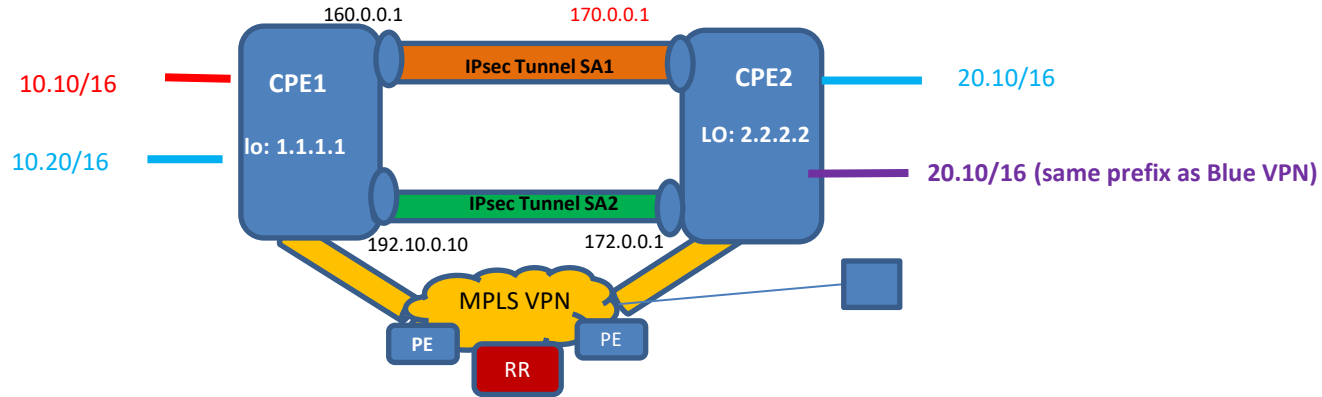


SDWAN Edge Discovery

<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

To indicate multiple types of underlay networks: MPLS VPN, IPsec, etc. Maybe "Hybrid" underlay is a better name?

BGP UPDATE 1

MP-NLRI:(AFI/SAFI = 1/1)
 Prefix: 10.1.1.x; 20.1.1.x
 Nexthop 2.2.2.2 /* C-PE-2*/
Encapsulation Extended Community: TunnelType= SDWAN-Hybrid
Color Extended Community: Color = RED

BGP UPDATE 2

Nexthop: x.x.x.x
 NLRI: SAFI = SDWAN
 Tunnel Encap Attr (SDWAN-Hybrid)
 Tunnel-egress-endpoint SubTLV
 GRE tunnel (via the L3VPN)
IPSec SA-IDs
 Color-SubTLV = RED

