The Power of Cisco SD-Access LISP Fabric

Simplified Deployment to Advanced Use Cases – Part 1

Mahesh Nagireddy
Technical Marketing Engineer

Devi Bellamkonda
Technical Marketing Engineer

BRKENS-1804

Cisco Webex App

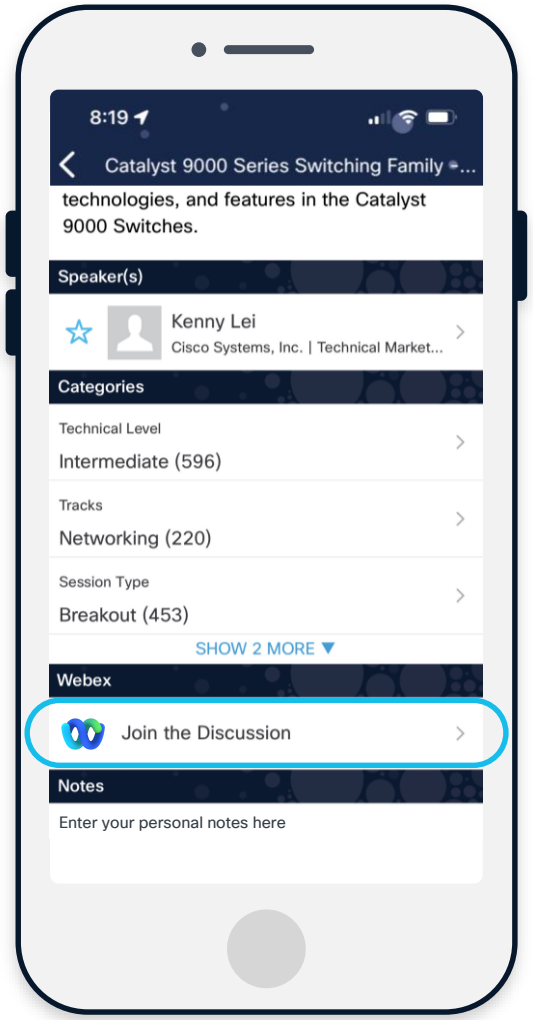
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKENS-1804**

About Us.. The SD-Access Dream Team

- **Origin Story**
  - 22 years of networking experience
  - From Network Ops, Design consulting, Pre-sales, and now Marketing
- **Common Things**
  - Passionate about SD-Access
  - CCIE
  - Loves to Travel
- **Uncommon Things**
  - Likes Scotch

- **Origin Story**
  - 19 years of networking experience
  - From Service Provider to Cisco TAC, and now Marketing
- **Common Things**
  - Passionate about SD-Access
  - CCIE
  - Loves to Travel ..but mostly carbs.
- **Uncommon Things**
  - Likes Beer

Why attend this session ?

"You've heard *why* SD-Access matters. Now see *how* it works"

Before We Begin – Session Guidelines

- **This Is a Demo-Driven Session**
  - **Quick** overview, then right into the deployment journey.
  - We dive straight into **hands-on configuration** using Catalyst Center, ISE, and network devices.
- **Assumed Knowledge**
  - We assume you're already familiar with:
    - Cisco SD-Access architecture & terminology
    - Basic LISP concepts and controller-based networking
- **Recommended Prerequisites:**
  - If you’re new to SD-Access, we highly suggest reviewing:
  - **BRKENS-2810:** SD-Access Fundamentals
  - **BRKENS-2811:** Policy and Segmentation
  - **BRKENS-2814:** Design Deep Dive
    (Available in the Cisco Live On-Demand Library)

Agenda

01 Part – 1

- Introduction
- Design Settings
- Catalyst Center to ISE Integration
- Underlay Automation
- Wired Steps
- Wireless Steps
- Policy

02 Part – 2

- LISP Extranet
- Dynamic Default Border
- Active & backup Internet
- Multiple Catalyst Center to ISE

For Your Reference

The PDF contains lot more information “For your Reference”

Cisco Live US SD-Access Fabric Learning Map

Sunday–8th

TECENS-2820 9:00AM
Cisco Software-Defined Access LISP: Architecture Overview

LTRENS-2509 9:00AM
Mastering Cisco SD-Access: LISP Pub/Sub and its Benefits Made Simple

TECENS-2850 2:00PM
Security in Enterprise - A cross-domain security primer across LAN, WLAN and WAN

Monday–9th

BRKENS-2810 10:00AM
Cisco Software-Defined Access LISP Solution Fundamentals

LTRENS-3751 1:00PM
SD-Access as Code with Cisco Catalyst Center and ISE Automation

IBOENS-1100 2:30PM
Cisco Catalyst Center and SD-Access Design Fundamentals

BRKENS-1804 3:30PM
The Power of Cisco SD-Access LISP Fabric: Simplified Deployment to Advanced Use Cases - Part 1

BRKENS-1851 4:00PM
Zero Trust: Secure the Workplace with Cisco Software-Defined Access

Tuesday–10th

BRKENS-1805 11:00AM
SD-Access in Action: Trusted Outcomes Across Education and Finance- Featuring UC Riverside & CIBC Bank

BRKENS-2824 2:00PM
Deploying Your First Cisco SD-Access Project

BRKENS-2804 4:00PM
The Power of Cisco SD-Access LISP Fabric: Simplified Deployment to Advanced Use Cases - Part 2

IBOENS-2828 4:30PM
Network Quest: Exploring Campus Fabrics and Secure Segmentation

Wednesday–11th

BRKENS-2816 10:30AM
Cisco SD-Access Transit: Advanced Design Principles

IBOENS-2826 10:30AM
Cisco SD-Access Design and Deployment Best Practices

BRKENS-2836 10:30AM
Endpoint profiling and segmentation using AI endpoint Analytics and Cyber Vision for next generation SD Access manufacturing plants

BRKENS-1806 1:00PM
Transforming Enterprise Networks with Cisco SD-Access: Real-World Strategies from CDW

BRKENS-3826 3:30PM
Advanced LISP SD-Access Forwarding Architecture

Thursday–12th

BRKENS-2650 8:30AM
Designing and Deploying Cisco SD-Access with BGP EVPN

BRKENS-2700 8:30AM
Fabric Networking in the Campus: What's the fuss and what are the choices?

BRKENS-3834 10:30AM
1 to 100: Master All Steps of Automated and Seamless Deployment, Integration, and Migration of Large SDA and SD-WAN Networks

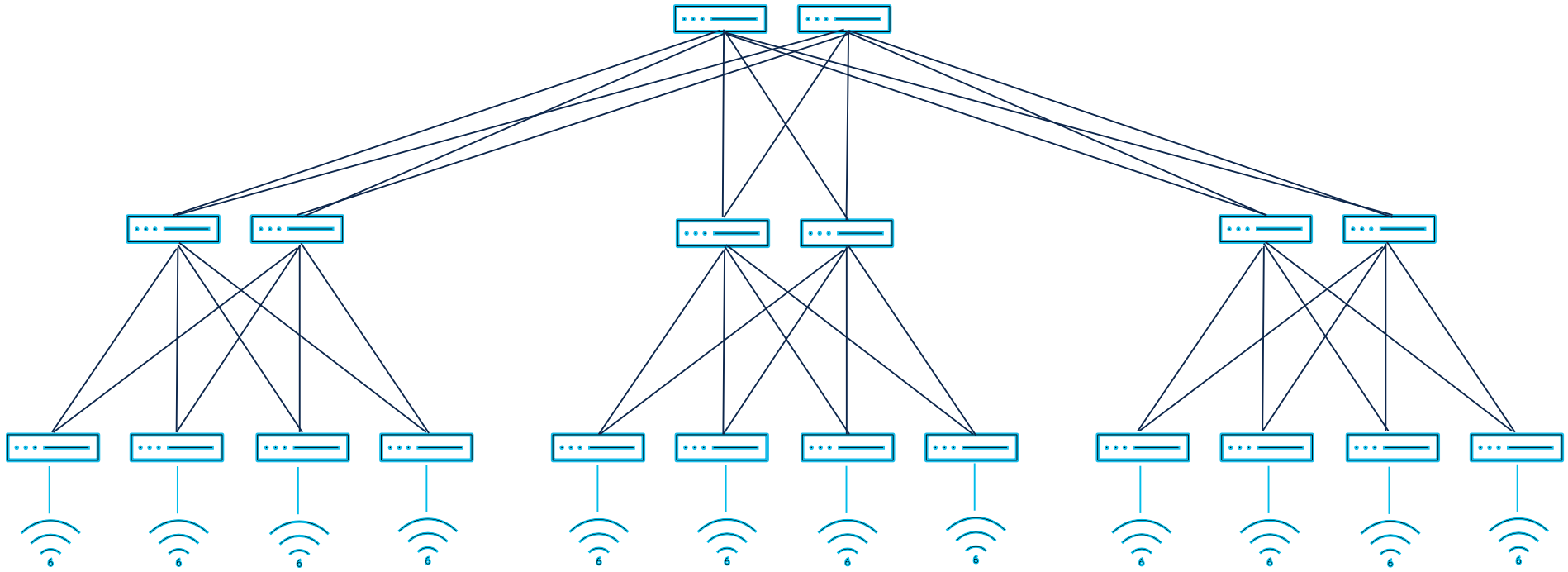
BRKENS-3810 2:30PM
How to Adopt Zero Trust using SD-Access and Default-Deny without Tears

