
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Designing seamless integration between Campus BGP EVPN and External Domains

Travis Jones - System Architect
CCIE #4603 DC, SP, R&S, Security & Voice
CCDE 2013::60

BRKENS-2050

Cisco Webex App

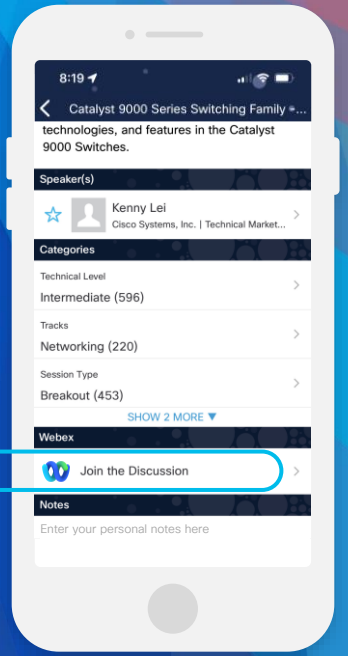
Questions?

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

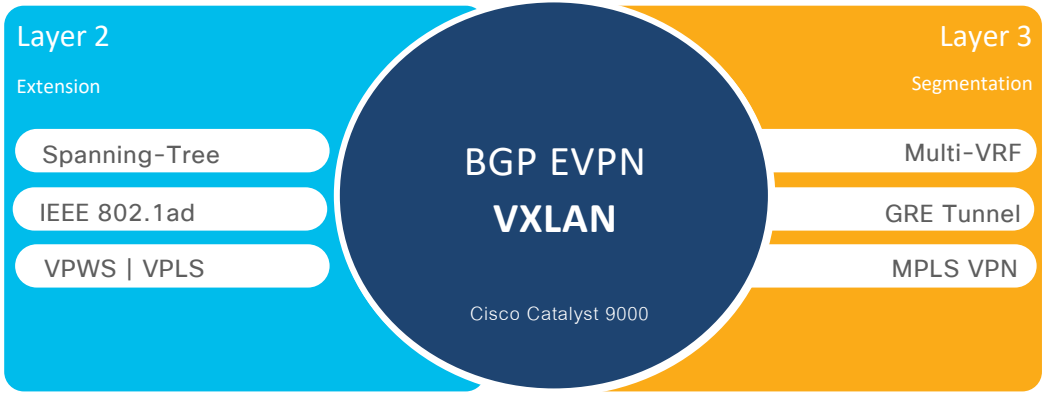
Webex spaces will be moderated by the speaker until June 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2050

Agenda

- Introduction
- Enterprise EVPN Reference Architecture
- External Fabric Domain Hand-off
  Terminate | Interworking | Re-Originate
- Layer-2 External Domain Handoff
- Layer-3 External Domain Handoff
- Border Network Extensions
- Catalyst 9000 EVPN Reference



EVPN Evolution

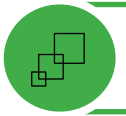
- **Product transition drives architecture transitions**
- **Convergence of traditional L2 overlay to simplified and scalable fabric**
- **Transition classic L3 overlays to enterprise-grade scalable fabric**
- **Unified end-to-end common fabric architecture reducing cost and complexity**

Enterprise Campus BGP EVPN Drivers

Industry Standard

One Fabric Architecture

Proven and Scalable



Hierarchical Fabric Domain

Flexible Overlay

Multi-vendor IT strategy

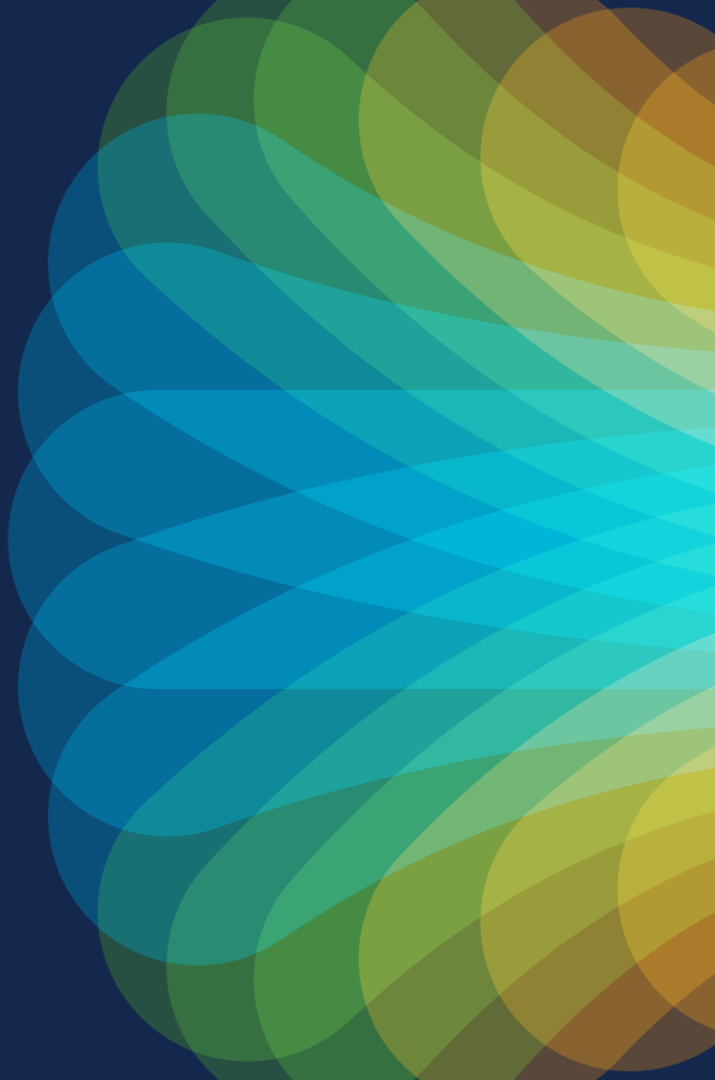
Unified operation across – Campus | DC | WAN

BGP Protocol History. Minimum new learning curve

Multi-tier Overlay network architecture

Use-case driven customize Overlay networks Types and Topologies

Enterprise EVPN Reference Architecture



cisco Live!

BGP EVPN System Role

BORDER-GATEWAY:
A gateway point between two or more BGP EVPN administrative domain boundary.

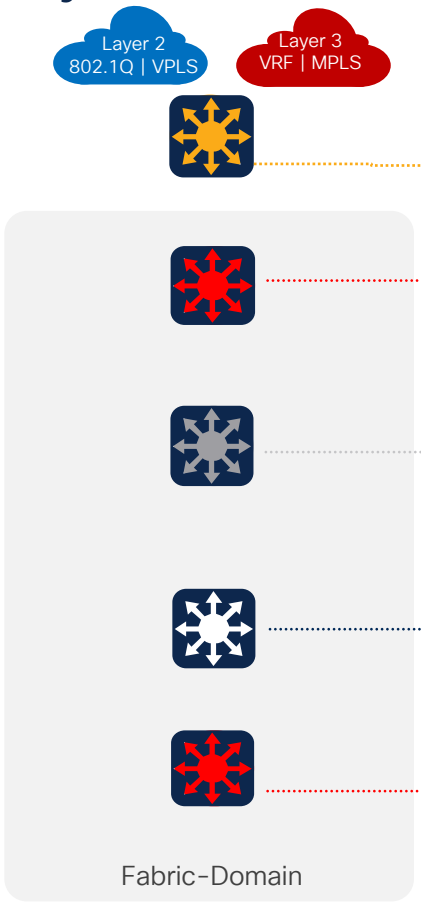
BORDER :
A gateway point between EVPN fabric and external network domain.

INTERMEDIATE :
A Layer 2 or Layer 3 (IP/MPLS) Underlay network system providing basic transport and forwarding plane.

SPINE :
Reflects the L2/L3 VPN BGP prefixes providing hierarchical neighbor peering, learning and distribution point.

VTEP (LEAF) :
An origination and termination point of VXLAN enabled overlay network.

* - Roadmap
★ - Recommended



Catalyst EVPN Scale and Performance Matrix

Cisco Catalyst BGP EVPN Configuration Guide
Scale and Performance Chapter

System Support	Mode
Nexus 9000	Standalone

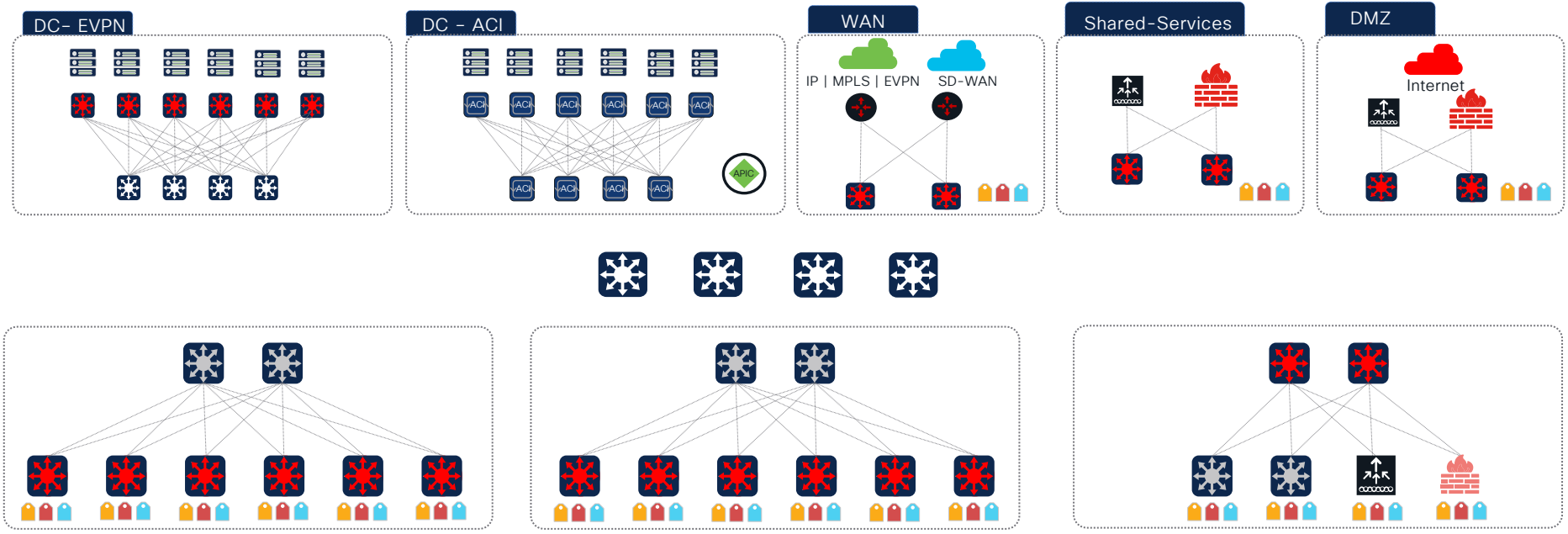
System Support	Mode
Catalyst 9300 – 9600 (9500-H/X/9600/X)	Standalone | Stack ★
Catalyst 8000 Edge | ASR 1000	Physical
Nexus 9000	Standalone
ASR 9000	Standalone

System Support	Mode
Any	Any

System Support	Mode
Catalyst 9300 – 9600 (9500-H/X & 9600/X)	Standalone | Stack
Catalyst 8000 Edge | ASR 1000	Physical | Virtual
Nexus 9000	Standalone
ASR 9000	Standalone

