

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Fabric Based Networking

What's the fuss and what are the choices?

Ashley Burton
Technical Solutions Architect
CCIE 3225
BRKENS-2700



#CiscoLiveAPJC

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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2700>



Fun Fact

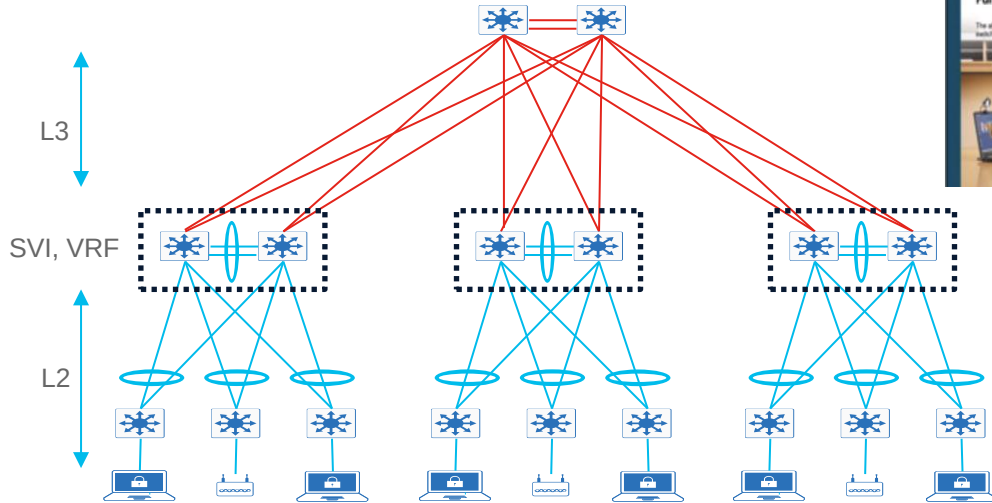


Polyester, Multifilament, Gut
Shape and Gauge
Tension
Flex/Stiffness
String Pattern

Agenda

- What is a network fabric?
- What are the drivers behind the adoption of fabric architectures?
- Fabric fundamentals
- What types of fabrics are available?
- BGP EVPN network fabrics
- LISP network fabrics
- Heads or Tails – driven by requirements
- Conclusion

The traditional enterprise network



Campus Network Design Fundamentals

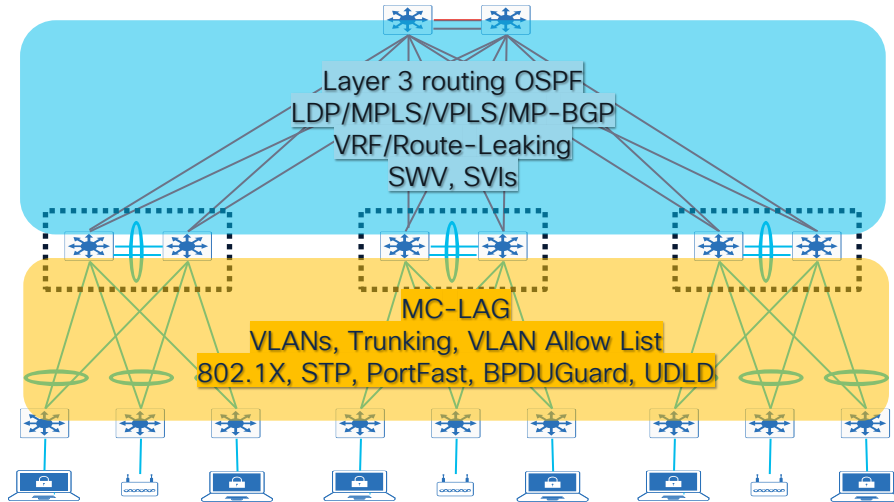
By Diane Teare, Catherine Paquet

Published Dec 8, 2005 by Cisco Press. Part of the Fundamentals series.

- Well known pattern, built for the last 20+ years
- Not much changed since
- Facilitates north-south connectivity
- Manual configuration and complexity

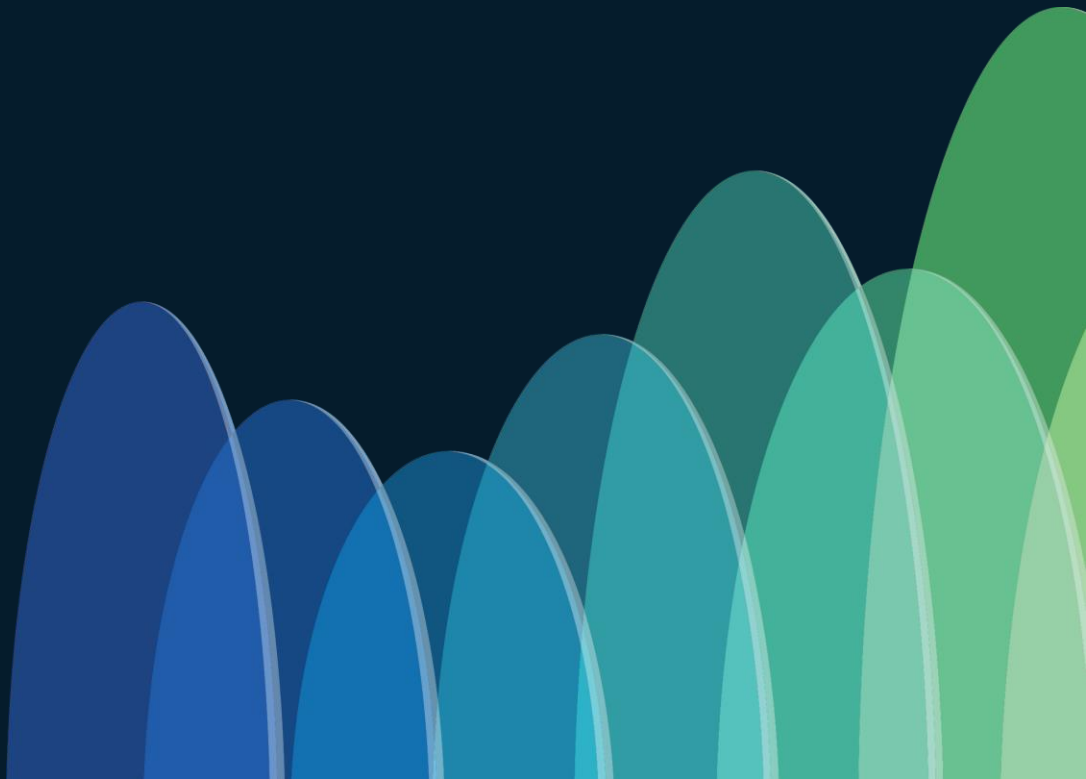
The traditional enterprise network

REALITY



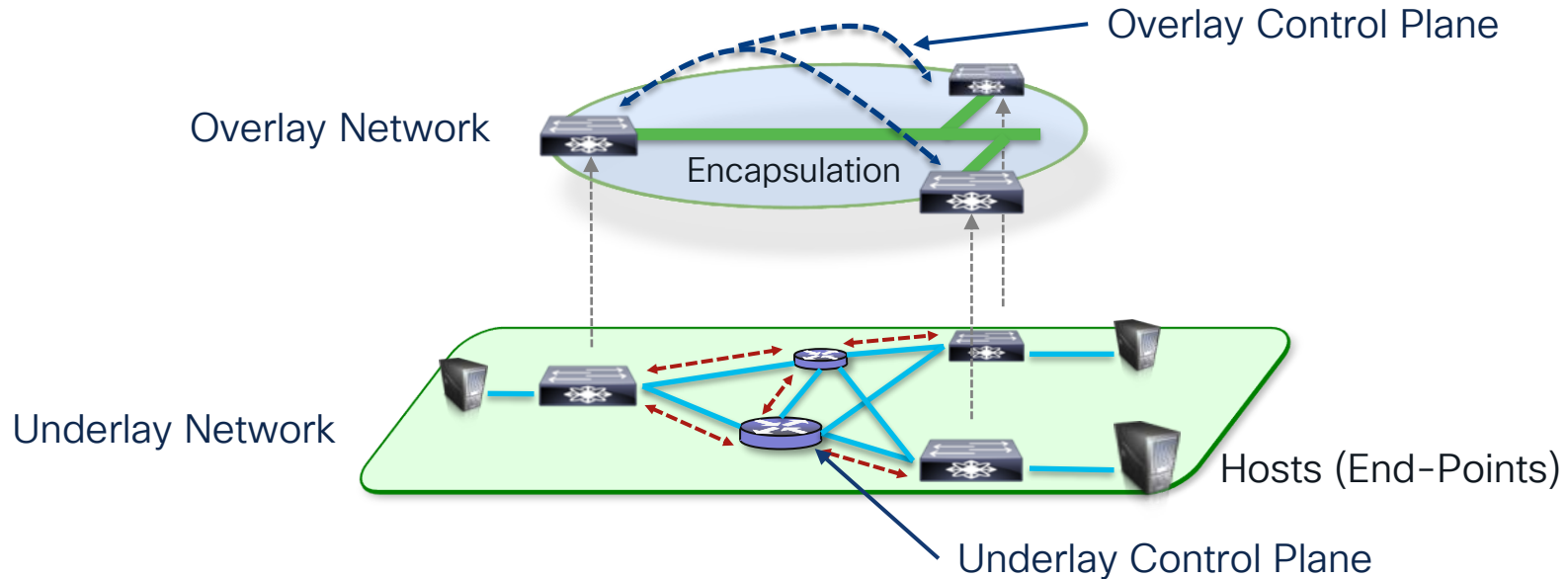
- Hard to automate – each device is unique
- Be-spoke “best guess config”
- Lots of protocols running on the same boxes
- Network security is an after thought
- Wireless is after thought

What is a network fabric?