BU-led sessions

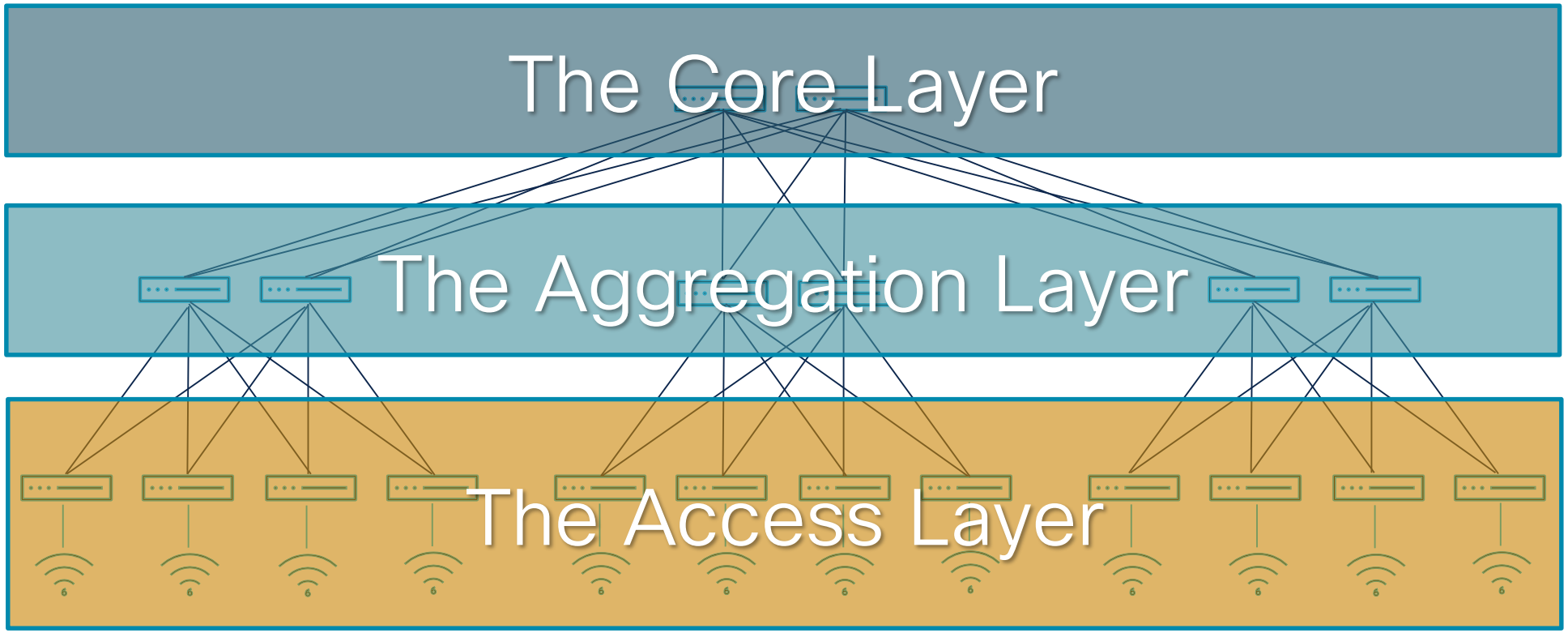
Software Defined Access Introduction

Network *Simplification*

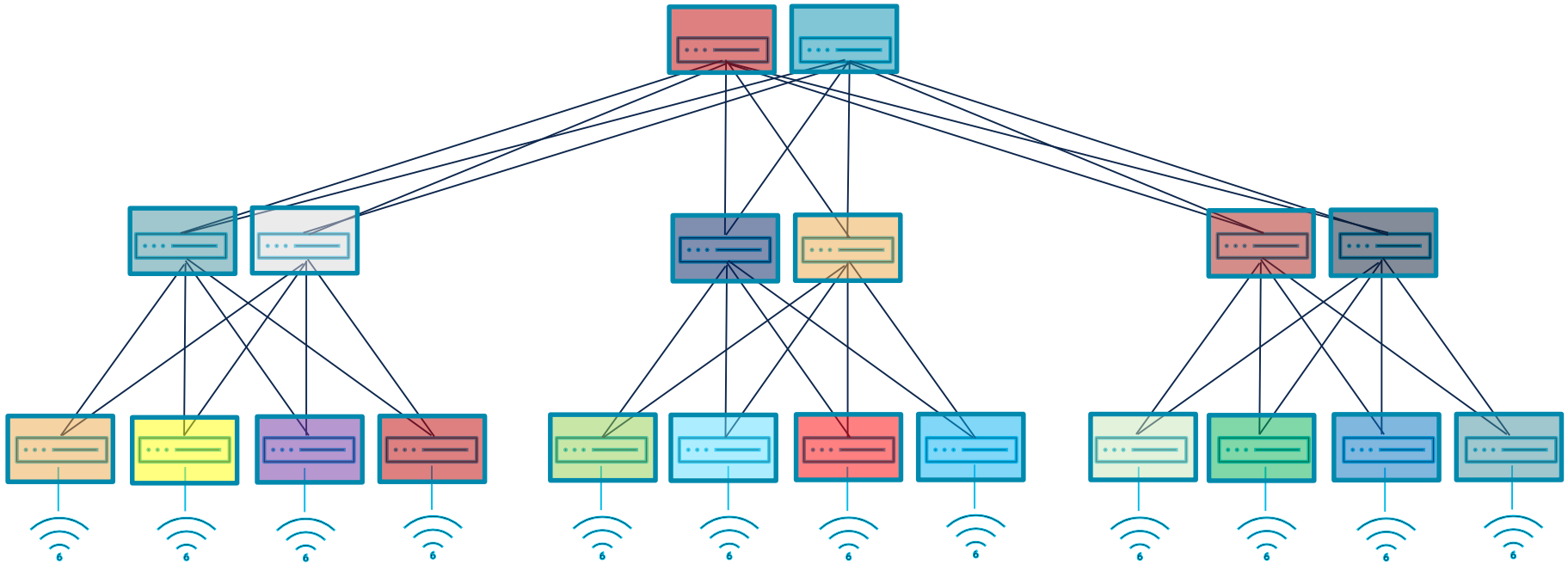
The Traditional Enterprise Network



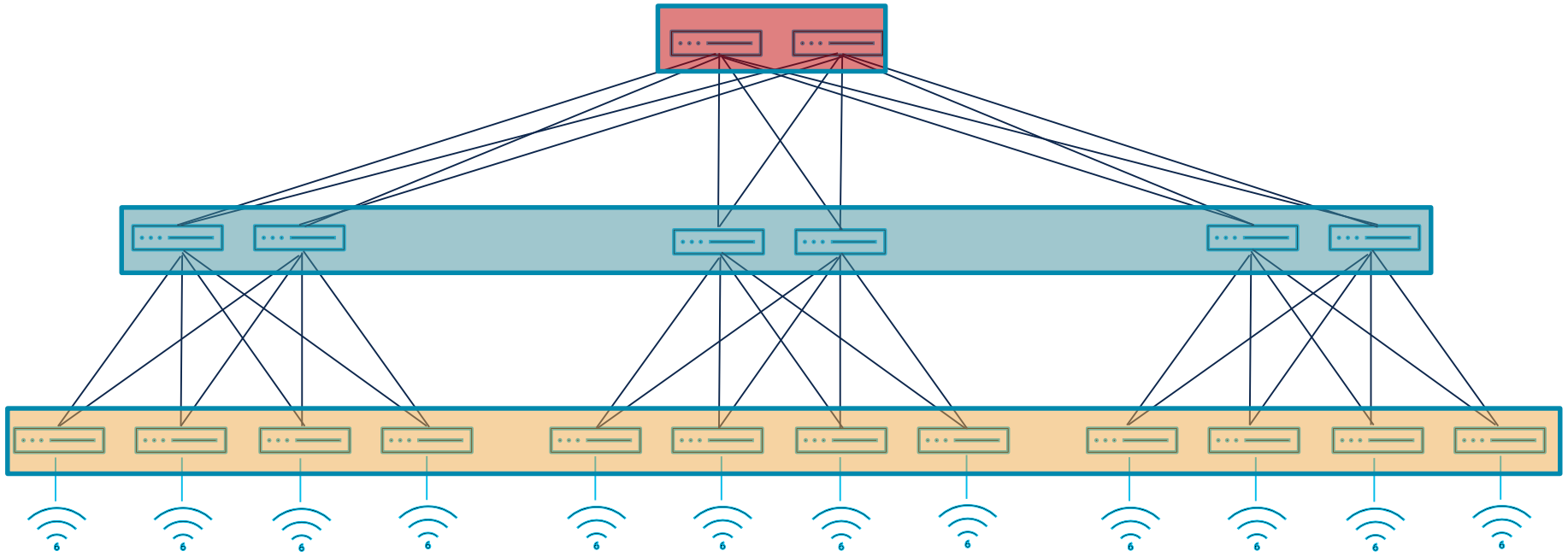
The Traditional Enterprise Network



Unique Configurations drive up complexity



Common Configurations with SD-Access



Zero Trust for Network Infrastructure

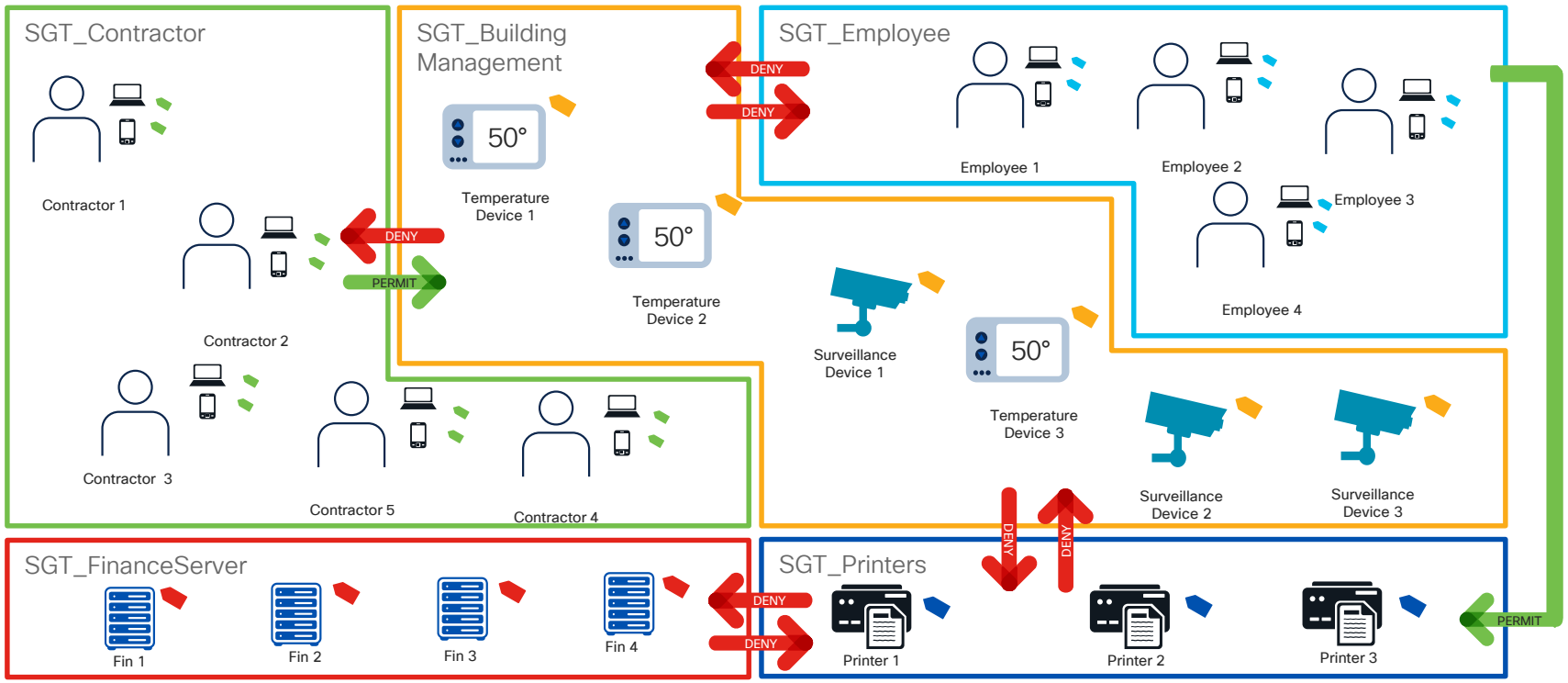
Can you see the business intent here?

```
access-list 102 permit tcp 131.249.33.123 0.0.0.127 lt 4765 71.219.207.89 0.255.255.255 eq 606
access-list 102 deny tcp 112.174.162.193 0.255.255.255 gt 368 4.151.192.136 0.0.0.255 gt 4005
access-list 102 permit ip 189.71.213.162 0.0.0.127 gt 2282 74.67.181.47 0.0.0.127 eq 199
access-list 102 deny udp 130.237.66.56 255.255.255.255 lt 3943 141.68.48.108 0.0.0.255 gt 3782
access-list 102 deny ip 193.250.210.122 0.0.1.255 lt 2297 130.113.139.130 0.255.255.255 gt 526
access-list 102 permit ip 178.97.113.59 255.255.255.255 gt 178 111.184.163.103 255.255.255.255 gt 959
access-list 102 deny ip 164.149.136.73 0.0.0.127 gt 1624 163.41.181.145 0.0.0.255 eq 810
access-list 102 permit icmp 207.221.157.104 0.0.0.255 eq 1979 99.78.135.112 0.255.255.255 gt 3231
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt 1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt 2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq 1479
access-list 102 permit ip 209.111.254.187 0.0.1.255 gt 4640 93.99.173.34 255.255.255.255 gt 28
access-list 102 permit ip 184.232.88.41 0.0.31.255 lt 2247 186.33.104.31 255.255.255.255 lt 4481
access-list 102 deny ip 106.79.247.50 0.0.31.255 gt 1441 96.62.207.209 0.0.0.255 gt 631
access-list 102 permit ip 39.136.60.170 0.0.1.255 eq 4647 96.129.185.116 255.255.255.255 lt 3663
access-list 102 permit tcp 30.175.189.93 0.0.31.255 gt 228 48.33.30.91 0.0.0.255 gt 1388
access-list 102 permit ip 167.100.52.185 0.0.1.255 lt 4379 254.202.200.26 255.255.255.255 gt 4652
access-list 102 permit udp 172.16.184.148 0.255.255.255 gt 4163 124.38.159.247 0.0.0.127 lt 3851
access-list 102 deny icmp 206.107.73.252 0.255.255.255 lt 2465 171.213.183.230 0.0.31.255 gt 1392
access-list 102 permit ip 96.174.38.79 0.255.255.255 eq 1917 1.156.181.180 0.0.31.255 eq 1861
access-list 102 deny icmp 236.123.67.53 0.0.31.255 gt 1181 31.115.75.19 0.0.1.255 gt 2794
access-list 102 deny udp 14.45.208.20 0.0.0.255 lt 419 161.24.159.166 0.0.0.255 lt 2748
access-list 102 permit udp 252.40.175.155 0.0.31.255 lt 4548 87.112.10.20 0.0.1.255 gt 356
access-list 102 deny tcp 124.102.192.59 0.0.0.255 eq 2169 153.233.253.100 0.255.255.255 gt 327
access-list 102 permit icmp 68.14.62.179 255.255.255.255 lt 2985 235.228.242.243 255.255.255.255 lt 2286
access-list 102 deny tcp 91.198.213.34 0.0.0.255 eq 1274 206.136.32.135 0.255.255.255 eq 4191
access-list 102 deny udp 76.150.135.234 255.255.255.255 lt 3573 15.233.106.211 255.255.255.255 eq 3721
access-list 102 permit tcp 126.97.113.32 0.0.1.255 eq 4644 2.216.105.40 0.0.31.255 eq 3716
access-list 102 permit icmp 147.31.93.130 0.0.0.255 gt 968 154.44.194.206 255.255.255.255 eq 4533
access-list 102 deny tcp 154.57.128.91 0.0.0.255 lt 1290 106.233.205.111 0.0.31.255 gt 539
access-list 102 deny ip 9.148.176.48 0.0.1.255 eq 1310 64.61.88.73 0.0.1.255 lt 4570
```

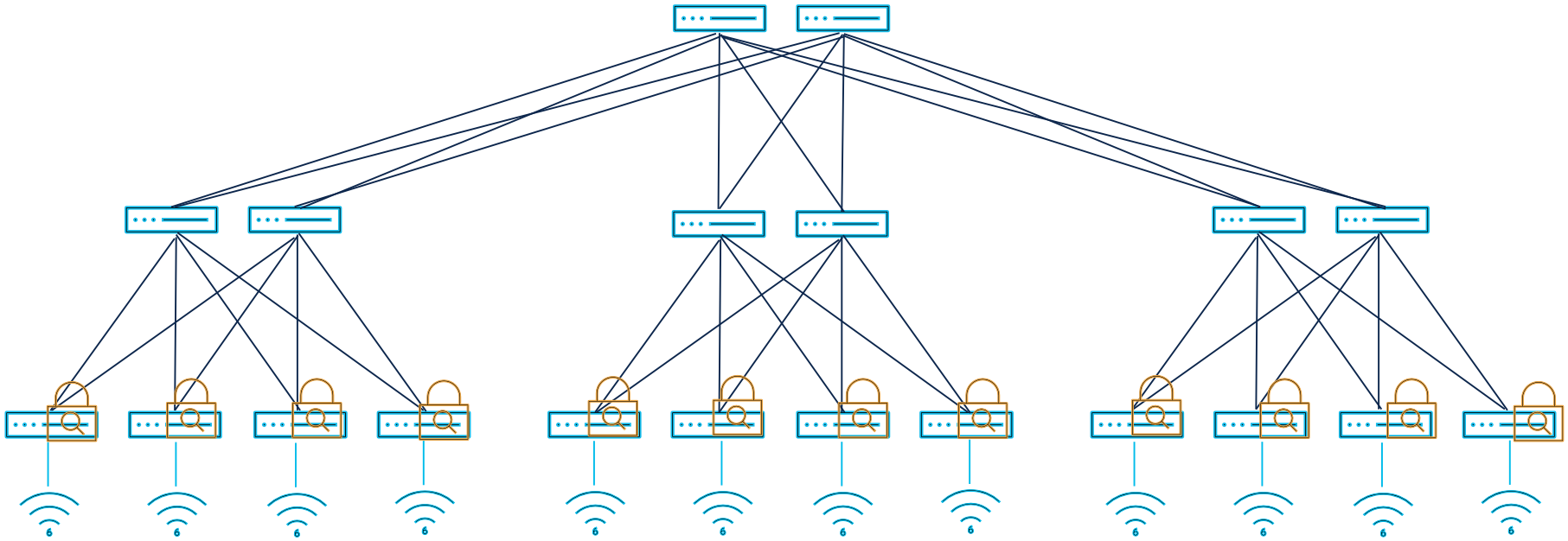
Can you spot the business intent here?

```
DMZ-Pod1#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 4:Employees to group 12:Development_Servers:
        Deny IP-00
IPv4 Role-based permissions from group 8:Developers to group 12:Development_Servers:
        Permit IP-00
```

