

CISCO *Live!*



#CiscoLive



The bridge to possible

Migrating Classical Enterprise Campus Networks to VXLAN EVPN Based Networks

Part 1

Nazim Khan – Customer Success Specialist

BRKENS-3096a



#CiscoLive

Cisco Webex App

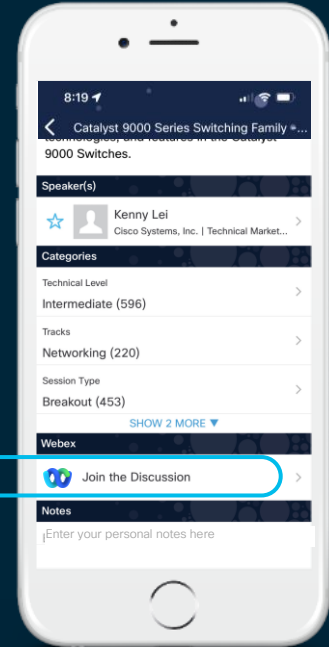
Questions?

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.

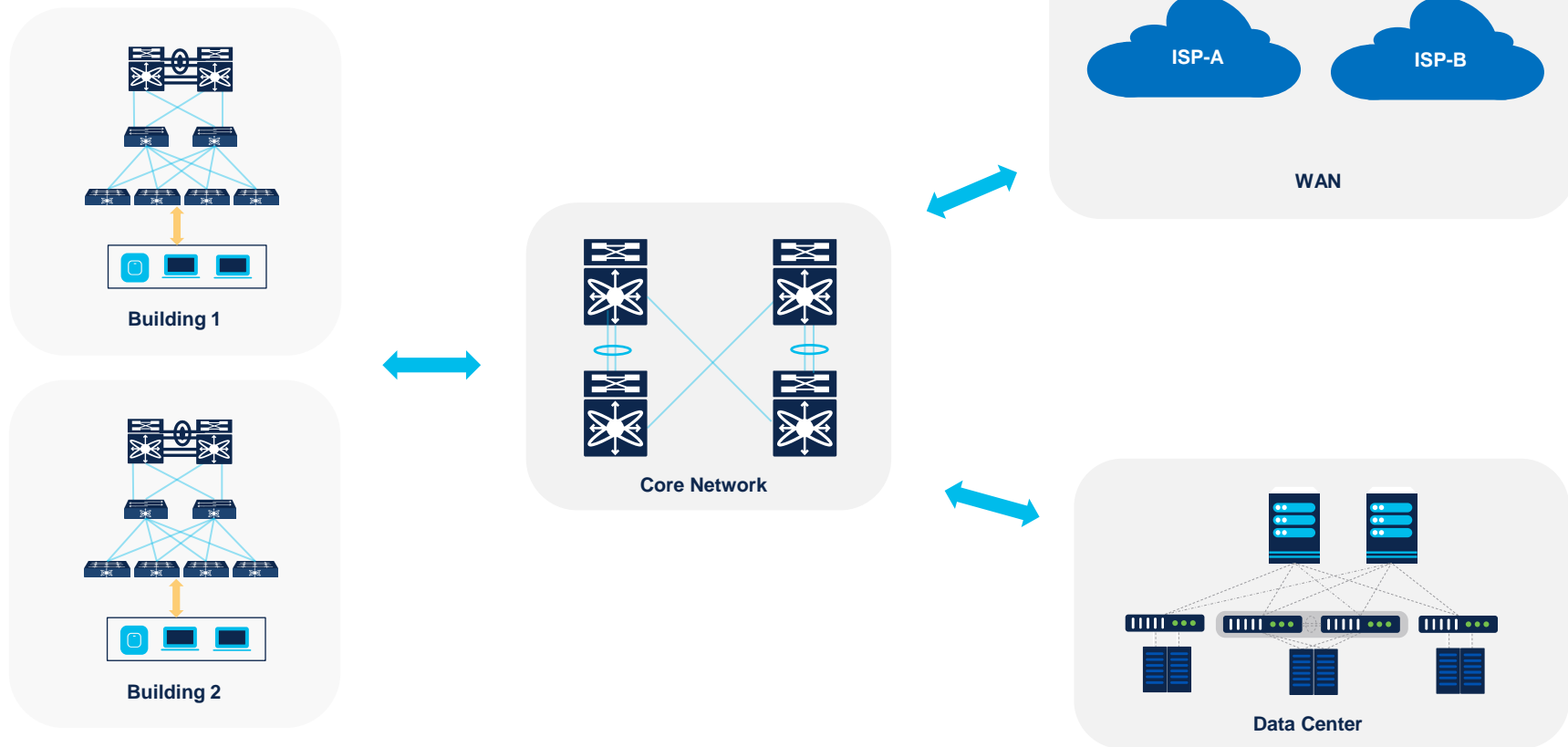


<https://cislive.ciscoevents.com/cislivebot/#BRKENS-3096a>

Agenda

- Introduction
- VXLAN EVPN Architecture overview
- Migration Strategies & Considerations
- Planning & Pre-requisites
- Automation Tools
- Key Take Away

