
cisco Live!
Let's go

The bridge to possible

SD-WAN Design Case Studies

Lessons Learned from Cisco's SD-WAN Design Council

Tom Kunath, Solutions Architect, @ccie1679

Agenda

- Introduction
  - What is design council
- Design Council case studies
  - Controller deployments
  - Underlay design
  - Horizontal scalability
  - Application SLA protection
  - SaaS Optimization

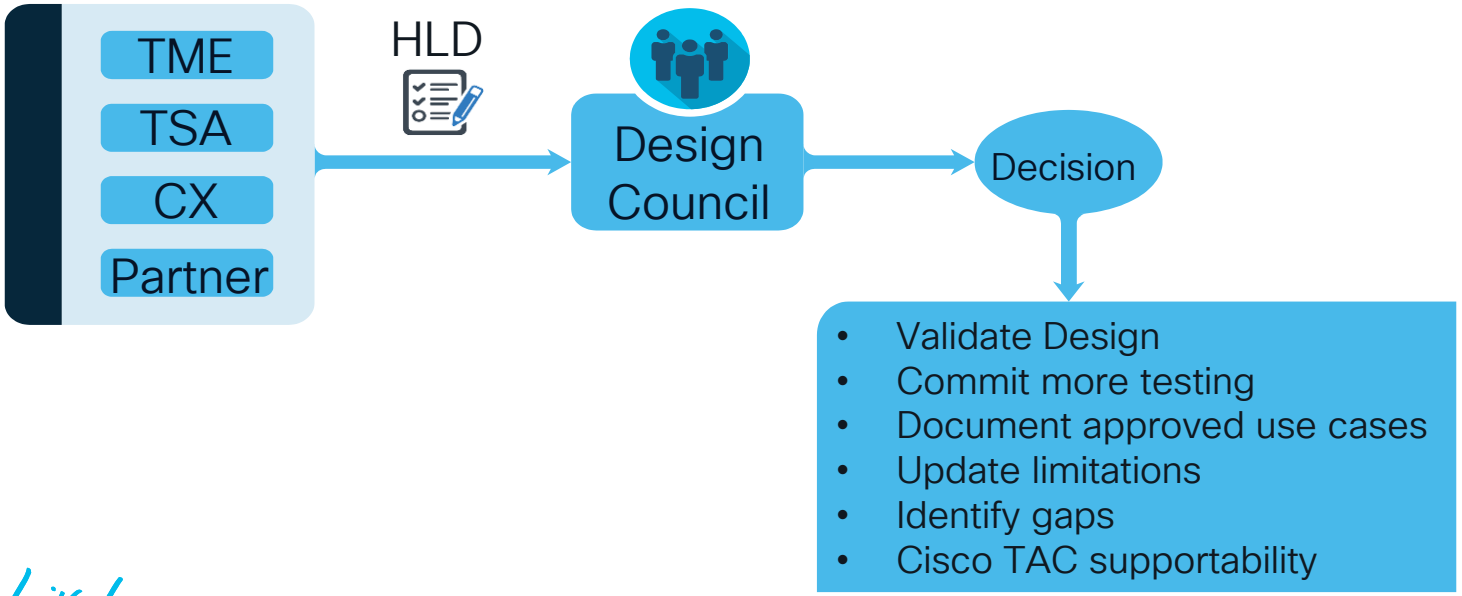
What I do @cisco

- Technical Marketing Engineer
- 19 years at Cisco, majority in Advanced Services
- 30+ years plan, design and implementation
- SD-WAN Mastery Collection video series creator
- Cisco Press author and technical editor
- Hybrid worker / Lab rat

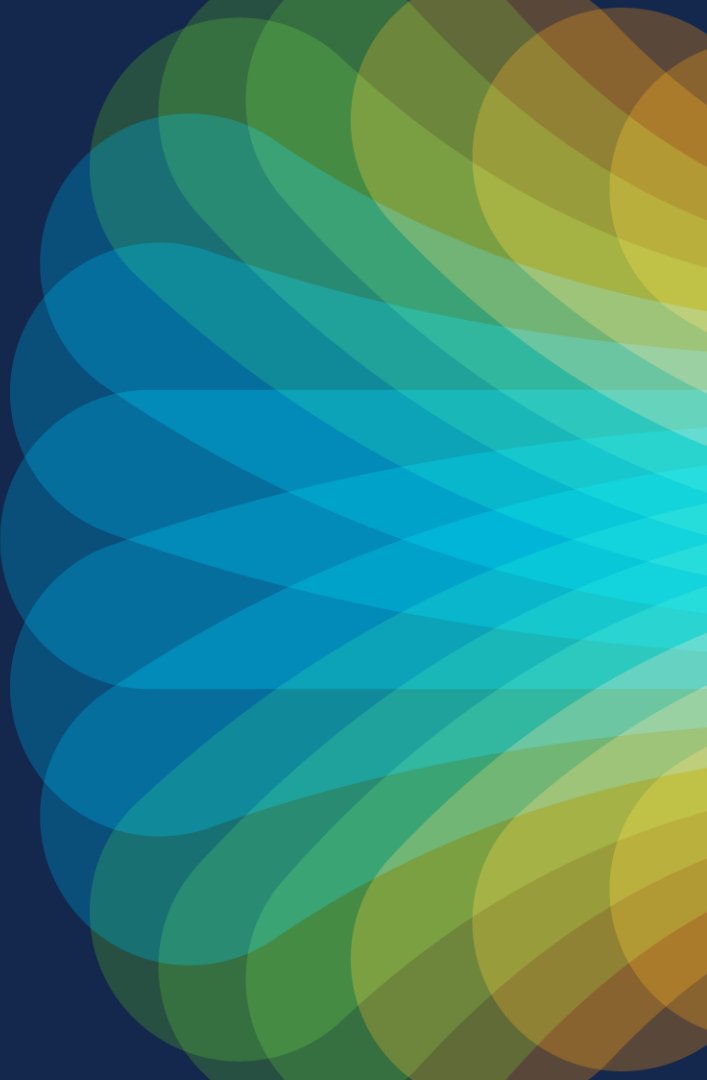
@ccie1679
tokunath@cisco.com
www.linkedin.com/in/tom-kunath1679

Cisco SD-WAN Design Council Introduction

- BU design council includes Cisco members of technical marketing, engineering, product management, and sales.
- Provides guidance for non-standard or undocumented SD-WAN designs



