

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC





Cisco Software-Defined Access LISP Solution Fundamentals

Jeff Lee
Solutions Engineer
CCIE#25598 (R&S)
BRKENS-2810



#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-2810>

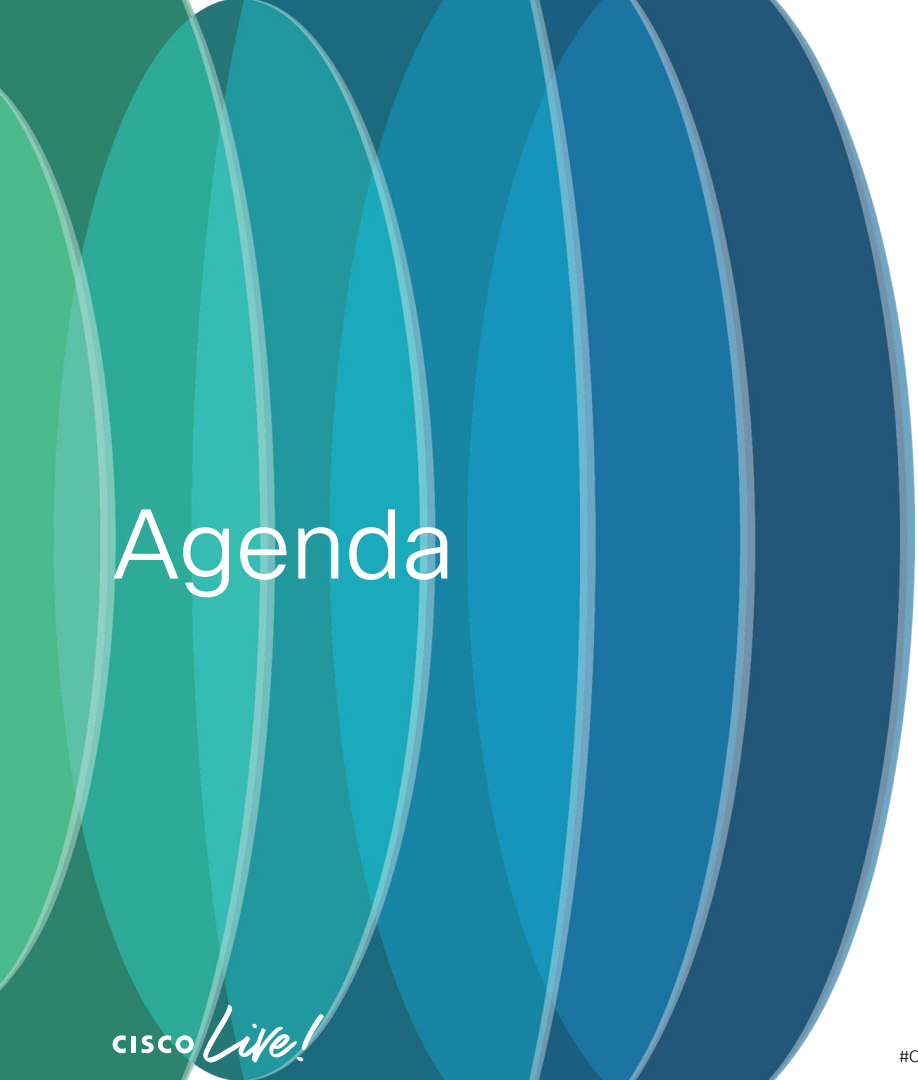


Who am I?

- Over 20 years networking experience
- 5 years in Cisco as Enterprise Networking Specialist
- Avid cyclist (used to be good)
- Keen (if not very good) skier

Jeff Lee
Solutions Engineer





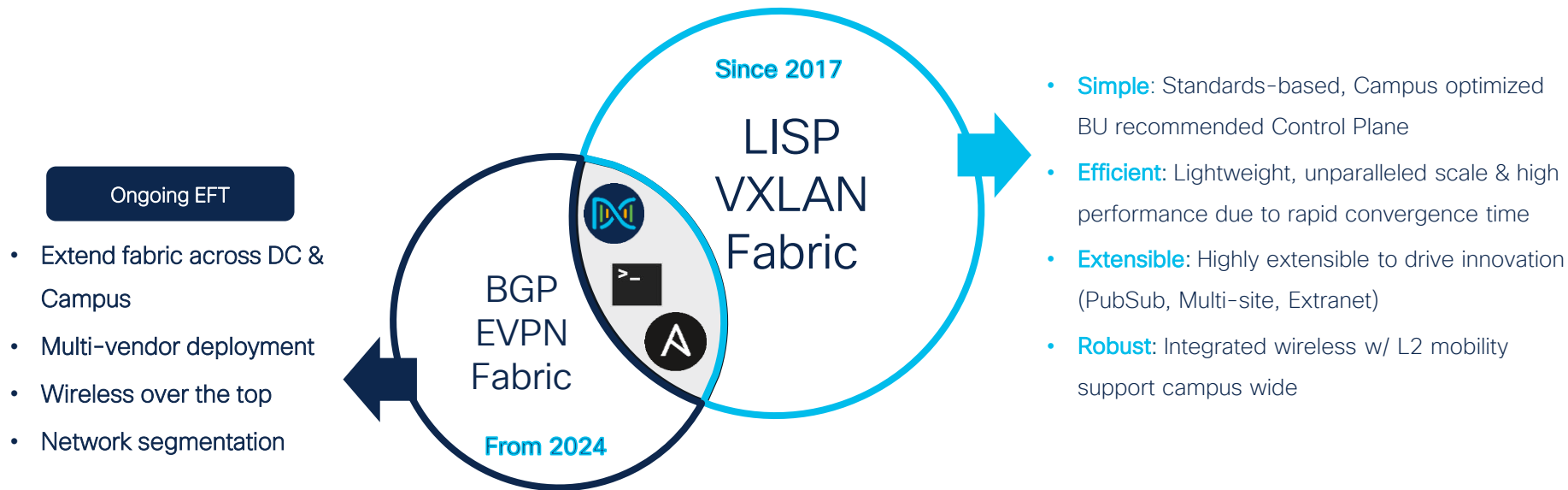
Agenda

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

Why Cisco SD-Access LISP?

Effortlessly Deploy Your Fabric of Choice

LISP Fabric is the **leading** choice for Enterprise customers!

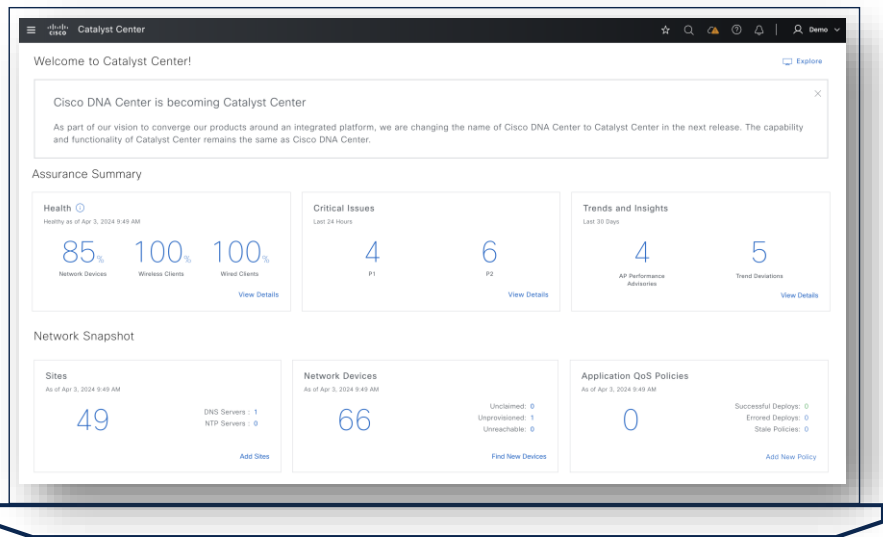


One Infrastructure | Single Data Plane | Consistent Zero-Trust Experience

Intent-Driven Automation

Standardised templates for consistent implementation

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!

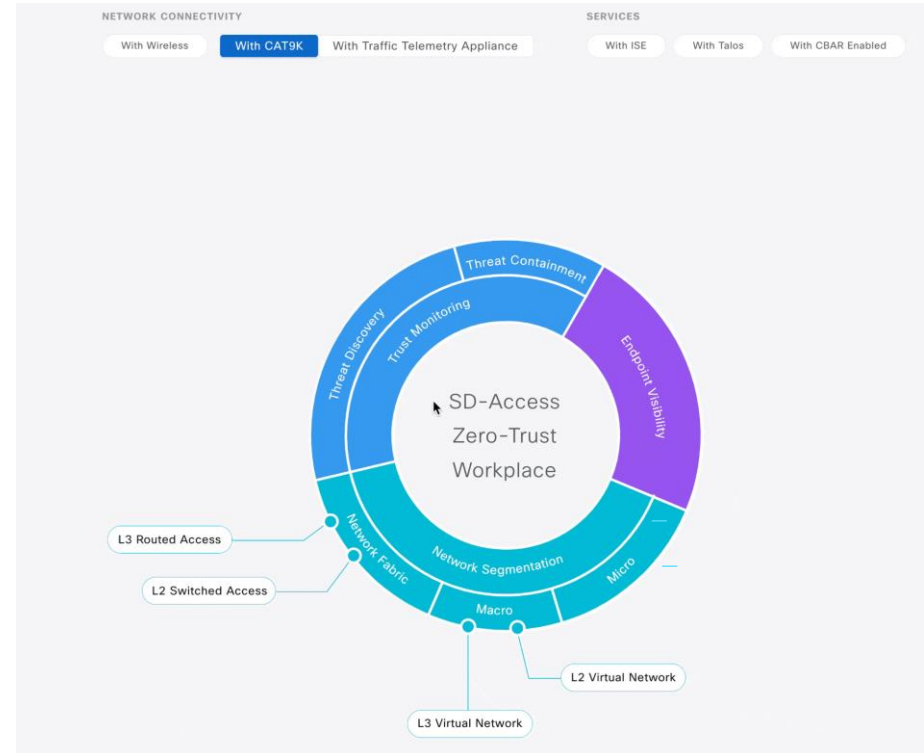
Easy for admins to configure and manage networks

SD-Access Zero-Trust Workplace

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

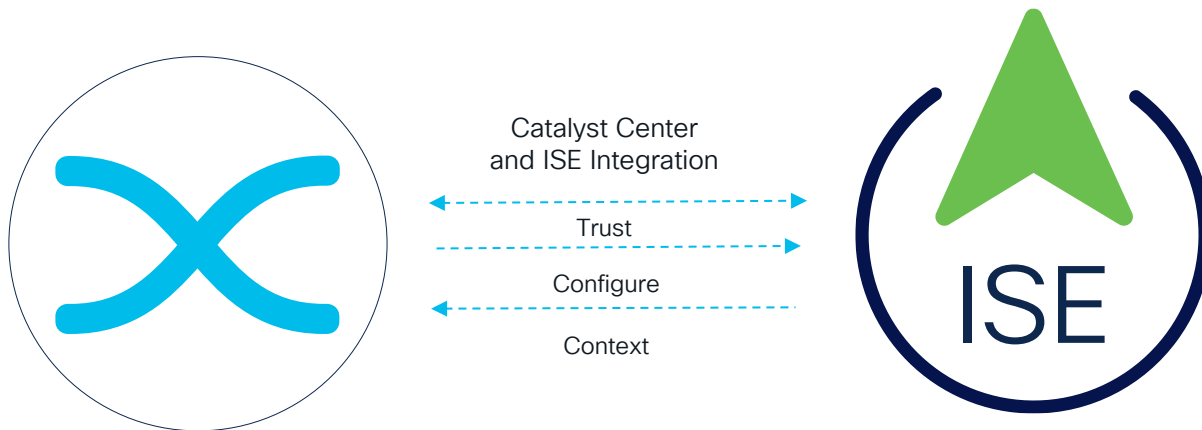


3 Pillars of SD-Access Zero Trust Workplace:
Visibility, Segmentation, and Trust.



Attribute-Based Policy and Segmentation

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

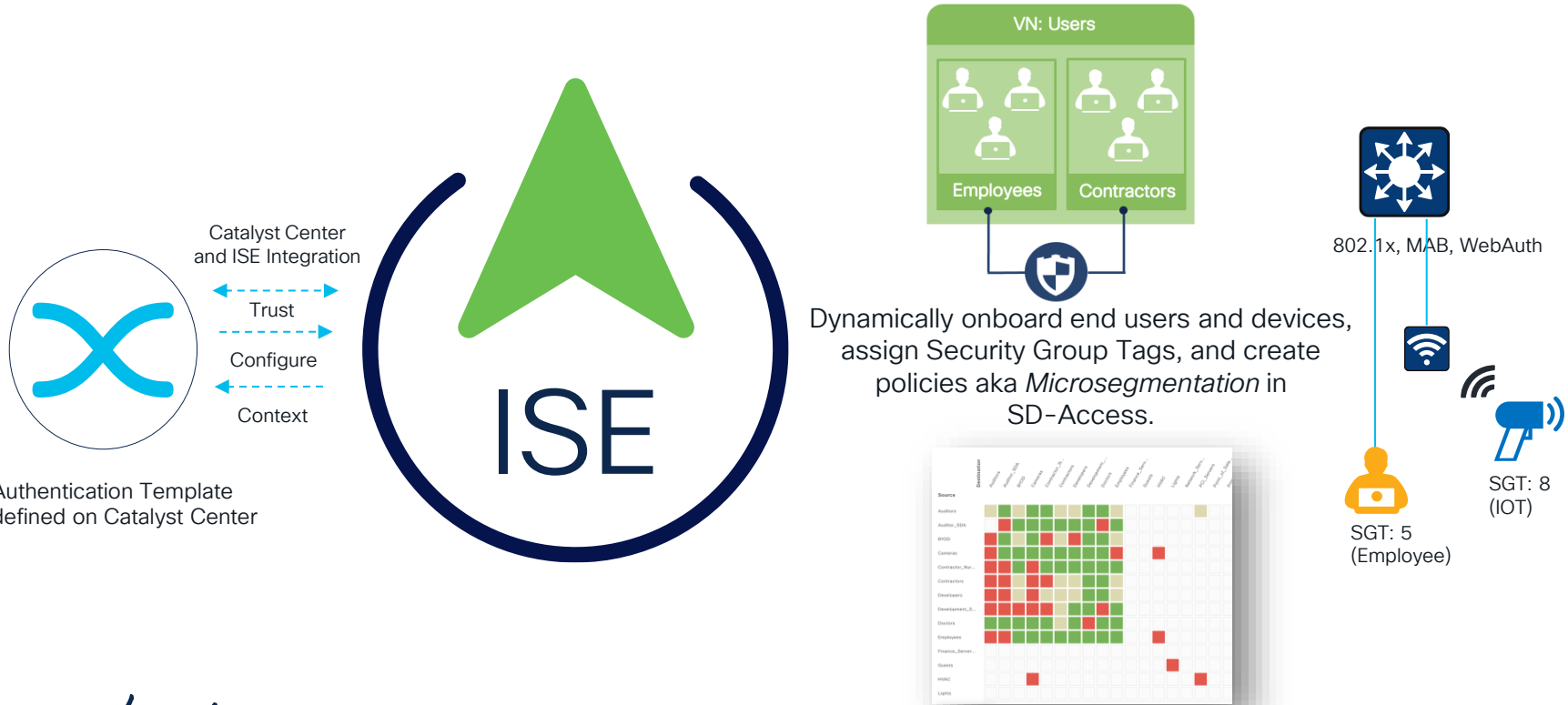


Automated configuration and segmentation policies
paired with scalable onboarding of endpoints.



Attribute-Based Policy and Segmentation

Move away from IPs and ACLs to Group Based Access Control



Benefits of Cisco Software-Defined Access

Enhance Security and Compliance



Deliver Consistent Experience



Boost Operational Effectiveness

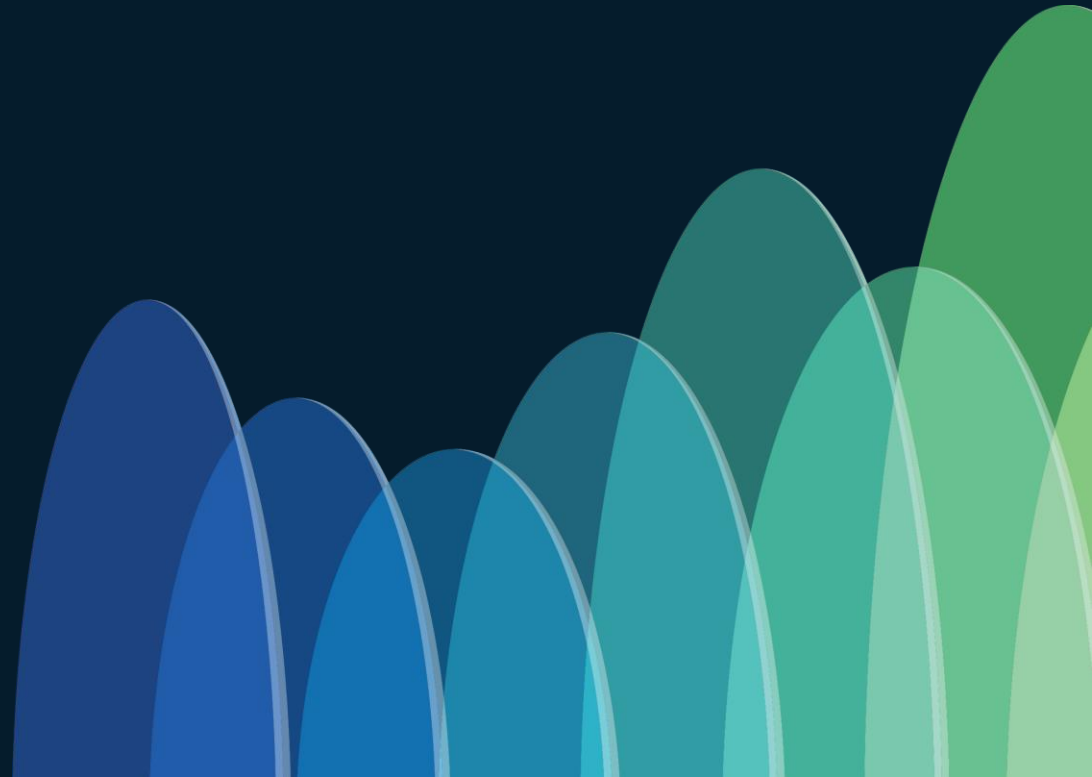


Gain Network Insights



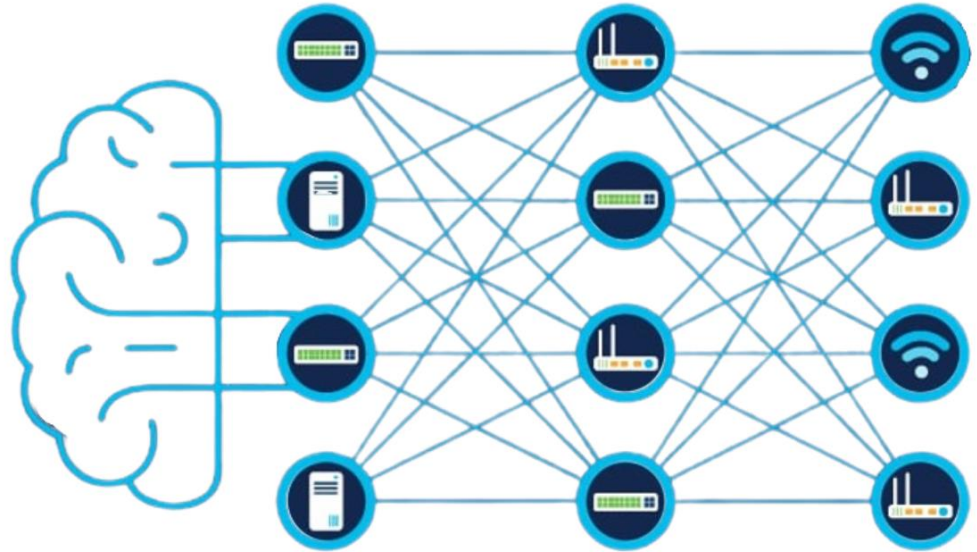
Roles and Terminology

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



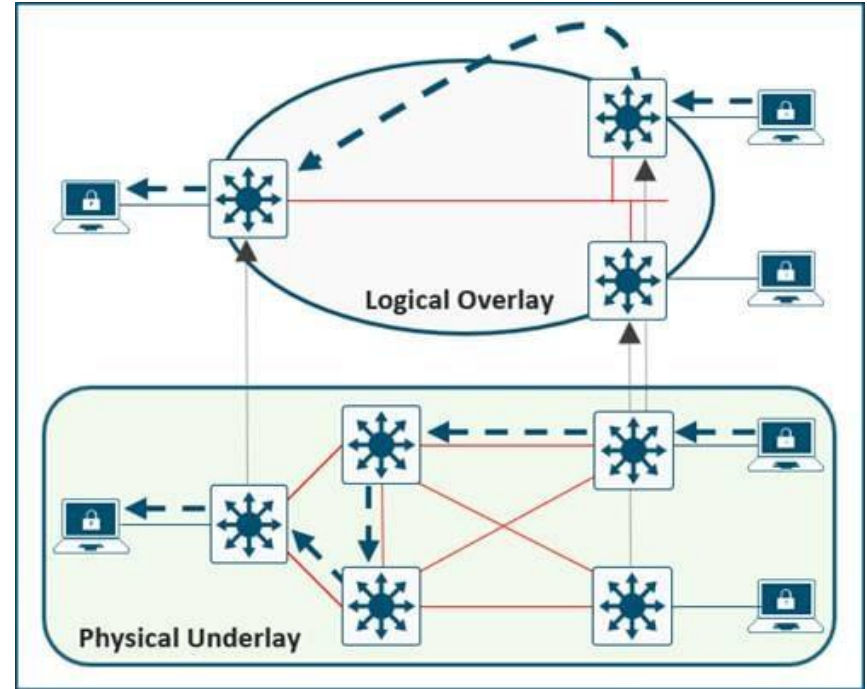
What is a Network Fabric?