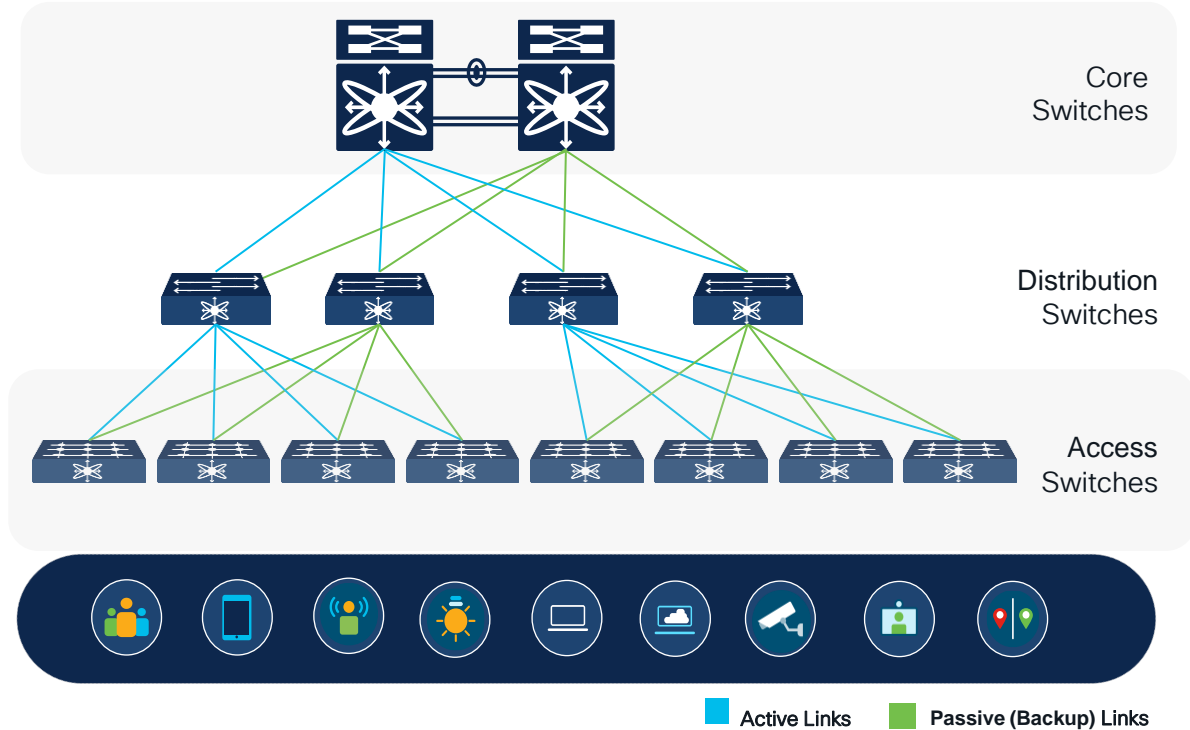
Typical Campus Network



Traditional 3-Tier Networks

Challenges

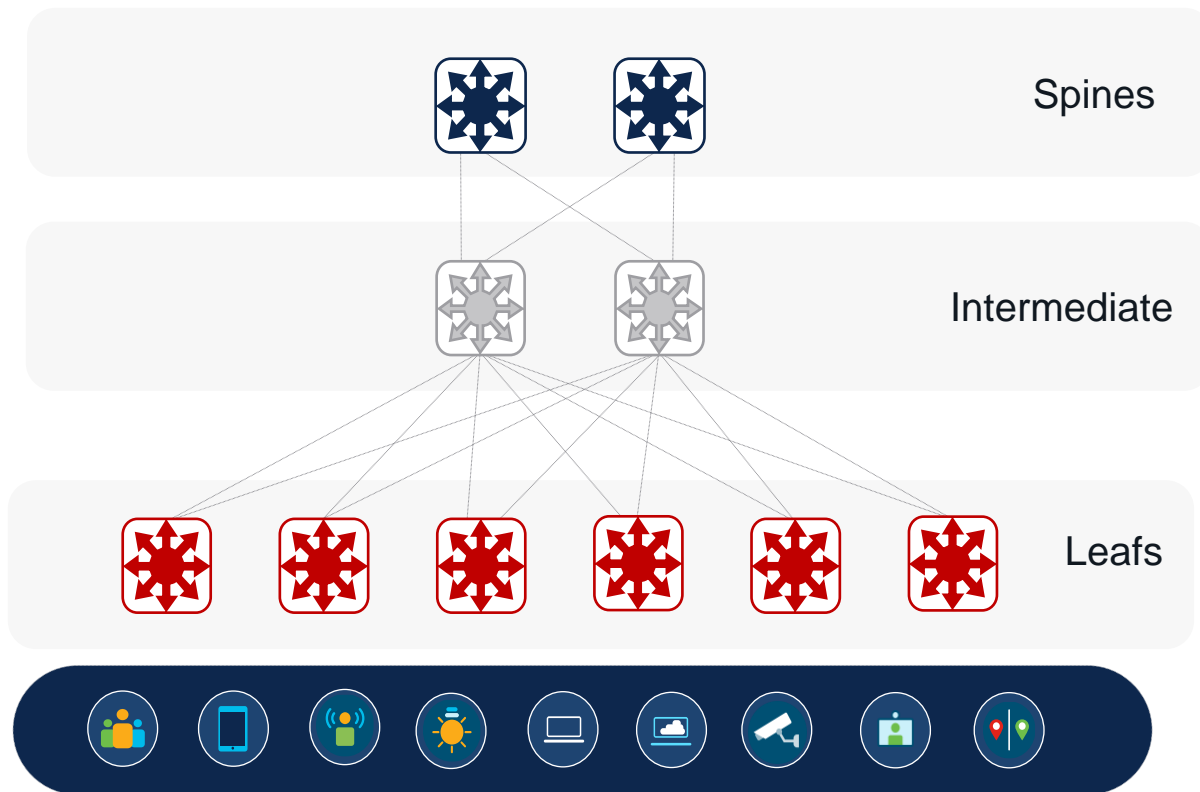
- Broadcast Domain – Spanning-Tree
- Flood & Learn Mechanism
- Mobility- Roaming
- VLAN Scale
- Load Balancing
- Resiliency
- Scalability



VXLAN EVPN Architecture

Benefits

- Any Subnet, Anywhere
- Layer-3 ECMP links end-to-end
- No Flooding with BGP Control Plane
- Extensible Scale & Resiliency
- Distributed Gateway on all Edge nodes (Leaf)
- Segmentation



What is ... ?

