Dynamic Networks to Hybrid Cloud DCs: Problem Statement and Mitigation Practices

draft-ietf-net2cloud-problem-statement-27

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

Summary of INTDIR, RTGDIR, OPSDIR, SECDIR, TSVART, DNSDIR, and GENART review
IETF 117 San Francisco
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-04

- **5G Edge Cloud: Multiple Instances at different Edge Cloud DC**
  - 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-10
Connect the on-demand 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-10
  - Desirable to have tools to discover cloud services in the same way as in on-premises infrastructure
Network: Site <-> Cloud & Cloud <-> Cloud

- **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

✓ **draft-dmk-rtgwg-multi-segment-sdwan-01**
Summary from the INTDIR, RTGDIR, OPSDIR, SECDIR, TSVART, DNSDIR, and GENART review

- 14 revisions to address more than 300 comments & discussions on the rtgwg mailing list

- Many thanks to the reviewers for suggesting the technical issues, improvements, wording suggestions, Ines Robles, David Black, Lukasz Bromirski, Sue Hares, Robert Raszuk, Michael Richardson, Pete Spacek, Gyan Mishra, ChongFeng Xie, Jakob Heitz, Deb Cooley, Hesham ElBakoury, Paul Kyzivat, Florian Obser, Scott Hollenbeck, Uri Blumenthal, Tim Wicinski, Benson Muite, etc.

- Major technical updates to address the comments & suggestions

  ✓ TSV-ART:

  ✓ RTG area:
  - adding 3GPP 5G various deployment models impacts;
  - Including IXP in the connection to Cloud;

  ✓ SEC area:
  - Adding security implications for the notifications of inbound BGP routes exceeding the threshold or limit
  - Emphasizing that IPsec is just as secure as, or more than, the L2/L3 VPN, even though the pairwise key management is much more complicated.
Major technical updates – Cont’

✓ DNSSDIR & DNSSSD:
• Improving the description on the DNS Practices for Hybrid Workloads
• include "Split Horizon DNS" into the document
• Adding recommendation on naming convention DNS record for the hybrid clouds scenario

✓ OPS area:
• Added description on resilience and availability approach based on the 3 major Cloud operators, including the Site failure behavior and notification

✓ Many wording improvement suggestions.

THANK YOU!
Next Step

- Ready for Working Group Last Call