Dynamic Networks to Clouds: problem statements and IETF Solutions

draft-ietf-net2cloud-problem-statement-39

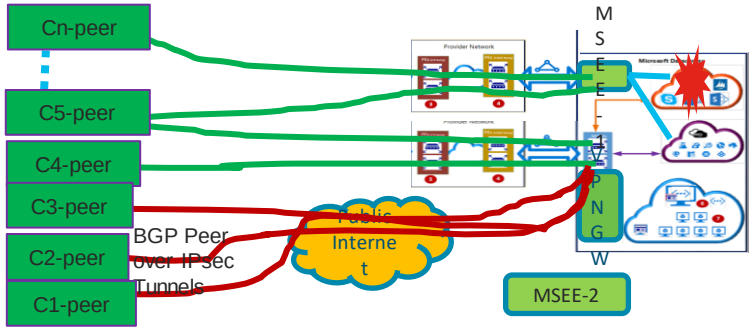
Linda.Dunbar@futurewei.com
Andy Mails (agmalis@gmail.com)
Christianjacquenet@orange.com
Mehmet.toy@verizon.com
kmajumdar@microsoft.com

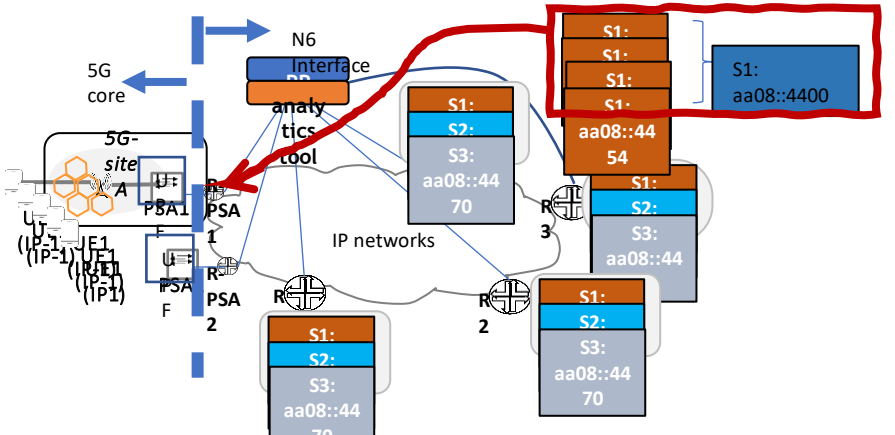
Summary of the Network Related Problems and Protocol Extensions

IETF 120 Vancouver

Summary of the key problems and the progress since 2017

- **Cloud DC GW: more peers & shorter durations without prior agreed policies.**
  - More BGP peering errors, such as capability mismatch, BGP cease notification, unwanted route leaks, missing Keepalives, etc.
  - ➢ Need proper notification when threshold crossing
- **Large number of routes change triggered by a site/pod failure or degradation**
  - One of the sites/pods have failure or reduced capacity. A group of routes (not entire AFI/SAFI) need to be switched. (VPN GW or Cloud GW are good; therefore, BFD doesn't detect the failures.)
  - ➢ draft-ietf-idr-5g-edge-service-metadata-22
- **5G Edge Clouds ANYCAST: Same service with multiple Instances at different Edge Cloud DCs**
  - The difference of routing distances is relatively small, Capacity at the Edge DC plays a bigger role for performance, Source (UEs) can ingress from different Ingress routers, etc.
  - ➢ draft-dunbar-cats-edge-service-metrics-01
- **Application Based Forwarding may require different forwarding topologies based on Application identifiers**
  - ➢ draft-ietf-idr-sdwan-edge-discovery-13



