Cisco SD-Access LISP Solution Fundamentals

Kedar Karmarkar - Principal Engineer, Technical Marketing

BRKENS-2810

Cisco SD-Access LISP Solution Fundamentals

- Why Cisco SD-Access LISP?
- Roles and Terminology
- Fabric Fundamentals
- Multiple Fabric
- Conclusion

Cisco Live EMEA SD-Access Learning Map

Sunday–9th

LABENS-2302 06:15 AM
SD-Access Troubleshooting

LABENS-2410 07:00 AM
Explore the Art of Cross-Domain Automation with SD-Access and SD-WAN

LABENS-2664 08:30 AM
Building the SD-Access Fabric with Ansible Playbooks: DIY SDA

TECENS-3820a 01:30 PM
Software-Defined Access - Architecture Deep Dive - Part 1

TECENS-2850 01:30 PM
Security in Enterprise - A cross-domain security primer across LAN, wLAN and WAN

Monday–10th

TECENS-3688 08:30AM
Advanced Cisco SD-Access Troubleshooting

TECENT-3688 08:30 AM
Advanced Cisco SD-Access Troubleshooting

TECENS-3820b 08:45 AM
Software-Defined Access - Architecture Deep Dive - Part 2

BRKENS-2810 02:15 PM
Cisco Software-Defined Access LISP Solution Fundamentals

Tuesday–11th

CCP-1897 08:00AM
SD-Access and Zero Trust: Strategy, Impact, and Vision

BRKENS-1852 08:00AM
TrustSec Refresh Reinforced with Common Policy Innovations

LTRENS-2509 08:30 PM
Mastering Cisco SD-Access: LISP Pub/Sub and its Benefits Made Simple

BRKENS-2811 02:30 PM
Connecting Cisco SD-Access LISP to the World: Use Cases and Segmentation

BRKENS-2824 04:30 PM
Deploying Your First Cisco SD-Access Project

Wednesday–12th

IBOENS-2820 09:00 AM
Deploying a Global SD-Access Zero-Trust Network

BRKENS-1803 12:30 PM
Real-World Success Stories Powered by Cisco SD-Access!

BRKENS-1851 01:00 PM
Zero Trust: Secure the Workplace with Cisco Software-Defined Access

LTRENS-3751 02:00 PM
SD-Access as Code with Cisco Catalyst Center and ISE Automation

BRKENS-2827 03:00 PM
Cisco SD-Access Migration Tools and Strategies

BRKENS-2502 05:00 PM
Cisco SD-Access LISP VXLAN Fabric Best Practices: Design and Deployment

Thursday–13th

BRKENS-2820 08:45 AM
Demystifying IP Multicast in SD-Access

BRKENS-3826 12:15 PM
Advanced LISP SD-Access Forwarding Architecture

BRKTRS-3821 02:15 PM
Mastering Troubleshooting with Cisco Catalyst Center & SD-Access

BRKENS-2819 03:00 PM
Cisco SD-Access and Multi-Domain Segmentation

IBOENS-2820 03:00 PM
Deploying a Global SD-Access Zero-Trust Network

BRKENS-3810 05:15 PM
How to Adopt Zero Trust using SD-Access and Default-Deny without Tears

Friday–14th

BRKENS-3834 11:00:AM
1 to 100: Master All Steps of Deployment, Seamless Integration, and Migration of Large SDA and SD-WAN Networks

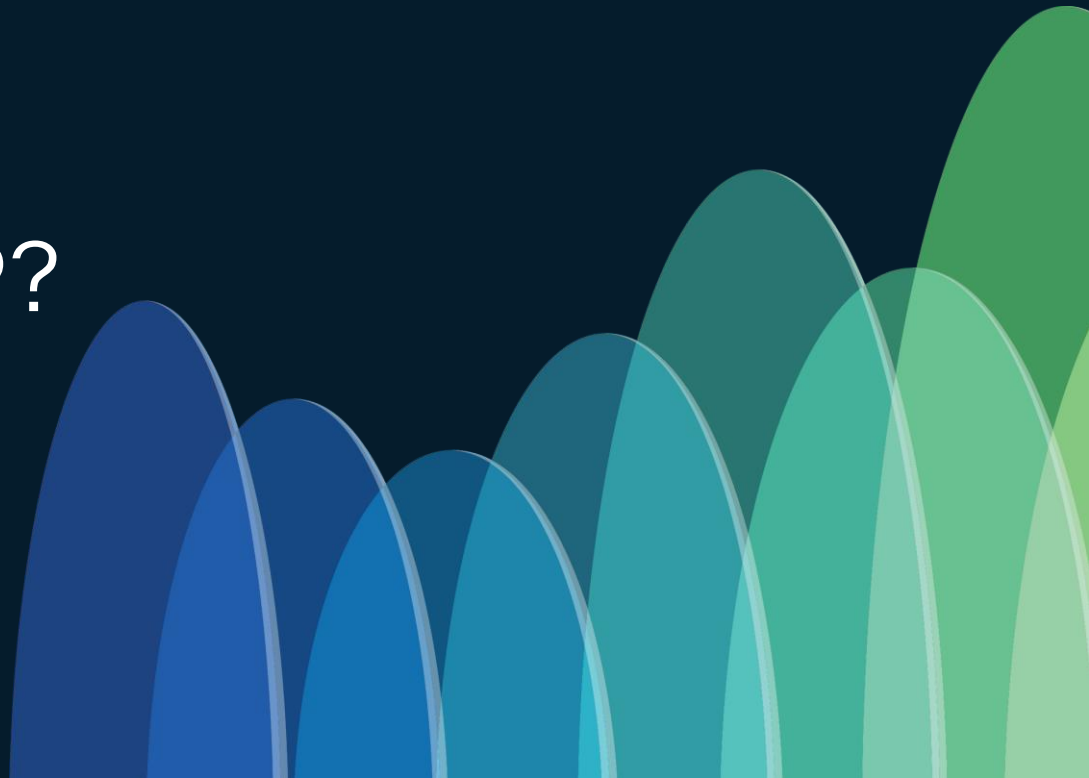
Capture The Flag
@Hub All week long

BU-led sessions

Catalyst Center

Cisco SD-Access LISP

Why Cisco SD-Access LISP?



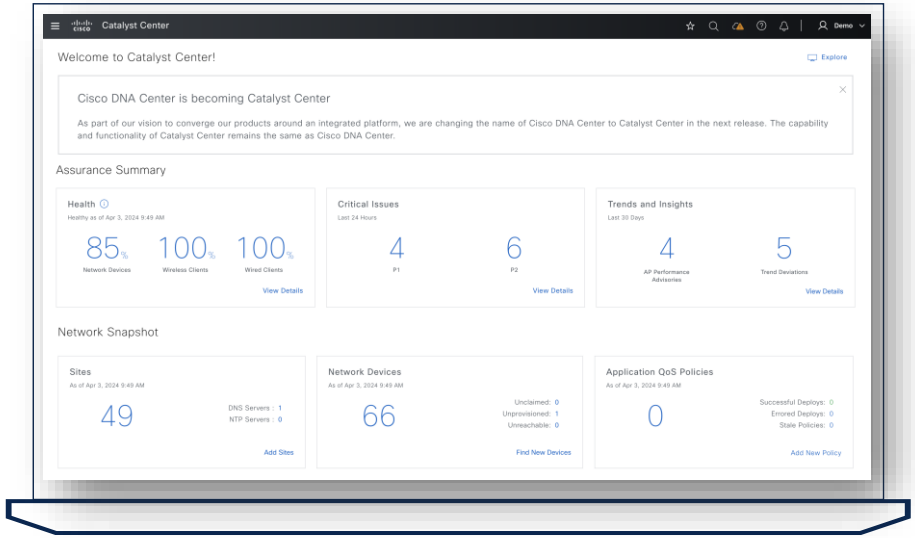
cisco Live!

Options for Orchestration of LISP Overlay

- Cisco Catalyst Center automated configuration of a Cisco LISP Fabric which includes Macro and Micro Segmentation
  - Includes SDA Automation Workflows and Integrations
  - Best practice standardized configurations, consistency in order of operations
  - Includes SDA Assurance and Telemetry
- OR
- CLI Configuration of Cisco LISP Fabric which includes Macro and Micro Segmentation
  - Open integration with heterogenous tooling (CLI, Ansible, NSO, etc)
  - Agile customization within the parameters of the LISP Fabric validated design
  - Can support Catalyst Center Device and Client Assurance

Intent-Driven Automation

Standardized templates for consistent implementation



Easy for admins to configure and manage networks

Configuration workflows to drive intent

Create Layer 3 Virtual Networks

Create a Layer 3 Virtual Network to host interconnect IP subnets.

Create Fabric Site

Create and configure an SD-Access Fabric Site and Fabric Zones. Fabric Zones are optional and reside within Fabric Sites.

Create Anycast Gateways

Create a gateway to attach IP pools to Layer 3 Virtual Networks.

Configure Multicast

Configure multicast routing within Cisco SD-Access Layer 3 Virtual Networks.

Create Extranet Policy

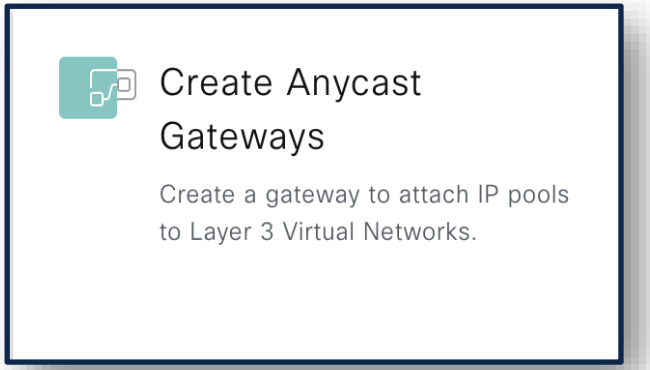
Create an Extranet Policy to share services between a Provider Virtual Network and one or more Subscriber Virtual Networks.

... and many more!

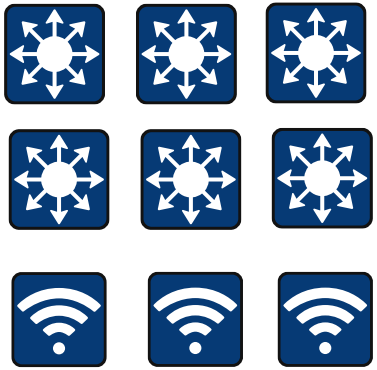
Intent-Driven Automation

Automation with highly flexible scale

Best practice configurations curated and validated extensively for each workflow.



Simple UI based guided workflow for the administrator to deploy with a few clicks.

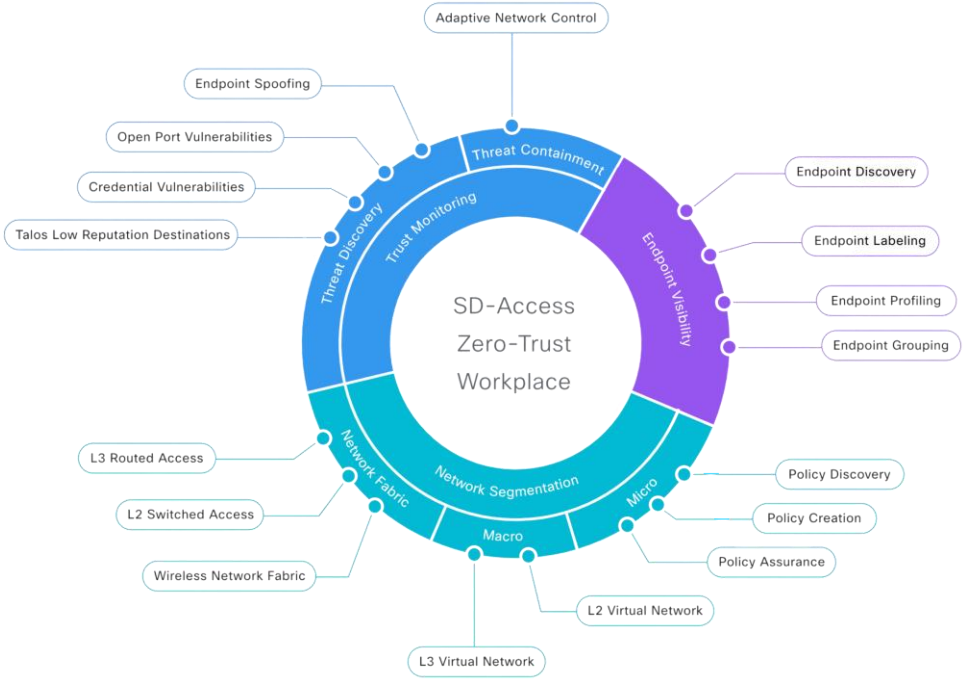


Configure multiple devices across or within a site in one-go!

SD-Access Zero-Trust Workplace

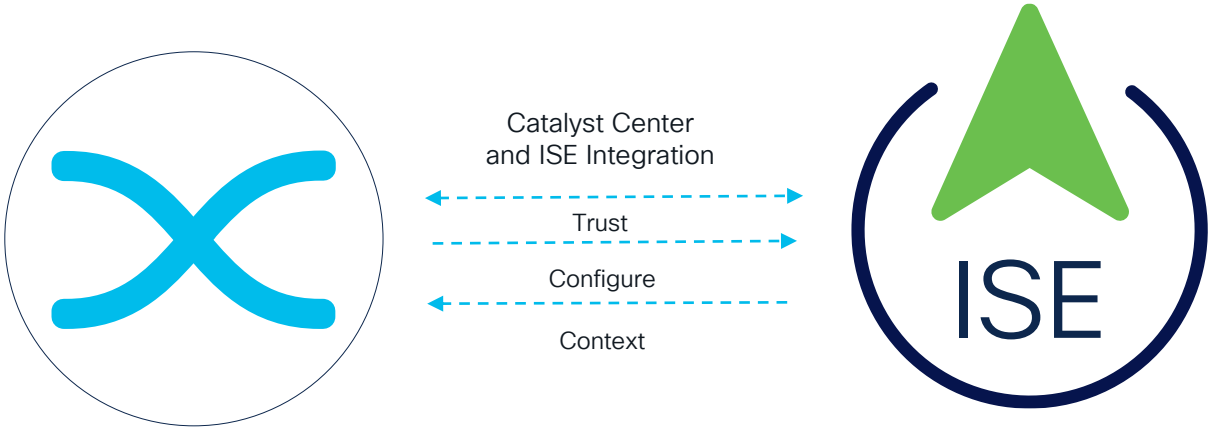
Based on the Organization's goal, explore and achieve Zero Trust for workplace.

3 Pillars of SD-Access Zero Trust Workplace: Visibility, Segmentation, and Trust.



Attribute-Based Policy and Segmentation

Catalyst Center and ISE integration facilitates automated configuration and segmentation at scale



Automated configuration and segmentation policies paired with scalable onboarding of endpoints.

Attribute-Based Policy and Segmentation

Move away from IPs and ACLs to Group Based Access Control

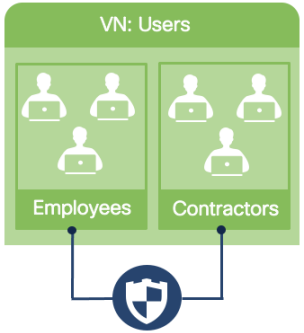
Catalyst Center and ISE Integration

Trust

Configure

Context

Authentication Template defined on Catalyst Center



Dynamically onboard end users and devices, assign Security Group Tags, and create policies aka *Microsegmentation* in SD-Access.

Tailormade for Campus Networks

Bringing together best of wired and wireless

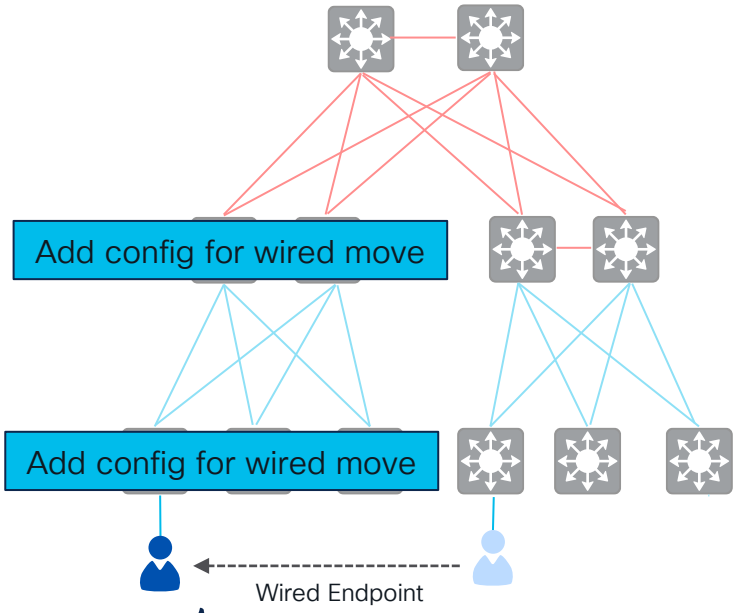
Campus =
People + Things

University ● Large Corporations ● Banks
Healthcare ● Manufacturing

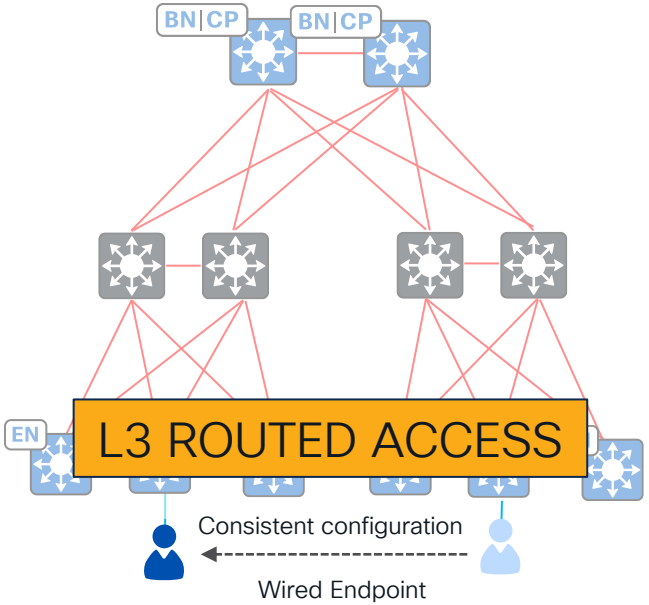
Tailormade for Campus Networks

Seamless and secure mobility of endpoints (Wired use-case)

Traditional Network



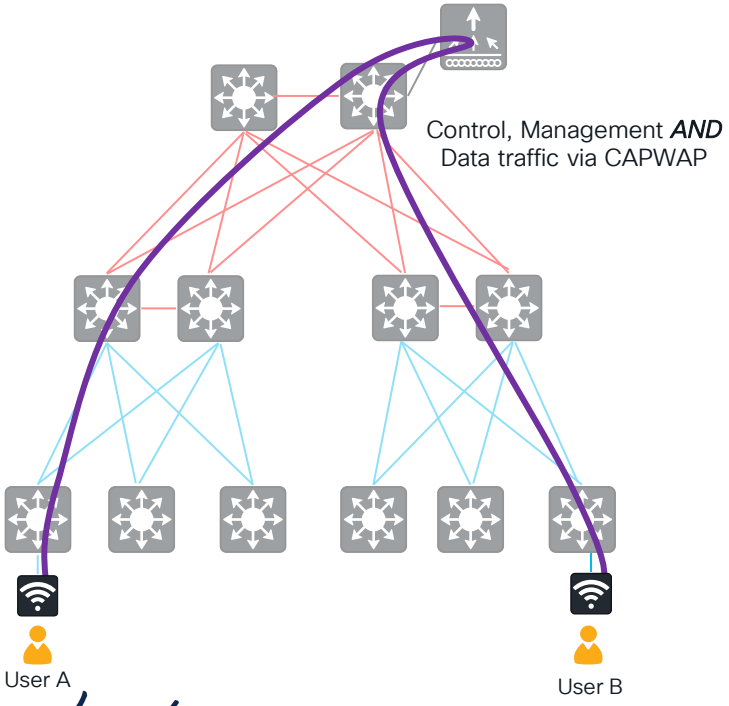
Software-Defined Access



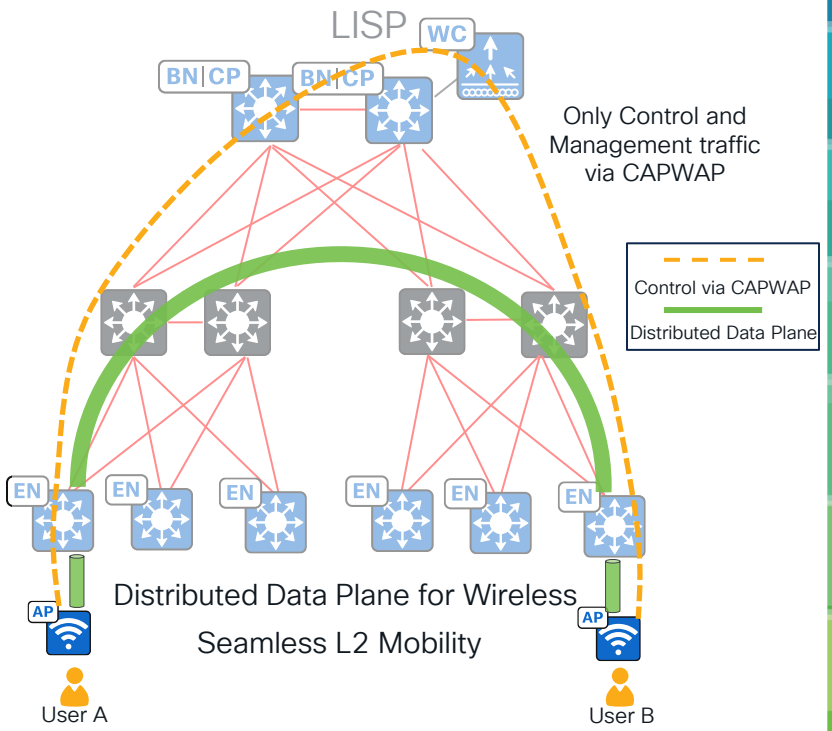
Tailormade for Campus Networks

Seamless and secure mobility of endpoints (Wireless use-case)

Traditional Network

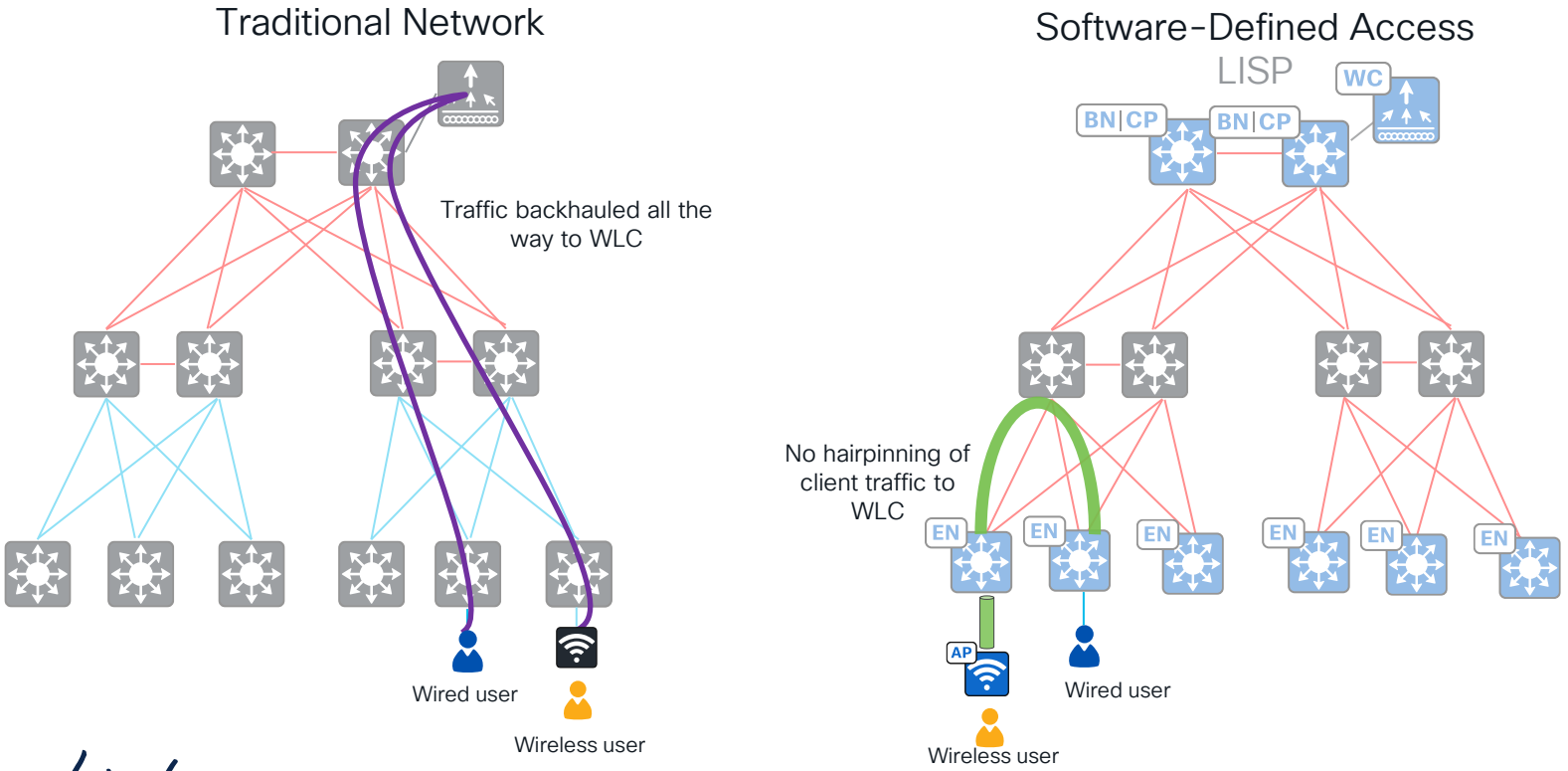


Software-Defined Access



Tailormade for Campus Networks

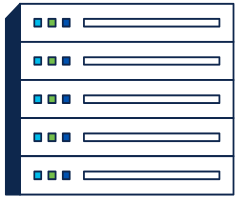
Example of traffic flow between wireless and wired endpoint



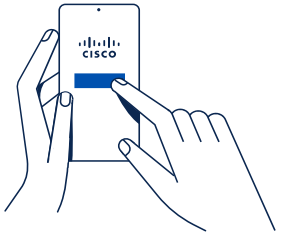
AI-Driven Insights and Telemetry

The more you know!

