The bridge to possible

Networkpeople DET

26-03-2024

Jesse Schmidt

Modern, Open and Scalable Fabrics

IETF Standard based Protocols

Cisco Catalyst Center

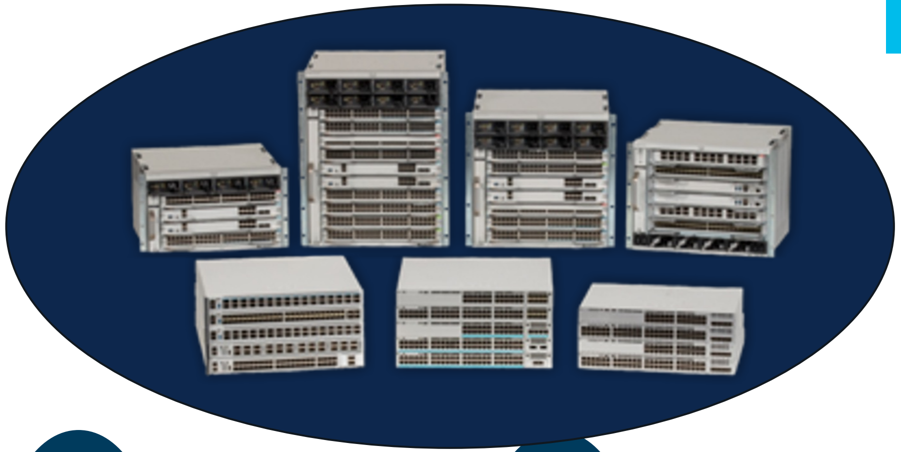
Cisco SD-Access

LISP Fabric*

*Cisco's Lead Motion

IETF

Cisco Catalyst 9000



BGP EVPN Fabric

IETF

Enterprise

Healthcare

Education

Financial

Public Sector

Manufacturing

Hospitality

Media

Transportation

Retail

Flexible Fabric Options Tailored to ***Customer Outcomes***!

Cisco SD-Access with LISP Control Plane VXLAN Data Plane

Cisco SD-Access with BGP EVPN Control Plane VXLAN Data Plane

Network Simplification

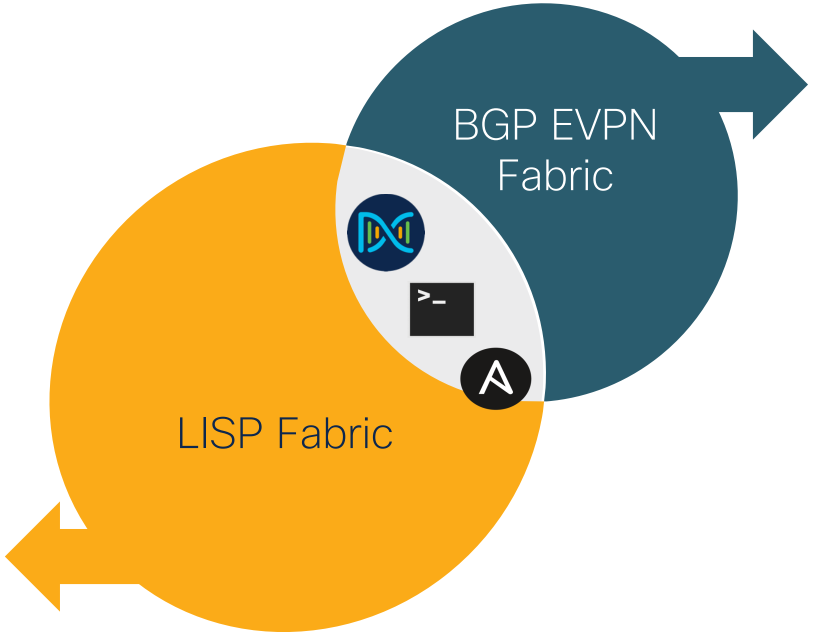
Lightweight, extensible, massive scale with rapid convergence. Single overlay for wired and wireless

Mobility First Requirement

Fabric Integrated Wireless, L2 Mobility, enhanced wireless performance

Segmentation

Zero-Trust Architecture with Unified Wired and Wireless Policy



One Fabric Architecture (Campus and DC)

Operational ease with a single familiar protocol

Multi-vendor interoperability

Vendor-agnostic solution with unique Cisco differentiators

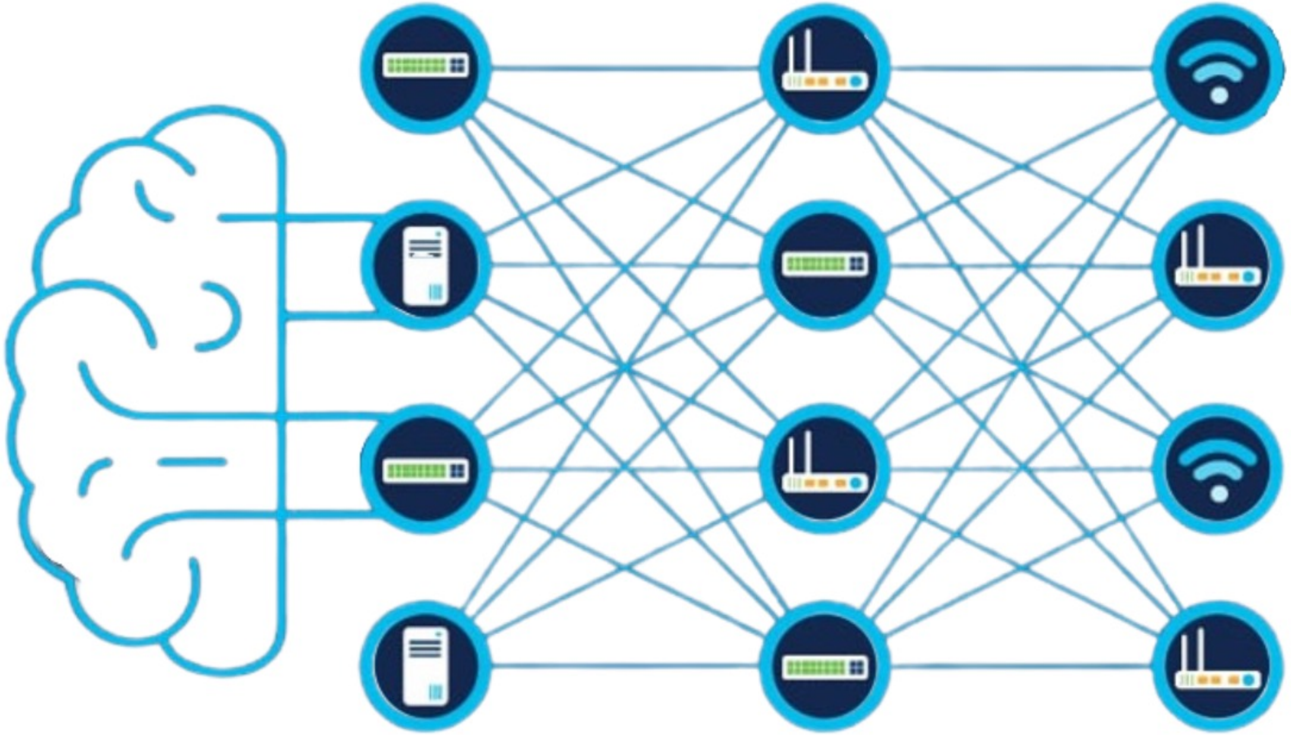
One Infrastructure | Single Data plane | Consistent Zero-Trust Experience

Roles and Terminology

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

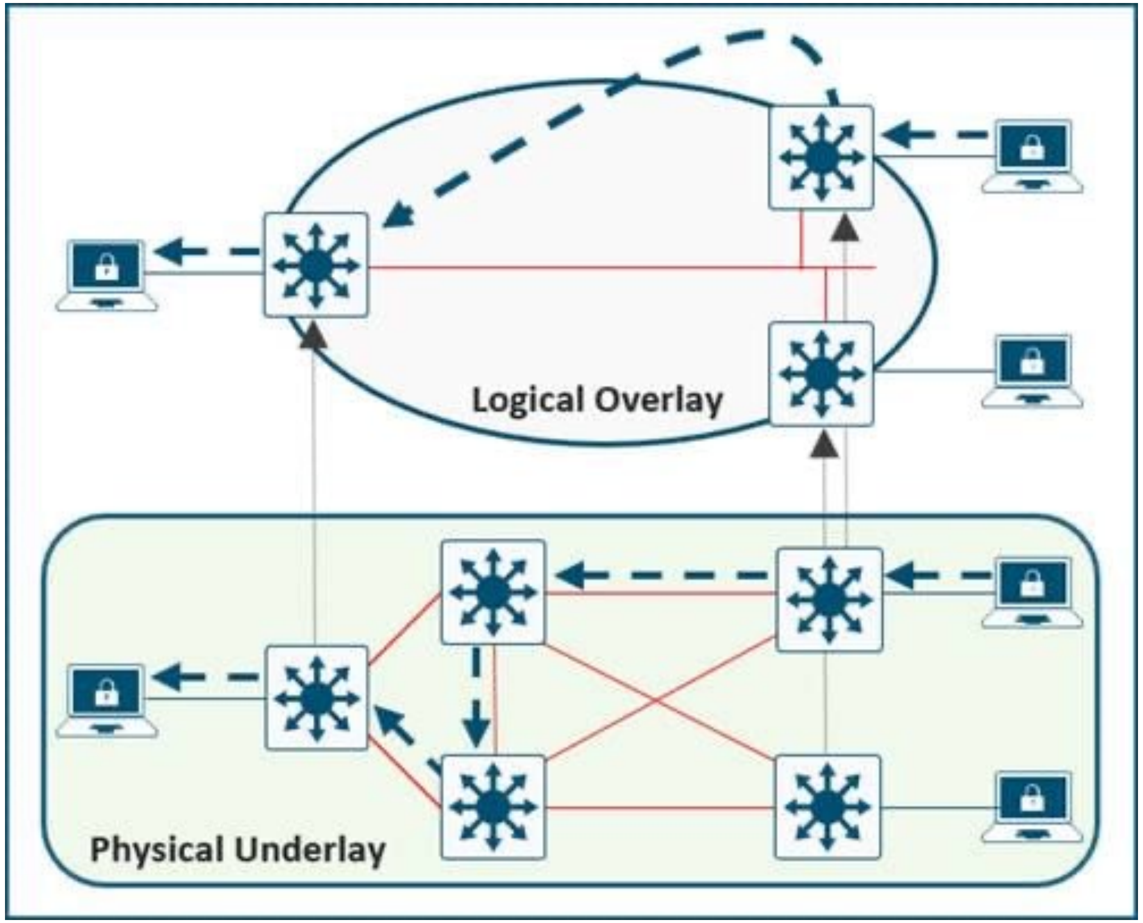
What is a Network Fabric?

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



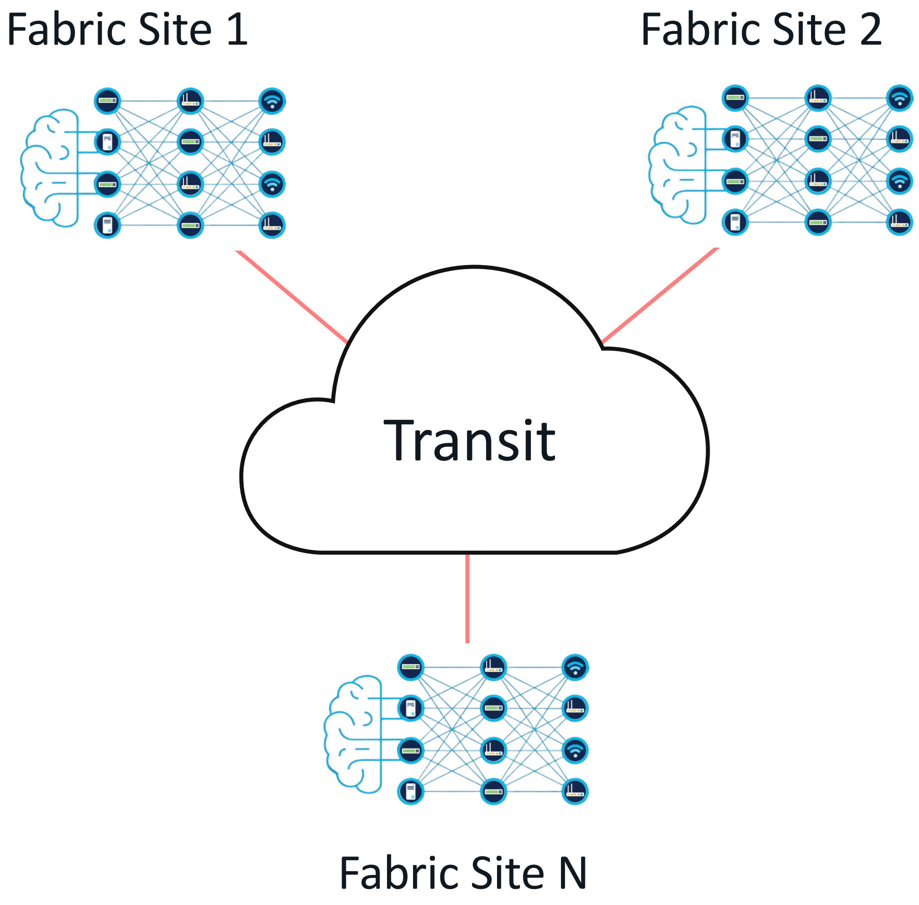
What is an Overlay?

- 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



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".