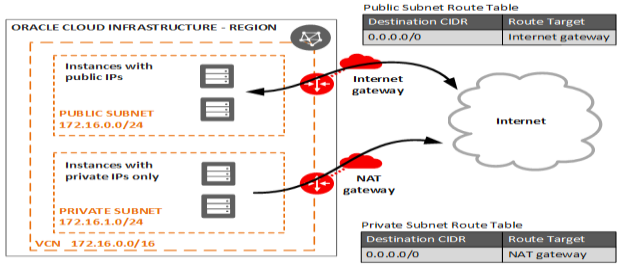


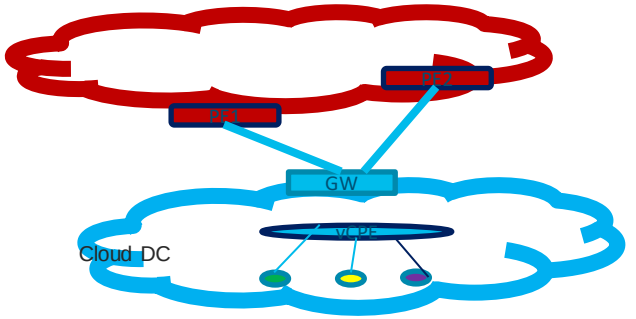
Dynamically Connect To Cloud Hosted Workloads

- **Issues with the DNS in the Context of Routing**
  - Need to establish policies and rules on how/where to forward DNS queries to

    Cloud's DNS can be configured to forward queries to customer managed authoritative DNS servers hosted on-premises and to respond to DNS queries forwarded by on-premises DNS servers.
  - Using global domain names even when an organization does not make all its namespace globally resolvable to avoid collision.

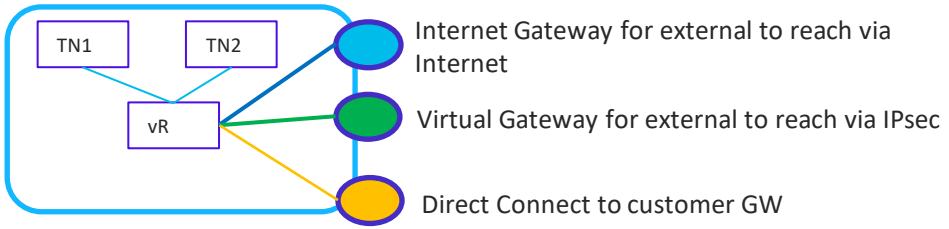
- **Cloud Discovery:** location of workloads and connectivity are not easily visible
  - Traffic Path Management: when a remote vCPE can be reached by multiple PEs of one provider VPN network, need to have methods to designate one of the egress PEs based on applications or performance.
  - Issues of Aggregating traffic over private paths and Internet paths
    - ✓ draft-ietf-idr-sdwan-edge-discovery-13
  - Desirable to have tools to discover cloud services in the same way as in on-premises infrastructure



