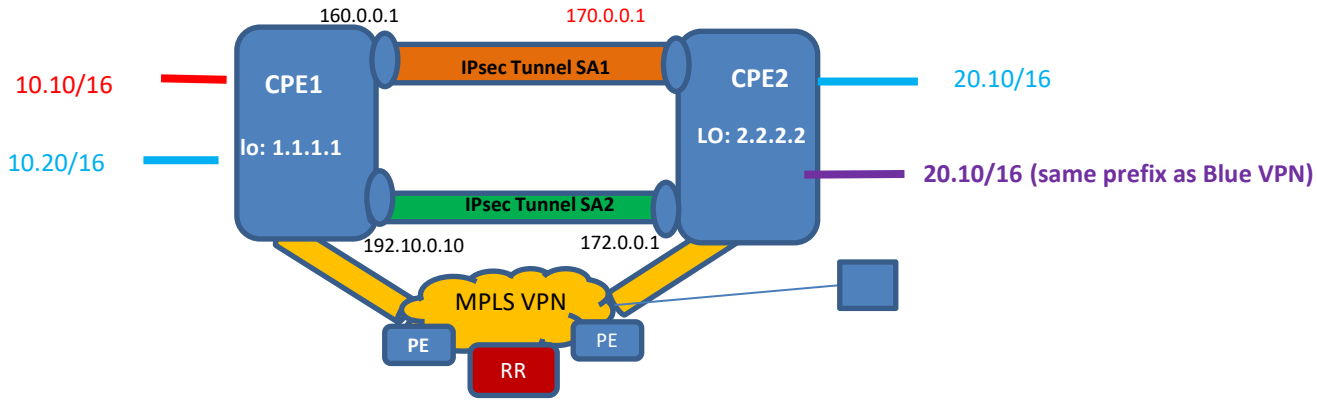
SDWAN Edge Discovery

https://datatracker.ietf.org/doc/draft-dunbar-idr-sdwan-edge-discovery/

Linda Dunbar
Sue Hares
Robert Raszuk
Kausik Majumdar
March 2021

Comparing with traditional IPsec configuration



BGP Controlled SDWAN: VRF, RT, RD

- BGP Route Target and Route Distinguisher enables:
  - Simpler Traffic Selector: Import/export Route Target
    - To achieve permission of the local and remote prefixes
  - Same client prefixes reuse: Route Distinguisher
- SDWAN policies dictate if a client network (VRF) can bind with IPsec SA.

➢ **With RR to control the policy, it scale much better for multi-node VPNs**

Traditional IPsec Configuration

- ➢ IPsec IKE to authenticate with each other
- ➢ Establish IPsec SA
  - Local key configuration
  - Remote Peer address (192.10.0.10<->172.0.01)
  - IKEv2 Proposal directly sent to peer
    - Encryption method, Integrity sha512
  - Transform set
- ➢ Attached client prefixes discovery
  - By running routing protocol within each IPsec SA
- ➢ Access List or Traffic Selector
    - Permit Local-IP1, Remote-IP2