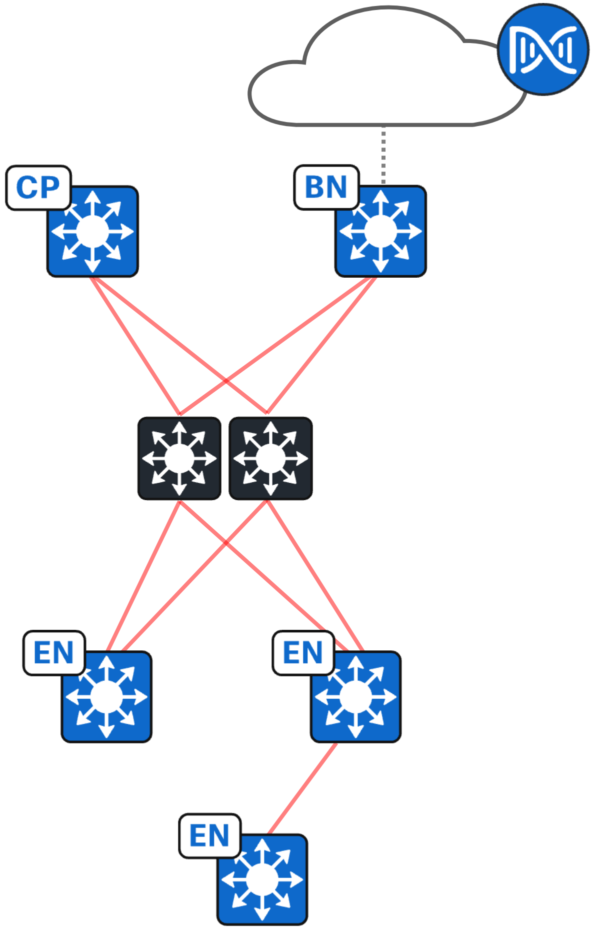
Roles and Terminology

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

Cisco SD-Access Roles

Mandatory Components

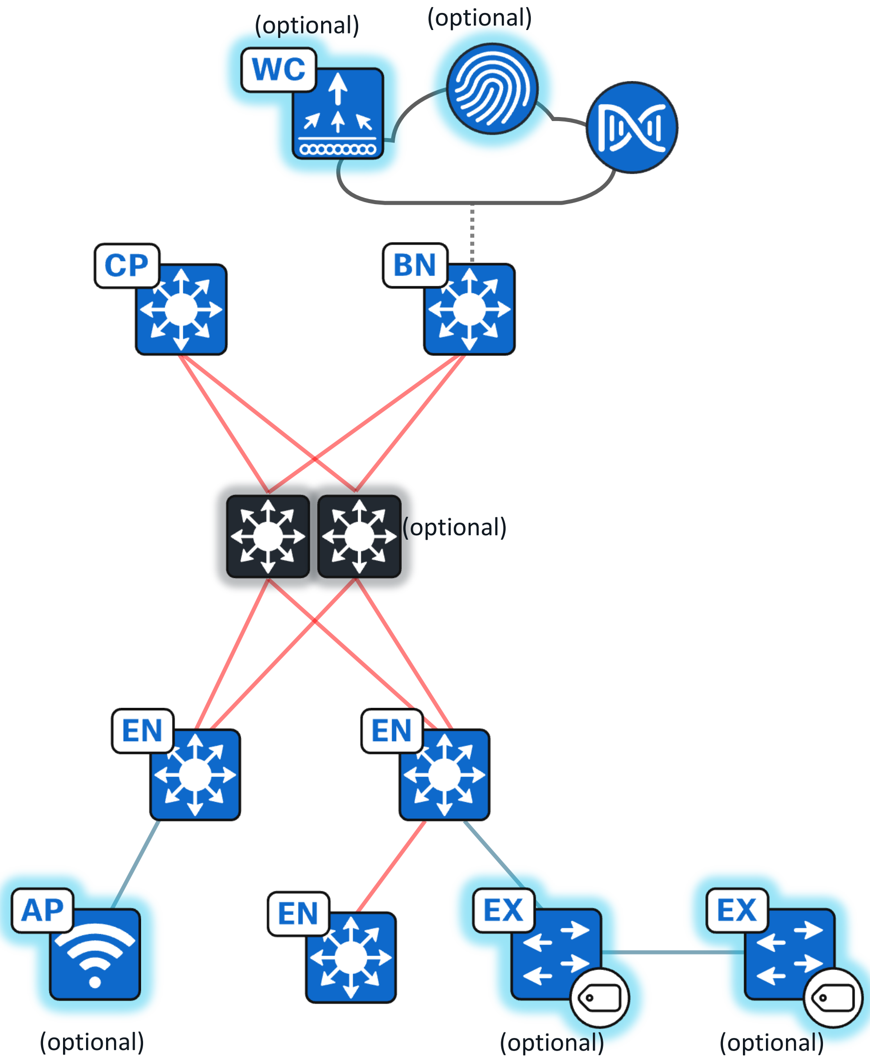
- **Cisco Catalyst Center** – GUI and APIs for intent-based automation of wired and wireless fabric devices.
- **Fabric Border Nodes** – A fabric device that connects external L3 and L2 networks to the Cisco SD-Access fabric.
- **Edge Nodes** – A fabric device that connects wired endpoints to the Cisco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

BN|CP

Border Node and Control Plane Node.

BN|CP|EN

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

BN|CP

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

BN|CP|EN

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

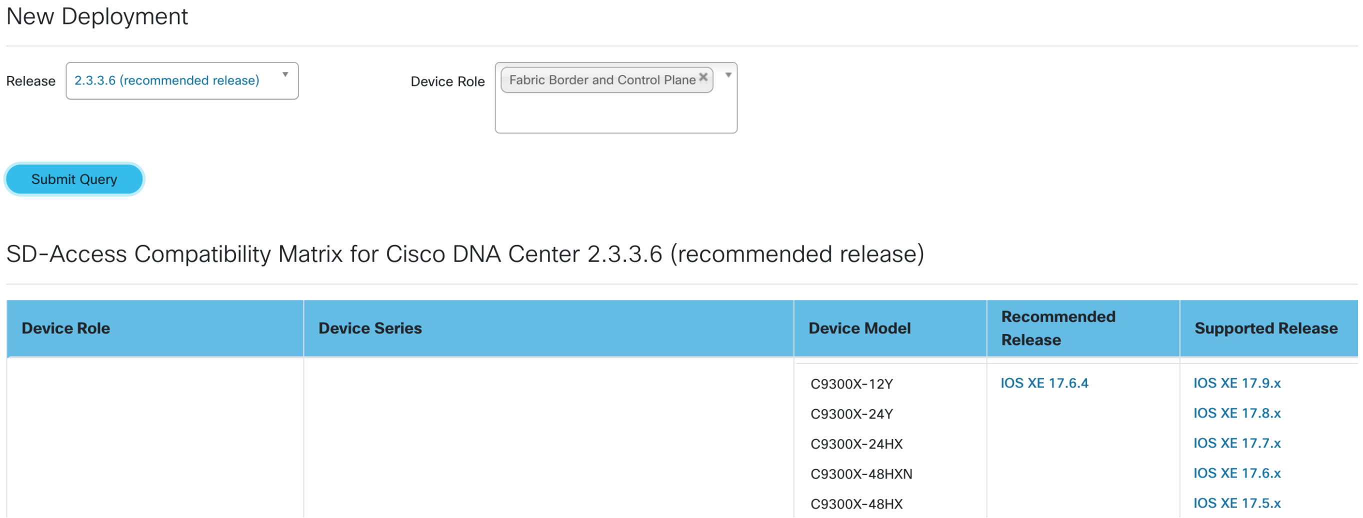
SD-Access Design Aides

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

Cisco SD-Access Design Tool

Create Design of Cisco SD-Access for your environment

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



New Deployment

Release: 2.3.3.6 (recommended release)

Device Role: Fabric Border and Control Plane

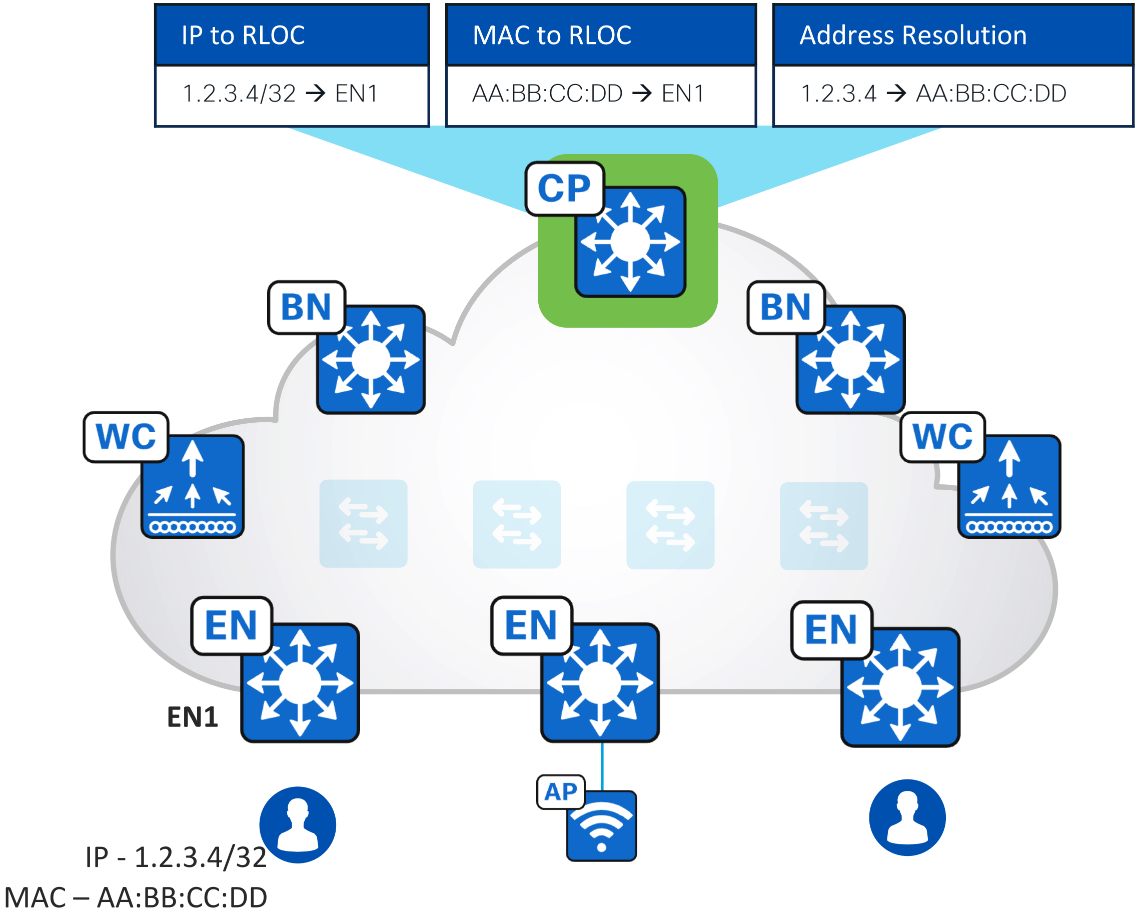
SD-Access Compatibility Matrix for Cisco DNA Center 2.3.3.6 (recommended release)

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

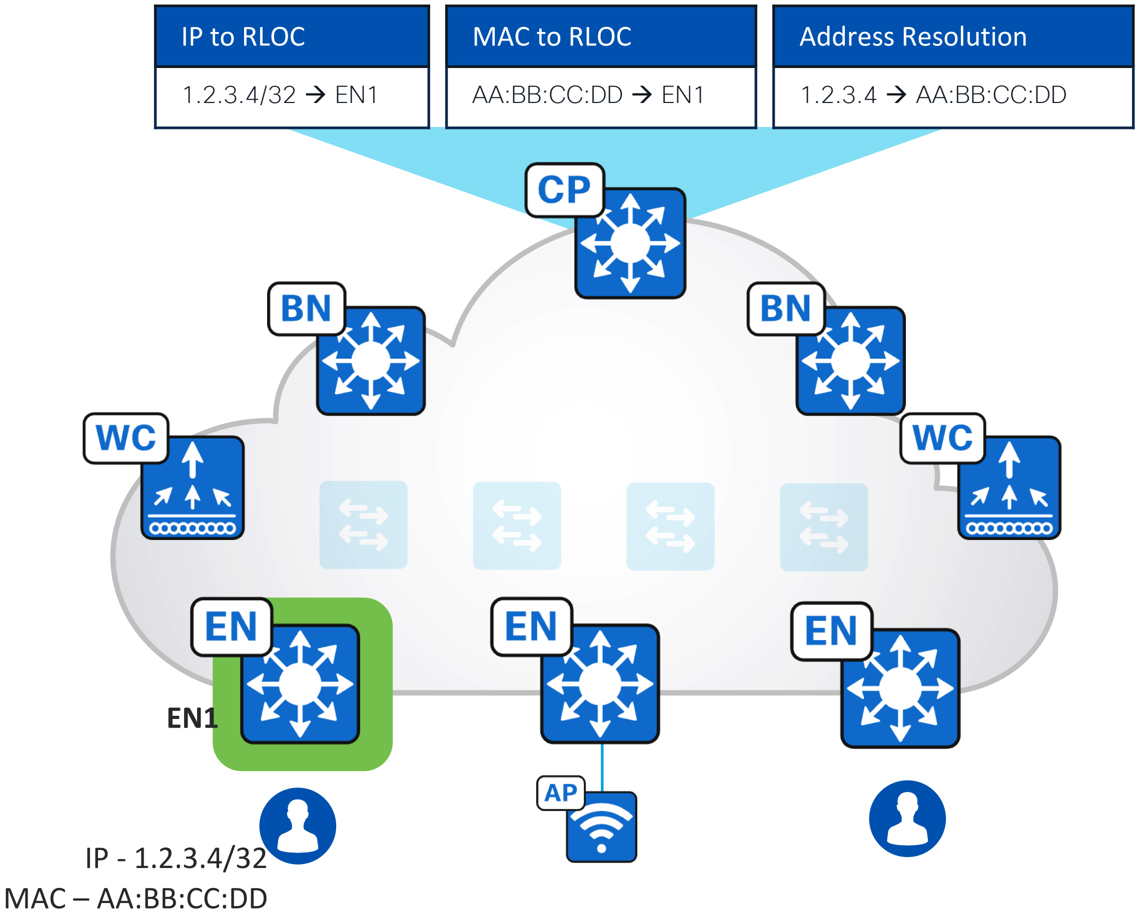


IP to RLOC	MAC to RLOC	Address Resolution
1.2.3.4/32 → EN1	AA:BB:CC:DD → EN1	1.2.3.4 → AA:BB:CC:DD

Cisco SD-Access Fabric

Edge Node Provides First Hop Services for Endpoints

- Responsible for Authenticating and Authorizing wired 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.

