Let's go

The bridge to possible

Software Defined Access

Fundamentals

Brandon Johnson – Technical Solution Architect

BRKENS-2810

Cisco Webex App

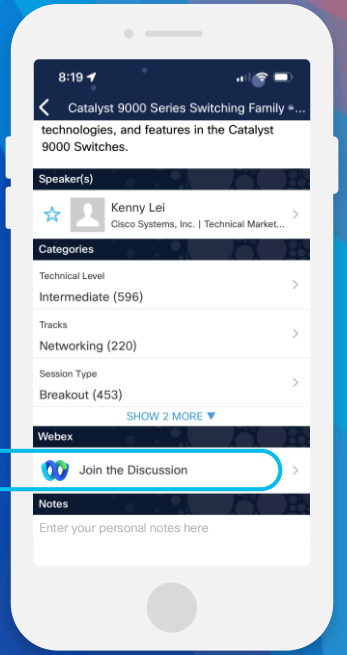
Questions?

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 December 22, 2023.

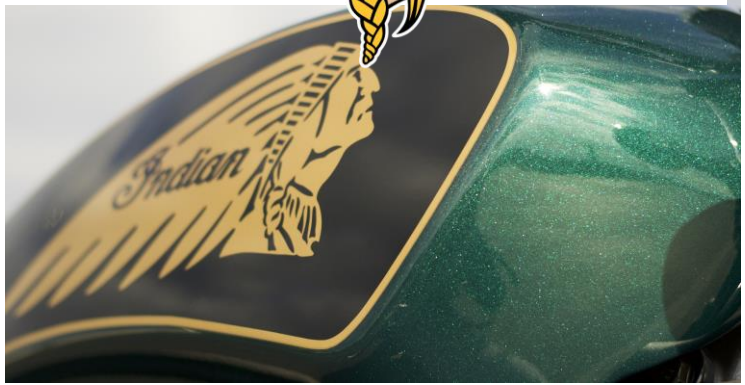


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2810

Brandon Johnson

28	Years in Networking
15	Years as a Partner
28	Years doing switching
13	Years at Cisco
37	Years in Australia

- Dad
- 4 Kids
- ❤ Guitar
- NFL
- Born U.S.
- Indian Motorcycles



Agenda

- Introduction
- Back to basics
- Underlay
- Overlay
- Operation
- Multiple Fabrics
- Conclusion

Why SD Access - Simplification

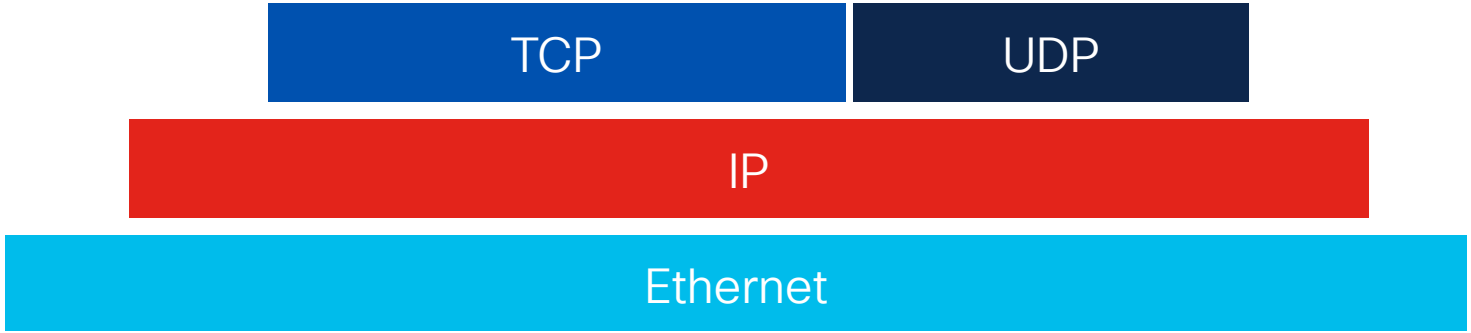
- SD-Access – simplifies wired and wireless
- IP Addressing simplification
- Improve Scaling both wired and wireless
- Policy Simplification and Improved Security
- Improved Performance
- Improved Availability
- Foundation for Zero Trust - Simplified and Continual Trust

How do networks work?

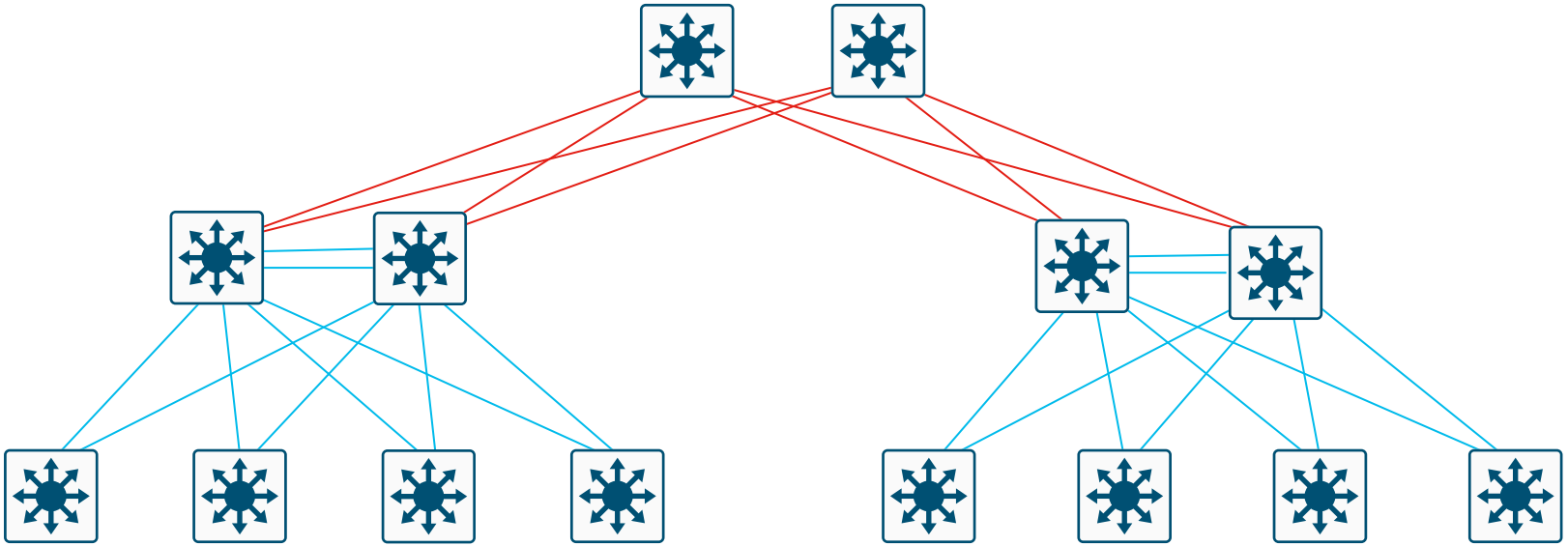
Ethernet

- Carrier Sense, Multiple Access / Collision Detection (CSMA/CD)
- Collision Avoidance (CSMA/CA) for Wireless
- Bridges, half-duplex switches propagated collision domain
- Full duplex switches eliminate collision domain by limiting it to the port
- Needs loop-free topology. (!SPANNING TREE PROTOCOL!)
- Broadcast domain
- Address Resolution Protocol to resolve IP addresses (broadcast)

Foundations – TCP/IP Stack

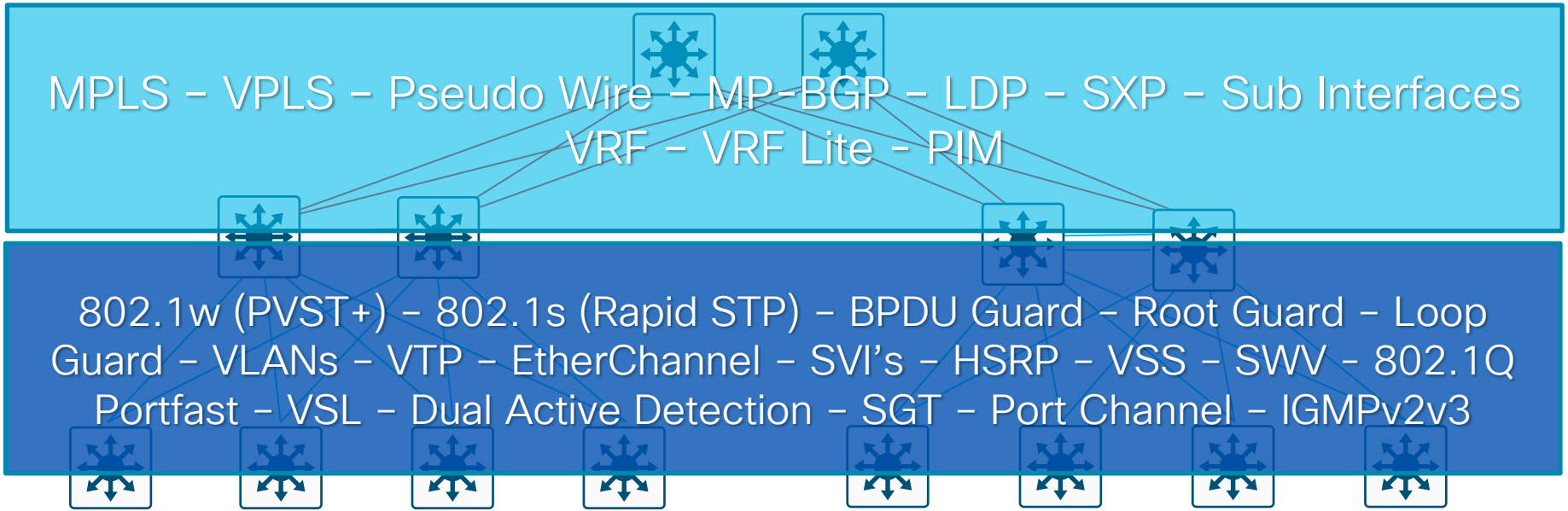


3 Tier Network Model – Mature – 30 years+



Layer 3 –
Layer 2 –

3 Tier Network Model – 30+ protocols to juggle



Layer 3 –

Layer 2 –

Time for a Fresh Start?

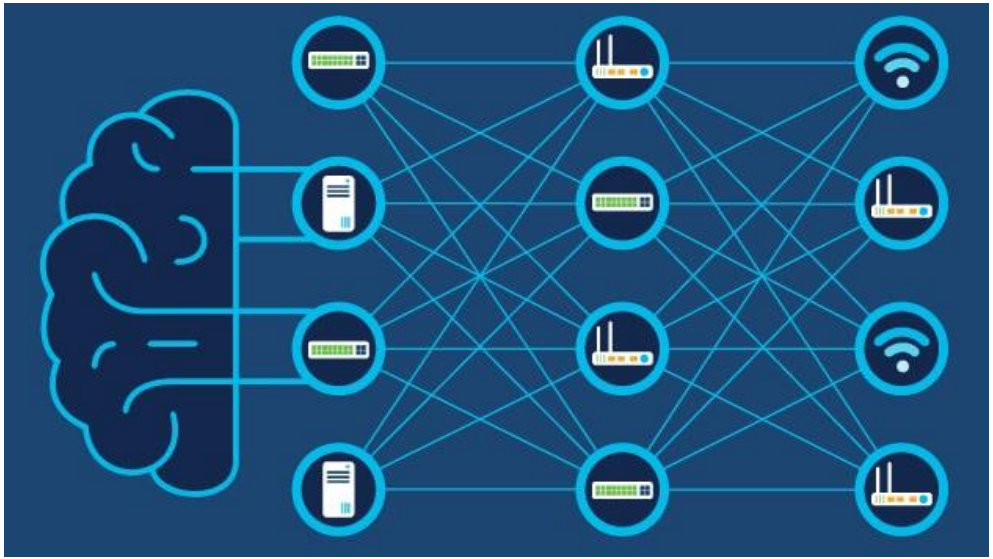
Roles and Terminology

1. Concepts
2. SD-Access Roles
3. Fabric Constructs

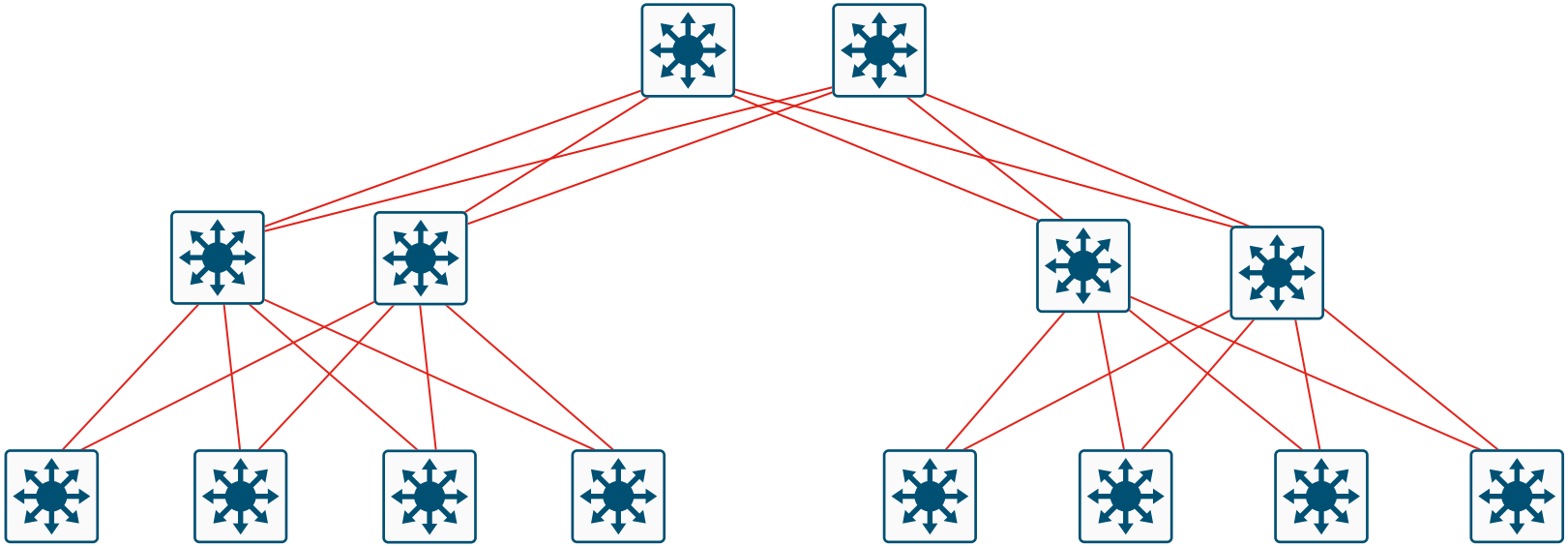
Fabric = Underlay + Overlay(s)

What is a Network Fabric?

- Mesh of connections between network devices.
- Transports data from source to destination.
- Usually refers to a virtualized, automated lattice of overlay connections.
- May (uncommonly) refer to physical wiring of a network .



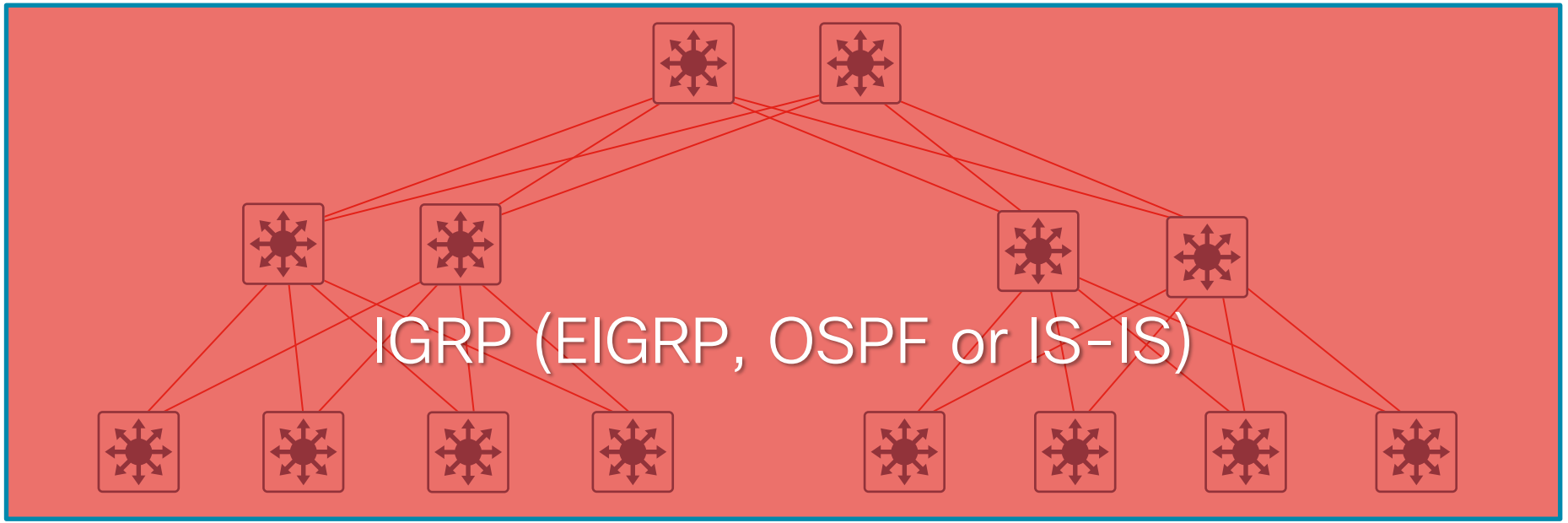
Underlay– Layer 3 only – minimal S.P.F. & no STP!



