnel-type

- Tunnel Encapsulation Attribute:
 - Tunnel-Type = ESP-Transport-Only-Payload
 - IPsec SA Property Sub-TLV reuse [draft-ietf-idr-sdwan-edge-discovery-10](#):
 - IPsec SA Nonce
 - IPsec Public Key
 - IPsec SA Proposal
- Add Tunnel Encap Attribute to VPN route
- Encrypt using ESP then encap into SRv6



Next step

- Welcome more comments and discussion
- Not limited to SRv6?
- Merge with Secure EVPN?