Net2Cloud Problem Statement and Gap Analysis

draft-dm-net2cloud-problem-statement-01

draft-dm-vpn-ext-to-dynamic-cloud-dc-gap-analysis-01

Linda Dunbar: linda.Dunbar@Huawei.com

Andy Malis: agmalis@gmail.com

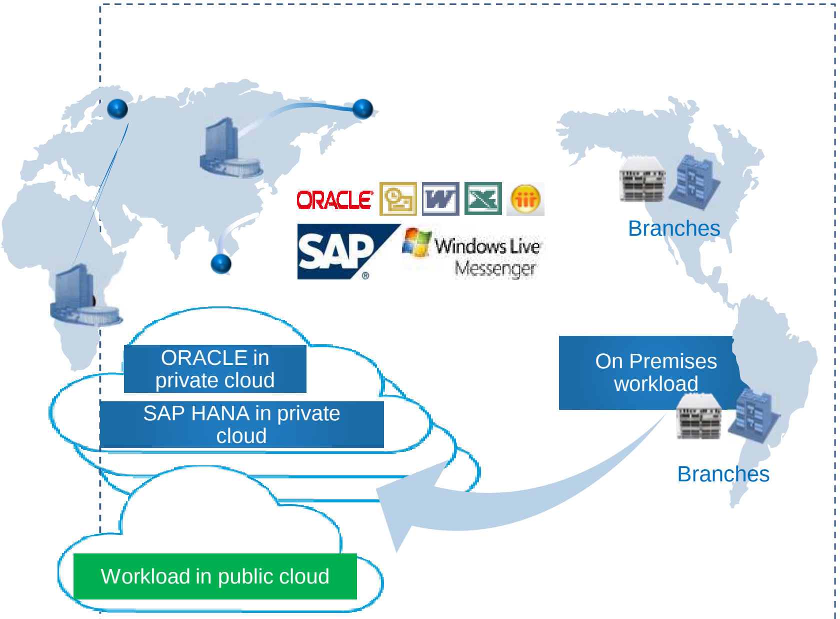
Christian Jacquenet: Christian.jacquenet@orange.com

Mehmet Toy: mehmet.toy@verizon.com

The Challenges Facing Enterprises Today?

- Digital transformation!
  - **Using more Cloud services to create better user experiences.**
  - **Motivation for moving workloads to Cloud DC:**
    - Less about reducing cost
    - More about Data Portability, App Portability
  - **Many types of Cloud DC:**
    - SAP HANA in private cloud, Oracle cloud, IBM cloud, many others in private cloud
    - In addition to AWS, Azure
- Access to DC resources needs to be optimized, regardless of the location of the end-users.

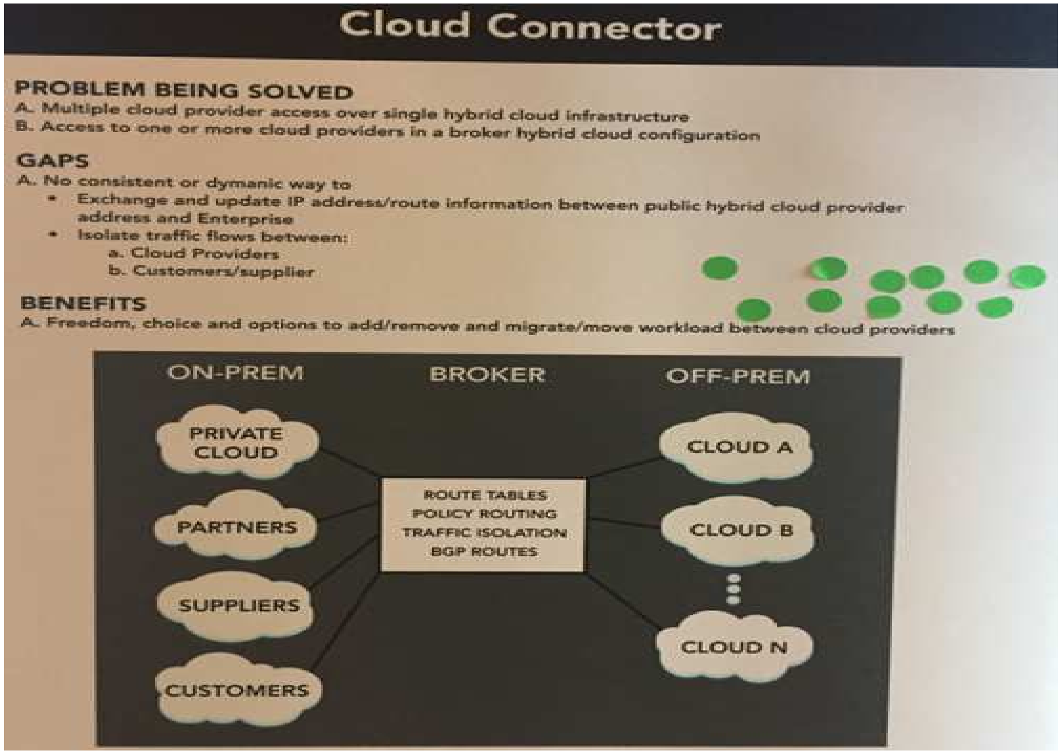
Promptly connecting Workload in remote sites and hybrid Cloud is highly desired for enterprises moving into the Digital Age



