cisco The bridge to possible

What's New in Cisco SD-Access

Scott Hodgdon
Technical Marketing Engineer Technical Leader

cisco Live!

BRKENS-2829

Cisco Webex App

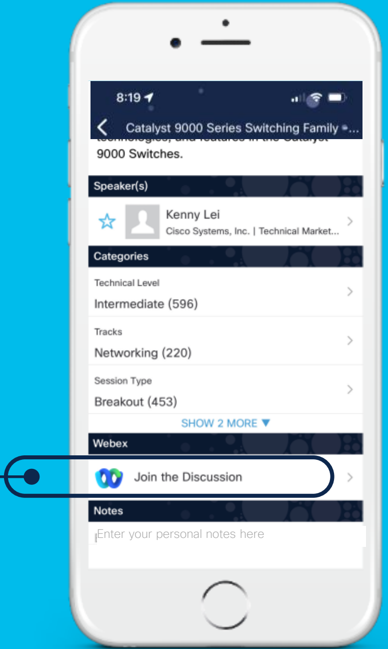
Questions?

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

How

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

Webex spaces will be moderated until February 24, 2023.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Who is Scott ?

Personal

- Based in Raleigh, NC (US)
- 22-year-old daughter in university

Career

- 22+ years as a Technical Marketing Engineer
- 13 Years focused on just Catalyst 6K Family
- 15 years as a Cisco Live Speaker
- 10 years as Cisco Live Session Group Manager for US and EMEA
- 2 Years as a Cisco Partner SE
- 2 Years Lead Network Engineer for 15-site Health Care network in North Carolina
- No formal technology schooling … I have a Business Degree with a Finance Concentration

Current Focus

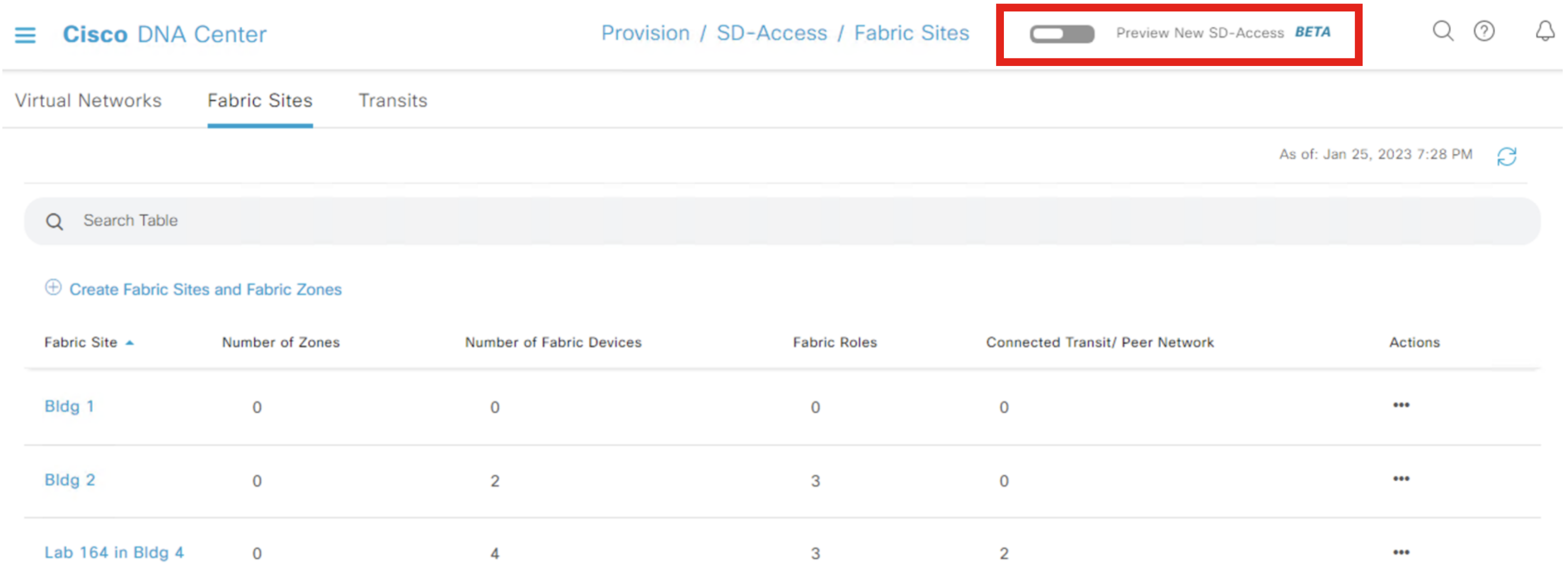
- Cisco SD-Access Enablement and Design since 2016

Agenda

- Layer 2 Switched Access Deployments
- LISP PubSub
  - Overview
  - Dynamic Default Borders
  - Backup Internet in SD-Access Transit
- SD-Access Extranet
- Fabric Zones
- Border Node Preference
- Zero-Trust Capabilities
  - Supplicant-Based Extended Nodes
  - Secure AP Onboarding

Note on Workflow Screenshots

All Screenshots in UI 1.0, not Beta



Cisco DNA Center
Provision / SD-Access / Fabric Sites
Preview New SD-Access BETA
Virtual Networks
Fabric Sites
Transits
Search Table
Create Fabric Sites and Fabric Zones

As of: Jan 25, 2023 7:28 PM

Fabric Site	Number of Zones	Number of Fabric Devices	Fabric Roles	Connected Transit/ Peer Network	Actions
Bldg 1	0	0	0	0	•••
Bldg 2	0	2	3	0	•••
Lab 164 in Bldg 4	0	4	3	2	•••

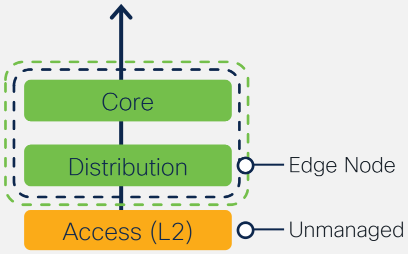
Layer 2 Switched Access Deployments

Evolve your switching fabric with SD-Access

🟩 Macro segmentation

▢ Micro segmentation

Fabric with unmanaged Layer 2 switched access*

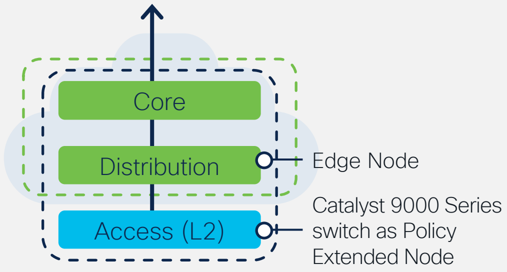


Use case: Keep your existing unmanaged switches

- Segmentation starts at distribution layer
- Integrated wired and wireless

Benefit: Allow tenants to bring their own network.

Fabric with managed Layer 2 switched access

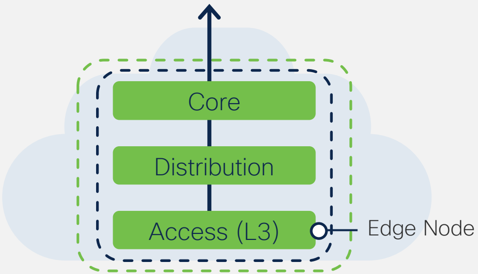


Use case: Retain Layer 2 access

- Extend segmentation down to Layer 2
- Integrated wired and wireless

Benefit: Security and automation at every layer

Fabric with Layer 3 routed access



Use case: Full SD-Access

- Full stack macro and micro segmentation
- Integrated wired and wireless
- Policy-based traffic steering
- Topology independence

Benefit: Experience all that SD-Access offers

*Available since Cisco DNA Center release 2.2.1.x

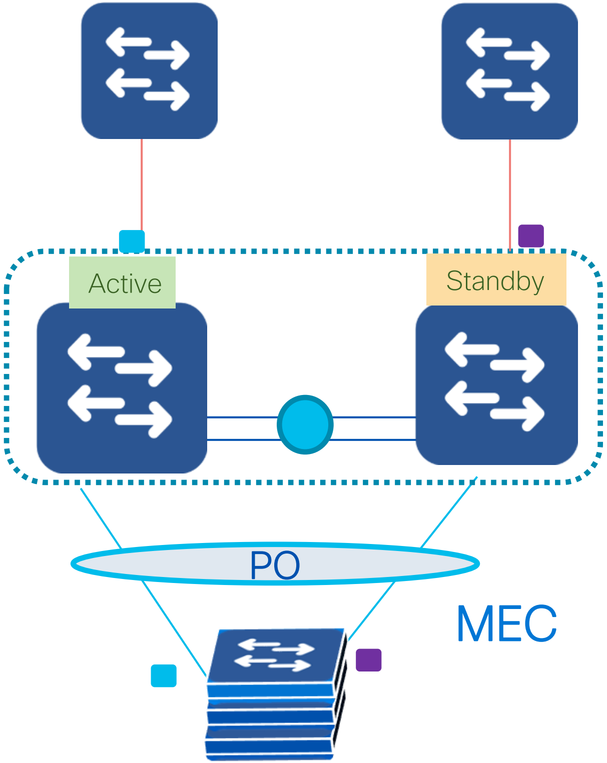
StackWise Virtual in Traditional Networking

Active/Active Data Plane

- Both the switches are capable of forwarding the traffic locally without sending it over Interconnected-Link

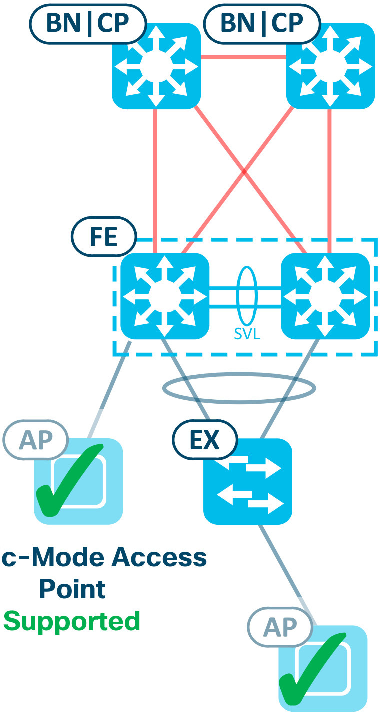
Multi-Chassis EtherChannel

- Port-Channel Spanning across multiple Chassis



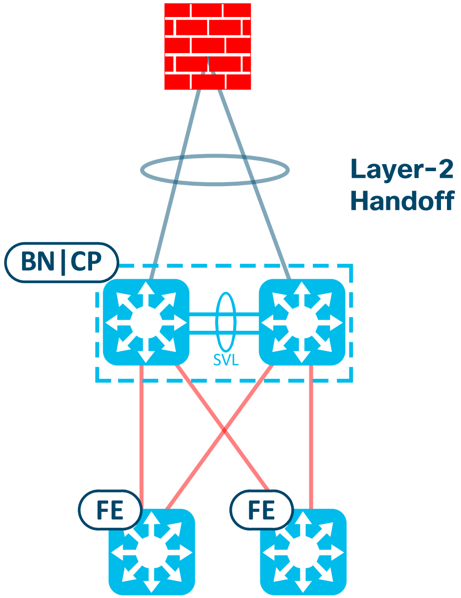
StackWise Virtual in SD-Access Topology Examples

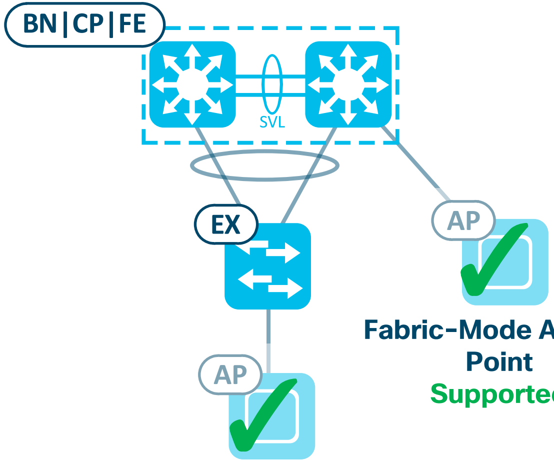
Cisco DNA Center ≥2.2.2.x



Fabric-Mode Access Point
Supported

Fabric-Mode Access Point
Supported





Fabric-Mode Access Point
Supported

Fabric-Mode Access Point
Supported

StackWise Virtual in SD-Access

Considerations

Link Types

If all links connected to the device are Layer 3, then no need for StackWise Virtual.

No ISSU Support

ISSU does not support LISP or Trustsec, which are key components of an SD-Access network.

StackWise Virtual Support as of 2.2.2.x Release

SVL Platform	Border Node	Edge Node	Control Plane Node	Colocated Border and Control Plane Node	Colocated Border and Edge Node	Fabric in a Box	Colocated Border and Control Plane Node with Embedded Wireless	Edge Node with Embedded Wireless	Fabric in a Box With Embedded Wireless
9400	2.1.2.x	2.1.2.x	2.1.2.x	2.1.2.x	2.1.2.x	2.1.2.x	2.2.2.x	2.2.2.x	2.2.2.x
9500/H	1.3.3.x	1.3.3.x	2.1.2.x	1.3.3.x	2.1.2.x	1.3.3.x	2.2.2.x	2.2.2.x	2.2.2.x
9600	2.1.2.x	Not supported	2.1.2.x	2.1.2.x	Not supported	Not supported	Not supported	Not supported	Not supported

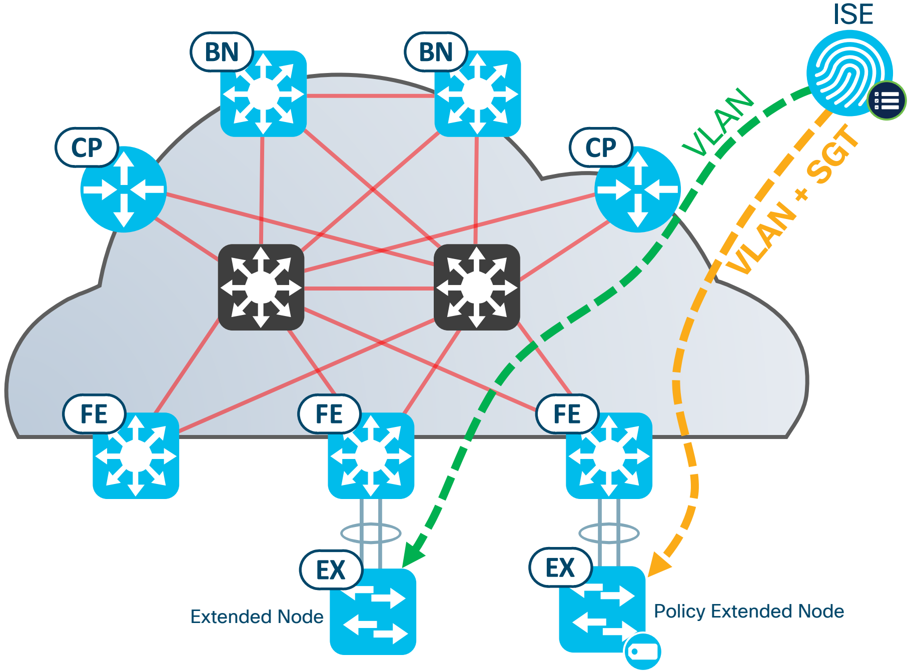
Policy Extended Node for Catalyst 9000 Series Switches

Feature

- Cisco DNA Center 1.3.3.x introduced Policy Extended Node (PEN) functionality for the IE3400 and IE3400H.
- ISE can assign VLAN and SGT to endpoint connected to a PEN upon Authentication/Authorization using 802.1x or MAB.
- Links connecting Edge Node to Policy Extended Node are configured with inline tagging so that SGT is propagated.
- The Policy Extended Node performs the SGACL enforcement.

Enhancement

- Cisco DNA Center 2.1.2.x extends PEN functionality to most Catalyst 9000 Series switches: C9200/L, C9300/L, C9400, C9500/H.
- Catalyst 9600 Series switches are not supported as Policy Extended Nodes.
- The Catalyst 9000 PEN can be deployed on as a switch stack (physical stacking), but not as a StackWise Virtual switch.



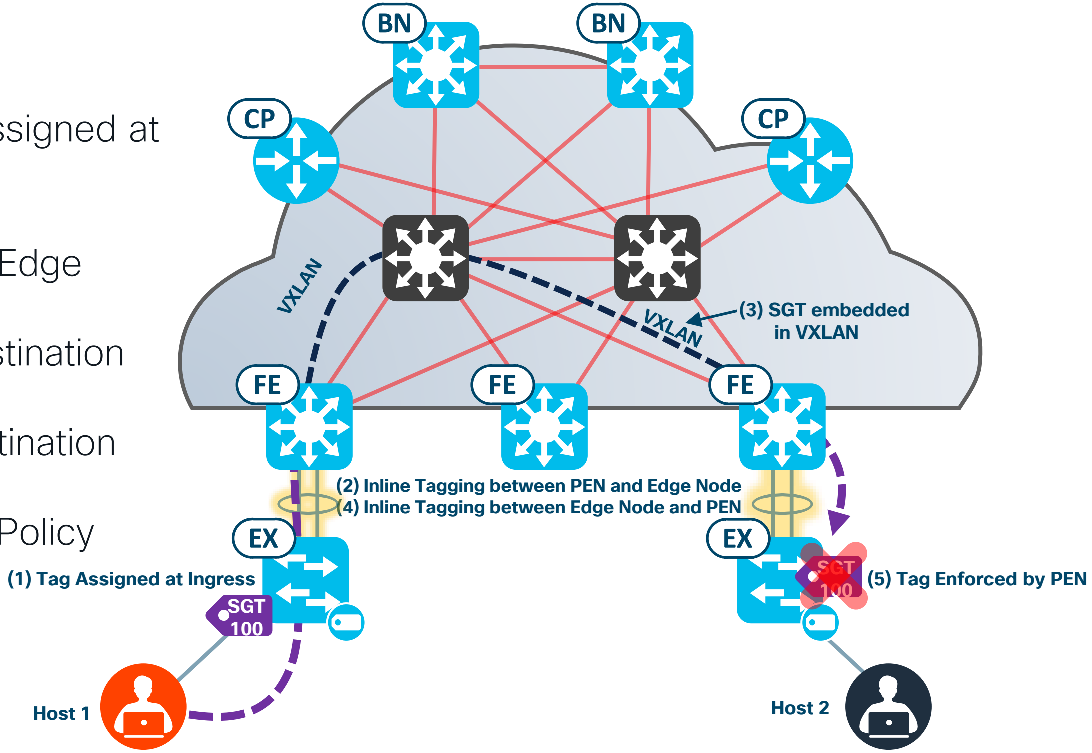
- IE3300
- IE4000
- IE4010
- IE5000
- 3560-CX
- CDB

- IE3400
- IE3400H
- New in 2.1.2.x
- C9200/L
- C9300/L
- C9400
- C9500
- C9500H

Flows from Policy Extended Nodes

Example: Host 1 and Host 2 are connected to different PENs.

1. Traffic from Host 1 has source SGT assigned at the Policy Extended Node via Authentication/Authorization with ISE.
2. The SGT is carried inline to First-Hop Edge Node.
3. The SGT is carried over VXLAN to destination Edge Node.
4. The SGT is carried inline from the destination Edge Node to the destination PEN.
5. The SGT enforcement is done by the Policy Extended Node.

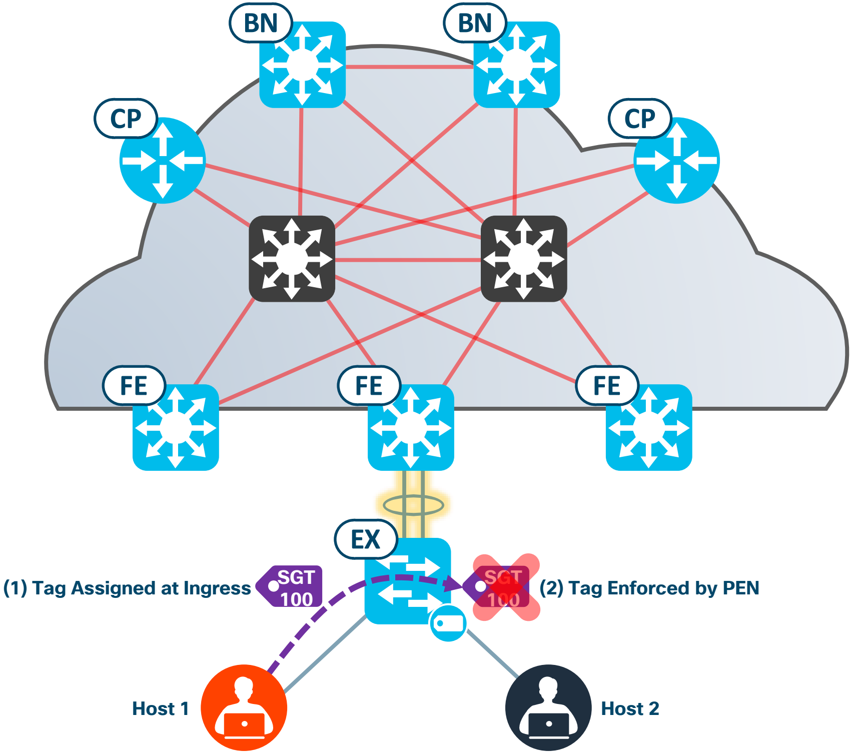

BN
BN
CP
CP
VXLAN
VXLAN
(3) SGT embedded in VXLAN
FE
FE
FE
(2) Inline Tagging between PEN and Edge Node
(4) Inline Tagging between Edge Node and PEN
EX
EX
(1) Tag Assigned at Ingress
SGT 100
SGT 100
(5) Tag Enforced by PEN
Host 1
Host 2

Flows from Policy Extended Nodes

Example: Host 1 and Host 2 are connected to the same PEN.