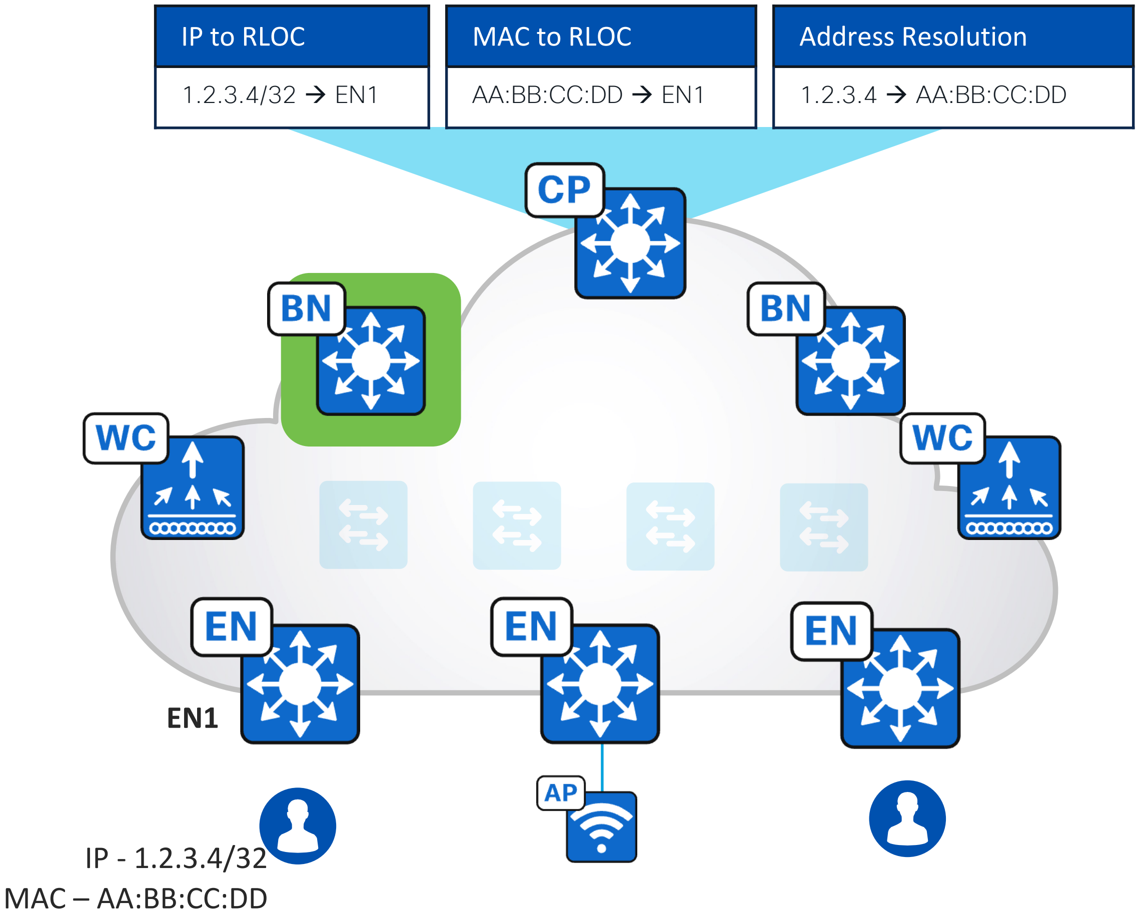


IP to RLOC	MAC to RLOC	Address Resolution
1.2.3.4/32 → EN1	AA:BB:CC:DD → EN1	1.2.3.4 → AA:BB:CC:DD

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.



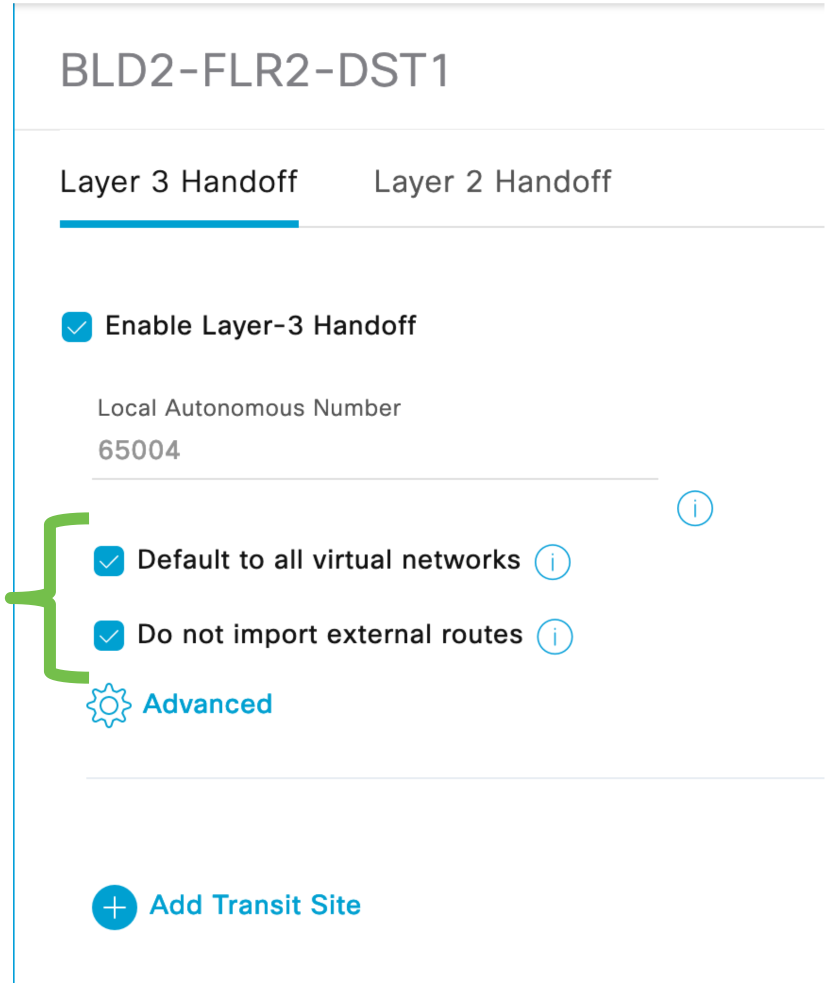
IP to RLOC	MAC to RLOC	Address Resolution
1.2.3.4/32 → EN1	AA:BB:CC:DD → EN1	1.2.3.4 → AA:BB:CC:DD

IP - 1.2.3.4/32
MAC – AA:BB:CC:DD

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.



BLD2-FLR2-DST1

☑ Enable Layer-3 Handoff

Local Autonomous Number: 65004

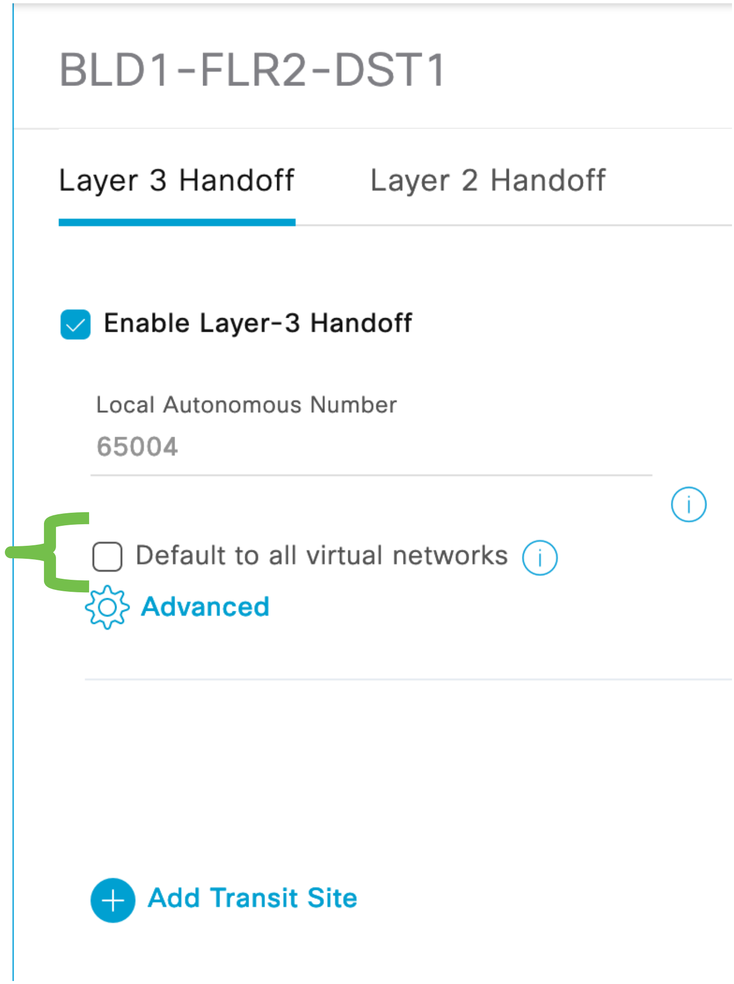
☑ Default to all virtual networks

☑ Do not import external routes

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.



BLD1-FLR2-DST1

☑ Enable Layer-3 Handoff

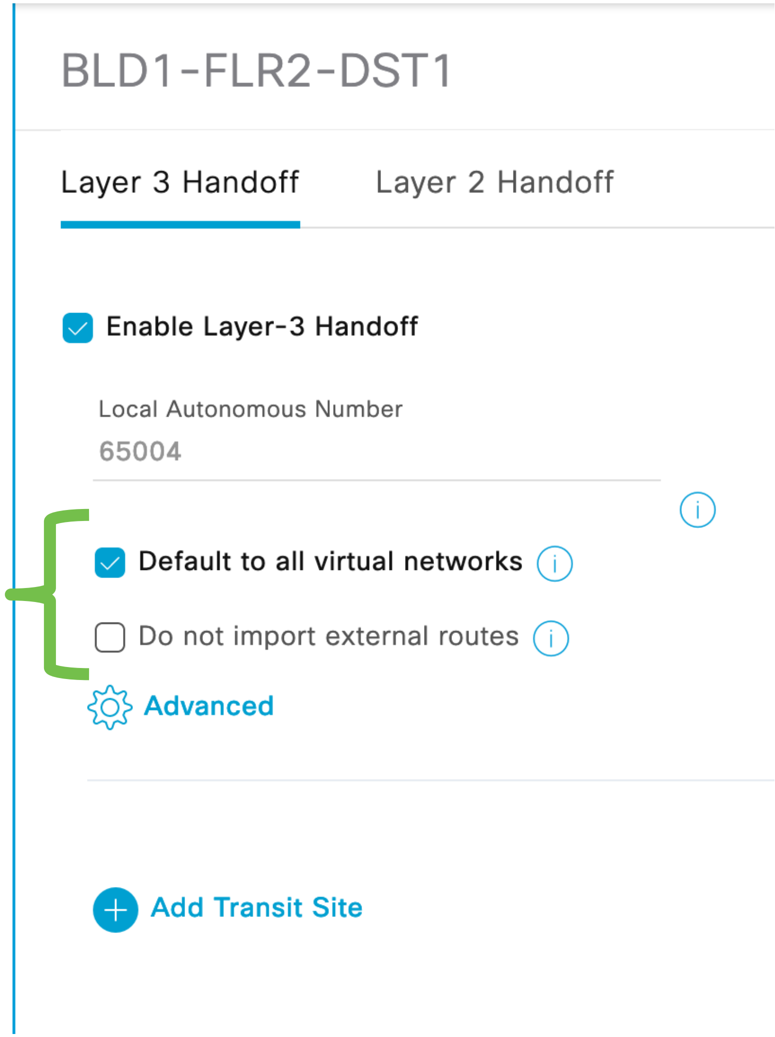
Local Autonomous Number: 65004

☐ Default to all virtual networks

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

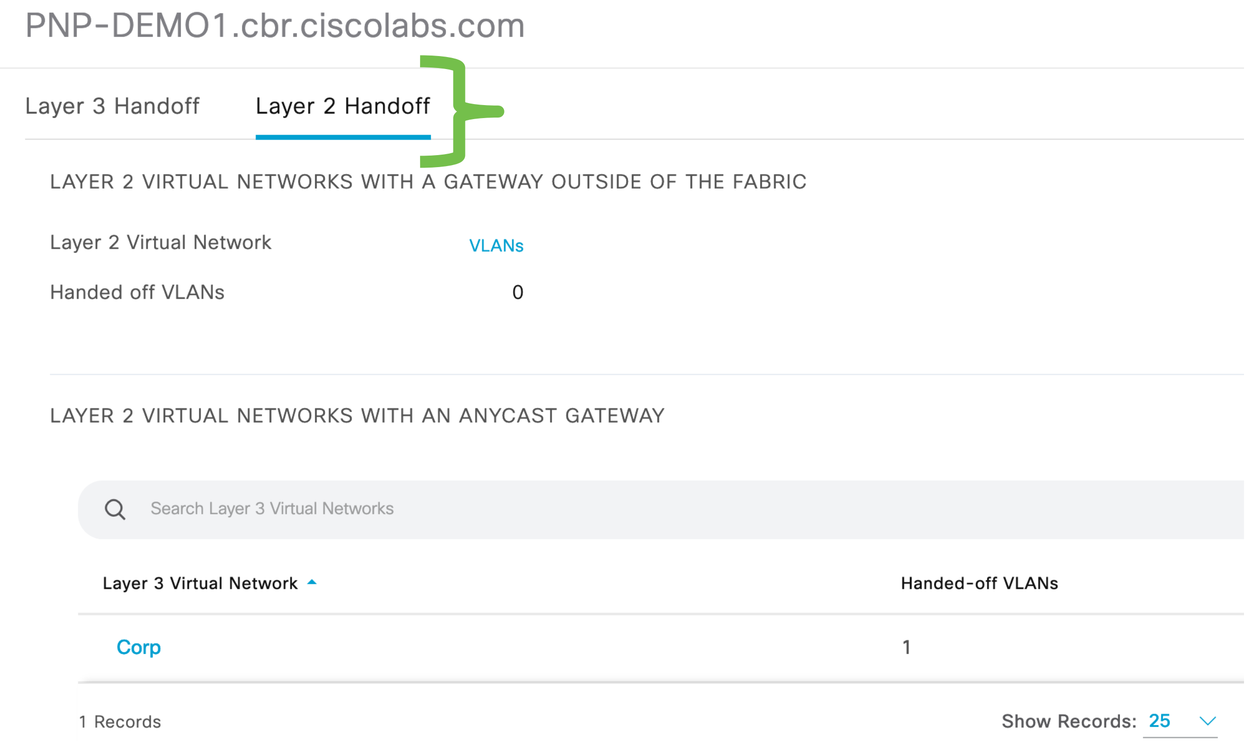
☑ Default to all virtual networks

□ Do not import external routes

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 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