VXLAN

- Standards based Encapsulation
 - RFC 7348
 - Uses UDP-Encapsulation
- Transport Independent
 - Layer-3 Transport (Underlay)
- Flexible Namespace
 - 24-bit field (VNID) provides ~16M unique identifier
 - Allows Segmentations

EVPN

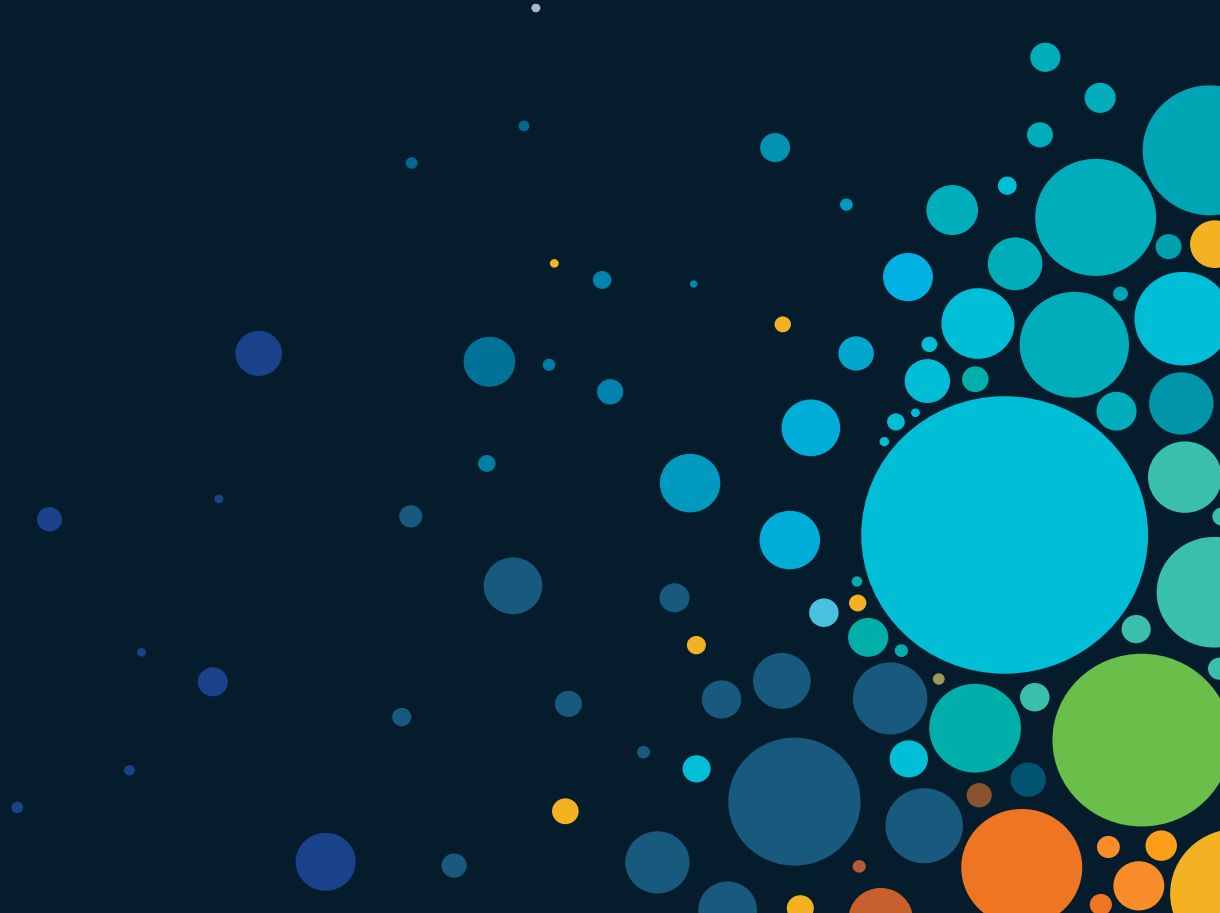
- Standards based Control-Plane
 - RFC 8365 (and RFC 7432)
 - Uses Multiprotocol BGP
- Uses Various Data-Planes
 - VXLAN (EVPN-Overlay), MPLS, Provider Backbone (PBB)
- Many Use-Cases Covered
 - Bridging, MAC Mobility, First-Hop & Prefix Routing, Multi-Tenancy (VPN)

Why BGP EVPN for Enterprise Campus ?