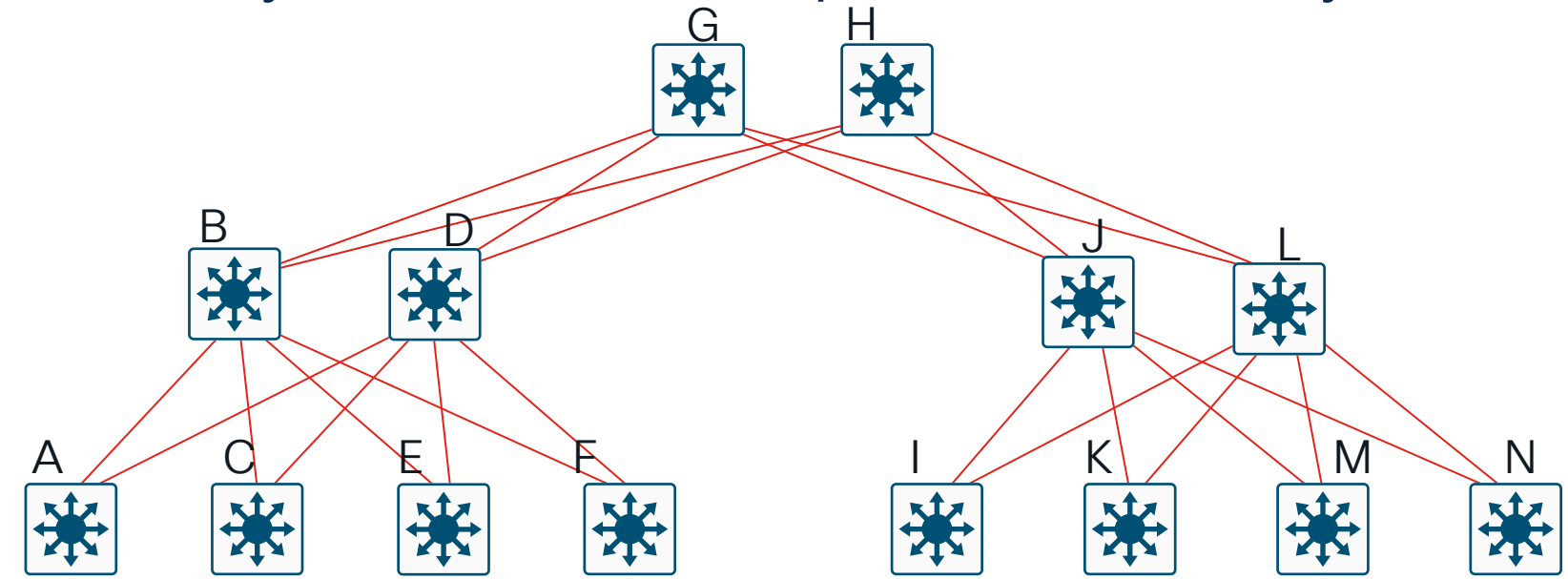
Layer 3 –

Layer 2 –

Underlay– Layer 3 only – One Protocol & E.C.M.P.

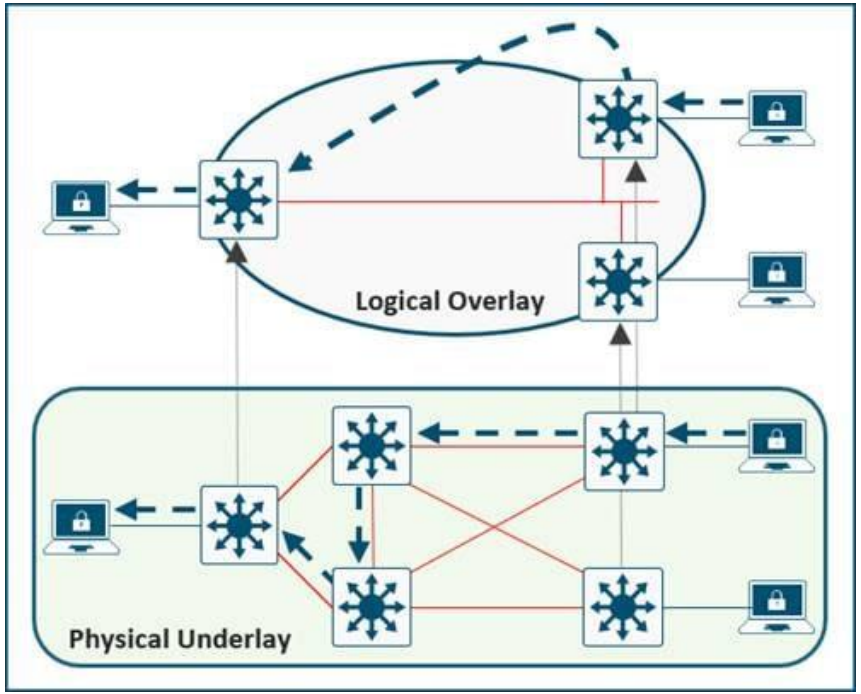


Underlay– Router ID, simple … but no Layer 2

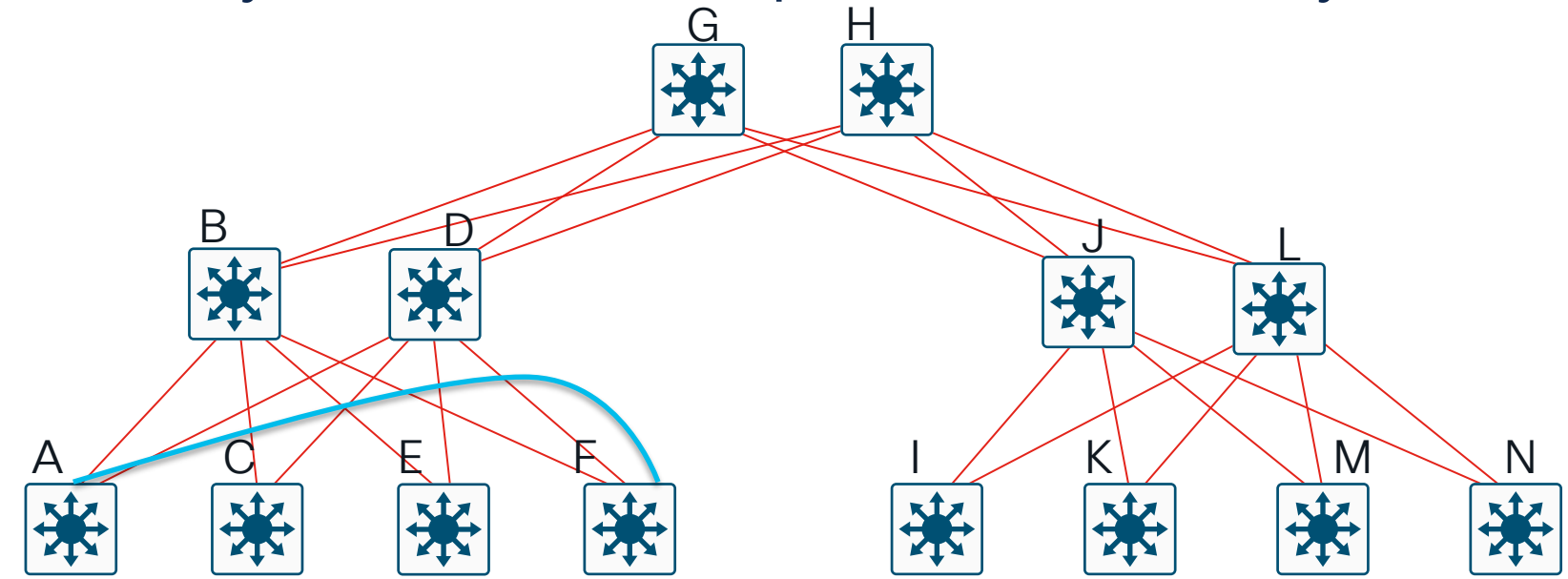


What is an Overlay?

- An Overlay network is a logical topology used to virtually connect devices, built over an arbitrary physical Underlay topology.
- Examples of overlay technologies:
  - GRE
  - MPLS
  - IPsec
  - CAPWAP
  - LISP
  - VXLAN
  - BGP EVPN
  - SD-WAN
  - ACI
  - OTV



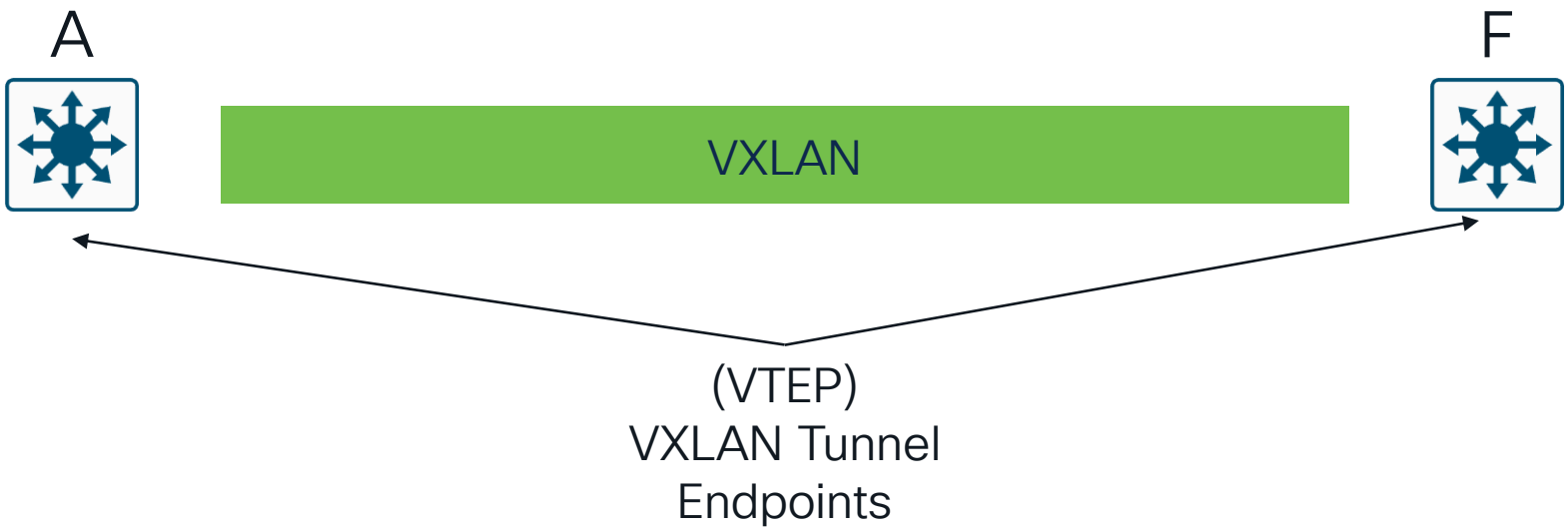
Add Layer 2 over the top. VXLAN Overlay



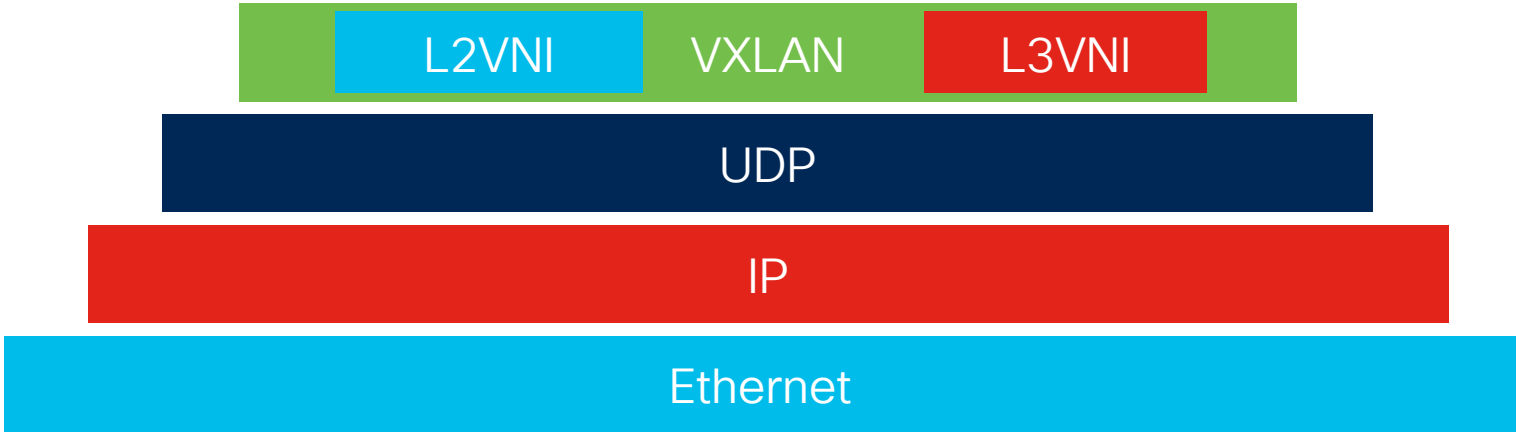
Layer 3 –

Layer 2 –

SD Access Fabric – VXLAN Tunnel



VXLAN – L2 and L3 Overlays



How do we know where everything is?

Cisco SD-Access Fabric

- Learns or keeps track of endpoints in the fabric.
- Control Plane: LISP
  - Locator/ID Separation Protocol.
  - IETF Standards Track RFC9300-RFC9305 and Informational RFC9299.

Lightweight, Efficient, Scalable and Extensible

LISP – Locator / ID Separation Protocol

- Tracks Endpoint IDs (EID) and the Location of the router hosting that Endpoint: Router Location (or RLOC)

- LISP originally for L3 uses – but can still be combined with VXLAN packets and we get L2 (RLOC == VTEP)

LISP Terms
========

ITR
ETR
PITR
PETR
} Tunnel Router Types

MS
MR
} Map DB Routers

ALT
LISP DDT

DB Attributes {
EID
RLOC

LISP

- LISP tracks the locator and identity of a device through the RLOC and EID
- Endpoint ID is address of the host , Route locator (RLOC) is router where that EID is connected. Eg. EID – Brandon , Locator – MEC Room 211
- “Works like DNS”

23.198.40.79 ???

www.ciscolive.com!!!

LISP0

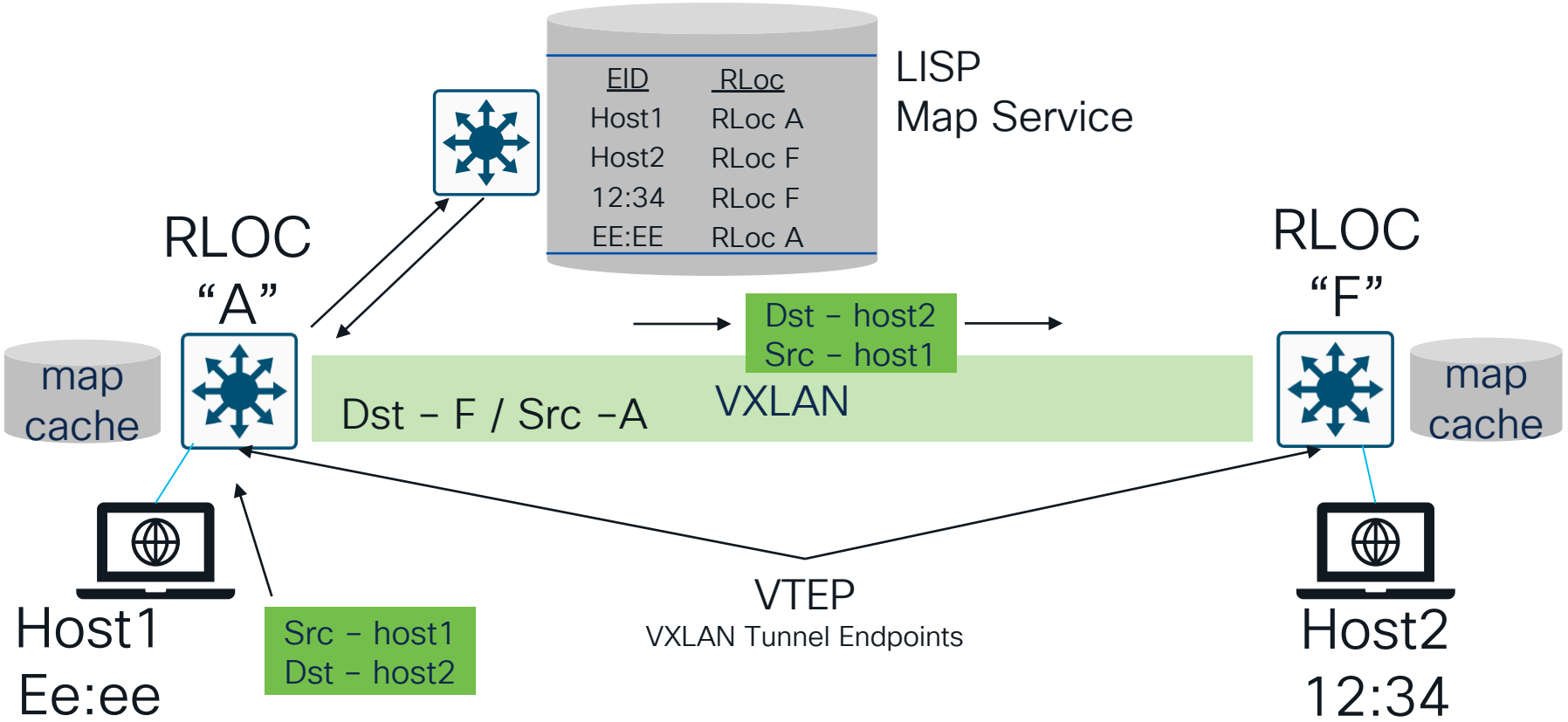
LISP IID 4000

Endpoint ID	Locator
192.168.10.9	10.10.10.1
192.168.10.10	10.10.10.2
192.168.10.11	10.10.10.1
192.168.10.12	10.10.10.1

