Cisco
Software Defined Access

Solution Fundamentals

Gareth Taylor
Solutions Engineer

BRKENS-2810

Agenda

01 Why Cisco SD-Access LISP?

02 Roles & Terminology

03 Fabric Fundamentals

04 Multiple Fabric Sites

05 Conclusion

Gareth Taylor

Solutions Engineer, Cisco NZ

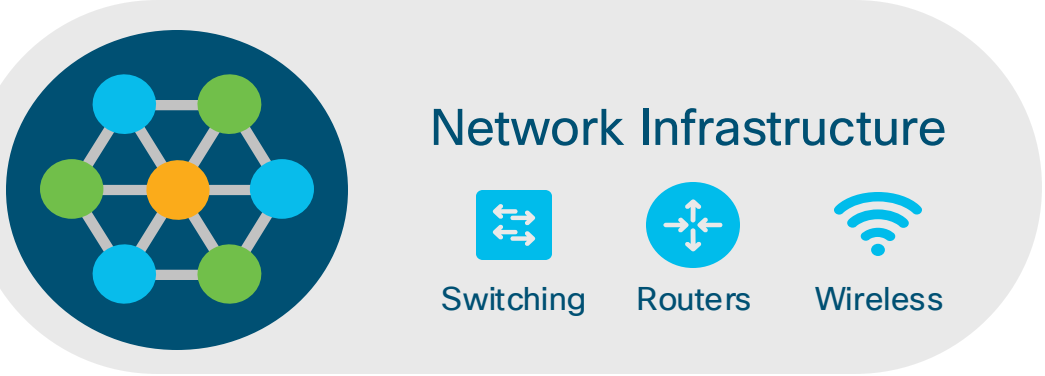
CCIE #4243 (ret)

- 25 years with Cisco
- Voice, Switching, Wireless, Security
- When not working, I’m out riding, or travelling.

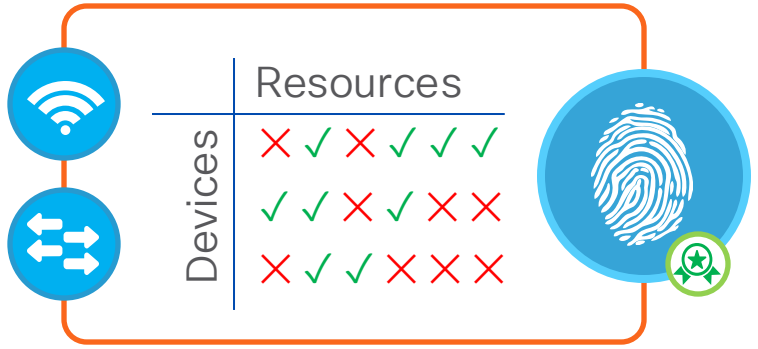
Why Cisco SD-Access LISP?

Traditional Networking Challenges

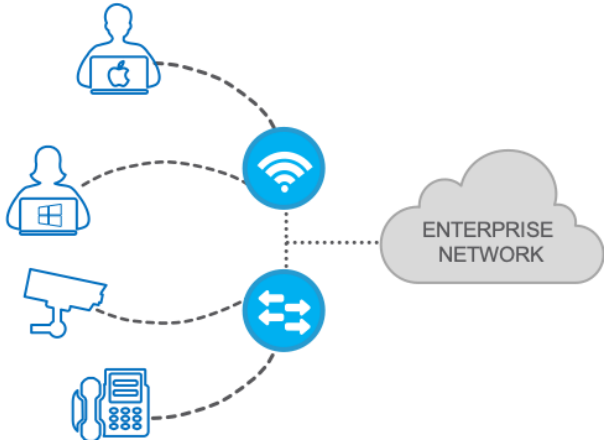
Network Deployment Challenges



Network Security Challenges



Wireless and Wired Challenges

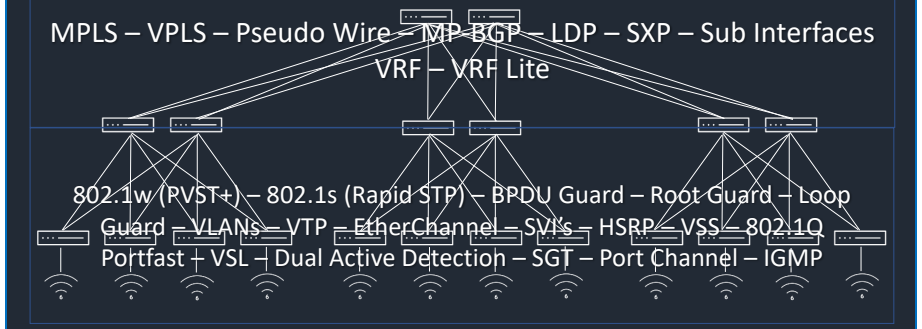


Network Operations Challenges

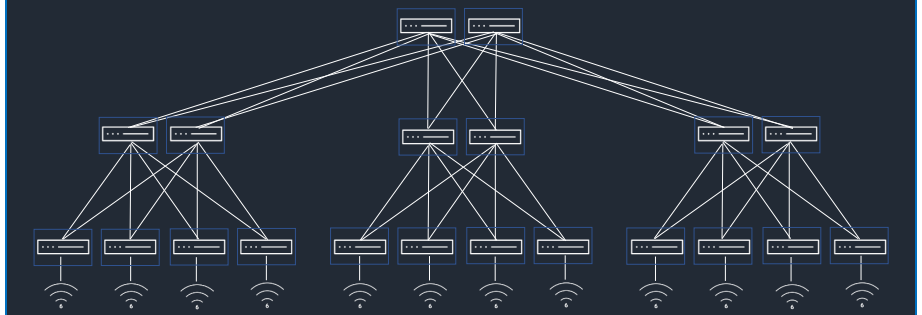
SDA Dramatically Simplifies the Network

Before

The *Traditional* Enterprise **Protocol** Stack

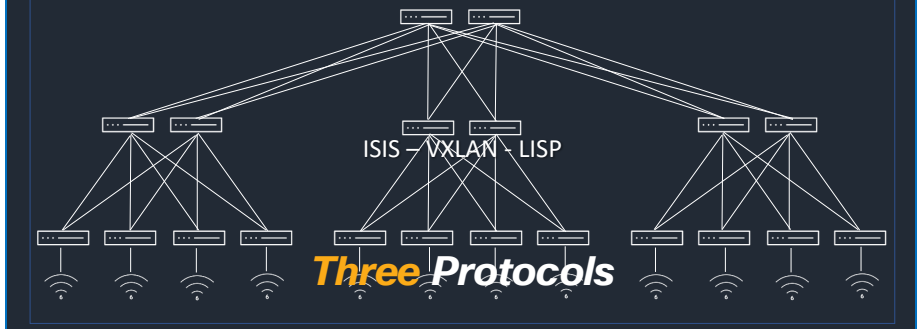


Unique **Configurations** Drive Up Complexity

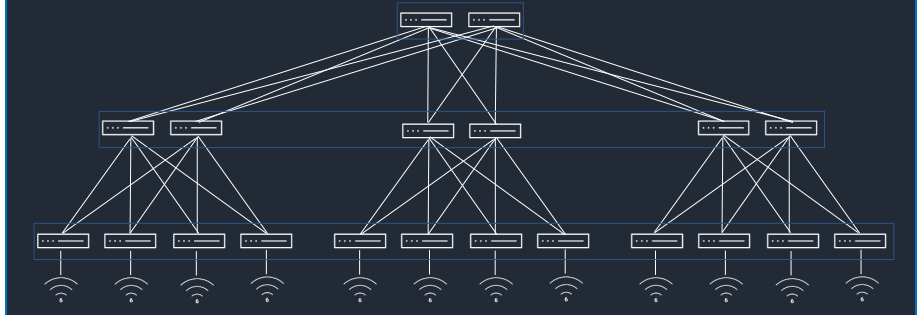


After

NEW Enterprise Protocol *Stack* with **SDA**

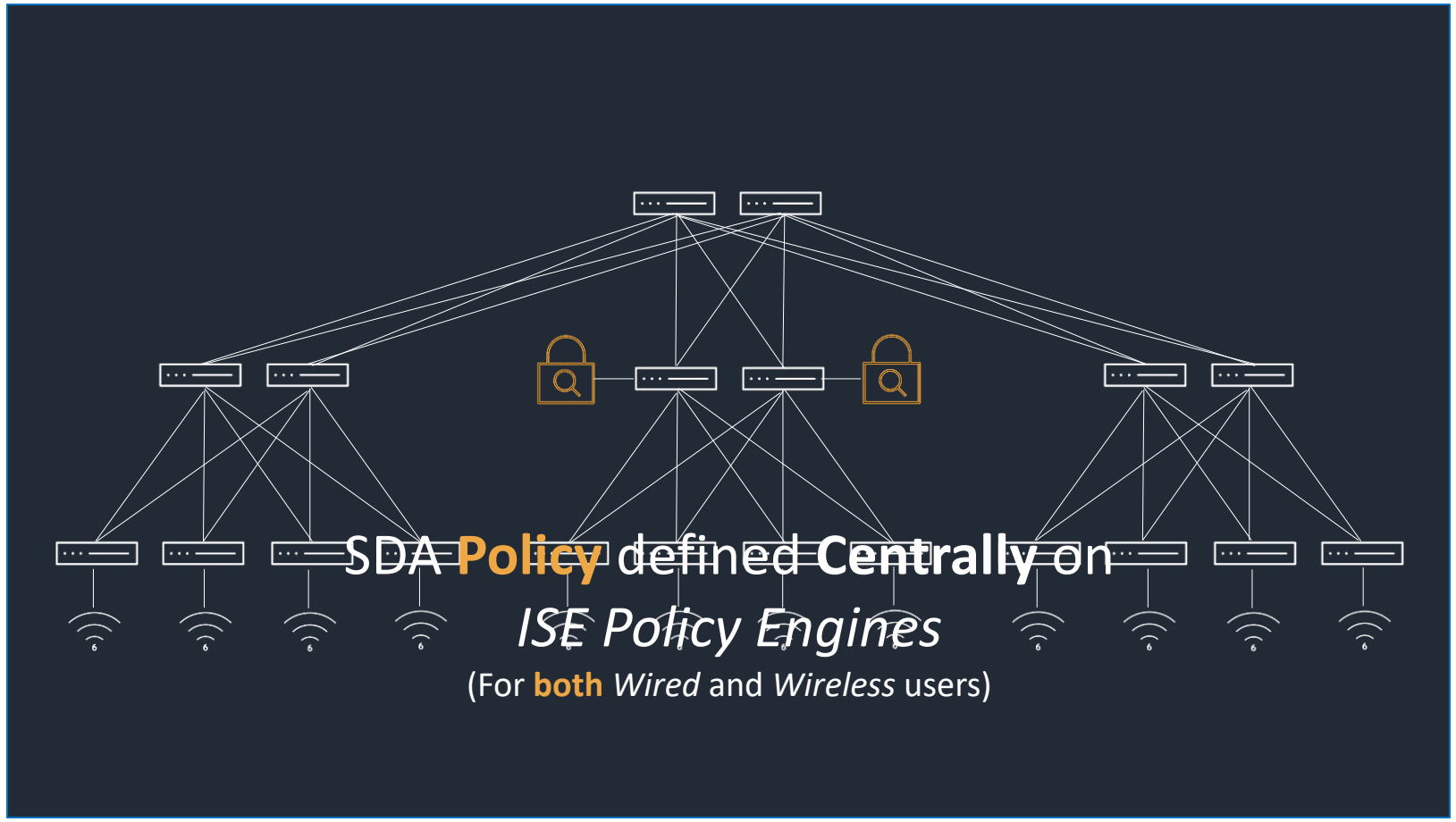


Common **Configurations** with **SDA**



***Eliminates* Layer 2** and ***Simplifies* Network Protocol Stack**

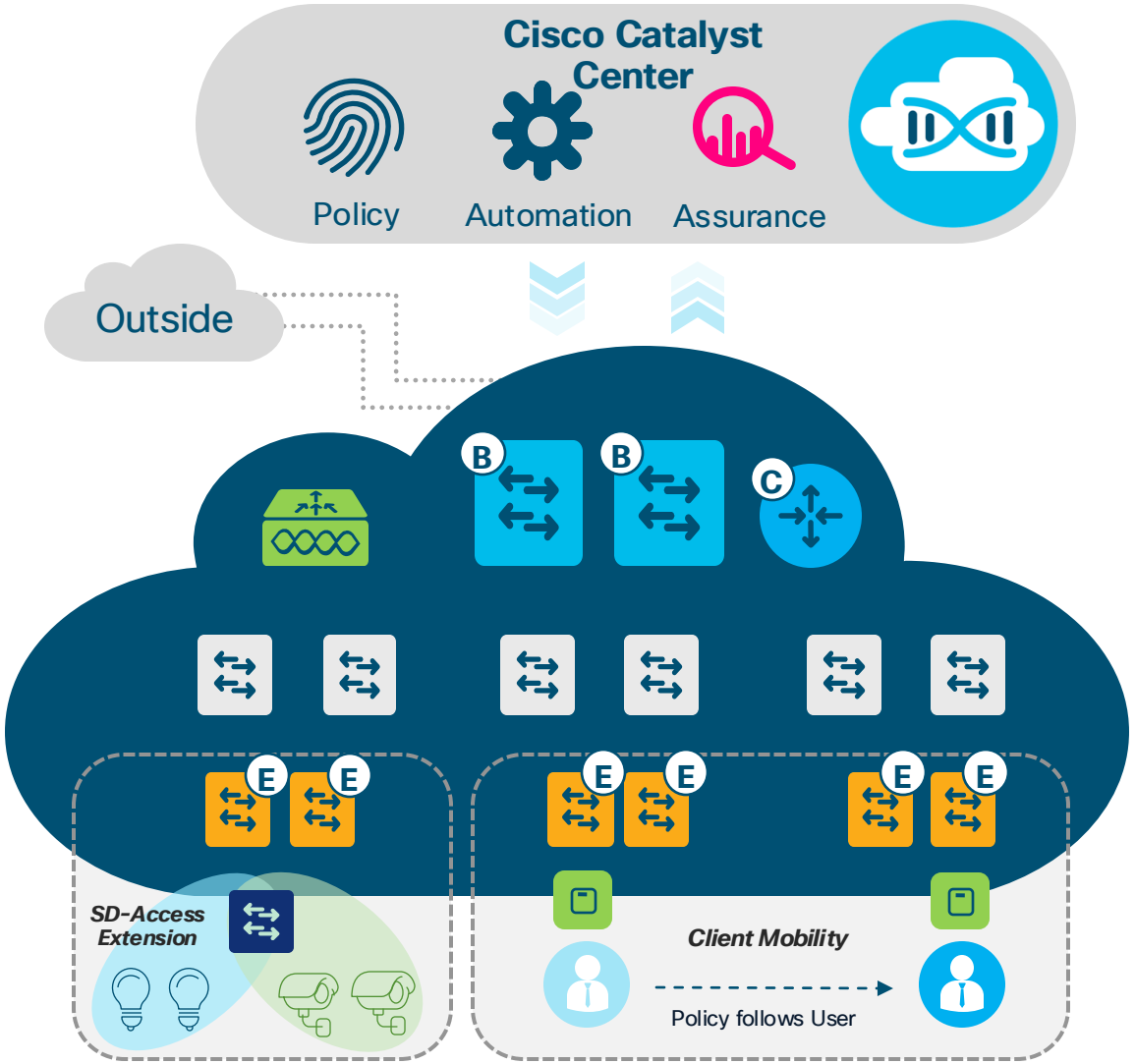
SDA Dramatically *Simplifies* the Network



Single Policy Store for
Wired and ***Wireless Users***

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

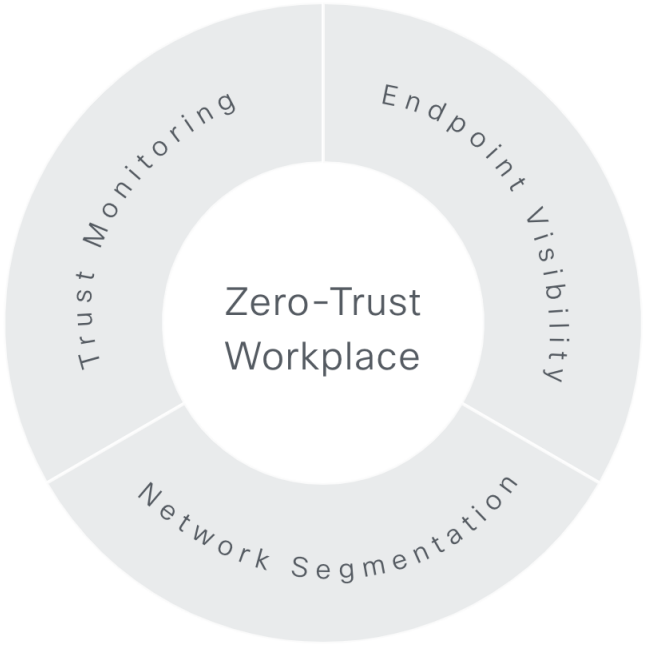
AI-Driven Insights and Telemetry

Analytics and visibility into user and application experience

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.



Modern, Open and Scalable Fabrics

IETF Standard based Protocols

Cisco Catalyst Center

Cisco SD-Access

LISP Fabric

IETF

Cisco Catalyst 9000

BGP EVPN Fabric

IETF

Enterprise Healthcare Education Financial Public Sector Manufacturing Hospitality Media Transportation Retail

cisco

Flexible Fabric Options Tailored to *Customer Outcomes*!

Cisco SD-Access with LISP Control Plane VXLAN Data Plane

Network Simplification

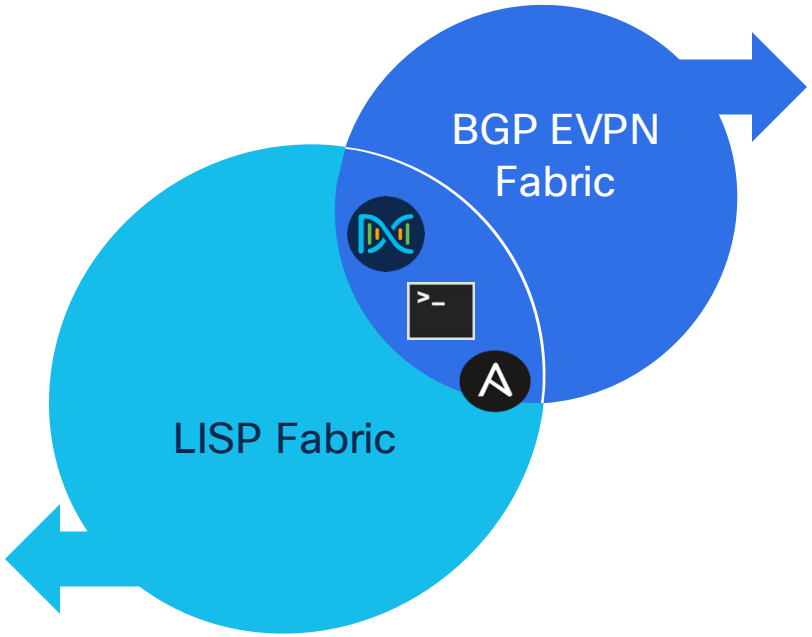
Lightweight, extensible, massive scale with rapid convergence. Single overlay for wired and wireless

Mobility First Requirement

Fabric Integrated Wireless, L2 Mobility, enhanced wireless performance

Segmentation

Zero-Trust Architecture with Unified Wired and Wireless Policy



BGP EVPN Control Plane VXLAN Data Plane

One Fabric Architecture (Campus and DC)

Operational ease with a single familiar protocol

Multi-vendor interoperability

Vendor-agnostic solution with unique Cisco differentiators

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

SD-Access Momentum

Deployments

5400+ TOTAL

Momentum

Double Digit

YoY growth in customers

Key Use case

60%

Wireless

Deployment Scale

38K+ Sites

2.6M+ Devices

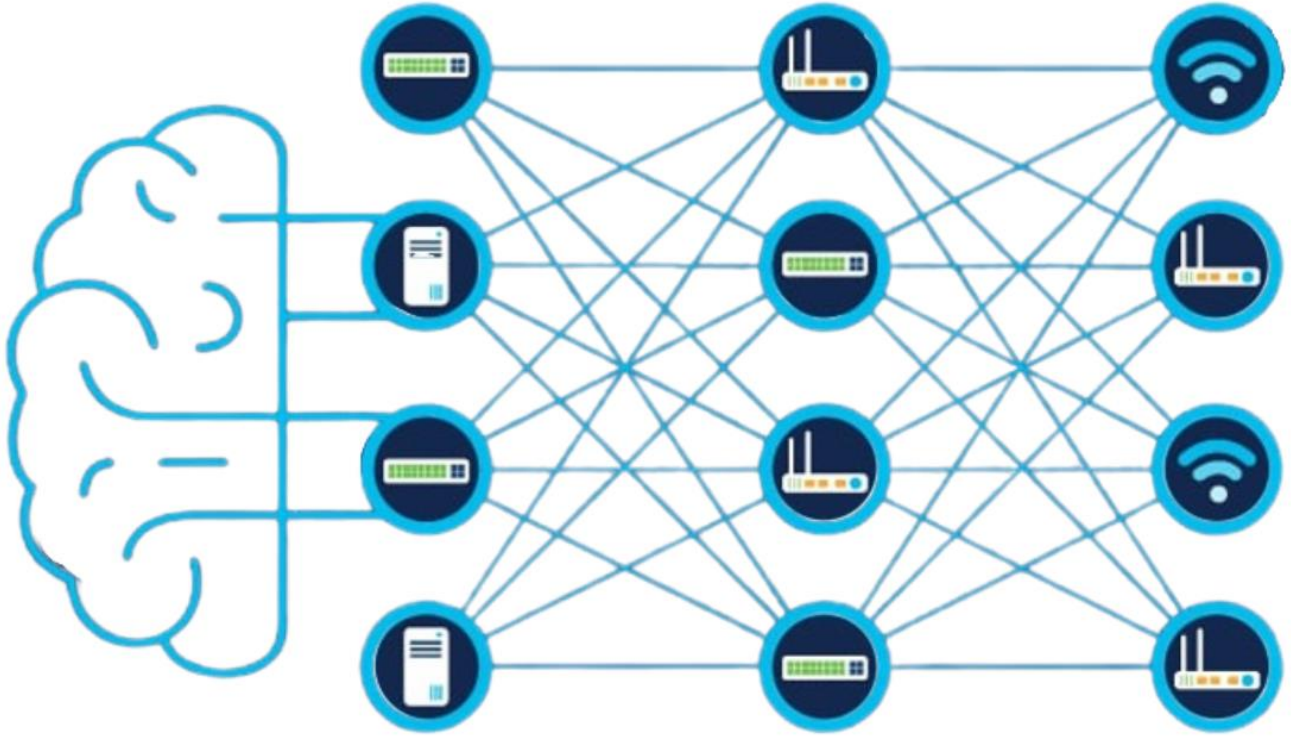
Top verticals: Education, Government, Finance, Healthcare and Manufacturing

