SR for SD-WAN over hybrid networks

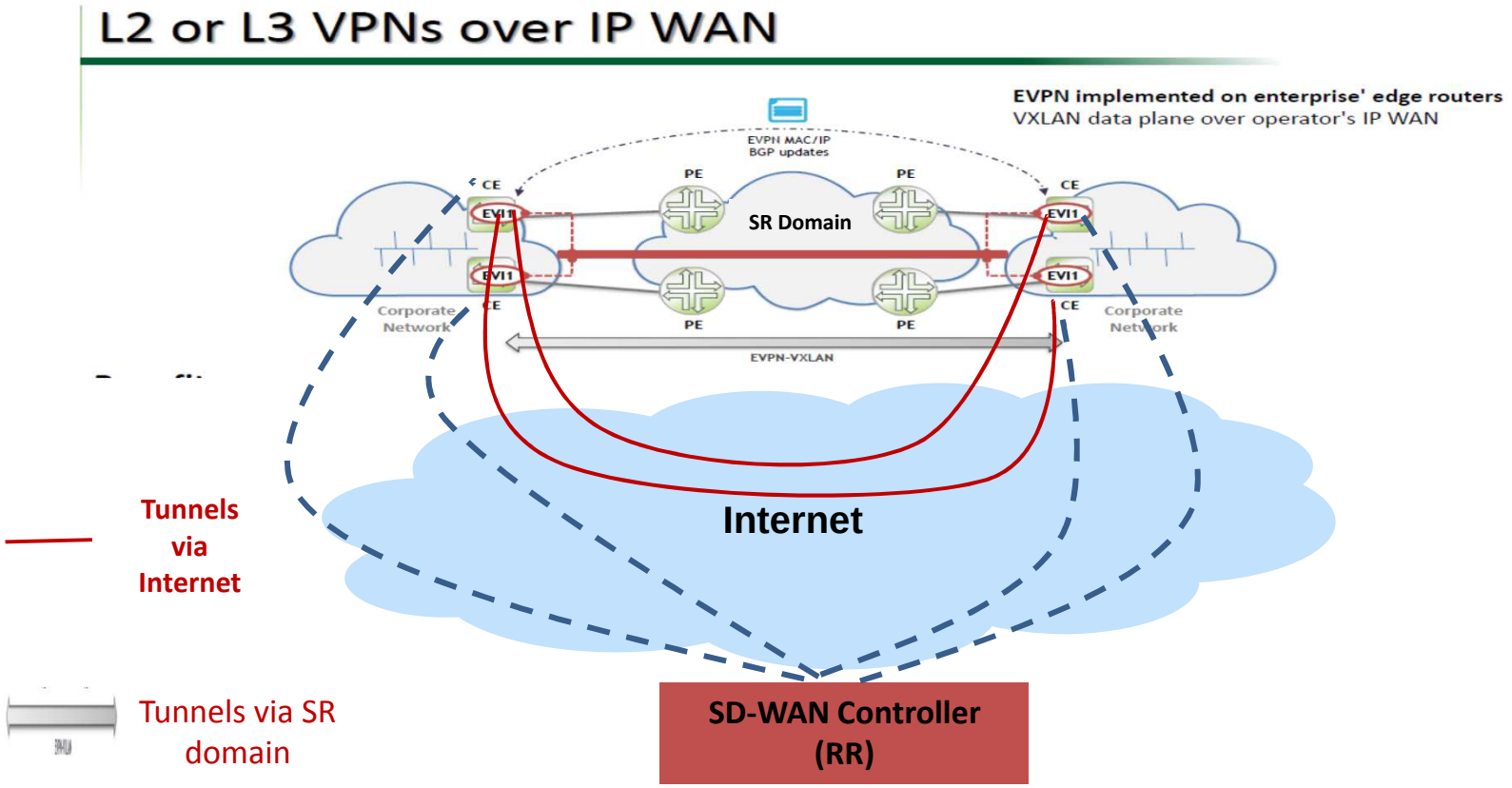
to optimize SD-WAN services over long distance

