cisco Live!

#CiscoLive

The bridge to possible

SD-WAN Routing Innovations and Use cases

Chandra Balaji Rajaram

BRKENT-1005

Cisco Webex App

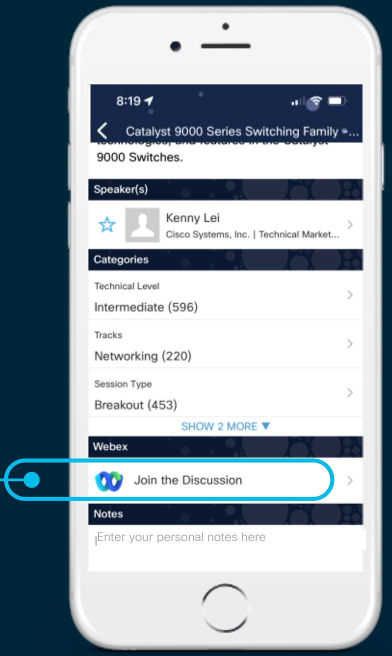
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile 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 June 17, 2022.



8:19

Catalyst 9000 Series Switching Family •...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-1005

cisco Live!

Agenda

- Introduction
- Per Class App-Aware Routing
- Per VPN QOS
- Service-VPN NAT Tracker
- Service-Side NAT with Data-policy
- BGP community propagation into OMP
- Summary

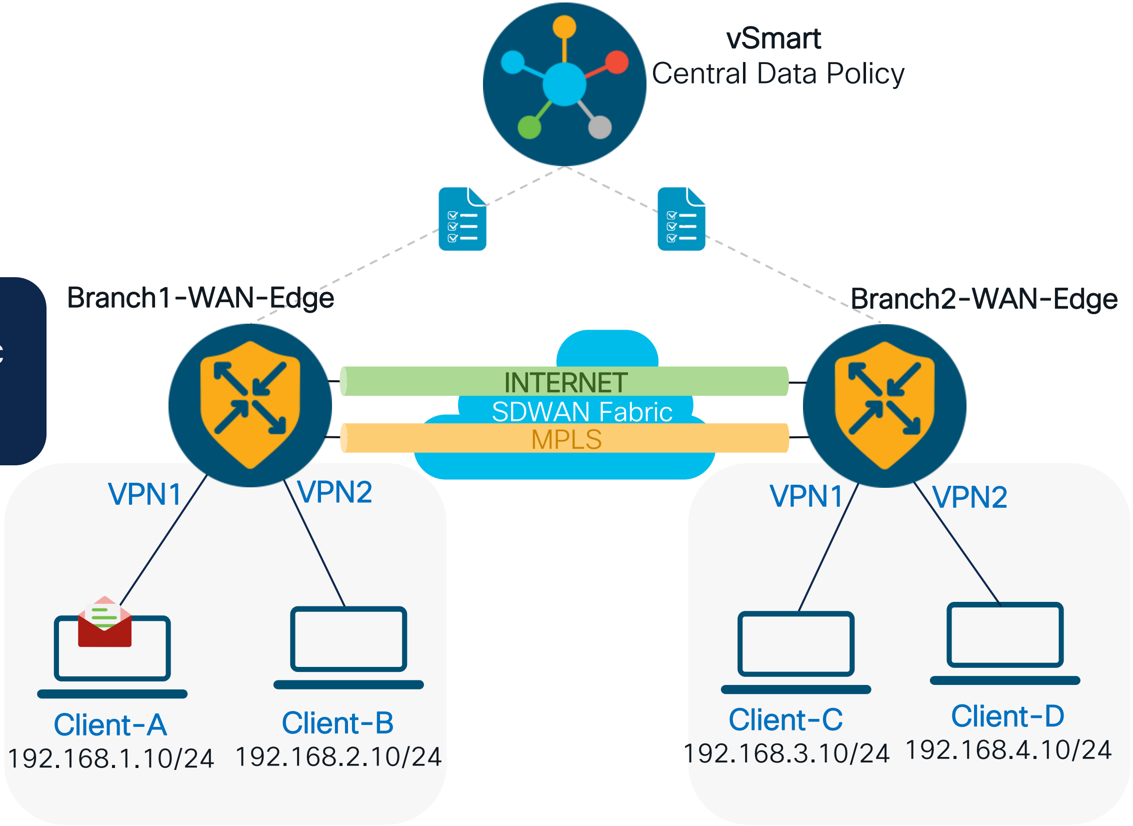
Disclaimer

- This presentation is not about Deep Dive session into SD-WAN routing features.
- This will only cover few of the routing features and its specific use cases related to SD-WAN.

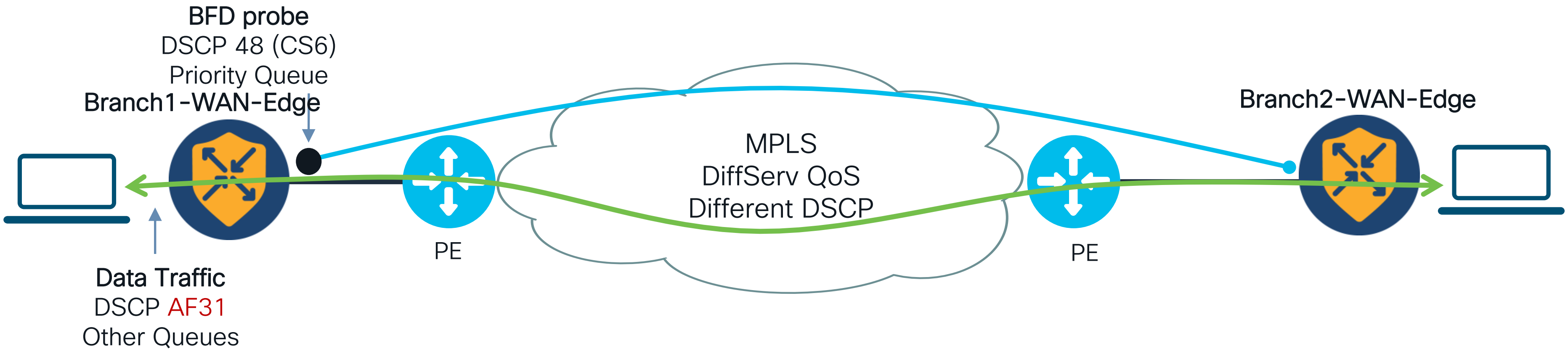
Per-Class Application Aware Routing

Scenario 1a:Packet flow from Service VPN to Overlay

Business Critical Application traffic is not performing well



Default mode of sending BFD probes

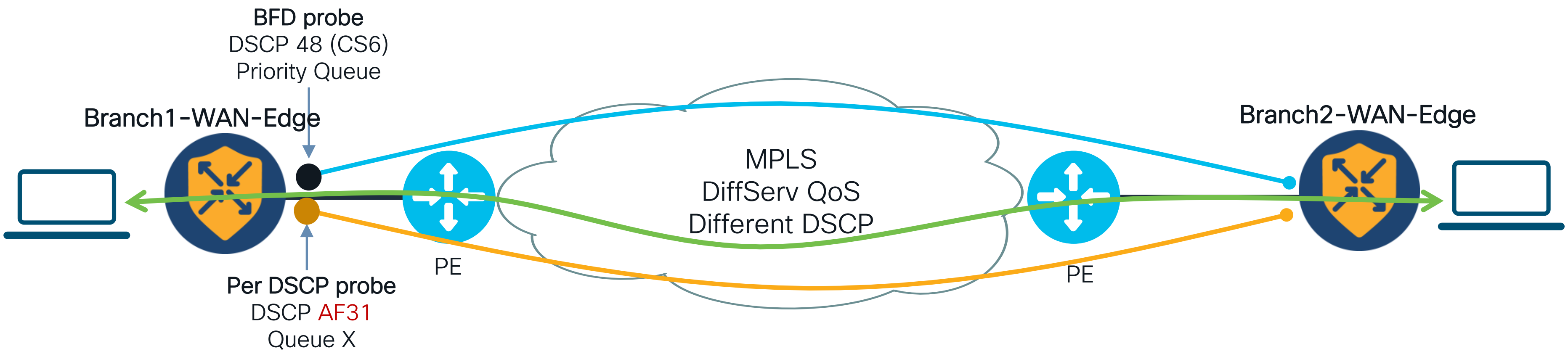


SLA metrics which are calculated by BFD probes are sent on priority queue marked as DSCP 48 (CS6)