Roles and Terminology

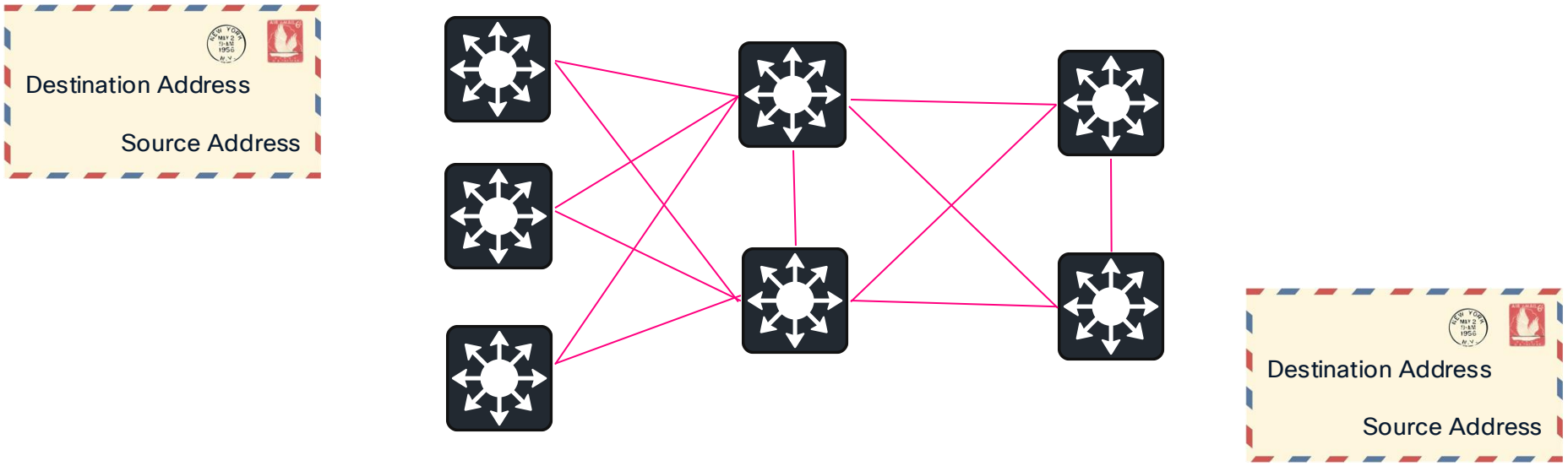
1. Concepts
2. SD-Access Roles
3. Fabric Constructs

What is a Network Fabric?

- Transports data from source to destination.
- Mesh of connections between network devices.
- Usually refers to a virtualized, automated lattice of overlay connections.

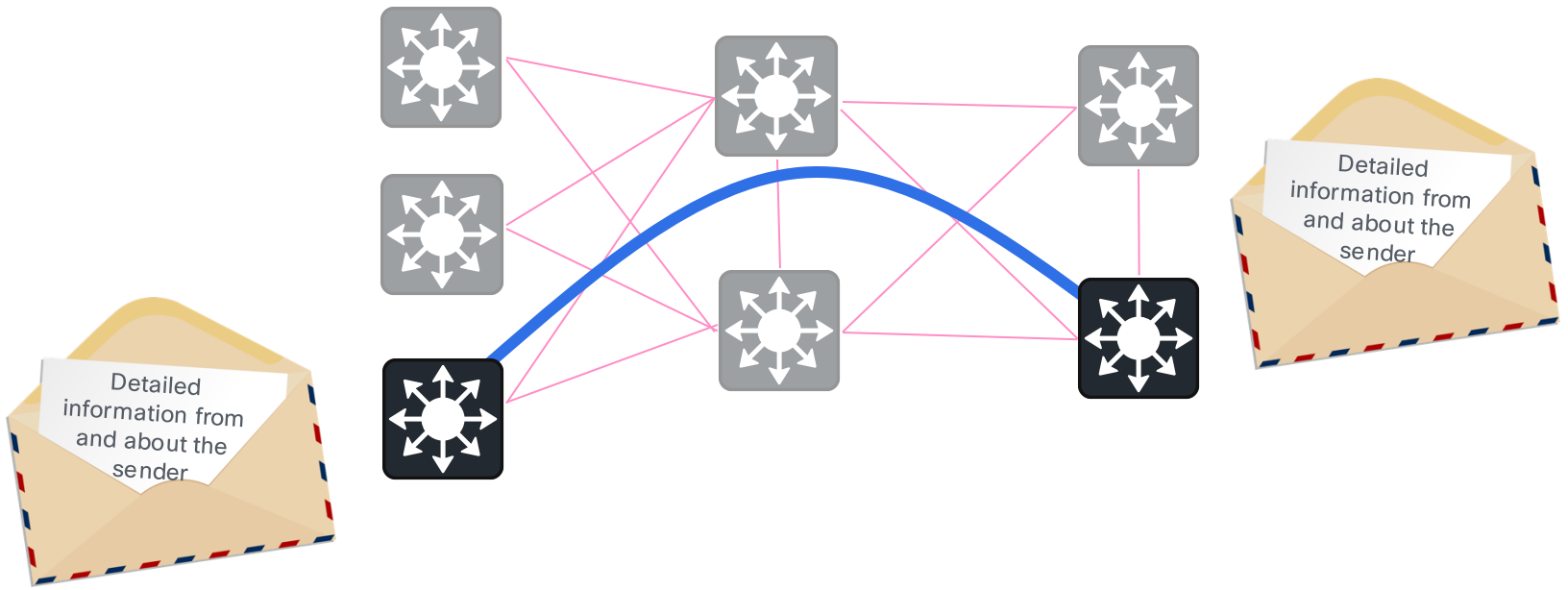


Underlay and Overlay



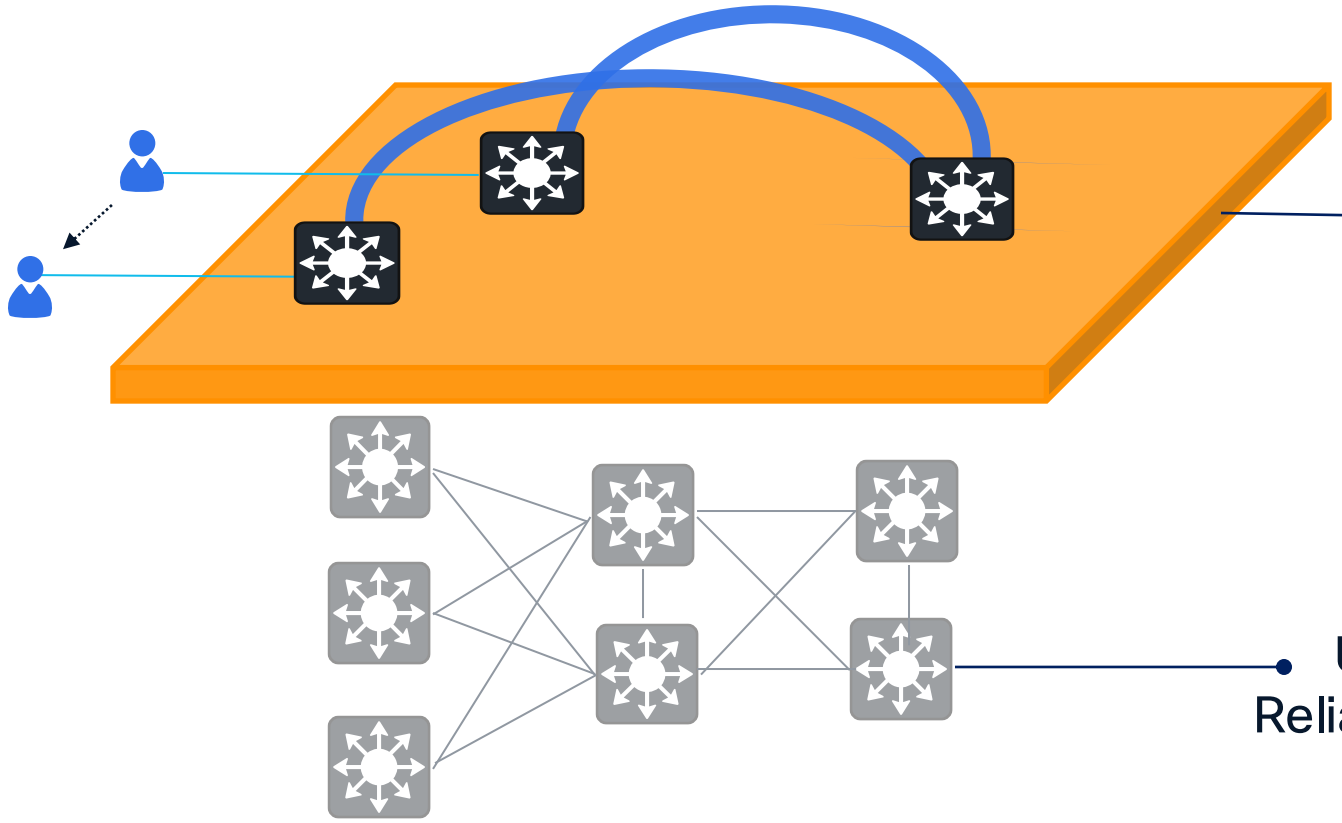
Underlay Network = Physical Infrastructure to provide IP reachability with redundancy and resiliency.

Underlay and Overlay



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

Underlay and Overlay

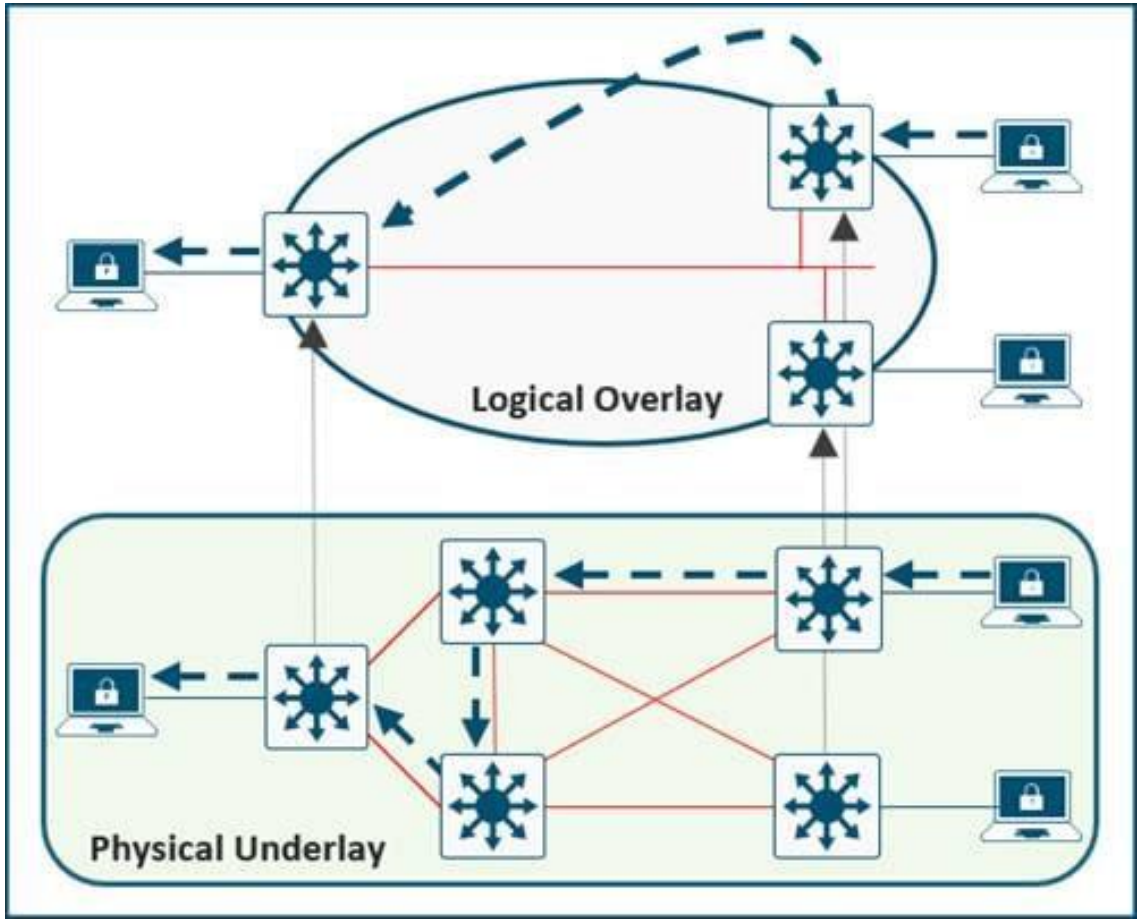


Overlay (Fabric): Flexible, Scalable and Extensible. Easy to add/modify services. Optimizes mobility events.

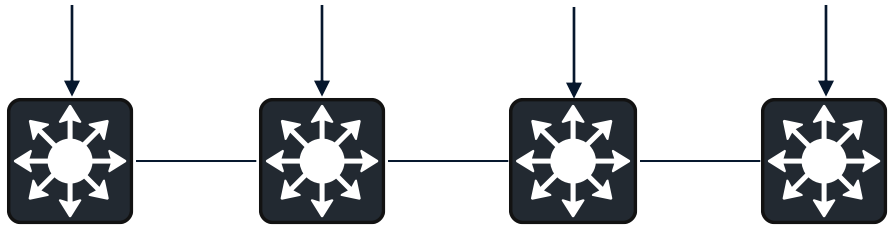
Underlay: Build and forget!
Reliable, manageable, and simple.

What is an Overlay?

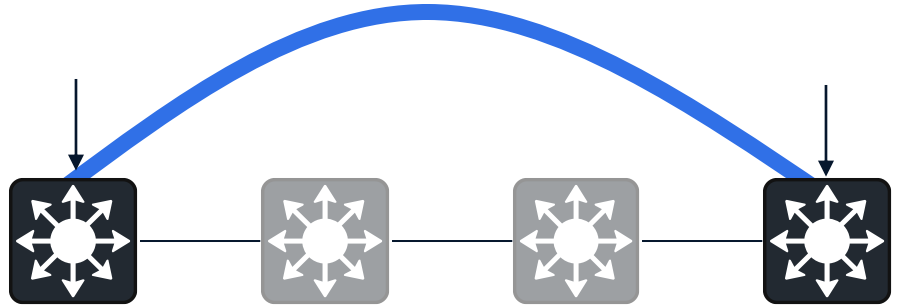
- An Overlay network is a logical topology used to virtually connect devices, built over an arbitrary physical Underlay topology.
- Examples of overlay technologies:
  - GRE
  - MPLS
  - IPsec
  - CAPWAP
  - LISP
  - VXLAN
  - BGP EVPN
  - SD-WAN
  - ACI
  - OTV



Underlay and Overlay

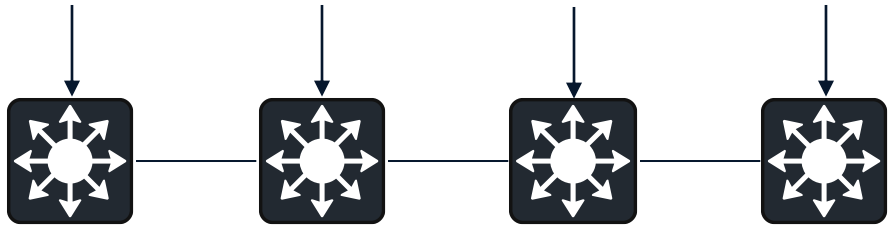


Would you configure network segmentation hop-by-hop?

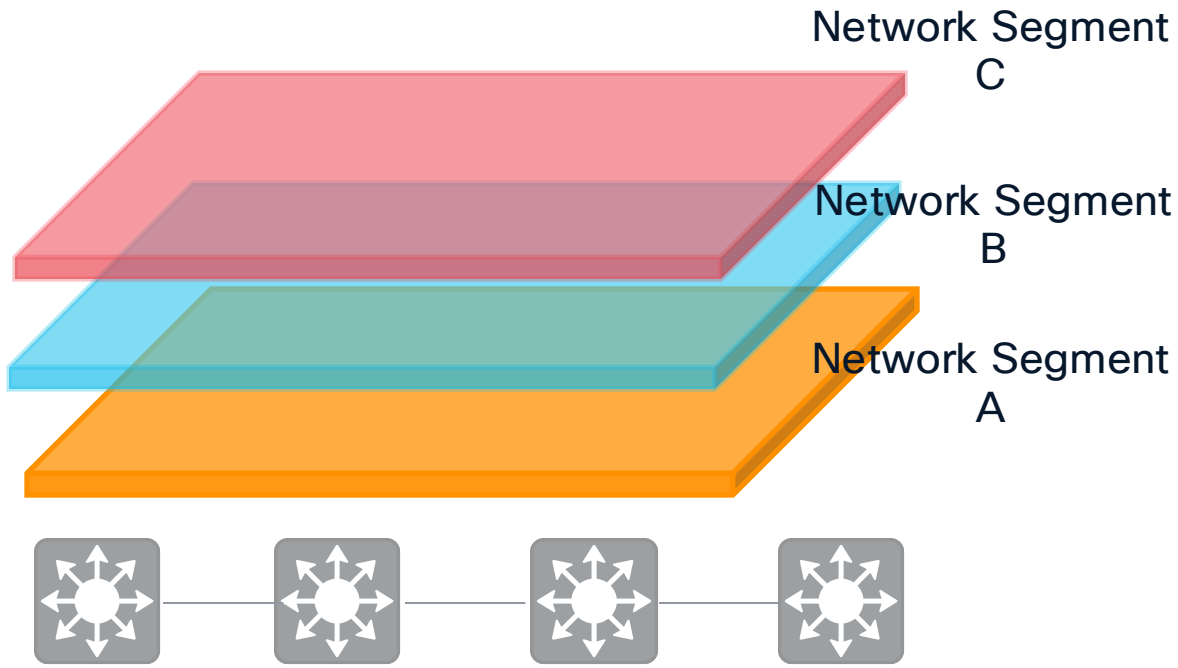


Or simply carry the segmentation tags in the overlay?

Underlay and Overlay



Would you configure network segmentation hop-by-hop?

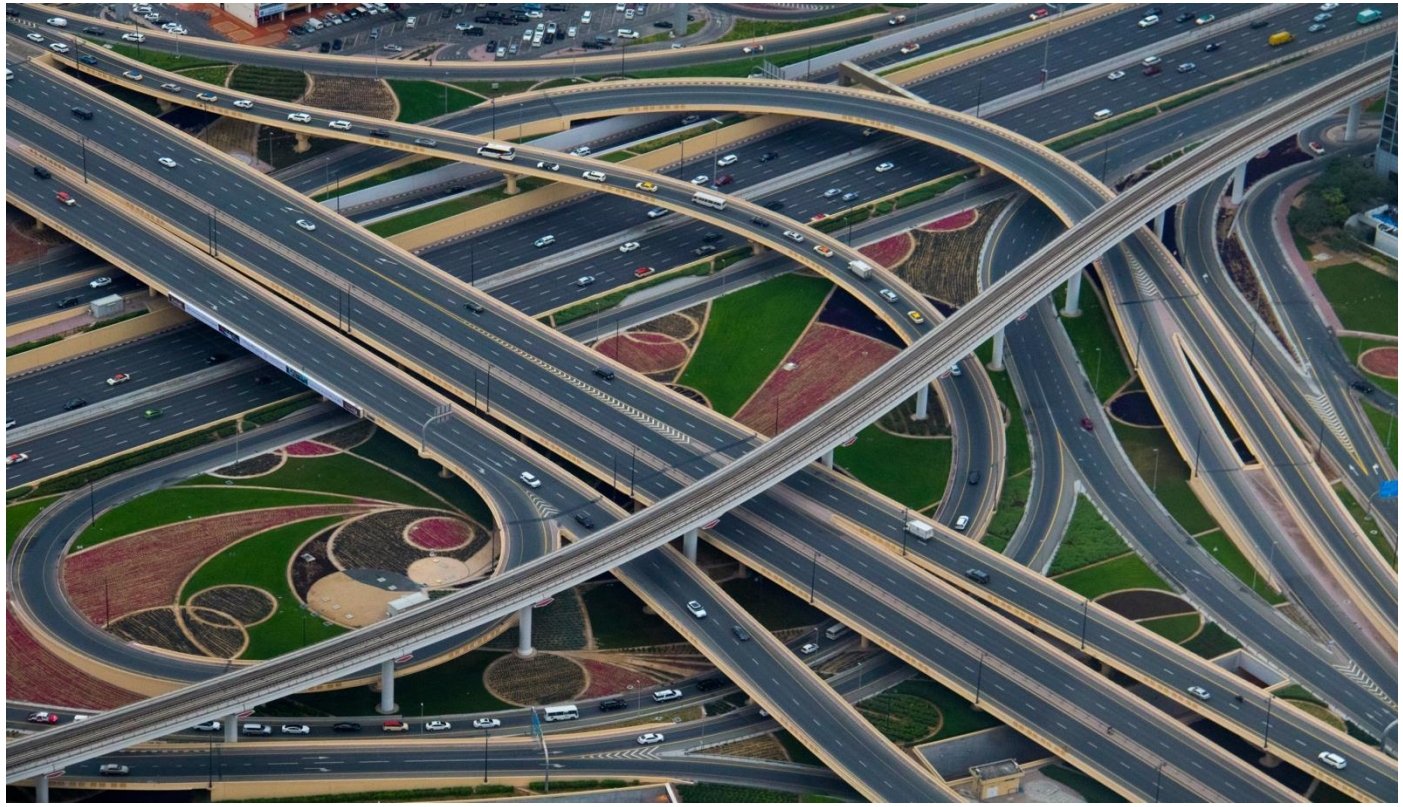


Multiple segments in the overlay that underlay is unaware of!

