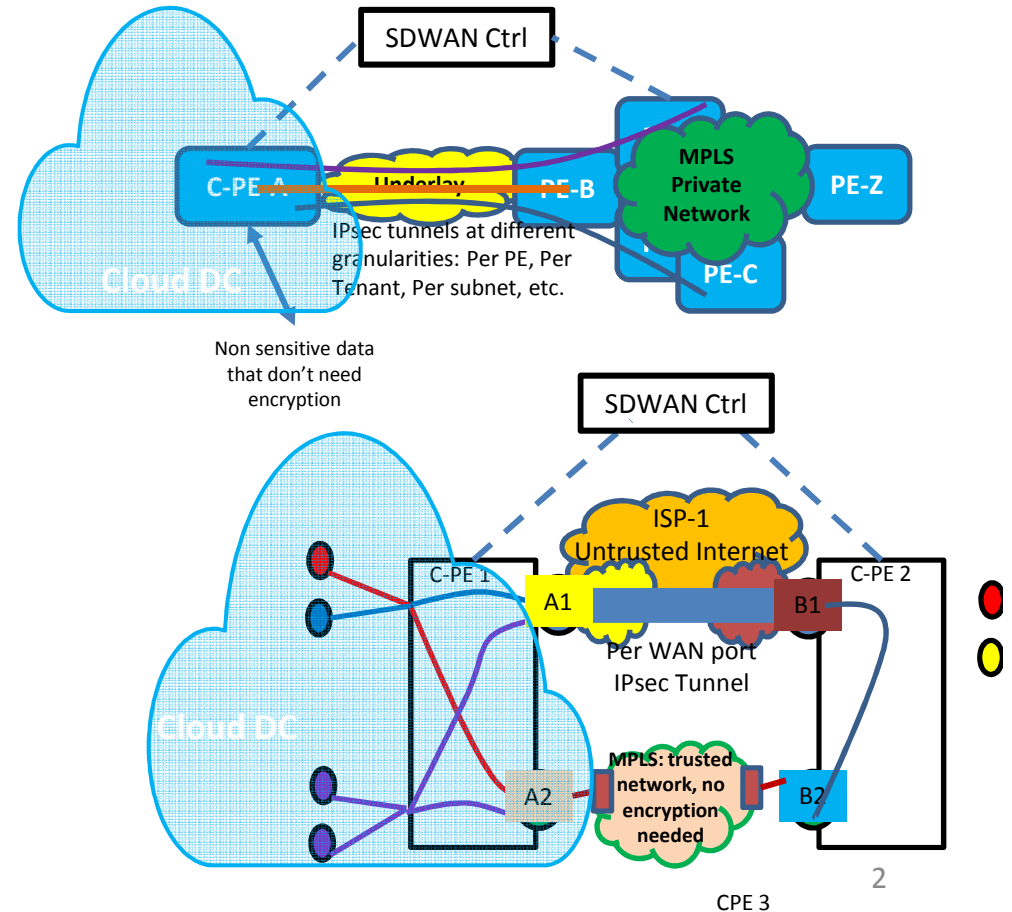


draft-dunbar-idr-sdwan-port-safi-01

Linda Dunbar
Sue Hares
Haibo Wang
Weiguo Hao
IETF 104 March 2019

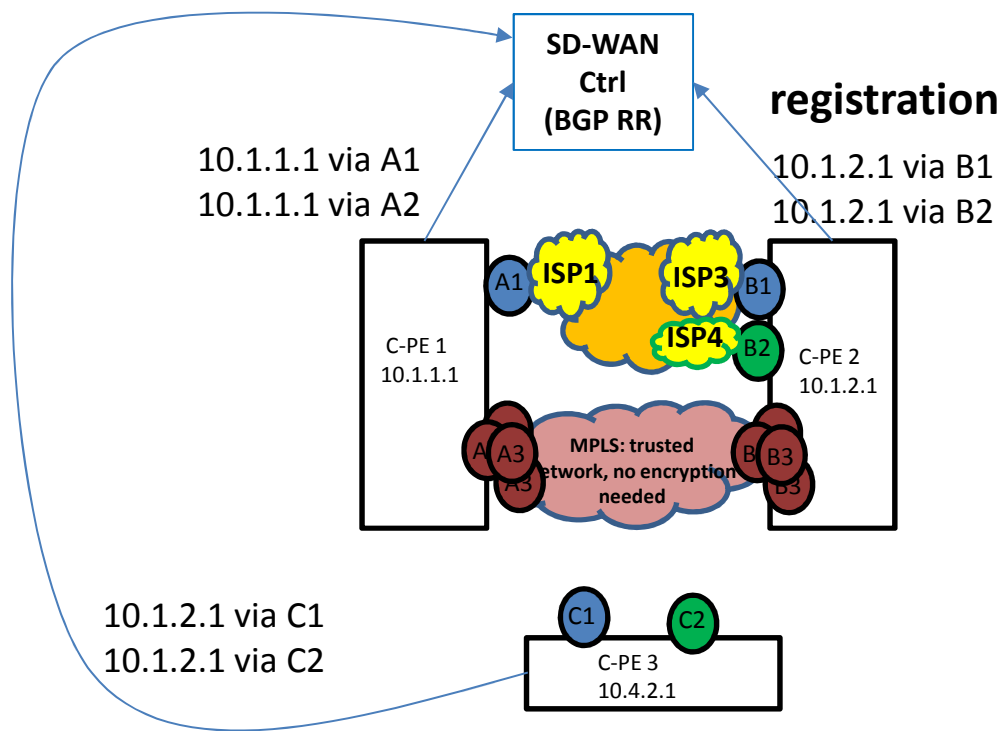
SD-WAN: Peer the onion

- **Homogeneous SD-WAN:**
 - edge encrypting all sensitive traffic to other edge nodes, regardless if the underlay is private or public.
- **SD-WAN over Hybrid Networks**
 - Key :
 - Traffic over Private VPN networks (e.g. MPLS) can go natively without encryption to achieve better performance, and
 - traffic over internet are carried by IPsec tunnels.
 - User specified policy governs a flow