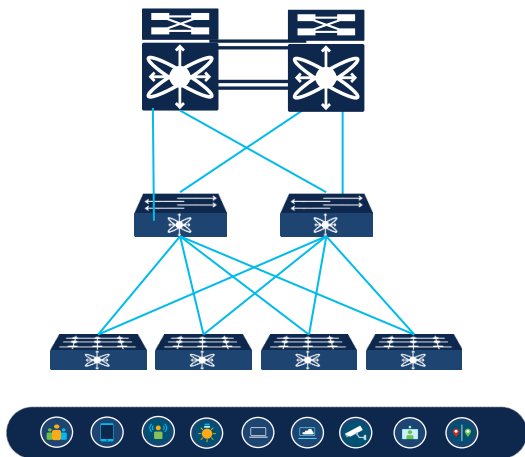
- Industry-standard
- One Fabric Architecture
- Proven & Scalable
- Hierarchical Fabric Domain
- Flexible Overlay

Migration Strategies



Migration Strategy -1 : Build and Move

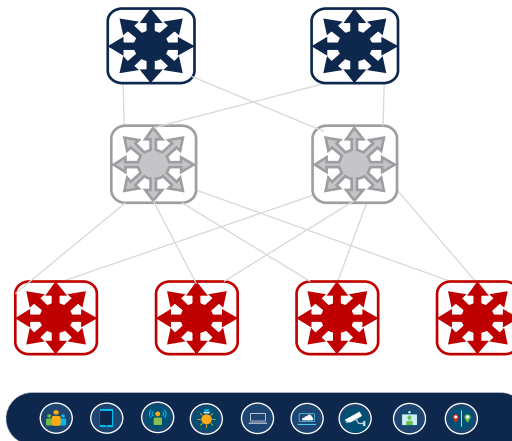
Classic 3-Tier Network



Layer 2

Layer 3

VXLAN EVPN Network



Deployment

Design & deploy new VXLAN BGP EVPN fabric

Integration

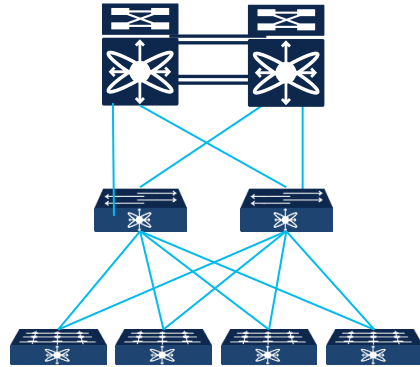
Connect VXLAN BGP EVPN to classical 3-tier network

Migration

Migrate end-points to use new VXLAN BGP EVPN fabric

Migration Strategy -2 : Phased Migration

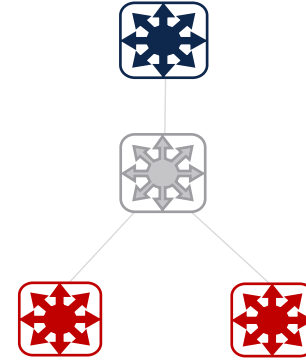
Classic 3-Tier Network



Layer 2

Layer 3

VXLAN EVPN Network



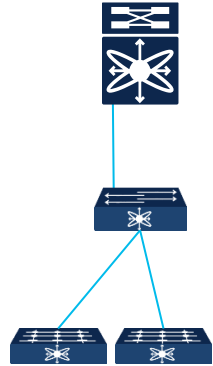
EVPN Island Deployment
Design & deploy new
minimalistic VXLAN BGP
EVPN fabric

Integration
Connect VXLAN BGP
EVPN to classical 3-tier
network

Phased Migration -1
Migrate few end-points
to use new VXLAN BGP
EVPN fabric

Migration Strategy -2 : Phased Migration

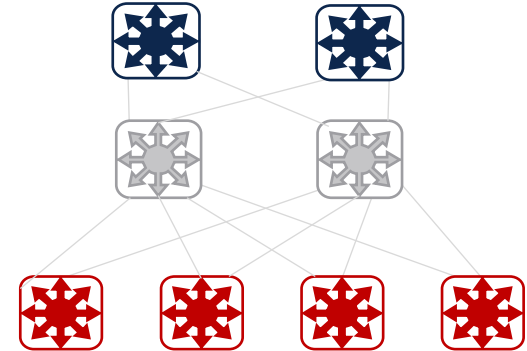
Classic 3-Tier Network



Layer 2

Layer 3

VXLAN EVPN Network



EVPN Island Deployment
Design & deploy new
minimalistic VXLAN BGP
EVPN fabric

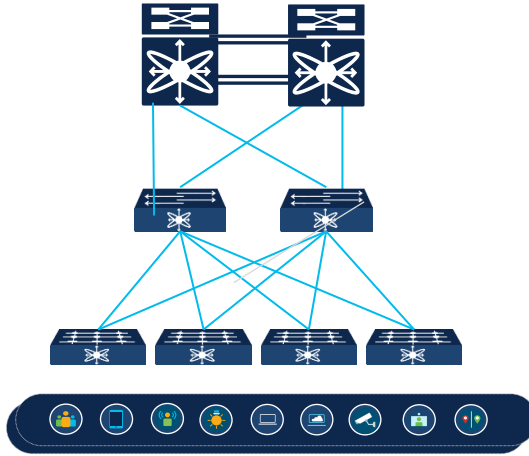
Integration
Connect VXLAN BGP
EVPN to classical 3-tier
network