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



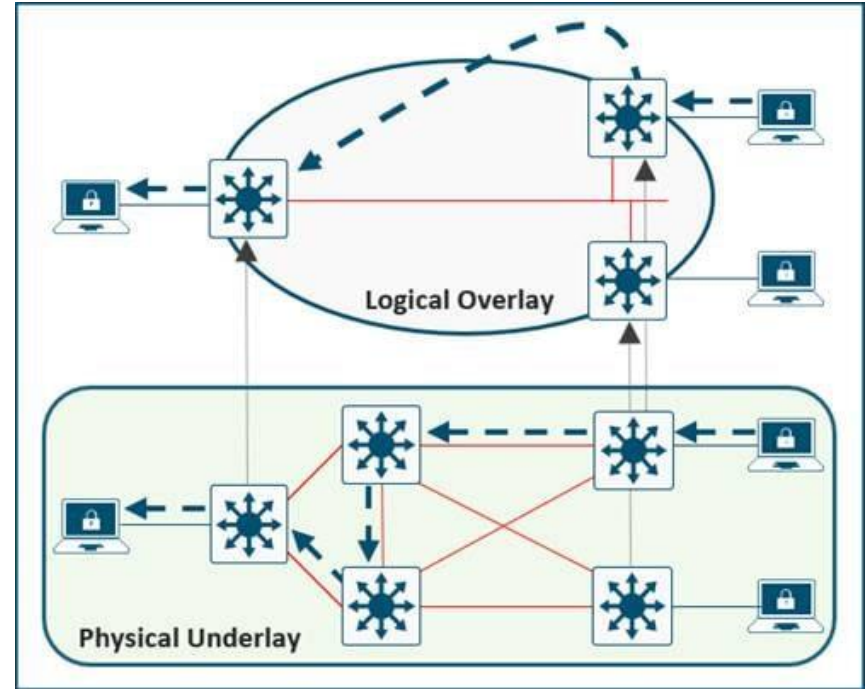
What is an Overlay?

- 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



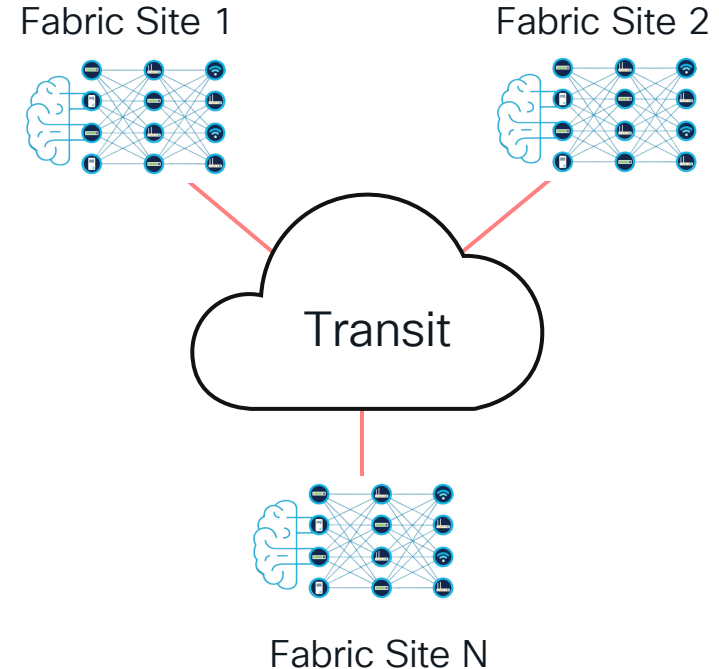
Why an Overlay?

- Underlay is simple and manageable.
- Maximise network reliability.
- Services – deliver using overlay.
- Mobility – map endpoints to edges.
- Scalability – reduce protocol state.
- Flexible and programmable.



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”.



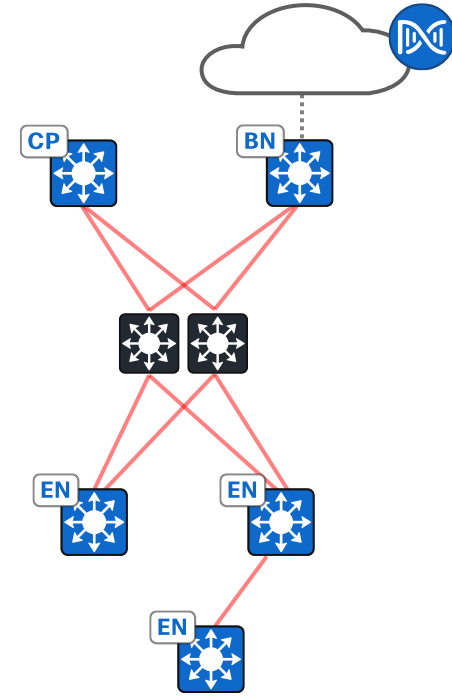
Roles and Terminology

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

Cisco SD-Access Roles

Mandatory Components

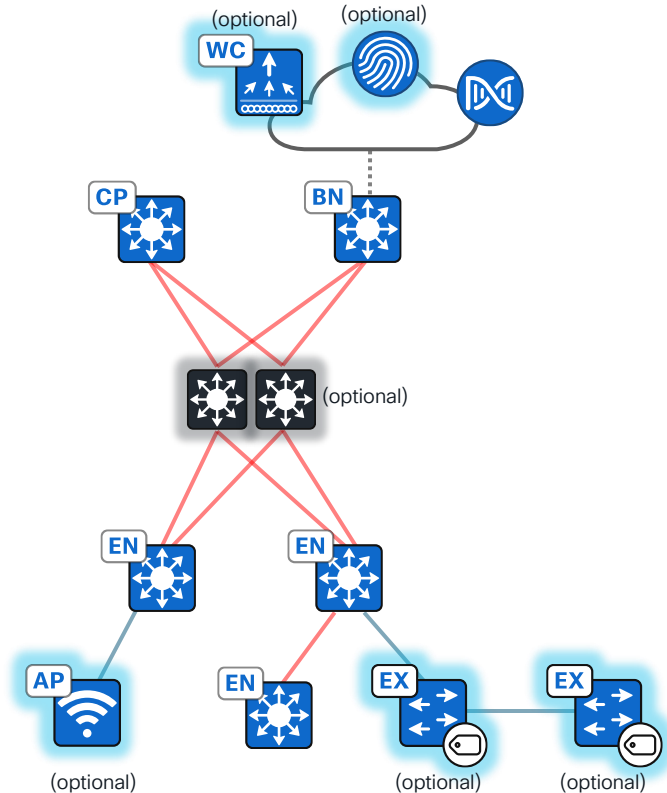
- **Cisco Catalyst Center** – GUI and APIs for intent-based automation of wired and wireless fabric devices.
- **Fabric Border Nodes** – A fabric device that connects external L3 and L2 networks to the Cisco SD-Access fabric.
- **Edge Nodes** – A fabric device that connects wired endpoints to the Cisco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



Cisco SD-Access Roles

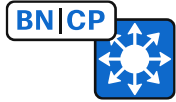
Optional Components

- **Identity Services Engine** – Highly recommended. NAC and ID 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 Roles

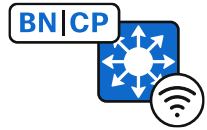
Some of the Supported Co-locations



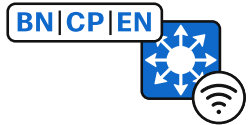
Border Node and Control Plane Node.



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.

SD-Access Design Aides

- Cisco Validated Design: <https://cs.co/sda-cvd>
- Design Tool (use Chrome Incognito): <http://cs.co/sda-design-tool>



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

New Deployment

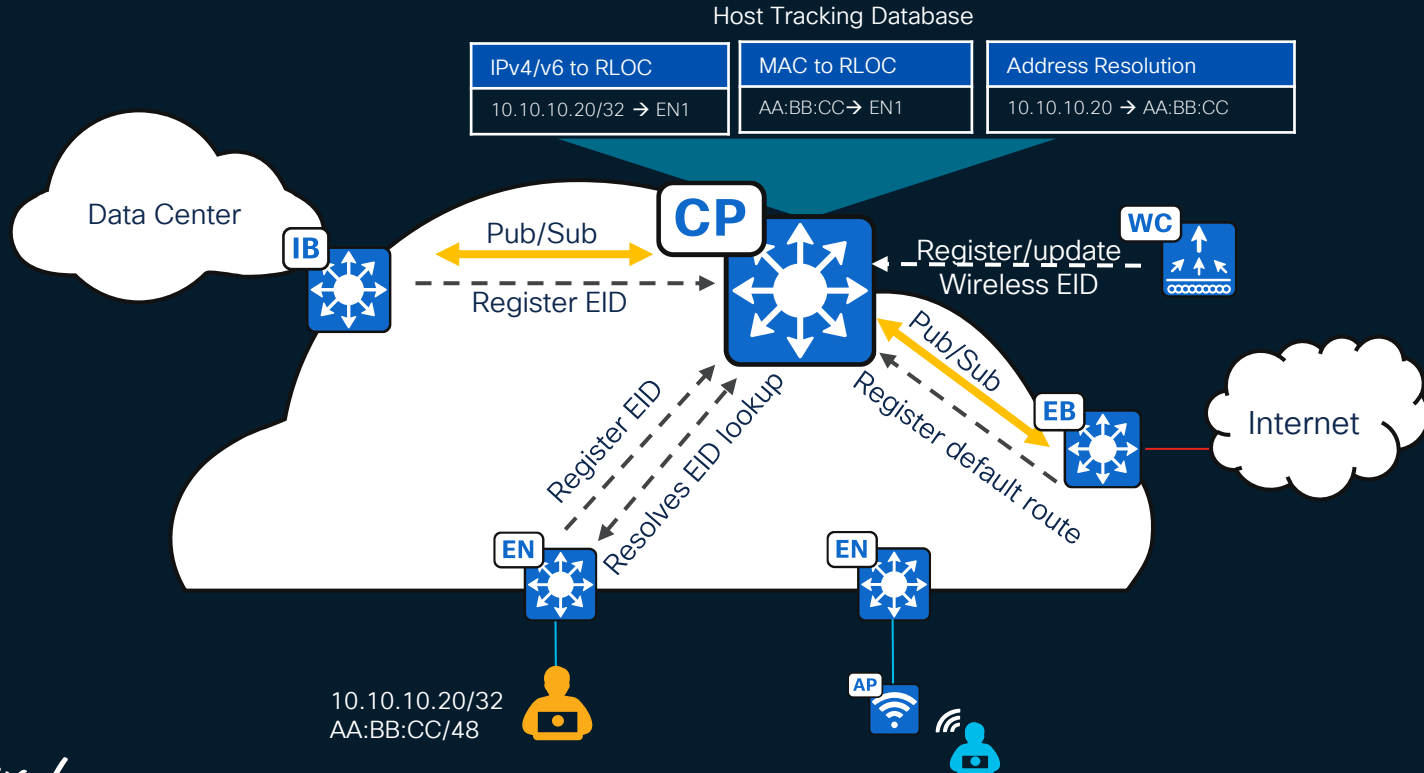
Release: Device Role:

SD-Access Compatibility Matrix for Cisco Catalyst Center 2.3.5.6 (recommended release)

Device Role	Device Series	Device Model	Recommended Release	Supported Release
	Cisco Catalyst 9300 Series Switches	C9300-24T C9300-24P C9300-24U C9300-24UX C9300-48T More ...	IOS XE 17.12.4	IOS XE 17.15.x IOS XE 17.12.x IOS XE 17.9.x IOS XE 17.6.x IOS XE 17.3.x More ...
		C9300-48UN C9300-24UB C9300-48UB C9300-24UXB	IOS XE 17.12.4	IOS XE 17.15.x IOS XE 17.12.x IOS XE 17.9.x IOS XE 17.6.x

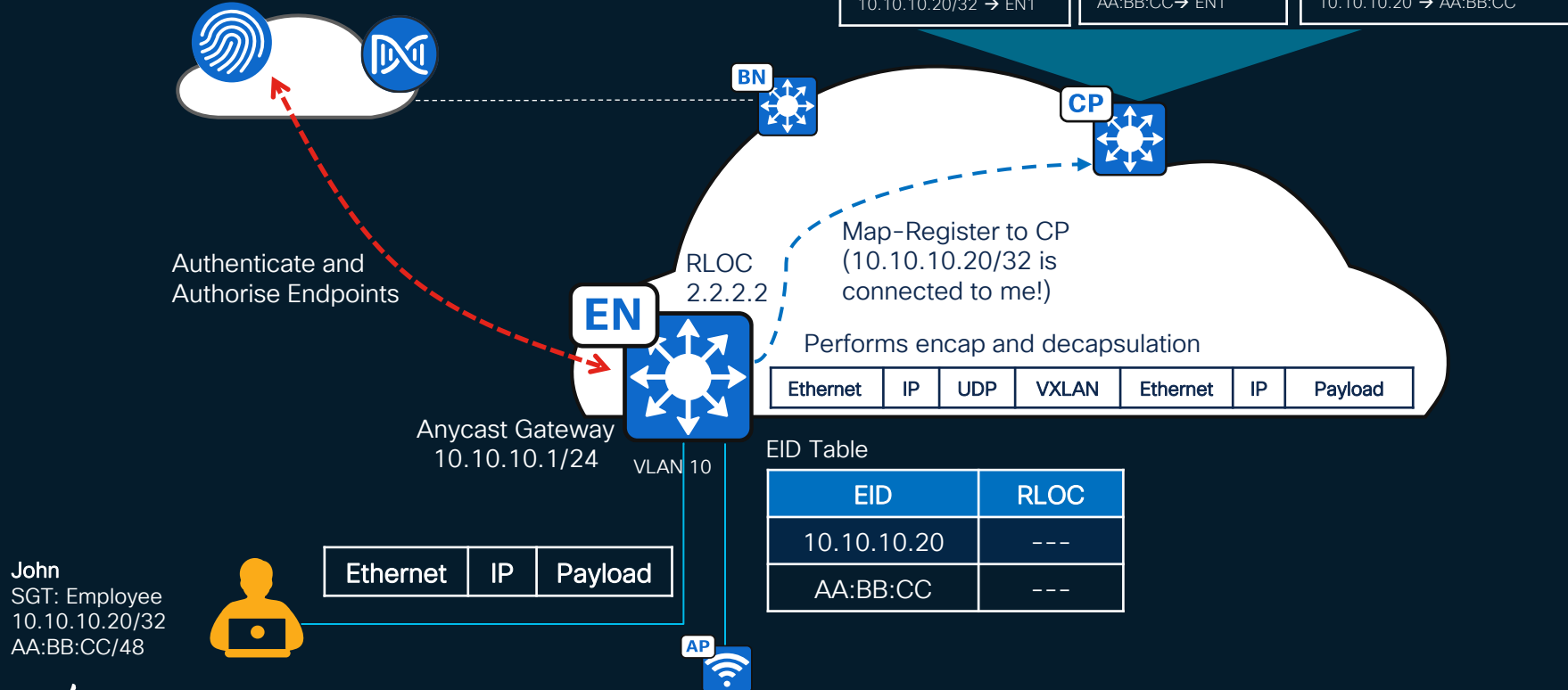
Control Plane Node

Maintains Host Tracking Database containing Endpoint Attribute to Location Mapping



Edge Node

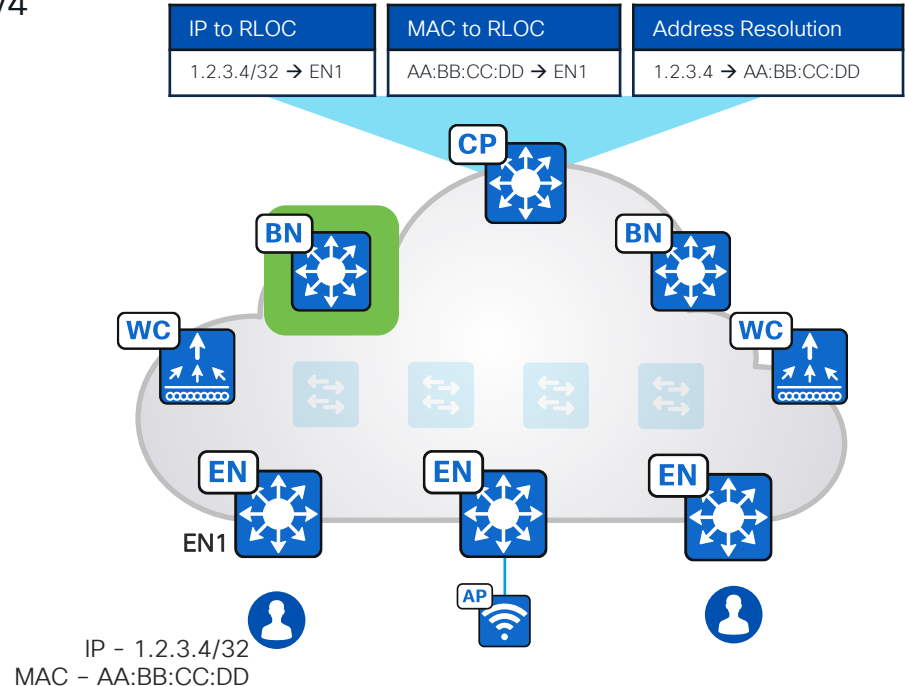
Provides First Hop Services for Endpoints



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.

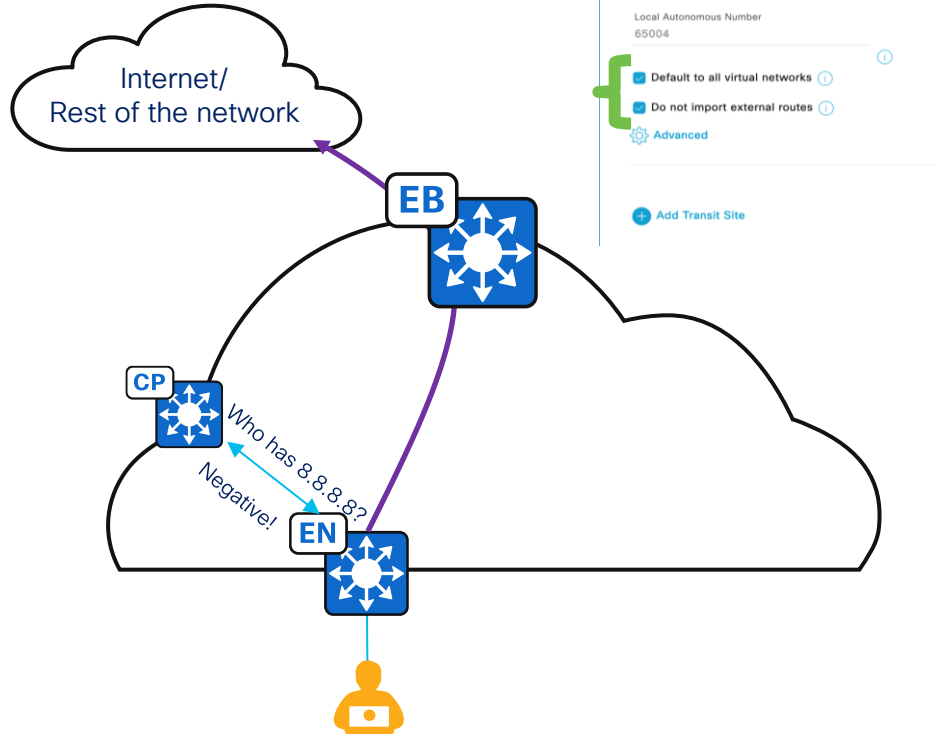


Cisco SD-Access Fabric

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.
- Acts as a gateway of last resort for the Fabric Site.
- Does not register eBGP prefixes from outside the Fabric Site into the fabric Control Plane.