Better Visibility leads to better Segmentation

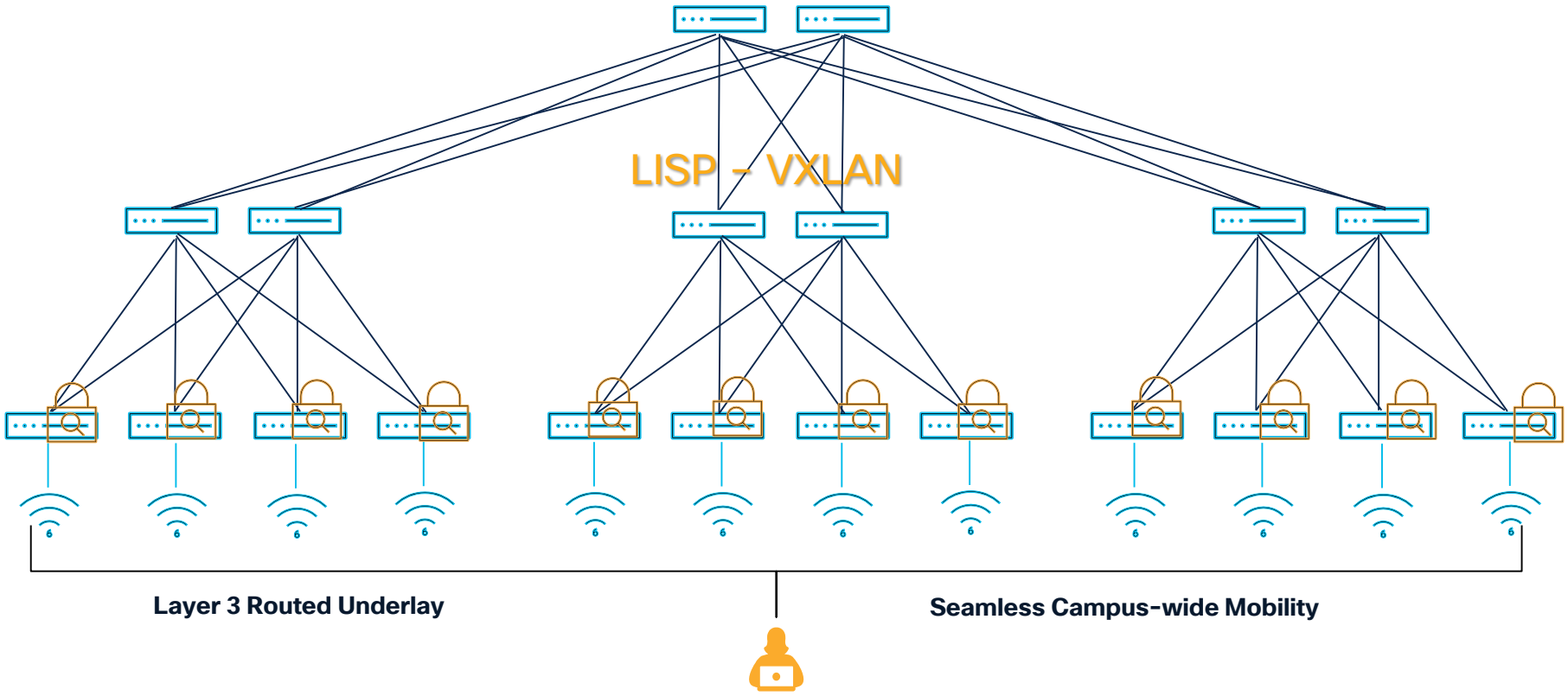


Fabric Architecture: Enabling Powerful Outcomes



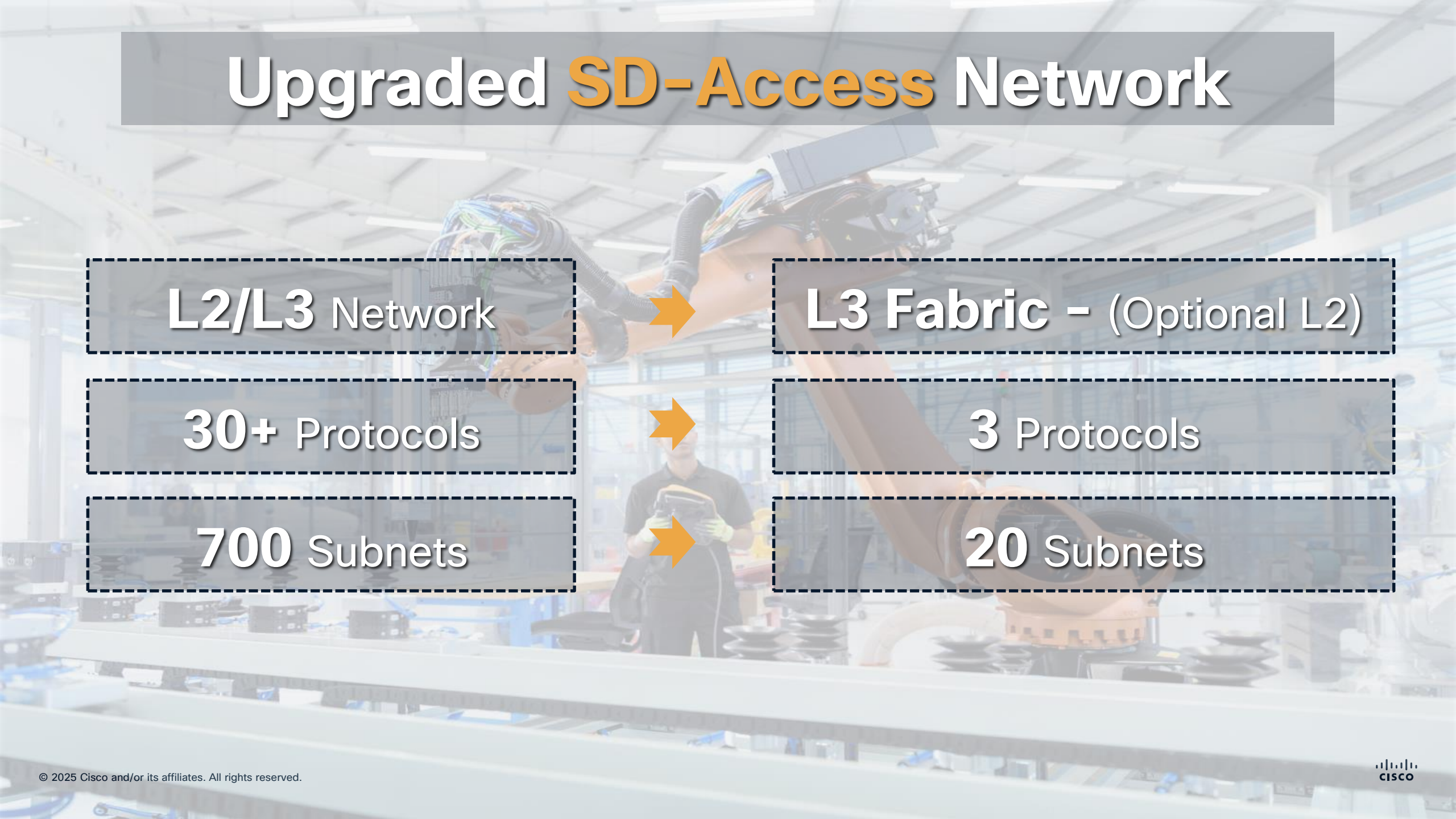
In **SD-Access, ISE** is used to **Authenticate/Authorize** the onboarding of Users in a **Fabric**
(and Devices and IOT based Things)

Fabric Architecture: Enabling Powerful Outcomes



Unified Wired/Wireless Management and Policy

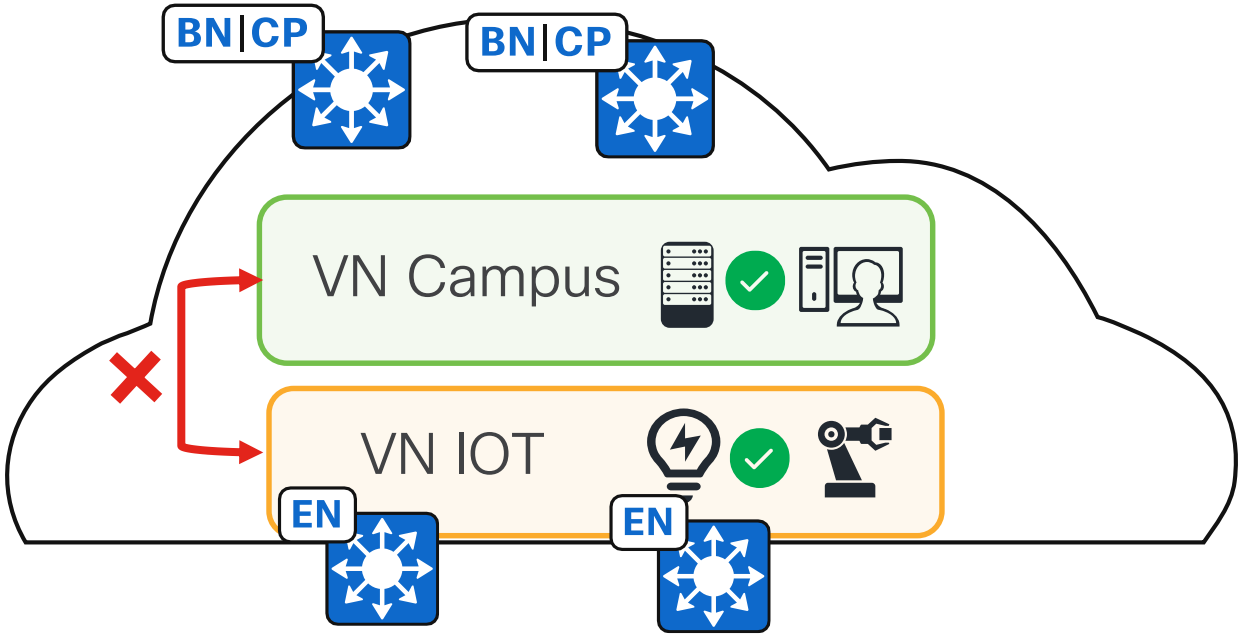
Upgraded SD-Access Network



L2/L3 Network	→	**L3 Fabric –** (Optional L2)
30+ Protocols	→	**3** Protocols
700 Subnets	→	**20** Subnets

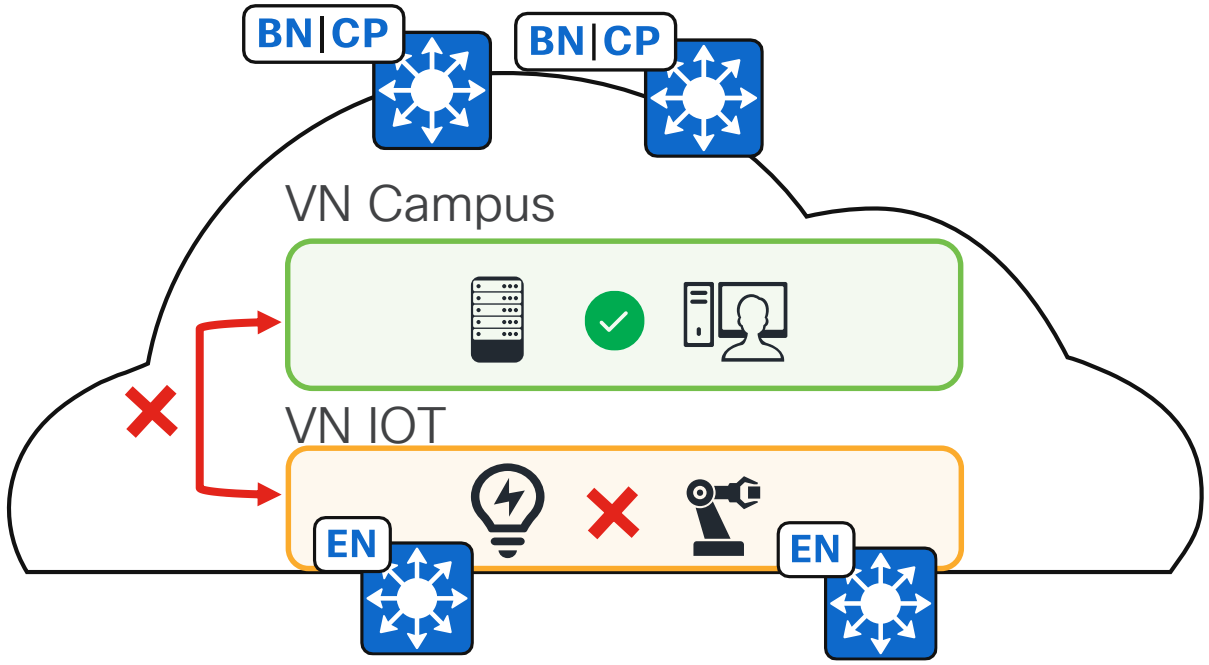
Segmentation with LISP SD-Access

Macro-Segmentation (VN) and Micro-segmentation (SGT)



Virtual Network (VN)

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

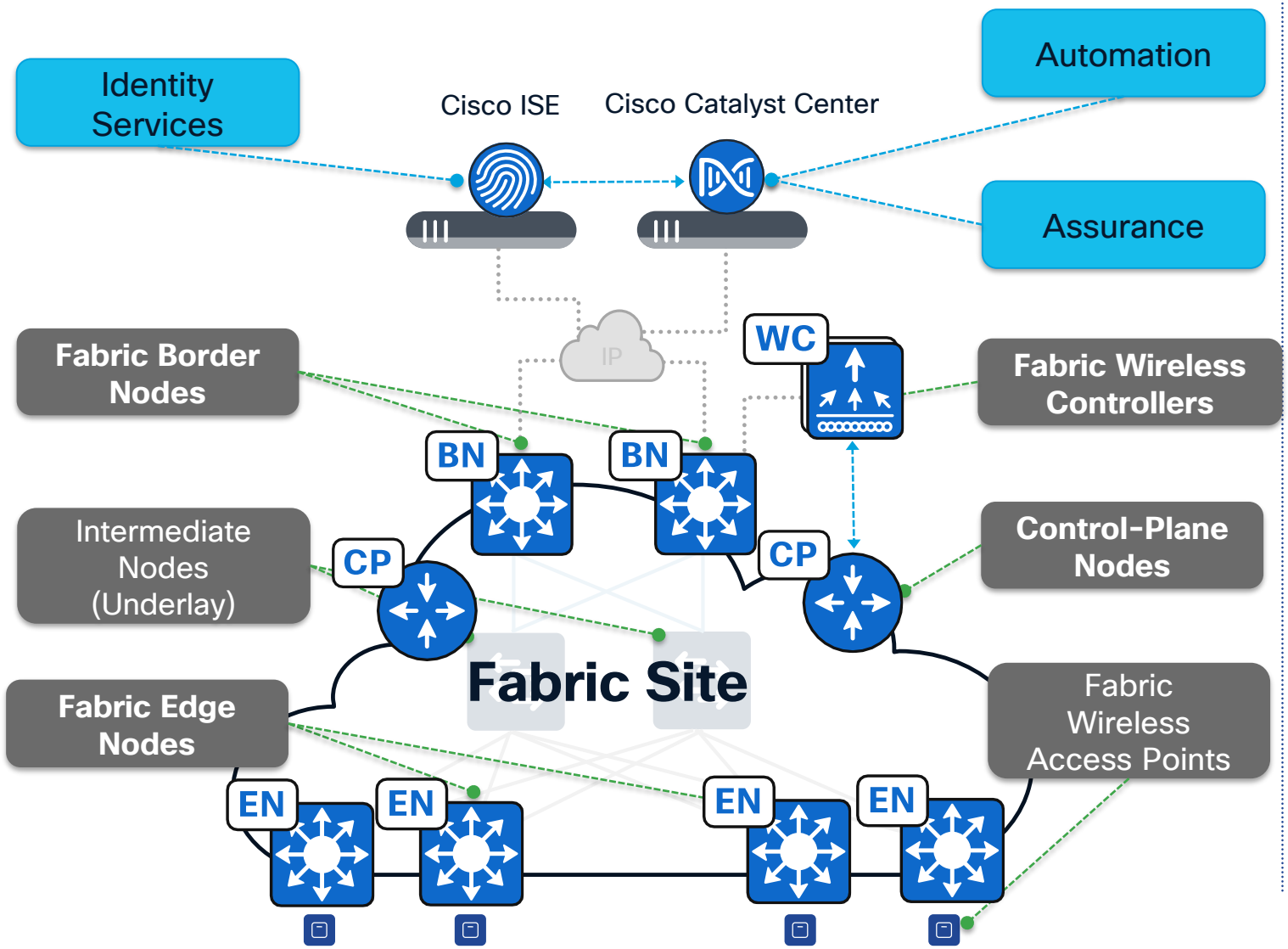


Security Group Tag (SGT)

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.