LISP IID 8000

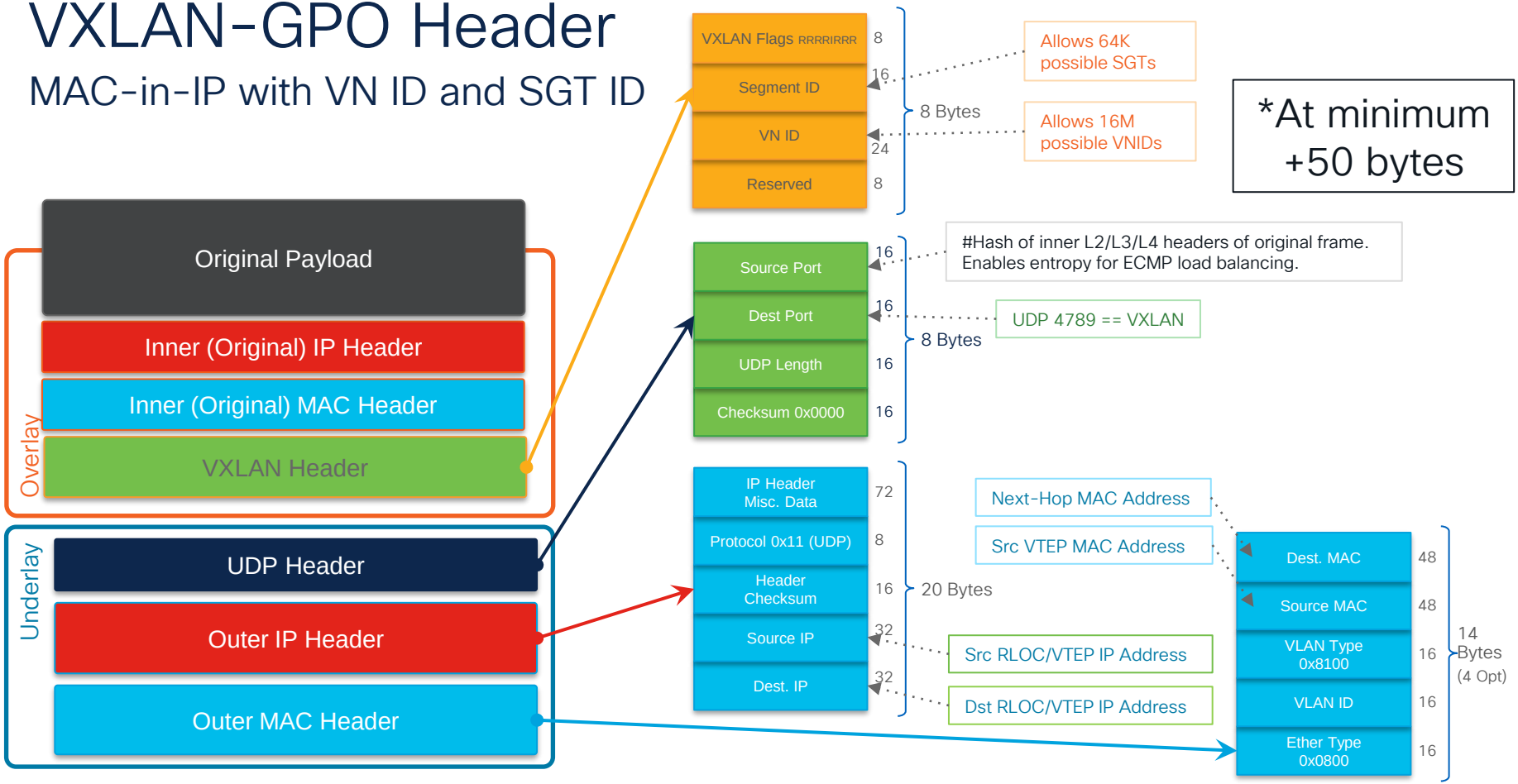
Endpoint ID	Locator
00:50:56:03:EF:EC	10.10.10.7
00:50:56:9C:F8:46	10.10.10.7
00:0C:2D:00:45:67	10.10.10.2
00:50:56:23:E7:17	10.10.10.8

SD Access Fabric – Learns via LISP, transmits VXLAN



VXLAN-GPO Header

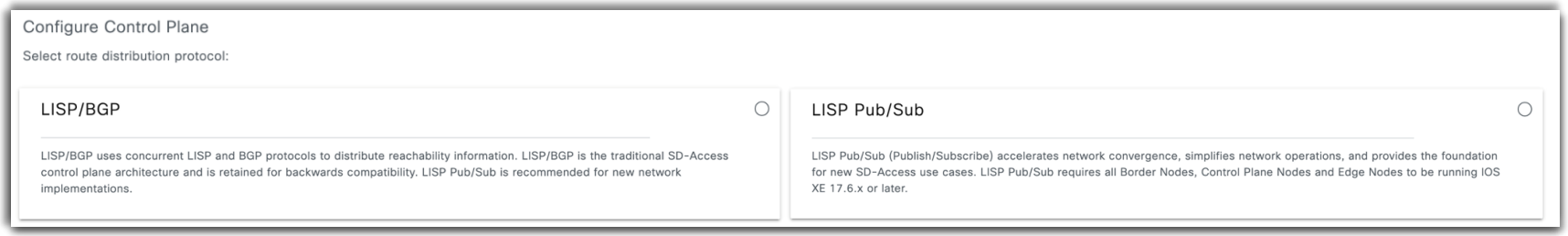
MAC-in-IP with VN ID and SGT ID



Roles and Terminology

1. Concepts
2. SD-Access Roles
3. Fabric Constructs

LISP in Cisco SD-Access



LISP/BGP

- Released circa 2017.
- Reliable and stable.
- BGP for route distribution.

LISP Pub/Sub

- Released in 2022 with DNA Center 2.2.3.x.
- Reliable and stable.
- Native LISP route distribution.
- Less Control Plane load.
- Faster convergence.
- Highly extensible.

LISP Pub/Sub

??? What is pub sub ???...

- LISP Pub/Sub is recommended for new deployments.
- In software architecture, publish–subscribe is a messaging pattern where publishers categorize messages into classes that are received by subscribers. This is contrasted to the typical messaging pattern model where publishers sends messages directly to subscribers.

- Similarly, subscribers express interest in one or more classes and only receive messages that are of interest, without knowledge of which publishers, if any, there are.

LISP Pub/Sub

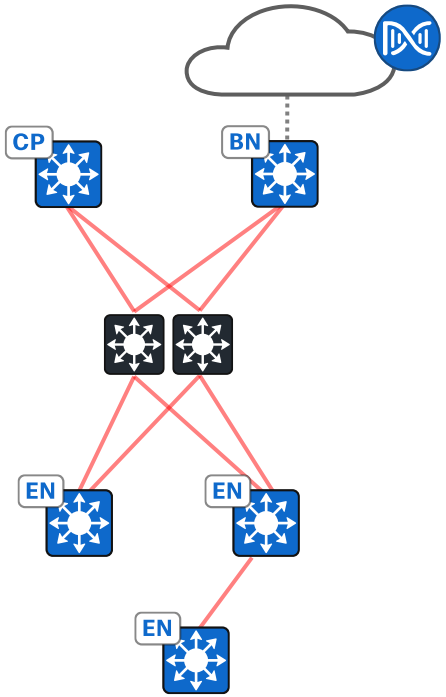
A Brief Digression, before you ask...

- No plans to end support for LISP/BGP.
- LISP Pub/Sub is recommended for new deployments.
- In Catalyst Center (fka DNA Center) 2.2.3.x new Fabric Sites can be configured as LISP/BGP or LISP Pub/Sub. Note minimum IOS XE versions.

Cisco SD-Access Roles

Mandatory Components

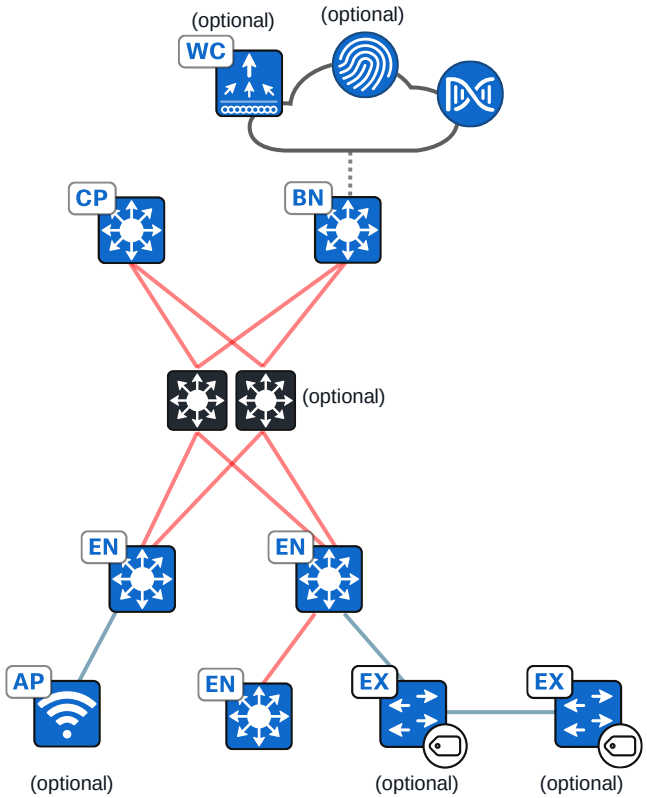
- **Cisco Catalyst Center** – GUI and APIs for intent-based automation of wired and wireless fabric devices.
- **Border** – A fabric device that connects external L3 and L2 networks to the Cisco SD-Access fabric.
- **Edges**– A fabric device that connects wired endpoints to the Cisco SD-Access fabric and optionally enforces micro-segmentation policy.
- **Control Plane**– Map System that tracks endpoints & routes.



Cisco SD-Access Roles

Optional Components

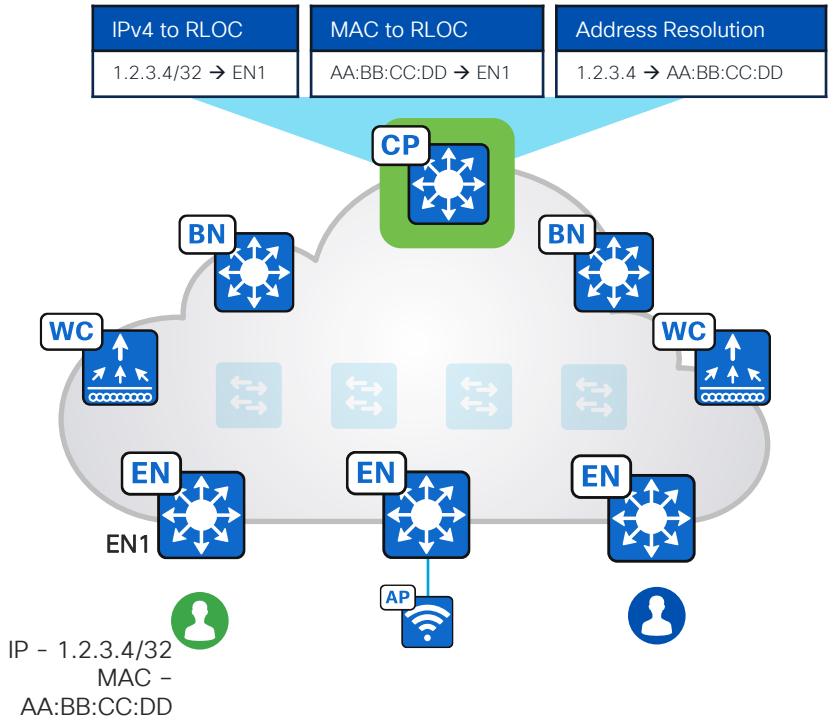
- **Identity Services Engine** – Highly recommended. NAC and Identity services for dynamic endpoint to Security Group Tag mapping and policy distribution.
- **Fabric Wireless Controller** and **Fabric APs** – Highly recommended. Connects wireless endpoints to the SD-Access fabric.
- **Extended Node** – A switch operating at Layer 2 that extends fabric connectivity and optionally enforces micro-segmentation policy.
- **Intermediate Nodes** – Moves data between fabric nodes. Can be one or many hops.



Cisco SD-Access Fabric

Control Plane Node Maintains a Host Tracking Database to Map Location Information

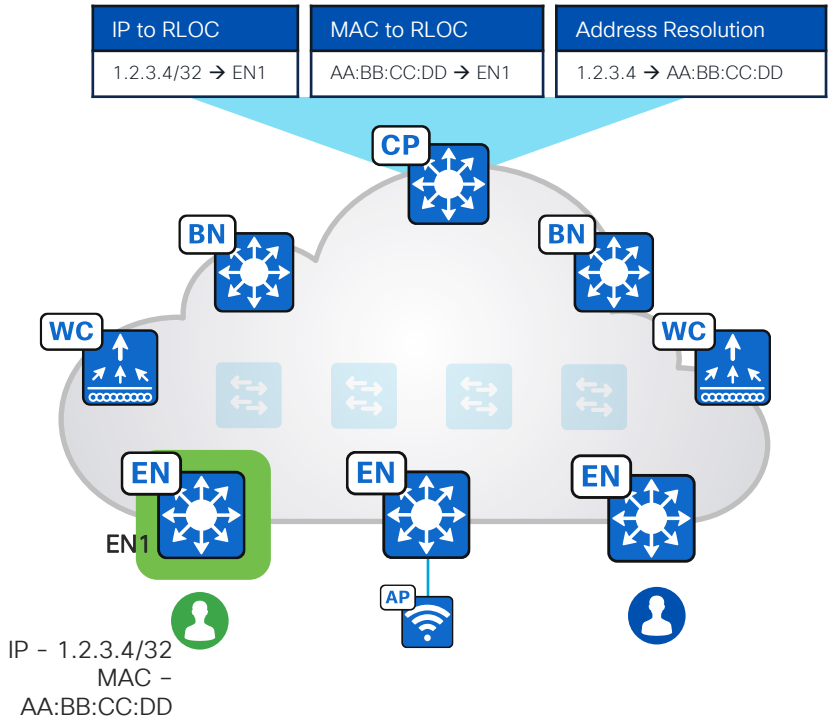
- A simple Database that maps Endpoint IDs to Locations, along with other attributes.
- Host Database supports multiple types of Endpoint ID lookup types (IPv4, IPv6 or MAC).
- Receives Endpoint ID map registrations from Edges, Border Nodes and Fabric WLC's.
- Resolves lookup requests from Edge Nodes and Border Nodes, to locate destination Endpoint IDs.
- Publishes registrations to Subscribers.



Cisco SD-Access Fabric

Edge Node Provides First Hop Services for Endpoints

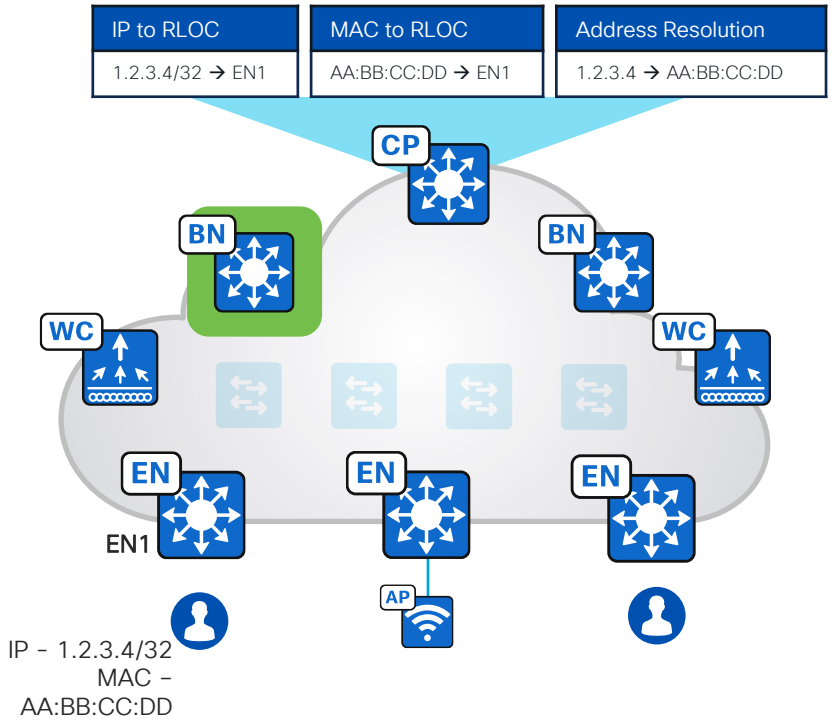
- Responsible for Authenticating and Authorizing endpoints (e.g. 802.1X, MAB, static) in concert with ISE.
- Register Endpoint IDs (IPv4, IPv6, MAC) with the Control Plane Nodes.
- Provide an Anycast Gateway for the connected wired and wireless endpoints.
- Performs VXLAN encapsulation and decapsulation of traffic to and from all connected wired endpoints.



Cisco SD-Access Fabric

Border Node is the Fabric Site Entry and Exit for Network Traffic

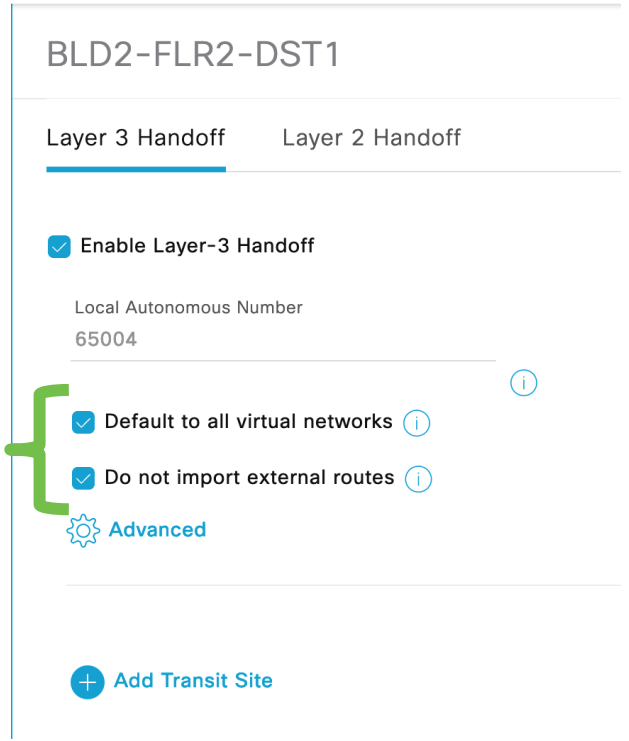
- Subscribes to LISP Control Plane Node IPv4 and IPv6 Tables.
- There are 4 types of Border Node:
  - External Border Node.
  - Internal Border Node.
  - Internal + External Border Node.
  - Layer 2 Border Node.