Data Traffic (depending on Application class) can potentially go out with different DSCP values thereby getting a different treatment in underlay network

For better performance of traffic, more accurate result of loss, latency and jitter is desired to direct right traffic to go out on right tunnel

Solution: Per-Class App Aware Routing



Continue to measure Liveliness of Tunnel by sending BFD probes on default DSCP 48 marking

Send Probe with Custom DSCP marking to measure real treatment of packet in SP network

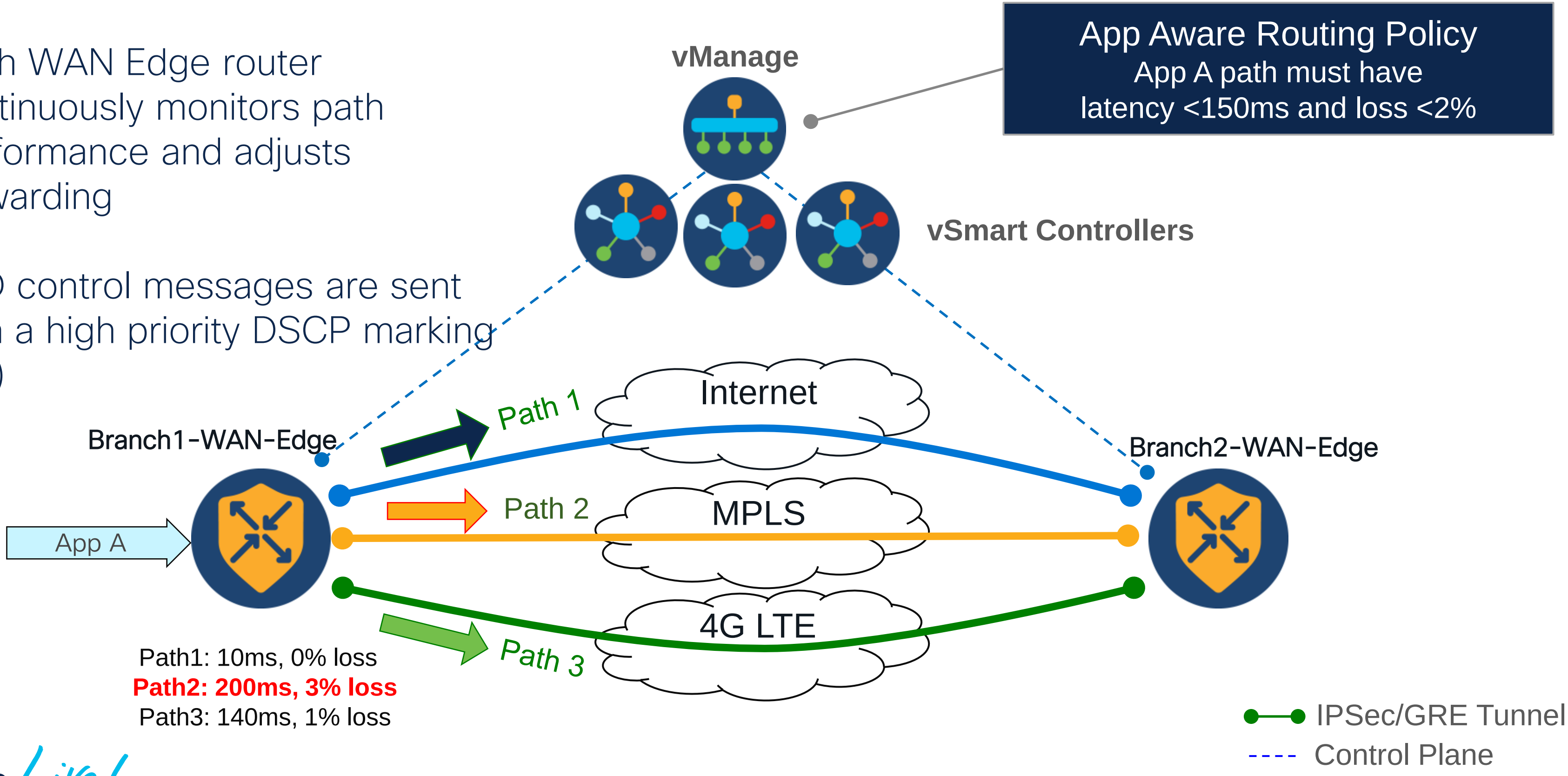
Send Probe out on user defined queues for different class of traffic

Provides option to change default marking of DSCP probes

Use case - Application Aware Routing

- Each WAN Edge router continuously monitors path performance and adjusts forwarding

- BFD control messages are sent with a high priority DSCP marking (48)

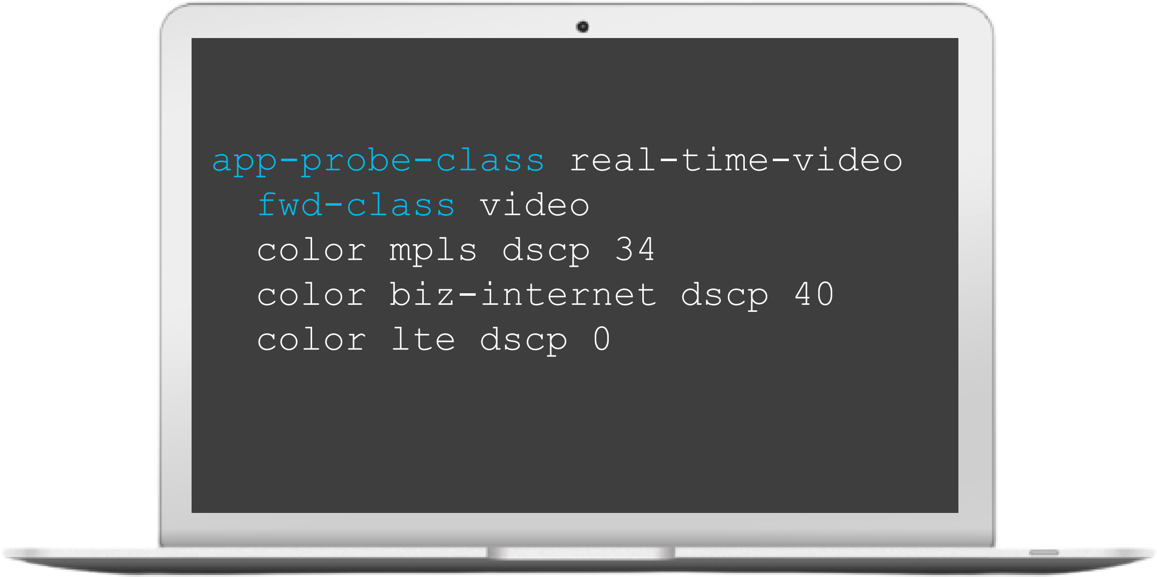


App Aware Routing Policy
App A path must have
latency <150ms and loss <2%

Path1: 10ms, 0% loss
Path2: 200ms, 3% loss
Path3: 140ms, 1% loss

Application probe class (app-probe-class)