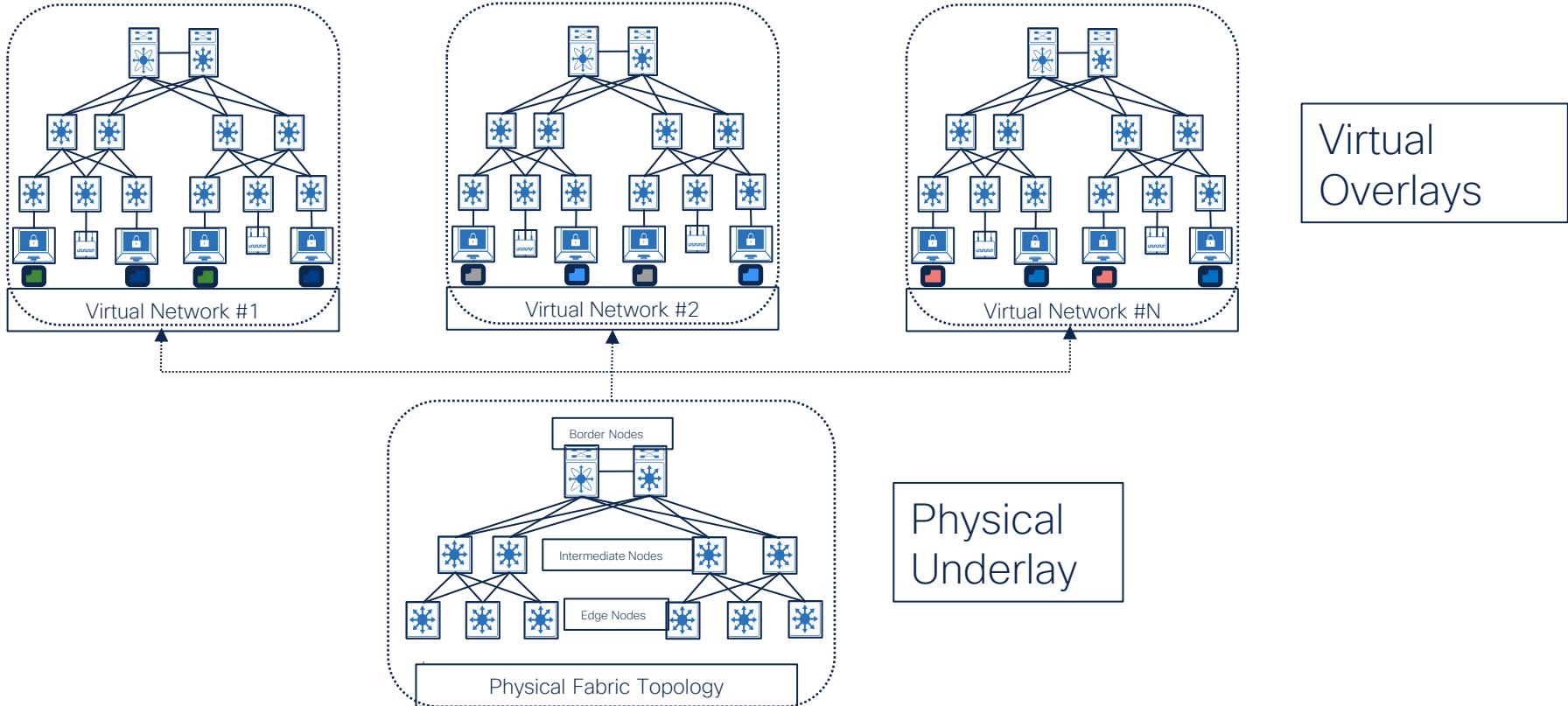


A Fabric is an Overlay

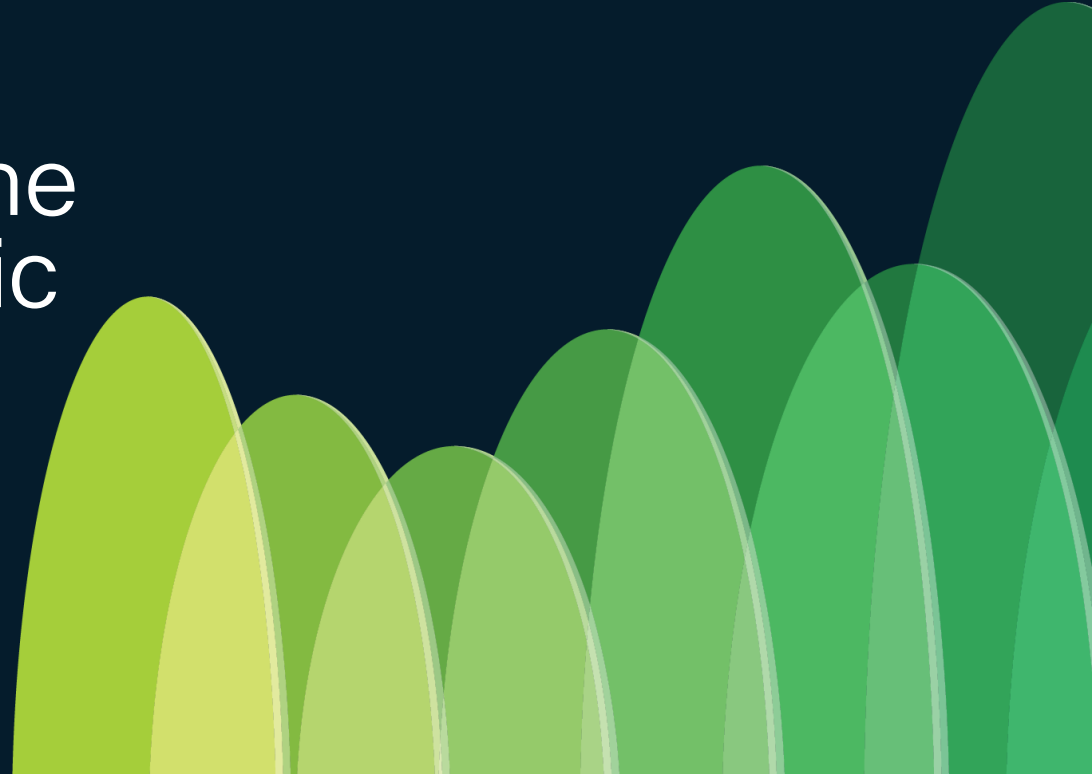
- A logical topology used to virtually connect devices, built on top of physical underlay topology
- Provides additional services not provided by the underlay



Fabric based networking



What are the
drivers behind the
adoption of fabric
architectures?



Why should I consider a fabric architecture?

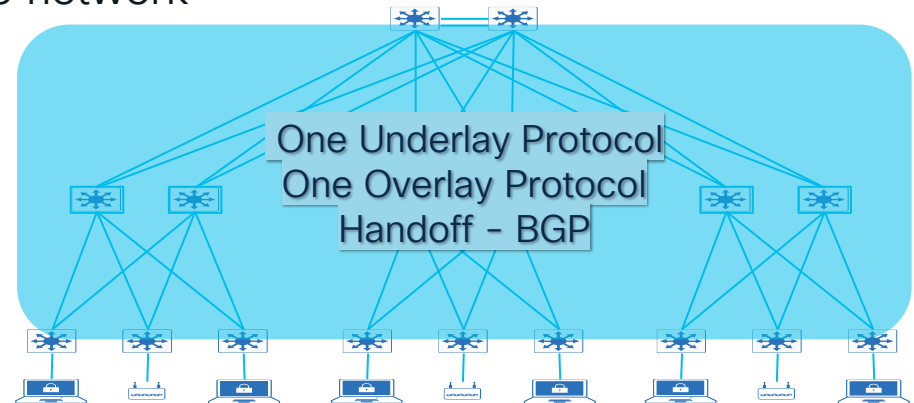


Business Outcomes

- Simplicity = Network Availability
- Segmentation
 - Security/Cyber
 - Isolate users, devices and IoT things
 - Contains blast radius of incident
 - IT/OT convergence
- Wireless Convergence
 - Improved wireless experience

Fabric solves network problems

- Fabric to the access removes Layer 2 protocols from the LAN
- Simple, scalable, reliable and *automatable* network
- Consistent access layer configurations
- Reliable Layer 2 extension over Layer 3 network
- Routing everywhere
- Convergence of wired and wireless