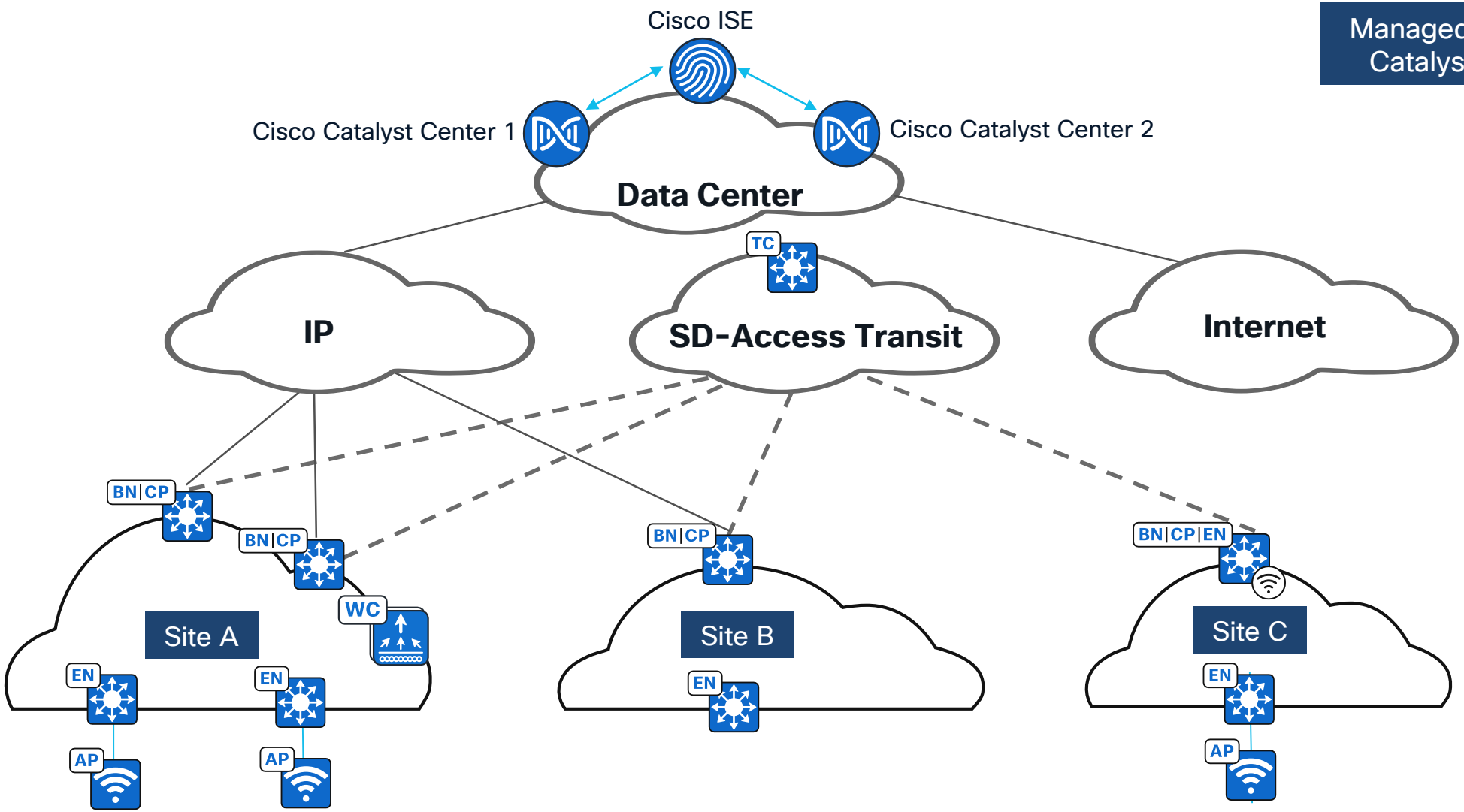
Fabric roles & terminology

For Your Reference

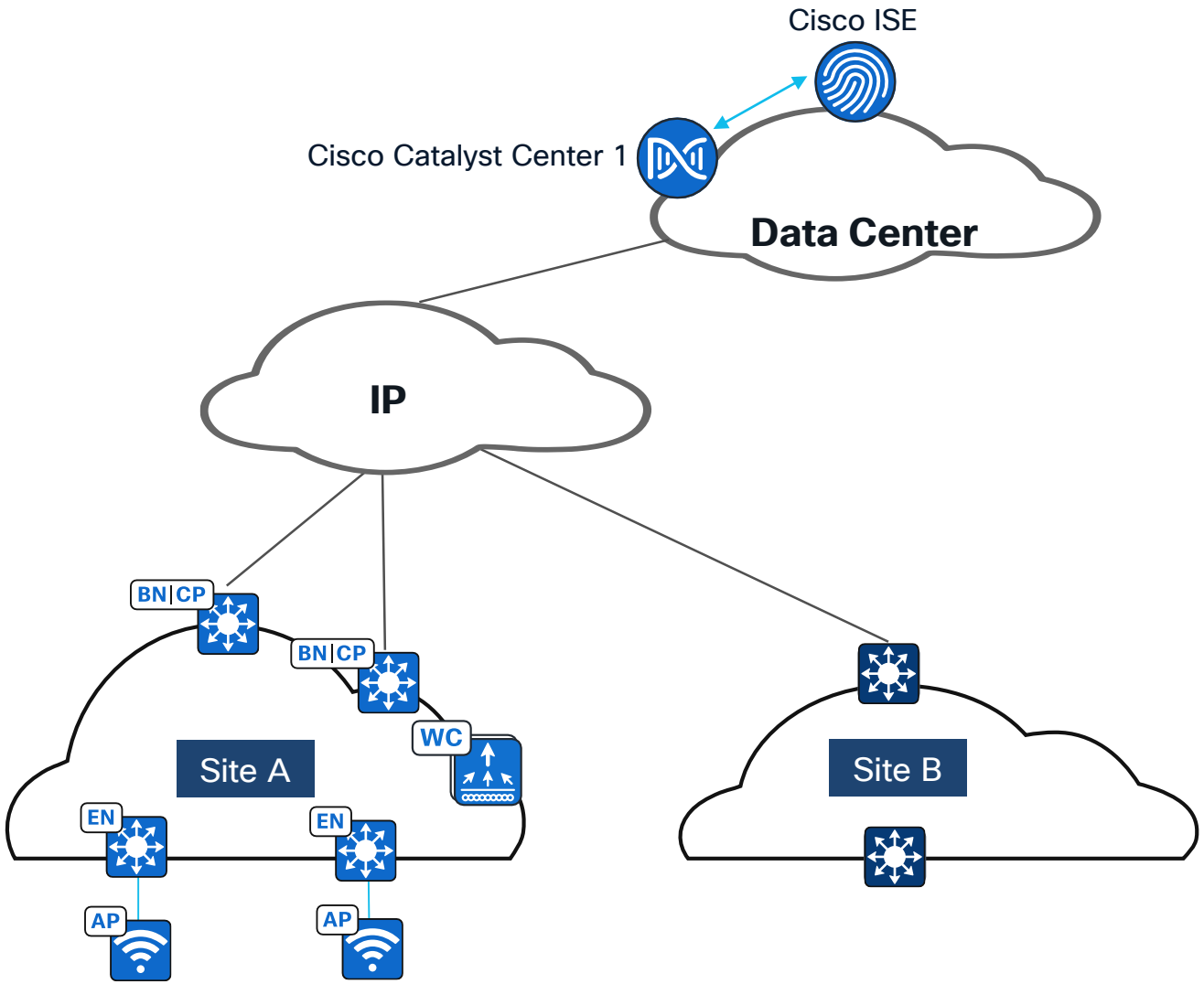


- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric device status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition

Two Sessions, One Map



Managed by Multiple Cisco Catalyst Center Solution



Topology for this session

Cisco Catalyst Center “Design Your Network” Settings

Why It Matters:

- **Operational Efficiency**: Reduces complexity and operational overhead.
- **Scalability**: Supports large-scale deployments with consistent configurations.

Key Benefits:

- Simplified Network Design
- Centralized Global Settings
- Image Management
- Enhanced Security and Policy Integration
- Wireless Optimization
- Templates

Cisco Catalyst Center “Design Your Network” Settings

For Your Reference

Why It Matters:

- **Operational Efficiency**: Reduces complexity and operational overhead.
- **Scalability**: Supports large-scale deployments with consistent configurations.

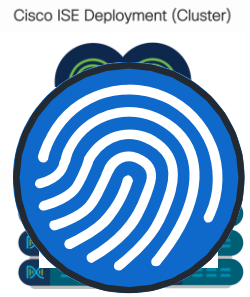
Key Benefits:

- **Simplified Network Design**:
  - Create structured network hierarchies (areas, buildings, floors) for better organization.
- **Centralized Global Settings**:
  - Configure AAA, DHCP, NTP, and security settings globally or customize them at the site level .
- **Image Management**:
  - Automate device management and provisioning with "golden images" for consistent configurations
- **Enhanced Security and Policy Integration**:
  - Translate business intent into network policies and integrate with Cisco Identity Services Engine (ISE) for zero-trust security
- **Wireless Optimization**:
  - Manage wireless settings globally such as SSIDs,RF,AP Profiles etc..
- **Templates**:
  - Use CLI and Feature templates for various use cases

Cisco Catalyst Center Design Settings Demonstration

Cisco Catalyst Center to ISE Integration

Cisco ISE Use Cases in SD-Access



Cisco ISE

Cisco Catalyst Center Cluster

Guest Access
Guest network automation

Host On-boarding
User authentication

Group Based Policies
SDA Segmentation

Assurance
Client 360

Multiple Cisco Catalyst Center
Shared Transit + Extranet

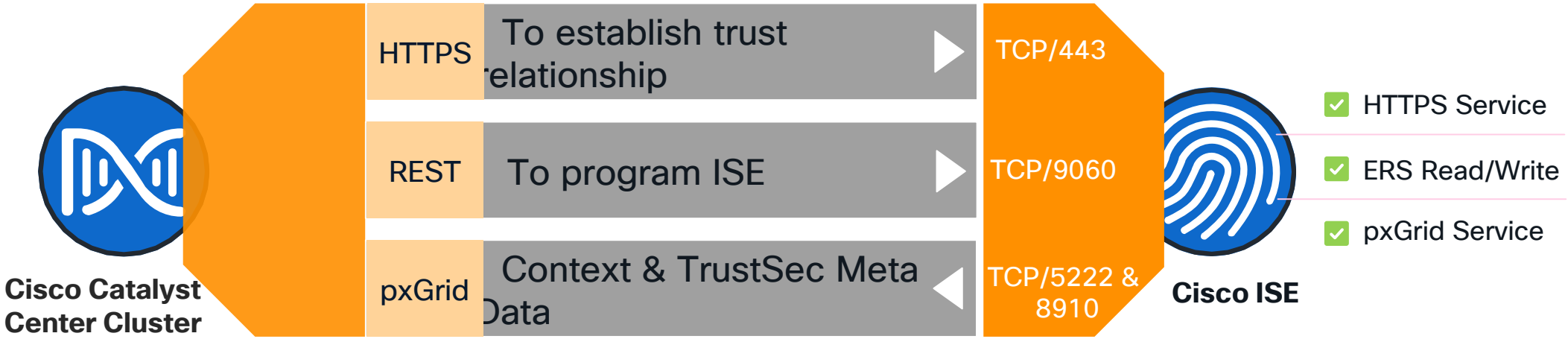
Device Administration
TACACS

Asset Visibility
Everything & Everyone on Network

Policy Analytics
Group to Group Interaction with automated policy

Security Ecosystem Integration
Context Sharing

Cisco Catalyst Center & ISE Communication



Cisco ISE: Enable below ISE Services

Administration > System >Deployment > Select ISE Host Name

Enable pxGrid Services

Administration > Settings > ERS Settings

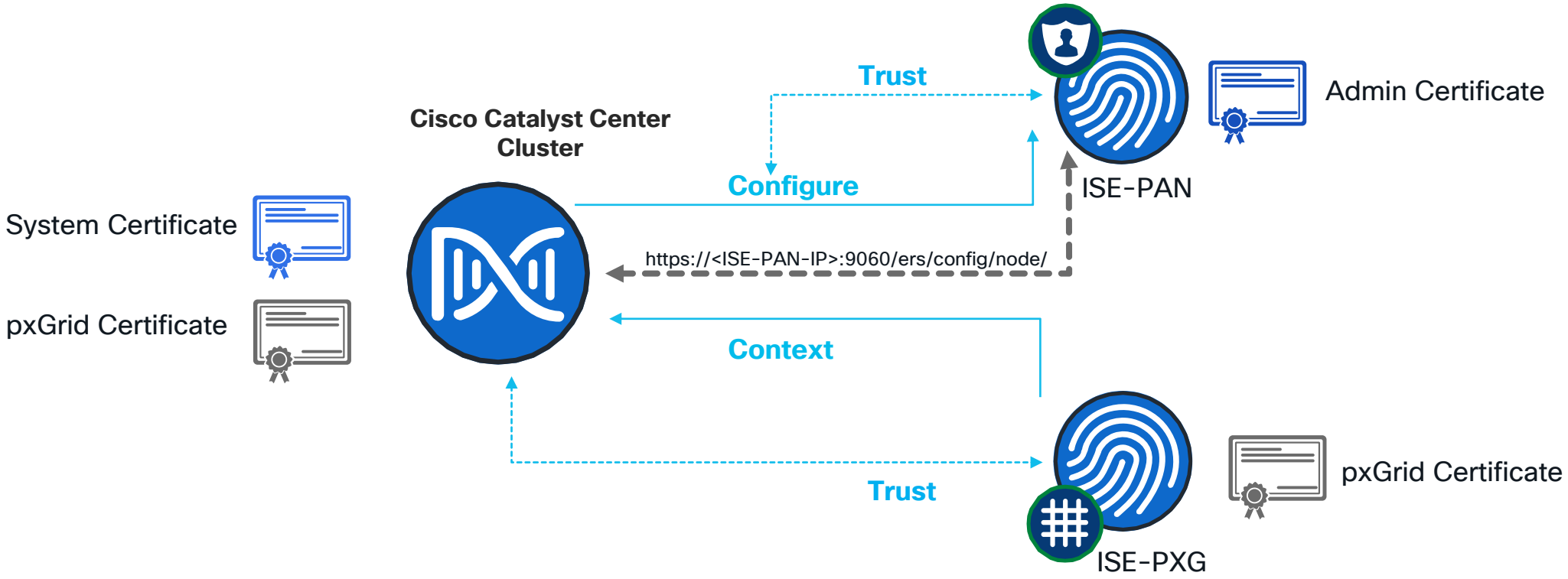
Enable *ERS for Read/Write* ***on PAN***

Enable *ERS for Read on* ***All other Nodes*** *incase of Distributed model*

Cisco Catalyst Center and ISE Integration

For Your Reference

How Catalyst Center Trust PxGrid Node



Cisco Catalyst Center Policy Overview

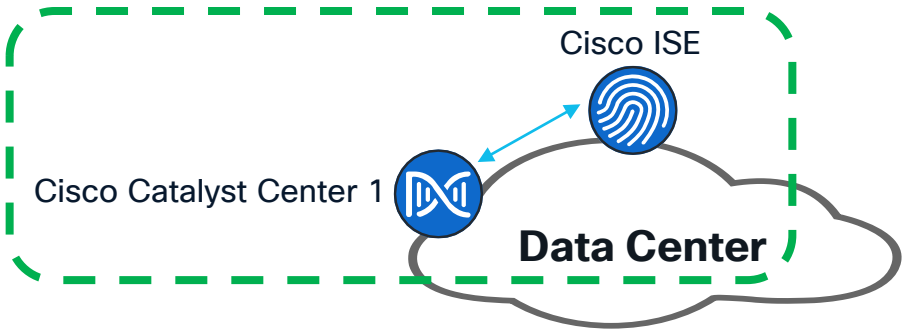
Policy Management

Policy Management on Cisco Catalyst Center

- **Policy Creation on Cisco Catalyst Center with ISE Read Only**
  - Security Groups(SGT)
  - Access Contract (SGACL)
  - Group-based Access Control Policy(TrustSec Policy)
- No Multi Matrices support on Cisco Catalyst Center
- Default Deny or Default Permit for all Sites
- Single SGACL association to GBP policy allowed

Policy Management on Cisco ISE

- **Policy Creation on Cisco ISE with Catalyst Center Read Only***
  - Security Groups(SGT)
  - Security Group ACL (SGACL)
  - TrustSec Policy
- **Multi Matrices support on Cisco ISE**
- Default Deny or Default Permit can be site specific with the use of Multi Matrix on ISE
- **Multi SGACL association to TrustSec policy allowed**

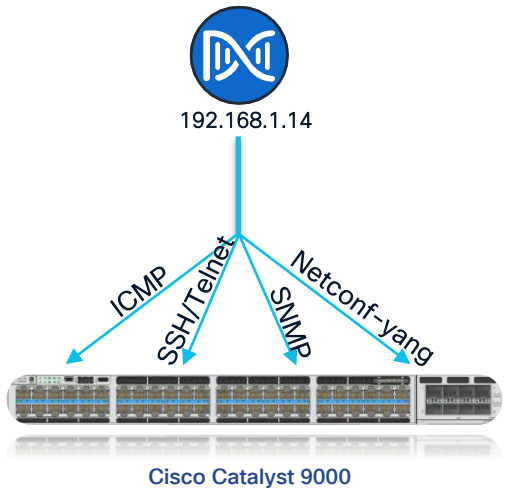


Lan Automation

Cisco Catalyst Center

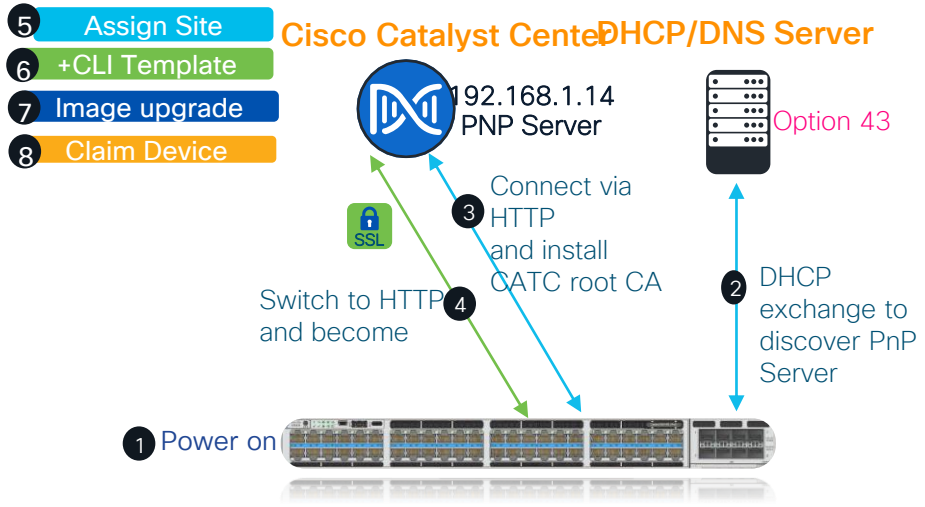
Device Onboarding options

Manual Discovery



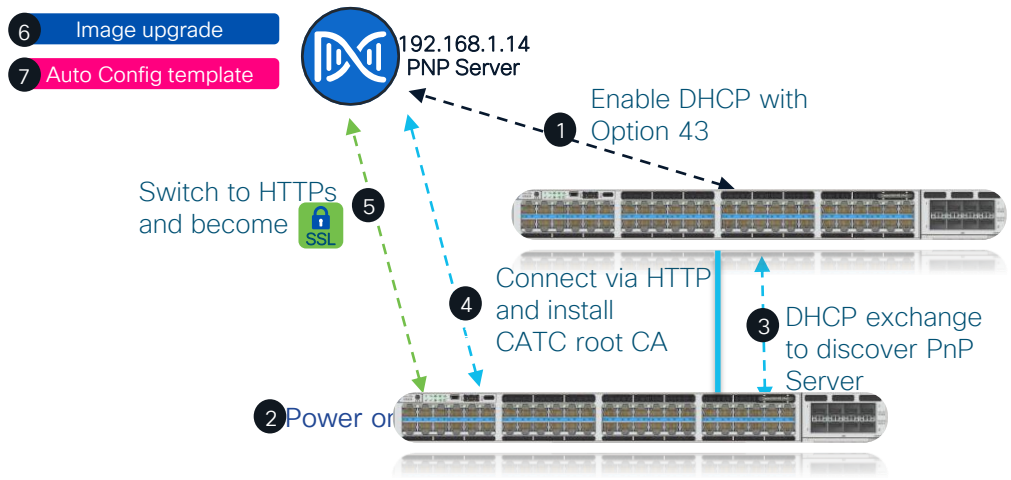
Device-by-Device onboarding with Manual configuration & Auto Image upgrade

Semi-Automated Discov



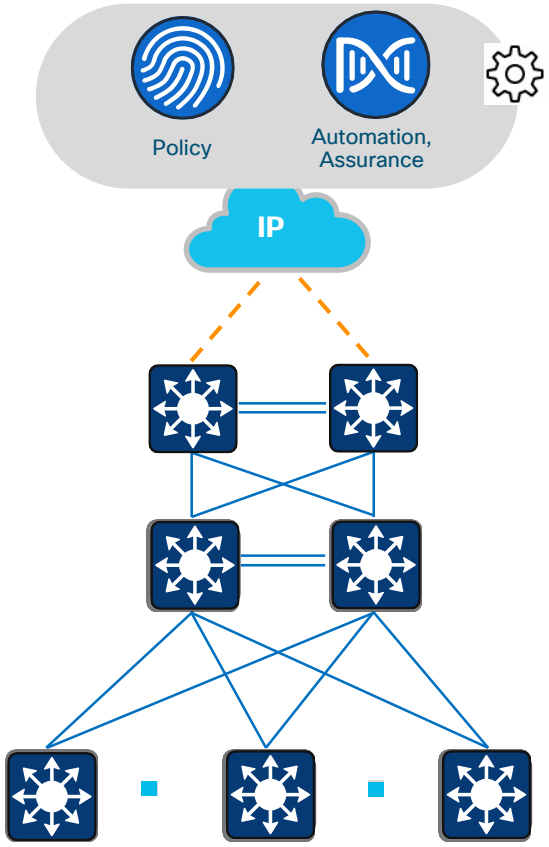
Device-by-Device onboarding with Cisco Plug and Play

Lan Automated Discov



Turnkey solution to onboard multiple switches with image management and best-practices configuration.
Underlay multicast to optimize overlay subnet multicast/broadcast distribution

What is Lan Automation?



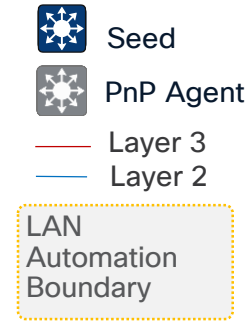
Traditional Networks

Lan Automation

- Simplifies network operations
- Frees IT staff from time-consuming, repetitive network configuration tasks
- Creates a standard, error-free underlay network

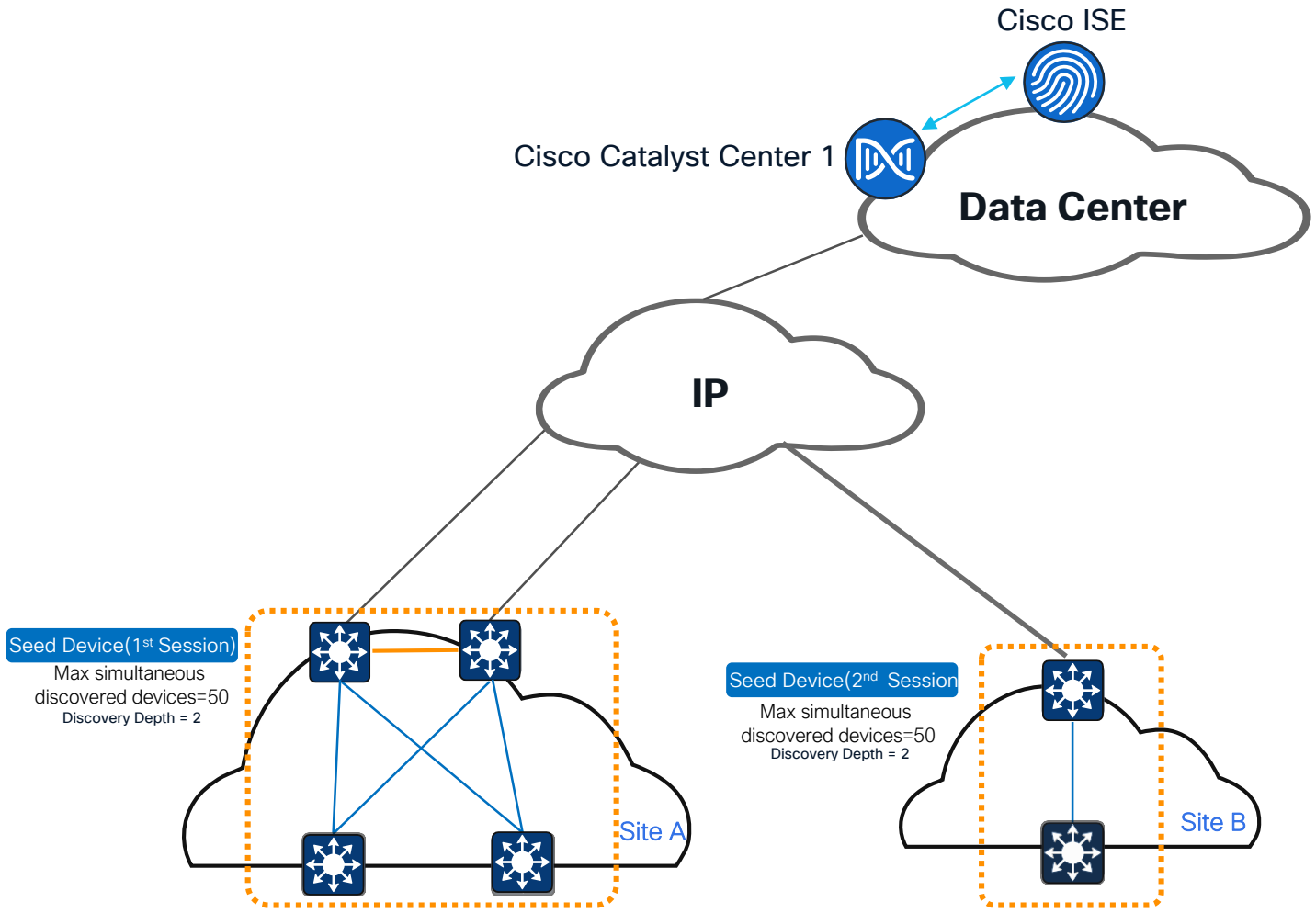
Lan Automation Benefits

- Zero-touch provisioning
- End-to-end topology
- Resilience
- Security
- Compliance



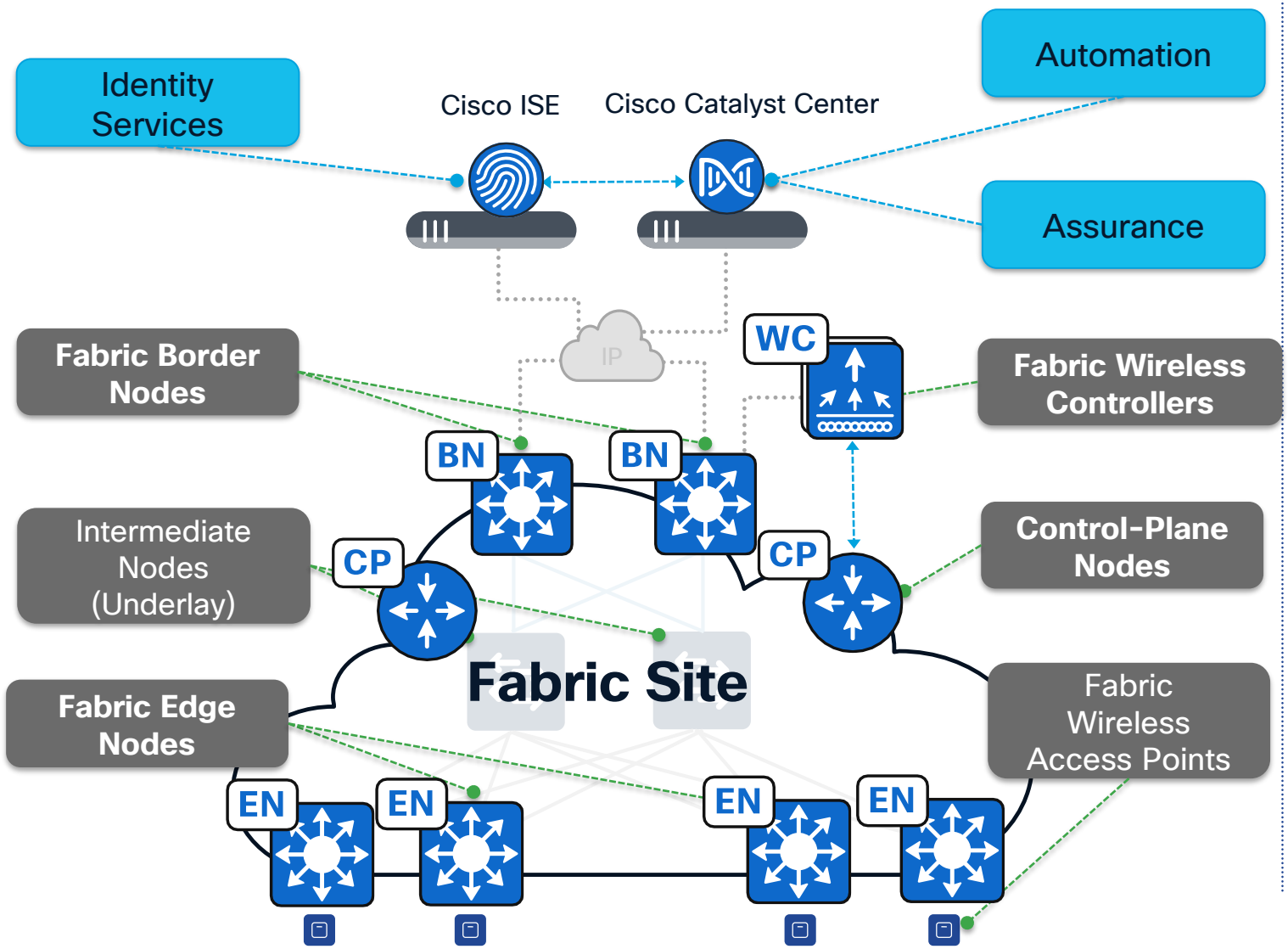
[Cisco SD-Access Zero-Touch Provisioning Using LAN Automation - BRKENS-2800]

Demo Topology



Cisco SD-Access Wired Fabric

Fabric roles & terminology

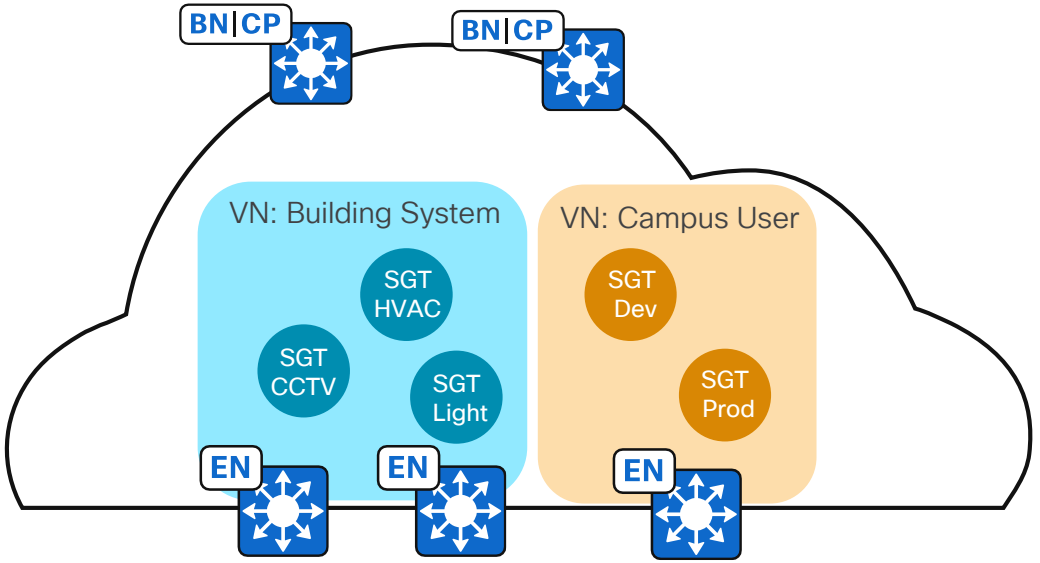


- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric device status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

Segmentation with LISP SD-Access

Segmentation within SD-Access can be achieved with the use of:

- Virtual Networks, referred to as **Macro-segmentation**.
- Cisco Group-Based Policy Security Group Tags (SGTs), referred to as **Micro–segmentation.**



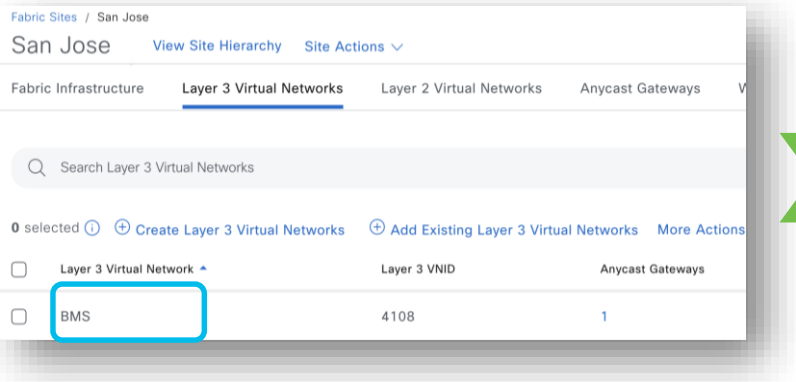
Micro-segmentation requires ISE to be part of the SD-Access solution. Macro–segmentation does not.

Macro-segmentation

Macro Segmentation logically separates a network topology into smaller virtual networks, using a unique network identifier and separate forwarding tables.

This is instantiated as Virtual Routing and Forwarding (VRF) instance on switches or routers and referred to as a Virtual network (VN) on Cisco Catalyst Center.

VN on Catalyst Center



VRF on the Device

```
sjc-e1#sh vrf
  Name Default RD  Protocols  Interfaces
  BMS   1:4108     ipv4       Vl3200
                              Lo0.4108
```

LISP Instance ID

```
instance-id 4108
 remote-rloc-probe on-route-change
 dynamic-eid BMS-IPV4
  database-mapping 9.1.1.0/24 locator-set rloc_<snip>
  exit-dynamic-eid
 !
 service ipv4
  eid-table vrf BMS
  <snip>
  exit-service-ipv4
 !
 exit-instance-id
!
instance-id 8195
 remote-rloc-probe on-route-change
 service ethernet
  eid-table vlan 3200
  database-mapping mac locator-set rloc_<snip>
  exit-service-ethernet
 !
```

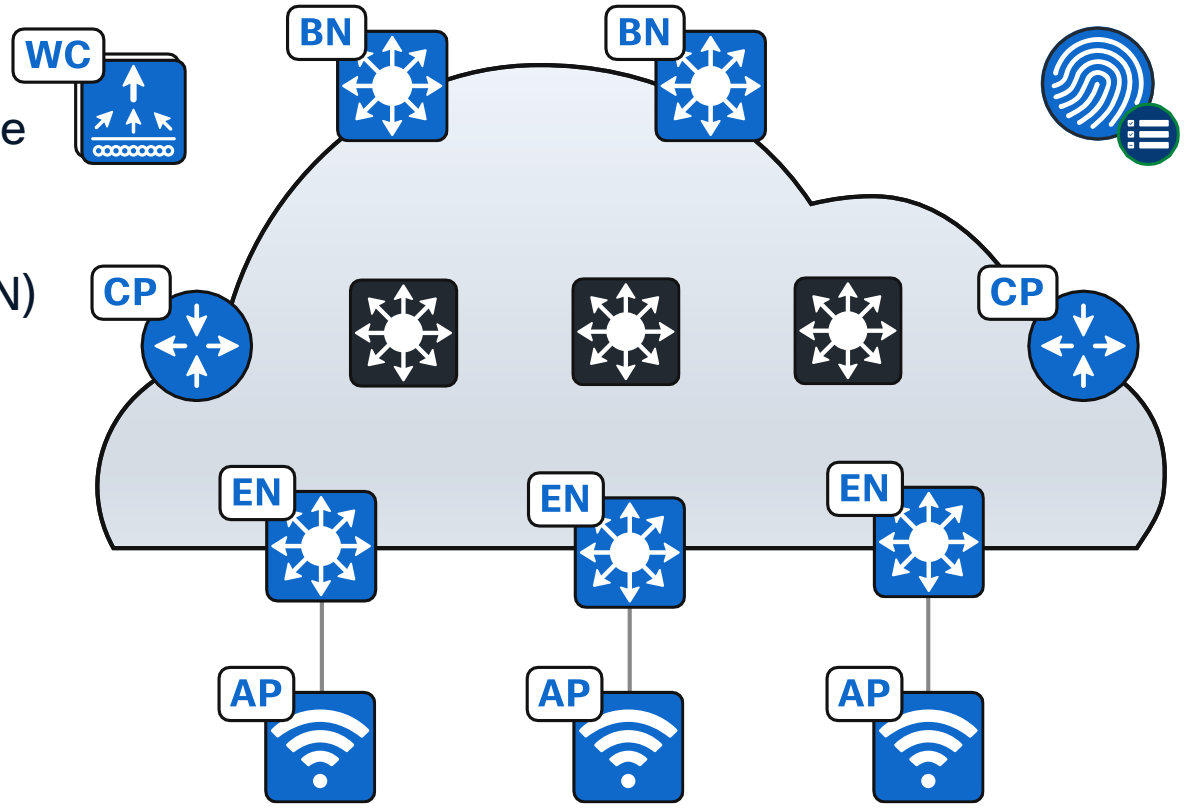
Fabric Constructs

Fabric Sites – A Closer Look

For Your Reference

Fabric Sites are an independent fabric area with a unique set of network device.

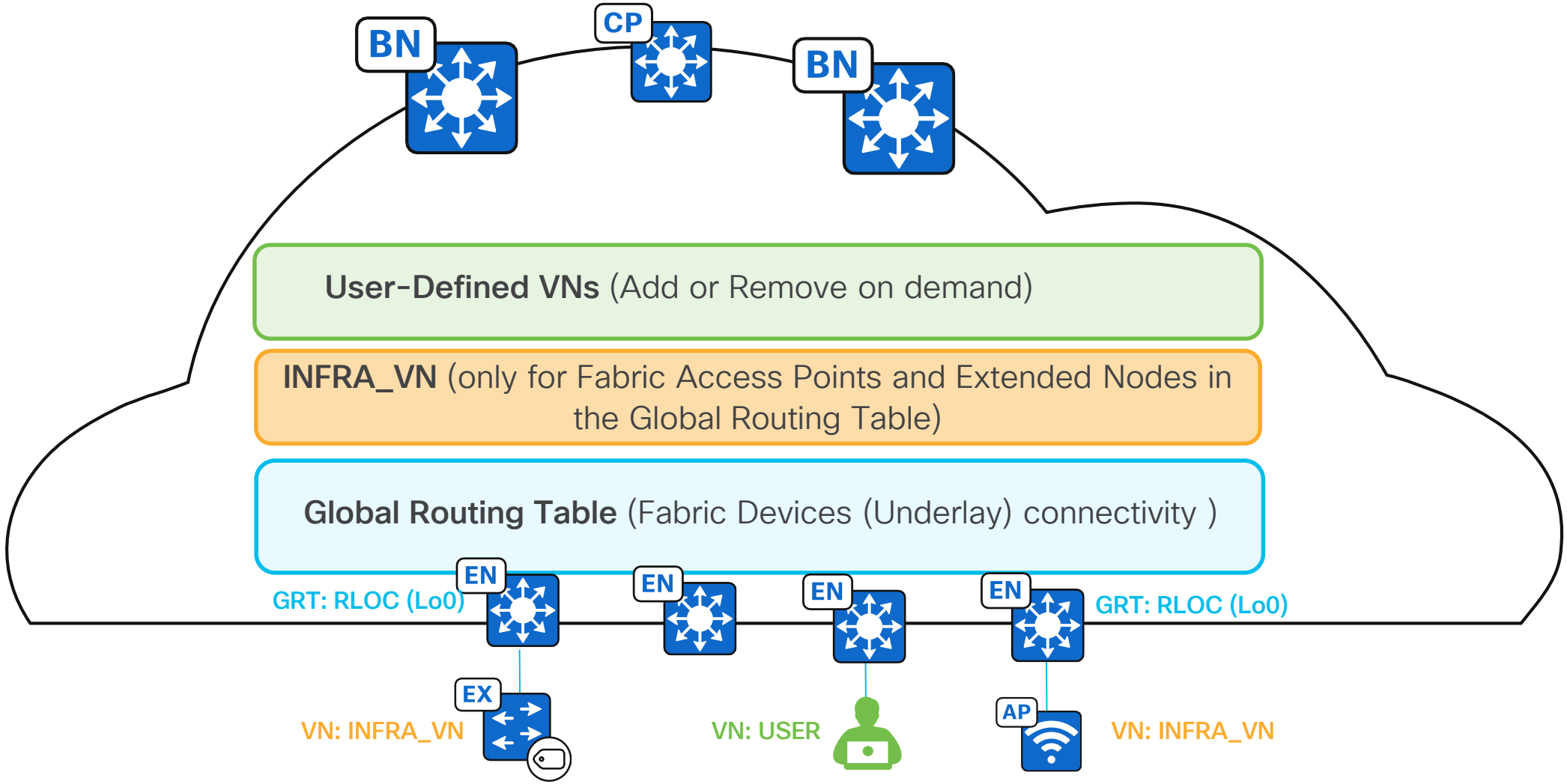
- Contains Control Plane Nodes, Border Nodes, and Edge Nodes.
- Contains Fabric WLC and ISE Policy Service Node (PSN)
- The Border Node is the ingress and egress for the Fabric Site.
- May cover a single location, multiple locations, or a subset of a location (floor of a building)



Cisco SD-Access Fabric

For Your Reference

Layer 3 Virtual Networks

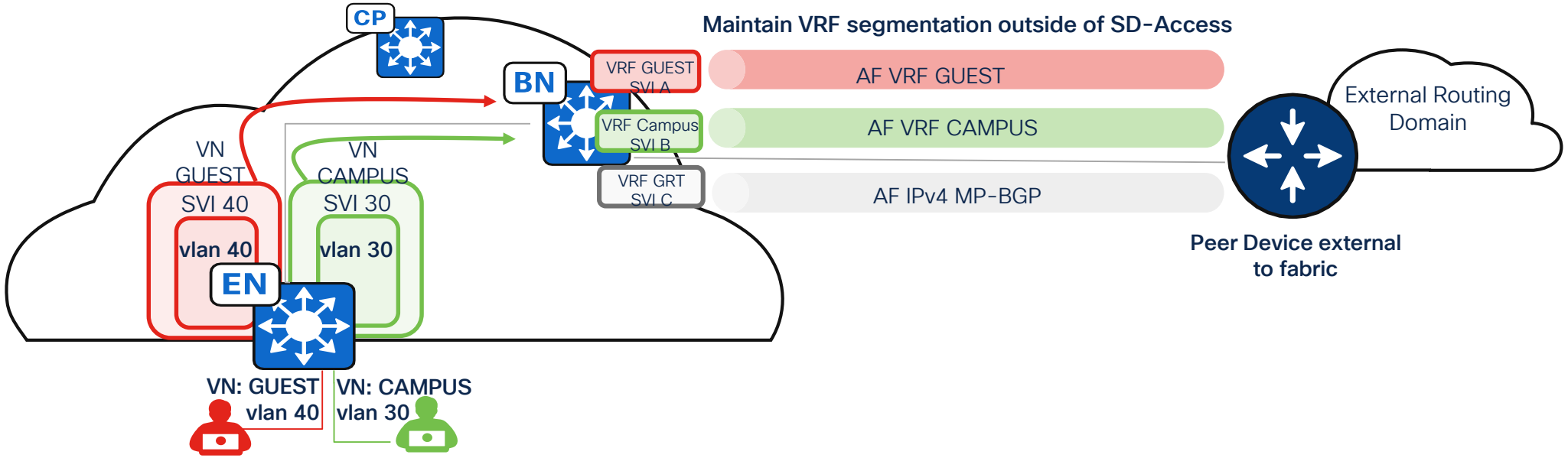


Cisco SD-Access Fabric

For Your Reference

Layer 3 Virtual Networks Handoff

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

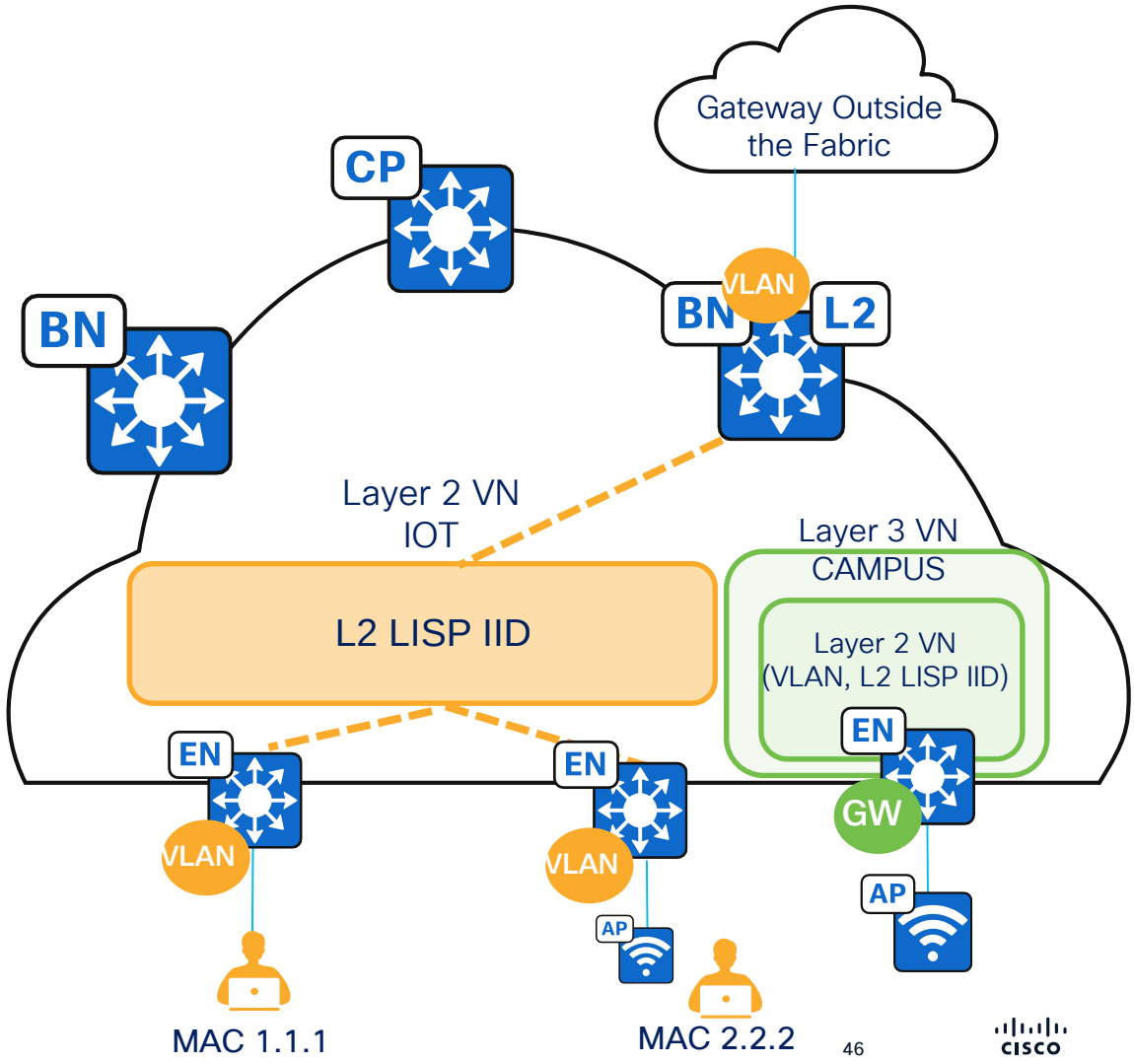


Cisco SD-Access Fabric

Layer 2 Virtual Networks

For Your Reference

- 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.