Underlay and Overlay

In context of SD-Access LISP

What about our good friend Underlay?



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

BGP VRF-Lite for external communications

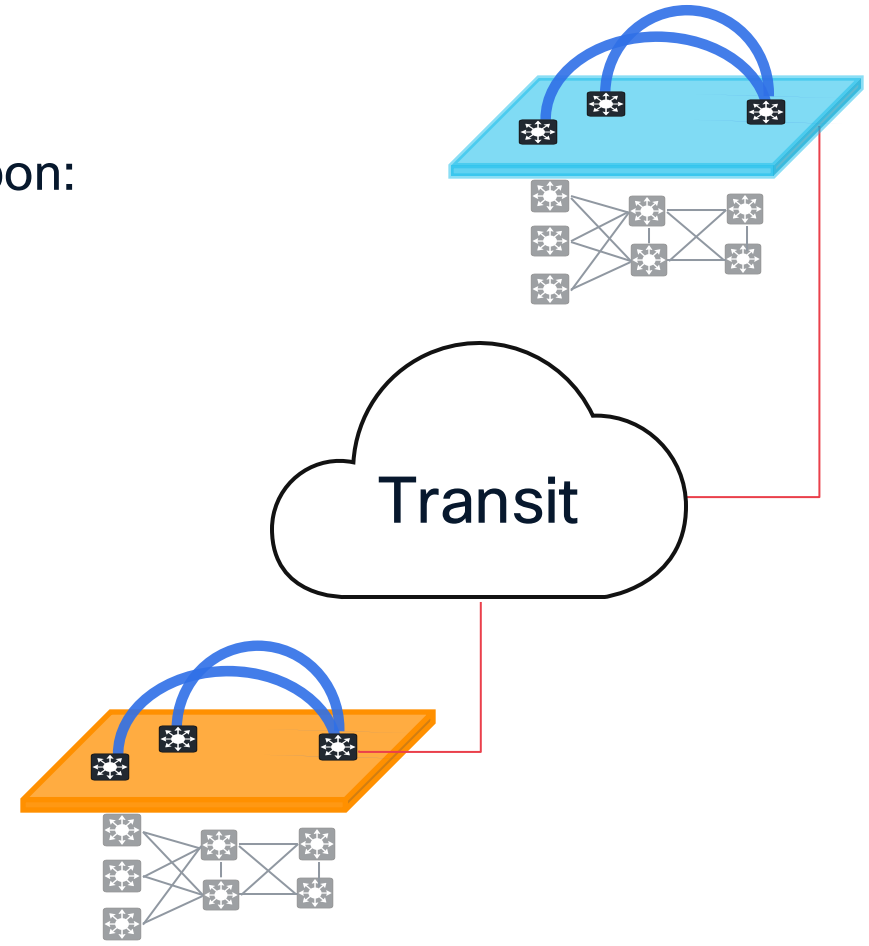
What is an SD-Access Fabric Site?

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:

- Collection of Edge Nodes, Border/CPs, and optionally Wireless LAN Controllers/Access Points.
- Geographical location.
- Required scale, network devices.
- Failure domain scoping.
- RTT.
- Underlay connectivity attributes.

Multiple fabric sites interconnected by a “Transit”.

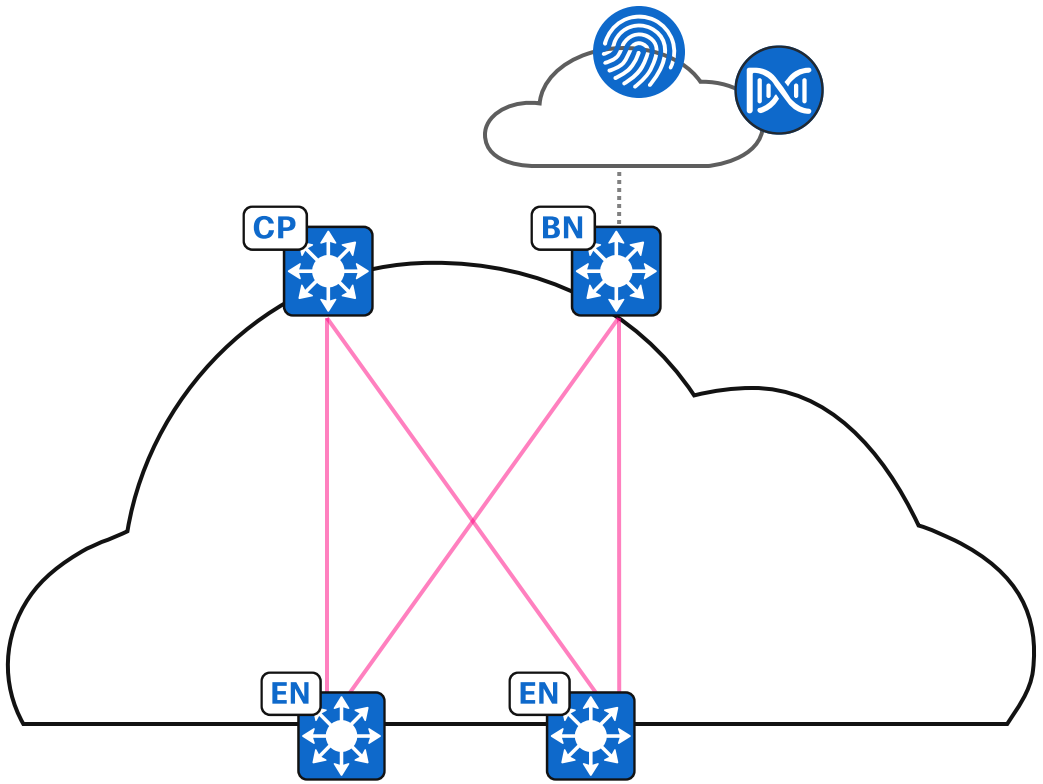


Roles and Terminology

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

Cisco SD-Access Roles

Key Roles for a Complete Wired and Wireless SDA Fabric 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

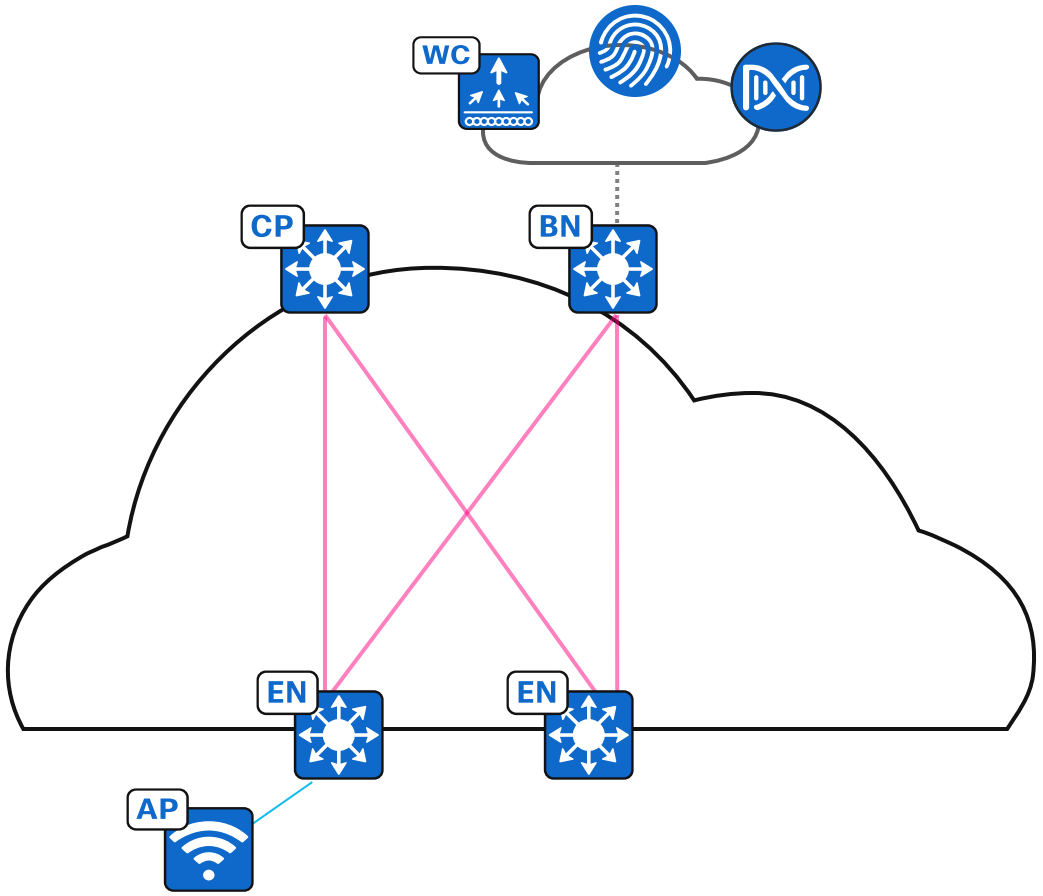
Connects external L3 and L2 networks to the Cisco SD-Access fabric.

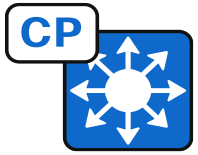
Edge Nodes

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

Cisco SD-Access Roles

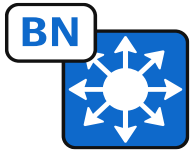
Key Roles for a Complete Wired and Wireless Campus Experience





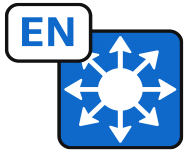
Control Plane Node

Map System that tracks endpoint to fabric node relationships.



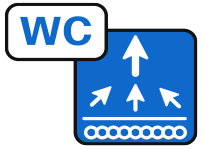
Border Nodes

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.

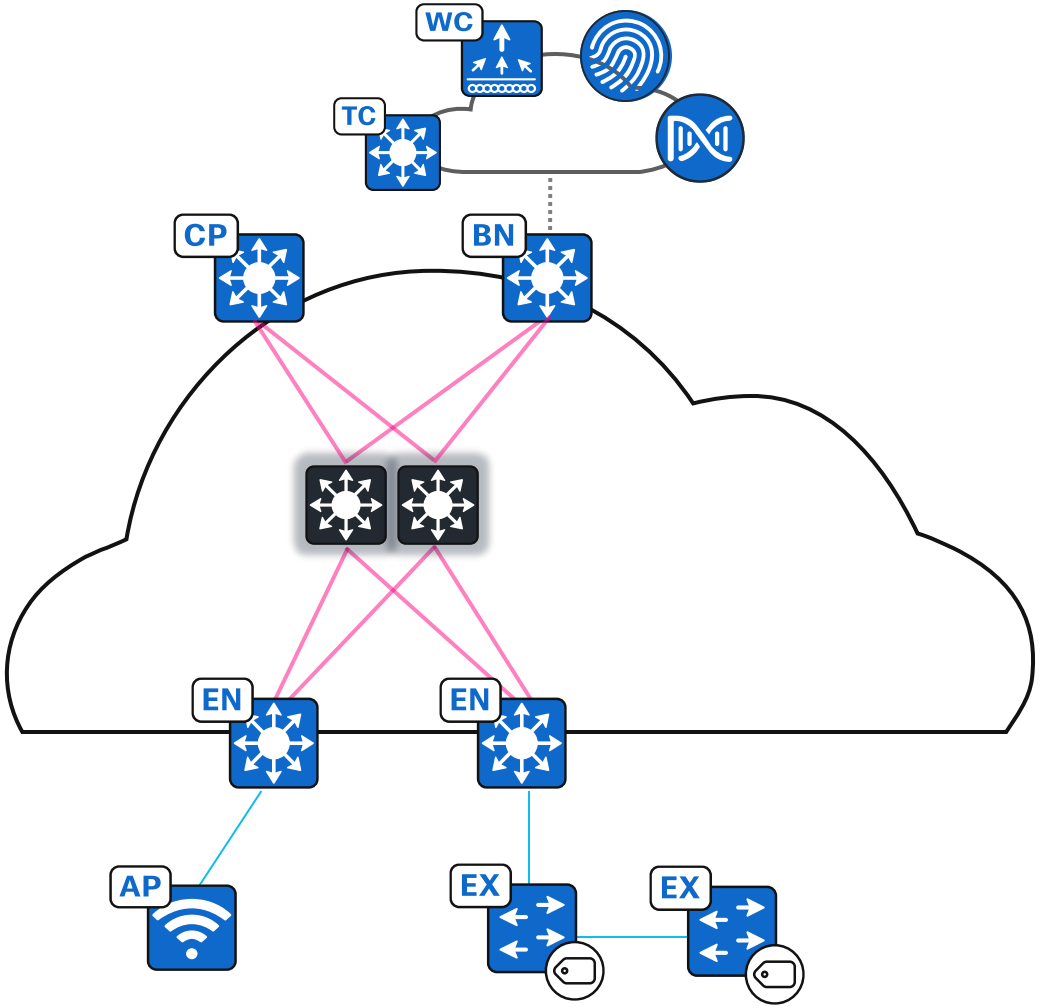
Fabric Access Point

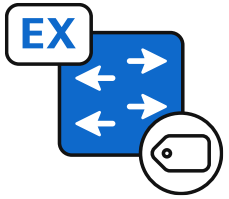
Switches endpoint traffic to the adjacent Edge Node.

Cisco SD-Access Roles

Additional Roles for Reference

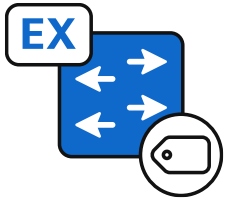
Additional Information





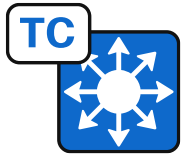
Extended Nodes

A switch operating at Layer 2 that extends fabric connectivity and optionally enforces micro-segmentation policy.



Policy Extended Nodes

Switch able to do Auth, VLAN & SGT assignment and policy enforcement at the edge, without VXLAN tunnelling.



Transit Control Plane Nodes

Facilitates connectivity of multiple SD-Access fabric sites while preserving end to end segmentation.

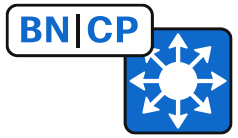
Intermediate Nodes

Moves data between fabric nodes. Can be one or many hops. Part of the underlay.

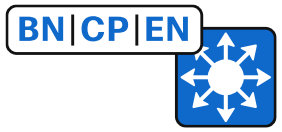
Cisco SD-Access Roles

Some of the Supported Colocations

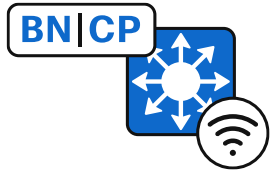
Additional Information



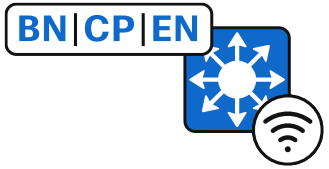
Border Node and Control Plane Node.



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



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



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

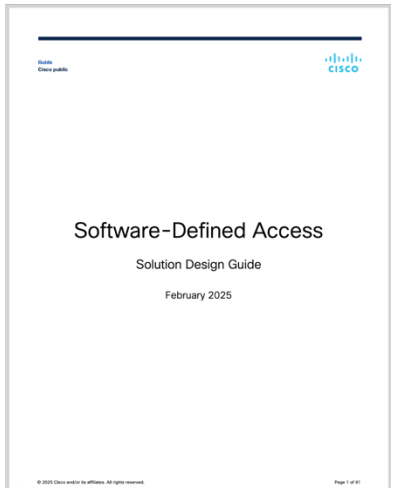
cisco

SD-Access Design Resources

Cisco Validated Design:
https://cs.co/sda-cvd

SDA Design Tool (use Chrome):
http://cs.co/sda-design-tool

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



SD Access Non-Fabric

Application: SDA LISP Release: 2.3.7.9 (recommended release) Device Role: Fabric Border and Control Plane Submit Query

Note:- From 2.3.7.x, Catalyst Center monitors third-party devices that are RFC 1213 SNMP MIB-II compliant. For details, see the Cisco Catalyst Center User Guide.
From 2.3.3.x, Catalyst Center scans End of Life (EoX) milestones for non-air gap customers. Supported devices: switches, hubs, routers, and wireless controllers (IOS/IOS-XE).

Device Role	Device Series	Device Model	Recommended Release	Supported Release
Fabric Border and Control Plane	Cisco Catalyst 8000V Cloud Edge Platform (Fabric Control Plane only)	C8000V	IOS XE 17.15.3a	IOS XE 17.18.x IOS XE 17.15.x IOS XE 17.12.x IOS XE 17.9.x

Cisco SD-Access Fabric

Control Plane Node Maintains a Host and Network Tracking Database

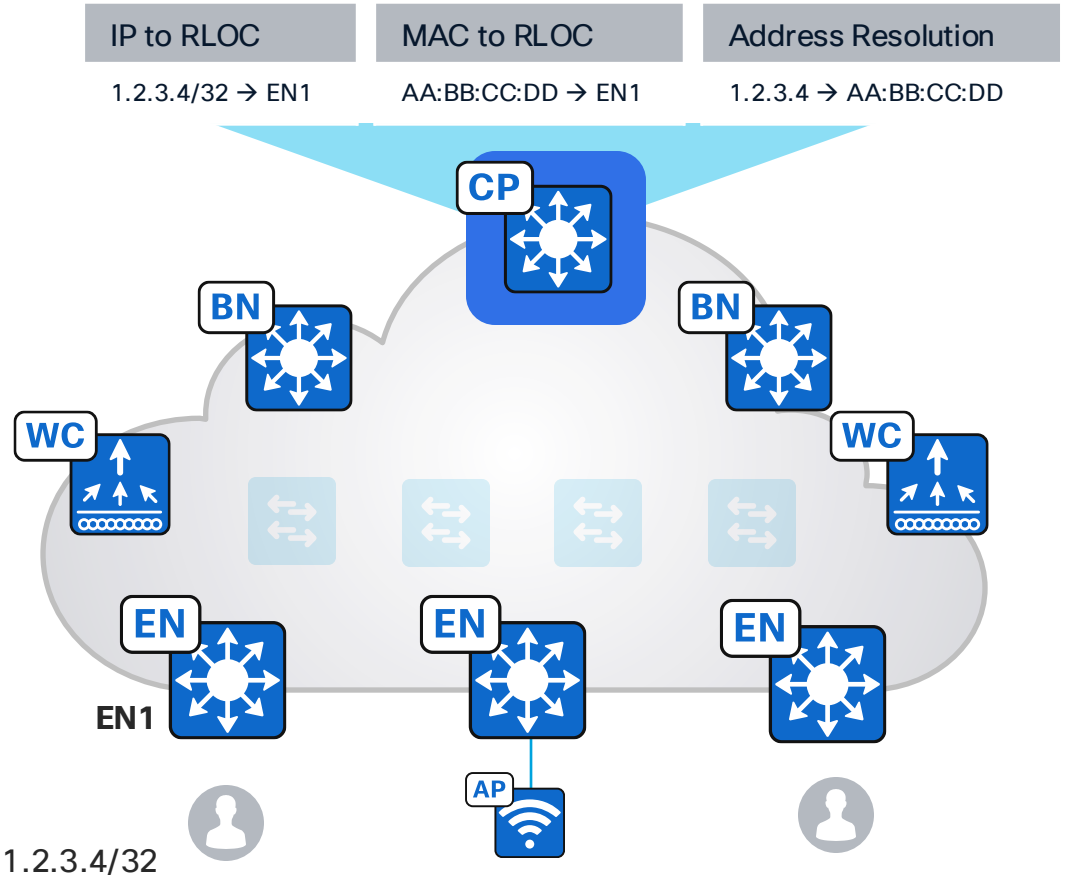
A simple Host Database that maps Endpoint IDs to locations, along with other attributes.

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.

Publishes registrations to Subscribers (Border Nodes).

Resolves lookup requests from Edge Nodes and Border Nodes, to locate destination Endpoint IDs.