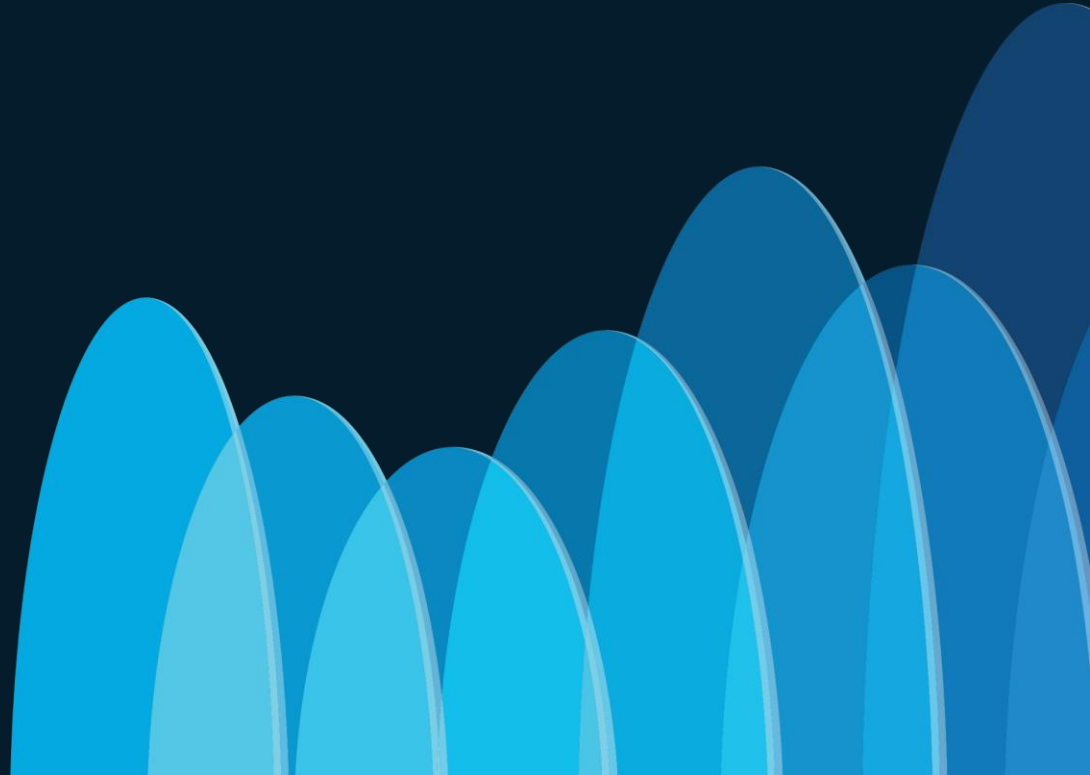


Fabric solves network CAMPUS problems

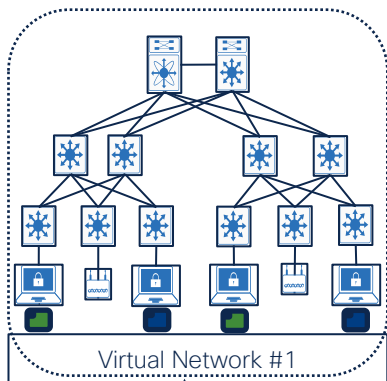
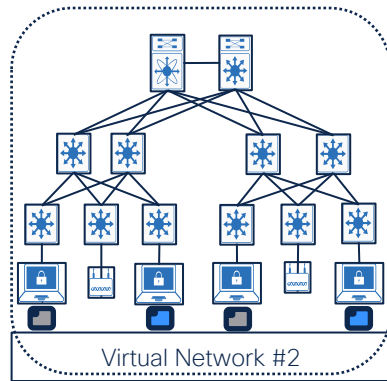
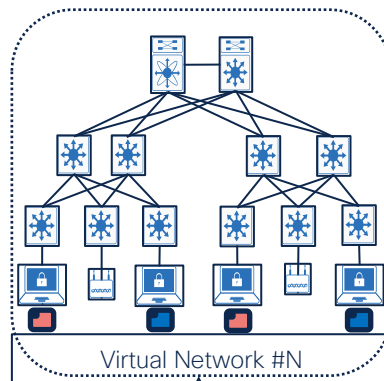
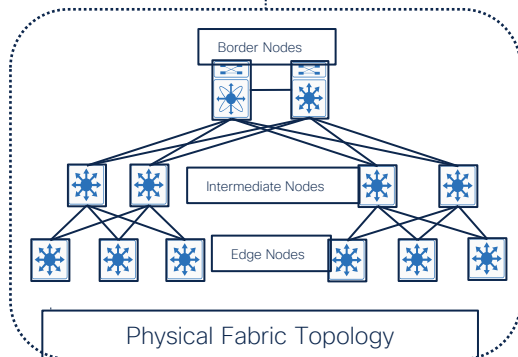
Three unique campus network requirements:

- Network topology is influenced by geography – cannot always build Leaf and Spine
- Wireless users are Roaming
- Massive amount of unmanaged, "headless" devices on the network – Segmentation

Fabric Fundamentals



Fabric based networking



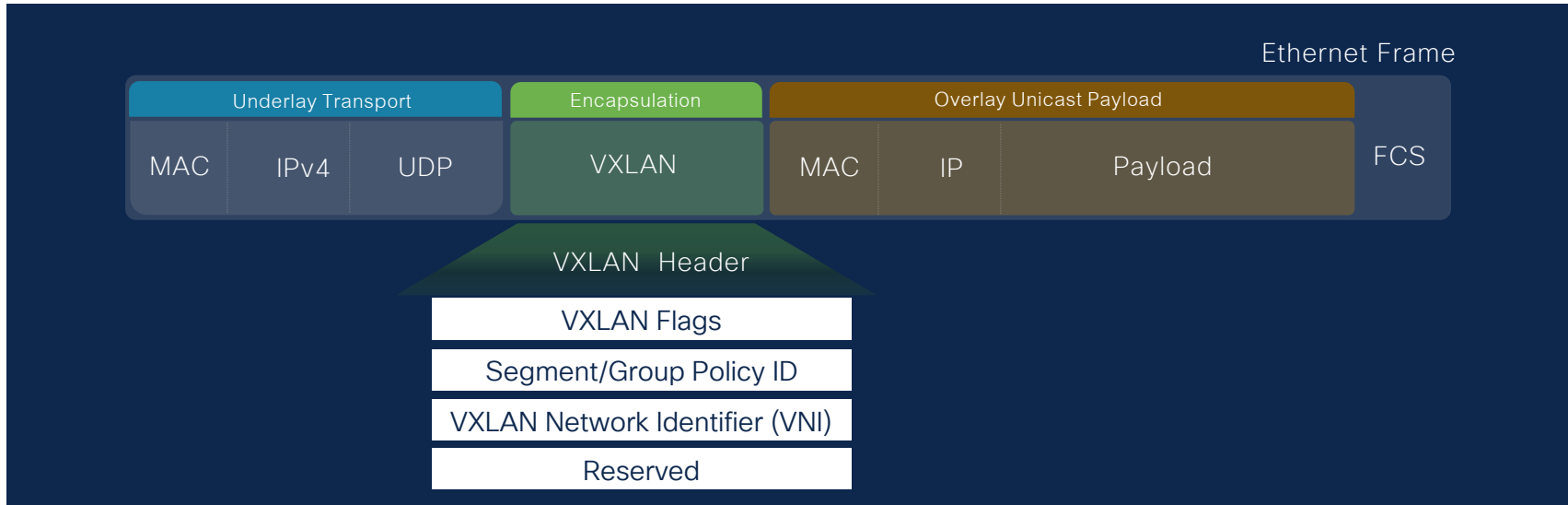
Overlay

- Device Connectivity
- Authentication
- Authorization
- Policy
- Segmentation

Underlay

- Predictable
- Low Touch
- Stable
- Simple

Policy in a fabric

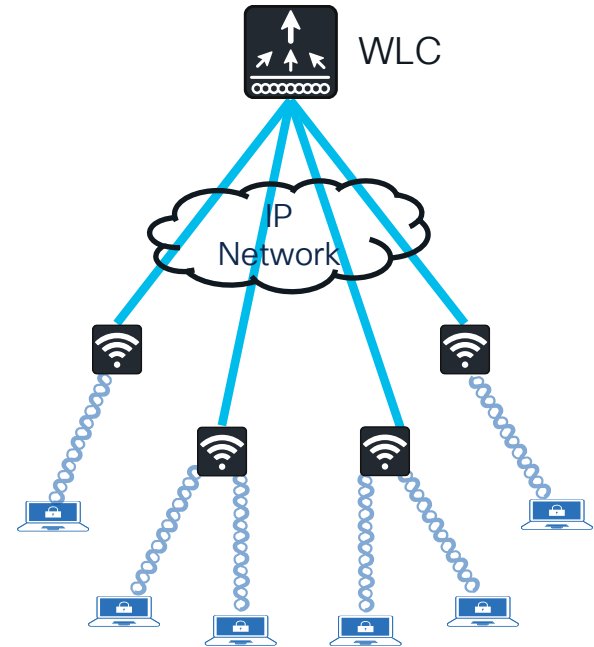


Macro Segmentation = VNID = VRF

Micro Segmentation within a VNID/VRF = SGT/GBP

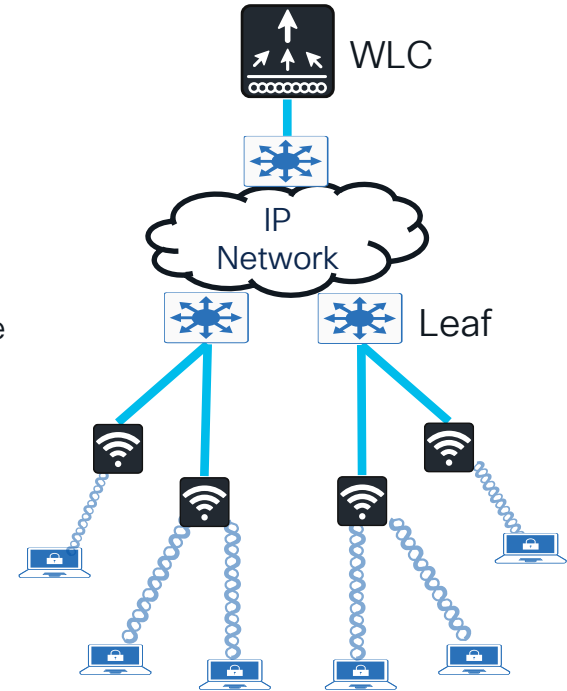
Wireless in a fabric architecture – centralised switching

- Pros:
 - Fast wireless roaming
 - Do not need to worry about subnet management
- Cons:
 - Suboptimal traffic flow
 - Performance bottleneck – especially with wireless-first approach
 - Different sets of policies for wired/wireless users
 - Need WLC hardware capable of pushing 10Gbps +
 - Need switch hardware with large TCAM tables adjacent to the WLC