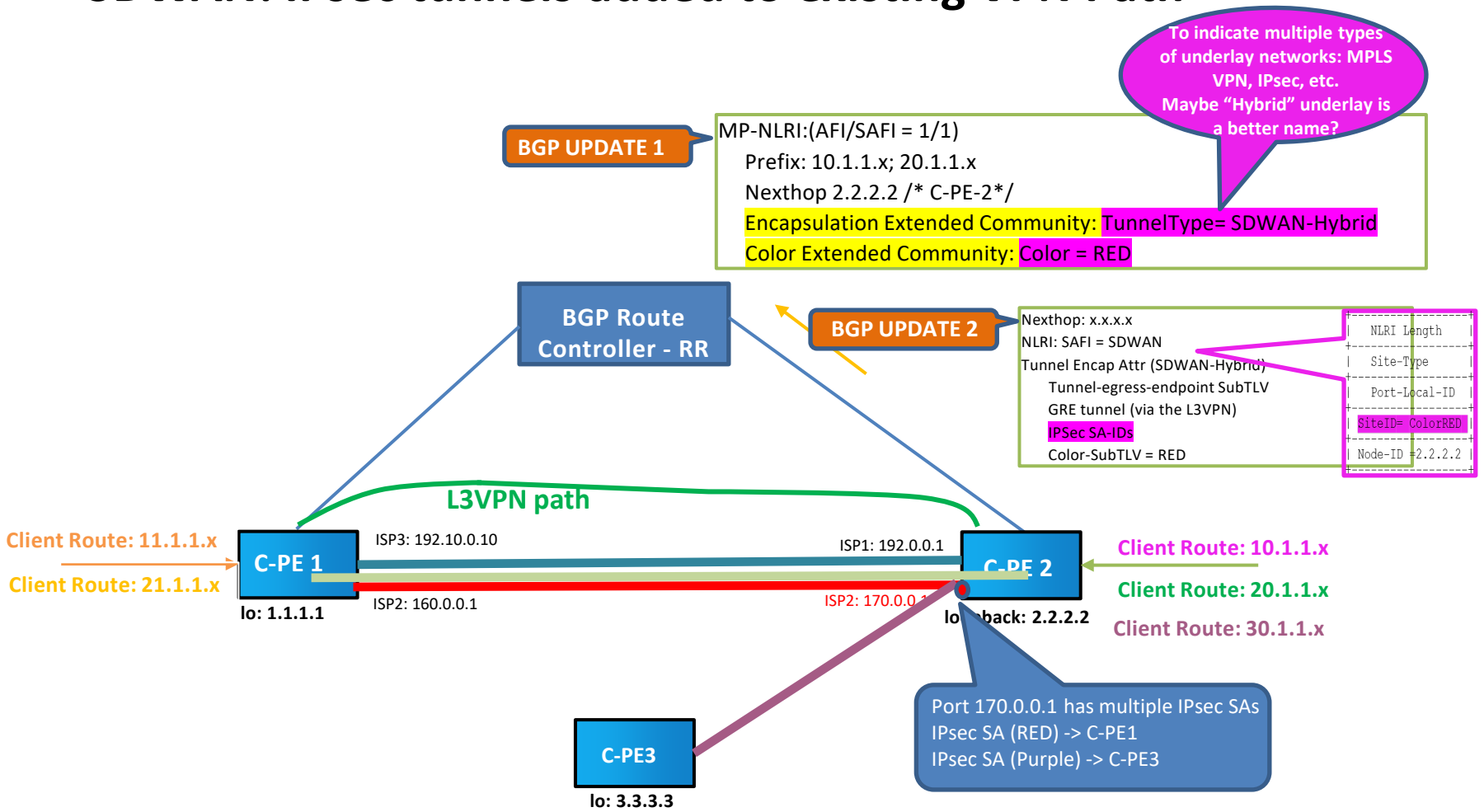
Simplification of BGP Controlled SDWAN's IPsec tunnel configuration

Traditional IPsec Configuration	BGP Controlled SDWAN's IPsec Configuration
IPsec IKE to authenticate peers	Not needed, as the SDWAN controller has authority to authenticate edges and peers
Remote Peer address configuration	Remote Peer policy is controlled by SDWAN Controller (RR)
IKEv2 Proposal directly sent to peer Encryption method, Integrity sha512	The IKEv2 proposals can be sent directly to Peer, or incorporated with BGP UPDATE
Transform set	Transform set either by BGP UPDATE or by IKEv2 message exchange
Client Prefix discovery By running separate instances of routing protocol within each IPsec SA	BGP UPDATE: Announce the client route Reachability for all parallel. No need to run multiple routing protocols in each IPsec tunnel.
Access List or Traffic Selector) Permit Local-IP1, Remote-IP2	More scalable multi-node Traffic Selector: BGP Route Target :Import/export Route Target

