



The bridge to possible

# Cisco Software-Defined Access Solution Fundamentals

A Look Under the Hood

Jerome Dolphin, Technical Marketing Engineer  
CCIE#17805 (R&S, SEC), CCDE#2013::3

# Cisco Webex App

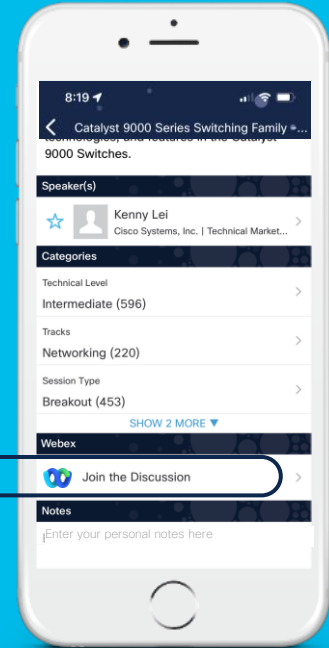
## Questions?

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 until February 24, 2023.

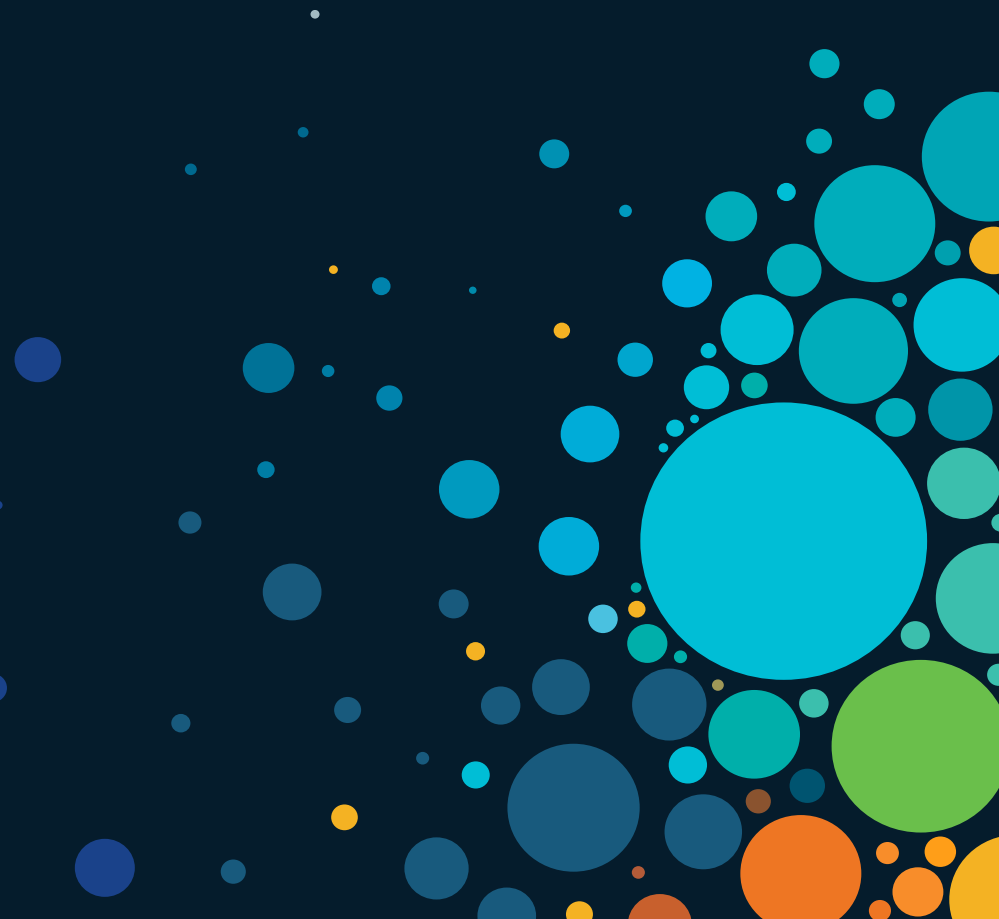




# Agenda

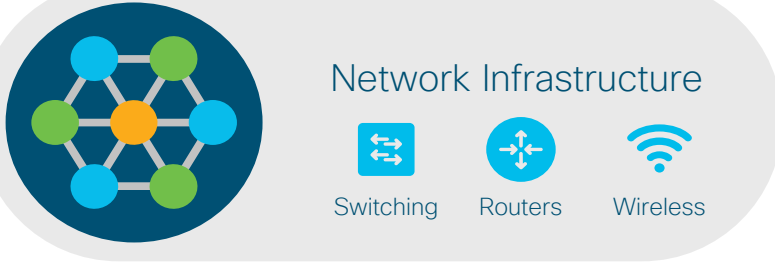
- Why Cisco SD-Access?
- Roles and Terminology
- Fabric Fundamentals
- Multiple Fabrics
- Conclusion

# Why Cisco SD- Access?

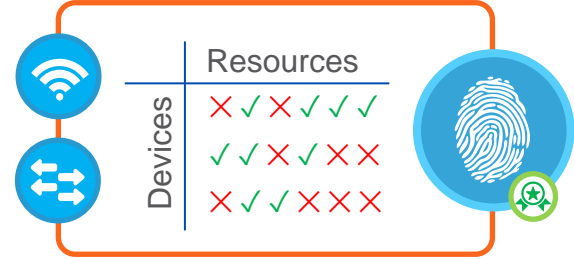


# Traditional Networking Challenges

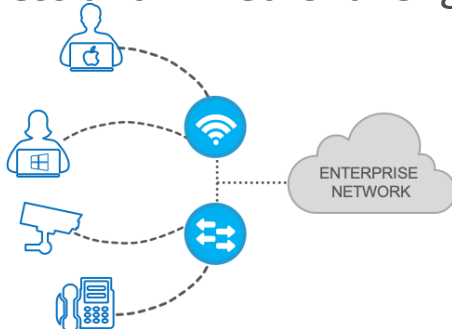
## Network Deployment Challenges



## Network Security Challenges



## Wireless and Wired Challenges

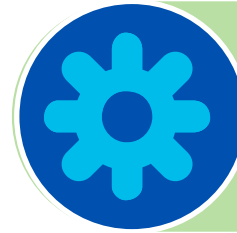
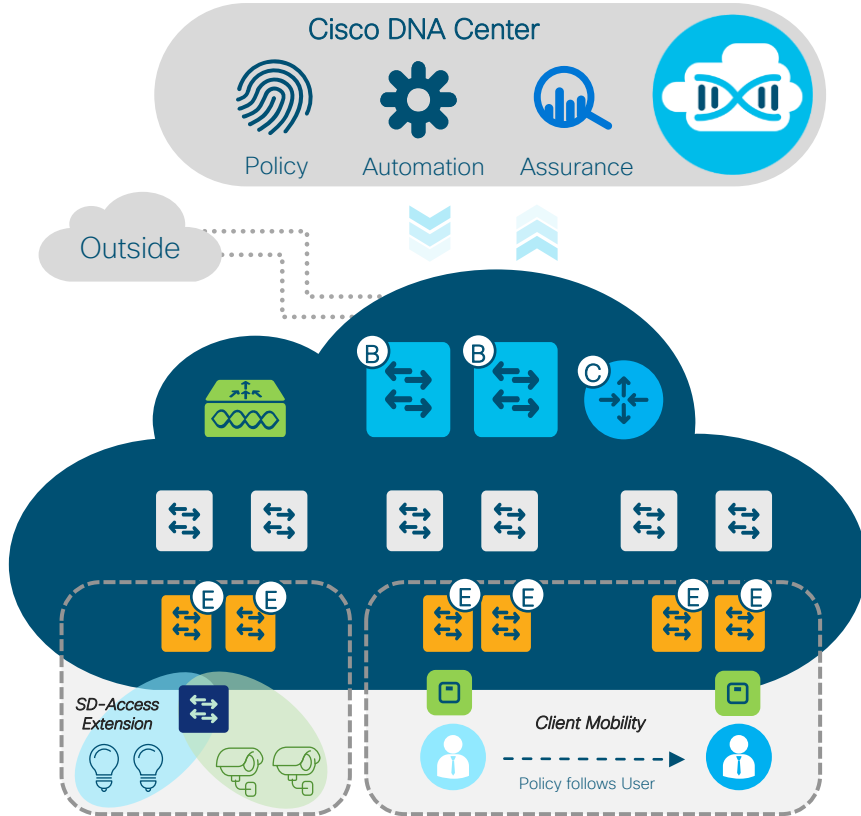


## Network Operations Challenges



# Cisco Software-Defined Access

## Intent-Based Networking



### One Automated Network Fabric

Single fabric for wired and wireless with full automation



### Identity-Based Policy and Segmentation

Policy definition decoupled from VLAN and IP address



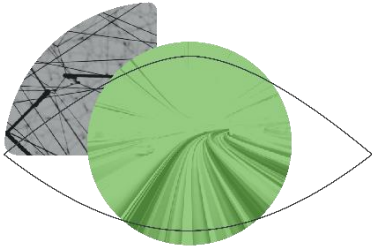
### AI-Driven Insights and Telemetry

Analytics and visibility into user and application experience

# Cisco Software-Defined Access

## Zero Trust for the Workplace

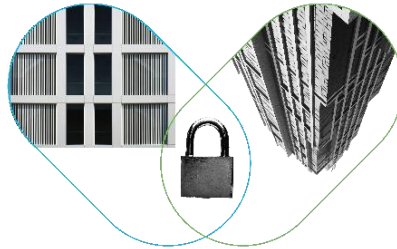
### Visibility



Grant the right level of network access to users and devices.



### Segmentation



Shrink zones of trust and grant access based on least privilege.



### Containment



Automate containment of infected endpoints and revoke network access.

Visibility, Segmentation and Containment are explored further in BRKENS-2819.

# Benefits of Cisco Software-Defined Access

Enhance Security and Compliance



Deliver Consistent Experience



Boost Operational Effectiveness



Gain Network Insights

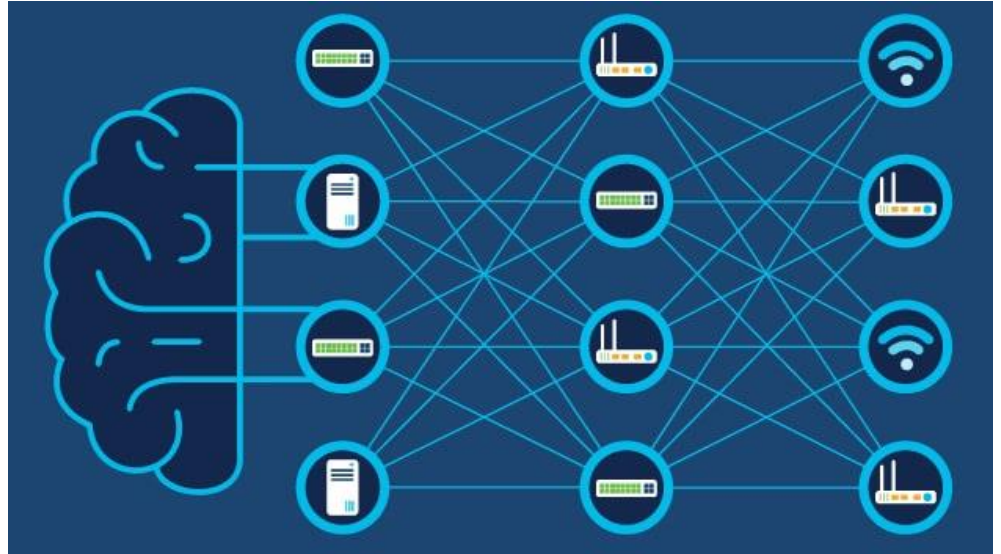


# Roles and Terminology

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

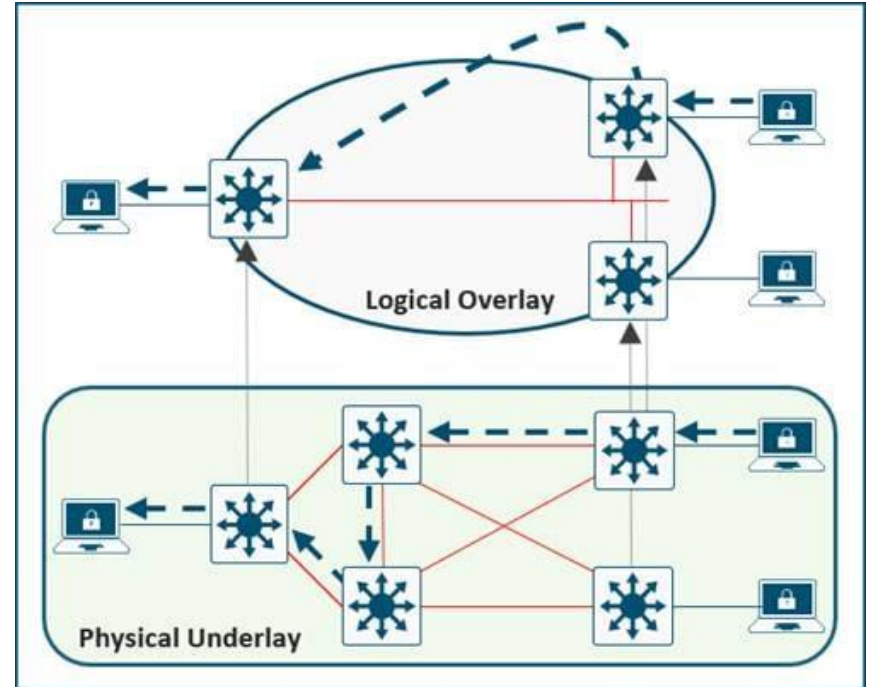
# What is a Network Fabric?