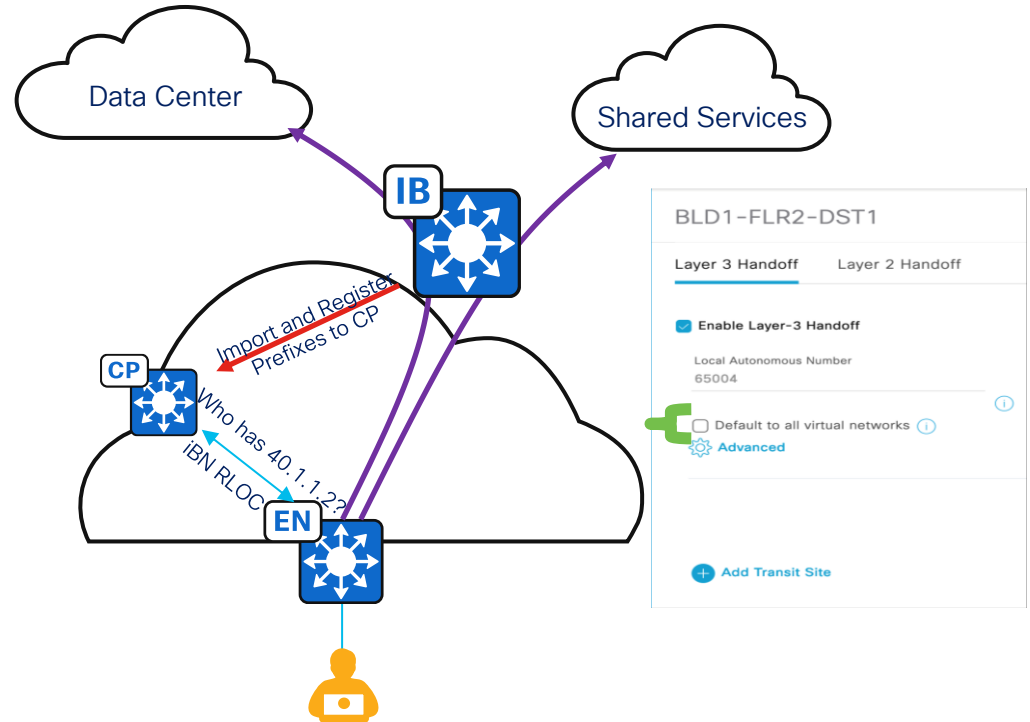


Cisco SD-Access Fabric

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.

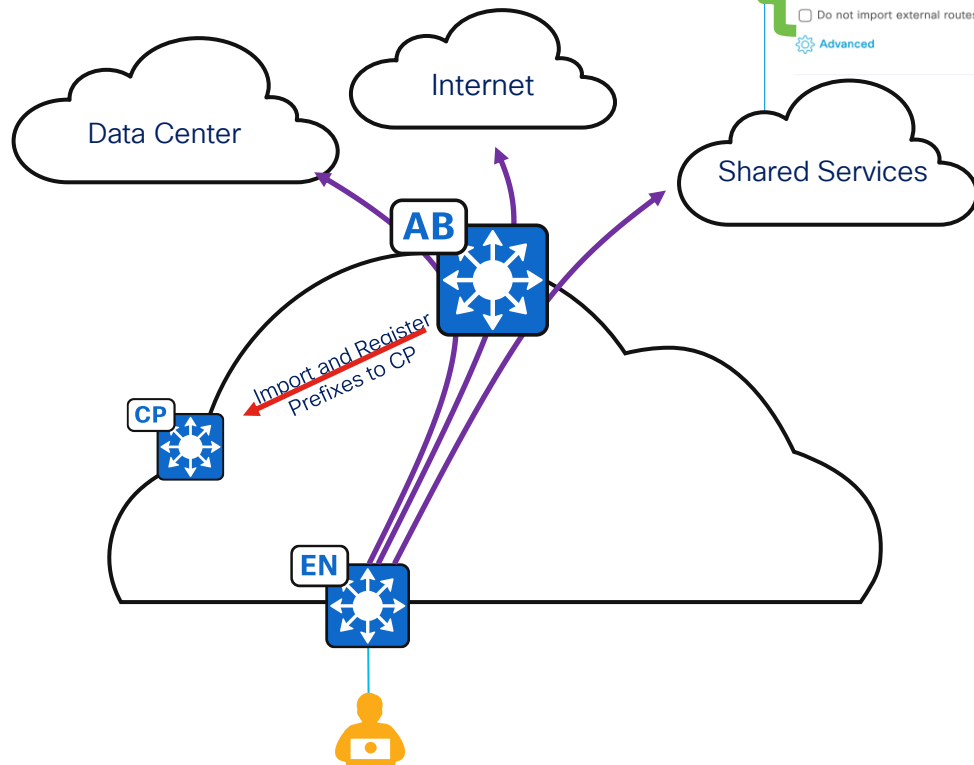


Cisco SD-Access Fabric

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.



BLD1-FLR2-DST1

Layer 3 Handoff

Layer 2 Handoff

☒ Enable Layer-3 Handoff

Local Autonomous Number
65004

☒ Default to all virtual networks ⓘ

☐ Do not import external routes ⓘ

Advanced

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.

PNP-DEMO1.cbr.ciscolabs.com

Layer 3 Handoff

Layer 2 Handoff



LAYER 2 VIRTUAL NETWORKS WITH A GATEWAY OUTSIDE OF THE FABRIC

Layer 2 Virtual Network

VLANs

Handed off VLANs

0

LAYER 2 VIRTUAL NETWORKS WITH AN ANYCAST GATEWAY



Search Layer 3 Virtual Networks

Layer 3 Virtual Network

Handed-off VLANs

Corp

1

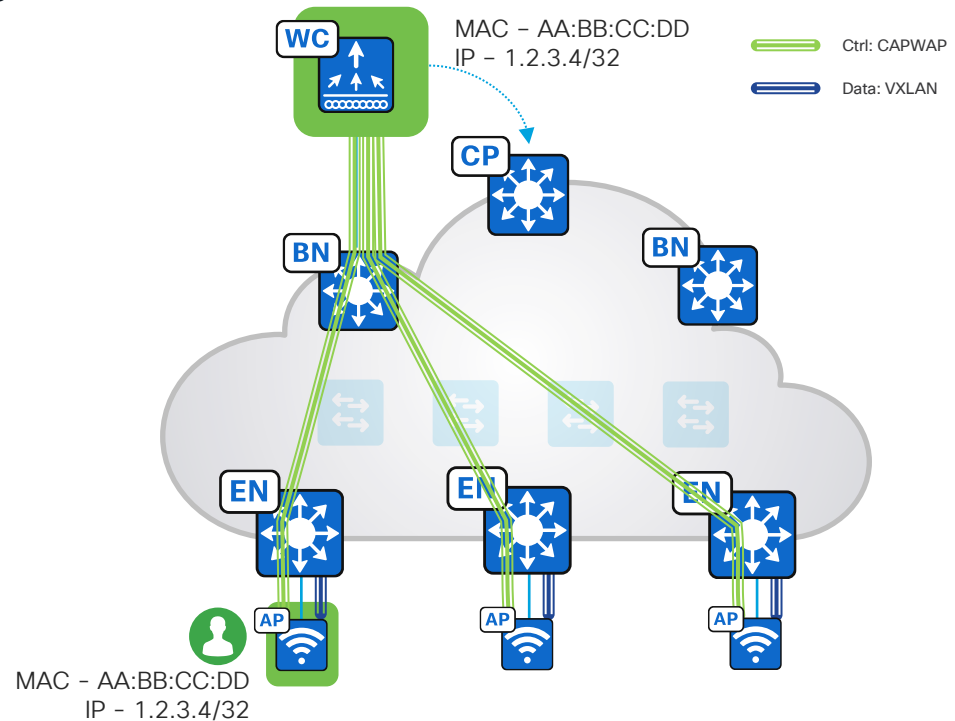
1 Records

Show Records: 25

Cisco SD-Access Fabric

Fabric Enabled Wireless for Unified Management, Policy and Data Planes

- Fabric WLC accessible through a Fabric Border Node (Underlay). Can be several hops away.
- Fabric Enabled APs reside in a dedicated IP range and communicate with the Fabric WLC (CAPWAP Control).
- Fabric WLC registers endpoints with the Control Plane Node.
- Fabric APs switch endpoint traffic to the adjacent Edge Node. No concentrator bottleneck. Wi-Fi 6 up to 9.6 Gbps. Wi-Fi 7 up to 46 Gbps.
- Wireless endpoints use same data plane and policy plane as wired endpoints.

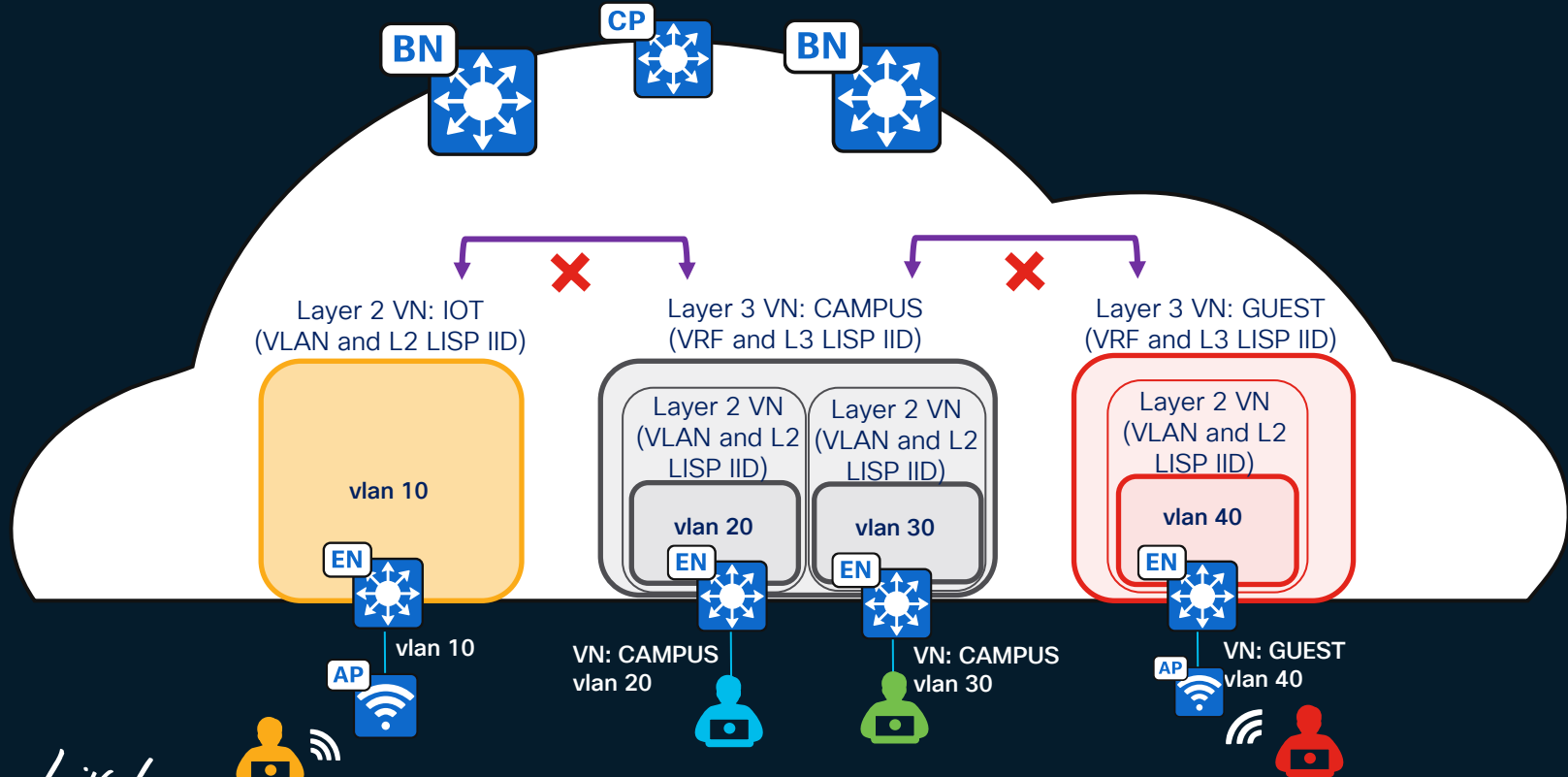


Roles and Terminology

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

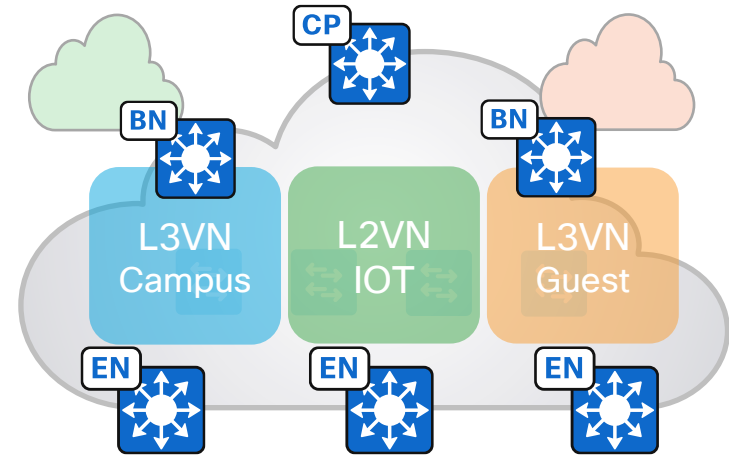
Virtual Networks

Overlay Network Virtualisation, also known as Macro-segmentation.



Virtual Networks

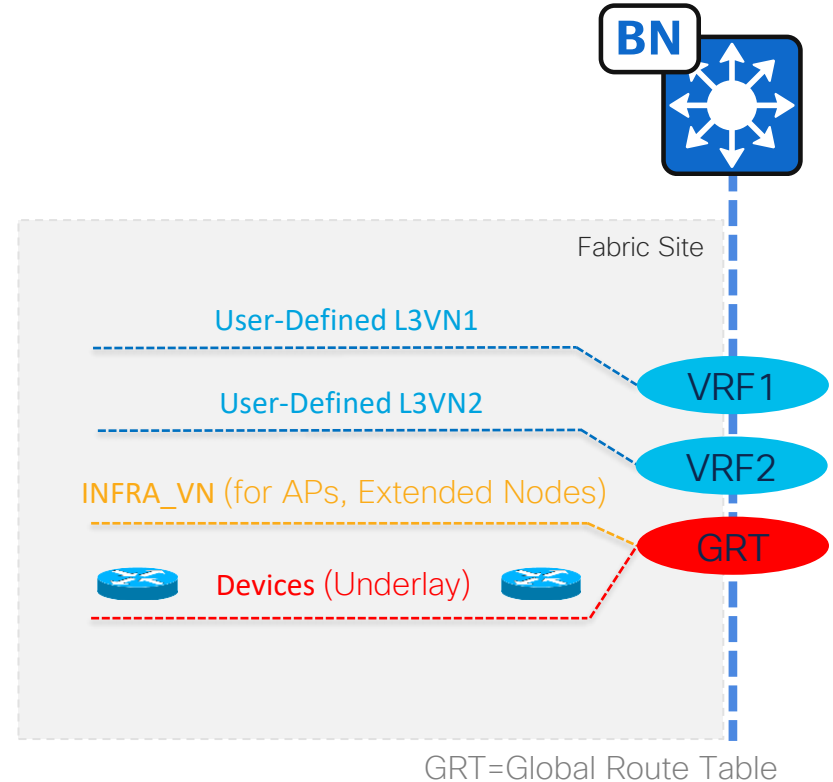
- Layer 3 Virtual Networks use VRFs and LISP Instance IDs to maintain separate routing topologies.
 - Endpoint IDs (IPv4/IPv6 addresses) are routed within an L3VN.
- Layer 2 Virtual Networks use LISP Instance IDs and VLANs to maintain separate switching topologies.
 - Endpoint IDs (MAC addresses) are 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

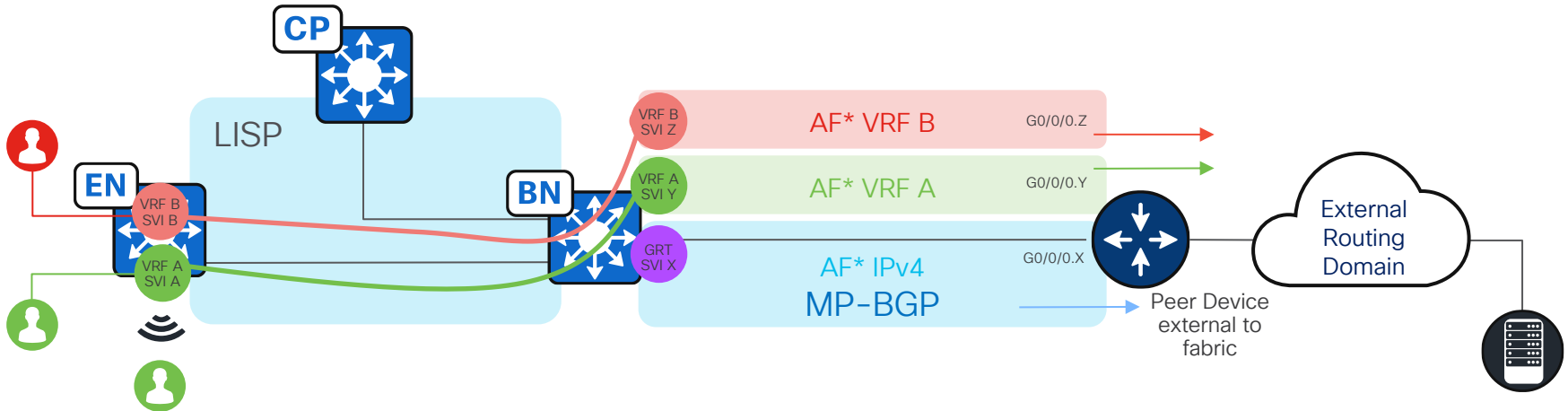
- **User-Defined VNs** can be added or removed on demand.
- **INFRA_VN** is only for **Fabric Access Points** and **Extended Nodes** in the Global Routing Table.
- **Fabric Devices (Underlay)** connectivity is in the **Global Routing Table**.



Cisco SD-Access Fabric

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

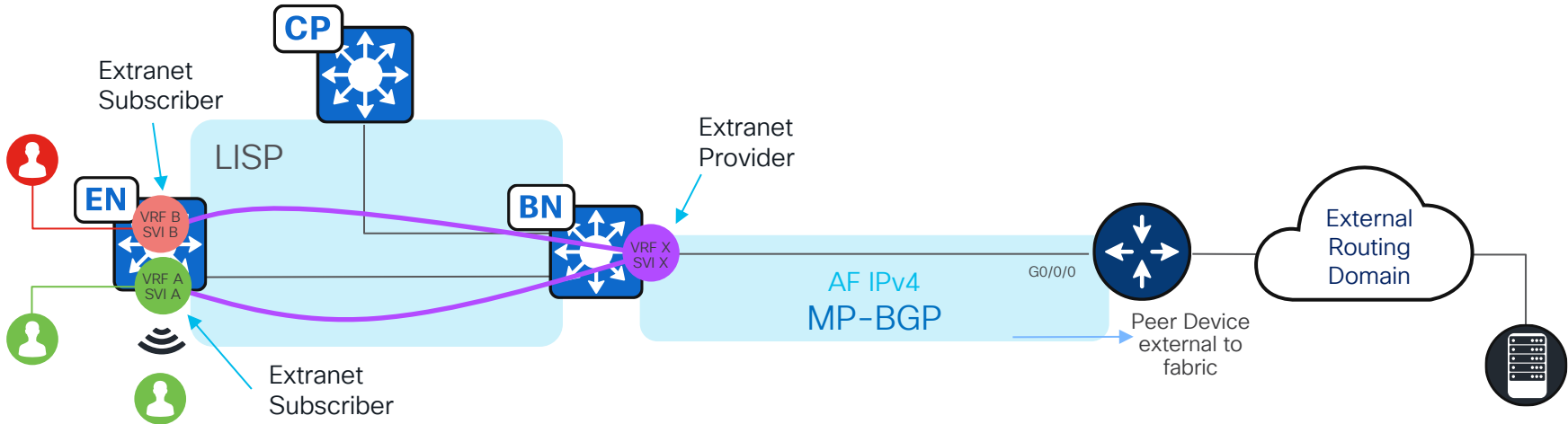
- A “Peer Device” may leak external routes into SD-Access Layer 3 Virtual Networks.
- Alternatively, maintain VRF segmentation outside of the SD-Access Fabric with a VRF-aware external routing domain.
- Peer Device is outside the fabric. Can be any platform (Router, Layer 3 switch, Firewall, etc.) with appropriate capabilities.



Cisco SD-Access Fabric

Extranet Provider Virtual Network Layer 3 Handoff

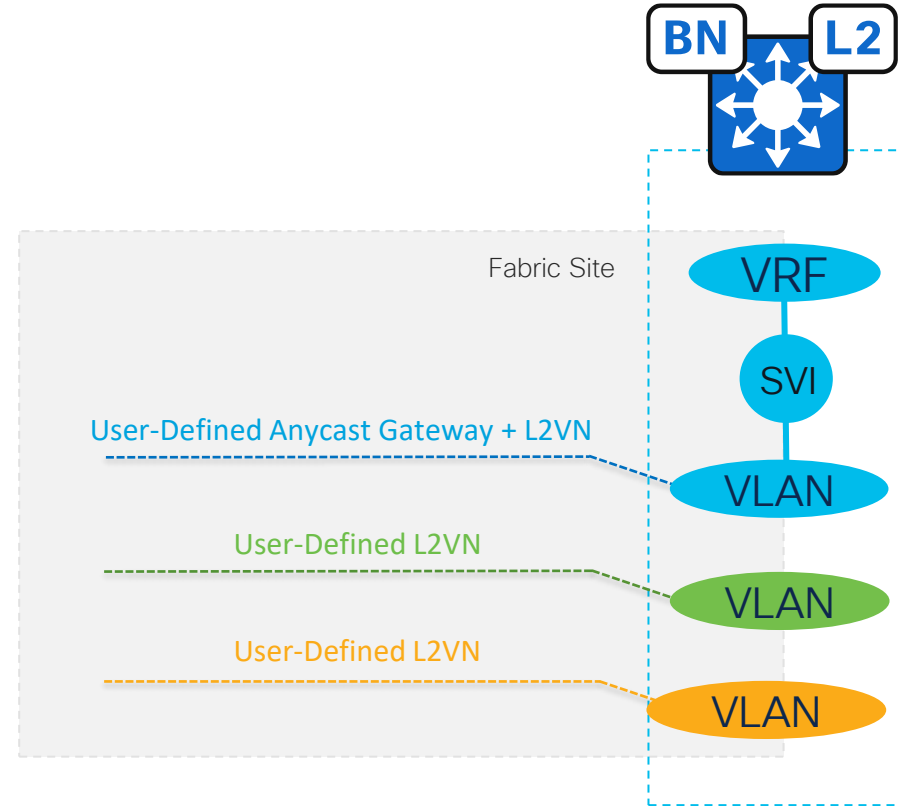
- Use an Extranet Policy to allow communication between one Provider Virtual Network and one or more Subscriber Virtual Networks.
- Extranet Policy is available from Catalyst Center 2.3.5.3. Requires LISP Pub/Sub Control Plane.