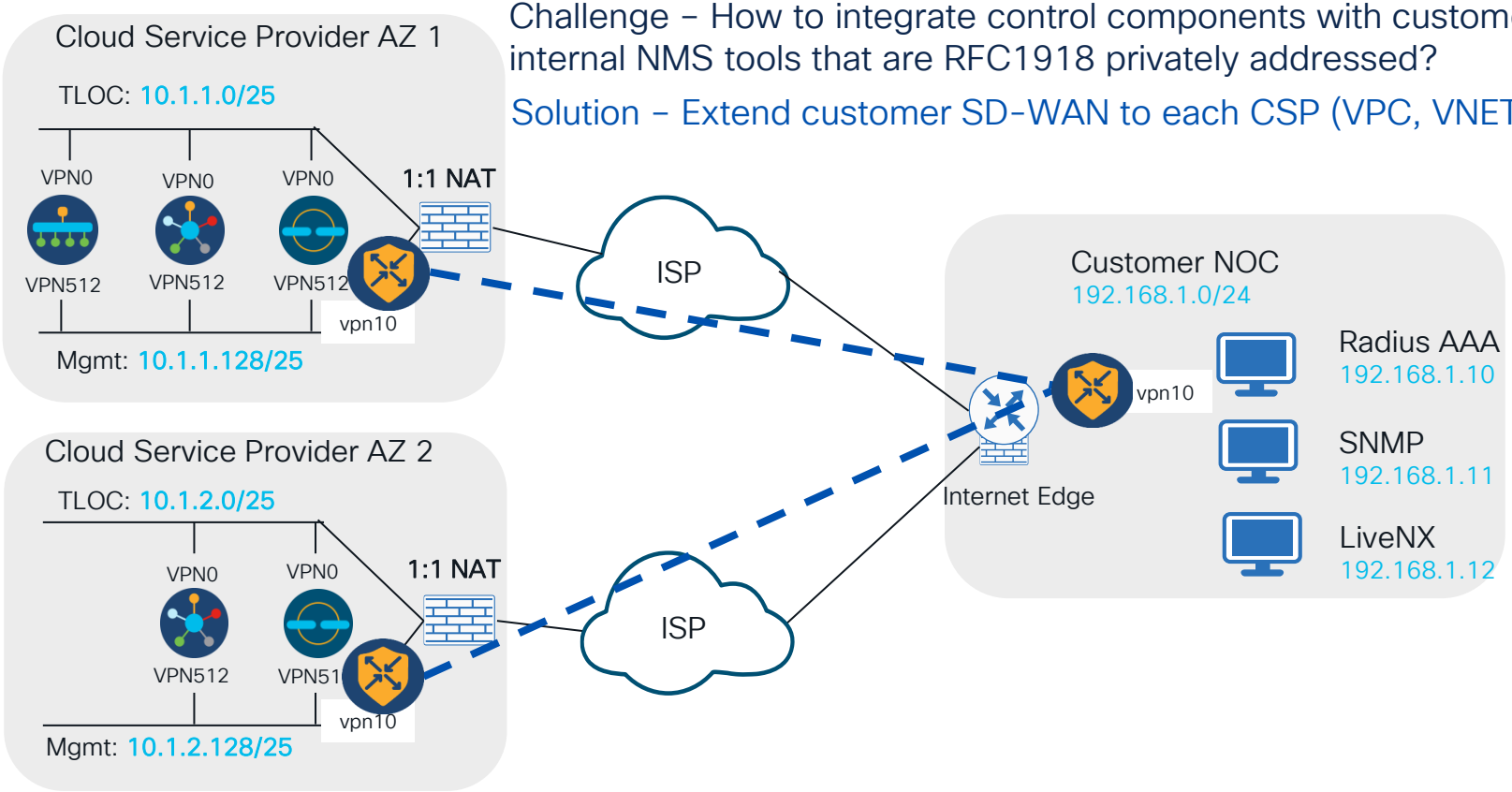
Controller Deployment



Use Case: NMS tools integration with Cloud-Hosted Control Components

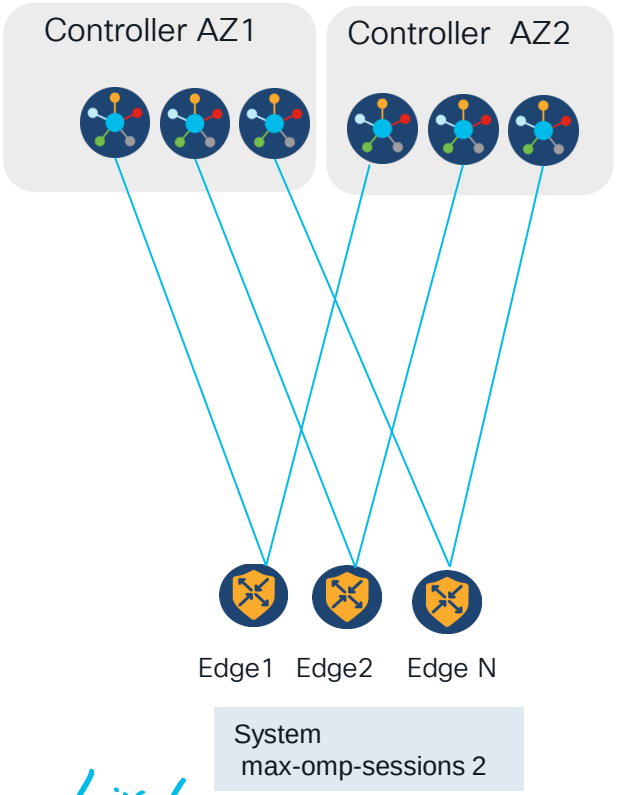
Challenge – How to integrate control components with customer internal NMS tools that are RFC1918 privately addressed?

Solution – Extend customer SD-WAN to each CSP (VPC, VNET)

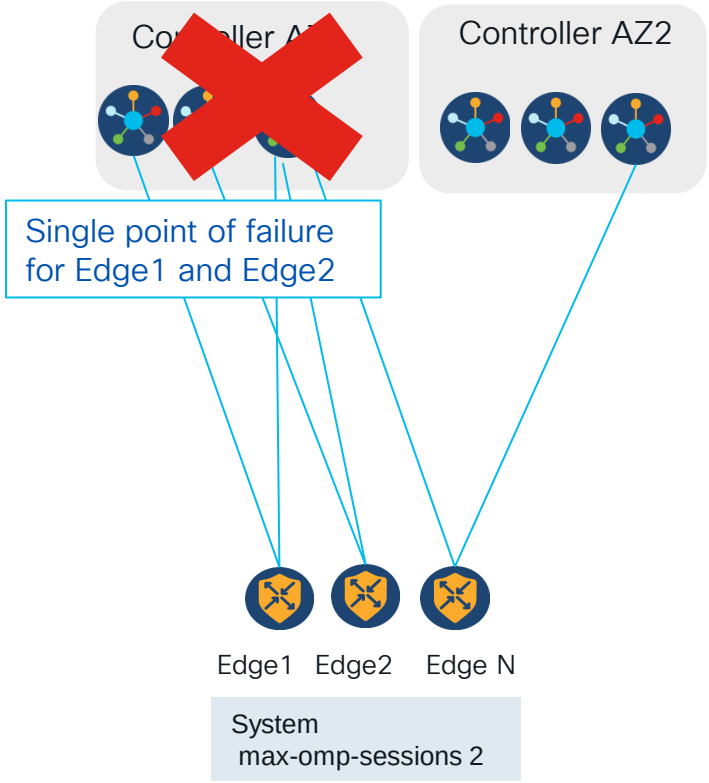


Use Case: Catalyst Controller High Availability
How to to protect against failure of a single CSP Availability Zone (AZ)