Cisco SD-Access Fabric

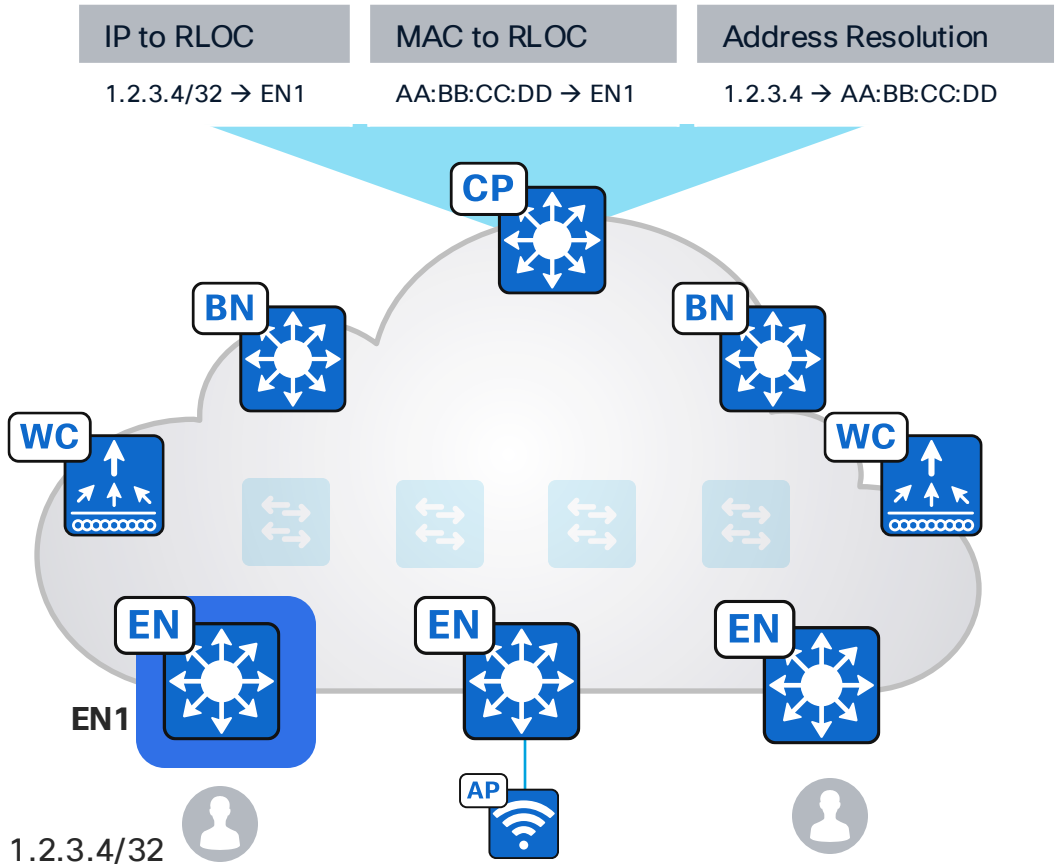
Edge Node Provides First Hop Services for Endpoints

Responsible for Authenticating and Authorizing wired endpoints (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.



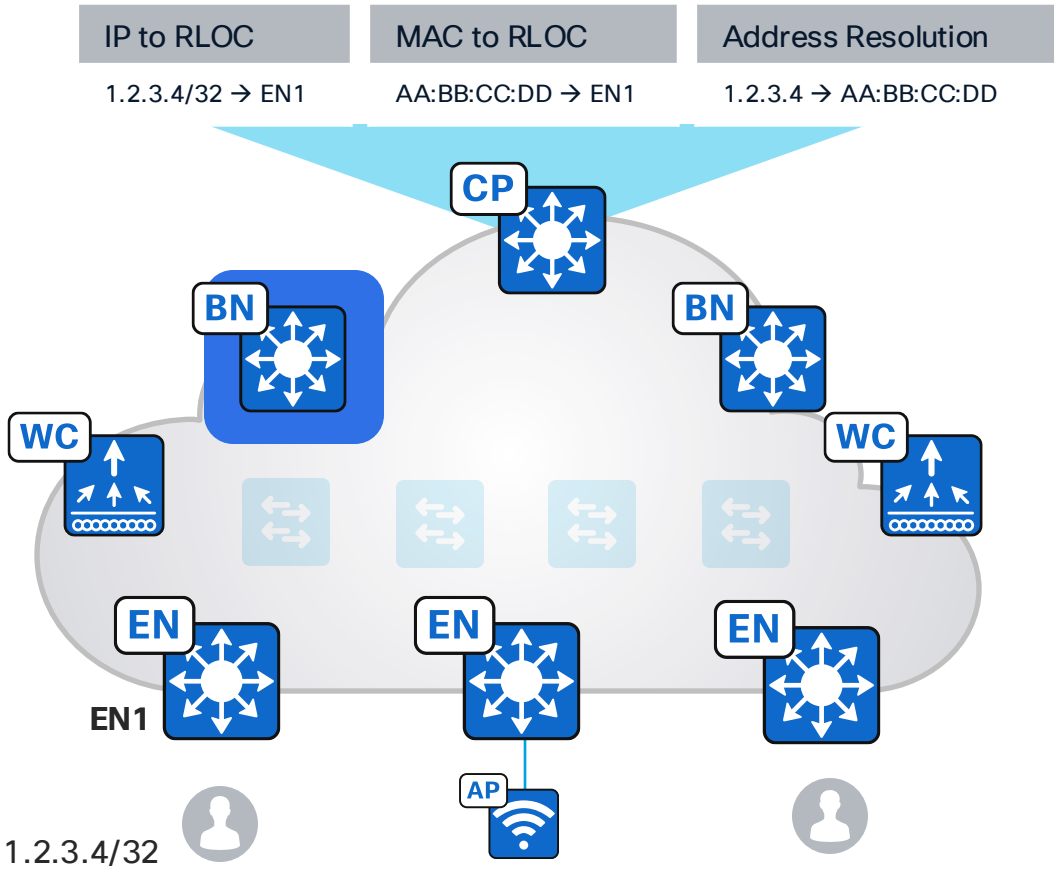
Cisco SD-Access Fabric

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.

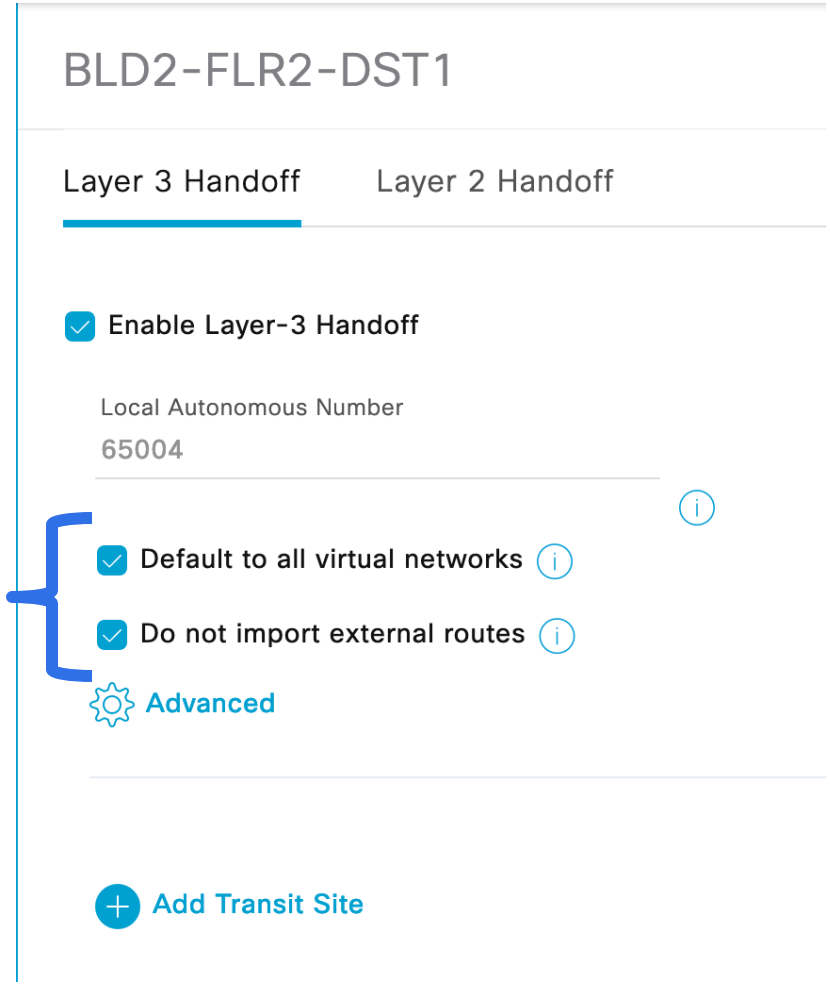


Cisco SD-Access Fabric

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.
- 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

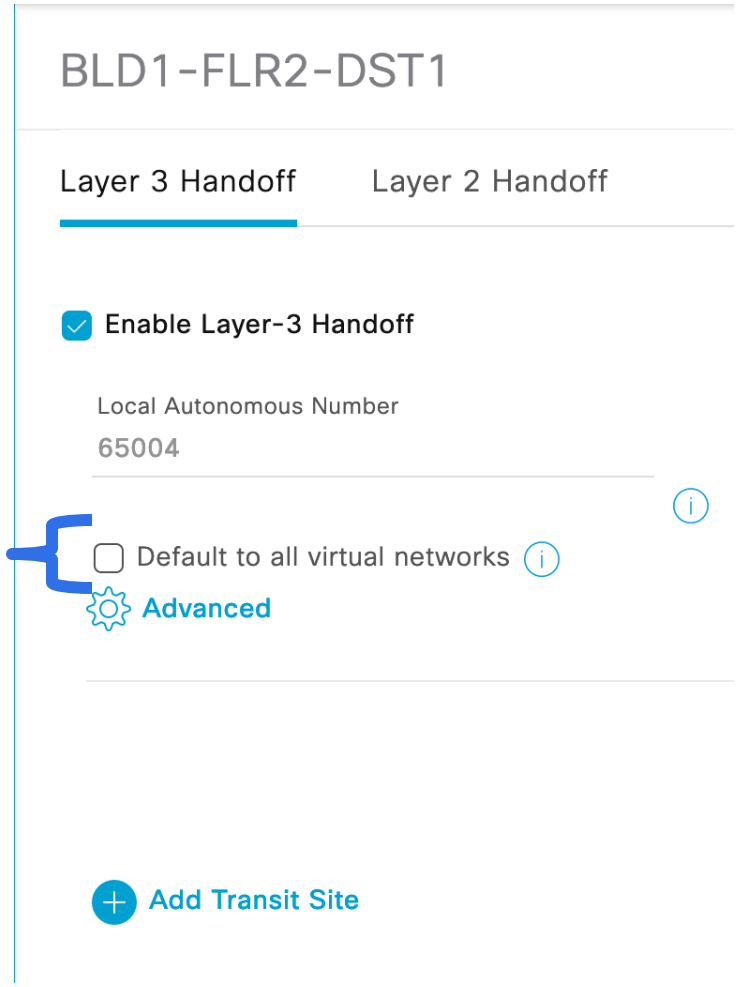
Border Node is the Fabric Site Entry and Exit for Network Traffic

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

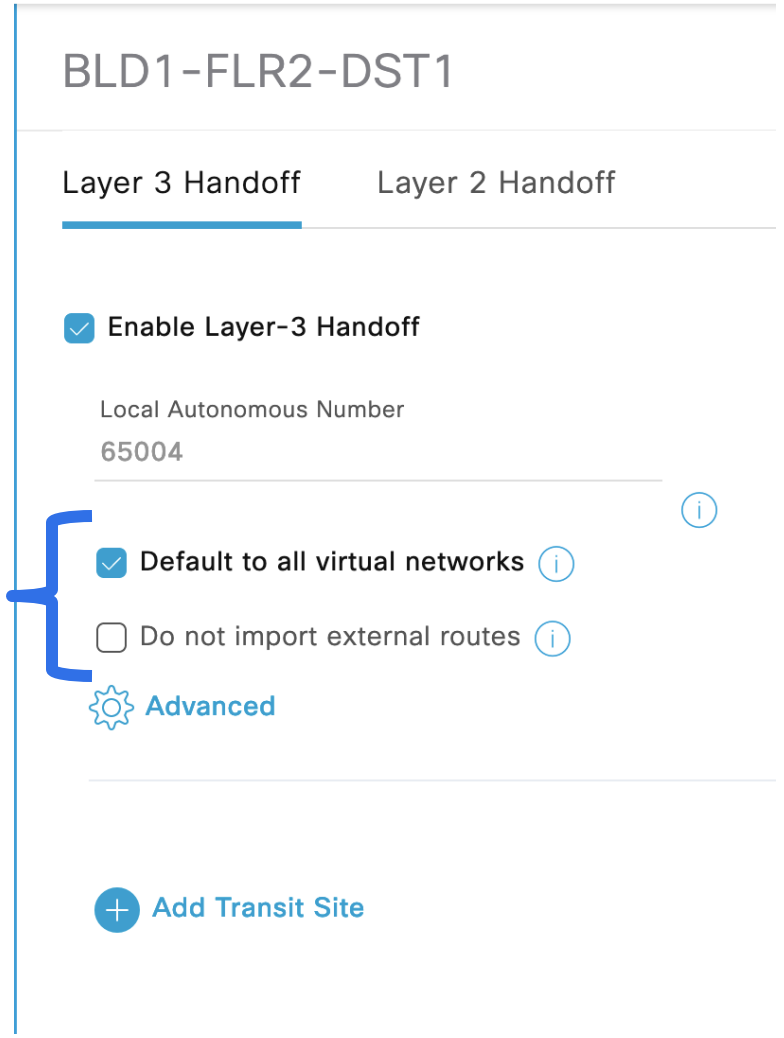
Border Node is the Fabric Site Entry and Exit for Network Traffic

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.

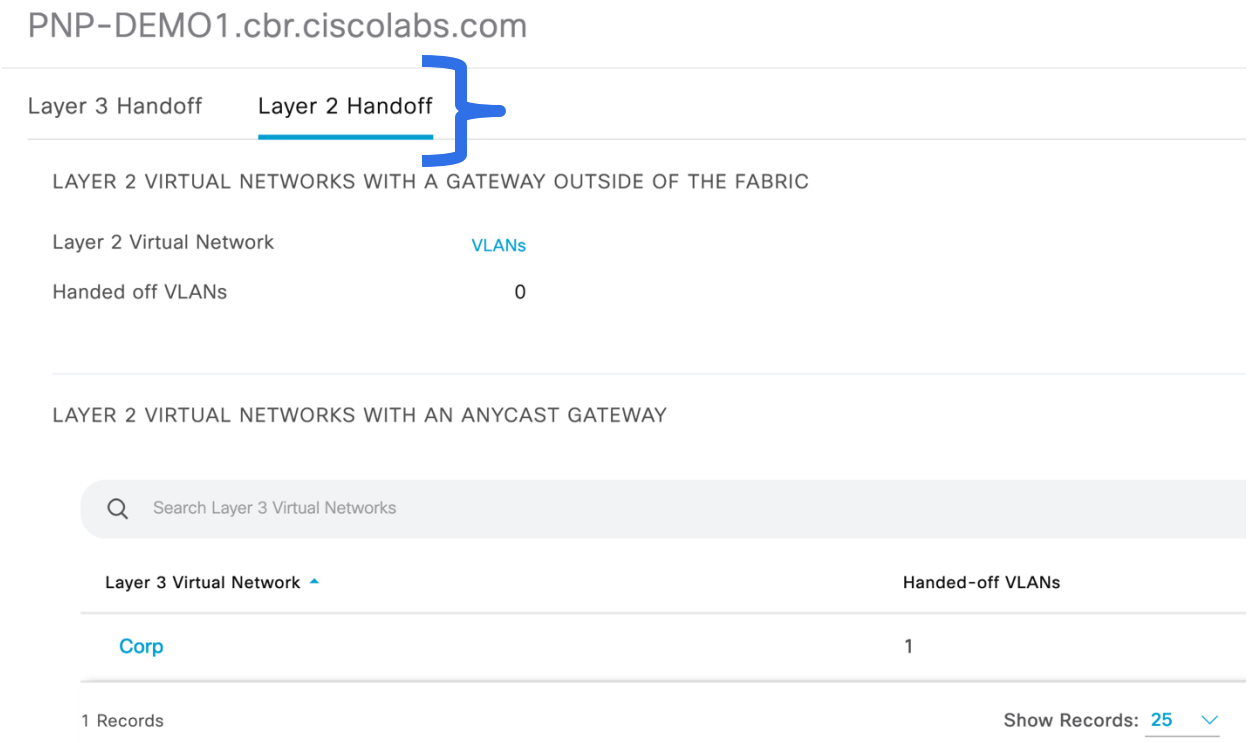


Cisco SD-Access Fabric

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

Layer 2 Border Node:

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



Cisco SD-Access Fabric

Fabric Enabled Wireless for Unified Management, Policy and Data Planes

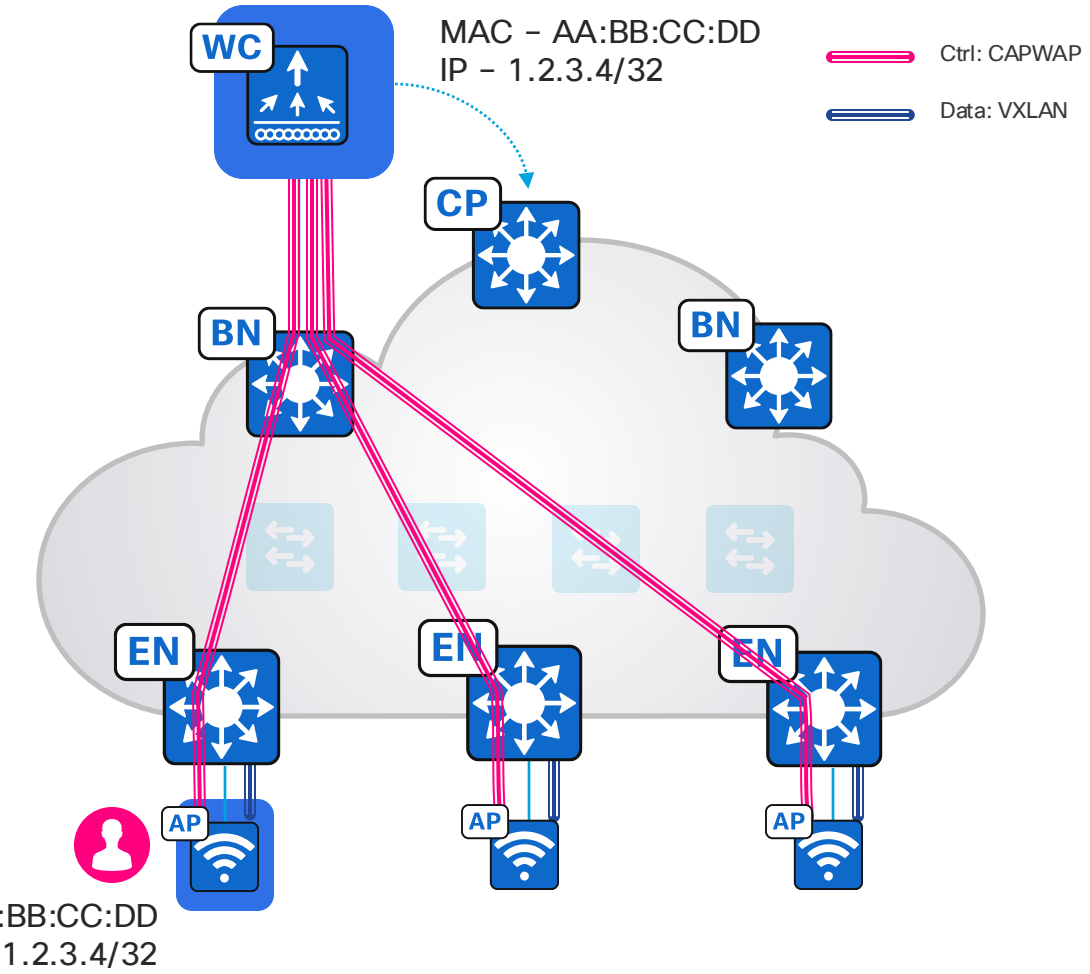
Fabric WLC accessible though a Fabric Border Node (Underlay). Can be several hops away.