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 Broadcast, unknown-unicast and multicast flooding. Be mindful of loop prevention.



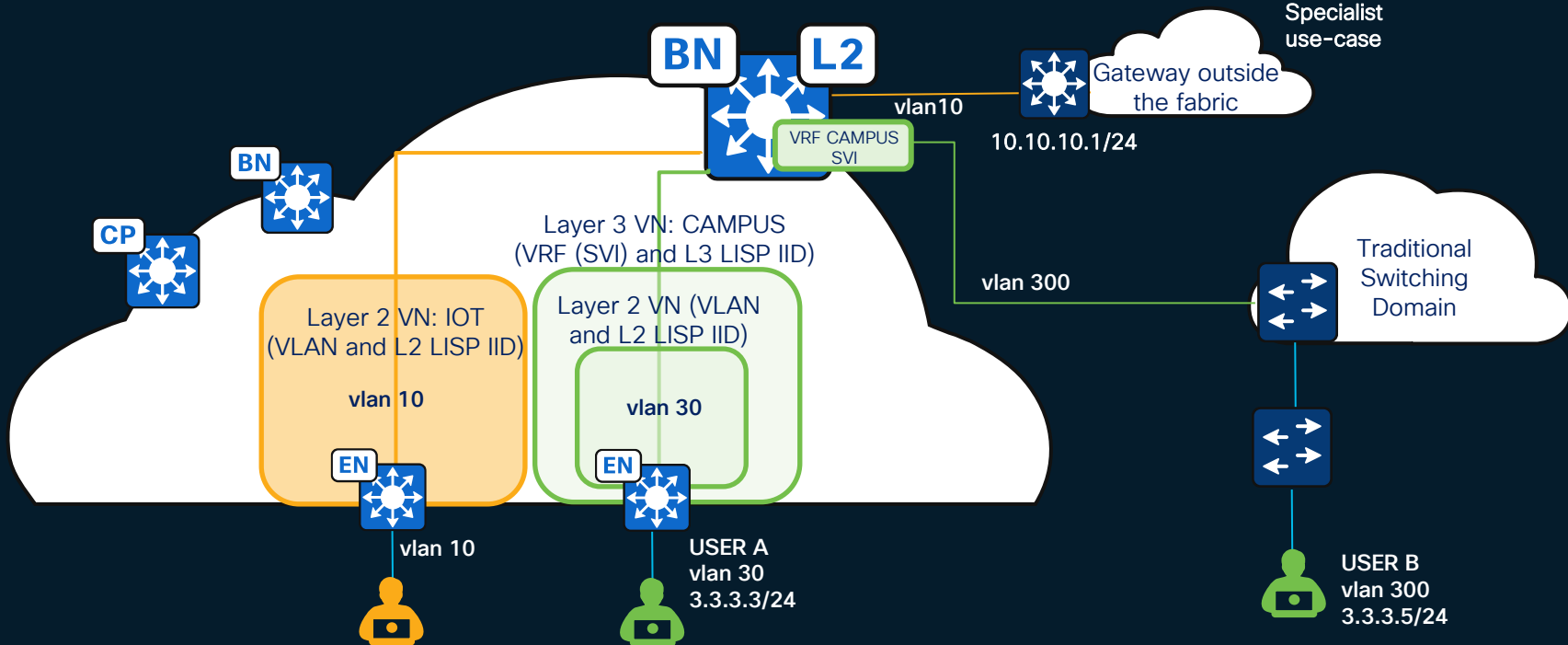
Layer 2 Virtual Networks

- CISCO** *Live!*



Layer 2 Handoff

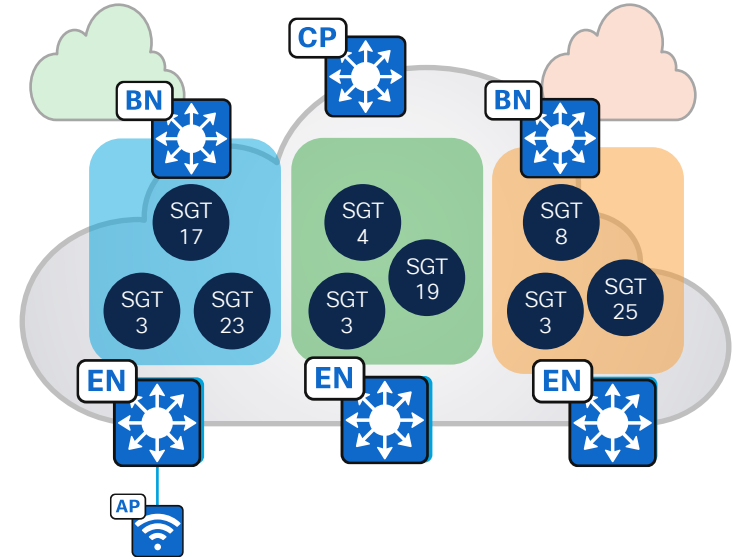
Layer 2 Virtual Networks handoff through a user-defined VLAN



Cisco SD-Access Fabric

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

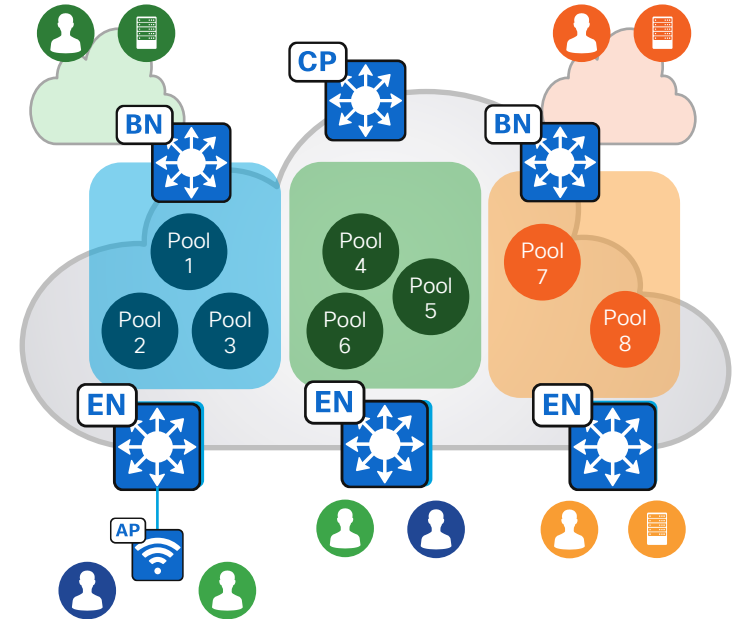
- Edge Nodes and Fabric APs assign a unique Security Group Tag (SGT) to each endpoint in concert with ISE.
- Edge Nodes and Fabric APs add an SGT to the fabric encapsulation.
- SGTs are used to implement IP-address-independent traffic policies.
- SGTs can be extended to numerous other networking technologies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



Cisco SD-Access Fabric

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

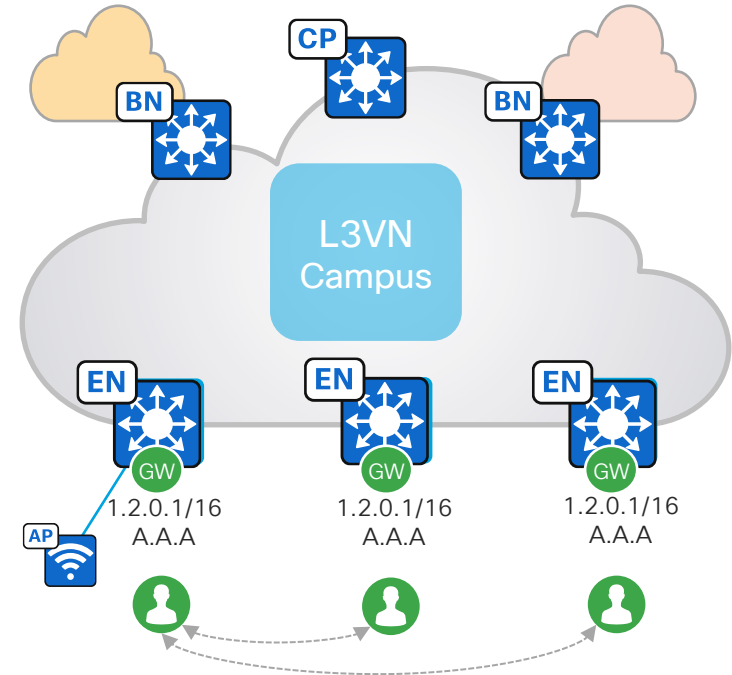
- Edge Nodes instantiate an access VLAN and a Switched Virtual Interface (SVI) with user-defined IPv4/IPv6 addresses per Host Pool.
- Host Pools assigned to endpoints dynamically by AAA or statically per port.
- Edge Nodes and Fabric WLCs register endpoint IDs (/32, /128 or MAC) with the Control Plane,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



Cisco SD-Access Fabric

Anycast Gateway Provides a Default Gateway for IP-Capable Endpoints

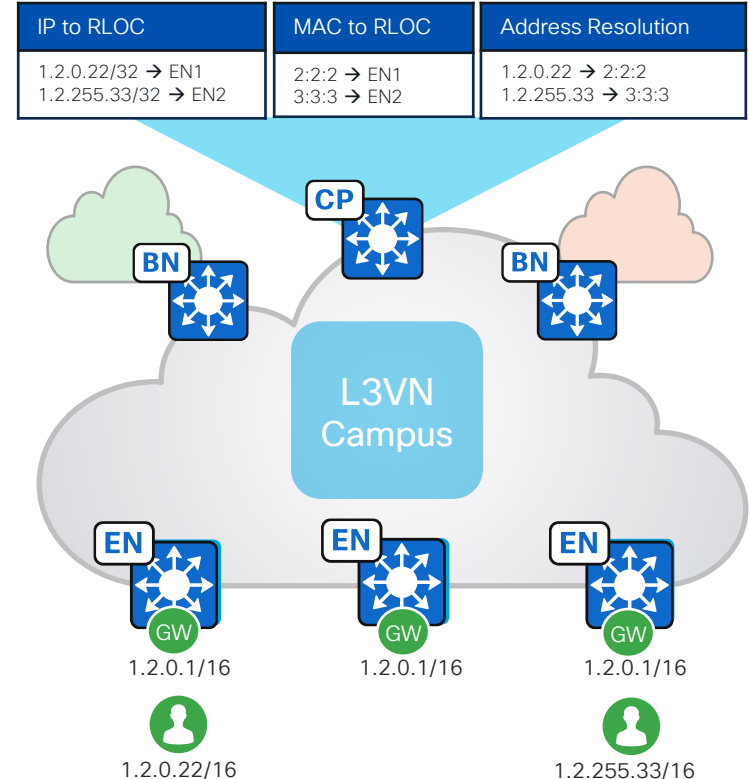
- Similar principle and behavior to FHRP with a shared virtual IPv4/IPv6 addresses and MAC address.
- The same Switch Virtual Interface (SVI) is present on all Edge Nodes with the same virtual IP and MAC.
- The wired or wireless endpoint can connect to any switch or AP in the fabric and communicate with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



Cisco SD-Access Fabric

Host Pools are “stretched” via the Overlay

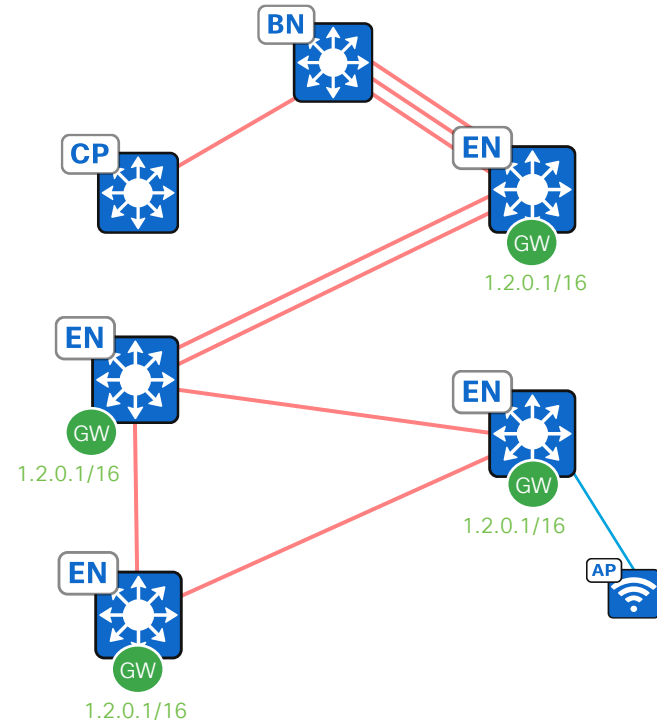
- Endpoint IPv4/IPv6 traffic arrives on an Edge Node and is then routed or switched by the Edge Node.
- Fabric Dynamic EID mapping allows endpoint-specific (/32, /128, MAC) advertisement and mobility.
- No longer need VLANs to interconnect endpoints across Edge Nodes, this happens in the Overlay without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



Cisco SD-Access Fabric

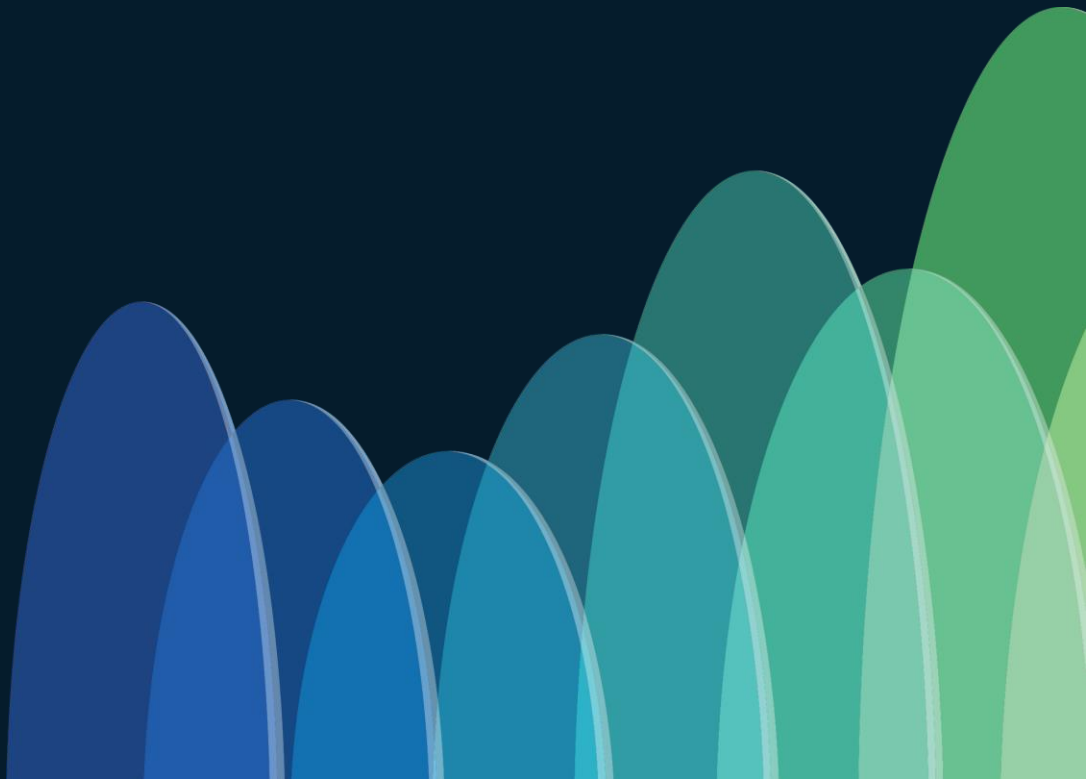
Accommodates any Physical Network Topology

- Overlays are agnostic to underlay physical topology.
- Any wired or wireless endpoint address anywhere, including environments with unusual cabling implementations.
- Routed underlay IGP takes care of load balancing and fast link/node fault convergence. Obsoletes less robust mechanisms like L2 Trunking and STP.



Fabric Fundamentals

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



Cisco SD-Access Fabric

Control Plane: LISP

- Locator/ID Separation Protocol.
- IETF Standards Track RFC9299-RFC9306 and RFC9347.
- IETF LISP Drafts.

Lightweight, Efficient, Scalable and
Extensible

Cisco SD-Access Fabric

Why LISP?

Scalable

Pull model • No massive routing tables • Creates 'DNS' for routing • Conversational learning • Massive Scalability • BGP and IGPs cannot scale like LISP • Purpose-built for scale • Address-Family Agnostic

Efficient

Supports IPv4, IPv6, and MAC Address Families • Wired and Wireless Unification • WLC participates in LISP control plane communication. • Wired and Wireless endpoints have policy applied at same point in the network. Host Mobility • Native support for this capability • Wired and Wireless Extensibility

Extensible

LISP Canonical Address Format (LCAF) allows for encoding of additional information beyond simply Address-Families • LISP has been actively developed, optimised, and enhanced for the last ten years.

Cisco SD-Access Fabric

Control Plane: Locator/ID Separation Protocol (LISP)

2022

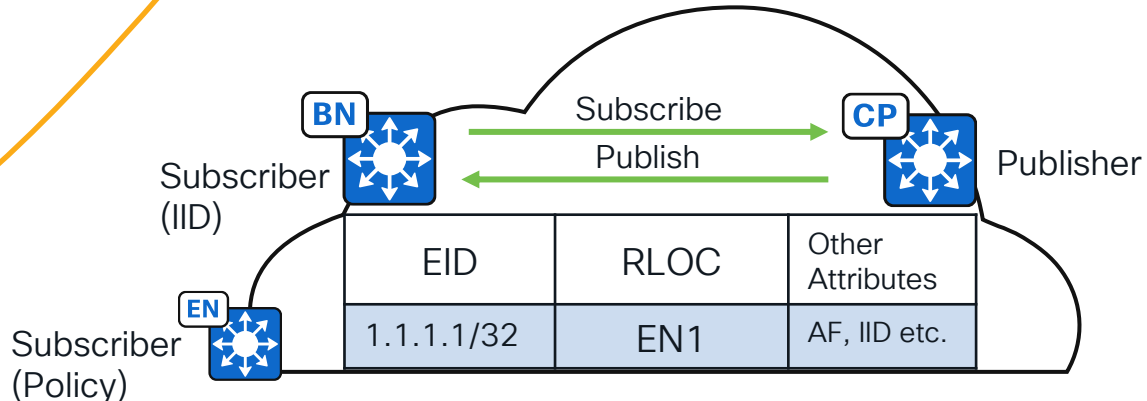
LISP Pub/Sub

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

LISP/BGP

Reliable and stable.
BGP transport.