- 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 .



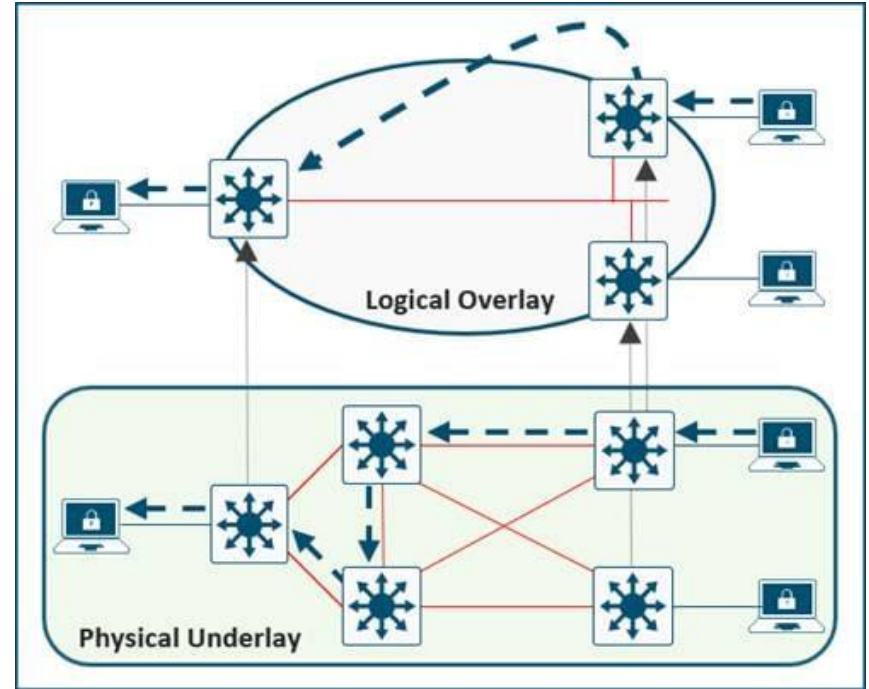
# What is an Overlay?

- 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



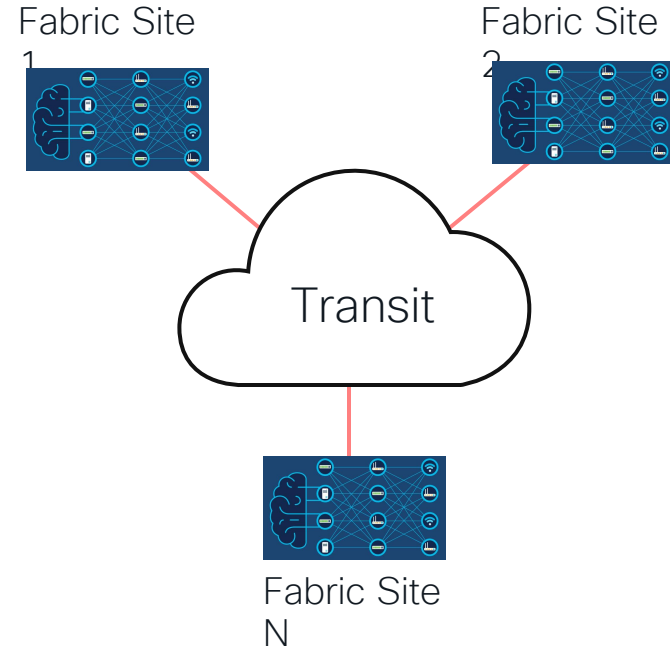
# Why an Overlay?

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



# 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”.



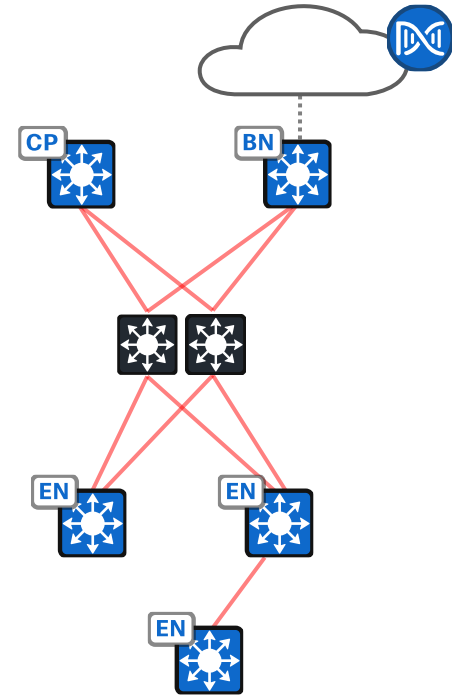
# Roles and Terminology

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

# Cisco SD-Access Roles

## Mandatory Components

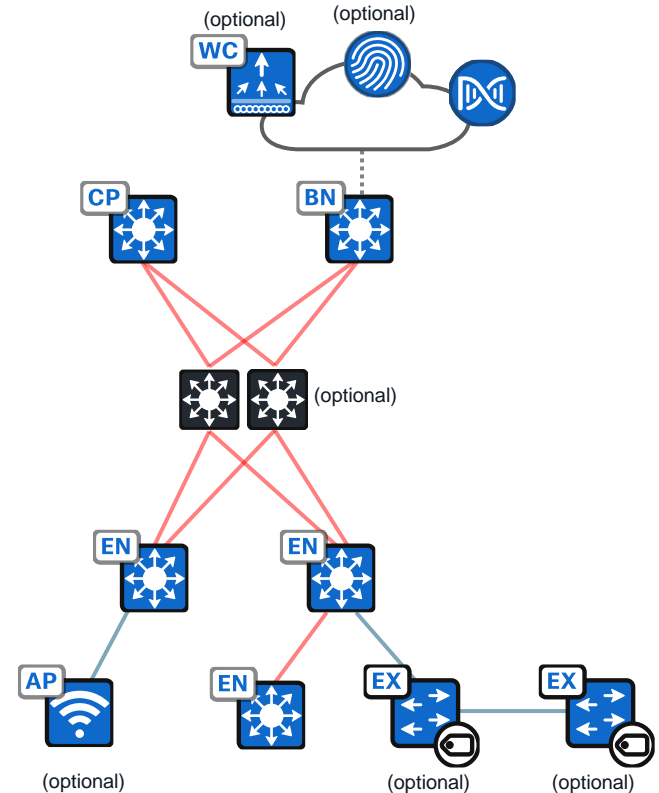
- **Cisco DNA Center** – GUI and APIs for intent-based automation of wired and wireless fabric devices.
- **Fabric Border Nodes** – A fabric device that connects external L3 and L2 networks to the Cisco SD-Access fabric.
- **Edge Nodes** – A fabric device that connects wired endpoints to the Cisco SD-Access 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

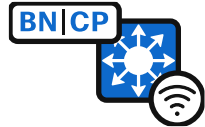
## Some of the Supported Colocations



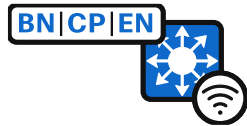
Border Node and Control Plane Node.



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.

# 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>

New Deployment

Release:  Device Role:

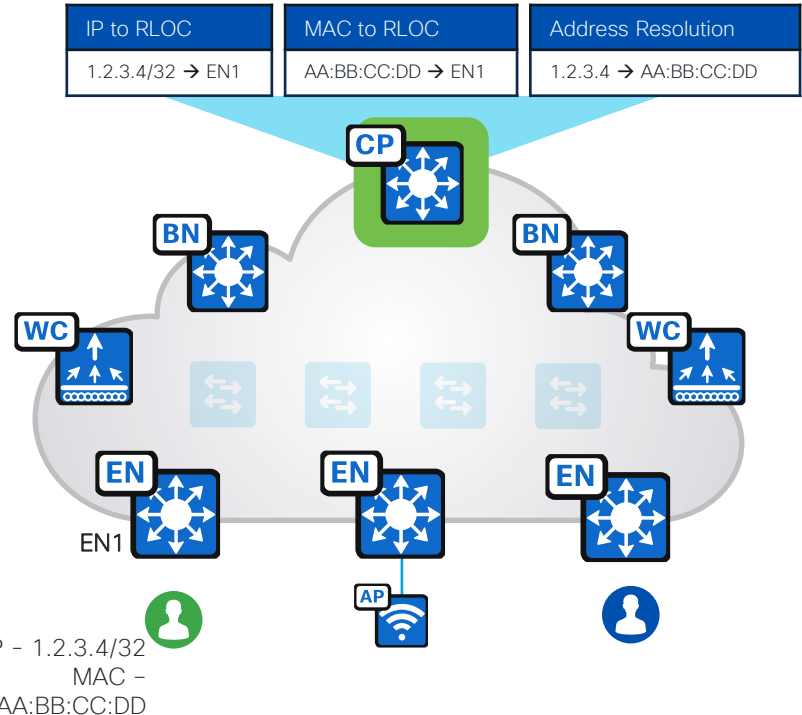
SD-Access Compatibility Matrix for Cisco DNA Center 2.3.3.6 (recommended release)

Device Role	Device Series	Device Model	Recommended Release	Supported Release
		C9300X-12Y	IOS XE 17.6.4	IOS XE 17.9.x
		C9300X-24Y		IOS XE 17.8.x
		C9300X-24HX		IOS XE 17.7.x
		C9300X-48HXN		IOS XE 17.6.x
		C9300X-48HX		IOS XE 17.5.x