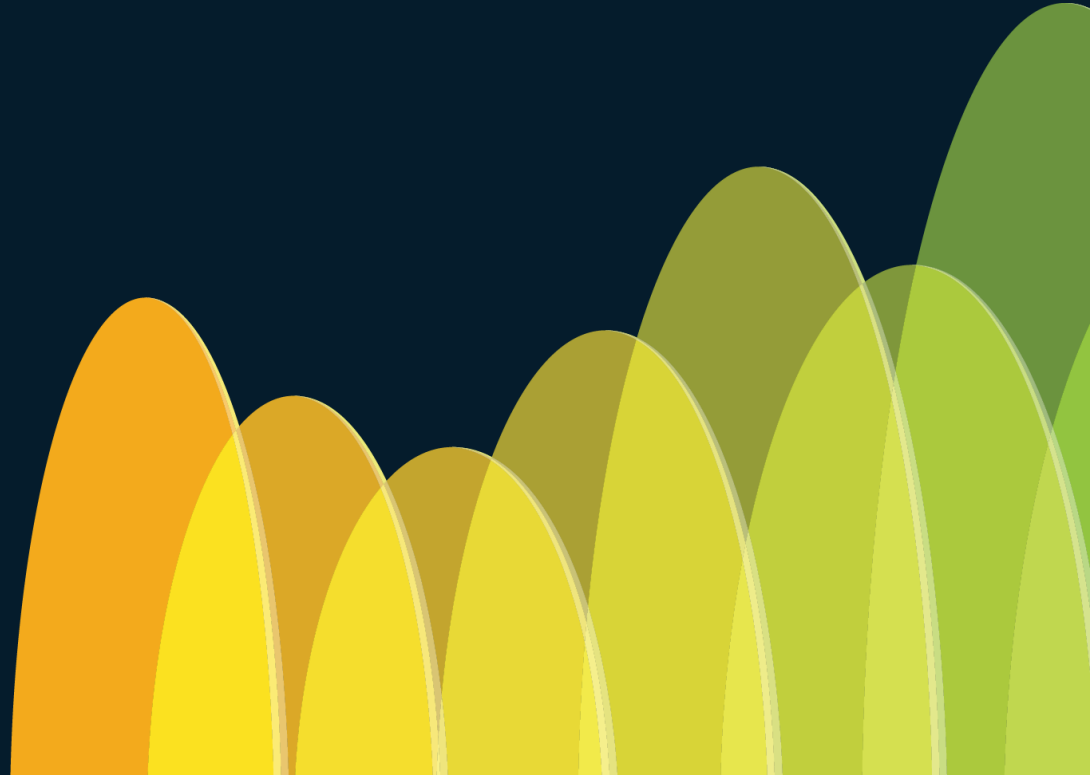


Wireless in a fabric architecture – distributed switching

- Pros:
 - No performance bottleneck, optimal traffic flow
 - Consistent policy for wired/wireless users
- Cons:
 - Relies on wired control plane
 - Must understand how AP's communicate with other and with the switching infrastructure.

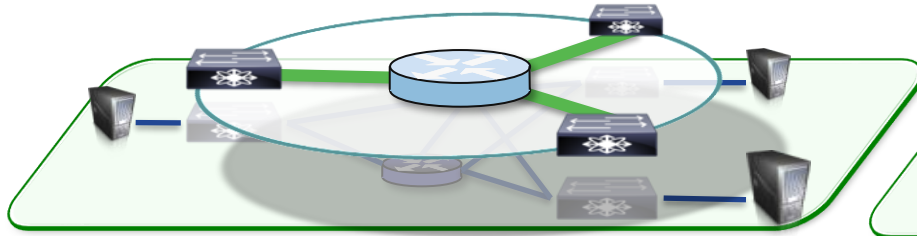


What types of
fabrics are
available ?



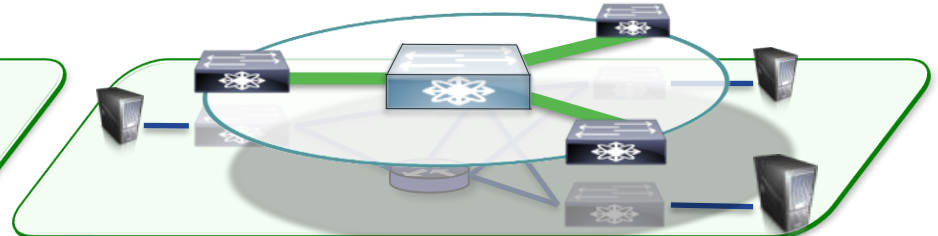
Fabrics with VXLAN Encapsulation

VXLAN Provides a Network with Segmentation & Scale



LISP

- **Network Simplification** Lightweight, extensible, massive scale with rapid convergence. Single overlay for wired/wireless
- **Mobility First Requirement** Fabric Integrated Wireless, L2 mobility, enhanced wireless performance
- **Segmentation** Zero-Trust Architecture with Micro and Macro Segmentation. Unified Wired + Wireless policy



BGP EVPN

- **One Fabric Architecture (Campus & DC)** Operational ease with a single familiar protocol
- **Multi-vendor interoperability** Vendor-agnostic
- **Flexibility** Customizable overlay network types and topologies
- **Segmentation** Zero-Trust Architecture with Micro and Macro Segmentation

IETF – Open standards

LISP

Dataracker Groups Documents Meetings Other User			
RFCs (30 hits)			
RFC 9437 (was draft-ietf-lisp-pubsub)	18 pages	2023-08	Proposed Standard RFC
Publicity/Subscribe Functionality for the Locator/ID Separation Protocol (LISP)			
RFC 9239 (was draft-ietf-lisp-introduction)	24 pages	2022-10	Informational RFC
An Architectural Introduction to the Locator/ID Separation Protocol (LISP)			
RFC 9300 (was draft-ietf-lisp-rf6830b4)	33 pages	2022-10	Proposed Standard RFC
The Locator/ID Separation Protocol (LISP)			
RFC 9301 (was draft-ietf-lisp-rf6833b4)	42 pages	2022-10	Proposed Standard RFC
Locator/ID Separation Protocol (LISP) Control Plane			
RFC 9302 (was draft-ietf-lisp-6834b4)	15 pages	2022-10	Proposed Standard RFC
Locator/ID Separation Protocol (LISP) Map-Versioning			
RFC 9303 (was draft-ietf-lisp-arc)	23 pages	2022-10	Proposed Standard RFC
Locator/ID Separation Protocol Security (LISP-SEC)			
RFC 9304 (was draft-ietf-lisp-rf68113b4)	5 pages	2022-10	Proposed Standard RFC
Locator/ID Separation Protocol (LISP): Shared Extension Message and IANA Registry for Packet Type Allocations			
RFC 9305 (was draft-ietf-lisp-gsq)	14 pages	2022-10	Proposed Standard RFC
Locator/ID Separation Protocol (LISP) Generic Protocol Extension			
RFC 9306 (was draft-ietf-lisp-vendor-leaf)	5 pages	2022-10	Experimental RFC
Vendor-Specific LISP Canonical Address Format (LCAF)			
RFC 8378 (was draft-ietf-lisp-signal-free-multicast)	21 pages	2018-05	Experimental RFC
Signal-Free Locator/ID Separation Protocol (LISP) Multicast			
RFC 8111 (was draft-ietf-lisp-ddt)	44 pages	2017-05	Experimental RFC
Locator/ID Separation Protocol Delegated Database Tree (LISP-DDT)			
RFC 8112 (was draft-farinacci-lisp-rig)	11 pages	2017-05	Informational RFC
Locator/ID Separation Protocol Delegated Database Tree (LISP-DDT) Referral Internet Group (RIG)			
RFC 8113 (was draft-ietf-lisp-type-iana)	6 pages	2017-03	Experimental RFC
Locator/ID Separation Protocol (LISP): Shared Extension Message & IANA Registry for Packet Type Allocations			
RFC 8060 (was draft-ietf-lisp-leaf)	38 pages	2017-02	Experimental RFC
LISP Canonical Address Format (LCAF)			
RFC 8061 (was draft-ietf-lisp-crypto)	18 pages	2017-02	Experimental RFC
Locator/ID Separation Protocol (LISP) Data-Plane Confidentiality			
RFC 8059 (was draft-ietf-lisp-join-contributors-for-lisp)	9 pages	2017-01	Experimental RFC
PM Join Attributes for Locator/ID Separation Protocol (LISP) Environments			
RFC 7954 (was draft-ietf-lisp-aid-block)	12 pages	2016-09	Experimental RFC
Locator/ID Separation Protocol (LISP) Endpoint Identifier (EID) Block			
RFC 7955 (was draft-ietf-lisp-aid-block-mgmt)	10 pages	2016-09	Informational RFC
Management Guidelines for the Locator/ID Separation Protocol (LISP) Endpoint Identifier (EID) Block			
RFC 7954 (was draft-ietf-lisp-aid-block)	18 pages	2016-04	Informational RFC
Locator/ID Separation Protocol (LISP) Impact			