WAN Ports Registration

SD-WAN node's private address and WAN Ports/Addresses registration.



- WAN ports can be from different network providers (A1/A2/A3/B1/B2/B3)
- Each PE advertises its WAN ports to Controller, which then propagates the advertisements to authorized peers.
- **PEs Loopback addresses & routes attached are not visible to some ISPs**

A1/A2/A3/B1/B2/B3 are logical address that can be applied to a set of ports

New NLRI for SDWAN WAN Ports

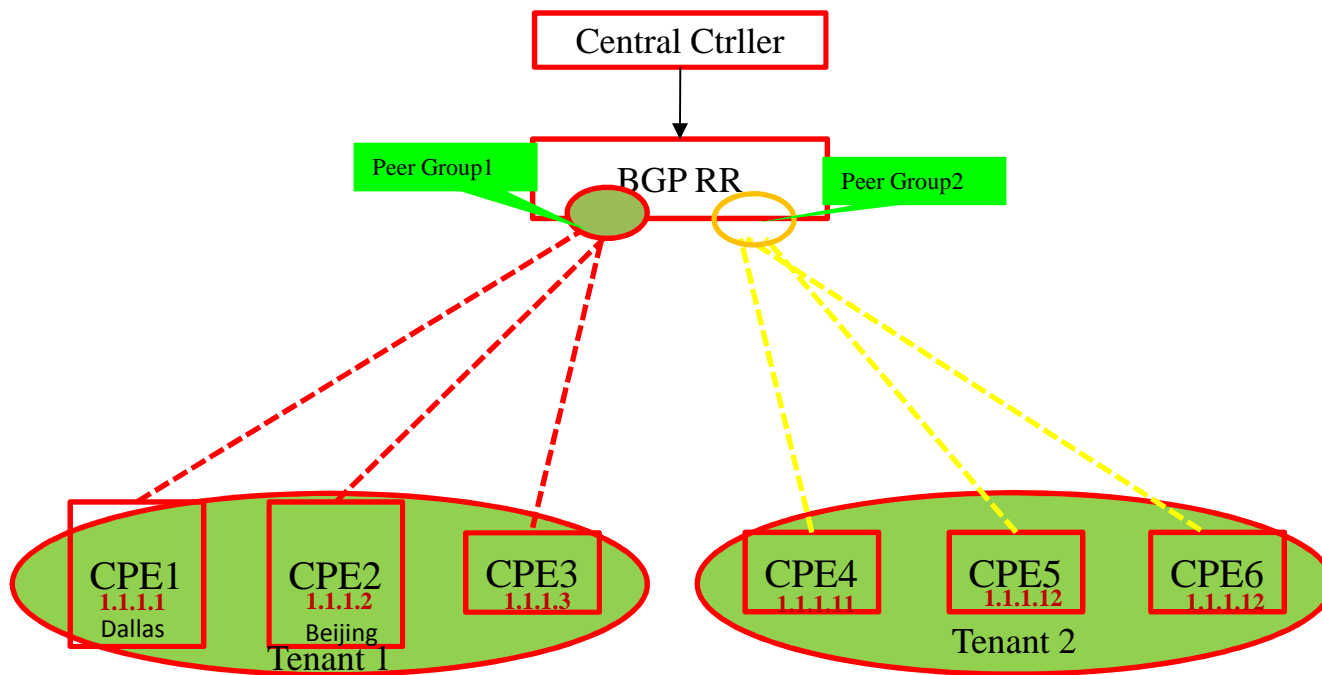
NLRI Length	1 octet
SDWAN-Type	2 Octets
Port-Distinguisher	4 octets
SDWAN-Site-ID	4 octets
SDWAN-Node-ID	4 or 16 octets

The new SAFI=74 has been assigned by IANA for advertising properties of WAN ports that face untrusted networks

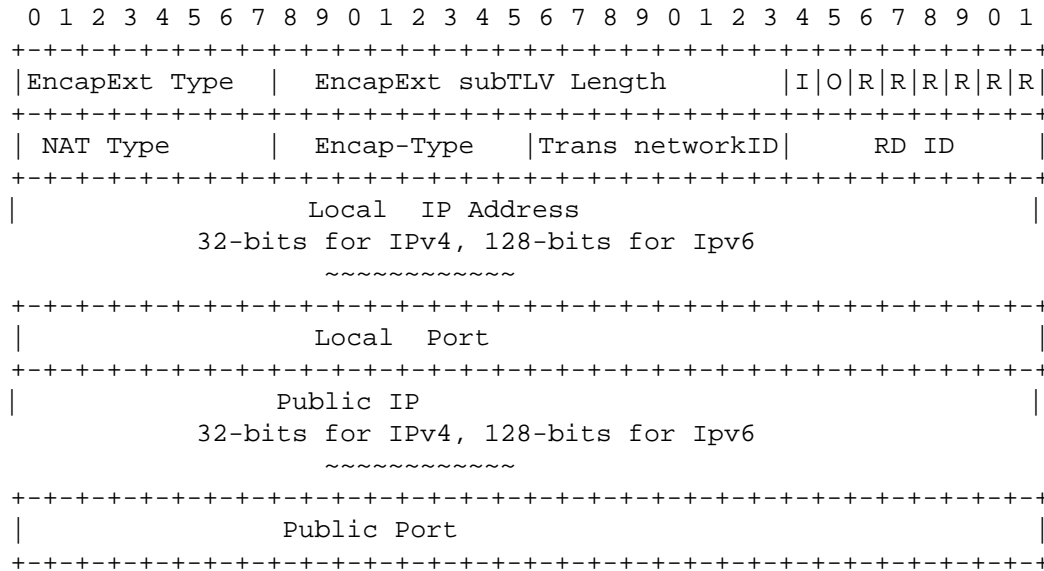
- SDWAN NLRI Length: expressed in bits as defined in [RFC4760].
- SDWAN-Type: to define the encoding of the rest of the SDWAN NLRI.
- Port Distinguisher: SDWAN node Port identifier.
- SDWAN-Site-ID: used to identify a common property shared by a set of SDWAN nodes.
- SDWAN Node ID: the SDWAN node identifier, (e.g. system ID or the loopback address (IPv4 or IPv6)).

SDWAN Ports scoped Advertisement

- Tenant Separation Method :



Extended Port Property



Flags:

-I bit (CPE port address or Inner address scheme)

If =0 → inner addr is IPv4.

If =1 → inner address is IPv6.

-O bit (Outer address scheme):

If =0 → the public (outer) address is IPv4.

If =1 → the public (outer) address is IPv6.

-R bits: reserved for future use.

Must be set to 0 now.

NAT Type: without NAT; 1:1 static NAT; Full Cone; Restricted Cone; Port Restricted Cone; Symmetric; or Unknown (i.e. no response from the STUN server).

Encap Type : the supported encap types for the port facing public network, such as IPsec+GRE, IPsec+VxLAN, IPsec without GRE, GRE (when packets don't need encryption)

Transport Network ID: Central Controller assign a global unique ID to each transport network ;

RD ID: Routing Domain ID , Need to be global unique.

Local IP: The local (or private) IP address of the port ;

Local Port: used by Remote SDWAN node for establishing IPsec to this specific port.

Public IP: The IP address after the NAT. If NAT is not used, this field is set to NULL.

Public Port: The Port after the NAT. If NAT is not used, this field is set to NULL.