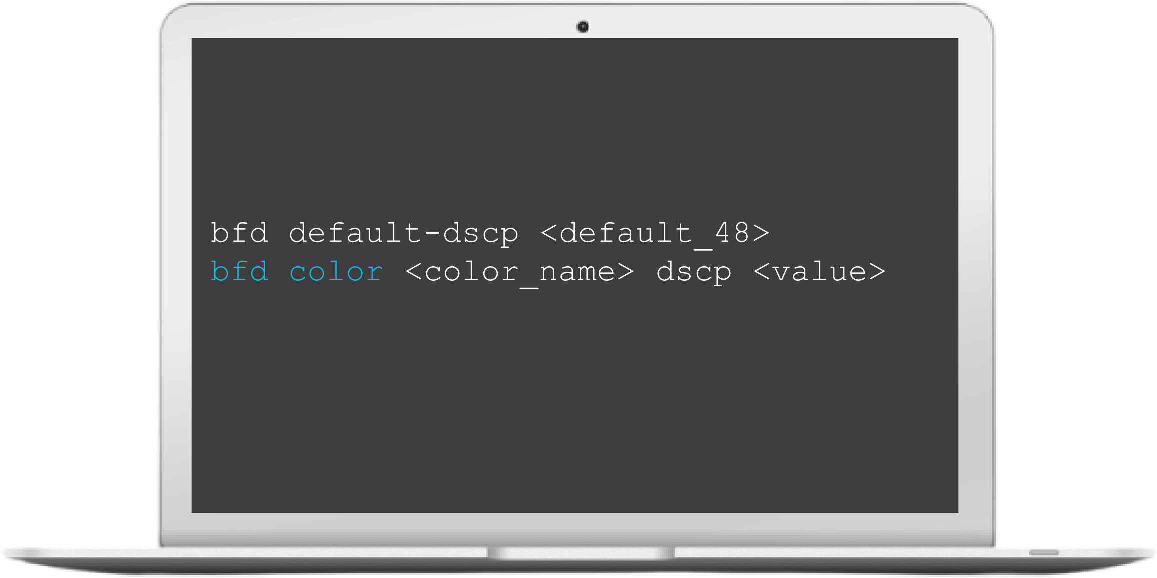
- App-probe-class
  - a forwarding class - determine the QoS queue in which the BFD echo request will be queued at the egress tunnel port
  - and a tuple of two items- color, dscp.
- This defines the marking per color that a particular class of applications will be forwarded on.



```
app-probe-class real-time-video
  fwd-class video
  color mpls dscp 34
  color biz-internet dscp 40
  color lte dscp 0
```

BFD Default Change

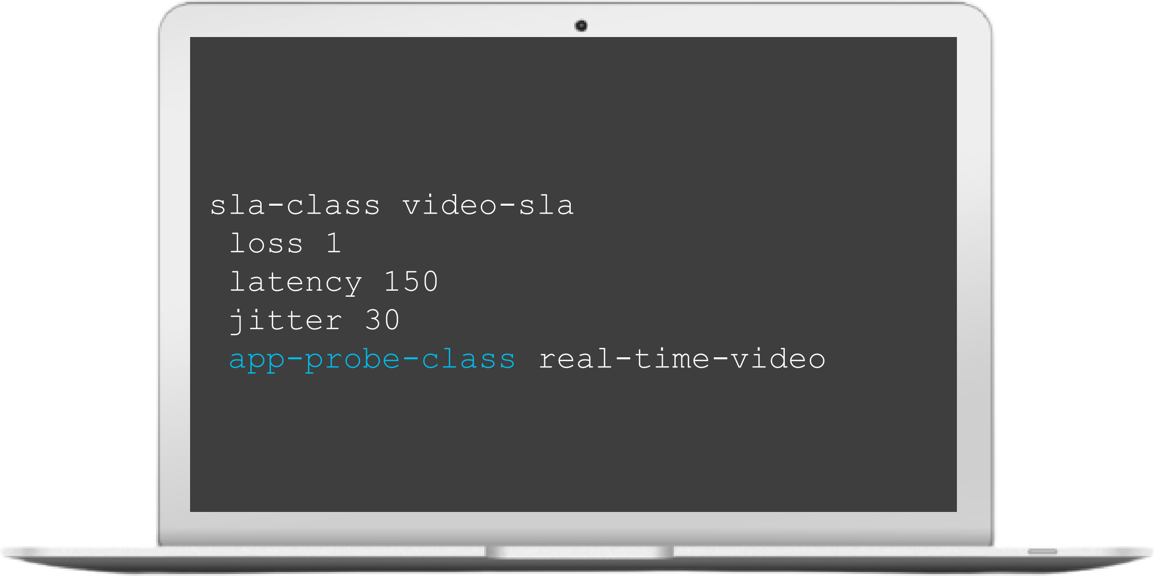
- The default bfd DSCP value is 48.
- User can change this value along with the option to configure this on a per color level.



```
bfd default-dscp <default_48>
bfd color <color_name> dscp <value>
```

SLA Class

- The application forwarding classes are referred to in the **sla-class**.
- This maps the metric thresholds for the applications with the app-probe-class.
- Only one app-probe-class can be configured



```
sla-class video-sla
 loss 1
 latency 150
 jitter 30
 app-probe-class real-time-video
```

Gotcha's

BFD Echo Response

BFD Echo Response packet is still marked as default DSCP

BFD Echo Request

Only BFD Echo Request packet is sent with Custom DSCP App probe marking

App Probe Class

Only one App probe class is mapped to SLA class

Default DSCP

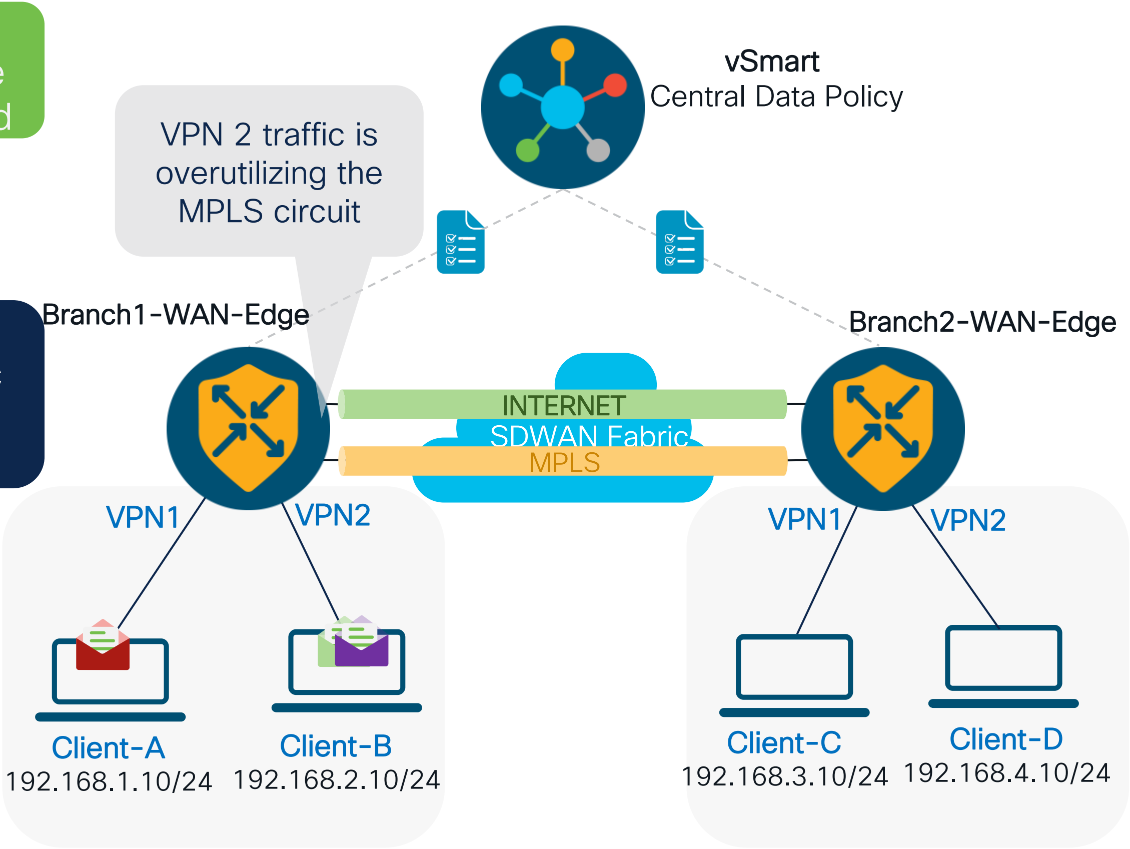
The Default DSCP class packets still gets queued to priority queue

