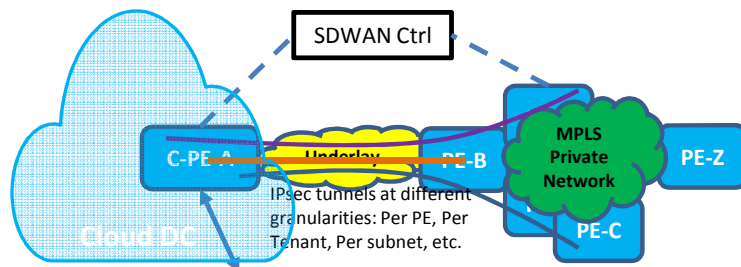# Network to Cloud DC (Net2Cloud) Update
IETF 104

draft-ietf-net2cloud-problem-statement-00
draft-ietf-net2cloud-gap-analysis-01
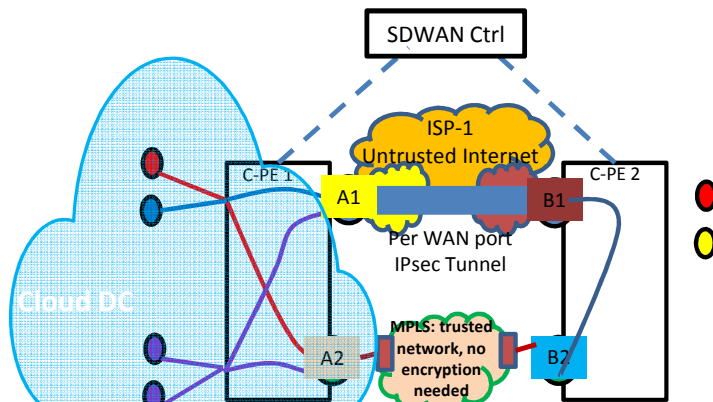
Linda.Dunbar@Huawei.com
Andy Mails (agmalis@gmail.com)
Christianjacquenet@orange.com
Mehmet.toy@verizon.com

Update since IETF 103

Homogeneous SD-WAN:

SDWAN Ctrl

MPLS Private Network

C-PE A — Underlay — PE-B — PE-Z

PE-C

IPsec tunnels at different granularities: Per PE, Per Tenant, Per subnet, etc.

Non sensitive data that don't need encryption

Cloud DC

SDWAN Ctrl

ISP-1 Untrusted Internet

C-PE 1 — A1 — B1 — C-PE 2

Per WAN port IPsec Tunnel

MPLS: trusted network, no encryption needed

A2 — B2

Cloud DC

SD-WAN over Hybrid Networks

Newly added for End Point Property Distribution

Regional Sites are fully meshed

CPEs in each cluster are controlled by the Regional RR

a. to advertise the identifiers of ports that support establishing SD-WAN overlay tunnels to other peers,

b. to advertise ports private addresses (or dynamically assigned IP addresses),

c. to advertise its supported IPsec capability, such as the supported encryption algorithms,
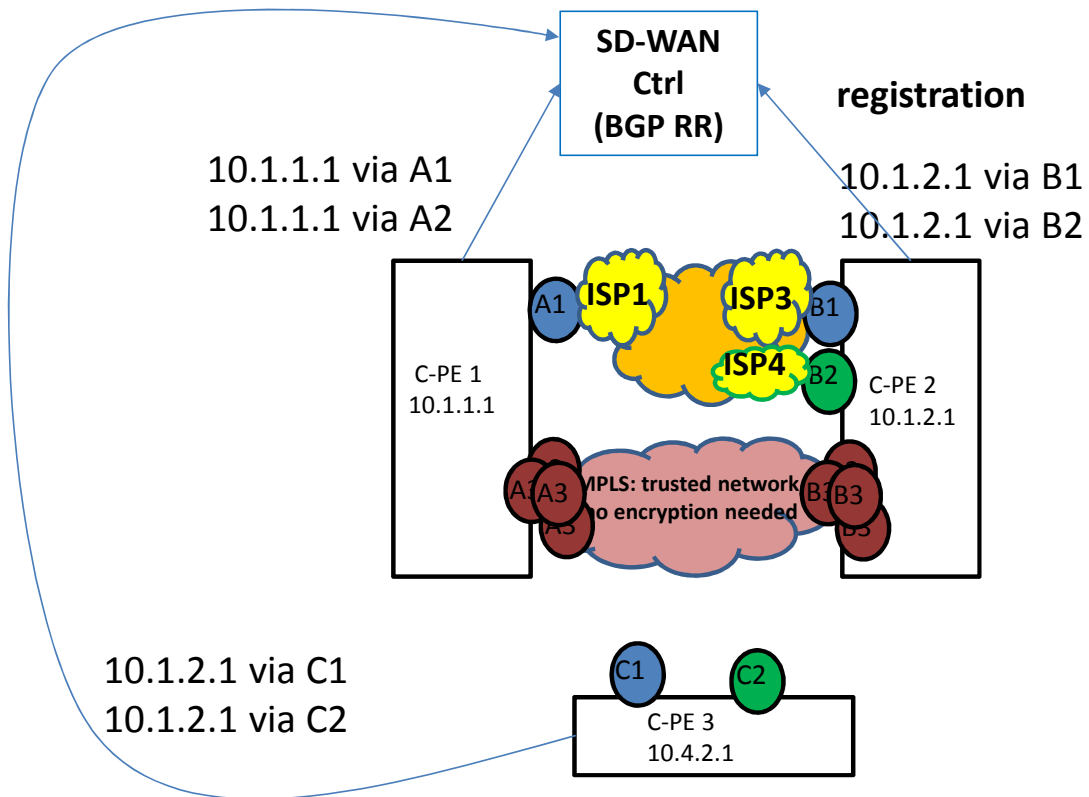
d. etc.

Tunnel Encap Gap:
How to advertise Tunnels not Yet associated with Client Routes?
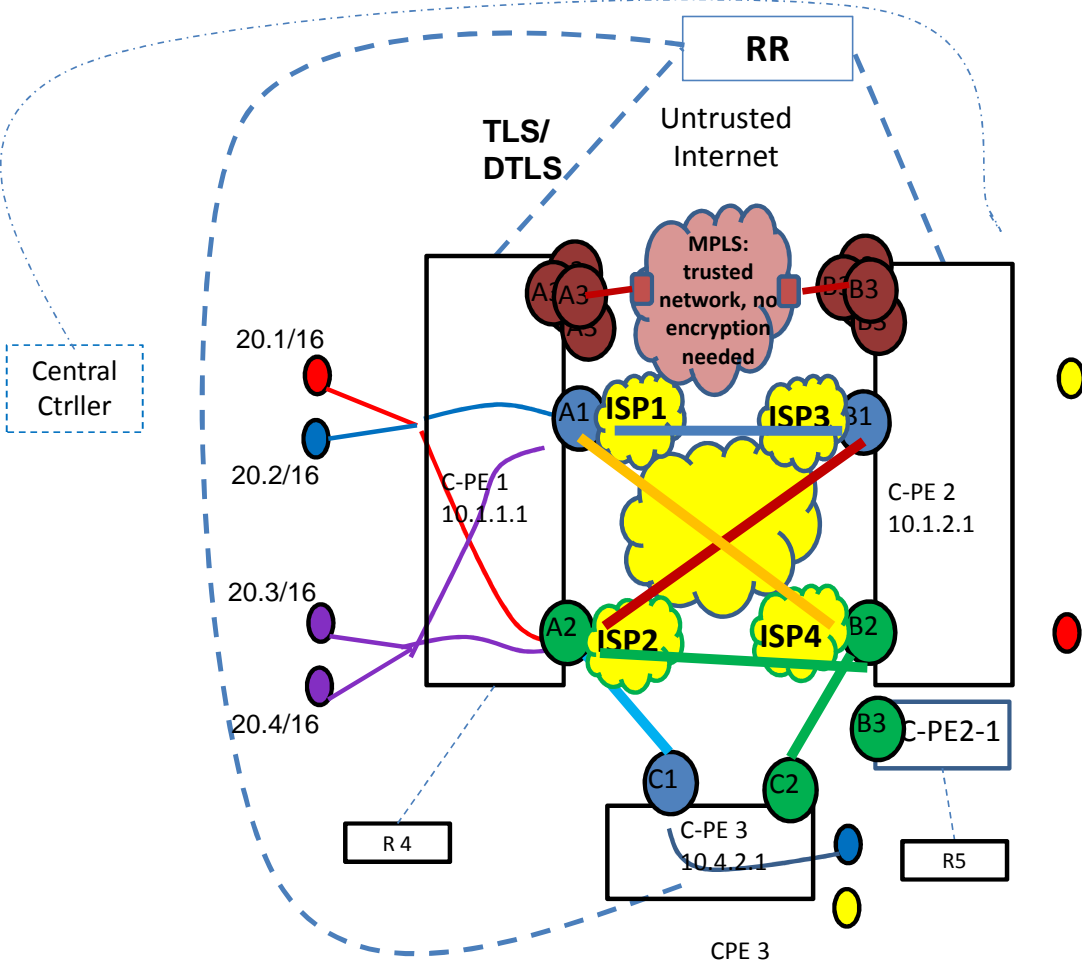
- Using Loopback address as the UPDATE?