EVPN

Dataracker Groups Documents Meetings Other User			
RFC 9469 (was draft-ietf-nvo3-evpn-applicability)			
Applicability of Ethernet Virtual Private Network (EVPN) to Network Virtualization over Layer 3 (NVO3) Networks			
RFC 9251 (was draft-ietf-bess-evpn-igmp-mid-proxy)	30 pages	2022-06	Proposed Standard RFC
Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Proxies for Ethernet VPN (EVPN)			
RFC 9161 (was draft-ietf-bess-evpn-proxy-arp-nd)	22 pages	2022-01	Proposed Standard RFC
Operational Aspects of Proxy ARP/ND in Ethernet Virtual Private Networks			
RFC 9135 (was draft-ietf-bess-evpn-inter-subnet-forwarding)	30 pages	2021-10	Proposed Standard RFC
Integrated Routing and Bridging in Ethernet VPN (EVPN)			
RFC 9136 (was draft-ietf-bess-evpn-prefix-advertisement)	31 pages	2021-10	Proposed Standard RFC
IP Prefix Advertisement in Ethernet VPN (EVPN)			
RFC 9047 (was draft-ietf-bess-evpn-na-flags)	10 pages	2021-06	Proposed Standard RFC
Propagation of ARP/ND Flags in an Ethernet Virtual Private Network (EVPN)			
RFC 9062 (was draft-ietf-bess-evpn-oam-req-fmwk)	16 pages	2021-06	Informational RFC
Framework and Requirements for Ethernet VPN (EVPN) Operations, Administration, and Maintenance (OAM)			
RFC 9014 (was draft-ietf-bess-dci-evpn-overlay)	24 pages	2021-05	Proposed Standard RFC
Interconnect Solution for Ethernet VPN (EVPN) Overlay Networks			
RFC 8560 (was draft-ietf-bess-evpn-vpls-seamless-integ)	16 pages	2019-05	Proposed Standard RFC
Seamless Integration of Ethernet VPN (EVPN) with Virtual Private LAN Service (VPLS) and Their Provider Backbone Bridge (PBB) Equivalents			
RFC 8584 (was draft-ietf-bess-evpn-df-election-framework)	32 pages	2019-04	Proposed Standard RFC
Framework for Ethernet VPN Designated Forwarder Election Extensibility			
RFC 8398 (was draft-ietf-bess-evpn-usage)	31 pages	2018-05	Informational RFC
Usage and Applicability of BGP MPLS-Based Ethernet VPN			
RFC 8365 (was draft-ietf-bess-evpn-overlay)	33 pages	2018-03	Proposed Standard RFC
A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)			
RFC 8317 (was draft-ietf-bess-evpn-atree)	23 pages	2018-01	Proposed Standard RFC
Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) and Provider Backbone Bridging EVPN (PBB-EVPN)			
RFC 8214 (was draft-ietf-bess-evpn-ospm)	17 pages	2017-08	Proposed Standard RFC
Virtual Private Wire Service Support in Ethernet VPN			
RFC 7734 (was draft-ietf-bess-spbm-evpn)	11 pages	2016-01	Proposed Standard RFC
Support for Shortest Path Bridging MAC Mode over Ethernet VPN (EVPN)			
RFC 7623 (was draft-ietf-l2vpn-pbb-evpn)	23 pages	2015-09	Proposed Standard RFC
Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)			
RFC 7332 (was draft-ietf-l2vpn-evpn)	55 pages	2015-02	Proposed Standard RFC
BGP MPLS-Based Ethernet VPN			
RFC 7209 (was draft-ietf-l2vpn-evpn-req)	15 pages	2014-05	Informational RFC
Requirements for Ethernet VPN (EVPN)			

- Interoperability
- Vendor lock-in – consider the automation and management tool

BGP EVPN network fabrics



Enterprise Campus BGP EVPN Drivers



Industry Standard



Multi-vendor IT strategy



One Fabric Architecture



Unified operation across network infrastructure



Proven and Scalable



BGP protocol history. Minimal new learning curve



Hierarchical Fabric Domain



Multi-tier overlay network architecture



Flexible Overlay



Use-case driven. Customized overlay networks types & topologies

BGP EVPN System Roles



BORDER-GATEWAY:

A gateway point of between two or more BGP EVPN administrative domain boundary



BORDER :

A gateway point of 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 : Route Reflector (not necessarily physical – can be collapsed to Border)

A BGP EVPN role that reflects the L2/L3 VPN prefixes providing hierarchical neighbor peering, learning and distribution point

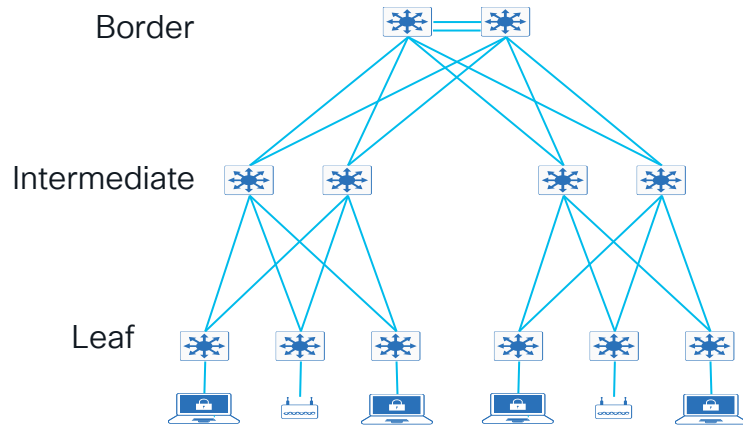


VTEP (LEAF) :

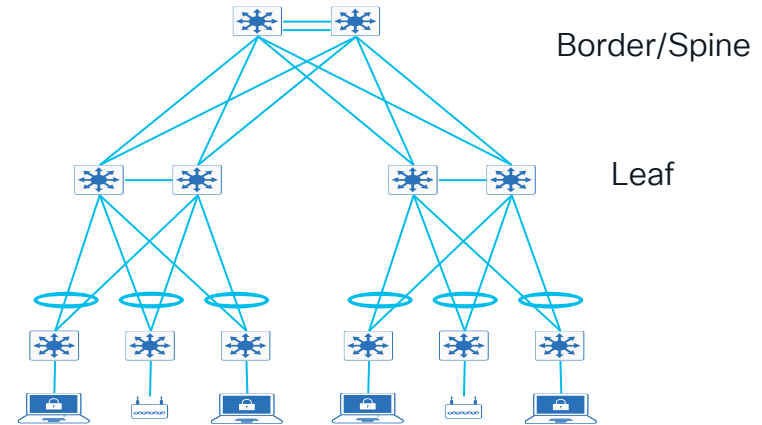
An origination and termination point of VXLAN enabled overlay network

BGP EVPN design considerations

Routed Access



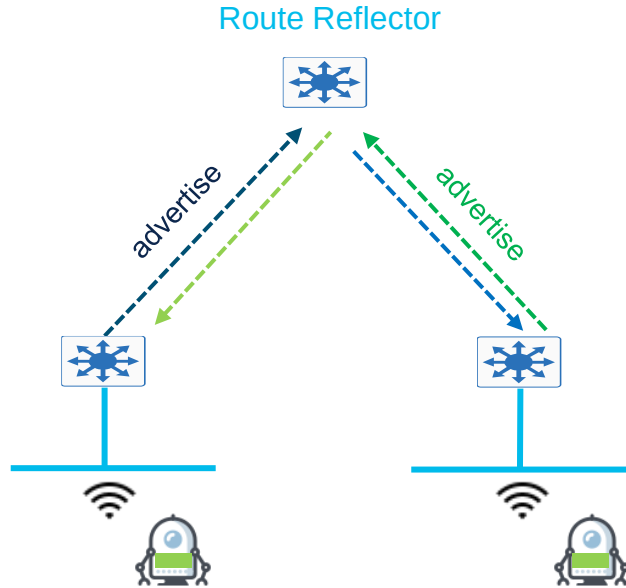
L2 Access with MLAG



Note: Dual Active ESI – Future IOS-XE release

BGP EVPN design considerations

Host registration



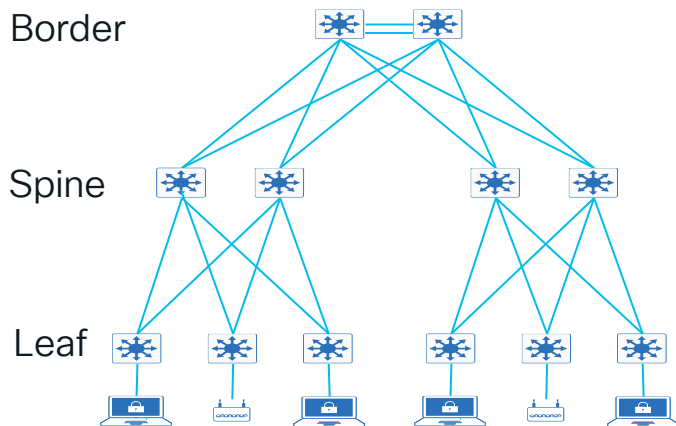
- Host Registration

- Leaf (BGP Speaker) advertises to route reflector – if /32 or new subnet
- Route reflector advertises to all edges
- This multiplies with additional route reflectors.
- I.e. in a design with 2 route reflectors each leaf switch will receive 2 updates when a host registers and 2 updates when a host leaves the fabric

BGP EVPN design considerations

IP Mobility

Routed Access

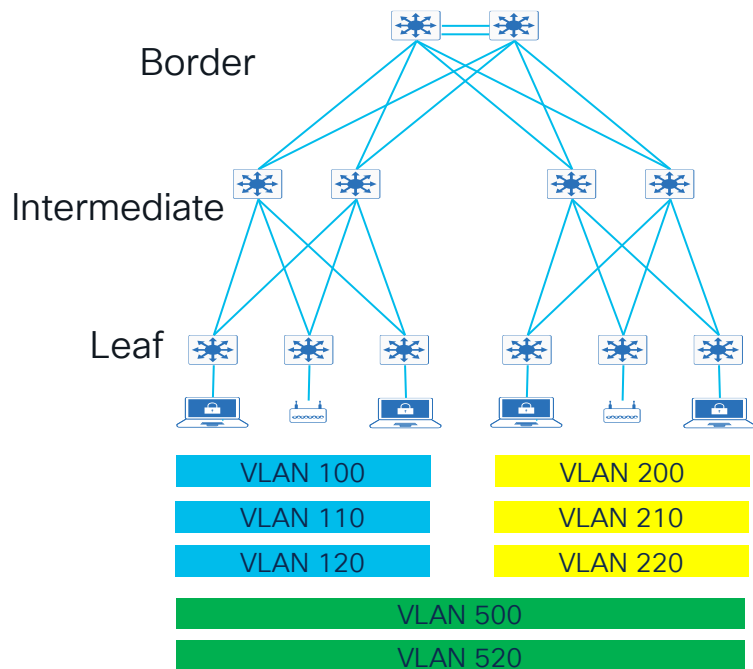


- Access Layer TCAM resources
 - Every access switch has a complete and consistent routing table
 - Fabric size is limited by TCAM resources in access switch (lowest common denominator)
 - Total number of host routes = maximum number of endpoints
- Note : Endpoint address
 - 1 x TCAM slot per IPv4 address
 - ~4 x TCAM slots per IPv6 address

BGP EVPN design considerations

Zones

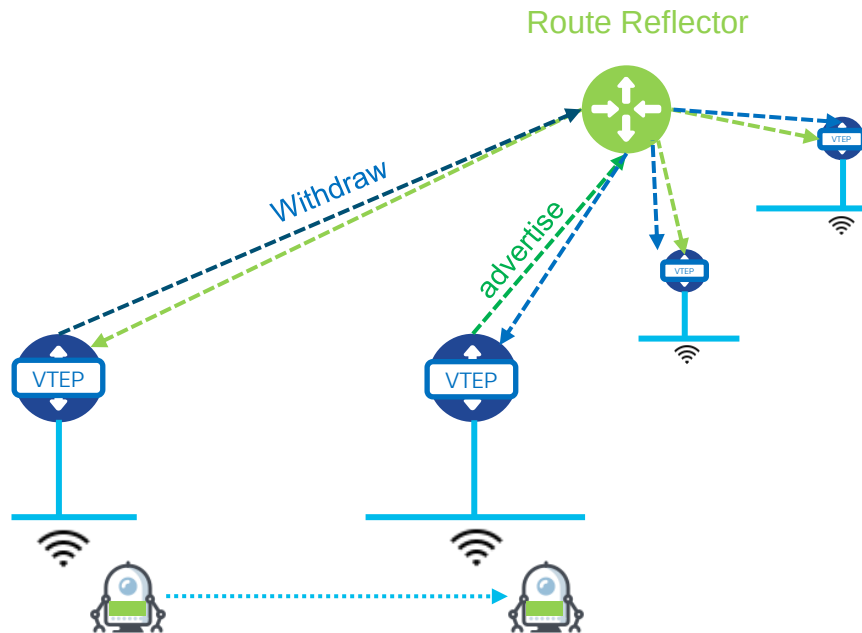
Routed Access



- Contain subnets to distribution blocks
 - Eliminates TCAM scale concern
- Restrict the number of stretched layer 2 VLANs

Mobility in the access

BGP Control Plane – Pervasive move signaling and processing



- Dense signaling:

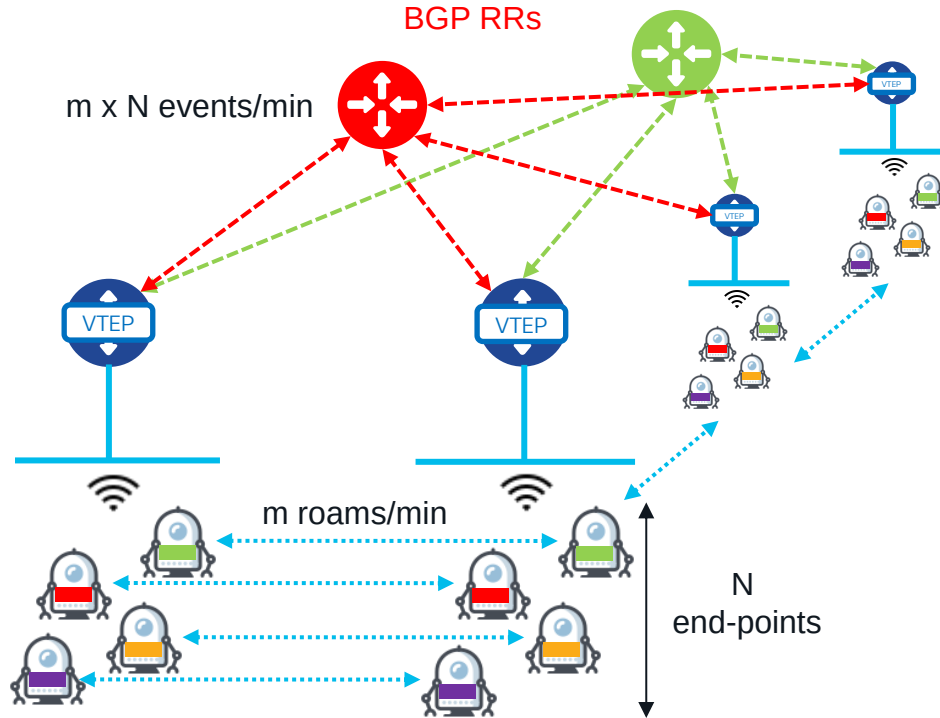
- All VTEP's are notified of the move **twice**
- Local events triggers a **global network-wide event**

- Processing:

- Path computation at RR and VTEP's
- Replication of the routing updates to all nodes

Mobility in the access

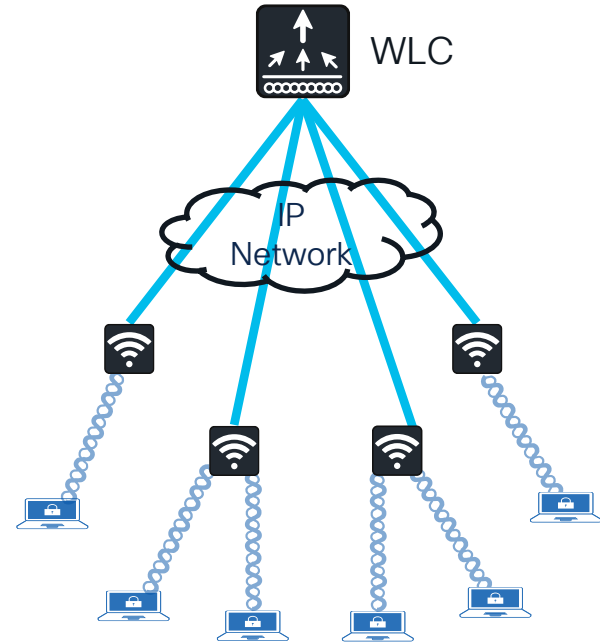
BGP Control Plane – Vertical Scale



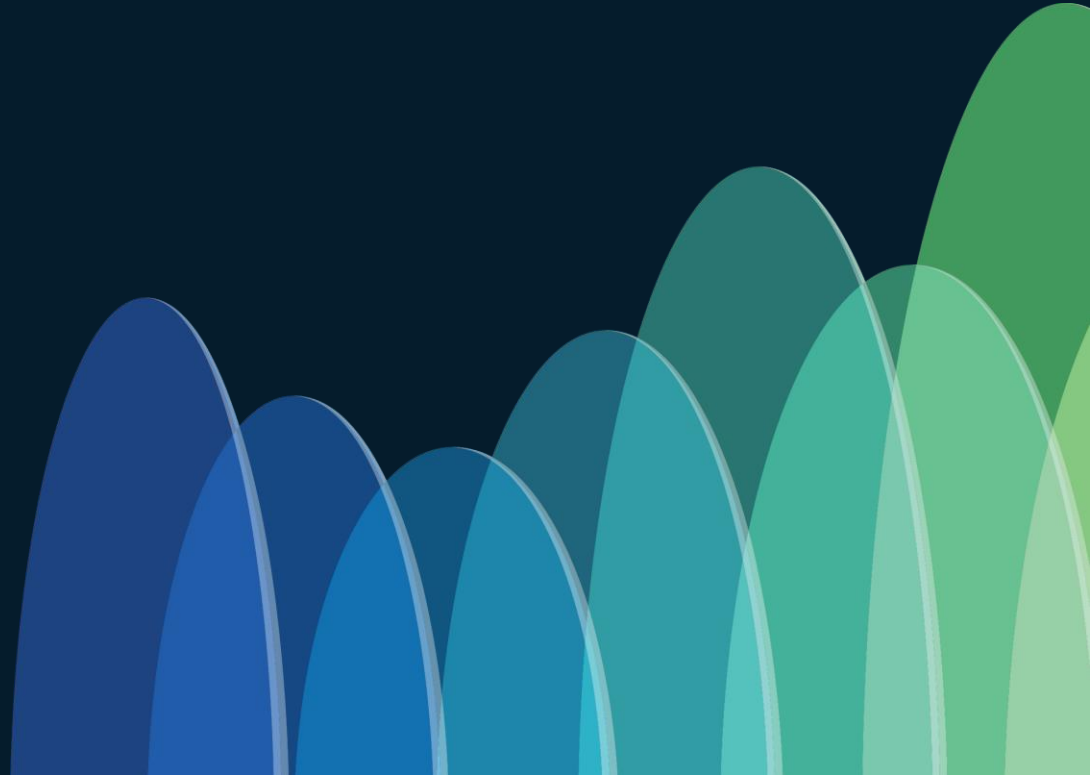
- Attempt to scope prefixes to different control plane nodes
 - VTEP processing all updates remains the bottleneck
 - Horizontally scale **NOT** achievable
- Network convergence and hence performance degrades as more VTEPs are added

BGP EVPN Wireless design considerations

- Number of wireless clients
- The size/scope of the wireless roam – can the fabric be broken into multiple roam zones?
- The number of roams per second/minute within the zone
- Number of leaf switches in the zone/campus



LISP network fabrics



SDA-LISP: Recommended by Cisco for Campus

3,600+ Campus Deployments
30% Year to Year Growth

Simple

- Industry standard-based and optimized for enterprise campus
- Configurations automated based on business intent

Efficient

- Scales to a large number of endpoints
- Rapid converge

Extensible

- Simple directory structure to map endpoints to locations
- Highly extensible to address new use cases

Wired + Wireless

- Centralized control plane with distributed data plane
- Seamless campus wide mobility

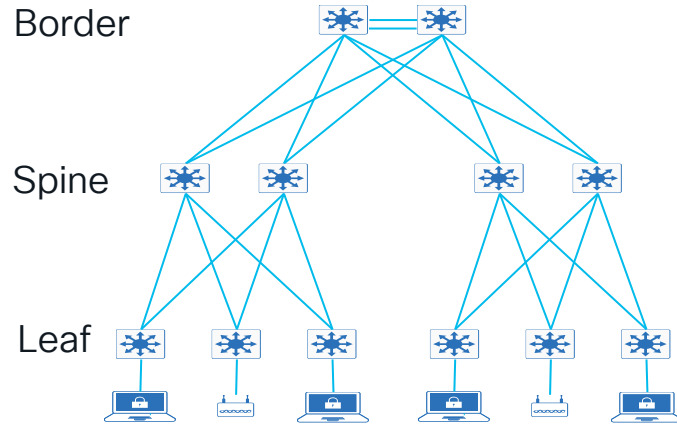
CISCO *Live!*



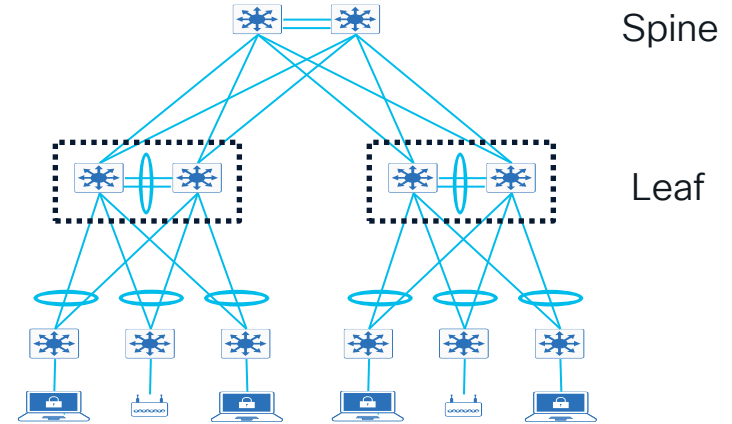
- © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

LISP design considerations

Routed Access



L2 Access with MLAG



LISP operations

LISP :: Mapping Resolution “Level of Indirection”

- LISP “Level of Indirection” is analogous to a DNS lookup

- DNS resolves IP addresses for URL Answering the “WHO IS” question

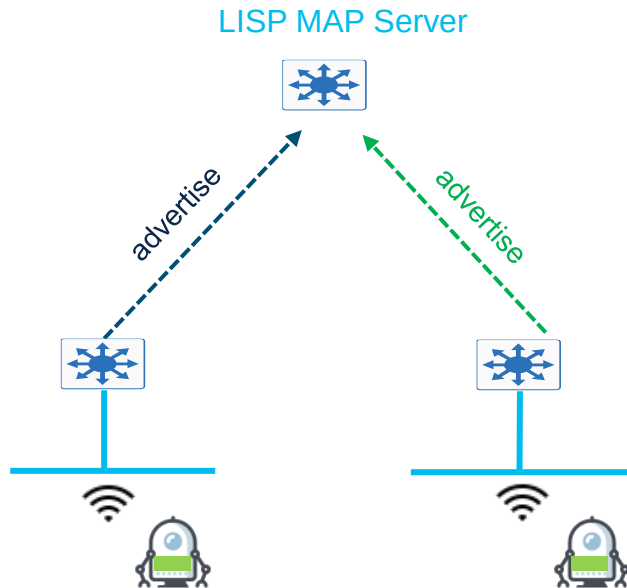


- LISP resolves locators for queried identities Answering the “WHERE IS” question



LISP design considerations

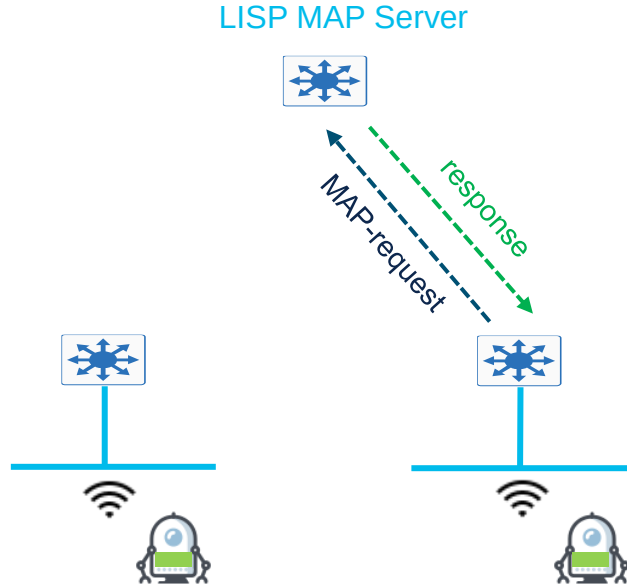
Host registration



- Host Registration
 - Leaf registers to MAP Sever
 - Endpoint ID – EID
 - Routing Locator – RLOC

LISP design considerations

Host resolution

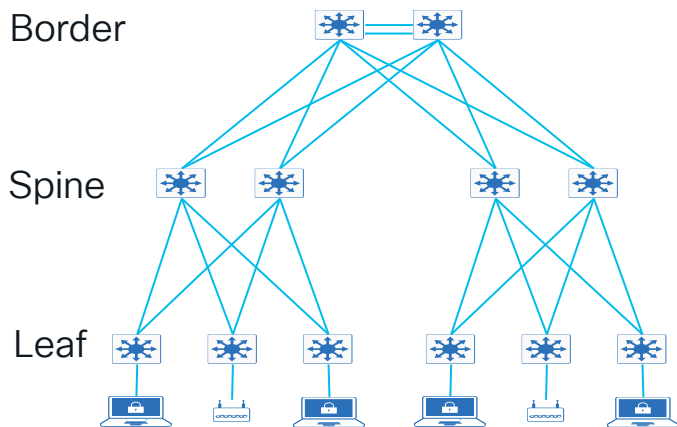


- Host resolution

- Leaf issues a MAP request to the MAP Server
- MAP Server responds to leaf
- Response is cached on leaf

LISP design considerations

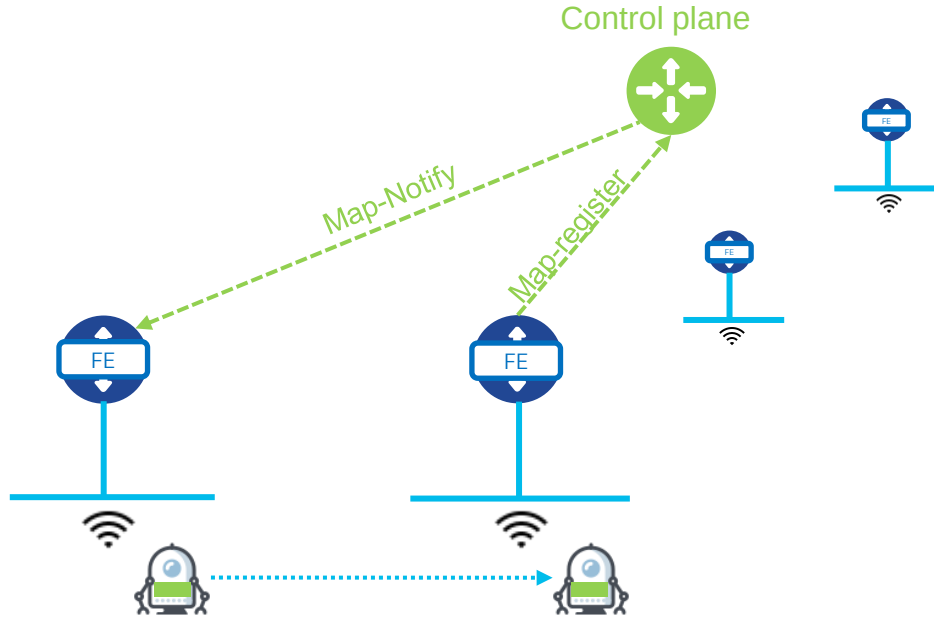
TCAM resources



- Leaf switch TCAM
 - Efficient and scalable
 - Doesn't limit the scale of the fabric
- Border Nodes
 - Need to know all routes of all hosts and therefore TCAM resources and number of routes limits the size of the entire fabric.