Cisco SD-Access Fabric

Border Node is the Fabric Site Entry and Exit for Network Traffic

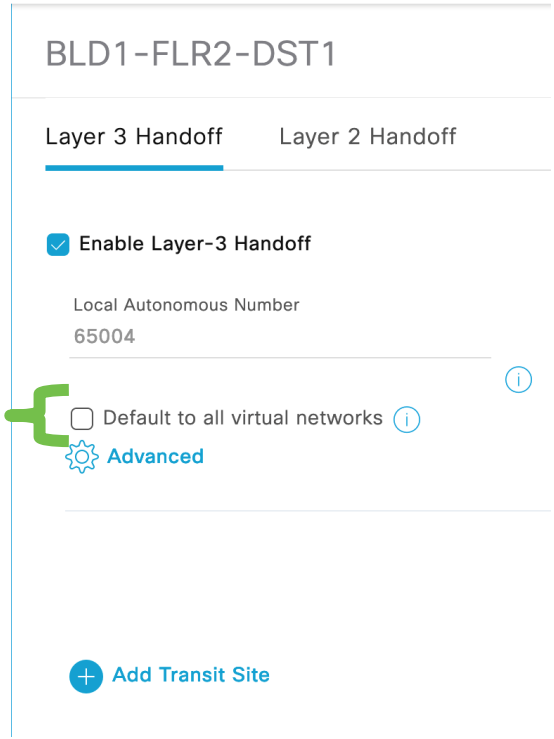
- External Border Node:
  - The most common configuration.
  - Exports all fabric subnets to outside the Fabric Site as eBGP summary routes.
  - Does not register IP prefixes from outside the Fabric Site into the fabric Control Plane.
  - Acts as a gateway of last resort for the Fabric Site.



Cisco SD-Access Fabric

Border Node is the Fabric Site Entry and Exit for Network Traffic

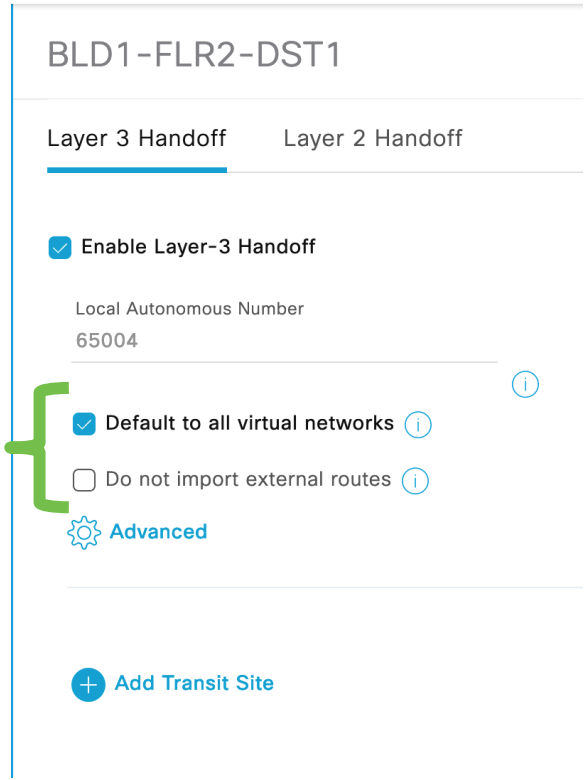
- Internal Border Node:
  - Exports all fabric subnets to outside the Fabric Site as eBGP summary routes.
  - Imports and registers eBGP-learned IPv4/IPv6 prefixes from outside the Fabric Site, into the fabric Control Plane.
  - Does not act as a gateway of last resort for the Fabric Site.



Cisco SD-Access Fabric

Border Node is the Fabric Site Entry and Exit for Network Traffic

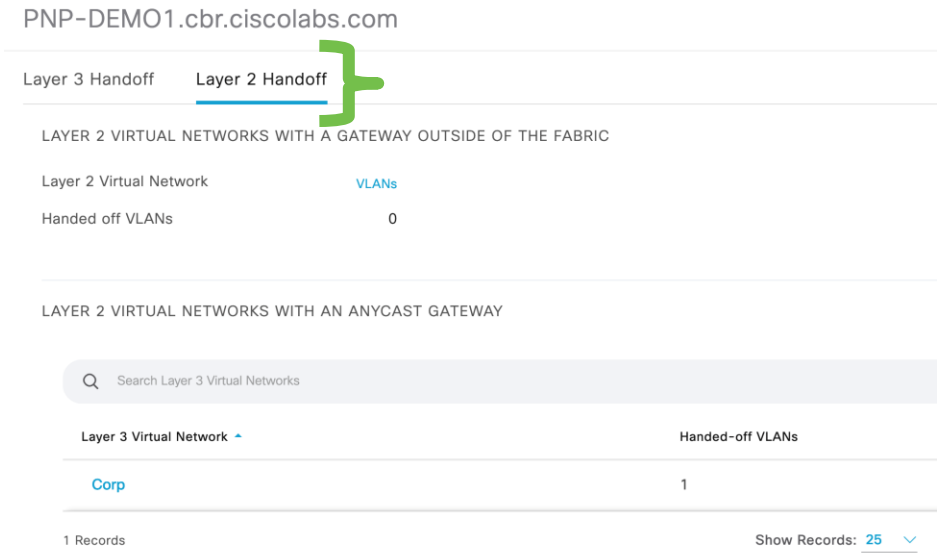
- Internal + External Border Node:
  - Exports all fabric subnets to outside the Fabric Site as eBGP summary routes.
  - Imports and registers eBGP-learned IPv4/IPv6 prefixes from outside the Fabric Site, into the fabric Control Plane.
  - Acts as a gateway of last resort for the Fabric Site.



Cisco SD-Access Fabric

Border Node is the Fabric Site Entry and Exit for Network Traffic

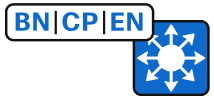
- Layer 2 Border Node:
  - Acts as Layer 2 handoff for pure Layer 2 Overlays or Layer 2 + Layer 3 Overlays.
  - Allows VLAN translation between SD-Access network segments and non-fabric VLAN IDs.
  - Dual homing requires link aggregation; STP it not tunneled within the SD-Access Fabric.
  - Ideally should be separate device from the Layer 3 Border Node.



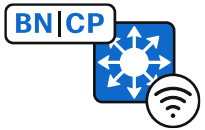
Cisco SD-Access Roles

Some of the Supported Colocations

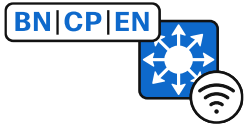
Border Node and Control Plane Node.



Border Node, Control Plane Node, and Fabric Edge Node.



Border Node, Control Plane Node, and Embedded Wireless Controller.

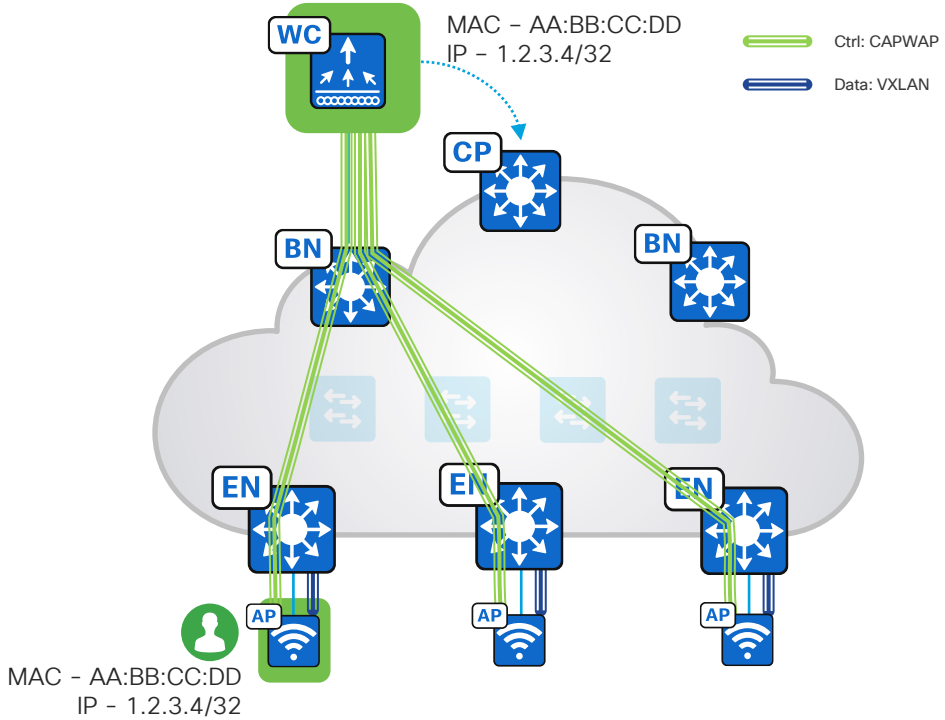


Border Node, Control Plane Node, Fabric Edge Node, and Embedded Wireless Controller.

Cisco SD-Access Fabric

Fabric Enabled Wireless Unifies Wired and Wireless Management, Policy and Data Planes

- Fabric WLC accessible though a Fabric Border Node (Underlay). Can be several hops away.
- Fabric Enabled APs reside in a dedicated IP range and communicate with the WLC (CAPWAP Control).
- Fabric WLC registers endpoints with the Control Plane Node.
- Fabric APs switch endpoint traffic to the adjacent Edge Node.
- Wireless endpoints use same data plane and policy plane as wired endpoints.



Roles and Terminology

1. Concepts
2. SD-Access Roles
3. Fabric Constructs

Virtual Networks (VN)

Commonly referred to as ”Macro Segmentation”

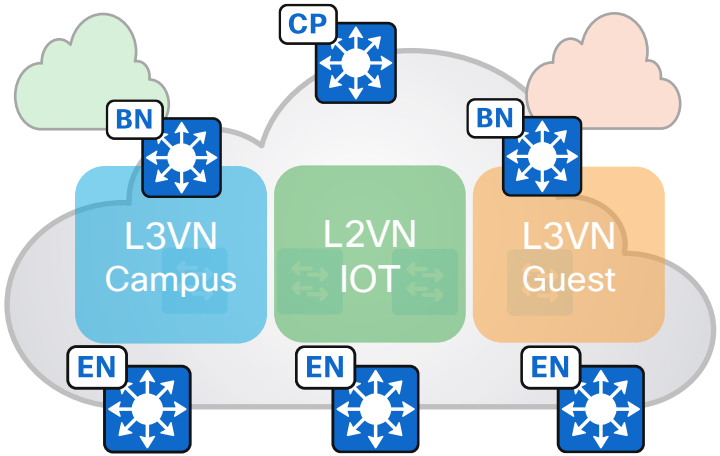
Switch / Routers	VRF
LISP Packet	LISP IID (Instance ID)
VXLAN Frame	VNID

VRF ⇔ IID ⇔ VNID

Cisco SD-Access Fabric

Virtual Networks (a.k.a. IIDs, VRFs, VNIDs ..etc)

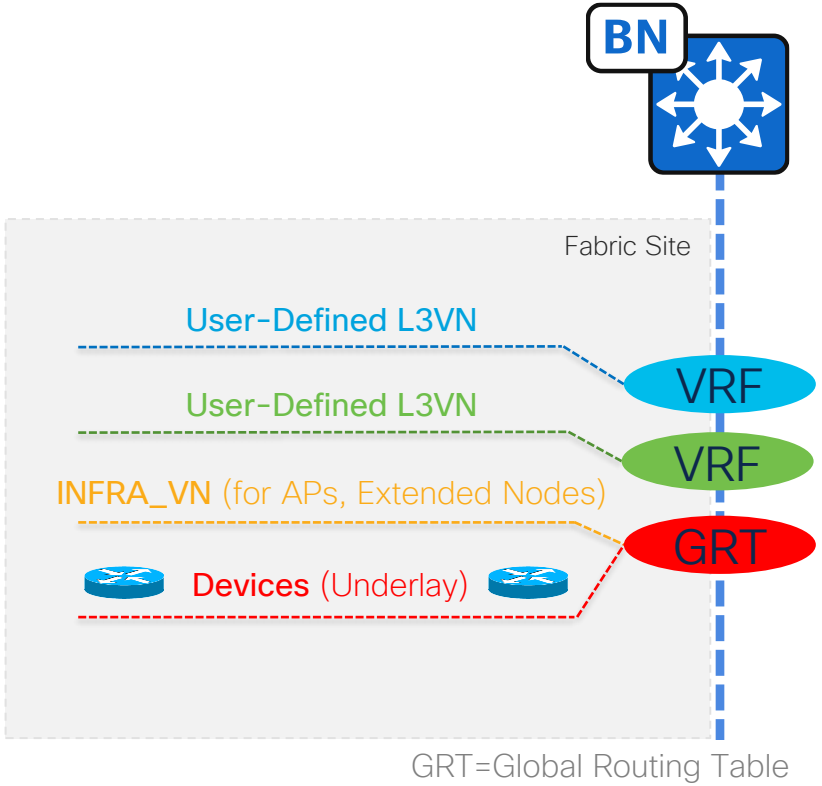
- Layer 3 Virtual Networks use VRFs and LISP Instance IDs to maintain separate routing topologies.
  - Endpoint IDs (IPv4/IPv6 addresses) are routed within an L3VN.
- Layer 2 Virtual Networks use LISP Instance IDs and VLANs to maintain separate switching topologies.
  - Endpoint IDs (MAC addresses) are switched within an L2VN.
- Edge Nodes, Border Nodes and Fabric APs add a VNID (the LISP IID) to the fabric encapsulation.

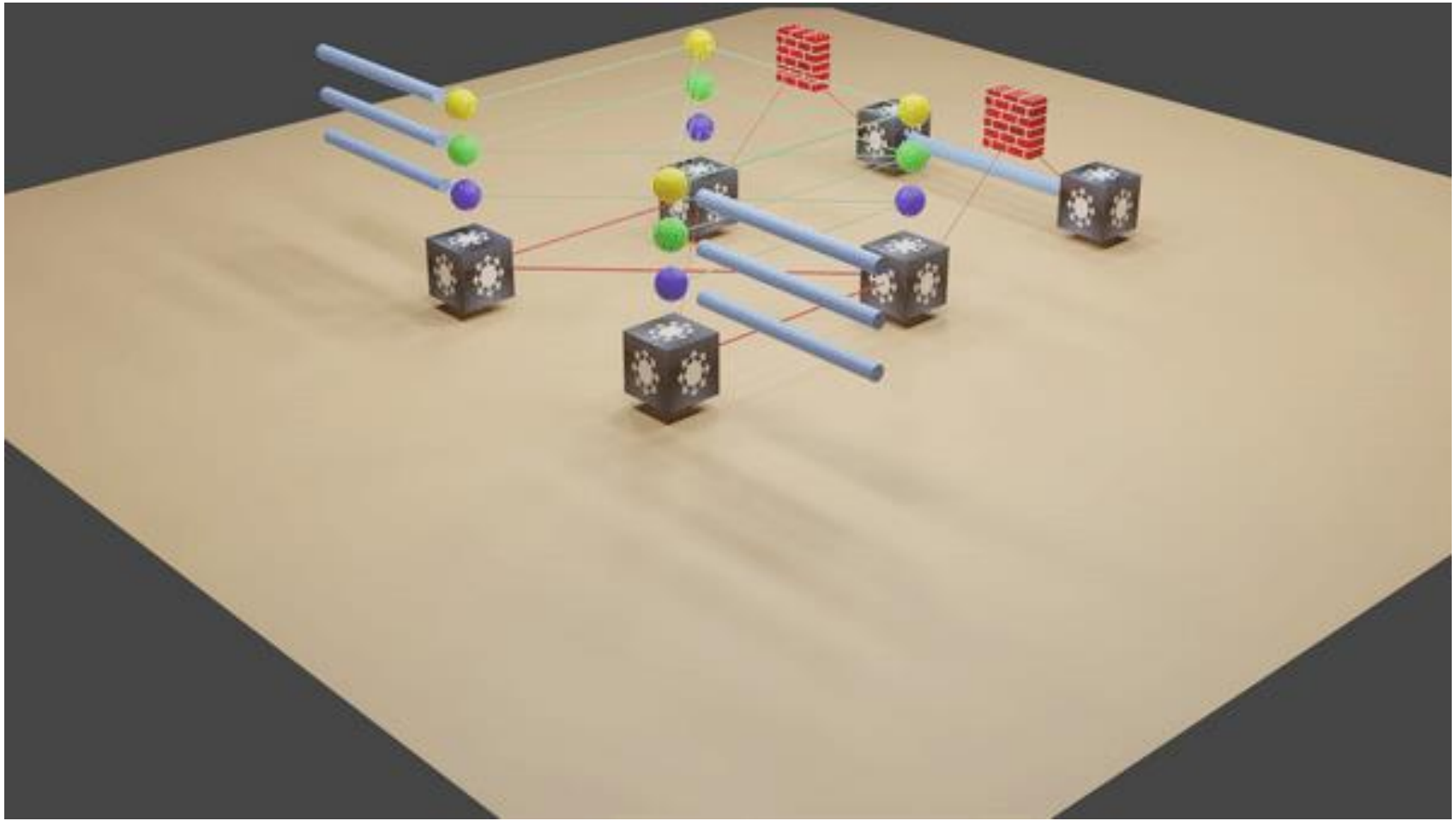


Cisco SD-Access Fabric

Layer 3 Virtual Networks

- Fabric Devices (Underlay) connectivity is in the Global Routing Table.
- INFRA_VN is only for Fabric Access Points and Extended Nodes in the Global Routing Table.
- User-Defined VNs can be added or removed on demand.
- DEFAULT_VN is the same as a user-defined VN. Present in the SD-Access UI by default. Not deployed to the Fabric Site by default.