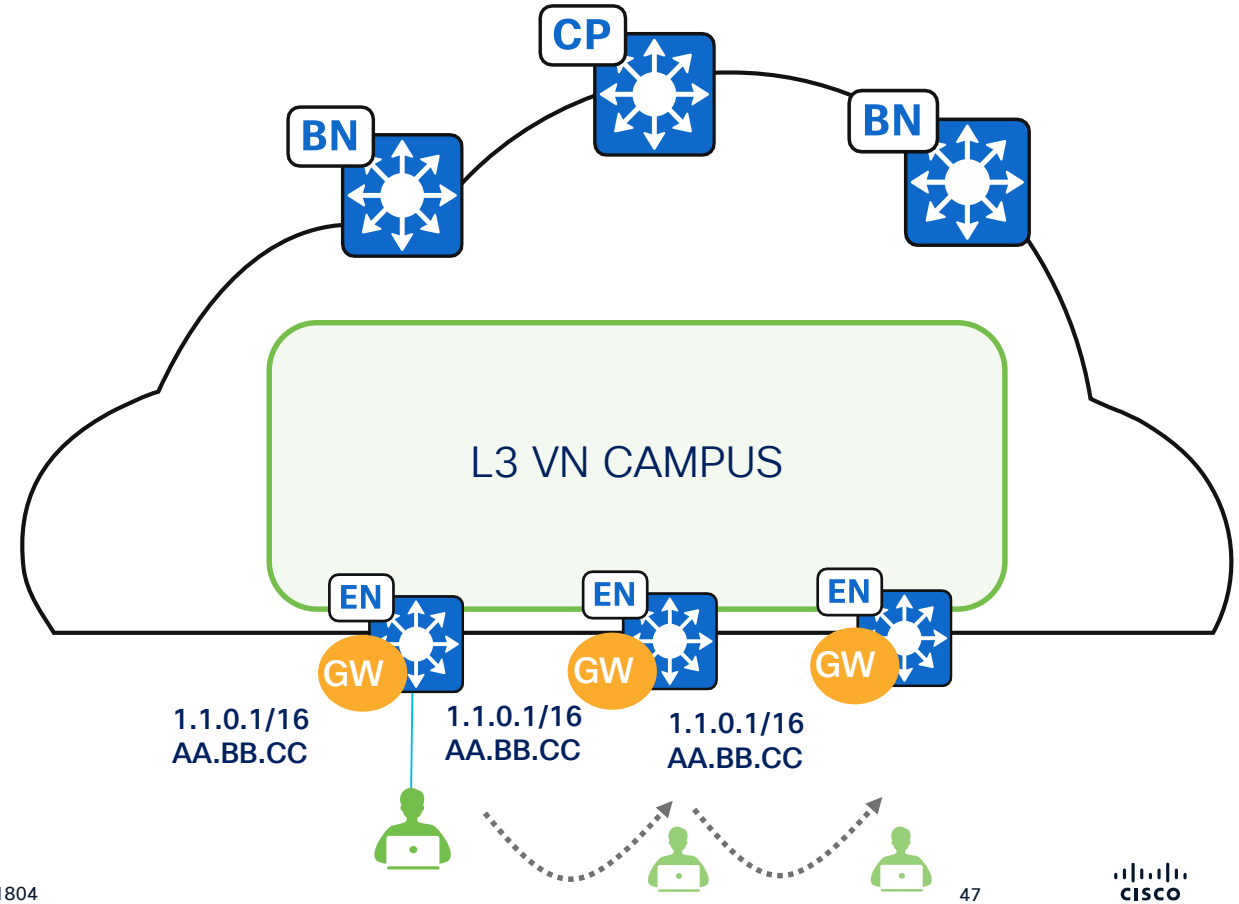


Cisco SD-Access Fabric

For Your Reference

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

For Your Reference

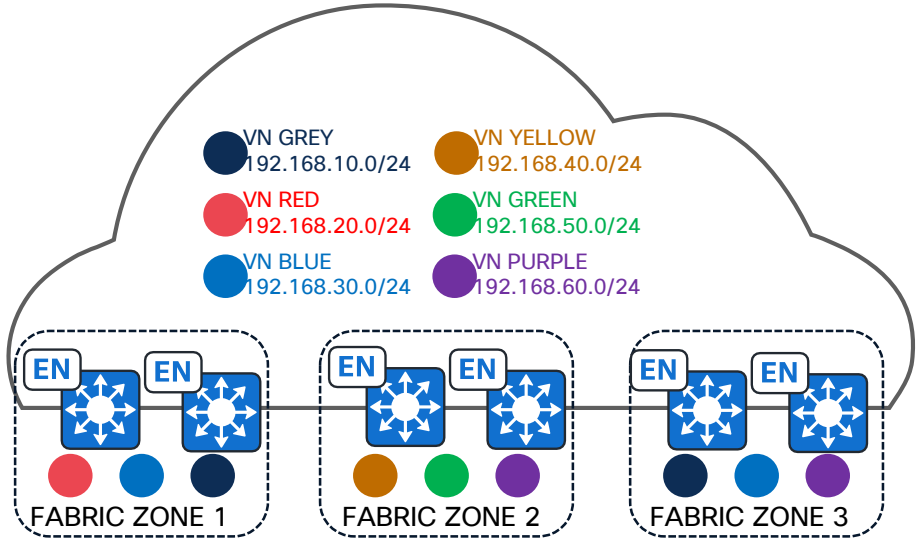
Fabric Zones

Overview

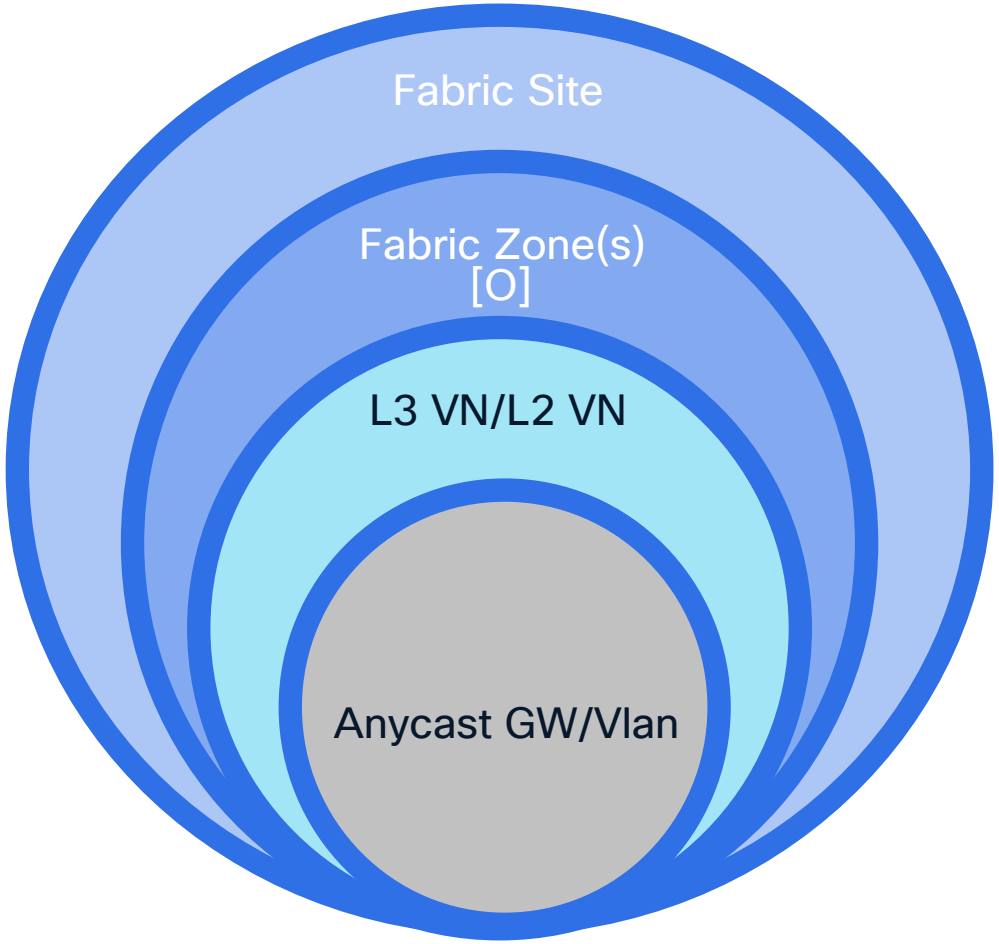
- Customers would like to restrict the VN/IP pool contained to a certain set of Fabric Edges.
- Customers requires the flexibility for granular control of IP Pool provisioning scope.
- Needed for compliance and security frameworks.

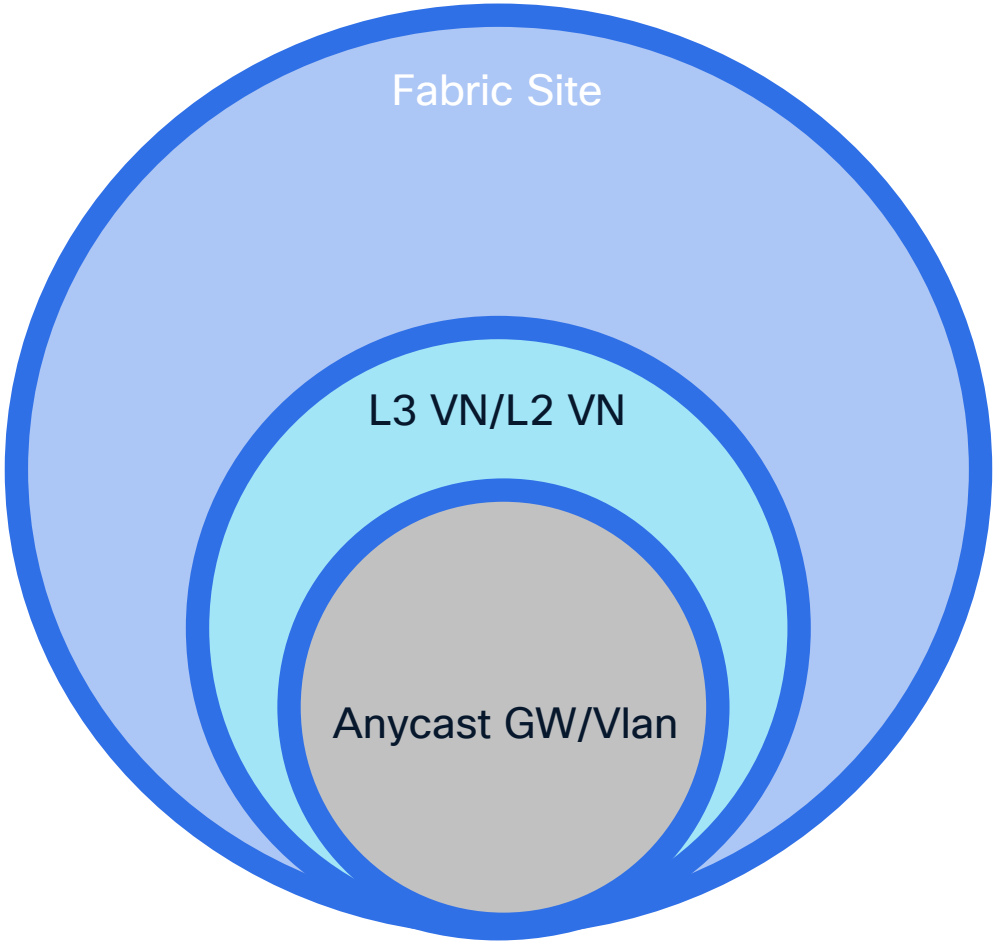
Details

- Cisco SD-Access introduces an optional construct known as Fabric Zones
- Provides the flexibility to assign and map selective pools within the VN's to be provisioned at fabric edges.
- Device role that can exist in a fabric zone are only Fabric Edges, extended nodes, and policy extended nodes.
- Fabric zone can inherit all the pools within the VN or a selective pool within the VN by using the workflow on the Cisco Catalyst Center.
- All the properties of the Pool such as layer2 flooding directed-broadcast would be inherited on the fabric zone.
- The addition of CP/Border/WLC device is not allowed at the fabric zone. They need to be assigned at the parent fabric site only.

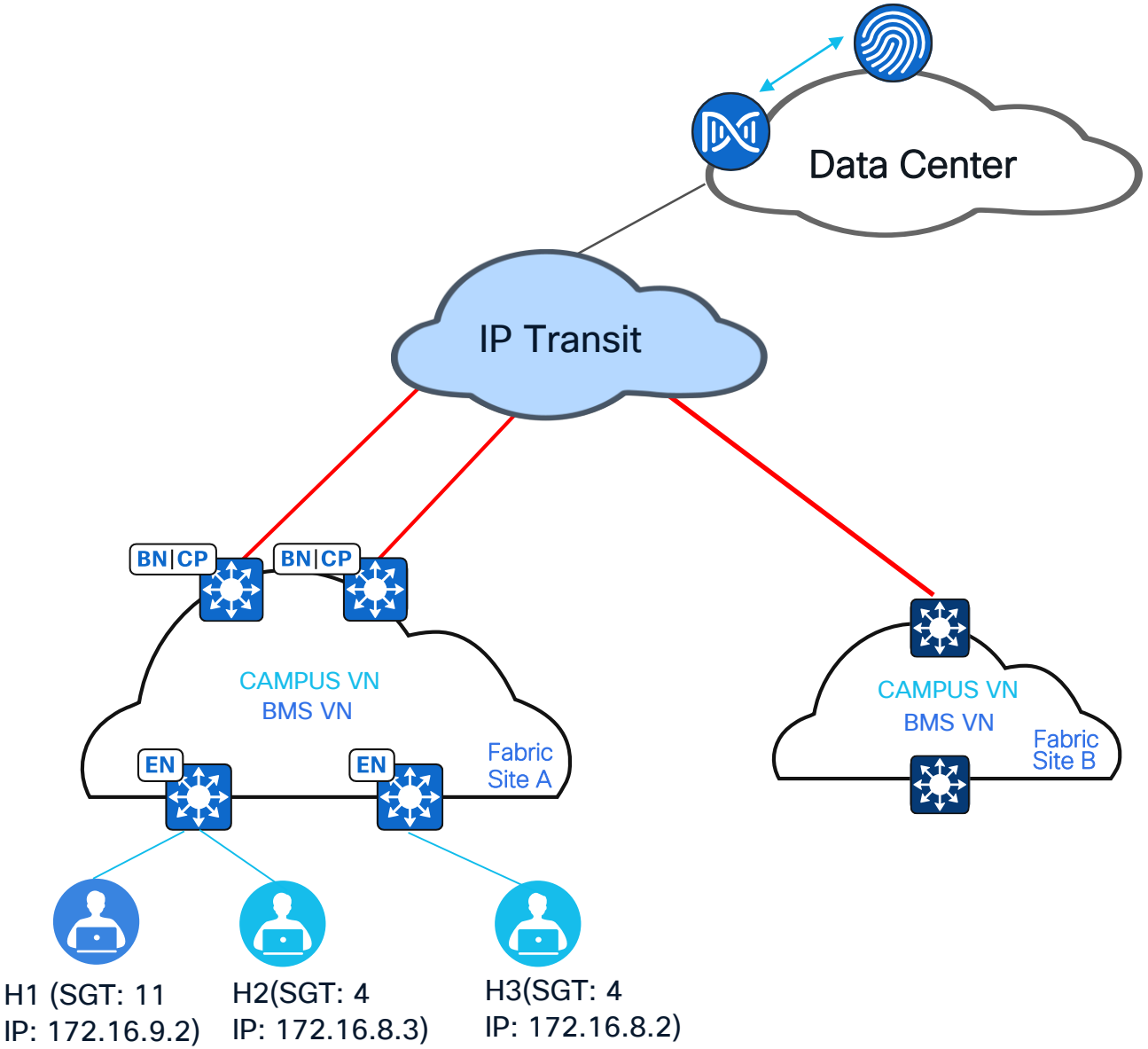


Macro Segmentation





Demo Topology

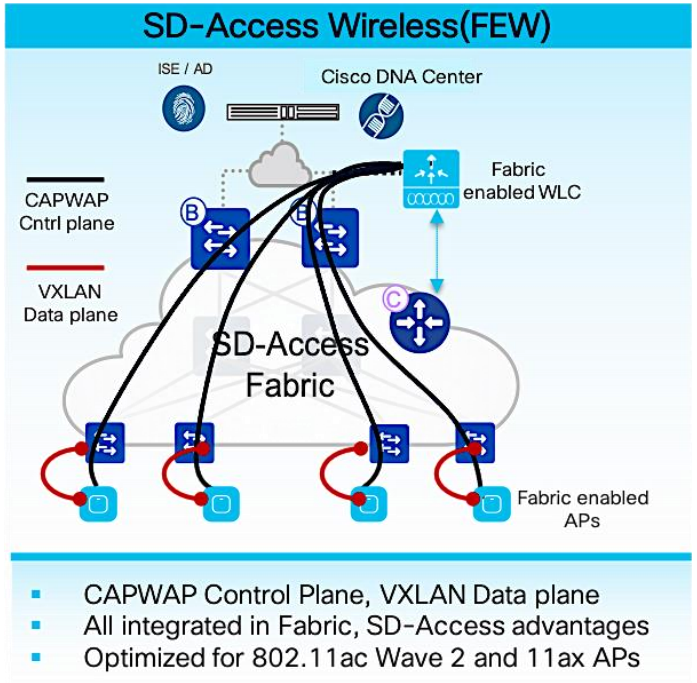


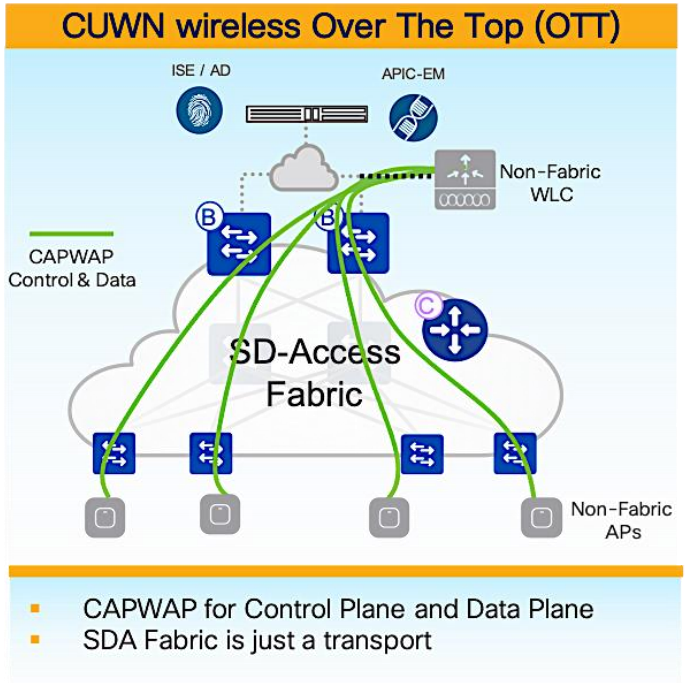
Cisco SD-Access Wireless

Cisco SD-Access Wireless

Wireless design options

Deployment types : FEW , OTT , Mixed Mode
Supported Platforms : C9800,3504,5520,8540, eWLC
AP Mode : Local, Flex connect*
Control-Plane Node Support : AireOS, C9800





Cisco SD-Access Wireless

Which controller to choose?