# Cisco SD-Access Fabric

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

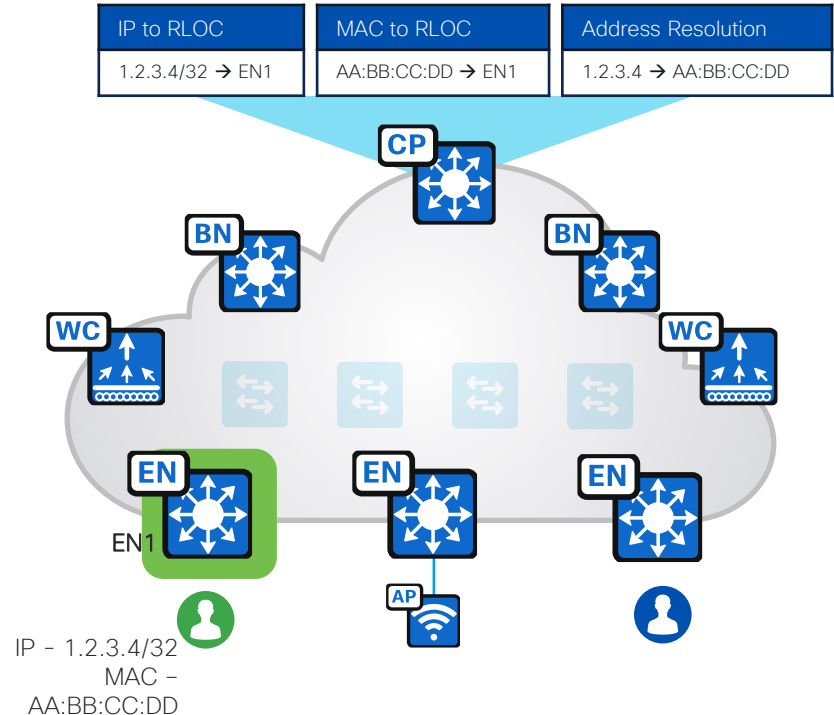
- A simple Host Database that maps Endpoint IDs to locations, along with other attributes.
- Host Database supports multiple types of Endpoint ID lookup types (IPv4, IPv6 or MAC).
- Receives Endpoint ID map registrations from Edge Nodes, Border Nodes and Fabric Wireless LAN Controllers.
- Resolves lookup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



# Cisco SD-Access Fabric

## Edge Node Provides First Hop Services for Endpoints

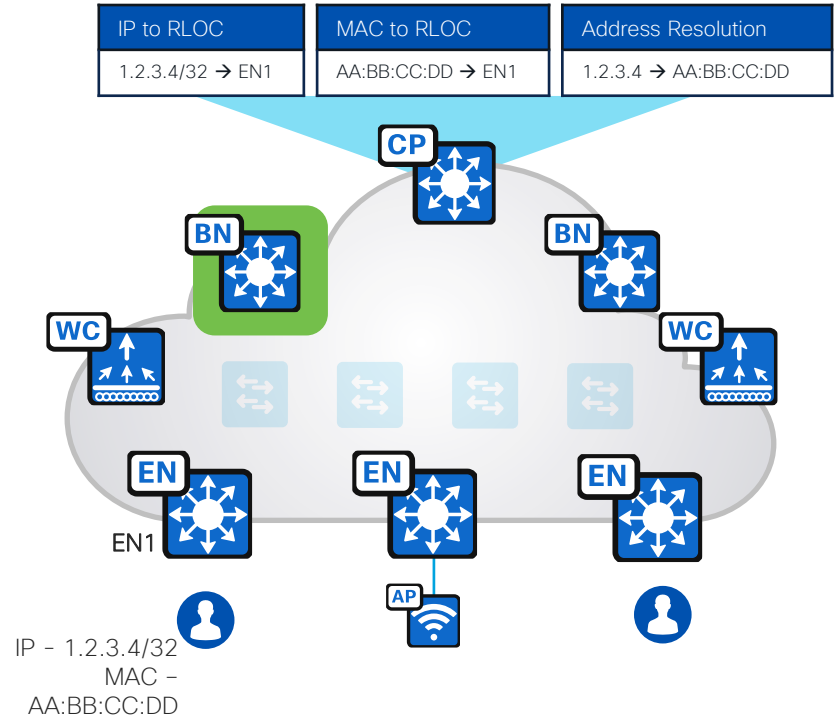
- Responsible for Authenticating and Authorizing endpoints (e.g. 802.1X, MAB, static) in concert with ISE.
- Register Endpoint IDs (IPv4, IPv6, MAC) with the Control Plane Nodes.
- Provide an Anycast Gateway for the connected wired and wireless endpoints.
- Performs VXLAN encapsulation and decapsulation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

The screenshot displays the configuration for a Border Node named "BLD2-FLR2-DST1". It features two tabs: "Layer 3 Handoff" (selected) and "Layer 2 Handoff". Under "Layer 3 Handoff", the "Enable Layer-3 Handoff" checkbox is checked. Below this, the "Local Autonomous Number" is set to "65004". A green bracket highlights three additional settings: "Default to all virtual networks" (checked), "Do not import external routes" (checked), and an "Advanced" gear icon. At the bottom, there is a button labeled "Add Transit 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.

The screenshot shows the configuration page for a Fabric Site named "BLD1-FLR2-DST1". At the top, there are two tabs: "Layer 3 Handoff" (which is selected and highlighted with a blue underline) and "Layer 2 Handoff". Below the tabs, there is a checked checkbox labeled "Enable Layer-3 Handoff". Underneath this, the "Local Autonomous Number" is set to "65004". There is an information icon (i) to the right of this field. Below that, there is an unchecked checkbox labeled "Default to all virtual networks" with an information icon (i) to its right. A green bracket highlights this checkbox. Below the checkbox is a gear icon and the word "Advanced". At the bottom of the configuration area, there is a blue button with a plus sign and the text "Add Transit 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.

The screenshot shows the configuration page for a Border Node named "BLD1-FLR2-DST1". At the top, there are two tabs: "Layer 3 Handoff" (which is selected and highlighted with a blue underline) and "Layer 2 Handoff". Below the tabs, there is a section for "Enable Layer-3 Handoff" with a checked checkbox. Underneath, the "Local Autonomous Number" is set to "65004". A green bracket on the left side of the interface groups the following two options: "Default to all virtual networks" (checked) and "Do not import external routes" (unchecked). Each of these options has an information icon (i) to its right. Below these options is an "Advanced" link with a gear icon. At the bottom of the configuration area, there is a blue button with a plus sign and the text "Add Transit 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 is not tunneled within the SD-Access Fabric.
  - Ideally should be separate device from the Layer 3 Border Node.

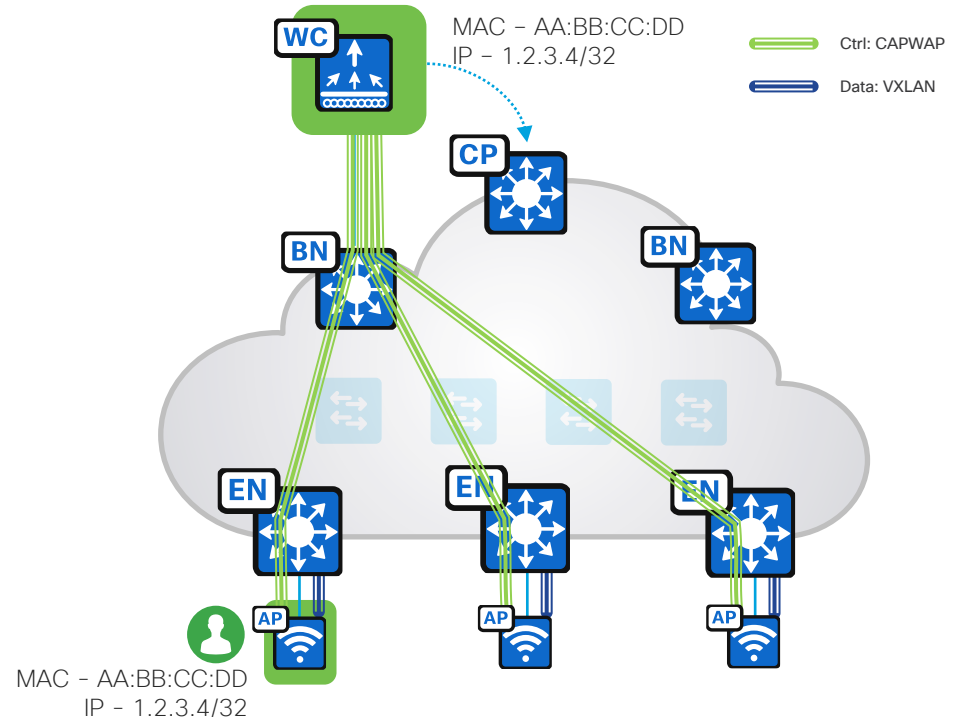
PNP-DEMO1.cbr.ciscolabs.com

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	
Q 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** Unifies Wired and Wireless 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 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.



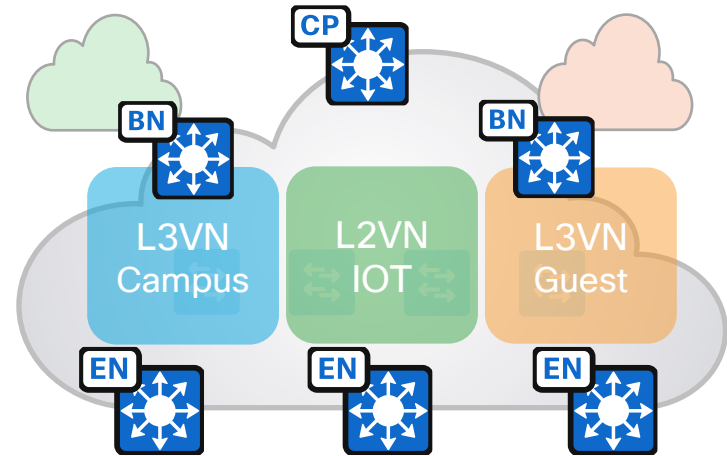
# Roles and Terminology

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

# Cisco SD-Access Fabric

## Virtual Networks

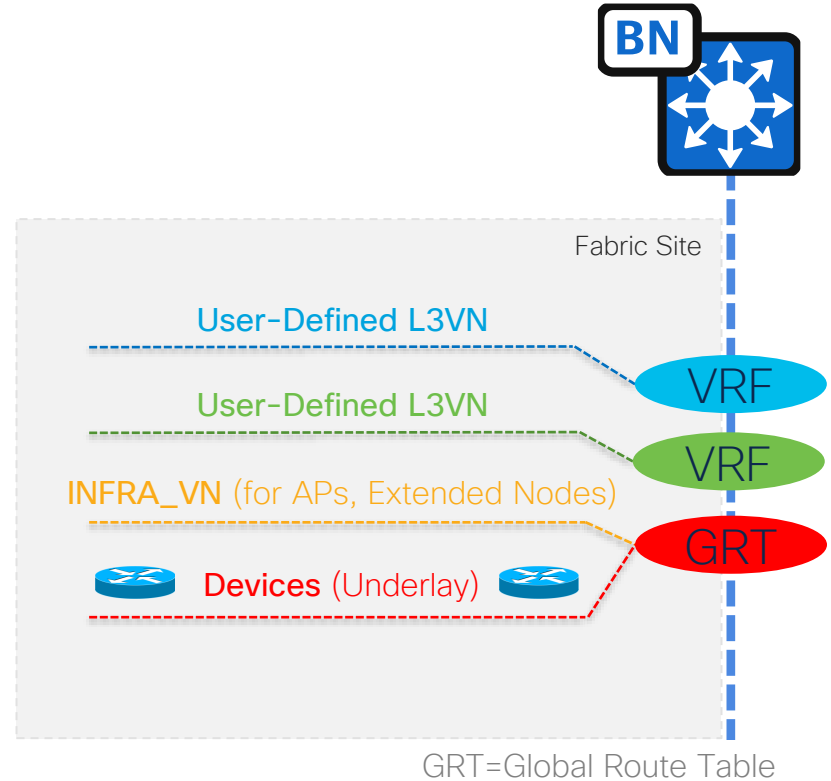
- Layer 3 Virtual Networks use VRFs and LISP Instance IDs to maintain separate routing topologies.
  - Endpoint IDs (IPv4/IPv6 addresses) are routed within an L3VN.
- Layer 2 Virtual Networks use LISP Instance IDs and VLANs to maintain separate switching topologies.
  - Endpoint IDs (MAC addresses) are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