Moving Workload, Data to Hybrid Cloud DCs for Data Portability and App Portability

Highly Desired Use Case by Enterprise Community

Abundant Geographical available Cloud DC resources make it possible for Enterprises' digital transformation.



Cloud Connector

PROBLEM BEING SOLVED

A. Multiple cloud provider access over single hybrid cloud infrastructure
B. Access to one or more cloud providers in a broker hybrid cloud configuration

GAPS

A. No consistent or dymanic way to

- Exchange and update IP address/route information between public hybrid cloud provider address and Enterprise
- Isolate traffic flows between:
  - a. Cloud Providers
  - b. Customers/supplier

BENEFITS

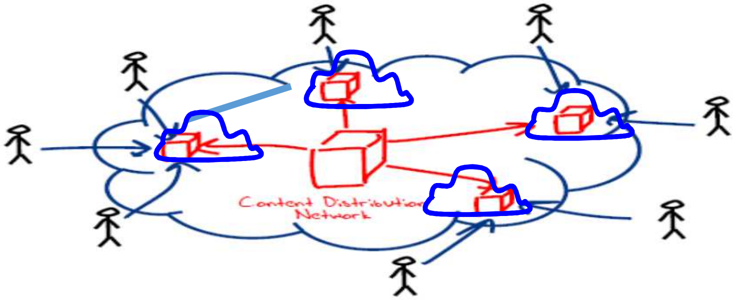
A. Freedom, choice and options to add/remove and migrate/move workload between cloud providers

ON-PREM
BROKER
OFF-PREM

PRIVATE CLOUD
PARTNERS
SUPPLIERS
CUSTOMERS

ROUTE TABLES
POLICY ROUTING
TRAFFIC ISOLATION
BGP ROUTES

CLOUD A
CLOUD B
CLOUD N

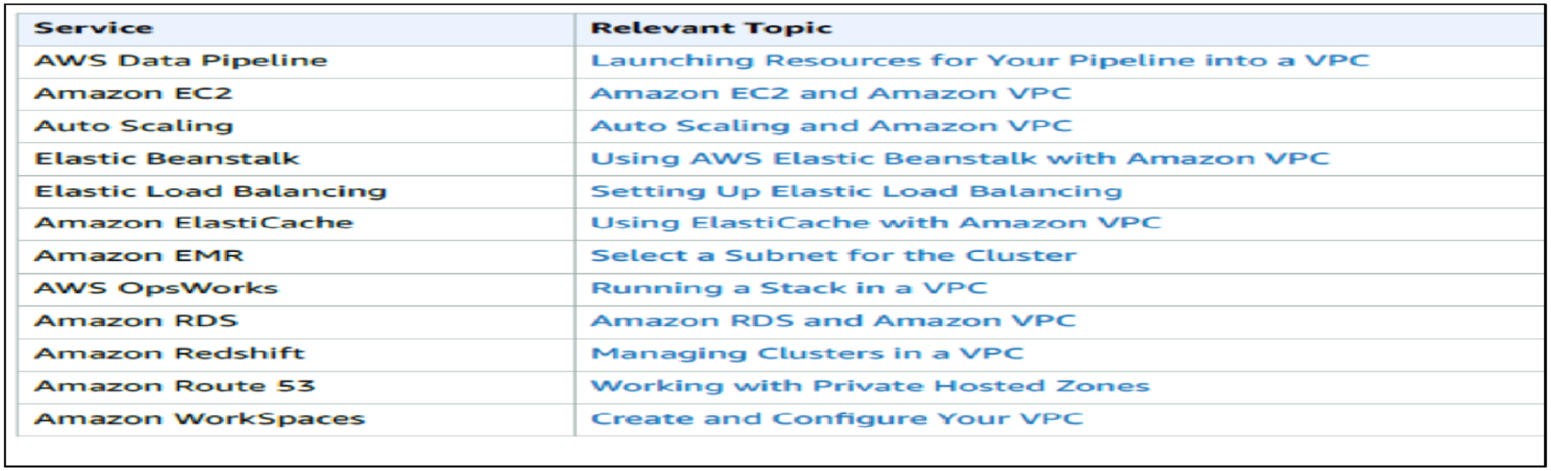


- For better QoE, users need to be close to their contents/data whatever their location,
- Network Service Provider have an opportunity to optimize (WAN) resource usage