1. Traffic from Host 1 has source SGT assigned at the Policy Extended Node via Authentication/Authorization with ISE.

1. The SGT enforcement is done by the Policy Extended Node without having to forward and hair-pin at the Edge Node.

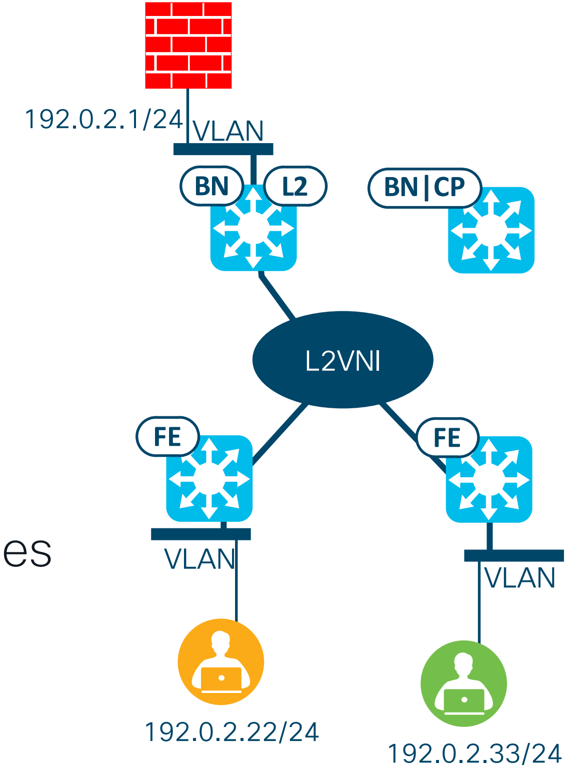


VLAN-Based L2VNI

Also known as “Gateway Outside the Fabric”

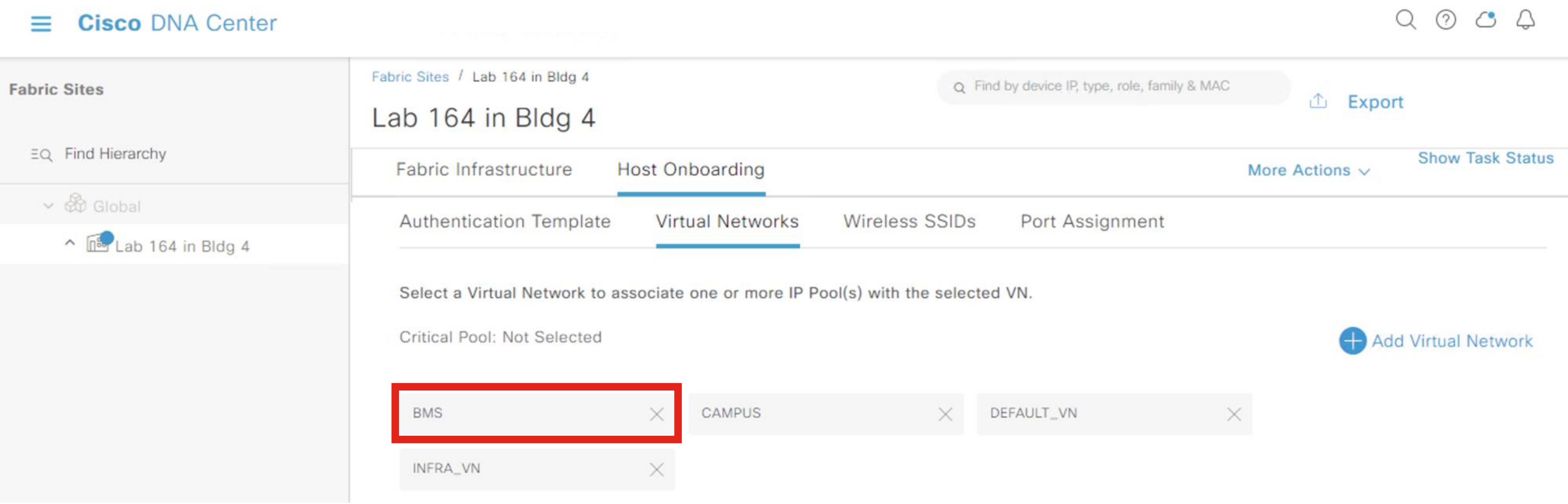
Best Practice : Dedicated Border for L2 Handoff

Considerations : Cat 9K Switches Only for Edge Nodes
and Border Nodes



VLAN-Based L2VNI

Workflow



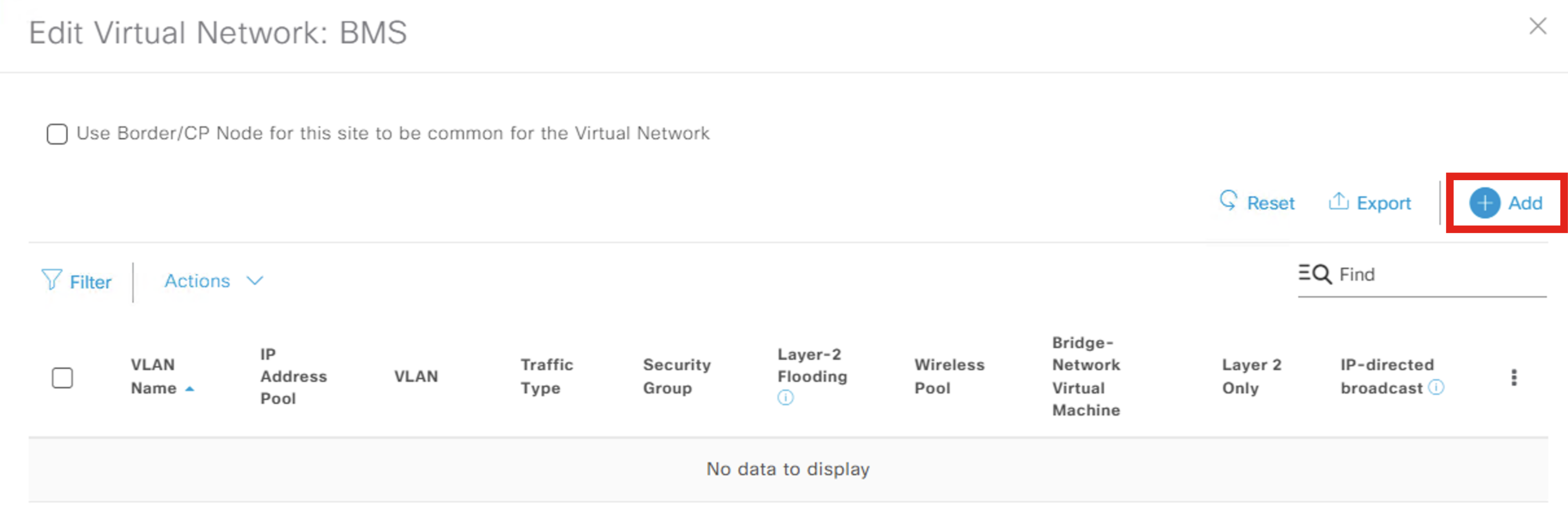
Select a Virtual Network to associate one or more IP Pool(s) with the selected VN.

Critical Pool: Not Selected

Select VN in Host Onboarding screen

VLAN-Based L2VNI

Workflow



Edit Virtual Network: BMS

□ Use Border/CP Node for this site to be common for the Virtual Network

□	VLAN Name	IP Address Pool	VLAN	Traffic Type	Security Group	Layer-2 Flooding	Wireless Pool	Bridge-Network Virtual Machine	Layer 2 Only	IP-directed broadcast

No data to display

Add an IP Pool to the VN

VLAN-Based L2VNI

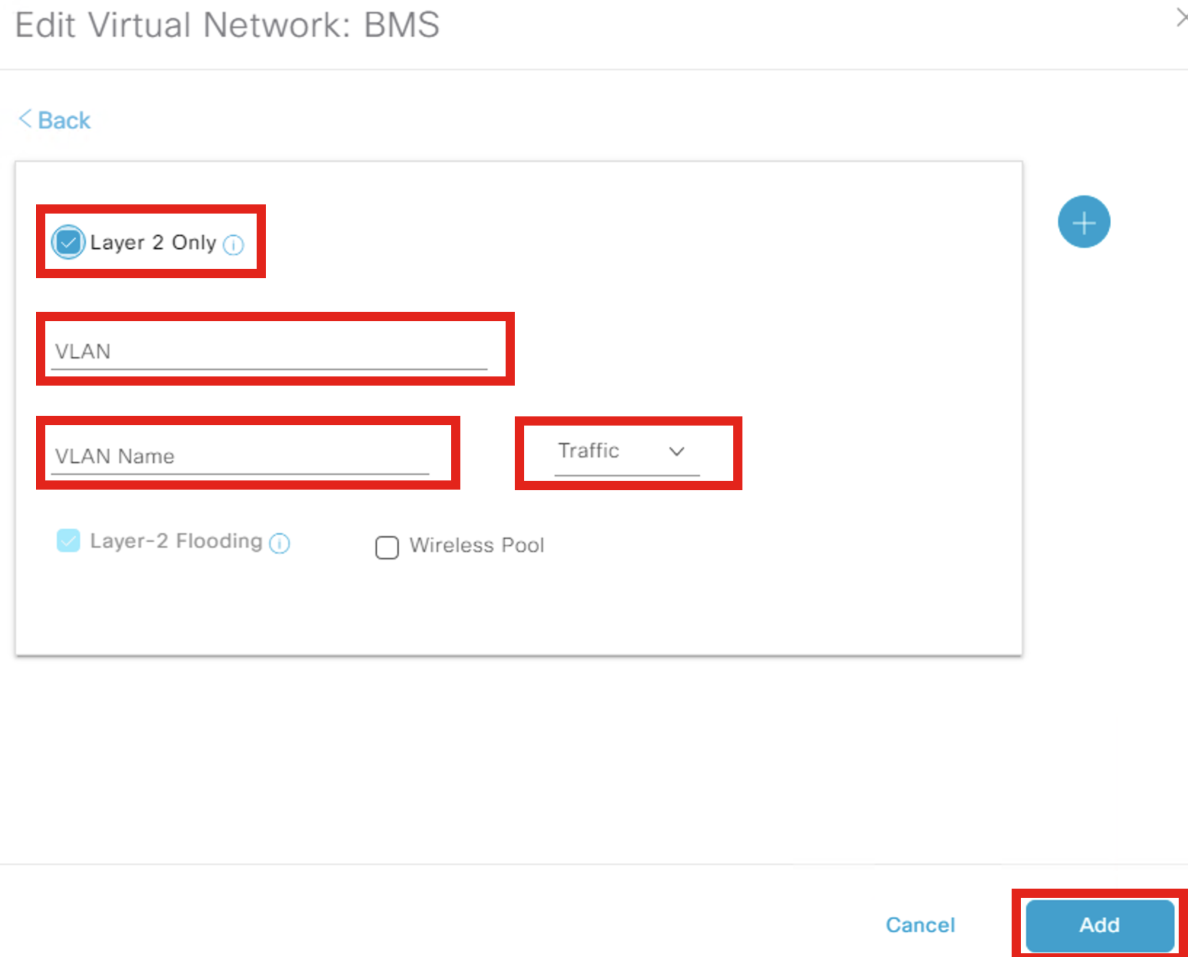
Workflow

Select "Layer 2 Only" Box

Fill in VLAN number, VLAN Name and Traffic Type fields

Layer-2 Flooding is enabled by default for Layer 2 Only services

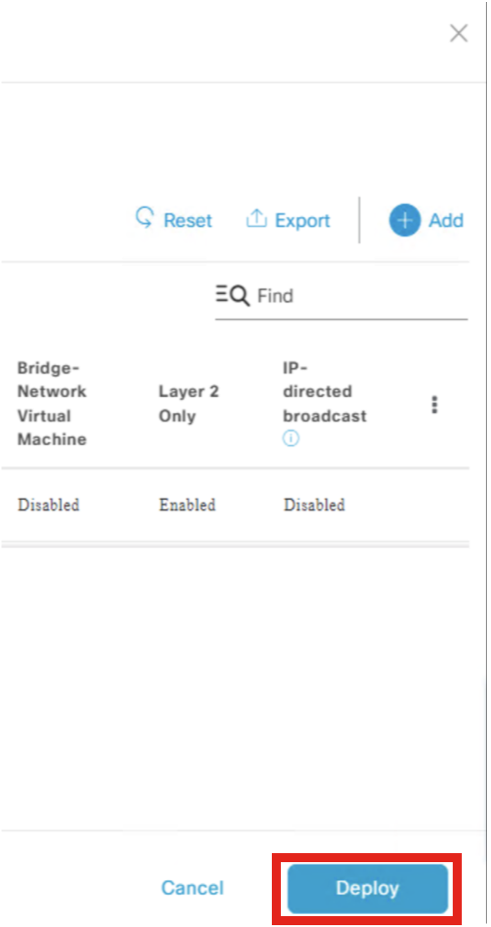
Click "Add" when done



Edit Virtual Network: BMS

VLAN-Based L2VNI

Workflow



Bridge-Network Virtual Machine	Layer 2 Only	IP-directed broadcast
Disabled	Enabled	Disabled

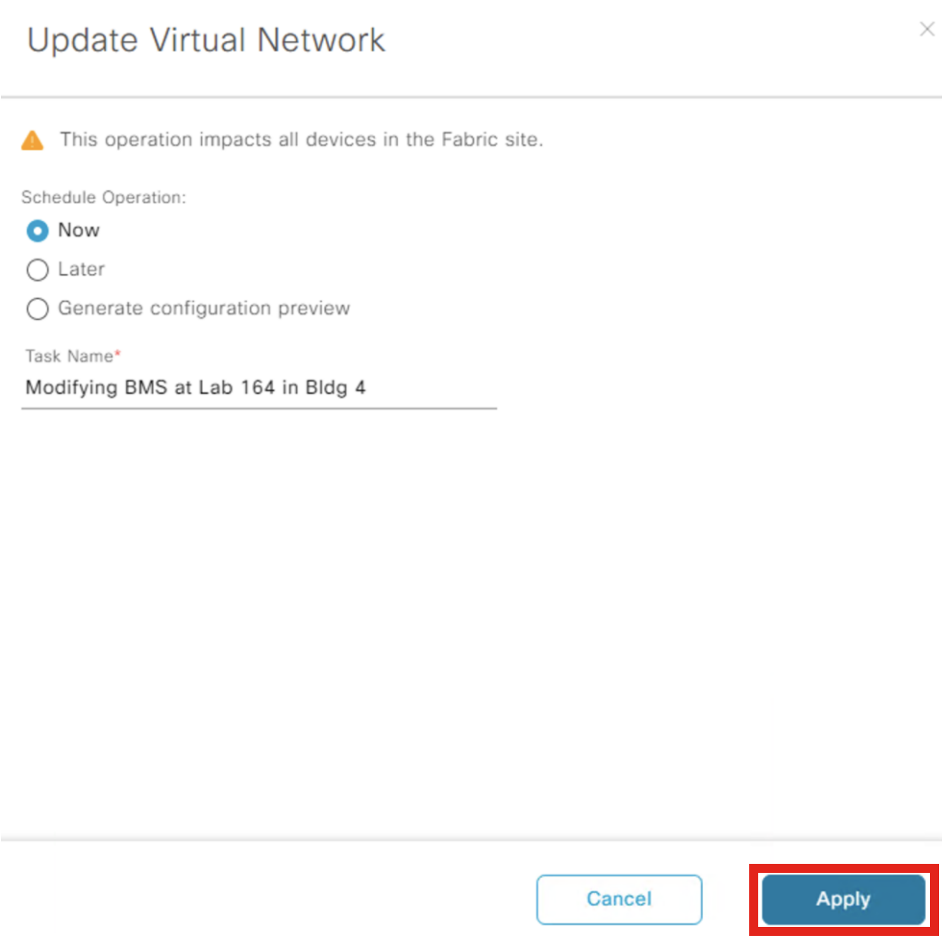
On the next screen, click “Deploy”

VLAN-Based L2VNI

Workflow

And then “Apply” on the screen after that .

You can apply immediately or schedule a time to have the change applied.



Update Virtual Network

This operation impacts all devices in the Fabric site.

Schedule Operation:

● Now

○ Later

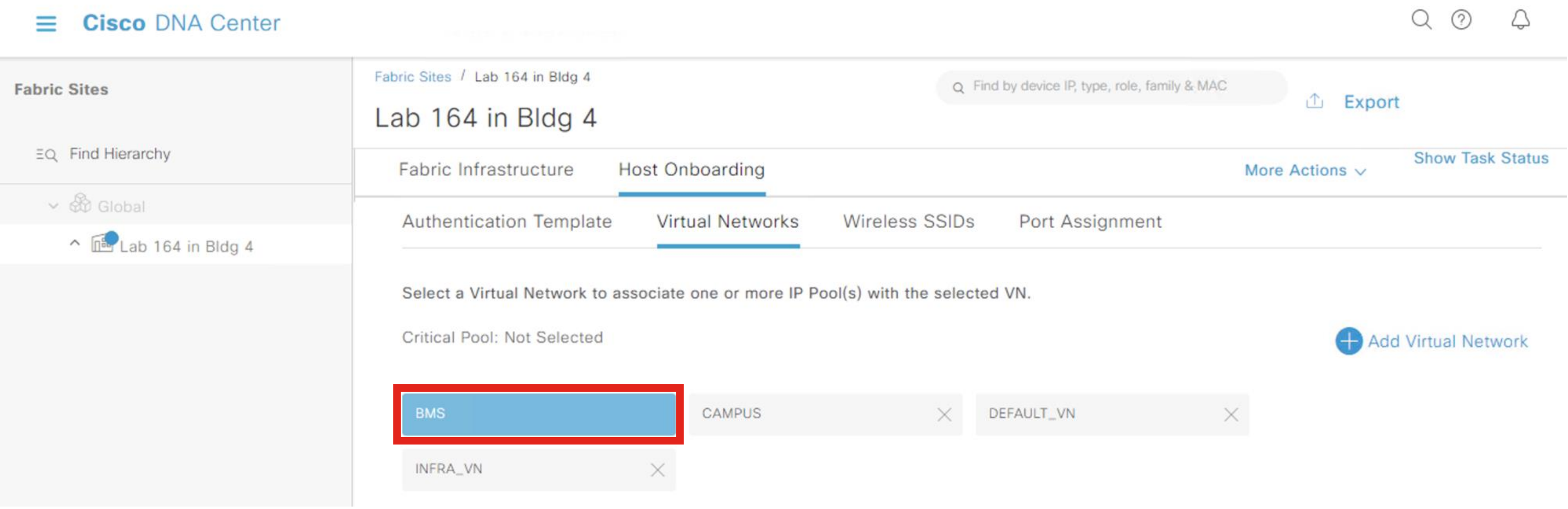
○ Generate configuration preview

Task Name*

Modifying BMS at Lab 164 in Bldg 4

VLAN-Based L2VNI

Workflow



Cisco DNA Center

Fabric Sites / Lab 164 in Bldg 4

Lab 164 in Bldg 4

Select a Virtual Network to associate one or more IP Pool(s) with the selected VN.

Critical Pool: Not Selected

Notice that “BMS” has turned blue, indicating an there is a VLAN / IP Pool assigne

VLAN-Based L2VNI

Design Considerations

Scale

- Uses same resources as IP Pool
- Total number of IP Pools + L2VNI VLANs cannot exceed published numbers in DNA Center Data Sheet

Hardware Support

- Only Fabric Sites with Catalyst 9K Edge Nodes and Layer 2 Handoff Border Nodes
- Routing platforms can be Control Plane Nodes and/or Layer 3 Handoff Border Nodes

Layer 2 Handoff

- Supported to collocate Layer 2 and Layer 3 Handoffs on same Border, but not Best Practice

SGTs

- SGT assignment and policy is supported in an VLAN-Based L2VNI

Multicast

- L3 multicast within VLAN-Based L2VNI is STRONGLY not recommended as it is flooded to all Edge Nodes

Layer 2 Switched Access in SD-Access

Design Considerations

Fabric Edge Node Scale

Cisco SD-Access edge node scale					
Catalyst Model	**9200-L**	**9200**	**9300/L/X**	**9400**	**9500/H**
Endpoints	2000	4000	6000	6000	6000

East-West Policy Enforcement at the Access ?

Gateway outside the fabric required ?

LISP PubSub

LISP Pub/Sub Control Plane

Basic Definitions

Publication

- The information that the mapping system sends to the Subscriber (the LISP device).
- Publishers – Control Plane Nodes, Transit Control Plane Nodes

Subscription

- The process LISP devices use to express interest for a certain portion of information within the mapping system.
- Subscribers – Border Nodes

LISP Pub/Sub

What Challenges are We Solving?