Layer 3 Virtual Network	Handed-off VLANs
Corp	1

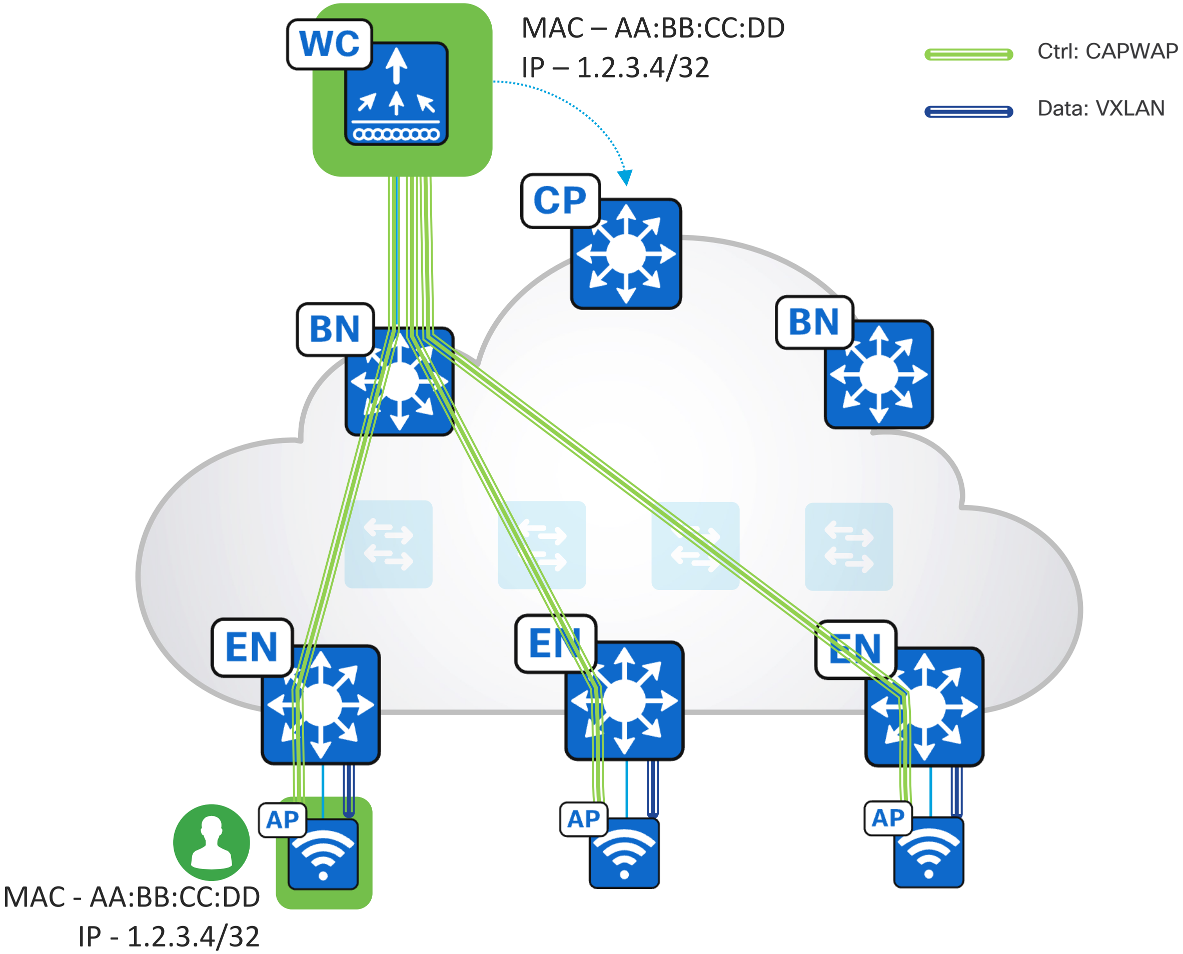
1 Records

Show Records: 25

Cisco SD-Access Fabric

Fabric Enabled Wireless for Unified Management, Policy and Data Planes

- Fabric WLC accessible 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. 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.



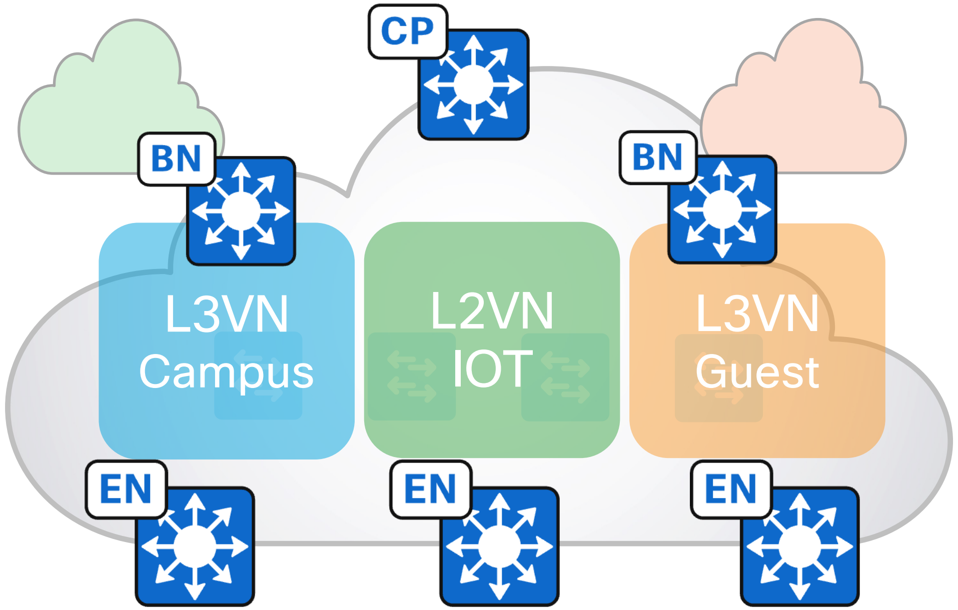
Roles and Terminology

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

Cisco SD-Access Fabric

Virtual Networks

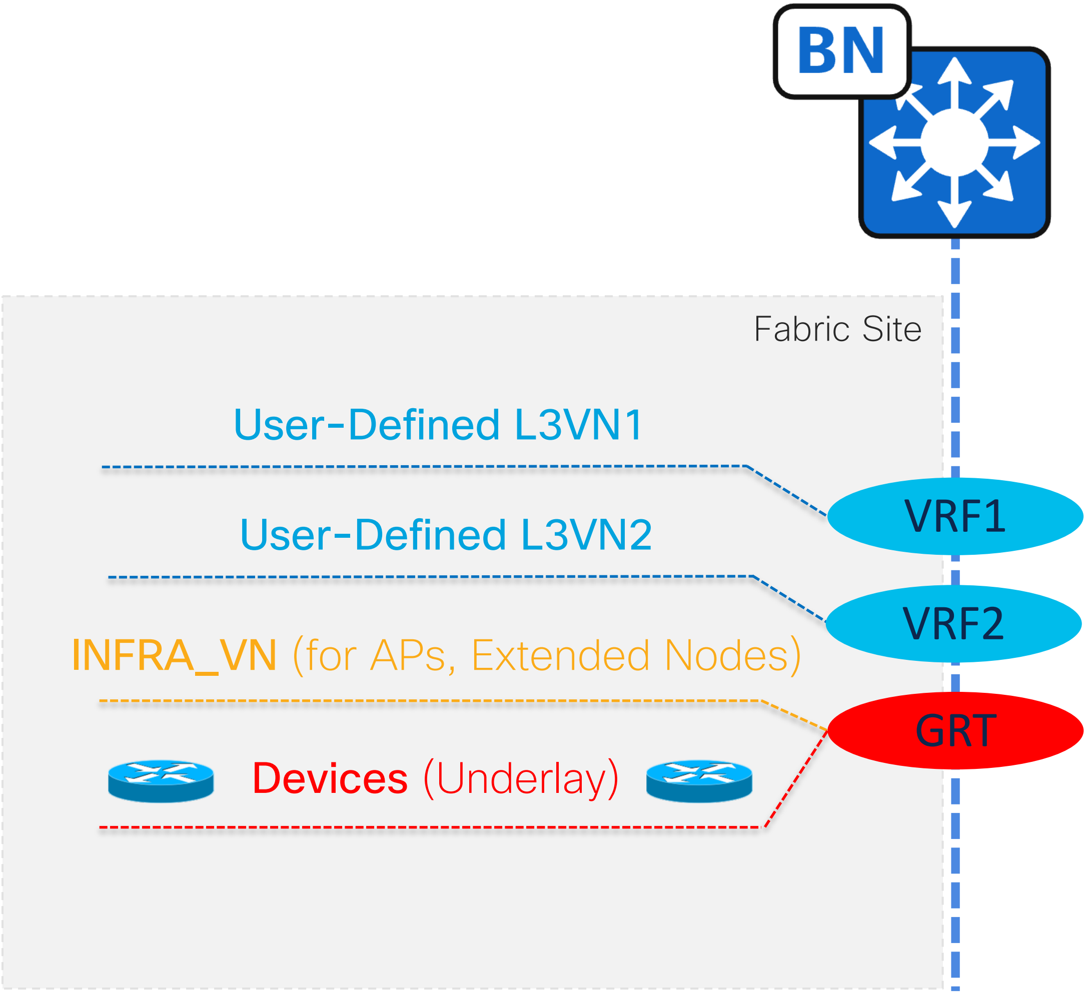
- Layer 3 Virtual Networks use VRFs and LISP Instance IDs to maintain separate routing topologies.
  - Endpoint IDs (IPv4/IPv6 addresses) are routed within an L3VN.
- Layer 2 Virtual Networks use LISP Instance IDs and VLANs to maintain separate switching topologies.
  - Endpoint IDs (MAC addresses) are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

- **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.