Per VPN QOS

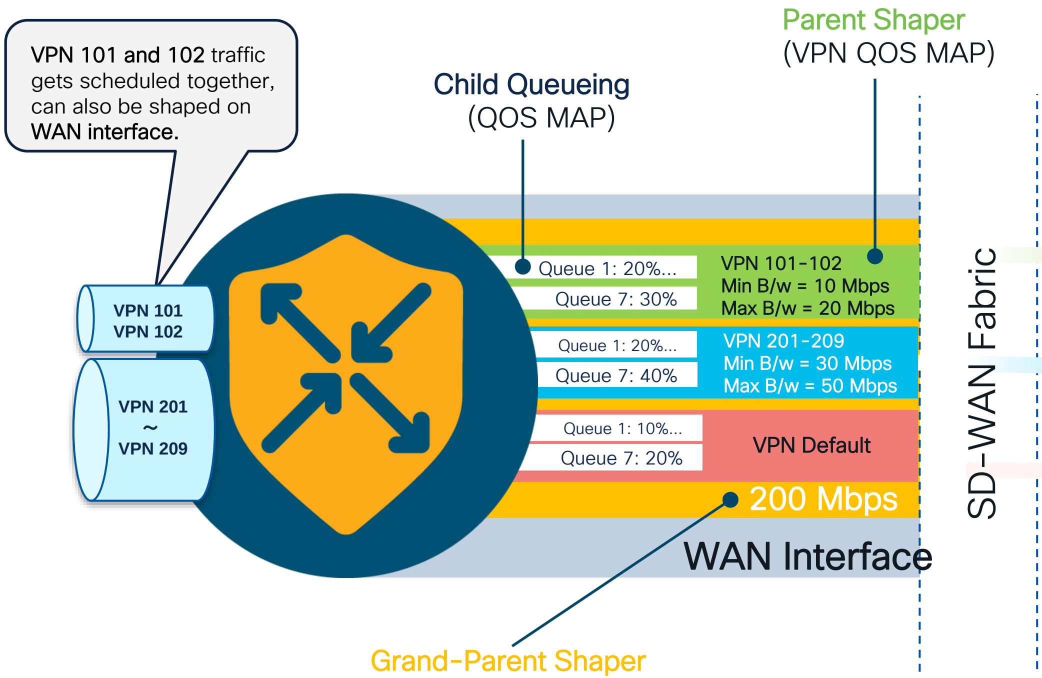
Scenario 1b:Packet flow from Service VPN to Overlay

1st issue of Application Probe Class got resolved

Business Critical Application traffic is STILL not performing well



Per-VPN QOS working



VPN-101-102

Min Guaranteed Bandwidth of 10Mbps
Max Bandwidth Shaped to 20Mbps

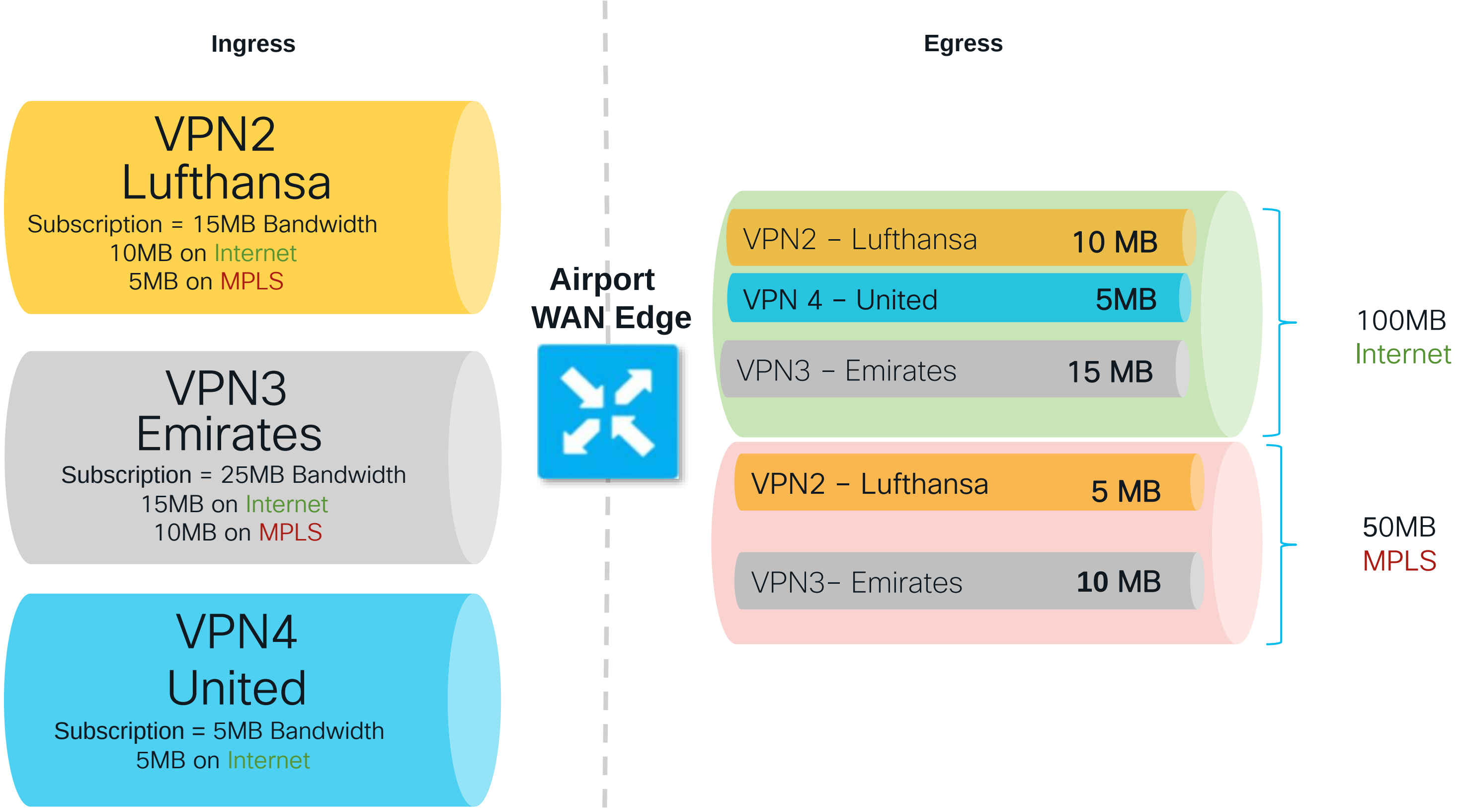
VPN 201-209

Min Guaranteed Bandwidth of 30Mbps
Max Bandwidth Shaped to 50Mbps

Default VPN

Minimum Guaranteed and Maximum Shaper is calculated from remaining Bandwidth

Use Case



Ingress

VPN2
Lufthansa
Subscription = 15MB Bandwidth
10MB on Internet
5MB on MPLS

VPN3
Emirates
Subscription = 25MB Bandwidth
15MB on Internet
10MB on MPLS

VPN4
United
Subscription = 5MB Bandwidth
5MB on Internet

Airport WAN Edge

Egress

VPN2 – Lufthansa **10 MB**
VPN 4 – United **5MB**
VPN3 – Emirates **15 MB**

100MB
Internet

VPN2 – Lufthansa **5 MB**
VPN3– Emirates **10 MB**

50MB
MPLS

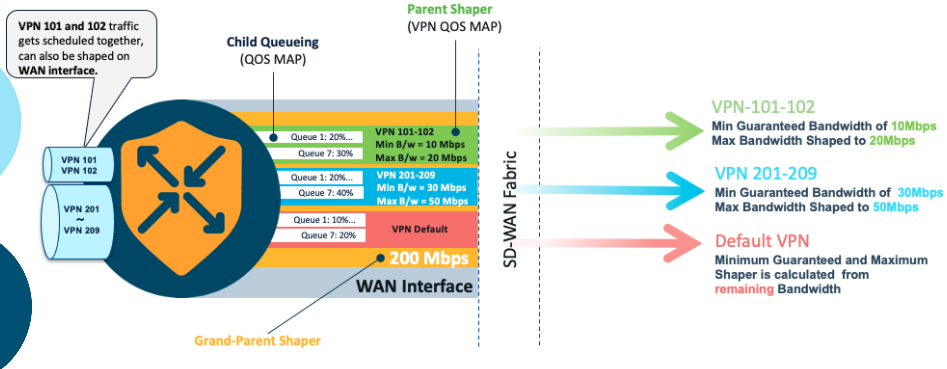
Per VPN QOS - model

Based on 3 Level Hierarchy

Provides differentiated level of QOS service on per VPN basis

Provides Capability to regulate throughput ratio on per VPN basis

Greedy VPN is limited to outbound bandwidth usage, hence avoids hogging of WAN resource for other VPNs



VPN-101-102
Min Guaranteed Bandwidth of 10Mbps
Max Bandwidth Shaped to 20Mbps

VPN 201-209
Min Guaranteed Bandwidth of 30Mbps
Max Bandwidth Shaped to 50Mbps

Default VPN
Minimum Guaranteed and Maximum Shaper is calculated from remaining Bandwidth

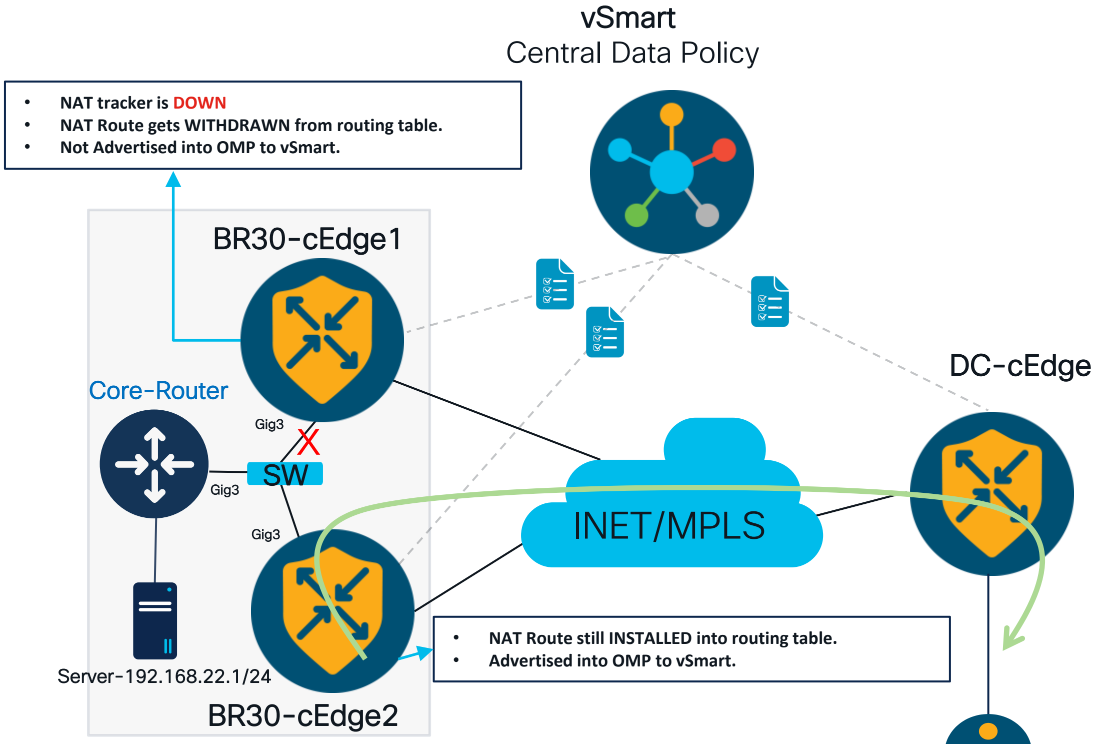
Service-VPN NAT Tracker

Service VPN NAT Tracker

Use Case

- In a HA deployment scenario, where two SD-WAN edge routers, advertise the same NAT OMP route, currently if a NAT source IP is not reachable, NAT route is still advertised into OMP causing the traffic coming from the other site to blackhole.

- NAT traffic fails to get routed through other router in the event of LAN failure.

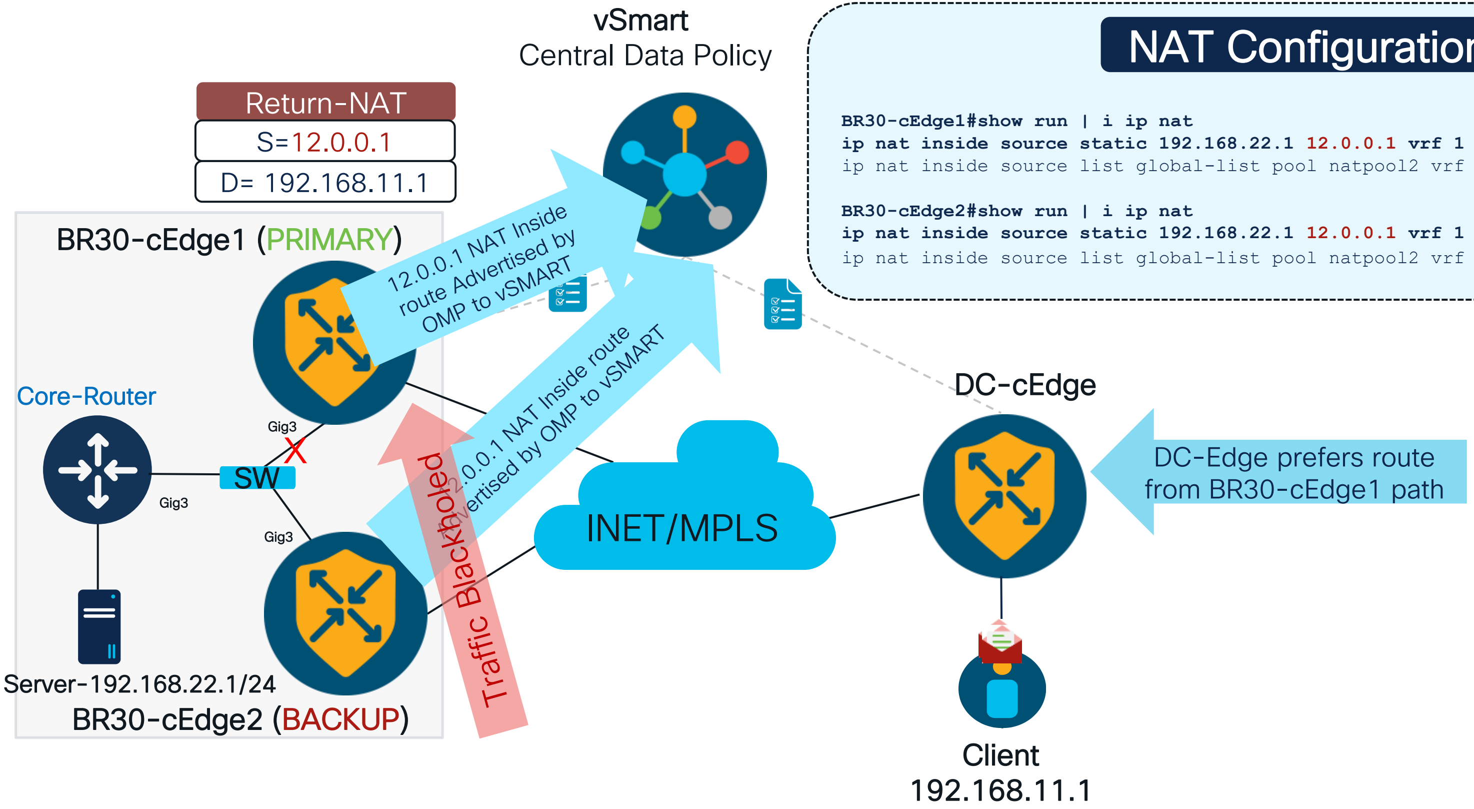


- NAT tracker is DOWN
- NAT Route gets WITHDRAWN from routing table.
- Not Advertised into OMP to vSmart.

- NAT Route still INSTALLED into routing table.
- Advertised into OMP to vSmart.

```
ip nat inside source static 192.168.22.1 12.0.0.1 vrf 1 match-in-vrf track 1
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf overload track 1
```

Use Case 2a- Scenario WITHOUT NAT tracker

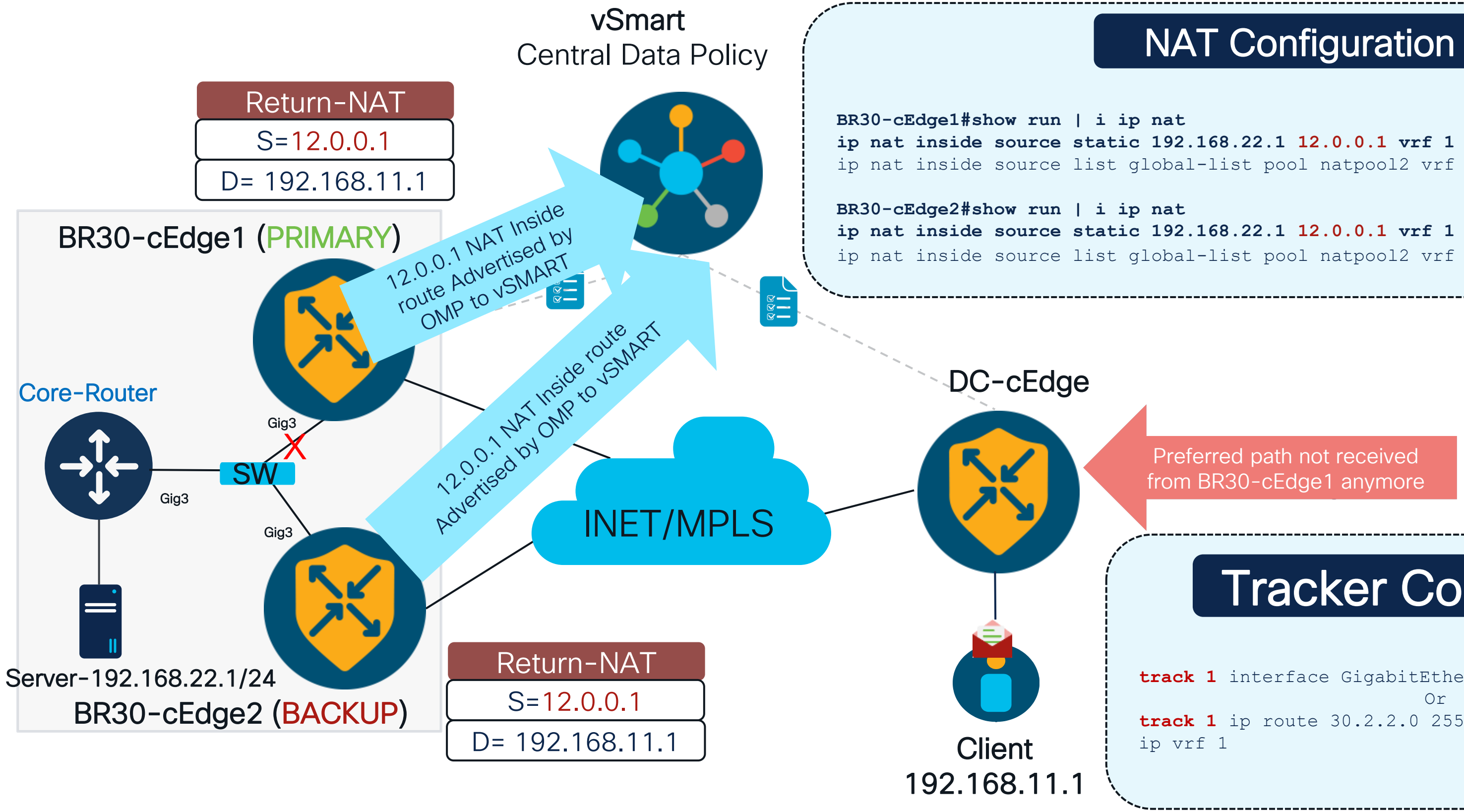


NAT Configuration

```
BR30-cEdge1#show run | i ip nat
ip nat inside source static 192.168.22.1 12.0.0.1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf overload

BR30-cEdge2#show run | i ip nat
ip nat inside source static 192.168.22.1 12.0.0.1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf overload
```

Use Case 2b : Scenario WITH NAT tracker



Preferred path not received from BR30-cEdge1 anymore

NAT Configuration

```
BR30-cEdge1#show run | i ip nat
ip nat inside source static 192.168.22.1 12.0.0.1 vrf 1 match-in-vrf track 1
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf overload

BR30-cEdge2#show run | i ip nat
ip nat inside source static 192.168.22.1 12.0.0.1 vrf 1 match-in-vrf track 1
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf overload
```

Tracker Configuration

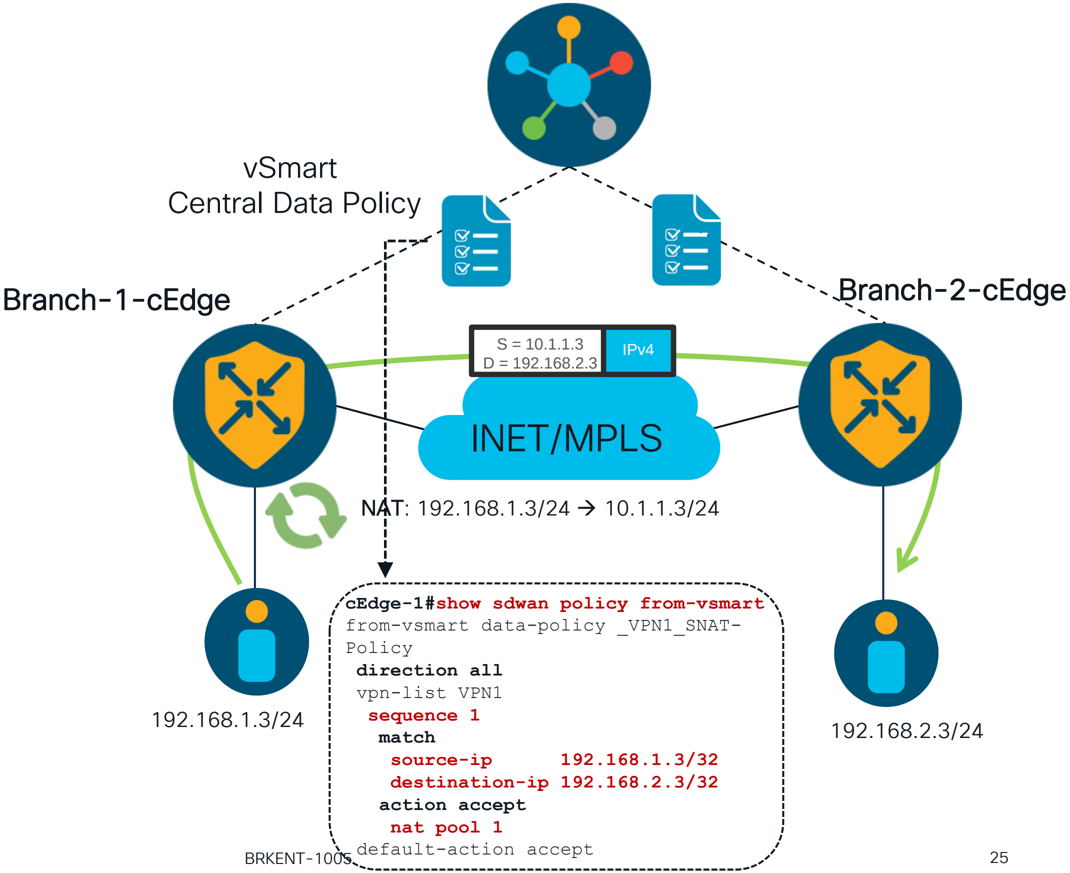
```
track 1 interface GigabitEthernet3 line-protocol
                            Or
track 1 ip route 30.2.2.0 255.255.255.0 reachability
ip vrf 1
```