https://datatracker.ietf.org/doc/draft-dunbar-sr-sdwan-over-hybrid-networks/

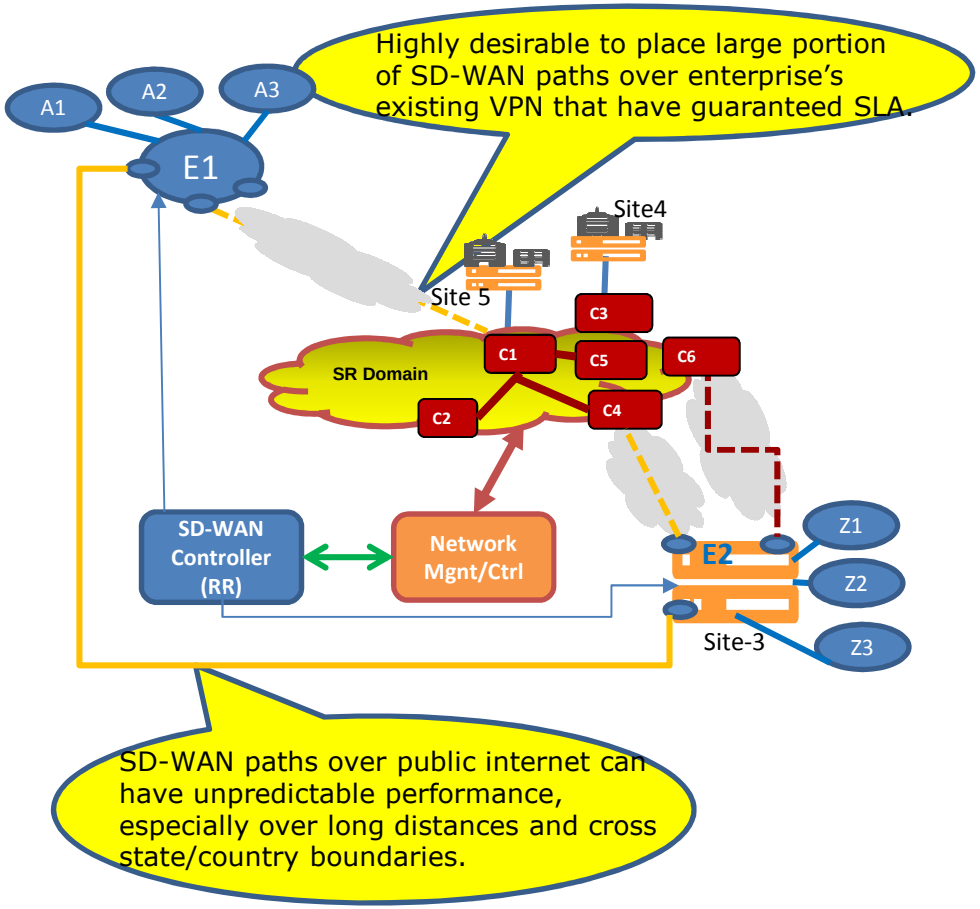
Linda.Dunbar@Huawei.com

Mehmet.toy@Verizon

Use Case 1: Classic SD-WAN
CPE based VPN: Integrating SR Routes & Internet Routes



Use Cases 2: SD-WAN end points are far apart, Different apps need different paths



For communication between "A1" <-> "Z1":

Optimal path: "A1"<-> E1 <–> C1<->C4 <–> "E2"<->Z1 (at Site-3)