2017

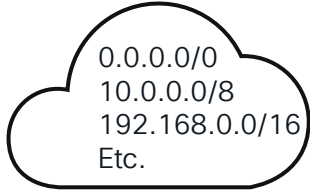


Fabric Operation

LISP Pub/Sub Walkthrough

Fabric Operation

Default ETR Registration

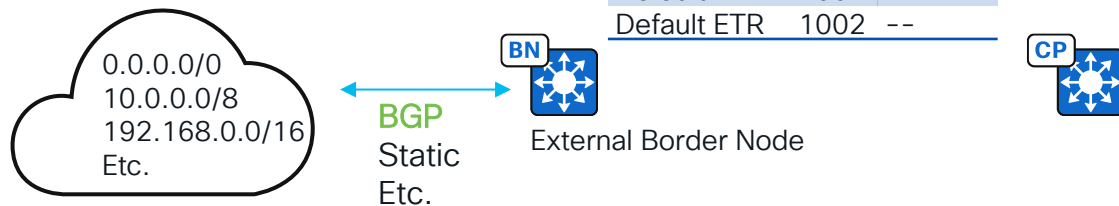


External Border Node



Fabric Operation

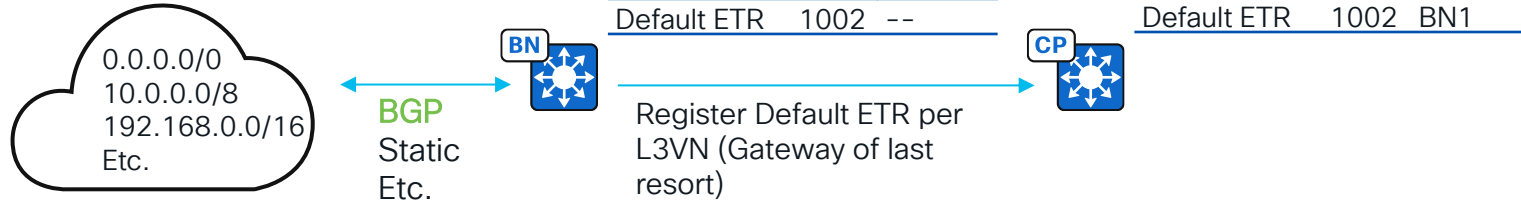
Default ETR Registration



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

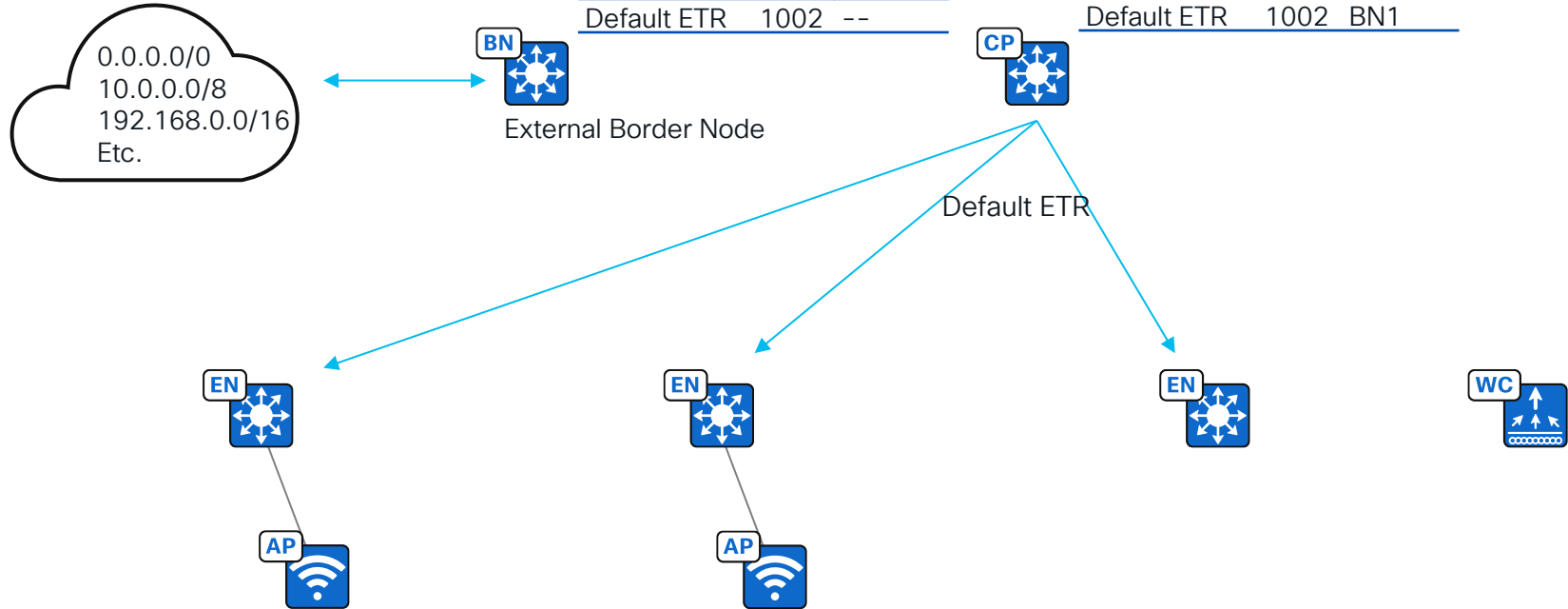
Fabric Operation

Default ETR Registration



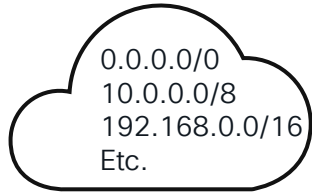
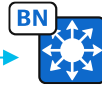
Fabric Operation

Edge Node Bootstrap



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



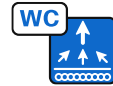
Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1



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

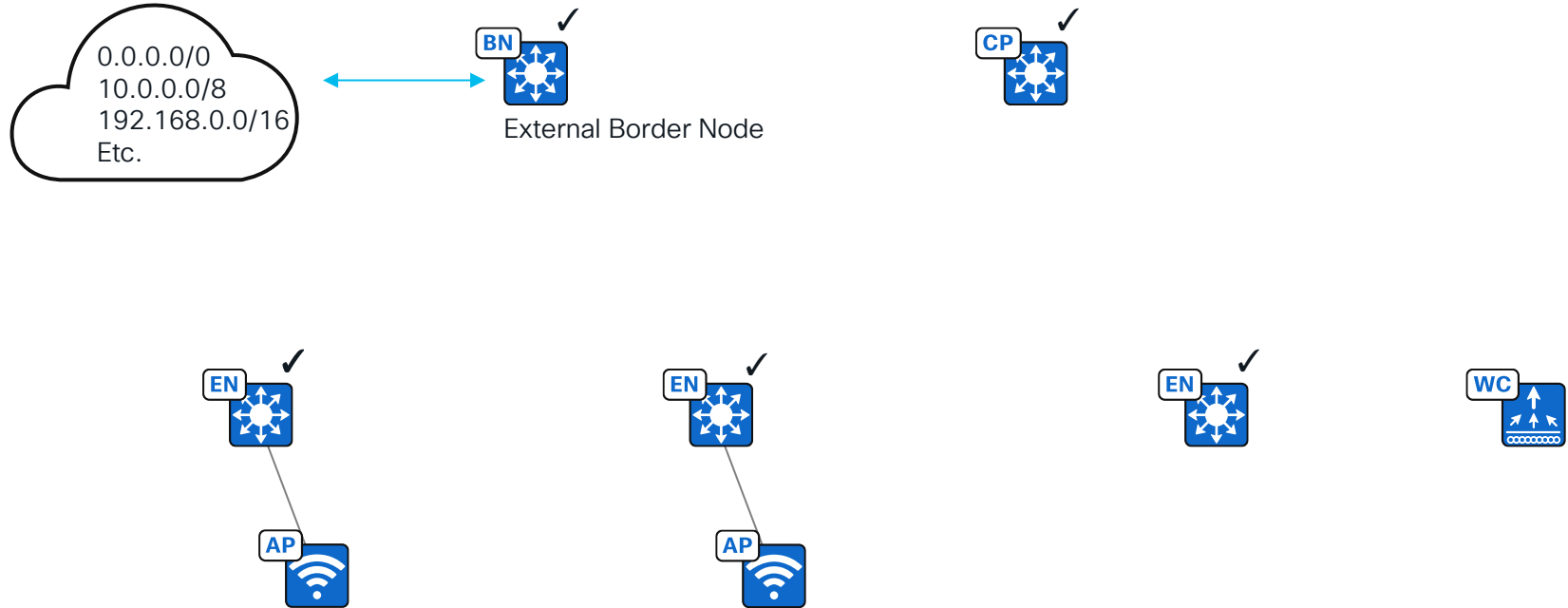


Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1



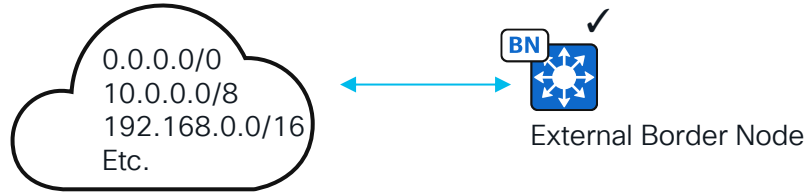
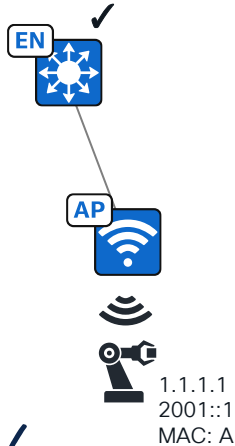
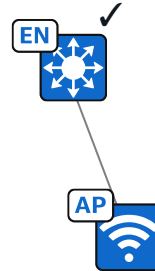
Fabric Operation

Edge Node Bootstrap

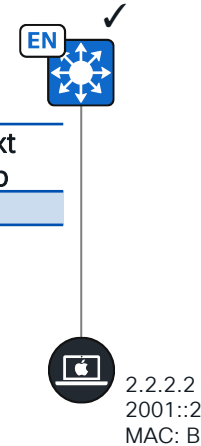
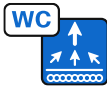


Fabric Operation

Endpoint Registration



Destination	IID	Next Hop
2.2.2.2	1001	--

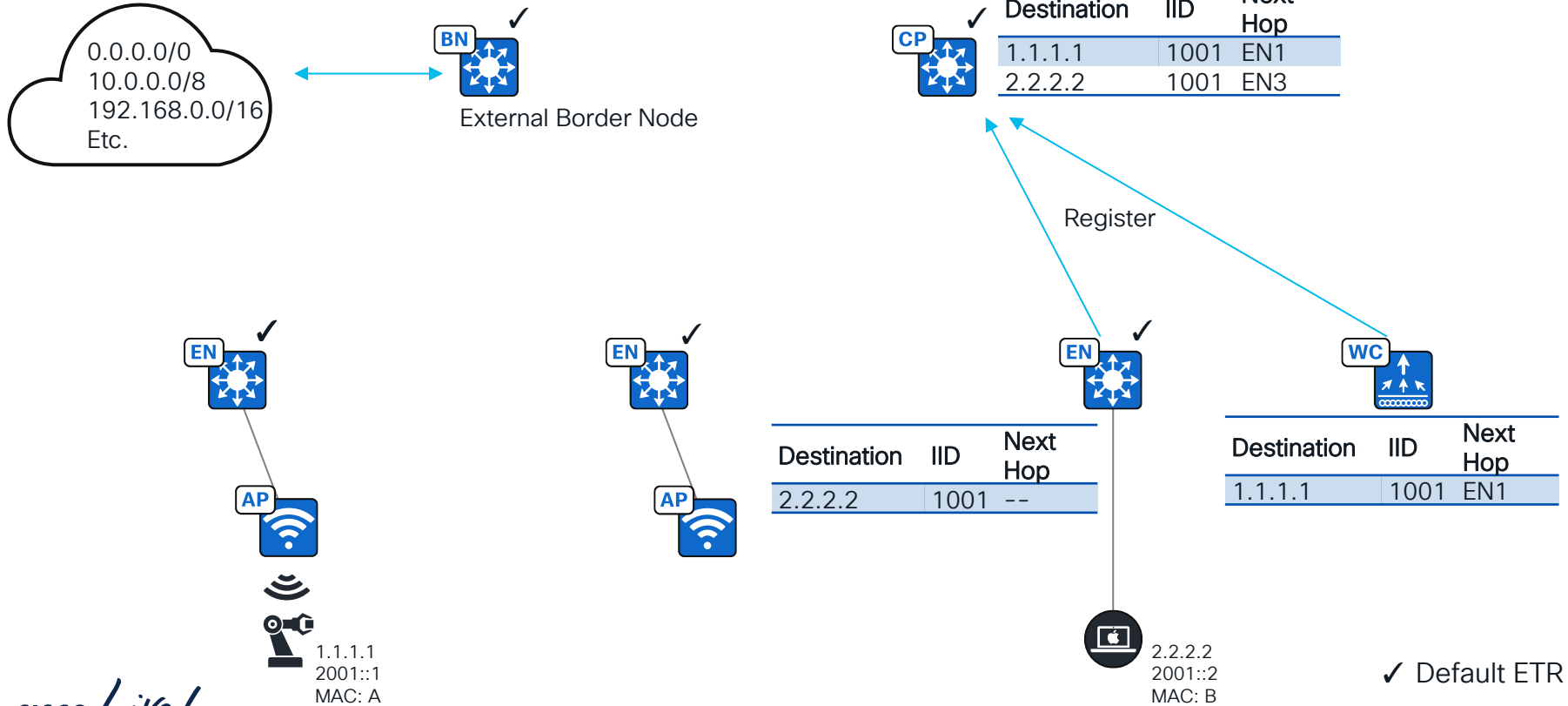


Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

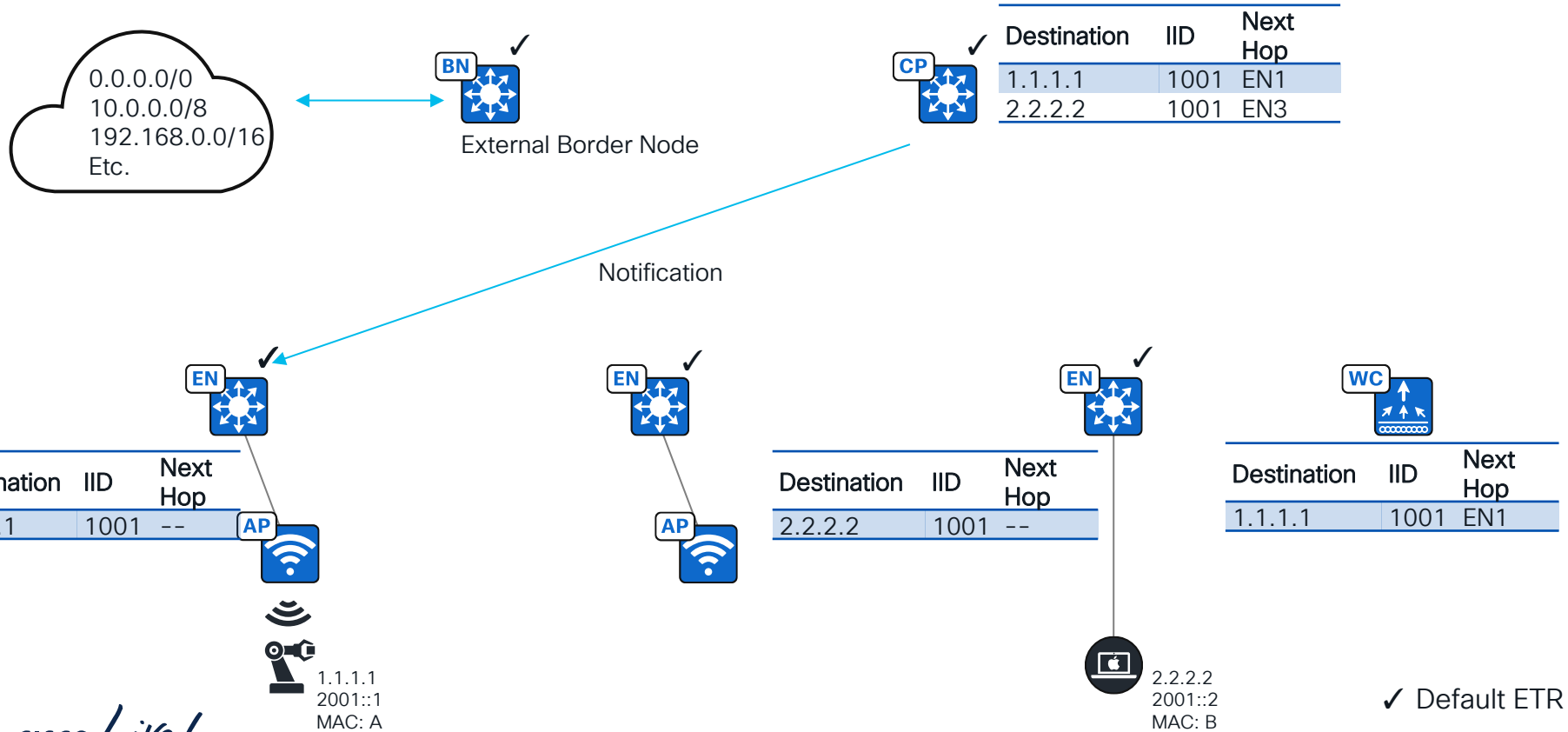
Fabric Operation

Endpoint Registration



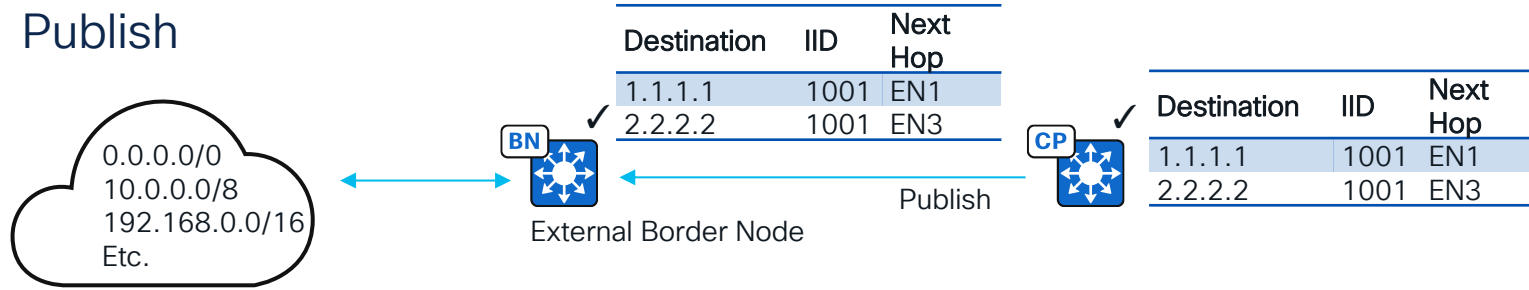
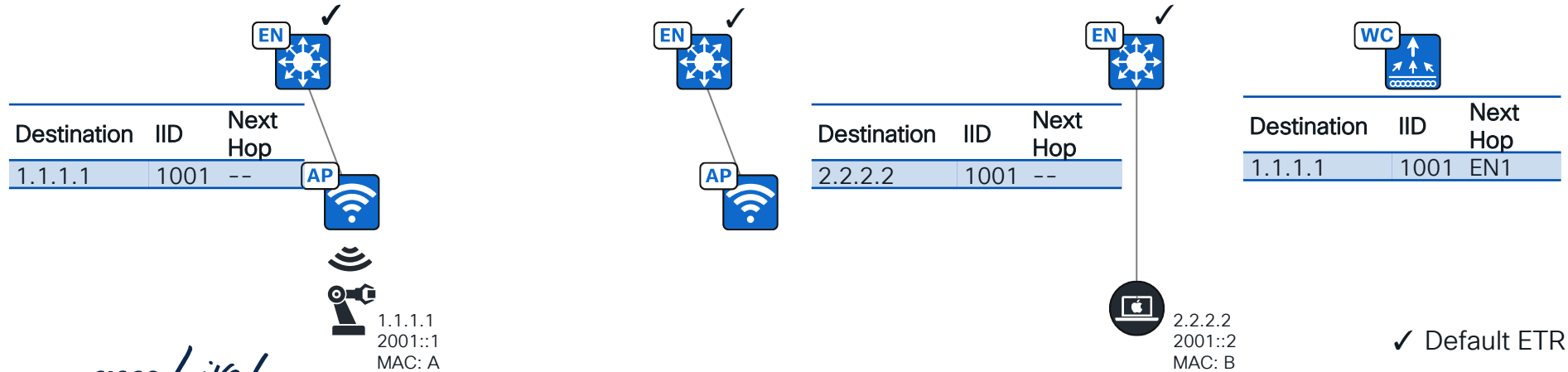
Fabric Operation

Endpoint Registration



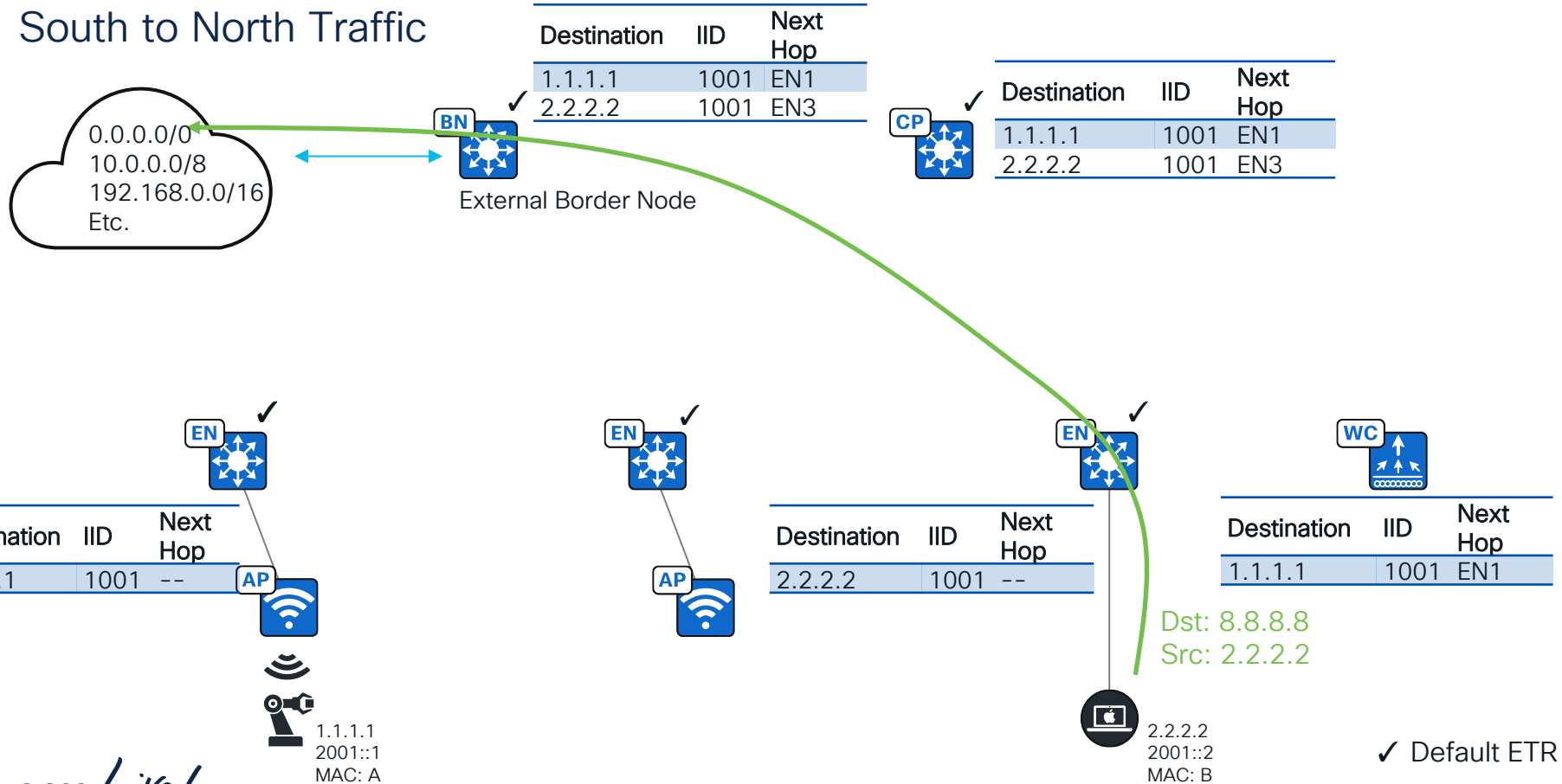
Fabric Operation

Publish



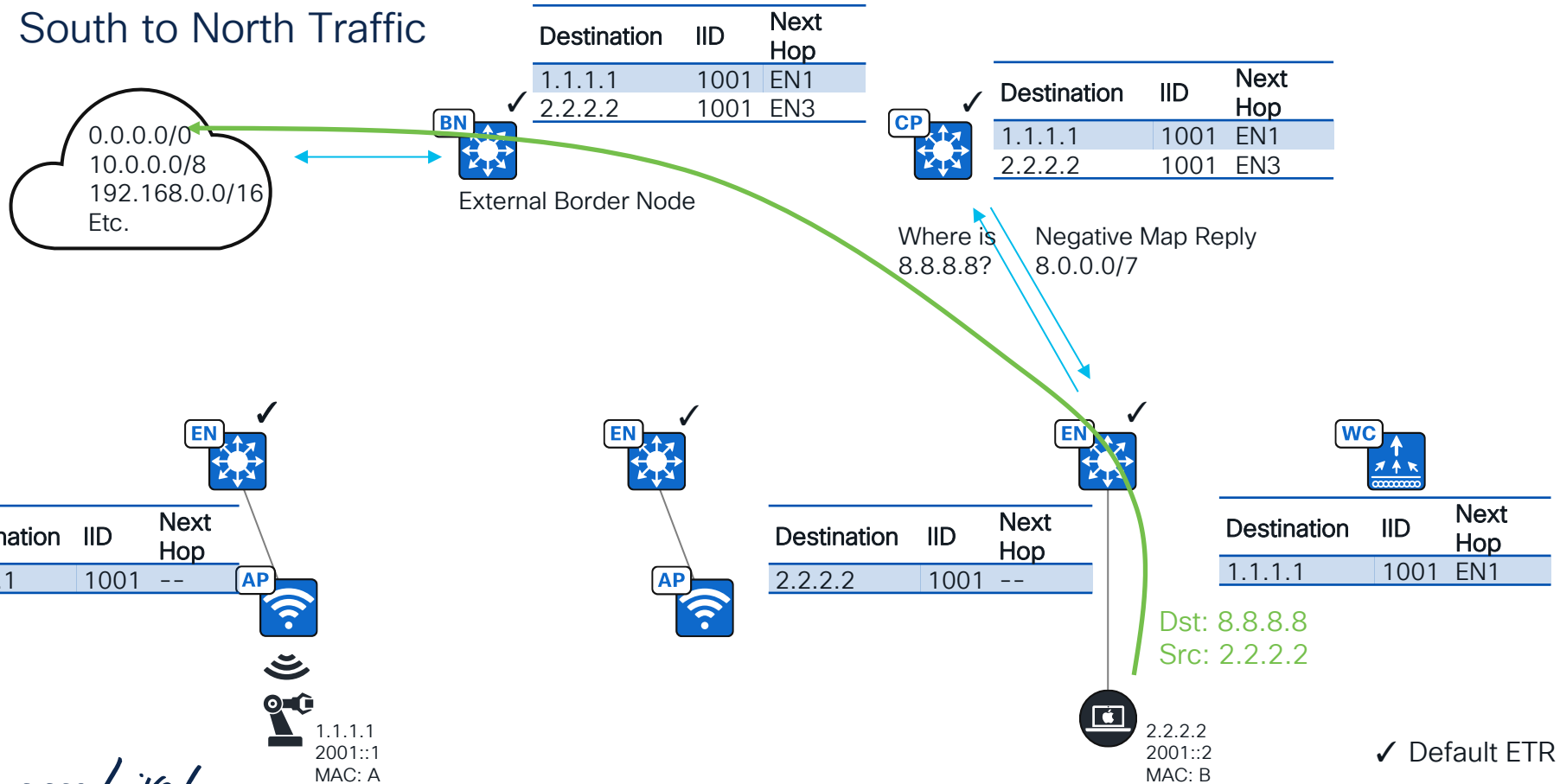
Fabric Operation

South to North Traffic



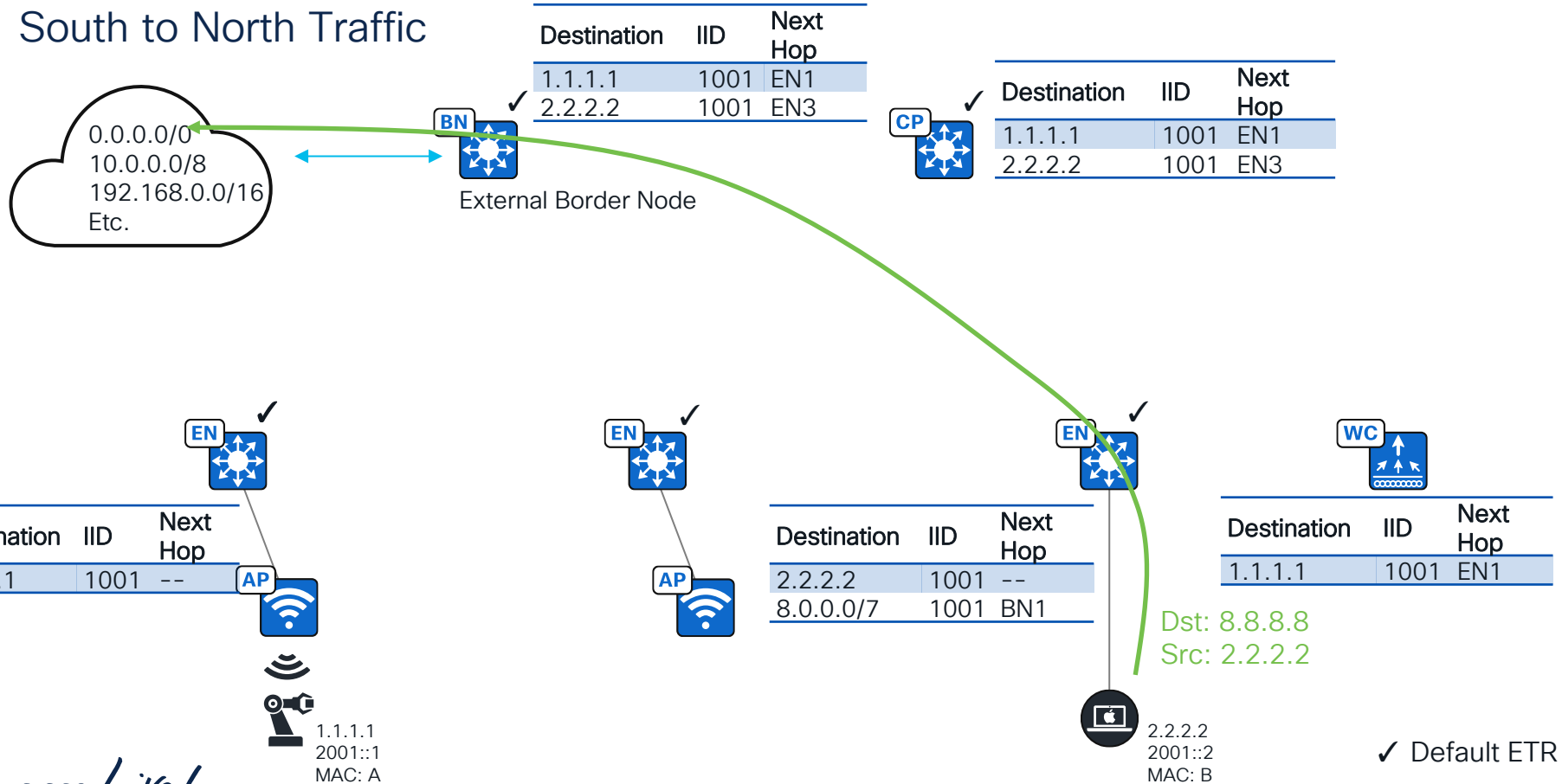
Fabric Operation

South to North Traffic



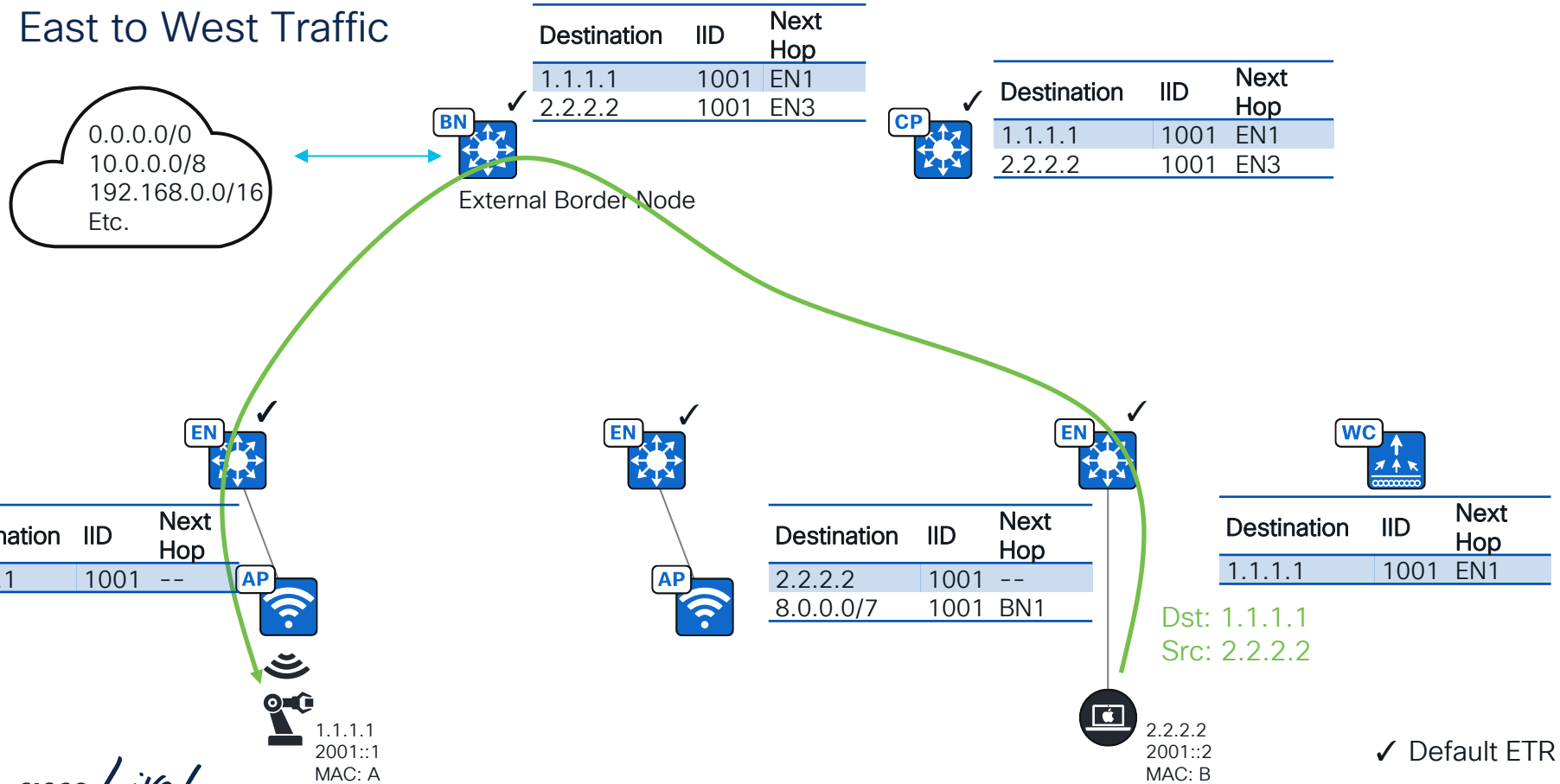
Fabric Operation

South to North Traffic



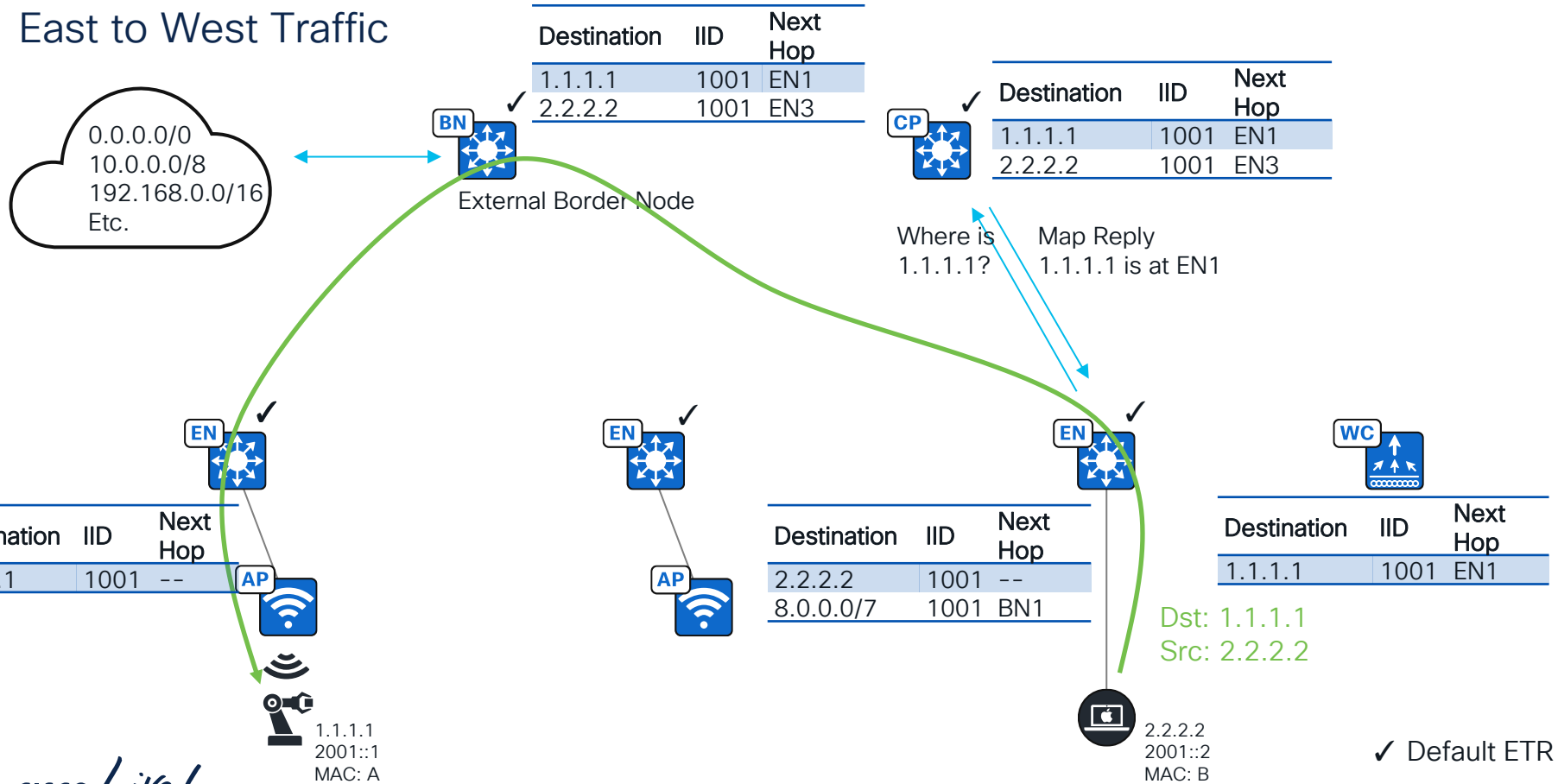
Fabric Operation

East to West Traffic



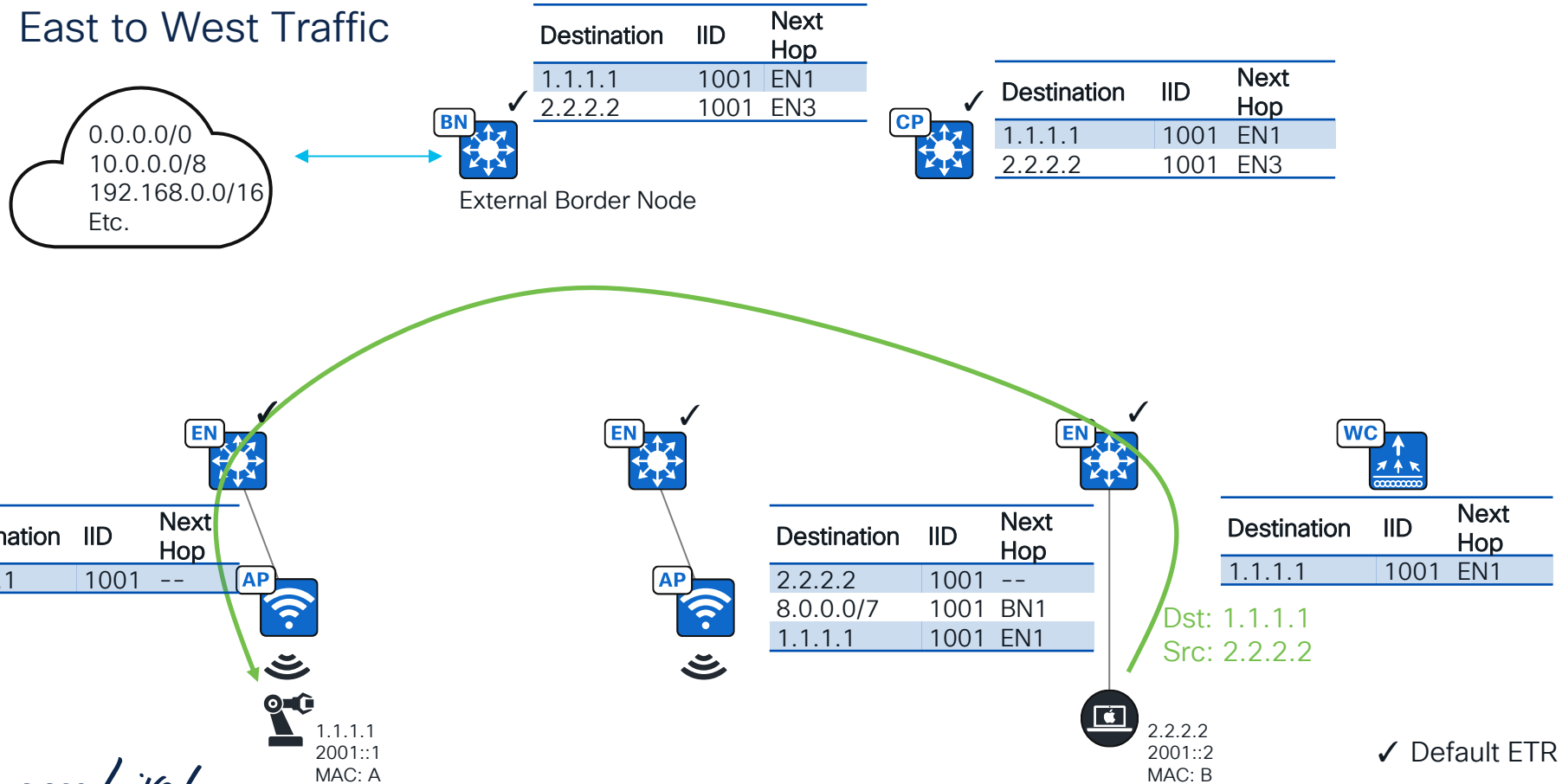
Fabric Operation

East to West Traffic



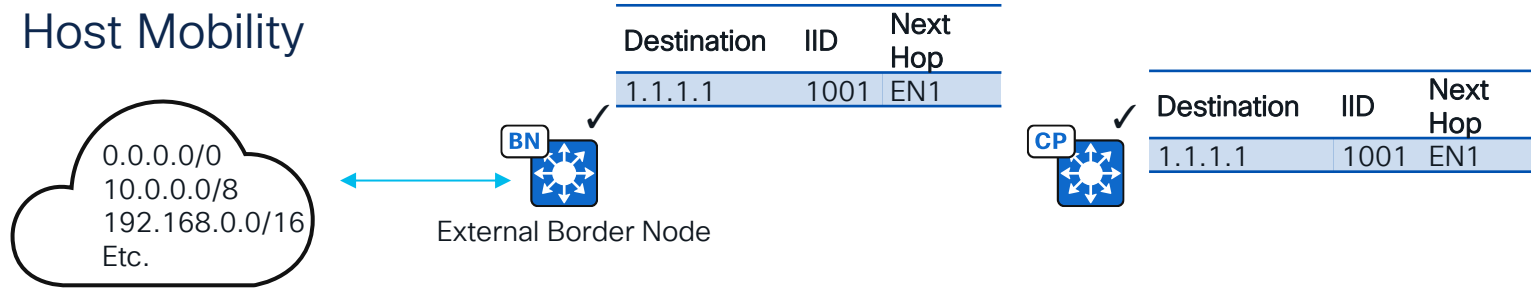
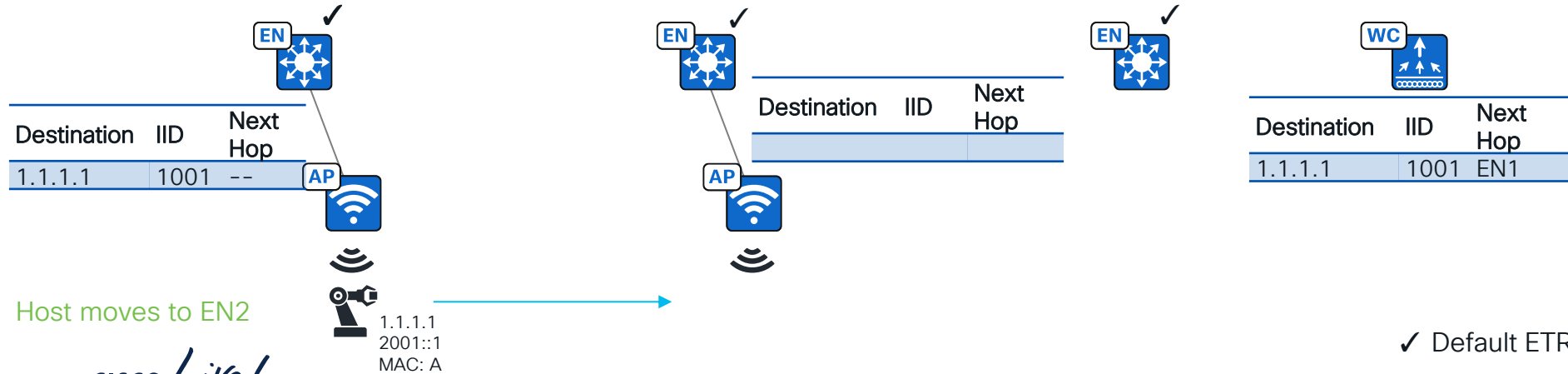
Fabric Operation

East to West Traffic



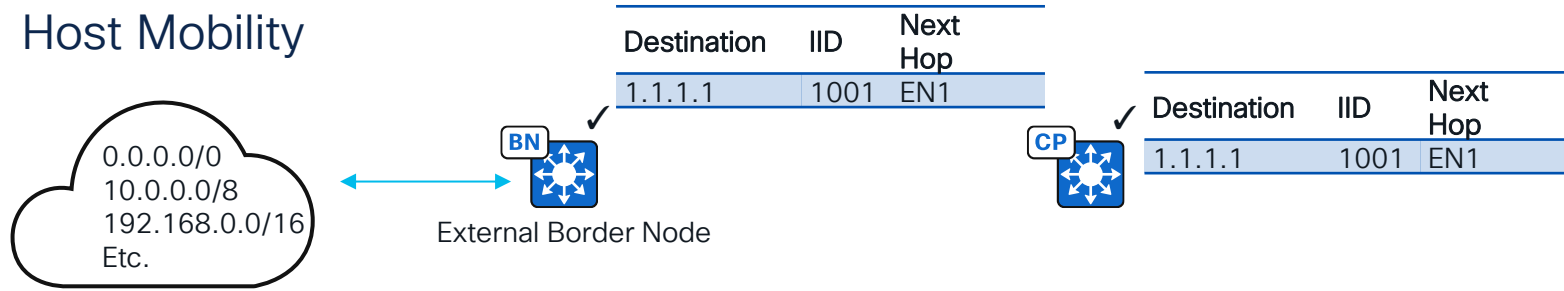
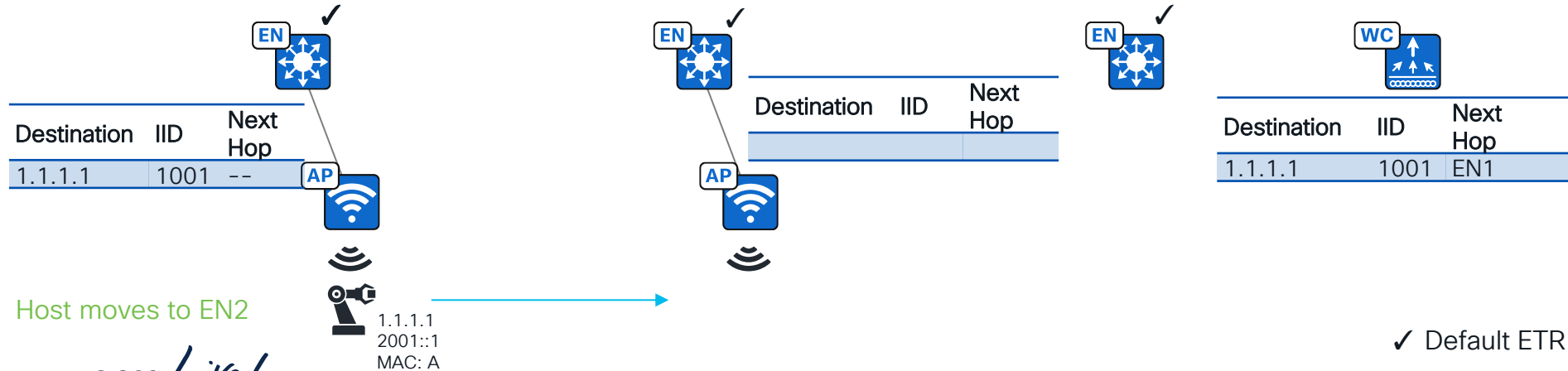
Fabric Operation

Host Mobility



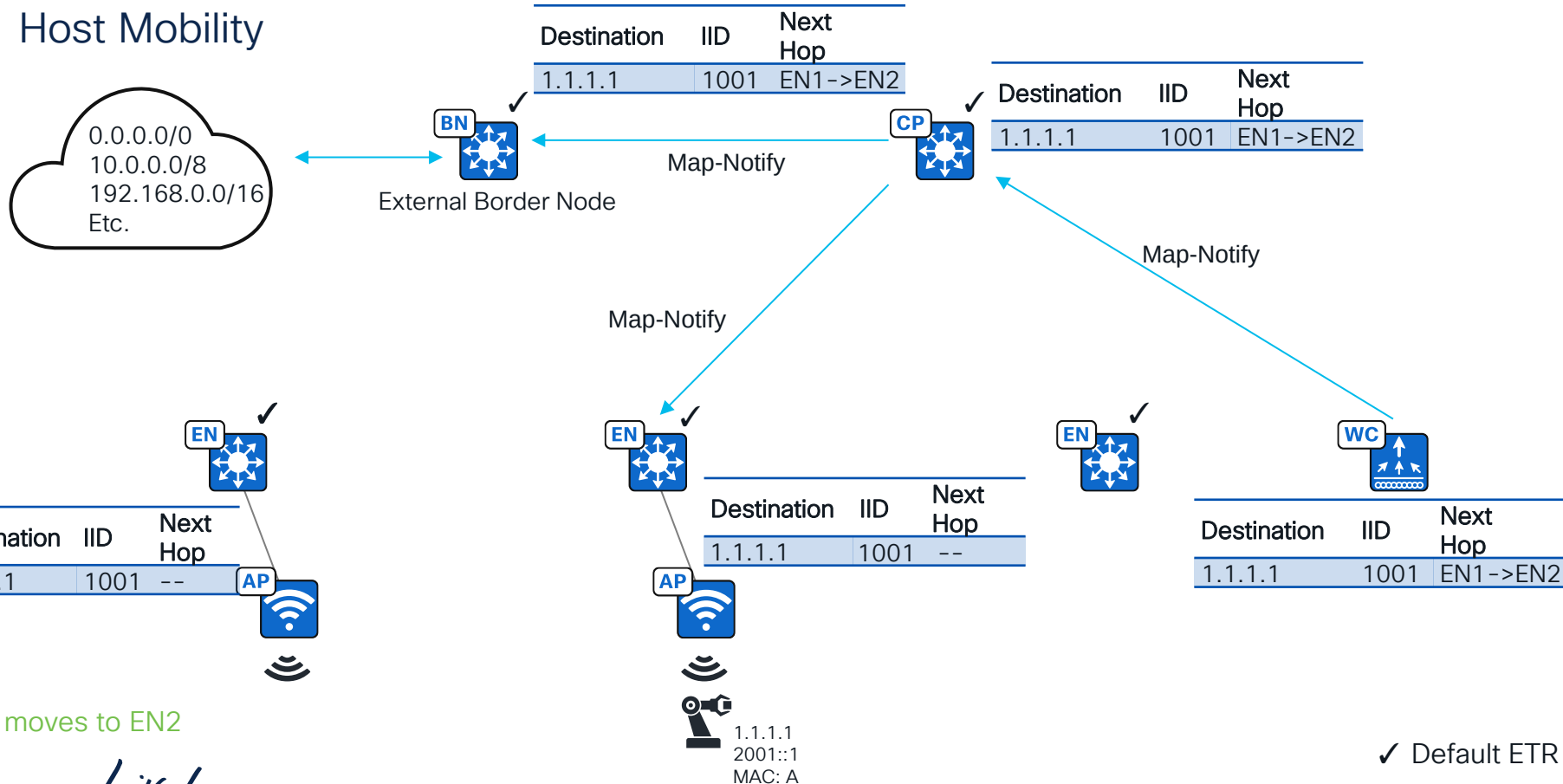
Fabric Operation

Host Mobility



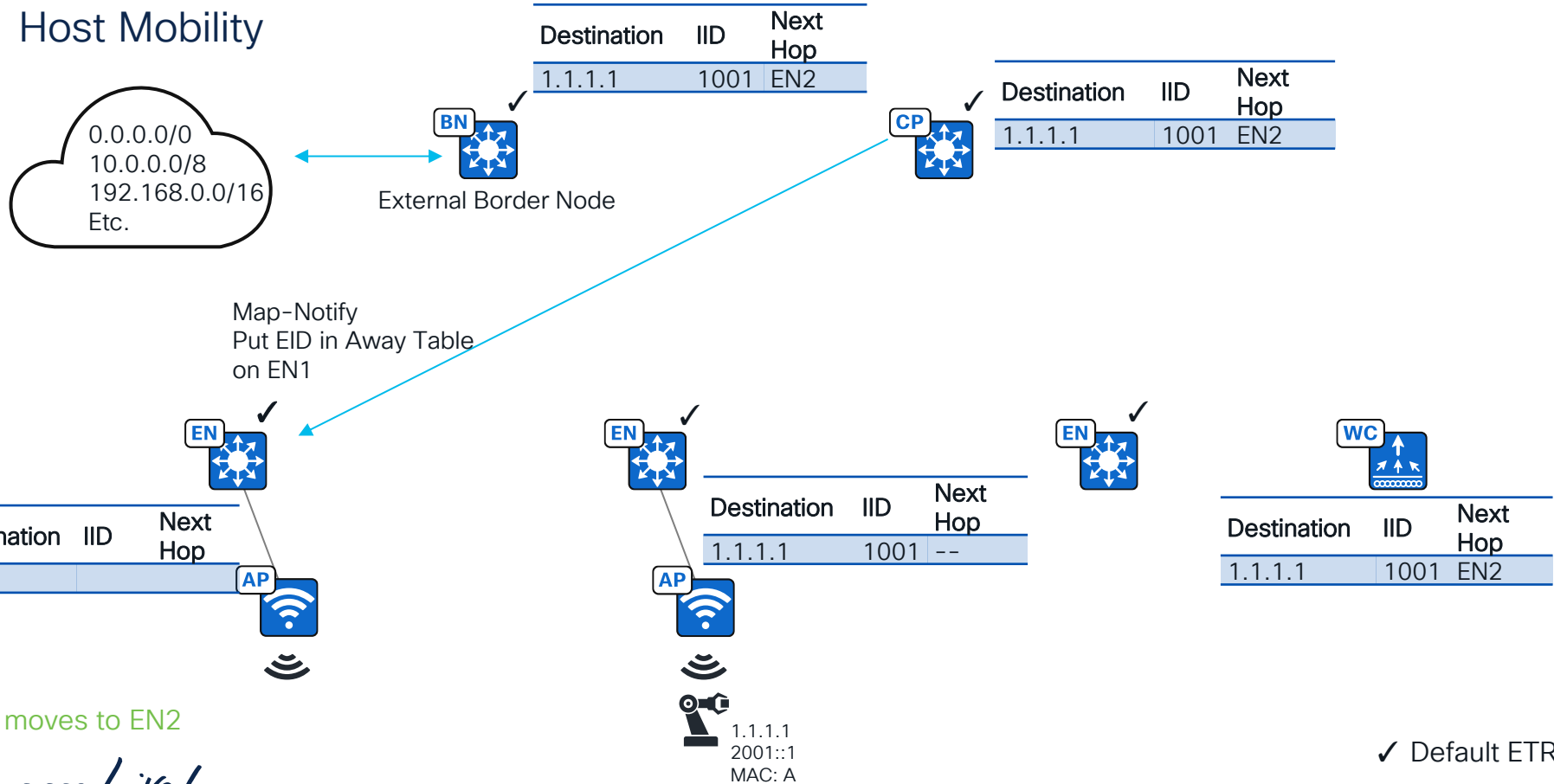
Fabric Operation

Host Mobility



Fabric Operation

Host Mobility

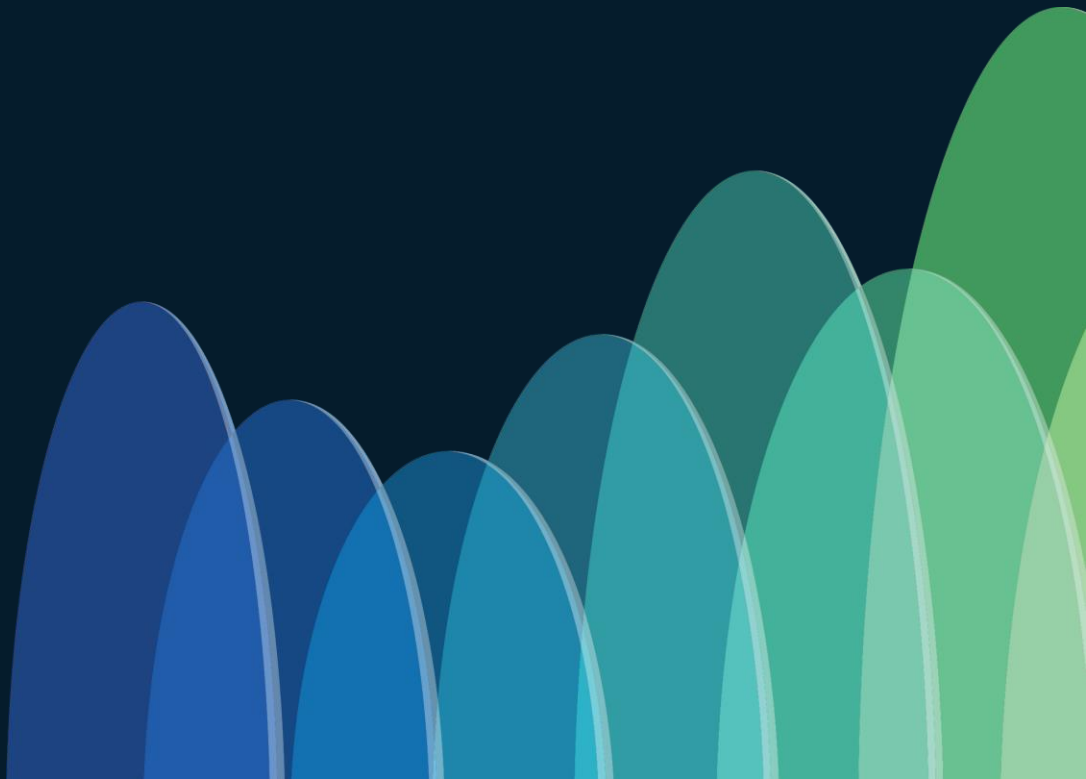


Advantages of LISP

- 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.

Fabric Fundamentals

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



Cisco SD-Access Fabric

Data Plane: VXLAN

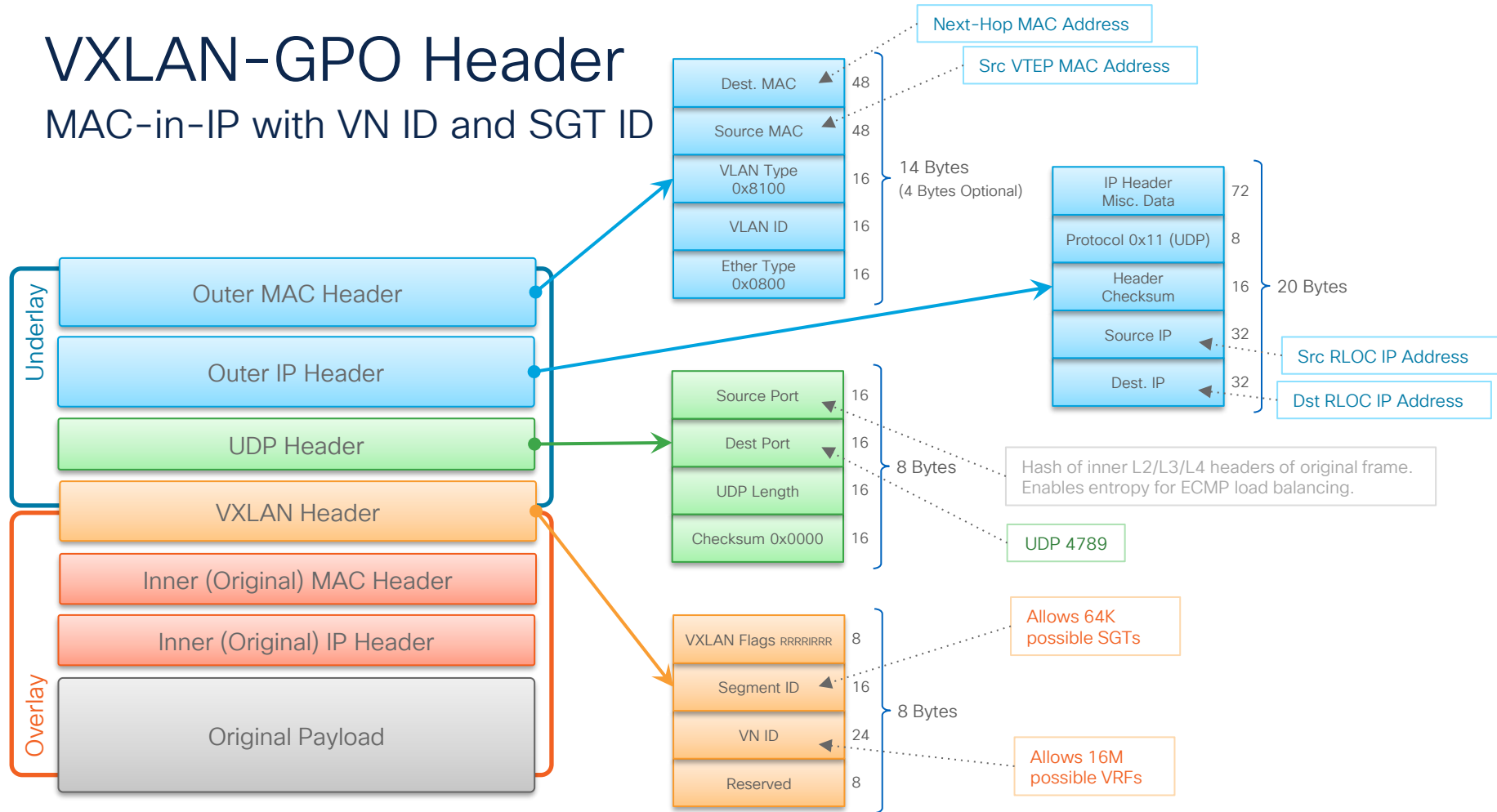
1. Control Plane: LISP
2. Data Plane: VXLAN



Supports L2
& L3 Overlay

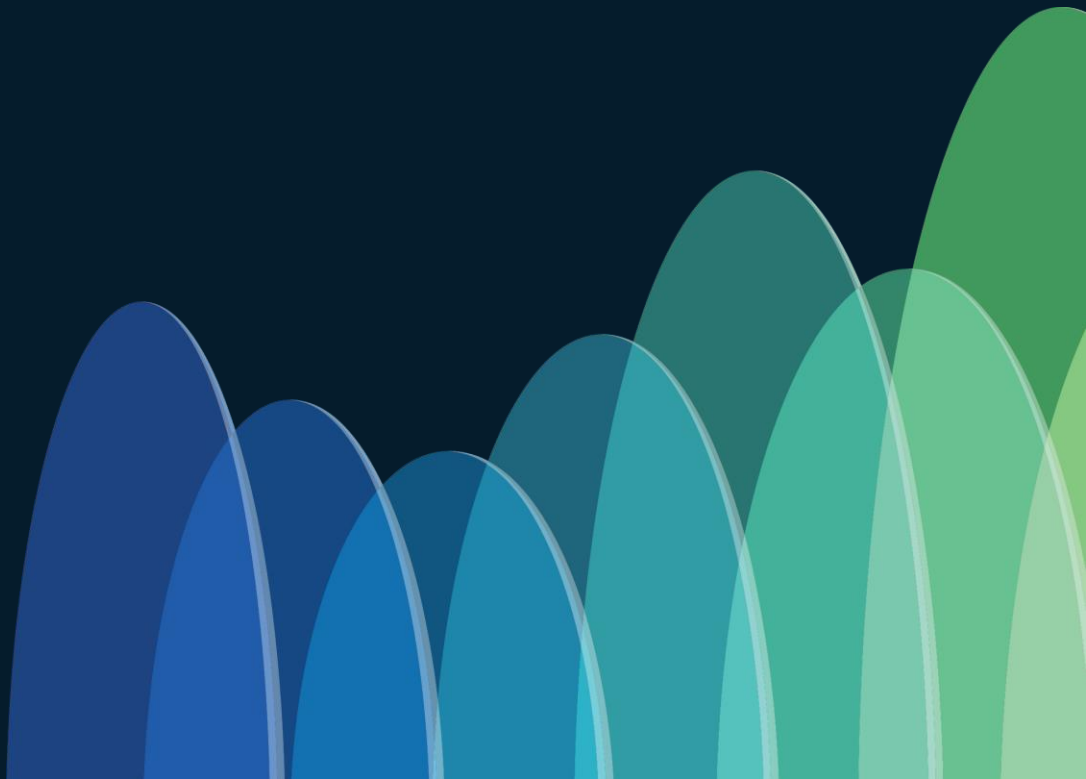
VXLAN-GPO Header

MAC-in-IP with VN ID and SGT ID



Fabric Fundamentals

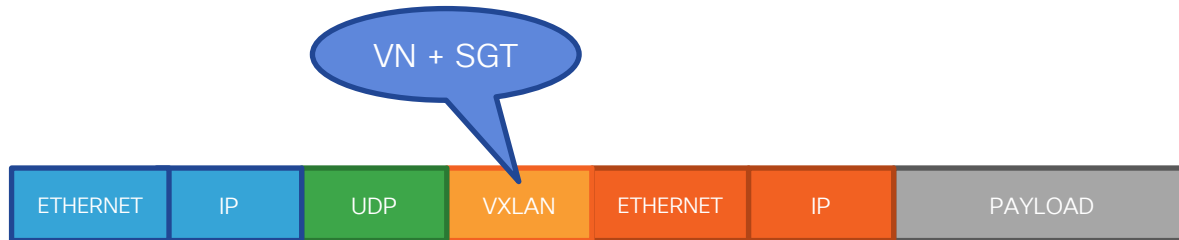
1. Control Plane
2. Data Plane
3. Policy Plane



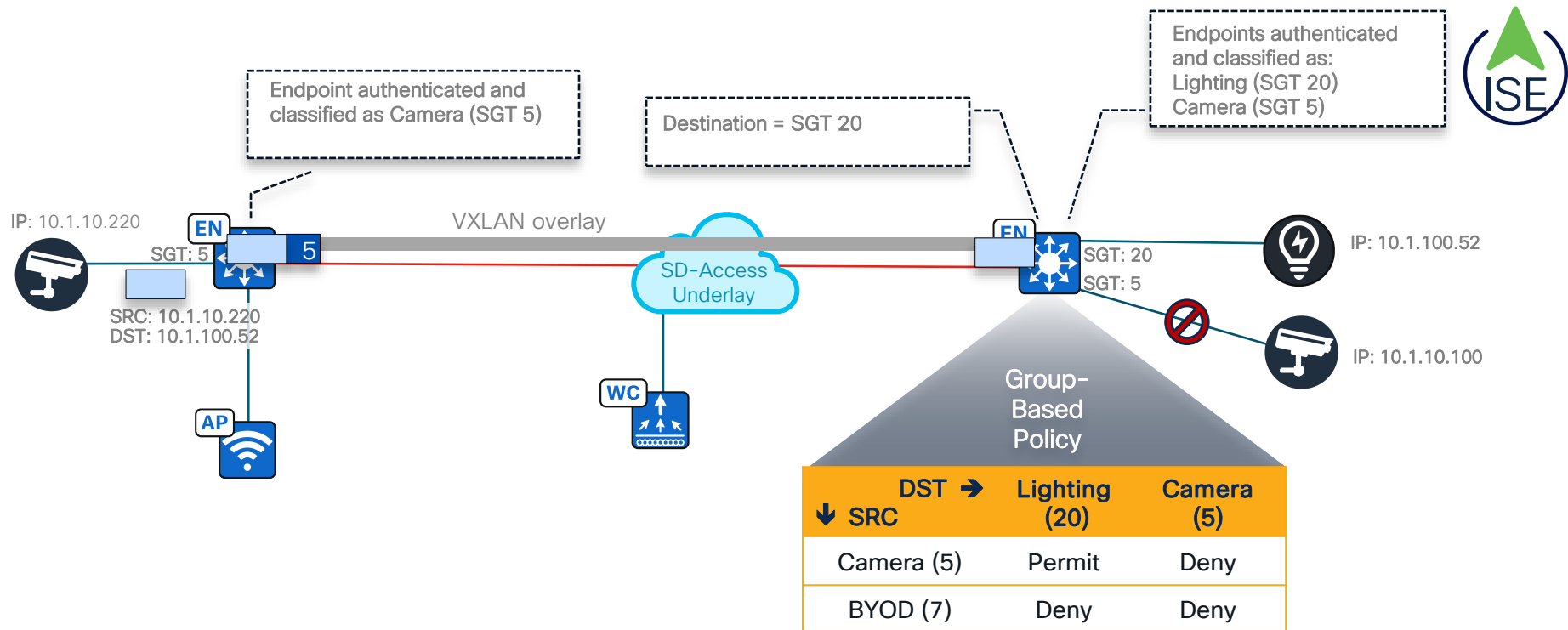
Cisco SD-Access Fabric

Policy Plane: Group-Based Policy

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

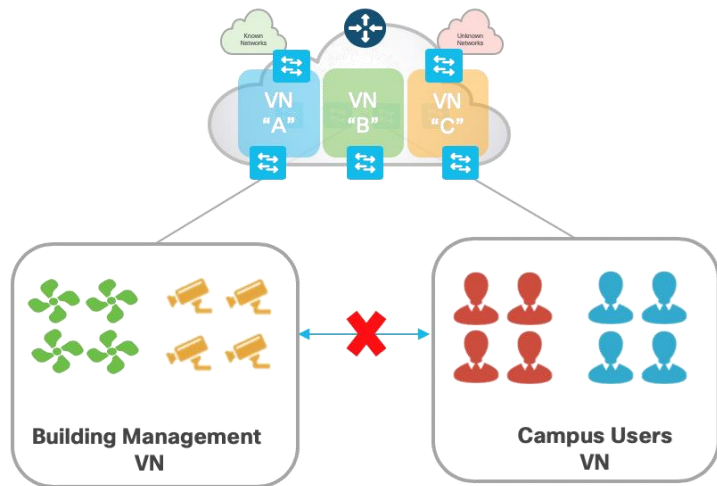


What is Security Group Tag and Group-Based Policy?



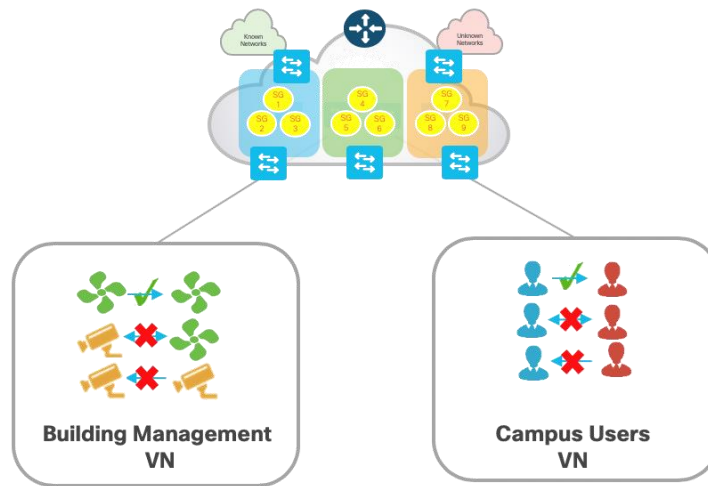
SD-Access Policy

Macro-Segmentation and Micro-Segmentation



Virtual Network (VN)

First-level segmentation ensures **zero communication** between forwarding domains. Ability to consolidate multiple networks into one physical network.

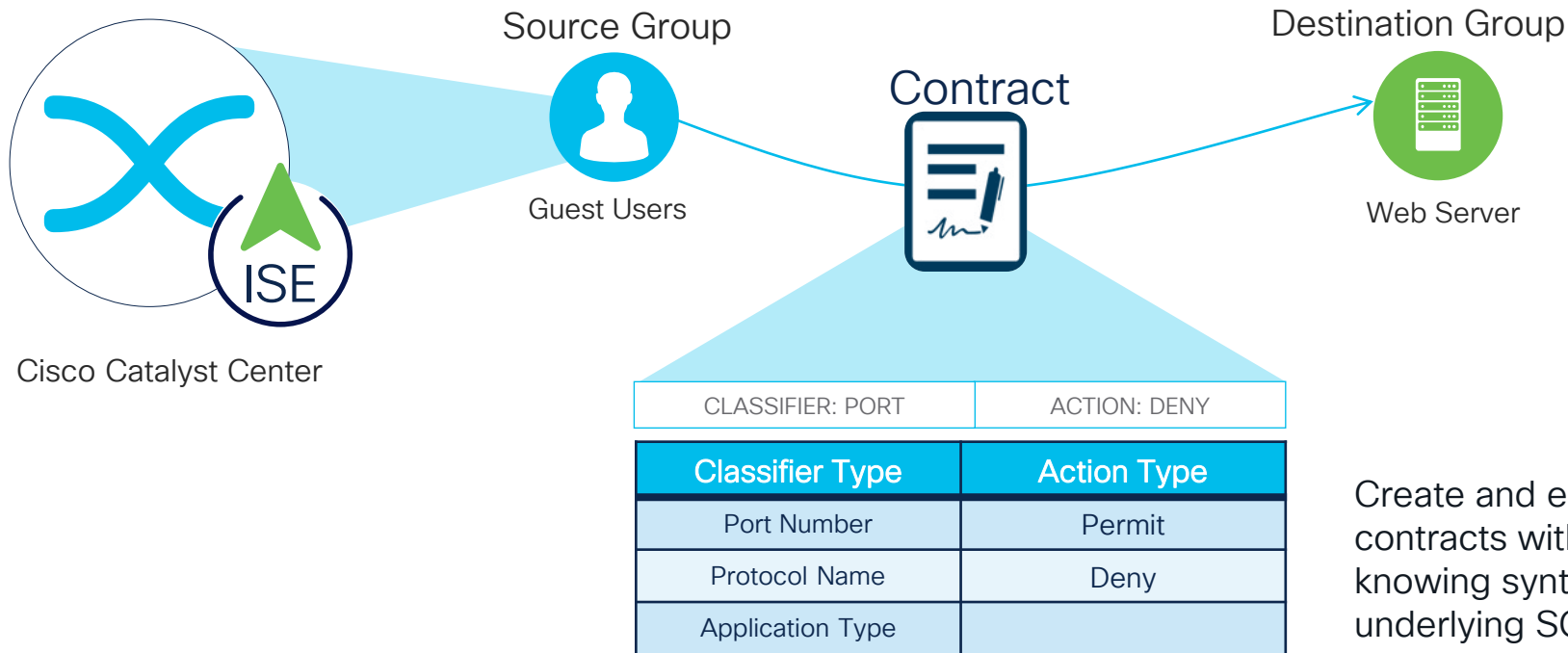


Security Group Tag (SGT)

Second-level segmentation ensures **Group-Based Access Control** between groups in a VN. Ability to segment per endpoint based on minimum necessary access (Zero Trust).

SD-Access Policy

Access Control Policies



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

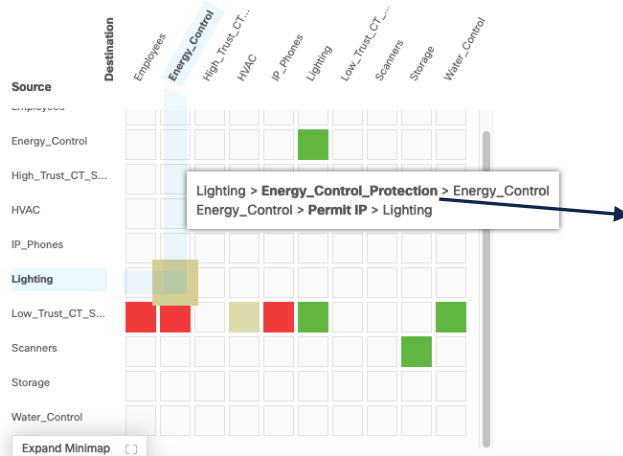
SD-Access Policy

Group-Based Access Control

Policies (11) [Enter full screen](#)

[Filter](#) [Deploy](#) [Refresh](#)

☒ Permit ☐ Deny ☐ Custom ☐ Default



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

Access Contract

Name: Energy_Control_Protection
Description:

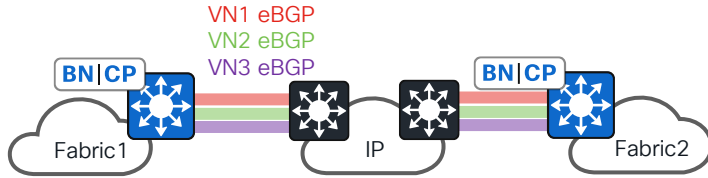
CONTRACT CONTENT (1)

#	Action	Application	Transport Protocol	Source / Destination	Port	Logging
1	Permit	https	TCP/UDP	Destination	443/443	OFF

Default Action: Permit
Logging: OFF

Multiple Fabrics

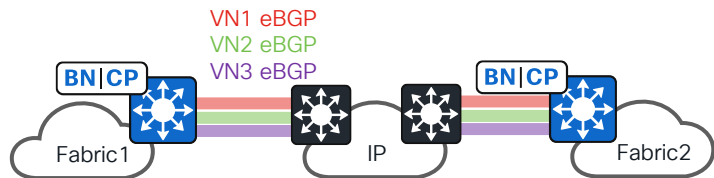
Transits, VN and SGT Preservation



IP-Based Transit

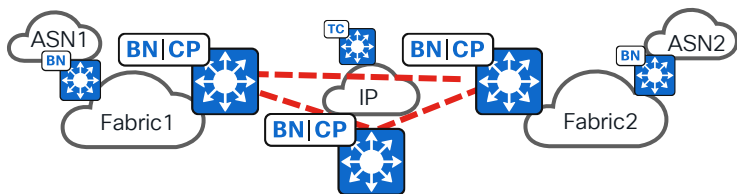
- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.

Transits, VN and SGT Preservation



IP-Based Transit

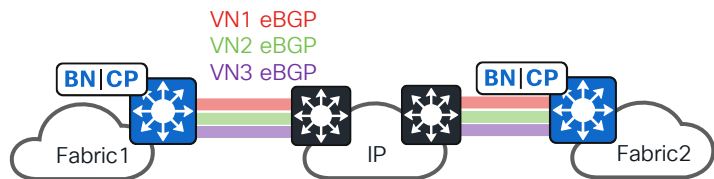
- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.



SD-Access Transit

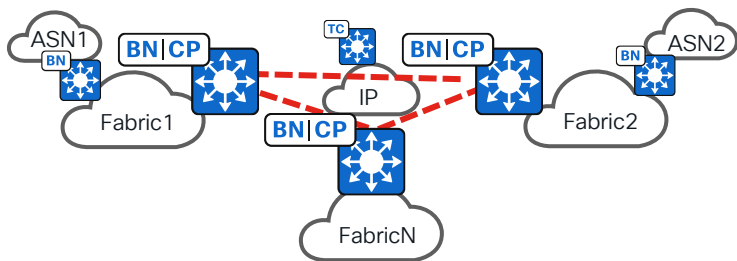
- SD-Access LISP/VXLAN between Fabric Sites.
- Natively preserves Layer 3 Virtual Networks and SGTs.
- Capable of fabric as a transit between external routing domains.

Transits, VN and SGT Preservation



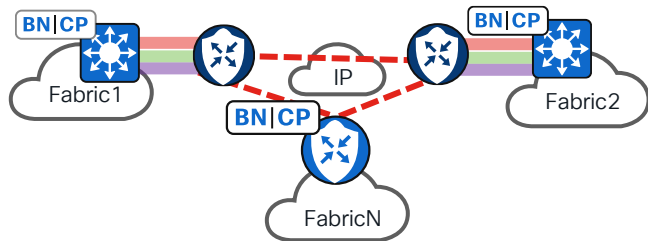
IP-Based Transit

- 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

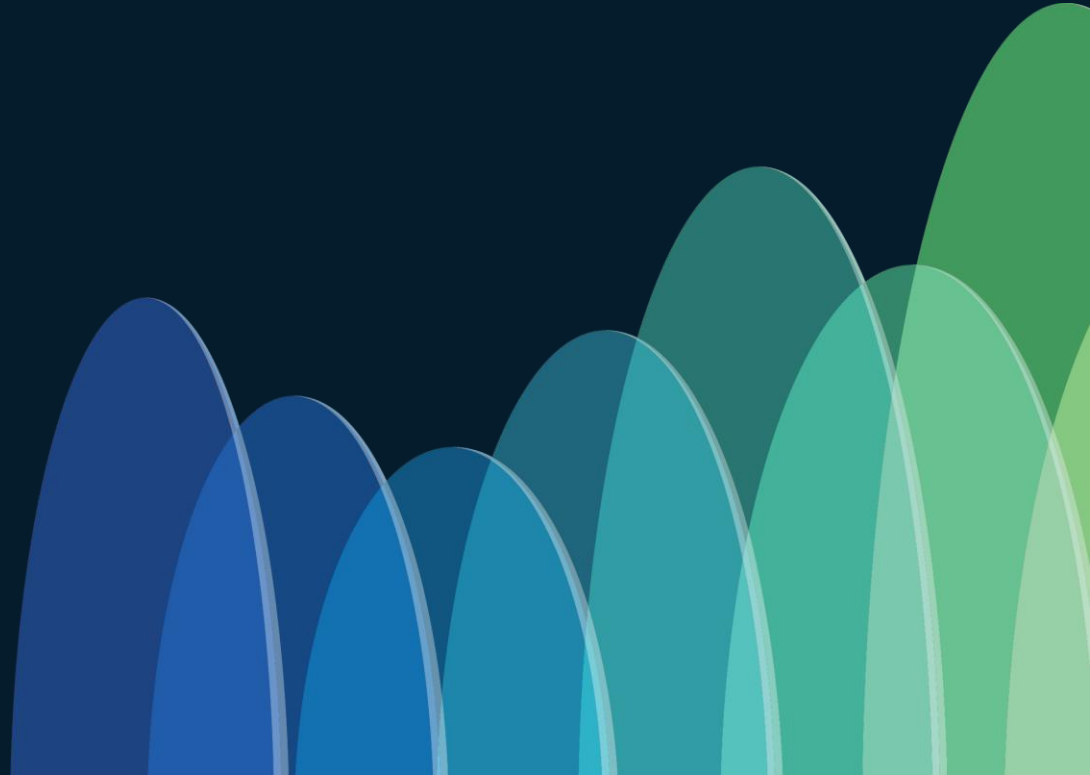
- SD-Access LISP/VXLAN between Fabric Sites.
- Natively preserves Layer 3 Virtual Networks and SGTs.
- Capable of fabric as a transit between external routing domains.



SD-WAN Transit

- Cisco SD-WAN between Fabric Sites.
- Capable of preserving Layer 3 Virtual Networks and SGTs.
- Dedicated SD-WAN Edge for design flexibility, Border Node port densities and port speeds. See [Independent Domains Prescriptive Deployment Guide](#).

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.

Cisco SD-Access LISP Collaterals



Cisco Software-Defined Access for Industry Verticals



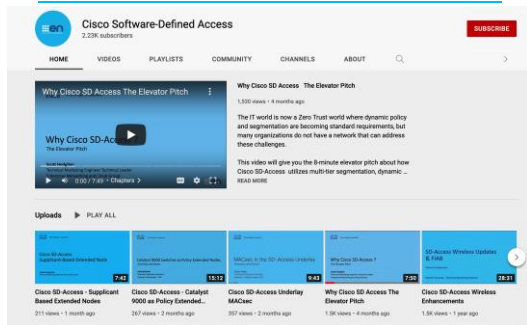
Cisco Software-Defined Access Enabling intent-based networking



Cisco Solution Validated Profiles (CVPs)

- [Cisco Large Enterprise and Government Profile](#)
- [Healthcare Vertical](#)
- [Financial Vertical](#)
- [Healthcare Vertical](#)
- [Manufacturing Vertical](#)
- [Retail Vertical](#)
- [University Vertical](#)

Cisco SD-Access YouTube Link



Cisco SD-Access Design Tool

EN&C Validated Designs

The Latest SD-Access Guides

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

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

Contact me at: jeffl2@cisco.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC