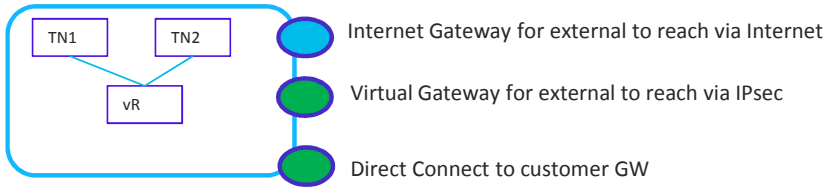
# Network to Cloud DC (Net2Cloud) Update
# IETF 105

**draft-ietf-net2cloud-problem-statement-03**
**draft-ietf-net2cloud-gap-analysis-02**

Linda.Dunbar@futurewei.com
Andy Mails (agmalis@gmail.com)
Christianjacquenet@orange.com
Mehmet.toy@verizon.com

# Problem Statement Update Since IETF 104

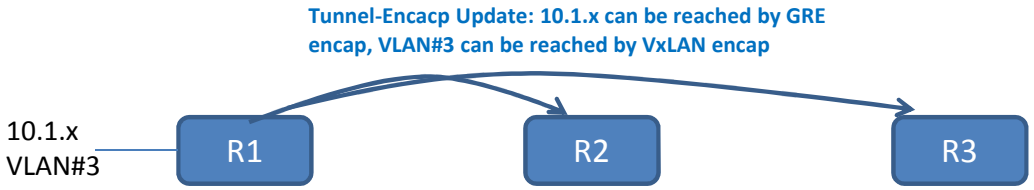
- Add a section to explain The role of SD-WAN techniques in Cloud DC connectivity (Section 1.2)
  - Focus on the issues associated with connecting enterprises to their workloads/applications instantiated in multiple third-party data centers (a.k.a. Cloud DCs)
- Add more details to VPC , Internet GW, Virtual GW, Transit  GW, and Direct Connect
  - VPC (Virtual Private Cloud) is a virtual network dedicated to one client account. It is logically isolated from other virtual networks in a Cloud DC. Each client can launch his/her desired resources, such as compute, storage, or network functions into his/her VPC. Most Cloud operators' VPCs only support private addresses, some support IPv4 only, others support IPv4/IPv6 dual stack.



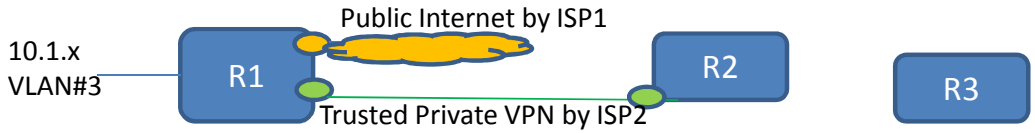

- Add details to multiple approaches to connect workloads in Cloud DCs, and associated problems
  - Cloud DCs do not expose their internal networks: can advertise all the routes instantiated in the Cloud DCs (even including the routes physically located to different sites). Result in inefficient routing and non visibility

# Gap analysis update since IETF 104
# Tunnel-Encap

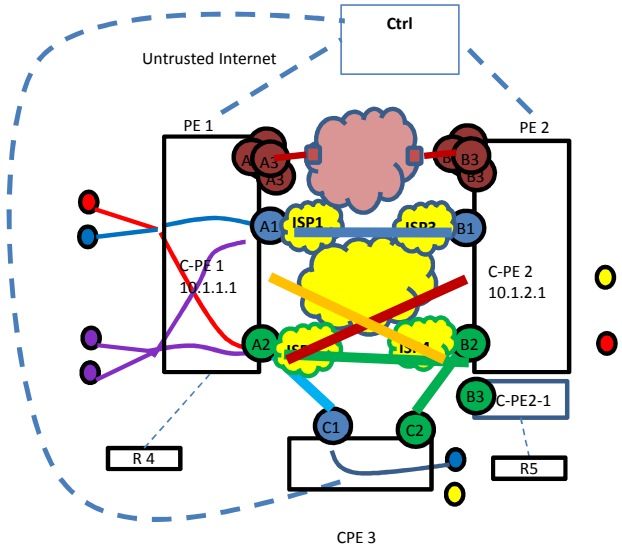
- Client routes distribution, just like EVPN or L3VPN using [Tunnel-Encap] to advertise all possible tunnels for clients routes.




- But Tunnel-Encap doesn't address the WAN ports properties:



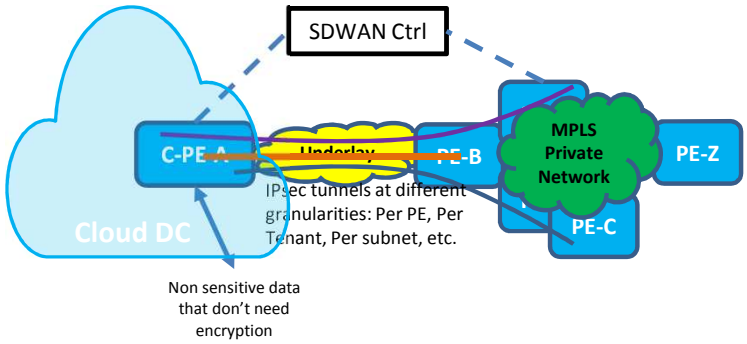

  - Each SDWAN edge node needs to advertise its WAN ports properties via the secure channel with the RR.
  - RR then propagates the received WAN ports properties to the authorized peers based on appropriate policies.

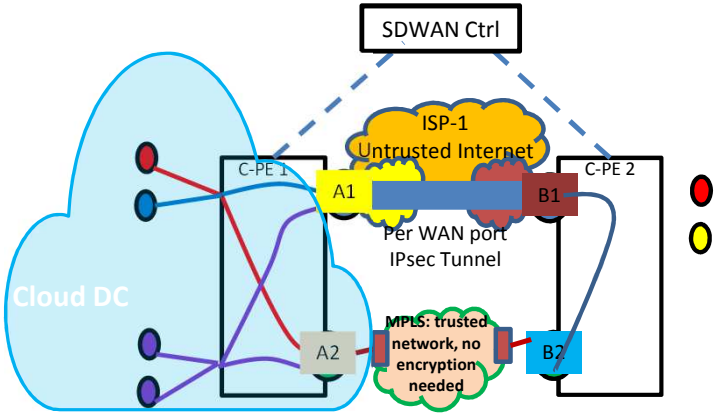



- SDWAN edges pairwise secure channel establishment BEFORE client routes are attached, such as IPsec parameters negotiation, public key exchange, etc.

# Gap Analysis Update since IETF 104: SECURE-EVPN

**Homogeneous SD-WAN:**

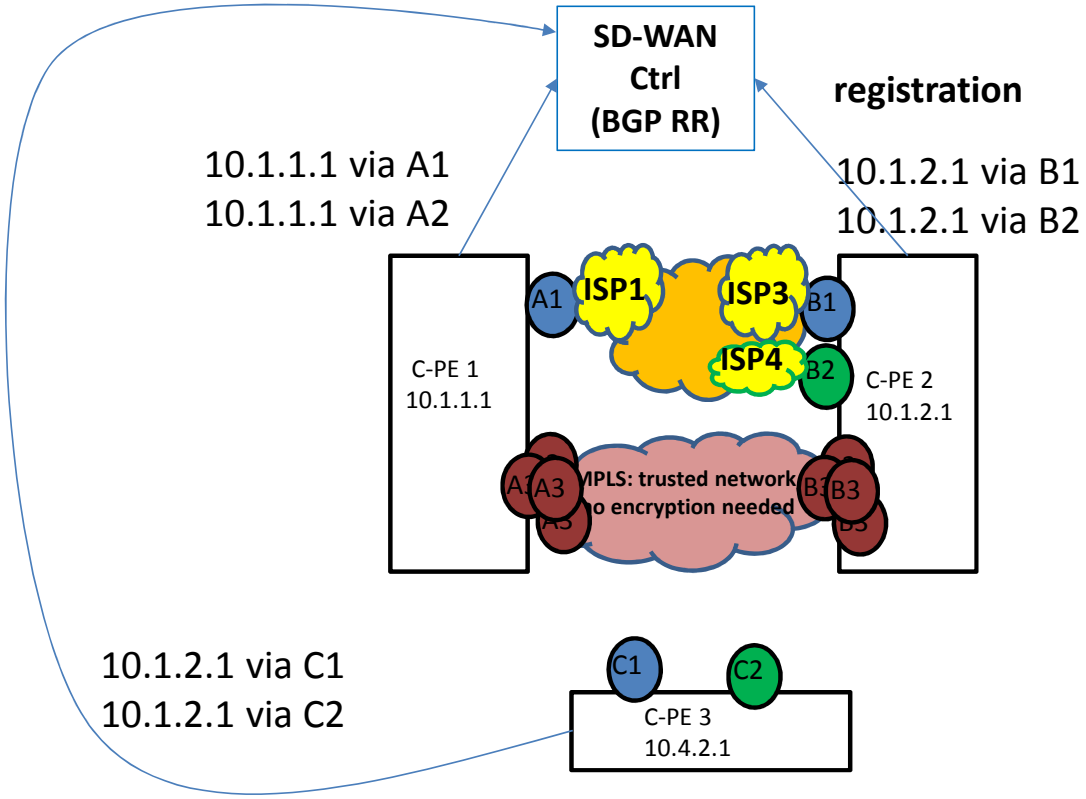



SD-WAN over Hybrid Networks

| Functionality | EVPN | IP-VPN | MVPN | VPLS | SDWAN |
|---|---|---|---|---|---|
| per PE | IPv4/v6 route | IPv4/v6 route | IPv4/v6 rte | IPv4/v6 | Y |
| per tenant | IMET (or new) | lpbk (or new) | I-PMSI | N/A | Y |
| per subnet | IMET | N/A | N/A | VPLS AD | Y |
| per IP | EVPN RT2/RT5 | VPN IP rt | *,G or S,G | N/A | Y |
| per MAC | EVPN RT2 | N/A | N/A | N/A | Y |
| **Per WAN Port** | **N/A** | **N/A** | **N/A** | **N/A** | **Property** |
| Cluster Of PEs | | | | | Y |

# WAN port property dynamic changes and propagations?




- 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

# Next Step

- Request for WGLC