Phased Migration -1
Migrate few end-points
to use new VXLAN BGP
EVPN fabric

Phased Migration -2
Migrate switches and
scale the EVPN fabric

Migration Strategy -3 : Flag Day

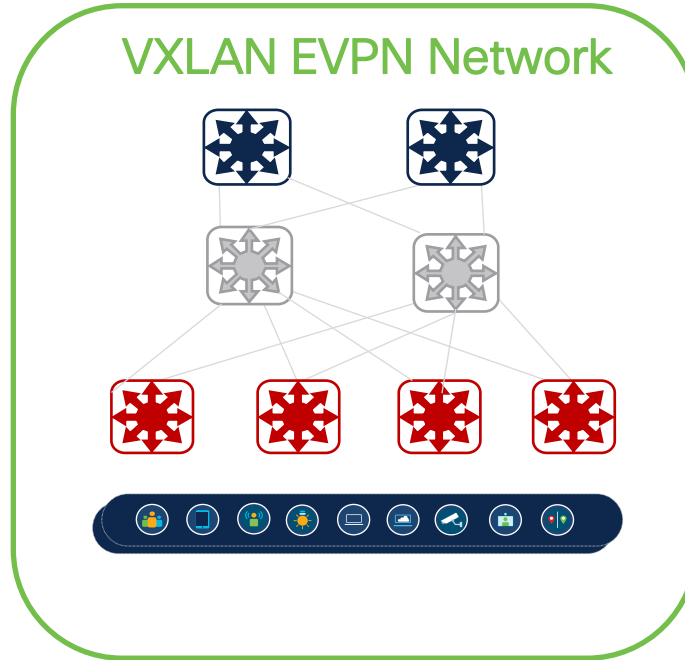
Classic 3-Tier Network



Backup Existing Network
Backup configuration,
device states of existing
classic 3-tier network

Prepare
Gracefully shutdown the
classic 3-tier network and
associated services

Migration Strategy -3 : Flag Day



Backup Existing Network
Backup configuration,
device states of existing
classic 3-tier network

Prepare
Gracefully shutdown the
classic 3-tier network and
associated services

Bring Up
Upgrade Software,
reconnect devices as per
VXLAN EVPN Architecture

Migration Strategies Comparison

Build & Move

- Seamless Migration
- Additional Hardware and resources required
- Opportunity to test & familiarize VXLAN EVPN
- Low Change Management Risks
- Moderate change window

Phased Migration

- Seamless Migration in phases
- Minimal additional hardware and resources required
- Opportunity to test & familiarize VXLAN EVPN
- Lowest Change Management Risks
- Long change window

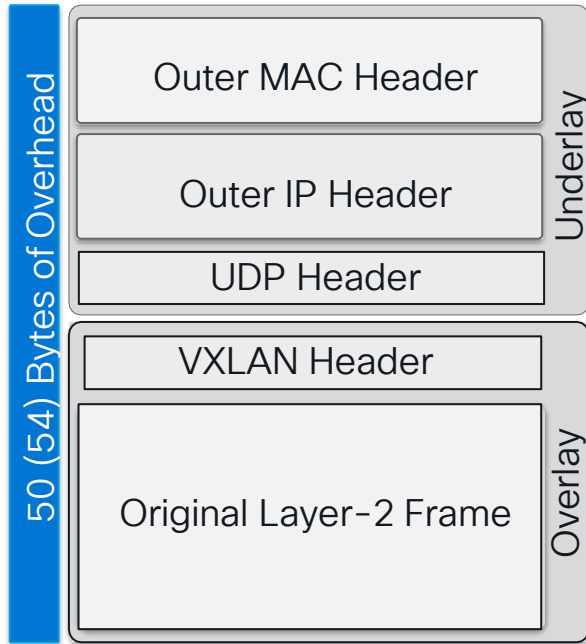
Flag Day

- Migration with downtime
- No Additional hardware and resources required*
- No opportunity to test & Familiarize VXLAN EVPN
- High Change Management Risks
- Minimal change window

* If existing devices can support VXLAN / EVPN and other required features

Planning & Pre-requisites

MTU and VXLAN

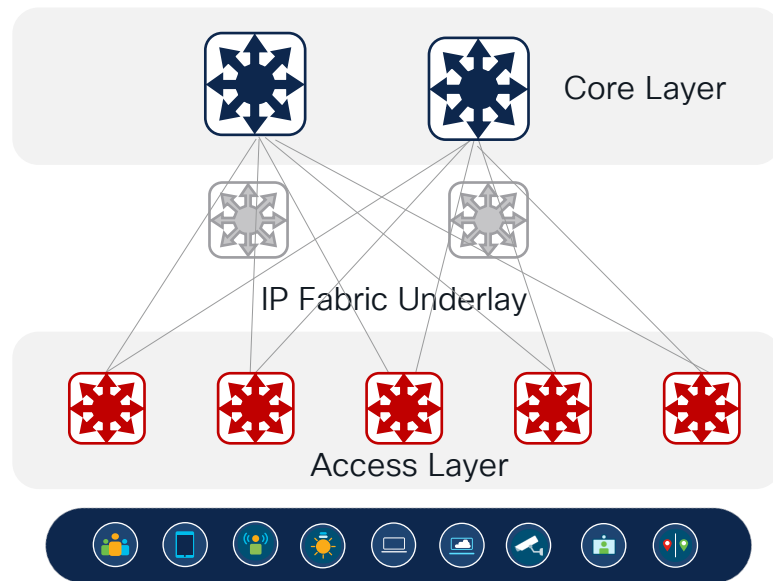


- VXLAN adds 50 Bytes (or 54 Bytes)
- Network switches support MTU up to 9216* bytes
 - Accommodates jumbo MTU plus overlay overhead (50/54bytes)
- Avoid Fragmentation
 - Adjust the Transport Network with appropriate MTU