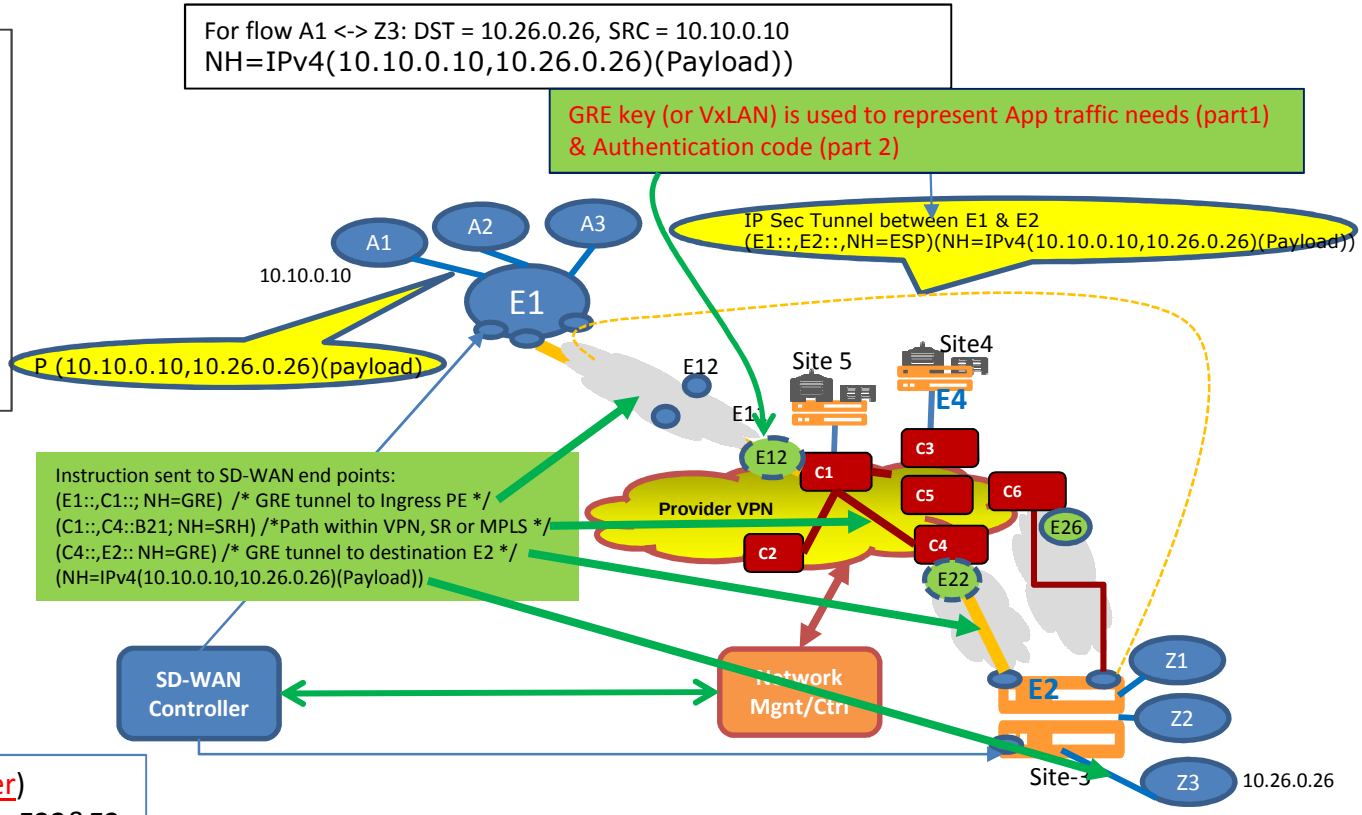
Problems:

- It is very difficult, if even possible, for PEs to determine which egress PEs is optimal for flows between "E1" <-> "E2" (as multiple PEs can reach E2 via SD-WAN paths).
- Steer the SD-WAN path over the Enterprise VPN as much as possible for better quality & control (cost, traffic management, delay, etc)

How & Why SR is useful for those use cases?

SR can easily force the path to traverse the explicit egress node (C4 or C6), or explicit segments through the SR Domain based on the SLA requested by the SD-WAN head-end nodes