Fabric Enabled APs reside in a dedicated IP range and communicate with the Fabric 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

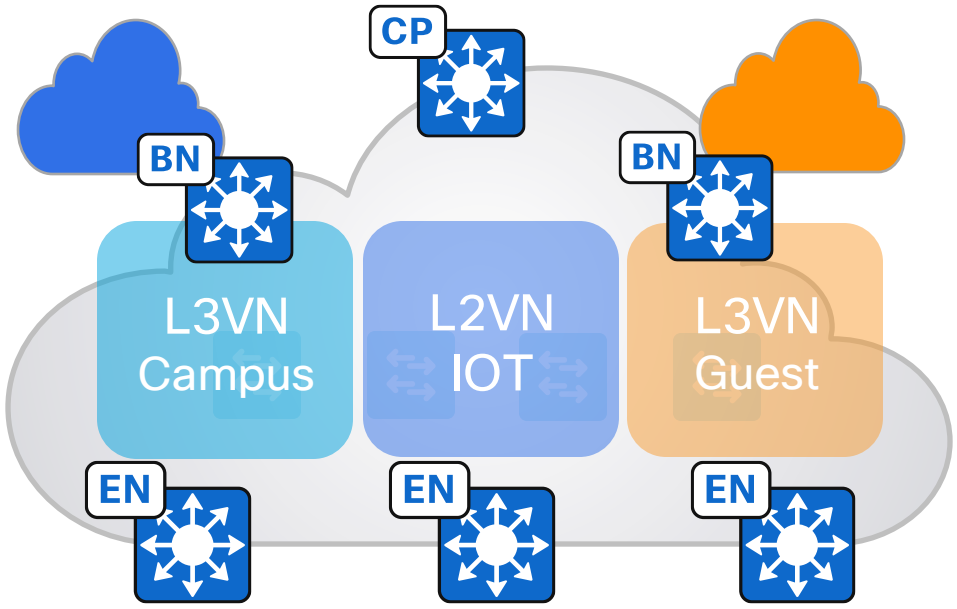
1. Concepts
2. SD-Access Roles
3. **Fabric Constructs**

Cisco SD-Access Fabric

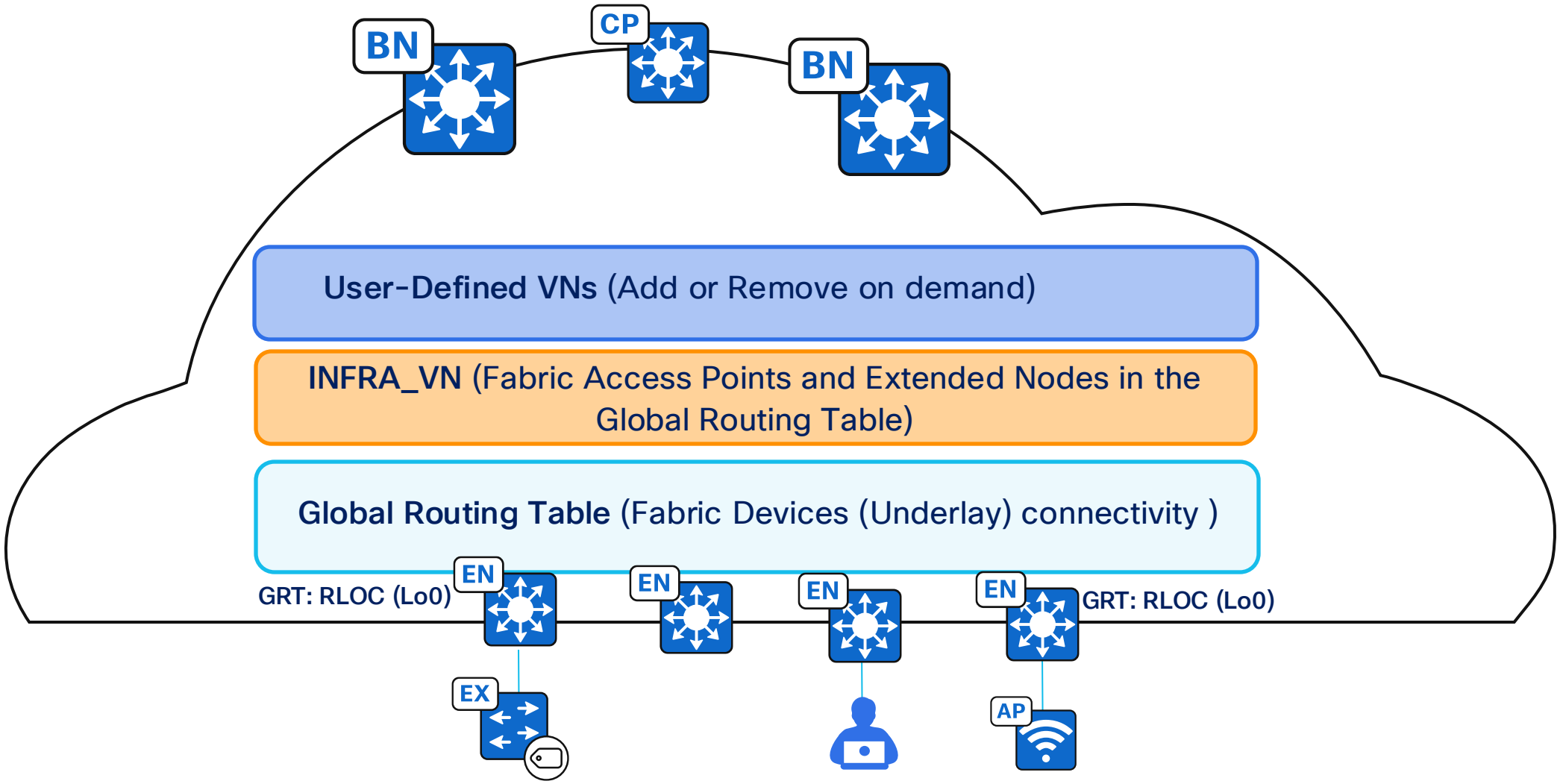
Virtual Networks

Additional Information

- 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.

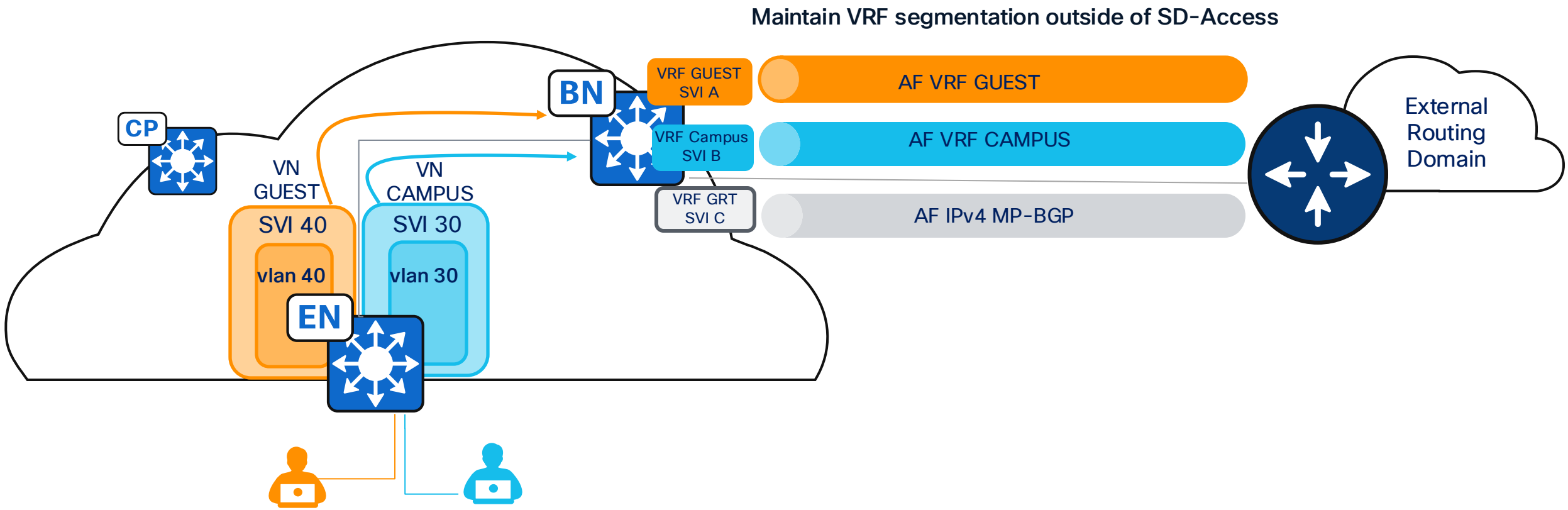


Layer 3 Virtual Networks



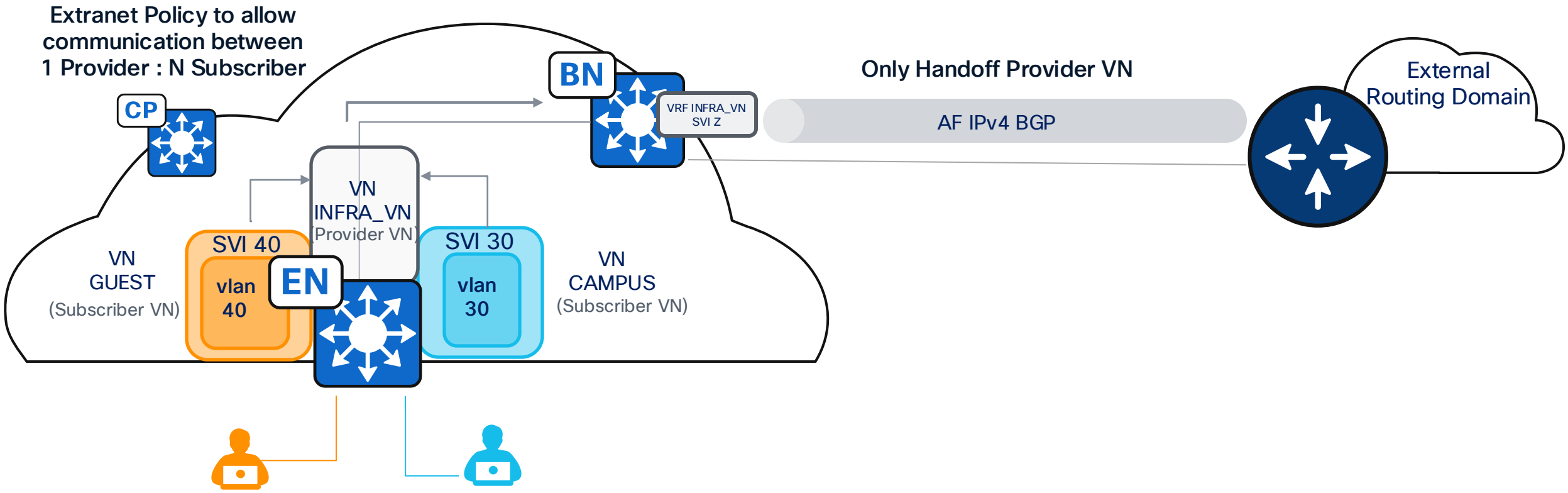
Layer 3 Handoff

Per-Layer-3-Virtual-Network Layer 3 Handoff using Peer Device



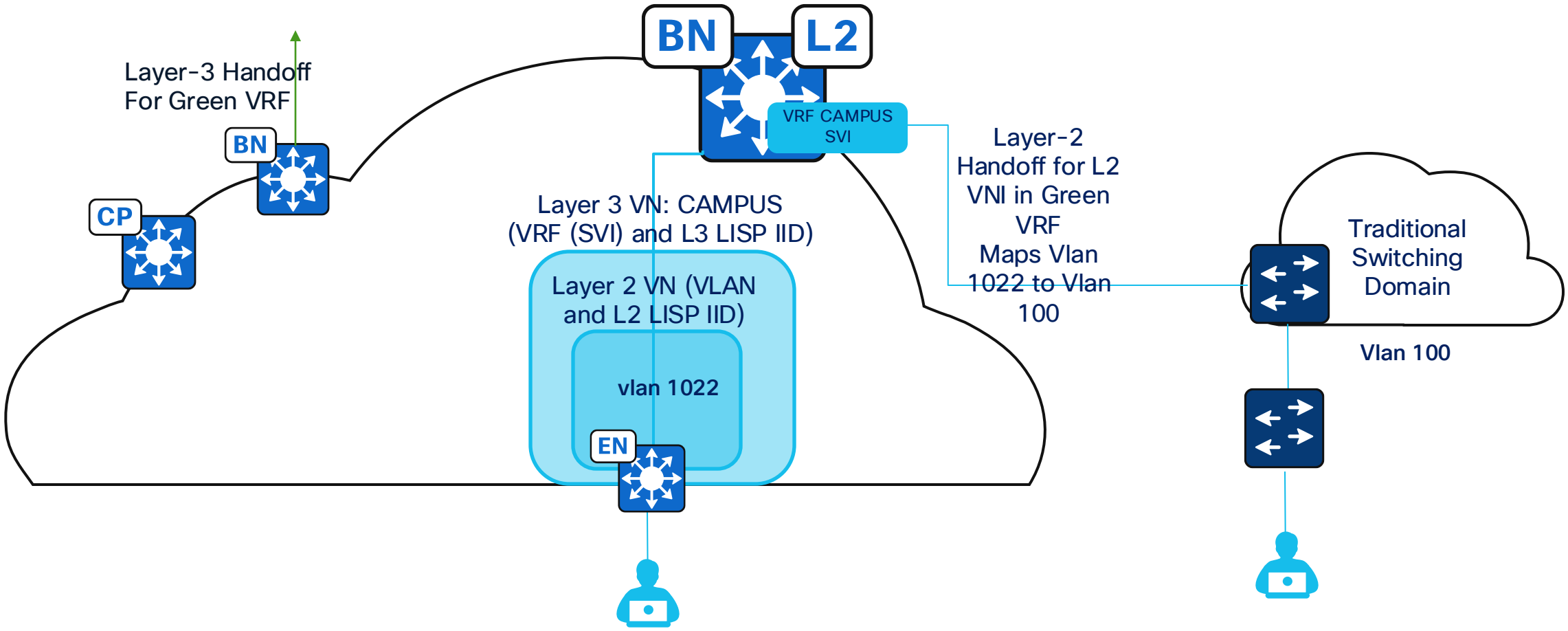
Extranet Layer 3 Handoff

Helps achieve route-leaking natively in LISP SD-Access Fabric



Layer 2 Handoff

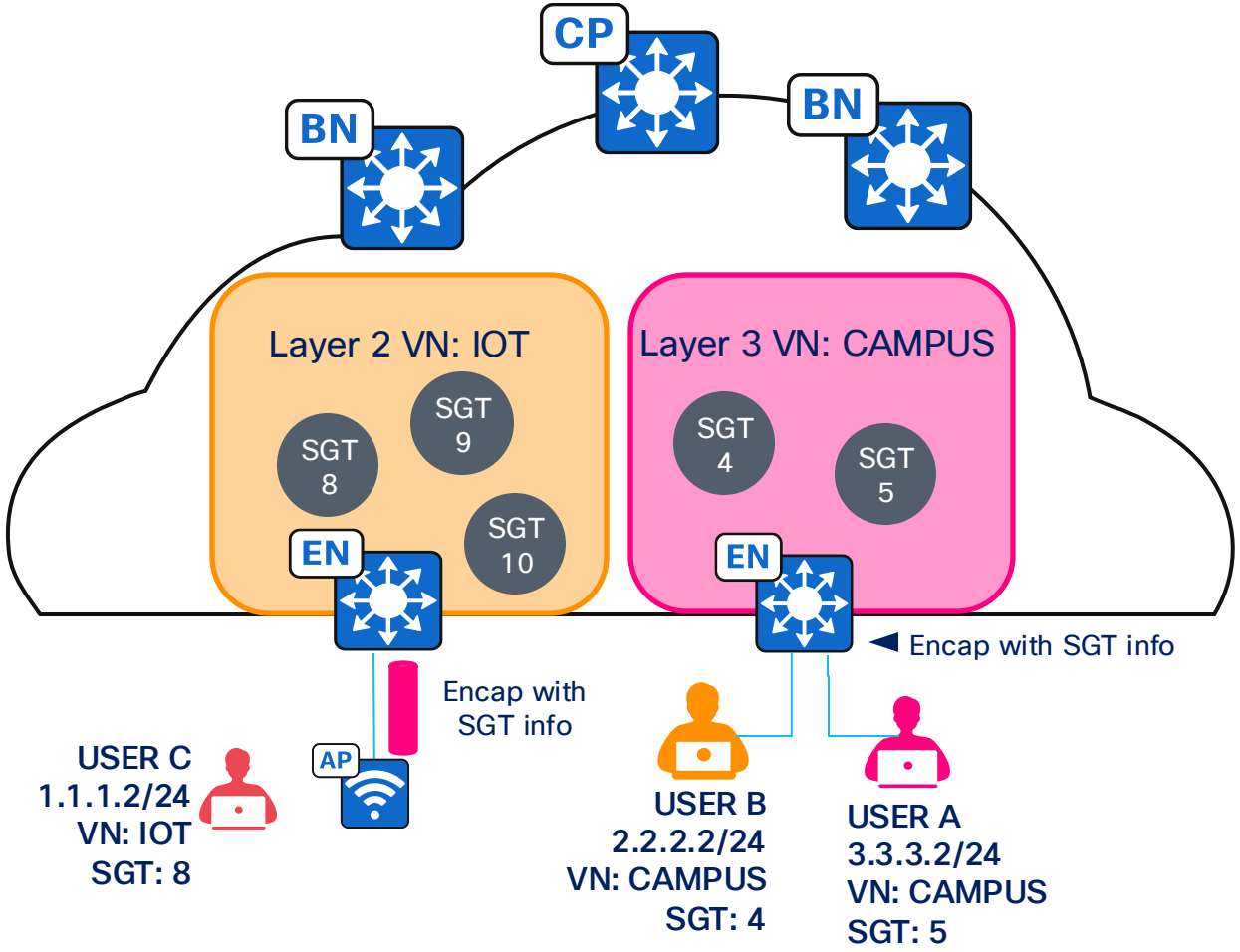
Layer 2 Virtual Networks handoff through a user-defined VLAN



Security Group Tag

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

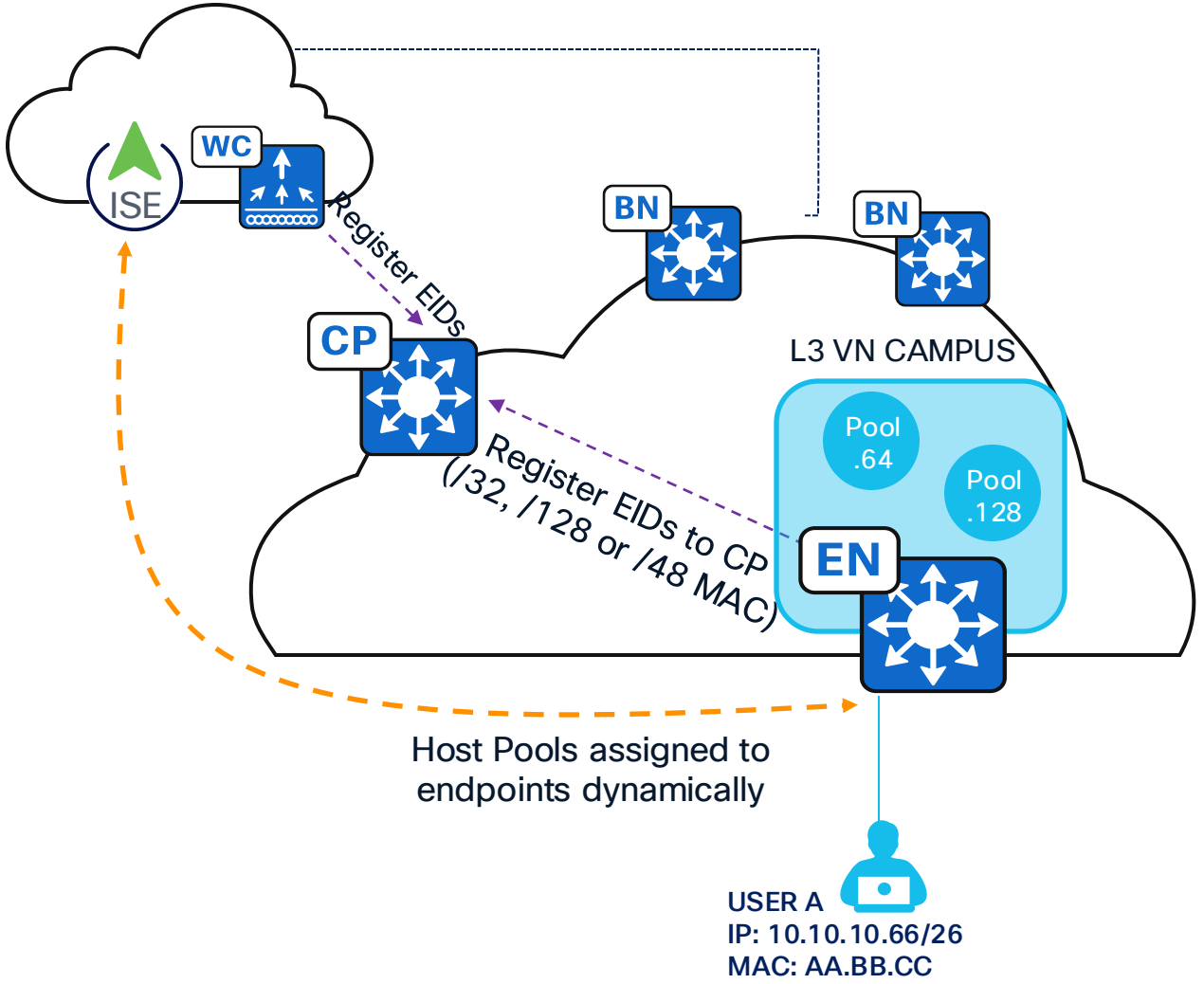
- Edge Nodes and Fabric APs assign a unique Scalable Group Tag (SGT) to each end endpoint in concert with ISE.
- Edge Nodes and Fabric APs add an SGT to the fabric encapsulation.
- SGTs are used to implement IP-address-independent access policies.
- SGTs can be extended to numerous other networking technologies 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

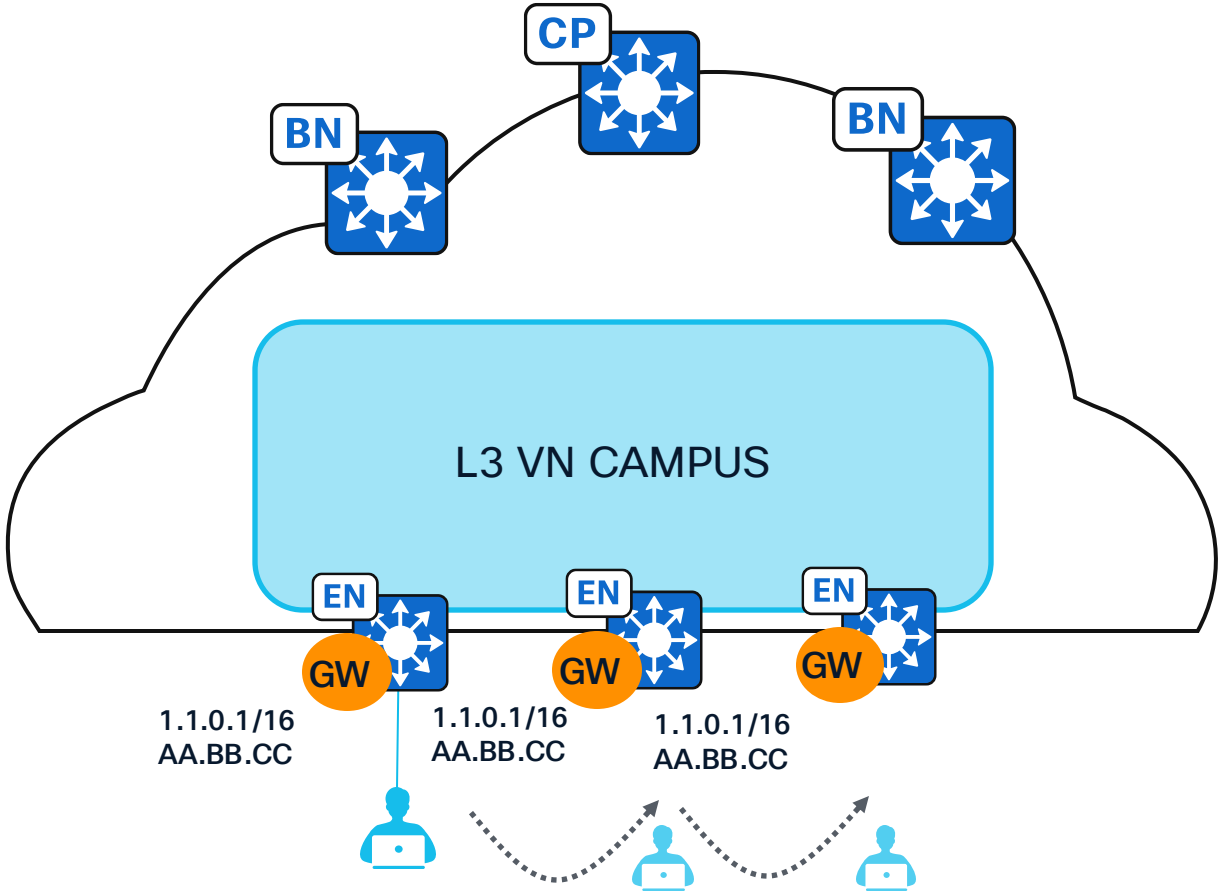
- Edge Nodes instantiate an access VLAN and a Switched Virtual Interface (SVI) with user-defined IPv4/IPv6 addresses per Host Pool.
- Host Pools assigned to endpoints dynamically by AAA or statically per port.
- Edge Nodes and Fabric WLCs register endpoint IDs (/32, /128 or MAC) with the Control Plane,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



Cisco SD-Access Fabric

Anycast Gateway Provides a Default Gateway for IP-Capable Endpoints

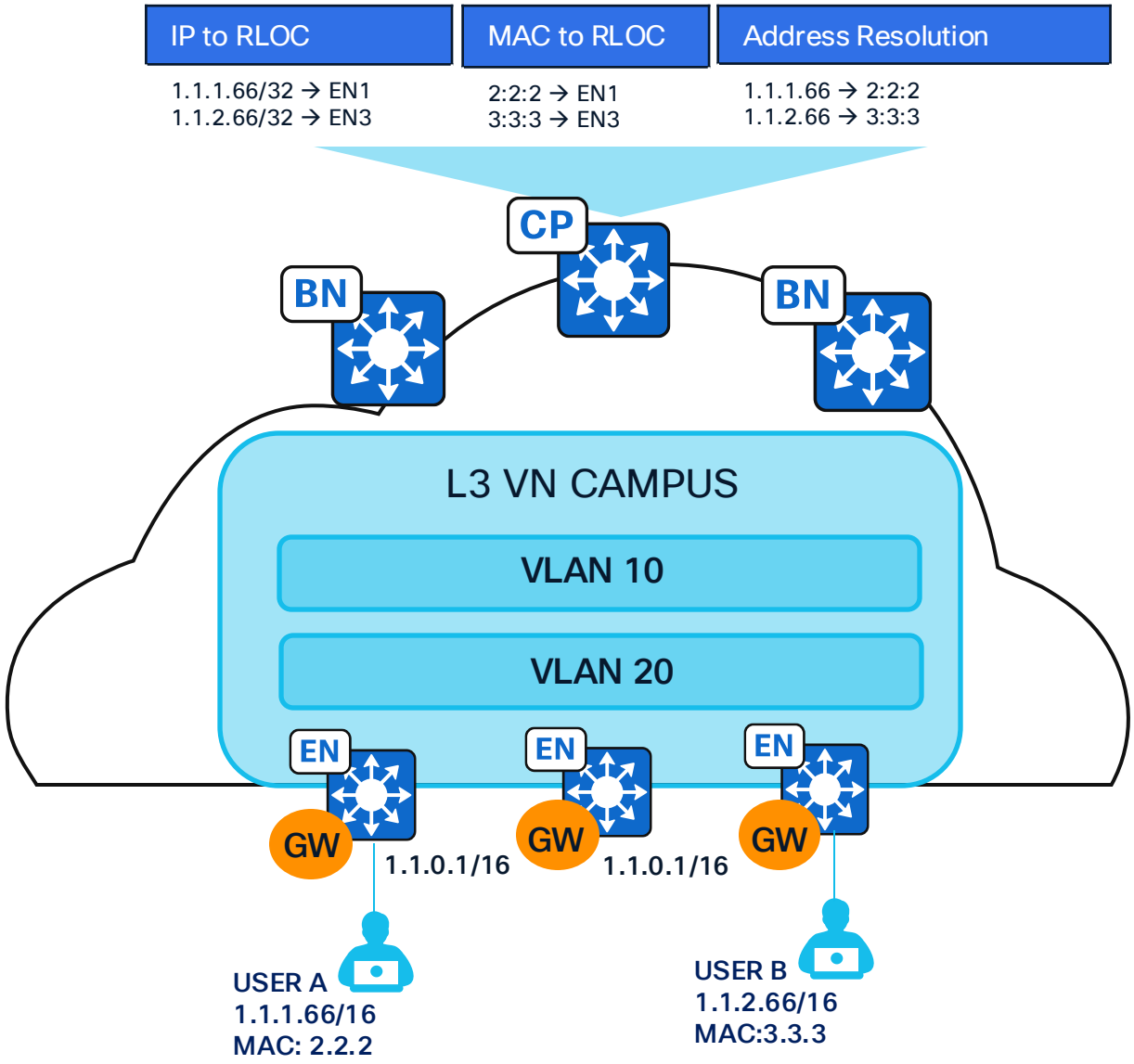
- Similar principle and behavior to FHRP with a shared virtual IPv4/IPv6 addresses and MAC address.
- The same Switch Virtual Interface (SVI) is present on all Edge Nodes with the same virtual IP and MAC.
- The wired or wireless endpoint can connect to any switch or AP in the fabric and communicate with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



Cisco SD-Access Fabric

Host Pools are “stretched” via the Overlay

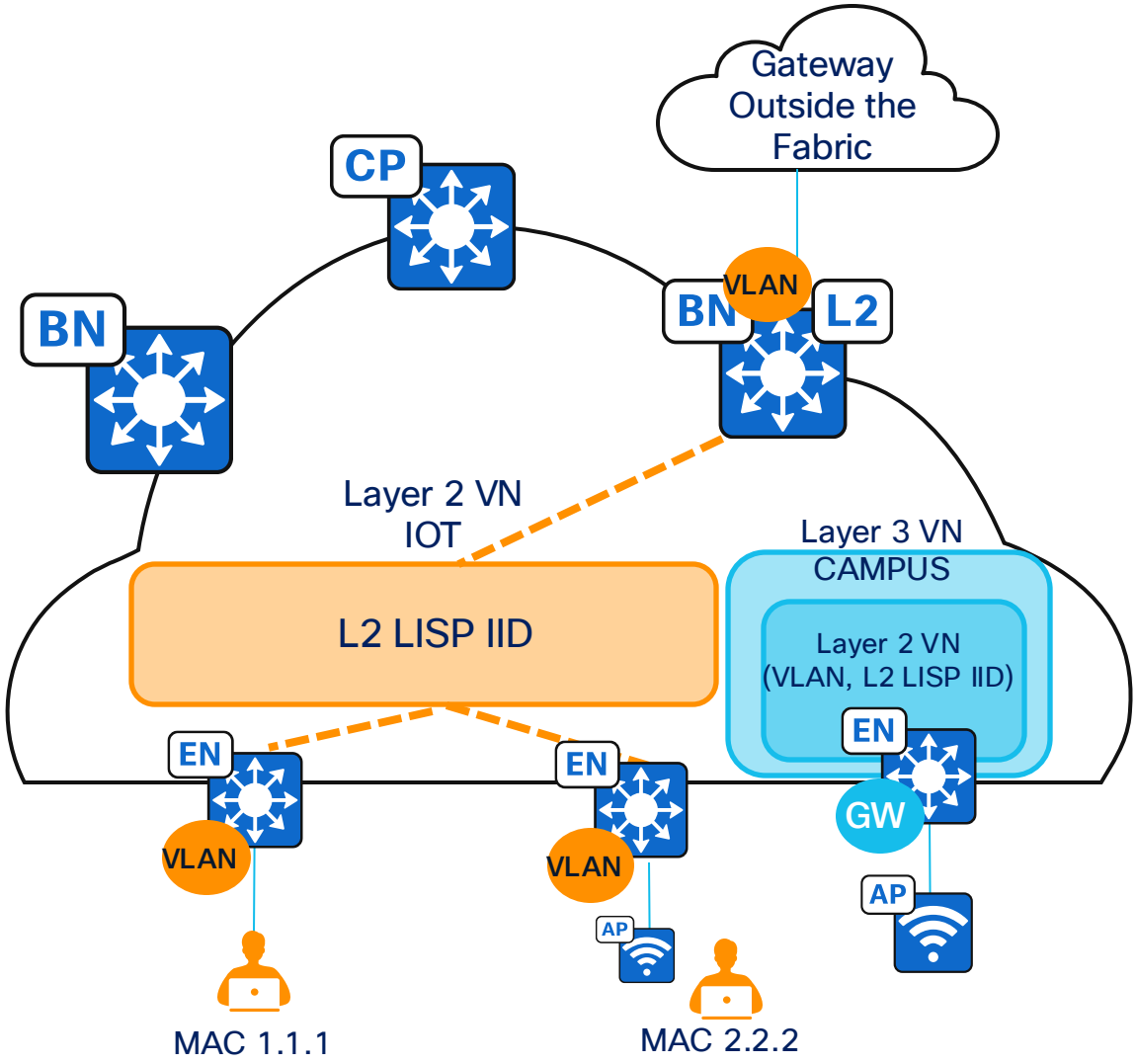
- Endpoint IPv4/IPv6 traffic arrives on an Edge Node and is then routed or switched by the Edge Node.
- Fabric Dynamic EID mapping allows endpoint-specific (/32, /128, MAC) advertisement and mobility.
- VLANs to connect endpoints across Edge Nodes, this happens in the Overlay without broadcast flooding.



Layer 2 Virtual Networks

Fabric is just a transport for Layer-2 adjacencies

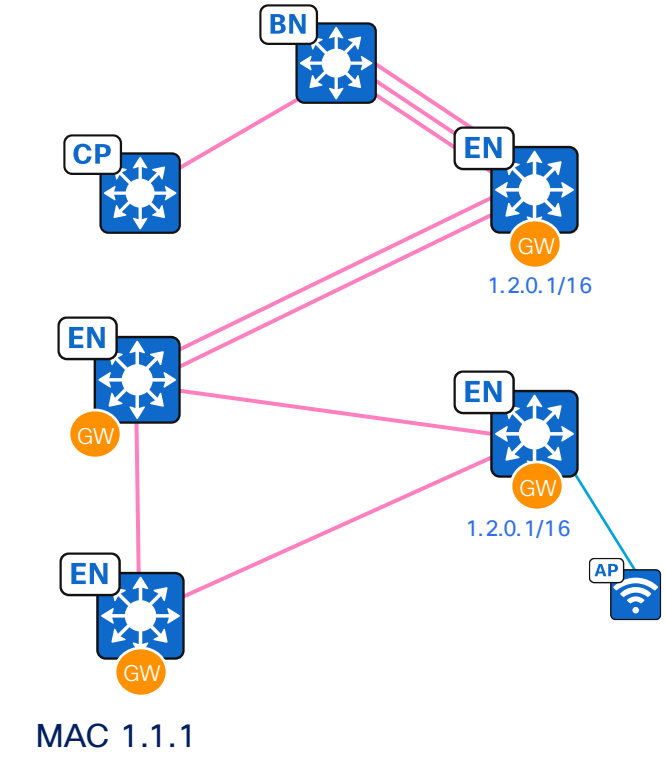
- By default, an L2VN is deployed with each Anycast Gateway and Layer 2 Flooding is disabled. Layer 2 Flooding can be enabled, if necessary, to service niche applications.
- L2VN can be deployed without an Anycast Gateway, and Layer 2 Flooding cannot be disabled.
- Sometimes referred to as “Gateway Outside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



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 mechanisms like L2 Trunking and STP.



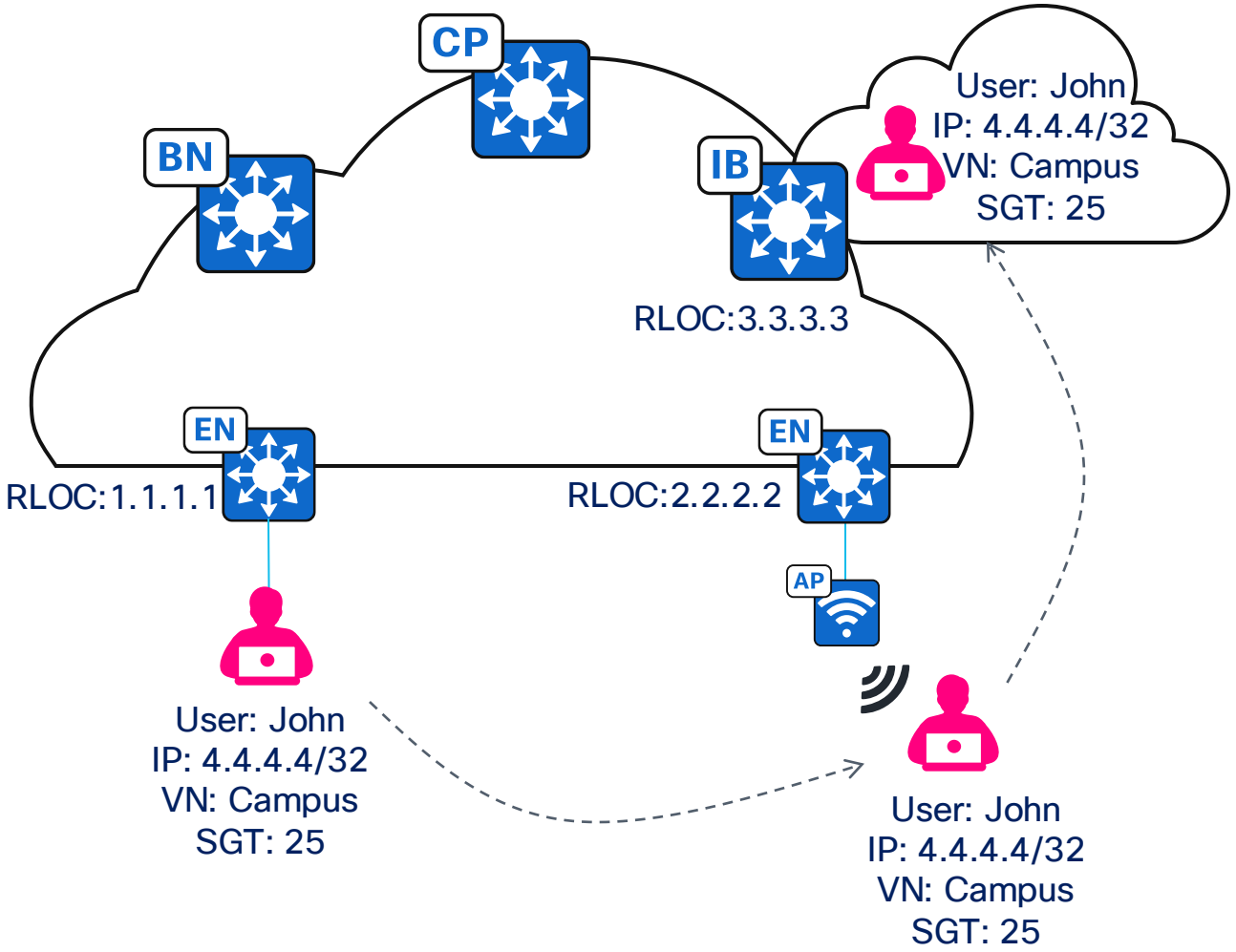
Fabric Fundamentals

Control 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-RFC9306 and Informational RFC9299)

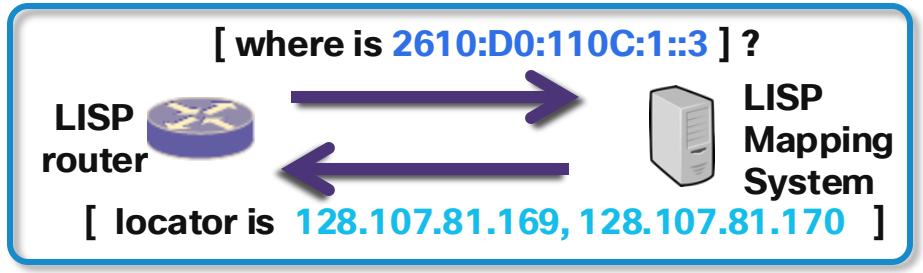
LISP Operations

LISP :: Mapping Resolution “Level of Indirection”

- LISP “Level of Indirection” is analogous to a DNS lookup
  - DNS resolves **IP addresses** for **URL** **Answering the “WHO IS” question**

DNS
Name-to-IP
URL Resolution

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



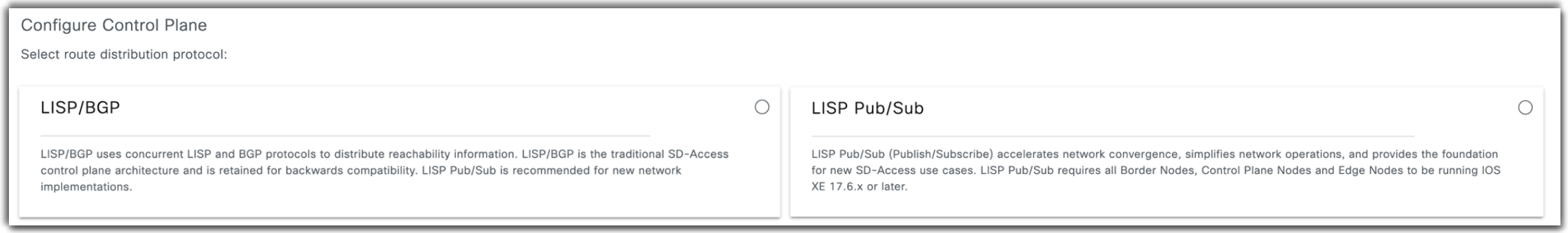
LISP
Identity-to-locator
Mapping Resolution

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**

LISP in Cisco SD-Access



LISP/BGP

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

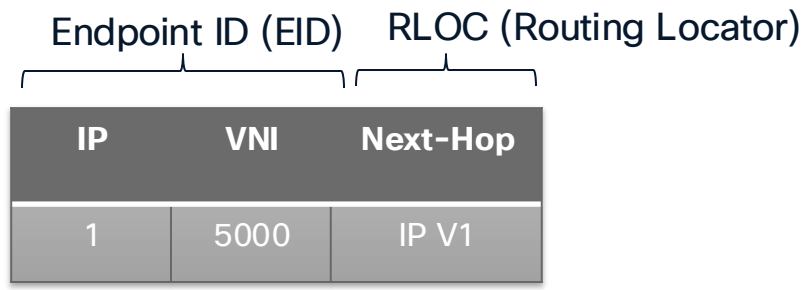
LISP Pub/Sub

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

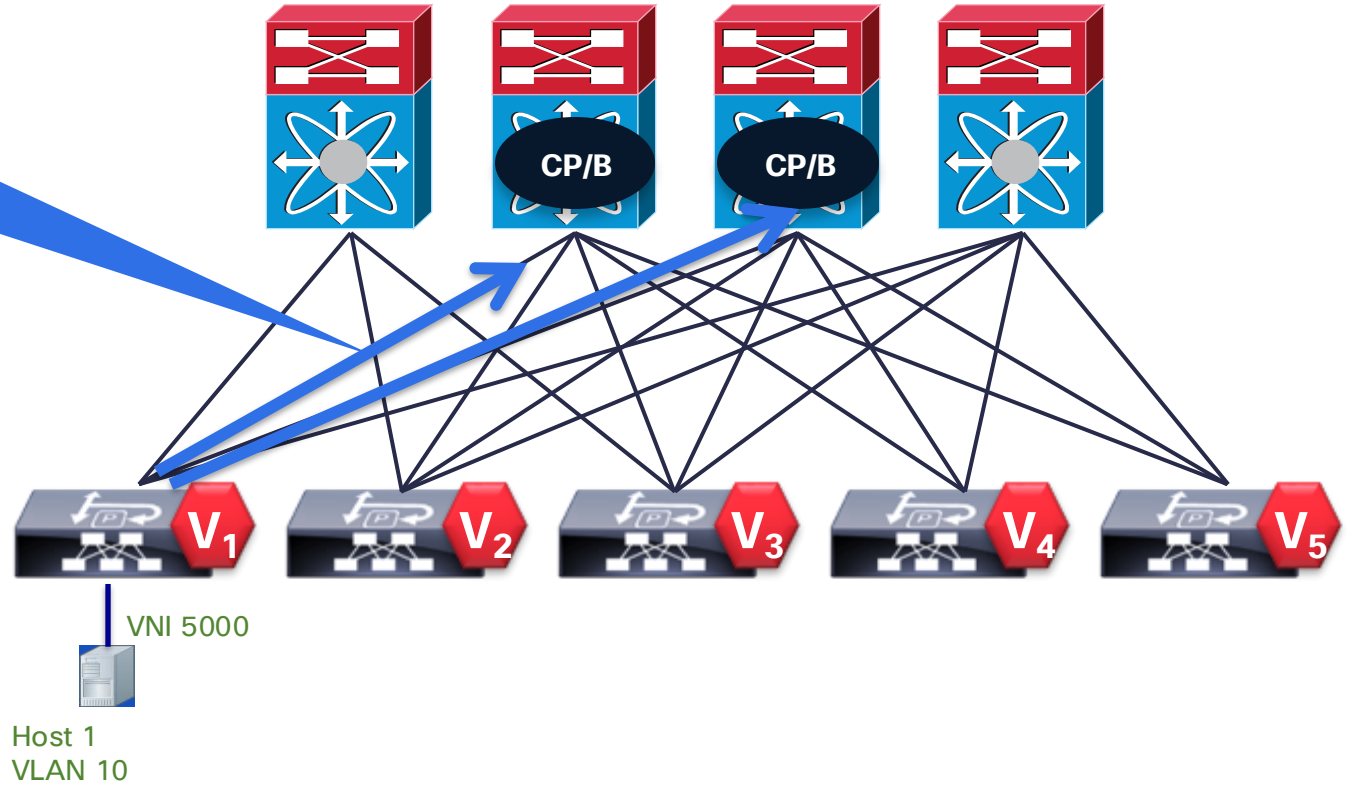
*Rebranded to Catalyst Center in late 2023

LISP Control Plane

Host Registration



Map Register
EID = IP1, VNI 5000
RLOC = xTR IP V1



V1 LISP Tunnel Router (xTR) & VTEP*

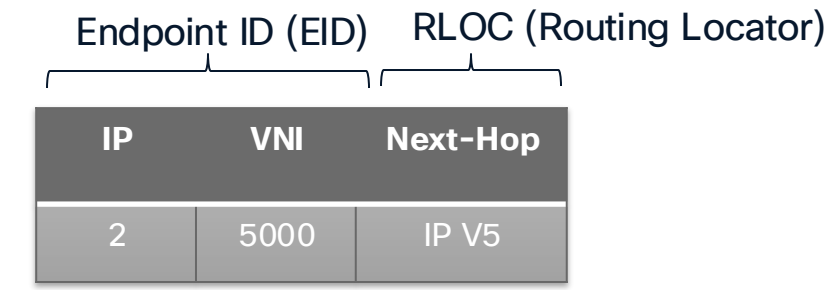
CP/B CP + Border

* VTEP = VXLAN Tunnel End-Point

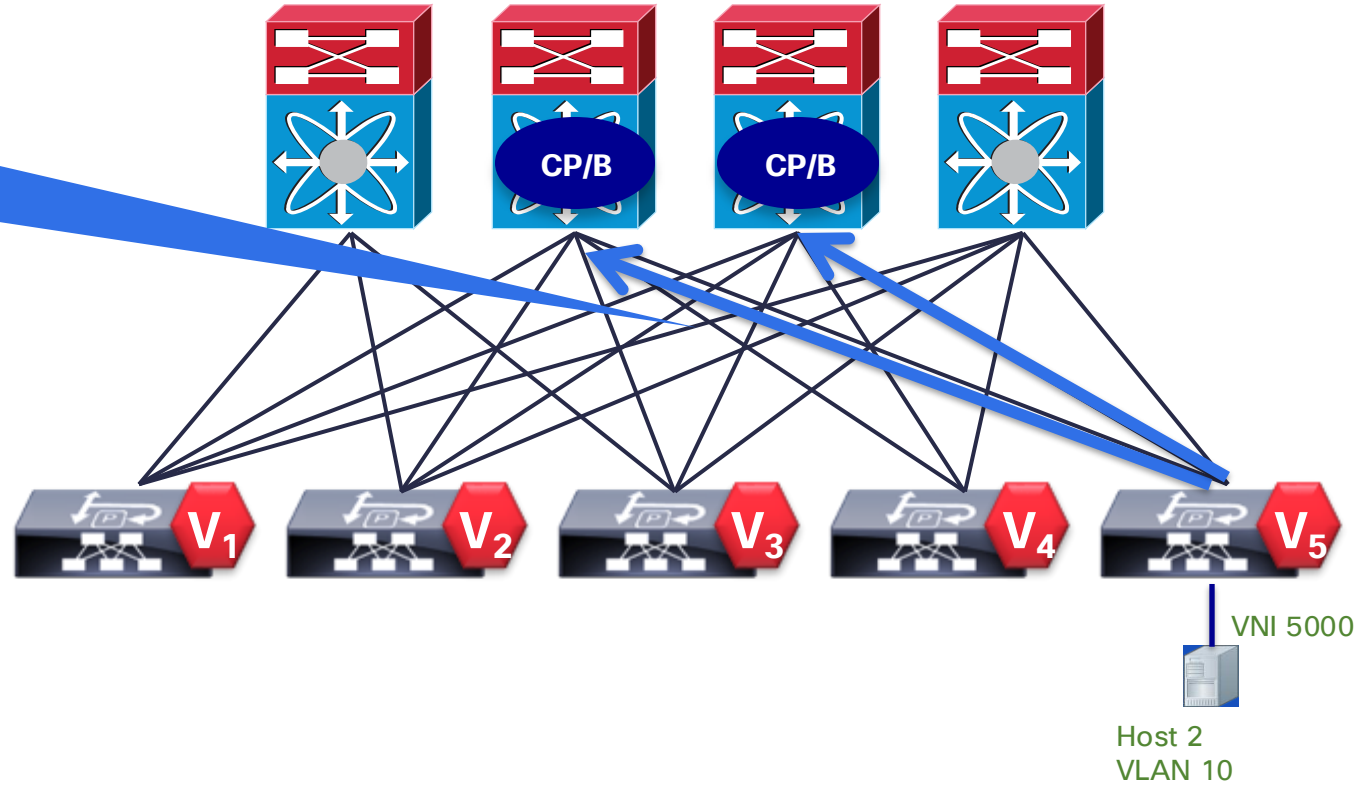
1. Attachment xTR registers host's IP (+MAC) in LISP
2. Scoped signaling between fabric nodes – fast convergence, scales and uses hardware resources efficiently

LISP Control Plane

Host Registration



Map Register
EID = IP2, VNI 5000
RLOC = xTR IP V5



V1 LISP Tunnel Router (xTR) & VTEP*

CP/B CP + Border

* VTEP = VXLAN Tunnel End-Point

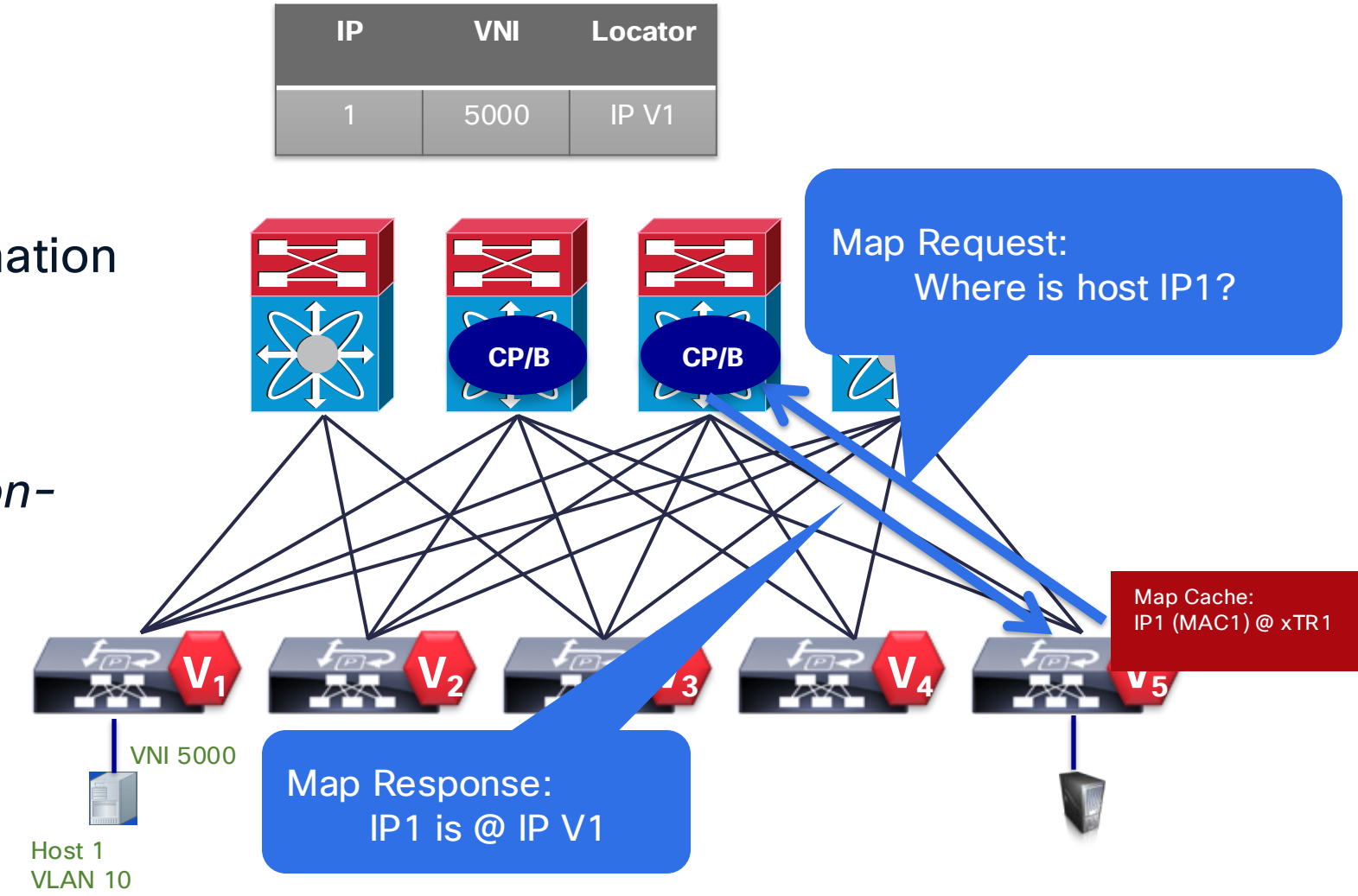
1. Attachment xTR registers host's IP (+MAC) in LISP
2. Scoped signaling between fabric nodes – fast convergence, scales and uses hardware resources efficiently

LISP Control Plane

Host Resolution

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

A key basic working principle:
*Use traffic signals to **pull** routes on-demand*



1. Host 2 wants to talk to host 1, the xTR (V5) issues a map-request
2. The Mapping System responds
3. The response is cached at the requesting xTR (V5): LISP map-cache

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)**

Cisco SD-Access Fabric

Control Plane: Locator/ID Separation Protocol (LISP)

LISP/BGP

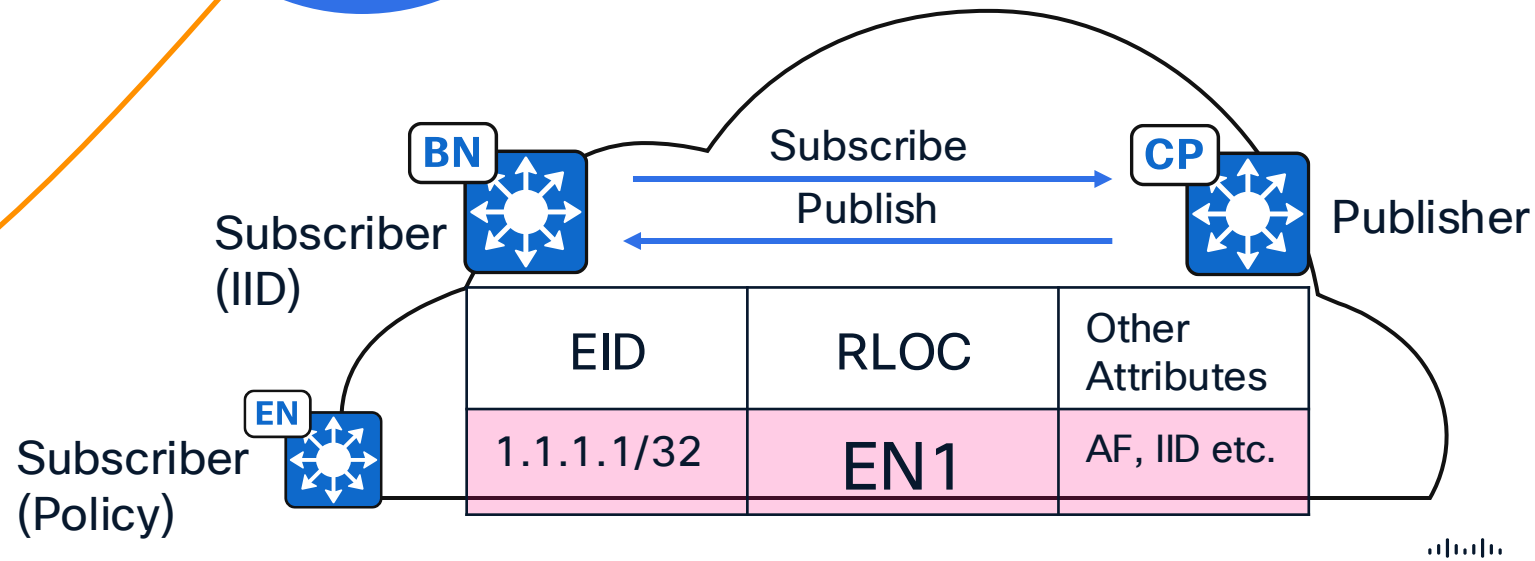
Reliable and stable.
BGP transport.

2017

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.



Fabric Fundamentals

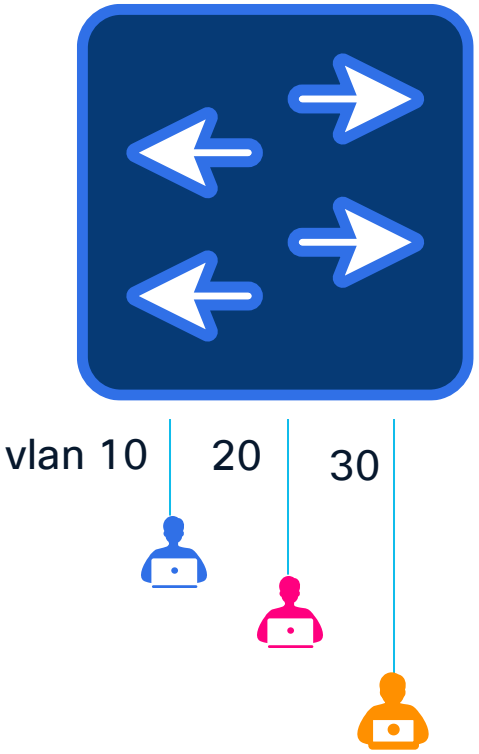
Data Plane

Cisco SD-Access Fabric LISP Data Plane

Virtual Extensible Local Area Network (VXLAN)

Additional Information

Traditional Layer 2 Networks Challenges



Spanning Tree Protocol

- Single active path
- Under-utilization
- Broadcast storms

No ECMP

- No load-balancing
- Suboptimal traffic flow

Mobility & Multitenancy

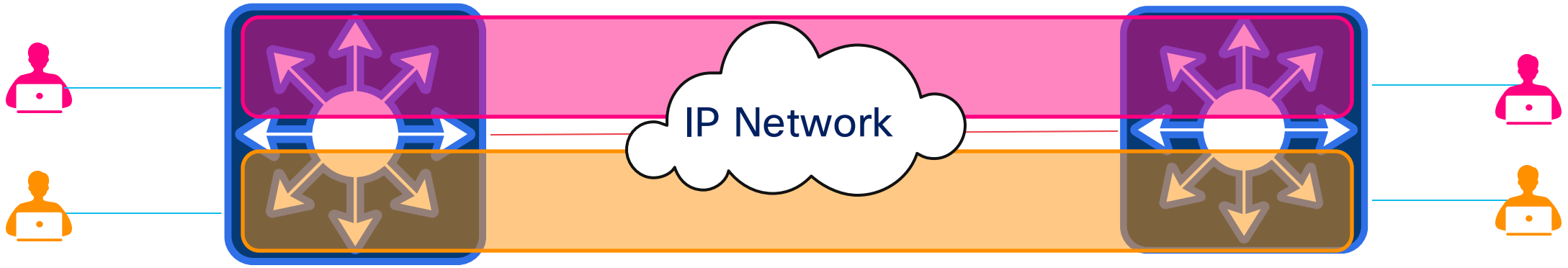
- Restricted to L2 domain
- Geographical limitation
- 12-bit VLAN ID = 4000 VLANs

cisco

Cisco SD-Access Fabric LISP Data Plane

Virtual Extensible Local Area Network (VXLAN)

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

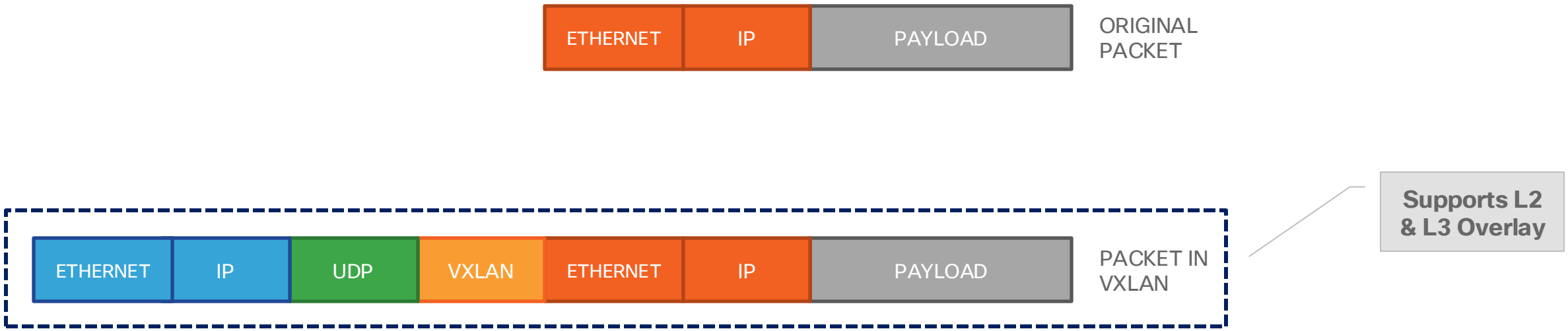


- ✓ Scalability: 16 million unique identifiers.
- ✓ Runs on top of L3, avoids need for STP.
- ✓ L2 traffic tunnelled over an L3 infrastructure.
- ✓ Handles broadcast, multicast, and unknown unicast traffic using multicast instead of flooding.
- ✓ Carries segmentation information.

Cisco SD-Access Fabric LISP Data Plane

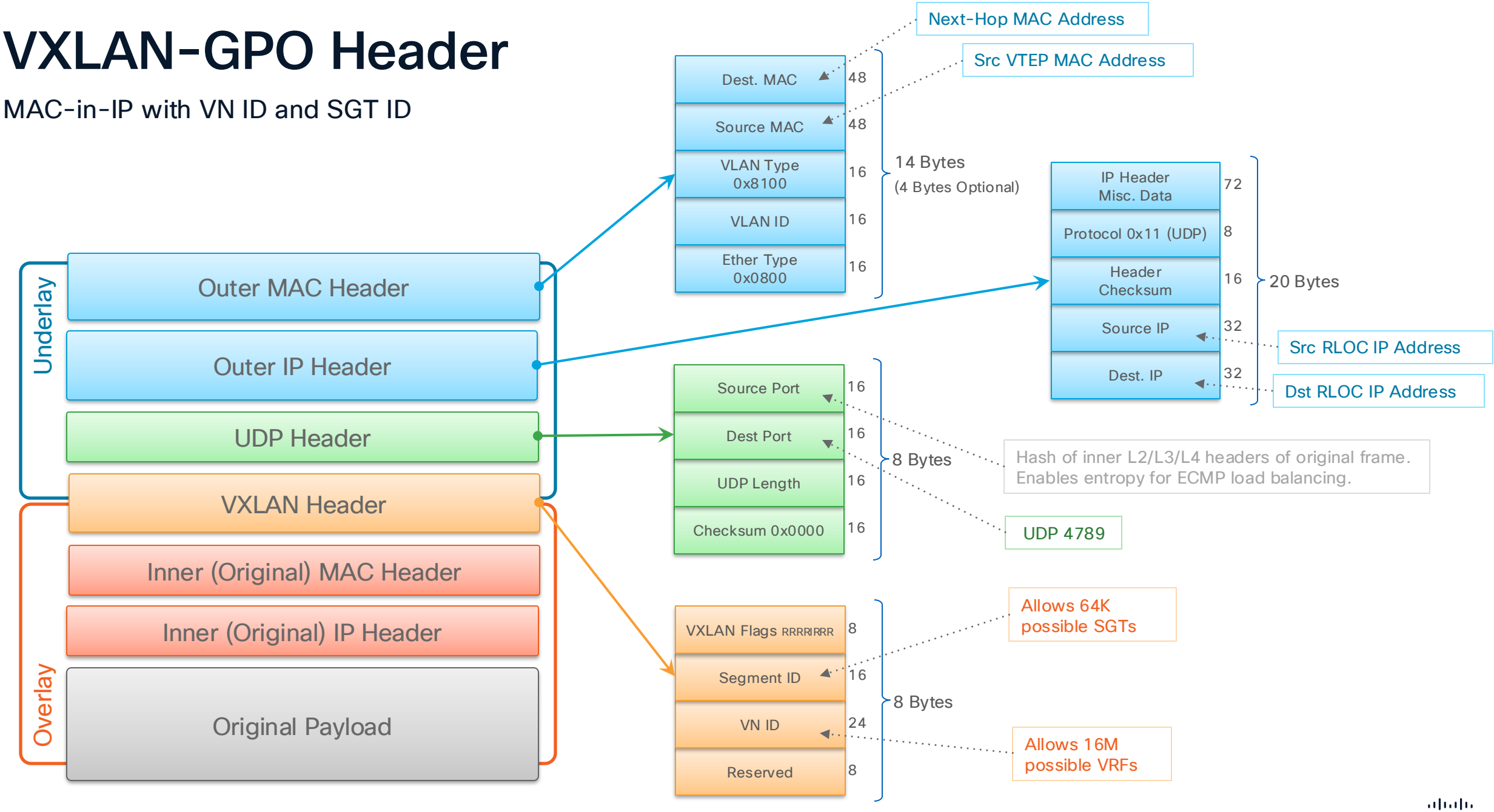
VXLAN Packet Format

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



VXLAN-GPO Header

MAC-in-IP with VN ID and SGT ID



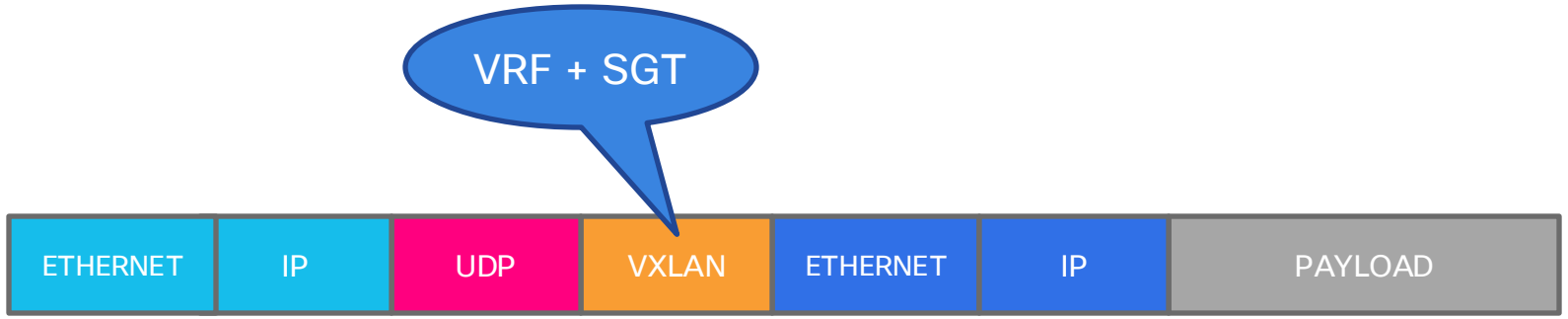
Fabric Fundamentals

Policy Plane

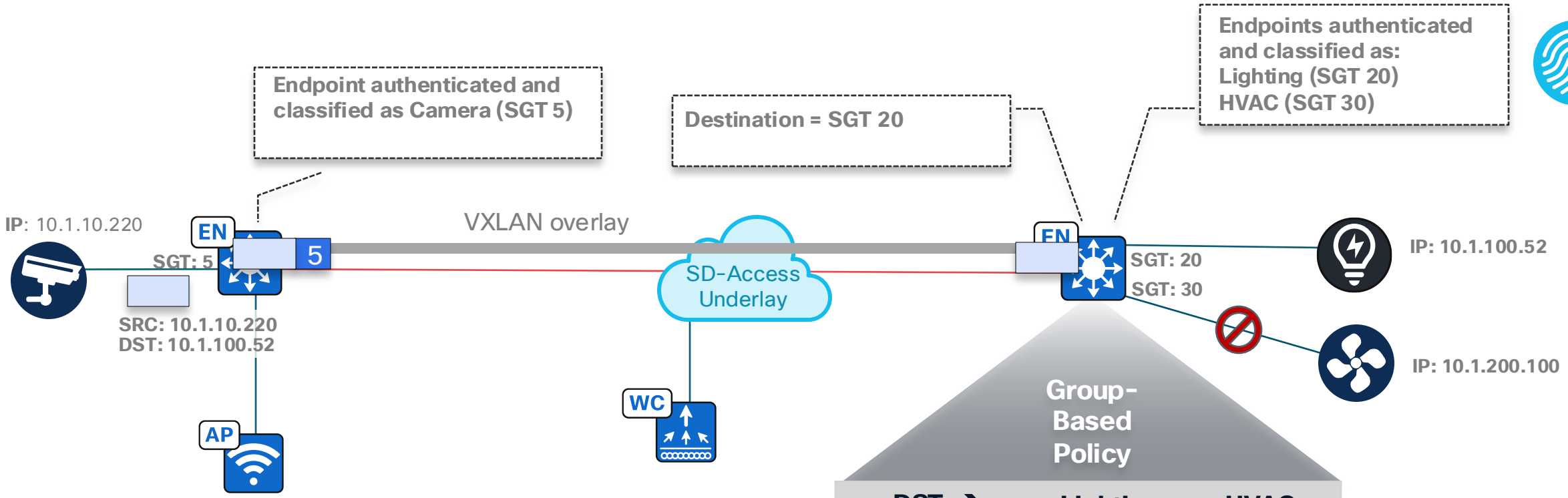
Cisco SD-Access Fabric LISP Data Plane

Policy Plane

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



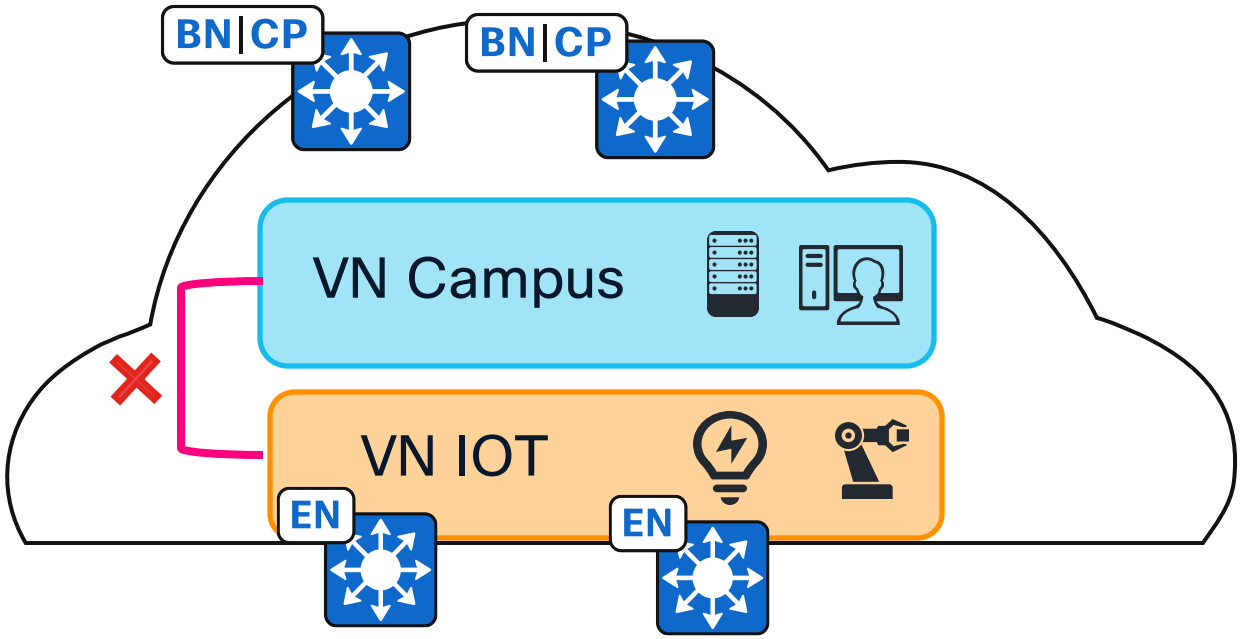
What is Security Group Tag and Group-Based Policy?



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

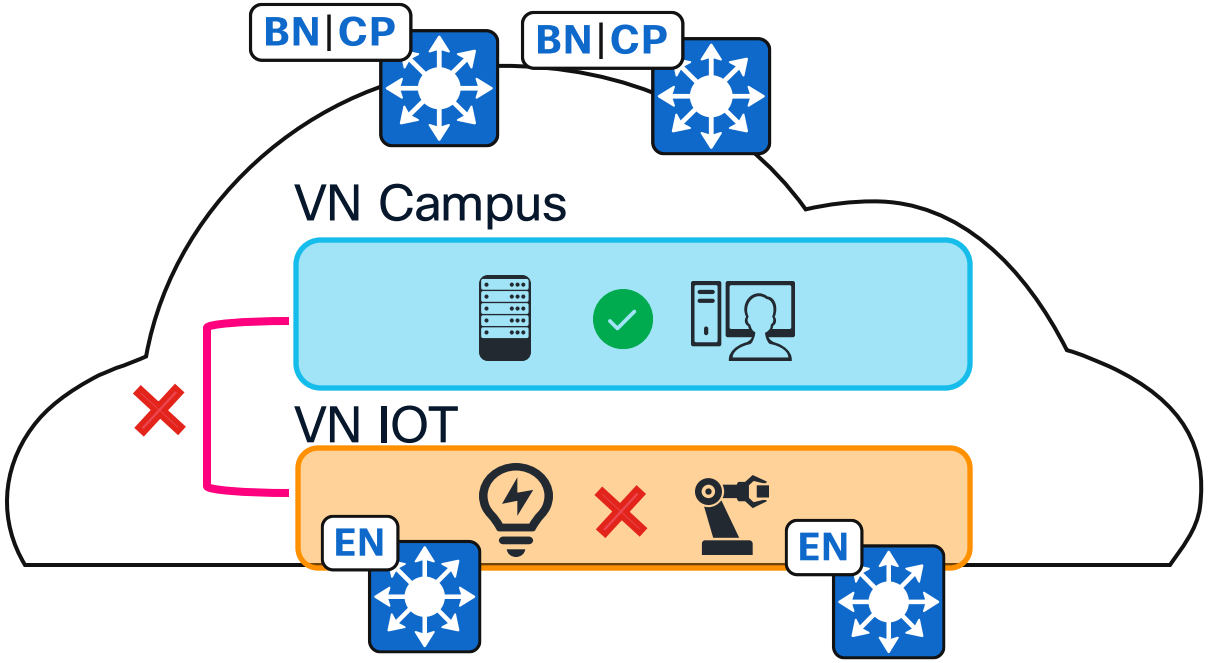
SD-Access Policy

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.

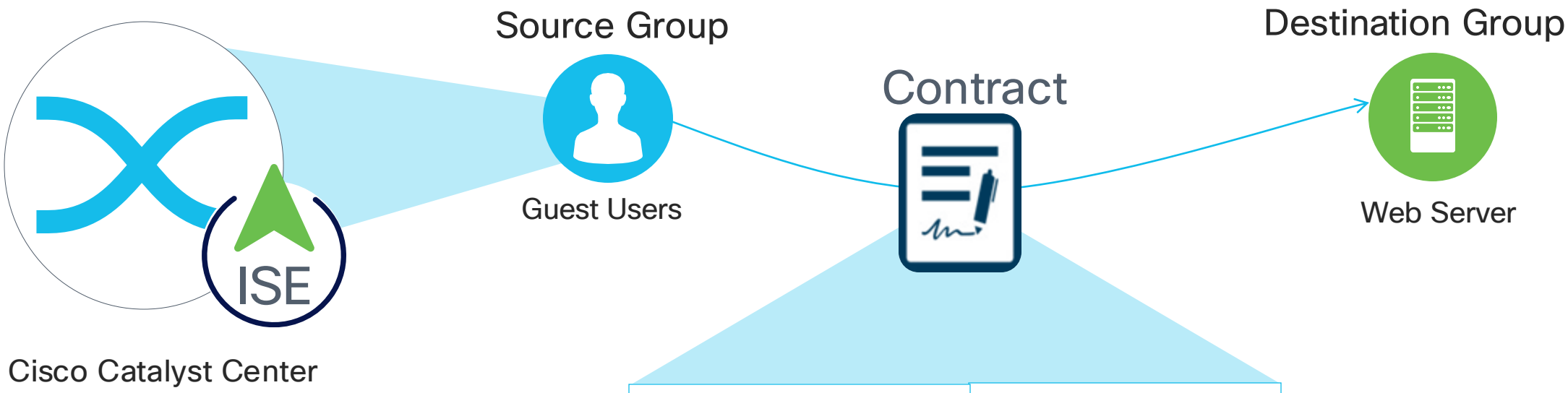


Security Group Tag (SGT)

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



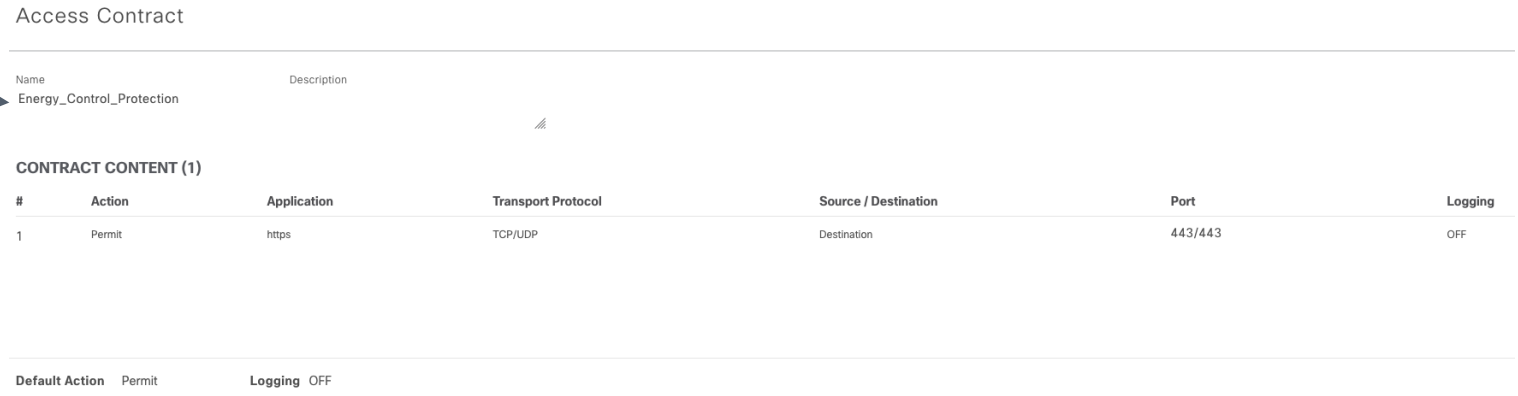
Classifier Type	Action Type
Port Number	Permit
Protocol Name	Deny
Application Type	Copy

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

SD-Access Policy

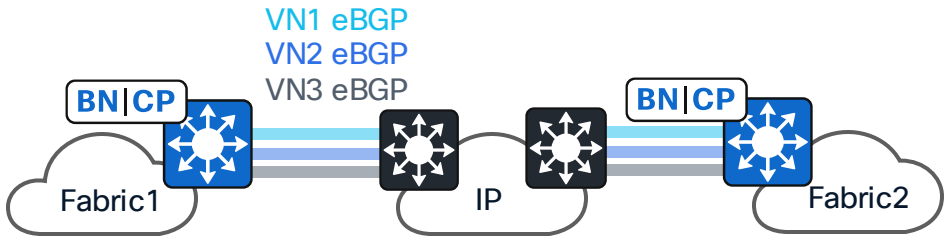
Group-Based Access Control Policy

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



Multiple Fabric Sites

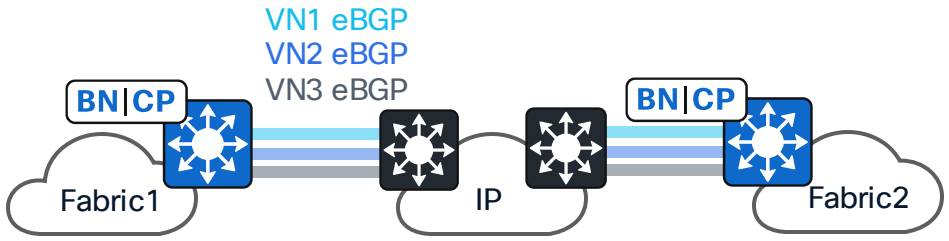
Transits for VN and SGT Preservation

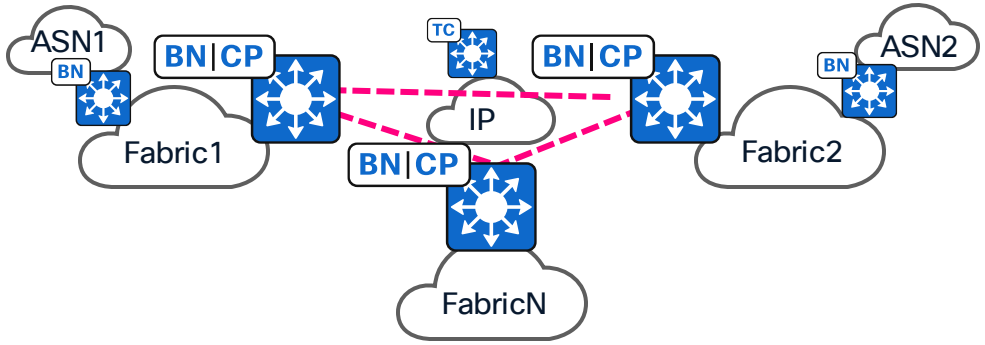


IP-Based Transit

- 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

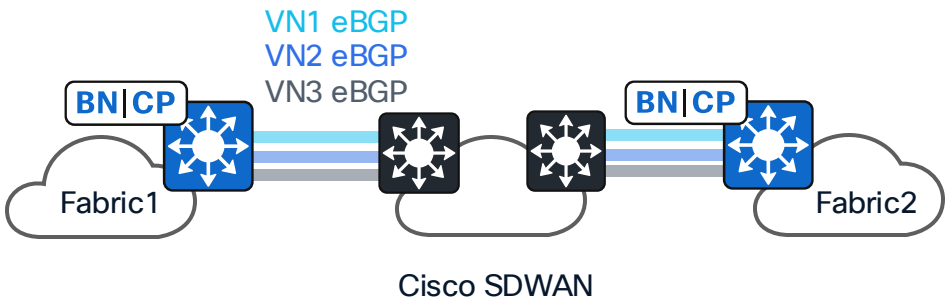
- Handoff from the Border is automated with Cisco Catalyst Center
- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.

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

Transits for VN and SGT Preservation



SD-WAN Transit

- Cisco / Meraki SD-WAN between Fabric Sites.
- Capable of preserving Layer 3 Virtual Networks and SGT's
- Dedicated SD-WAN Edge for design flexibility, Border Node port densities and port speeds

Conclusion

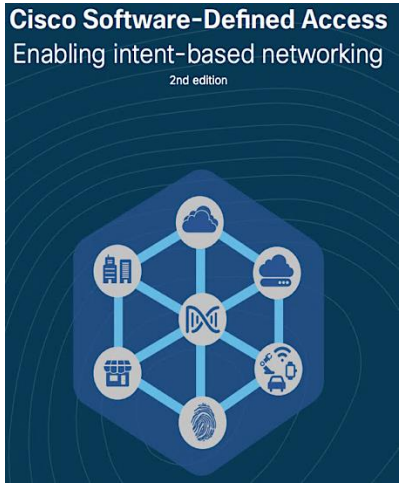
Cisco’s SD-Access LISP provides a secure, flexible, and automated way to meet the security and operational challenges faced by an everchanging environment.

Cisco SD-Access Collaterals

Cisco Software-Defined Access for Industry Verticals

Cisco Software-Defined Access

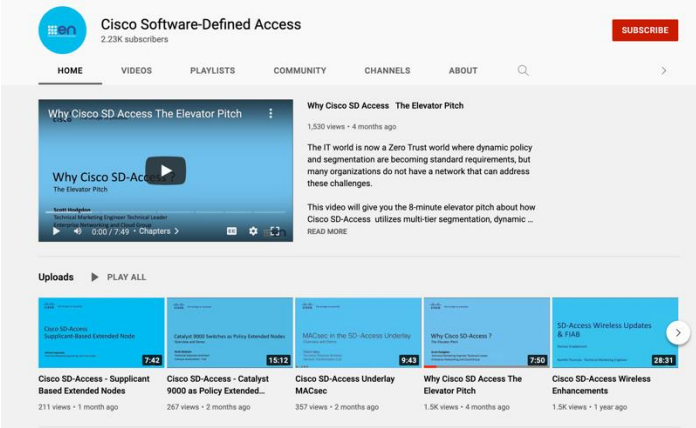
Enabling intent-based networking



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



Multiple Cisco Catalyst Center to ISE

Cisco SD-Access Design Tool

EN&C Validated Designs

The Latest SD-Access Guides

Continue your education

FULL CONFERENCE | IT LEADERSHIP | FULL CONFERENCE PLUS

Cisco SD-Access LISP VXLAN Fabric Best Practices: Design and Deployment [BRKENS-2502]

Schedule **Tuesday, Nov 11 | 1:45 PM - 3:15 PM AEDT | Room 210**

Ash Burton, Technical Solutions Architect, Cisco

SD-Access as Code with Cisco Catalyst Center and ISE Automation [LTRENS-3751]

Schedule **Tuesday, Nov 11 | 2:15 PM - 4:15 PM AEDT | Instructor Led Lab, Theatre 1 - World of Solutions**

Senthil Kumar Kumar, Principal Architect, Cisco

Mastering Troubleshooting with Cisco Catalyst Center & SD-Access [BRKTRS-3821]

Schedule **Tuesday, Nov 11 | 5:00 PM - 6:00 PM AEDT | Room 210**

Won Choi, Customer Delivery Engineering Technical Leader, Cisco

EVPN Campus: Design and Implementation [BRKENS-2041]

Schedule **Wednesday, Nov 12 | 8:30 AM - 10:00 AM AEDT | Room 210**

Sergey Nasonov, Solutions Engineer, Cisco Systems, Inc.

Goodbye CLI, Hello Cloud: The Future of Campus Networking with IOS-XE and Dashboard [BRKENS-2601]

Schedule **Wednesday, Nov 12 | 1:00 PM - 2:30 PM AEDT | Room 211**

Leigh Jewell, Technical Solutions Architect, Cisco

What's New in SD-Access? [BRKENS-2568]

Schedule **Wednesday, Nov 12 | 4:15 PM - 5:45 PM AEDT | Room 210**

Mahesh Nagireddy, Technical Marketing Engineer, Technical Leader, Cisco

Contact me at: gartaylo@cisco.com

Complete your session evaluations

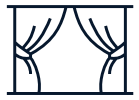
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events 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 Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: gartaylo@cisco.com

Thank you

cisco Live !


CISCO