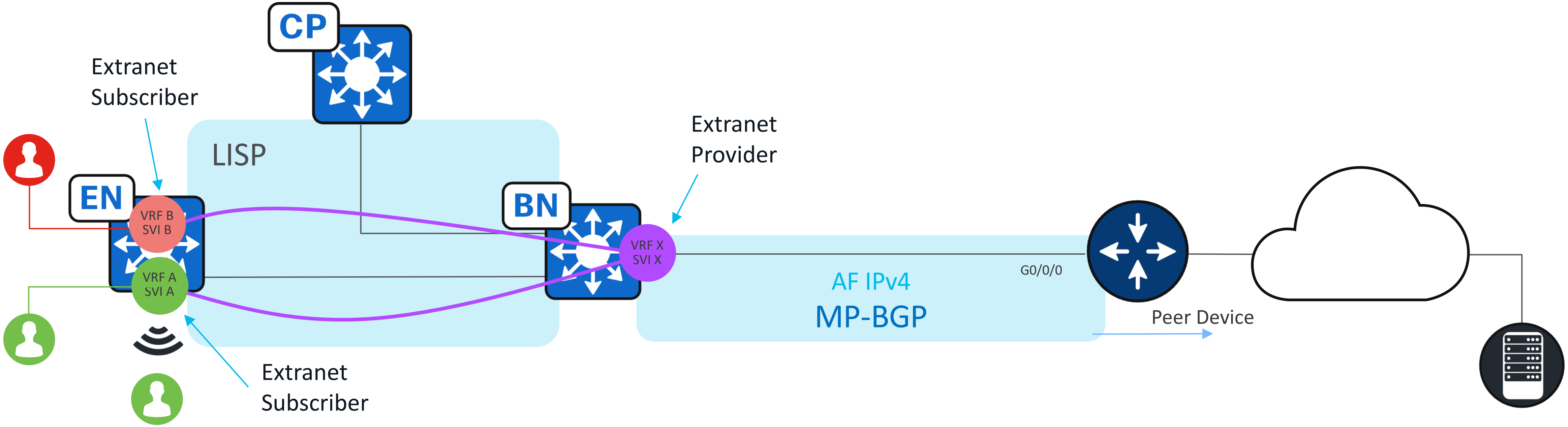


GRT=Global Route Table

Cisco SD-Access Fabric

Extranet Provider Virtual Network Layer 3 Handoff

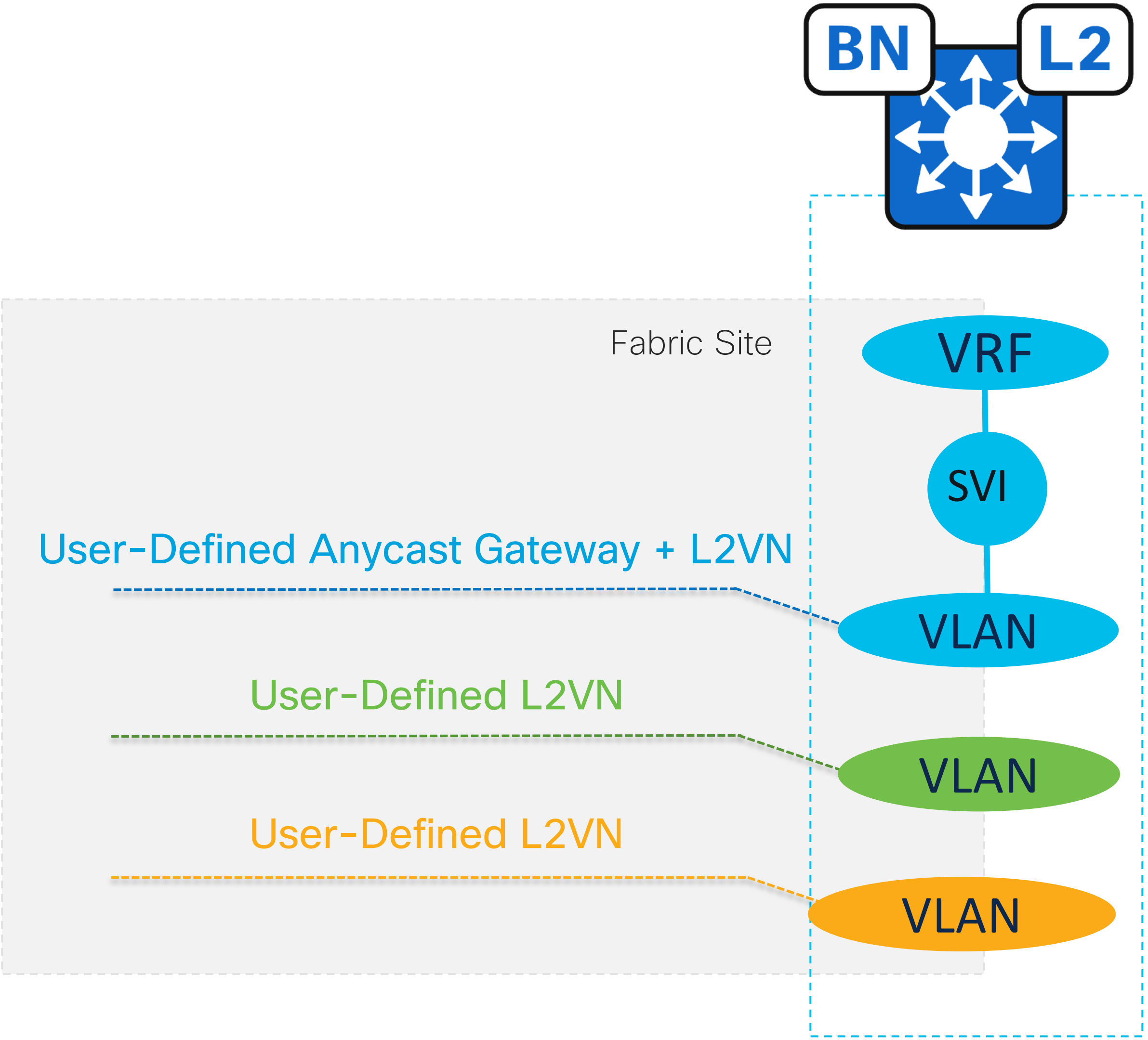
- Use an Extranet Policy to allow communication between one Provider Virtual Network and one or more Subscriber Virtual Networks.
- Extranet Policy is available from SD-Access 2.3.5.3. Requires LISP Pub/Sub Control Plane.



Cisco SD-Access Fabric

Layer 2 Handoff

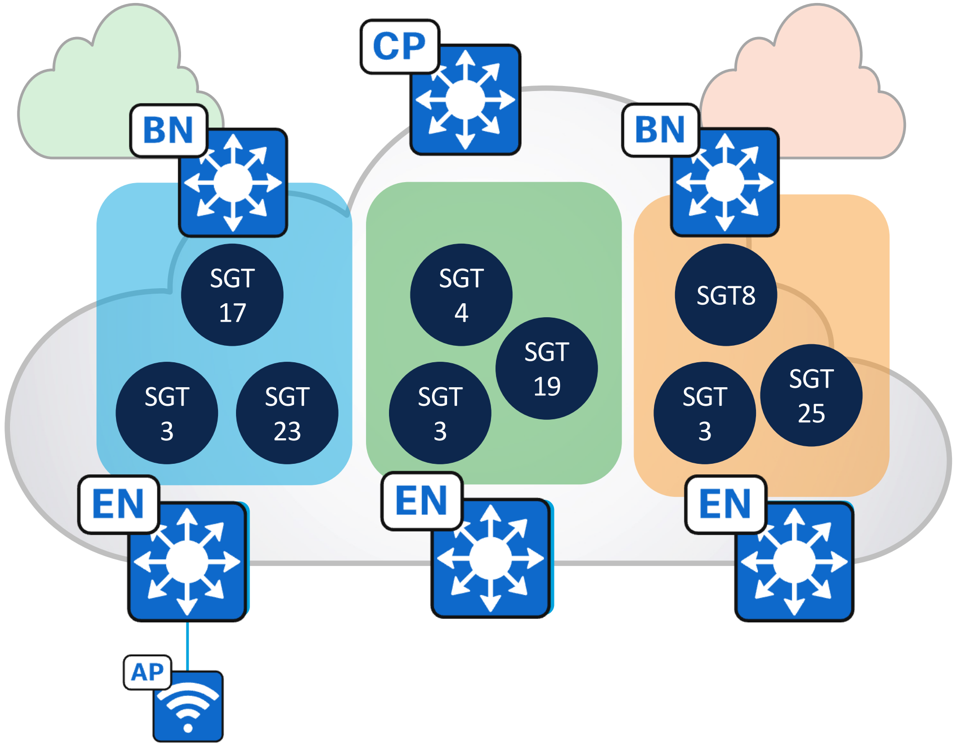
- Ancient wisdom: Route whenever you can, switch when you must.
- Layer 2 Virtual Networks handoff through a user-defined VLAN.
- Layer 2 Virtual Networks may implement Broadcast, unknown-unicast and multicast flooding. Be mindful of loop prevention.



Cisco SD-Access Fabric

A Security Group Tag Assigns a "Group" to Each Endpoint

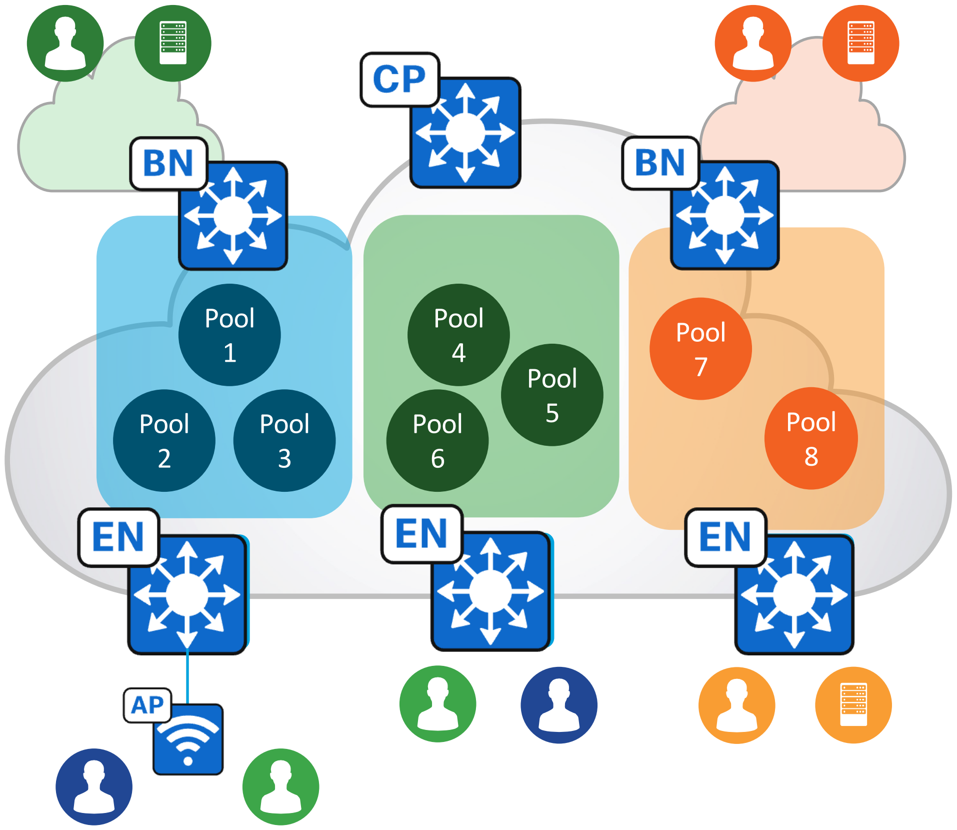
- Edge Nodes and Fabric APs assign a unique Security Group Tag (SGT) to each endpoint in concert with ISE.
- Edge Nodes and Fabric APs add an SGT to the fabric encapsulation.
- SGTs are used to implement IP-address-independent traffic policies.
- SGTs can be extended to numerous other networking technologies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

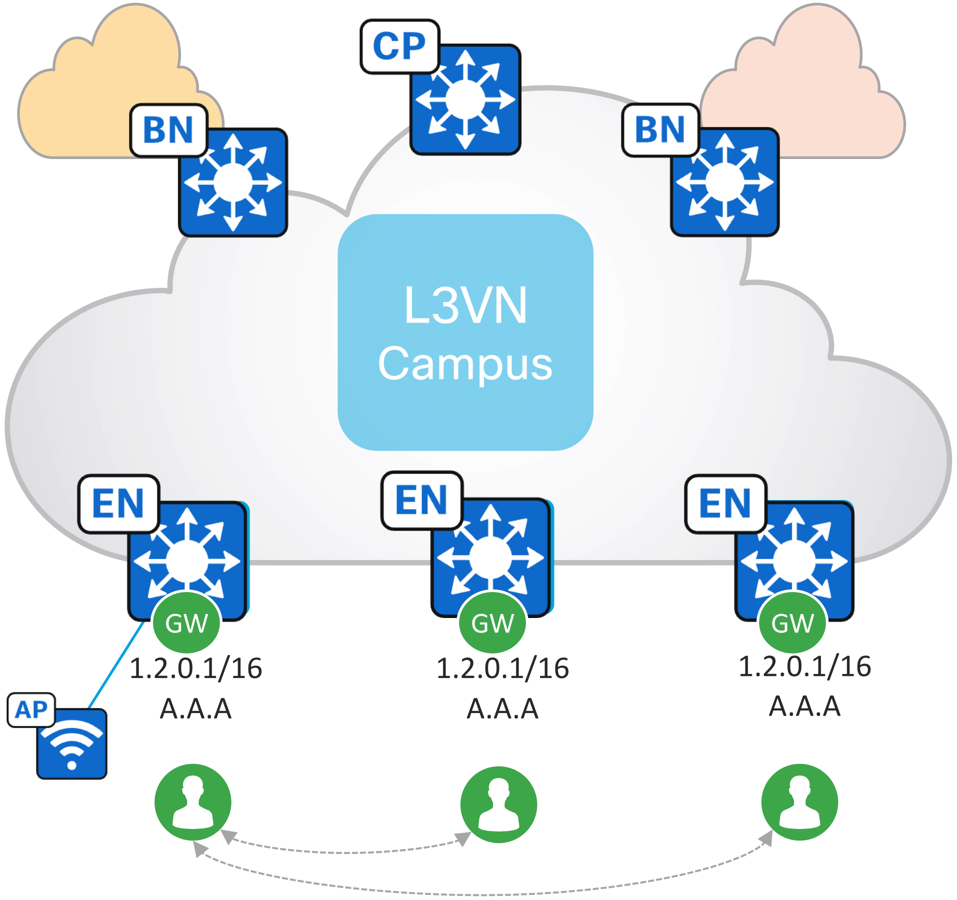
- Edge Nodes instantiate an access VLAN and a Switched Virtual Interface (SVI) with user-defined IPv4/IPv6 addresses per Host Pool.
- Host Pools assigned to endpoints dynamically by AAA or statically per port.
- Edge Nodes and Fabric WLCs register endpoint IDs (/32, /128 or MAC) with the Control Plane,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