Doesn't need every domain to support SR



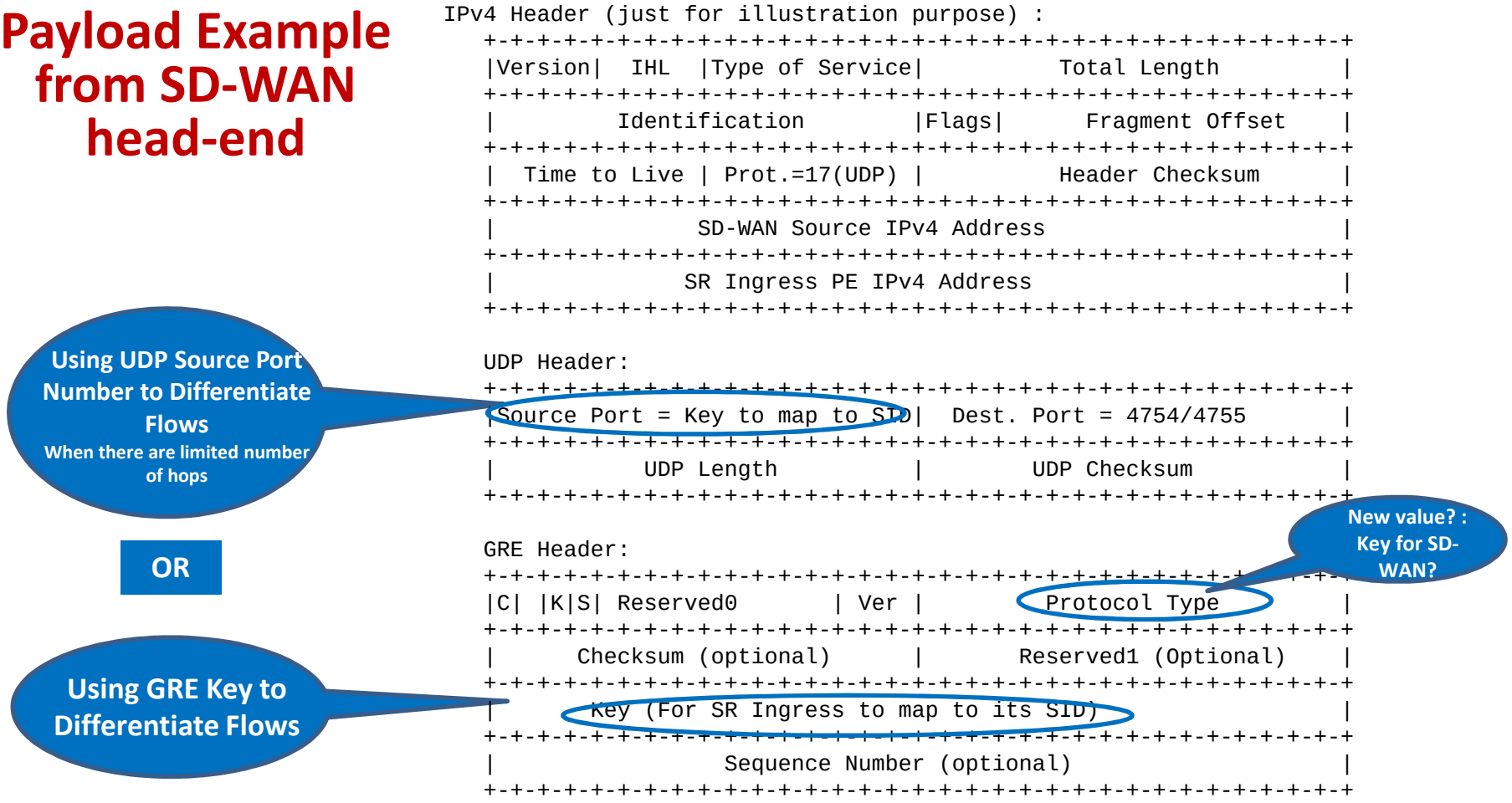
1) Ipsec between E1 & E2 (scale better)
2) Ipsec between E1 & E12, E12&E22, E22&E2

Two Approaches for SR Ingress Node

1. Controller installs the entire SID stack at E1.
   - Requires CPEs in the same administrative domain as SR
   - This approach requires less processing at the SR Ingress PE nodes, but requires more changes to SD-WAN Source nodes and require more header bytes added to the packets when traversing through 3rd party internet. Some SD-WAN nodes might not be capable of supporting encapsulating packets with the SID stack.

2. Controller delivers to E1 a “Key” that the SR ingress PE can use to map to the SID stack when the packets arrive at the SR Ingress PE.
   - This approach requires SR Ingress PE nodes to map the “Key” to the SID Stack and prepend the SID stack to the packets (Same processing for other traffic except the mapping is from the received “Key” carried in the payload).