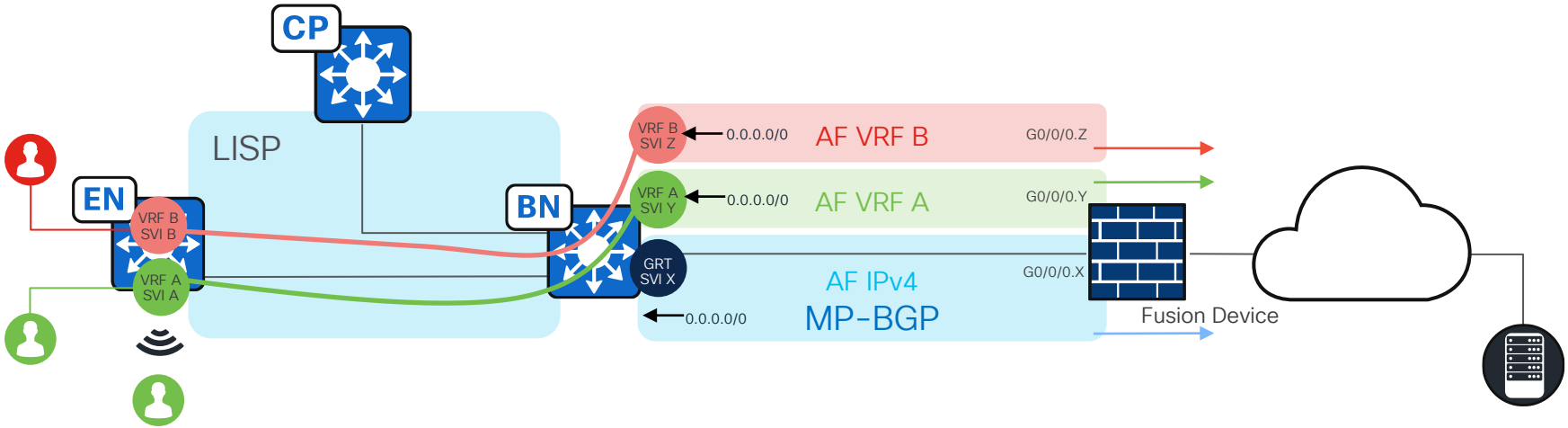




Cisco SD-Access Fabric

Per-Layer-3-Virtual-Network Layer 3 Handoff

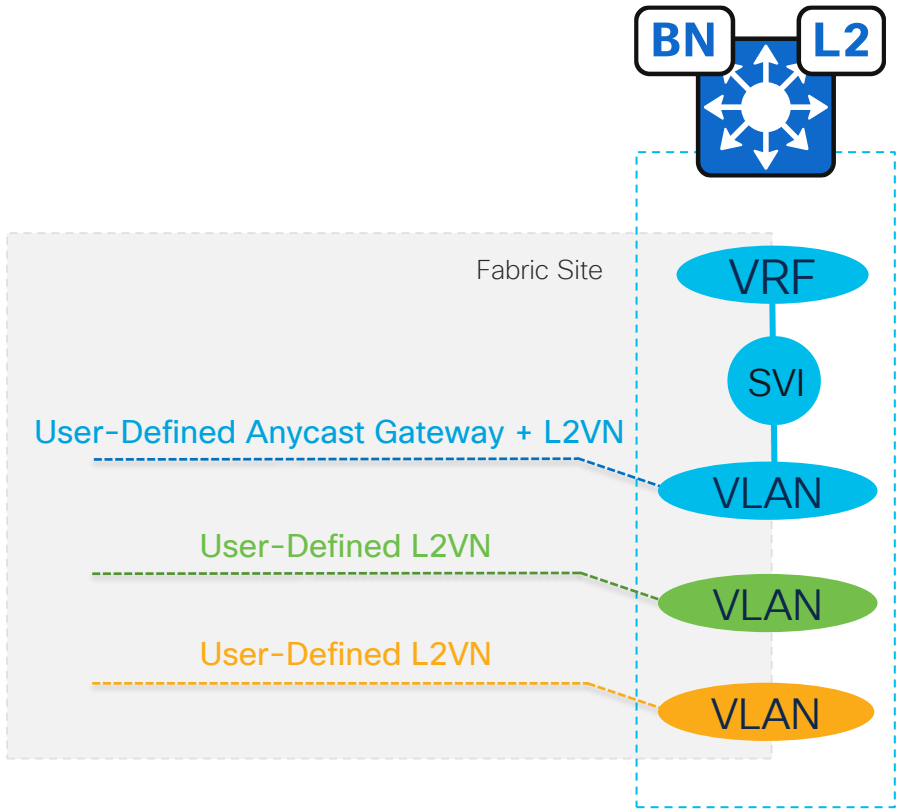
- Use a ”Fusion Device” to leak external routes into SD-Access Layer 3 Virtual Networks.
- Alternatively, maintain VRF segmentation outside of the SD-Access Fabric with a VRF-aware external routing domain.
- Fusion Device is outside the fabric. Can be any platform (router, Layer 3 switch, firewall, etc.) with appropriate capabilities.



Cisco SD-Access Fabric

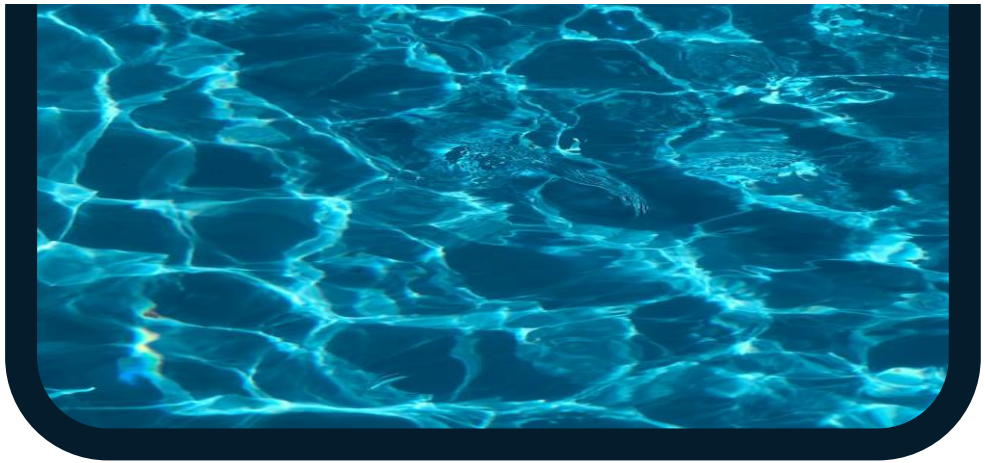
Layer 2 Handoff

- Ancient wisdom: Route whenever you can, switch when you must.
- Layer 2 Virtual Networks handoff through a user-defined VLAN.
- Layer 2 Virtual Networks may implement BUM flooding. Important to be mindful of loop prevention.

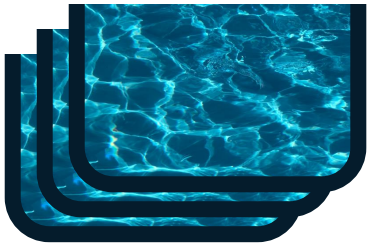


IP Pools – Address Management

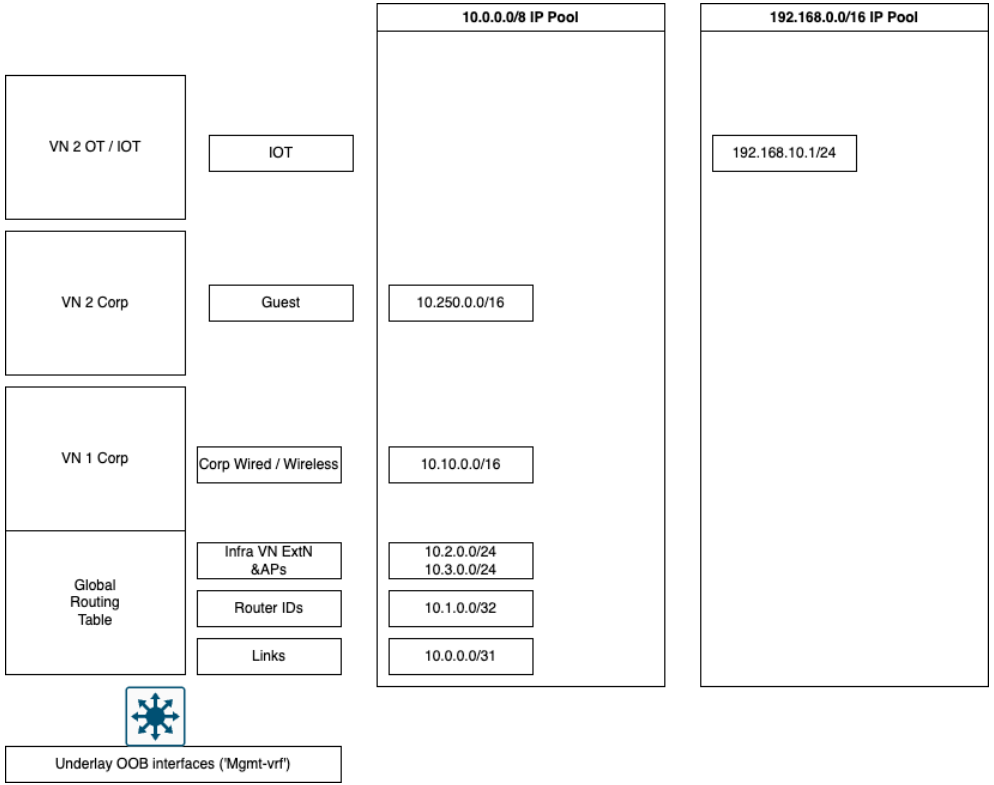
IP Pools are range of useable addresses



Host pools



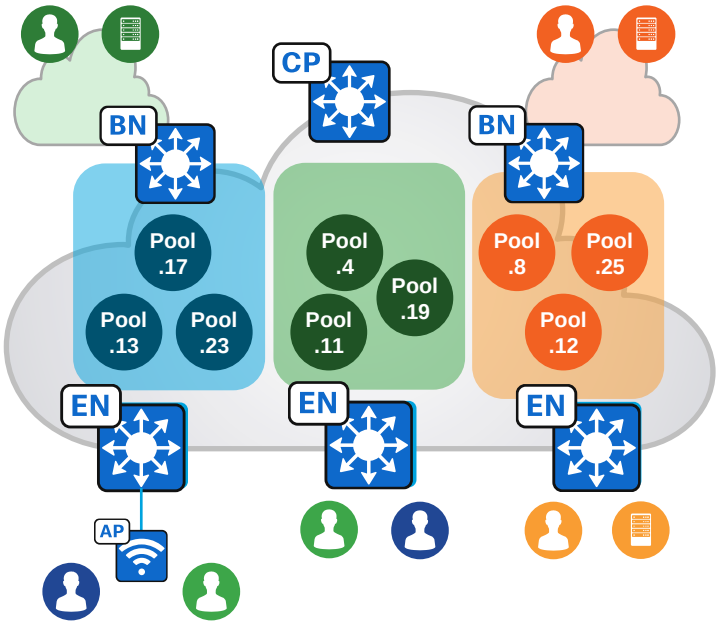
IP Pools – Address Management – Have a plan



Cisco SD-Access Fabric

Host Pools Provide a Default Gateway and Basic IP Services for Endpoints

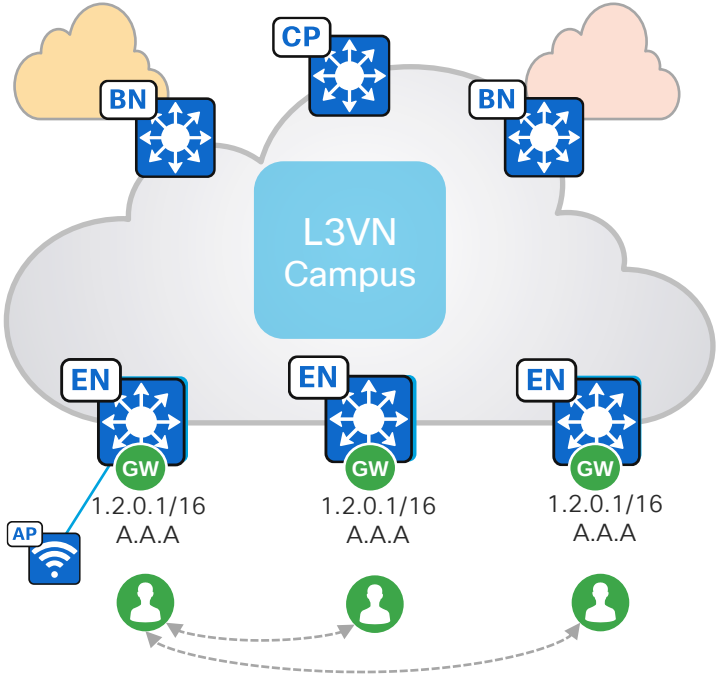
- Edge Nodes instantiate an access VLAN and a Switched Virtual Interface (SVI) with user-defined IPv4/IPv6 addresses per Host Pool.
- Host Pools assigned to endpoints dynamically by AAA or statically per port.
- Edge Nodes and Fabric WLCs register endpoint IDs (/32, /128 or MAC) with the Control Plane, enabling IP mobility; any IP address anywhere.



Cisco SD-Access Fabric

Anycast Gateway Provides a Default Gateway for IP-Capable Endpoints

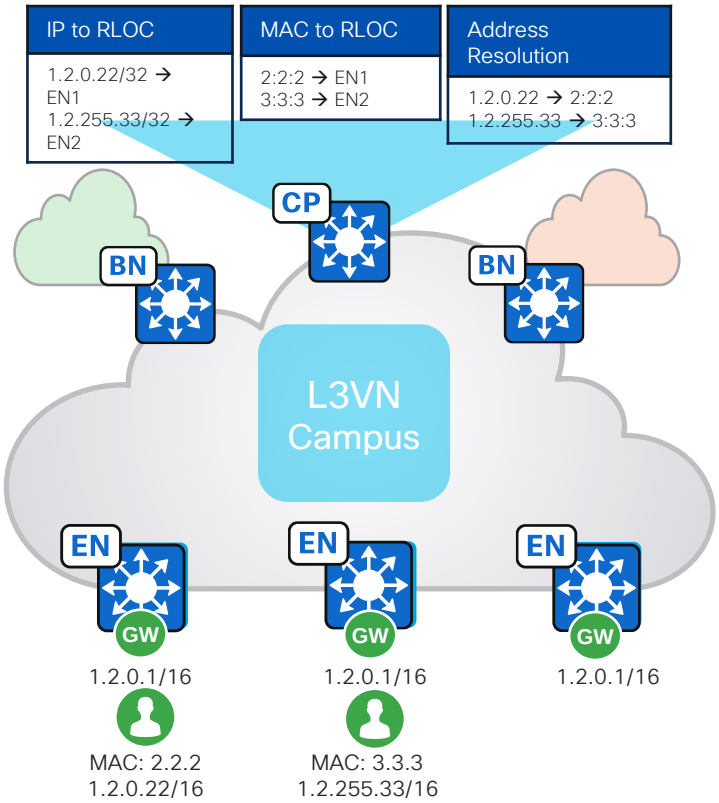
- Similar principle and behavior to FHRP with a shared virtual IPv4/IPv6 addresses and MAC address.
- The same Switch Virtual Interface (SVI) is present on all Edge Nodes with the same virtual IP and MAC.
- The wired or wireless endpoint can connect to any switch or AP in the fabric and communicate with the same Anycast Gateway.



Cisco SD-Access Fabric

Host Pools are “stretched” via the Overlay

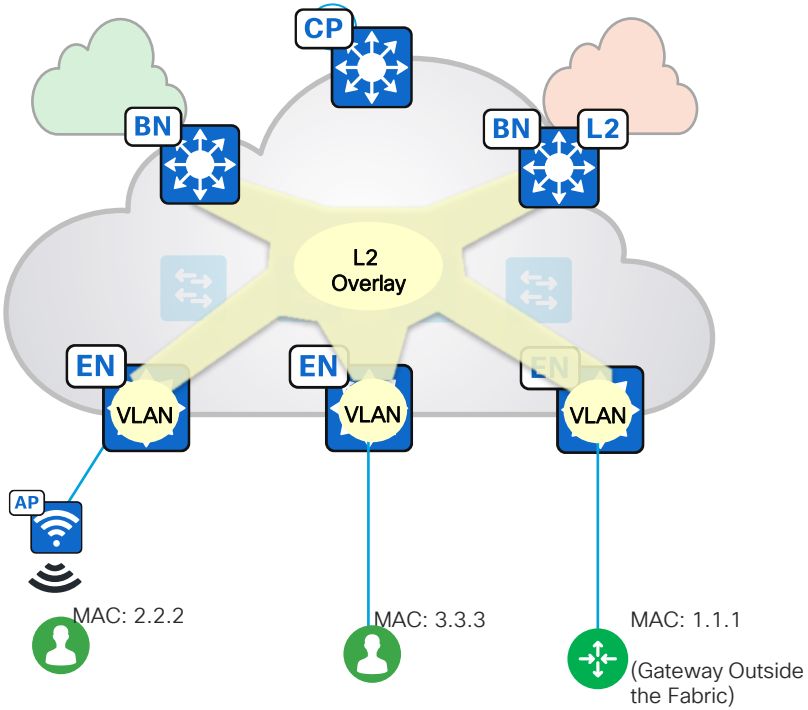
- Endpoint IPv4/IPv6 traffic arrives on an Edge Node and is then routed or switched by the Edge Node.
- Fabric Dynamic EID mapping allows endpoint-specific (/32, /128, MAC) advertisement and mobility.
- No longer need VLANs to interconnect endpoints across Edge Nodes, this happens in the Overlay without broadcast flooding.