Cisco SD-Access Fabric

Anycast Gateway Provides a Default Gateway for IP-Capable Endpoints

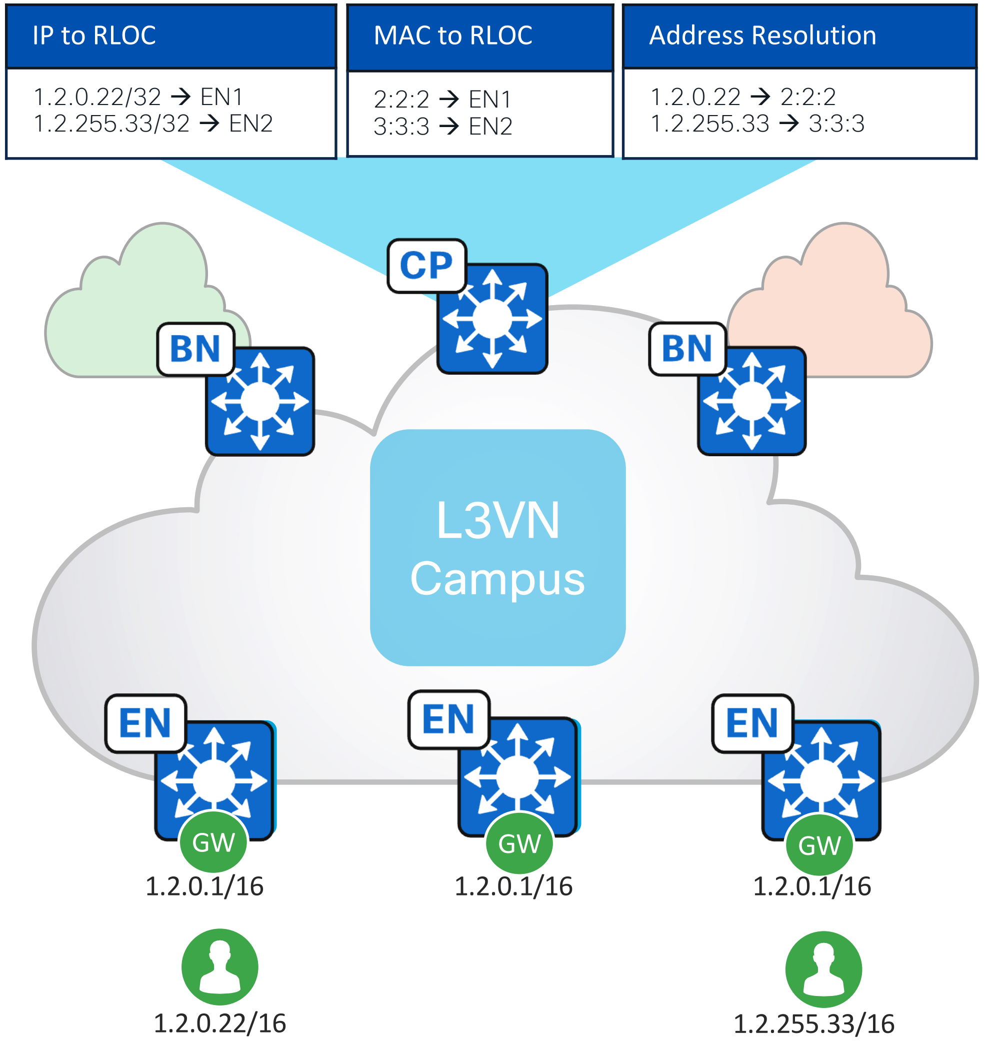
- Similar principle and behavior to FHRP with a shared virtual IPv4/IPv6 addresses and MAC address.
- The same Switch Virtual Interface (SVI) is present on all Edge Nodes with the same virtual IP and MAC.
- The wired or wireless endpoint can connect to any switch or AP in the fabric and communicate with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



IP to RLOC
1.2.0.22/32 → EN1 1.2.255.33/32 → EN2

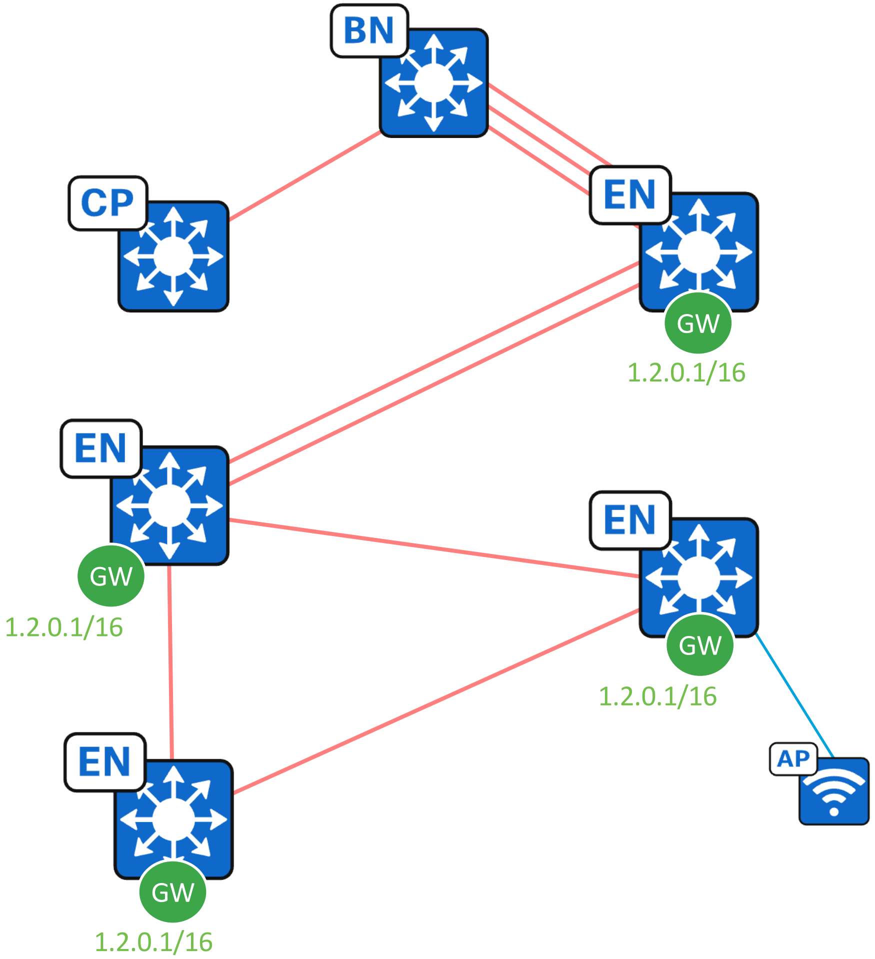
MAC to RLOC
2:2:2 → EN1 3:3:3 → EN2

Address Resolution
1.2.0.22 → 2:2:2 1.2.255.33 → 3:3:3

Cisco SD-Access Fabric

Accommodates any Physical Network Topology

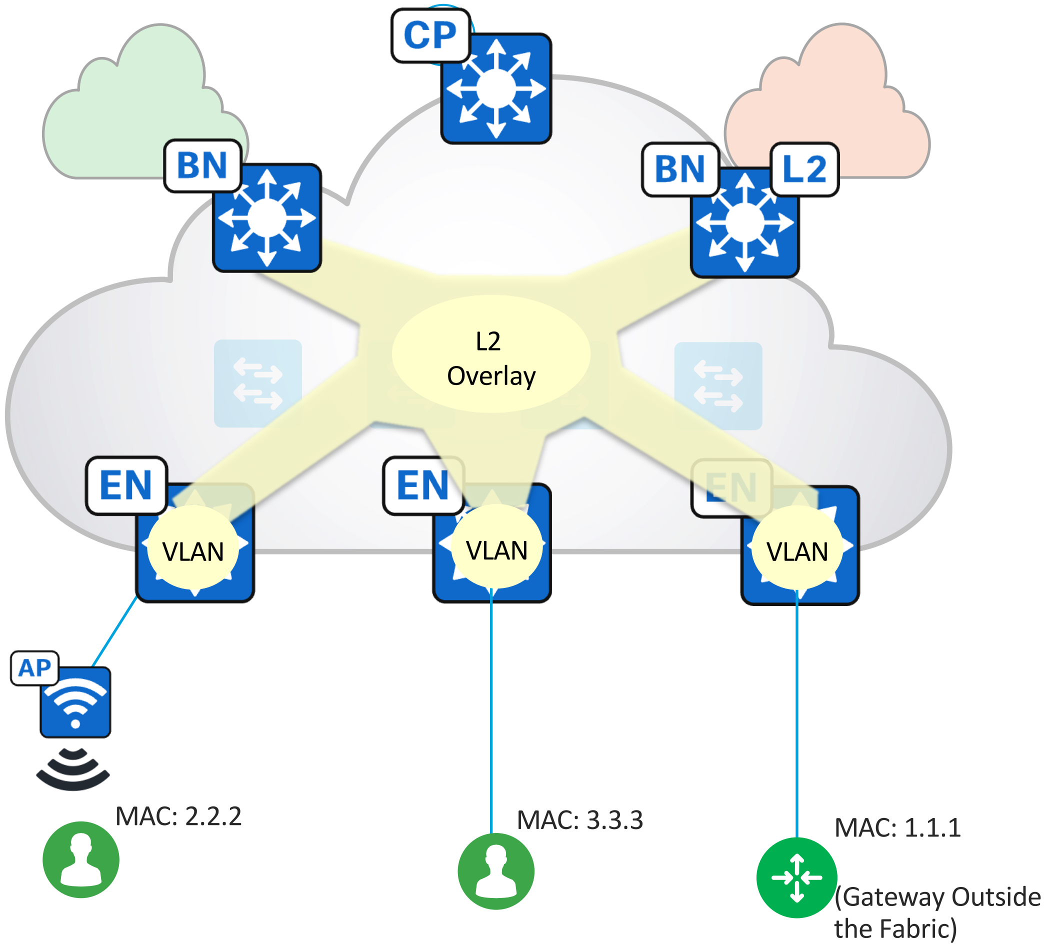
- Overlays are agnostic to underlay physical topology.
- Any wired or wireless endpoint address anywhere, including environments with unusual cabling implementations.
- Routed underlay IGP takes care of load balancing and fast link/node fault convergence. Obsoletes less robust mechanisms like L2 Trunking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



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.
  - Often 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

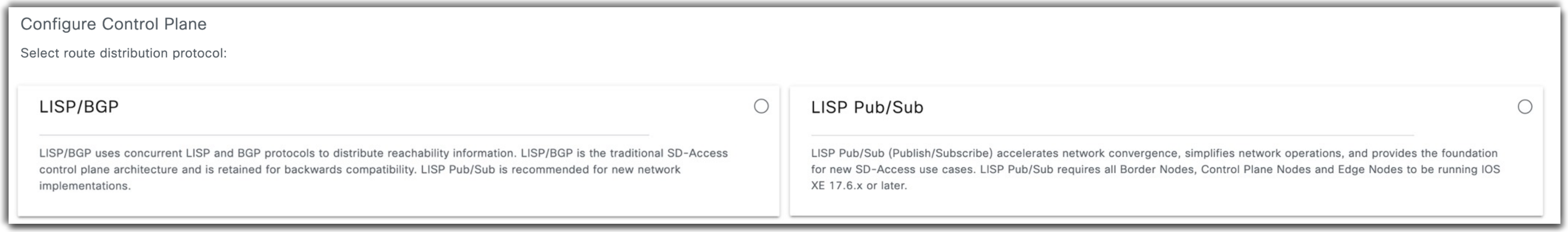
1. Control Plane
2. Data Plane
3. Policy Plane

Cisco SD-Access Fabric

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

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

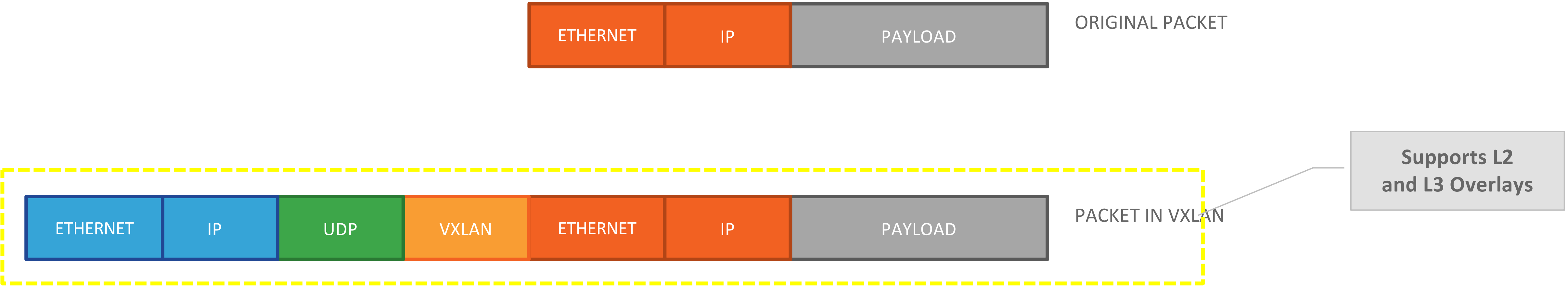
*Rebranded to Catalyst Center in late 2023

Fabric Fundamentals

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

Cisco SD-Access Fabric

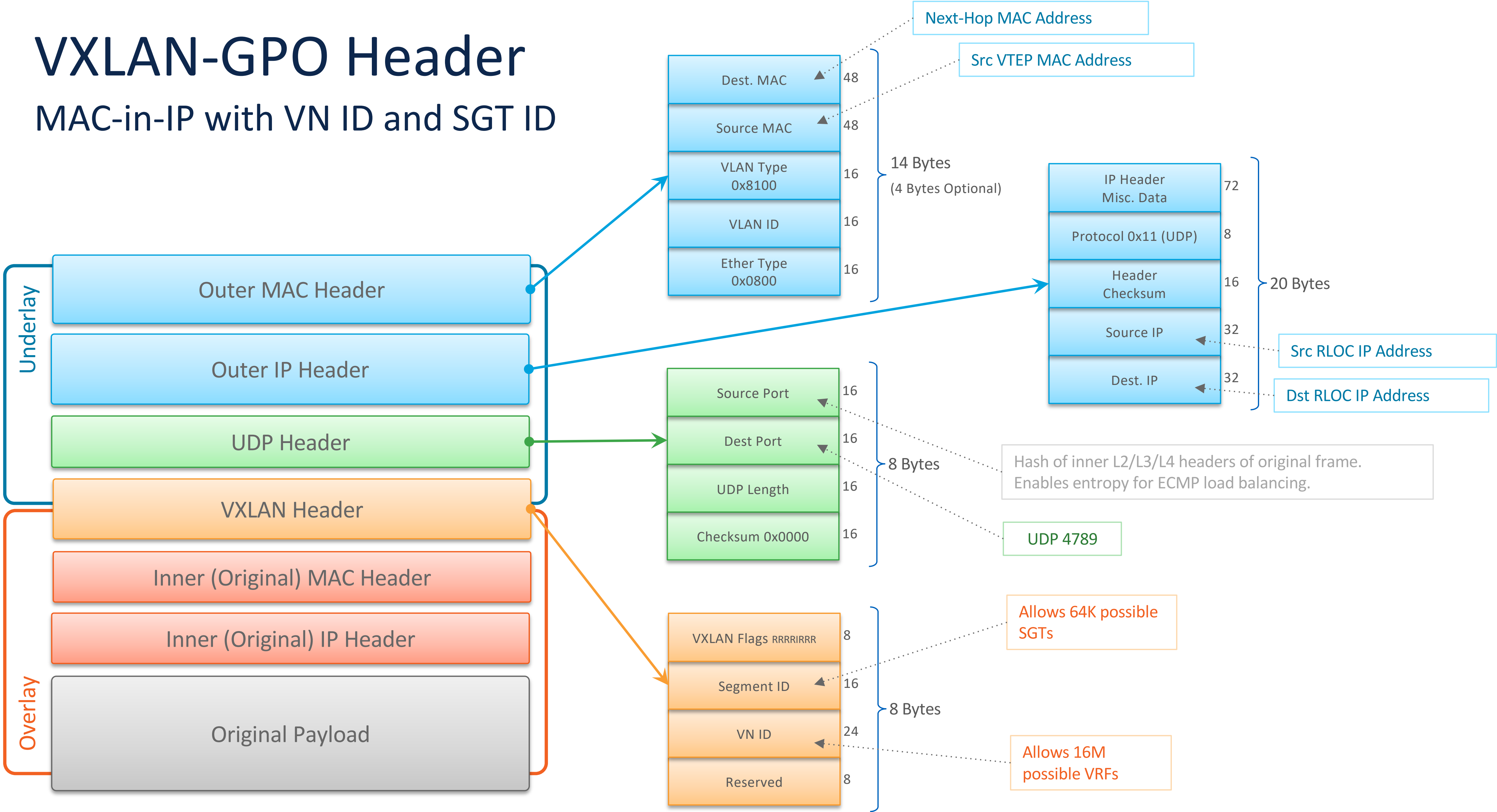
1. **Control Plane: LISP**
2. **Data Plane: VXLAN**