SD-Access – WLC Scale

Platform	Number of APs	Number of Clients
Aironet 3504	150	3,000
Aironet 5520	1,500	20,000
Aironet 8540	6,000	40,000
Catalyst 9800L	250	5,000
Catalyst 9800-CL (4 CPUs / 8 GB RAM)	1,000	10,000
Catalyst 9800-40	2,000	32,000
Catalyst 9800-CL (6 CPUs / 16 GB RAM)	3,000	32,000
Catalyst 9800-80	6,000	64,000
Catalyst 9800-CL (10 CPUs / 32 GB RAM)	6,000	64,000

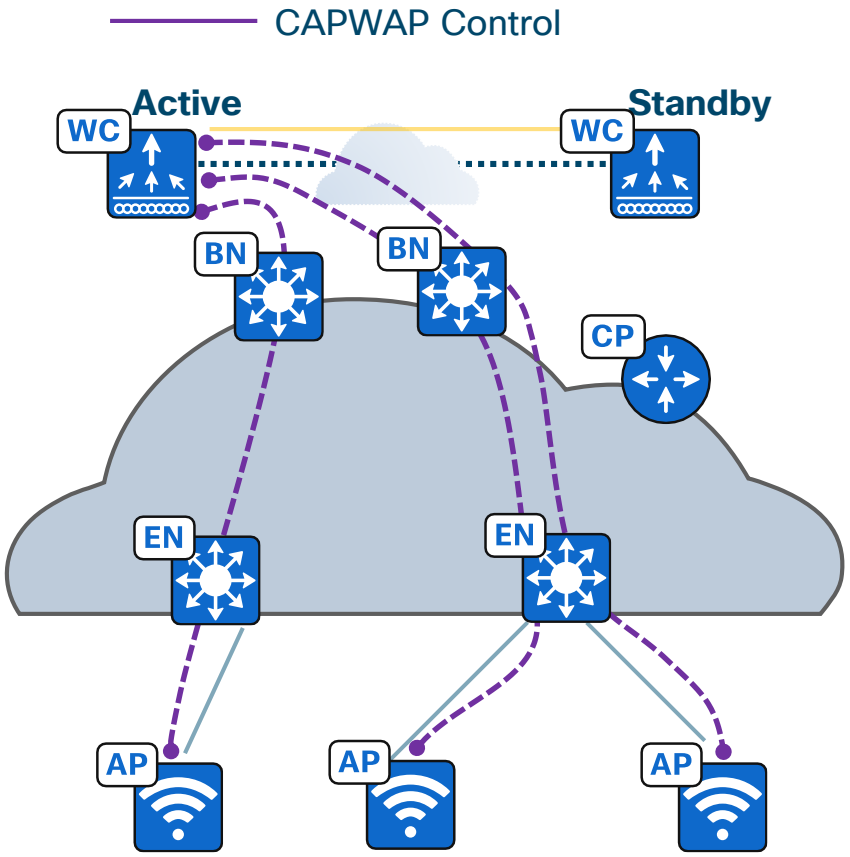
SD-Access – Embedded Wireless

Platform	Number of APs	Number of Clients
Catalyst 9200/L	Not Supported	Not Supported
Catalyst 9300 L	50	1000
Catalyst 9300 (Single Switch)	200	4000
Catalyst 9300 (Switch Stack)	200	4000
Catalyst 9400/9500/9500H	200	4000

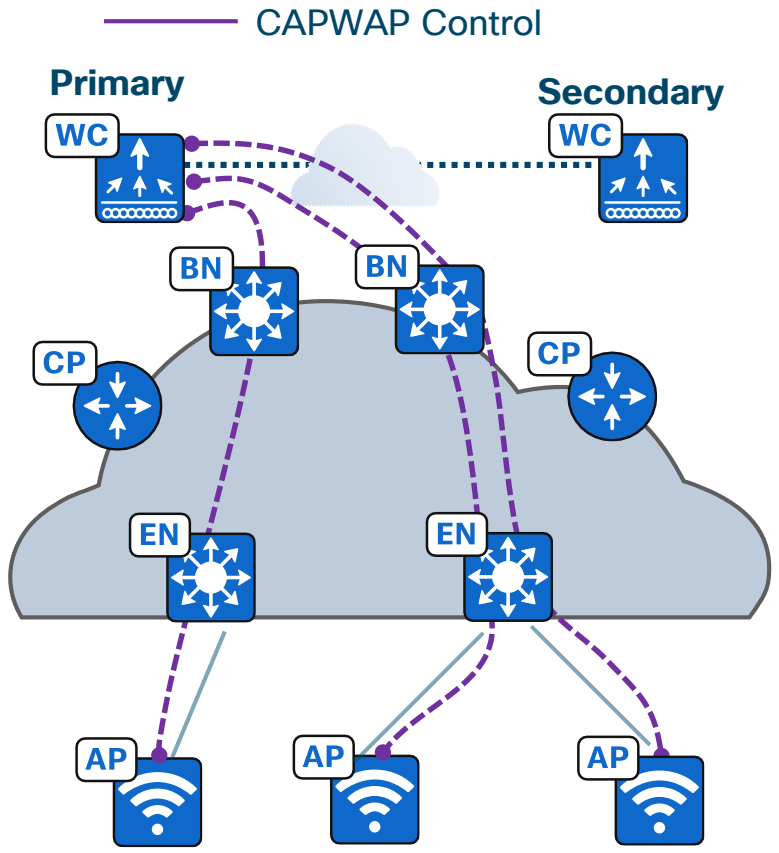
Cisco SD-Access overlay

Fabric enabled wireless- N+1 HA vs SSO

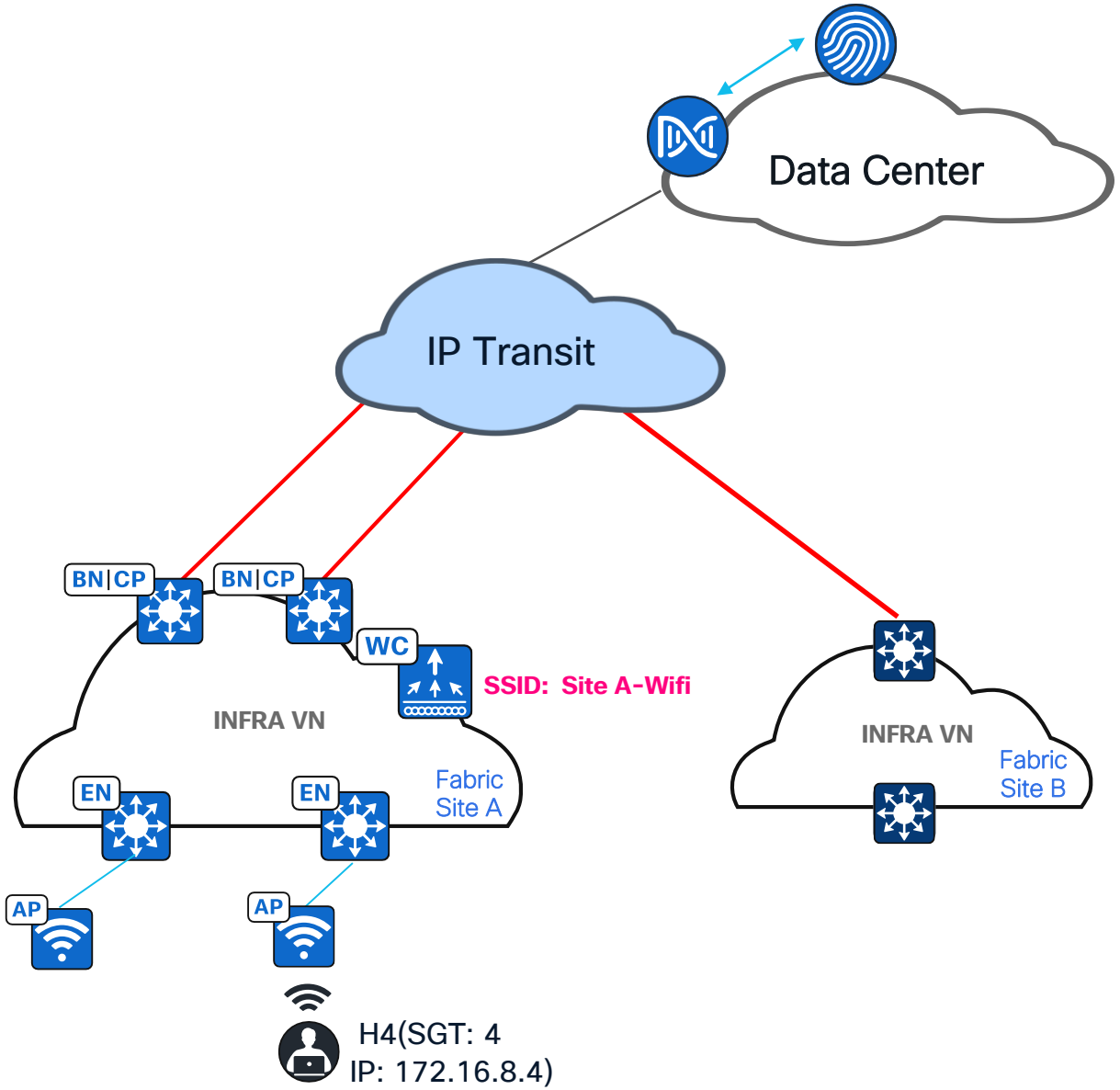
Stateful Redundancy with SSO



Stateless Redundancy with N+1 HA



Demo Topology



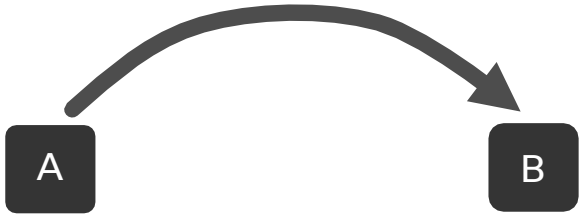
Cisco SD-Access Policy

Cisco Trustsec Functions

Classification

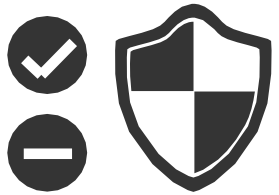
(Assigning SGTs)

- Static Assignments
- Dynamic Assignments



Propagation

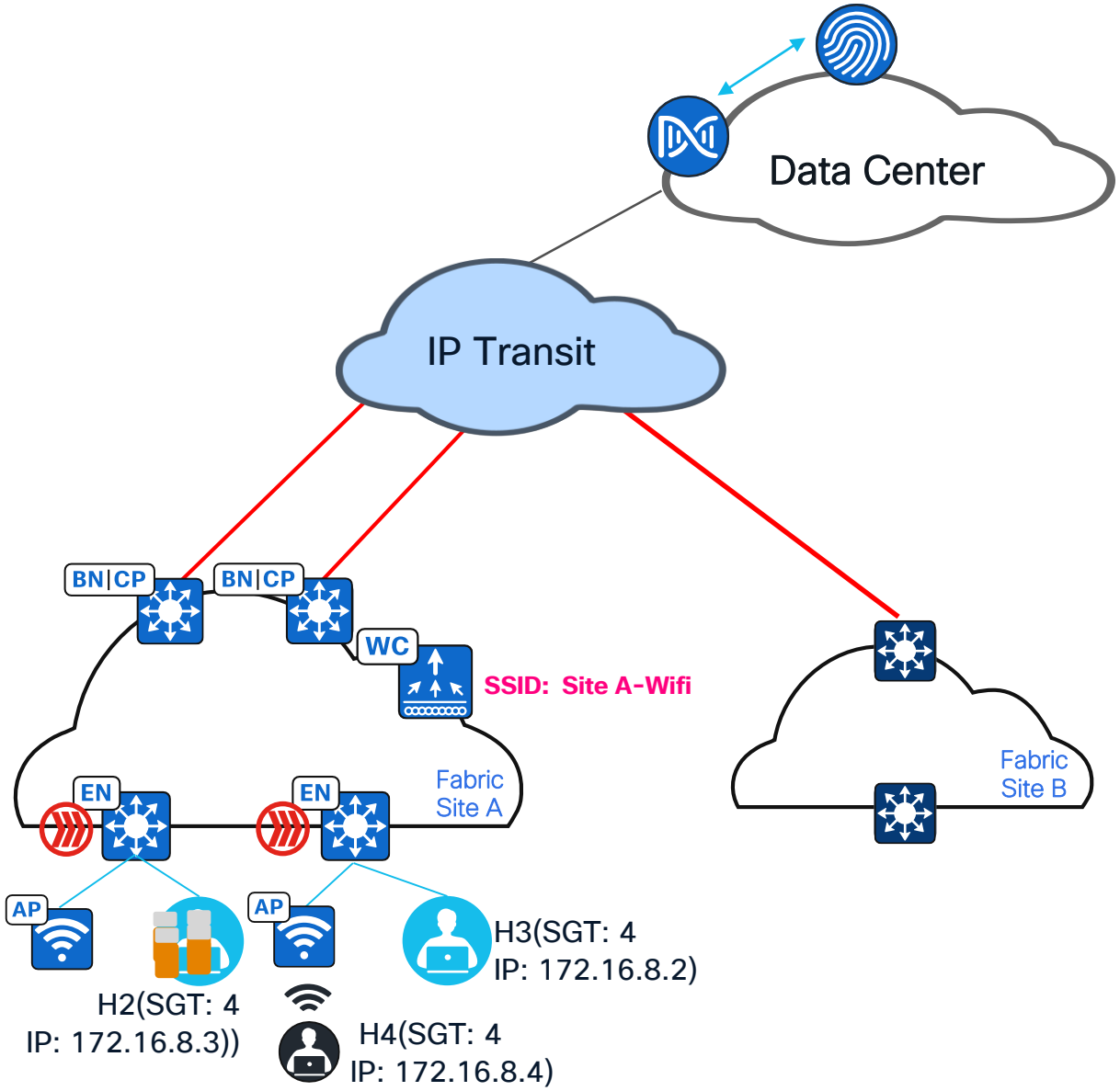
- Inline SGT
- SXP
- WAN Options

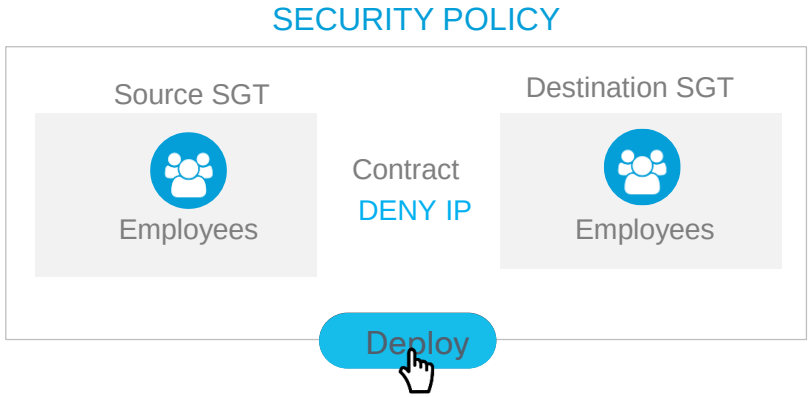


Enforcement

- Security Group ACL
- SG Firewall

Demo Topology





Wrapping Up – Key Takeaways & What's Next

- **What We Covered Today**
  - Real-time SD-Access LISP Fabric deployment using Catalyst Center
  - Integration with ISE for policy enforcement
  - Overlay bring-up and host onboarding
- **Coming Up in Part 2**
  - Advanced LISP topics:
    - LISP Extranet and dynamic default border scenarios
  - Multi-Catalyst Center + ISE integration
- **Stay Sharp Between Sessions**
  - Review BRKENS-2810, 2811, 2814 in the Cisco Live On-Demand Library
  - Explore documentation & lab it out—*break things!*

Complete your session evaluations

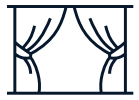
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

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

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

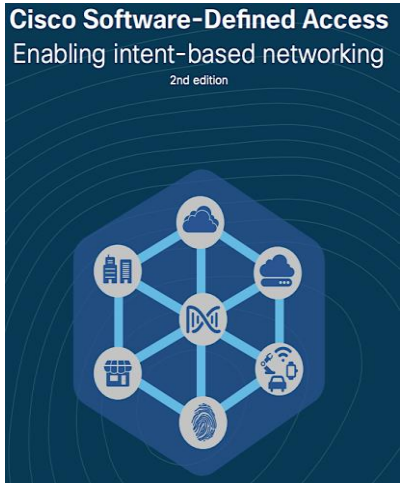
Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact us at: Webex App created for this session

Cisco SD-Access LISP Collaterals

Cisco Software-Defined Access for Industry Verticals

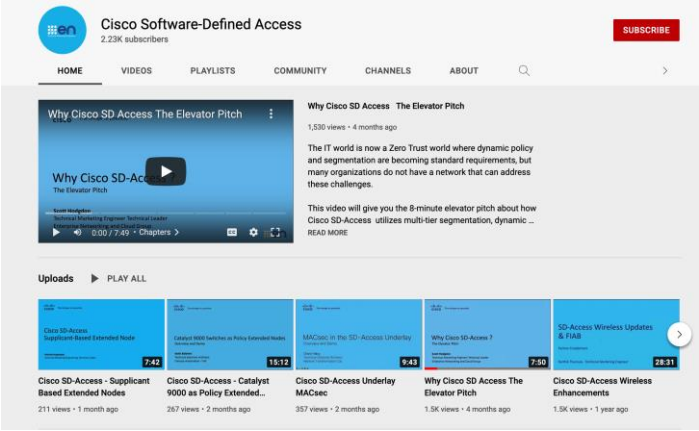
Cisco Software-Defined Access
Enabling intent-based networking



Cisco Solution Validated Profiles (CVPs)

- Cisco Large Enterprise and Government Profile
- Healthcare Vertical
- Financial Vertical
- Healthcare Vertical
- Manufacturing Vertical
- Retail Vertical
- University Vertical

Cisco SD-Access YouTube Link



Cisco SD-Access Design Tool

EN&C Validated Designs

The Latest SD-Access Guides

Thank you

cisco Live !


CISCO