What you want

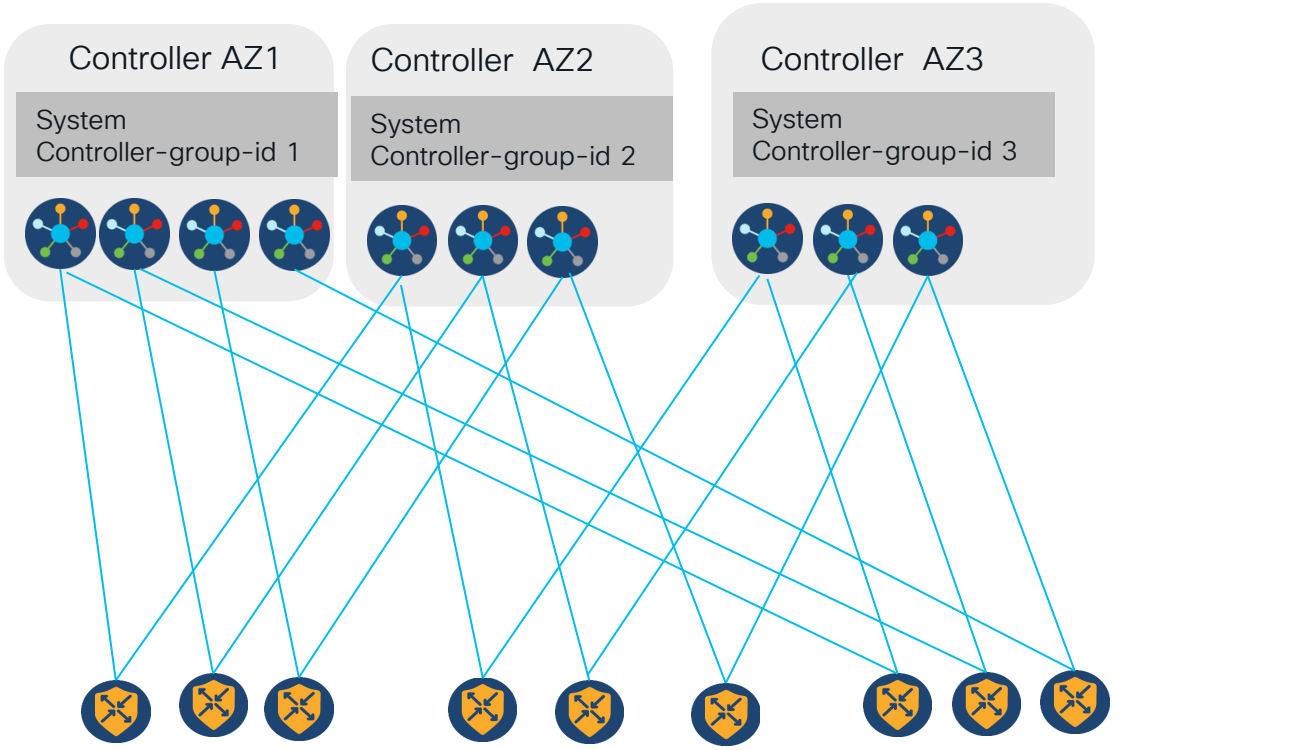


What you might get with default hashing method



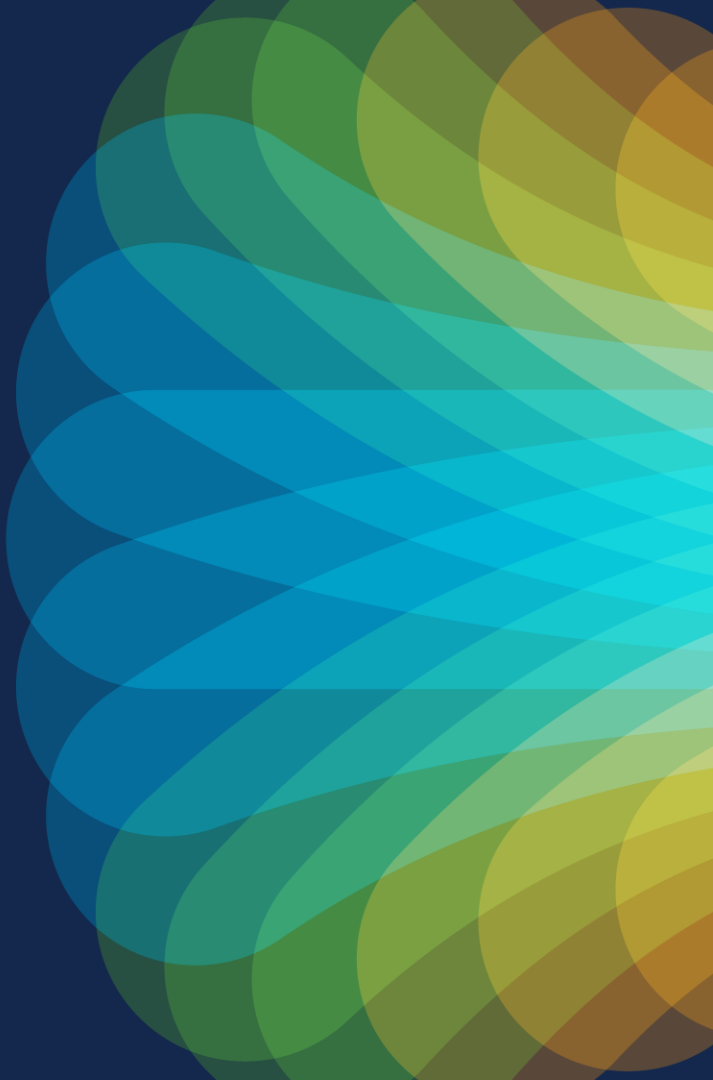
Solution: Deterministic TLS control connections
Controller Groups (CG)

Regionalize controllers with different controller group affinities

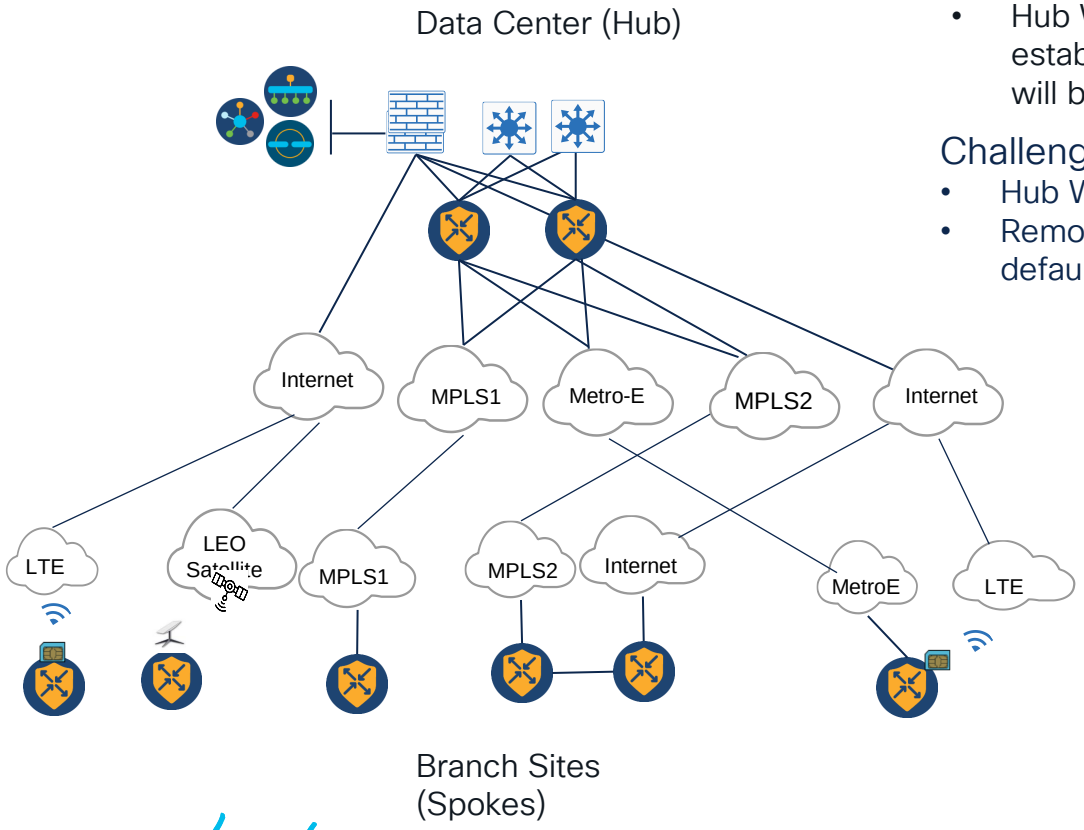


Regionalize WAN Edge with controller-group-lists

Underlay Routing



Use Case: Secure Hub Site Design

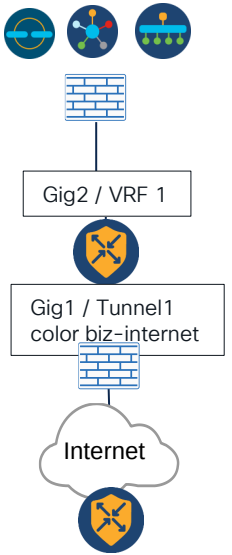


Hub Requirements:

- Controllers and WAN edge firewall-protected
- Hub WAN edge TLS connections to controllers established over TLOC (Prerequisite before IPSec tunnels will be formed)

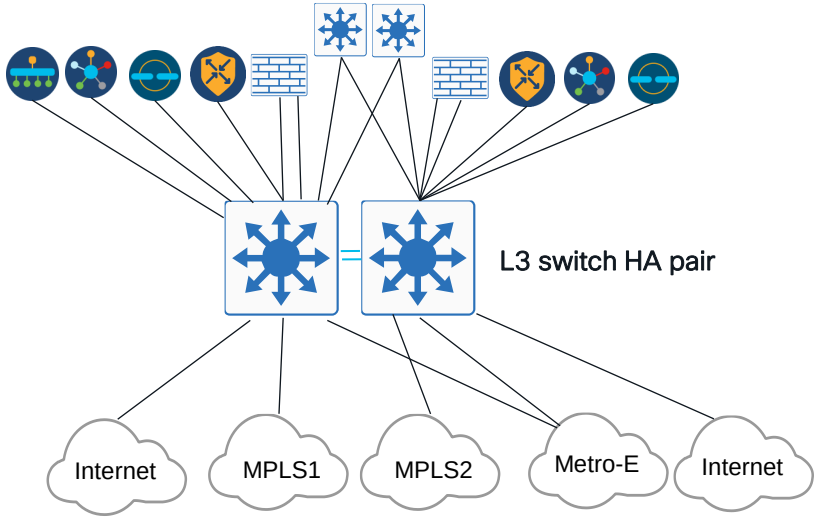
Challenges:

- Hub WAN Edge TLOC (Gig1) has no route to controllers
- Remote WAN edge cannot reach controllers via Hub (by default)

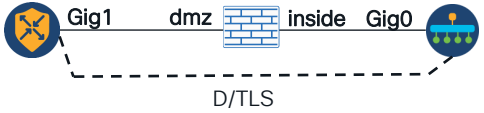


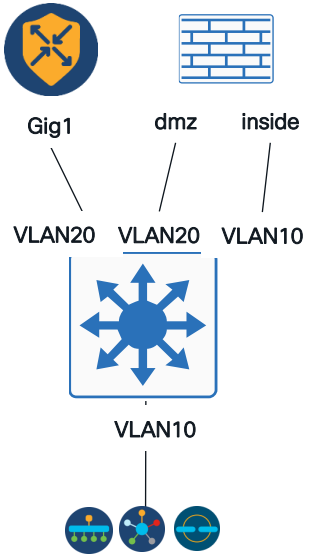
Solution: Collapsed backbone design at hub
Deploy switches for flexible underlay manipulation

Collapsed Backbone design at Hub Site
All devices and transports connect to L3 switch HA pair

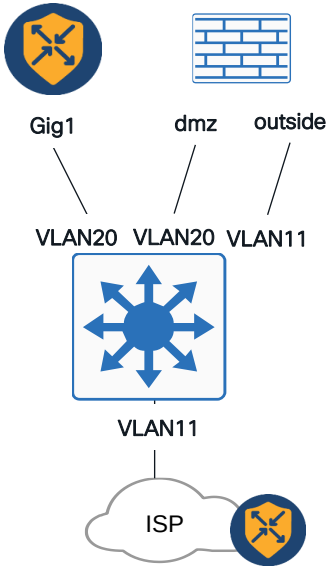


VLAN Service Chain 1 (TLS)
Hub edge – Firewall – Controllers

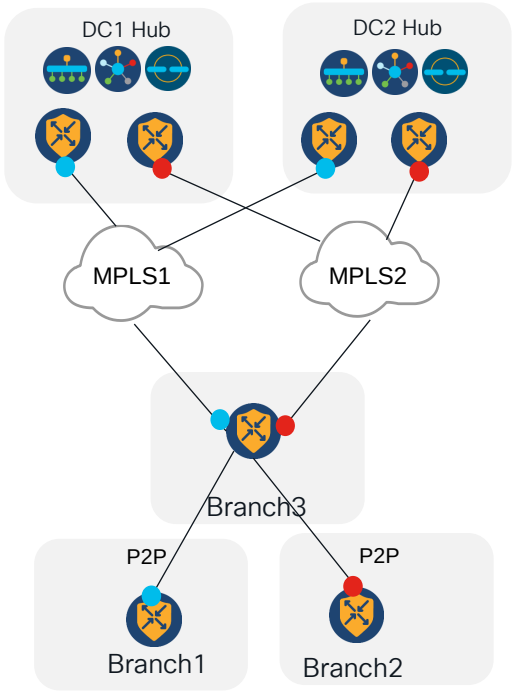




VLAN Service Chain 2 (IPSEC)
Hub edge – Firewall – Remote Edge

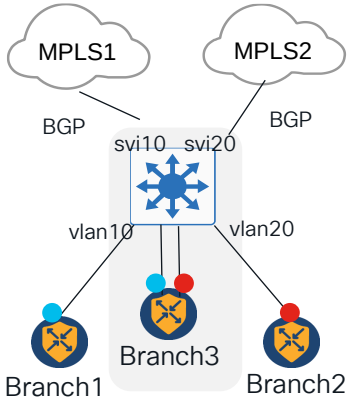


Use Case: Branch router as regional hub for remote branches

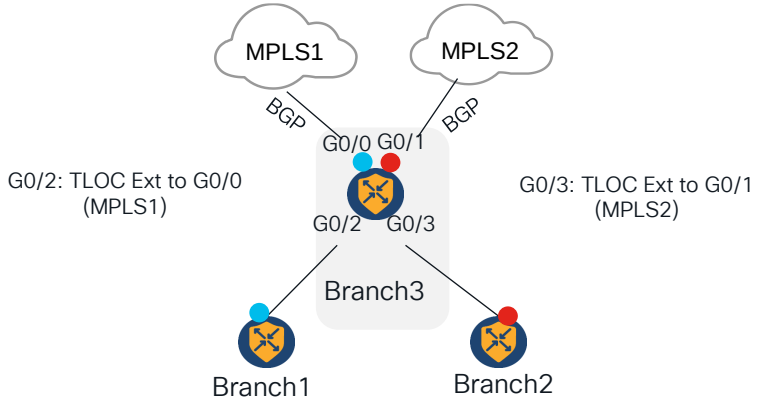


Remote sites with no MPLS availability

Preferred Solution: Add a switch at regional hub

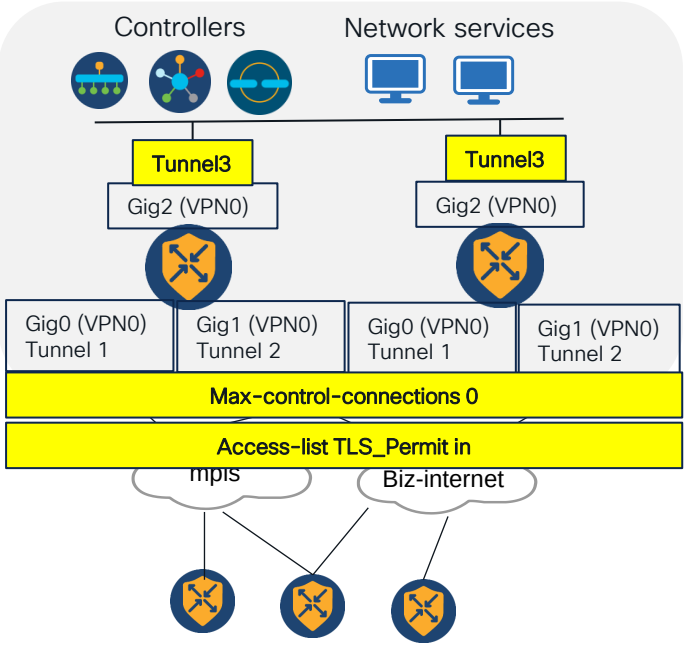


Solution without extra switch : TLOC Extensions at regional hub



Use Case: On-premise deployment in Colo facility
No additional switch available

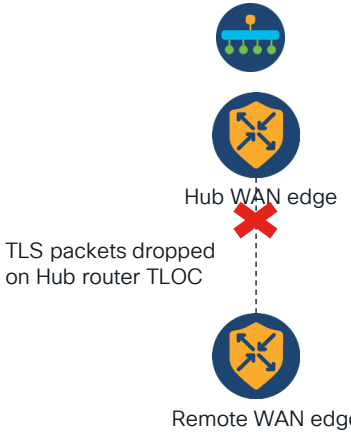
Proposed Design



Design Challenges

1. Hub WAN edge cannot reach controllers over Tunnels

2. Remote edge cannot reach controllers due to implicit ACL



Solution

1.1 Define Tunnel3 as additional TLOC on Hub to establish TLS control connections

1.2 Disable control connection attempts on Tunnel1/2 with “max-control-connections 0”

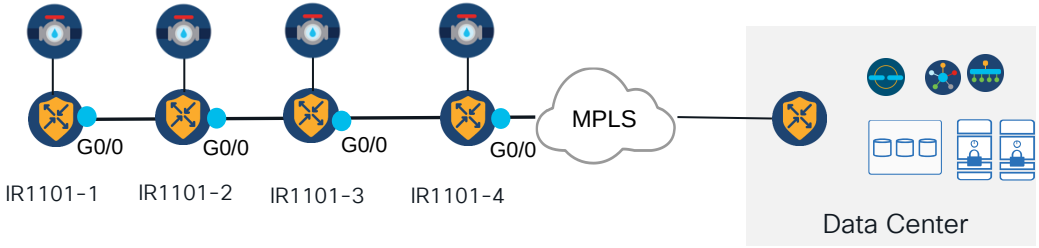
2. Define ‘explicit ACL’ with TLS source-ports allowed on Hub router

```
access-list TLS_Permit
 sequence 1
  match
  source-port 12346 12366 12386 12406
12426 12546
   protocol    17
  !
  action accept
  !
 default-action drop
!
sdwan
interface Gig0 / Gig1
tunnel-interface
Access-list TLS_Permit in
```

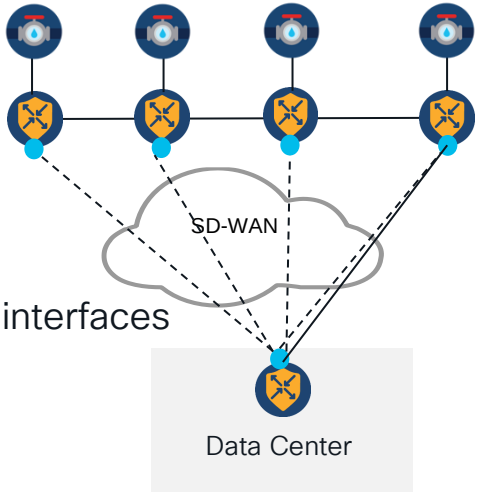
Use Case: Daisy chaining IoT SD-WAN routers

Remote locations with limited transport choices

Physical Topology



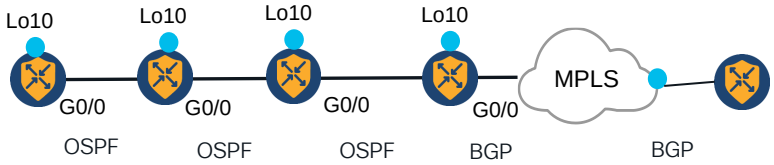
Required Hub-Spoke logical topology



Challenge: Transit routing prohibited by implicit ACL across (Gig0/0) TLOC interfaces

Solution

- Use Loopback interface as TLOC sources (unbound)
- Enable underlay routing protocol (OSPF and BGP)

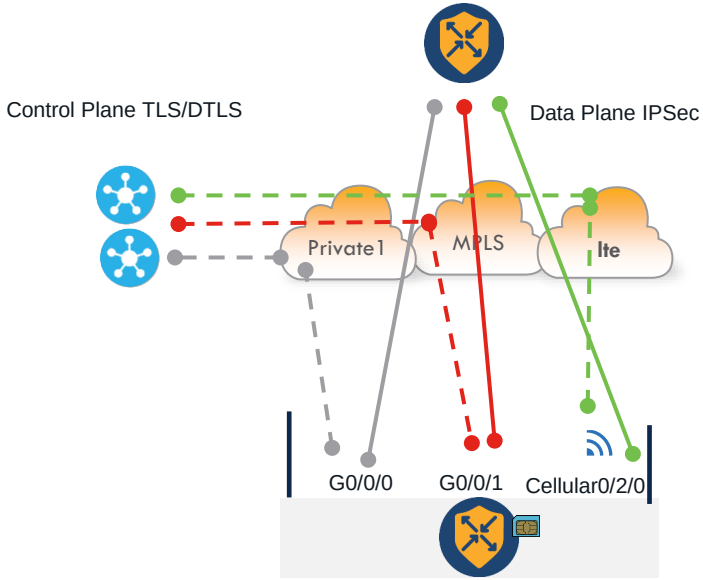


Use Case: Cellular WAN bandwidth optimization

Reducing SD-WAN overhead and maximizing throughput

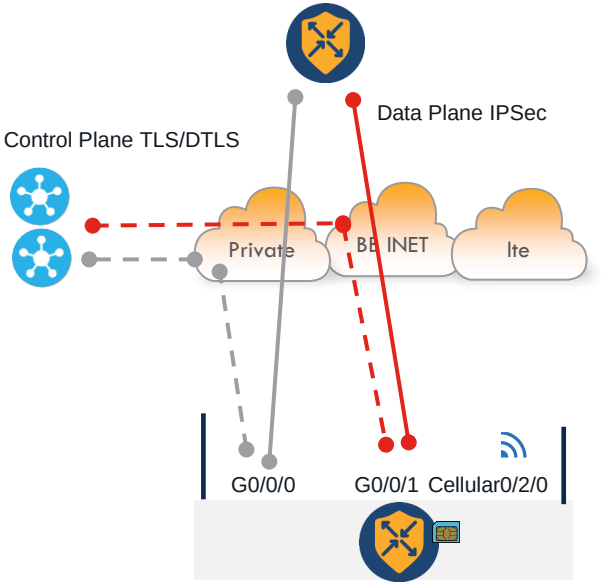
Cellular “always-on” (Default)

- Cellular-only deployments or when load-sharing with other transport (s)
- Recommend **reducing overhead on cellular interfaces** with ‘low-bandwidth-link’ and increasing OMP hello-intervals
- **Adaptive QoS traffic shaping** to increase/decrease shaping rate based on available bandwidth feedback from OMP



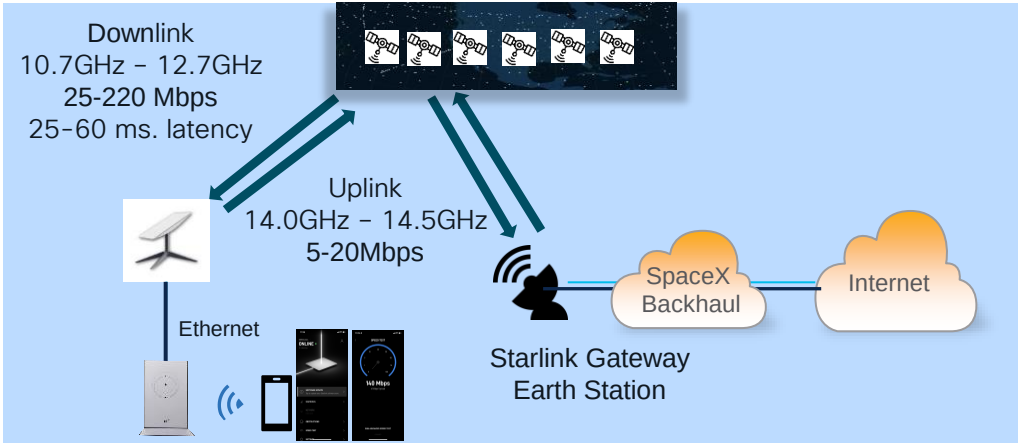
Cellular “last-resort-circuit”

- Cellular radio enabled but no tunnels established unless control and data plane tunnels go down on all other transports
- BFD/OMP tuning and Adaptive QoS recommended



Use Case: Starlink Satellite as SD-WAN Transport

- Starlink is a constellation of 5,500+ Low Earth Orbit (LEO) satellites offering internet access
- The business class CPE includes a dish, PoE injector, ethernet cable and wifi router that can be replaced
- Periodic traffic as dish roams to different satellite every ~2 min



Challenges

- Packet loss can impact real-time application quality
- If excessive, loss can trigger IPSec anti-replay errors
- Asymmetric Tx and Rx Bandwidth that may fluctuate
- Higher latency than terrestrial transport types

Solution

- Deploy AAR to avoid Starlink for realtime apps
- Increase IPSec anti-replay window size
- Enable adaptive QoS and low-bandwidth-link
- Enable App-QoE TCP Optimization

WAN Edge Horizontal Scalability

Use Case: High Scale Hub and Spoke Deployment
Hub WAN Edge Horizontal Scalability

Requirement 1: 18,000 tunnels at hub site

- Catalyst 8500 is highest performing SD-WAN platform supporting up to 8000 IPSec tunnels
- Customer has 9,000 sites with dual transports requiring 18,000 tunnels in each hub location
- **How to spread IPSec Tunnels horizontally across 3 different Hub routers in each DC?**

Requirement 2: 600Gbps aggregate bw at Hub

- Aggregate throughput required for all sites exceeds the current throughput capacity of a single Catalyst 8500
- **How to distribute traffic across 3 different hub routers in a horizontal fashion?**

Requirement 3: 600 VRFs at hub site

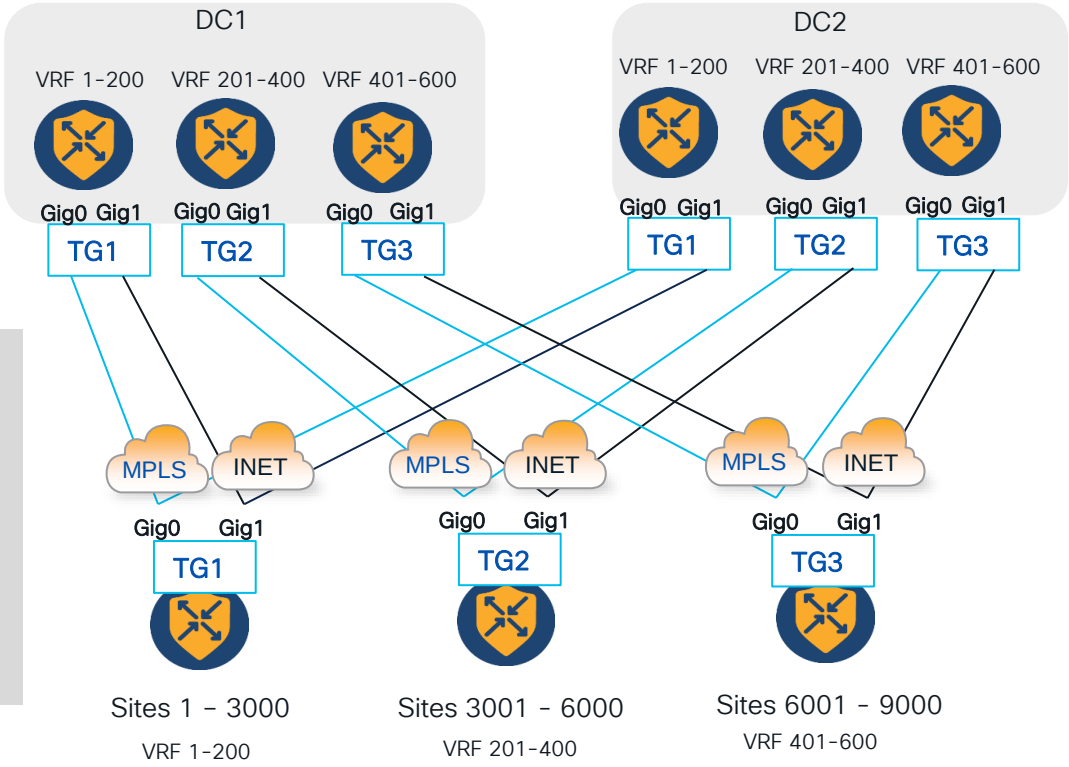
- Remote sites are different companies that require separation into different VRFs
- 600 VRFs are required to accommodate all partners – Catalyst 8500 supports 300 VRFs
- **How to distribute 600 VRFs across 3 Hub routers?**

Solution: Tunnel Groups for deterministic tunnel placement on hub

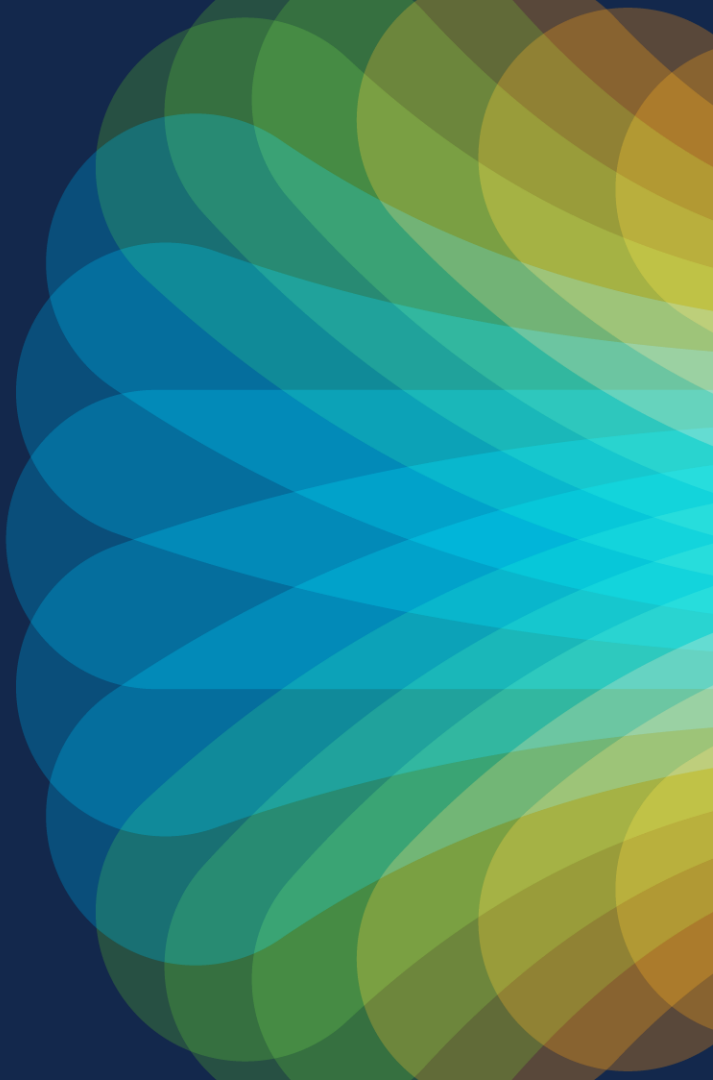
Result after Tunnel Group

- VRFs distributed across Hubs
- Tunnels and Traffic distributed across Hubs

```
sdwan
interface GigabitEthernet0
  tunnel-interface
   encapsulation ipsec
   color mpls
   Group 1
interface GigabitEthernet1
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   Group 1
```

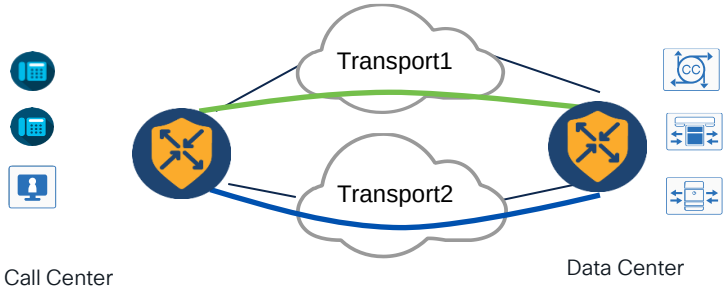


High Availability



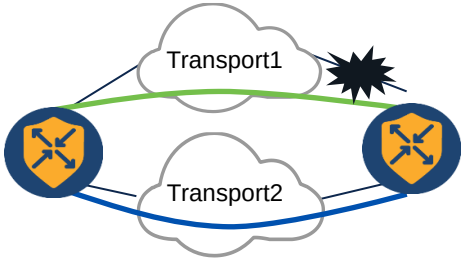
Use Case: Faster convergence for Branch Call Center traffic

How to improve SD-WAN resiliency to support 99.99% uptime SLA for VoIP?