Payload Example from SD-WAN head-end



Security Consideration

- Potential DDoS attack to the PEs with ports facing internet. I.e. the PE resource being attacked by unwanted traffic.

- Potential risk of provider VPN network bandwidth being stolen by the entities who spoofed the addresses of SD-WAN end nodes.

❑ **Enable Anti-DDoS feature to prevent major DDoS attack to those PEs**

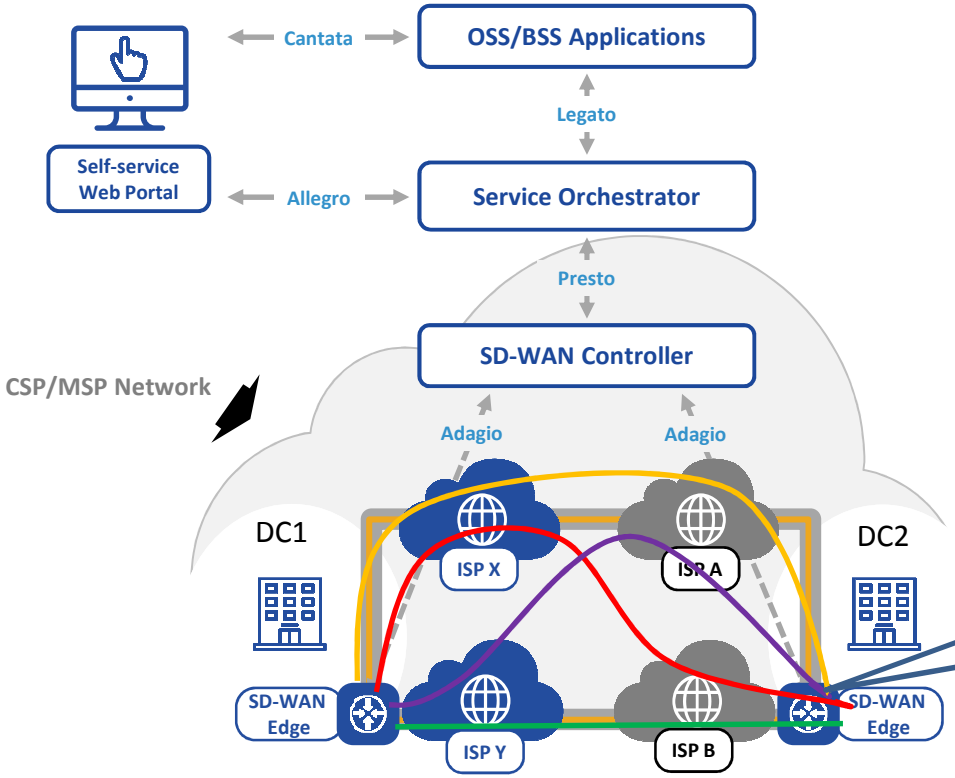
❑ **Requiring TLS/DTLS between Remote SD-WAN edge to PE? Or another layer of Ipsec between CPE <->PE? (overkill)**

❑ **Trade off between bandwidth being stolen vs. extra cost to prevent unpaid traffic traversing through its VPN networks.**

- **Embed a key in the packets, which can be changed periodically, like the digital signature**
- **key can be encoded in the GRE Key field**

MEF: SD-WAN Service Use Case 2

WAN Resiliency: SD-WAN Service over Multiple ISPs



- SD-WAN service with multiple ISPs to increase WAN resiliency
- Easily add off-net sites to an existing SD-WAN service deployment
- Use Forward Error Correction to achieve an SLA across an Internet-based underlay network

Multiple overlay paths between DC1 <-> DC2.
Simple IP forwarding can result in some routes congested and others empty. Or some paths more expensive than others

IDR & EVPN Extension

https://datatracker.ietf.org/doc/draft-dm-net2cloud-problem-statement/
https://datatracker.ietf.org/doc/draft-dm-net2cloud-gap-analysis/

SD-WAN IPsec Auto management

https://datatracker.ietf.org/doc/draft-ietf-i2nsf-sdn-ipsec-flow-protection/