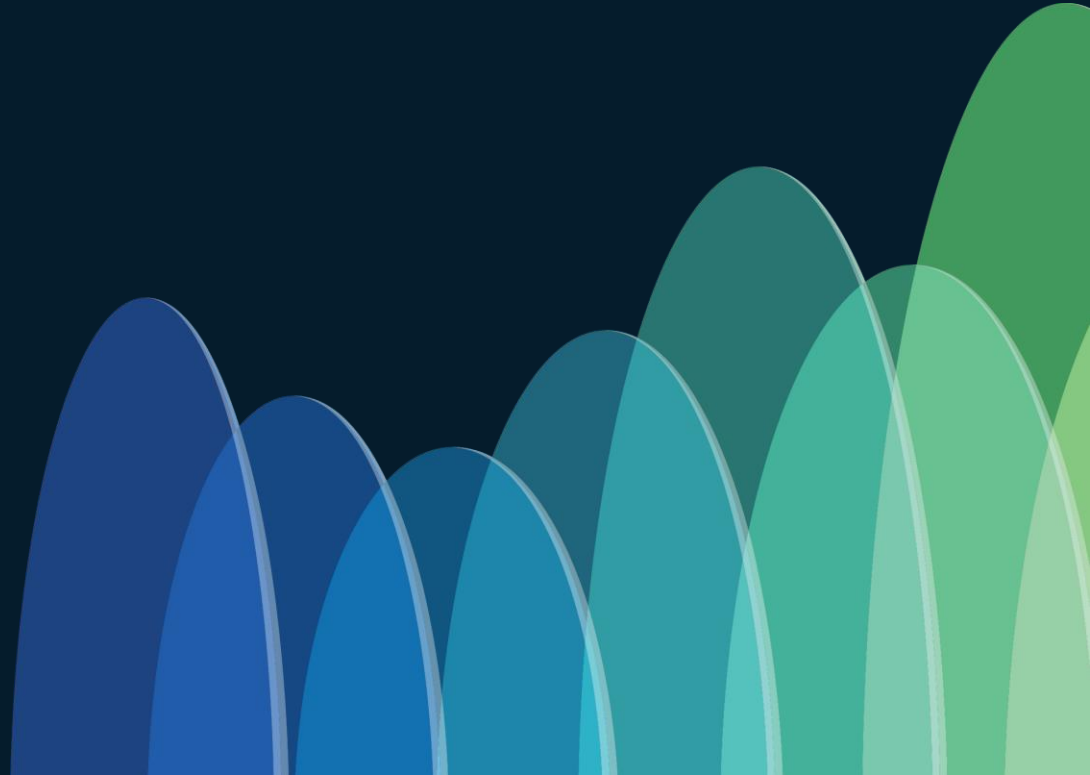
Mobility in the access

LISP Control Plane - Scoped move signaling



- Sparse signaling: Only the FEs involved in the move
- Light processing: Only mapping updates, no path calculation
- The rate of events at the FEs is a fraction of the total rate of events
- $\text{Rate@FE} = (m \times N) / \text{number of FEs}$

Heads or Tails



The Engineering Triangle

Fabric technology options

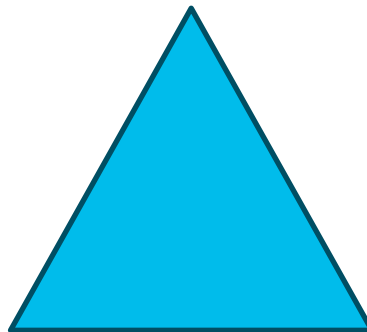
BGP EVPN

- **CAN** meet all 3 of the requirements individually
- **CAN** meet ANY 2 of the 3 requirements at the same time

LISP

- **CAN** meet all 3 of the requirements individually
- **CAN** meet ANY 2 of the 3 requirements at the same time
- **CAN** meet all 3 of the requirements at the same time

Large Scale
3 Tier Architecture



Distributed Wi-Fi Data Plane
Campus Wide Roaming

Protocol Simplification
L3 to the Access

Customer #1 - Heads

Requirements



Single Fabric Overlay from DC to Campus



Macro and Micro Segmentation



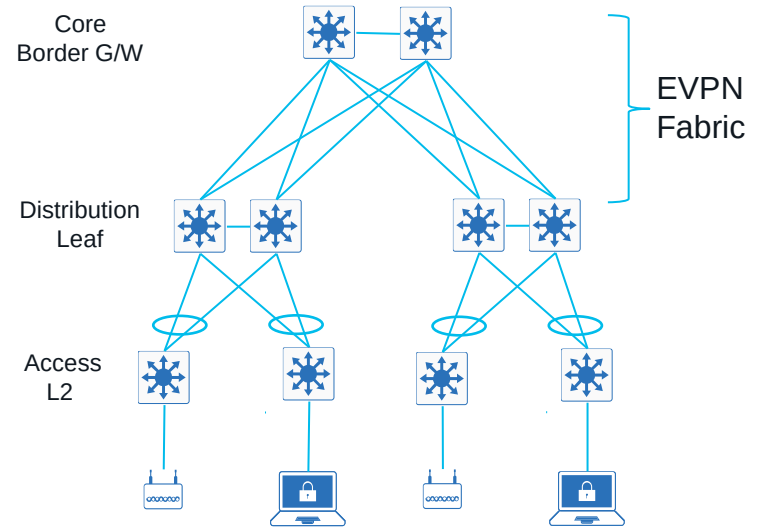
Maintain existing L2 access layer



Customer #1 - Heads

Solution

- BGP EVPN control plane
- L2 access with MLAG to Distribution
- Existing cloud managed access
- Macro (VRF) and Micro (SGT) segmentation
- L2 mobility within the distribution block. Can extend campus wide with scale consideration



Cloud Campus Fabric with BGP EVPN VXLAN CVD

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/Cloud_Campus_Fabric_with_BGP_EVPN_VXLAN_CVD_v0_9.html

Customer #2 - Tails

Requirements



Automated Campus fabric



Macro and Micro Segmentation



Reduce Campus complexity
Configuration and troubleshooting



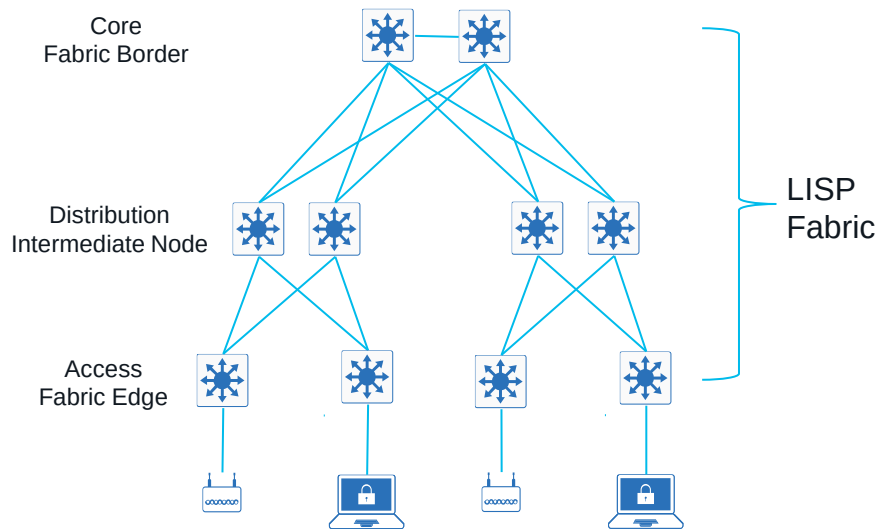
Campus wide L2 mobility



Customer #2 - Tails

Solution

- LISP control plane
- Routed access underlay – no L2 protocols
- Macro (VRF) and Micro (SGT) segmentation
- Campus wide L2 mobility



Cisco SD-Access Solution Design Guide CVD

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html>

Conclusion



Flexible deployment options

Fabric with LISP or with BGP EVPN

Catalyst
Center



Do It Yourself with
CLI



DIY using
Ansible/Terraform



Catalyst Center Architecture Flexibility

SD-Access with LISP or SD-Access with BGP EVPN

Catalyst Center 2.3.7.2
IOS-XE: 17.12

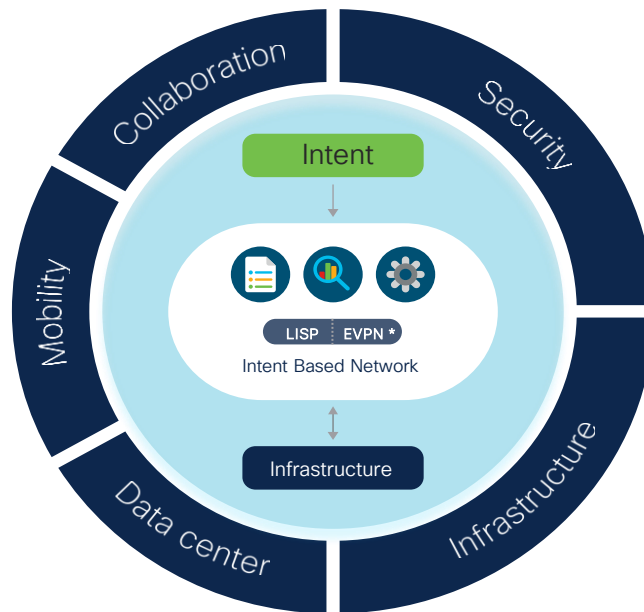
LISP VxLAN

Simple: Standards-based, Campus optimised Control Plane

Efficient: Lightweight, unparalleled scale & high performance due to rapid convergence time

Extensible: Highly extensible to drive innovation (Pub Sub, Multi-site, Extranet)

Robust: Integrated wireless w/ L2 mobility support campus wide



BGP EVPN VxLAN

Unified Fabric: Extend Fabric across Campus and Data Center

Use-case Driven: Customizable Overlay Network Types and Topologies. Use case driven topologies

Industry Standard: Multi-vendor deployment

Proven & Scalable: Leveraging BGP Control-Plane

One Infrastructure | Single Data plane | Consistent Zero-Trust Experience

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC