

# SD-WAN Design Case Studies

**cisco** Live !

Lessons Learned from Cisco's SD-WAN Design Council

Tom Kunath  
Solutions Architect, Technical Marketing Engineering

# Webex App

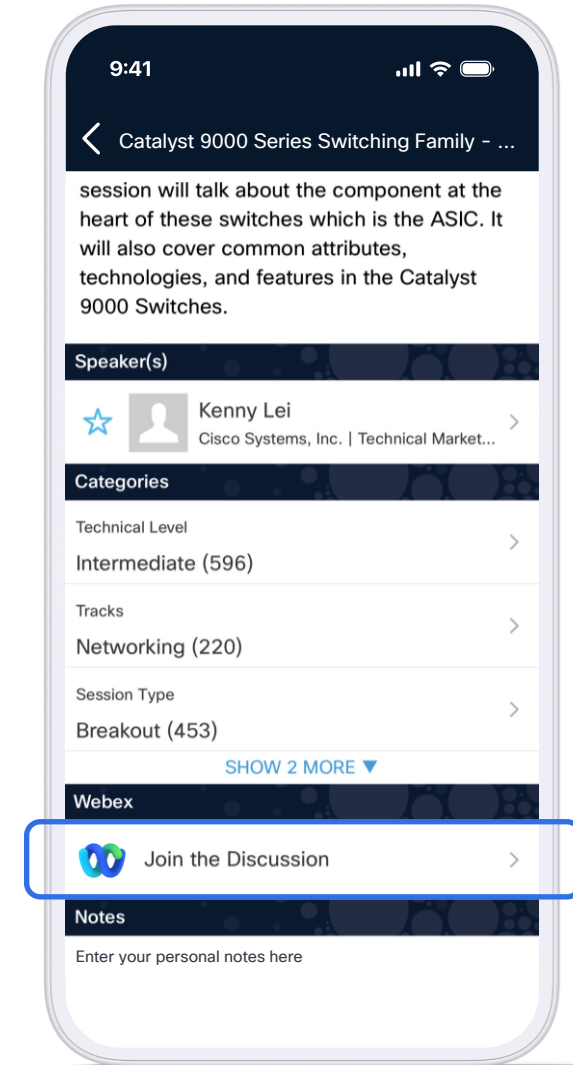
## Questions?

Use Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Events App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

**Webex spaces will be moderated by the speaker until February 27, 2026.**



# What I do @Cisco

- Solutions Architect, Technical Marketing
- 22 years at Cisco, 35 years industry (CCIE #1679)
- Enterprise and SP routing and security design focus
- Currently focused on Critical National Infrastructure Next-Gen Architectures



Cisco U Studio Producer



Remote Office

# What I do outside of work

- Enjoying quality time with my wife, our two children, and our energetic dog
- Inspired by travel and the excitement of outdoor adventures
- Enjoy cycling, surfing, and snowboarding whenever possible.

[tokunath@cisco.com](mailto:tokunath@cisco.com)  
[www.linkedin.com/in/tom-kunath1679](https://www.linkedin.com/in/tom-kunath1679)



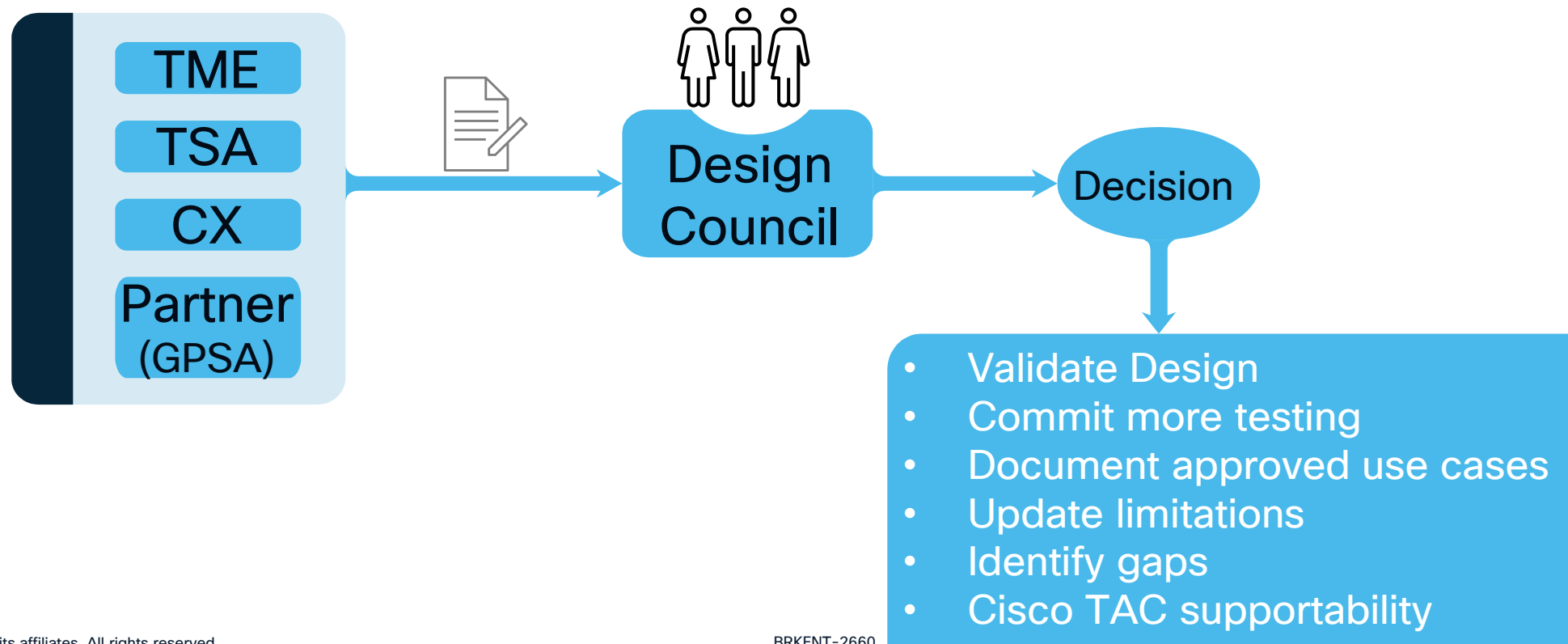
Cisco Live EMEA 2026 “pregame” in the Austrian Alps

# Agenda

- 01 Design Council Introduction**
- 02 Critical Site High Availability**
- 03 SD-WAN Underlay design**
- 04 Security/Segmentation**
- 05 Cellular and Satellite**
- 06 Cloud SaaS Optimizations**

# Cisco SD-WAN Design Council Introduction

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



# Critical Site High Availability

# Critical Site High Availability

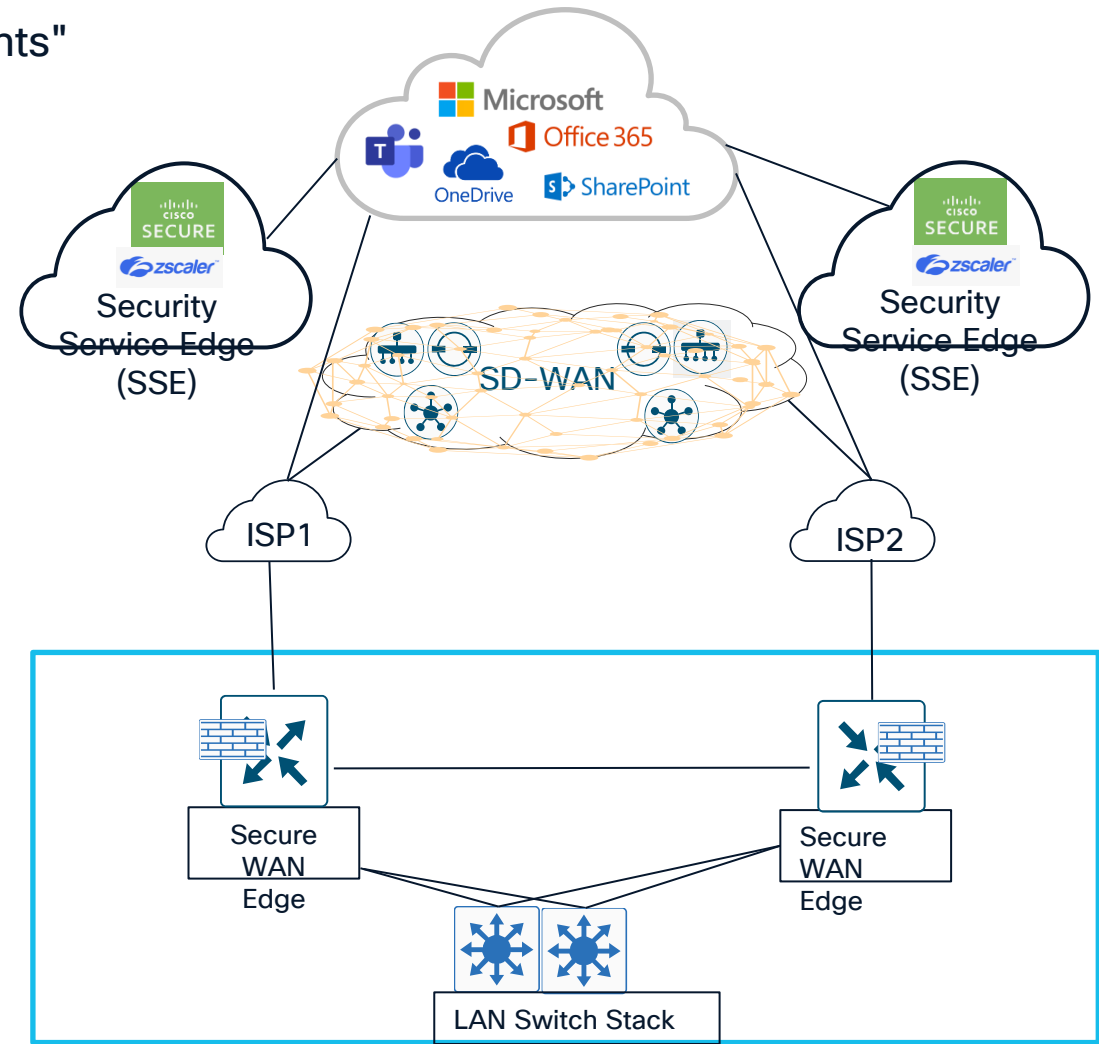
Mission-critical sectors such as defense, public safety, healthcare, energy and transportation require near-zero network downtime to ensure safety and operational continuity.

These standards are typically defined by "Service Level Agreements" (SLAs) measured in "nines."

| Availability Tier | Uptime percentage | Yearly downtime tolerance |
|-------------------|-------------------|---------------------------|
| "Four Nines"      | 99.99%            | 52.6 minutes              |
| "Five Nines"      | 99.999%           | 5.26 minutes              |

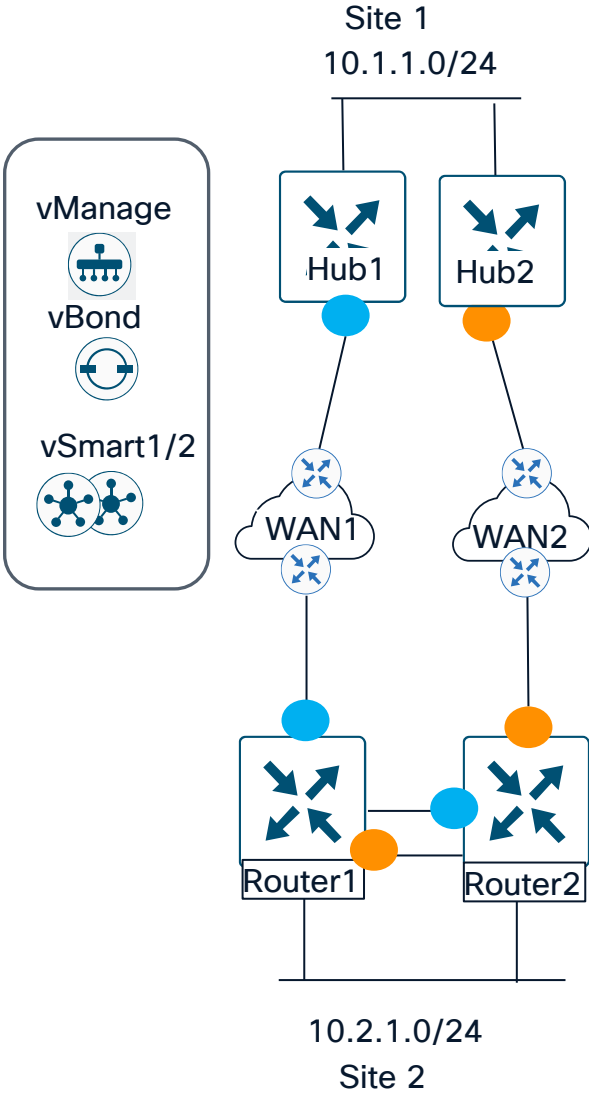
To eliminate single points of failure, N+1 redundancy is implemented across all primary network layers.

| Infrastructure Layer         | Redundant Components                                                                                                                   |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| SD-WAN Fabric                | Dual WAN Edge Routers, transport circuits and VPN (IPsec or GRE) tunnels.                                                              |
| Direct Internet Access (DIA) | Dual WAN edge routers/ISP circuits for Internet breakout, with redundant Next-Generation Firewalls (NGFW) for Internet edge protection |
| Cloud Security / SSE         | Dual WAN edge routers/ISP circuits diverse IPsec tunnels to diverse Secure Service Edge (SSE) points of presence.                      |