- Using the WAN port address in the UPDATE?

- When a route 20.1/16 can be egressed by all WAN ports, include multiple Remote-end-point subTLVs for the 20.1/16?

- If 20.2/16 can also egress A1/A2, the Port-TLV for A1/A2 are repeated in each of the route update?
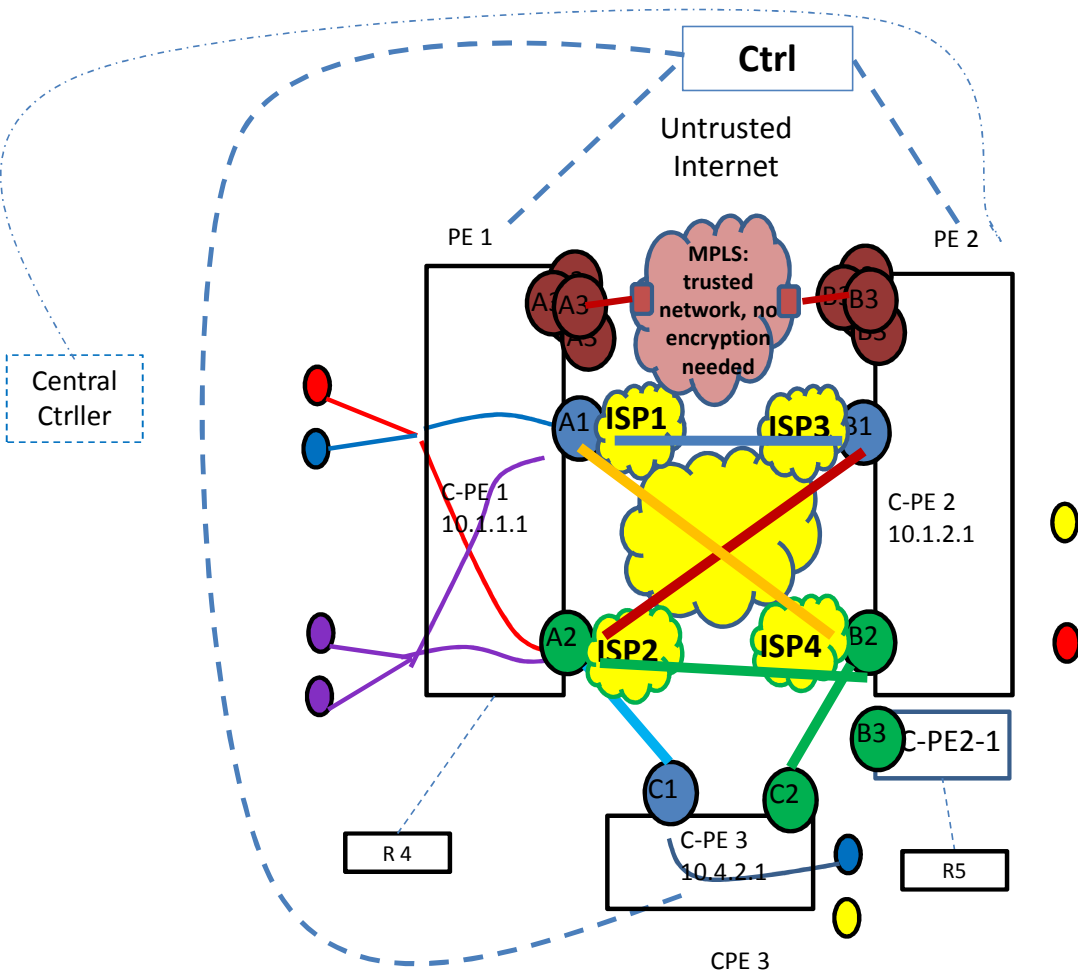
WAN port property dynamic changes and propagations?