Distinct Types of Cloud Services

1. Direct Cloud services offered directly by Cloud Operators who manage & own the infrastructure
   - such as AWS, Azure, etc,

AWS Cloud Service Example:

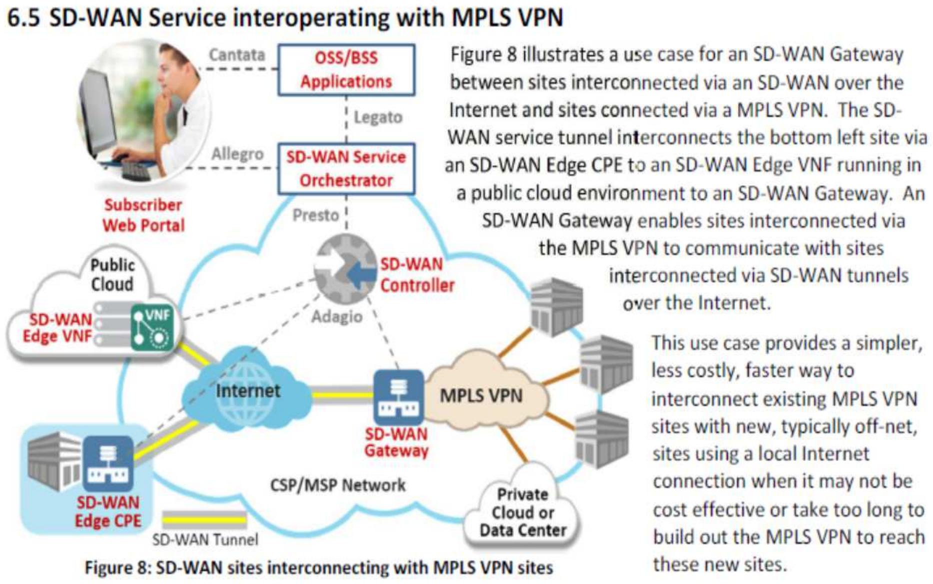


Service	Relevant Topic
AWS Data Pipeline	Launching Resources for Your Pipeline into a VPC
Amazon EC2	Amazon EC2 and Amazon VPC
Auto Scaling	Auto Scaling and Amazon VPC
Elastic Beanstalk	Using AWS Elastic Beanstalk with Amazon VPC
Elastic Load Balancing	Setting Up Elastic Load Balancing
Amazon ElastiCache	Using ElastiCache with Amazon VPC
Amazon EMR	Select a Subnet for the Cluster
AWS OpsWorks	Running a Stack in a VPC
Amazon RDS	Amazon RDS and Amazon VPC
Amazon Redshift	Managing Clusters in a VPC
Amazon Route 53	Working with Private Hosted Zones
Amazon WorkSpaces	Create and Configure Your VPC

2. Cloud Service Providers, who utilize resources from Cloud Operators to offer Managed Cloud services
   - broker who has connectivity to Cloud DCs

Consumers (i.e. enterprises) can buy services directly from the Cloud Operators, or buy Managed Cloud Services.

MEF: Cloud & SD-WAN related Activities



6.5 SD-WAN Service interoperating with MPLS VPN

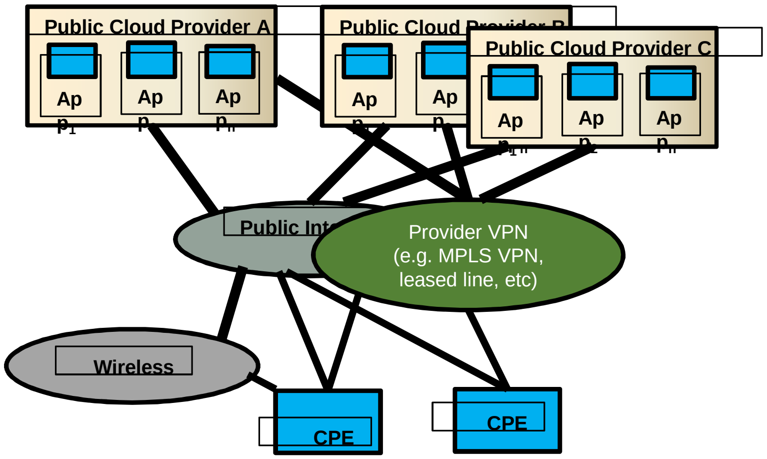
Cantata
OSS/BSS Applications
Legato
Allegro
SD-WAN Service Orchestrator
Subscriber Web Portal
Presto
Public Cloud
SD-WAN Controller
SD-WAN Edge VNF
VNF
Adagio
Internet
MPLS VPN
SD-WAN Gateway
SD-WAN Edge CPE
CSP/MSP Network
Private Cloud or Data Center
SD-WAN Tunnel

Figure 8: SD-WAN sites interconnecting with MPLS VPN sites

Figure 8 illustrates a use case for an SD-WAN Gateway between sites interconnected via an SD-WAN over the Internet and sites connected via a MPLS VPN. The SD-WAN service tunnel interconnects the bottom left site via an SD-WAN Edge CPE to an SD-WAN Edge VNF running in a public cloud environment to an SD-WAN Gateway. An SD-WAN Gateway enables sites interconnected via the MPLS VPN to communicate with sites interconnected via SD-WAN tunnels over the Internet.