System Support	Mode
Catalyst 9300L | 9300 | 9300X Series	Standalone | StackWise ★
Catalyst 9400 | 9400X Series	Standalone | StackWise-Virtual ★
Catalyst 9500 | 9500X Series	Standalone | StackWise-Virtual ★
Catalyst 9600 | 9600X Series	Standalone | StackWise-Virtual ★

Enterprise BGP EVPN Reference Architecture



Industry Standard
- Standard-based Fabric
- Multi-vendor interoperable
- Broad innovation adoption

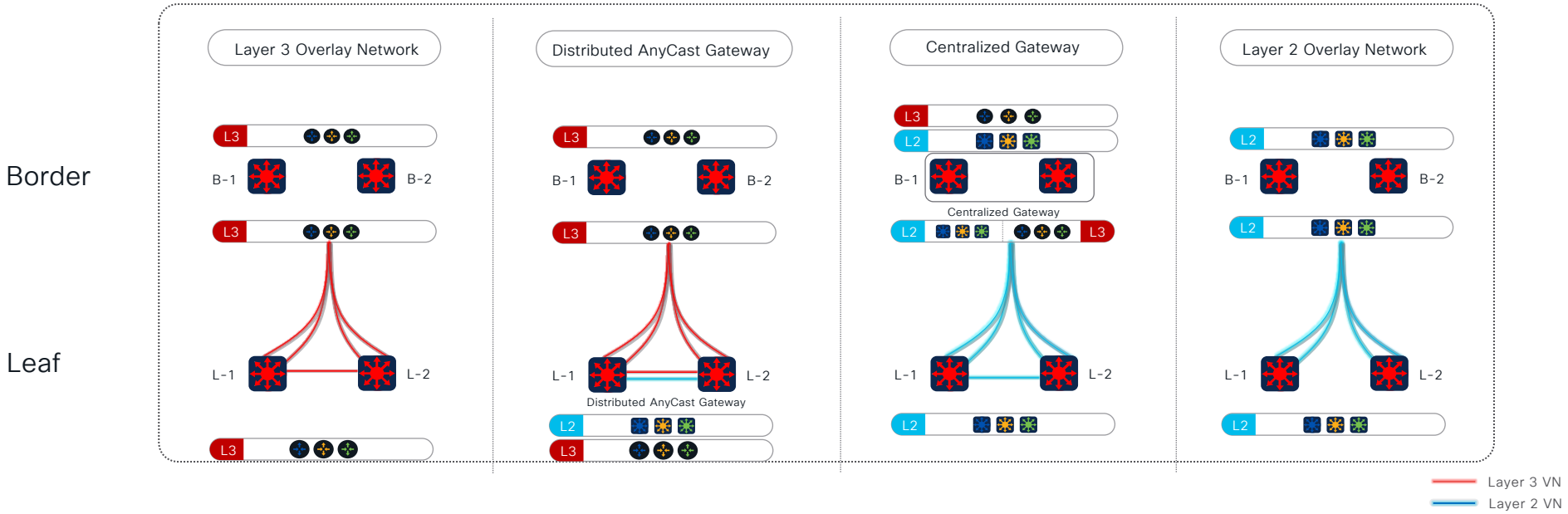
Unified Fabric
- Cross-PIN single fabric
- Extensible beyond site
- Simplified Management

Proven
- Reliable control-plane
- Multi-protocol capabilities
- Less new learning-curve

Hierarchical
- Non-blocking architecture
- Structured & Scalable fabric
- Hybrid system role support

Flexible
- Complex network solution
- Tailored L2/L3 overlays
- Deep eco-system integration

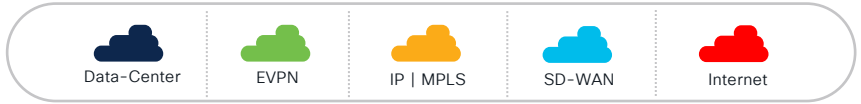
Border – BGP EVPN Overlay Network Types



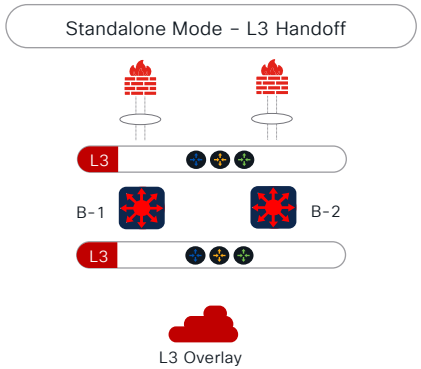
Flexible Overlays

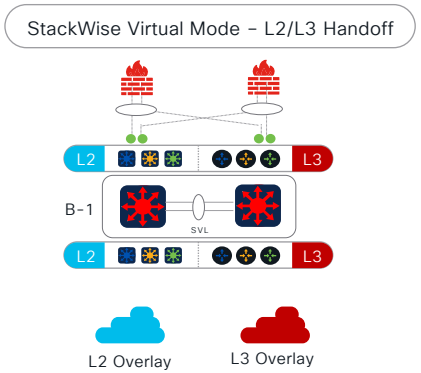
- Flexible Routing and Bridging overlay network support
- Unique overlay Layer 3 or Layer 2 forwarding network to address key use-cases
- Tailored L2/L3 network boundary point at Border and Leaf
- Seamless Layer 2 and 3 network handoff external domains

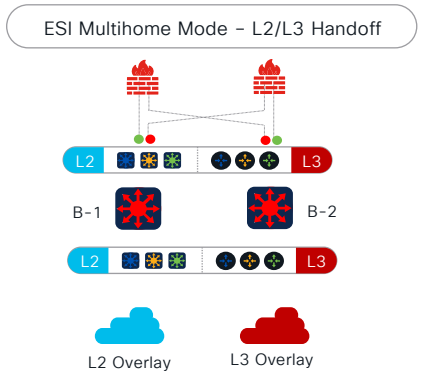
Border – Catalyst 9000 System Modes



Border







Forwarding VLAN
Blocking VLAN

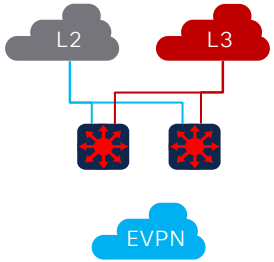
Route First rule.
Bridge-only – IF and where needed
Borders in individual Standalone mode
Seamless Layer 3 handoff

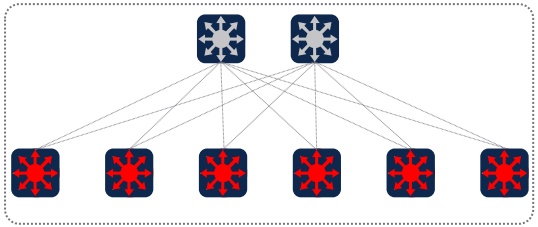
Layer 2 bridging beyond fabric.
Borders in StackWise Virtual mode
Loop-free L2 and overlay fabric
Flexible Layer 2 and 3 handoff

Layer 2 bridging beyond fabric
Standard-based EVPN ESI support
Per-VLAN auto load-balancing
Loop-free L2 and overlay fabric

External Domain Handoff Types

Terminate





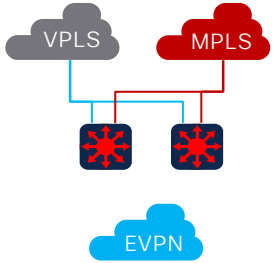
BGP EVPN fabric termination at Border

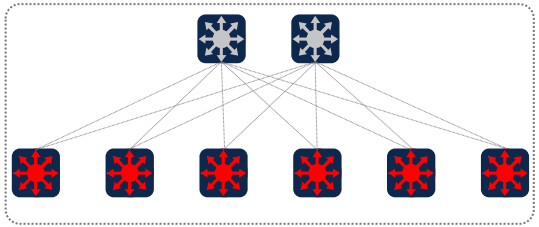
Simple Layer 2 / Layer 3 handoff

Layer 3 VRF segmentation to L3 system

L2 extension handoff, only if needed.

Interworking





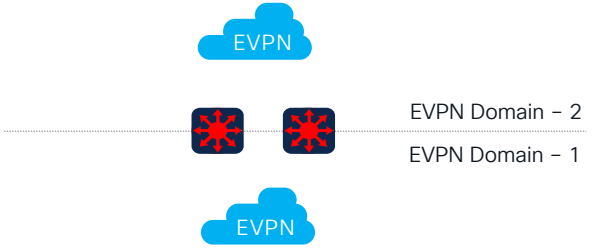
Integrated fabric interworking at Border

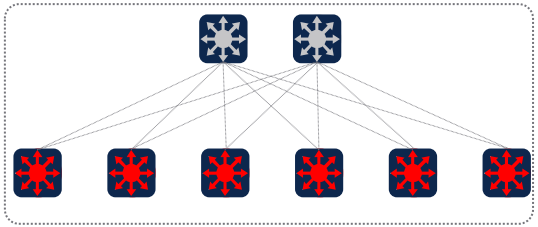
Seamless EVPN & classic overlay ”stitching”

End-to-End network segmentation

Loop-free Layer 2 overlays across domains

Re-Originate





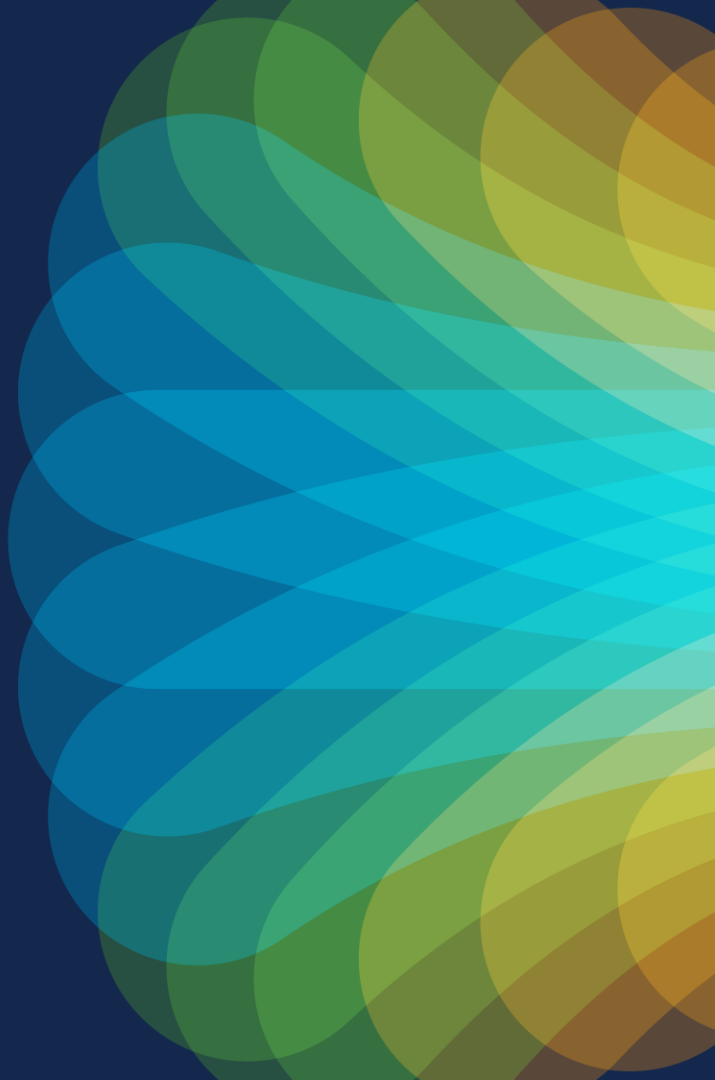
BGP EVPN fabric re-origination at Border