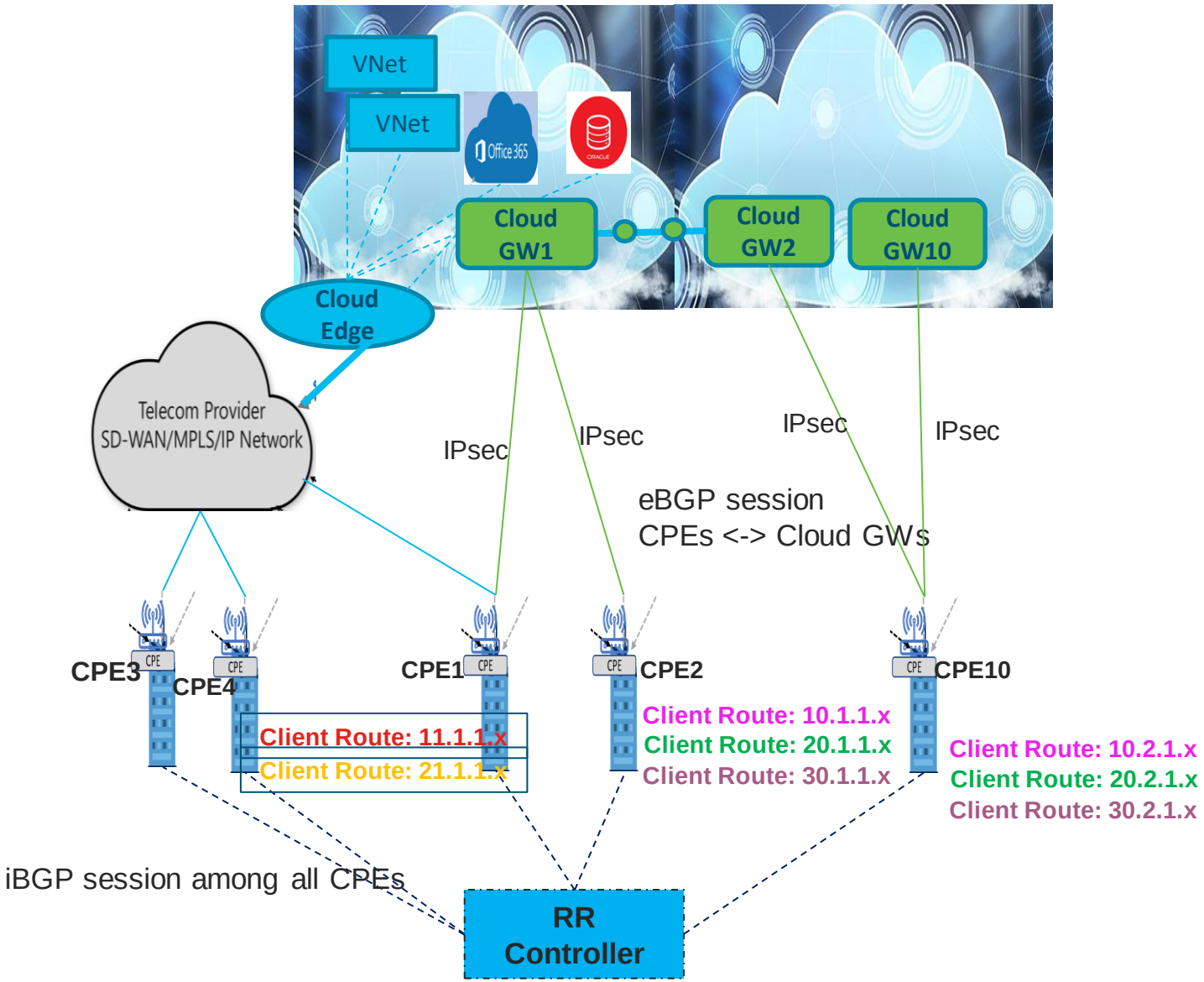


Network:
Site <-> Cloud
Cloud Backbone

- **IPsec P2P doesn’t scale well with Multipoint mesh connection & poor performance.**
- **Multiple types of connections to workloads in a Cloud DCs**
  - it is not visible to Apps in a Cloud DC what type of network access is used.
- **Difficult to collect end to end performance metrics**
- **Problems of L2/L3VPN extending to Hybrid Cloud DC**
  - PE might not have direct connections to Cloud DCs
  - Most Cloud DCs don’t’ expose their internal network. Difficult to extend MPLS-based L2/L3 VPN into Cloud DCs



Geographic Faraway Branches Connected via Cloud Backbone:
draft-ietf-rtgwg-multi-segment-sdwan-02



Why?

- The public internet among those branches might have limited bandwidth, unpredictable connection, or be prone to cyber-attacks.
- The network paths from CPEs to the Cloud GW have more reliable connections and are constantly monitored by sophisticated network functions.
- Easier to utilize Cloud-based security functions, such as Firewalls, DDoS, etc., to apply consistent policy enforcement for workloads/services to the Cloud and across the branches.
- Easier to utilize the Cloud-based tools and SaaS to collect and analyze the threat of traffic.
- Utilize the Cloud Backbone to interconnect those branches.

Security: Lightweight Authentication for Steering traffic Cross Clouds

- https://datatracker.ietf.org/doc/draft-dunbar-secdispatch-ligthtweight-authenticate/
- For transit traffic across Cloud Backbone, Cloud GWs do not decrypt and re-encrypt the payloads. The header information is used for steering encrypted traffic across Cloud Backbone → resides outside the IPsec ESP header.
- Authenticating these additional headers is important in certain environments to prevent malicious actors from tampering with header information.

Using BGP to control network connections to Cloud DCs

- draft-ietf-bess-bgp-sdwan-usage-23
- This document explores the complexities involved in managing large scale Software Defined WAN (SD-WAN) overlay networks to connect to Cloud DCs. Its objective is to illustrate how the BGP-based control plane can effectively manage large-scale SD-WAN overlay networks with minimal manual intervention.

Cloud GW discovery for Enterprise networks

- https://datatracker.ietf.org/doc/draft-sheng-idr-gw-exchange-in-sd-wan/
- The document describes the control plane enhancement for enterprise CPEs connected by Cloud Backbone to exchange the associated GW information