Service-side NAT with Data-policy

Static NAT with Data-policy

Use Case

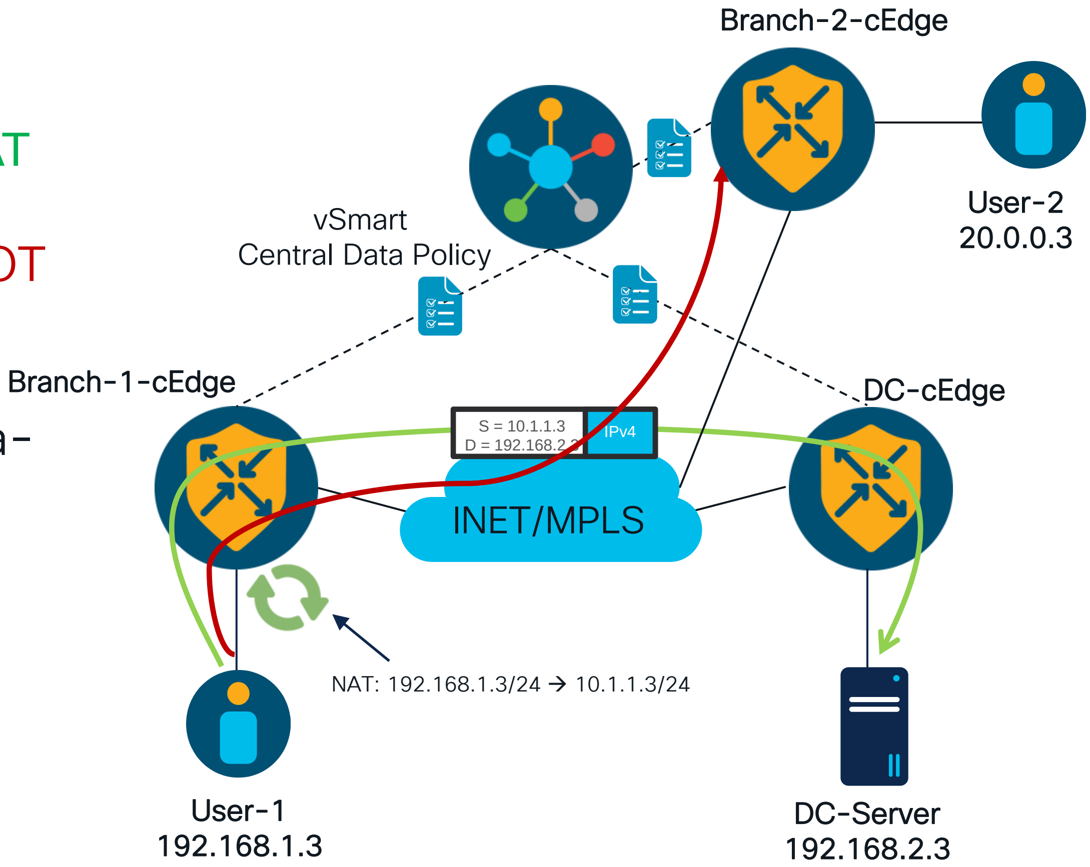
Service-Side Static NAT functionality was introduced to allow the branches using overlapping ip addresses in the respective Service VPNs. This is required in the cases like Acquisition. The Initial version didn't support the Static NAT functionality along with the flexibility of Data-policy.



```
cEdge-1#show sdwan policy from-vsmart
from-vsmart data-policy _VPN1_SNAT-
Policy
 direction all
 vpn-list VPN1
  sequence 1
   match
    source-ip      192.168.1.3/32
    destination-ip 192.168.2.3/32
   action accept
    nat pool 1
 default-action accept
```

Use case

- User-1→DC Server : Should NAT
- User1→User-2 : Should NOT NAT
- Match and Set condition of Data-policy is utilized to fulfil the NAT requirement as per use-case.