*Cisco Catalyst 9k switches only support 9198 Byte for Layer-3 Traffic

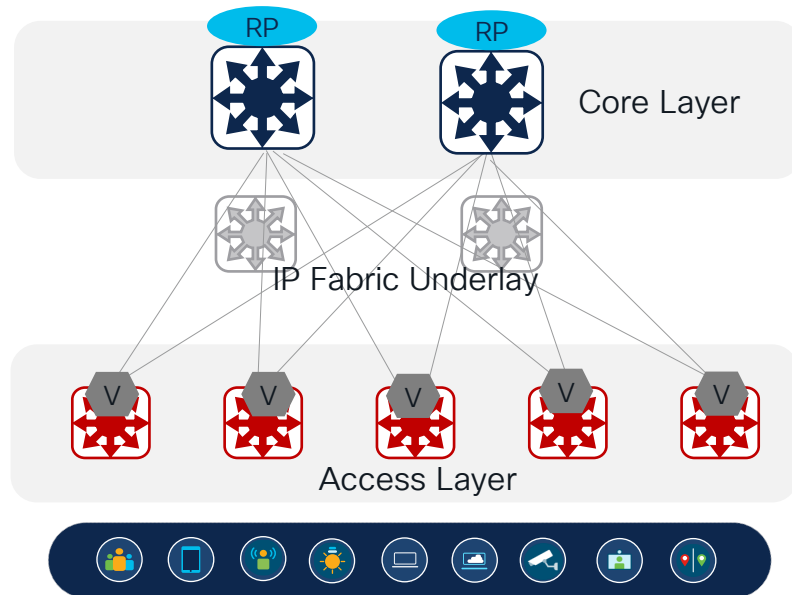
Interface Principles

- Routed Ports and Interfaces
 - Layer-3 Interfaces between Access and Core (no switchport) Or SVI
 - For each Point-to-Point (P2P) connection, minimum /31 required (IPv4)
 - Alternatively, use IP Unnumbered /32
- Loopback as Source-Interface for VTEP



IP Addressing Principles

- Prepare an IP addressing Plan
- Separate Interface functions through IP addressing (aggregates)
 - Unicast Routing – Routing Protocol Peering (p2p)
 - Unicast Routing – Routing Identifier (RID)
 - VTEP (NVE) Loopback
 - Multicast Routing Loopback (RP)



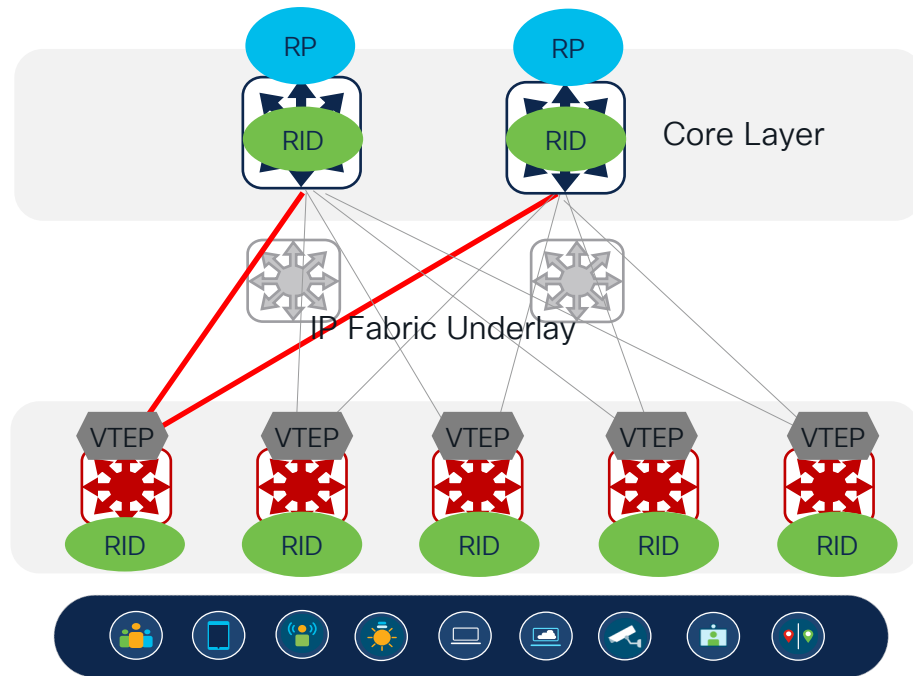
IP Addressing Principles

P2p Agg : 10.1.1.0/24
10.1.1.0/30
10.1.1.4/30
10.1.1.8/30

RID Agg : 10.10.10.0/24
10.10.10.1/32
10.10.10.2/32
10.10.10.3/32

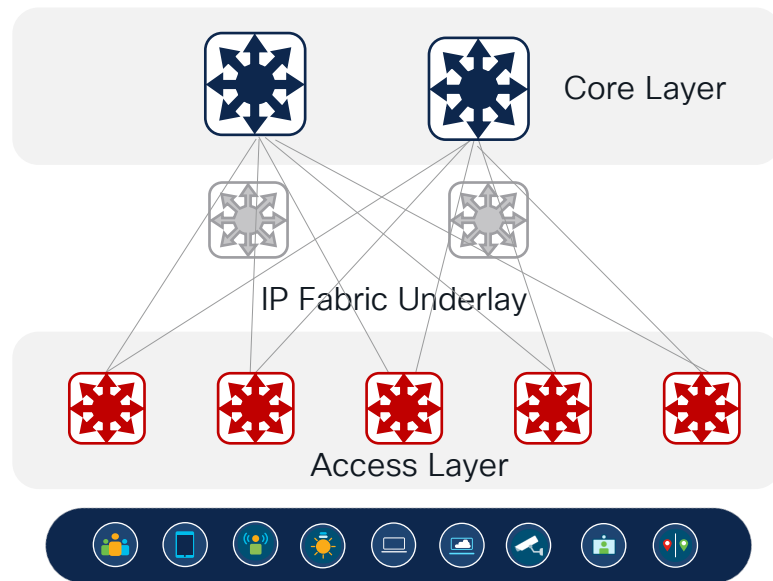
VTEP Agg : 10.200.200.0/24
10.200.200.1/32
10.200.200.2/32
10.200.200.3/32