Supports L2 and L3 Overlays

VXLAN-GPO Header

MAC-in-IP with VN ID and SGT ID



Underlay

Outer MAC Header

Outer IP Header

UDP Header

Overlay

VXLAN Header

Inner (Original) MAC Header

Inner (Original) IP Header

Original Payload

Field	Bits
Dest. MAC	48
Source MAC	48
VLAN Type 0x8100	16
VLAN ID	16
Ether Type 0x0800	16

14 Bytes
(4 Bytes Optional)

Next-Hop MAC Address

Src VTEP MAC Address

Field	Bits
IP Header Misc. Data	72
Protocol 0x11 (UDP)	8
Header Checksum	16
Source IP	32
Dest. IP	32

20 Bytes

Src RLOC IP Address

Dst RLOC IP Address

Field	Bits
Source Port	16
Dest Port	16
UDP Length	16
Checksum 0x0000	16

8 Bytes

Hash of inner L2/L3/L4 headers of original frame.
Enables entropy for ECMP load balancing.

UDP 4789

Field	Bits
VXLAN Flags RRRRIRRR	8
Segment ID	16
VN ID	24
Reserved	8

8 Bytes

Allows 64K possible SGTs

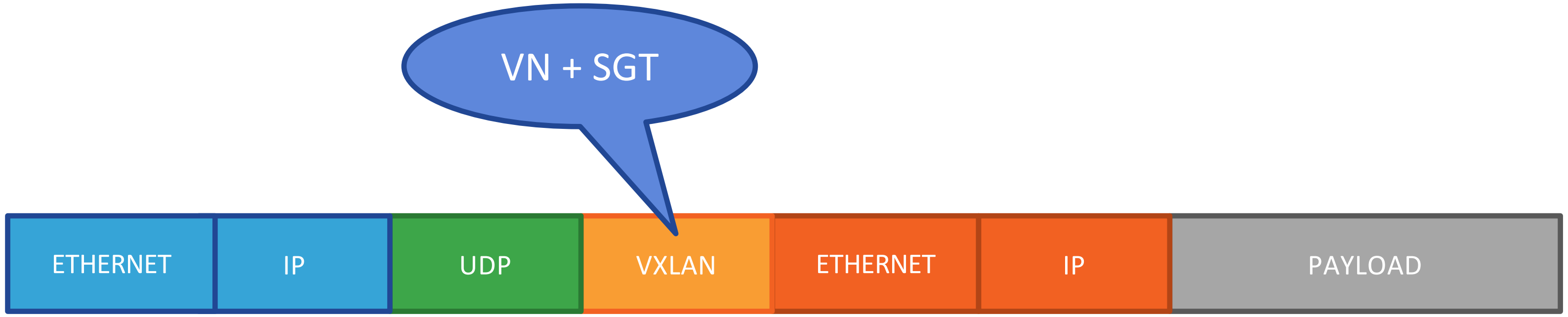
Allows 16M possible VRFs

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**

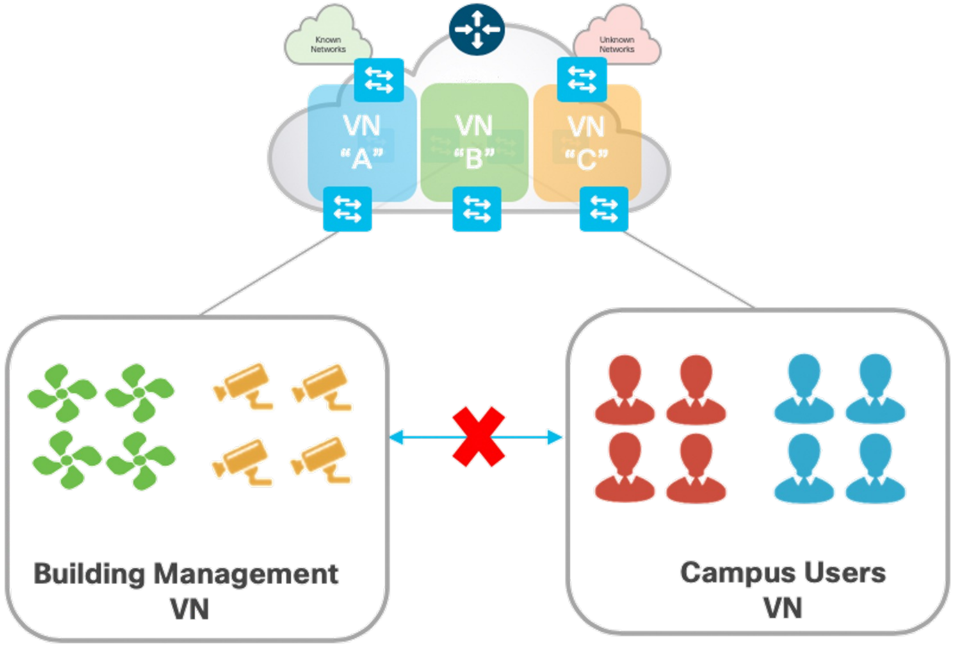


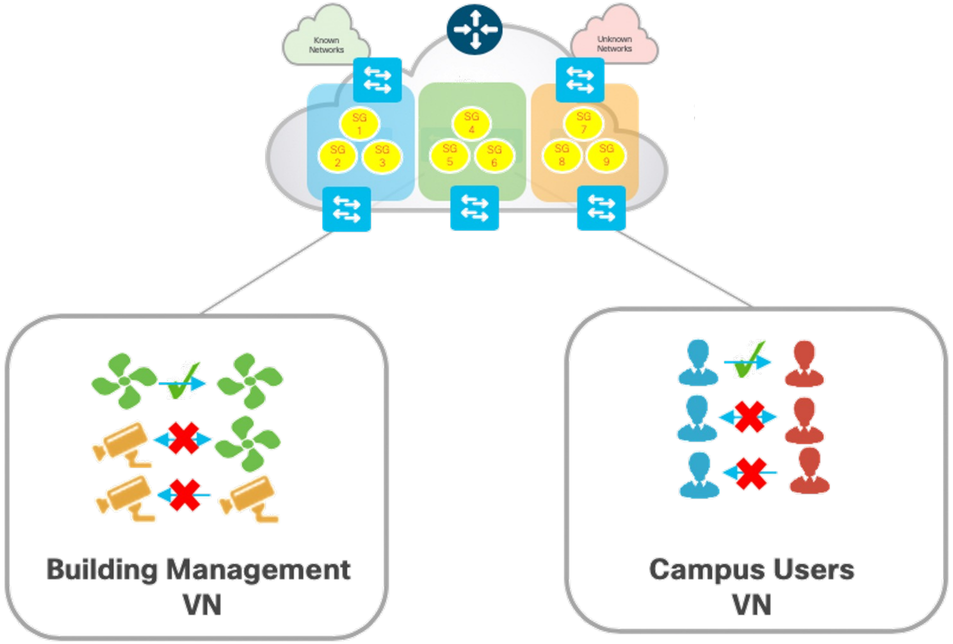
Virtual Routing & Forwarding

Security Group Tagging

SD-Access Policy

Macro-Segmentation and Micro-Segmentation





Virtual Network (VN)

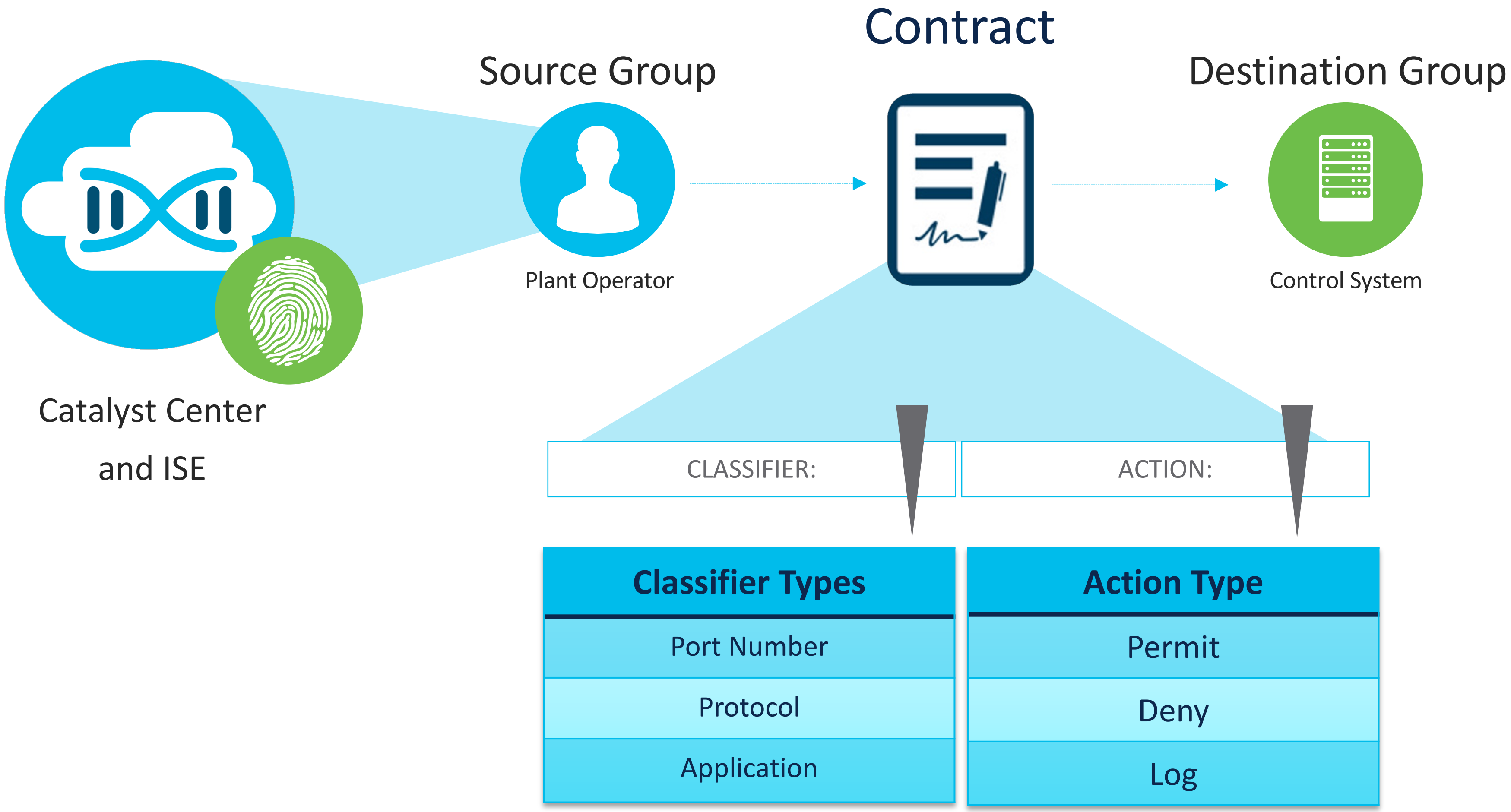
First-level segmentation ensures **zero communication** between forwarding domains. Ability to consolidate multiple networks into one physical network.

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 Contracts



Contract

Source Group

Destination Group

Plant Operator

Control System

Catalyst Center and ISE

CLASSIFIER:

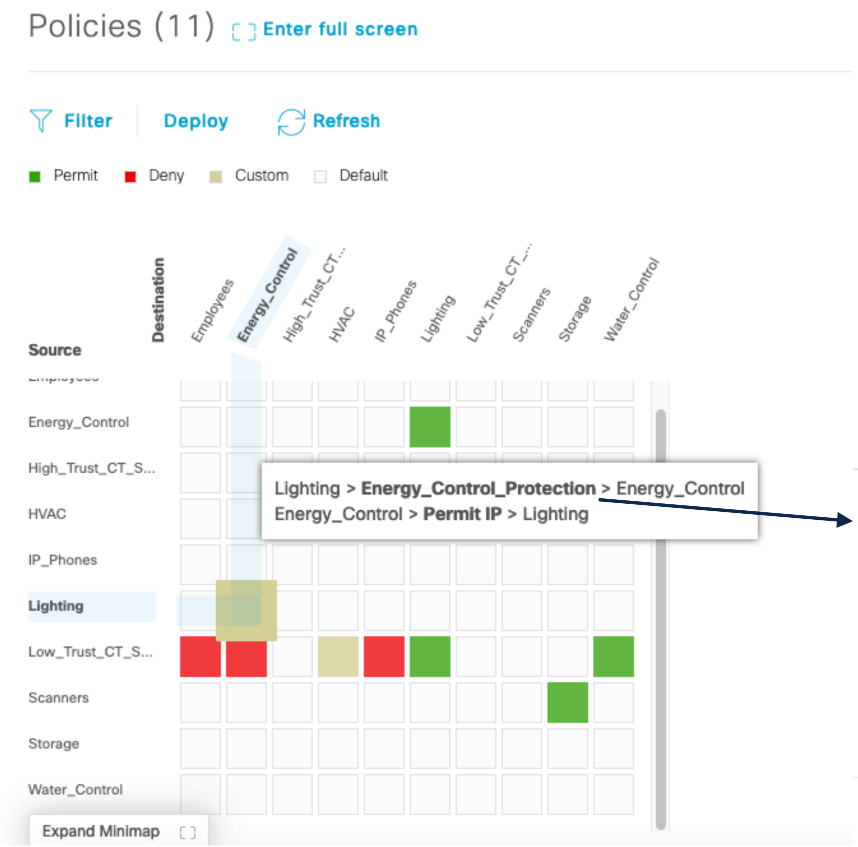
ACTION:

Classifier Types
Port Number
Protocol
Application

Action Type
Permit
Deny
Log

SD-Access Policy

Group-Based Access Control



Policies (11) Enter full screen

Filter Deploy Refresh

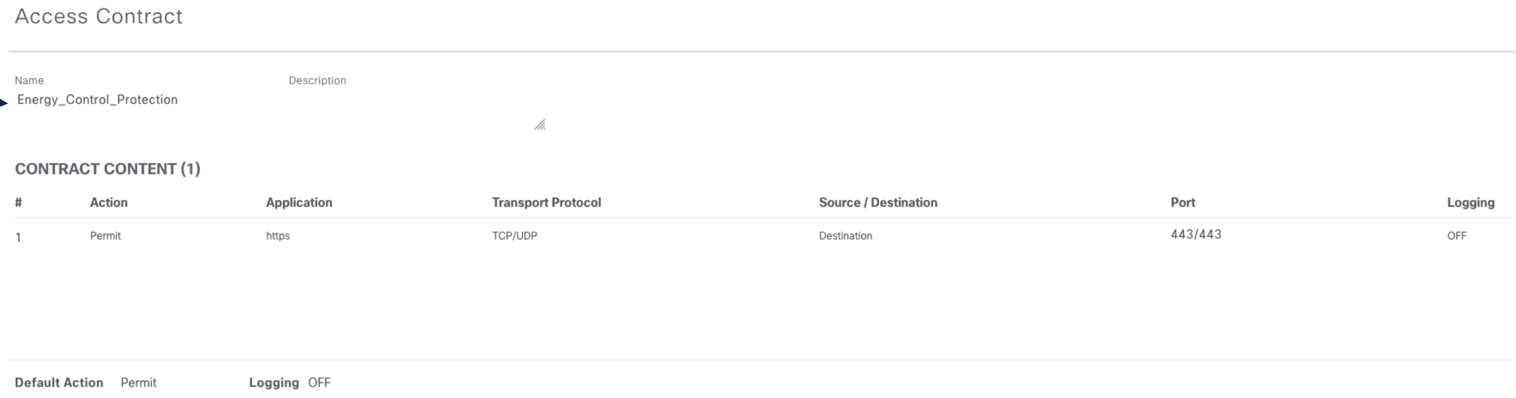
🟩 Permit 🟥 Deny ▨ Custom □ Default

Source \ Destination	Employees	Energy_Control	High_Trust_CT...	HVAC	IP_Phones	Lighting	Low_Trust_CT_...	Scanners	Storage	Water_Control
Employees	□	□	□	□	□	□	□	□	□	□
Energy_Control	□	□	□	□	□	🟩	□	□	□	□
High_Trust_CT_S...	□	□								
HVAC	□	□								
IP_Phones	□	□	□	□	□	□	□	□	□	□
Lighting	□	▨	□	□	□	□	□	□	□	□
Low_Trust_CT_S...	🟥	🟥	□	▨	🟥	🟩	□	□	□	🟩
Scanners	□	□	□	□	□	□	□	□	🟩	□
Storage	□	□	□	□	□	□	□	□	□	□
Water_Control	□	□	□	□	□	□	□	□	□	□

Lighting > **Energy_Control_Protection** > Energy_Control
Energy_Control > **Permit IP** > Lighting

Expand Minimap

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



Access Contract

Name: Energy_Control_Protection

Description:

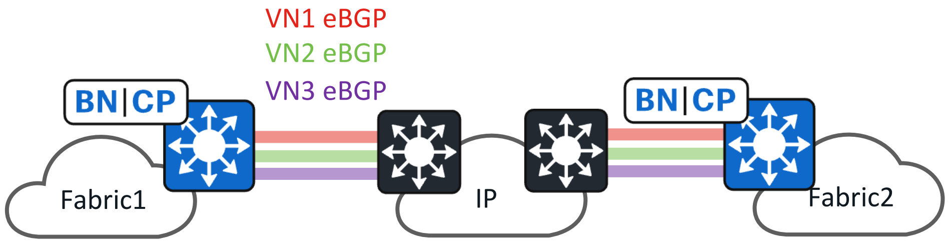
CONTRACT CONTENT (1)

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

Default Action Permit **Logging** OFF

Multiple Fabrics

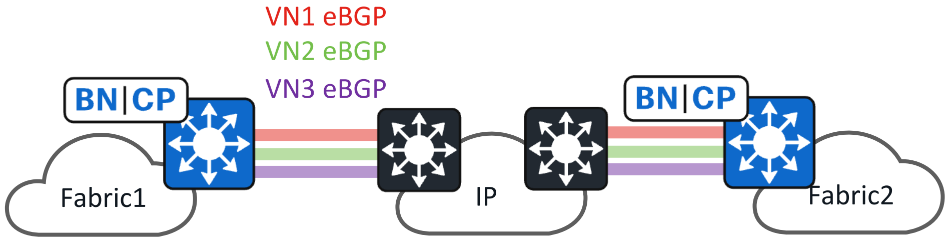
Transits, VN and SGT Preservation



IP-Based Transit

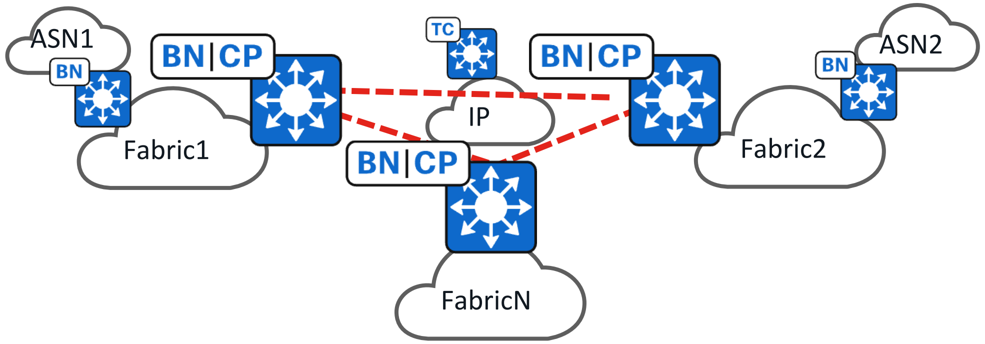
- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.

Transits, VN and SGT Preservation



IP-Based Transit

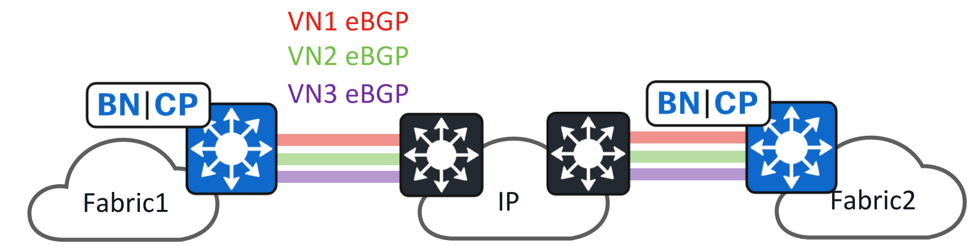
- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.



SD-Access Transit

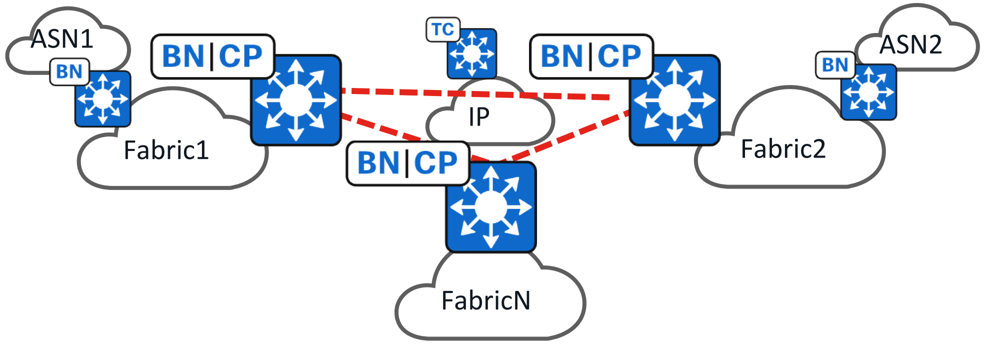
- SD-Access LISP/VXLAN between Fabric Sites.
- Natively preserves Layer 3 Virtual Networks and SGTs.
- Capable of fabric as a transit between external routing domains.

Transits, VN and SGT Preservation



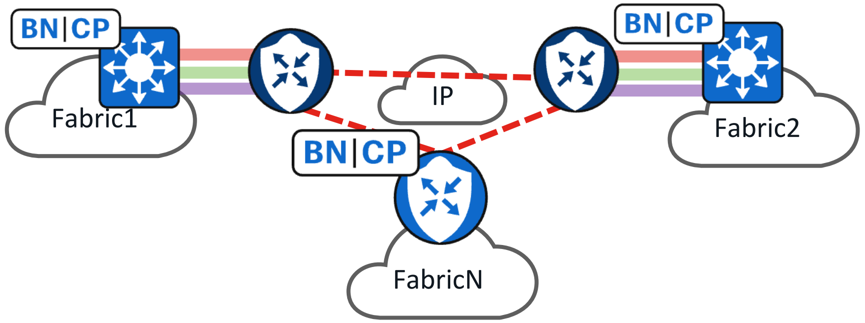
IP-Based Transit

- 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

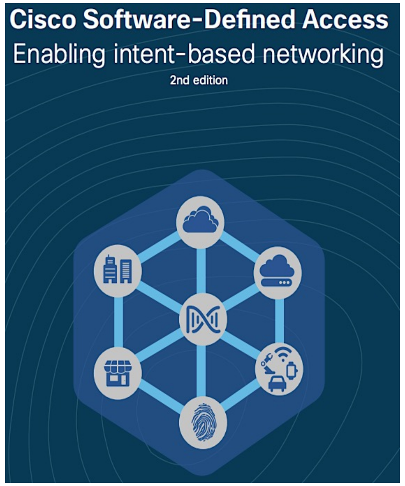
- Cisco SD-WAN between Fabric Sites.
- Capable of preserving Layer 3 Virtual Networks and SGTs.
- Dedicated SD-WAN Edge for design flexibility, Border Node port densities and port speeds. See Independent Domains PDG.

Cisco SD-Access Collaterals

Cisco Software-Defined Access for Industry Verticals

Cisco Software-Defined Access for Industry Verticals
From Design to Migration

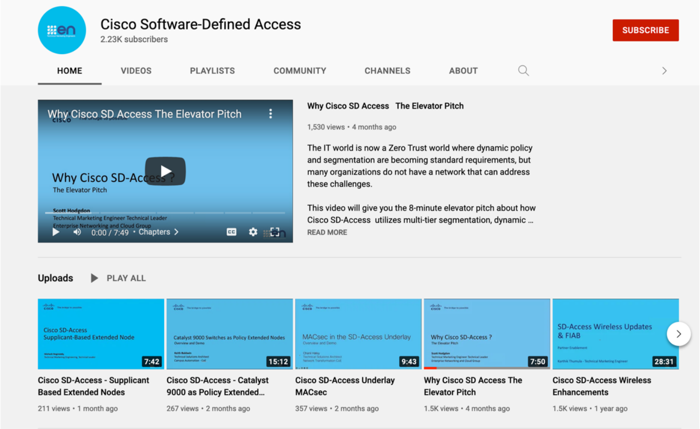
Cisco Software-Defined Access
Enabling intent-based networking


Cisco Software-Defined Access
Enabling intent-based networking
2nd edition

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 Software-Defined Access
2.23K subscribers

Why Cisco SD Access The Elevator Pitch

1,530 views • 4 months ago

The IT world is now a Zero Trust world where dynamic policy and segmentation are becoming standard requirements, but many organizations do not have a network that can address these challenges.

This video will give you the 8-minute elevator pitch about how Cisco SD-Access utilizes multi-tier segmentation, dynamic ...

READ MORE

Uploads PLAY ALL

Cisco SD-Access
Supplicant-Based Extended Node
7:42
Catalyst 9000 Switches as Policy Extended Nodes
Overview and Demo
15:12
MACsec in the SD-Access Underlay
Overview and Demo
9:43
Why Cisco SD-Access ?
The Elevator Pitch
7:50
SD-Access Wireless Updates & FIAB
Partner Enablement
28:31

Cisco SD-Access - Supplicant Based Extended Nodes	Cisco SD-Access - Catalyst 9000 as Policy Extended...	Cisco SD-Access Underlay MACsec	Why Cisco SD Access The Elevator Pitch	Cisco SD-Access Wireless Enhancements
211 views • 1 month ago	267 views • 2 months ago	357 views • 2 months ago	1.5K views • 4 months ago	1.5K views • 1 year ago

Multiple Cisco DNA Center to ISE

Cisco SD-Access Design Tool

EN&C Validated Designs

The Latest SD-Access Guides

The bridge to possible

Thank you