Distribution of Prefixes

Current Method:

- Exporting LISP registrations to the RIB
- Redistribute into BGP
- Advertise via BGP
- Import BGP into LISP Map-Cache

This has limitations based on the protocol used for distribution such as:

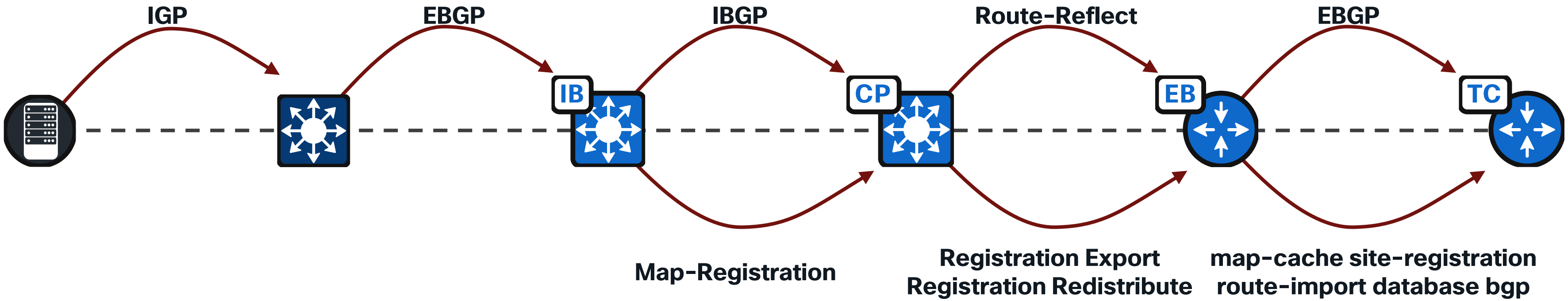
- The address-families that are supported by the other routing protocol (BGP)
- The convergence mechanisms and timers by the other routing protocol (BGP)

LISP/BGP Control Plane

Before LISP Pub/Sub

Reliance on BGP

- To push LISP Site-Registration table to another device, another protocol was needed.
- BGP was used as that transport
- This created an underlying reliance on BGP.


IGP
EBGP
IBGP
Route-Reflect
EBGP
IB
CP
EB
TC
Map-Registration
Registration Export
Registration Redistribute
map-cache site-registration
route-import database bgp

LISP/BGP Control Plane

Before LISP Pub/Sub – Reliance on BGP

BGP can be counted on to converge reliably, even deterministically.

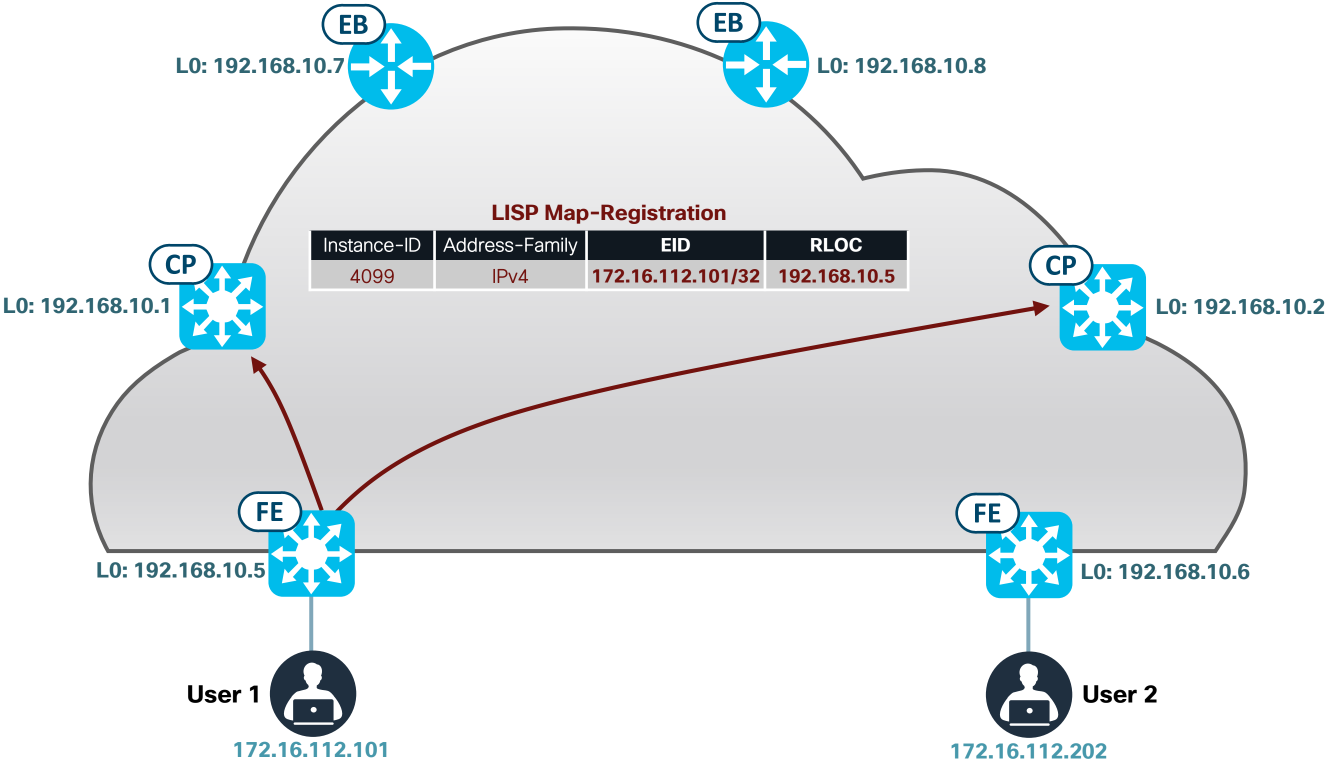
- BGP does not converge quickly.

BGP is a “heavy” protocol

- Expertise required to appropriately configure, support, and troubleshoot the protocol.
- The expertise needed increases significantly when using multiple address-families such as BGP VPNv4 and VPNv6 address families.

LISP Pub/Sub

Registration and Publication – Within a Site

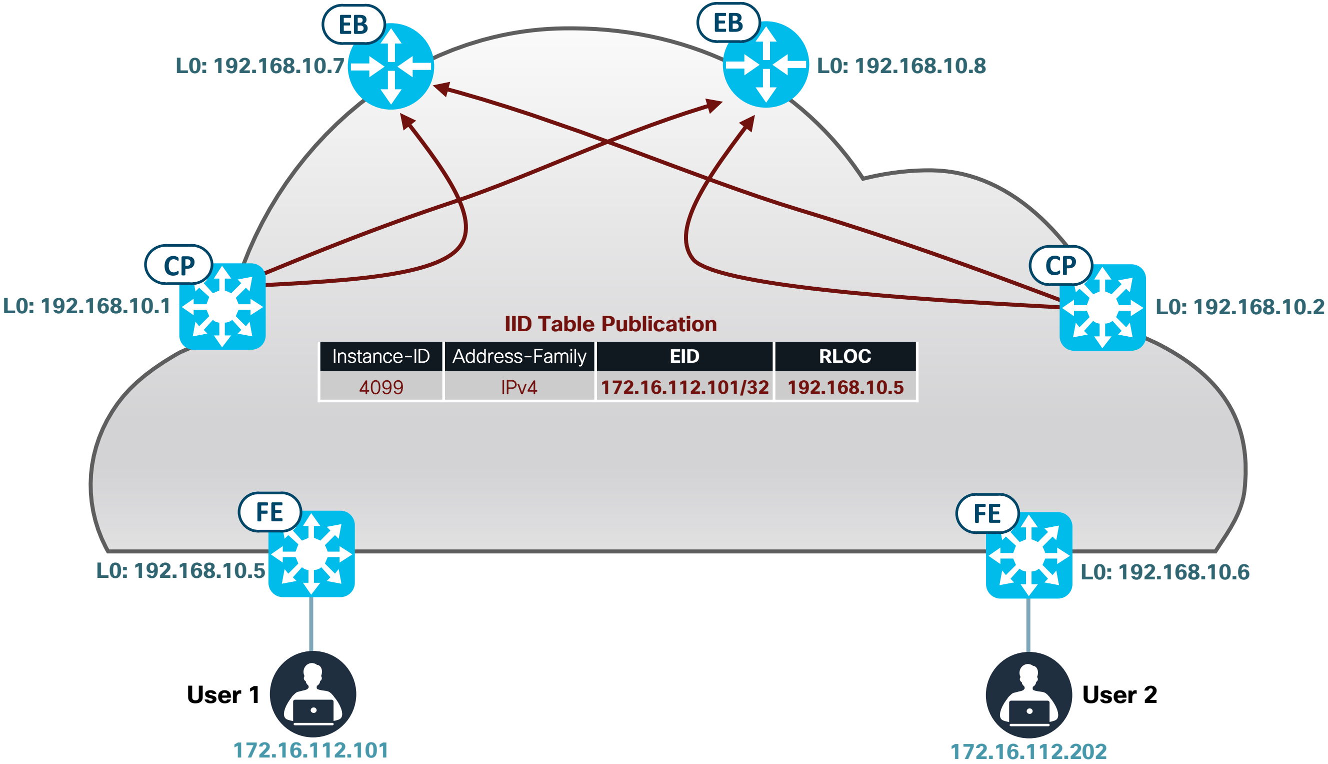


LISP Map-Registration

Instance-ID	Address-Family	EID	RLOC
4099	IPv4	172.16.112.101/32	192.168.10.5

LISP Pub/Sub

Registration and Publication – Within a Site

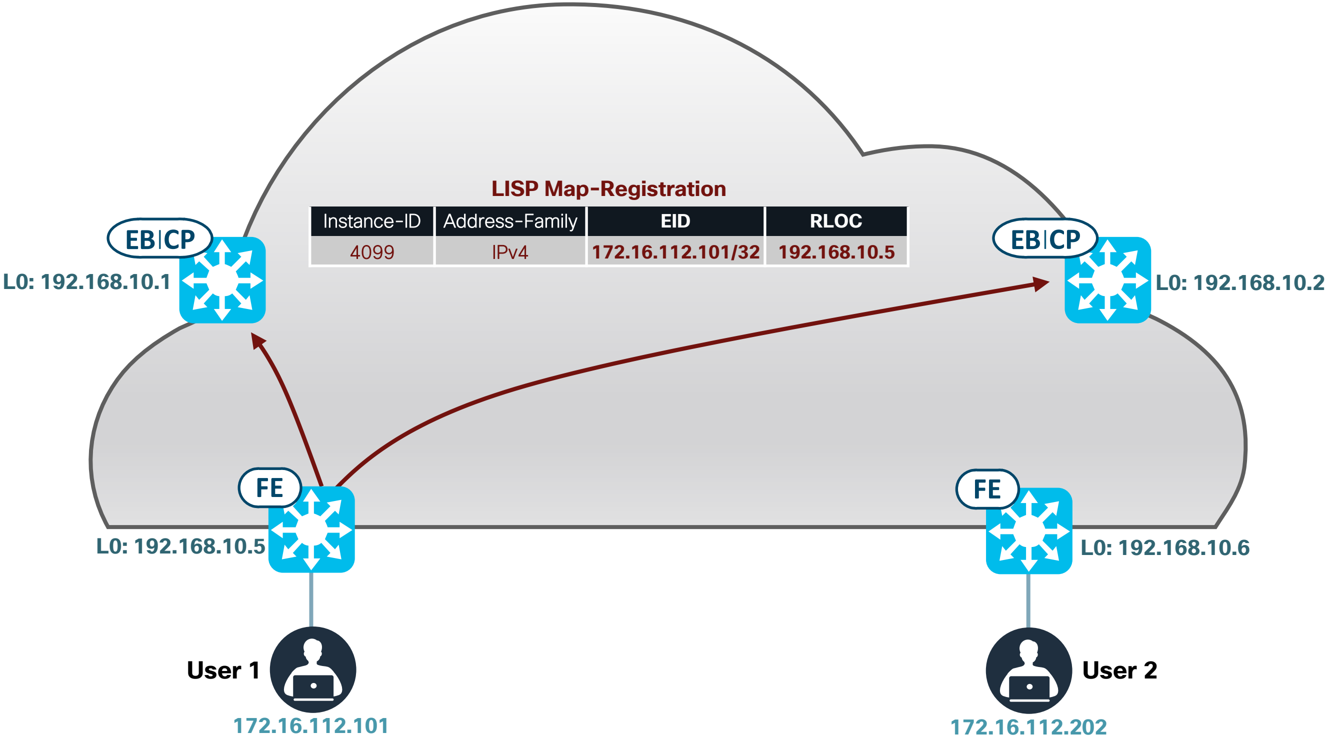


IID Table Publication

Instance-ID	Address-Family	EID	RLOC
4099	IPv4	172.16.112.101/32	192.168.10.5

LISP Pub/Sub

Registration and Publication – Within a Site

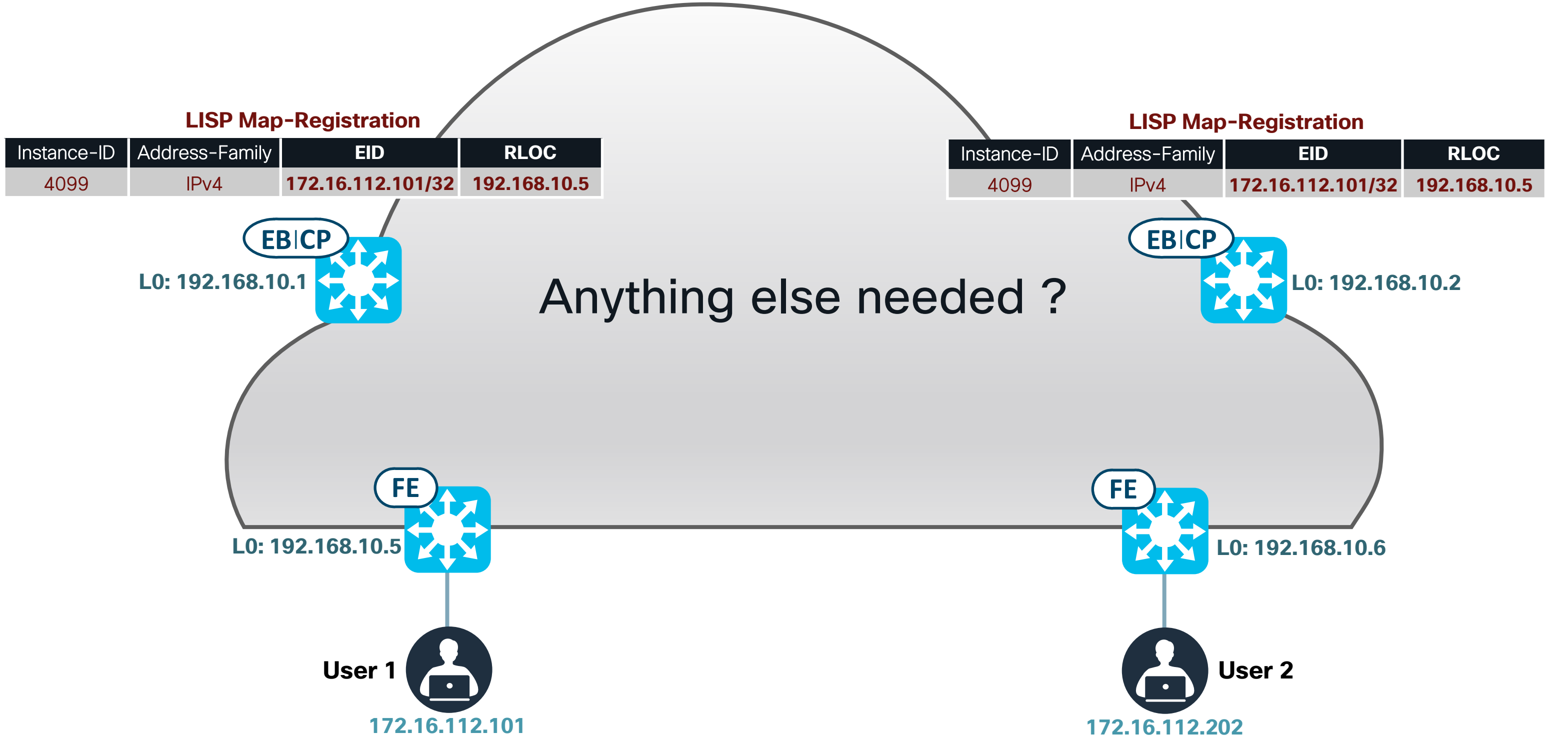


LISP Map-Registration

Instance-ID	Address-Family	EID	RLOC
4099	IPv4	172.16.112.101/32	192.168.10.5

LISP Pub/Sub

Registration and Publication – Within a Site



LISP Map-Registration

Instance-ID	Address-Family	EID	RLOC
4099	IPv4	172.16.112.101/32	192.168.10.5

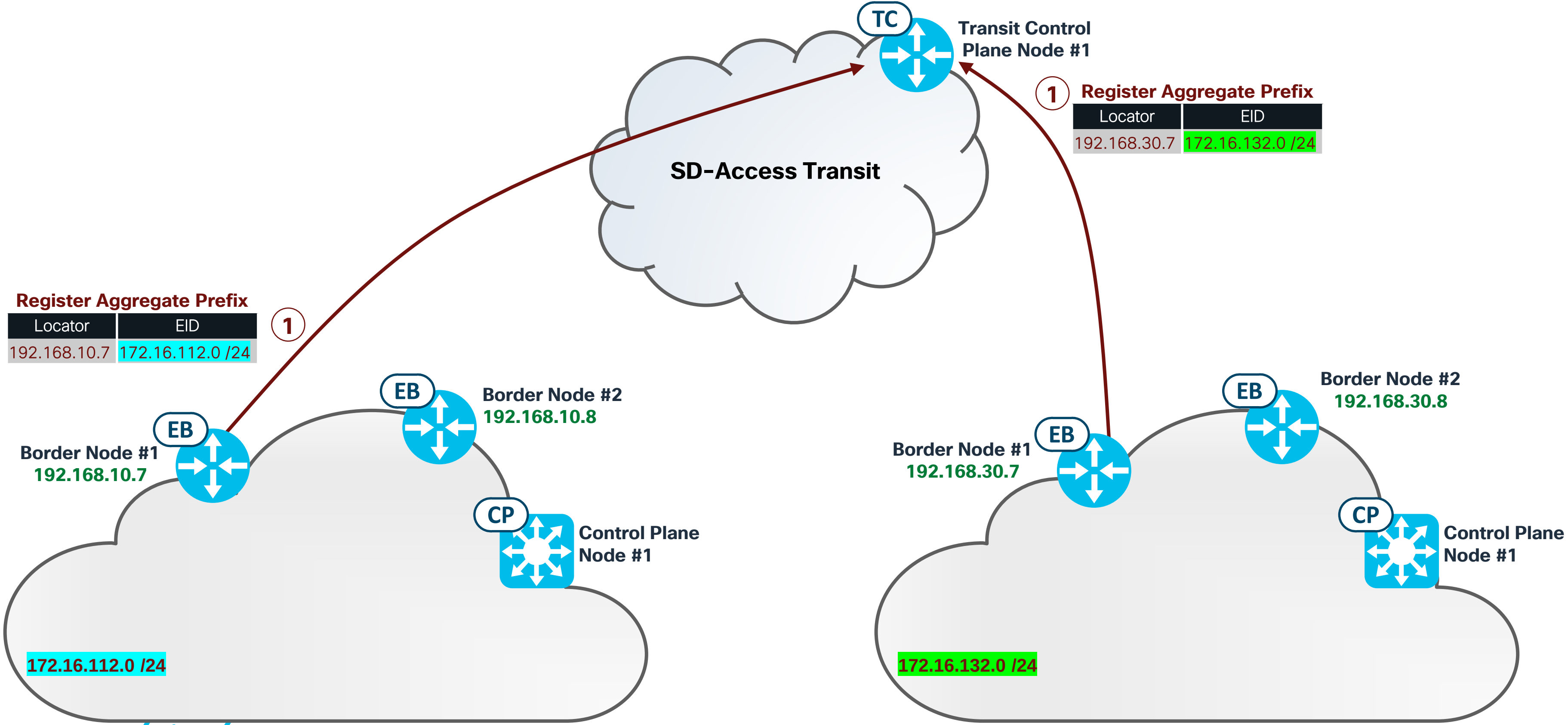
LISP Map-Registration

Instance-ID	Address-Family	EID	RLOC
4099	IPv4	172.16.112.101/32	192.168.10.5

Anything else needed ?