Cisco SD-Access Fabric

Layer 2 Virtual Networks

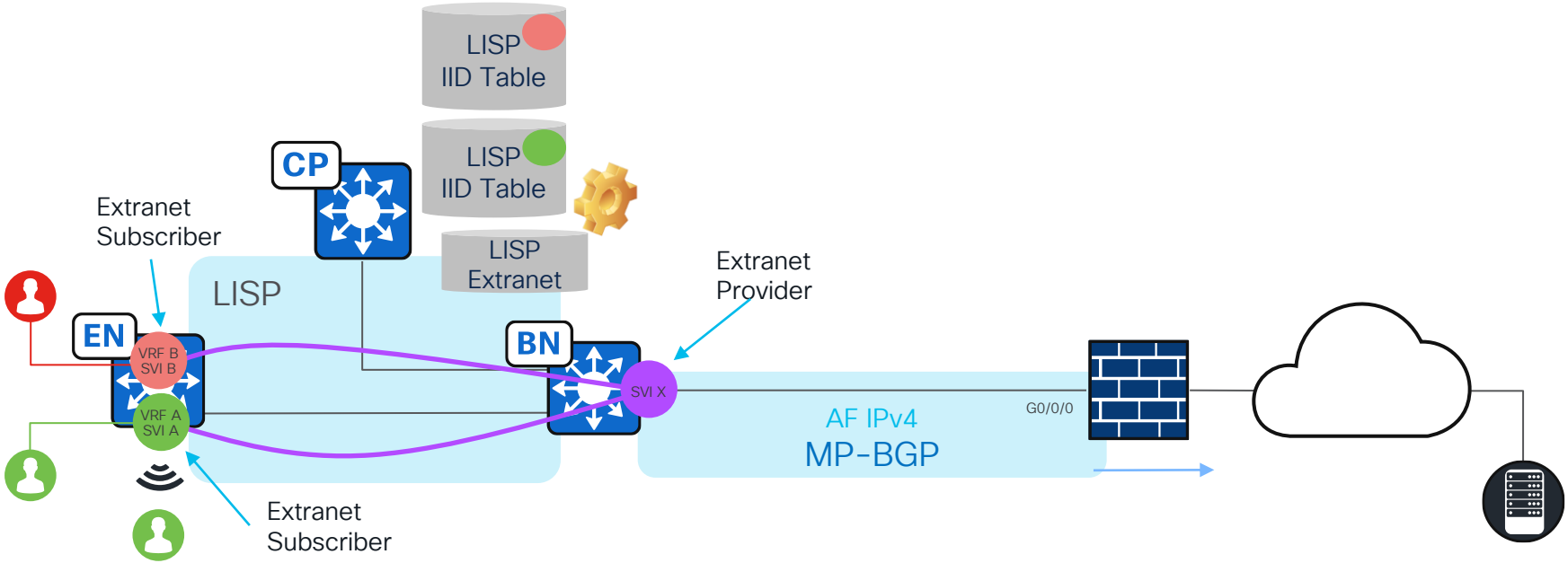
- By default, an L2VN is deployed with each Anycast Gateway and Layer 2 Flooding is disabled. Layer 2 Flooding can be enabled, if necessary, to service niche applications.
- L2VN can be deployed without an Anycast Gateway, and Layer 2 Flooding cannot be disabled.
  - Sometimes referred to as “Gateway Outside the Fabric”.
- If Layer 2 Flooding is enabled, a Multicast Underlay P2MP tunnel is established between all Fabric Nodes.



Cisco SD-Access Fabric

Extranet Provider Virtual Network Layer 3 Handoff

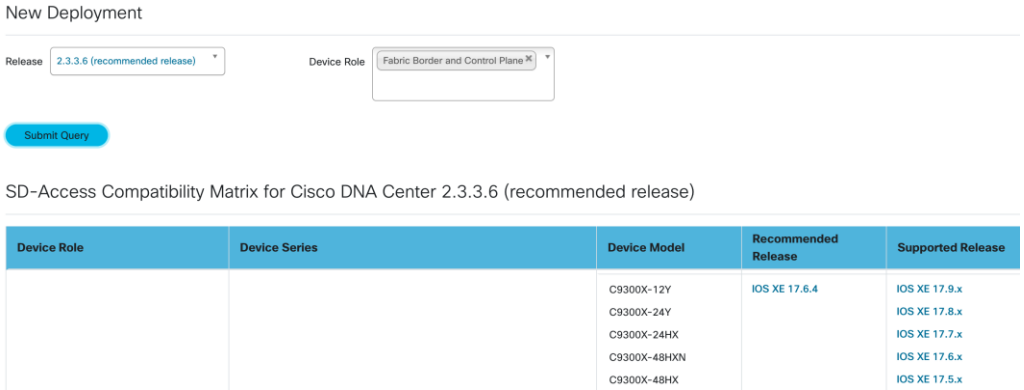
- Use an Extranet Policy to allow communication between one Provider Virtual Network and one or more Subscriber Virtual Networks.



SD-Access Design Aides

- Cisco Validated Design: https://cs.co/sda-cvd
- Design Tool: http://cs.co/sda-design-tool

- Compatibility Matrix: http://cs.co/sda-compatibility-matrix

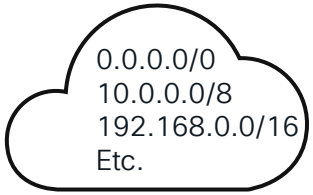


Fabric Fundamentals

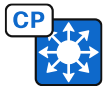
1. Control Plane
2. Data Plane
3. Policy Plane

Fabric Operation

Default ETR Registration

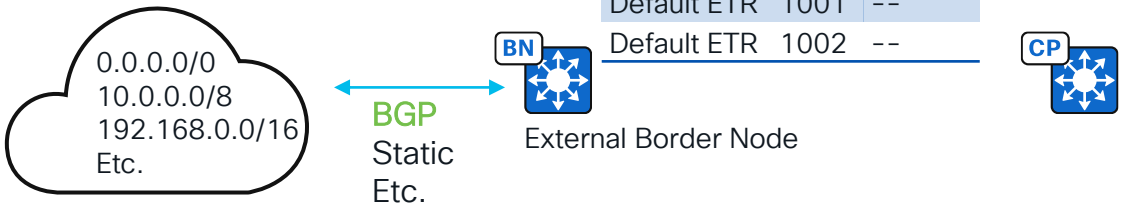


External Border Node



Fabric Operation

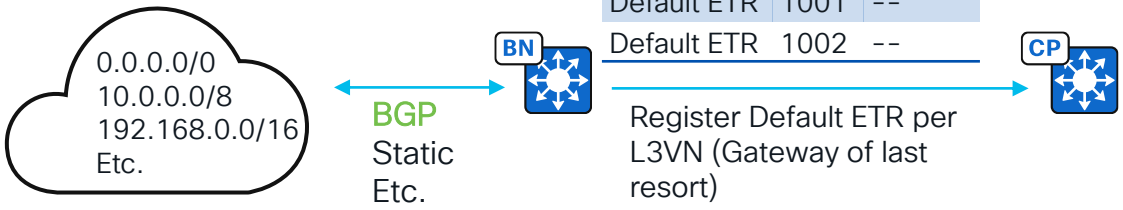
Default ETR Registration



Destination	IID	Next Hop
Default ETR	1001	--
Default ETR	1002	--

Fabric Operation

Default ETR Registration



Destination	IID	Next Hop
Default ETR	1001	--
Default ETR	1002	--

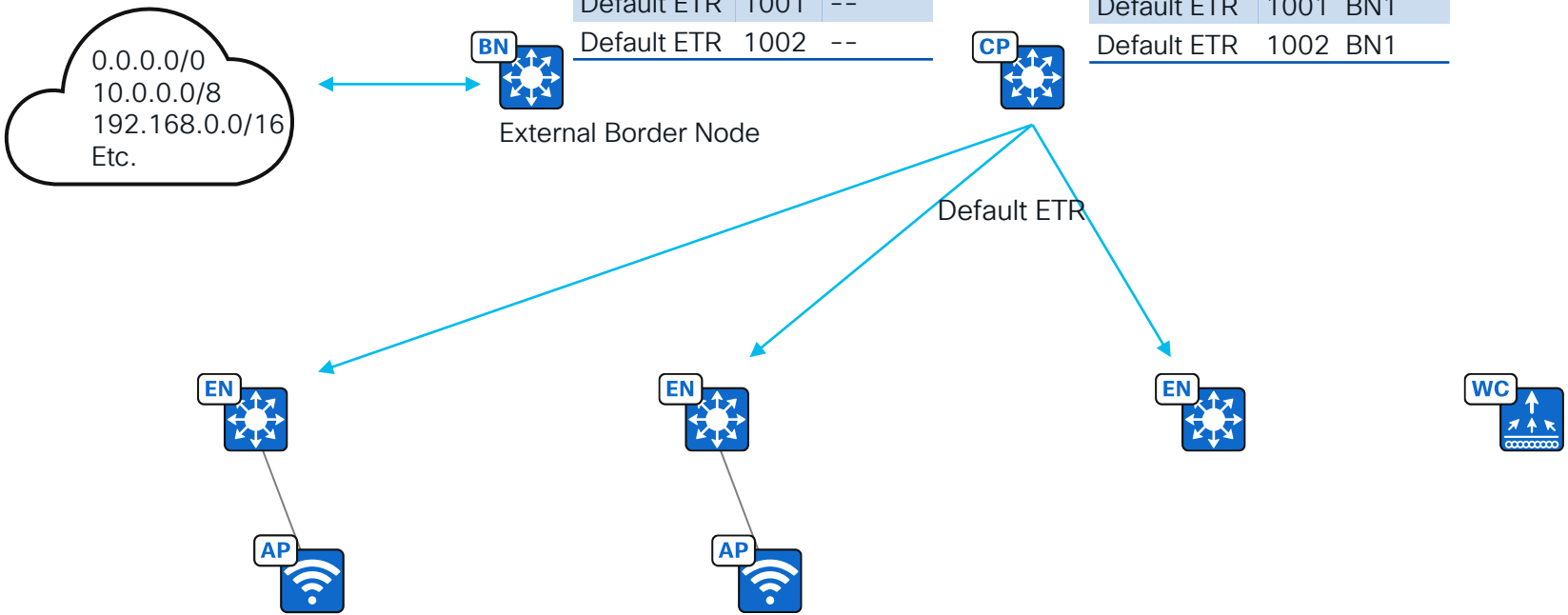
Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1

Fabric Operation

Edge Node Bootstrap

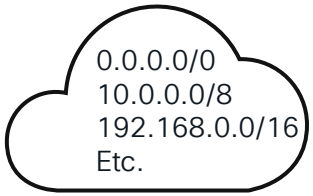
Destination	IID	Next Hop
Default ETR	1001	--
Default ETR	1002	--

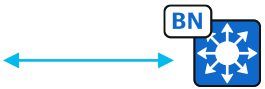
Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1



Fabric Operation

Edge Node Bootstrap



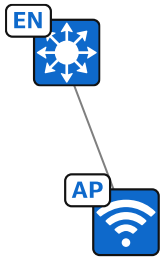


External Border Node

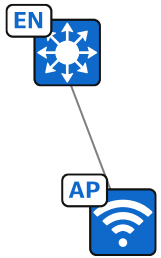
Destination	IID	Next Hop
Default ETR	1001	--
Default ETR	1002	--

Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1

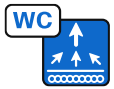
Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1



Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1

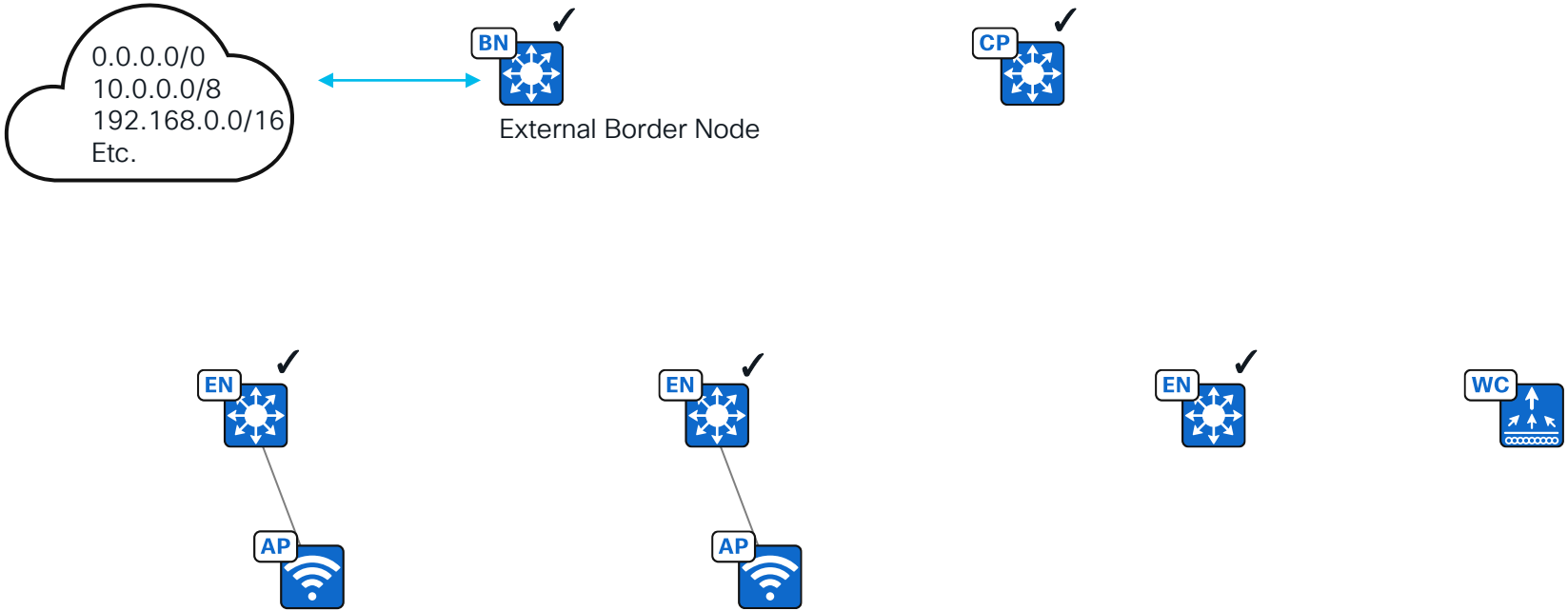


Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1



Fabric Operation

Edge Node Bootstrap



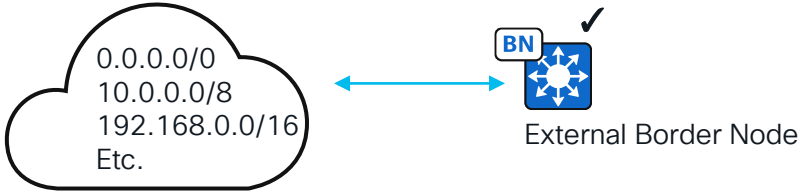
✓ Default ETR

Fabric Operation

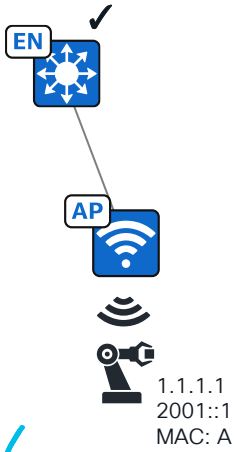
Endpoint Registration

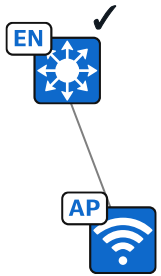
Fabric Operation

Endpoint Registration



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3





Destination	IID	Next Hop
2.2.2.2	1001	--

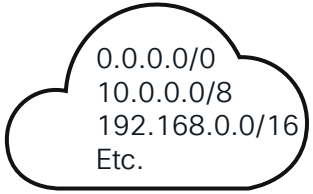
Destination	IID	Next Hop
1.1.1.1	1001	EN1

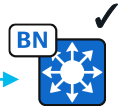
Register

✓ Default ETR

Fabric Operation

Endpoint Registration



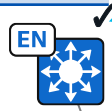


External Border Node

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

Notification

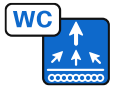
Destination	IID	Next Hop
1.1.1.1	1001	--