# SD-WAN Failure Scenarios

## Traffic loss during reconvergence

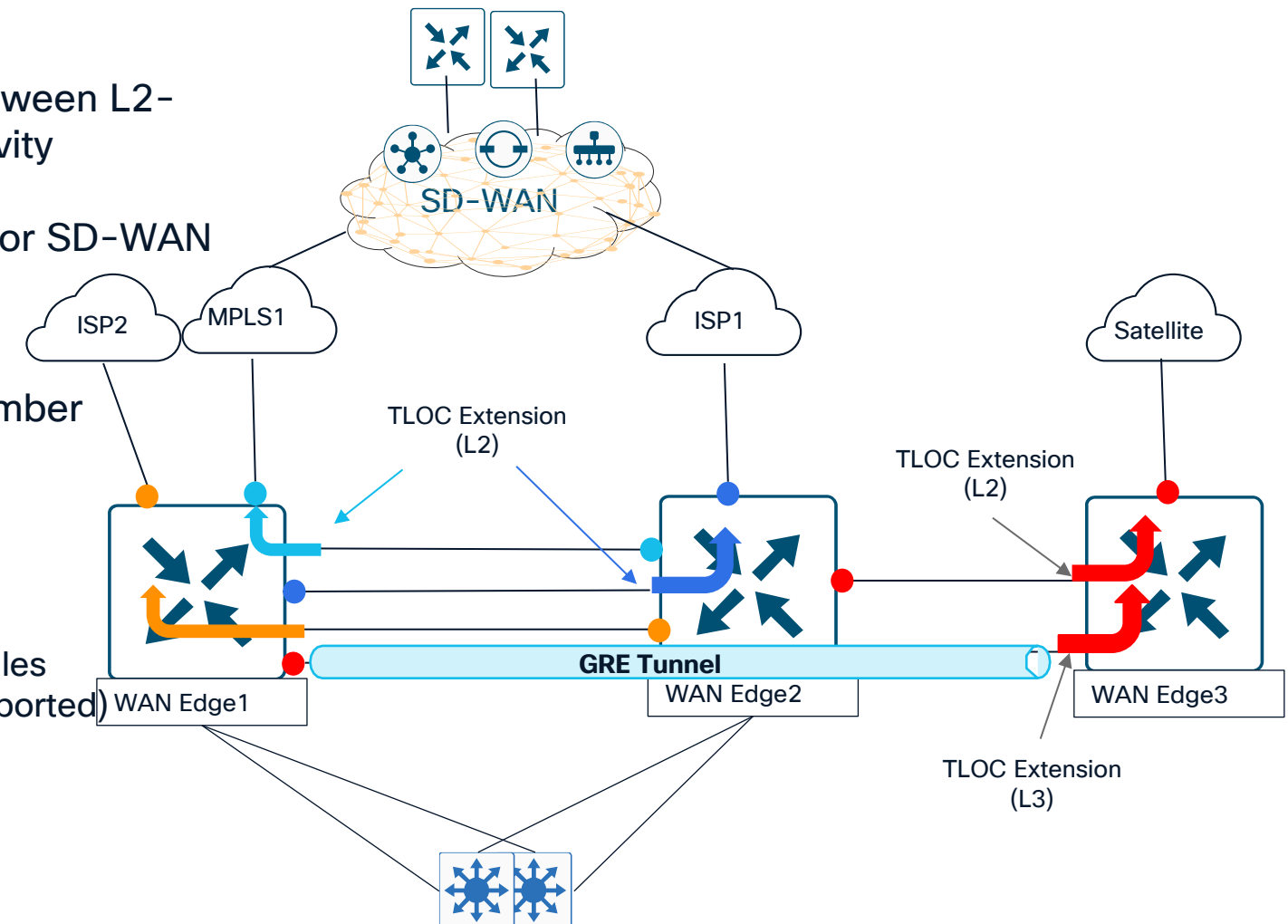


| Failure                                                         | Expected traffic loss                                                                                                                    | Description                                                                                                                                                                                  |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local WAN circuit down hard                                     | 1-2 sec                                                                                                                                  | Loss of light on TLOC interface brings interface/tunnel down which triggers local OMP reconvergence                                                                                          |
| Remote WAN circuit or router down hard                          | <= 7 sec (default timers)                                                                                                                | BFD timer expiration brings tunnel down and triggers local OMP reconvergence                                                                                                                 |
| Remote site LAN interface failure                               | <=10 seconds (assuming route scale within platform support)                                                                              | Remote router sends OMP update to vSmart which reflects to local router to trigger OMP reconvergence                                                                                         |
| WAN Soft failures (packet drops, latency)                       | <= 12 min for Application-Aware Routing (AAR) SLA violation detection and reroute<br><br>Enhanced AAR (EAAR) can reduce loss to 10-20sec | Traditional AAR dependent on BFD timers (hello timers and poll-interval)<br><br>EAAR inserts metadata in packet headers for performance measurement, greatly reducing failure detection time |
| vSmart failure (all instances)<br><br>Up to 12 vSmart supported | No loss until graceful restart or IPsec rekey expiration                                                                                 | 12-hour GR / 24-hour IPsec Rekey – can be extended to 7, 14 days.<br><br>Router reboot during outage will not be onboarded until vBond restored                                              |
| vBond failure (all instances)<br><br>Up to 12 vBond supported   | No loss                                                                                                                                  | Router reboot during outage will not be onboarded until vBond restored                                                                                                                       |
| vManage failure                                                 | No loss                                                                                                                                  |                                                                                                                                                                                              |

# SD-WAN Access Redundancy

## TLOC Extensions

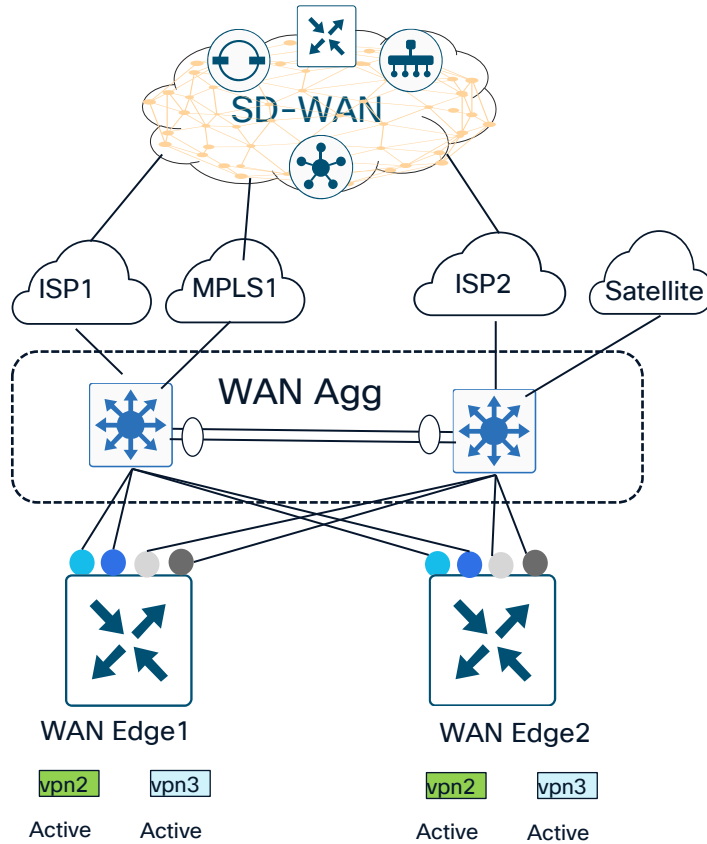
- TLOC Extensions provide adjacent/redundant WAN edge access to locally-connected WAN transport
- Dedicated Ethernet cables or switch VLAN between L2-adjacent WAN edge routers provide connectivity
- TLOC extension function as "cross-connect" for SD-WAN tunneled-traffic (TLS/dTLS, IPsec/GRE)
- Can become operationally complex as the number of transports and WAN edge routers increase



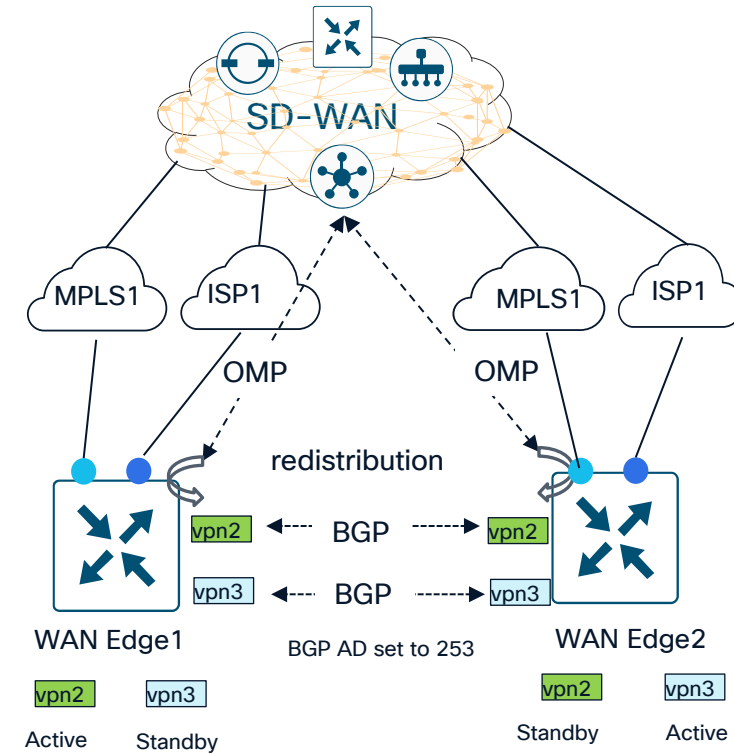
# SD-WAN High Availability

Alternate Designs to TLOC Extensions

## WAN aggregation layer



## Active/Standby WAN Edge



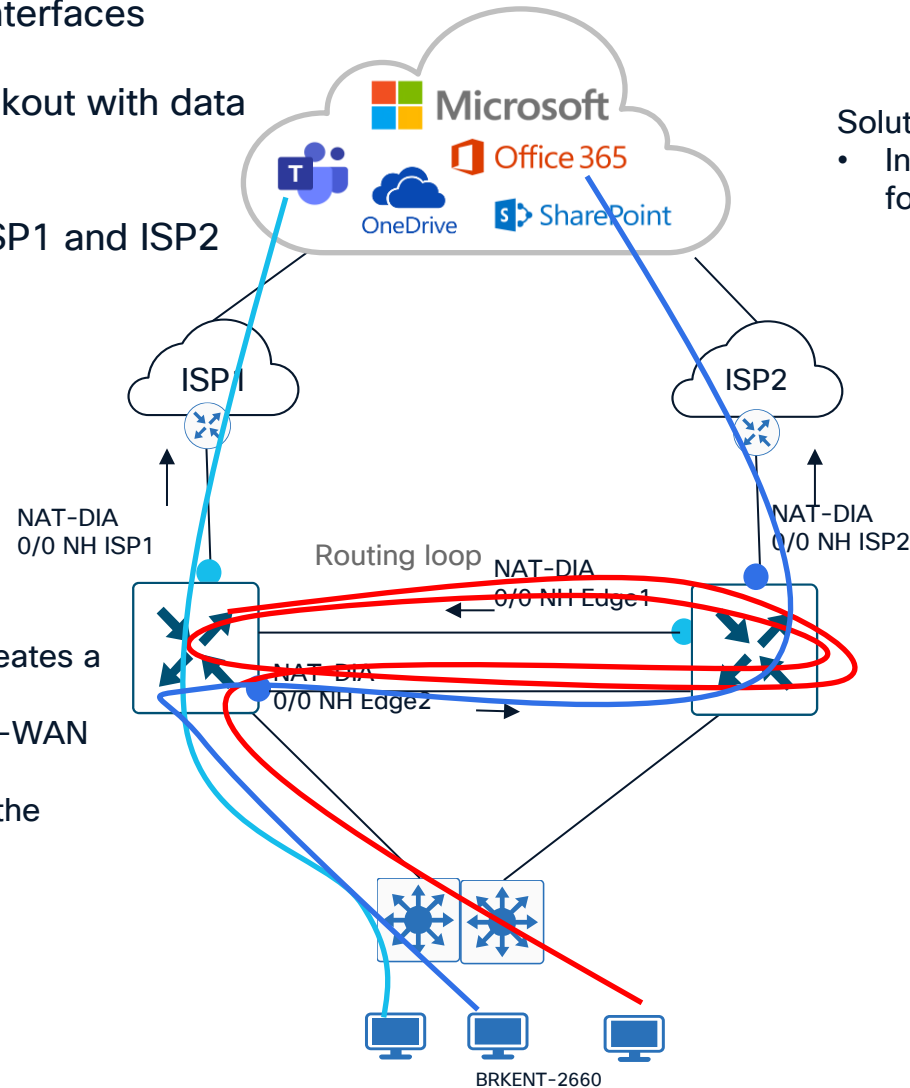
# Direct Internet Access (DIA) HA

## Dual DIA (Local ISP + TLOC Ext link)

- Each WAN edge has two NAT-DIA interfaces
- Internet traffic redirected to DIA breakout with data policy or default routing
- Internet traffic load-sharing across ISP1 and ISP2

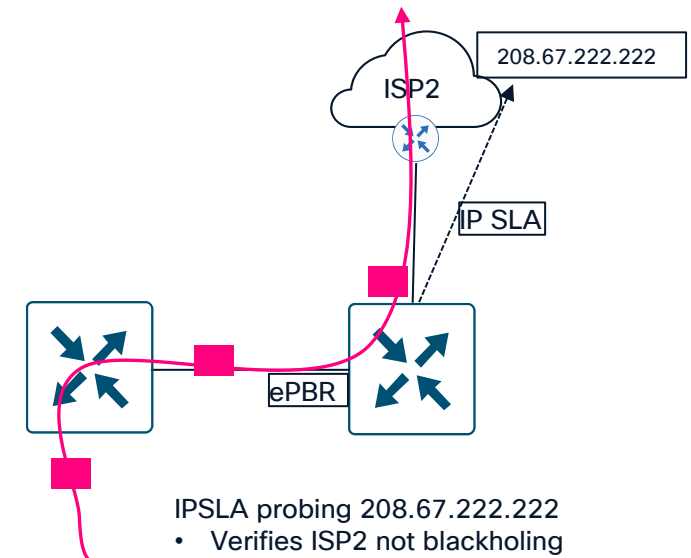
Problem: Opposing default routes in VPN0 creates a potential routing loop over cross-link

- TLOC extensions apply specifically to SD-WAN tunneled traffic.
- Unencapsulated IPv4/IPv6 traffic follows the standard VPN0 routing rules.



Solution : Enhanced Policy Based Routing (ePBR)

- Internet-bound traffic received on TLOC extension interface forwarded to ISP gateway NH



IPSLA probing 208.67.222.222

- Verifies ISP2 not blackholing

ePBR route map applied inbound on VPN0 TLOC extension interface

- Tracks IPSLA state
- Sets NH to ISP2 gateway IP if IPSLA state is UP

# Direct Internet Access (DIA) Faster Failover

## DIA NAT Tracker limitations and workaround

- Requirement: Reduce DIA convergence time to 10 sec for critical SaaS application
- Current Solution: DIA NAT Tracker
- Current limitation: 20 seconds minimum.

### System

tracker diatracker-cisco

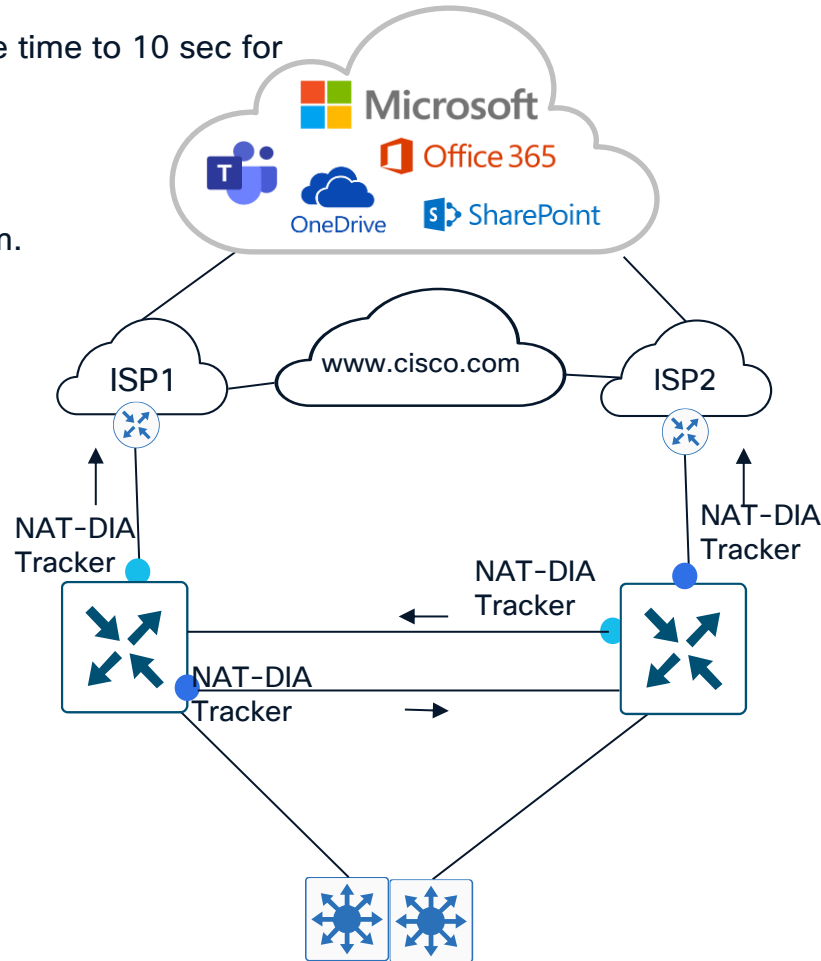
tracker-type interface

endpoint-dns-name www.cisco.com

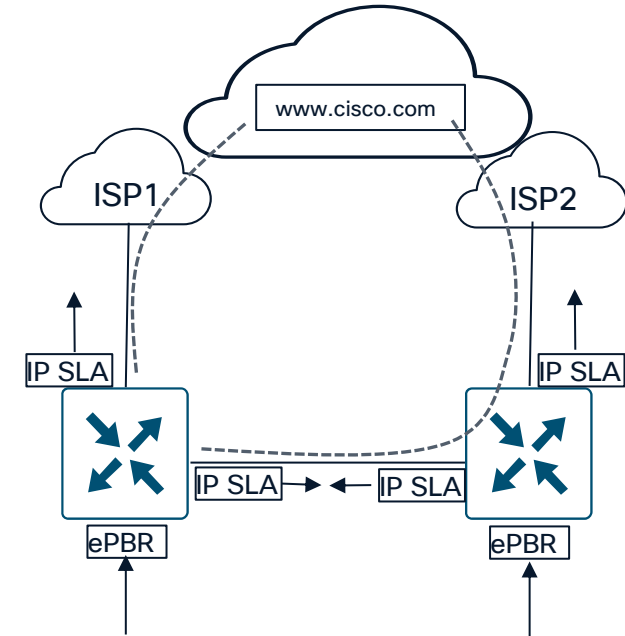
interval 20

multiplier 1

threshold 300



Workaround: Enhanced PBR (ePBR) with fast probing IP SLA tracking (cli add-on template)

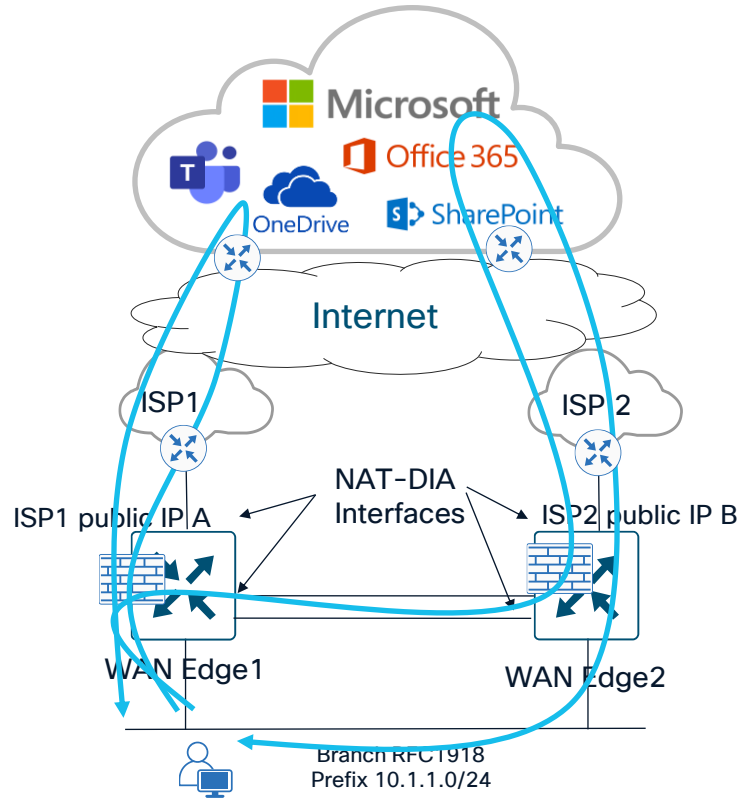


ePBR route map applied inbound on Service VPN interface

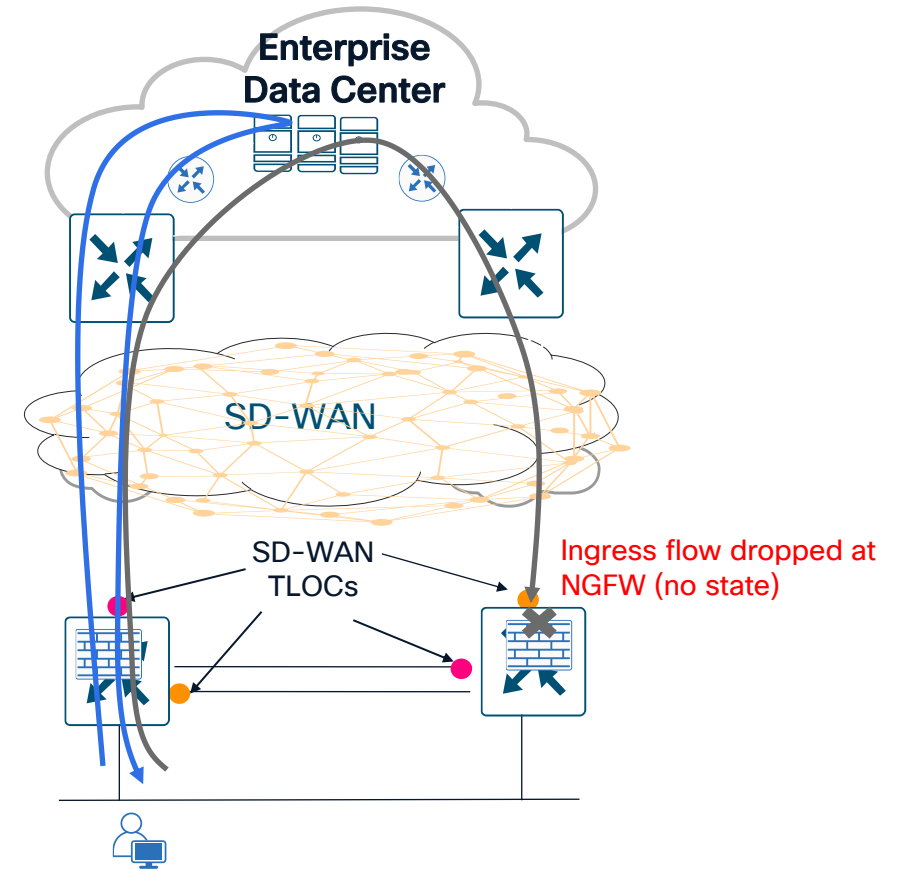
- Sends IP SLA probes at 5 sec intervals across both DIA links to Internet IP
- Sets NH to local ISP gateway IP if IPSLA state is UP from primary interface
- Sets NH to adjacent WAN edge router if IPSLA state for primary is down

# NGFW Redundancy

## DIA and SD-WAN traffic-flows



DIA-NAT enforces traffic symmetry and guarantees bidirectional traffic through the same NGFW

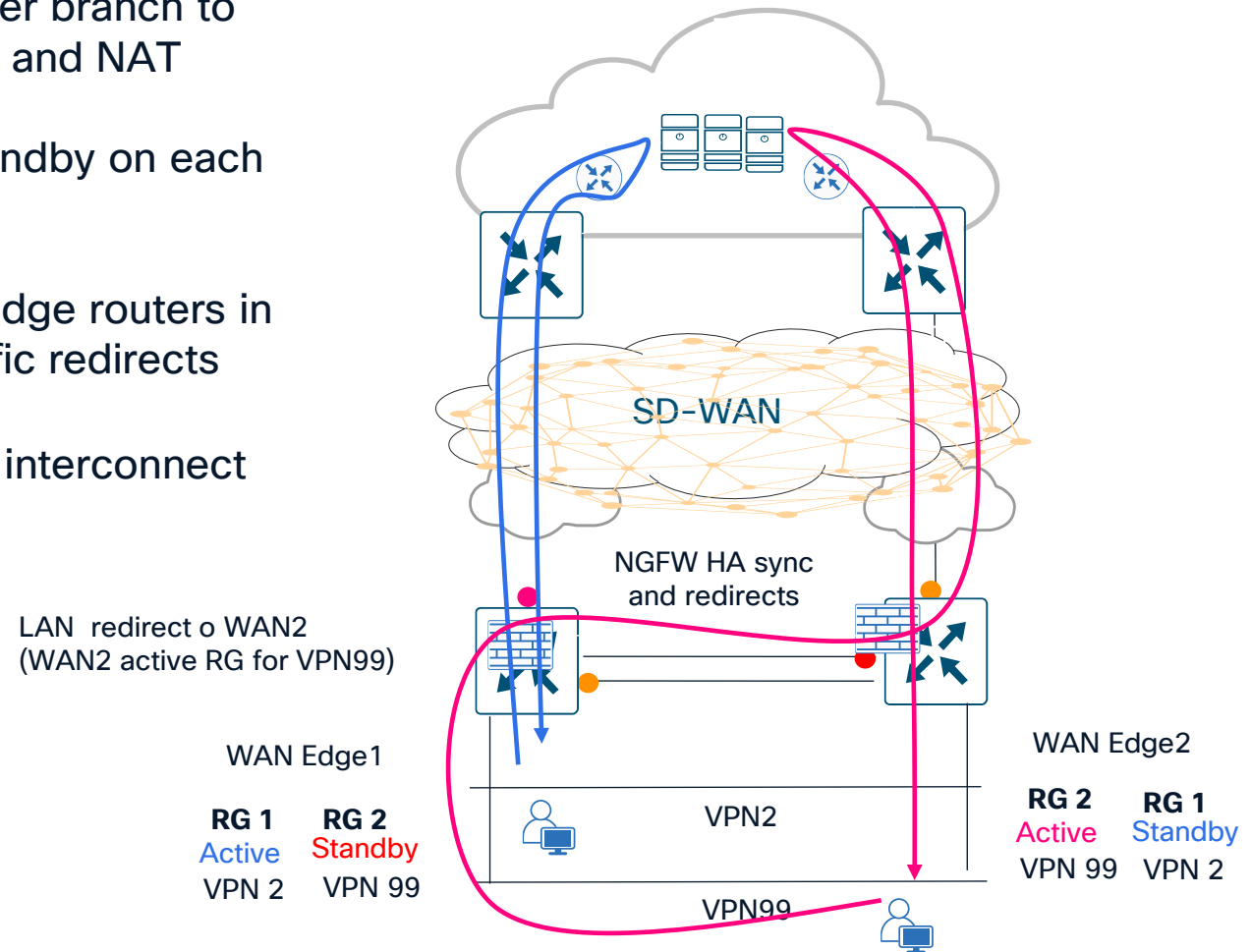


SD-WAN symmetry not guaranteed – Packets returning on different Edge dropped by NGFW (no flow state)

# NGFW Redundancy

## Cisco Catalyst SD-WAN Firewall High Availability (20.15)

- 20.15/17.15 introduces capability for a dual router branch to configure High availability with state sync for FW and NAT
- Redundancy Groups designated as Active or Standby on each WAN Edge for selected VPN(s)
- Dedicated Inter-connect link(s) connects WAN edge routers in HA mod - Session synchronization and data traffic redirects
- LAN/WAN traffic redirects across the dedicated interconnect if received by standby RG

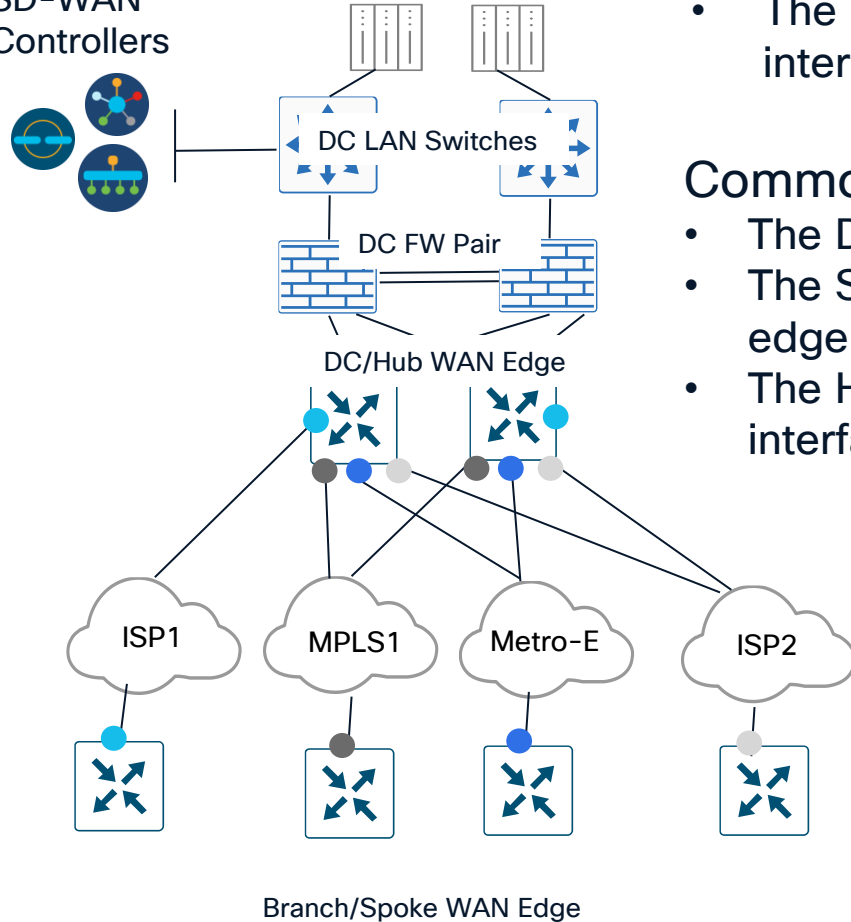


# Underlay Routing

# On-prem Controller Hosting in DC/Hub

Common Problem: Hub and Spoke routers not establishing control connections

SD-WAN  
Controllers

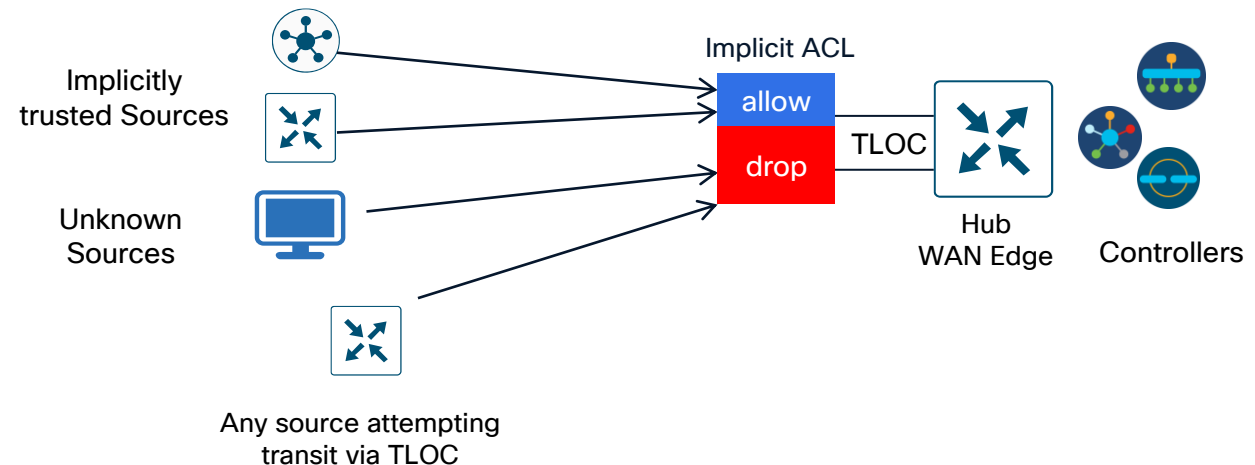


## SD-WAN Control Connection rules

- The WAN edge initiates TLS/DTLS control connections sourced from each TLOC interface to controllers, following routes in the global routing table.

## Common Problems:

- The DC FW is blocking all control connections since the TLS/DTLS ports are not open
- The Spoke WAN edge cannot establish control connections through the Hub WAN edge because the implicit ACL on the TLOC interface blocks transit TLS/DTLS traffic
- The Hub WAN edge does not initiate control connections because it lacks a TLOC interface or a route to LAN-hosted controllers



# OnPrem controller reachability workaround

## Explicit ACL and new Hub TLOC for control connections

### Problem 1:

Spoke WAN edge not forming control connections  
Implicit ACL on hub TLOCs dropping inbound TLS

### Solution1:

Explicit ACL to permit inbound TLS and dTLS ports

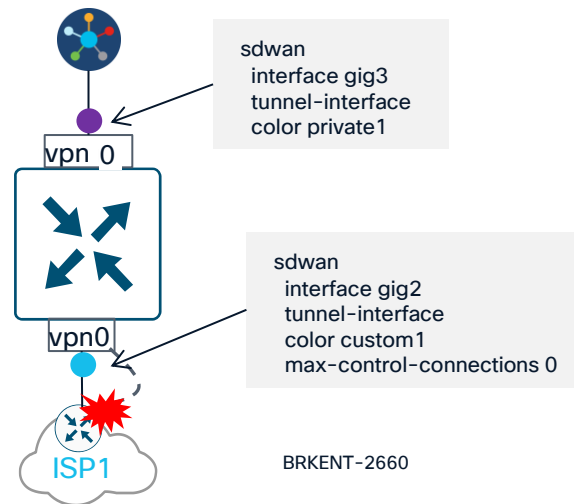
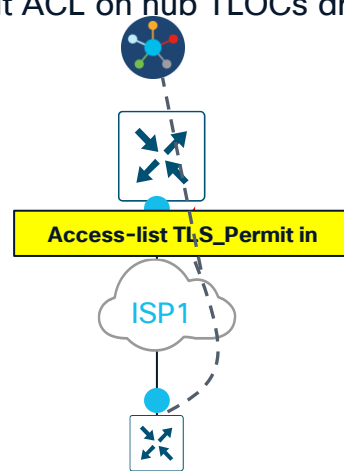
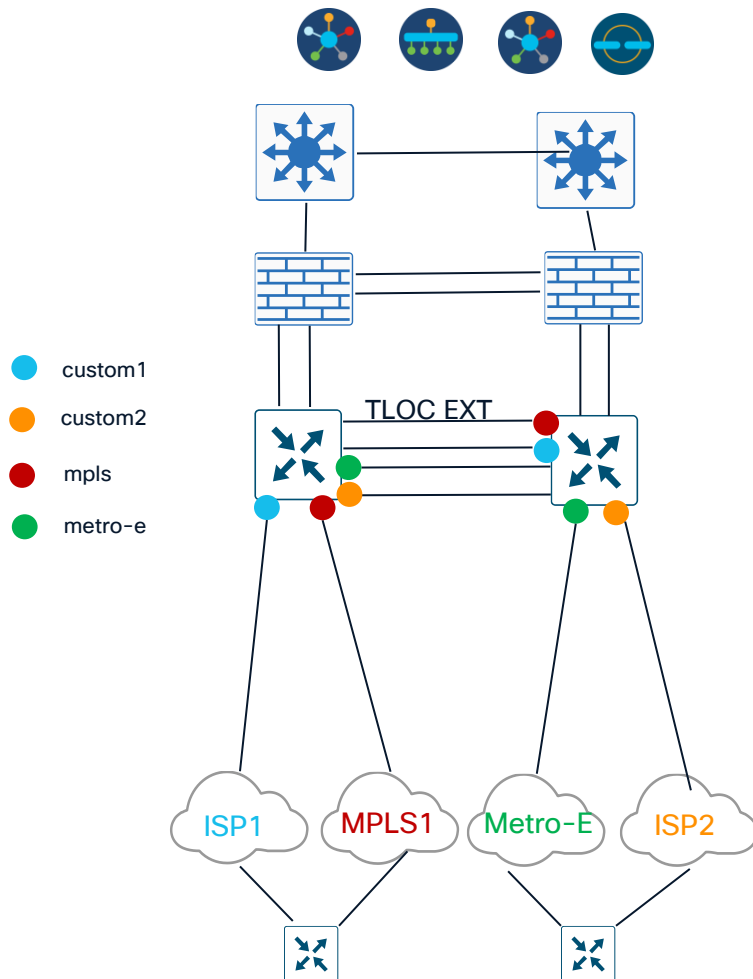
```
access-list TLS_Permit
sequence 1
match
source-port 12346 12366 12386 12406 12426 12546
protocol 17
action accept
!
sequence 2
match
source-port 23456 23556 23656 23756 23856 23956
24056 24156
protocol 6
action accept
```

Problem 2: Hub WAN edge not forming control connections  
No route in VPN0 towards controllers

### Solution 2:

Additional TLOC added to hub router  
for control connections only

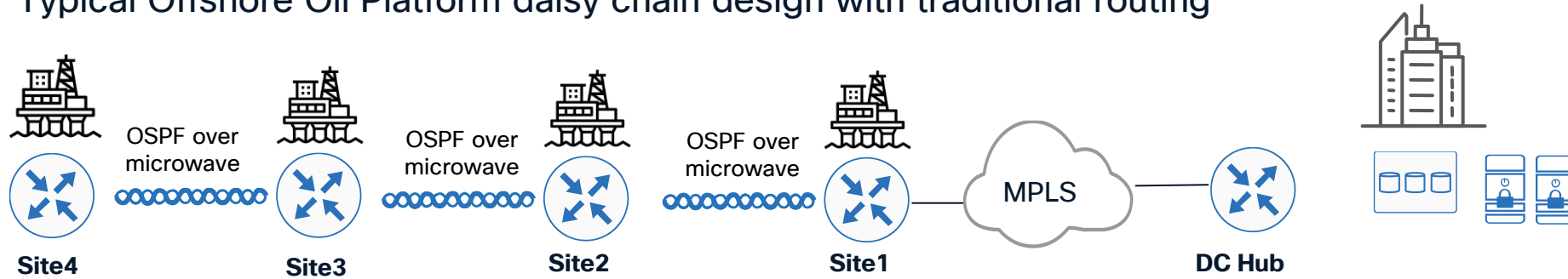
Control connection prerequisite disabled on  
other TLOCs with max-control-connections 0



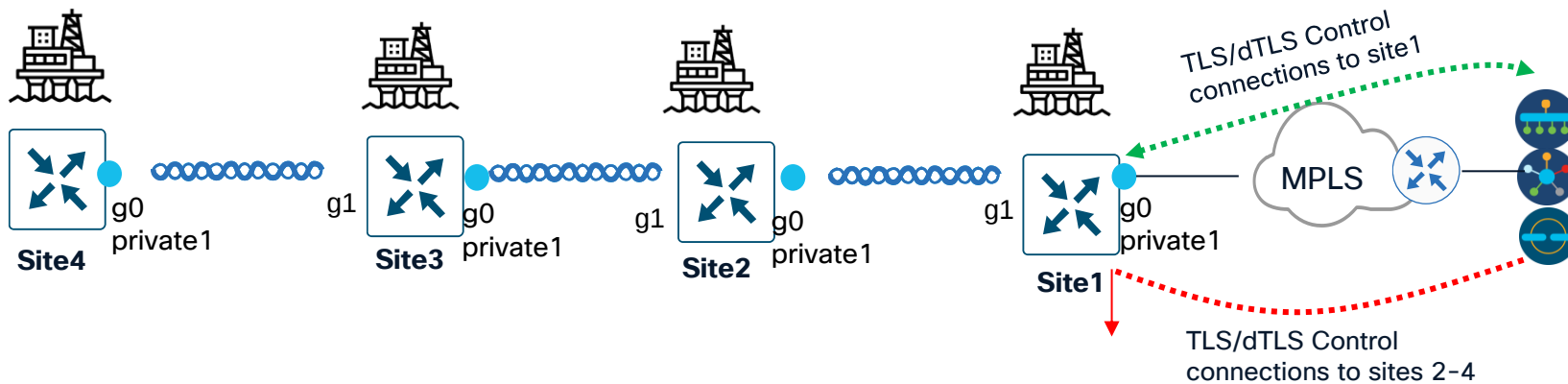
# Daisy chain transports

Problem: Downstream WAN edge not establishing control connections

Typical Offshore Oil Platform daisy chain design with traditional routing



Problem with SD-WAN migration: Control connections only establish to first site in daisy chain



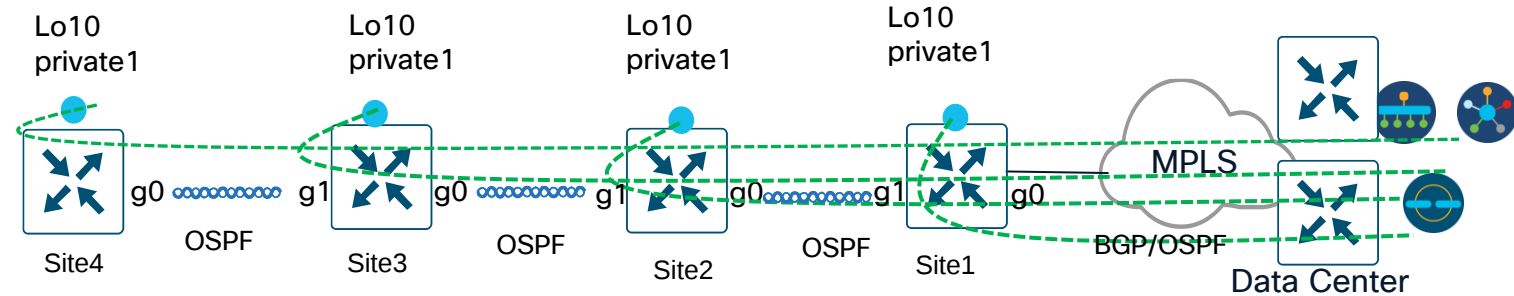
iACL TLOC dropping TLS/dTLS transit packets

BRKENT-2660

# Daisy chain transports

## Loopback TLOCs as workaround for implicit ACL

Solution: Define the TLOC using a Loopback interface to remove the implicit ACL on the physical interface and advertise it's IP into OSPF across the daisy chain

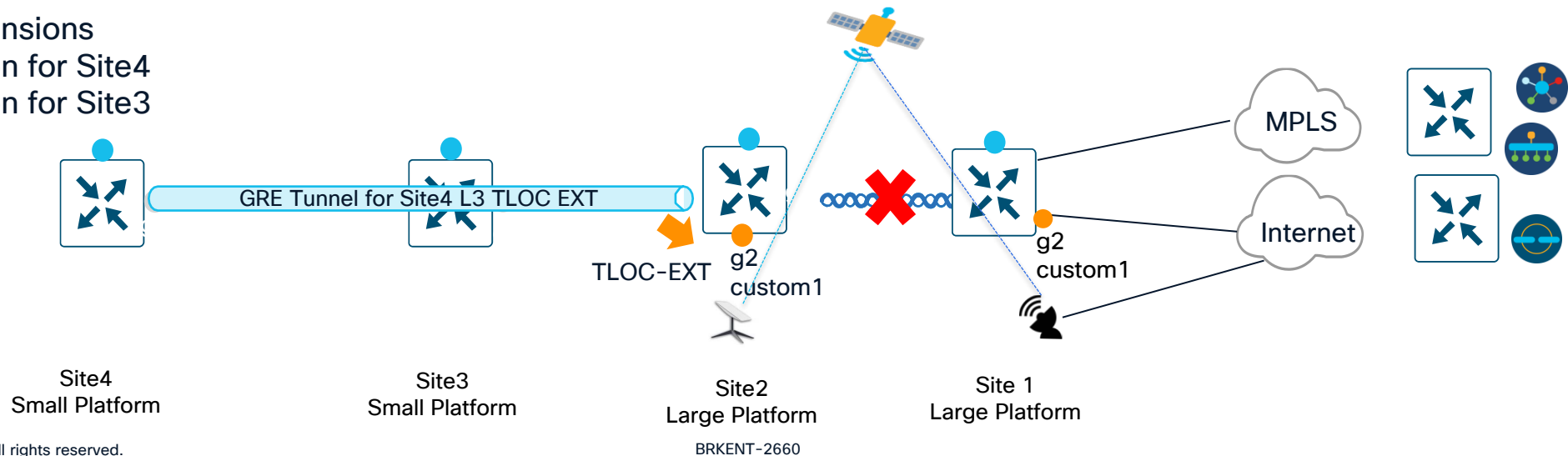


Additional Requirement: Satellite Internet added to site 2 for redundancy

- How can Site3 and 4 share this link over backhaul in the event of upstream microwave failure?

Solution: TLOC Extensions

- L3 TLOC extension for Site4
- L2 TLOC extension for Site3



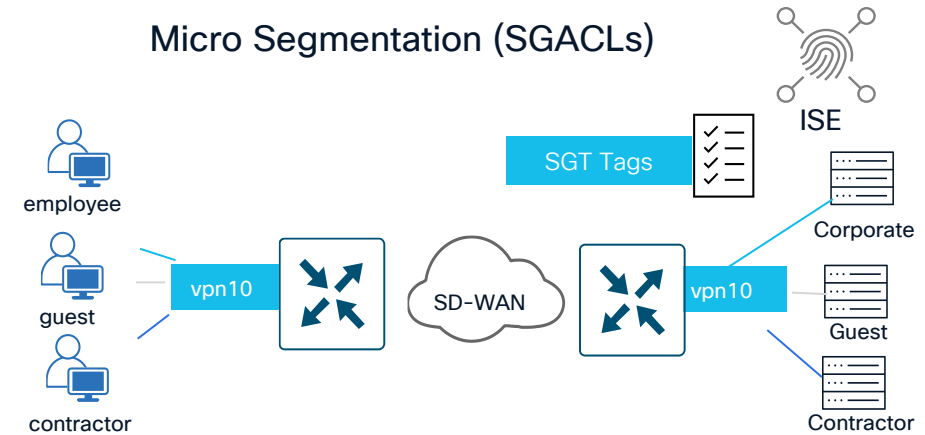
# Segmentation

# Common Segmentation Methods

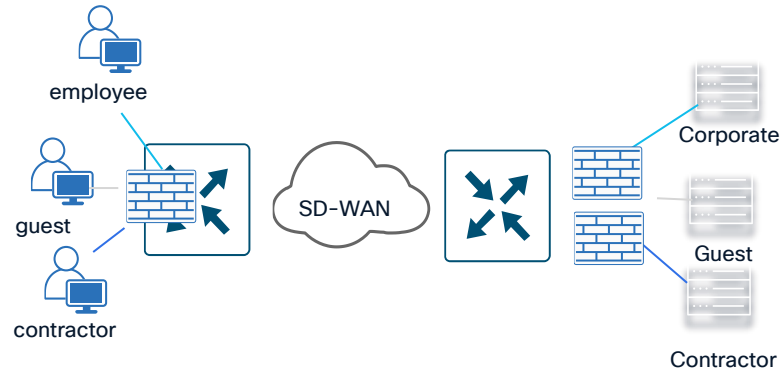
## Macro Segmentation (VRF/VPN)



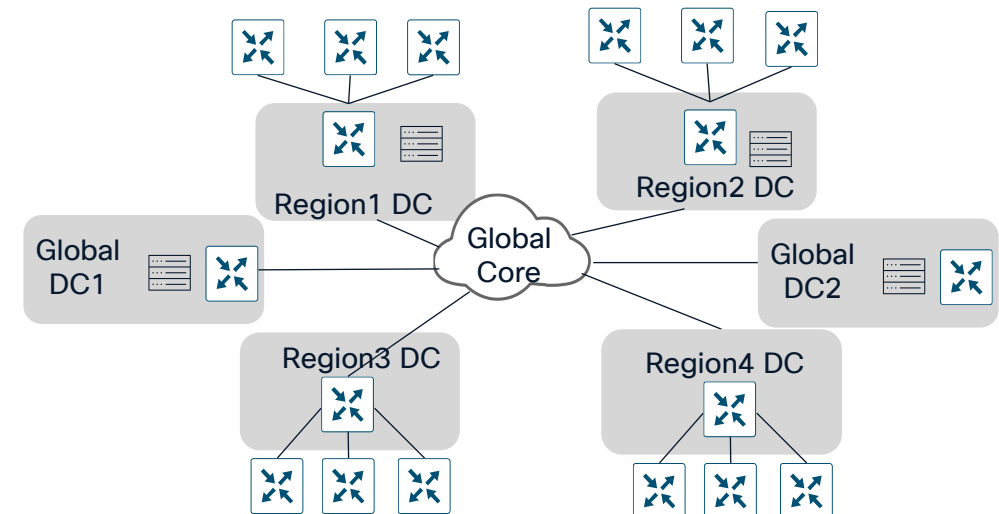
## Micro Segmentation (SGACLs)



## Firewall Segmentation (Access Control Policies)



## Regional Segmentation (Routing Policy)



# Traffic Segmentation: Perimeter Defense

## DDoS defense for Enterprise Financial Data Center

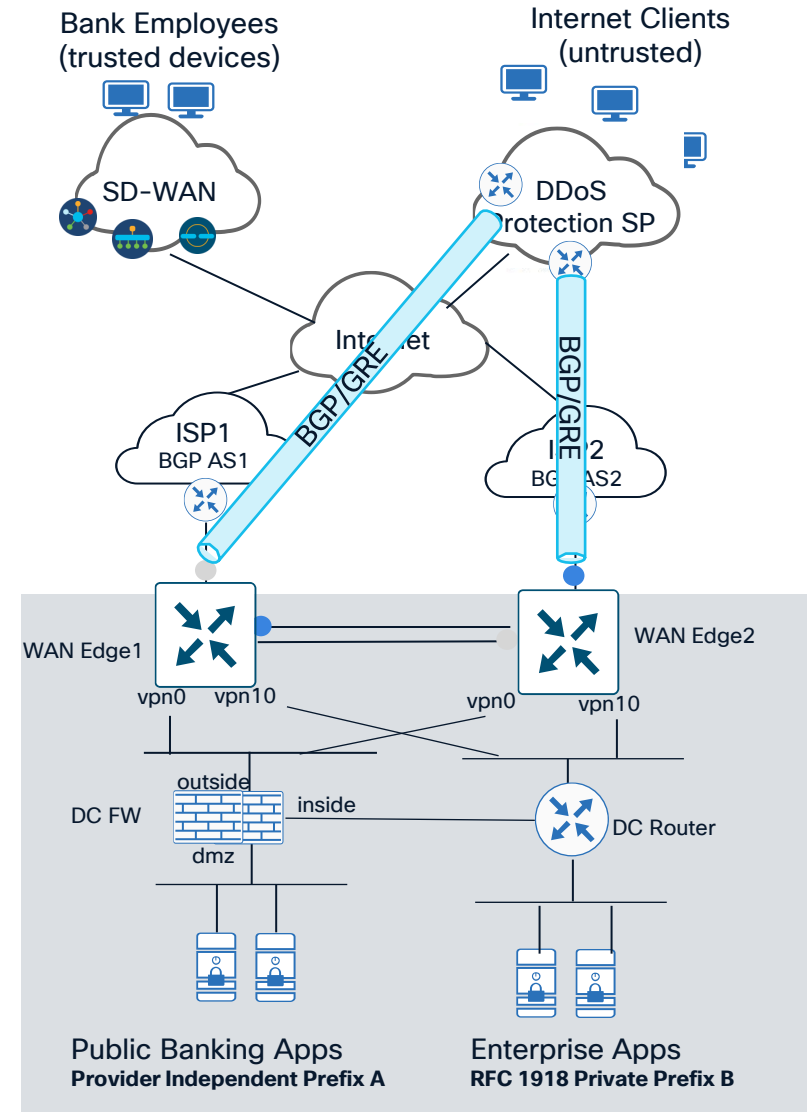
### Global Financial Enterprise with several Critical Data Centers

- Public Banking and Enterprise Servers hosted in DC
- Internet breakout at each WAN edge via VPN0 extension to ISP
- Cloud Service provider contracted to protect DC from DDoS attacks

### How to insert DDoS defense provider between Internet and Bank DC?

Solution: BGP over GRE tunnels between WAN edge routers and SP

- DDoS provider spoofs DC public prefixes to attract Internet traffic destined to provider independent (PI) server prefixes
- WAN edge routers announce PI prefixes with BGP over GRE
- Malware filtered, legitimate traffic to DC forwarded over GRE



# **SD-WAN Optimizations for low-speed links**

## **Cellular and Satellite**

# SD-WAN Optimizations for IoT/Cellular deployments

Cellular as only transport

## IoT use case and design trends

IoT substations are often deployed in remote locations with limited transport choices

- Applications typically involve sensors that transmit small infrequent packets

SD-WAN is an increasingly attractive technology for IoT applications

- Secure fabric, automated bring up, centralized configuration and management

## Challenges with SD-WAN and Cellular

Control/Data plane overhead may consume a high proportion of cellular bandwidth

- BFD probes over IPSec (~2.2 Kbps/ tunnel)
- OMP hellos to controllers (~80 Kbps/session)
- Statistics upload Catalyst Manager (up to 1.2 Mbps per export)



### Roadways and Intersections

Improve public safety, operational efficiency, and traffic management.

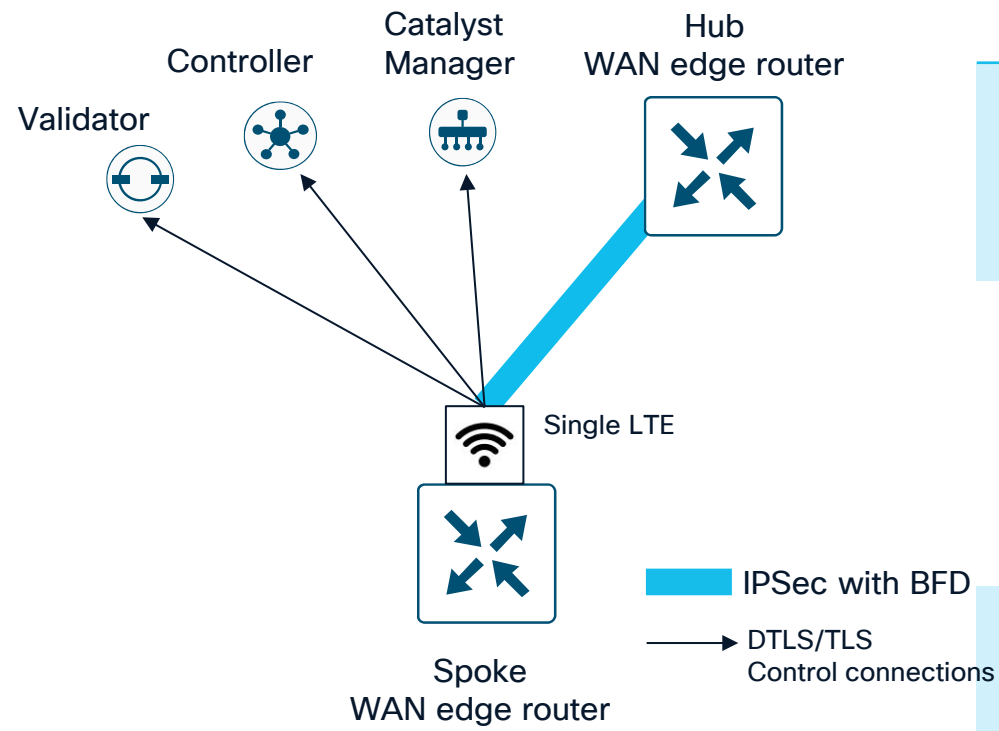


### Public Transportation

Connect your mass transit and rail operations to improve efficiency, security, and passenger experience.

# SD-WAN Overhead Measurement (20.15)

Secure Roadways CVP baseline measurement with default protocol timers



SD-WAN test topology

| Plane                       | Parameter                                                                                                                     | Defaults                                                            | 24-hr volume | 30-day volume |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|--------------|---------------|
| Data: BFD<br>(1 BFD Tunnel) | hello-interval/hello-tolerance<br>pmtu-discovery<br>app-route<br>poll-interval/multiplier                                     | 1/12 sec disabled<br>10 min/multiplier 6                            | 169 MB       | 5.14 GB       |
| Control: OMP<br>(1 TLS/OMP) | keepalive/holdtime<br>eor-timer<br>graceful-restart timer<br>advertisement-interval<br>max-omp-sessions<br>low-bandwidth-link | 20/60 sec<br>300 sec<br>12 hours<br>1 sec<br>2 sessions<br>disabled |              |               |
| Management<br>(1 TLS)       | Statistics export                                                                                                             | enabled                                                             |              |               |

<https://www.cisco.com/c/dam/en/us/td/docs/Technology/Roadways/Secure-Cellular-Roadways-CVD-Solution-Guide.pdf>

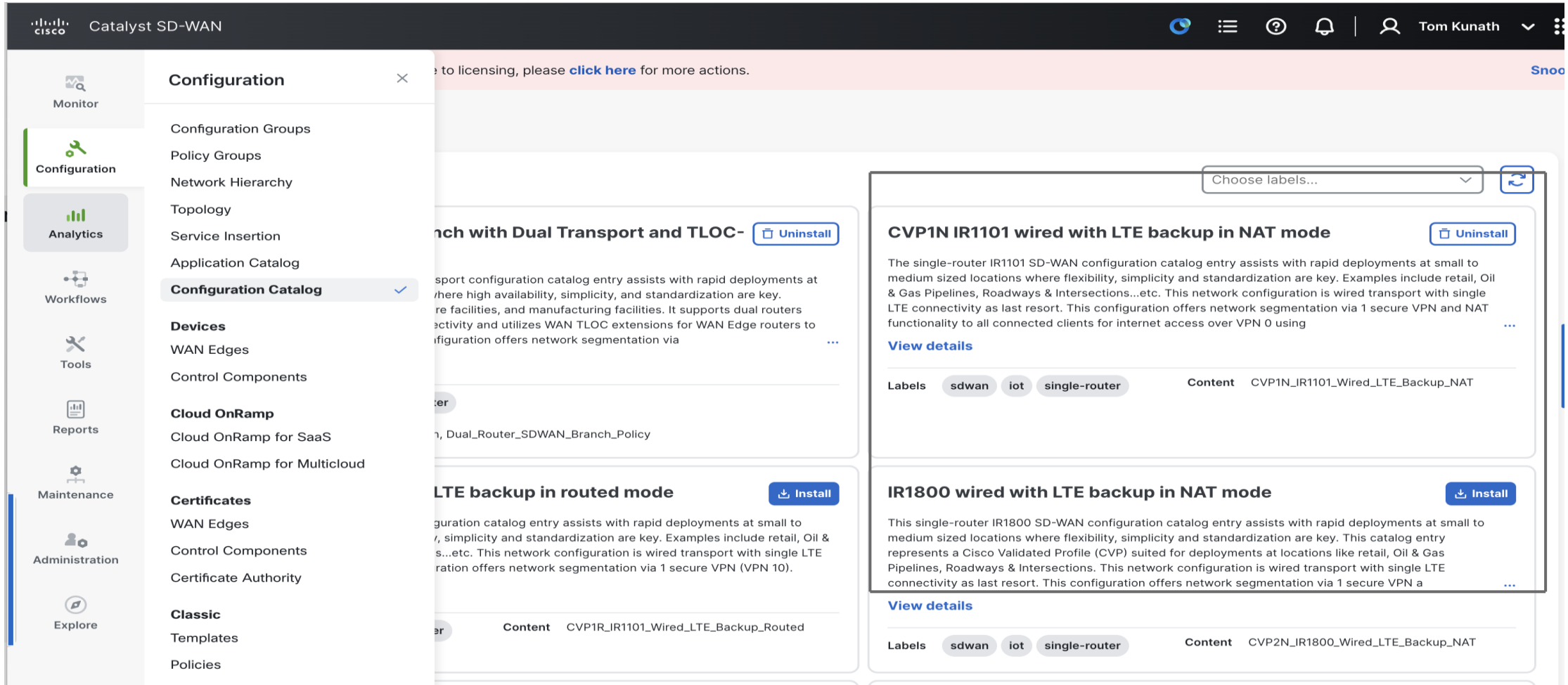
# SD-WAN Overhead Reduction on LTE testing

BFD and vManage Statistics test iterations \*

| Iteration | Parameter                                                                                                                                   | 24-hour volume | 30-day volume |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------|----------------|---------------|
| 1         | Default timers (all planes)<br>All stats and data collection disabled                                                                       | 169.89 MB      | 5.1 GB        |
| 2         | BFD hello modified to 10 sec<br>All stats and data collection enabled                                                                       | 85.51 MB       | 2.56 GB       |
| 3         | BFD hello modified to 10 sec<br>All stats and data collection disabled                                                                      | 82.17 MB       | 2.46 GB       |
| 4         | BFD hello modified to 10 sec<br>All stats disabled except<br>Device System Status', 'Device Health' statistics<br>and 'Interface statistics | 83 MB          | 2.49 GB       |

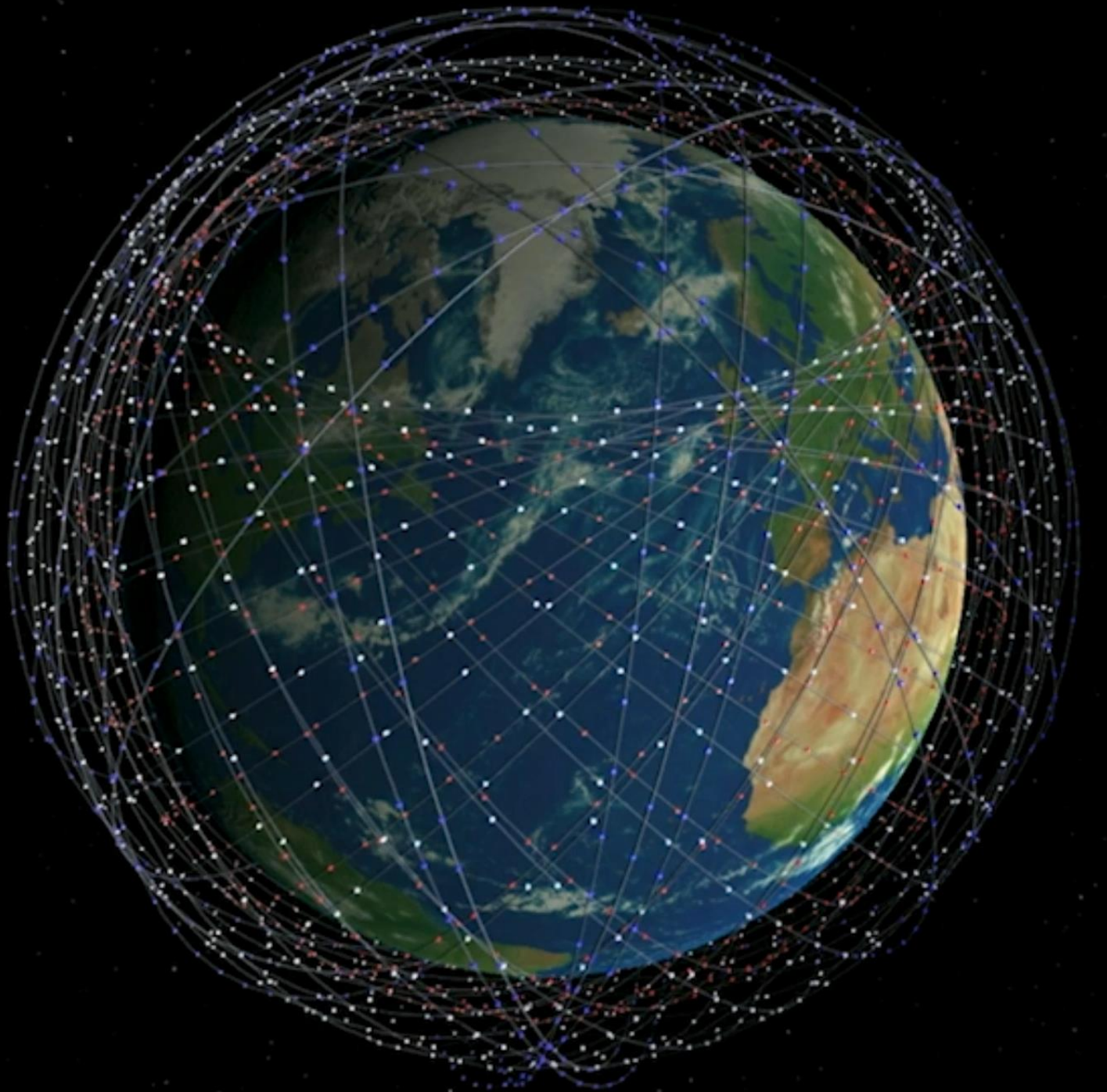
# SD-WAN Configuration Catalog

## UX2.0 Configuration groups for IoT Cisco Validated Profiles (CVP)



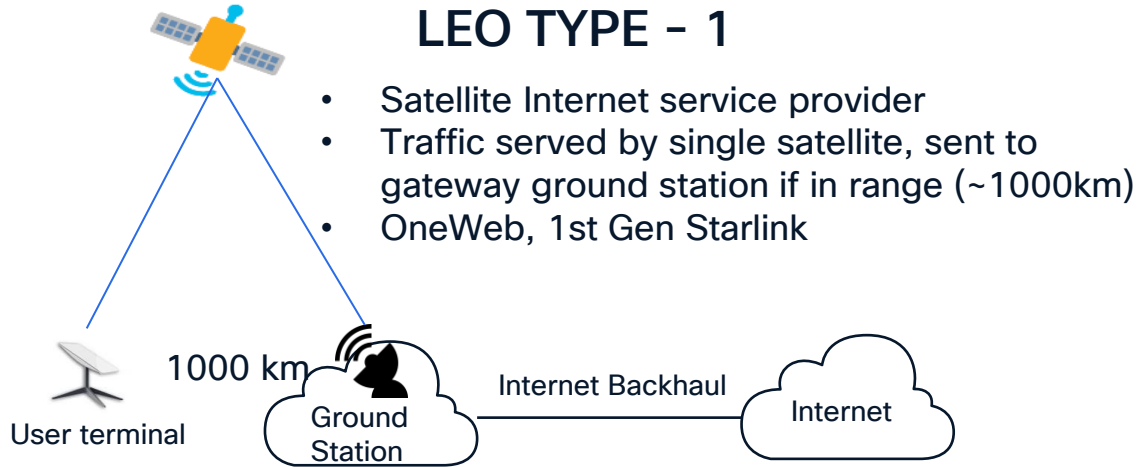
<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/config-groups/configuration-group-guide/config-catalog.html>

# LEO Satellite

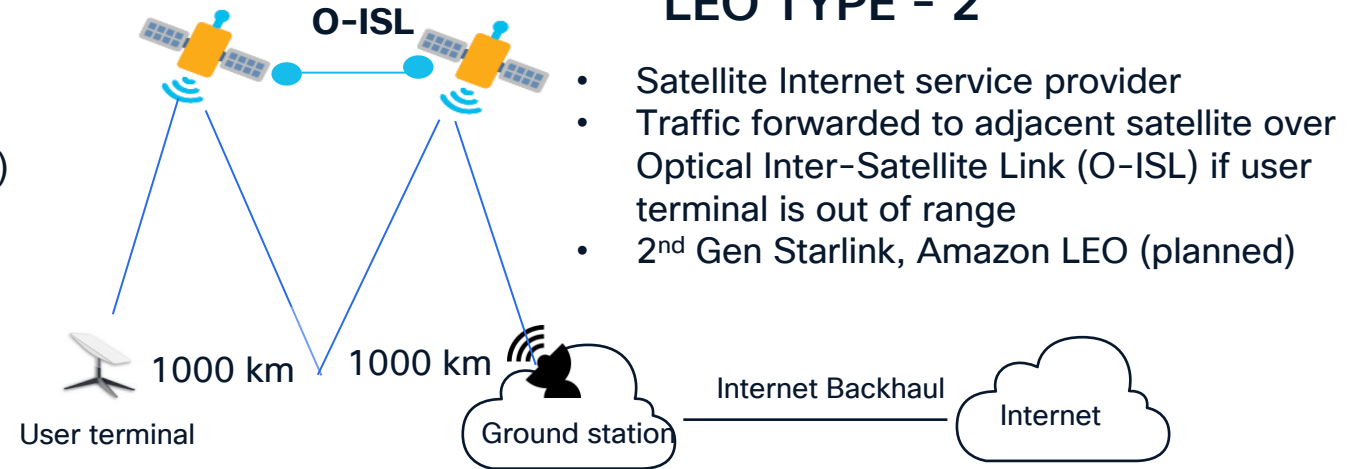


# LEO Satellite Communication Architectures

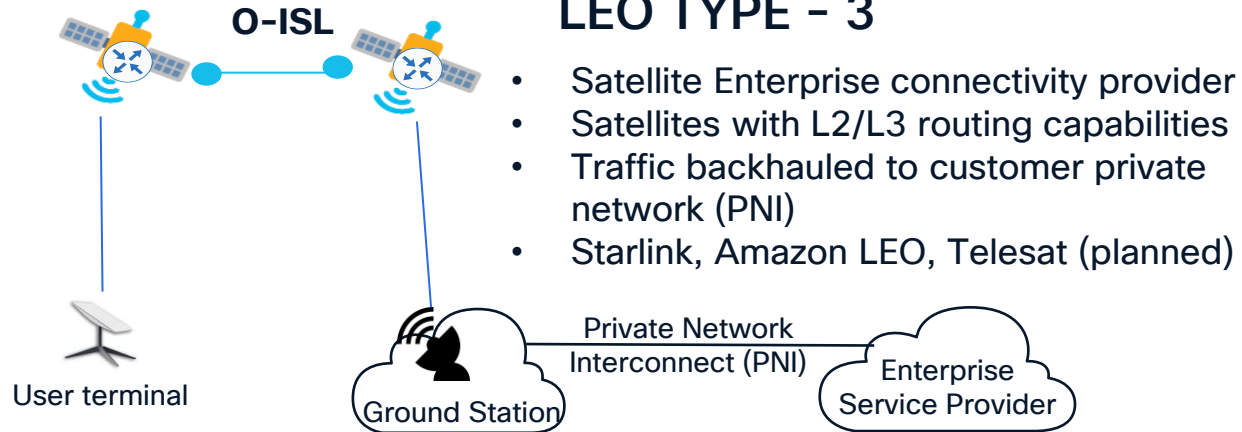
## LEO TYPE - 1



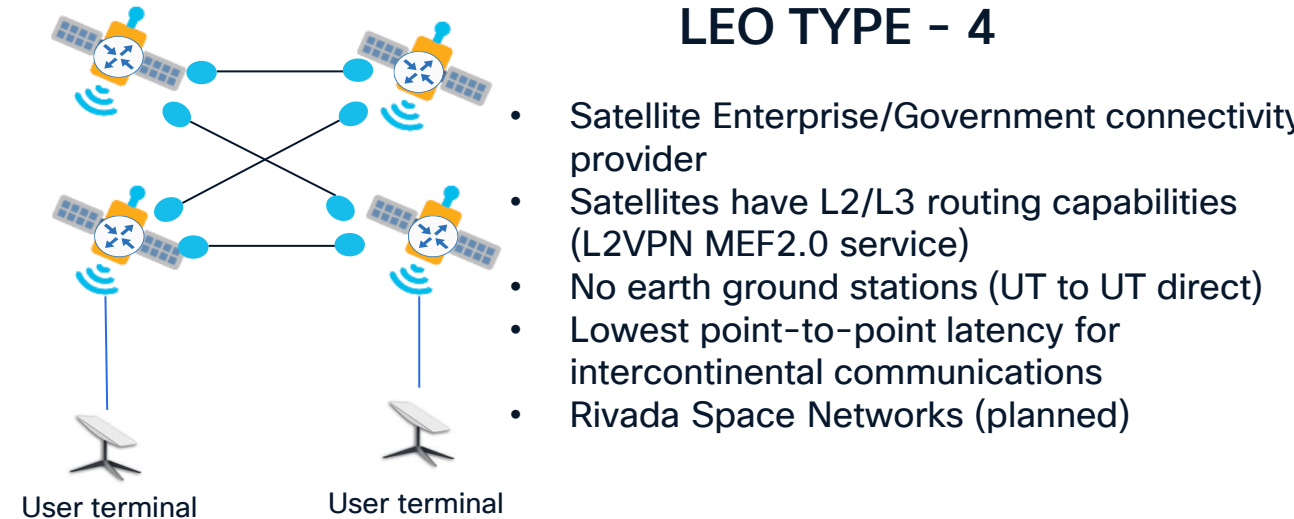
## LEO TYPE - 2



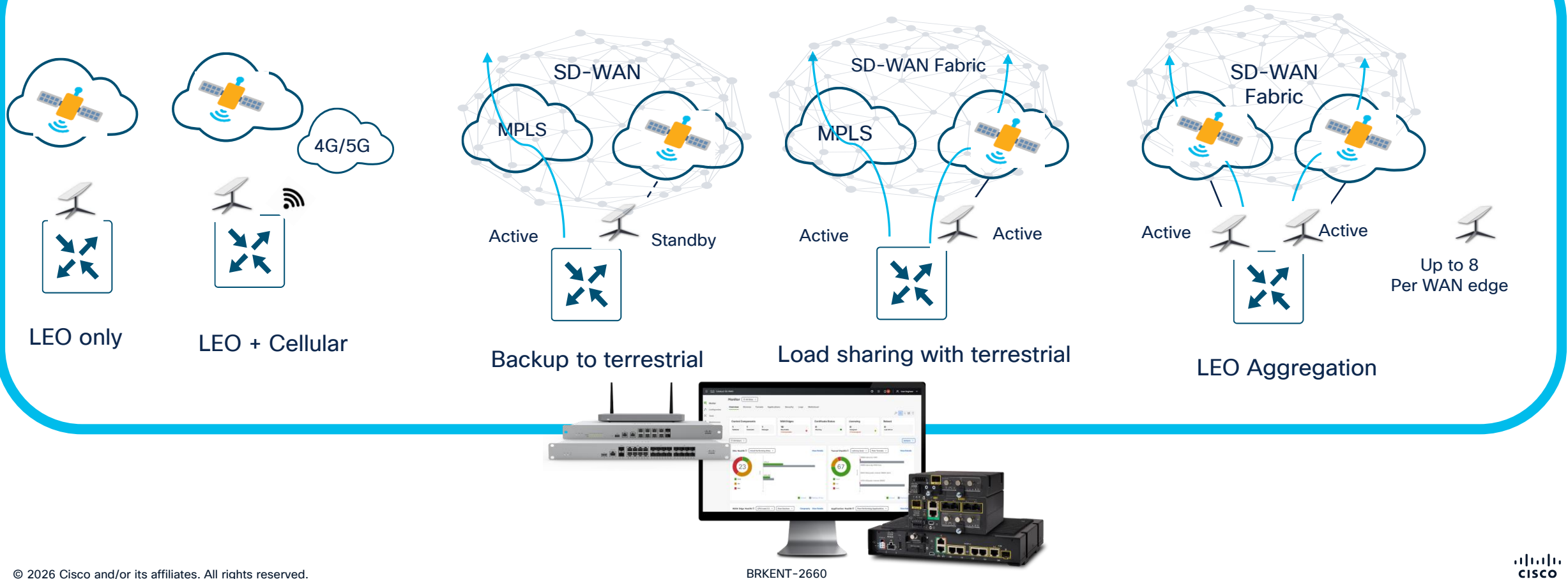
## LEO TYPE - 3



## LEO TYPE - 4



# Catalyst SD-WAN use cases with LEO Satellite



# Catalyst SD-WAN with Starlink

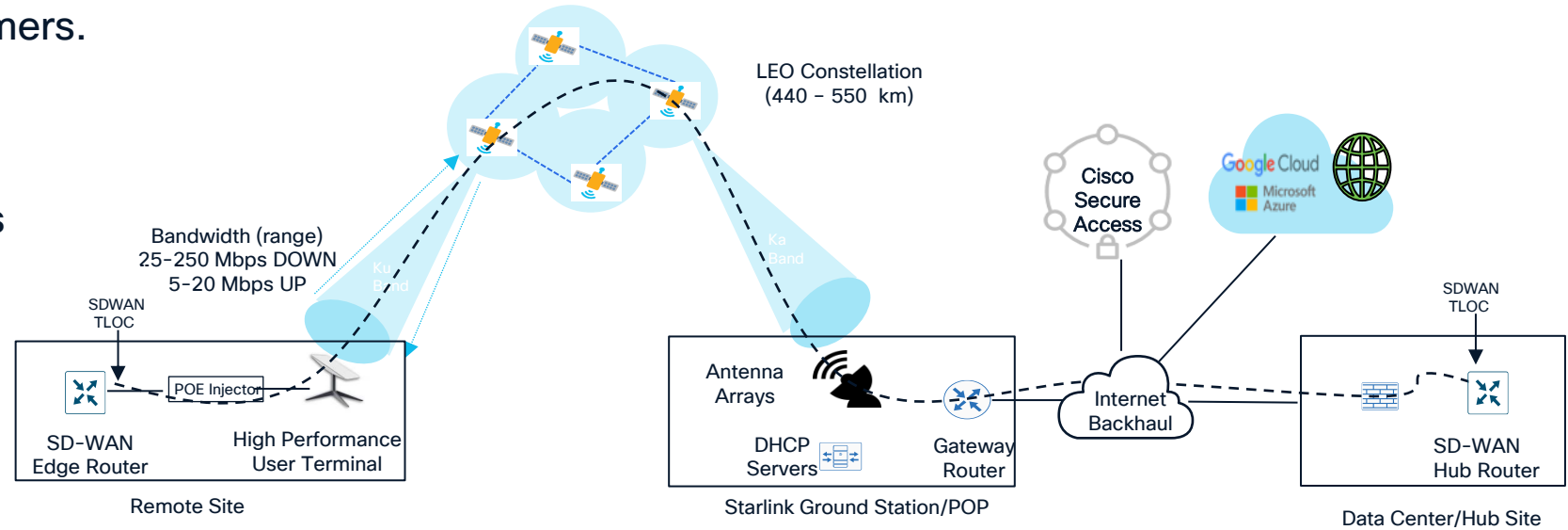
Starlink is a constellation of LEO satellites offering Internet and private access to residential and business customers.

As of Jan 2026:

- 9500+ deployed satellites
- 200 ground stations
- 9+ million subscribers in 155 countries

CPE includes a user terminal and basic wifi router that can be replaced by a Catalyst SD-WAN router with power injector

Starlink priority plan and public IP recommended for SD-WAN deployments to avoid CGNAT issues



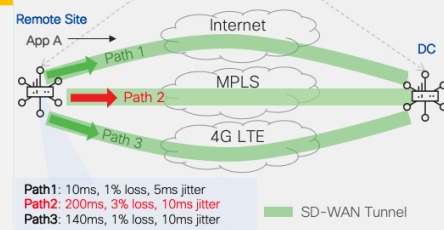
## Challenges

- LEO satellite networks can experience **higher latency, loss and bandwidth fluctuations** than traditional networks
  - Latency: 20-60ms (land users)
  - Loss 1-2% with spikes up to 4% and beyond
- TCP's reliability mechanisms are designed to handle some packet loss, but even 1% packet loss can significantly degrade application performance

# Catalyst SD-WAN Application Experience Features

## Application Aware routing

- Detects brownout conditions in overlay path.
- SLA based traffic steering
- Automatic failover to secondary path if primary path fails.



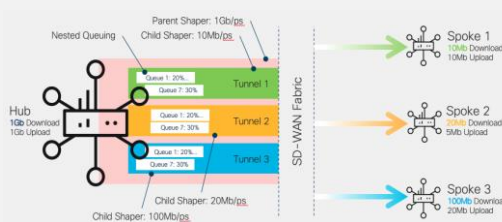
## Packet Duplication

- Send duplicate packets over alternate path
- Mitigate packet loss for critical voice or video traffic
- Enhances Application quality of experience

110 110  
1011 1011  
010 010  
110 110  
1011 1011  
010 010

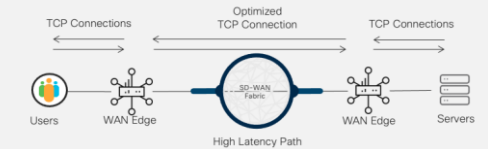
## Quality of Service (QoS)

- Manage and avoid network congestion
- Guaranteed Bandwidth
- Traffic queueing and shaping
- Prioritize critical application traffic over other traffic.



## TCP optimization

- BBR2 Congestion control algorithm
- Window scaling
- Large Initial windows
- Selective acknowledgement
- Helps in reducing latency and increase throughput



## Forward Error Correction

- Protects against packet loss
- Protocol agnostic (TCP/UDP)
- Enhances Application quality of experience



## DRE, LZW

- Traffic optimization techniques
- Byte level caching & Data compression
- Protocol agnostic



# App-QoE feature Efficacy with Starlink

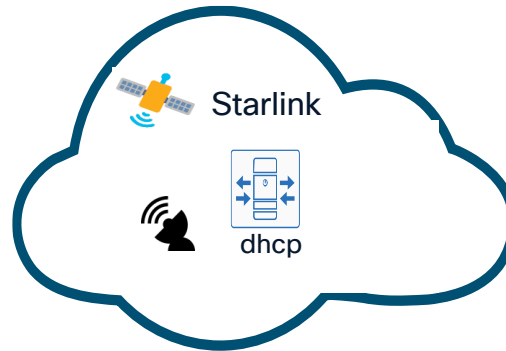
iPerf3 Throughput Testing

| Test                                                                     | Download   | Upload     | Throughput improvement      |
|--------------------------------------------------------------------------|------------|------------|-----------------------------|
| Speedtest Baseline (UDP)                                                 | 250 Mbps   | 17 Mbps    | N/A (Baseline)              |
| IPerf3 Baseline (TCP)                                                    | 55 Mbps    | 9 Mbps     | N/A (Baseline)              |
| iPerf3 throughput improvement with <b>Forward Error Correction (FEC)</b> | 130 Mbps   | 11 Mbps    | 2.38X down, 1.2X up         |
| iPerf3 throughput improvement with <b>Packet duplication</b>             | 70 Mbps    | 11 Mbps    | 1.3X down, 1.2X up          |
| iPerf3 throughput improvement with <b>TCP optimization</b>               | 230 Mbps   | 18 Mbps    | 4X down, 2X up              |
| File download (4.3Gb) with <b>DRE/LZ</b>                                 | 86 seconds | Not tested | Download time reduced by 3X |

# Catalyst SD-WAN with Starlink

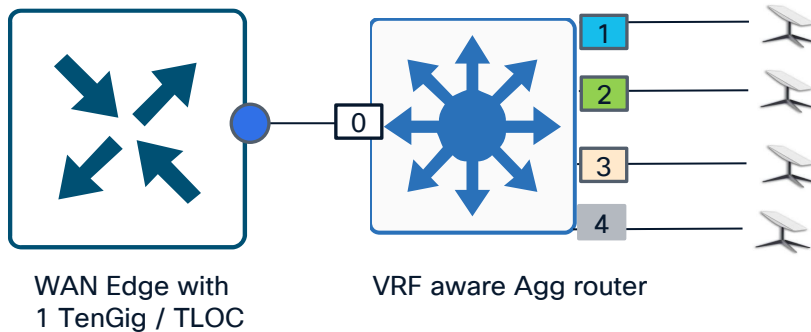
## Challenges with multiple UT aggregation

Problem: Interface might not install DHCP-learned IP address



- Routers reject dynamic IP allocations if different Ethernet interfaces receive IPs from common DHCP scopes (violates IP routing rules)
- No support for static IP addresses, even for business class users

## Workaround: VRF aware router for Starlink UT aggregation

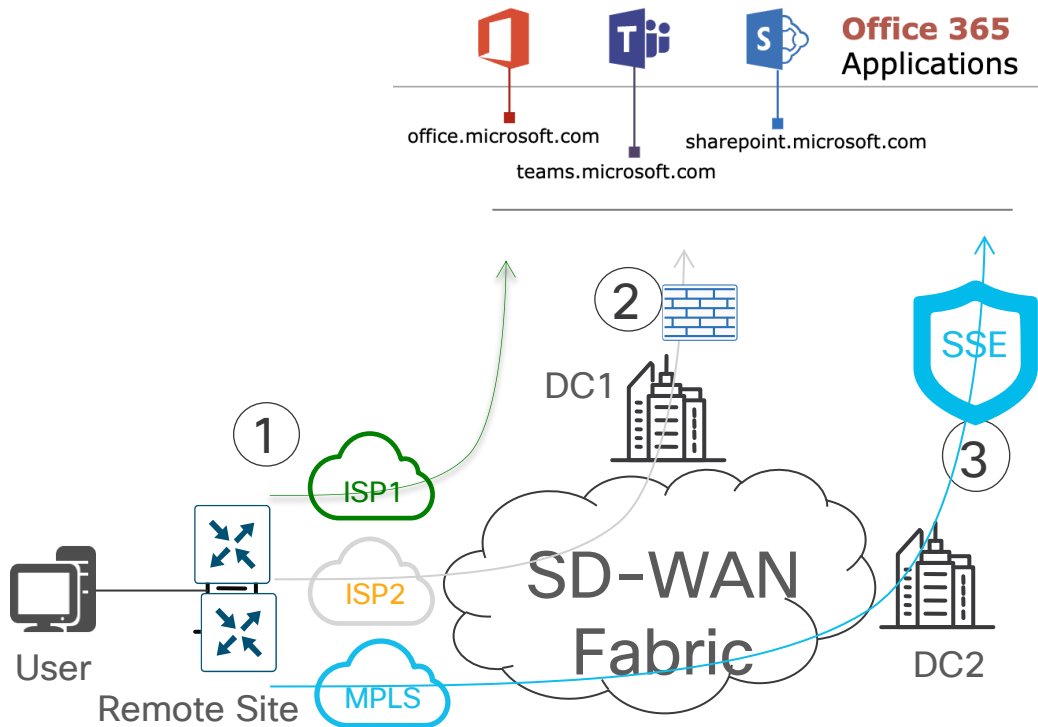


- Virtual Routing and Forwarding (VRF) interfaces support overlapping addresses and are deployed as DHCP clients with NAT enabled
- Redistribution of each VRF into Global Routing Table (GRT)
- WAN edge router has single TLOC, load-balancing across multiple UT done Agg router
- Feature request opened for Transport interface segmentation on SD-WAN WAN edge router

# Cloud SaaS Path Optimization

# Fast Track SaaS Optimization

Unlocking SaaS App Visibility Through First Packet Match



## Business intent

- MS Teams forwarded over DIA path ISP1
- Other SaaS: Prefer better performing path across SD-WAN overlay to DC1 or DC2 breakout

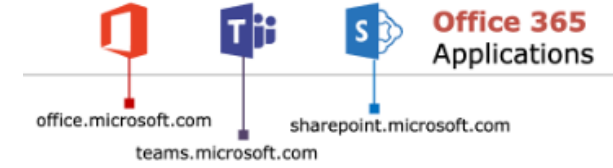
## Problem

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

## Solution

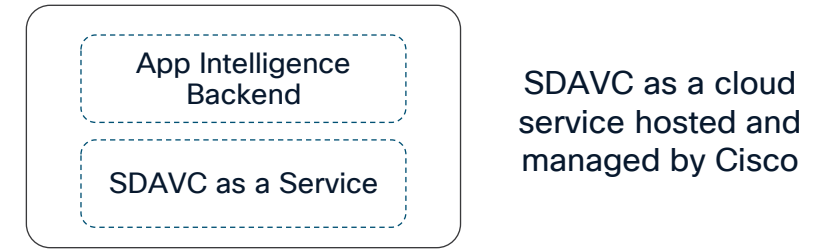
- SD-AVC as a Service
- Application Catalog

# SDAVC as a Service

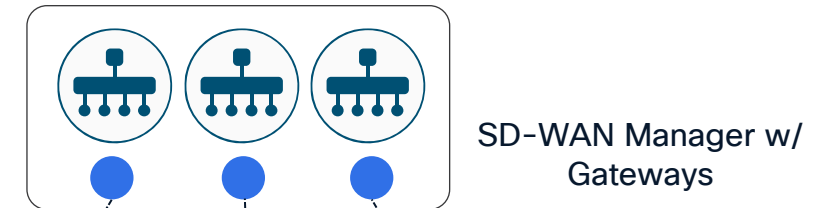


## Control Plane SDAVC as a Service

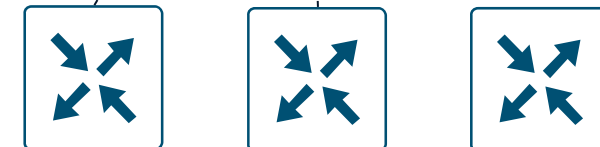
- Cloud Service pulls M365 URL Categories using M365 web service.
- Dynamically pre-populates Edge router's NBAR cache with M365 IP addresses and URL Categories.
- Easy deployment: enabled by default, with automatic Cloud authentication
- Dynamic Update of built in Protocol Pack



SD-WAN Manager  
(Proxy to SDAVCaaS)



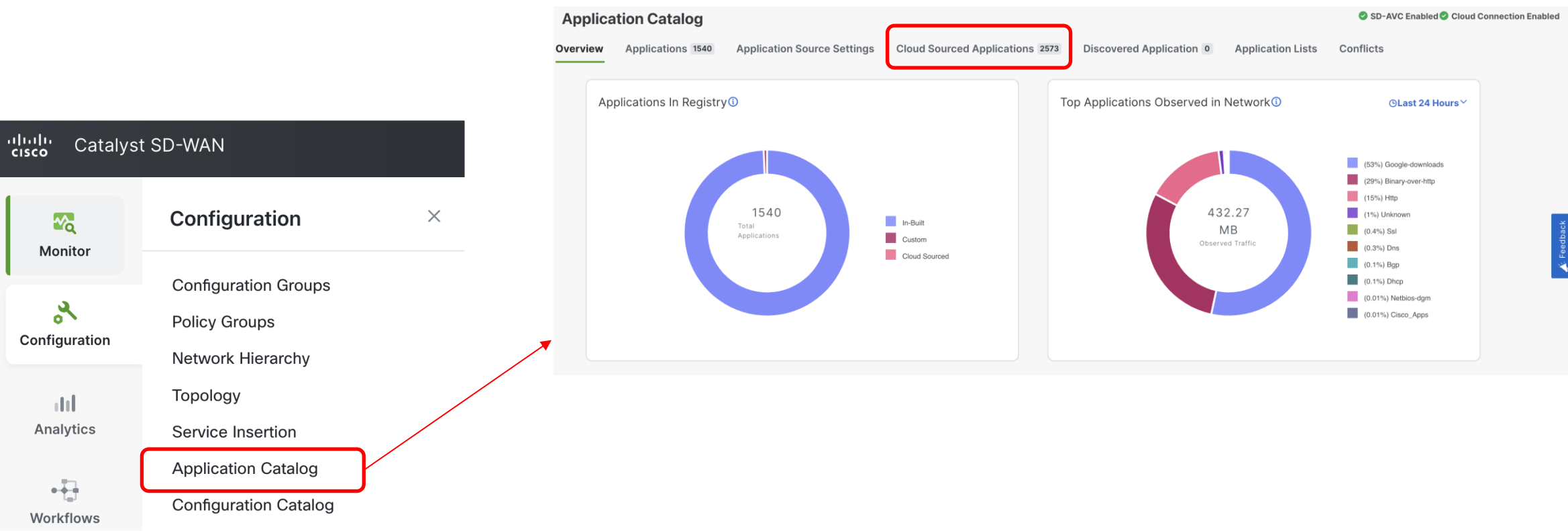
Inside DTLS Channel



## Data Plane NBAR Agents

# Application Catalog

Manage application visibility and control operations from Application Catalog which provides view into latest status of Applications (Built-in, Custom & Cloud Sourced Apps) and usage.



# Catalyst Manager Workflow (20.15)

Enable SD-AVC



Update application registry and NBAR protocol packs



Update Application lists



Update Policies (as needed)

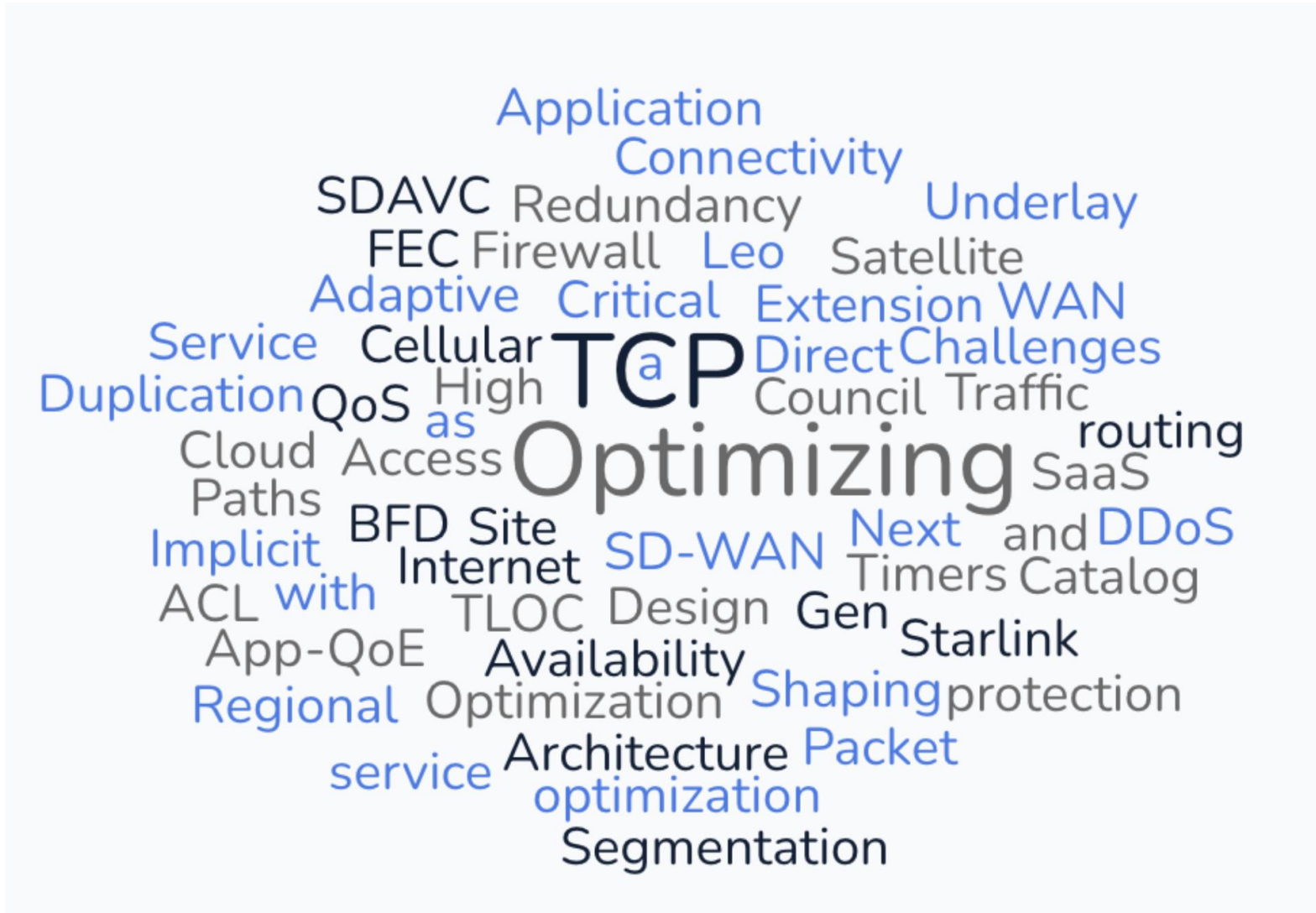
Administration -> Settings -> Data Collection and Settings -> Select **Cloud Services**

Configuration -> **Application Catalog** -> Cloud-Sourced Applications **select and apply** interesting applications to update Catalyst Manager application registry and push NBAR protocol pack to devices

Configuration -> **Application Catalog** -> Application Lists

Configuration -> Policies | Policy-Groups

# Summary



# Webex App

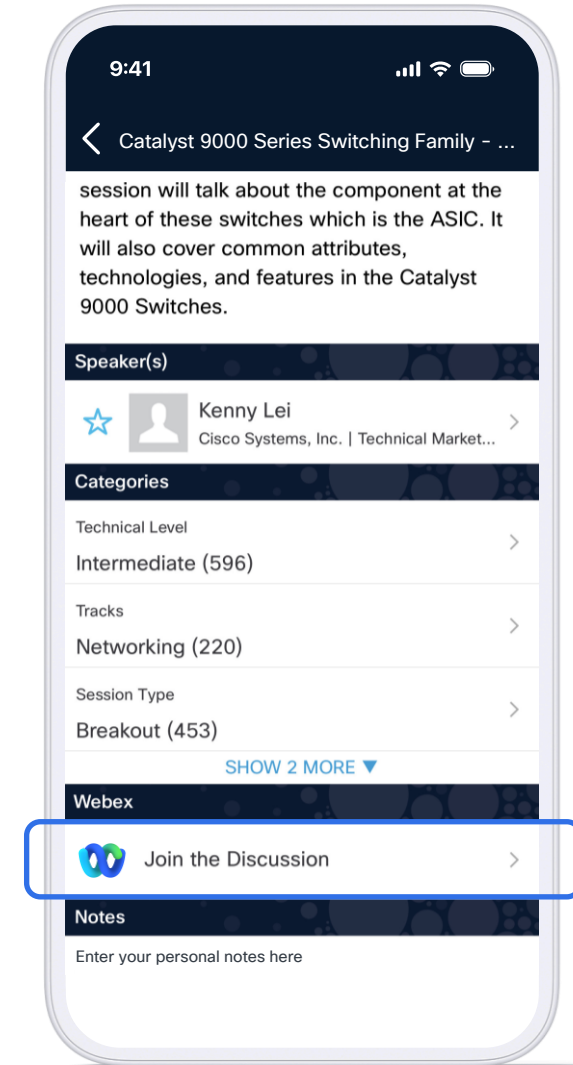
## Questions?

Use Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Events App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

**Webex spaces will be moderated by the speaker until February 27, 2026.**



# Complete your session surveys



**Complete your surveys** in the Cisco Events App.



**Complete** a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.  
(from 11:30 on Thursday, while supplies last)

# Continue your education



**Visit** the Cisco Showcase for related demos



**Book** your one-on-one Meet the Engineer meeting

**Visit** the Technical Solutions Clinics to discuss your technical questions



**Attend** the interactive education with DevNet, Capture the Flag, and Walk-in Labs



**Visit** the On-Demand Library for more sessions at [CiscoLive.com/On-Demand](https://CiscoLive.com/On-Demand)

Thank you

**CISCO** Live !