SD-WAN Ctrl (BGP RR)

registration

10.1.1.1 via A1
10.1.1.1 via A2

10.1.2.1 via B1
10.1.2.1 via B2

ISP1 ISP3
A1 B1
ISP4 B2

C-PE 1
10.1.1.1

C-PE 2
10.1.2.1

MPLS: trusted network no encryption needed
A1 A3 B3 B3

10.1.2.1 via C1
10.1.2.1 via C2

C1 C2

C-PE 3
10.4.2.1

- A1/A2/A3/B1/B2/B3 WAN ports can be from different network providers.
- Each PE advertise its WAN ports to Controller, which then propagate 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

Three different Tiers of SD-WAN Control Plane

Ctrl

Untrusted Internet

Central Ctrller

PE 1

PE 2

MPLS: trusted network, no encryption needed

A1A3

D1B3

A1 ISP1

ISP3 B1

C-PE 1 10.1.1.1

C-PE 2 10.1.2.1

A2 ISP2

ISP4 B2

B3 C-PE2-1

C1

C2

R 4

C-PE 3 10.4.2.1

R5

CPE 3

1. **End Node Registration & Initial setup: SD-WAN node's private address and WAN Ports/Addresses registration to the SD-WAN Controller.**
2. **Controller facilitated IPsec SA association establishment among WAN Ports**
3. **Attached routes distribution using BGP RR:**
   - **EVPN**
   - **IPVPN**
   - **Or something else**

IRTFopen Fabric Edge Presentation
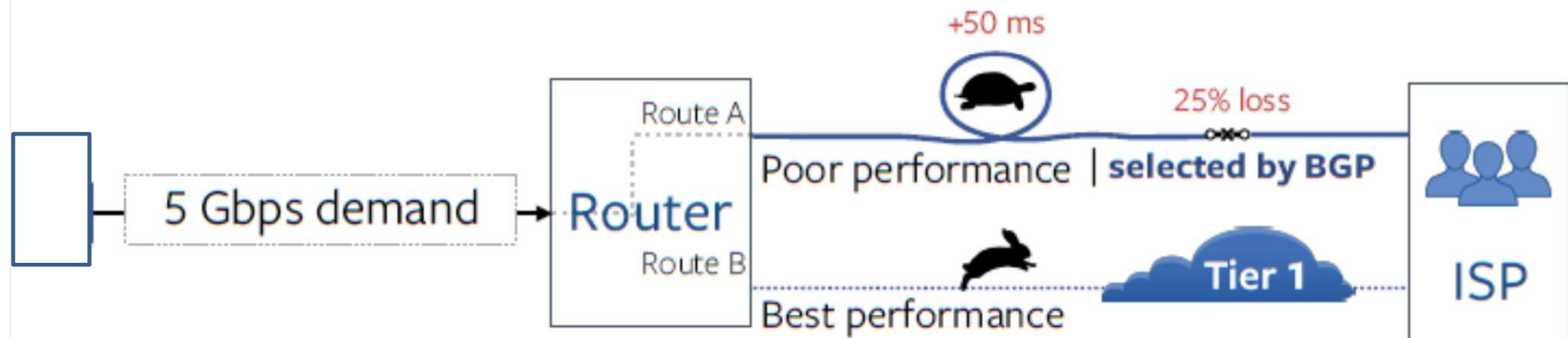
Next Step

Please follow up the discussion in BESS, IDR, IPsecme, I2NSF and Opsawg for the related work:

- ➢   Routing Area:
  - ▪ IDR WG
    draft-dunbar-idr-sdwan-port-safi-00

  - ▪ BESS WG:
    draft-sajassi-bess-secure-evpn-01
    draft-rosen-bess-secure-l3vpn-00
    draft-dunbar-bgp-sdwan-usage-00 (to be uploaded)

- ➢   Security Area
  - ▪ I2NSF WG:
    SDN controller managed IPsec keys: draft-ietf-i2nsf-sdn-ipsec-flow-protection-03
  - ▪ IPsecme WG:
    draft-carrel-ipsecme-controller-ike-01

- ➢ Ops Area:
  - ▪ Opsawg:
    SD-WAN service data models: https://datatracker.ietf.org/doc/draft-sun-opsawg-sdwan-service-model/