1.1.1.1
2001::1
MAC: A

Destination	IID	Next Hop
2.2.2.2	1001	--

2.2.2.2
2001::2
MAC: B

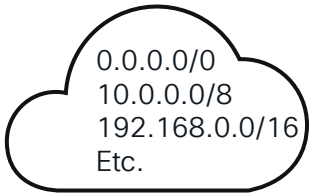


Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

Fabric Operation

Publish



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

BN ✓

External Border Node

Publish

CP ✓

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

Destination	IID	Next Hop
1.1.1.1	1001	--

EN ✓

AP

1.1.1.1
2001::1
MAC: A

EN ✓

AP

Destination	IID	Next Hop
2.2.2.2	1001	--

EN ✓

2.2.2.2
2001::2
MAC: B

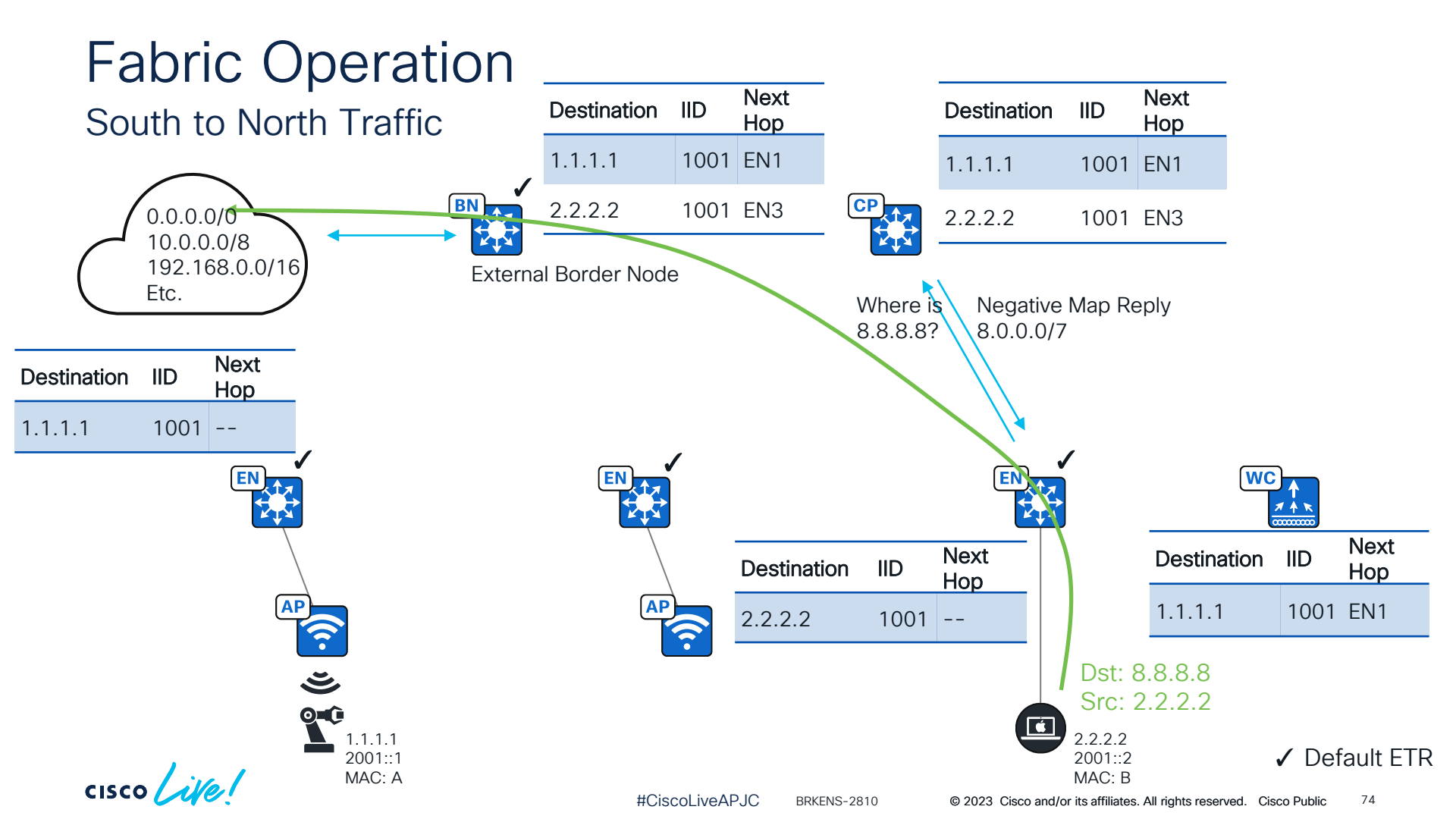
WC

Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

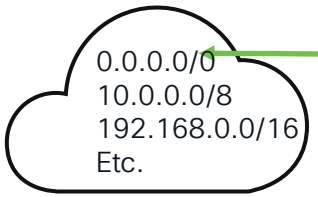
Fabric Operation

South to North Traffic



Fabric Operation

South to North Traffic



External Border Node

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

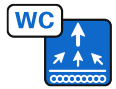
Destination	IID	Next Hop
1.1.1.1	1001	--

1.1.1.1
2001::1
MAC: A

Destination	IID	Next Hop
2.2.2.2	1001	--
8.0.0.0/7	1001	BN1

2.2.2.2
2001::2
MAC: B

Dst: 8.8.8.8
Src: 2.2.2.2

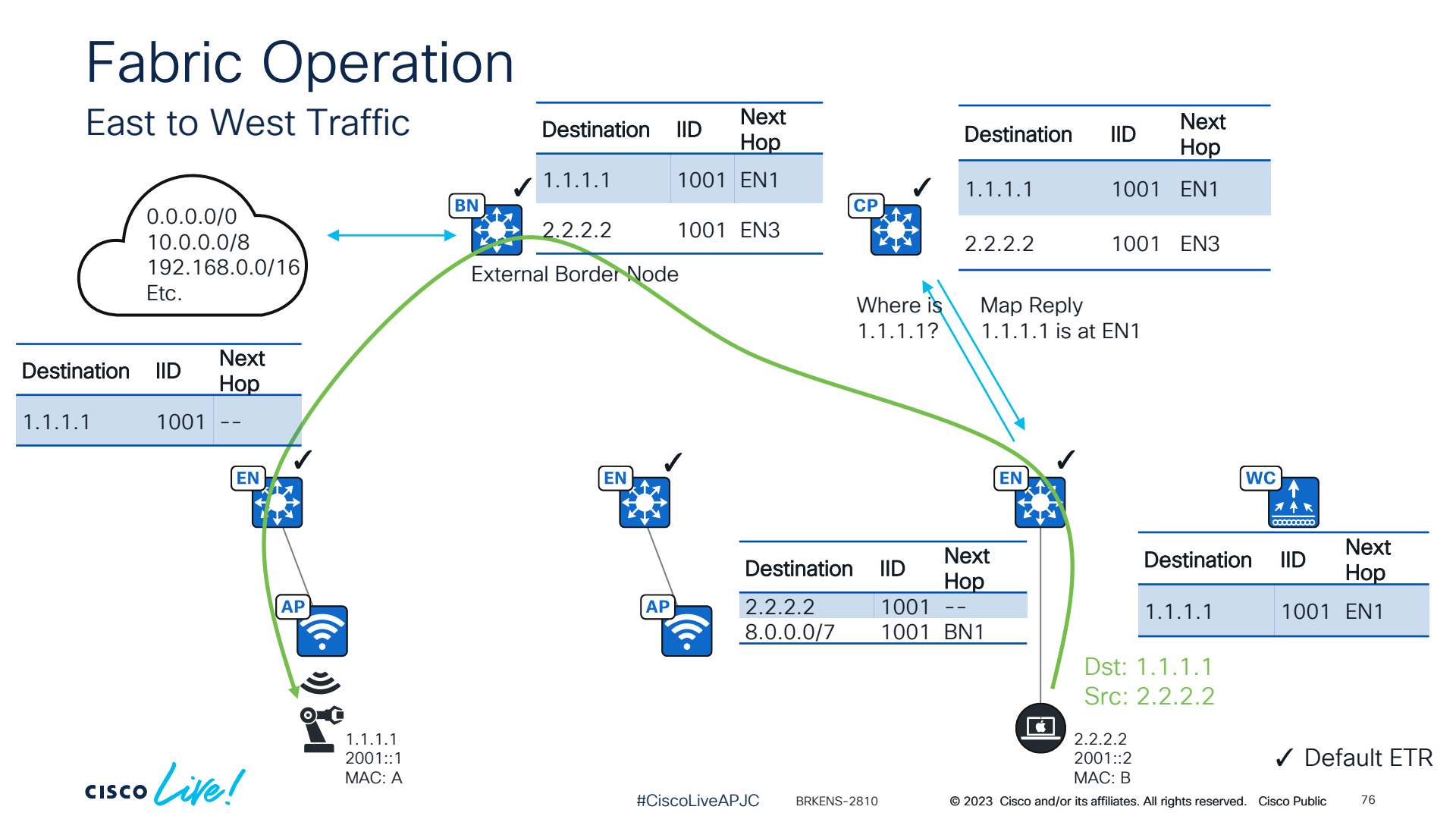


Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

Fabric Operation

East to West Traffic



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

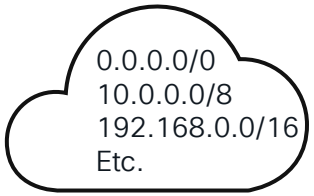
Destination	IID	Next Hop
1.1.1.1	1001	--

Destination	IID	Next Hop
2.2.2.2	1001	--
8.0.0.0/7	1001	BN1

Destination	IID	Next Hop
1.1.1.1	1001	EN1

Fabric Operation

East to West Traffic



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

BN ✓ External Border Node

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

CP ✓

Destination	IID	Next Hop
1.1.1.1	1001	--

EN ✓ AP

1.1.1.1
2001::1
MAC: A

EN ✓ AP

Destination	IID	Next Hop
2.2.2.2	1001	--
8.0.0.0/7	1001	BN1
1.1.1.1	1001	EN1

EN ✓

Dst: 1.1.1.1
Src: 2.2.2.2

2.2.2.2
2001::2
MAC: B

WC

Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

Advantages of LISP

- Optimised resource usage on Edge Nodes:
  - “Pull” only the information needed, like DNS. By comparison BGP pushes all routing information to all Edge Nodes.
- Underlay network is simple and stable:
  - IGP routing from Border Node to Edge Node. Maybe PIM. No L2, no VLANs, no link bundling, no STP, no MPLS.
- Unified wired and wireless data plane and policy plane.
  - No wireless concentrator bottleneck = higher throughput.
- Receive future innovations in later SD-Access + IOS XE releases.

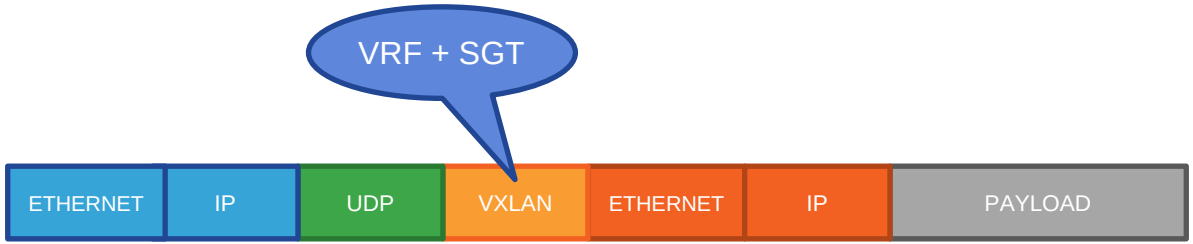
More LISP for the Inquisitive

- BRKENS-2828 – LISP Architecture Evolution
  - Roaming.
  - Extranet.
  - SD-Access Transit.
  - Dynamic Default Border.
  - Backup Internet.
  - LISP Priority (SD-Access traffic steering).
  - Affinity ID (SD-Access Transit traffic steering).
  - Etc.

Fabric Policy Security Groups

Cisco SD-Access Fabric

1. Control Plane: LISP
2. Data Plane: VXLAN
3. Policy Plane: Group-Based Policy

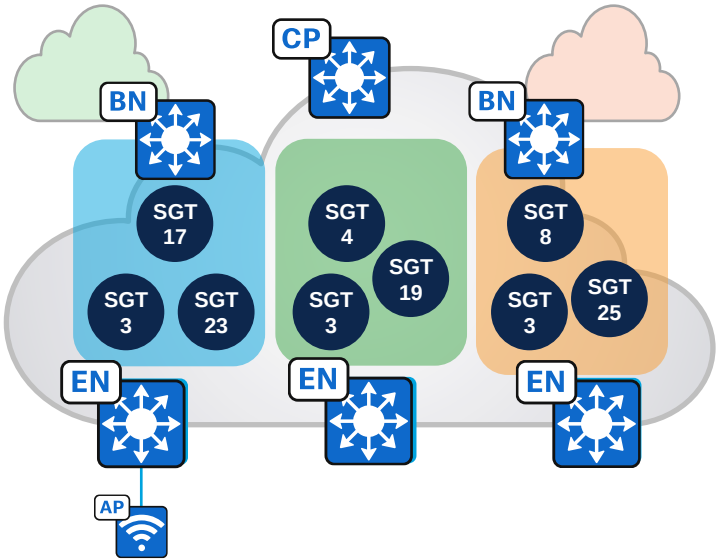


Virtual Routing & Forwarding
Security Group Tagging

Cisco SD-Access Fabric

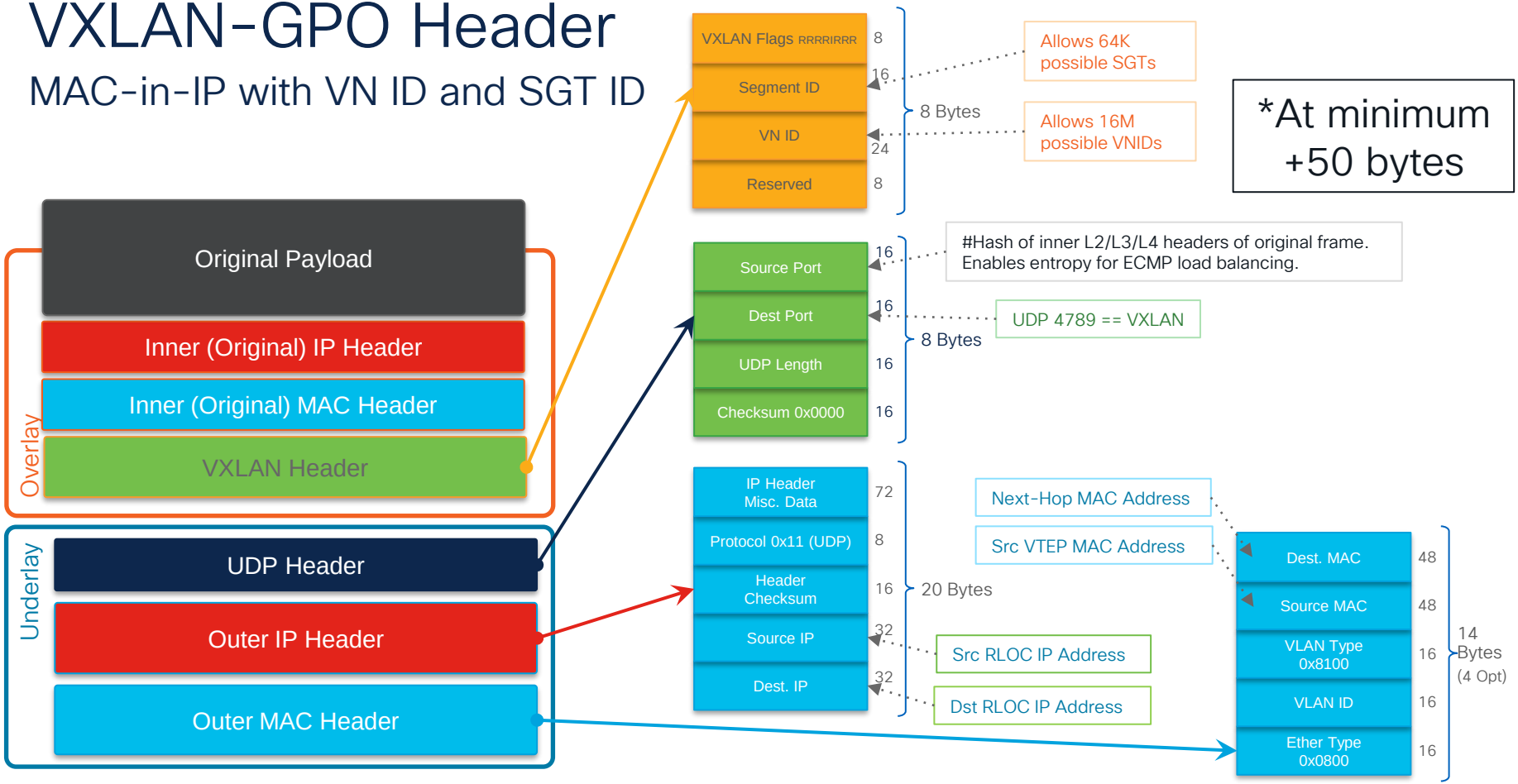
A Security Group Tag Assigns a “Group” to Each Endpoint

- Edge Nodes and Fabric APs assign a unique Scalable Group Tag (SGT) to each end endpoint in concert with ISE.
- Edge Nodes and Fabric APs add an SGT to the fabric encapsulation.
- SGTs are used to implement IP-address-independent traffic policies.
- SGTs can be extended to numerous other networking technologies e.g., Cisco Secure Firewall, Cisco SD-WAN, some third-party devices, etc.