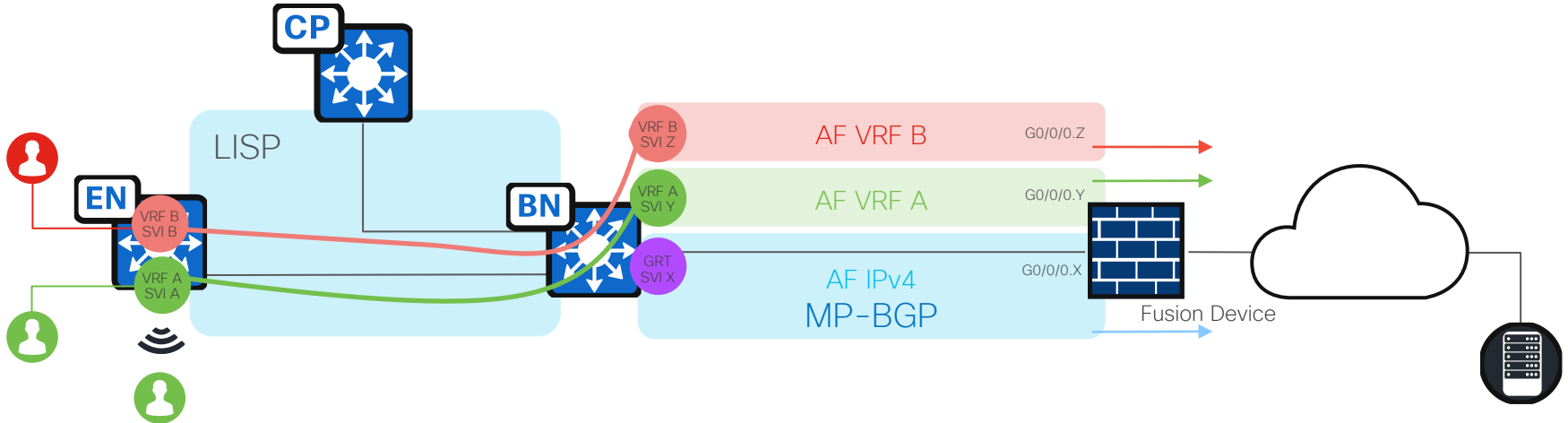
- **Fabric Devices (Underlay)** connectivity is in the **Global Routing Table**.
- **INFRA\_VN** is only for **Fabric Access Points** and **Extended Nodes** in the Global Routing Table.
- **User-Defined VNs** can be added or removed on demand.
- **DEFAULT\_VN** is the same as a user-defined VN. Present 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

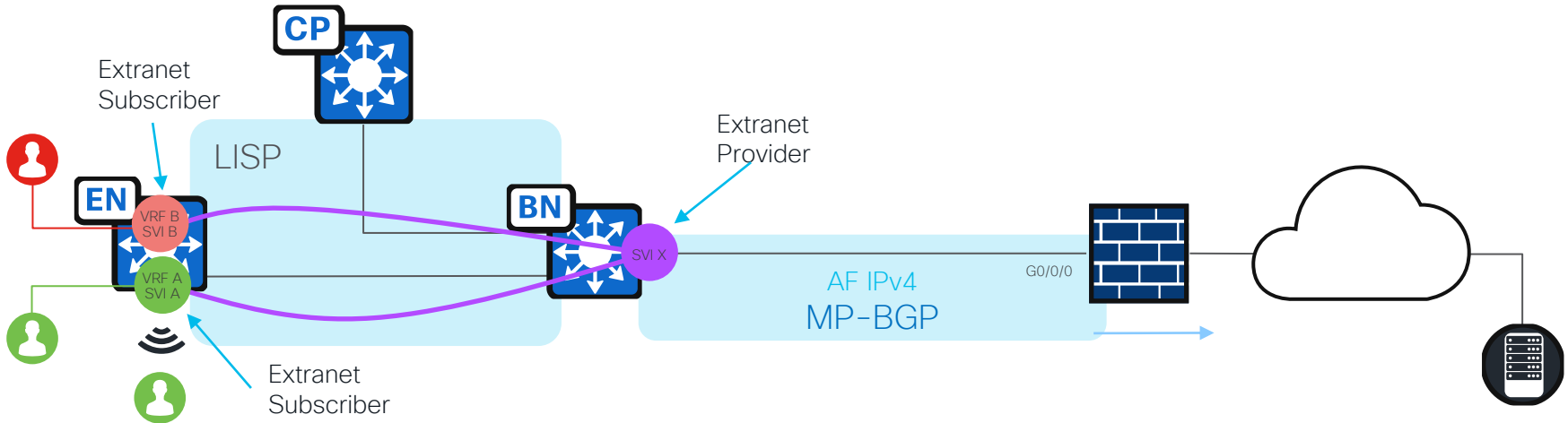
- Use a "Fusion Device" to leak external routes into SD-Access Layer 3 Virtual Networks.
- Alternatively, maintain VRF segmentation outside of the SD-Access Fabric with a VRF-aware external routing domain.
- Fusion Device is outside the fabric. Can be any platform (router, Layer 3 switch, firewall, etc.)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



# Cisco SD-Access Fabric

## Extranet Provider Virtual Network Layer 3 Handoff

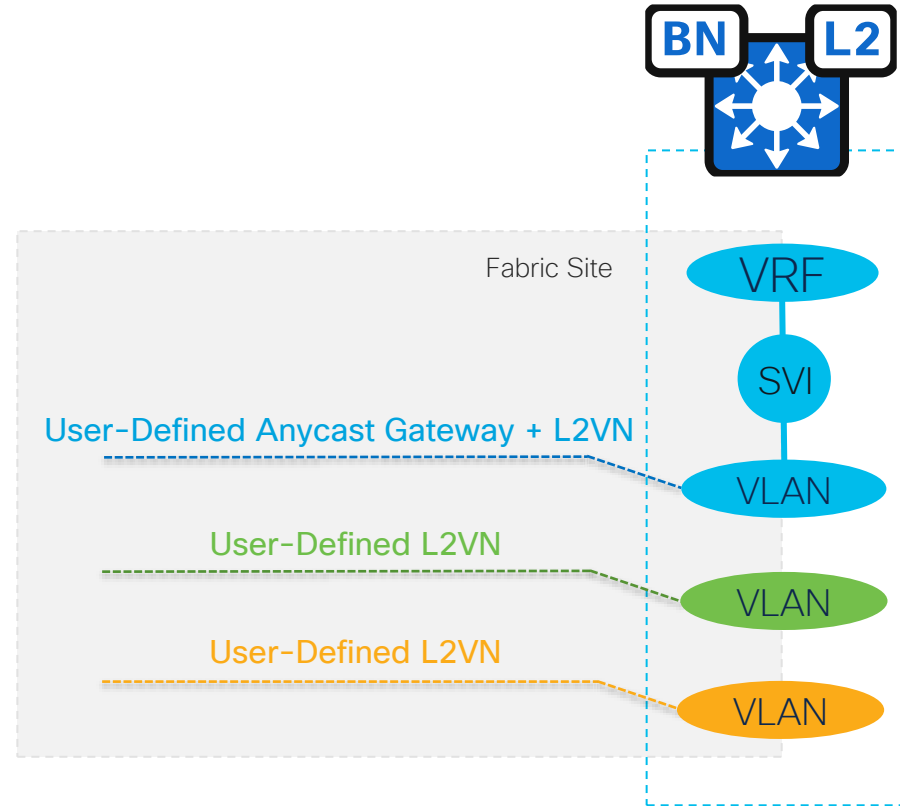
- Use an Extranet Policy to allow communication between one Provider Virtual Network and one or more Subscriber Virtual Networks.
- Extranet Policy is roadmap for SD-Access 2.3.5.0 ETA ~Q2CY23. Requires LISP Pub/Sub Control Plane. Please read the release collateral for details of functionality and design considerations.



# Cisco SD-Access Fabric

## Layer 2 Handoff

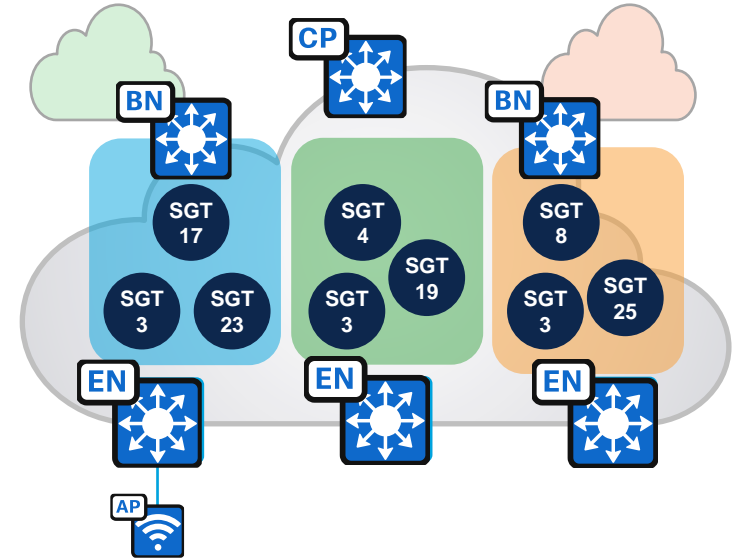
- Ancient wisdom: Route whenever you can, switch when you must.
- Layer 2 Virtual Networks handoff through a user-defined VLAN.
- Layer 2 Virtual Networks may implement BUM flooding. Important to be mindful of loop prevention.



# Cisco SD-Access Fabric

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

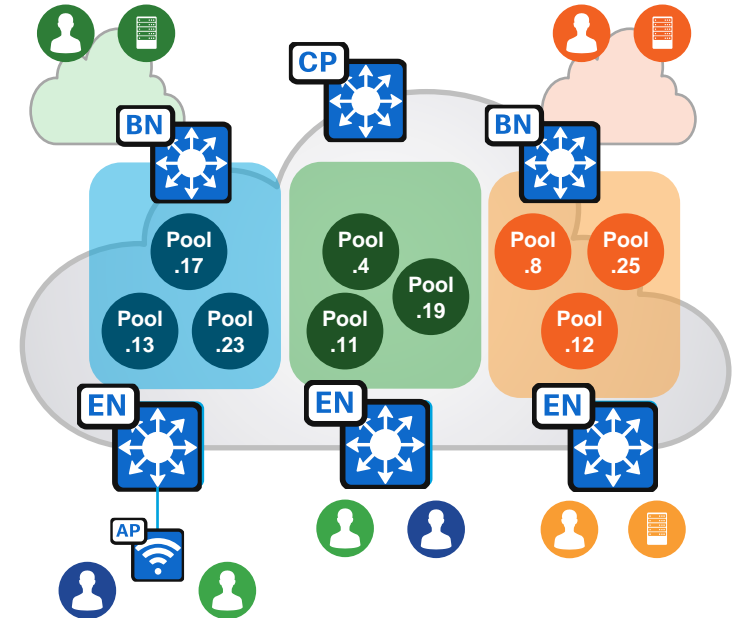
- Edge Nodes and Fabric APs assign a unique Scalable Group Tag (SGT) to each end endpoint in concert with ISE.
- Edge Nodes and Fabric APs add an SGT to the fabric encapsulation.
- SGTs are used to implement IP-address-independent traffic policies.
- SGTs can be extended to numerous other networking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



# Cisco SD-Access Fabric

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

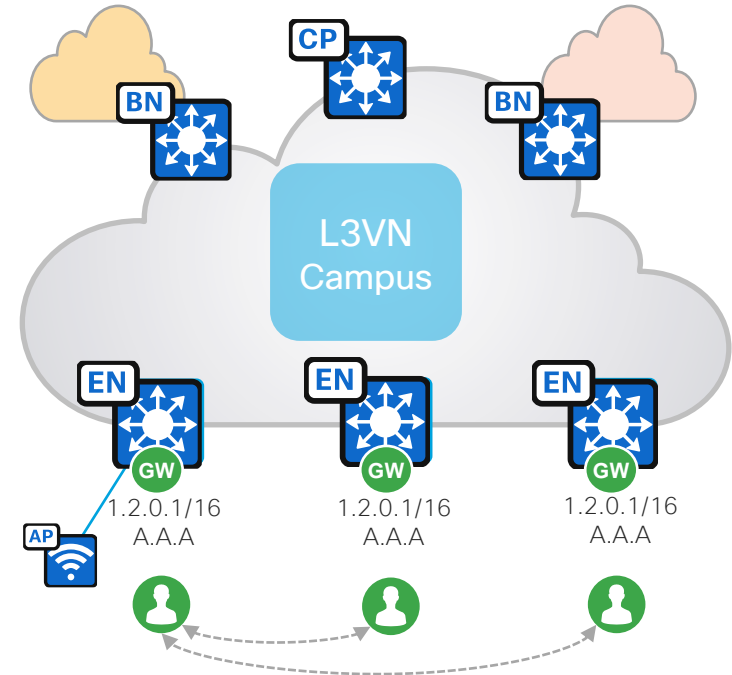
- Edge Nodes instantiate an access VLAN and a Switched Virtual Interface (SVI) with user-defined IPv4/IPv6 addresses per Host Pool.
- Host Pools assigned to endpoints dynamically by AAA or statically per port.
- Edge Nodes and Fabric WLCs register endpoint IDs (/32, /128 or MAC) with the Control Plane,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



# Cisco SD-Access Fabric

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

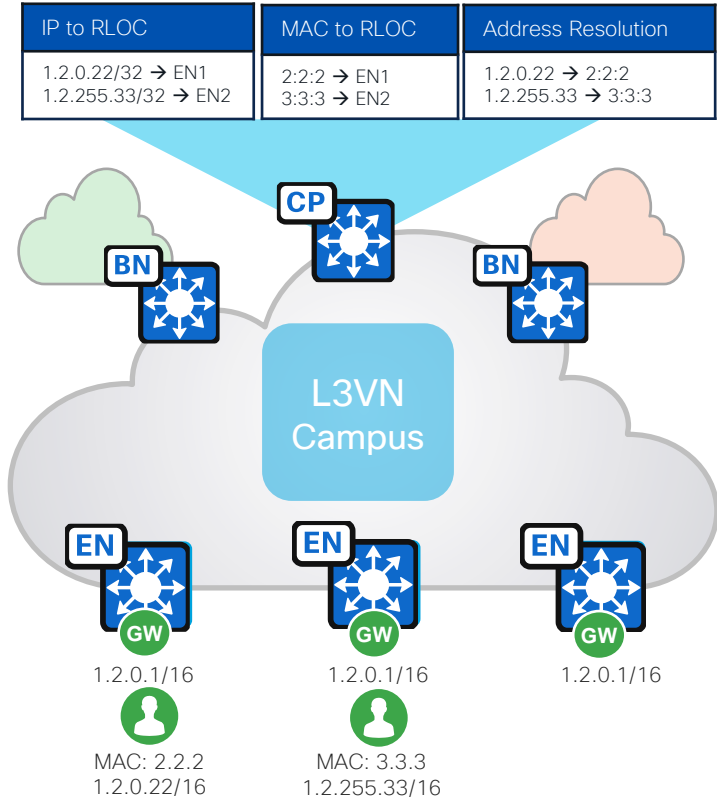
- Similar principle and behavior to FHRP with a shared virtual IPv4/IPv6 addresses and MAC address.
- The same Switch Virtual Interface (SVI) is present on all Edge Nodes with the same virtual IP and MAC.
- The wired or wireless endpoint can connect to any switch or AP in the fabric and communicate with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



# Cisco SD-Access Fabric

Host Pools are “stretched” via the Overlay

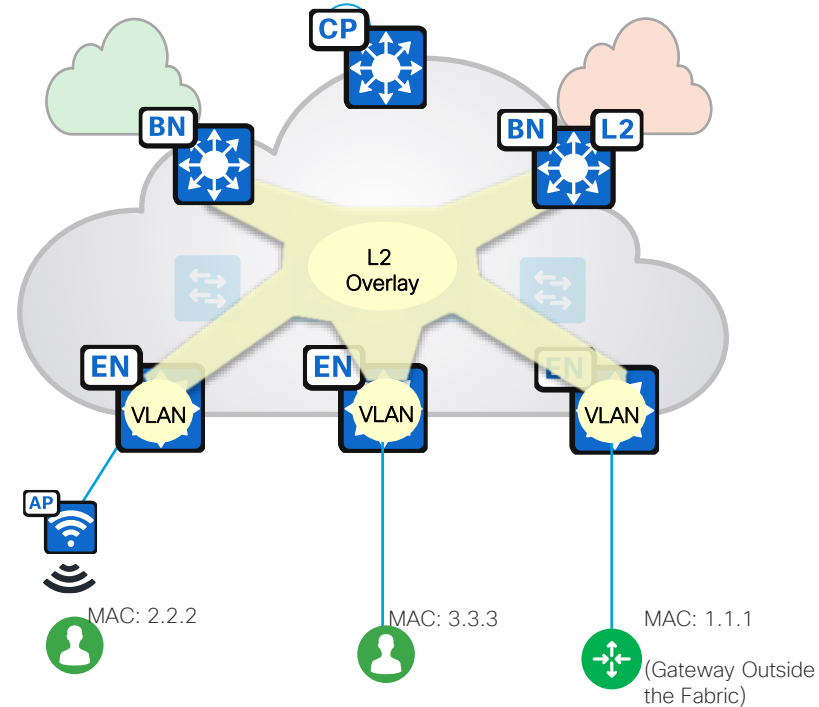
- Endpoint IPv4/IPv6 traffic arrives on an Edge Node and is then routed or switched by the Edge Node.
- Fabric Dynamic EID mapping allows endpoint-specific (/32, /128, MAC) advertisement and mobility.
- No longer need VLANs to interconnect endpoints across Edge Nodes, this happens in the Overlay without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



# 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 RFC9300-RFC9305 and Informational RFC9299.

Lightweight, Efficient, Scalable and Extensible

# LISP in Cisco SD-Access

## Configure Control Plane

Select route distribution protocol:

### LISP/BGP



LISP/BGP uses concurrent LISP and BGP protocols to distribute reachability information. LISP/BGP is the traditional SD-Access control plane architecture and is retained for backwards compatibility. LISP Pub/Sub is recommended for new network implementations.

### LISP Pub/Sub



LISP Pub/Sub (Publish/Subscribe) accelerates network convergence, simplifies network operations, and provides the foundation for new SD-Access use cases. LISP Pub/Sub requires all Border Nodes, Control Plane Nodes and Edge Nodes to be running IOS XE 17.6.x or later.

## LISP/BGP

- Released circa 2017.
- Reliable and stable.
- BGP transport.

## LISP Pub/Sub

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

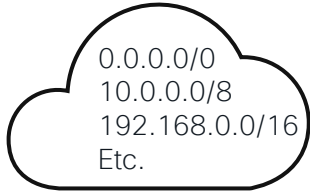
# LISP Pub/Sub

A Brief Digression, before you ask...

- No plans to end support for LISP/BGP.
- LISP Pub/Sub is recommended for new deployments.
- In DNA Center 2.2.3.x new Fabric Sites can be configured as LISP/BGP or LISP Pub/Sub. Note minimum IOS XE versions.
- First phase of LISP/BGP to LISP Pub/Sub migration workflow is under development now.
  - Migrate IP-Based Transit Fabric Sites.
  - ETA CY2023.
- Second phase of LISP/BGP to LISP Pub/Sub under planning.
  - Migrate SD-Access Transit Fabric Sites.
- Official release collateral will explain functionality.

# Fabric Operation

## Default ETR Registration

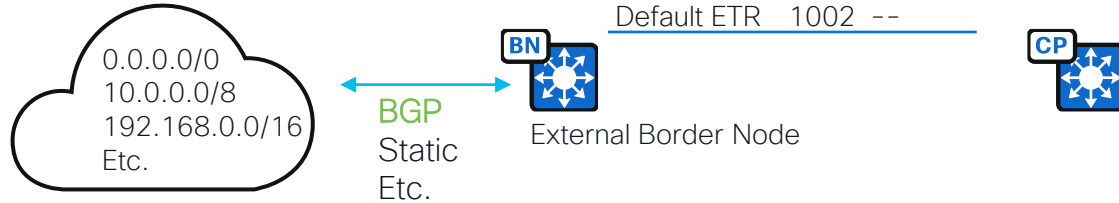


External Border Node



# Fabric Operation

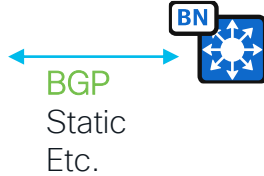
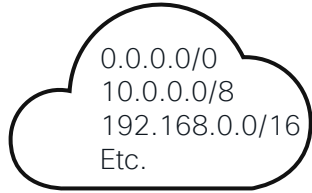
## Default ETR Registration



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	--

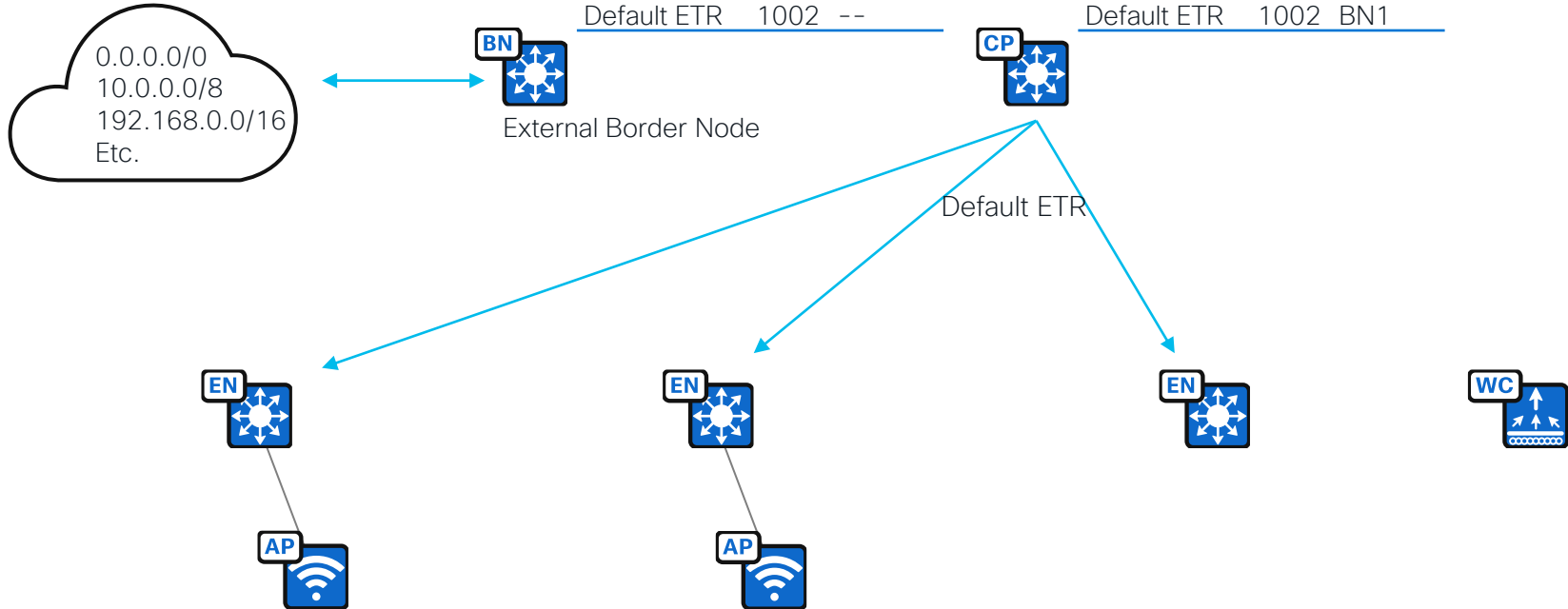
Register Default ETR per L3VN (Gateway of last resort)



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

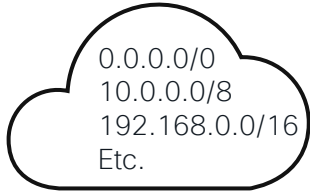
# Fabric Operation

## 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



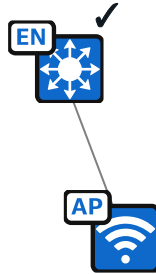
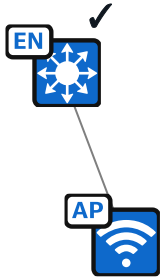
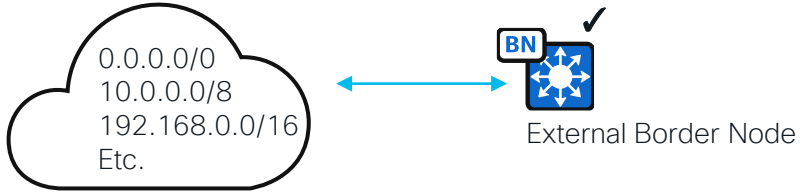
Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1

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

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

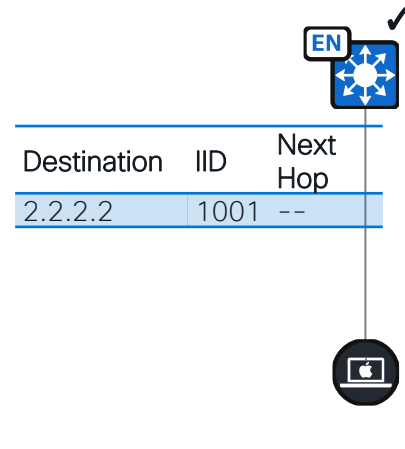
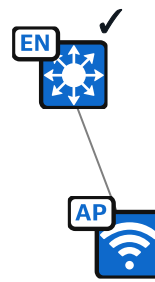
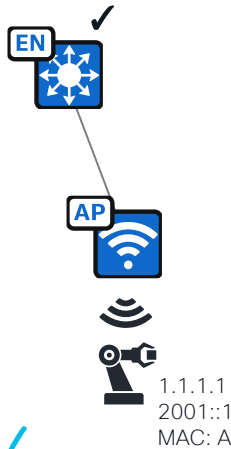
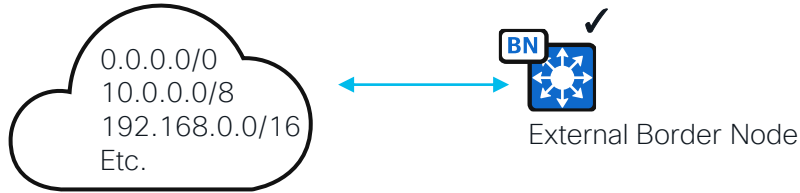
# Fabric Operation

## Edge Node Bootstrap



# Fabric Operation

## Endpoint Registration



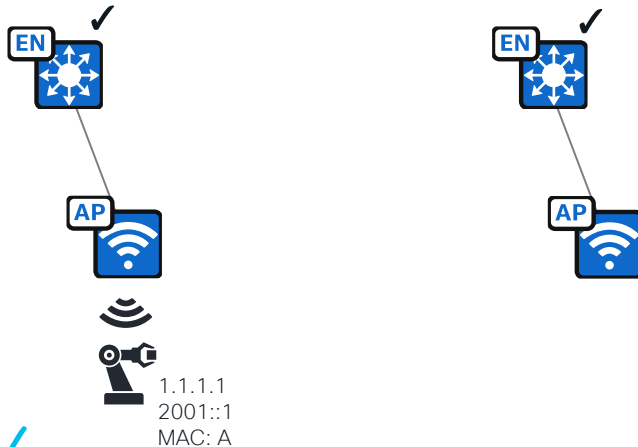
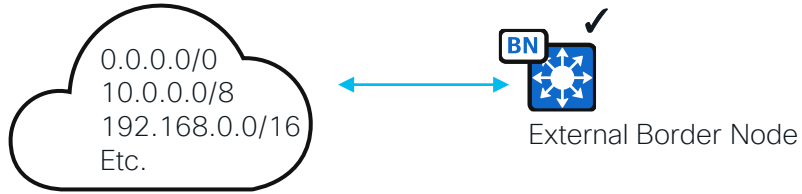
Destination	IID	Next Hop
2.2.2.2	1001	--

Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

# Fabric Operation

## Endpoint Registration



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

Register

Destination	IID	Next Hop
2.2.2.2	1001	--

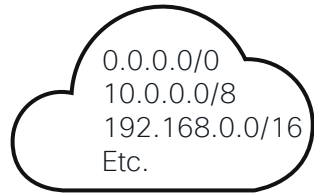
Destination	IID	Next Hop
1.1.1.1	1001	EN1



✓ Default ETR

# Fabric Operation

## Endpoint Registration



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

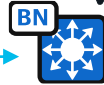
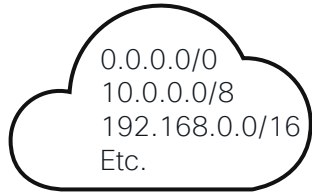


Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

# Fabric Operation

## Publish



External Border Node

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3



Publish

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	--



2.2.2.2  
2001::2  
MAC: B

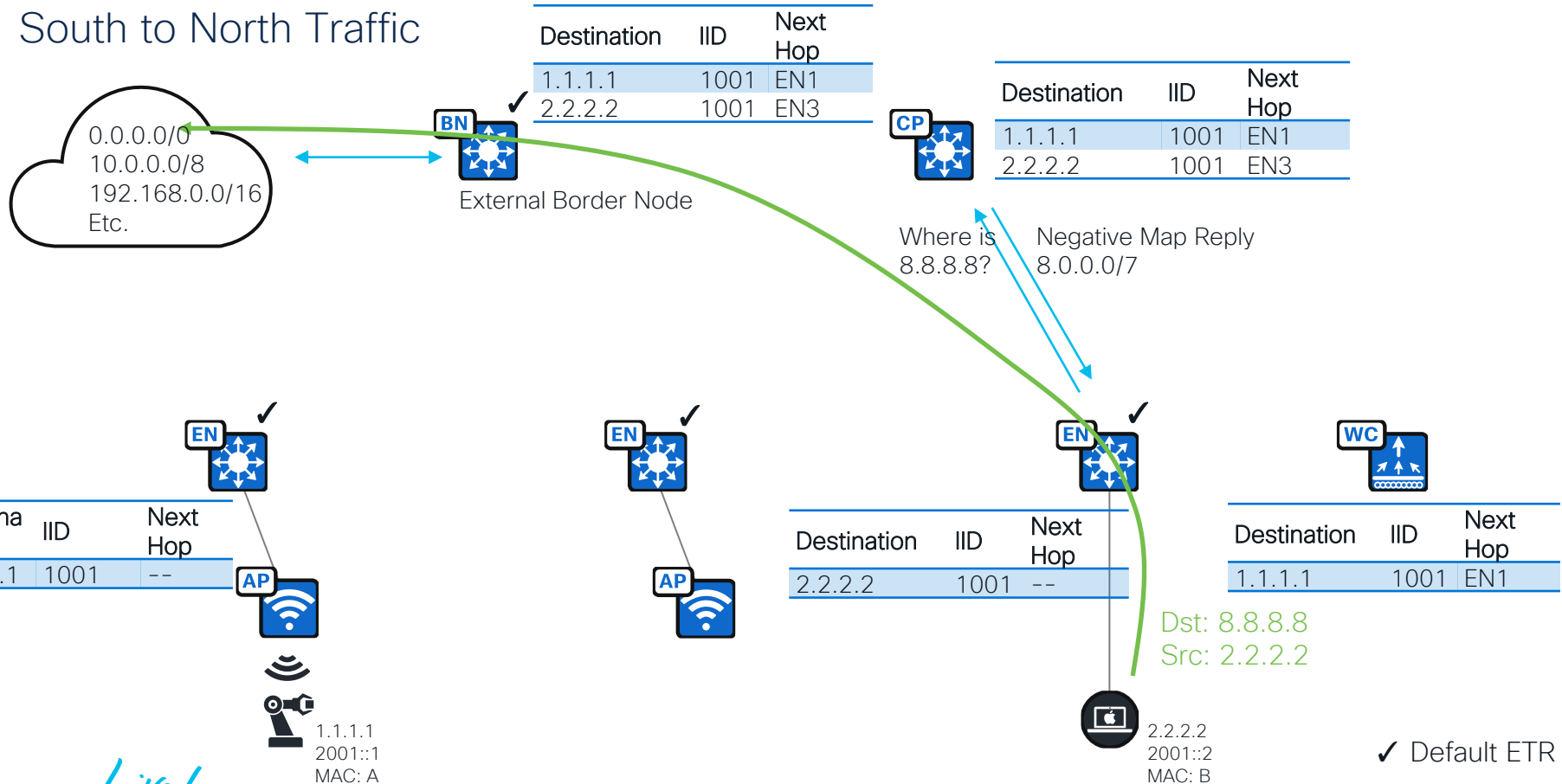


Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

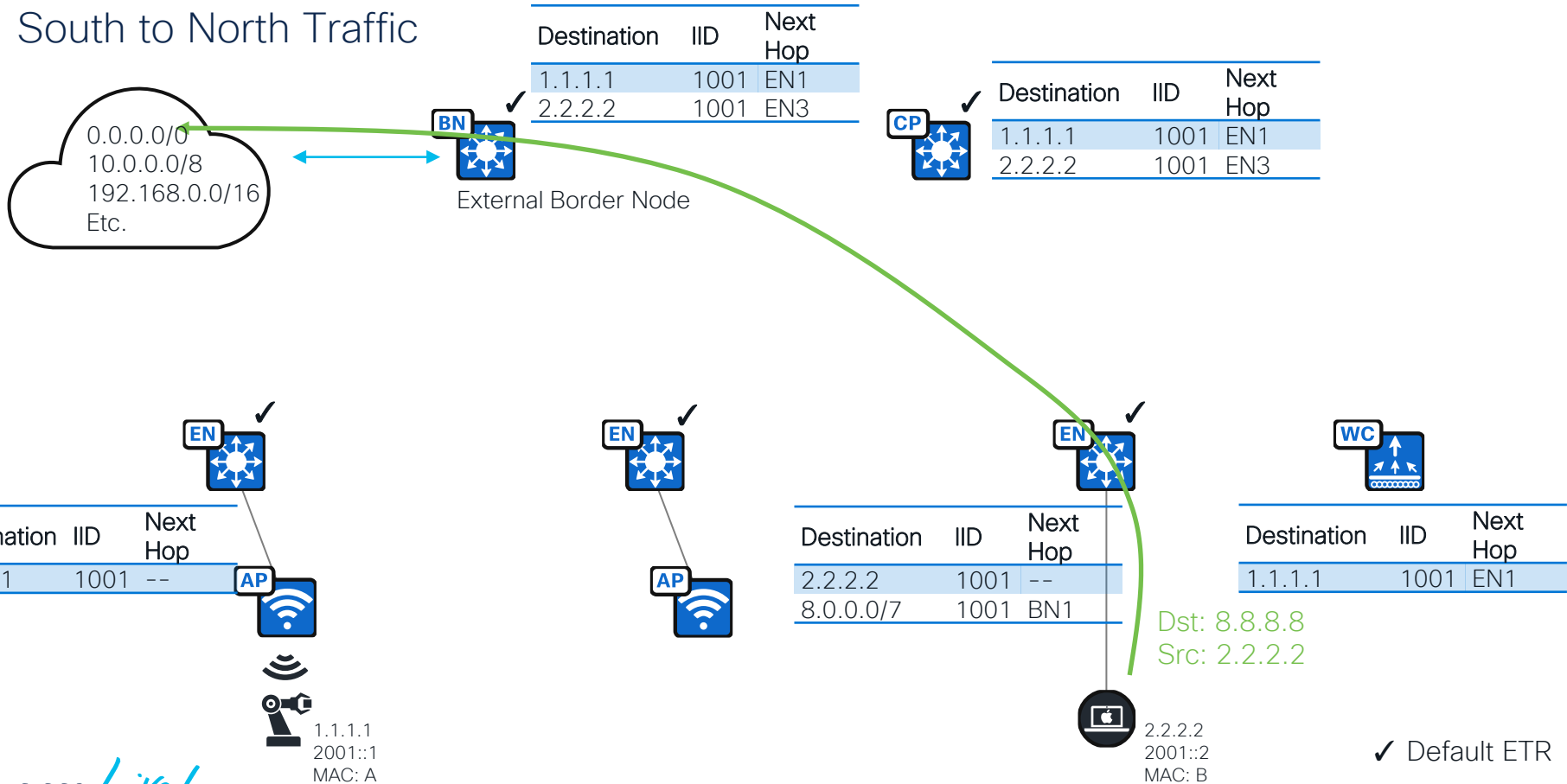
# Fabric Operation

## South to North Traffic



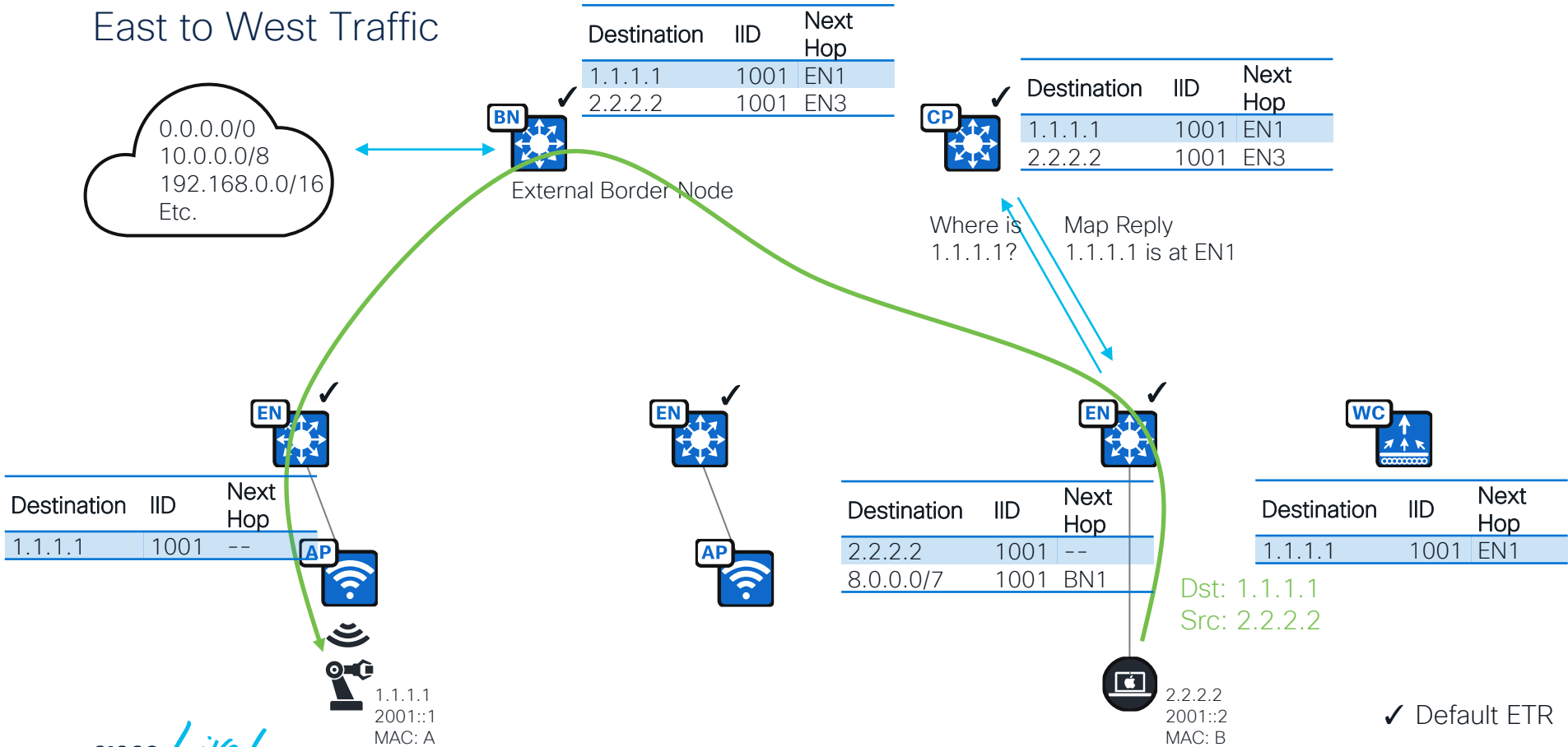
# Fabric Operation

## South to North Traffic



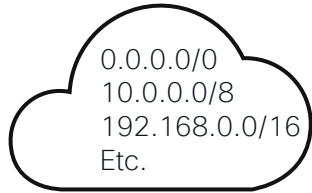
# Fabric Operation

## 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	--



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

Destination	IID	Next Hop
1.1.1.1	1001	EN1



1.1.1.1  
2001::1  
MAC: A



2.2.2.2  
2001::2  
MAC: B

Dst: 1.1.1.1  
Src: 2.2.2.2

✓ 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

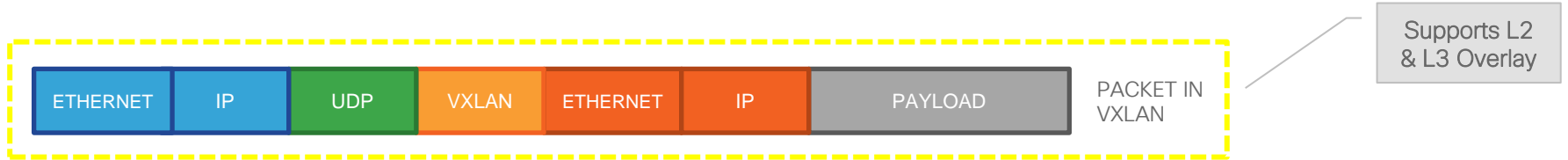
- BRKENS-2828 – LISP Architecture Evolution
  - Roaming.
  - Extranet.
  - SD-Access Transit.
  - Dynamic Default Border.
  - Backup Internet.
  - LISP Priority (SD-Access traffic steering).
  - Affinity ID (SD-Access Transit traffic steering).
  - Etc.

# Fabric Fundamentals

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

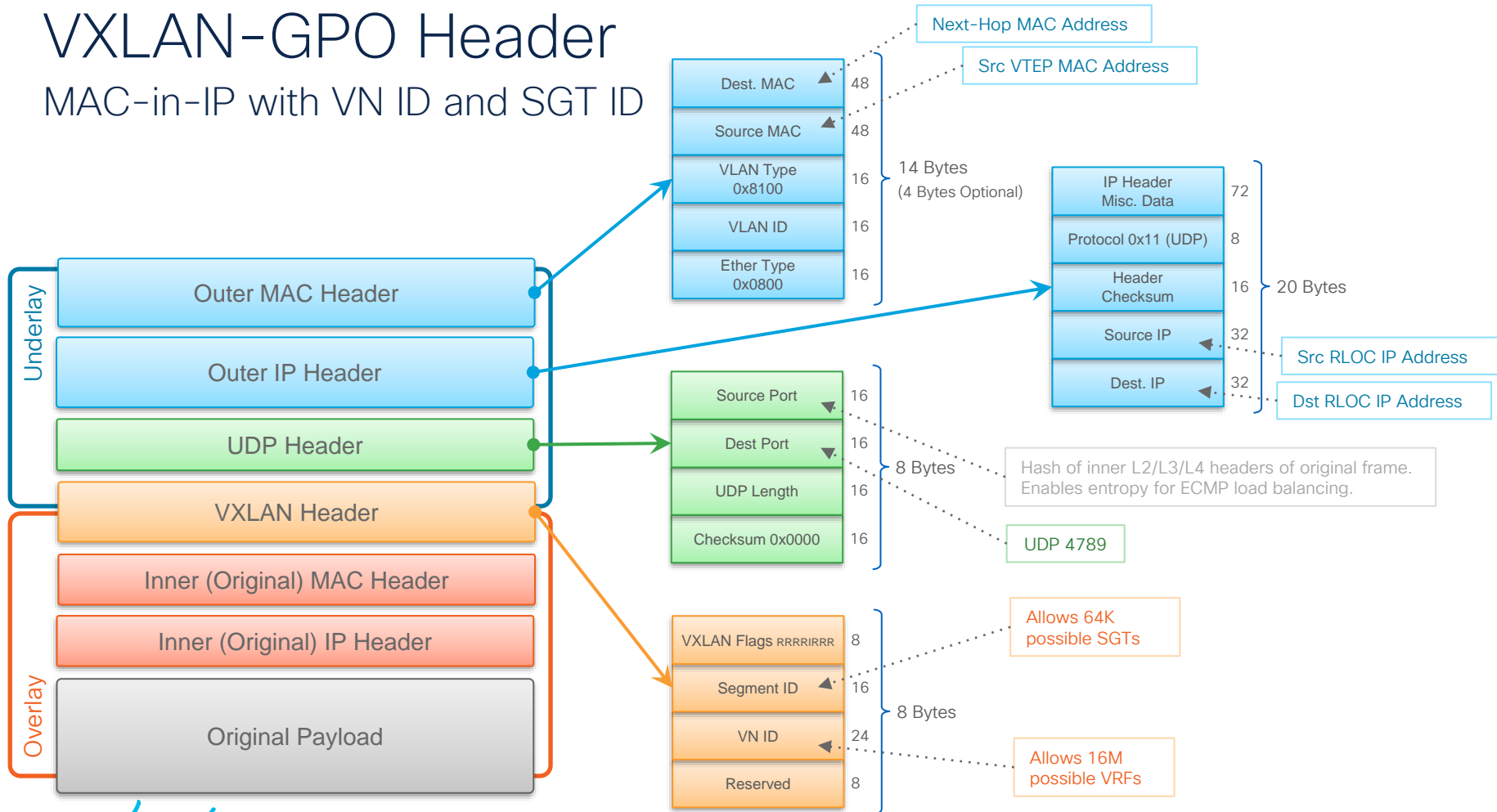
# Cisco SD-Access Fabric

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



# VXLAN-GPO Header

## MAC-in-IP with VN ID and SGT ID



# Fabric Fundamentals

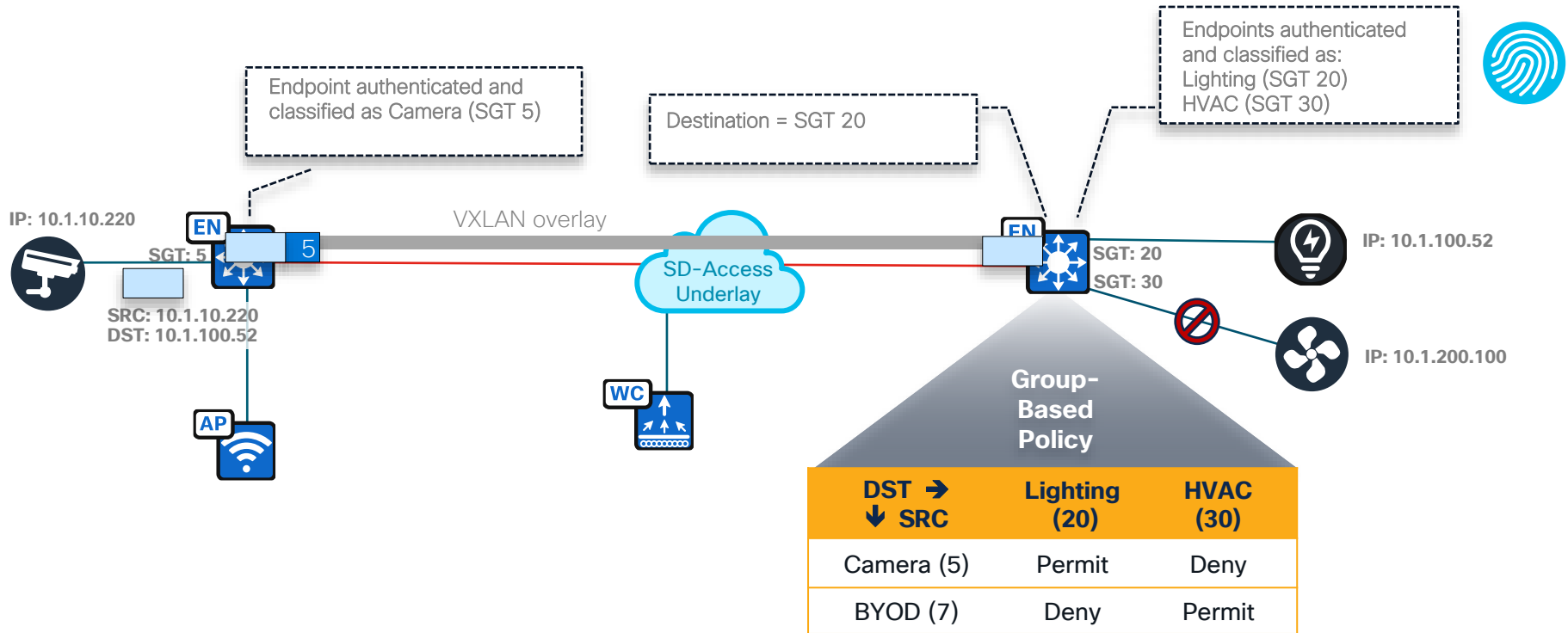
1. Control Plane
2. Data Plane
3. Policy Plane

# Cisco SD-Access Fabric

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

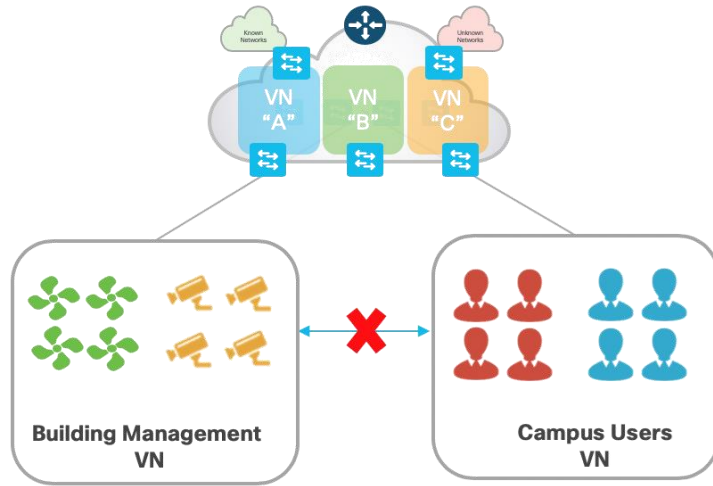


# What is Security Group Tag and Group-Based Policy?



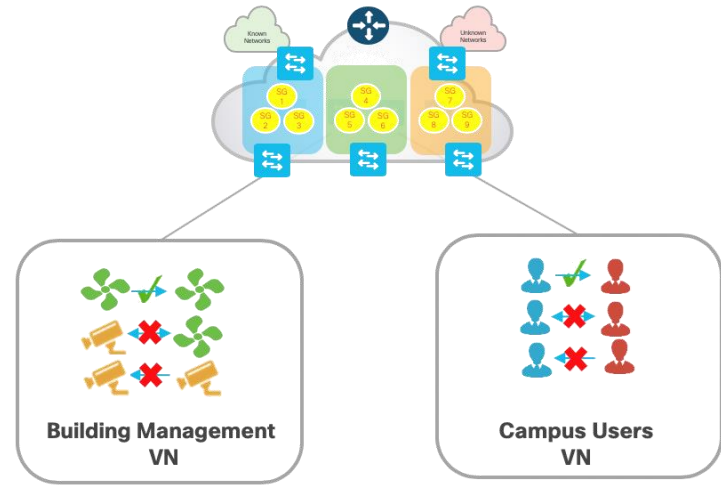
# SD-Access Policy

## Macro-Segmentation and Micro-Segmentation



### Virtual Network (VN)

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

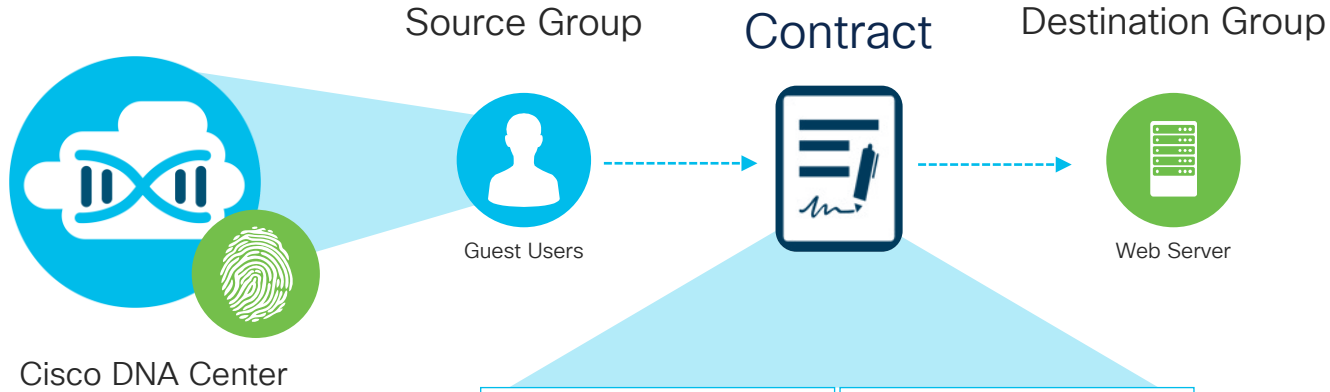


### Security Group Tag (SGT)

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

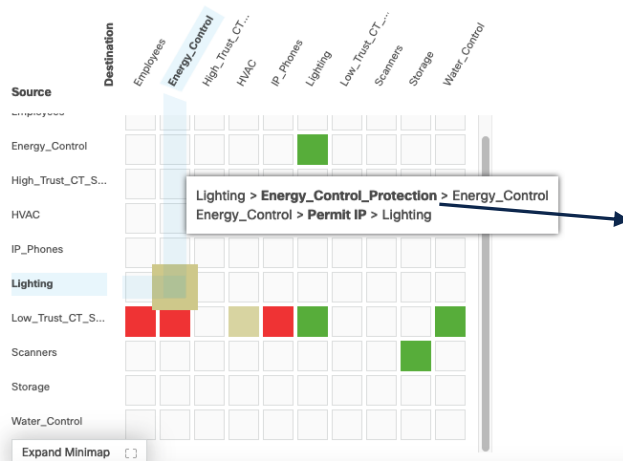
# SD-Access Policy

## Group-Based Access Control Policy

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

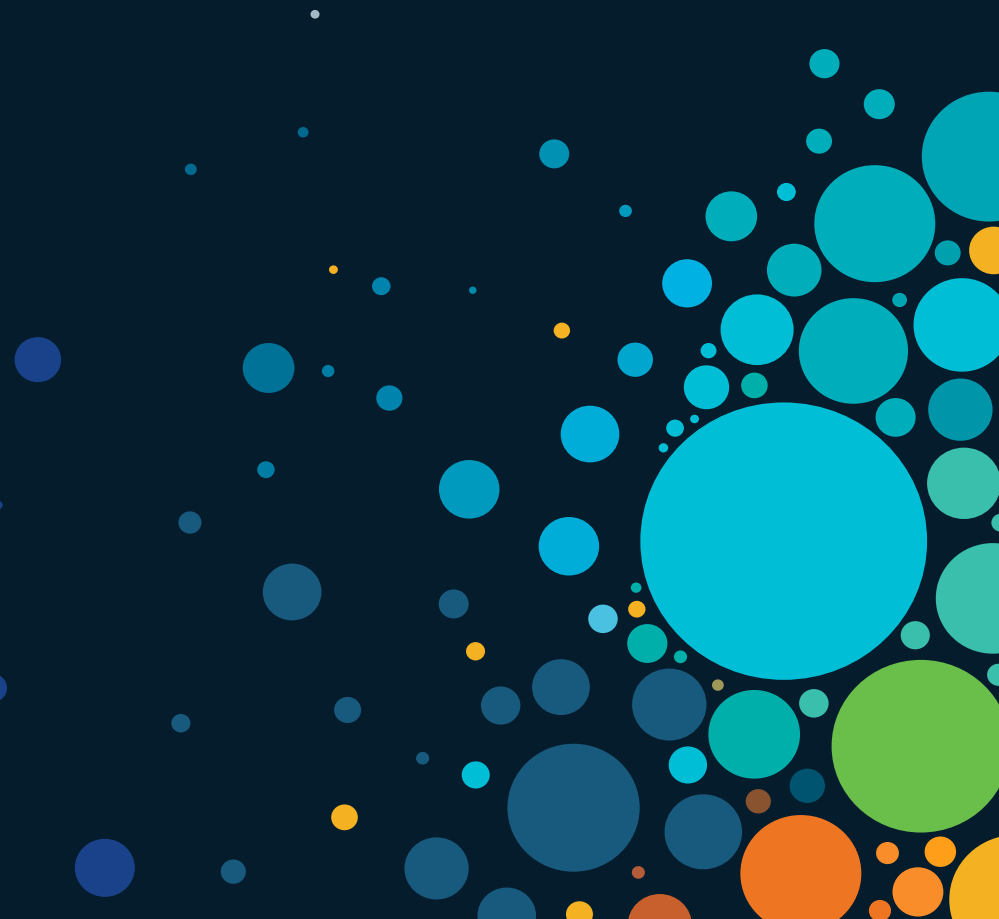
Description:

### CONTRACT CONTENT (1)

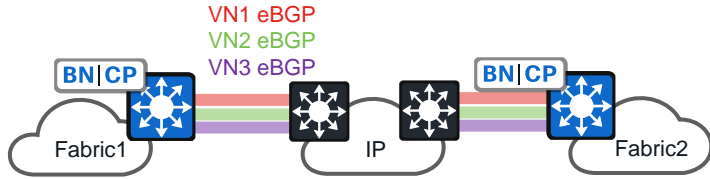
#	Action	Application	Transport Protocol	Source / Destination	Port	Logging
1	Permit	https	TCP/UDP	Destination	443/443	OFF

Default Action: Permit    Logging: OFF

# Multiple Fabrics



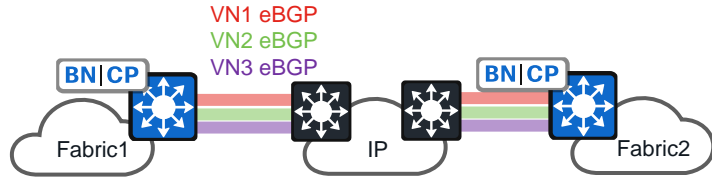
# Transits for VN and SGT Preservation



## 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

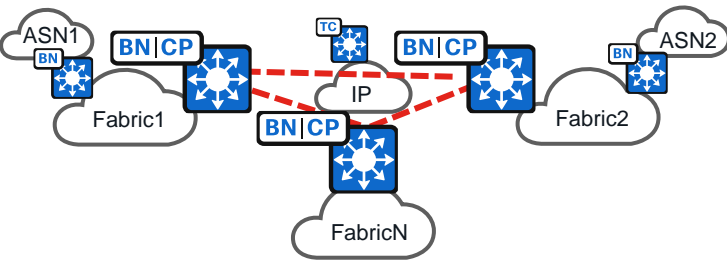


## IP-Based Transit

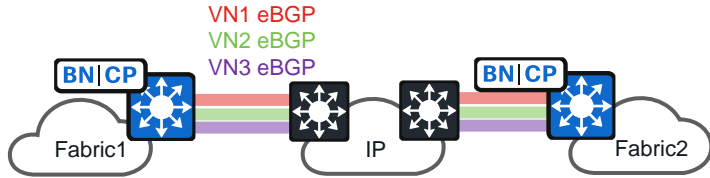
- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.

## 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 implementation flexibility, Border Node port density and speed. [Independent Domains PDG](#).
- Colocated SDWAN Edge for L3VN-VPN stitching with SGT data plane. IMPORTANT: Read [Integrated Domains PDG](#) for functional restrictions.

# 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, for those prepared to brave 0830 on Friday.
- LISP is at the core of Cisco SD-Access: Efficient, scalable, flexible and evolving.

# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at



<https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>

# Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand).



The bridge to possible

Thank you

CISCO *Live!*

CISCO *Live!*

ALL IN