L3 segmentation between fabric domains

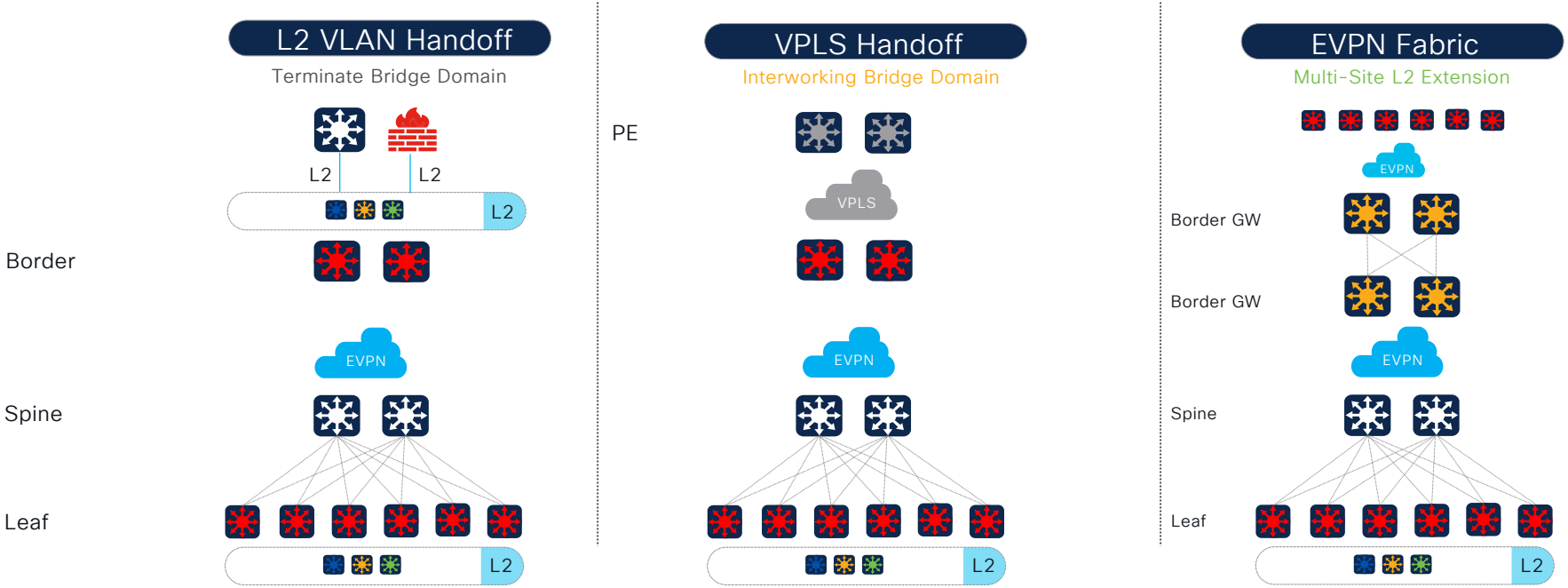
Can collapse with Border/Spine role

L2 and Multicast in overlay unsupported

Layer 2 – External Domain Handoff Types



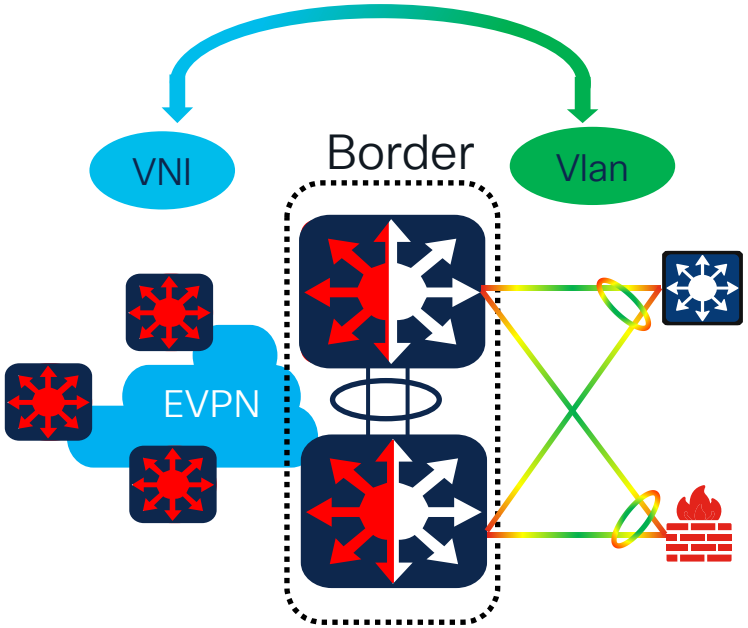
Layer – 2 Handoffs Alternatives



Seamless Layer 2 Handoff

- Multiple end-to-end seamless Layer 2 extensions supports across fabric and beyond
- Terminate L2 overlays and perform simple Layer 2 trunk handoff to non-fabric devices, i.e., Firewalls
- Integrated EVPN Border and VPLS PE function to extend multi-domain L2 for seamless migrations
- Extendable Layer 2 EVPN domains with highly scalable Catalyst and Nexus 9000 Multisite Border Gateway

L2 VLAN Handoff (Terminate)




```
vlan configuration 101
member evpn-instance 101 vni 10101
!
vlan configuration 102
member evpn-instance 102 vni 10201
!
interface GigabitEthernet 1/0/1
switchport mode trunk
switchport allowed vlan 101,102
!
interface nve1
no ip address
source-interface Loopback0
host-reachability protocol bgp
member vni 10101 mcast-group 225.0.0.101
member vni 10102 mcast-group 225.0.0.101
!
```

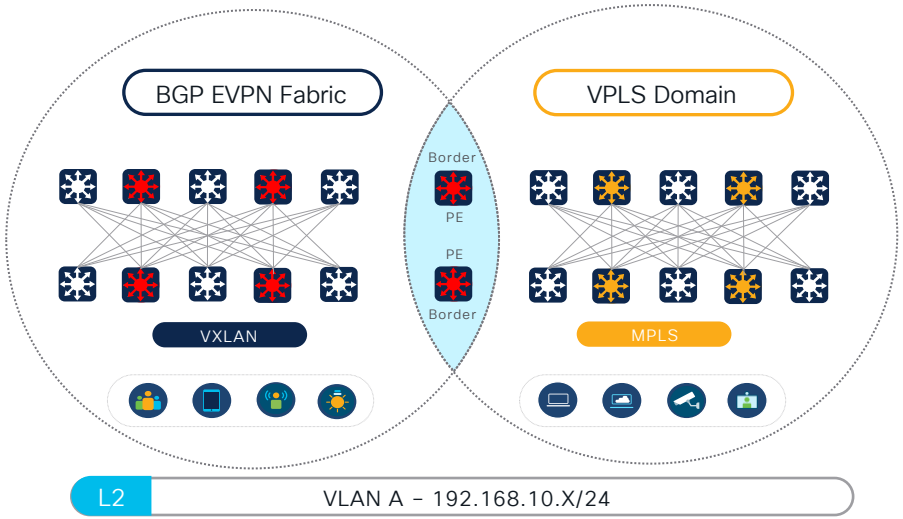
Transparent Handoff

Loop-free Traditional Network. Loop-free Fabric.

Cisco StackWise Virtual with unified system simplifies Layer 2 interworking between EVPN L2 VNI and traditional Layer 2 VLAN based networks

Layer 2 Multi-home with All-Active supporting per-flow load-sharing and best-in-class redundancy

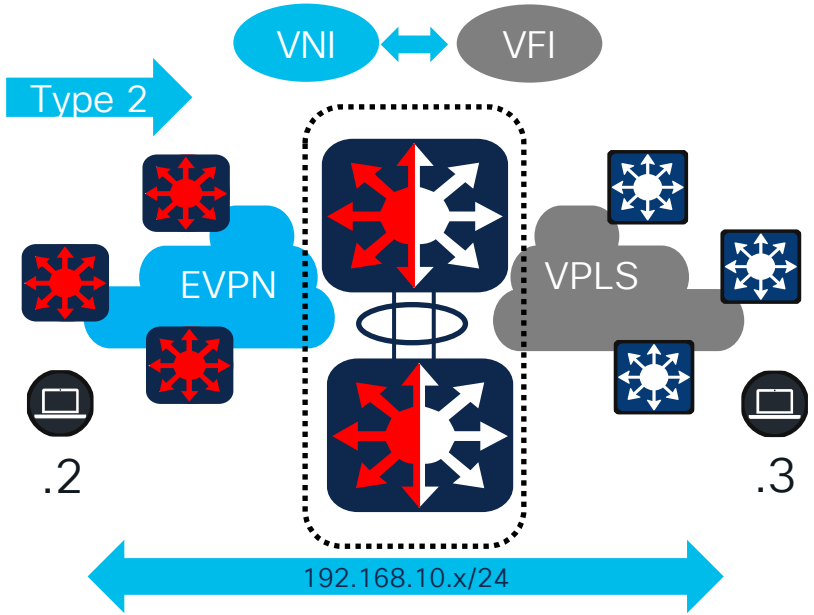
Interdomain L2 Extensions (Interworking)



Flexible Layer 2 Interworking

- Seamless VPLS to BGP EVPN VXLAN Layer 2 interworking function
- Two Catalyst 9000 Border design alternatives –
  - Shared Border/PE with integrated BGP EVPN and VPLS interworking
  - Dedicated Border with Layer 2 VLAN handoff to remote VPLS PE system
- Flexible Bridging-only, integrated Routed and Bridging interworking between EVPN and VPLS domains

L2 VPLS Handoff (Interworking)

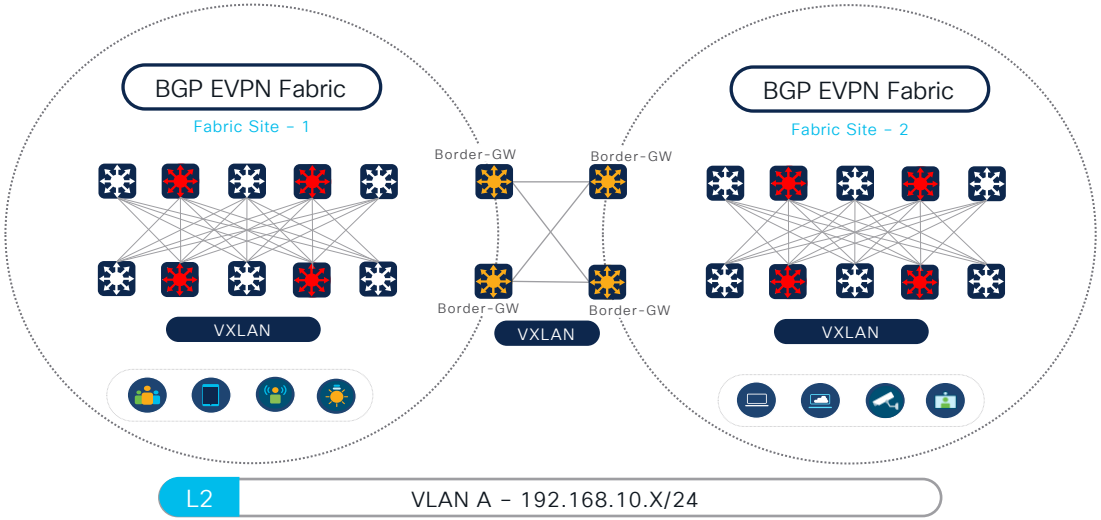



```
l2vpn vfi context VPLS-VFI
vpn id 1
member 10.12.12.5 encapsulation mpls
!
vlan configuration 11
member access-vfi VPLS-VFI
member evpn-instance 1 vni 6000
!
```

Intuitive Interworking

- Simplified command-line syntax to “stitch” bridge-domain between VPLS VFI and BGP EVPN VXLAN EVI
- Loop-free Layer 2 domains with two Catalyst 9000 Border System mode alternatives –
  - Cisco StackWise Virtual - Loop-free, all-active VFI to EVI mappings supporting best-in-class inter-domain load-sharing and redundancy
  - Standalone – Loop-free, automatic per VFI to EVI active/standby forwarding between two individual Border/PE systems

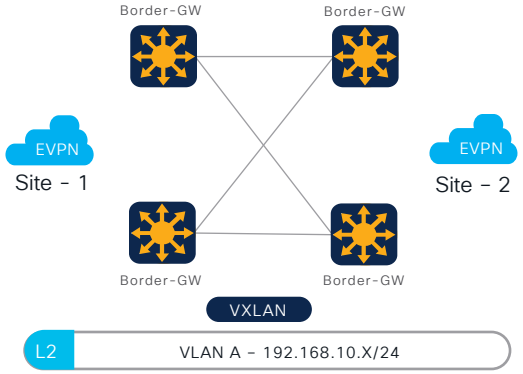
Multisite EVPN L2 Extensions (Re-Originate)



Hierarchical Layer 2 Architecture

- Structured and hierarchical end-to-end Layer 2 overlay network architecture
- Nexus 9K Multisite – Across geographic locations or sub-divided single large site
- Multisite EVPN fabric domains reduce fault-domain size with multi-tier broadcast control management
- Termination and re-origination for each Layer 2 overlay segments at Nexus 9K Border-Gateway

Multisite EVPN L2 Extensions (Re-Originate)



NXOS - BGW

```
vlan 2
!
evpn
 vni 2000002 l2
!
evpn multisite border-gateway 100
 split-horizon per-site
!
interface nve1
  multisite border-gateway interface loopback2
  member vni 2000002
   multisite ingress-replication
     mcast-group 225.1.0.1
!
```

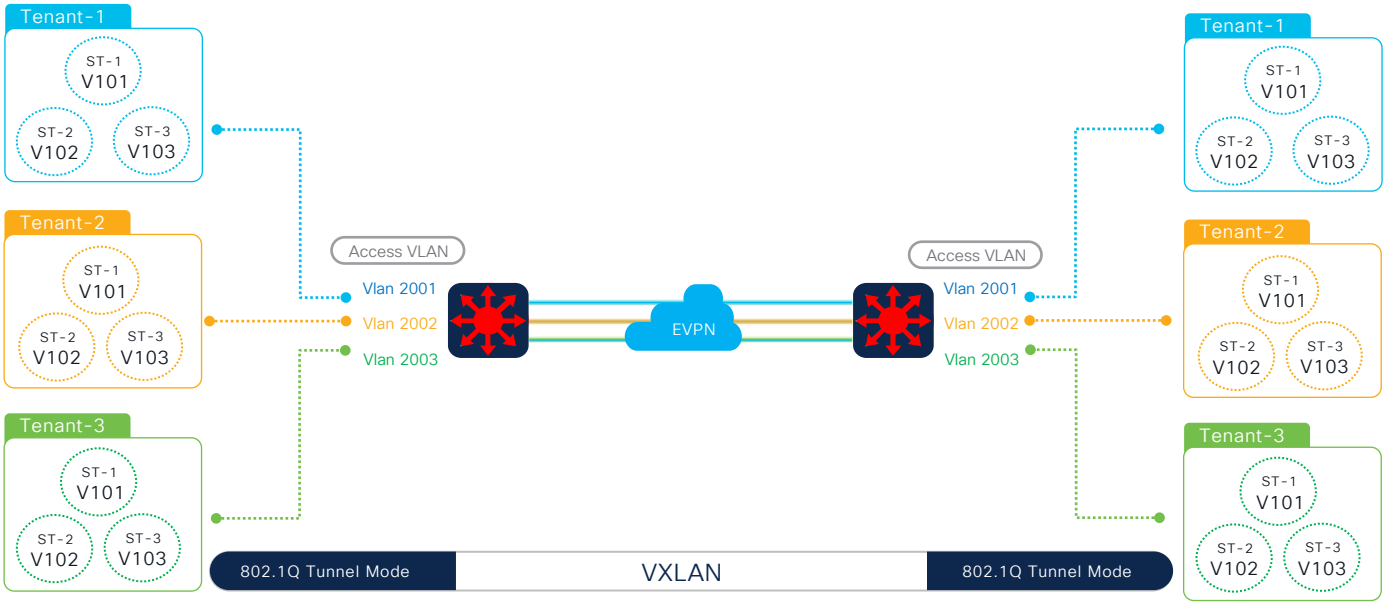
NXOS - BGW

```
!
interface Ethernet1/1
  description CONNECTED TO REMOTE BGW
 evpn multisite dci-tracking
 !
 interface Ethernet1/2
   description CONNECTED TO INTERNAL SPINE
  evpn multisite fabric-tracking
!
router bgp 200
  rd dual id 1
  neighbor 172.16.0.29
    remote-as 200
    peer-type fabric-external
    address-family l2vpn evpn
      rewrite-evpn-rt-asn
```

Structured Network Extension

- Loop-free Layer 2 overlay extension with overlay control and data-plane hierarchy
- Isolated BUM domains with rate-limit BUM control-management at Border-Gateway
- Flexible underlay BUM replication modes – Multicast | Ingress
- Seamless Catalyst 9000 to Nexus 9000 interworking function

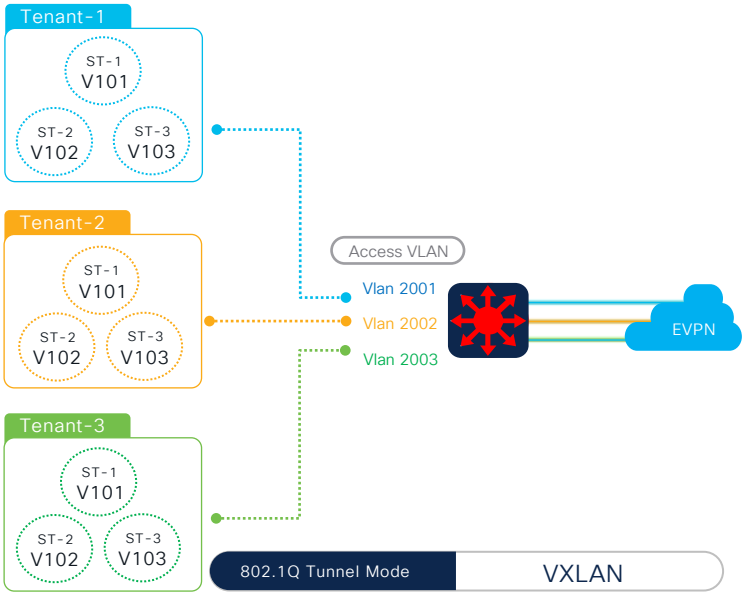
Multi-Tenant Layer 2 Network Extensions



Scalable Multi-Tenant L2 Networks

- Scalable Layer 2 EVPN VXLAN architecture for multi-tenant solutions
- *N Sub-Tenant* VLAN IDs : 1 Access VLAN mapping with CE facing interface in IEEE 802.1Q tunnel mode
- Single, unused Access VLAN mapped to EVI transparently forward 802.1Q over VXLAN
- Flexible L2 overlay topology – Point-to-Point, Partial-Mesh, Hub-n-Spoke or Full-mesh across fabric

IEEE 802.1Q over VXLAN




```
!
l2vpn evpn instance 1 vlan-based
 encapsulation vxlan
 replication-type static
 ip local-learning disable
!
device-tracking policy MULTI-TENANT-L2-POLICY
 no protocol ndp
 no protocol dhcp6
 no protocol arp
 no protocol dhcp4
!
vlan 2001
! name MULTI-TENANT-ACCESS-VLAN
!
vlan configuration 2001
 member evpn-instance 1 vni 10001
 device-tracking attach-policy MULTI-TENANT-L2-POLICY
!
interface nve1
member vni 10001 mcast-group 239.1.1.1
!
interface Teng1/0/1
 description CONNECTED TO TENANT-1 L2 NETWORK
 switchport mode dot1q-tunnel
 switchport access vlan 2001
!
```

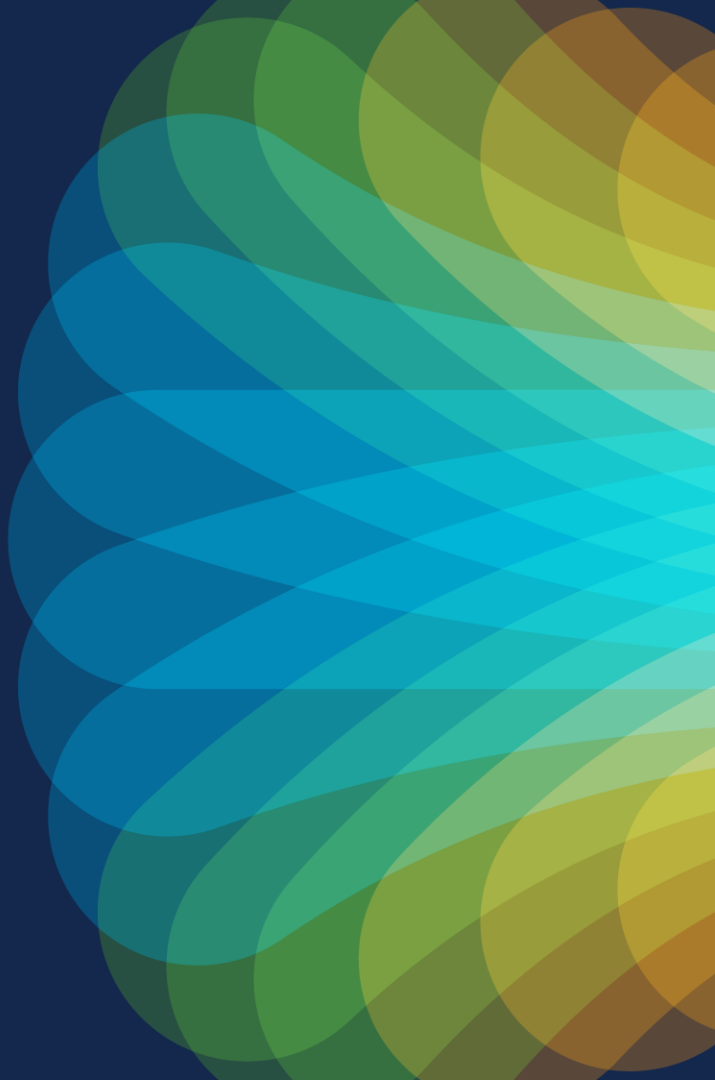
One Access VLAN per Tenant network

Layer 2 overlay network support. Layer 3 routing unsupported.

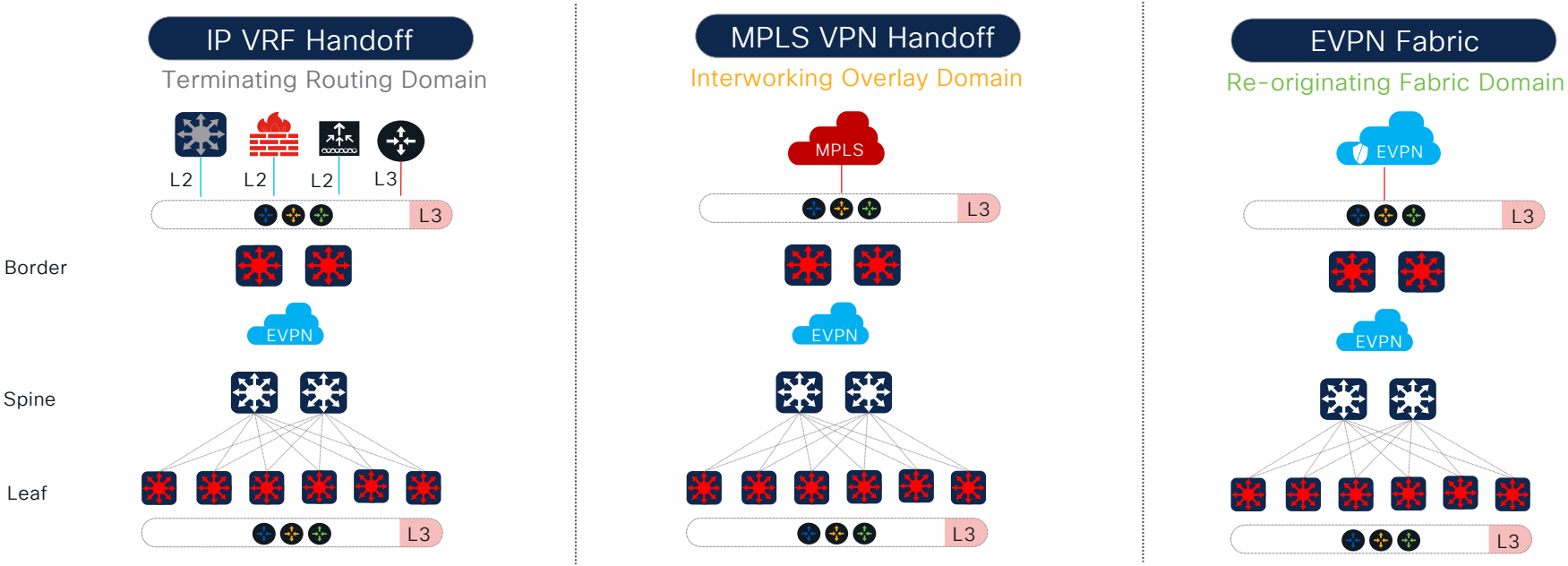
Disable protocol validation policy on local VXLAN Access VLAN

Co-exist with Access/Trunk ports for standard Layer 2 and Layer 3 overlay network

Layer 3 – External Domain Handoff Types



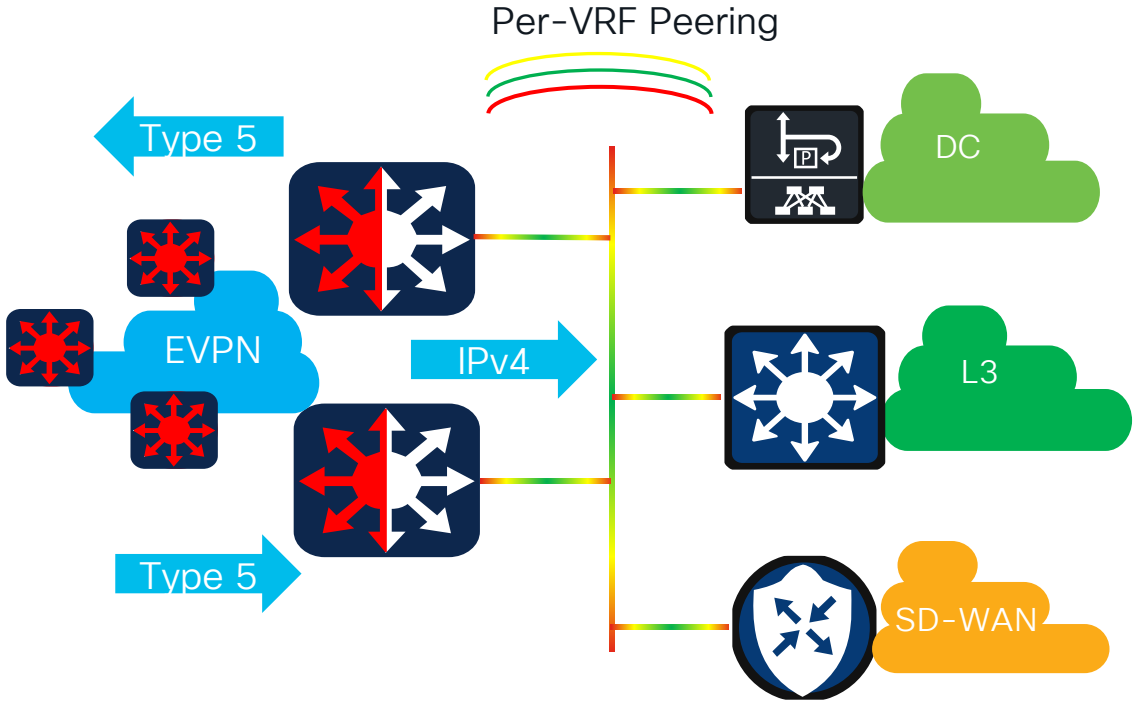
Layer – 3 Handoffs Alternatives



Integrated Extranet

- Transparent EVPN handoff to Layer 2 or Layer 3 to traditional underlay segmented networks
- Seamless multi-domain interworking at Border – IP, MPLS VPN, EoMPLS/VPLS, SD-WAN, etc.
- Extendable Unicast | Multicast support for IPv4 and IPv6 between EVPN to external domain
- Dedicated or collapsed system-role – Leaf, Spine, Border, Border-Leaf, Border-Spine

L3 Network Handoff (Terminate)

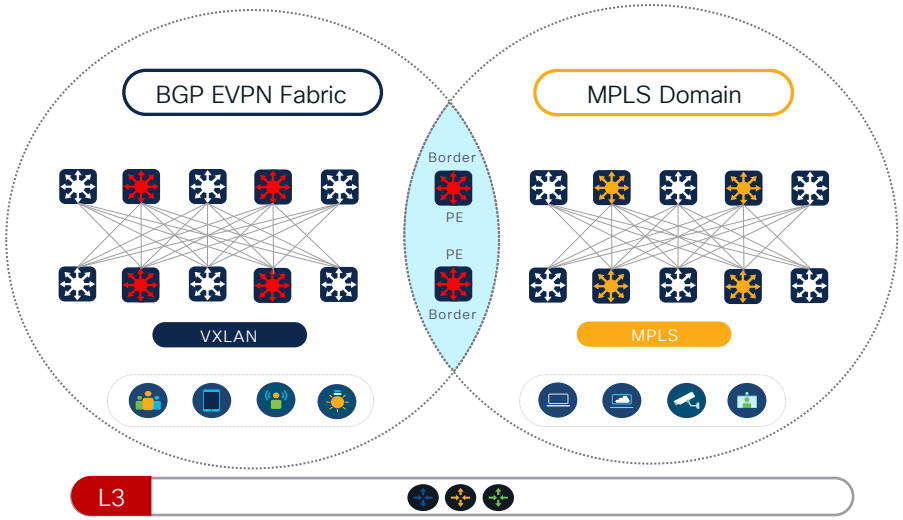



```
!
vrf definition green
rd 192.168.255.1:101
 address-family ipv4 unicast
   route-target both 65535:101
   route-target both 65535:101 stitching
!
interface Vlan 10
 vrf forwarding green
 ip address 192.168.1.2 255.255.255.252
!
router bgp 65535
 address-family ipv4 vrf green
   advertise l2vpn evpn
   neighbor 192.168.1.1 remote-as 65534
 !
```

L3 Domain Handoff

- End-to-End segmentation between Campus, DC, & SDWAN Domains
- Standard Multi-VRF handoff over L2 Trunk SVI, Layer 3 Sub-interface and more
- Integration to L3 services to Firewall, Fusion Router, etc.

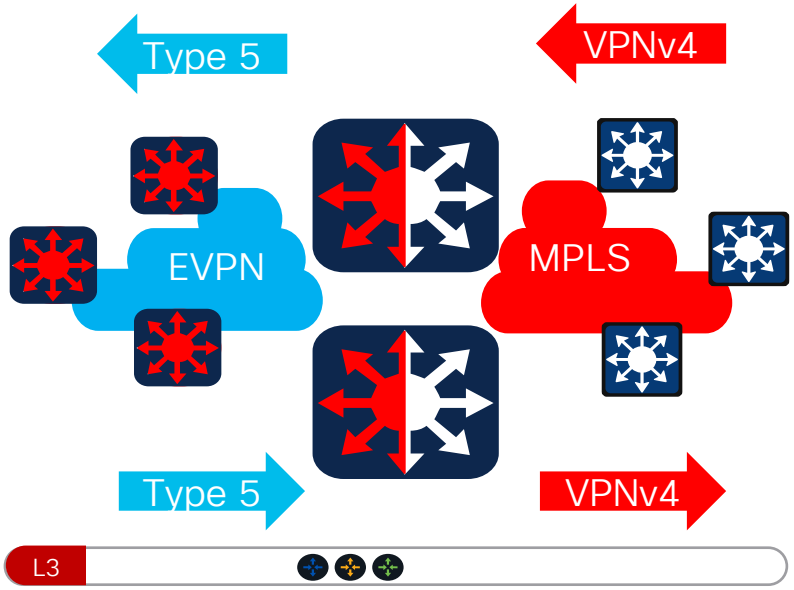
Interdomain L3 Segmentations (Interworking)



Flexible Layer 3 Interworking

- Integrated MPLS VPN to BGP EVPN VXLAN Layer 3 interworking function as EVPN Border + MPLS PE
- Independent control-plane and data-plane, yet tightly integrated for end-to-end transparent segmentation
- Seamless IPv4 and IPv6 overlay network interworking with VPNv4/VPNv6
- Transparent Multicast interworking support between EVPN TRM domain to MPLS mVPN

L3 Overlay Handoff (Interworking)




```
!
mpls label mode all-vrfs protocol all-afs per-vrf
!
router bgp 65001
!
address-family vpnv4 unicast
  import l2vpn evpn re-originate
  neighbor <RR> next-hop-self all
!
address-family l2vpn evpn
  import vpnv4 unicast re-originate
 neighbor <RR> next-hop-self all
!
```

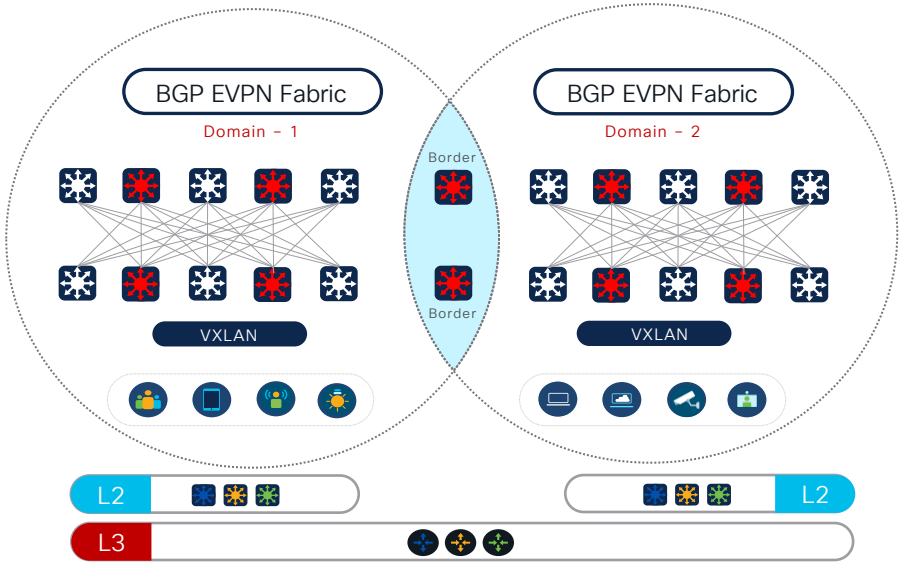
Integrated Overlay Interworking

Simplified command-line syntax to “stitch” routing-domain between MPLS VPNv4/v6 and BGP EVPN address-families