This use case provides a simpler, less costly, faster way to interconnect existing MPLS VPN sites with new, typically off-net, sites using a local Internet connection when it may not be cost effective or take too long to build out the MPLS VPN to reach these new sites.

MEF Cloud Service Architecture

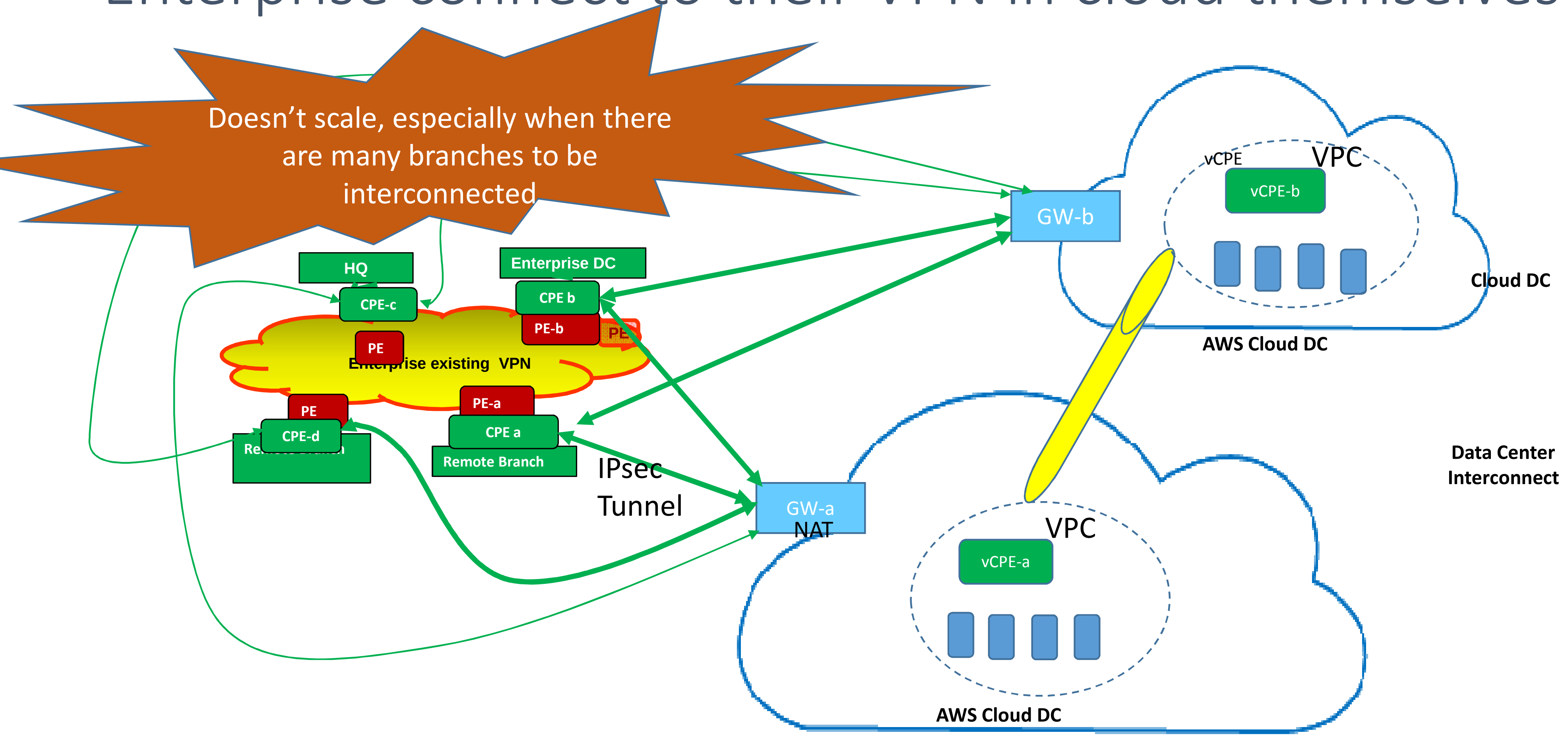


Key Takeaway relevant to IETF:

- basic assumptions (BGP/MPLS VPN design, possibly augmented with IPsec, SDN/NFV environments)
- Requirement of dynamics of “tunnel” (transport facility) establishment with relevant, customer-specific, QoS/Security/Routing policy enforcement schemes