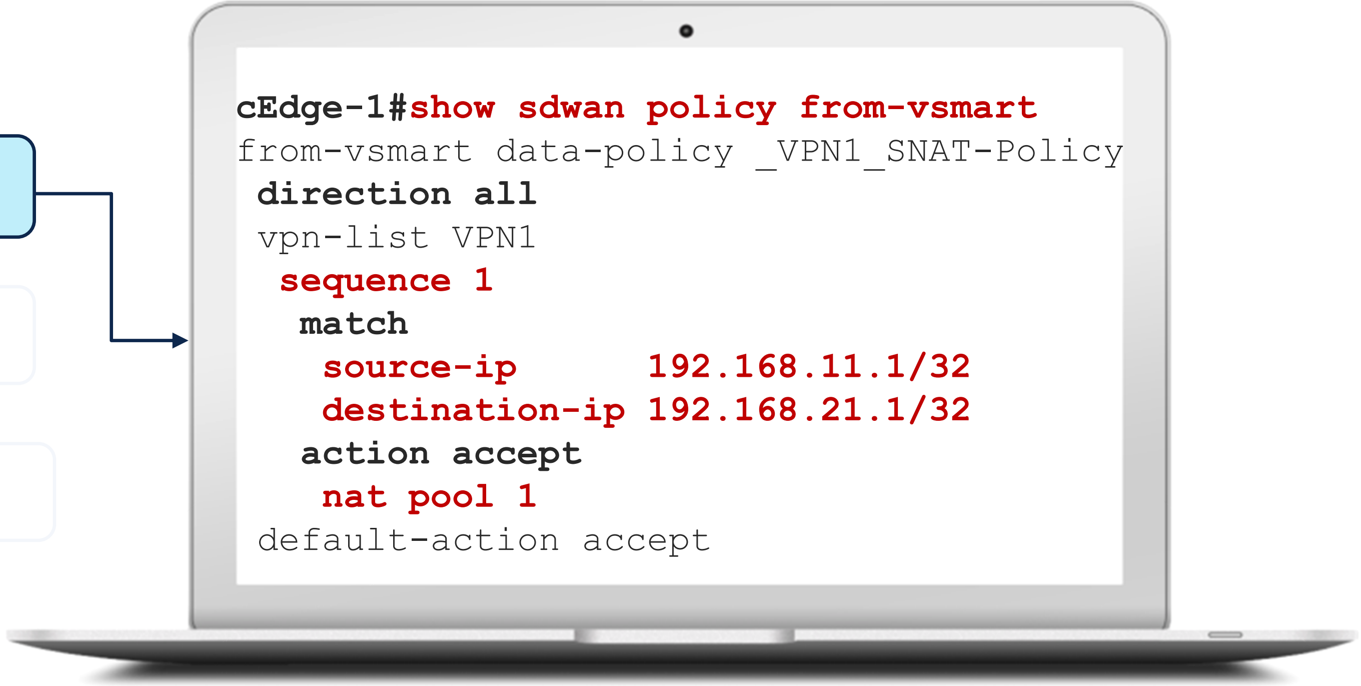


CLI configuration workflow: **Step 1**

Verify Data-Policy

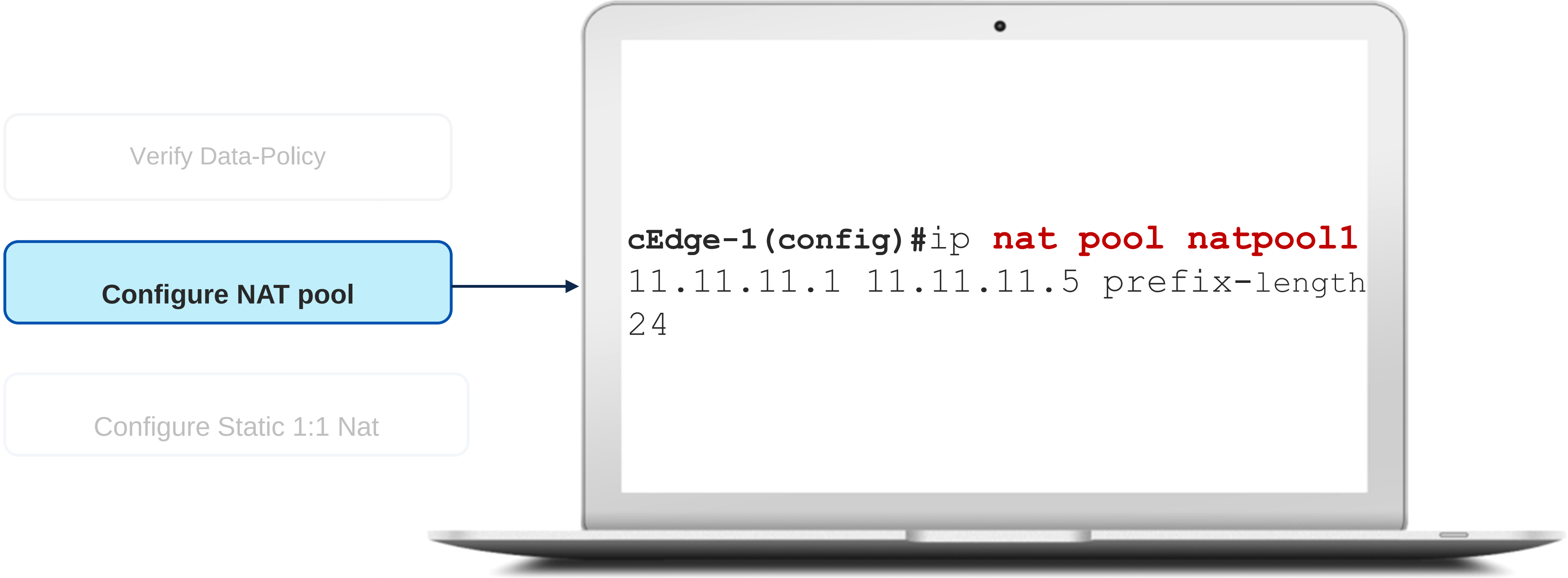
Configure NAT pool

Configure Static 1:1 Nat



```
cEdge-1#show sdwan policy from-vsmart
from-vsmart data-policy _VPN1_SNAT-Policy
 direction all
 vpn-list VPN1
  sequence 1
   match
    source-ip      192.168.11.1/32
    destination-ip 192.168.21.1/32
   action accept
    nat pool 1
 default-action accept
```

CLI configuration workflow: **Step 2**



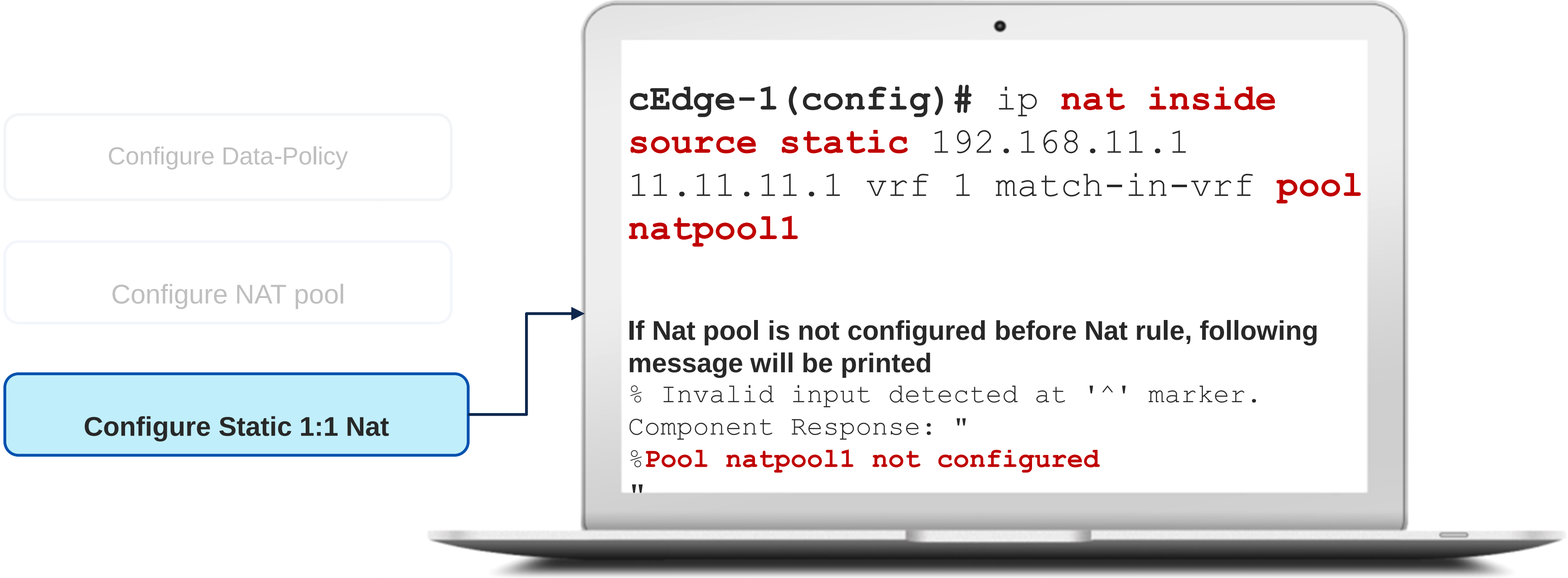
Verify Data-Policy

Configure NAT pool

Configure Static 1:1 Nat

```
cEdge-1(config)#ip nat pool natpool1
11.11.11.1 11.11.11.5 prefix-length
24
```

CLI configuration workflow: **Step 3**



Configure Data-Policy

Configure NAT pool

Configure Static 1:1 Nat

```
cEdge-1(config)# ip nat inside
source static 192.168.11.1
11.11.11.1 vrf 1 match-in-vrf pool
natpool1
```

If Nat pool is not configured before Nat rule, following message will be printed

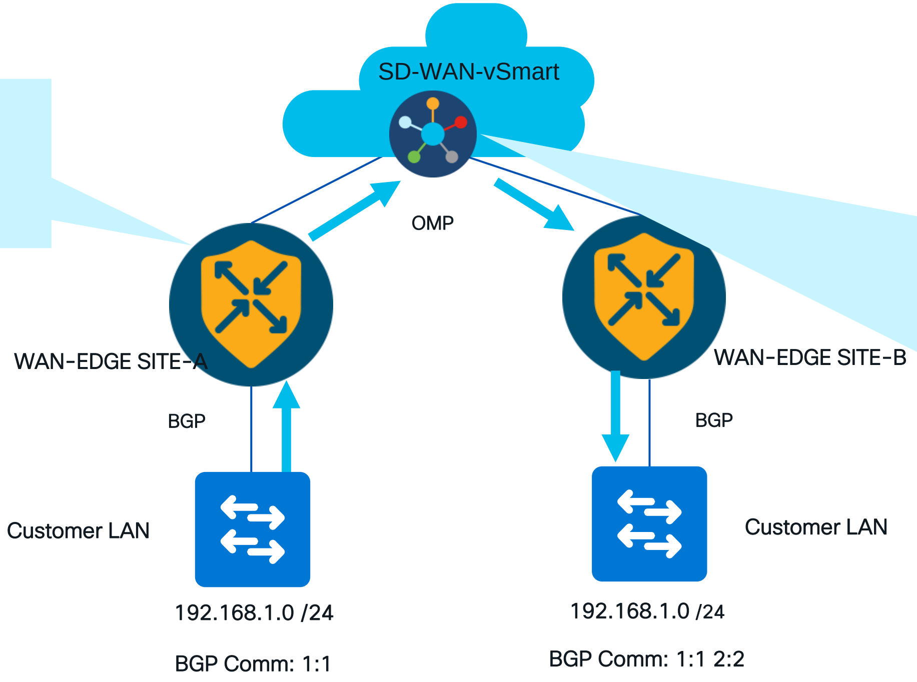
```
% Invalid input detected at '^' marker.
Component Response: "
%Pool natpool1 not configured
"
```

BGP community propagation into OMP

BGP community Propagation into OMP

```
route-map BGP-to-omp permit 100
 match community list COMM-1:1
 set community 2:2 additive
```

GUI support for local policy



```
policy
 lists
  site-list test-site-list
    site-id 500
  !
  community-list COM-1:1
   community 0:1234
   community 1:1
 !
control-policy test-policy
  sequence 1
   match route
    community-list COM-1:1
   !
   action accept
    set
     preference 1500
     community 2:2
      additive
    !
   !
  !
  default-action accept
!
  apply-policy
 site-list test-site-list
  control-policy test-policy out
 !
!
```

GUI support for central policy

Gotchas

- Central policy support for matching community and configuring policies
- GUI support for central policy
  - Standard community list
  - Expanded community list
  - Additive support
- GUI support for local policy
  - Expanded list only with variable support
  - Route-map under VPN template during BGP to OMP redistribution

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!

- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.

- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

#CiscoLive

cisco Live!

#CiscoLive