Flexibility to maintain or rewrite Route-Targets and re-originate on each side domain to support backward compatibility

Catalyst 9000 Border + PE System mode alternatives – StackWise Virtual or Standalone modes

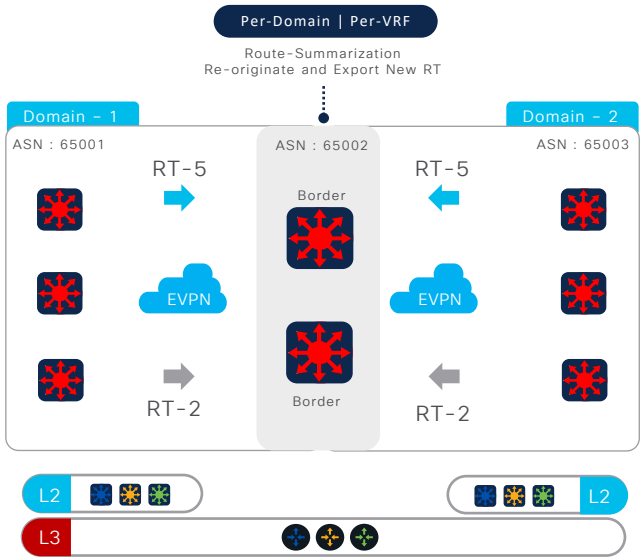
Multi-Domain BGP EVPN Fabric (Re-Originate)



Multi-Domain Layer 3 Extensions

- Re-originating Layer 3 BGP EVPN fabric at Border to support multi-domain fabric architecture
- Isolated BGP control-plane and VXLAN data-plan within each fabric domains
- Border provides overlay network prefix route-summarization, RT re-origination and export as self next-hop
- Layer 2 overlay and Multicast overlay boundary limited within each domain. Multi-Site recommended for cross–domain.

Multi-Domain Border Route Re-origination




```
!
vrf definition green
 rd 192.168.255.1:101
!
address-family ipv4 unicast
 route-target import 65001:101 stitching
 route-target export 65001:1001 stitching
 route-target import 65003:101 stitching
 route-target export 65003:1001 stitching
!
router bgp 65002
!
address-family ipv4 unicast vrf green
 aggregate-address <DOMAIN-1-NETWORK> <MASK> route-map <DOMAIN-1> summary-only
 aggregate-address <DOMAIN-2-NETWORK> <MASK> route-map <DOMAIN-2> summary-only
!
route-map DOMAIN-1 permit 10
 set extcommunity rt 65001:1001
!
route-map DOMAIN-2 permit 10
 set extcommunity rt 65003:1001
!
```

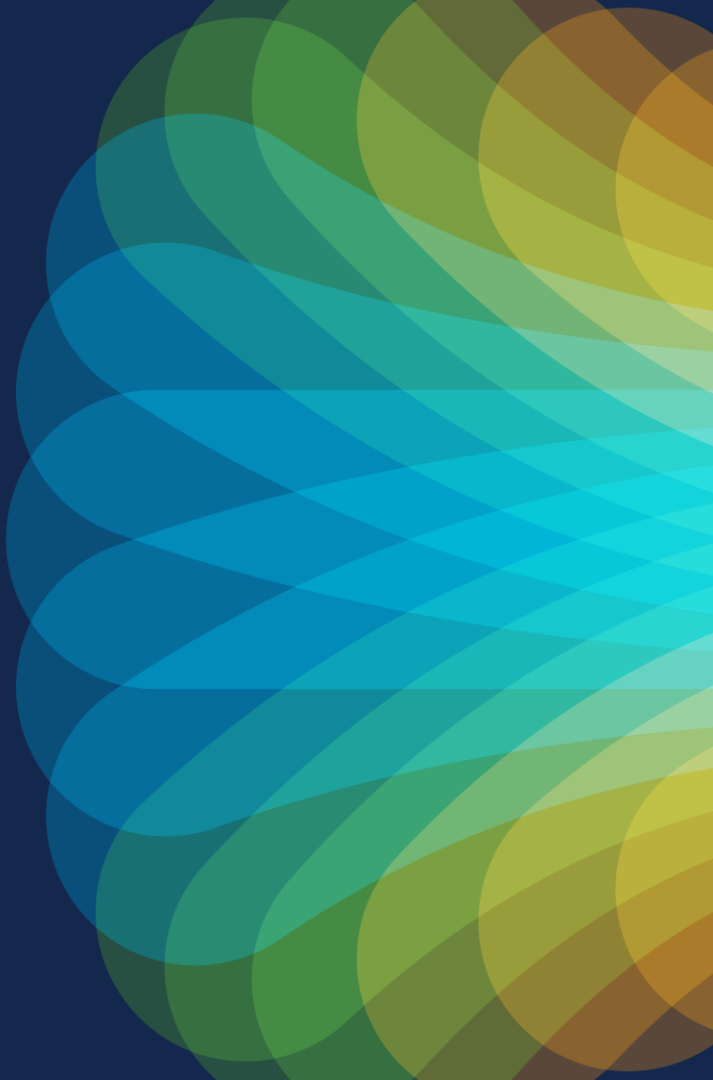
Per-VRF IPv4/v6 Route-Summarization at Border

Per EVPN domain route summarization at the Border system

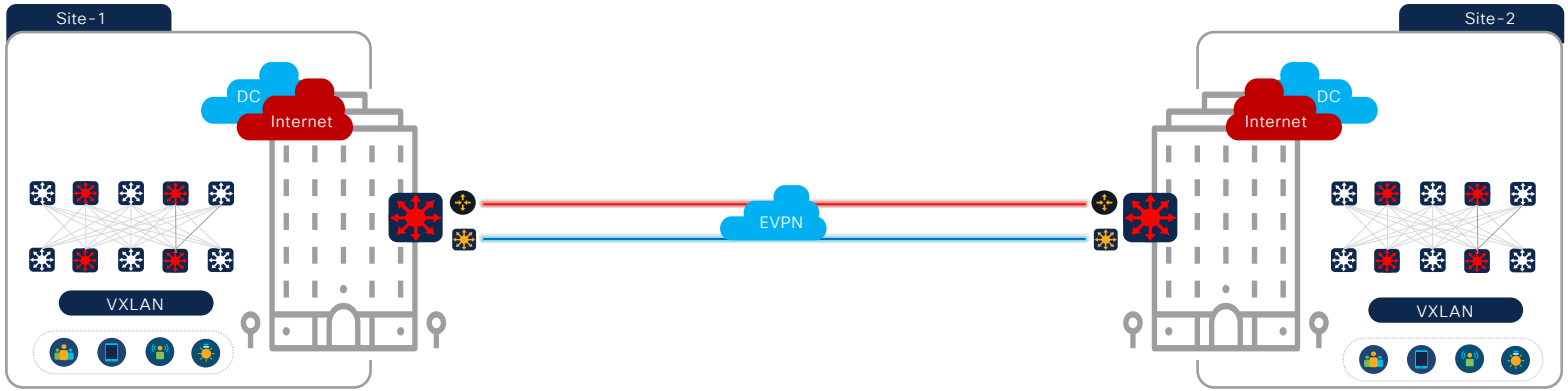
New Summary route = New export Route-Target to be imported by remote Leaf. Border automatically sets itself as Next-Hop

Simple and isolated fault domain with scalable Layer 3 segmented multi-domain fabric extension

EVPN Border Network Extensions



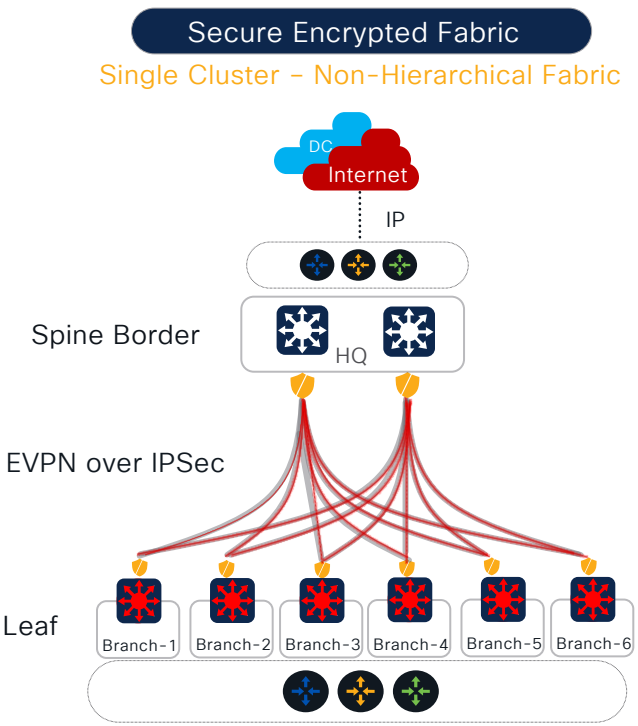
Site-to-Site Fabric Extension

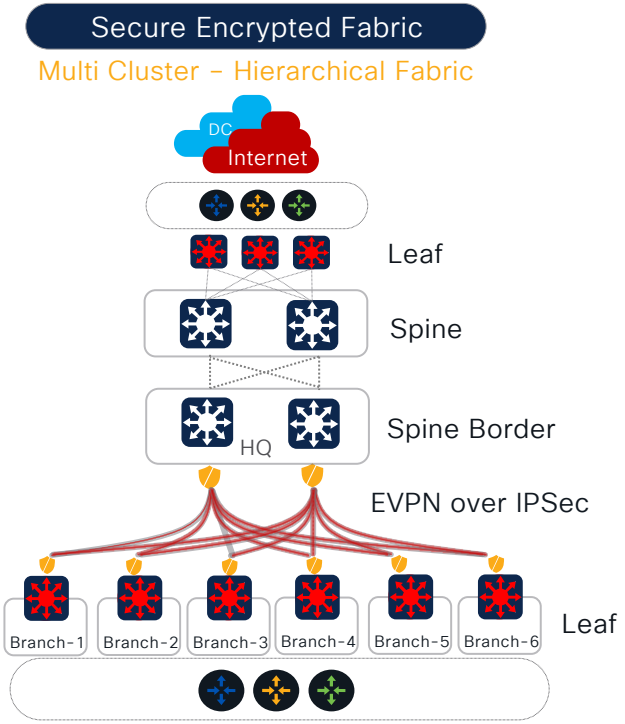


Inter-Site EVPN Fabric

- Simple point-to-point BGP EVPN Fabric between two sites
- Spine-less design with direct i-BGP/e-BGP peering.
- Flexible Underlay – IP or MPLS. MTU size consideration with Static, Path-MTU discovery, MSS-Adjust.
- Flexible Overlay – Layer 2 extension, Layer 3 segmentation or both.