RP Agg : 10.254.254.0/24
10.254.254.1/32



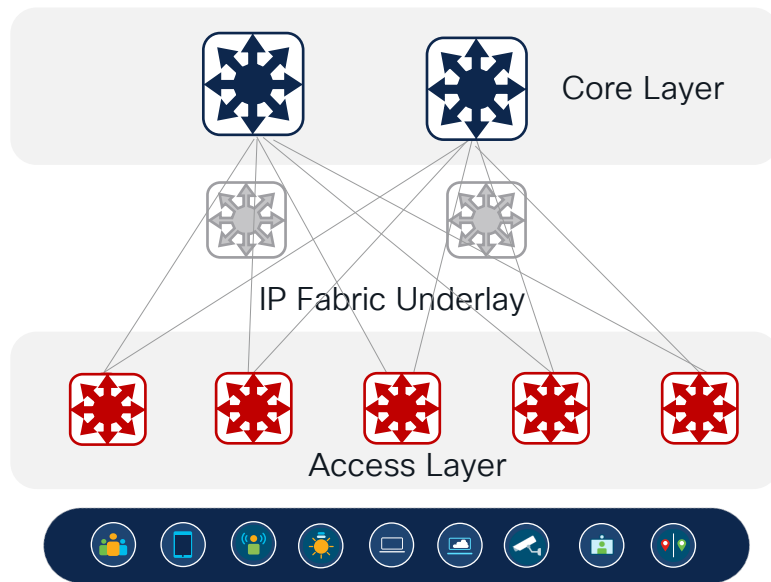
Unicast Routing - OSPF

- OSPF – watch your Network type!
 - Network Type Point-2-Point (P2P)
 - Preferred (only LSA type-1)
 - No DR/BDR election
- Suits well for routed interfaces/ports
- Full SPF calculation on Link Change



Unicast Routing - IS-IS

- IS-IS – what was this CLNS?
- Independent of IP (CLNS)
- Well suited for routed interfaces/ports
- No SPF calculation on Link change
- Fast Re-convergence
- Not everyone is familiar with it

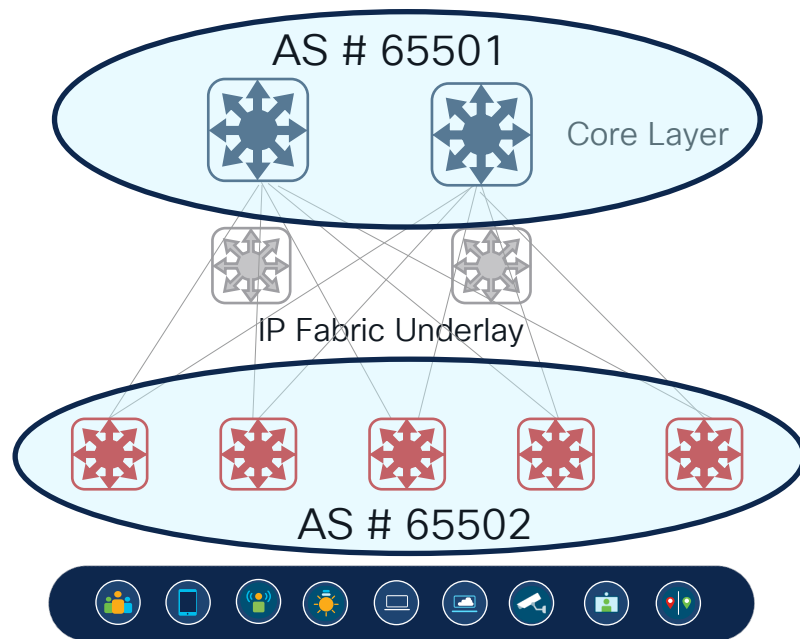


Unicast Routing - eBGP

- eBGP Underlay Routing – Service Provider style
 - Two Different Models
 - Two-AS
 - Multi-AS
- BGP is a Distance Vector Protocol
 - AS* are used to calculate the Path (AS_Path)

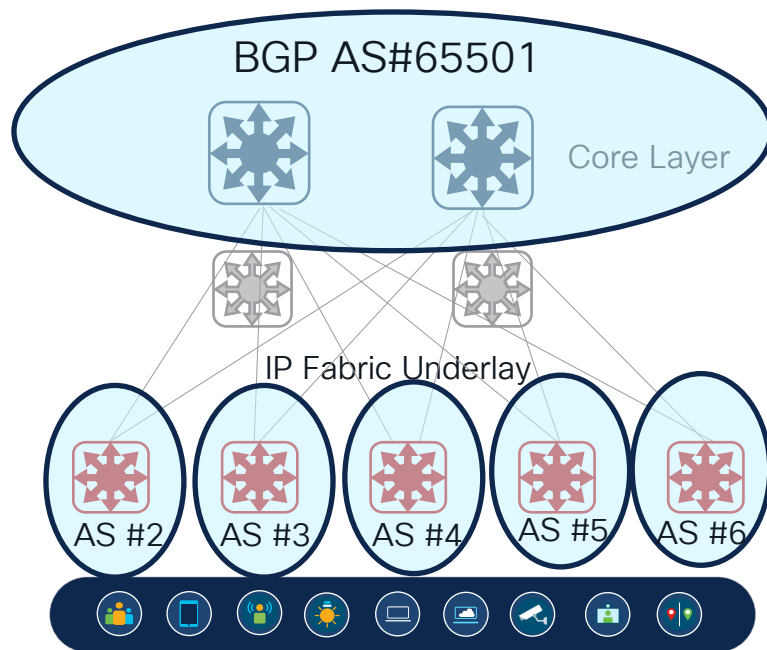
Unicast Routing - eBGP

- eBGP - TWO-AS, yes it works!
- eBGP peering for Underlay
 - Spine is not a Route-Reflector (eBGP)
 - Retain Route-targets
 - Disable BGP AS-Path check
- Underlay is Reachability !
 - Advertise all loopbacks
- Special Overlay Control-Plane treatment
 - Next-Hop needs to be unchanged
 - Disable BGP AS-path check