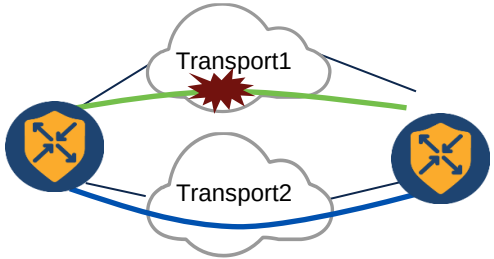


99.99% uptime SLA can only tolerate 52.6 minutes yearly downtime

Hard Failure may result in **7 seconds packet loss** (Assuming CVD-recommended BFD timers)



Soft Failure (brownout) may result in up to **12-minute packet loss** (Assuming CVD-recommended BFD/AAR Timers)



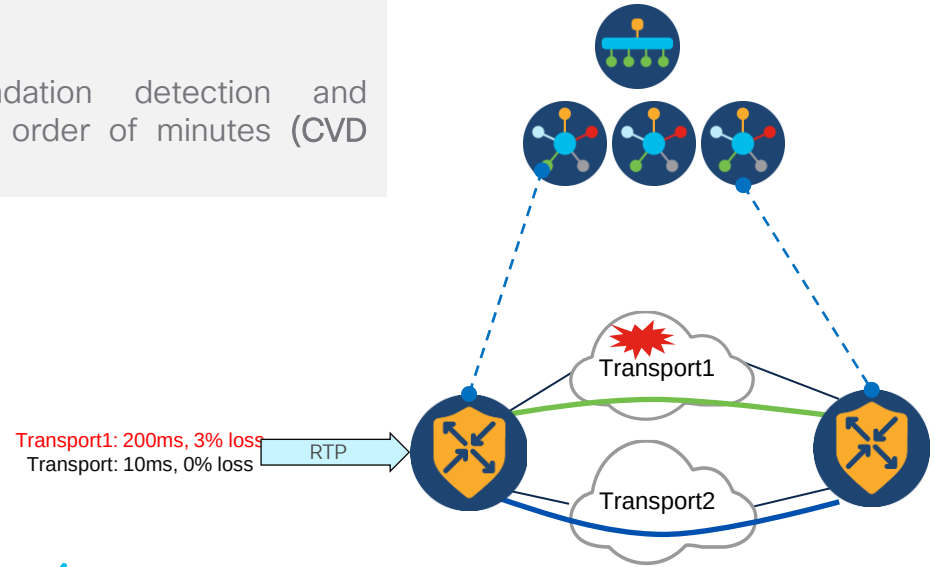
Solution 1: Enhanced AAR (EAAR) (20.12/17.12)

AAR (Original)

BFD probes used for tunnel performance metrics (loss/latency/jitter) measurements

Tunnel degradation detection and failover in the order of minutes (CVD values 12 min)

App Aware Routing Policy
SLA for RTP application requires path with latency <150ms and loss <2%



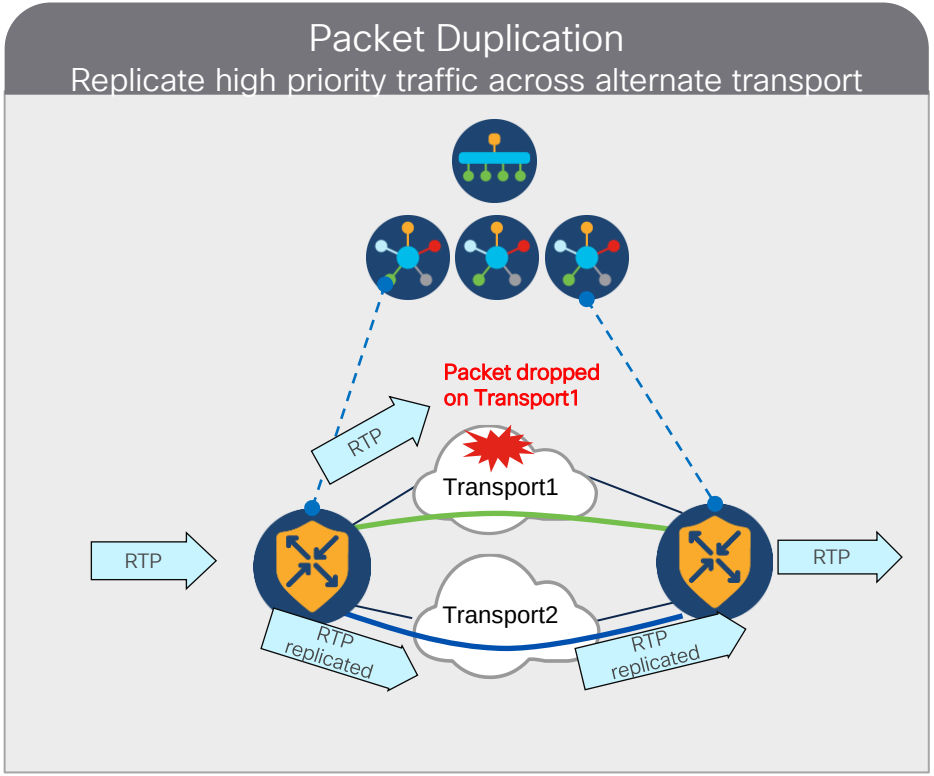
EAAR Improvements

Enhanced (passive) tunnel performance metrics measurements by using **inline data**

Faster tunnel degradation detection and switchover in the order of seconds (minimum 10 sec) to another path when SLA not met

SLA Dampening prevents churn

Solution 2: Packet Duplication (20.12/17.12)

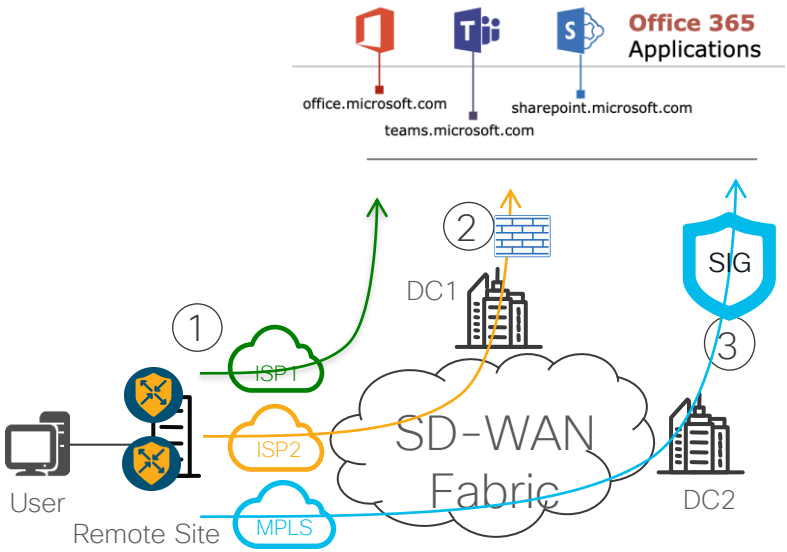


Packet Duplication Policy

```
viptela-policy:policy
 data-policy _Call_Centers
  vpn-list VPN1
    sequence 1
     match
      app-list APP-voip-RTP
      source-ip 0.0.0.0/0
     !
     action accept
      loss-protect pkt-dup
      loss-protection packet-duplication
```

Cloud SaaS Path Optimization

Fast Track SaaS Optimization
Unlocking SaaS App Visibility Through First Packet Match



Business intent
- MS Teams forwarded over DIA path via local NGFW
- Other SaaS: Prefer better performing path across SD-WAN overlay to DC1 or DC2

Proposed Solution
- Cloud OnRamp for SaaS with support for SIG (20.3.4)

Problem
- How to achieve first packet match of MS applications for immediate traffic-steering of MS Teams to DIA?

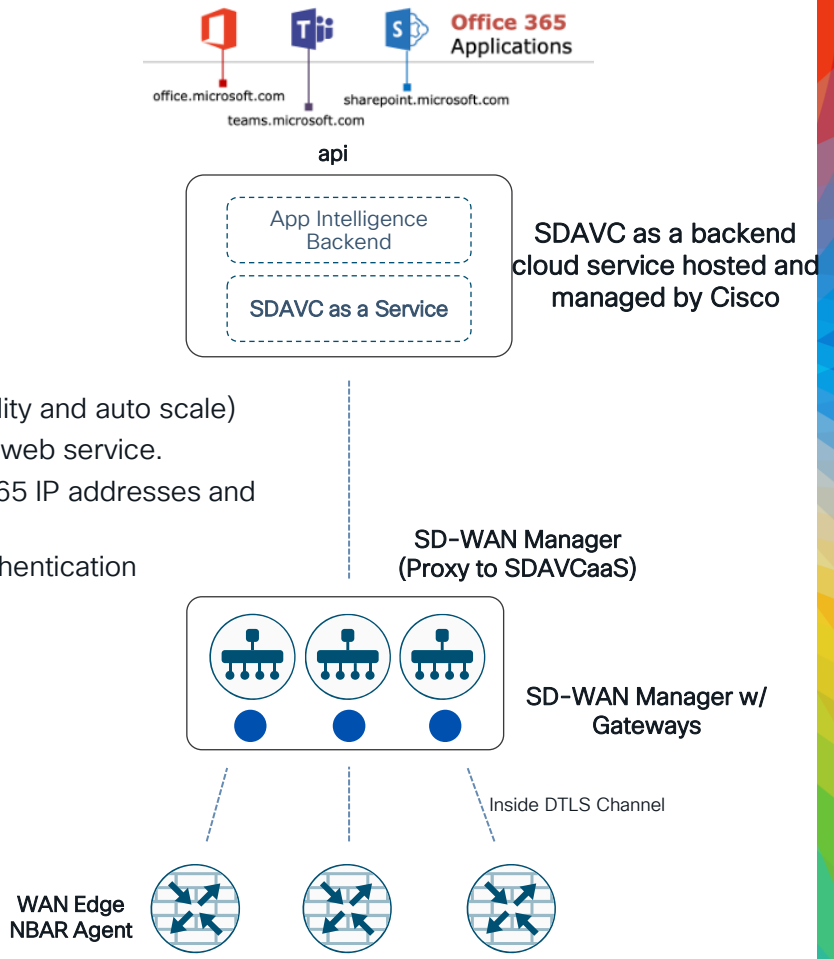
Solution
- CoRSaaS with service-area classification (20.8.1)
- SD-AVC as a service

SDAVC as a Service

Control Plane
SDAVC as a Service

- Separate/decoupled SDAVC backend cloud service (brings agility and auto scale)
- SDAVC Cloud Service pulls M365 URL Categories using M365 web service.
- Dynamically pre-populates Edge router's NBAR cache with M365 IP addresses and URL Categories.
- Easy deployment: enabled by default, with automatic Cloud authentication
- Dynamic Update of built in Protocol Pack

Data Plane
NBAR Agents



Summary

Cisco Catalyst SD-WAN Design Case Studies

Deep Dives into technical solutions on how Cisco customers have leveraged Cisco Catalyst SD-WAN to achieve business outcomes

SCAN ME

Small Branch Design Case Study Video Series

NEW

Only on Cisco U

SCAN ME

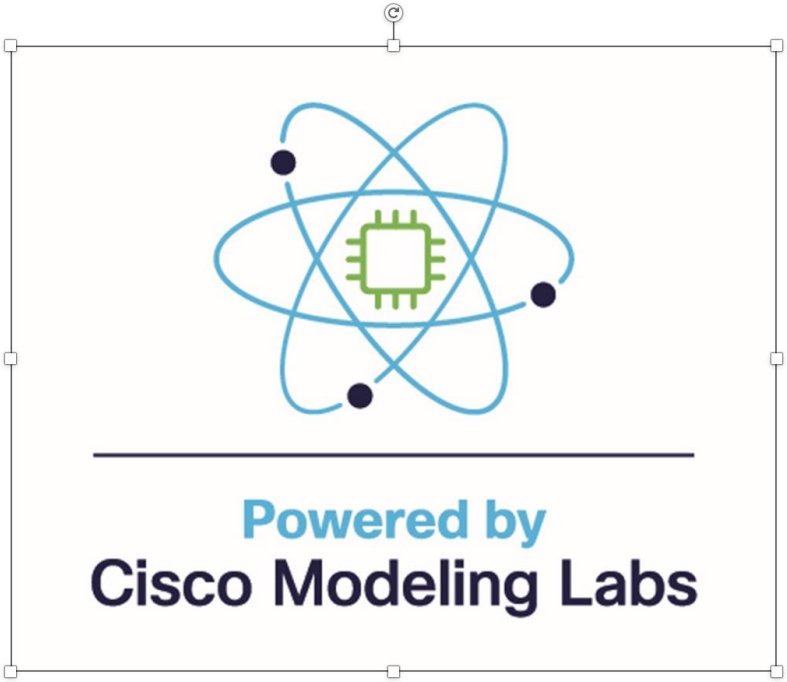
cisco Live!

Become a power user

Cisco Live Amsterdam Exclusive:
Save 25% on CML-Personal and CML-Personal Plus.

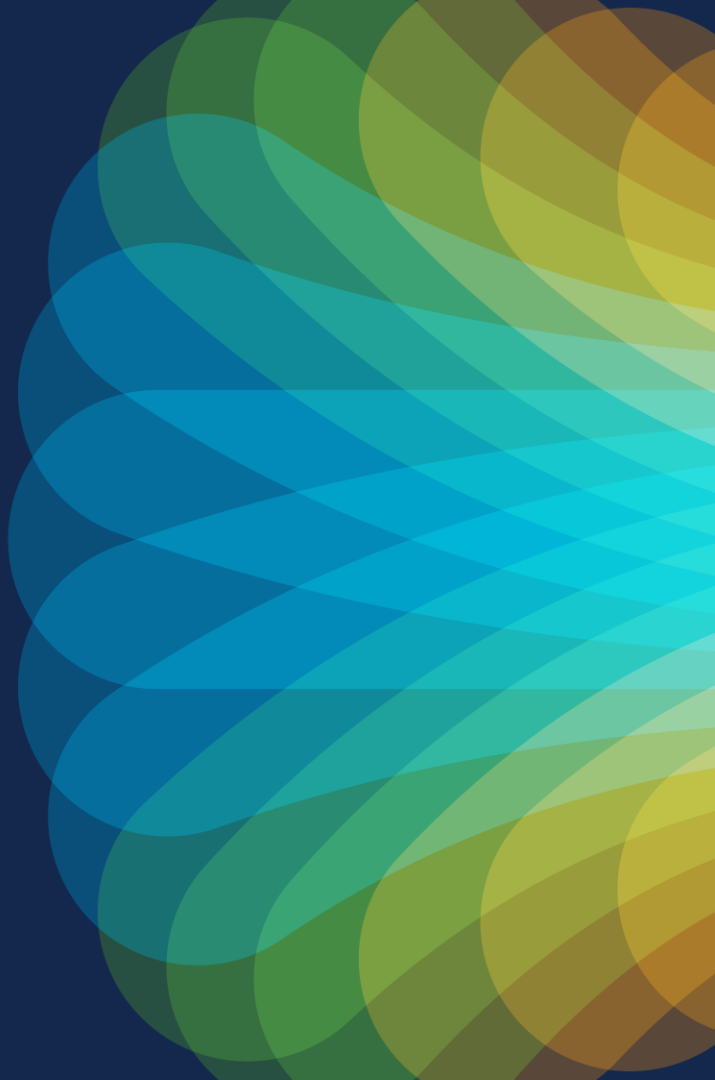
Visit the Learning & Certification booth to learn more.

cisco Live!



The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go