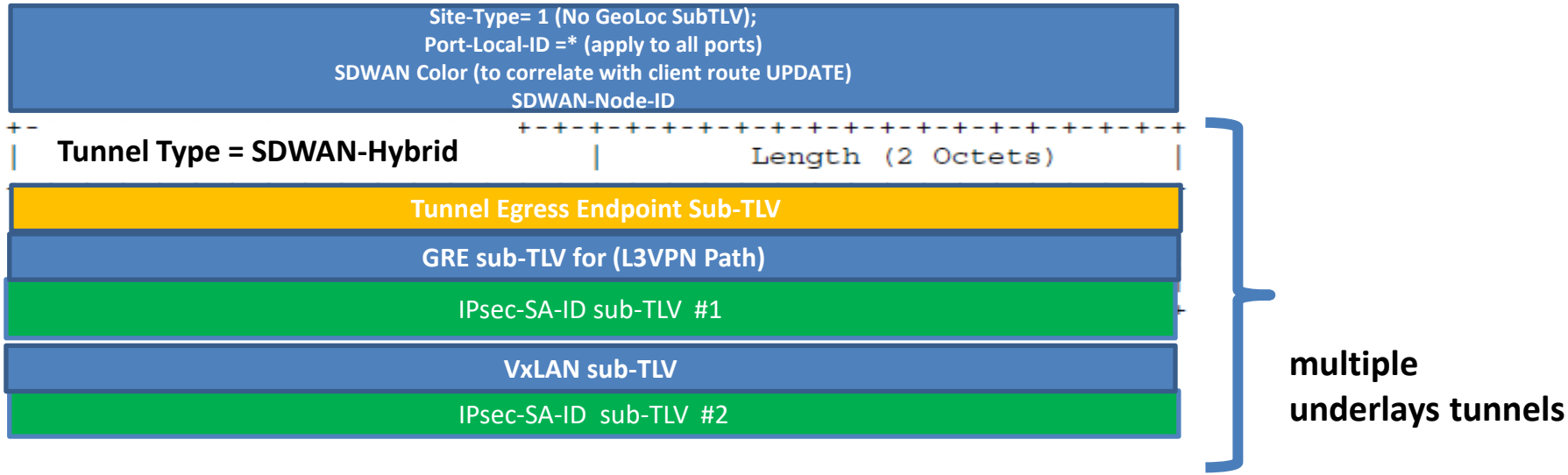
Optimization by BGP controlled SDWAN

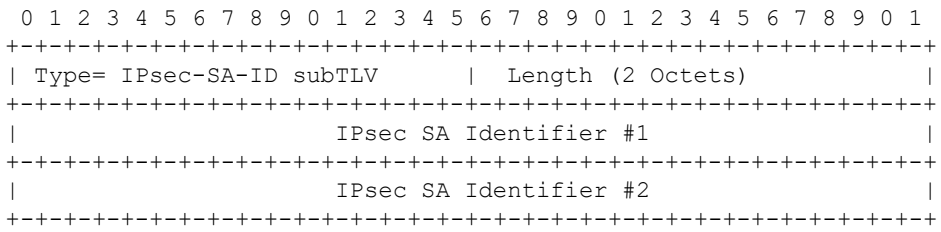
Same as traditional IPsec exchange, or can be exchanged via BGP RR

SDWAN: IPsec tunnels added to existing VPN Path

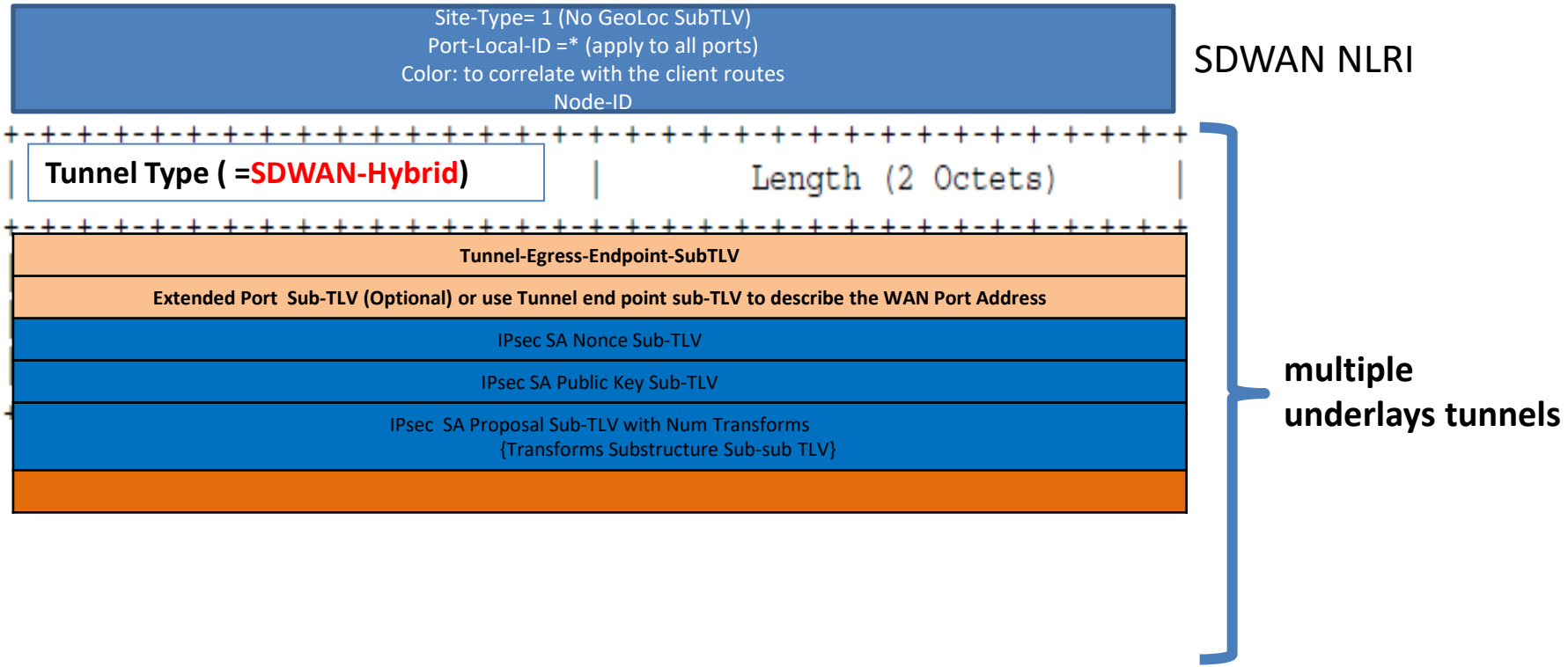


Hybrid Tunnels: with Pre-configured IPsec SA IDs





Hybrid Tunnels: with detailed IPsec SA sub-TLVs




We want
your feedback!