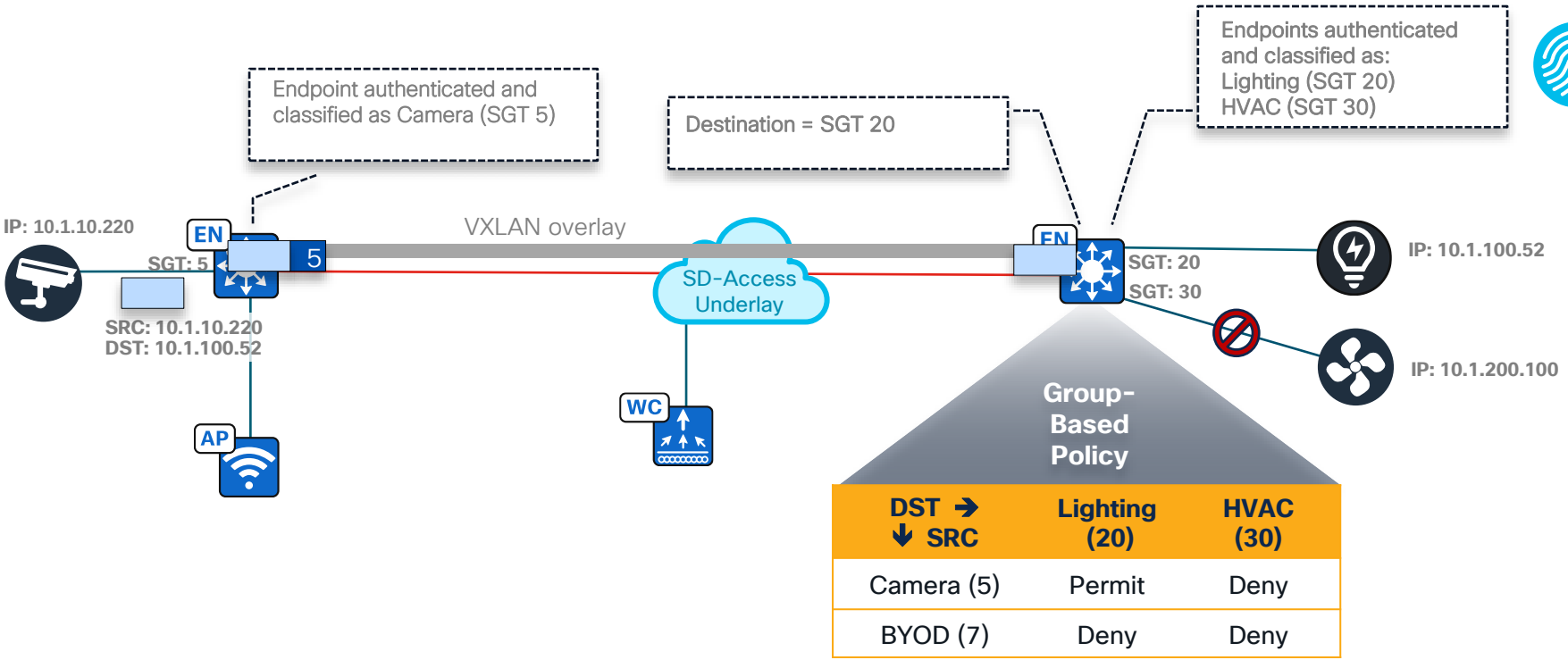


VXLAN-GPO Header

MAC-in-IP with VN ID and SGT ID

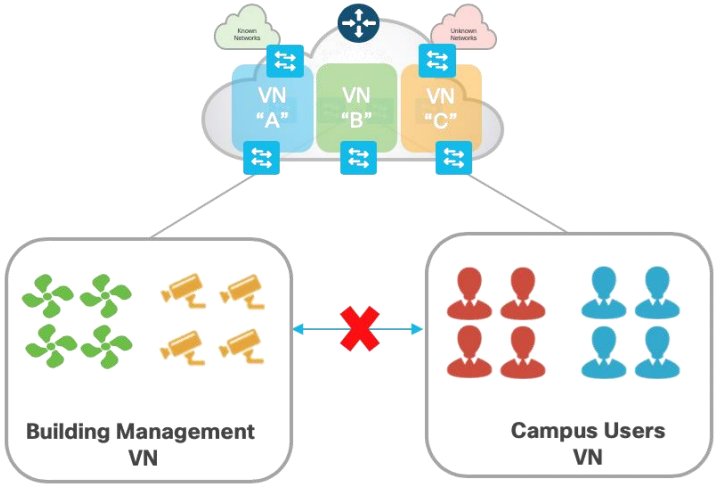


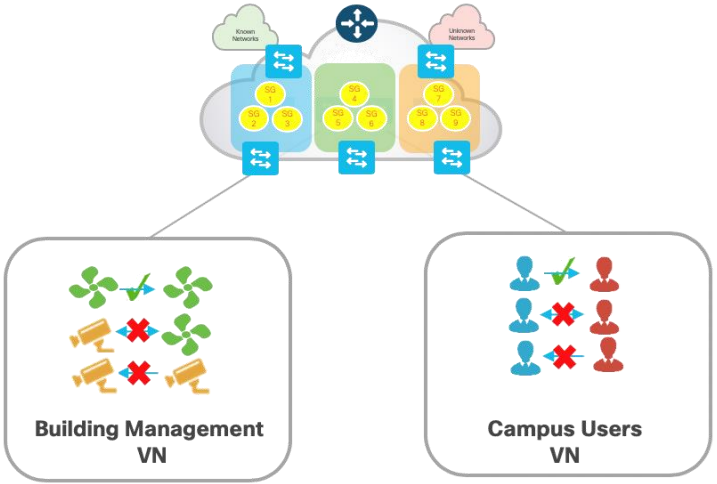
What is Security Group Tag and Group-Based Policy?



SD-Access Policy

Macro-Segmentation and Micro-Segmentation





Virtual Network (VN)

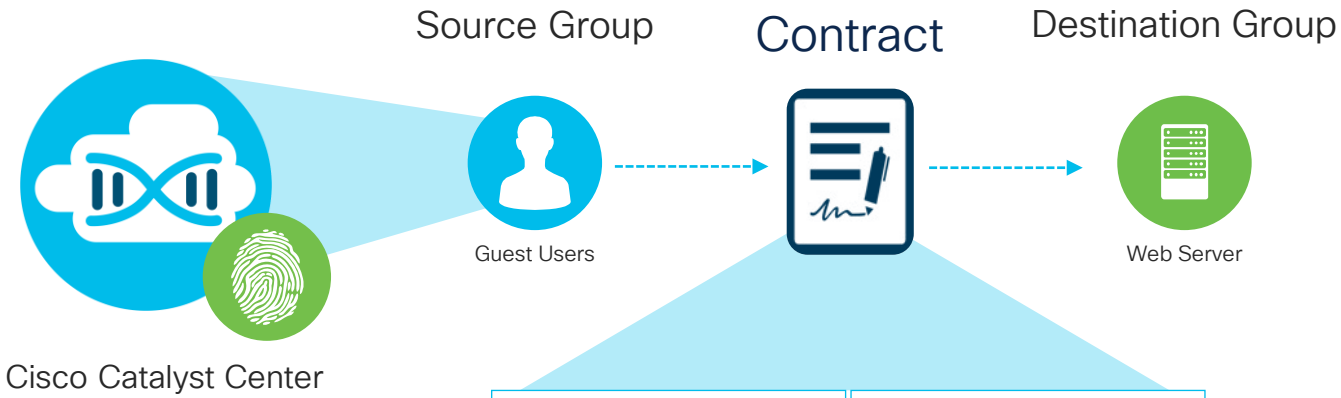
First-level Segmentation ensures **zero communication** between forwarding domains. Ability to consolidate multiple networks into one management plane.

Security Group Tag (SGT)

Second-level Segmentation ensures **role-based access control** between groups in a VN. Ability to segment the network into lines of business or functional blocks.

SD-Access Policy

Access Control Policies



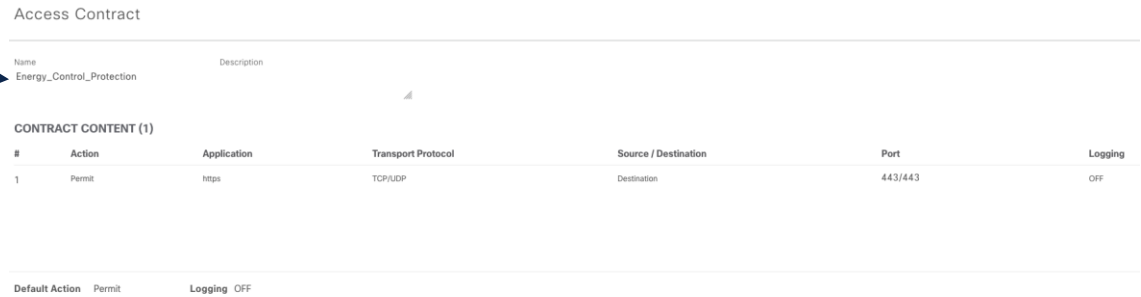
CLASSIFIER: PORT ▼ | ACTION: DENY ▼

Classifier Type	Action Type
Port Number	Permit
Protocol Name	Deny
Application Type	Copy

SD-Access Policy

Group-Based Access Control Policy

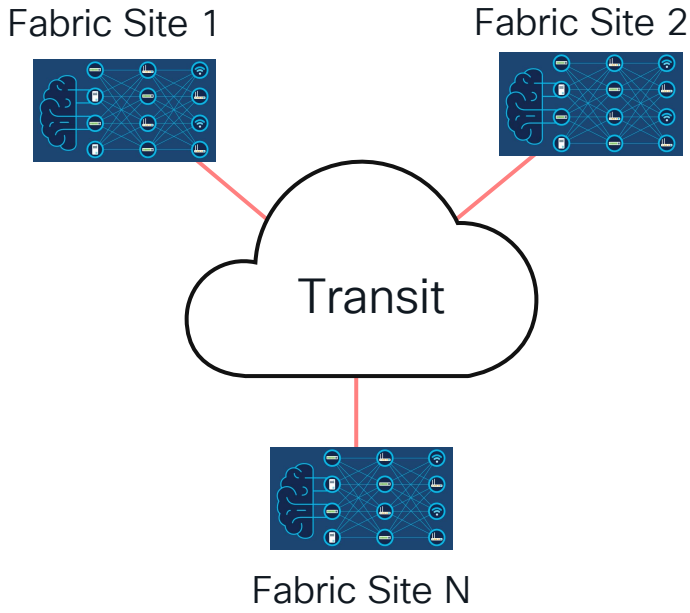
1. Select Source Group(s)
2. Select Destination Group(s)
3. Select Access Contract(s)



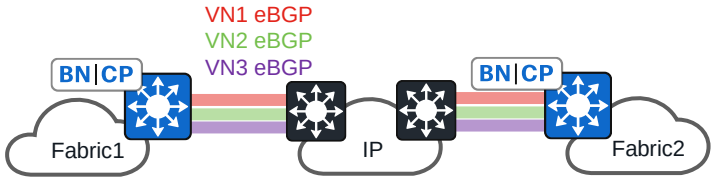
Multiple Fabrics

What is Fabric Site?

- An instance of an SD-Access Fabric.
- Typically defined by disparate geographical locations, but not always.
- Can also be defined by:
  - Endpoint scale.
  - Failure domain scoping.
  - RTT.
  - Underlay connectivity attributes.
- Typically interconnected by a “Transit”.



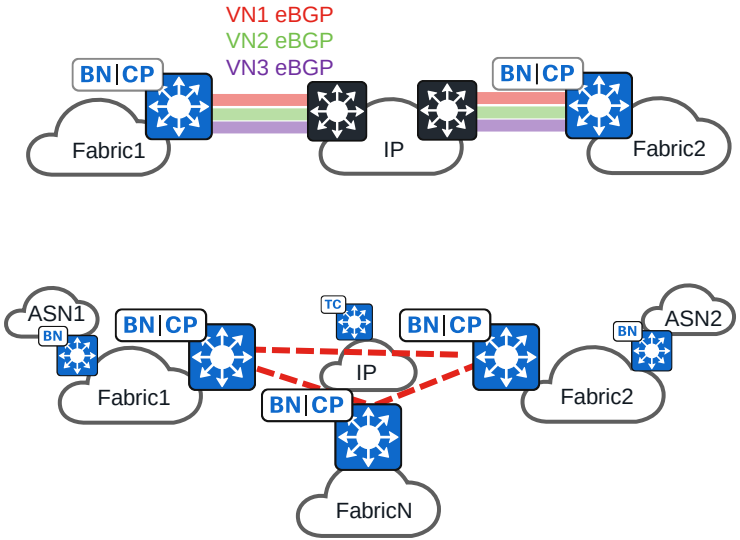
Transits for VN and SGT Preservation



IP-Based Transit

- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.

Transits for VN and SGT Preservation



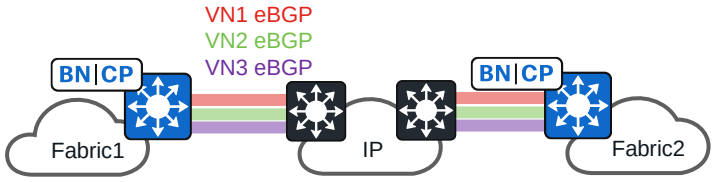
IP-Based Transit

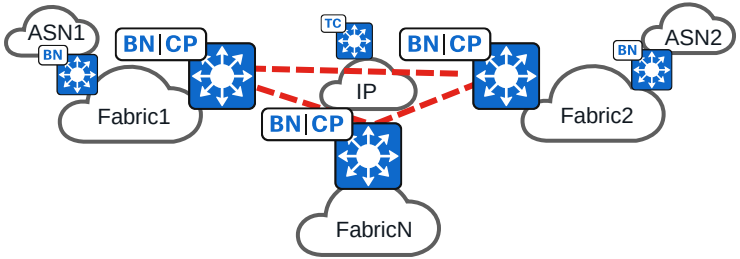
- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.

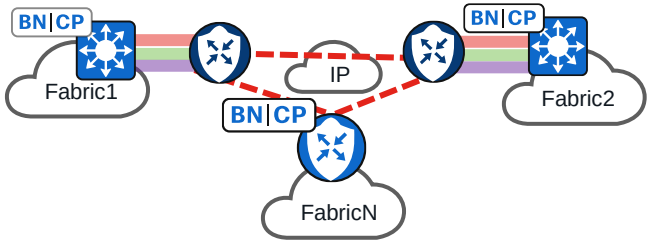
SD-Access Transit

- SD-Access LISP/VXLAN between Fabric Sites.
- Preserves Layer 3 Virtual Networks and SGT.
- Fabric as a transit between external routing domains.

Transits for VN and SGT Preservation







IP-Based Transit

- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.

SD-Access Transit

- SD-Access LISP/VXLAN between Fabric Sites.
- Preserves Layer 3 Virtual Networks and SGT.
- Fabric as a transit between external routing domains.

SD-WAN Transit

- Cisco SD-WAN between Fabric Sites.
- Separate SD-WAN Edge for flexibility, Border Node port density and speed. Independent Domains Prescriptive Design Guide, includes functional restrictions. Or Co-located SDWAN Edge for L3VN-VPN stitching with SGT data plane.

Conclusion

Conclusion

- Cisco SD-Access provides one interface for Fabric Automation, Identity-Based Policy, Segmentation, AI-Driven Insights and Assurance.

- Cisco SD-Access is a turnkey foundation for Zero Trust for the Workplace: Visibility, Segmentation and Containment.
  - BRKENS-2819 explores this angle further, 1:30 on Thursday.

- LISP is at the core of Cisco SD-Access: Efficient, scalable, flexible and evolving.

Why SD Access - Simplification

- SD-Access – simplifies wired and wireless
- IP Addressing simplification
- Improve Scaling both wired and wireless
- Policy Simplification and Improved Security
- Improved Performance
- Improved Availability
- Foundation for Zero Trust - Simplified and Continual Trust

cisco Live!

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.

Meet the Expert Opening Hours:

Tuesday	**3:00pm – 7:00pm**
Wednesday	**11:15am – 7:00pm**
Thursday	**9:30am – 4:00pm**
Friday	**10:30am – 1:30pm**

Session Surveys

We would love to know your feedback on this session!

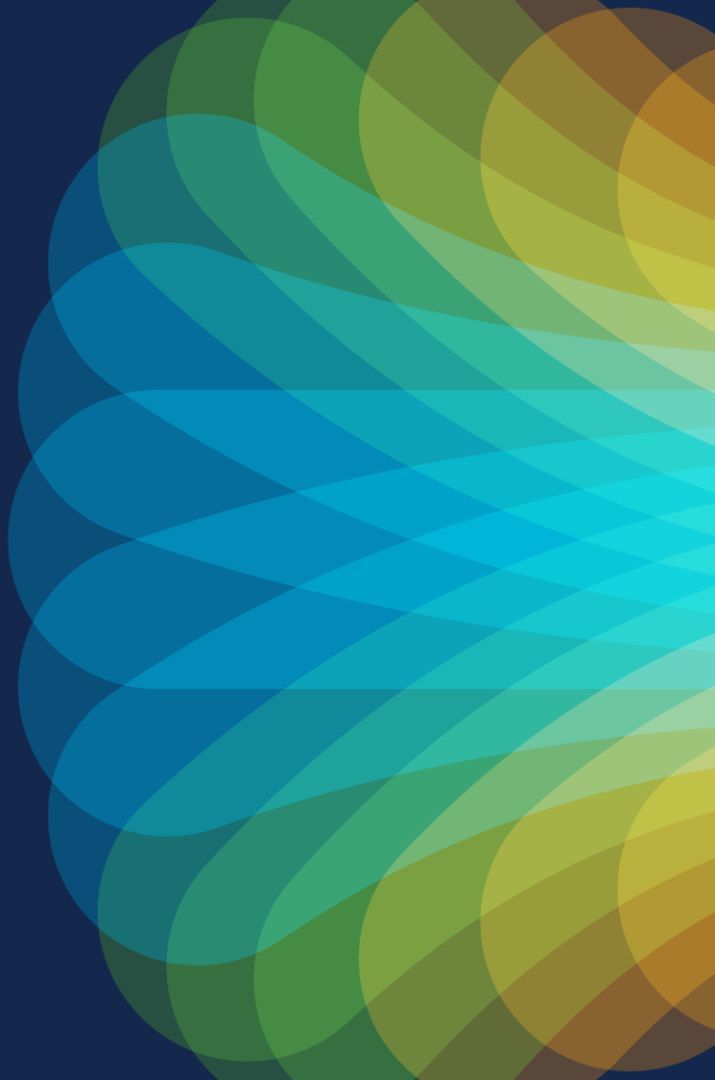
- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt

Continue your education

- Visit the Cisco Showcase 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

The bridge to possible

Thank you




cisco Live!
Let's go
#CiscoLiveAPJC