What is Net2Cloud?
High Level Key Components
and potential new Protocol Works

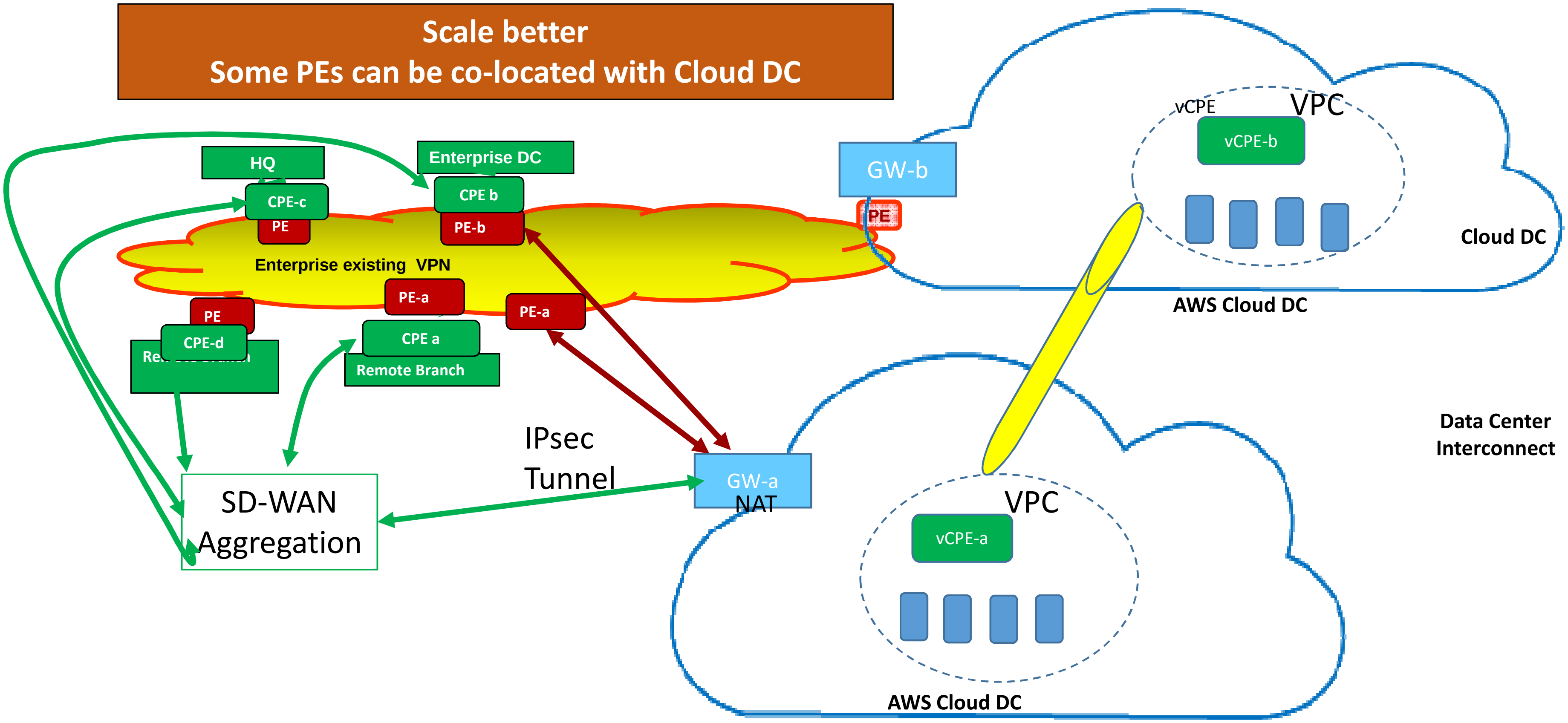
Enterprise connect to their VPN in cloud themselves

