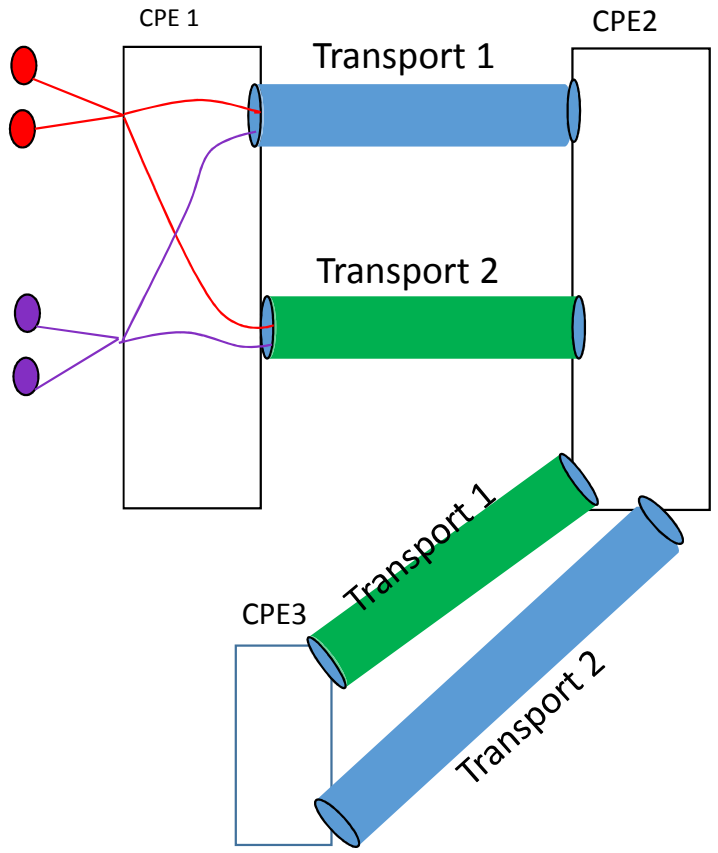
Net2Cloud -- SD-WAN
IETF 103

draft-dm-net2cloud-problem-statement-03
draft-dm-net2cloud-gap-analysis-02

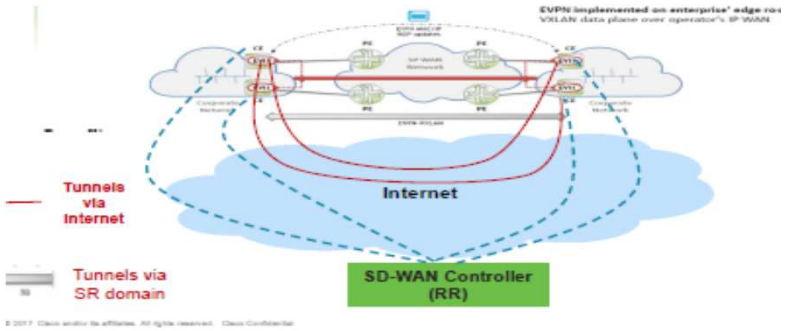
Linda.Dunbar@Huawei.com
Andy Mails (agmalis@gmail.com)
Christianjacquenet@orange.com
Mehmet.toy@verizon.com

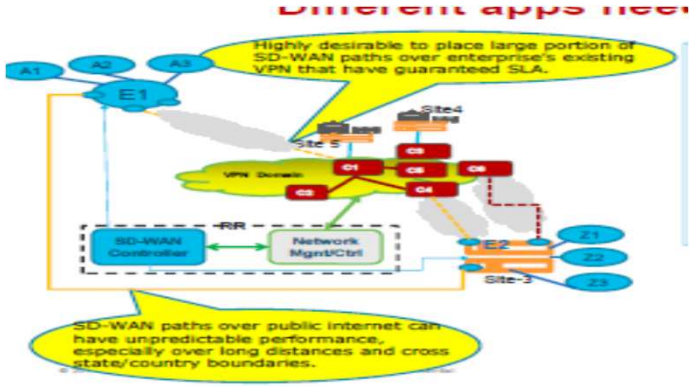
Update since IETF 102:
Key Characteristics for Large Scale SD-WAN Aggregating Multiple Transport Networks between sites

1. SD-WAN IPsec - Transport establishment needs to be separate from Routes/services attached to each site.
2. Route distribution has to be independent from multiple transport networks between sites
   - Site based routes (instead of port based routes)
3. Transport selection between sites are local section. Same service can use different Transport networks between sites.
   - Different services, routes, or VLANs can be carried by one SD-WAN Transport; same service/routes/VLAN can be carried by different SD-WAN Transport at different time depending on the policies specified by users.
4. Managing IPsec Keys and re-Keys are complicated, it does not scale well if a SD-WAN end point has to manage many fine-grained tunnels with its peers, such as per route, per VLAN based SD-WAN IPsec tunnel.