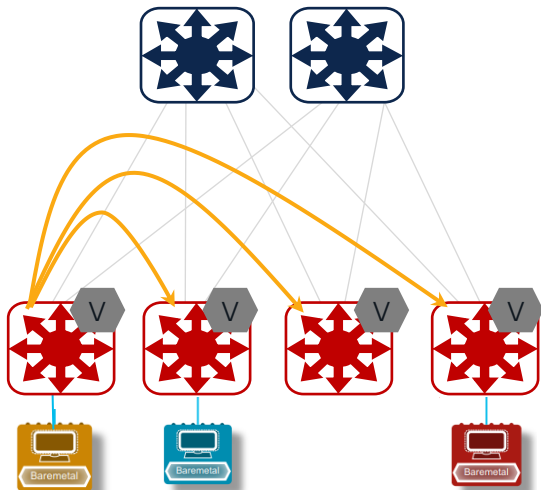
Unicast Routing - eBGP

- eBGP - Multi-AS, rebuild the Internet
- eBGP peering for Underlay
 - Spine is not a Route-Reflector(eBGP)
 - Retain Route-Targets
 - Next-Hop needs to be unchanged
- Underlay is Reachability !
 - Advertise all loopbacks
- Special Overlay Control-Plane treatment
 - Next-Hop needs to be unchanged

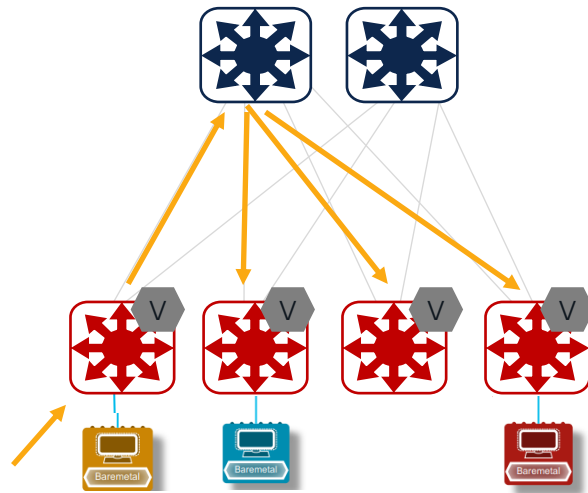


Overlay Broadcast, Unknown Unicast, Multicast (BUM) Forwarding

INGRESS-REPLICATION



MULTICAST-REPLICATION



Two mechanics to handle Broadcast, Unknown Unicast and Link-Local Multicast (BUM):

- Ingress-Replication – Convert each BUM packet to multiple Unicast packets and transmit to each remote VTEP
- Multicast-Replication – Convert each BUM packet to single Multicast packets and transmit in Underlay network

Multicast Enabled Underlay for BUM

- Only PIM ASM is supported on Catalyst 9k
- Multi-Destination Traffic (Broadcast, Unknown Unicast, etc.) needs to be replicated to ALL VTEPs serving a given VNI
- Each VTEP is Multicast Source & Receiver
- For a given VNI, all VTEPs act as a Sender and a Receiver
- Aggregation Switches make good Rendezvous-Point (RP) Locations in Topologies
- Reserve a range of Multicast Groups (Destination Groups/DGroups) to service the Overlay and optimize for diverse VNIs

Automation Tools

- DIY
- Ansible Playbook
- Intent Based Networking



Key Takeaways

VXLAN EVPN Overview

Migration Strategies

EVPN Fabric Considerations

Automation Tools

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

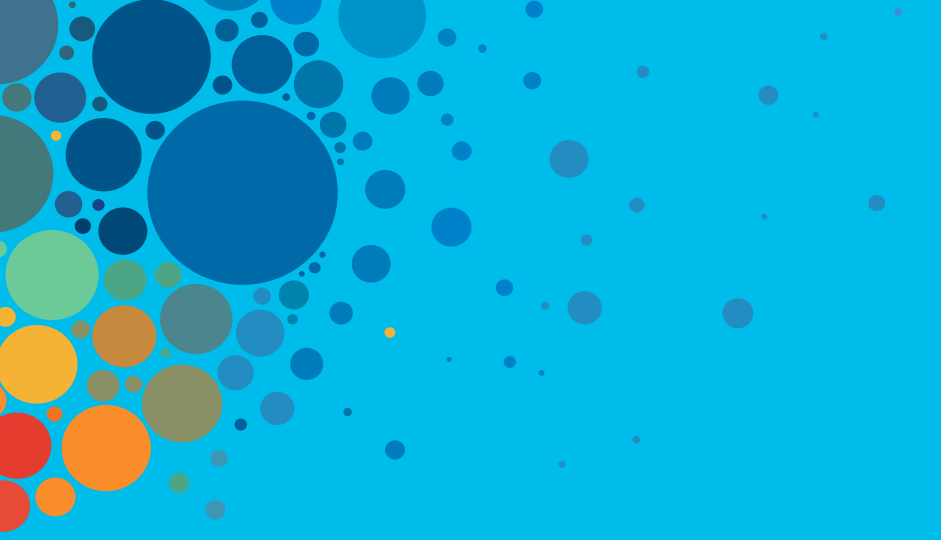
Cisco Guided Study Groups

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

CISCO *Live!*



#CiscoLive