NLRI Length
Site-Type
Port-Local-ID
SiteID= ColorRED
Node-ID =2.2.2.2

BGP Route Controller - RR

L3VPN path

Client Route: 11.1.1.x
 Client Route: 21.1.1.x

C-PE 1
 lo: 1.1.1.1

ISP3: 192.10.0.10
 ISP2: 160.0.0.1

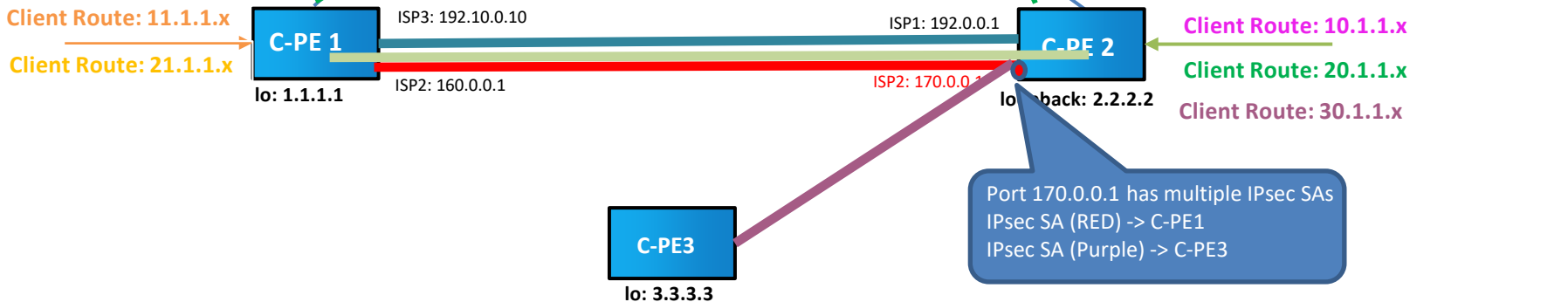
ISP1: 192.0.0.1
 ISP2: 170.0.0.1

C-PE 2
 lo: back: 2.2.2.2

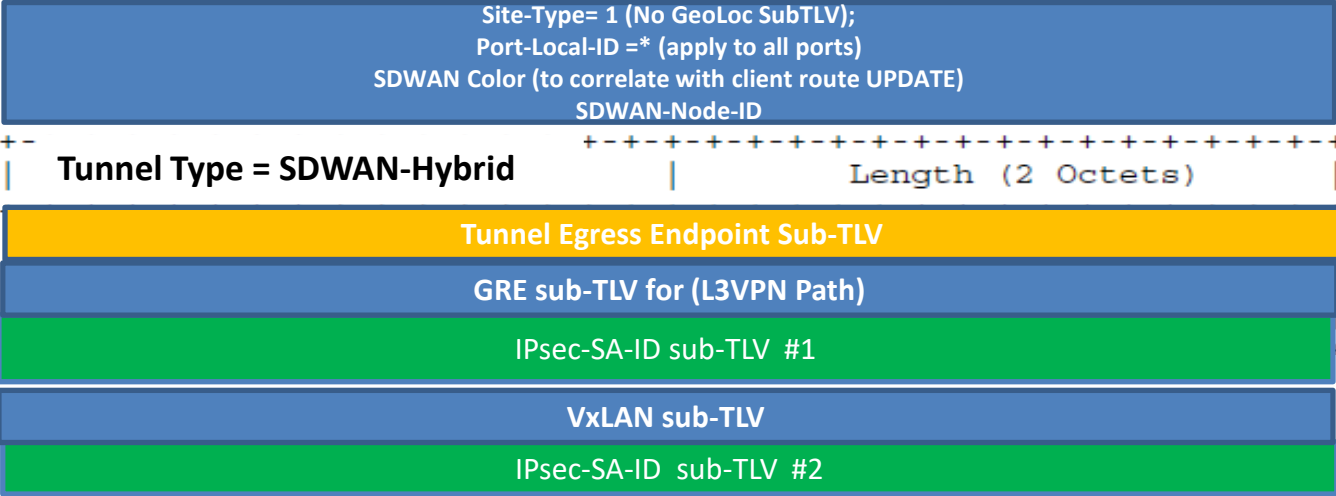
Client Route: 10.1.1.x
 Client Route: 20.1.1.x
 Client Route: 30.1.1.x

C-PE3
 lo: 3.3.3.3

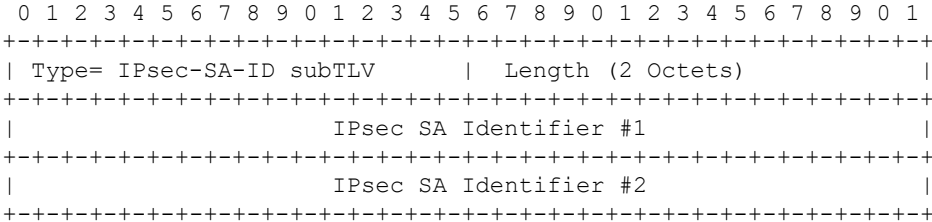
Port 170.0.0.1 has multiple IPsec SAs
 IPsec SA (RED) -> C-PE1
 IPsec SA (Purple) -> C-PE3