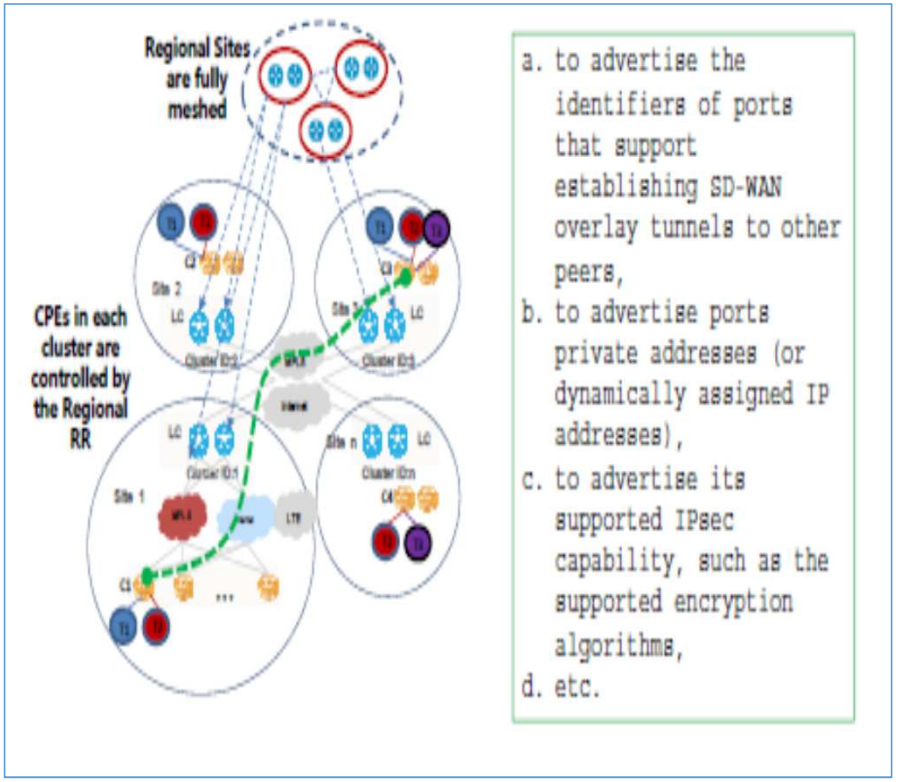


Update since IETF 102





Newly added for End Point Property Distribution



Gap: draft-ietf-idr-tunnel-encaps-10

- Tunnel-Encap requires Tunnels being associated with routes.
  - Needs more to achieve switching services from one tunnel to another Tunnel, or merge services from multiple Tunnels to one.
  - It was suggested to a “Fake Route” for a SD-WAN node to use [Tunnel-Encap] to advertise its SD-WAN tunnel end-points properties:
    - using “Fake Route” can create deployment complexity for large SD-WAN networks with many tunnels. E.g. ,
- Doesn’t have subTLV for IPsec attributes propagation
- Doesn’t have subTLV for NAT property propagation.

Gap of draft-rosen-bess-secure-l3vpn-01

- The use case is specific about a remote CPE node to be integrated with the L3VPN network. With IPsec key pre-provisioned.
- It assumes that C-PE and RR are connected by IPsec tunnel.
  - With zero touch provisioning, we need an automatic way to synchronize the IPSec SA between C-PE and RR. The draft assumes:
  - A C-PE must also be provisioned with whatever additional information is needed in order to set up an IPsec SA with each of the red RRs
- No periodic refreshment of the keys.
- IPsec usually only send configuration parameters to two end points and let the two end points to negotiate the KEY. Now we assume that RR is responsible for creating the KEY for all end points. When one end point is compromised, all other connections are impacted.