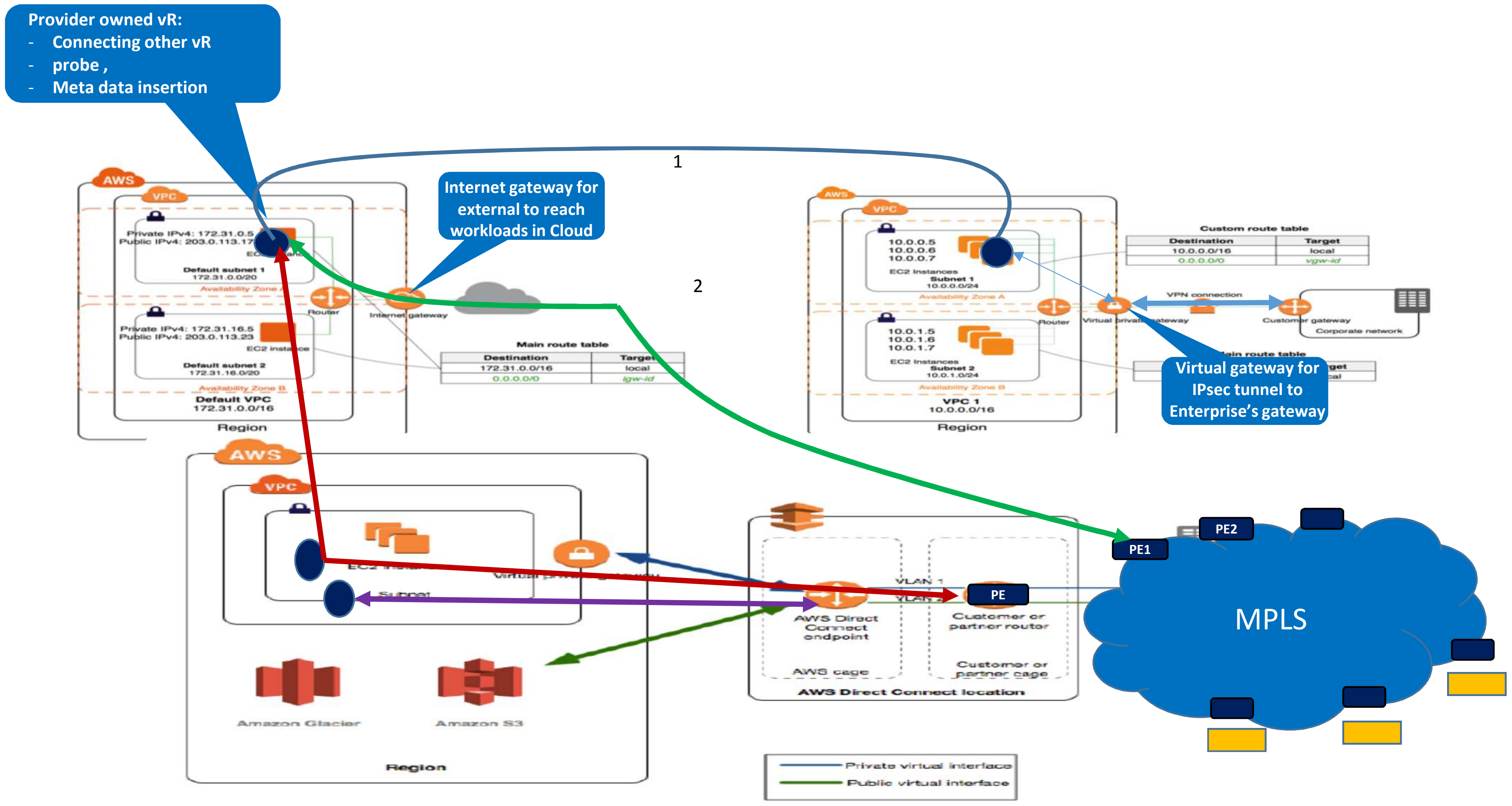


Doesn’t scale, especially when there are many branches to be interconnected

MPLS VPN Service Provider facilitated Interconnection

Scale better
Some PEs can be co-located with Cloud DC





Provider owned vR:
- Connecting other vR
- probe ,
- Meta data insertion

Internet gateway for external to reach workloads in Cloud

Virtual gateway for IPsec tunnel to Enterprise's gateway

SOME PROPRIETARY APPROACHES

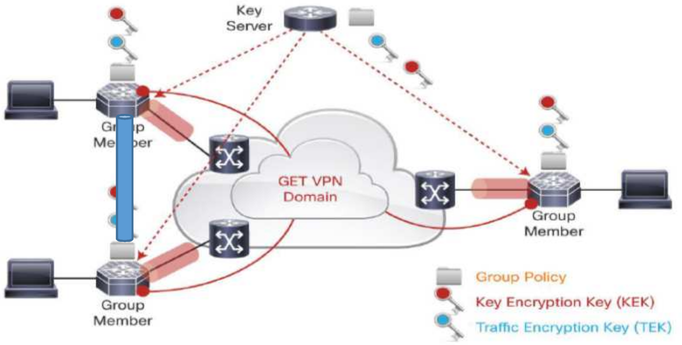
Using NHRP establish mGRE tunnels among spoke nodes

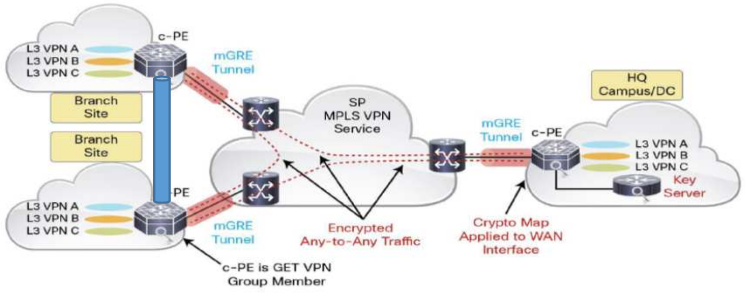
- ❑ **NHRP: was standardized by IETF ION(Interworking over NBMA networks) WG Original purpose: IP Address to ATM address resolution**

  [- Expired draft: https://datatracker.ietf.org/doc/draft-detienne-dmvpn/](https://datatracker.ietf.org/doc/draft-detienne-dmvpn/)

- ❑ **In SD-WAN Dynamic Spoke nodes interconnect: :**
  Purpose: VPN address to {Public Address & IPsec Key} resolution

- **CPE register its VPN address and its public IP address with NHRP server (a.k.a. controller)**
- **When CPE 1 needs to establish group secure tunnels with a set of CPEs (CPE2, CPE3, CPE4 …), CPE1 requests the Controller to get public IP addresses and IPsec Tunnel key for a group of tunnels CPE1<->CPE2, CPE1<->CPE3, CPE1<-CPE4, ..**



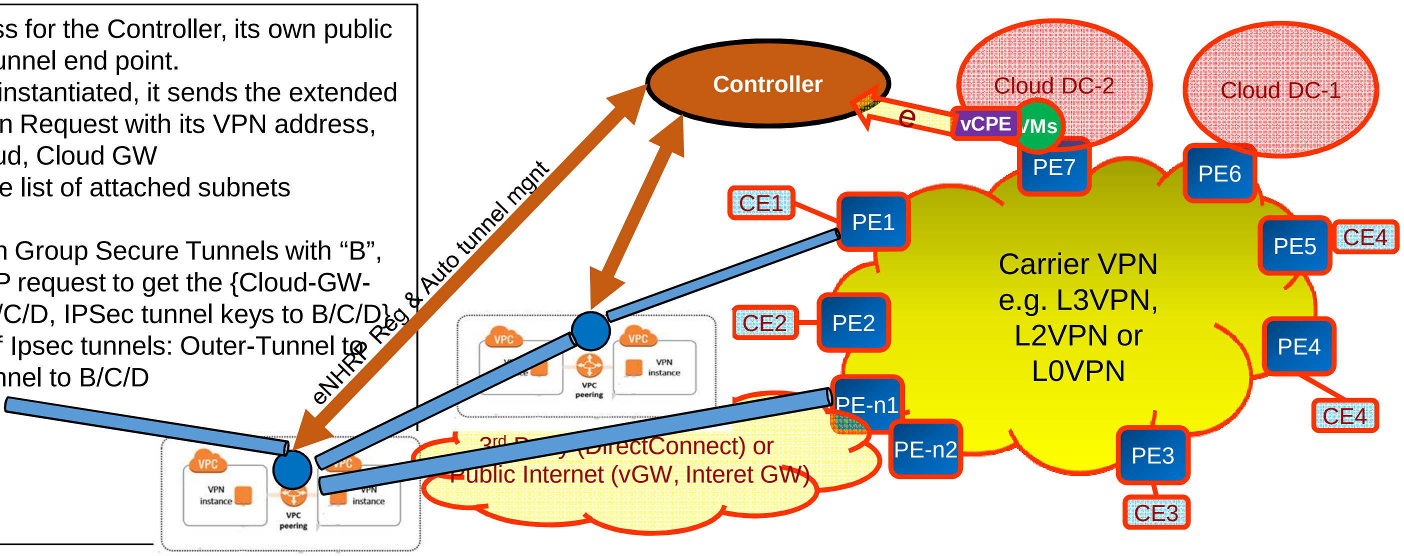


For Cloud DC Access & Interconnect (via Virtual routers)

Purpose: VPN address to {Cloud-Internal-private-address, Cloud-Gateway-address, IPsec-Keys} resolution

1. All CPEs has default address for the Controller, its own public IP addresses, and its own tunnel end point.
2. When a virtual router "A" is instantiated, it sends the extended NHRP (eNHRP) Registration Request with its VPN address, local private address in Cloud, Cloud GW
   - potentially register the list of attached subnets

3. When "A" needs to establish Group Secure Tunnels with "B", "C", "D", "A" sends a eNHRP request to get the {Cloud-GW-Addr, Private-Address for B/C/D}, IPSec tunnel keys to B/C/D}
There could be two layers of Ipsec tunnels: Outer-Tunnel to the CloudGW, and inside tunnel to B/C/D



IP: **S=Remote-a public IP** **Dst= Ctrl-public**	**Tunnel header: GRE or VxLan**	**NHRP Registration** **S=Remote-a tunnel Address** **Dst = Ctrl – tunnel address**	**Hold Time**	**List of Local Private addresses attached to Remote-a**

Attached in CIE (Client Information Entry)

App driven Floating PE selection and designated egress PE

Combine Carrier VPNs and SD-WAN to Support Dynamic Endpoints and to reduce latency & improve QoS over long Distances

- Multiple instances running in different Cloud DCs.
Need App driven Floating PE selection

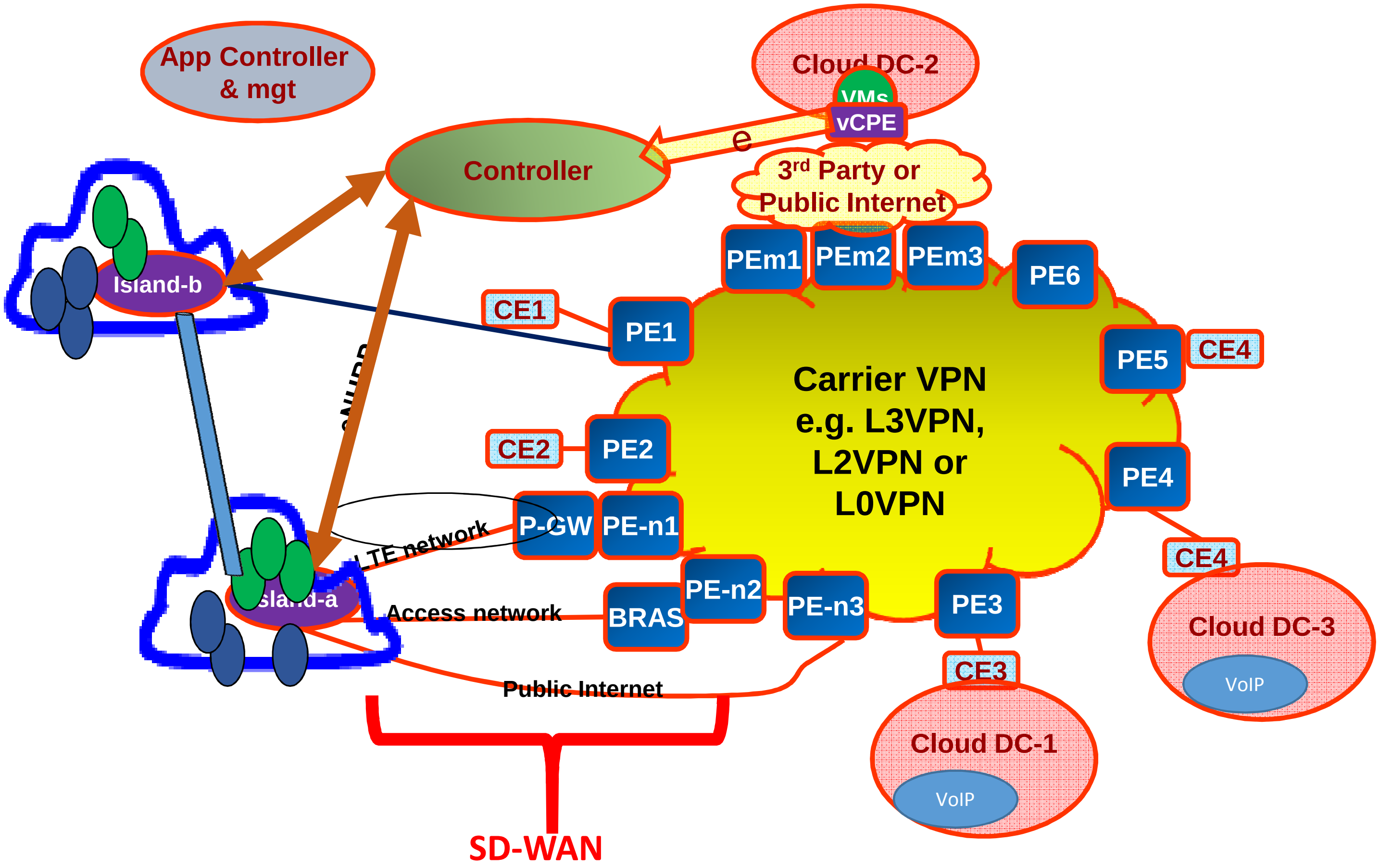
- NHRP might not work well,
  E.g. utilize gRPC to use the APIs exposed by AWS/Azure

- Data plane:
e.g. https://datatracker.ietf.org/doc/draft-detienne-dmvpn/

- What we to tell the network, & how to do it

- Running BGP on Island-a requires GRE tunnels being established first.

- RFC 7024 (Virtual Hub & Spoke) and Hierarchical VPN is not enough



WHY BRING TO IETF:

- Whether there is an interest of the IETF community to investigate:
  - Access-to-DC networking,
  - Routing among micro DCs via Overlay
    - draft-purkayastha-dcrouting-leading-indicators
  - Dynamic Tunnel (Ipsec Tunnel) management, cloud resource provisioning

To determine whether there is a need for enhancements to existing protocols or

Whether a new protocol is necessary