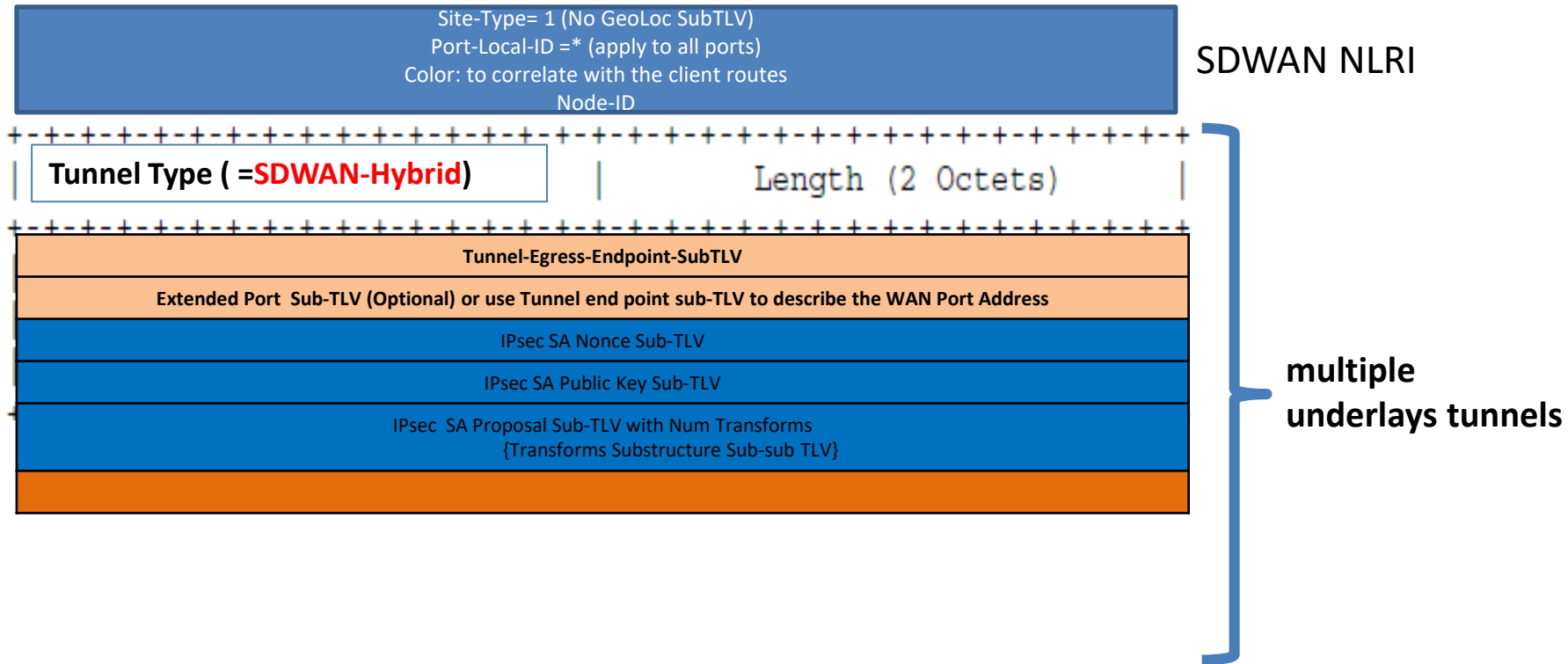
Hybrid Tunnels: with Pre-configured IPsec SA IDs



multiple underlays tunnels



Hybrid Tunnels: with detailed IPsec SA sub-TLVs





We want
your feedback!

The graphic consists of four overlapping speech bubbles. The top bubble is green and contains the word 'We'. The middle bubble is blue and contains the word 'want'. The bottom-left bubble is orange and contains the word 'your'. The bottom-right bubble is pink and contains the word 'feedback!'. The bubbles overlap in a way that creates a sense of depth and movement.