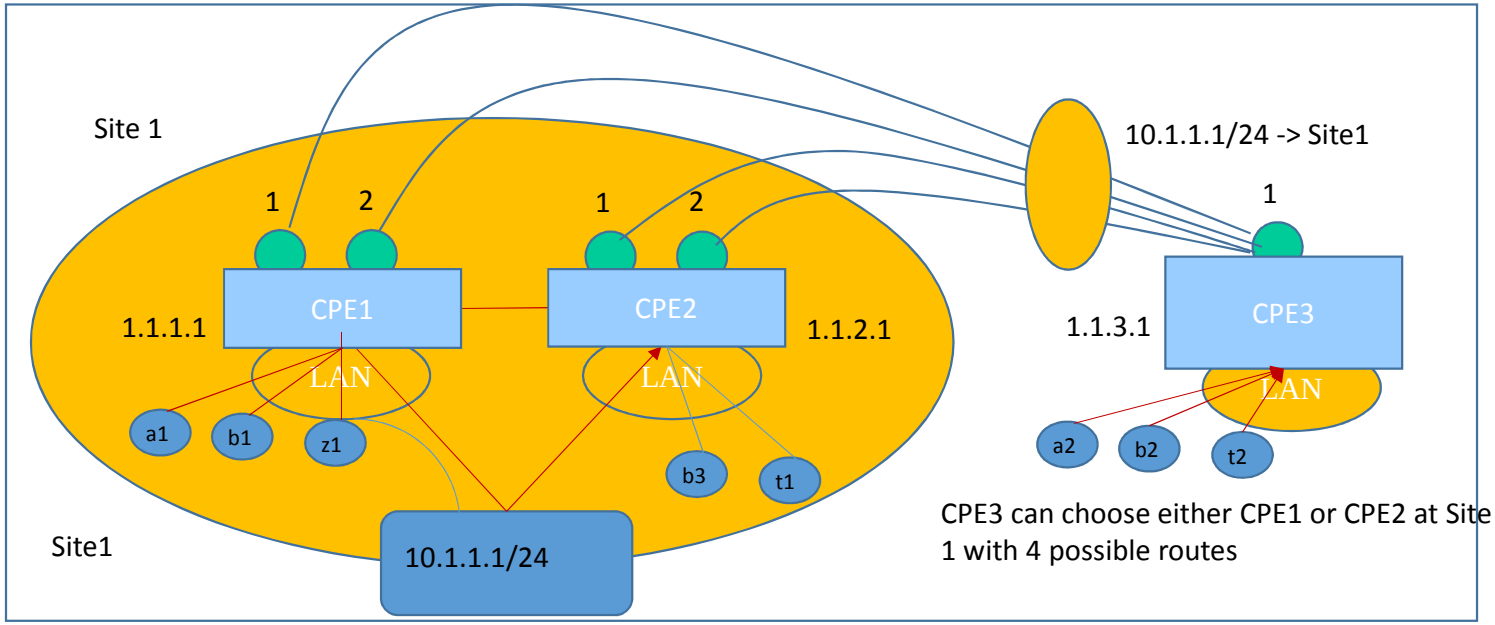
To stimulate the discussions…..

Protocols work for IETF?