Encrypted BGP EVPN Fabric Extension

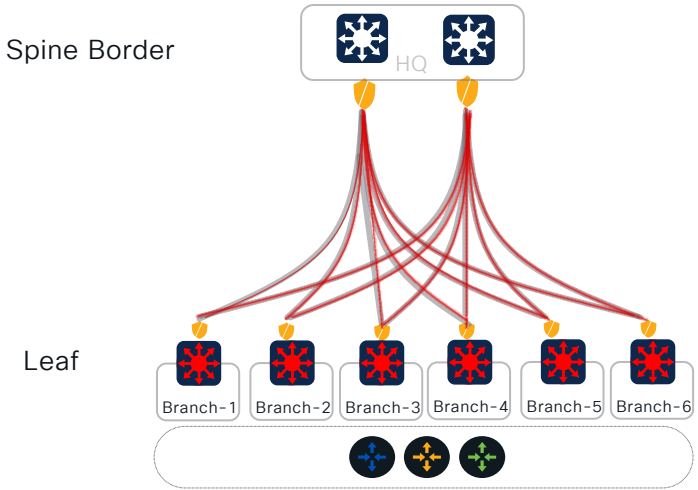




Encrypted EVPN Fabric

- High performance Catalyst 9300-X/9400X IPsec underlay network solution
- Simplified and scalable Layer 3 overlay fabric with integrated or co-located Spine/RR
- Single fabric cluster across WAN or “stitch” to EVPN fabric at central-office
- Unicast | Multicast support for IPv4 and IPv6 in overlay

Encrypted BGP-EVPN Fabric Configuration

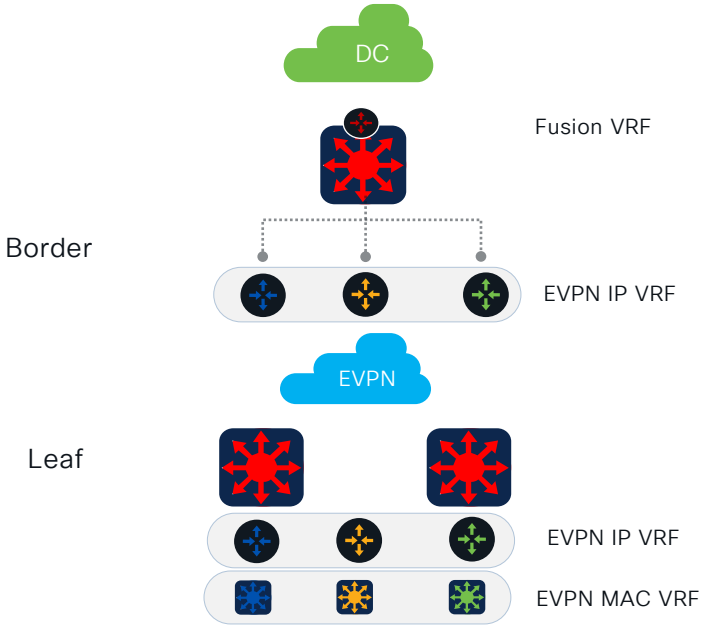



```
interface Loopback 0
 description BGP ROUTER ID
 ip address <IP> <MASK>
 ip ospf <BGP ROUTER INSTANCE ID1> area <ID>
!
interface Loopback 1
 description IPSEC TUNNEL SOURCE INTERFACE
 ip address <IP> <MASK>
 ip ospf <IPSEC-TUNNEL-IGP-INSTANCE-ID1> area <ID>
!
interface Loopback 10
 description IPSEC UNDERLAY TUNNEL SOURCE INTERFACE
 ip address <IP> <MASK>
 ip ospf <IPSEC-TUNNEL-UNDERLAY IGP-INSTANCE-ID2> area <ID>
!
interface Tunnel <ID>
 ip address <IP> <MASK>
 ip ospf <IPSEC-TUNNEL-IGP-INSTANCE-ID> area <ID>
 tunnel mode ipsec ipv4
 tunnel source Loopback 1
 tunnel destination <HUB-1 IP ADDRESS>
 tunnel protection ipsec profile <IPSEC-PROFILE-NAME>

router bgp 1
 bgp router-id interface Loopback0
 no bgp default ipv4-unicast
 neighbor <REMOTE BGP ROUTER ID> remote-as 1
 neighbor <REMOTE BGP ROUTER ID> update-source Loopback0
!
```

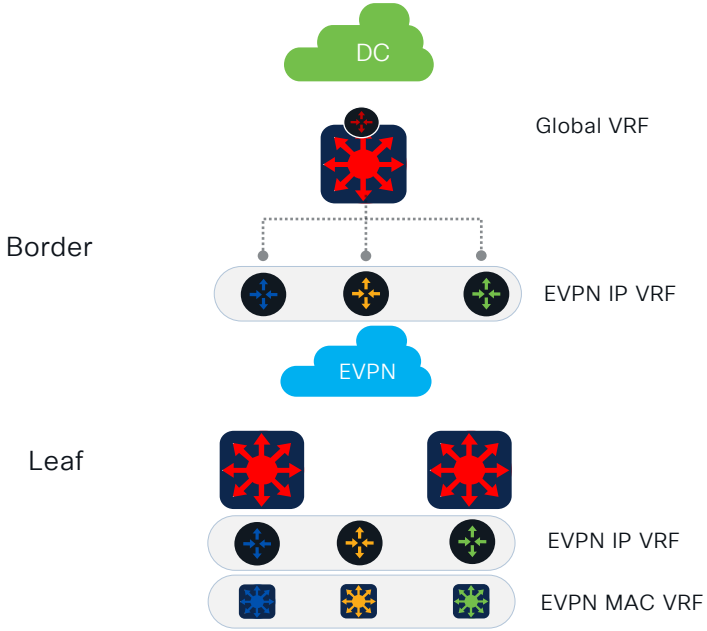
Fusion VRF Extranet

EVPN | Non-EVPN VRF Route-Leaking



Global VRF Extranet

EVPN | Global VRF Route-Leaking

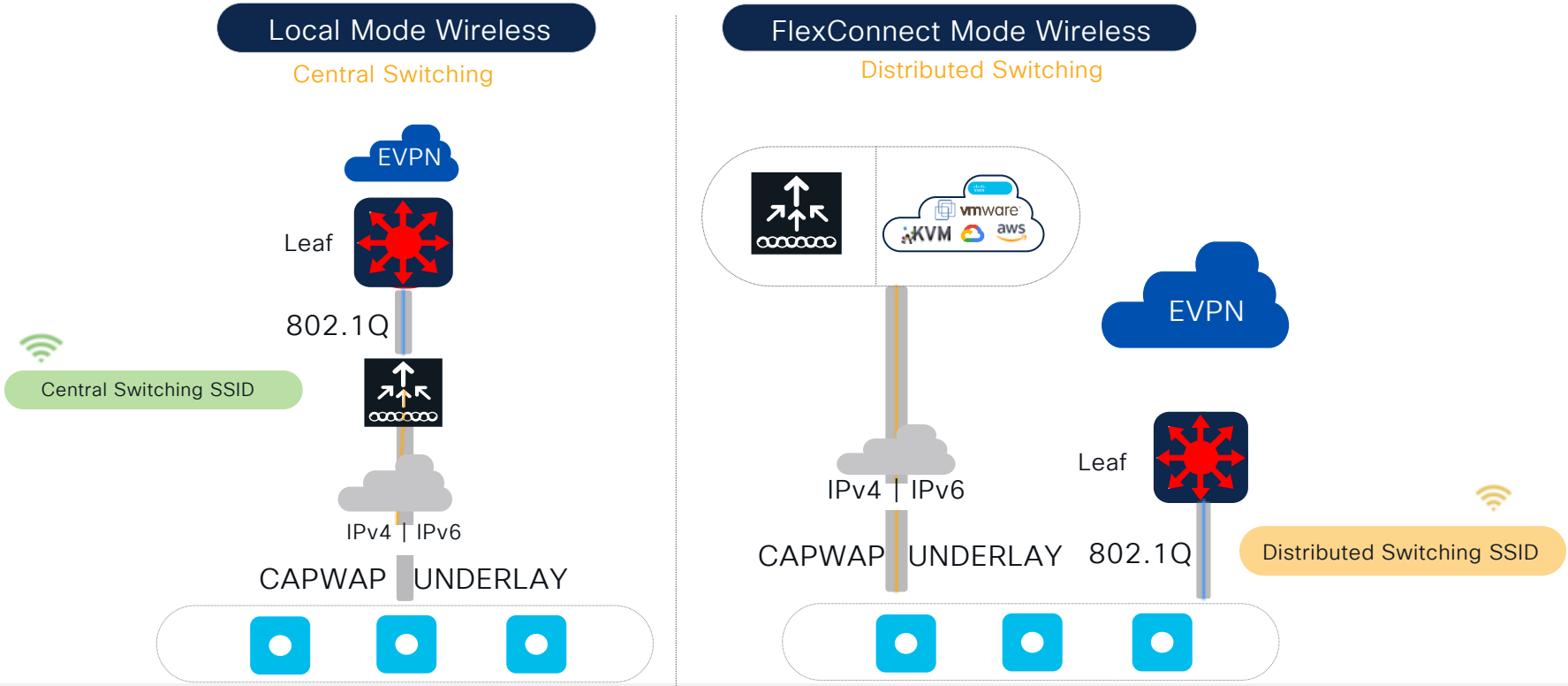


Integrated Extranet

Policy-based stateless extranet Unicast routing

Flexible route-leaking solution - EVPN-EVPN | EVPN-Non EVPN VRF | EVPN-Global

Various external Unicast routing protocol handoff



Seamless Wireless

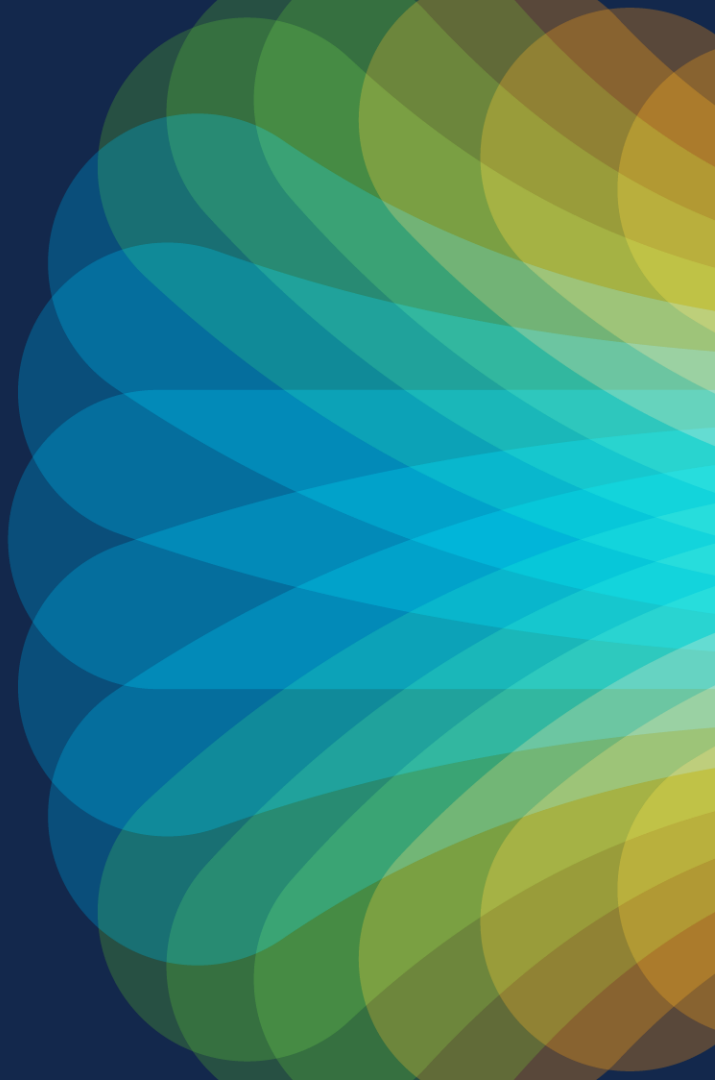
Transparent Wireless integration in fabric. Intact WLC and AP communication in Underlay

Flexible SSID alternatives – Central Switching, Local Switching, Central + Local Switching

Fabric boundary initiates from Wireless Client IP gateway. Flex Local seamless roaming* up to 100 AP.

Consistent Wired and Wireless network access control policy enforcement

Catalyst 9000 EVPN Reference



cisco Live!

Configuration Guide

Completed Chapters

BGP EVPN VXLAN Overview
Configuring EVPN VXLAN Layer 2 Overlay Network
Configuring EVPN VXLAN Layer 3 Overlay Network
Configuring EVPN VXLAN Integrated Routing and Bridging
Configuring Spine Switches in a BGP EVPN VXLAN Fabric
Configuring DHCP Relay in a BGP EVPN VXLAN Fabric
Configuring VXLAN-Aware Flexible NetFlow
Configuring Tenant Routed Multicast
Configuring EVPN VXLAN External Connectivity
Cisco DNA Service for Bonjour Overview
Configuring Cisco DNA Service for Bonjour over EVPN VXLAN Layer 3 Overlay Networks
Troubleshooting BGP EVPN VXLAN
Feature History and Information for BGP EVPN VXLAN

More Coming Soon ...

Reference

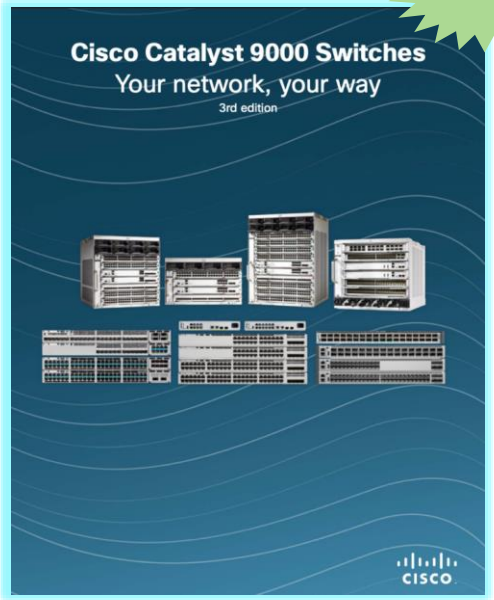
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-5/configuration_guide/vxlan/b_175_bgp_evpn_vxlan_9600_cg.html

Would You Like to Know More?

Catalyst 9000 Series Enterprise Switches

- **cisco.com/go/cat9K**
- Cisco Catalyst 9000 at-a-Glance
- Cisco Catalyst 9000 Family FAQ
- Catalyst 9000 Series - Cisco Community
- Catalyst 9000 Series – CiscoLive Library

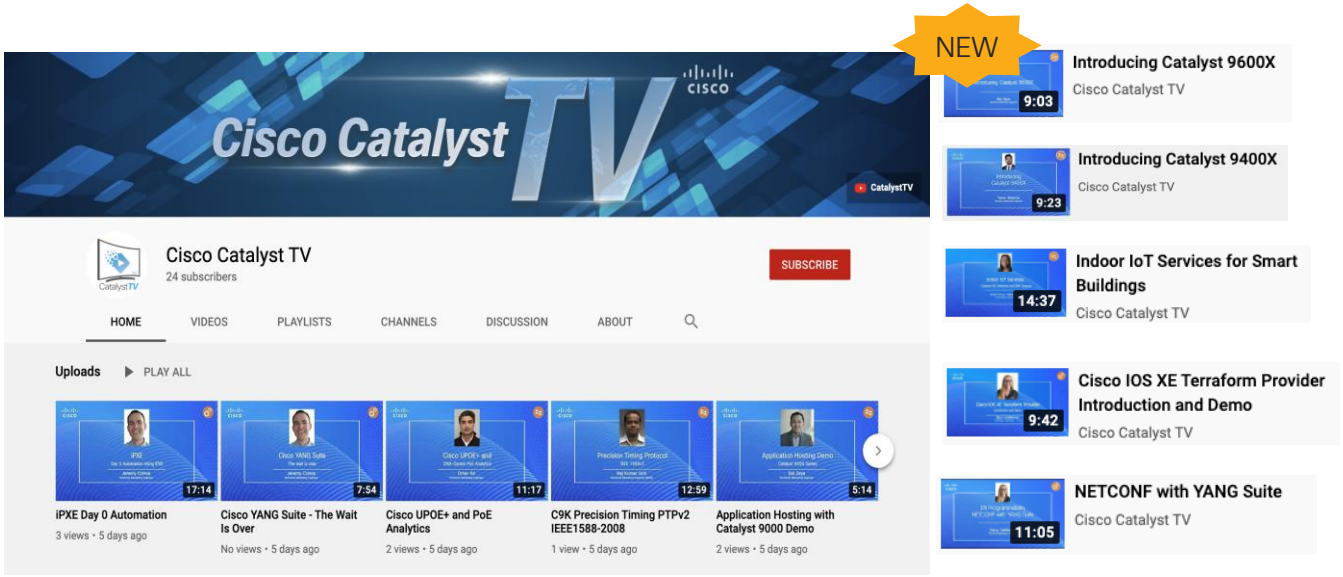
FREE



cs.co/cat9kbook

Cisco Catalyst TV @ YouTube

This channel is all about Cisco Catalyst Platforms and its services and software solutions. Subscribe and Explore Playlists Catalyst Switching and Catalyst Programmability & Automation for videos and demos by the Technical Marketing Engineers on latest, relevant and exciting topics.



SUBSCRIBE

Cs.co/CatalystTV

Fill out your session surveys!

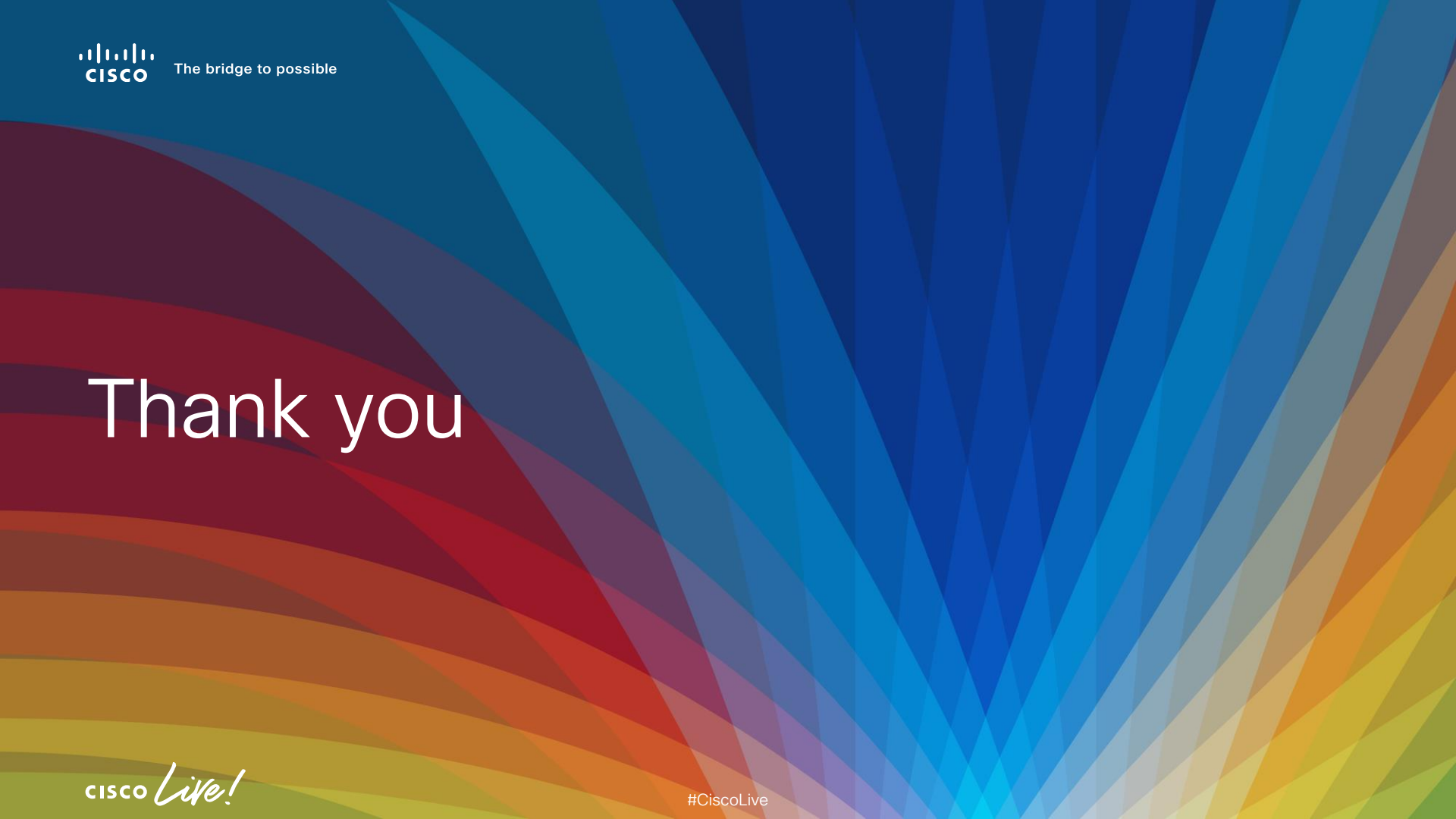
Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

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

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


cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLive

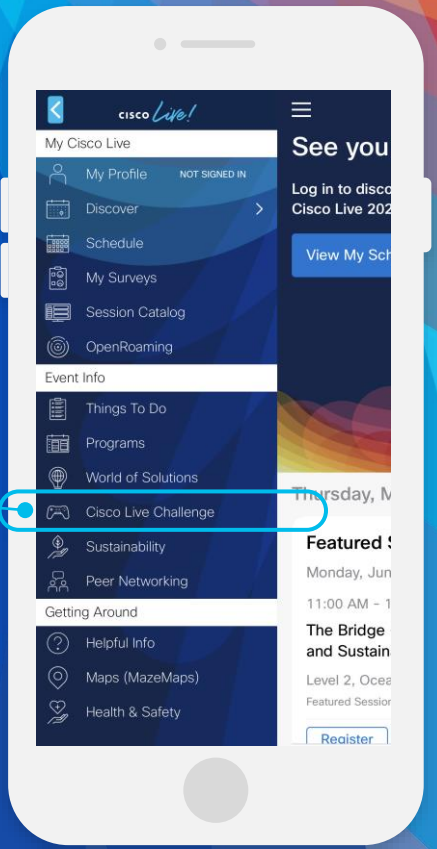
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:




cisco Live!
Let's go
#CiscoLive