End user insights

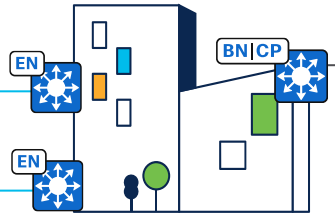


Network health and status



Application Visibility & Performance

Onboarding, Connectivity, IPv4/v6,
Device Type, MAC, VLAN, Trust Score etc.



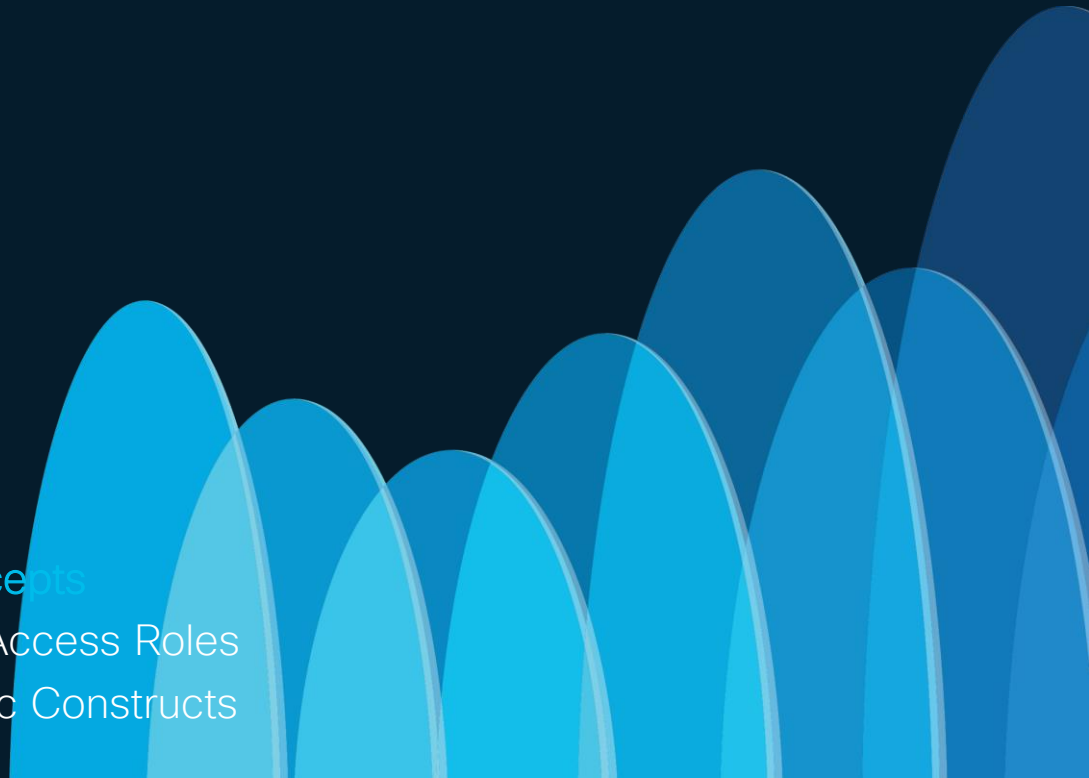
Site Health, System Health, Topology,
Issues and Suggested Actions

Data Center / Cloud Hosted Apps

Application Usage/Throughput, Business Relevant
Application Health, Integrations, Trends

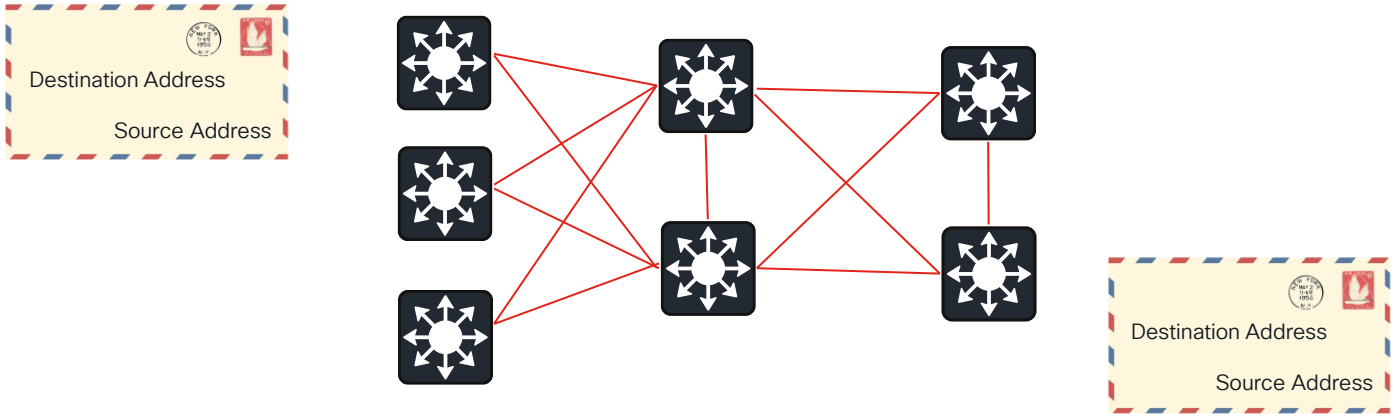
Roles and Terminology

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



Underlay and Overlay

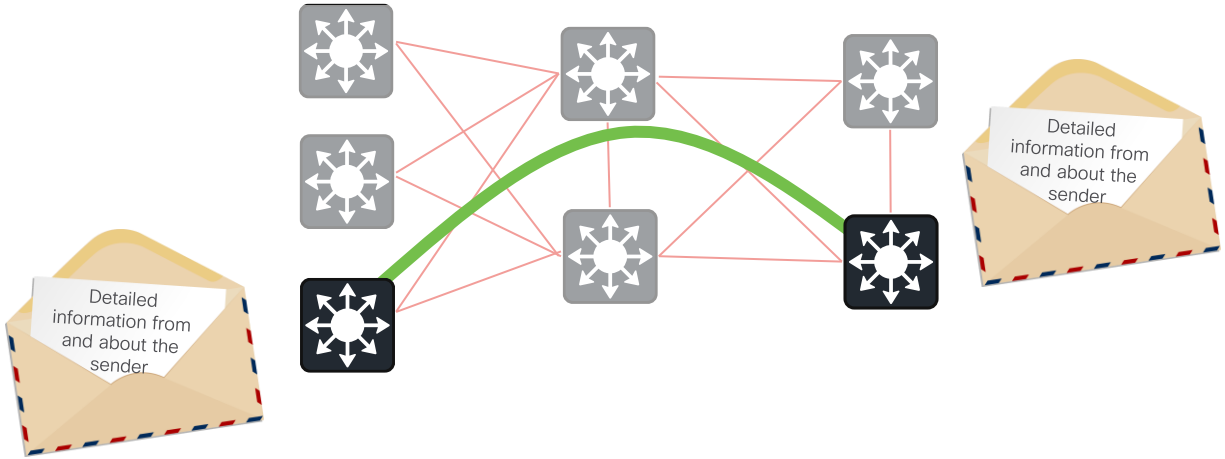
Generally Speaking



Underlay Network = Physical Infrastructure to provide IP reachability with redundancy and resiliency.

Underlay and Overlay

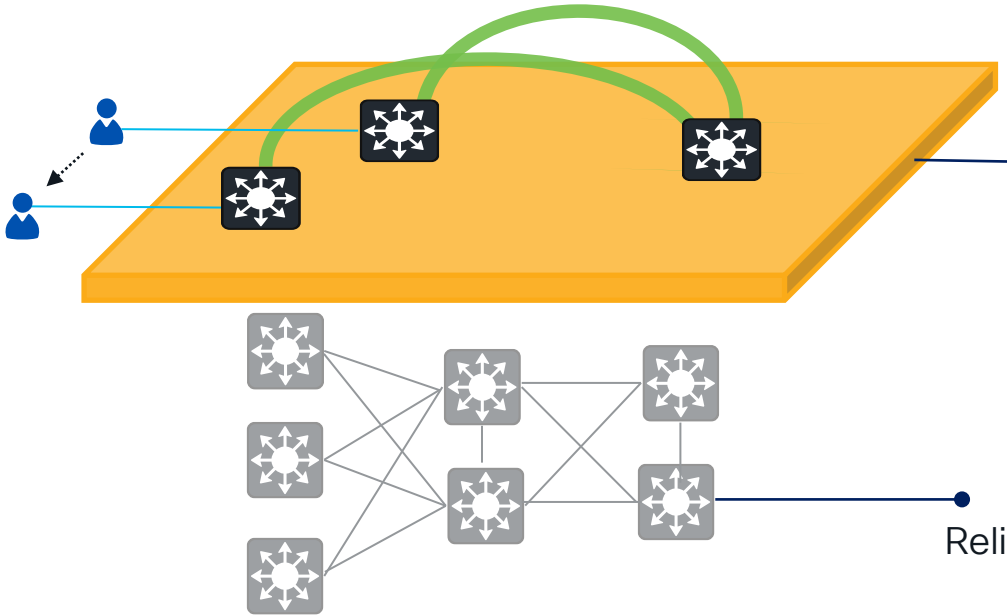
Generally Speaking



Overlay Network = Logical topology used to virtually connect devices to provide additional services, not delivered by the Underlay.

Underlay and Overlay

But why?

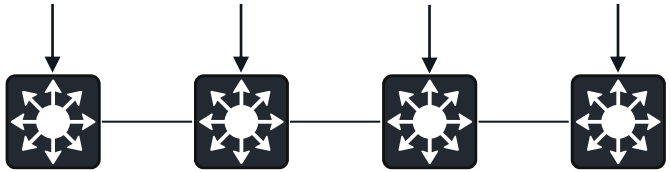


Overlay (Fabric): Flexible, Scalable and Extensible. Easy to add/modify services. Optimizes mobility events.

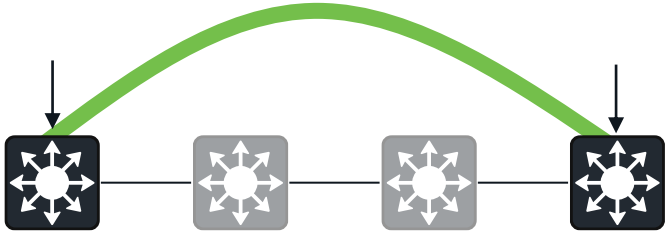
Underlay: Build and forget! Reliable, manageable, and simple.

Underlay and Overlay

But why?



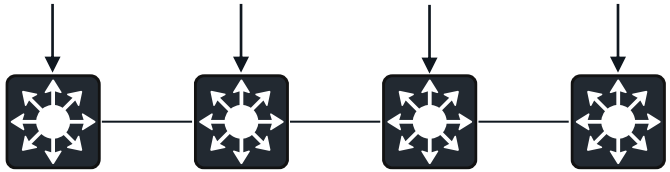
Would you rather configure network segmentation hop-by-hop?



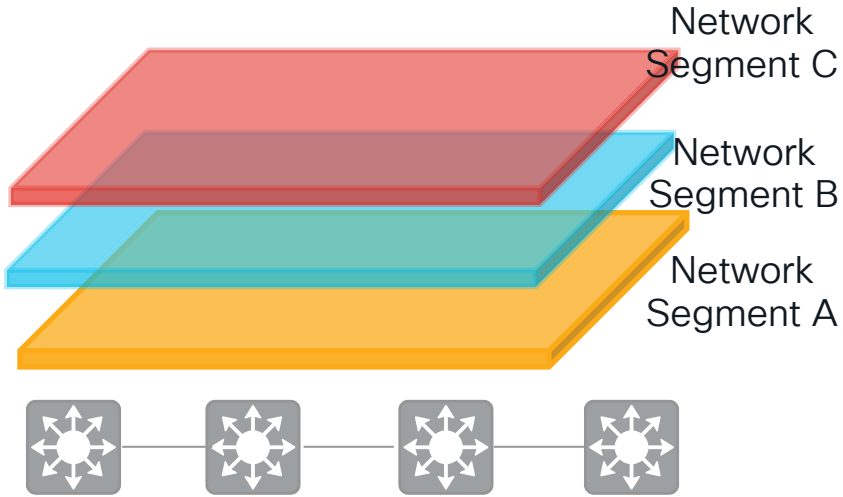
Or simply carry the segmentation tags in the overlay?

Underlay and Overlay

But why?



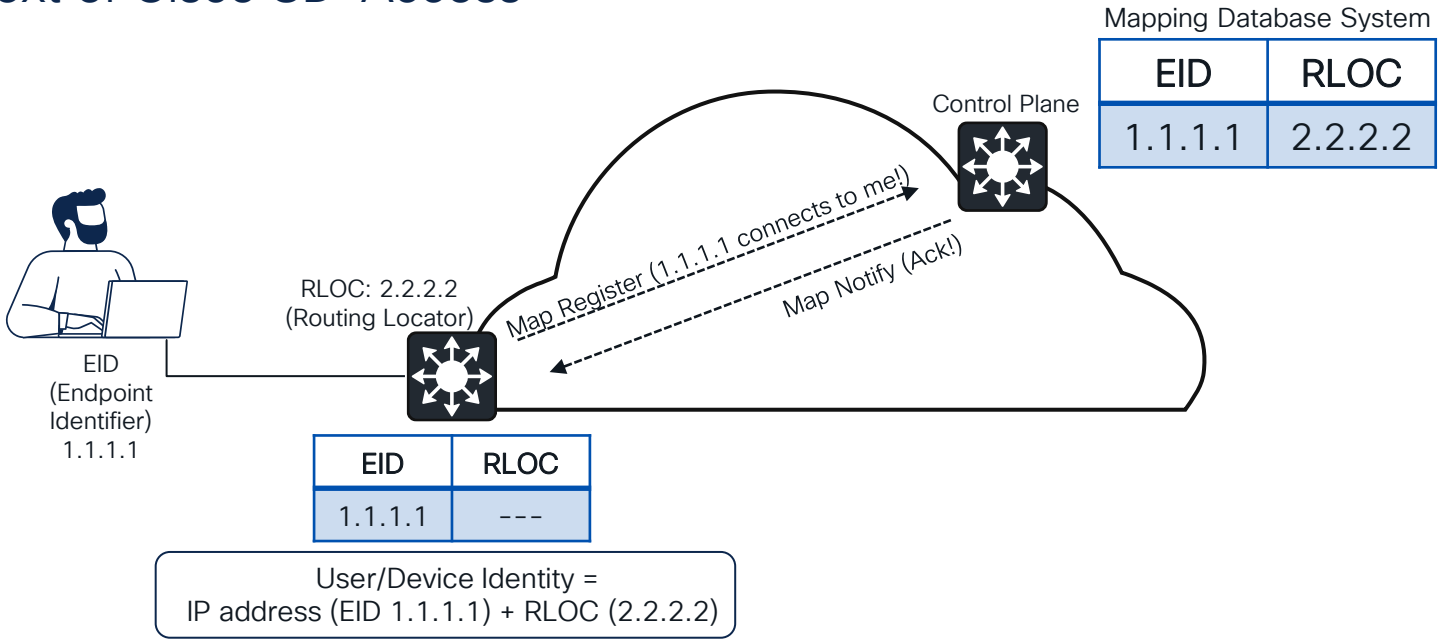
Would you rather configure network segmentation hop-by-hop?



Multiple segments in the overlay that underlay is unaware of!

Underlay and Overlay

In context of Cisco SD-Access



Locator **I**dentity **S**eparation **P**rotocol

Control Plane Protocol of choice. Lightweight, Extensible, and Scalable.
Supports Layer 3 Overlay. Pull Based Model. Scoped Signaling.

Fundamental Design Principle in LISP

- A key basic design objective:
  Distribute routing/mapping information **only where it is required**

- A basic working principle:
  *Use traffic signals to **pull** routes* **when required**

Advantages of using LISP as Overlay Control Plane

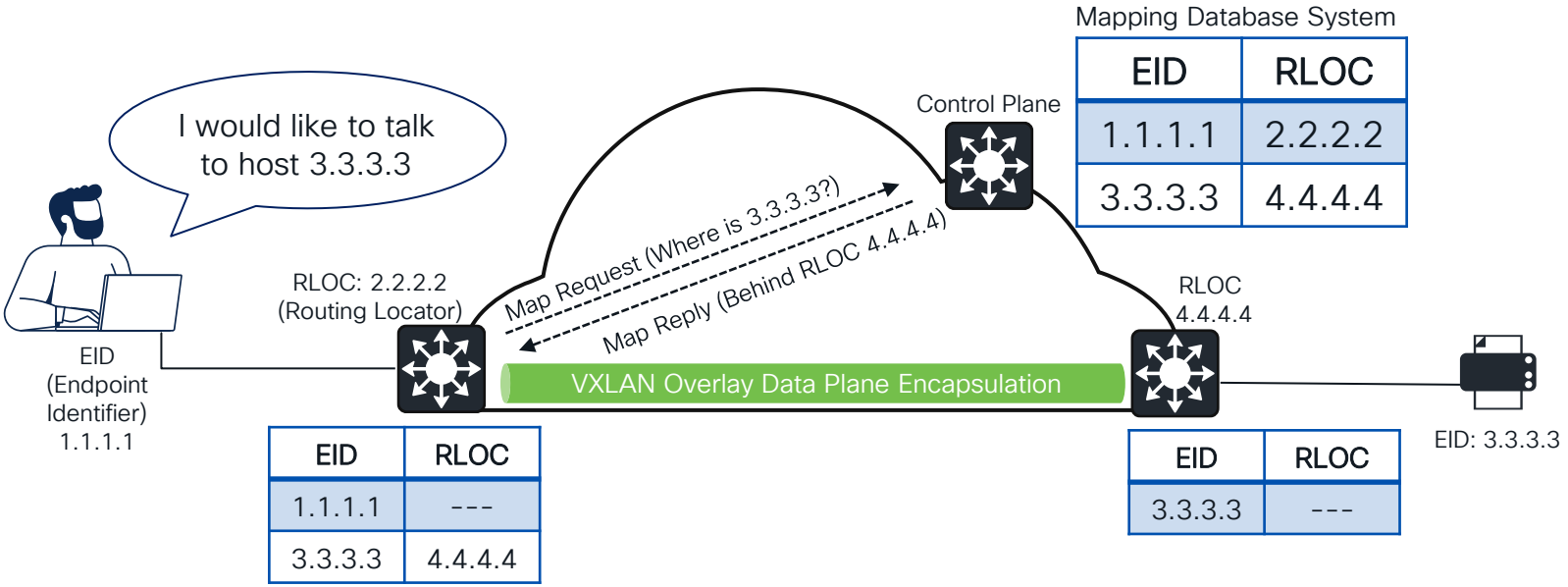
- Network simplicity all the way down to the access and in fabric operations
- Network that uses resources (like TCAM, CPU, Memory) efficiently
- Flexibility in scale of network design not compromised by protocol limitations
- Improve the wireless throughput and roaming performance at large scale with a fast-converging network with the Wireless Integration with LISP
- Wired/Wireless consistency in configuration, policies, and troubleshooting
- Smart, efficient, fast-converging, reliable, scalable network that is extensible
- Interoperability with 3rd party as well as Cisco
- Standards-based network

Advantages of using LISP as Overlay Control Plane

Features	LISP
Standards-based	Yes
Resource usage	Very light
Protocol working	Simple
Built for	Overlays
Signaling	Scoped (Pull-on-demand, Push where you need)
Silent Host Wake-Up Support	No flood, Efficient
Path calculation algorithms	Not needed
Convergence	Fast
Wireless Integration	Yes
Extensibility	Fast
Scale	Massive and Flexible
Most useful for	Overlay (Indexing exercise)

Underlay and Overlay

In context of Cisco SD-Access



Virtual e**X**tensible **L**ocal **A**rea **N**etwork

Data Plane Protocol of choice. Supports Layer 3 and Layer 2 Overlay.

Underlay and Overlay

In context of SD-Access

What about our good friend Underlay?

A

B

IGP of your choice that gets information from Source RLOC to Destination RLOC, the best way it can.

BGP VRF-Lite for external communications

What is an SD-Access Fabric Site?

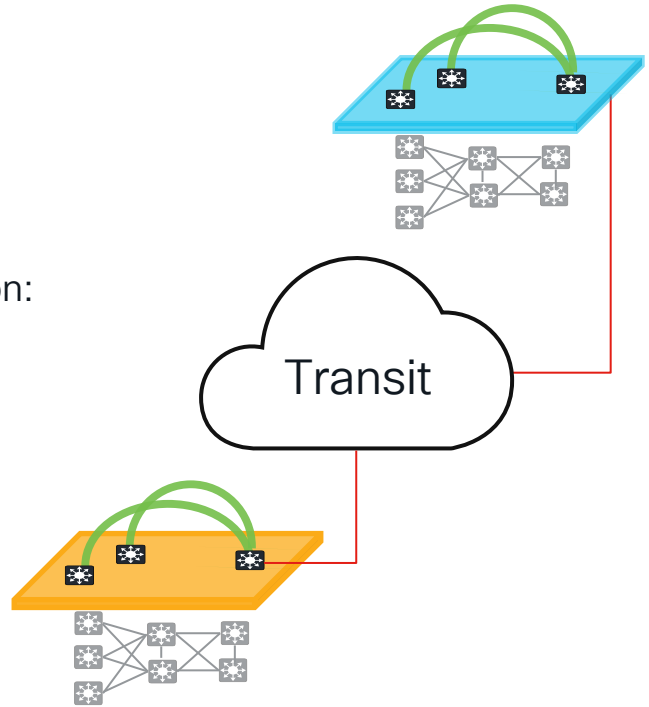
Definition and more

SD-Access Fabric Site offers programmable overlays for wired and wireless campus networks, enabled on a single physical infrastructure.

A single fabric site could be demarcated and defined based upon:

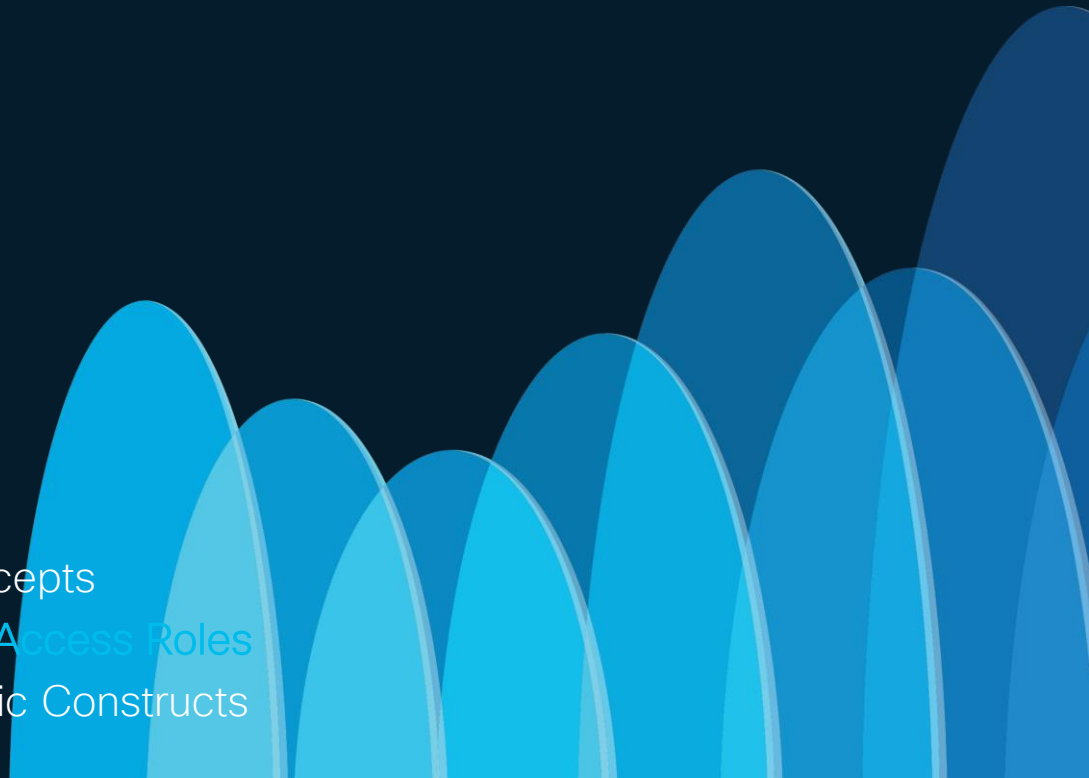
- Geographical location.
- Endpoint scale.
- Failure domain scoping.
- RTT.
- Underlay connectivity attributes.

Multiple fabric sites interconnected by a “Transit”.



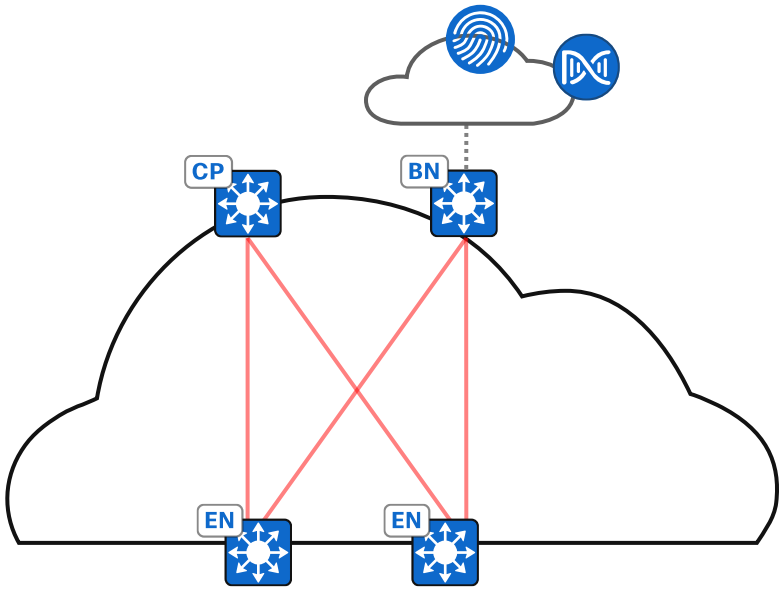
Roles and Terminology

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



Cisco SD-Access Roles

Key Roles for a Complete Wired and Wireless Campus Experience



Cisco Catalyst Center

GUI and APIs for intent-based automation of wired and wireless fabric devices.

Identity Service Engine

NAC and ID services for dynamic endpoint to Security Group Tag mapping and policy distribution.

Control Plane Node

Map System that tracks endpoint to fabric node relationships.

Border Nodes

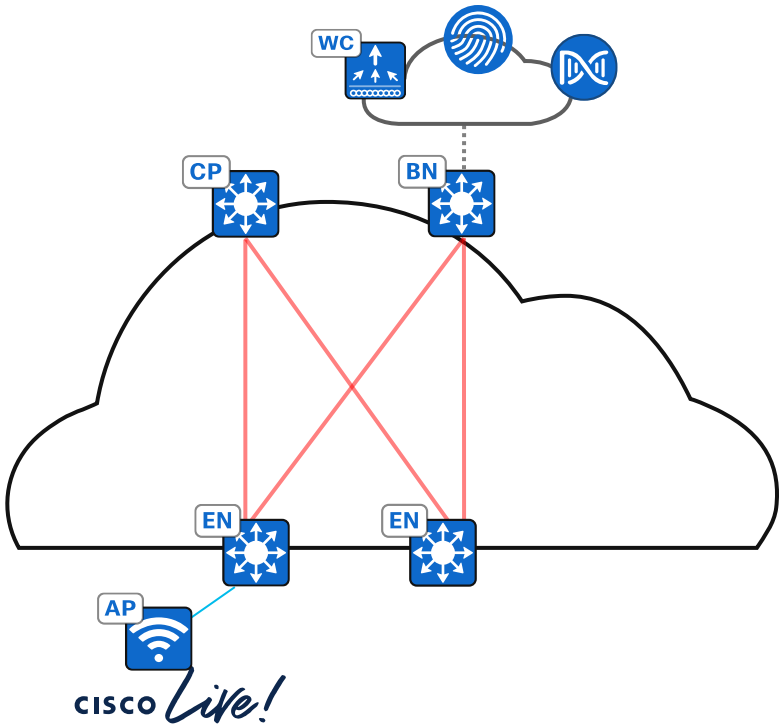
Connects external L3 and L2 networks to the Cisco SD-Access fabric.

Edge Nodes

Connects wired endpoints to the Cisco SD-Access fabric and optionally enforces micro-segmentation policy.

Cisco SD-Access Roles

Key Roles for a Complete Wired and Wireless Campus Experience



Control Plane Node
Map System that tracks endpoint to fabric node relationships.

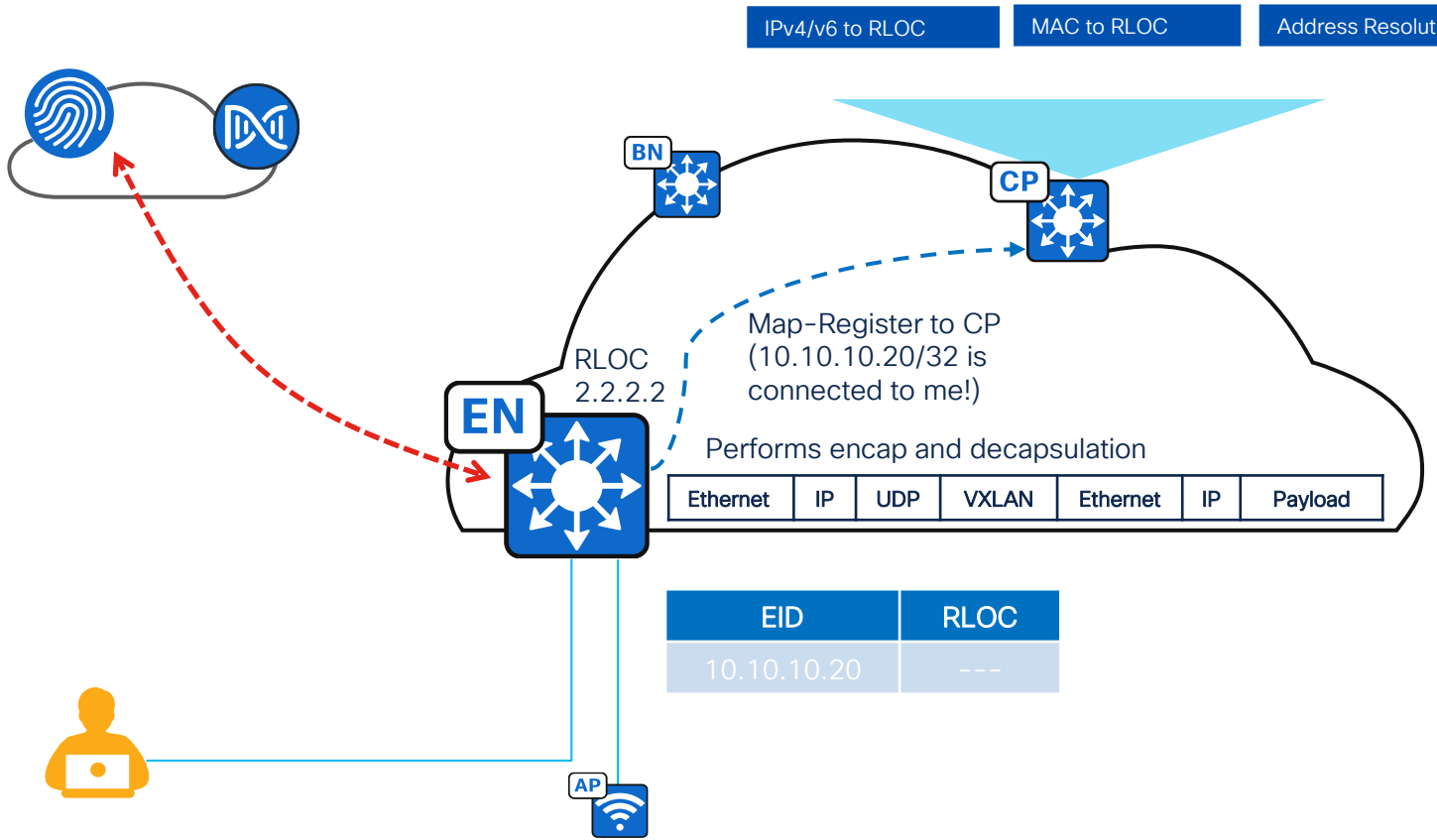
Border Nodes
Connects external L3 and L2 networks to the Cisco SD-Access fabric.

Edge Nodes
Connects wired endpoints and Fabric APs to the Cisco SD-Access fabric and optionally enforces micro-segmentation policy.

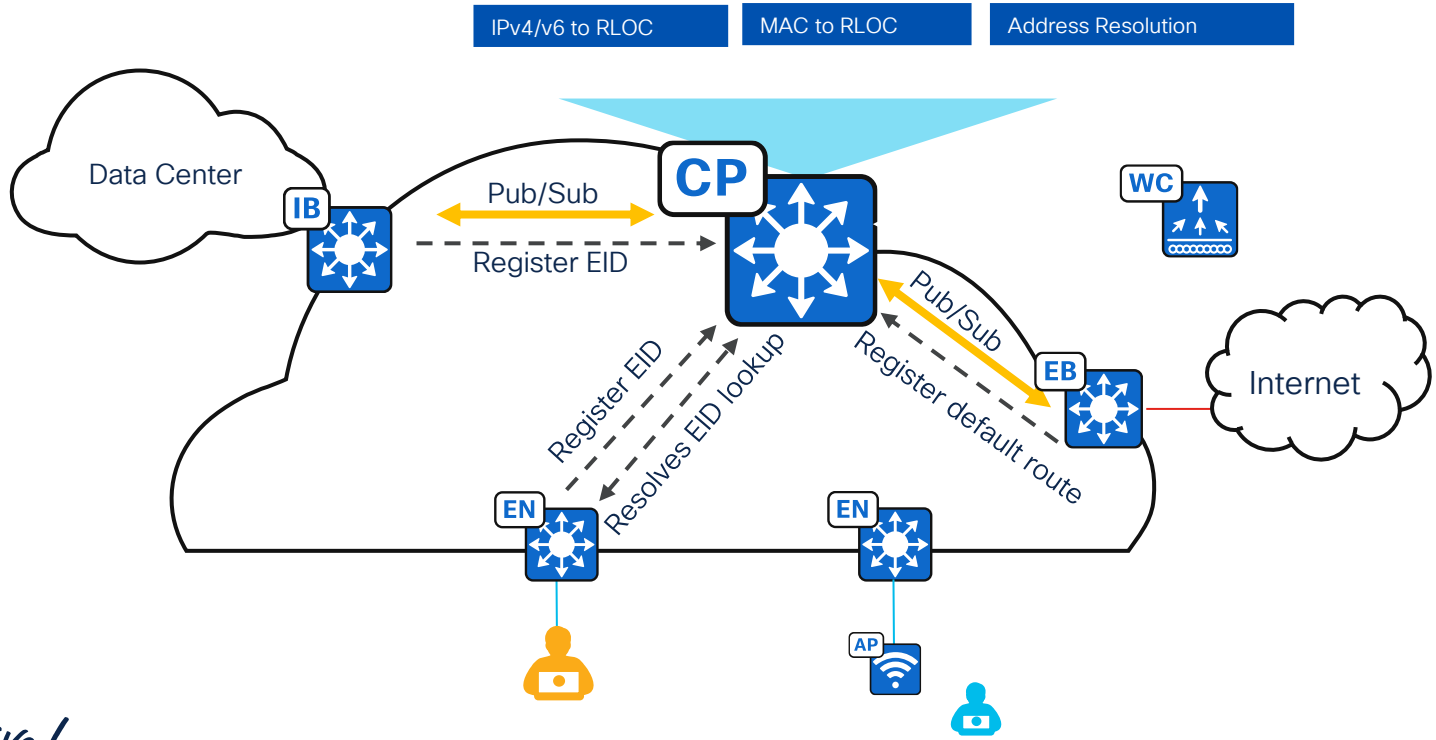
Fabric Wireless Controller
Fabric WLC is integrated into the SD-Access Control Plane (LISP) communication.

Fabric Access Point
Switches endpoint traffic to the adjacent Edge Node.

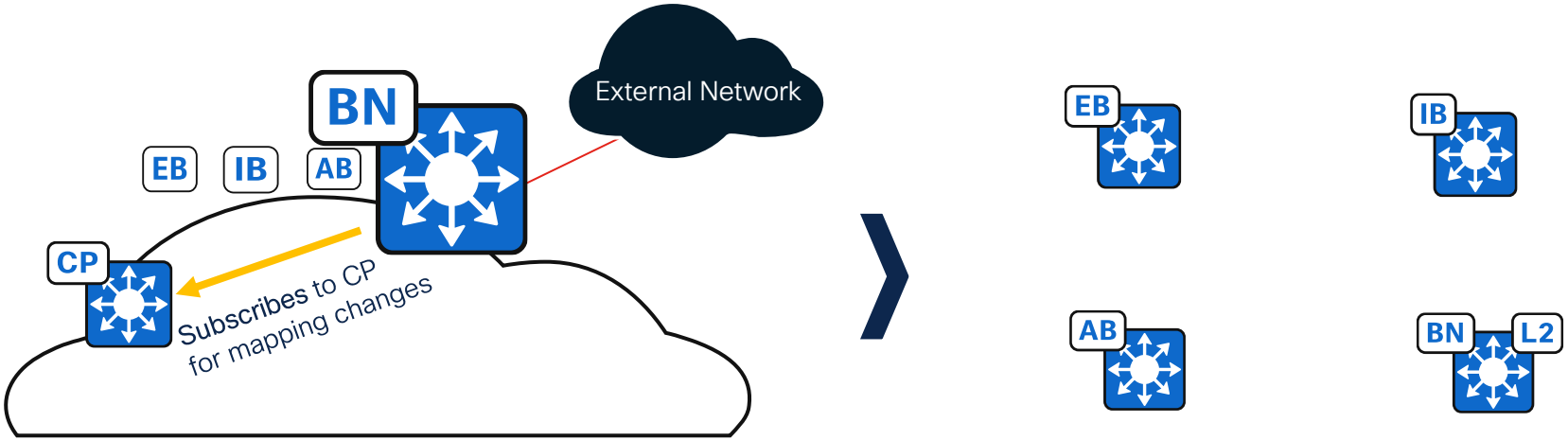
Edge Node



Control Plane Node



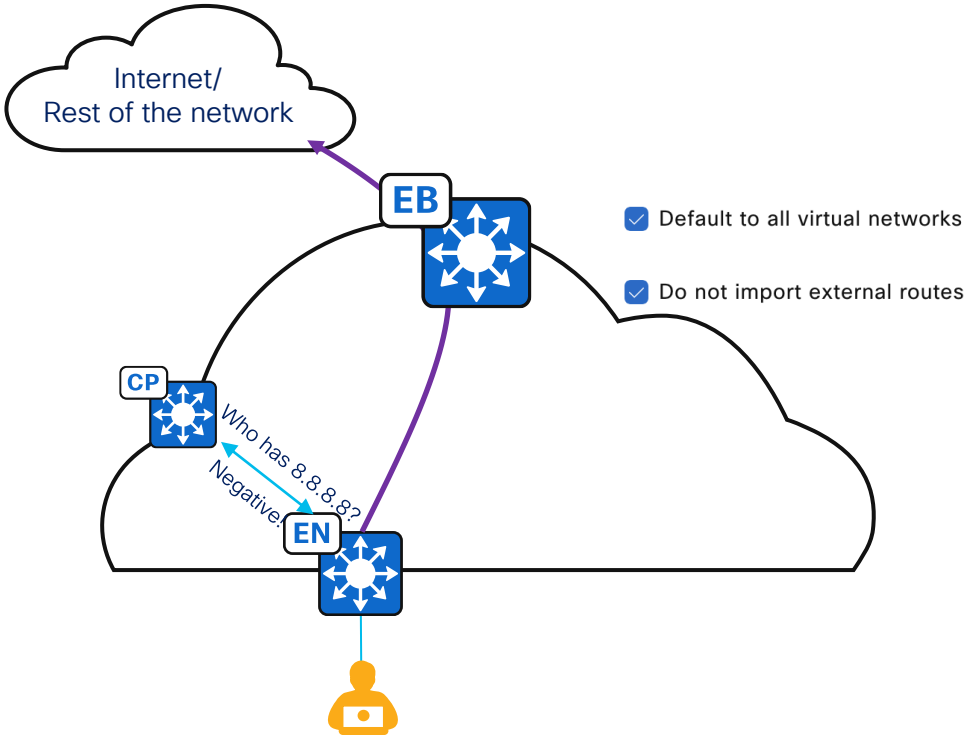
Border Node



Cisco SD-Access Fabric

• External Border Node

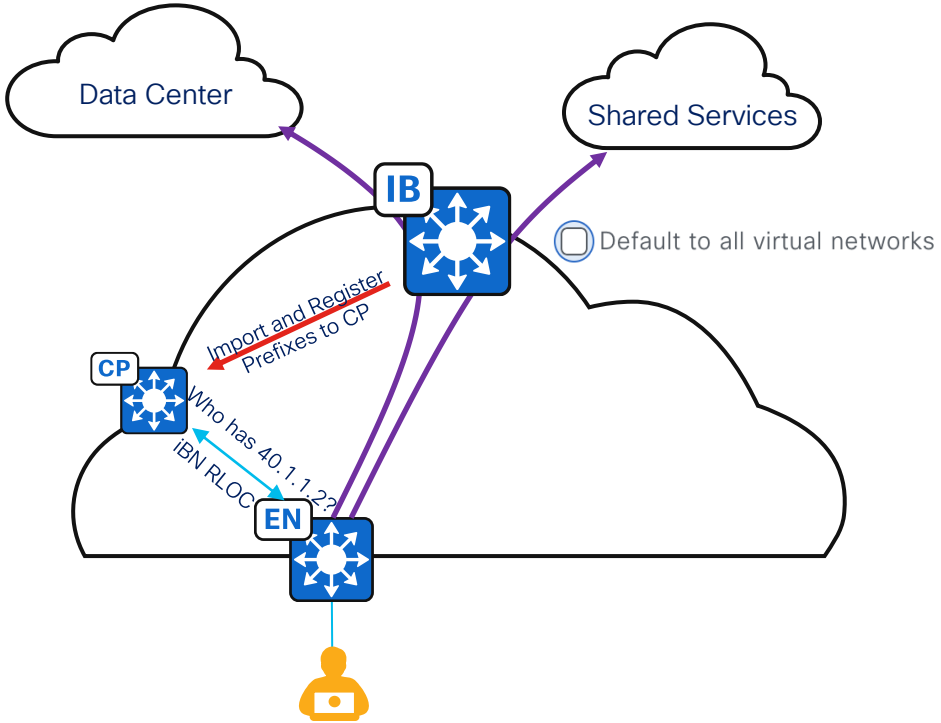
- The most common configuration.
- Needs a default route to register as an External Border with CP.
- Exports all fabric subnets to outside the Fabric Site as eBGP summary routes.
- Does not register IP prefixes from outside the Fabric Site into the fabric Control Plane.
- Acts as a gateway of last resort for the Fabric Site.
- Use this when all you get is a default route from upstream network



Cisco SD-Access Fabric

- Internal Border Node

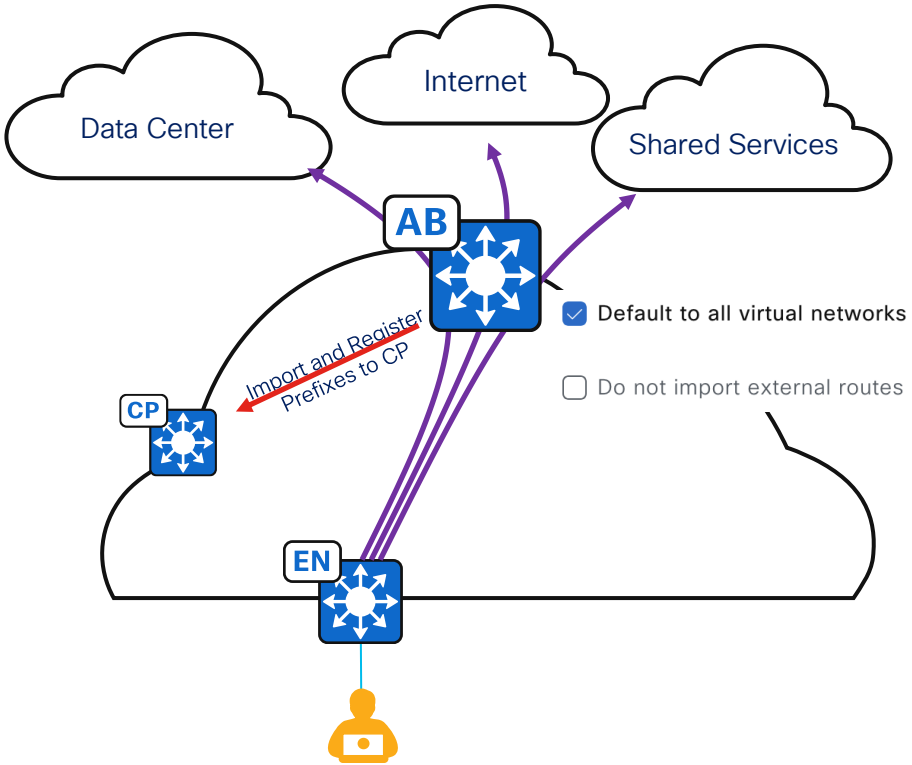
- Exports all fabric subnets to outside the Fabric Site as eBGP summary routes.
- Imports and registers eBGP-learned IPv4/IPv6 prefixes from outside the Fabric Site, into the fabric Control Plane.
- Does not act as a gateway of last resort for the Fabric Site.



Cisco SD-Access Fabric

- Internal + External Border Node

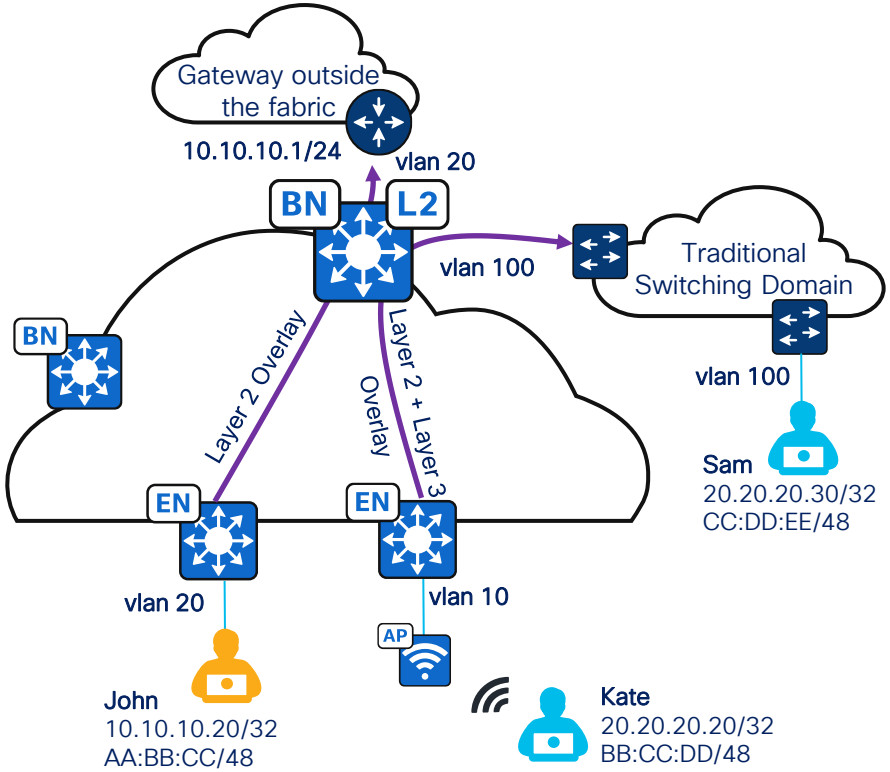
- Exports all fabric subnets to outside the Fabric Site as eBGP summary routes.
- Imports and registers eBGP-learned IPv4/IPv6 prefixes from outside the Fabric Site, into the fabric Control Plane.
- Acts as a gateway of last resort for the Fabric Site.
- Use when you have default route as well as specific routes that are advertised from upstream network/s with a single point of exit outside fabric.



Cisco SD-Access Fabric

- Layer 2 Border Node

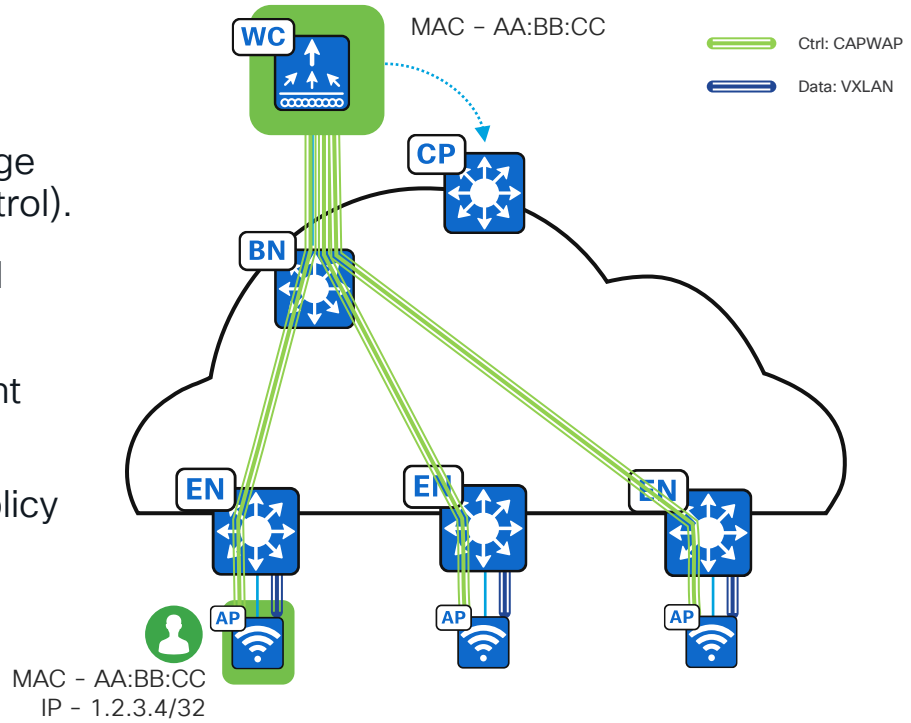
- Acts as Layer 2 handoff for pure Layer 2 Overlays or Layer 2 + Layer 3 Overlays.
- Allows VLAN translation between SD-Access network segments and non-fabric VLAN IDs.
- Dual homing requires link aggregation; or use Flex Link+ on downstream Layer-2 switches.
- Ideally should be separate device from the Layer 3 Border Node.



Cisco SD-Access Fabric

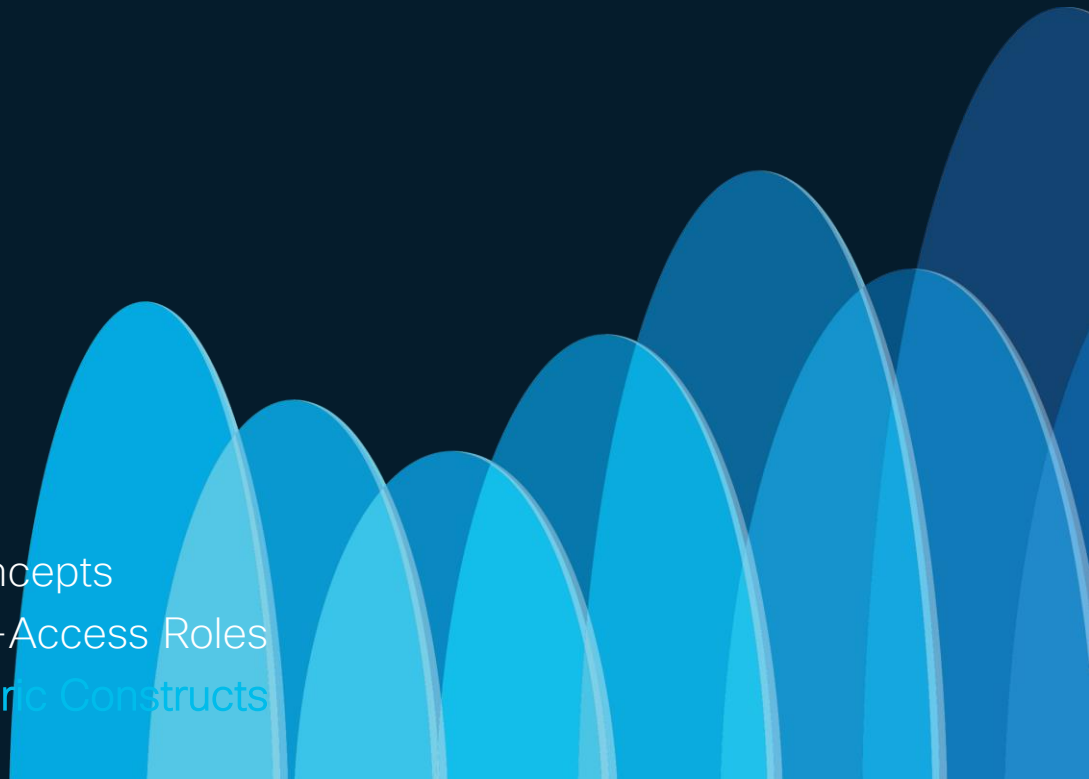
- Fabric Enabled Wireless Unifies Wired and Wireless Management, Policy and Data Planes

- 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.

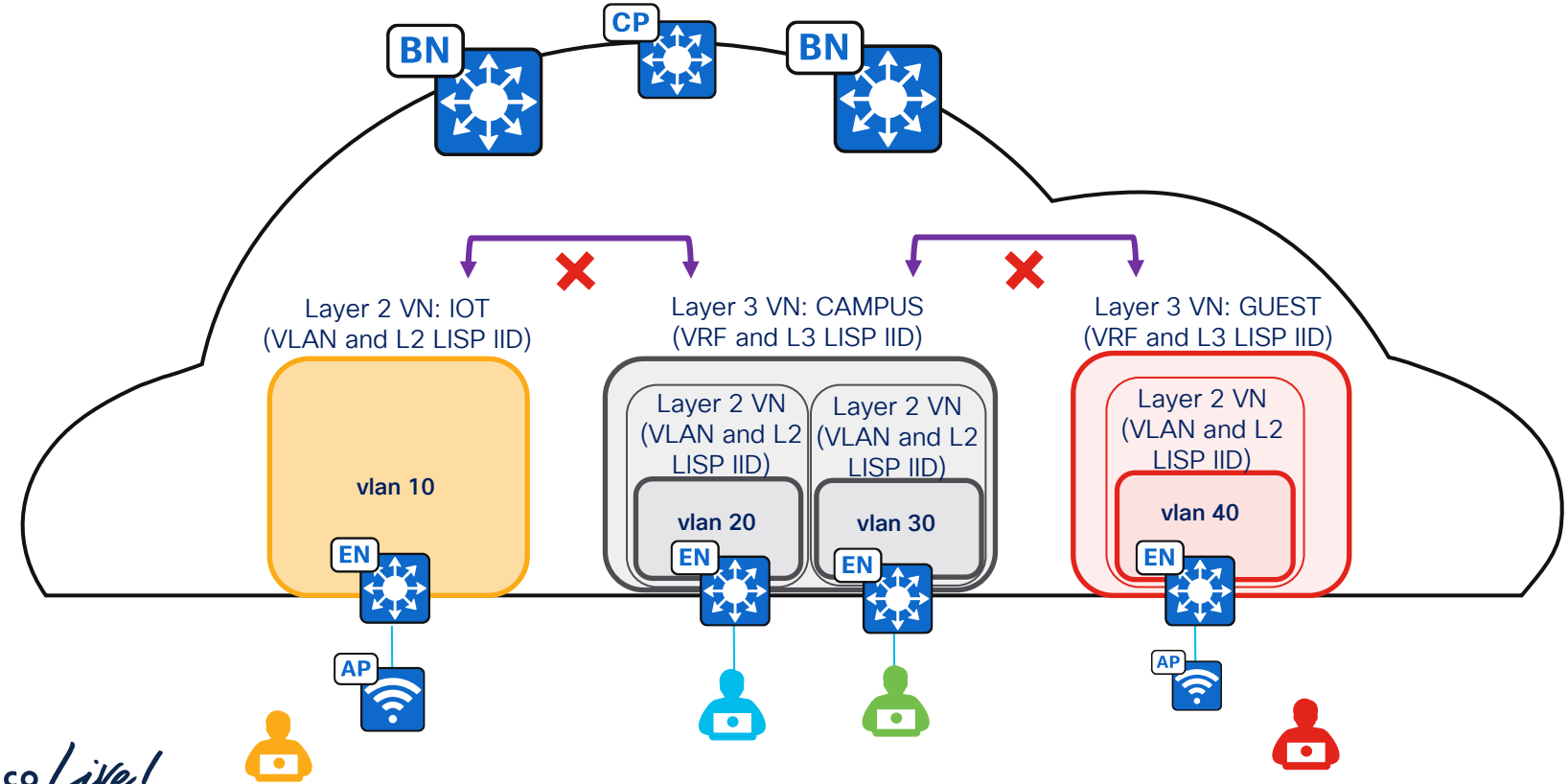


Roles and Terminology

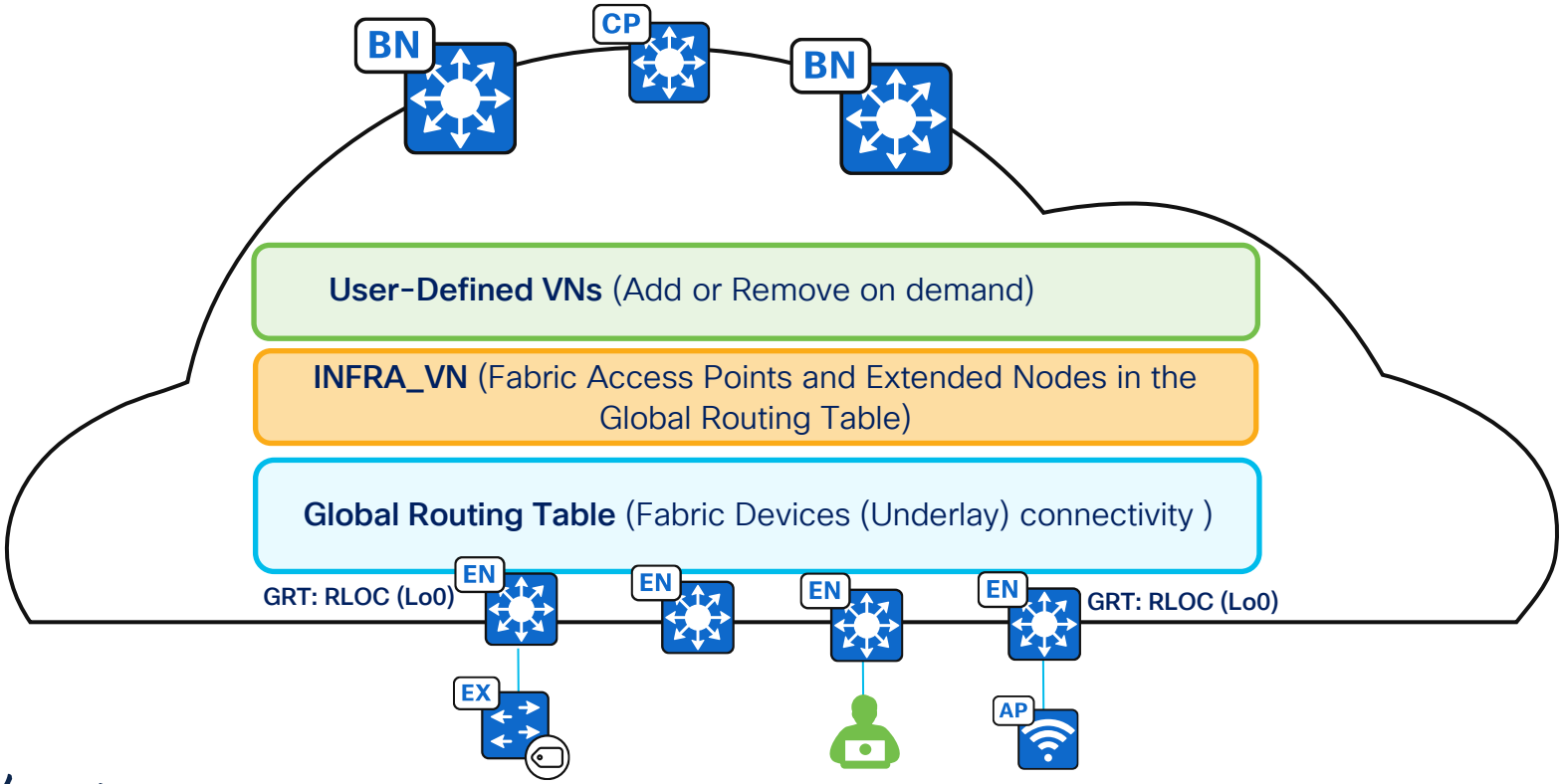
1. Concepts
2. SD-Access Roles
3. Fabric Constructs



Virtual Networks



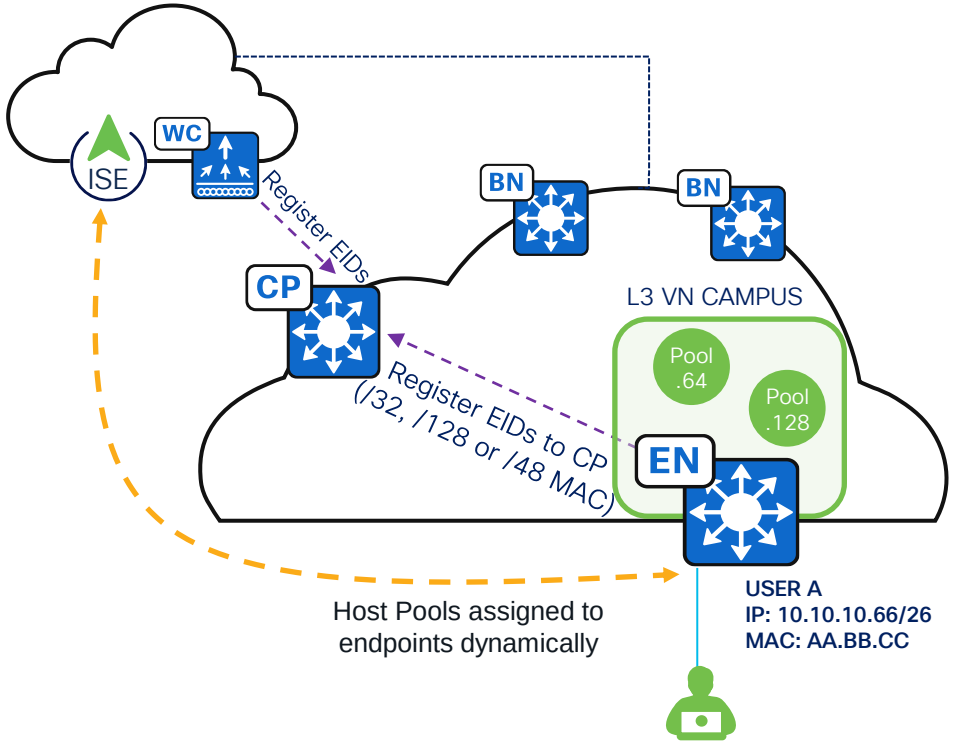
Layer 3 Virtual Networks



Cisco SD-Access Fabric

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

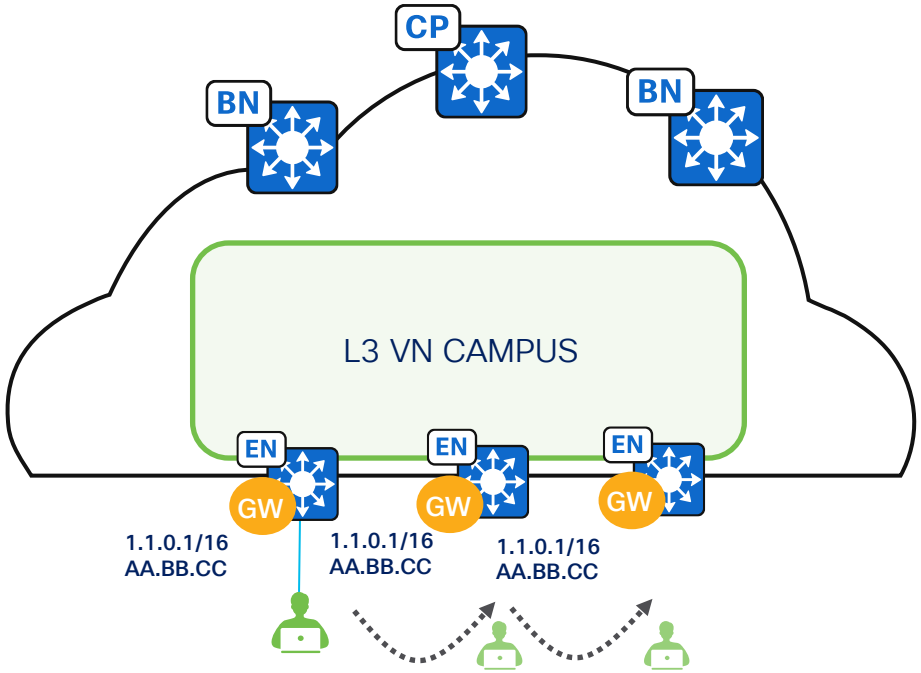
- Edge Nodes instantiate an access VLAN and a Switched Virtual Interface (SVI)
  with user-defined IPv4/IPv6 addresses per Host Pool.
- Host Pools assigned to endpoints dynamically by AAA or statically per port.
- Edge Nodes and Fabric WLCs register endpoint IDs (/32, /128 or MAC) with the Control Plane,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



Cisco SD-Access Fabric

- Anycast Gateway Provides a Default Gateway for IP-Capable Endpoints

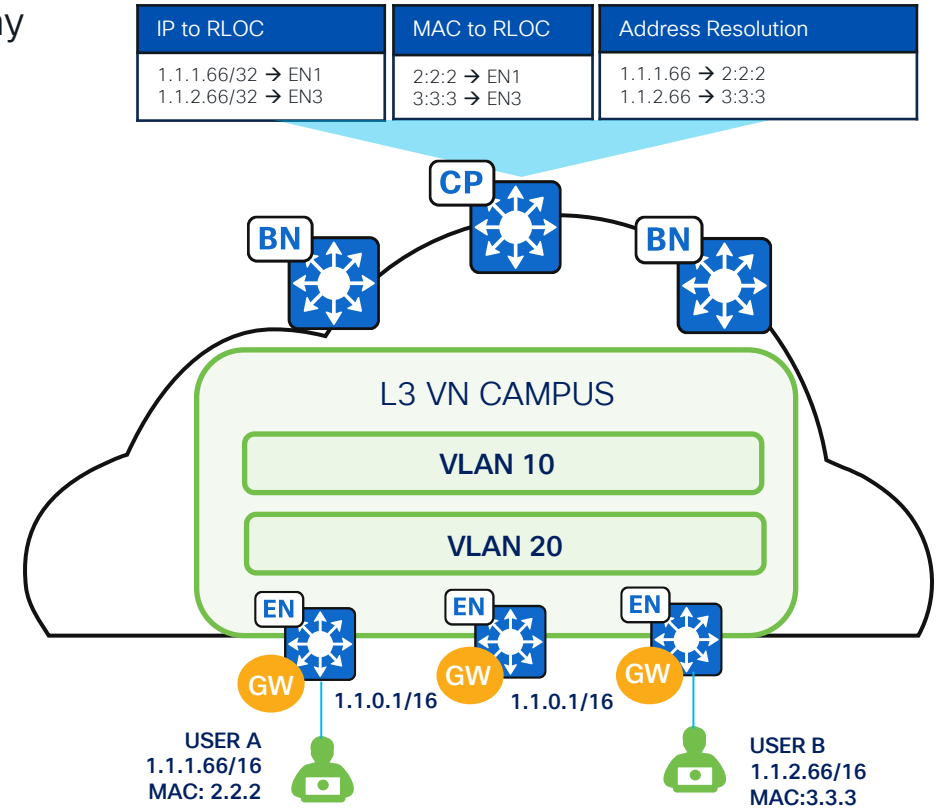
- Similar principle and behavior to FHRP with a shared virtual IPv4/IPv6 addresses and MAC address.
- The same Switch Virtual Interface (SVI) is present on all Edge Nodes with the same virtual IP and MAC.
- The wired or wireless endpoint can connect to any switch or AP in the fabric and communicate with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



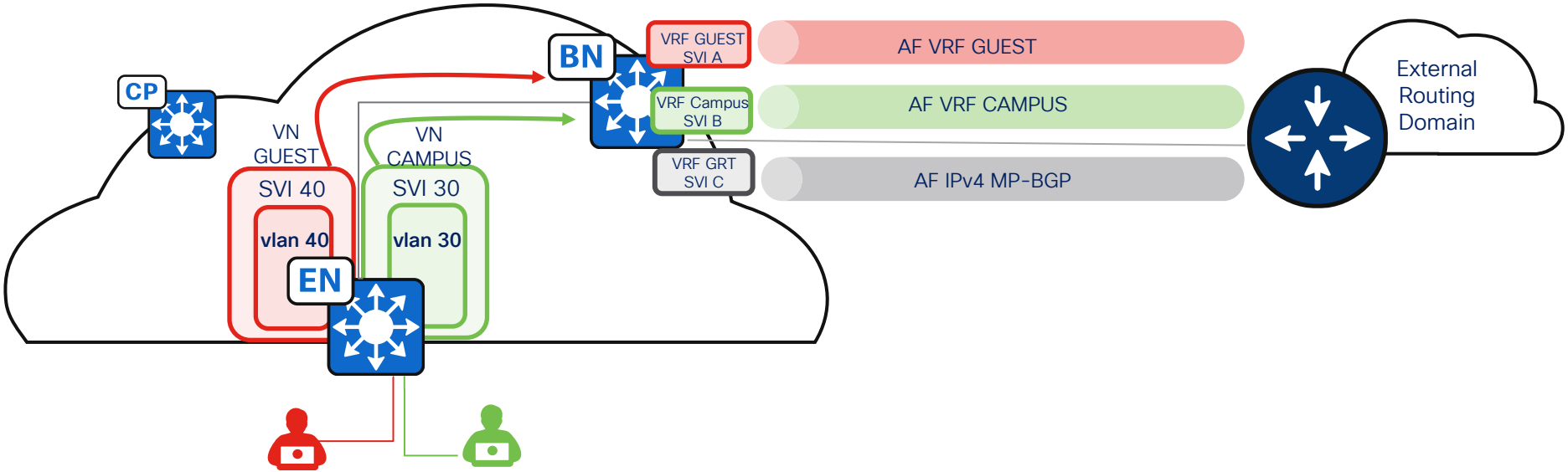
Cisco SD-Access Fabric

- Host Pools are “stretched” via the Overlay

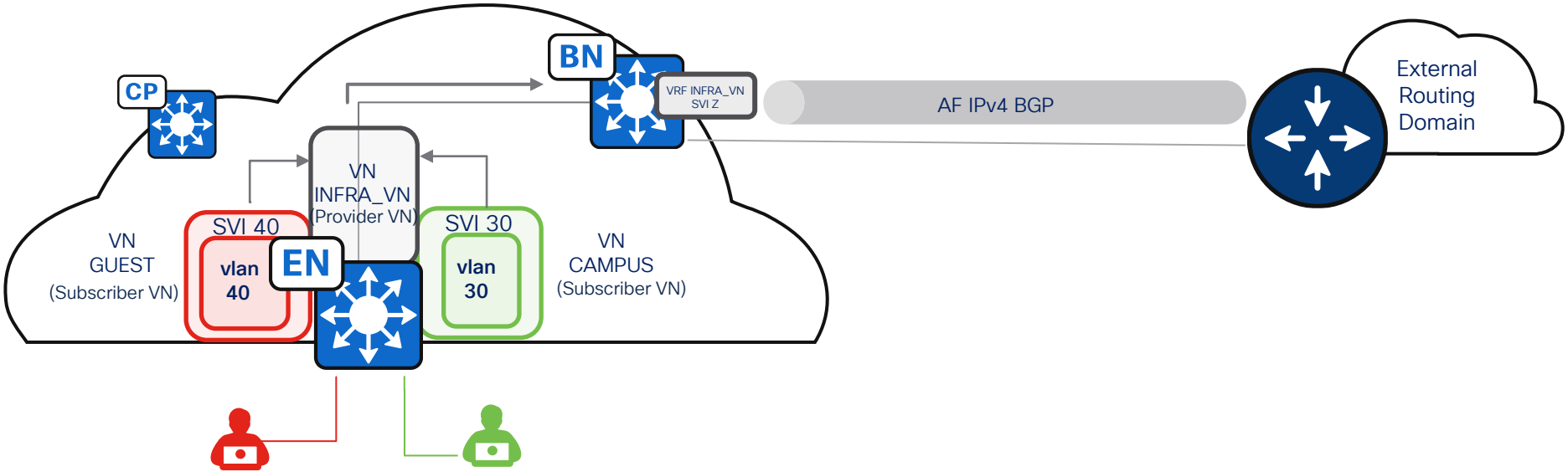
- Endpoint IPv4/IPv6 traffic arrives on an Edge Node and is then routed or switched by the Edge Node.
- Fabric Dynamic EID mapping allows endpoint-specific (/32, /128, MAC) advertisement and mobility.
- No longer need VLANs to interconnect endpoints across Edge Nodes, this happens in the Overlay without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



Layer 3 Handoff



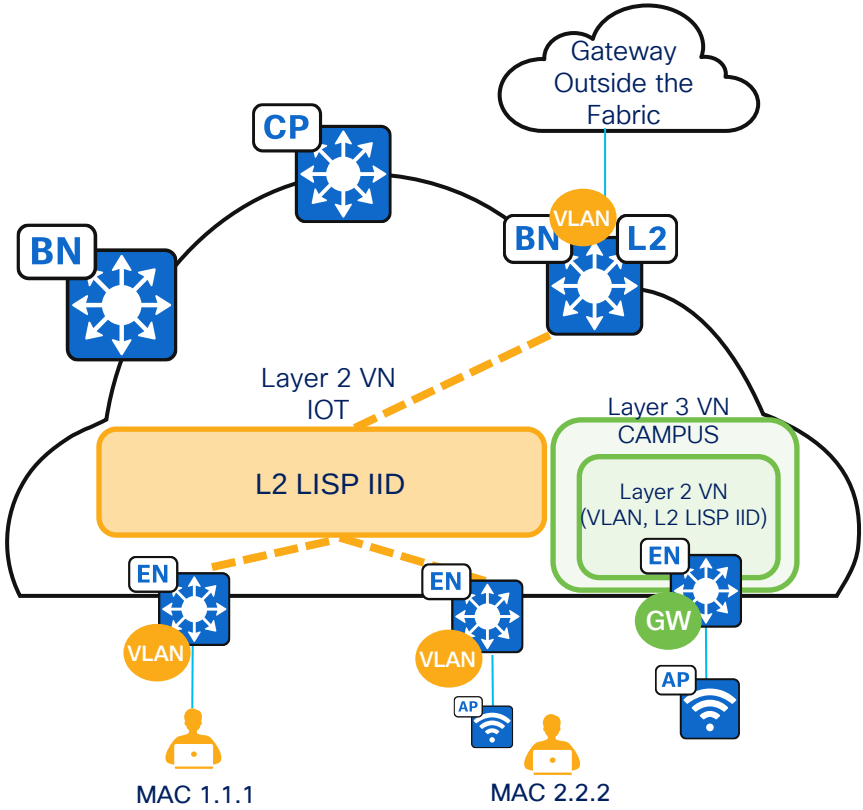
Extranet Layer 3 Handoff



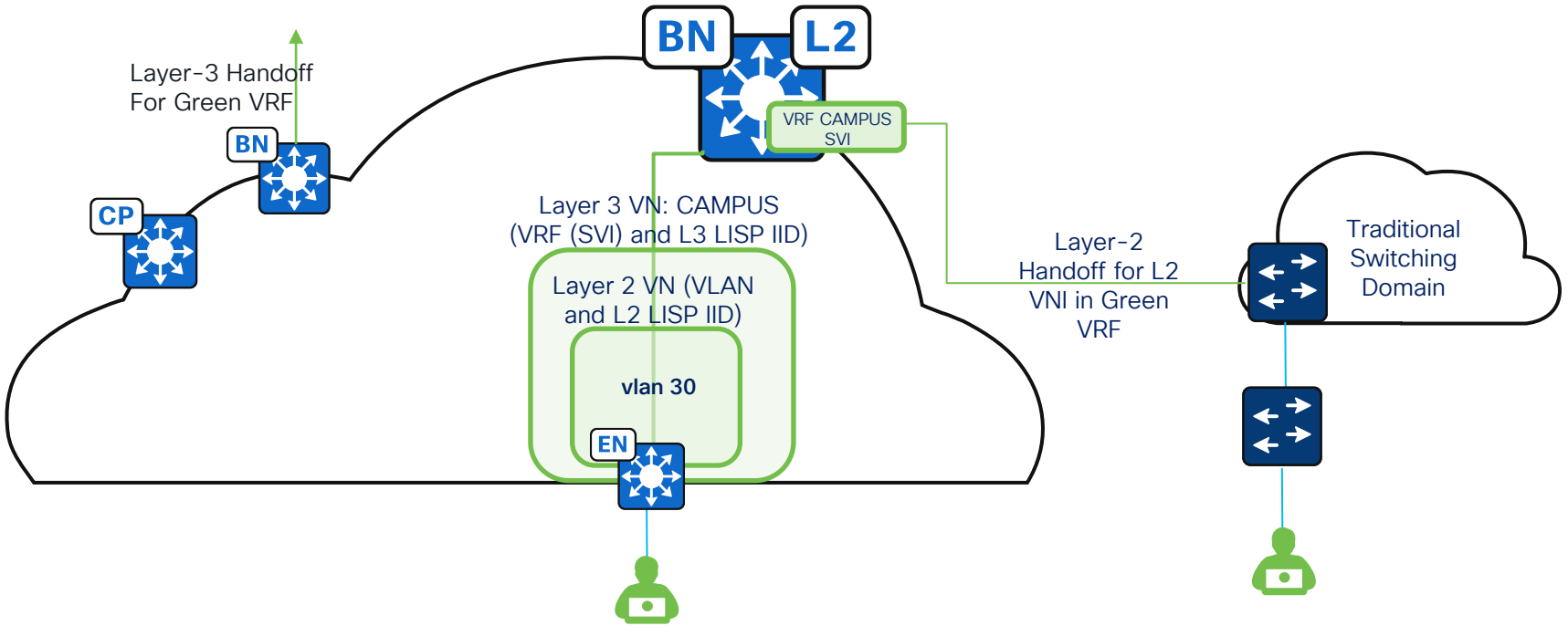
Cisco SD-Access Fabric

Layer 2 Virtual Networks

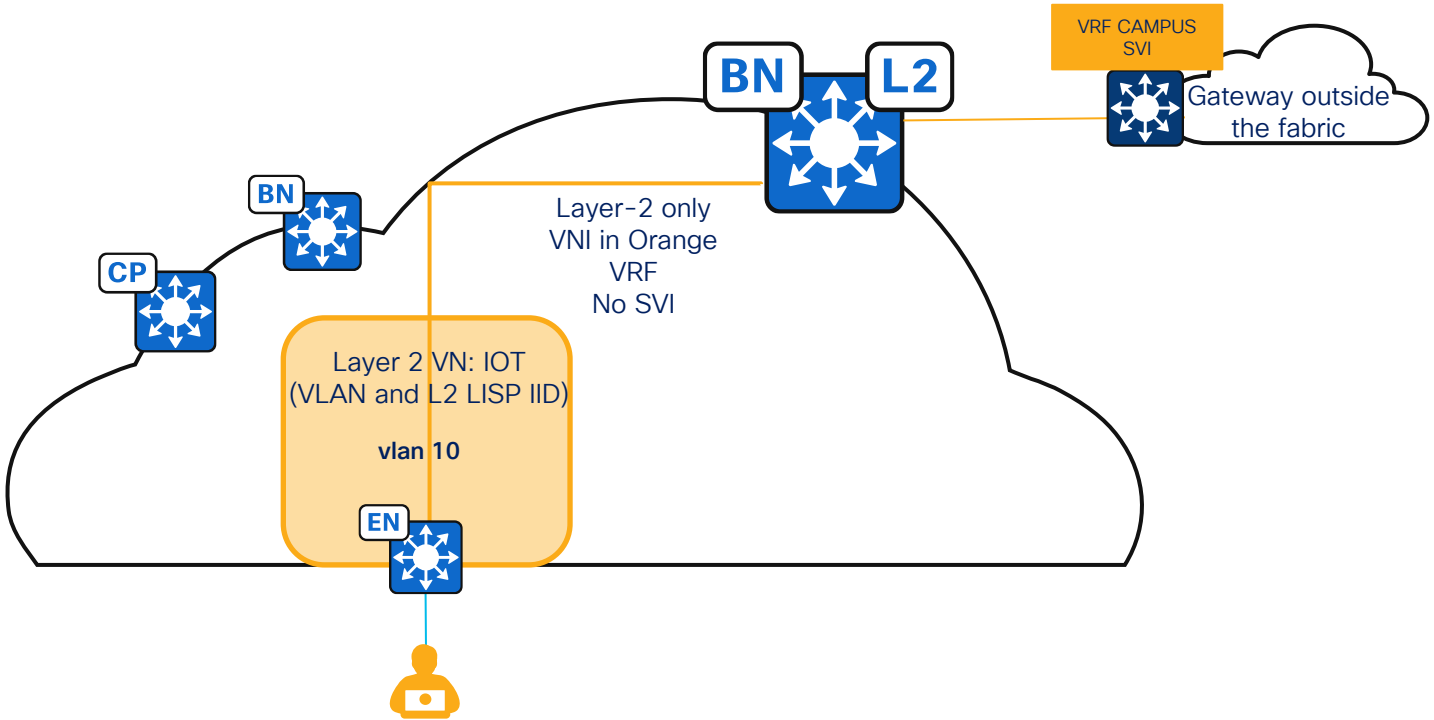
- By default, an L2VN is deployed with each Anycast Gateway and Layer 2 Flooding is disabled. Layer 2 Flooding can be enabled, if necessary, to service niche applications.
- L2VN can be deployed without an Anycast Gateway, and Layer 2 Flooding cannot be disabled.
  - Sometimes referred to as “Gateway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



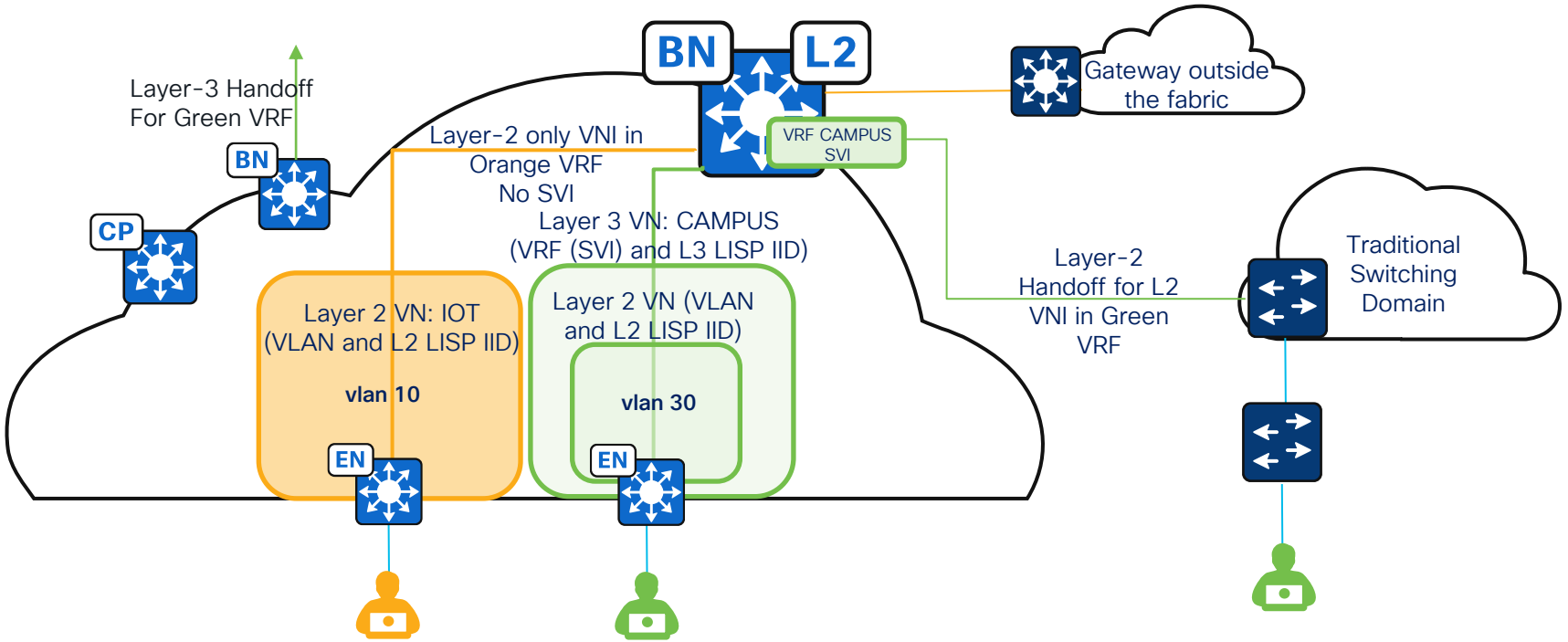
Layer 2 Handoff



Gateway Outside The Fabric (GwOTF)



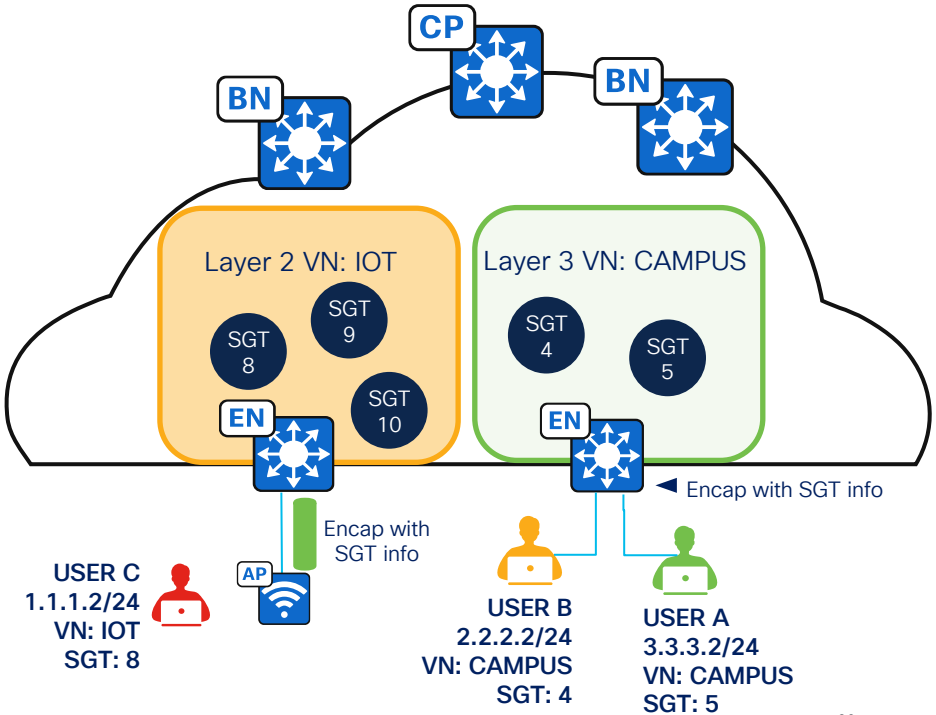
Mutually Exclusive – But Co-existence for different VRFs



Cisco SD-Access Fabric

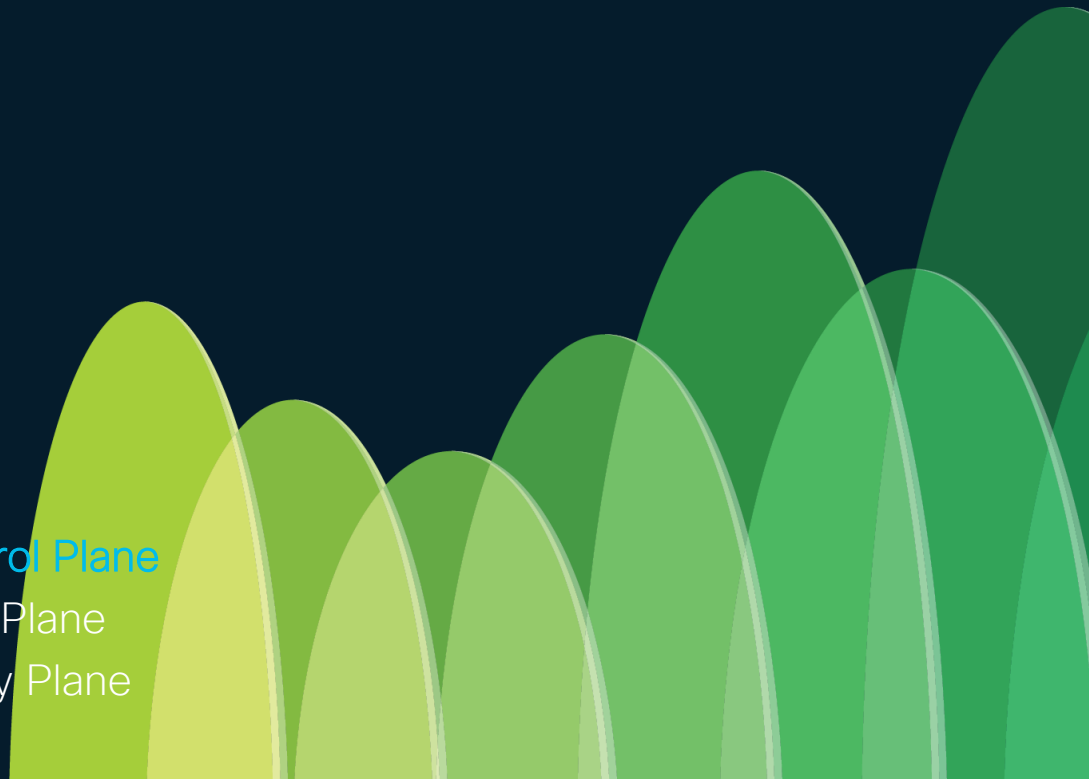
- A Security Group Tag Assigns a “Group” to Each Endpoint

- 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.



Fabric Fundamentals

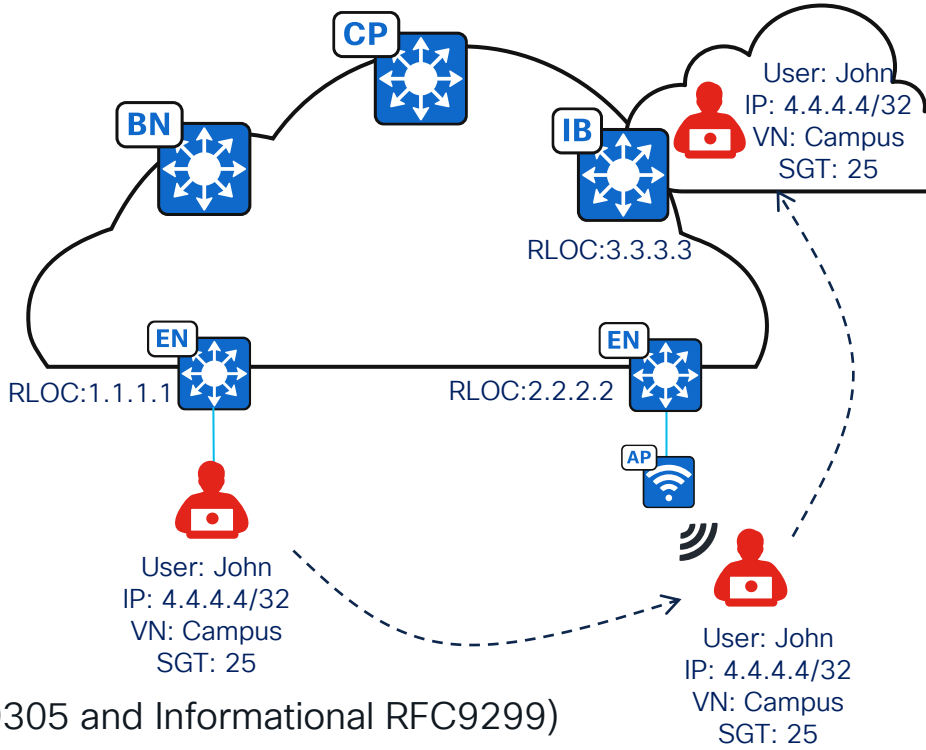
1. Control Plane
2. Data Plane
3. Policy Plane



Cisco SD-Access Fabric

- Control Plane: Locator/ID Separation Protocol (LISP)

Where you are in a network can change, but ***who*** you are in the network remains the same.



(IETF Standards Track RFC9300-RFC9305 and Informational RFC9299)

Cisco SD-Access Fabric

- Control Plane: Locator/ID Separation Protocol (LISP)

LISP Pub/Sub

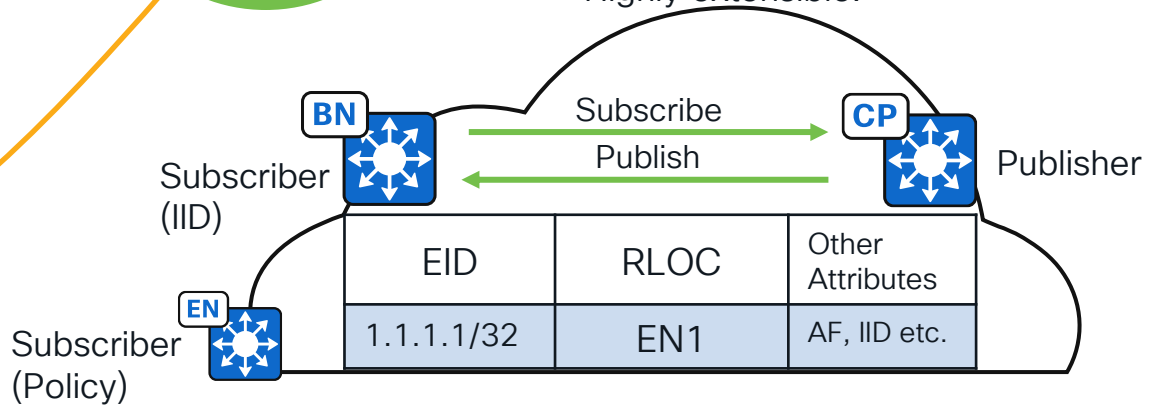
Released with Catalyst Center 2.2.3.x.
Reliable and stable.
Native LISP transport.
Less Control Plane load.
Faster convergence.
Highly extensible.

2022

LISP/BGP

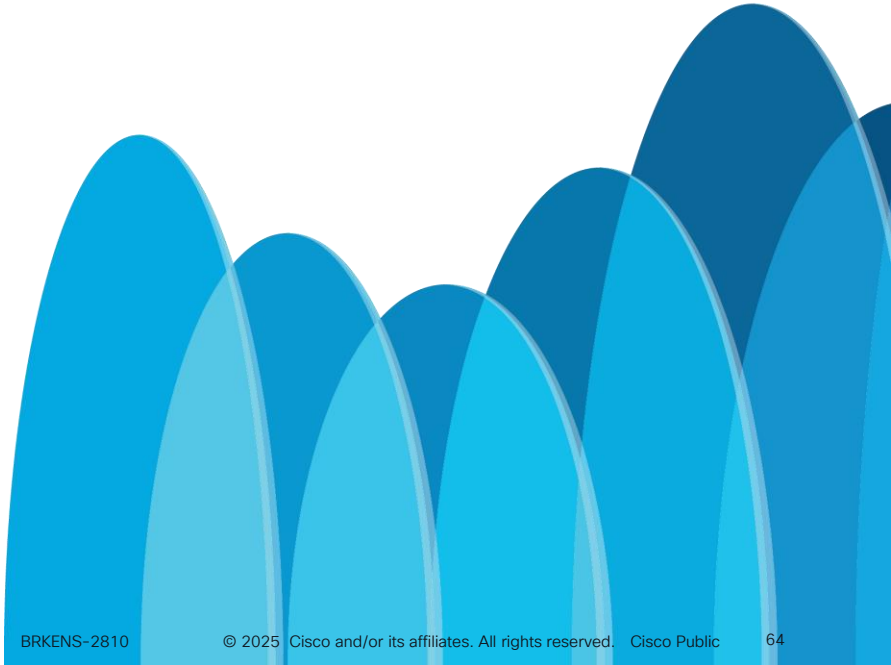
Reliable and stable.
BGP transport.

2017



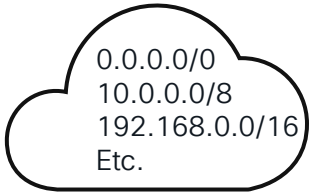
Fabric Operation

LISP Pub/Sub Walkthrough

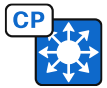


Fabric Operation

Default ETR Registration



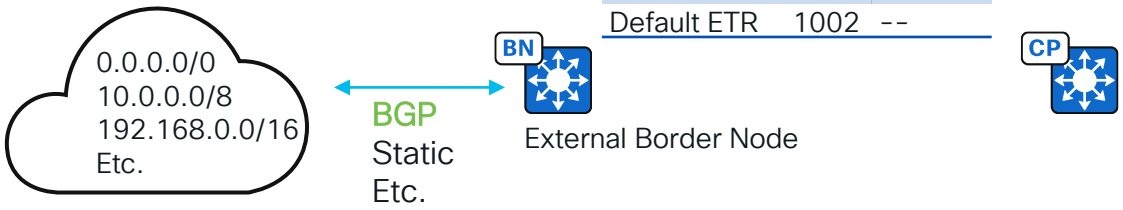
External Border Node



Fabric Operation

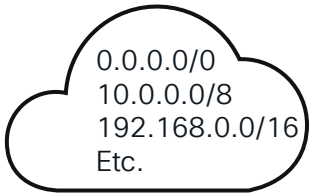
Default ETR Registration

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

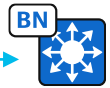


Fabric Operation

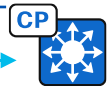
Default ETR Registration



BGP
Static
Etc.



Register Default ETR per L3VN (Gateway of last resort)



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

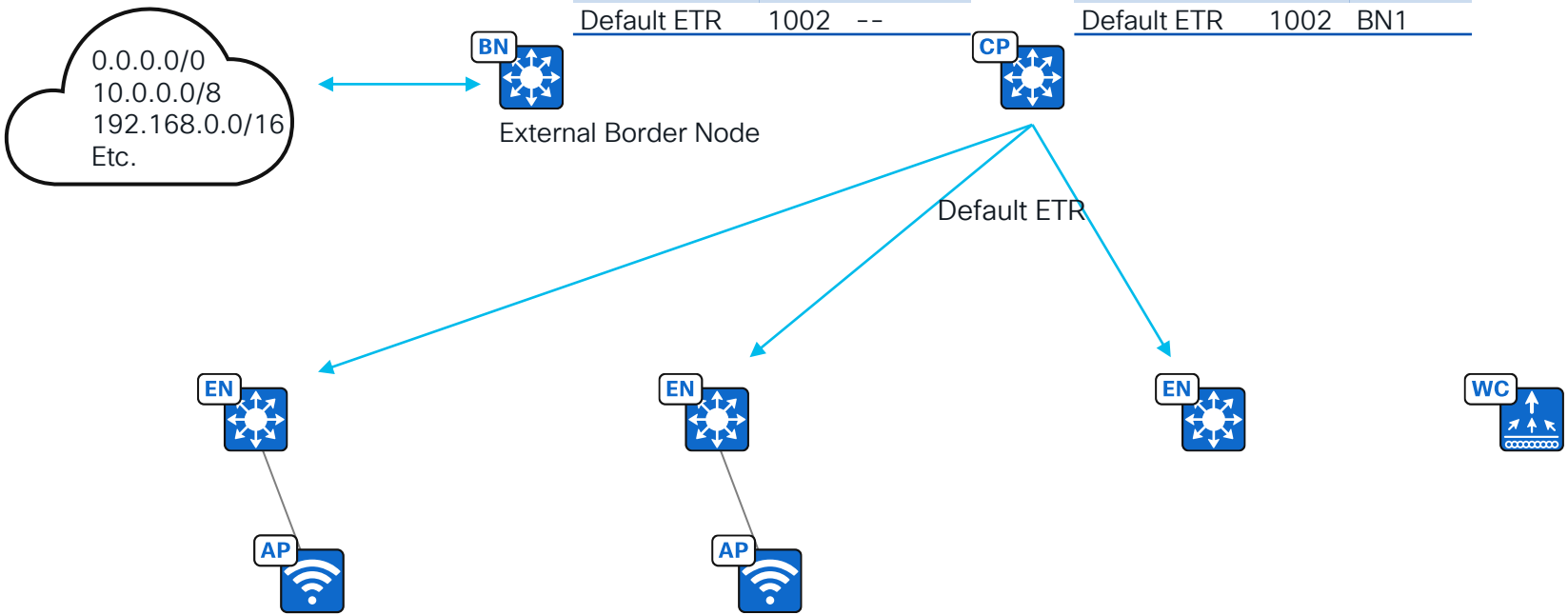
Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1

Fabric Operation

Edge Node Bootstrap

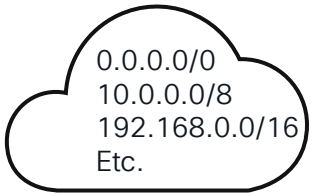
Destination	IID	Next Hop
Default ETR	1001	--
Default ETR	1002	--

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



Fabric Operation

Edge Node Bootstrap



External Border Node

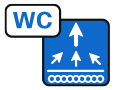
Destination	IID	Next Hop
Default ETR	1001	--
Default ETR	1002	--

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

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

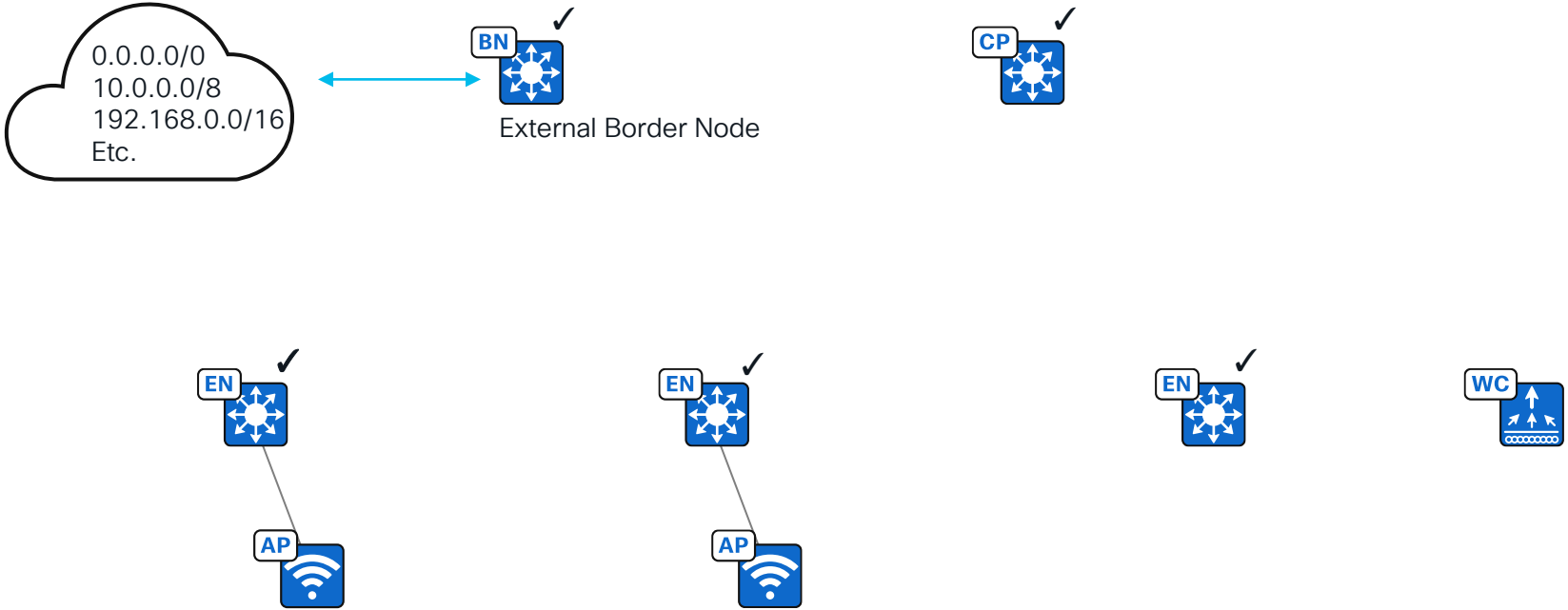
Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1

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



Fabric Operation

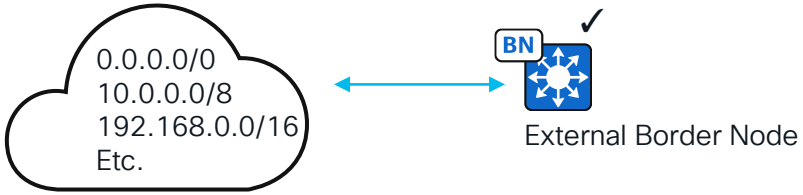
Edge Node Bootstrap



✓ Default ETR

Fabric Operation

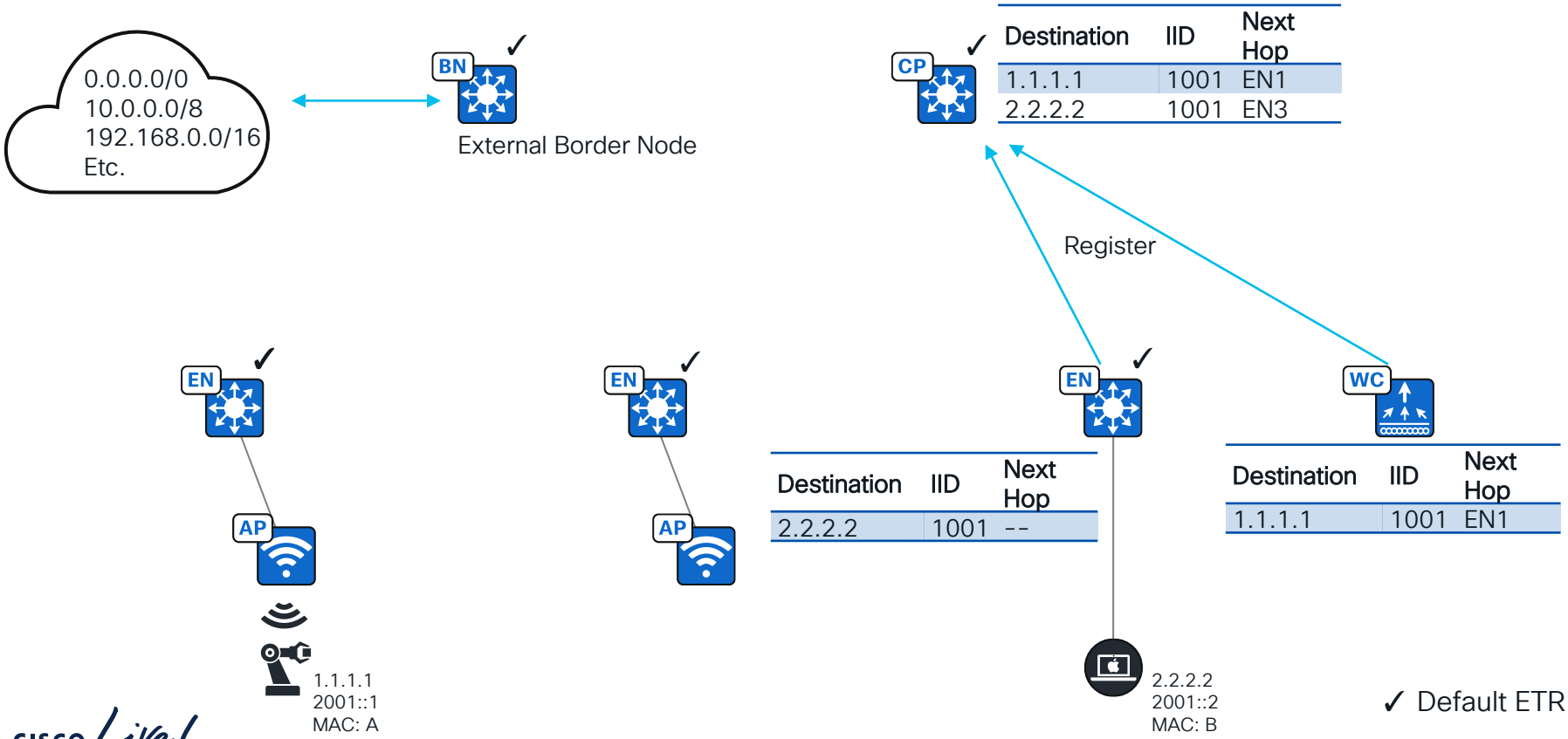
Endpoint Registration



✓ Default ETR

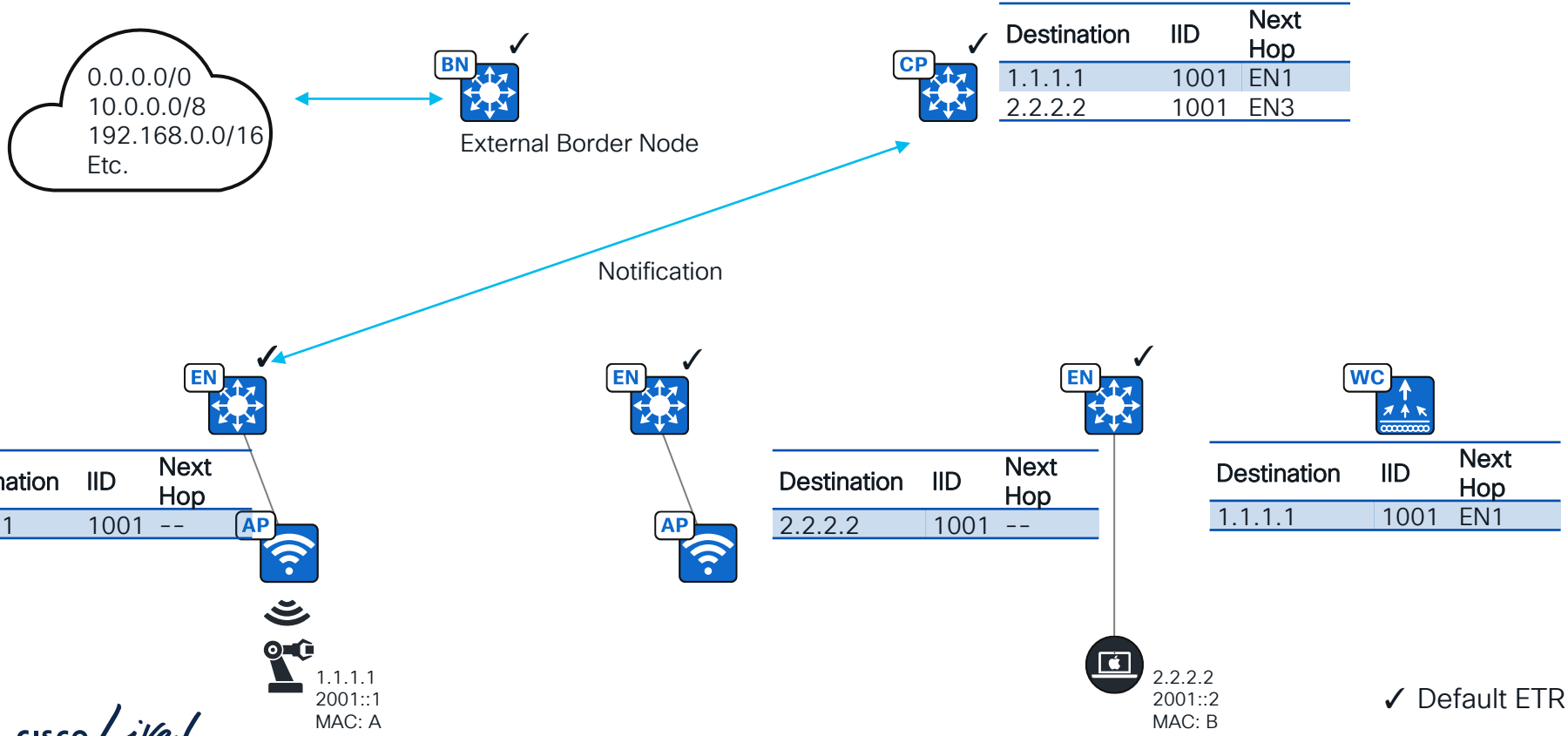
Fabric Operation

Endpoint Registration



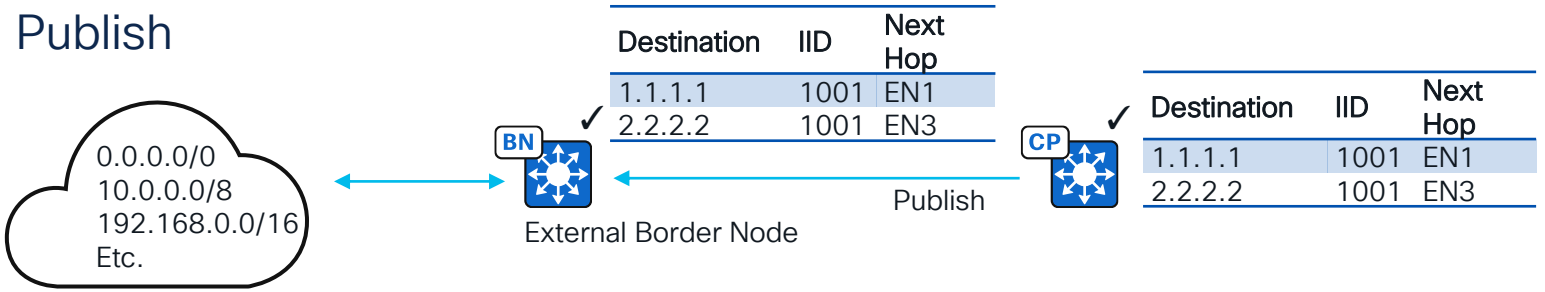
Fabric Operation

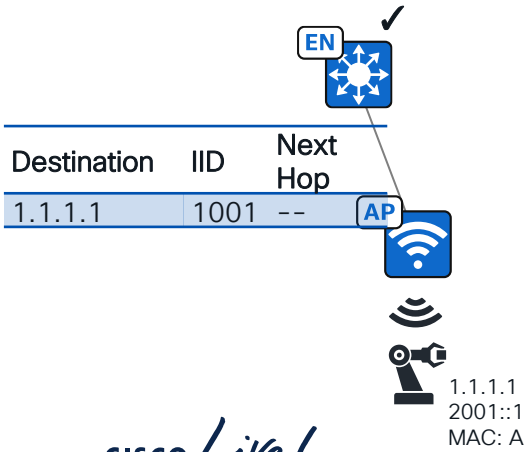
Endpoint Registration

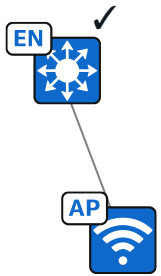


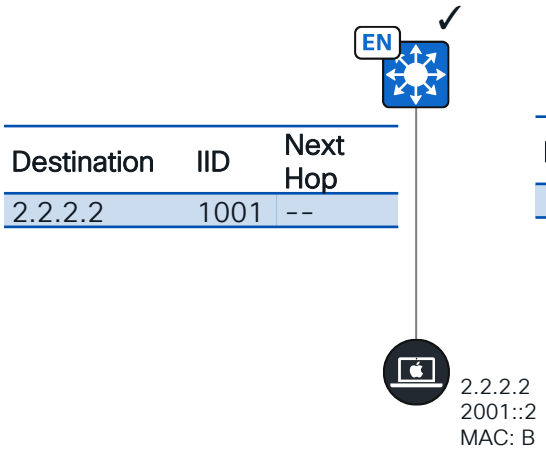
Fabric Operation

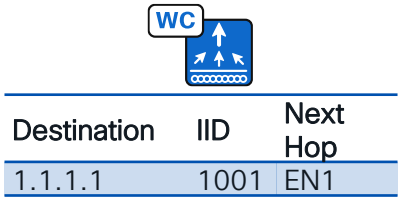
Publish







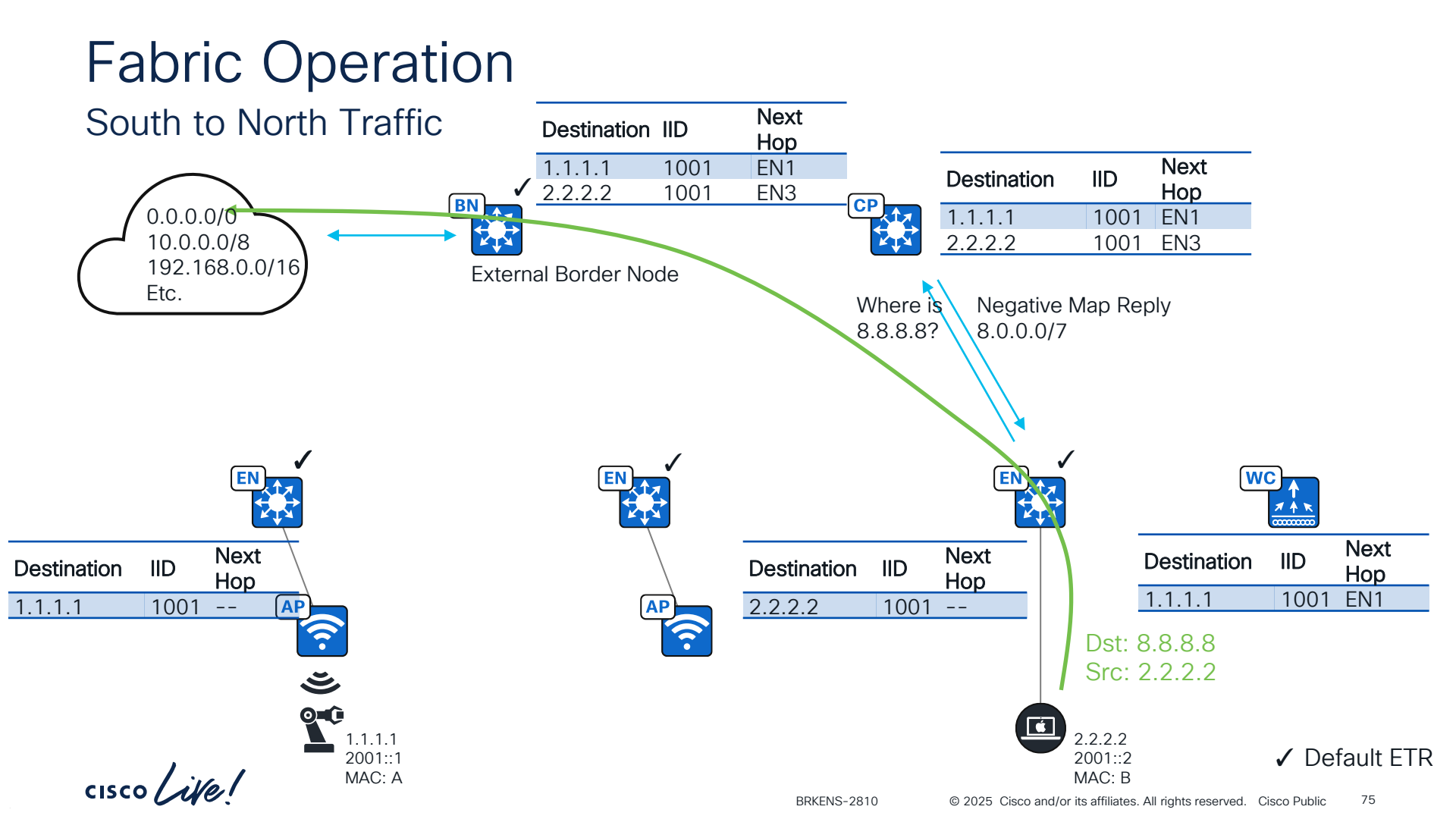




✓ Default ETR

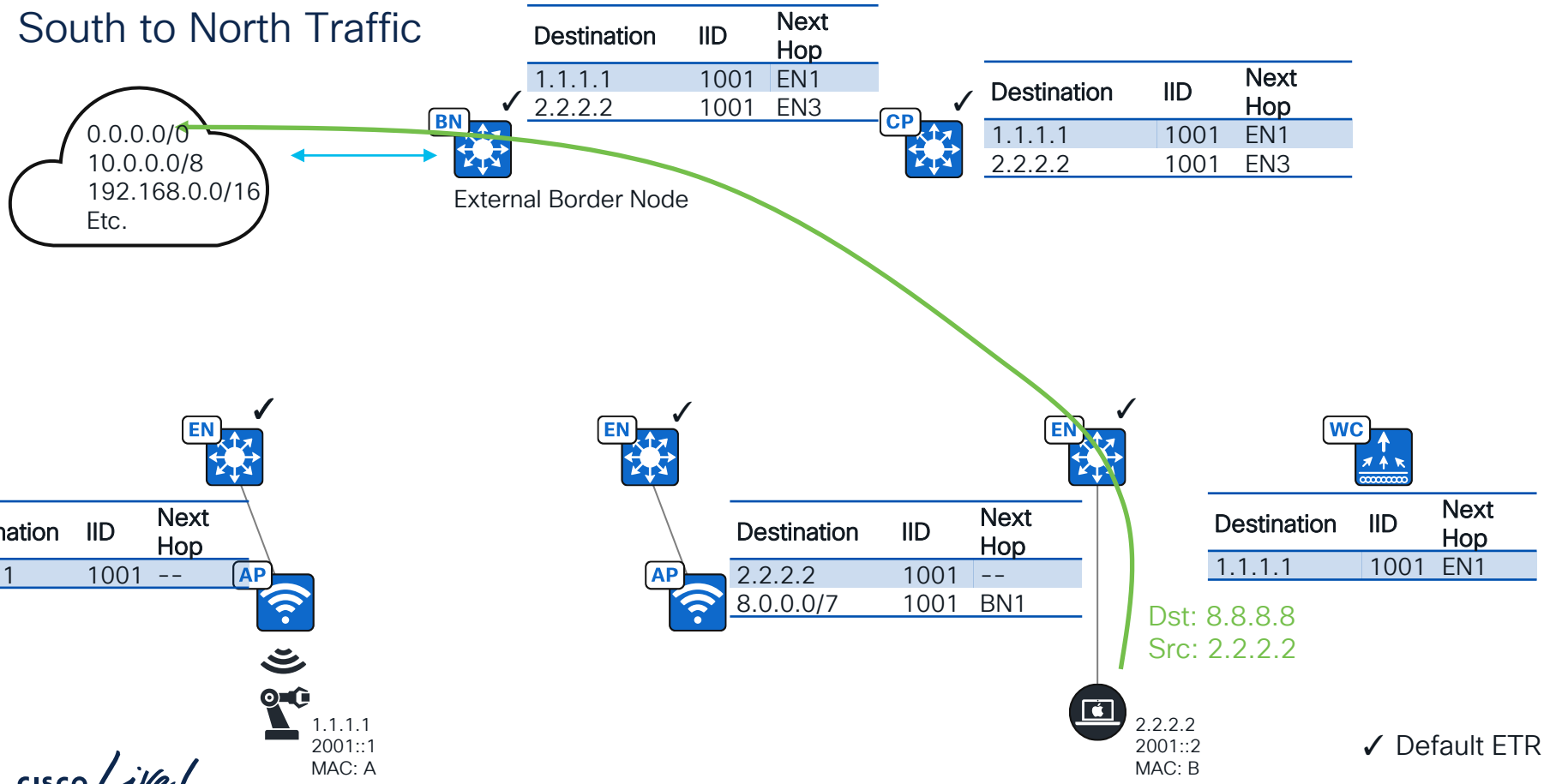
Fabric Operation

South to North Traffic



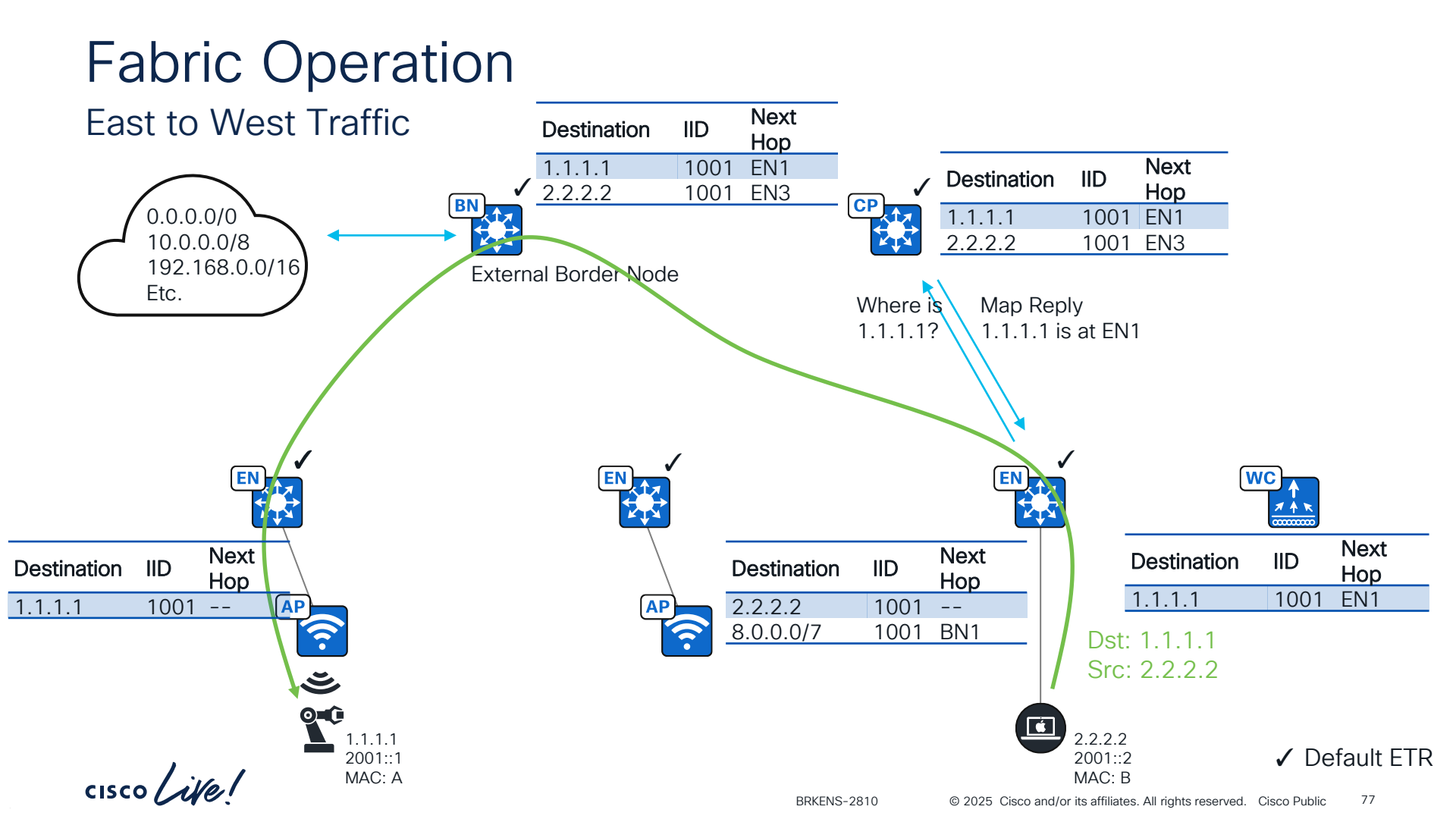
Fabric Operation

South to North Traffic



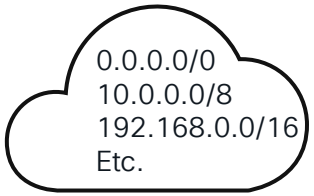
Fabric Operation

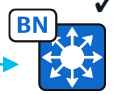
East to West Traffic



Fabric Operation

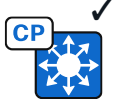
East to West Traffic





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

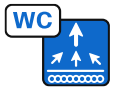
Destination	IID	Next Hop
1.1.1.1	1001	--

1.1.1.1
2001::1
MAC: A

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

2.2.2.2
2001::2
MAC: B

Dst: 1.1.1.1
Src: 2.2.2.2



Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

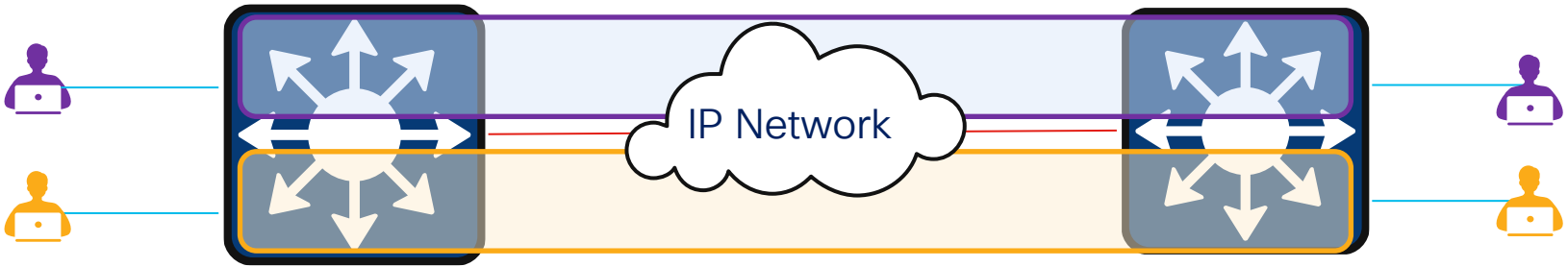
Fabric Fundamentals

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

Cisco SD-Access Fabric

Data Plane: Virtual Extensible Local Area Network (VXLAN)

VXLAN extends Layer 2 and Layer 3 overlay networks over a Layer 3 underlay network

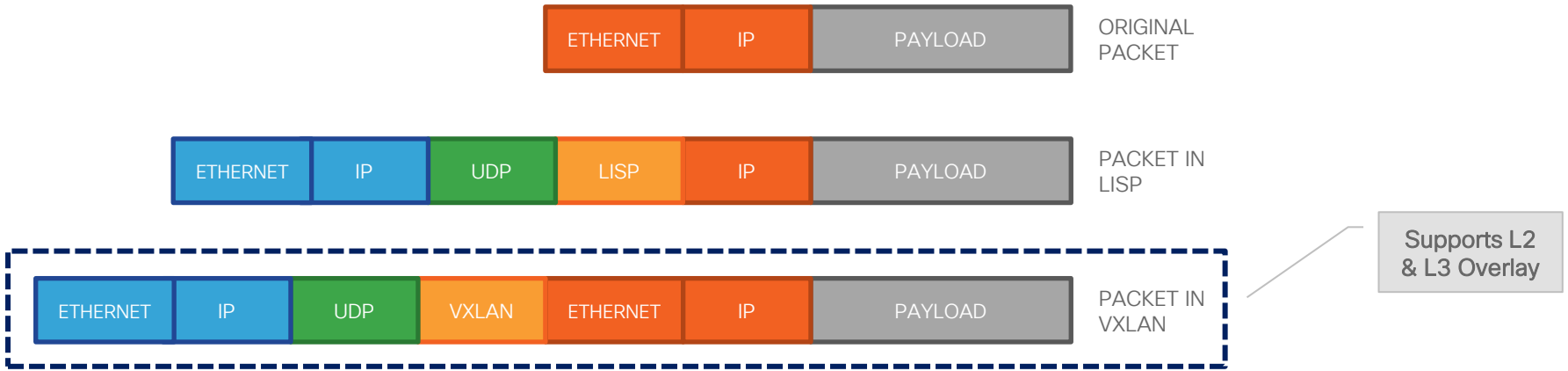


- ✓ Scalability: 16 million unique identifiers.
- ✓ Runs on top of L3, avoids need for STP.
- ✓ L2 traffic tunnelled over an L3 infrastructure.
- ✓ Handles broadcast, multicast, and unknown unicast traffic using multicast instead of flooding.
- ✓ Carries segmentation information.

Cisco SD-Access Fabric

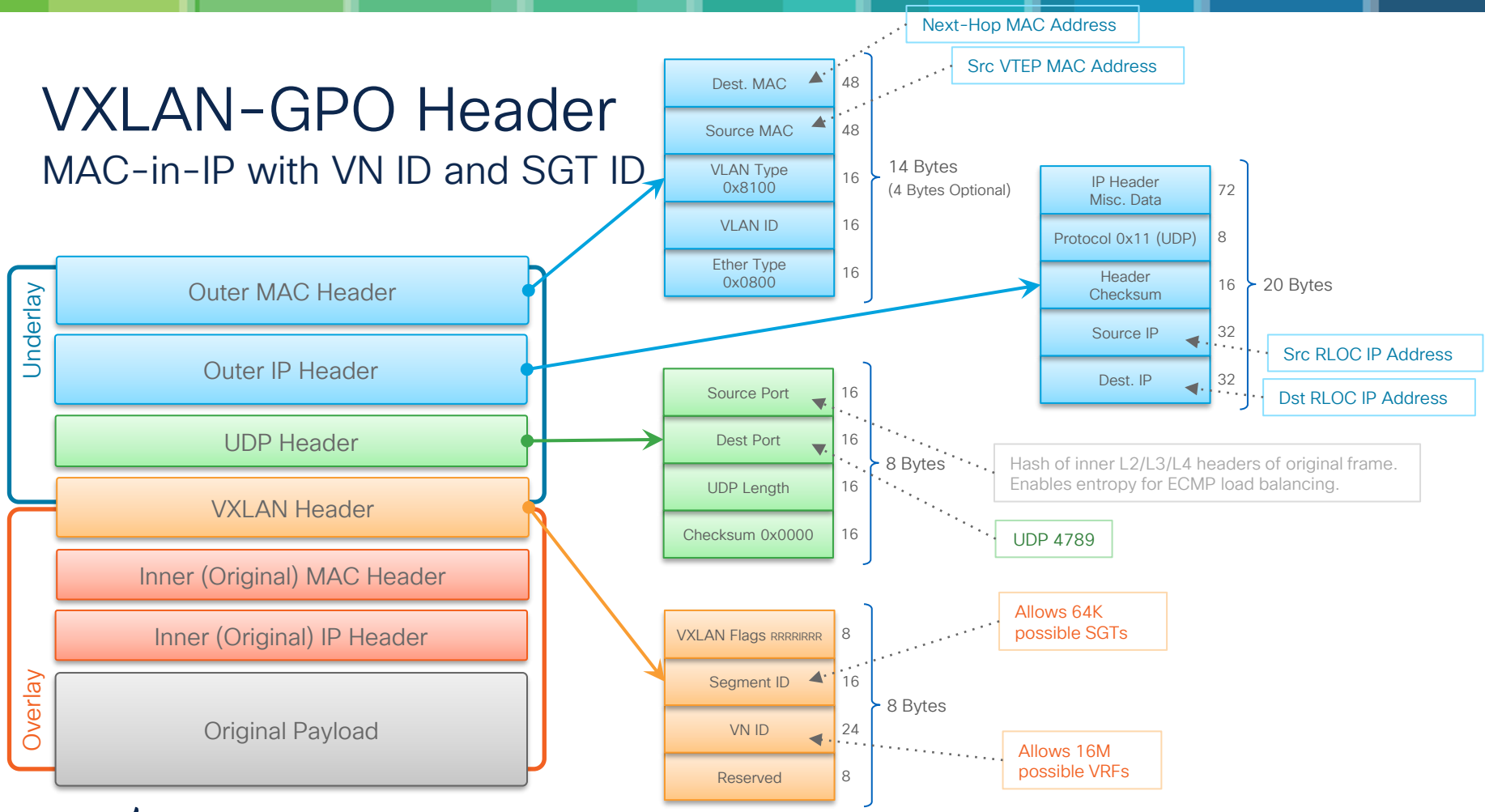
Data Plane: VXLAN

1. Control Plane: LISP
2. Data Plane: VXLAN



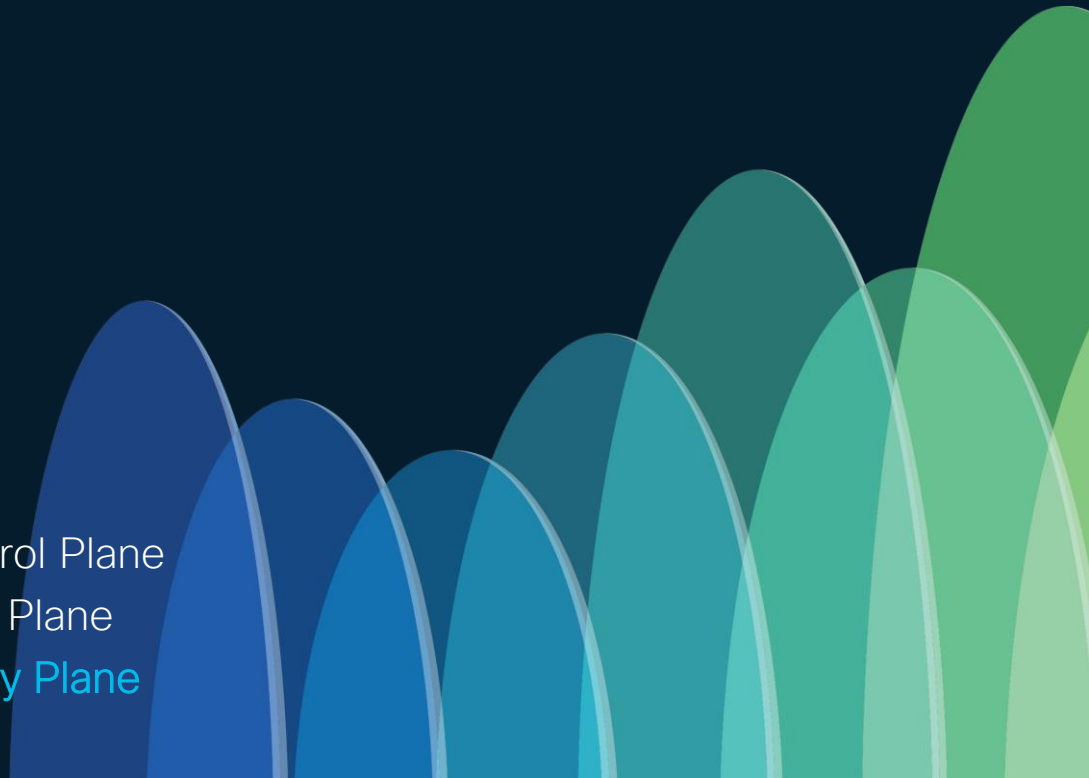
VXLAN-GPO Header

MAC-in-IP with VN ID and SGT ID



Fabric Fundamentals

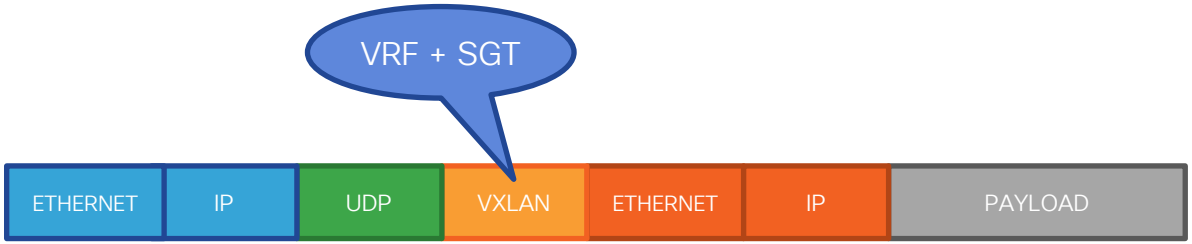
1. Control Plane
2. Data Plane
3. Policy Plane



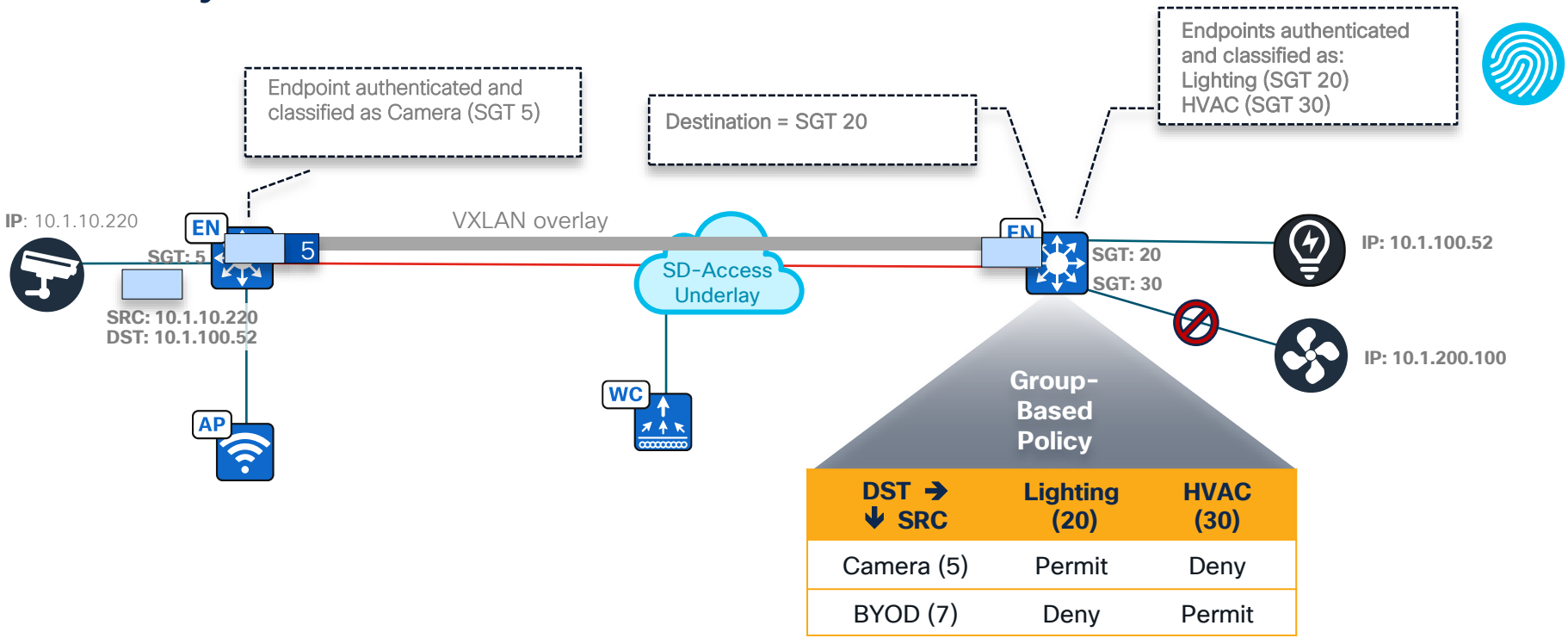
Cisco SD-Access Fabric

Policy Plane: Group-Based Policy

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



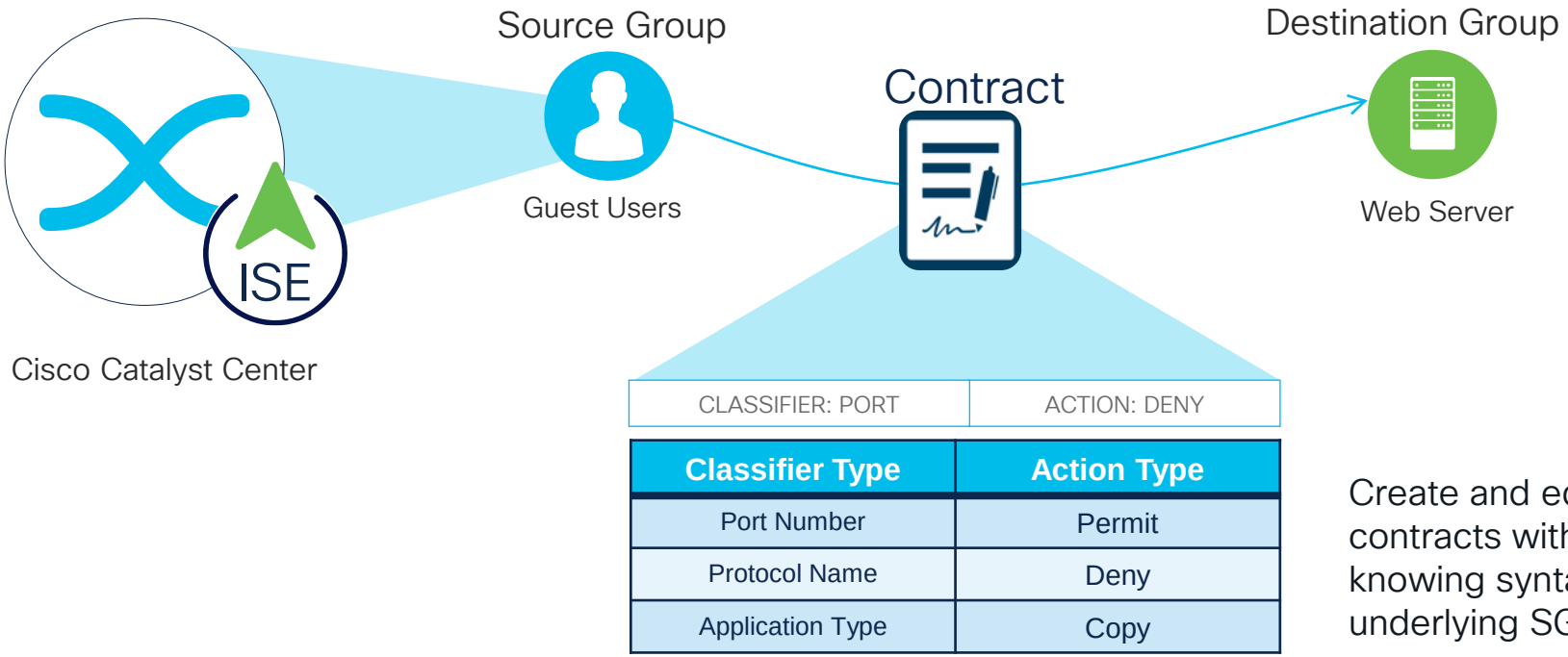
What is Security Group Tag and Group-Based Policy?



DST → ↓ SRC	Lighting (20)	HVAC (30)
Camera (5)	Permit	Deny
BYOD (7)	Deny	Permit

SD-Access Policy

Access Control Policies



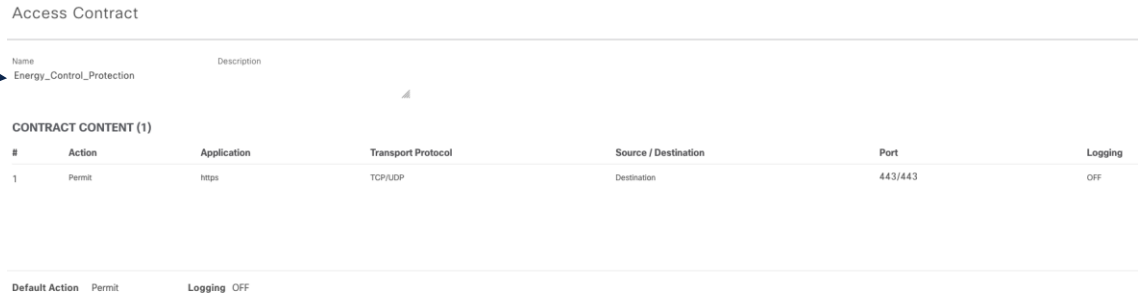
Classifier Type	Action Type
Port Number	Permit
Protocol Name	Deny
Application Type	Copy

Create and edit access contracts without knowing syntax for underlying SGACLs.

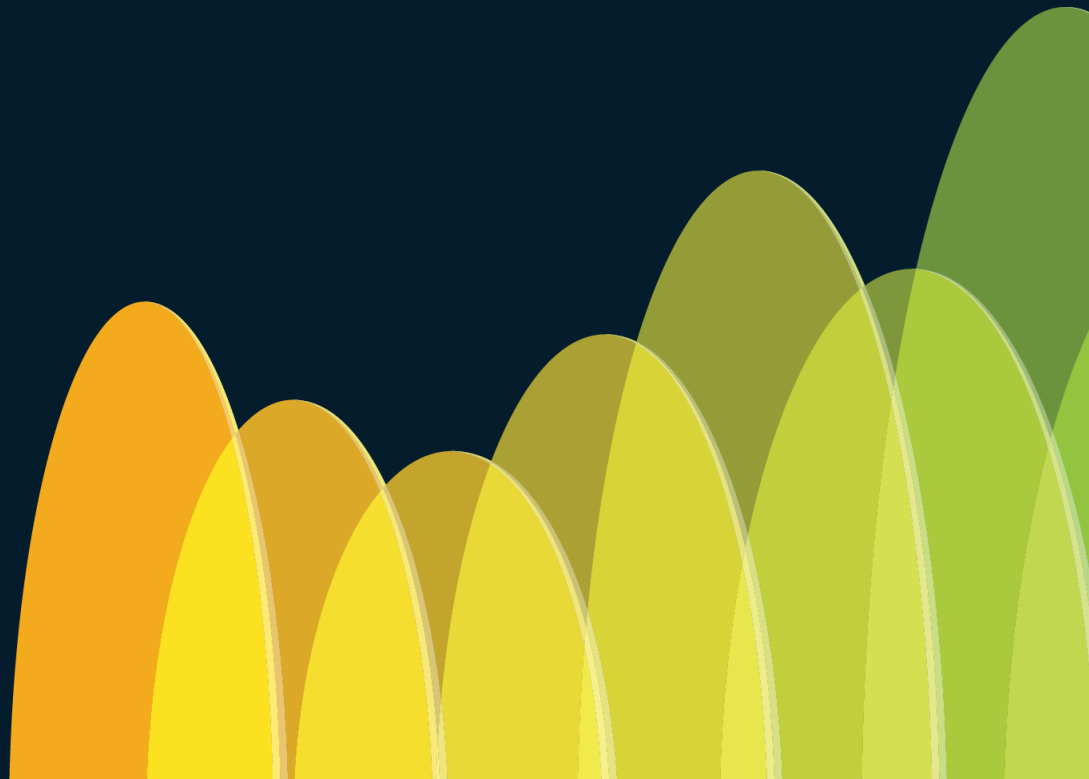
SD-Access Policy

Group-Based Access Control Policy

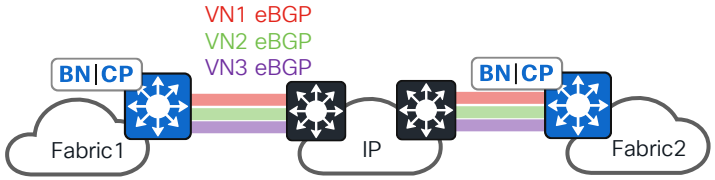
1. Select **Source Group**(s)
2. Select **Destination Group**(s)
3. Select **Access Contract**(s)



Multiple Fabrics



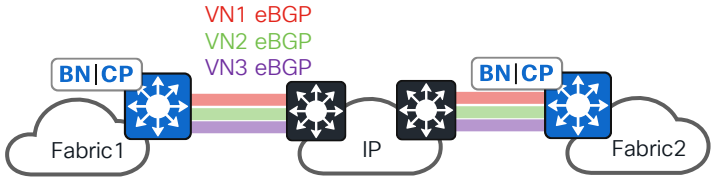
Transits for VN and SGT Preservation

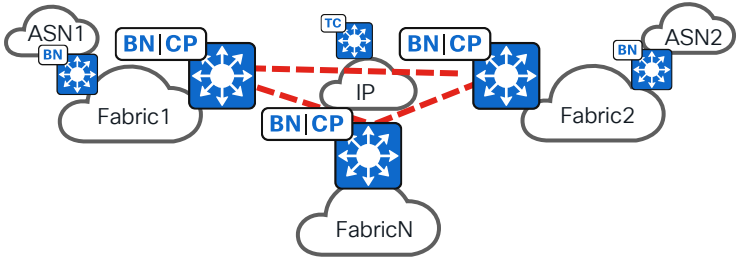


IP-Based Transit

- 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

- Handoff from the Border is automated with Cisco Catalyst Center
- 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.

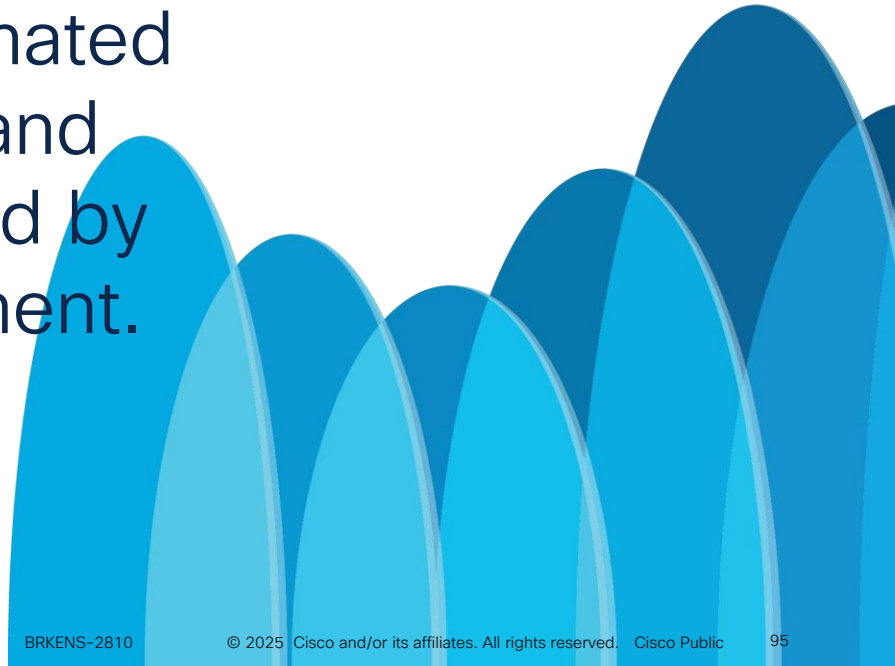
SD-Access Transit

- Automated from Cisco Catalyst Center
- Used only for inter-fabric-site traffic
- Uses VXLAN data plane between Fabric Sites.
- Preserves Layer 3 Virtual Networks and SGT.
- Fabric as a transit between external routing domains.

Watch BRKENS-2816 for SD-Access Transit deep dive

Conclusion

Cisco's SD-Access LISP provides a secure, flexible, and automated way to meet the security and operational challenges faced by an ever-changing environment.



Global Partner Solution Advisors

NEW – Fully Virtualized, SD-Access Secure Campus Lab

Virtualized SD-Access Lab

- Fully Customizable Topology with virtualized 9kv's and 8kv's
- Access on dCloud or build on your existing Data Center
- Fraction of the cost
- GPSA mentored lab buildout support available!

CTF Mission

- Experience the SD-Access Virtual Lab at Capture the Flag in The World of Solutions
- Use Cases – Fabric Sites and Virtual Network Provisioning, Fusion Automation, Extranet, Micro Segmentation, and more!

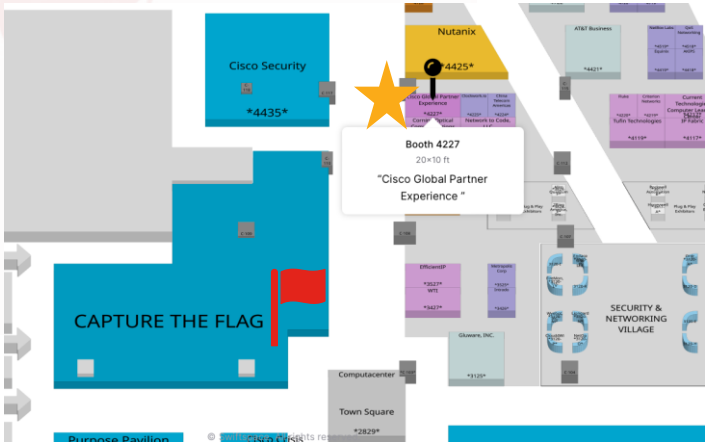
Contact

- GPSA is your source for no-cost, partner enabment and practice building!
- Visit the Global Partner Experience booth across from Capture the Flag, for more information.

Virtual SD-Access Lab on dCloud

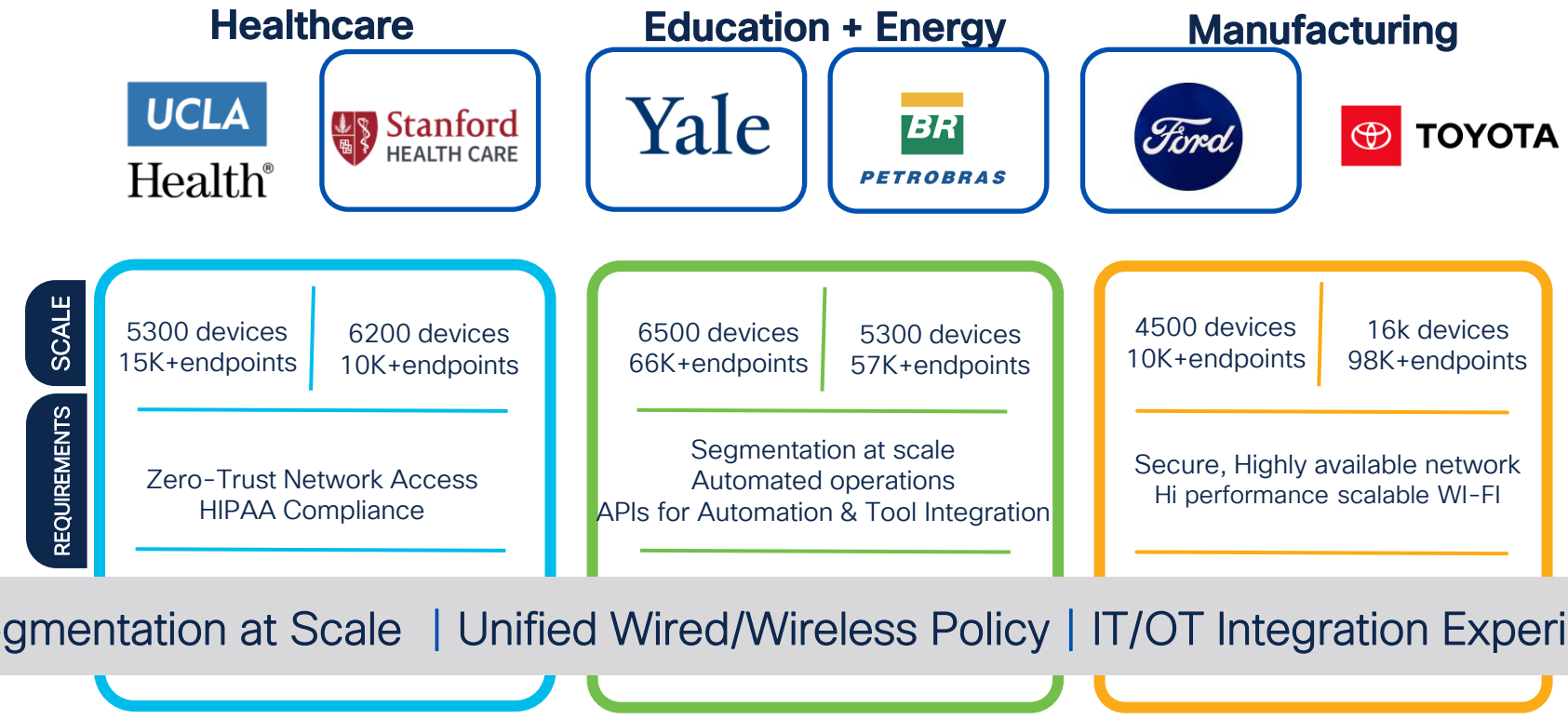
GPSA Sales Connect Page

CTF at Cisco Live
Check out Secure Campus Section



cisco Live!

SD-Access LISP Customer Success



Segmentation at Scale | Unified Wired/Wireless Policy | IT/OT Integration Experience

BRKENS 1801, BRKENS 1802, CIUG-1003

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

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

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

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

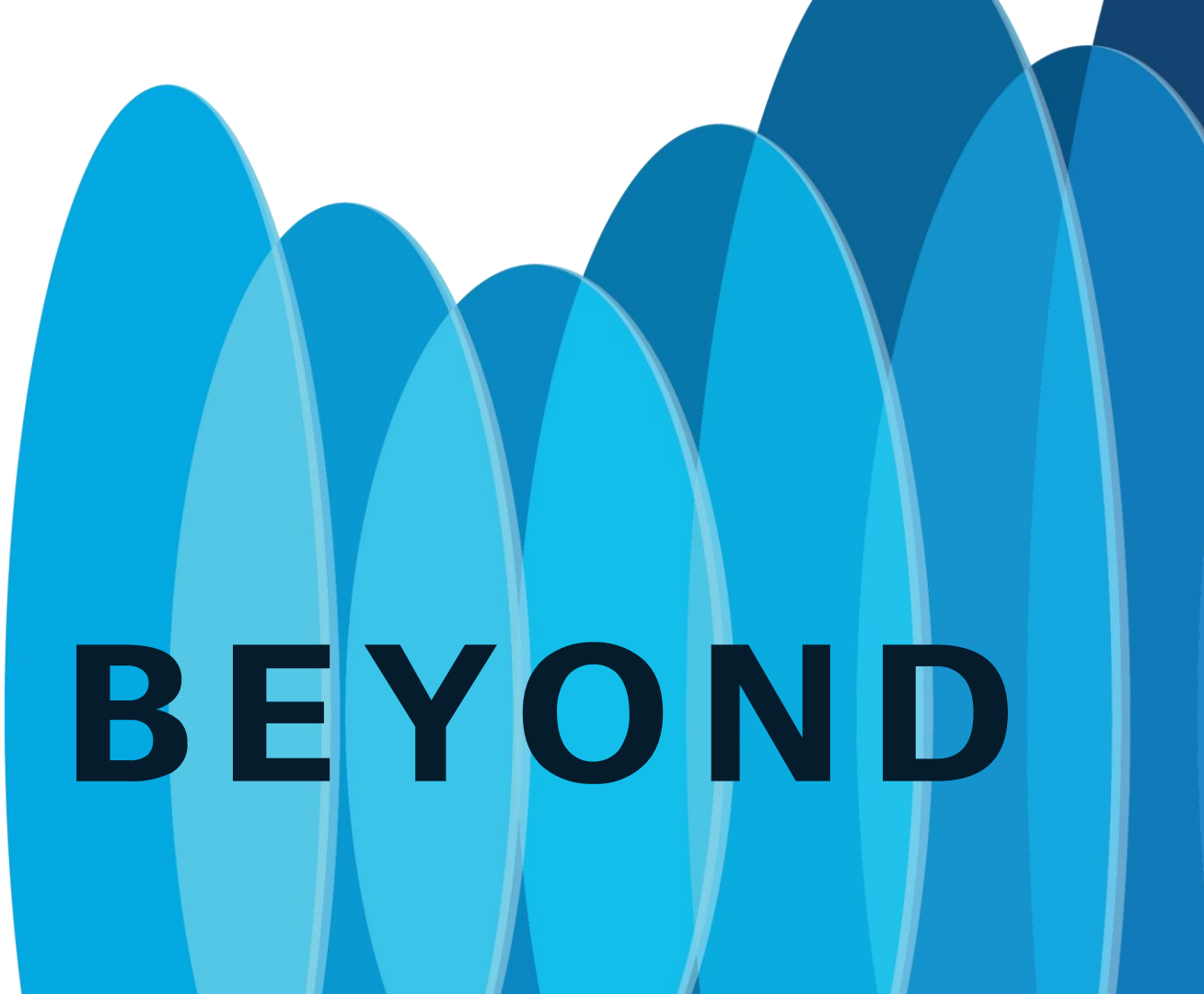
All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

Thank you

cisco Live!

cisco Live!



GO BEYOND