e.g.
draft-dunbar-idr-bgp-sdwan-overlay-ext-02
draft-sajassi-bess-secure-evpn-00

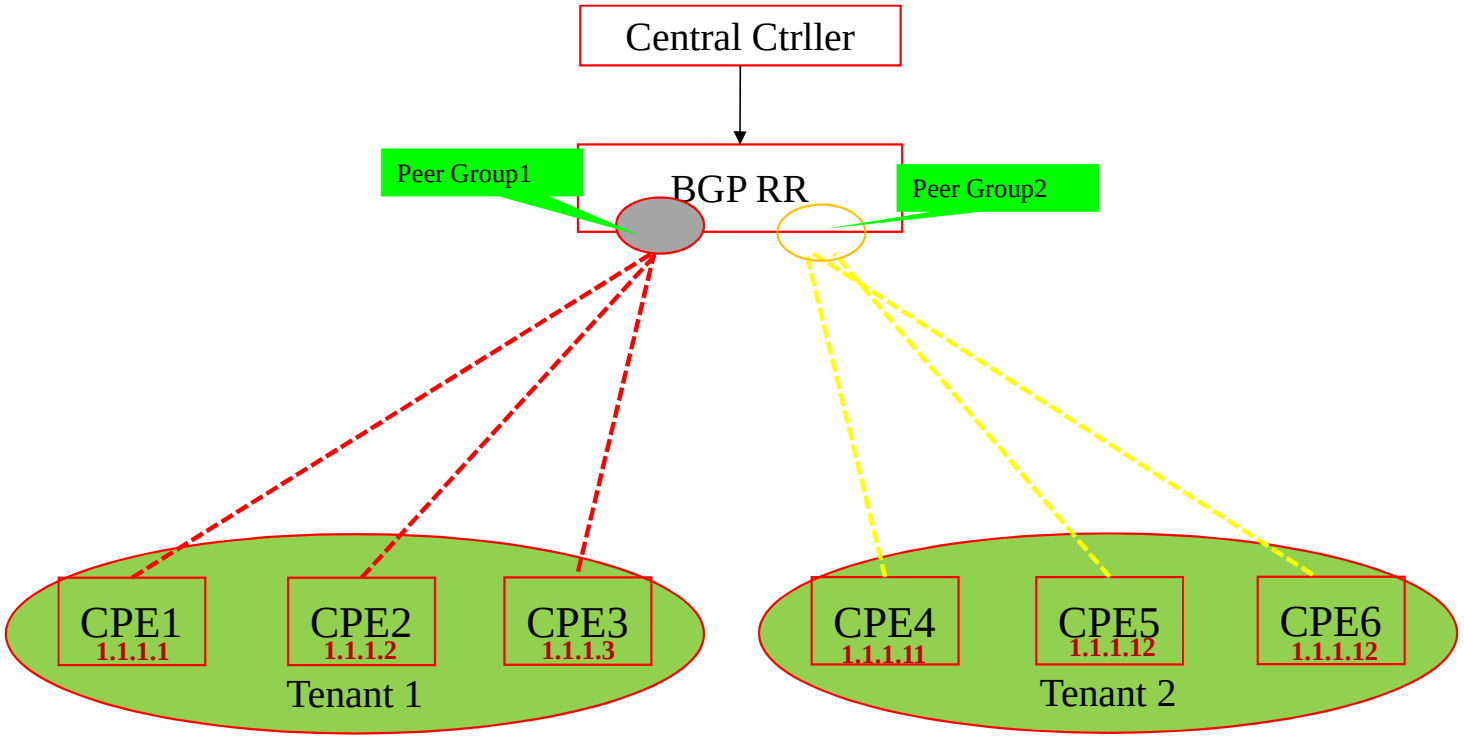
BGP Solution Briefing

- Unlike NHRP/DSVPN, every node use BGP to distribute its Tunnel end point properties
- Defines a new BGP SAFI with a new NLRI in order to advertise a SD-WAN edge node's capabilities in establishing SD-WAN overlay tunnels with other SD-WAN nodes through third party networks.
  - The goal is for SD-WAN network to scale, enabling SD-WAN overlay tunnels among large number of SD-WAN nodes to be established with few provisioning needed



Tunnel Information Advertisement Method

- Tenant Separation Method：



CPE1：

- Receiving SD-WAN IPSEC infor、report WAN ports information to Controller via SD-WAN SAFI
- RR send to CPE2、CPE3 （using Policy Filtering to only send to Peers belong to same tenant)
- CPE2、CPE3 upon receiving SD-WAN IPSEC config information, start to negotiate with peers on IPsec tunnel establishing and establish the key.
- SD-WAN IPSEC tunnel is added to the Service Tunnel (IDR-Tunnel-encap) to be used for Route Advertisement

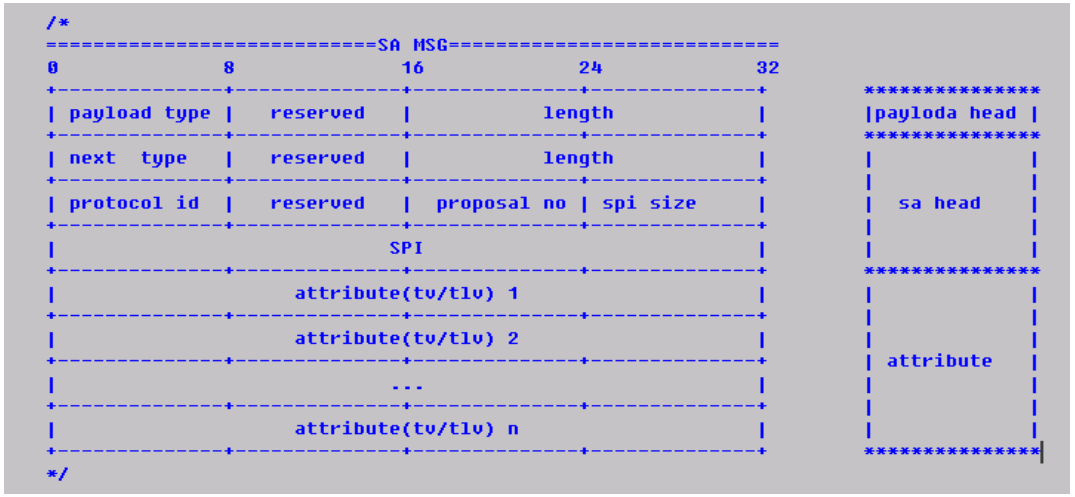
For Tenant Separation: CPEs belonging to same Tenant are added to a Peer Group

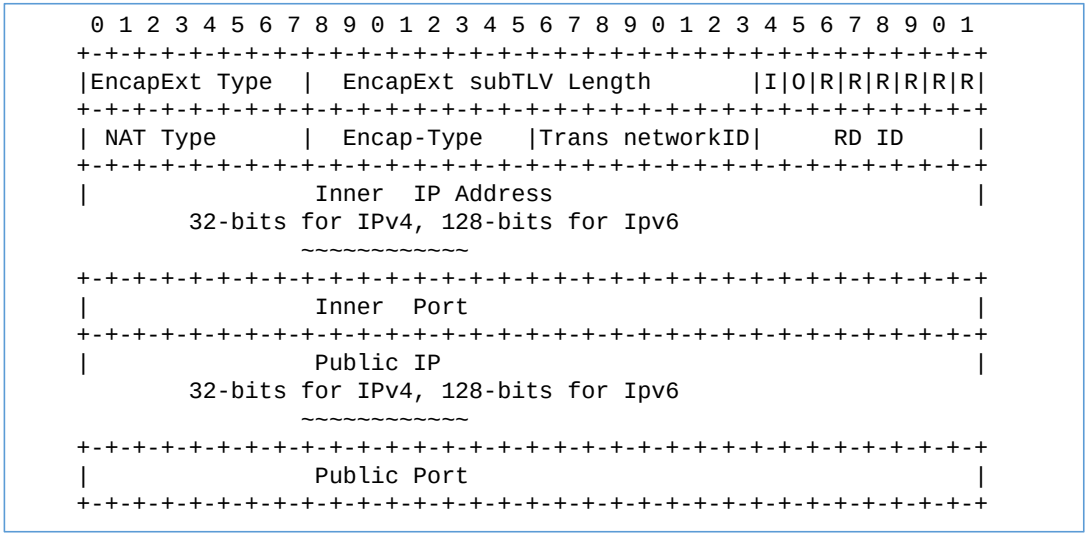
```
peer group1 route-policy tenant1-in import
peer group1 route-policy tenant1-out export
route-policy tenant1-in permit node 10
  apply community 100:1 addtitive
route-policy tenant1-out permit node 10
  if-match community-filter 1
ip community-filter 1 permit 100:1
```

Others are configured in similar way

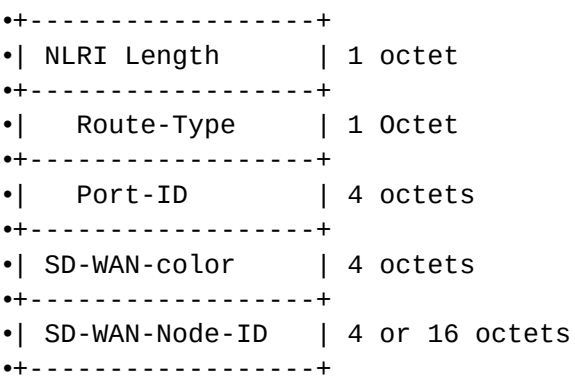
Tunnel-Encap Extension Details

- Utilize the Tunnel Encapsulation Attribute specified in draft-ietf-idr-tunnel-encaps-10
  - Tunnel Type: SD-WAN-Tunnel
  - EncapExt SubTLV (value is 128-255)
    - for describing additional information about the SD-WAN tunnel end-points, such as NAT property.
    - Added IPv6 for both private & public addresses
  - IPsec-SA Attribute SubTLV
    - for establishing IPsec SA with other peers.





SD-WAN Transport Network Property advertisement



- Route-Type: to define the encoding of the rest of the SD-WAN Overlay NLRI.
- Port ID: one (SD-WAN) node can have multiple ports, and each port can support multiple SD-WAN tunnels to different peers. The Port ID is used to identify the port, a.k.a. link identifier.
- SD-WAN-color: used to identify a common property shared by a set of SD-WAN nodes, such as the property of a specific geographic location.
- SD-WAN Node ID: the SD-WAN NLRI advertisement is sent out by the SD-WAN node to indicate all the available ports supporting SD-WAN tunnels. The SD-WAN Node ID can be the node's system ID, such as the loopback address of the SD-WAN node.

Next Step

- Request for RTGWG adoption:
  - **draft-dm-net2cloud-problem-statement-03**
  - **draft-dm-net2cloud-gap-analysis-02**