LISP Pub/Sub

Registration and Publication – SD-Access Transit



TC

Transit Control Plane Node #1

SD-Access Transit

1 Register Aggregate Prefix

Locator	EID
192.168.30.7	172.16.132.0 /24

Register Aggregate Prefix

Locator	EID
192.168.10.7	172.16.112.0 /24

1

EB

Border Node #1
192.168.10.7

EB

Border Node #2
192.168.10.8

CP

Control Plane Node #1

172.16.112.0 /24

EB

Border Node #1
192.168.30.7

EB

Border Node #2
192.168.30.8

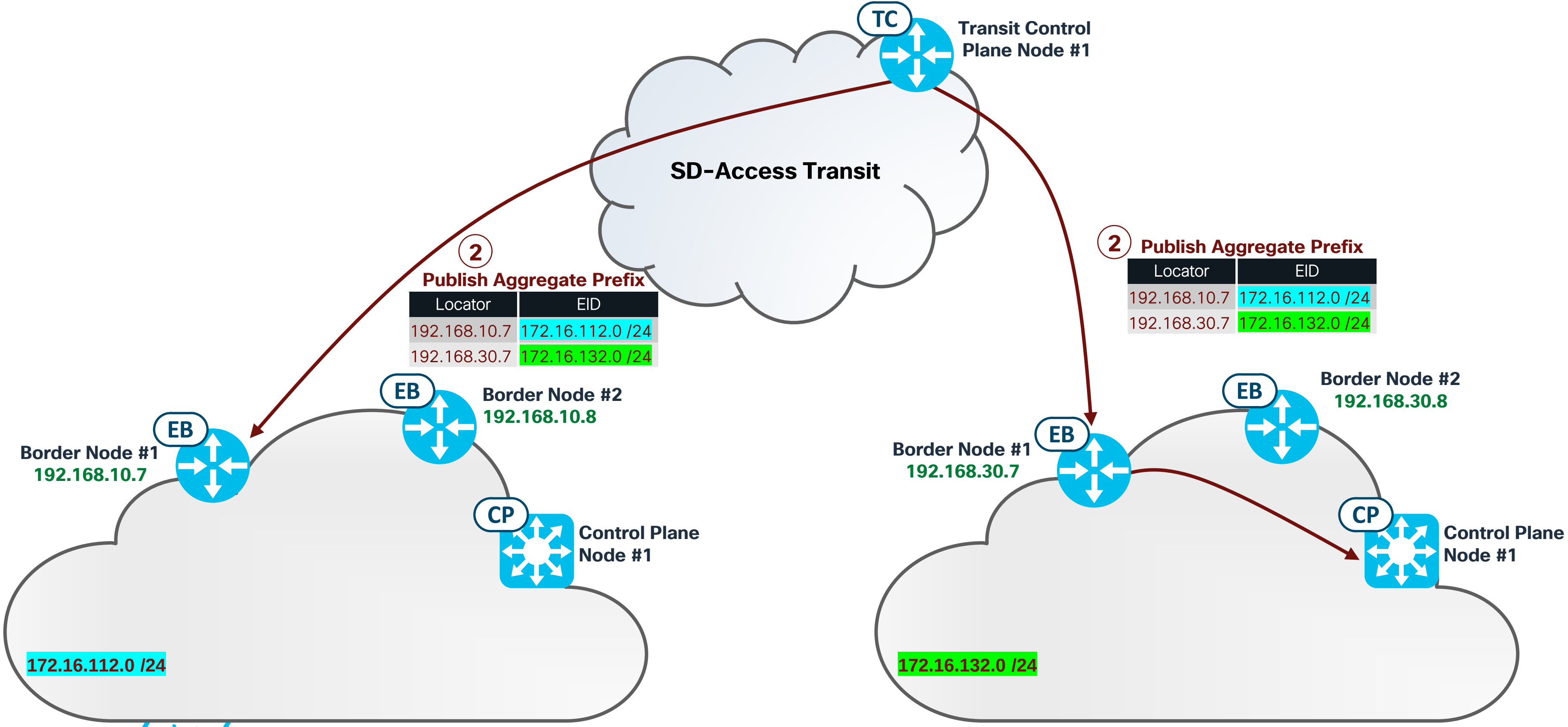
CP

Control Plane Node #1

172.16.132.0 /24

LISP Pub/Sub

Registration and Publication – SD-Access Transit



2 Publish Aggregate Prefix

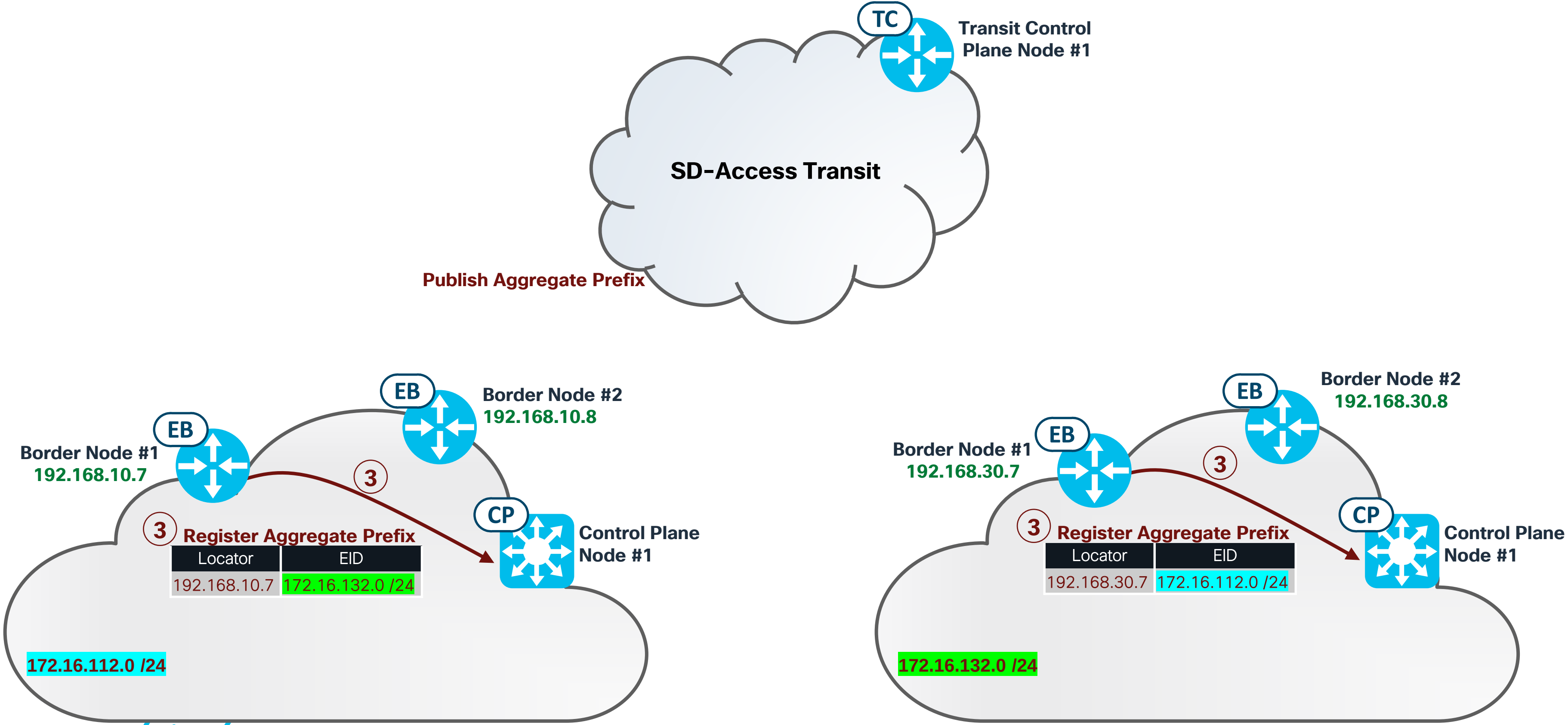
Locator	EID
192.168.10.7	172.16.112.0 /24
192.168.30.7	172.16.132.0 /24

2 Publish Aggregate Prefix

Locator	EID
192.168.10.7	172.16.112.0 /24
192.168.30.7	172.16.132.0 /24

LISP Pub/Sub

Registration and Publication – SD-Access Transit

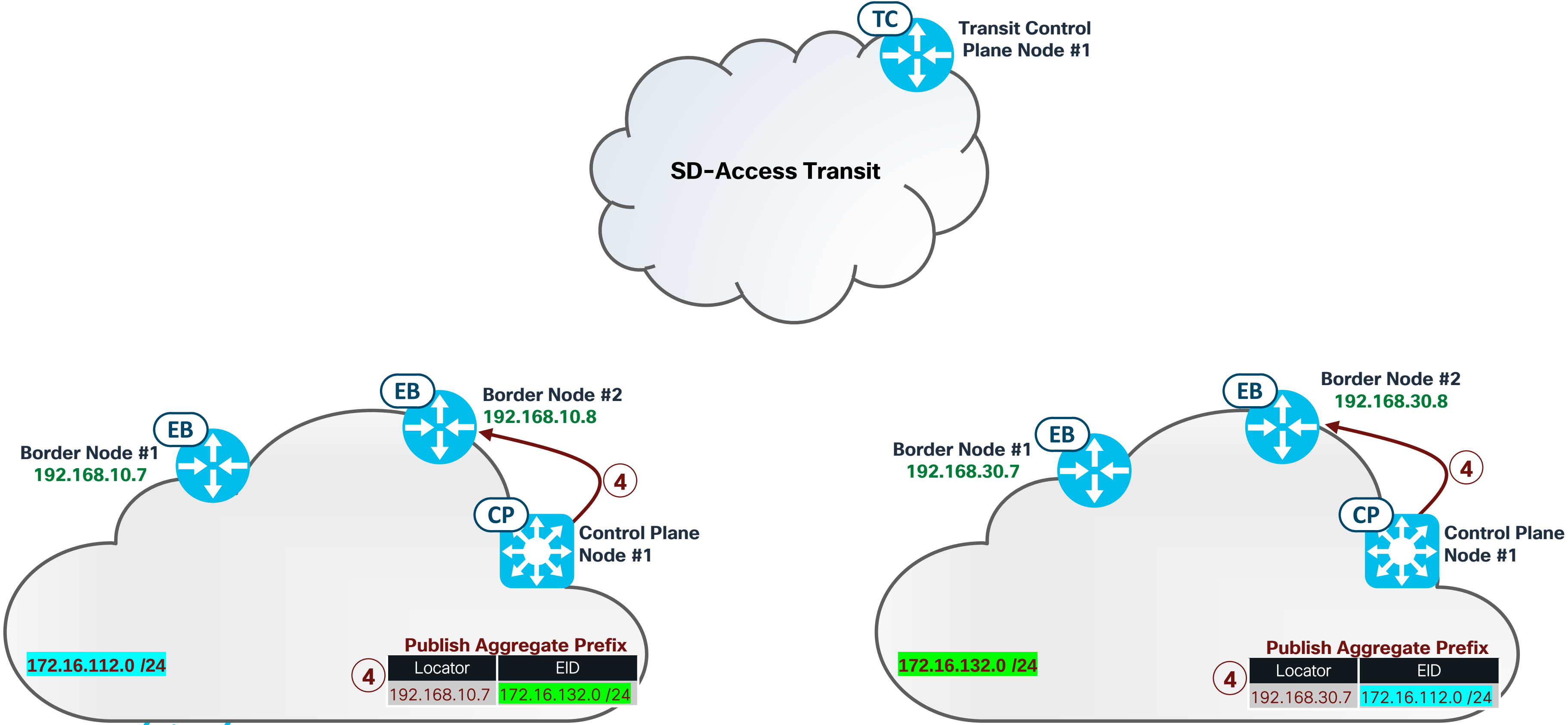


Locator	EID
192.168.10.7	172.16.132.0 /24

Locator	EID
192.168.30.7	172.16.112.0 /24

LISP Pub/Sub

Registration and Publication – SD-Access Transit



Publish Aggregate Prefix

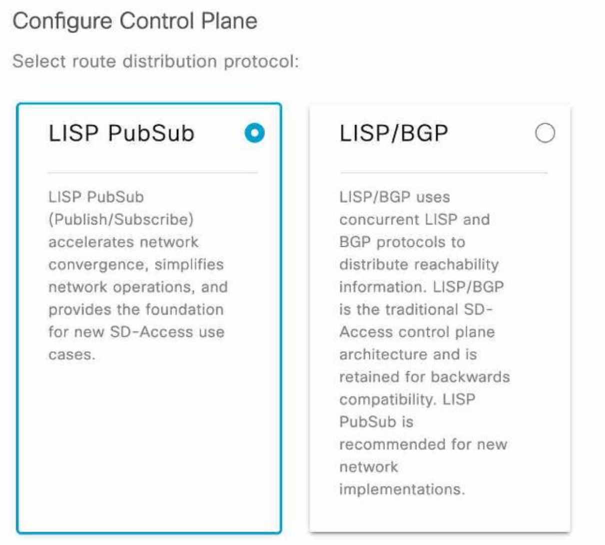
Locator	EID
192.168.10.7	172.16.132.0 /24

Publish Aggregate Prefix

Locator	EID
192.168.30.7	172.16.112.0 /24

LISP Pub/Sub

Enabling in DNA Center



Configure Control Plane

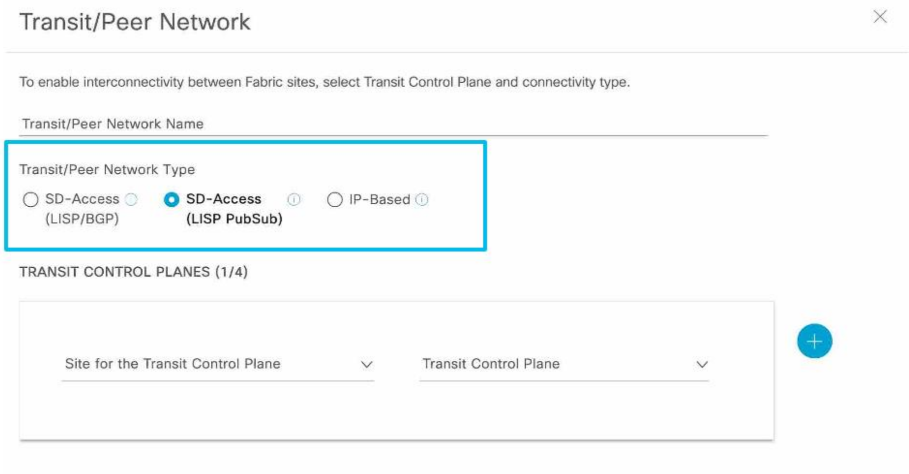
Select route distribution protocol:

LISP PubSub ●

LISP PubSub (Publish/Subscribe) accelerates network convergence, simplifies network operations, and provides the foundation for new SD-Access use cases.

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 PubSub is recommended for new network implementations.



Transit/Peer Network

To enable interconnectivity between Fabric sites, select Transit Control Plane and connectivity type.

Transit/Peer Network Name

Transit/Peer Network Type

○ SD-Access (LISP/BGP) ● **SD-Access (LISP PubSub)** ○ IP-Based

TRANSIT CONTROL PLANES (1/4)

Site for the Transit Control Plane

Transit Control Plane

- LISP Pub/Sub can be enabled when adding Control Plane node/s to fabric.
- We can have up to 4 Transit Control Plane Nodes with LISP Pub/Sub-based fabrics.

LISP PubSub

Design Considerations

Software Requirements

- IOS XE 17.6.1 or newer
- DNA Center 2.2.3.3 or newer

Hardware Requirements

- Any supported Control Plan Node that can run IOS XE 17.6.1 or newer

Site Requirements

- Supported for only newly created sites
- Upgrade of existing sites planned

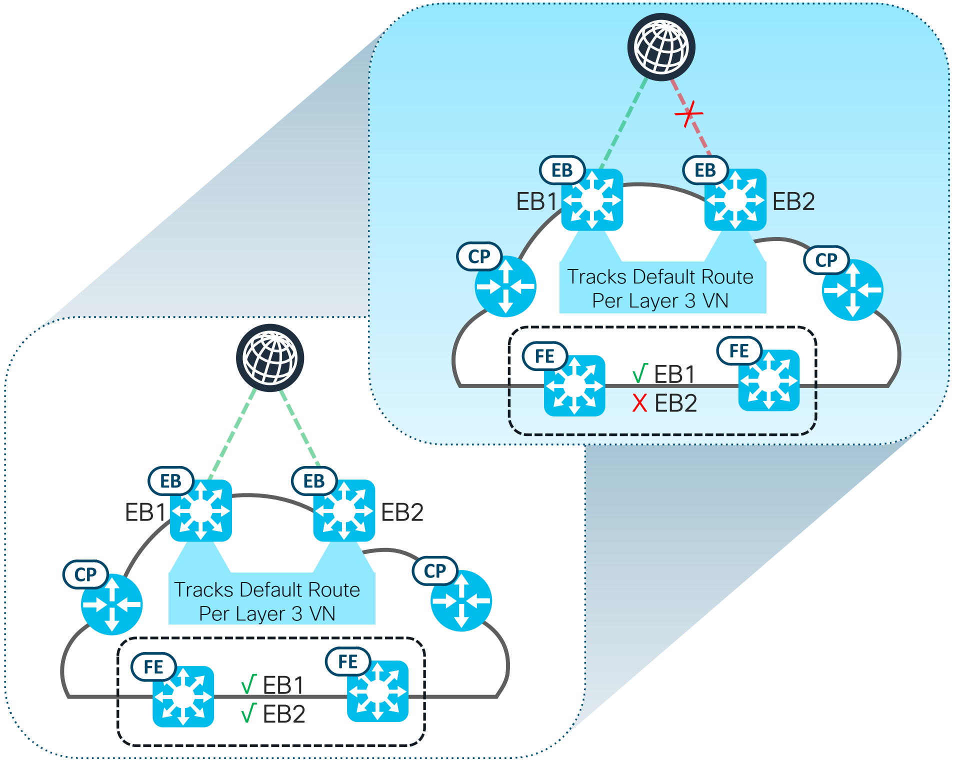
Transit Requirements

- All SD-Access Transit sites must be the same LISP type
- IP Transit sites can be a mix of LISP types

LISP PubSub

With Dynamic Default Border

- External Border/s within a fabric site registers the default route with local/transit Control Plane node/s.
- When hosts want to reach out to Internet/unknown prefixes, Fabric Edge nodes will send map-request to Control Plane node/s which replies with RLOC of External Border node/s which has default route registered with Control Plane node/s.
- When the upstream link to External Border node/s goes down (default route is removed from rib), that Border will send an update to Control plane node/s that default route is no more available, and uplink is down
- Also, at the same time for the actively received internet traffic Border sends a LISP message requesting Fabric Edges to update their map-cache entries
- Then, Fabric Edge node/s will send map-request to Control Plane node/s to get updated information on External Border node/s with active default route/s and traffic is dynamically converged.

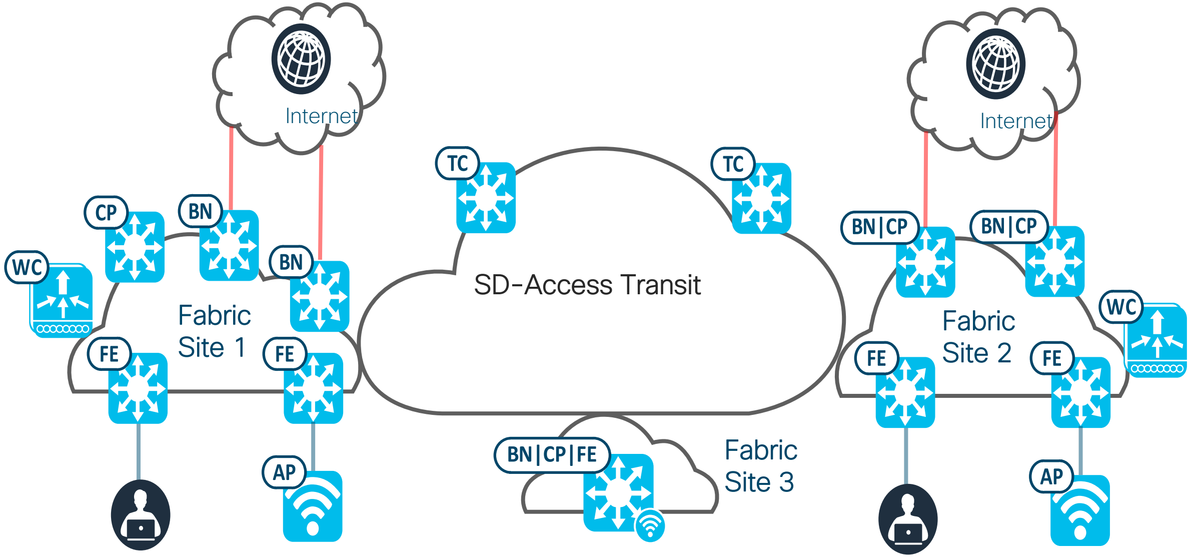

EB
EB1
EB
EB2
CP
Tracks Default Route Per Layer 3 VN
CP
FE
√ EB1
X EB2
FE
EB
EB1
EB
EB2
CP
Tracks Default Route Per Layer 3 VN
CP
FE
√ EB1
√ EB2
FE

LISP PubSub

Backup Internet

- Publishers : Transit/Control Plane Nodes
- Subscribes : Borders Nodes

- With LISP Pub/Sub, fabric sites with local internet connectivity connected via SD-Access transit can act as backup for other sites with Internet access.
  - E.g.: Fabric sites 1, 2 can act as backup internet access for each other.
  - Fabric Site 3 with no local Internet access will load balance and share internet between sites 1,2.
  - Sites with local internet connectivity will prefer the local connectivity over the remote connectivity

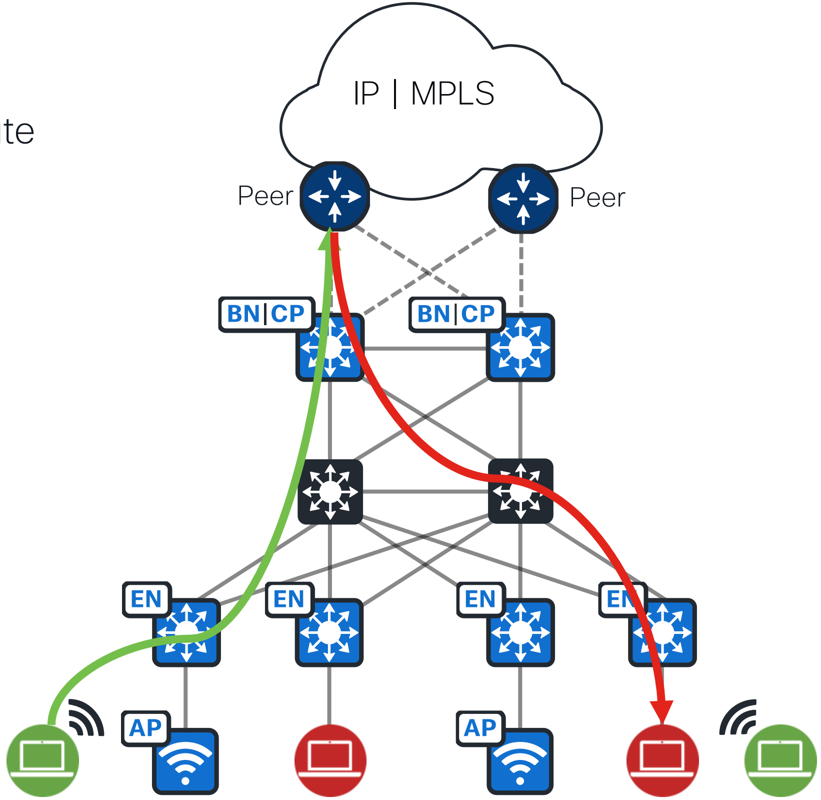


SD-Access Extranet

SD-Access Extranet

Shared Services Challenges with existing Architecture

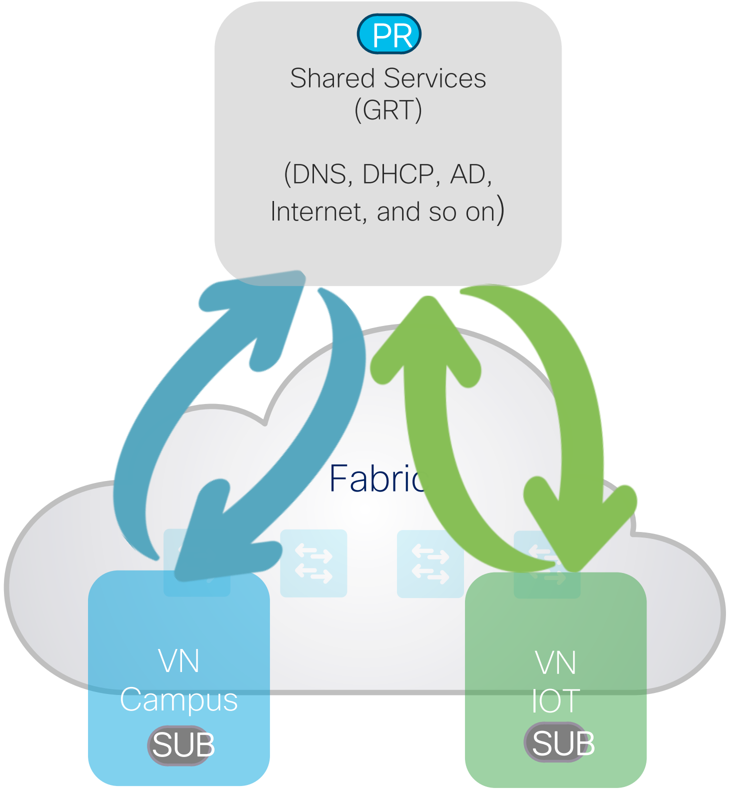
- Manual Route Leaking configurations using Route Targets can be complex
- Peer resource consideration
- Traffic Hair pinning across Peer device
- Peer throughput could be a bottleneck



SD-Access Extranet

Global Routing Table Use Case

VN/VRF/IID → GRT



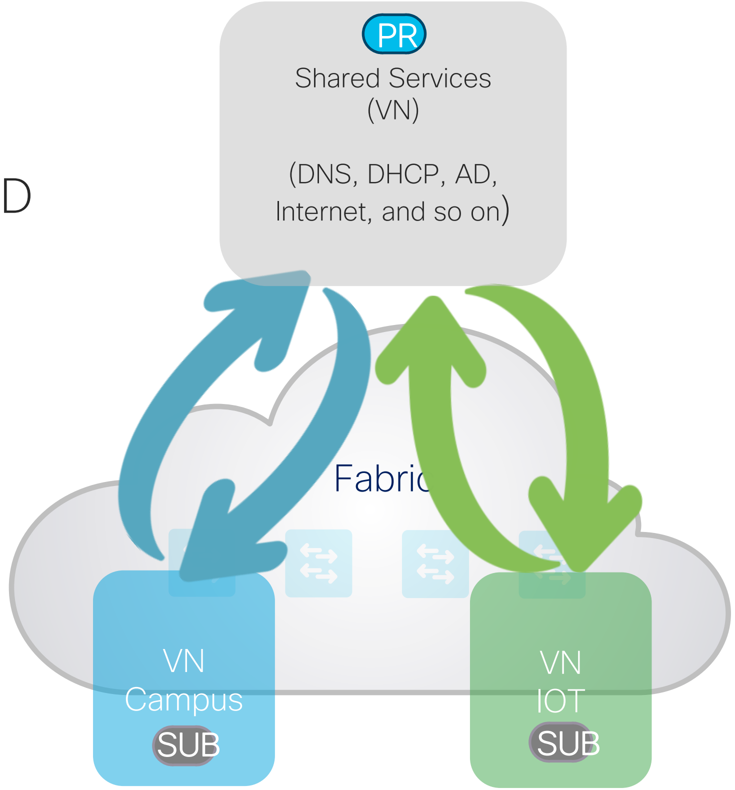
PR Provider VN

SUB Subscriber VN

SD-Access Extranet

Any Virtual Network Use Case

VN/VRF/IID → VN/VRF/IID



PR Provider VN

SUB Subscriber VN

SD-Access Extranet

Design Considerations

SD-Access Extranet policy:

VN Policy	Provider VN	Subscriber VN
Provider VN	NO	YES
Subscriber VN	YES	NO

Traffic between clients in Provider VNs is dropped, even if allowed by a policy outside the Fabric Site.

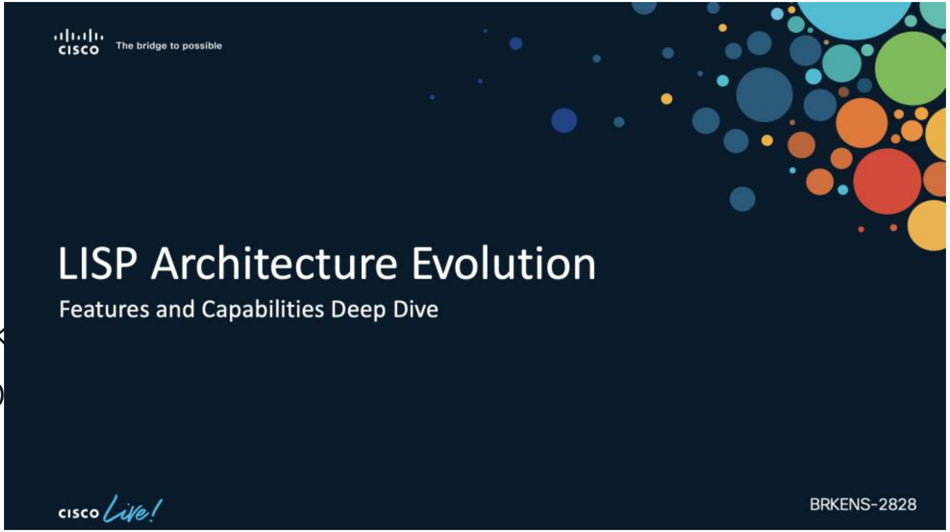
Would you like to know more?

Check out the following session:

BRKENS-2828

LISP Architecture Evolution

This session is a deeper dive into LIS
Pub/Sub , Border Convergence, Back
Internet, SD-Access Extranet and mo



LISP Architecture Evolution

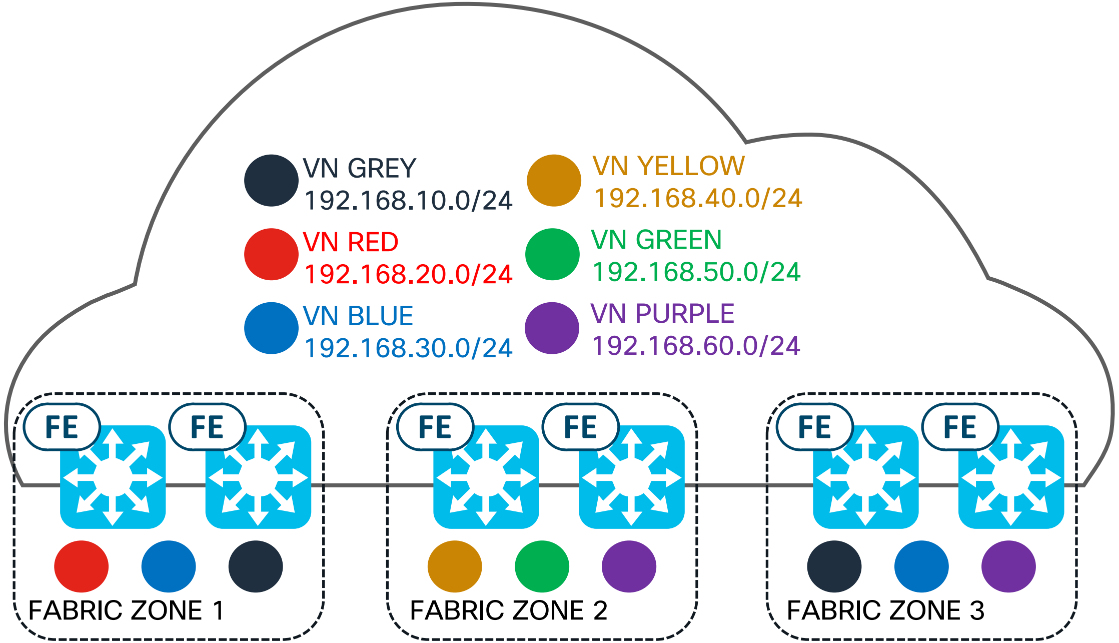
Features and Capabilities Deep Dive

BRKENS-2828

Fabric Zones

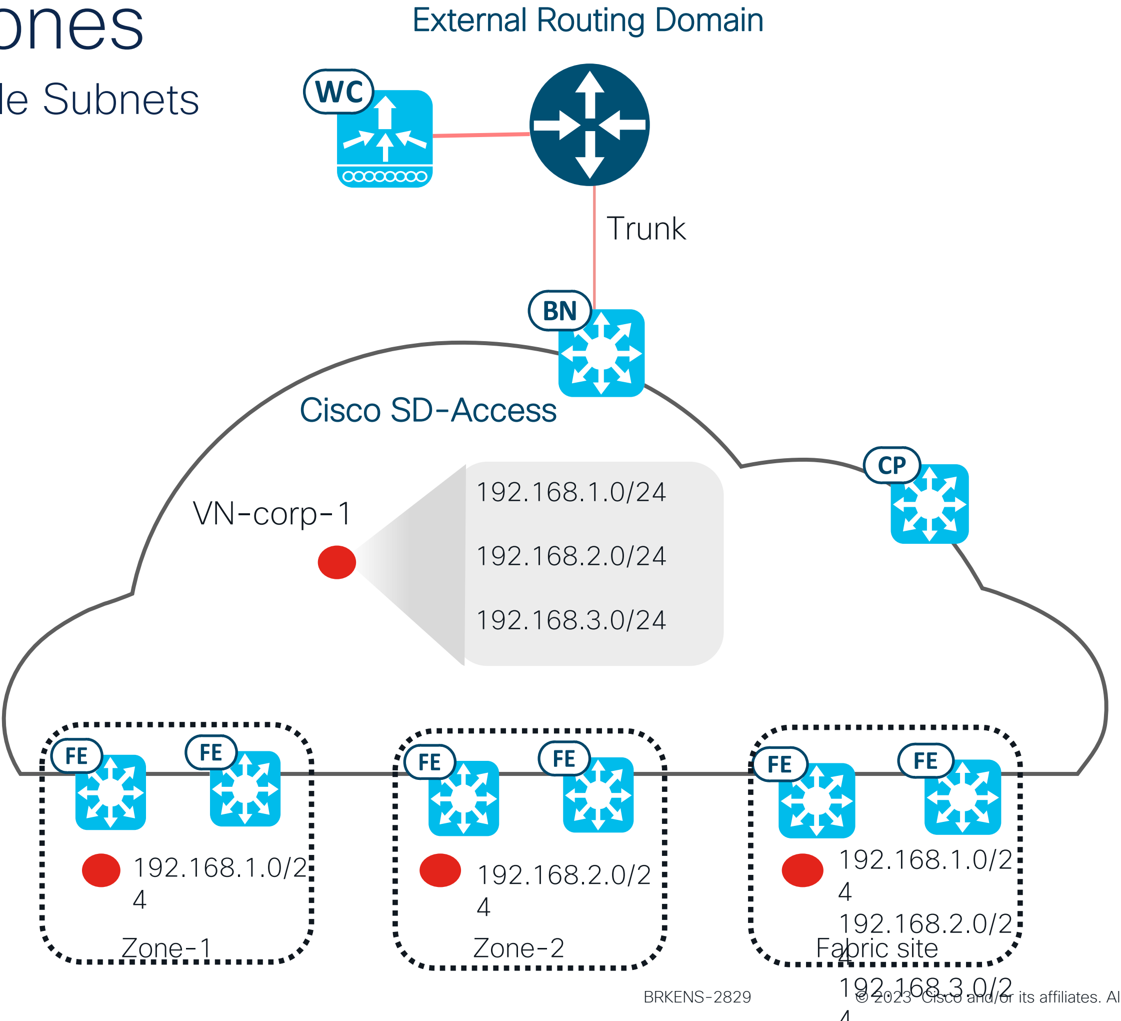
Fabric Zones

Overview



Fabric Zones

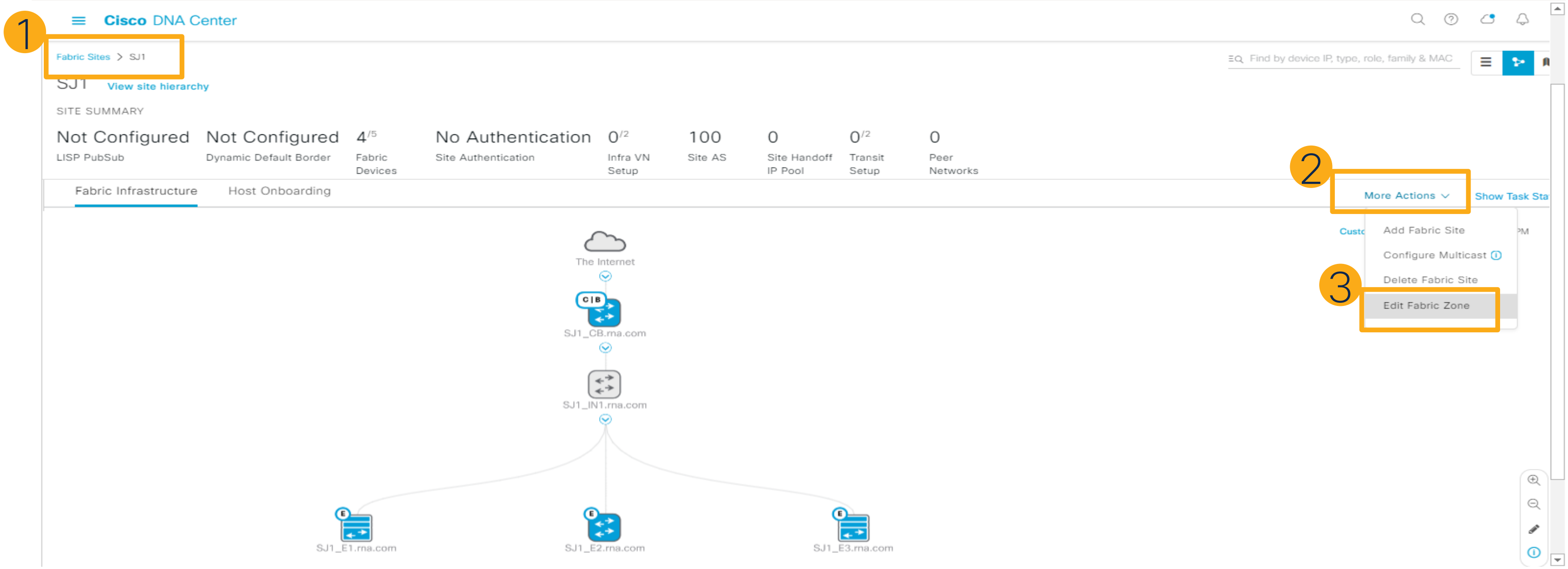
One VN, Multiple Subnets



Fabric Zones

Adding to Existing Fabric Sites

- ❑ Step 1: Edit Fabric Zone
  - ➢Provision → Fabric Sites → More Actions → Edit Fabric Zone



Fabric Sites > SJ1

SJ1 View site hierarchy

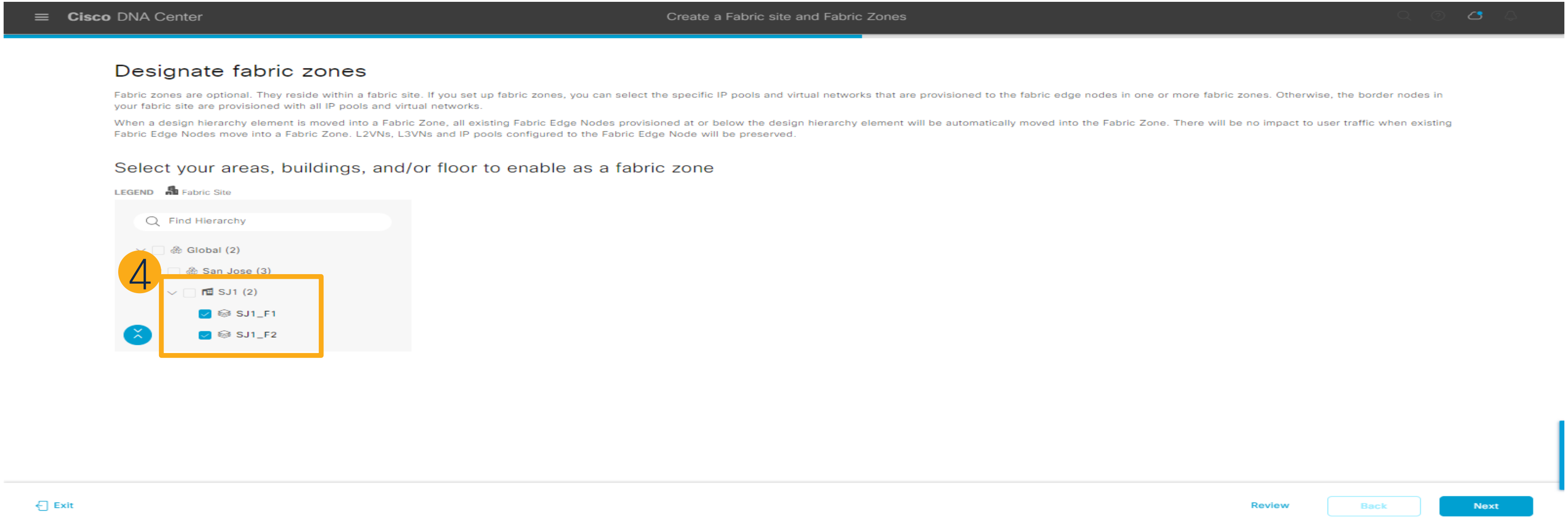
SITE SUMMARY

Not Configured	Not Configured	4/5	No Authentication	0/2	100	0	0/2	0
LISP PubSub	Dynamic Default Border	Fabric Devices	Site Authentication	Infra VN Setup	Site AS	Site Handoff IP Pool	Transit Setup	Peer Networks

Fabric Zones

Adding to Existing Fabric Sites

- ❑ Step 2: Designate Fabric Zones based on design hierarchy
  - ➢Select areas, buildings and/or floors



Designate fabric zones

Fabric zones are optional. They reside within a fabric site. If you set up fabric zones, you can select the specific IP pools and virtual networks that are provisioned to the fabric edge nodes in one or more fabric zones. Otherwise, the border nodes in your fabric site are provisioned with all IP pools and virtual networks.

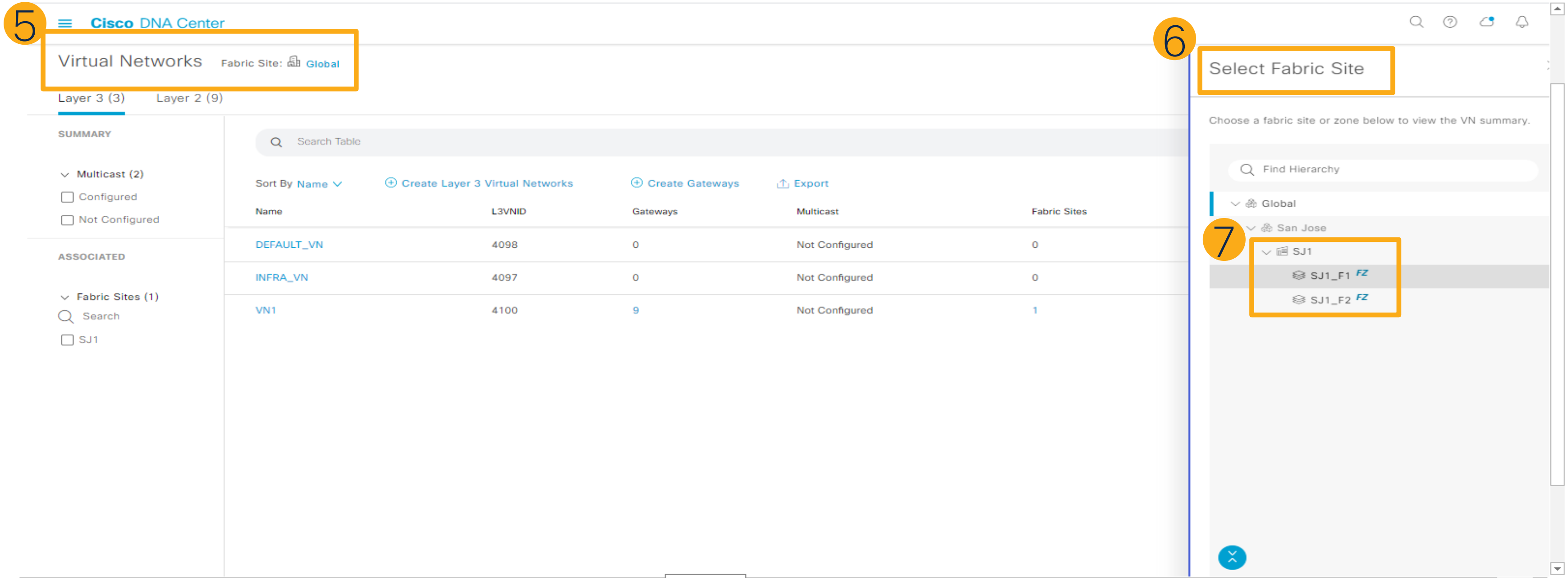
When a design hierarchy element is moved into a Fabric Zone, all existing Fabric Edge Nodes provisioned at or below the design hierarchy element will be automatically moved into the Fabric Zone. There will be no impact to user traffic when existing Fabric Edge Nodes move into a Fabric Zone. L2VNs, L3VNs and IP pools configured to the Fabric Edge Node will be preserved.

Select your areas, buildings, and/or floor to enable as a fabric zone

Fabric Zones

Adding to Existing Fabric Sites

- ❑ Step 3: Select Fabric Zone Virtual Network
  - ➢Provision → Virtual Networks → Select Fabric Site



Virtual Networks Fabric Site: Global

Layer 3 (3) Layer 2 (9)

SUMMARY

Multicast (2)
☐ Configured
☐ Not Configured

ASSOCIATED

Fabric Sites (1)
Search
☐ SJ1

Search Table

Sort By Name ⌄ ⊕ Create Layer 3 Virtual Networks ⊕ Create Gateways Export

Name	L3VNID	Gateways	Multicast	Fabric Sites
DEFAULT_VN	4098	0	Not Configured	0
INFRA_VN	4097	0	Not Configured	0
VN1	4100	9	Not Configured	1

Select Fabric Site

Choose a fabric site or zone below to view the VN summary.

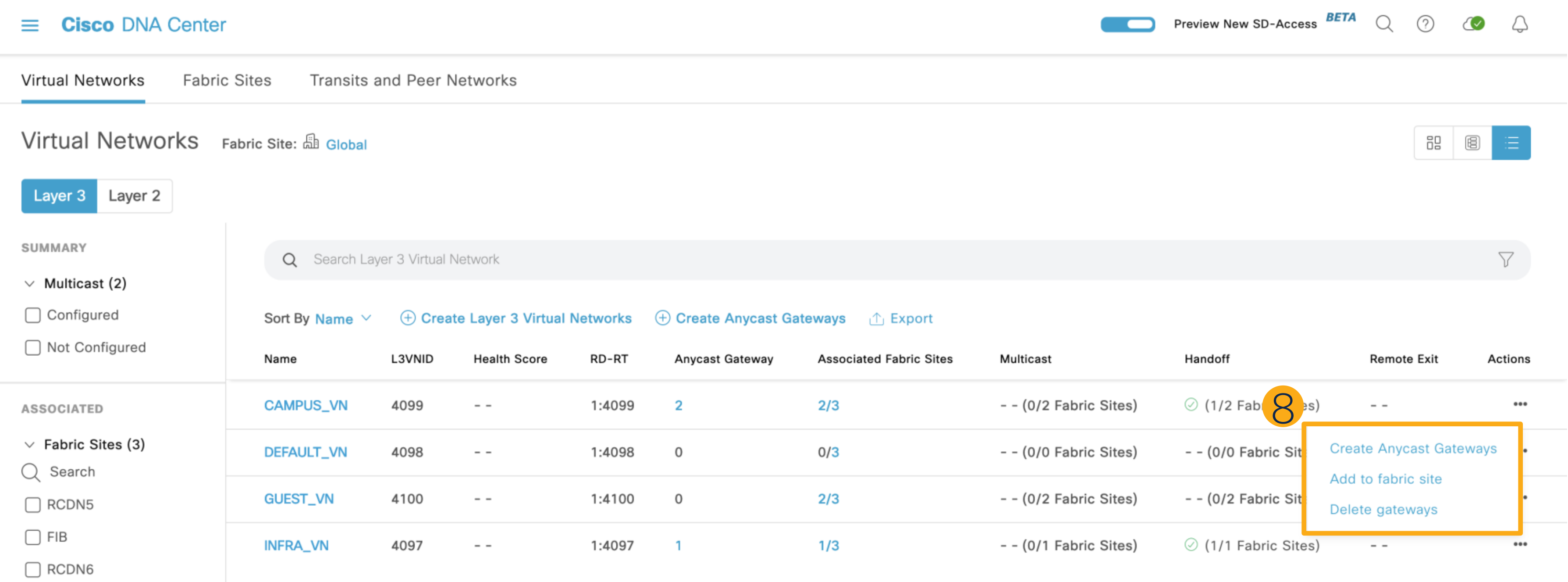
Find Hierarchy

- Global
  - San Jose
    - SJ1
      - SJ1_F1 FZ
      - SJ1_F2 FZ

Fabric Zones

Adding to Existing Fabric Sites

- ❑ Step 4: Edit L2/L3 VN and Gateways
    - ➢ Add Layer 2/Layer 3 VN and Create/Delete Gateways



Virtual Networks Fabric Site: Global

SUMMARY

- Multicast (2)
  - □ Configured
  - □ Not Configured

ASSOCIATED

- Fabric Sites (3)
  - Search
  - □ RCDN5
  - □ FIB
  - □ RCDN6

Search Layer 3 Virtual Network

Sort By Name ⊕ Create Layer 3 Virtual Networks ⊕ Create Anycast Gateways Export

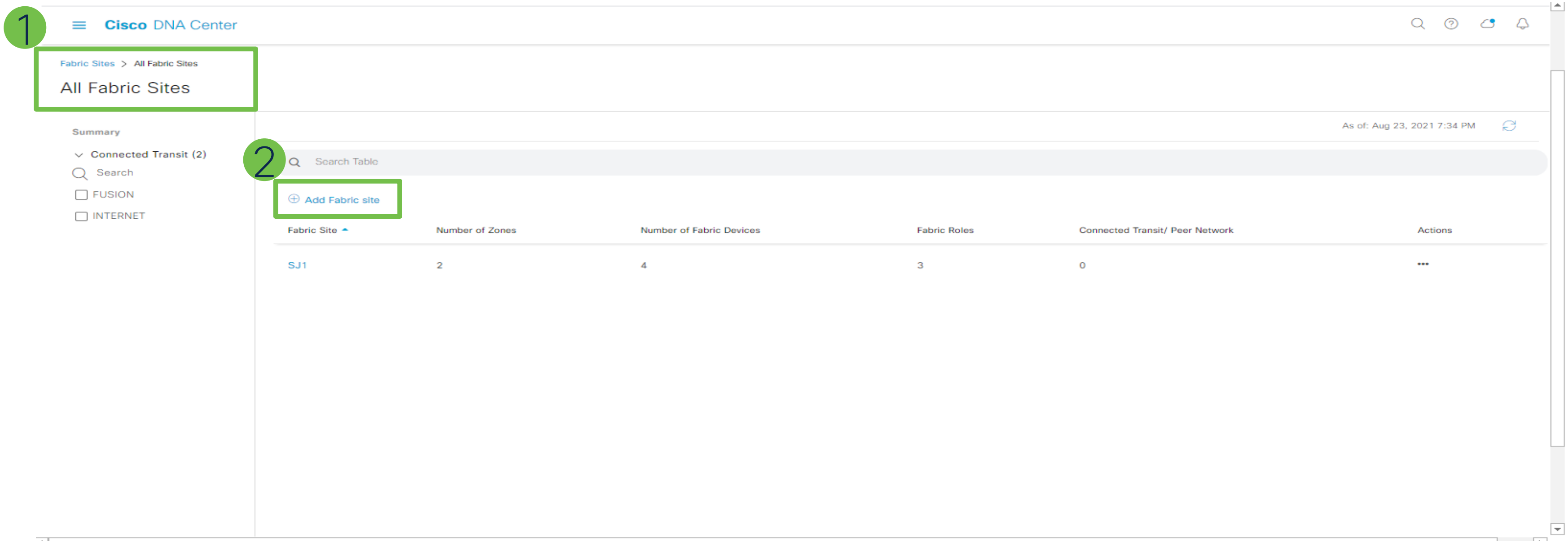
Name	L3VNID	Health Score	RD-RT	Anycast Gateway	Associated Fabric Sites	Multicast	Handoff	Remote Exit	Actions
CAMPUS_VN	4099	- -	1:4099	2	2/3	- - (0/2 Fabric Sites)	✓ (1/2 Fab es)	- -	•••
DEFAULT_VN	4098	- -	1:4098	0	0/3	- - (0/0 Fabric Sites)	- - (0/0 Fabric Sit		•
GUEST_VN	4100	- -	1:4100	0	2/3	- - (0/2 Fabric Sites)	- - (0/2 Fabric Sit		•
INFRA_VN	4097	- -	1:4097	1	1/3	- - (0/1 Fabric Sites)	✓ (1/1 Fabric Sites)	- -	•••

- Create Anycast Gateways
- Add to fabric site
- Delete gateways

Fabric Zones

Adding to New Fabric Sites

- ❑ Step 1: Add Fabric site
  - ➢Provision → Fabric Sites → All Fabric Sites → Add Fabric Site



Fabric Sites > All Fabric Sites

All Fabric Sites

Summary

- Connected Transit (2)
- Search
- □ FUSION
- □ INTERNET

As of: Aug 23, 2021 7:34 PM

Search Table

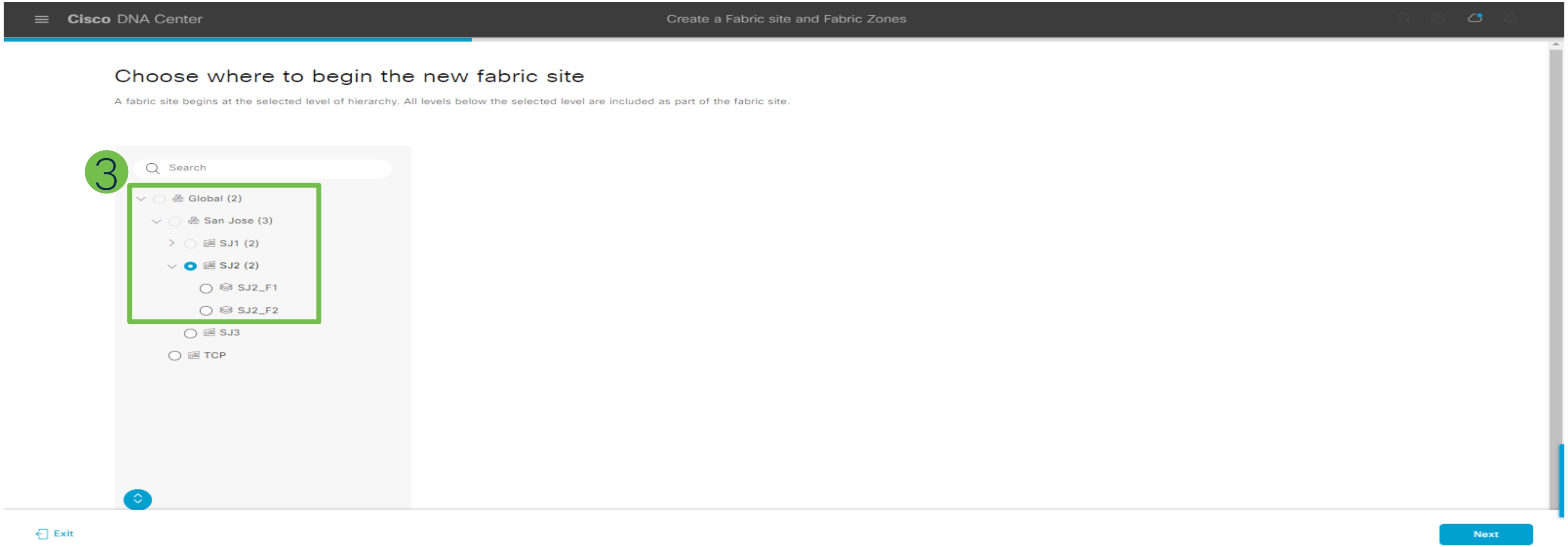
⊕ Add Fabric site

Fabric Site ▲	Number of Zones	Number of Fabric Devices	Fabric Roles	Connected Transit/ Peer Network	Actions
SJ1	2	4	3	0	•••

Fabric Zones

Adding to New Fabric Sites

- ❑ Step 2: Choose new Fabric Site
  - ➢Select level of hierarchy as part of new Fabric Site



Choose where to begin the new fabric site

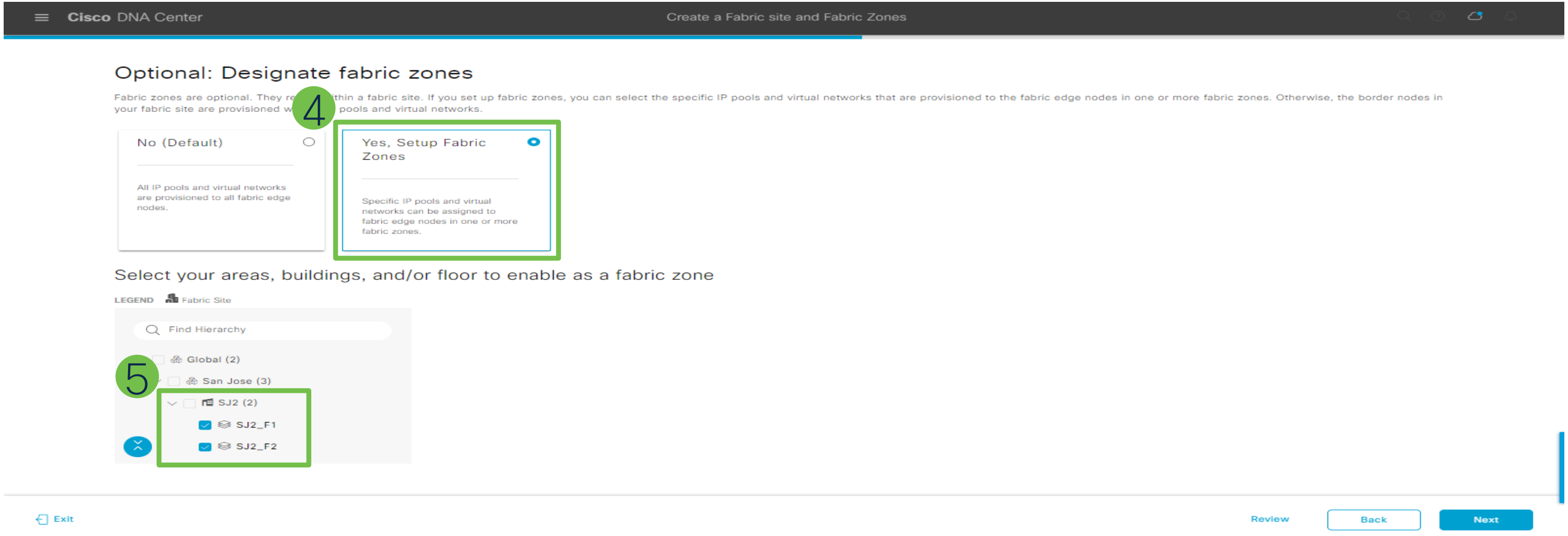
A fabric site begins at the selected level of hierarchy. All levels below the selected level are included as part of the fabric site.

- ○ Global (2)
  - ○ San Jose (3)
    - ○ SJ1 (2)
    - ● SJ2 (2)
      - ○ SJ2_F1
      - ○ SJ2_F2
    - ○ SJ3
  - ○ TCP

Fabric Zones

Adding to New Fabric Sites

- ❑ Step 3: Designate Fabric Zones
  - ➢Enable Fabric Zones and Select area, building and/or floor



Optional: Designate fabric zones

Fabric zones are optional. They re thin a fabric site. If you set up fabric zones, you can select the specific IP pools and virtual networks that are provisioned to the fabric edge nodes in one or more fabric zones. Otherwise, the border nodes in your fabric site are provisioned w pools and virtual networks.

4

○ No (Default)

All IP pools and virtual networks are provisioned to all fabric edge nodes.

● Yes, Setup Fabric Zones

Specific IP pools and virtual networks can be assigned to fabric edge nodes in one or more fabric zones.

Select your areas, buildings, and/or floor to enable as a fabric zone

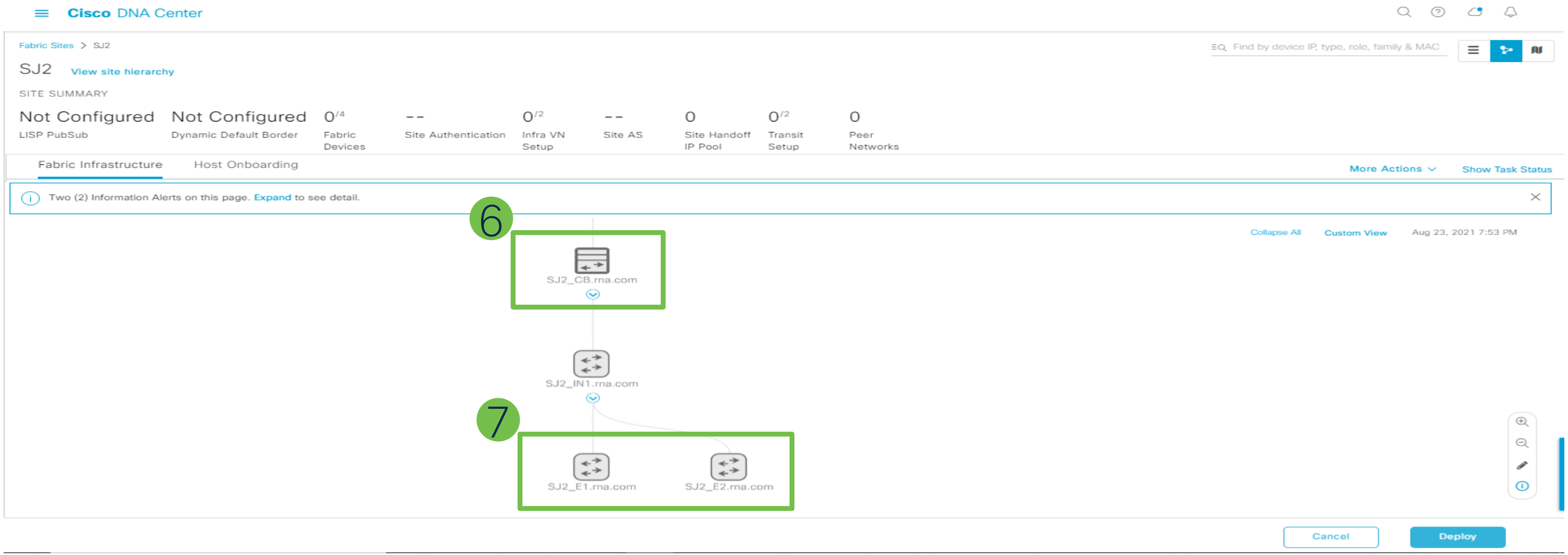
5

- □ Global (2)
  - □ San Jose (3)
    - □ SJ2 (2)
      - ☑ SJ2_F1
      - ☑ SJ2_F2

Fabric Zones

Adding to New Fabric Sites

- Step 4: Enable Fabric nodes at Fabric Site and Fabric Zone
  - Enable CP and Border at Fabric Site and Fabric Zones at Edge Nodes



Cisco DNA Center

Fabric Sites > SJ2

SJ2 View site hierarchy

SITE SUMMARY

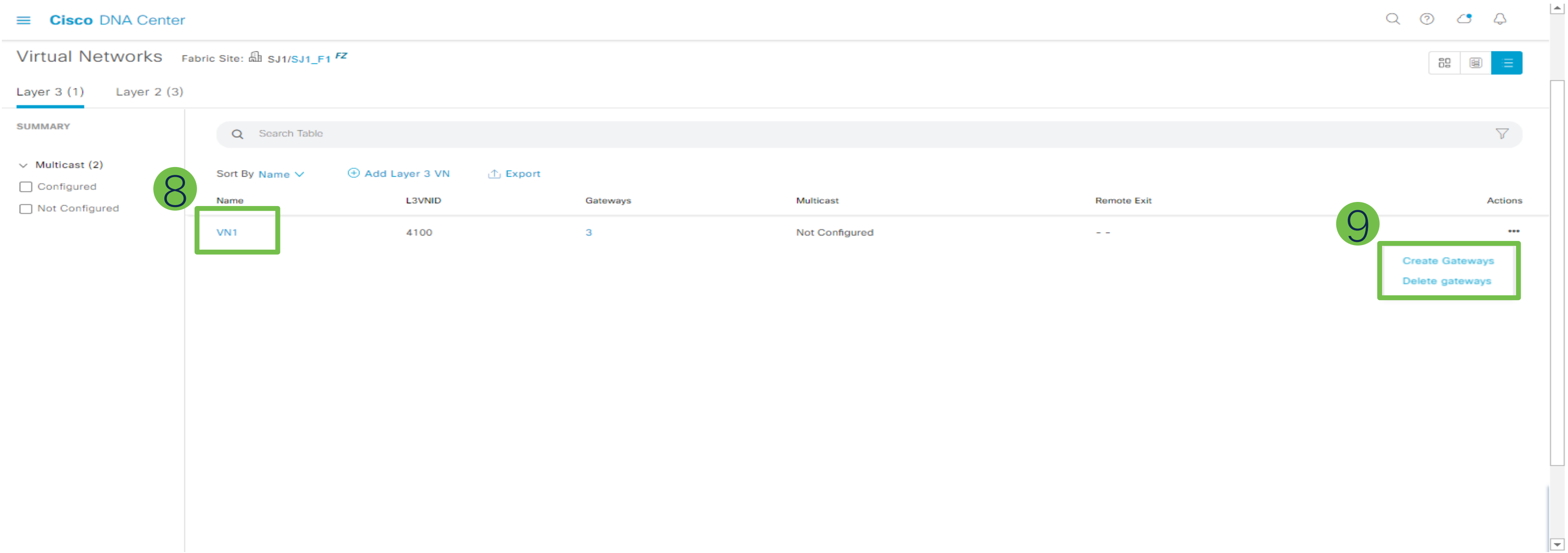
Not Configured	Not Configured	0/4	--	0/2	--	0	0/2	0
LISP PubSub	Dynamic Default Border	Fabric Devices	Site Authentication	Infra VN Setup	Site AS	Site Handoff IP Pool	Transit Setup	Peer Networks

Two (2) Information Alerts on this page. Expand to see detail.

Fabric Zones

Adding to New Fabric Sites

- ❑ Step 5: Select Virtual Network of a Fabric Zone
  - ➤Add VN and Create Gateways at Fabric Site and Fabric Zones



Virtual Networks Fabric Site: SJ1/SJ1_F1 FZ

Layer 3 (1) Layer 2 (3)

SUMMARY

Multicast (2)

□ Configured

□ Not Configured

Search Table

Sort By Name ∨ ⊕ Add Layer 3 VN Export

Name	L3VNID	Gateways	Multicast	Remote Exit	Actions
VN1	4100	3	Not Configured	- -	•••

Create Gateways

Delete gateways

Border Node Preference

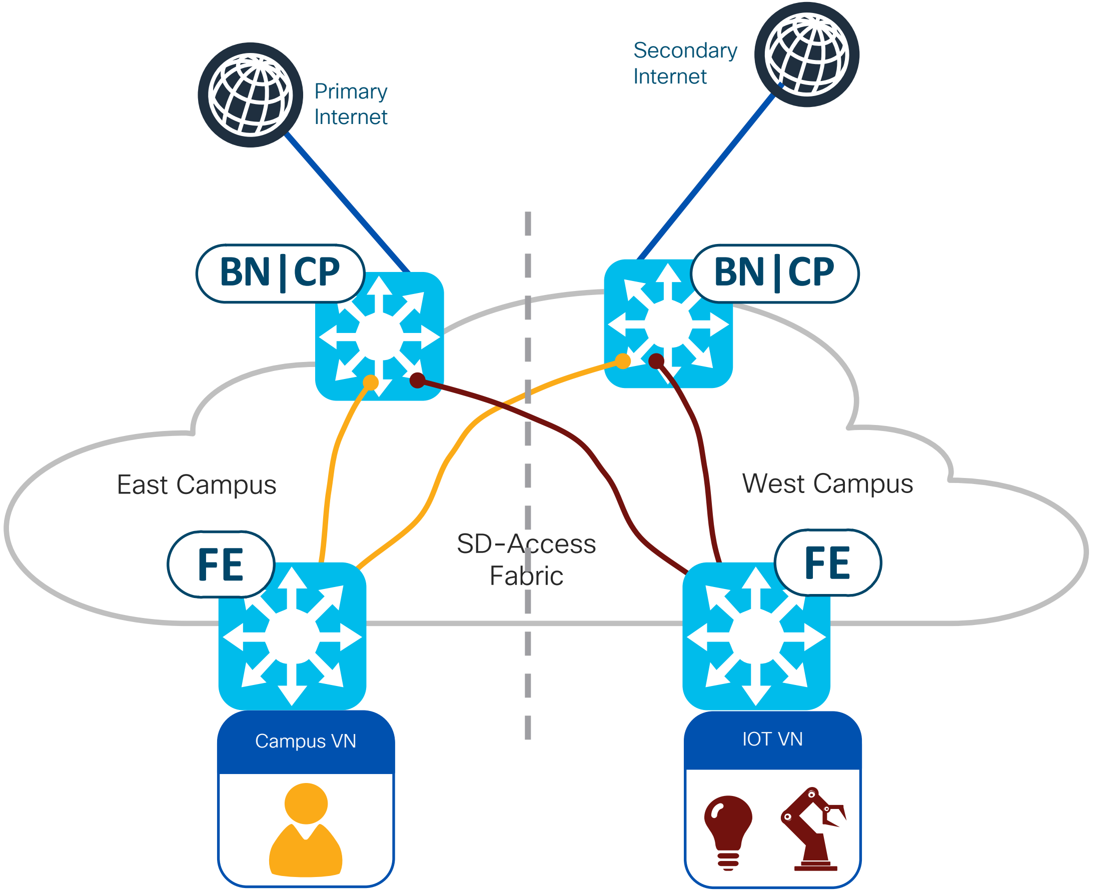
Border Node Preference in Fabric

Without Preference

All traffic from all Virtual Networks is load balanced across all Borders within a site.

Traffic may be routed to a border that then needs to send traffic back to another border, resulting in sub-optimal traffic pathing and more challenging troubleshooting.

Software upgrades can be disruptive without the ability to gracefully move traffic.



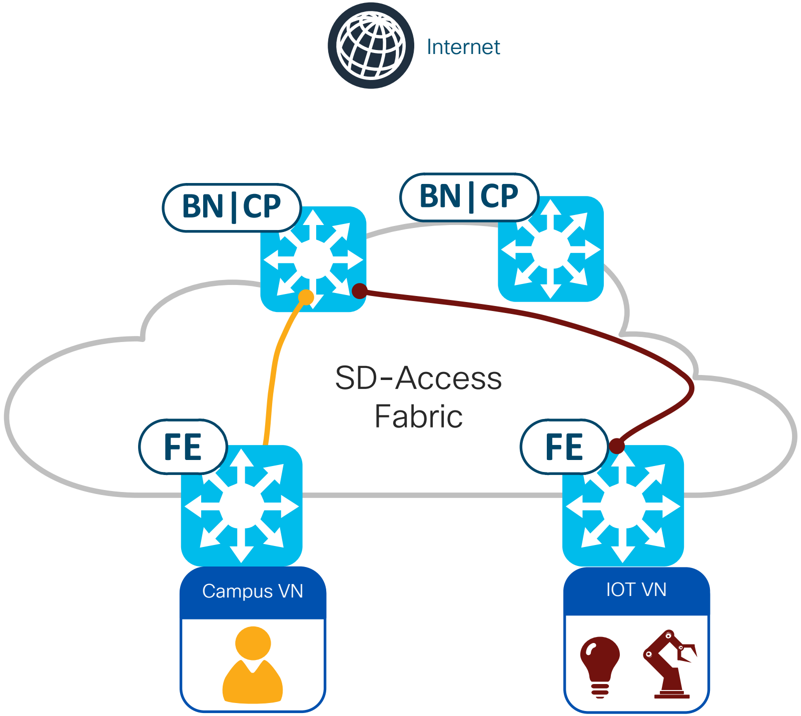
Border Node Preference in Fabric

Use Case

- Traffic egressing a fabric site via a Border of choice gives customers flexibility in deploying their Cisco SD-Access networks as their sites might be connected to high bandwidth circuits or border nodes located in different datacenters.

Details

- Cisco DNA Center provides users with an option to select a border node to route your network traffic. If your network is configured with more than one border, you can set a priority value for each border node. Traffic is routed through the border node that has the lowest priority.
- Users can set the priority values between 1 and 9 (1 is the highest priority and 9 is the lowest. Lower number is the preferred Border).
- By default (if user do not set a priority value), the border is assigned a priority value of 10. If border priorities are not set (or same across Borders), traffic is load balanced across the border nodes.
- User can modify border node priority in Day N without removing devices from fabric.



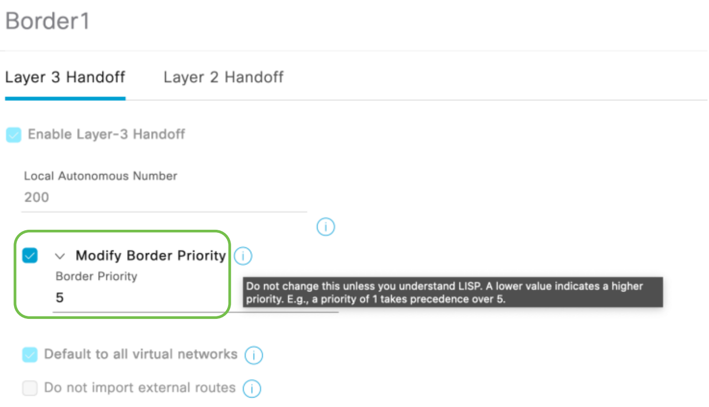
Border Node Preference in Fabric

Details

- The priority value set for a border is applicable to all the virtual networks that are handed-off from that border. Border priority is supported for both unicast and multicast traffic.
- If an SD-Access Transit interconnects the fabric sites, an external border with the Lowest priority is chosen to send traffic to external networks.
- This is supported for both IPv4 and IPv6.

Considerations

- Supported with both Lisp Pub/Sub and Lisp BGP fabrics.
- All Virtual Networks traffic within a site will traverse via the preferred Border via Cisco DNA Center UI.



Border1

Layer 3 Handoff | Layer 2 Handoff

☑ Enable Layer-3 Handoff

Local Autonomous Number: 200

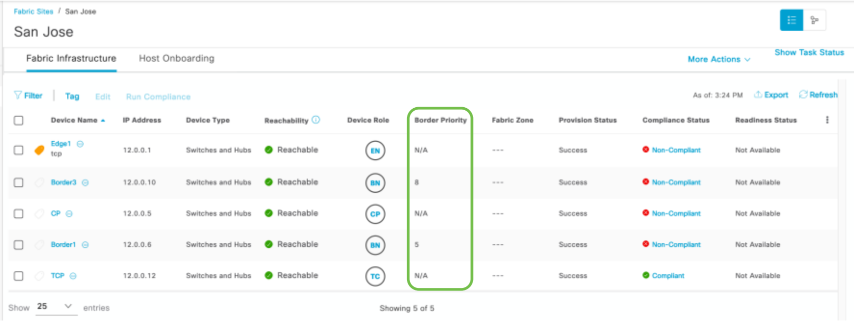
☑ Modify Border Priority

Border Priority: 5

Do not change this unless you understand LISP. A lower value indicates a higher priority. E.g., a priority of 1 takes precedence over 5.

☑ Default to all virtual networks

☐ Do not import external routes



Fabric Sites / San Jose

San Jose

Fabric Infrastructure | Host Onboarding | More Actions | Show Task Status

Filter | Tag | Edit | Run Compliance | As of: 3:24 PM | Export | Refresh

☐	Device Name	IP Address	Device Type	Reachability	Device Role	Border Priority	Fabric Zone	Provision Status	Compliance Status	Readiness Status
☐	Edge1 tcp	12.0.0.1	Switches and Hubs	Reachable	EN	N/A	---	Success	Non-Compliant	Not Available
☐	Border3	12.0.0.10	Switches and Hubs	Reachable	BN	8	---	Success	Non-Compliant	Not Available
☐	CP	12.0.0.5	Switches and Hubs	Reachable	CP	N/A	---	Success	Non-Compliant	Not Available
☐	Border1	12.0.0.6	Switches and Hubs	Reachable	BN	5	---	Success	Non-Compliant	Not Available
☐	TCP	12.0.0.12	Switches and Hubs	Reachable	TC	N/A	---	Success	Compliant	Not Available

Show 25 entries

Showing 5 of 5

Zero Trust Capabilities

(Secure AP Onboarding)

Zero Trust Capabilities

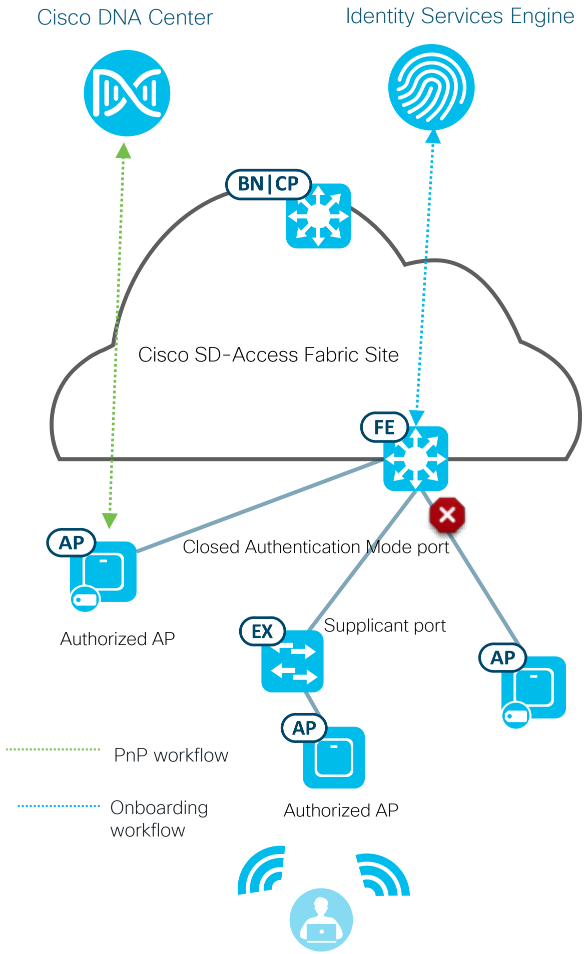
Secure AP Onboarding

- Onboard and enable Dot1x on the Access point connected to an Edge Node , Extended Node or Policy Extended Node on closed authentication ports.

- Protect the network from attachment of unauthorized Access Points by maintaining closed authentication on all access ports.

- Secure AP onboarding is done by authorizing the Access Point on a closed authentication port by allowing limited access to DHCP/DNS and Cisco DNA Center for PnP workflow

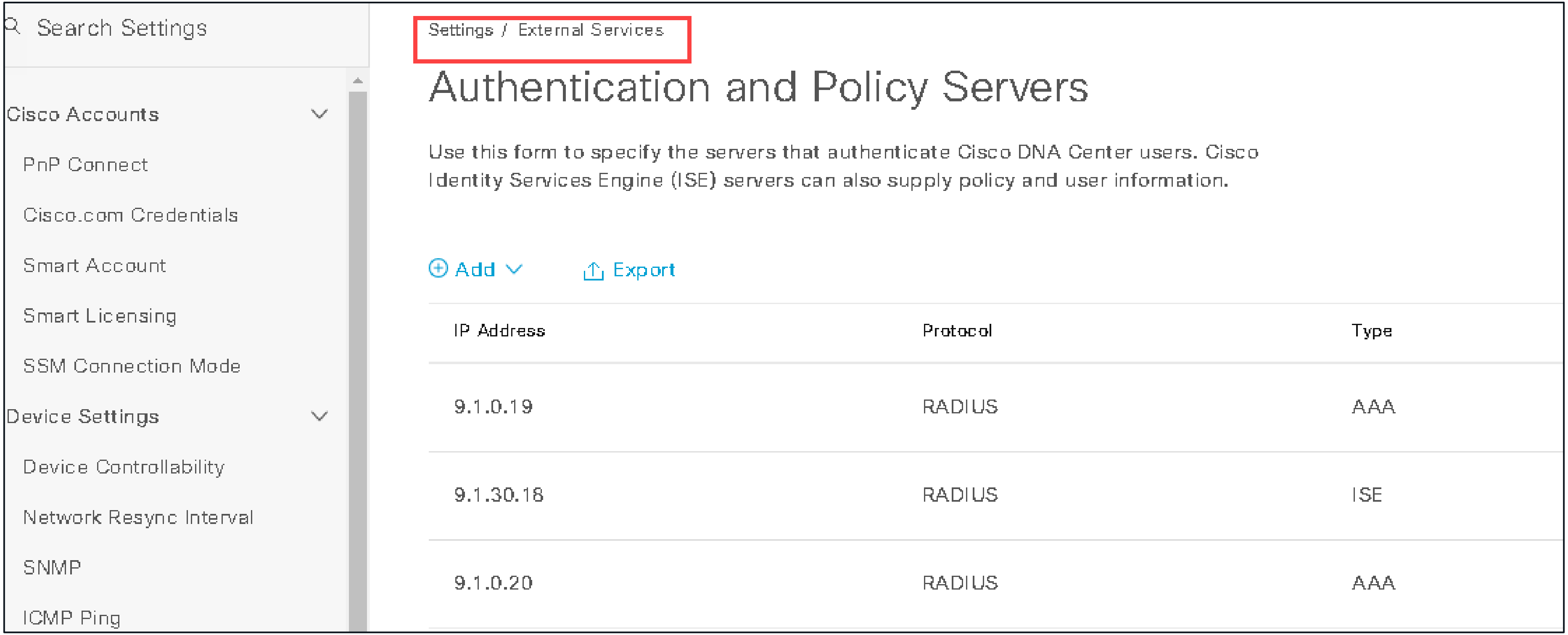
- The PnP workflow on the Cisco DNA Center is enhanced to enable dot1x supplicant on the Access Point



Secure AP Onboarding

Steps

Add ISE or any external AAA server on the Cisco DNA



Authentication and Policy Servers

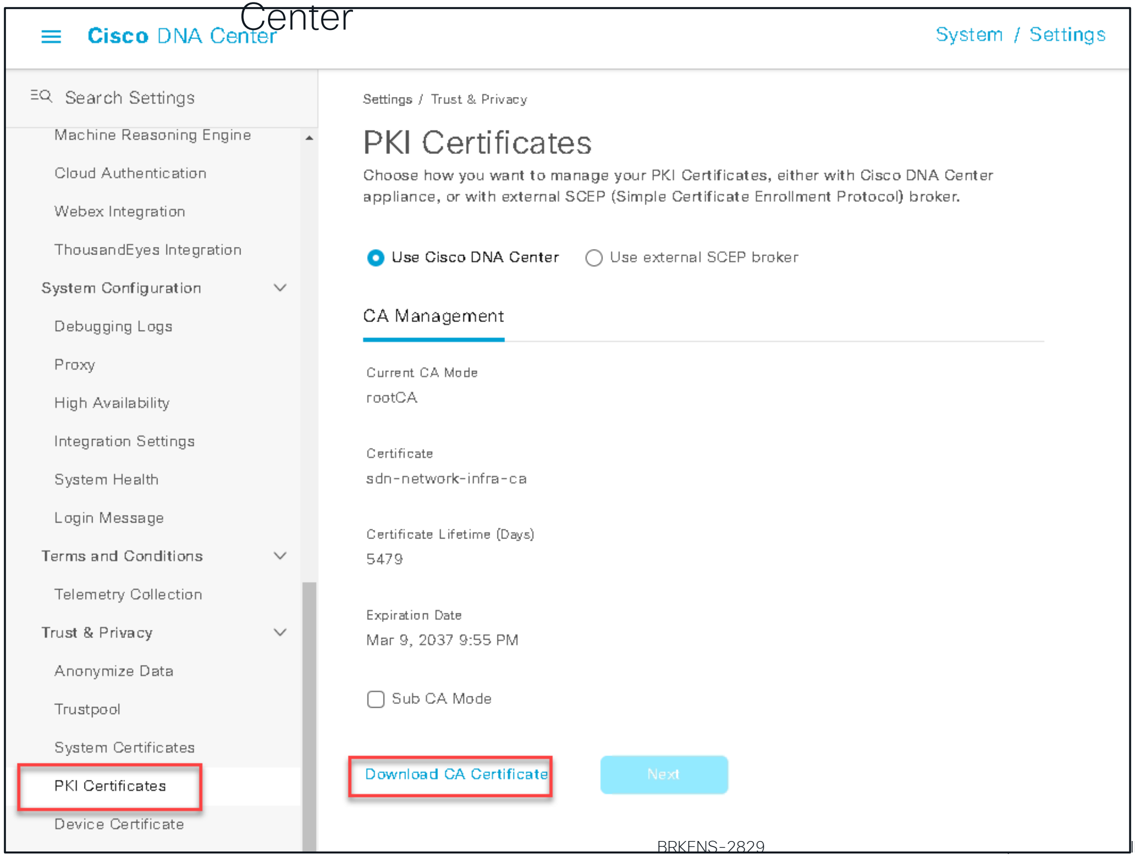
Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

IP Address	Protocol	Type
9.1.0.19	RADIUS	AAA
9.1.30.18	RADIUS	ISE
9.1.0.20	RADIUS	AAA

Secure AP Onboarding

Steps

Create CA certificate in Cisco DNA Center



Settings / Trust & Privacy

PKI Certificates

Choose how you want to manage your PKI Certificates, either with Cisco DNA Center appliance, or with external SCEP (Simple Certificate Enrollment Protocol) broker.

● Use Cisco DNA Center ○ Use external SCEP broker

CA Management

Current CA Mode
rootCA

Certificate
sdn-network-infra-ca

Certificate Lifetime (Days)
5479

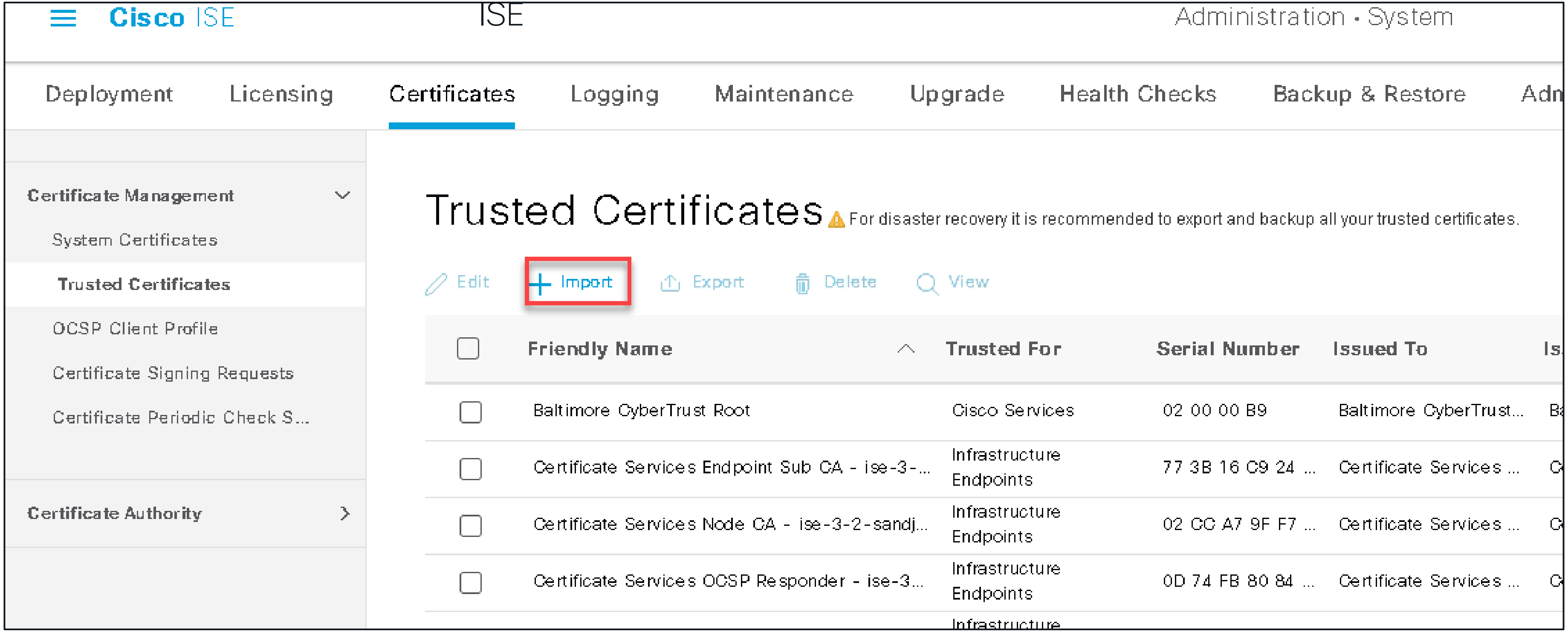
Expiration Date
Mar 9, 2037 9:55 PM

□ Sub CA Mode

Secure AP Onboarding

Steps

Import DNA Center created certificate into ISE



Trusted Certificates

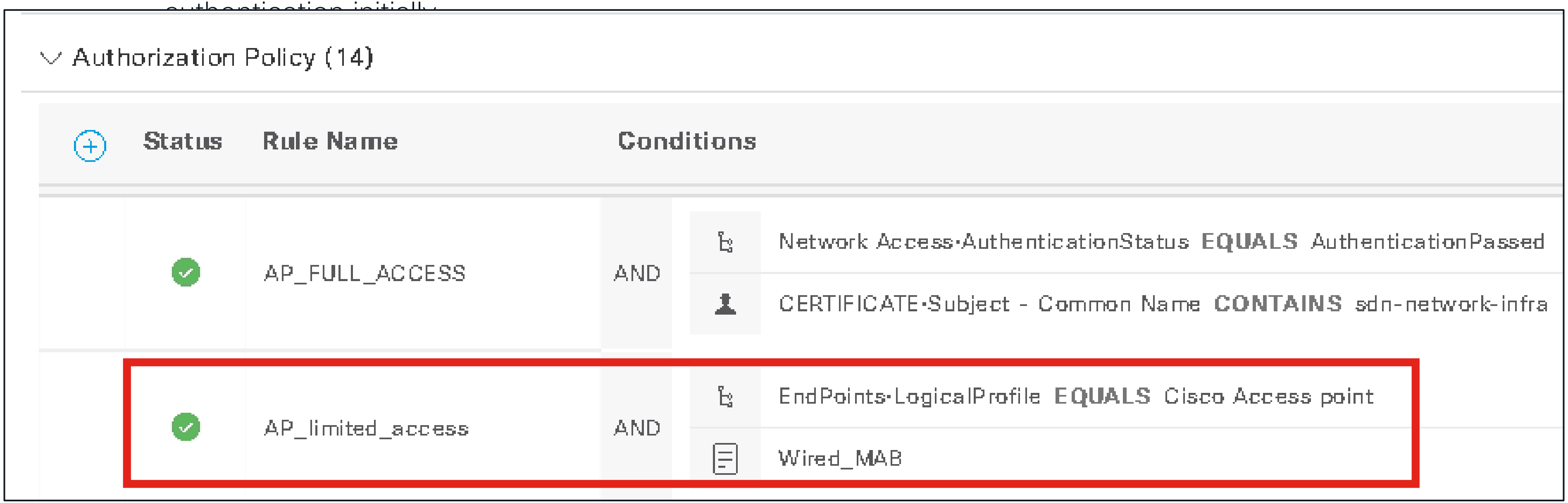
⚠ For disaster recovery it is recommended to export and backup all your trusted certificates.

□	Friendly Name	Trusted For	Serial Number	Issued To	Is
□	Baltimore CyberTrust Root	Cisco Services	02 00 00 B9	Baltimore CyberTrust...	Ba
□	Certificate Services Endpoint Sub CA - ise-3-...	Infrastructure Endpoints	77 3B 16 C9 24 ...	Certificate Services ...	C
□	Certificate Services Node CA - ise-3-2-sandj...	Infrastructure Endpoints	02 CC A7 9F F7 ...	Certificate Services ...	C
□	Certificate Services OCSP Responder - ise-3...	Infrastructure Endpoints	0D 74 FB 80 84 ...	Certificate Services ...	C
		Infrastructure			

Secure AP Onboarding

Onboarding Process

Access Points out of factory don’t have a dot1x supplicant and goes through a MAB authentication initially



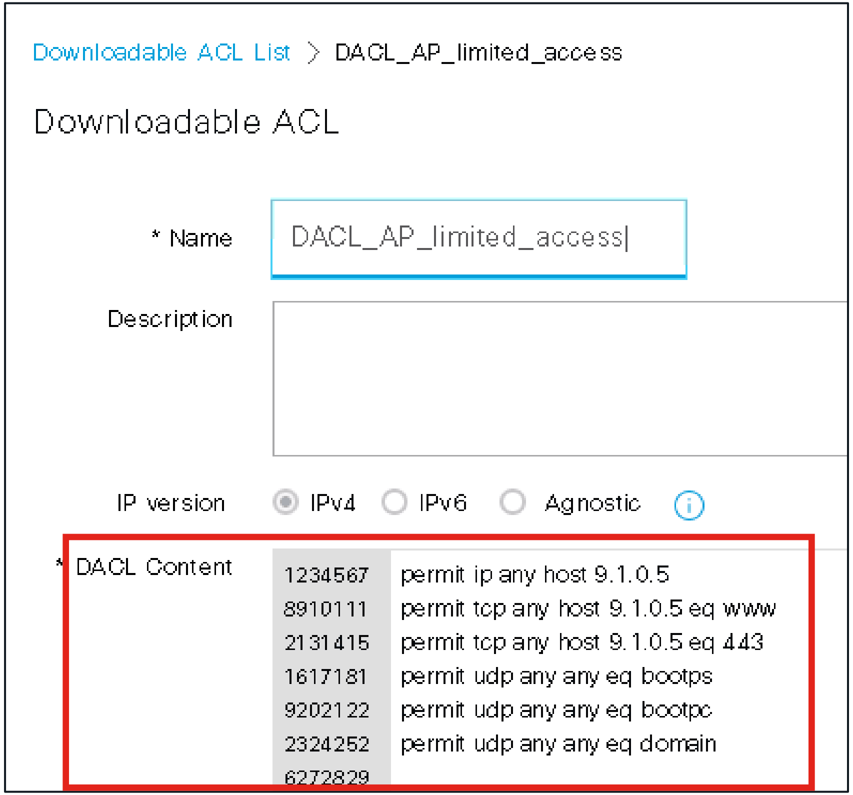
Authorization Policy (14)

Status	Rule Name		Conditions
✓	AP_FULL_ACCESS	AND	Network Access·AuthenticationStatus **EQUALS** AuthenticationPassed CERTIFICATE·Subject - Common Name **CONTAINS** sdn-network-infra
✓	AP_limited_access	AND	EndPoints·LogicalProfile **EQUALS** Cisco Access point Wired_MAB

Secure AP Onboarding

Onboarding Process

As part of MAB authentication and authorization, a VLAN and an ACL is returned providing limited access to do PnP.



Downloadable ACL List > DACL_AP_limited_access

Downloadable ACL

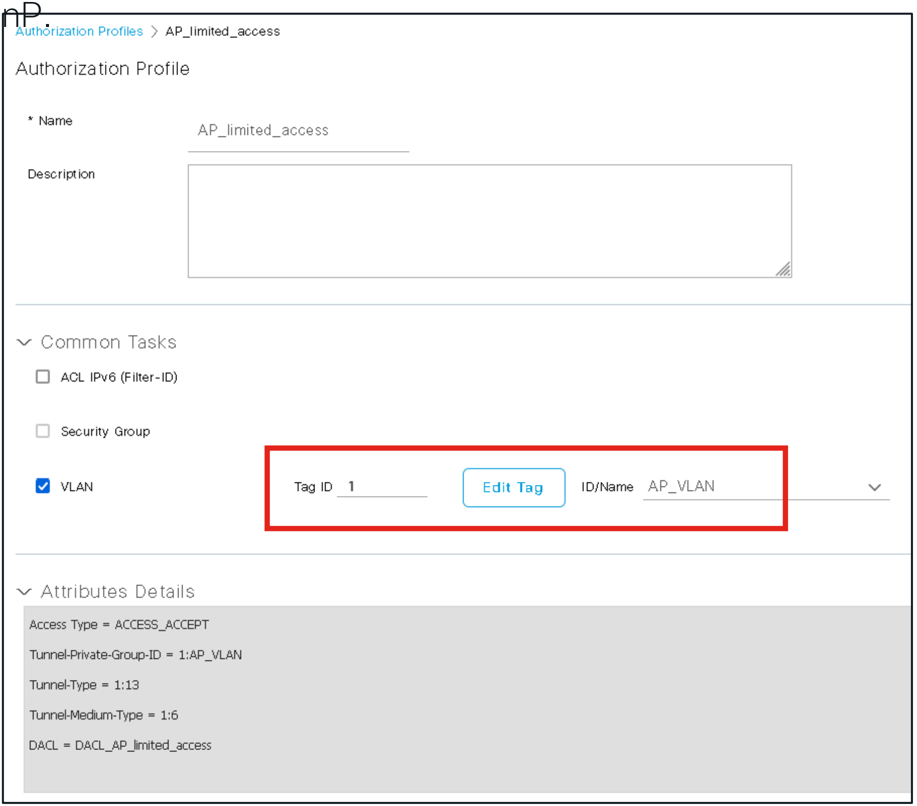
* Name: DACL_AP_limited_access

Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content

```
permit ip any host 9.1.0.5
permit tcp any host 9.1.0.5 eq www
permit tcp any host 9.1.0.5 eq 443
permit udp any any eq bootps
permit udp any any eq bootpc
permit udp any any eq domain
```



Authorization Profiles > AP_limited_access

Authorization Profile

* Name: AP_limited_access

Description:

Common Tasks

□ ACL IPv6 (Filter-ID)

□ Security Group

☑ VLAN — Tag ID 1 | Edit Tag | ID/Name AP_VLAN

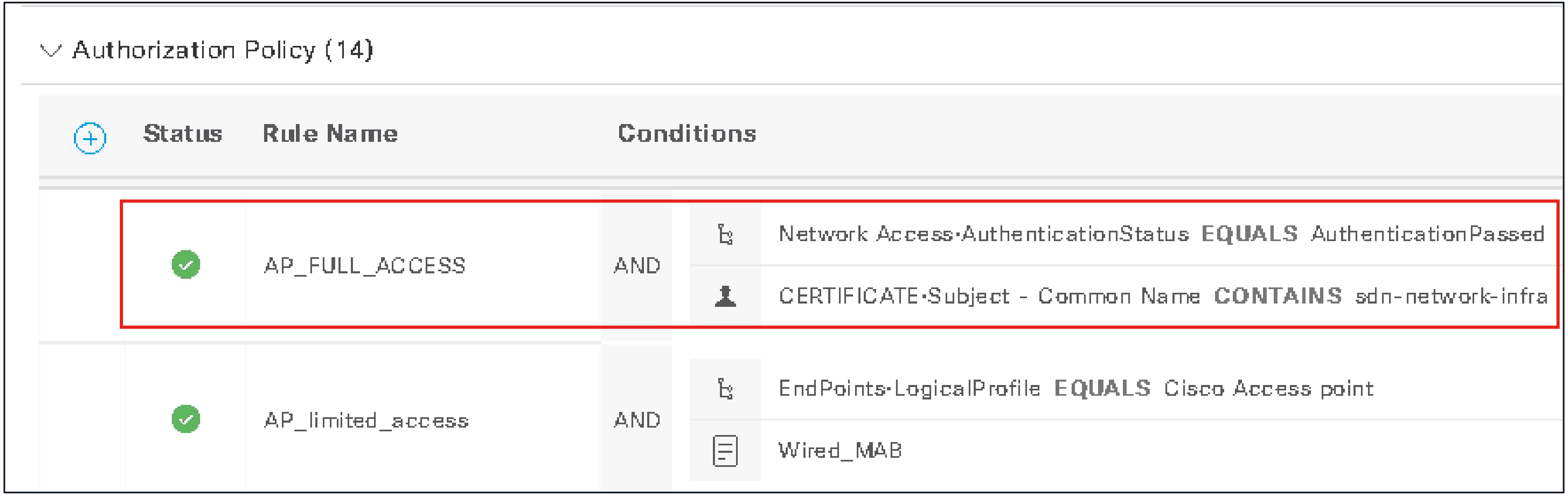
Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:AP_VLAN
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
DACL = DACL_AP_limited_access
```

Secure AP Onboarding

Onboarding Process

Once the PnP workflow is completed the AP does a dot1x authentication resulting in a full access to the network .



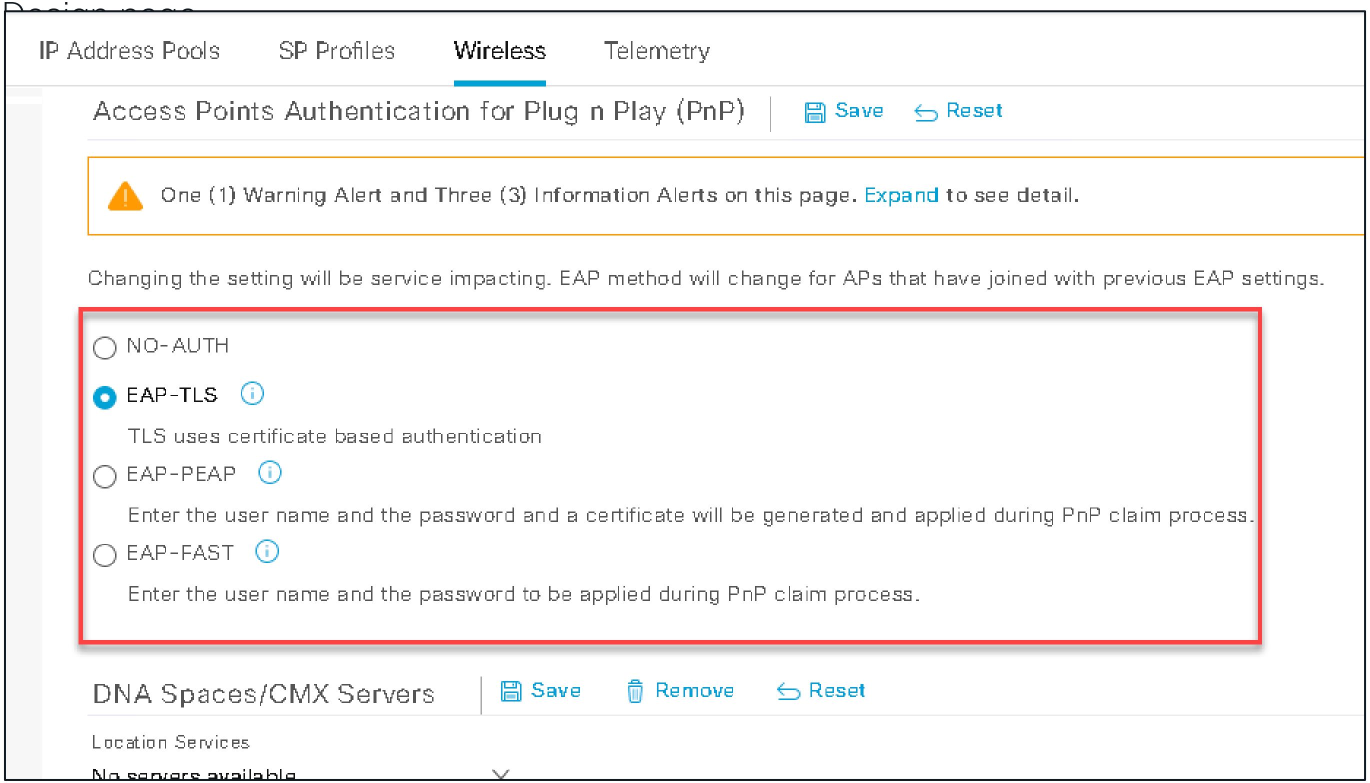
Authorization Policy (14)

Status	Rule Name		Conditions
✓	AP_FULL_ACCESS	AND	Network Access·AuthenticationStatus **EQUALS** AuthenticationPassed CERTIFICATE·Subject - Common Name **CONTAINS** sdn-network-infra
✓	AP_limited_access	AND	EndPoints·LogicalProfile **EQUALS** Cisco Access point Wired_MAB

Secure AP Onboarding

Onboarding Process

The authentication option for AP is enabled on the wireless network settings under Design page



Access Points Authentication for Plug n Play (PnP) | Save Reset

One (1) Warning Alert and Three (3) Information Alerts on this page. Expand to see detail.

Changing the setting will be service impacting. EAP method will change for APs that have joined with previous EAP settings.

○ NO-AUTH

● EAP-TLS ⓘ

TLS uses certificate based authentication

○ EAP-PEAP ⓘ

Enter the user name and the password and a certificate will be generated and applied during PnP claim process.

○ EAP-FAST ⓘ

Enter the user name and the password to be applied during PnP claim process.

DNA Spaces/CMX Servers | Save Remove Reset

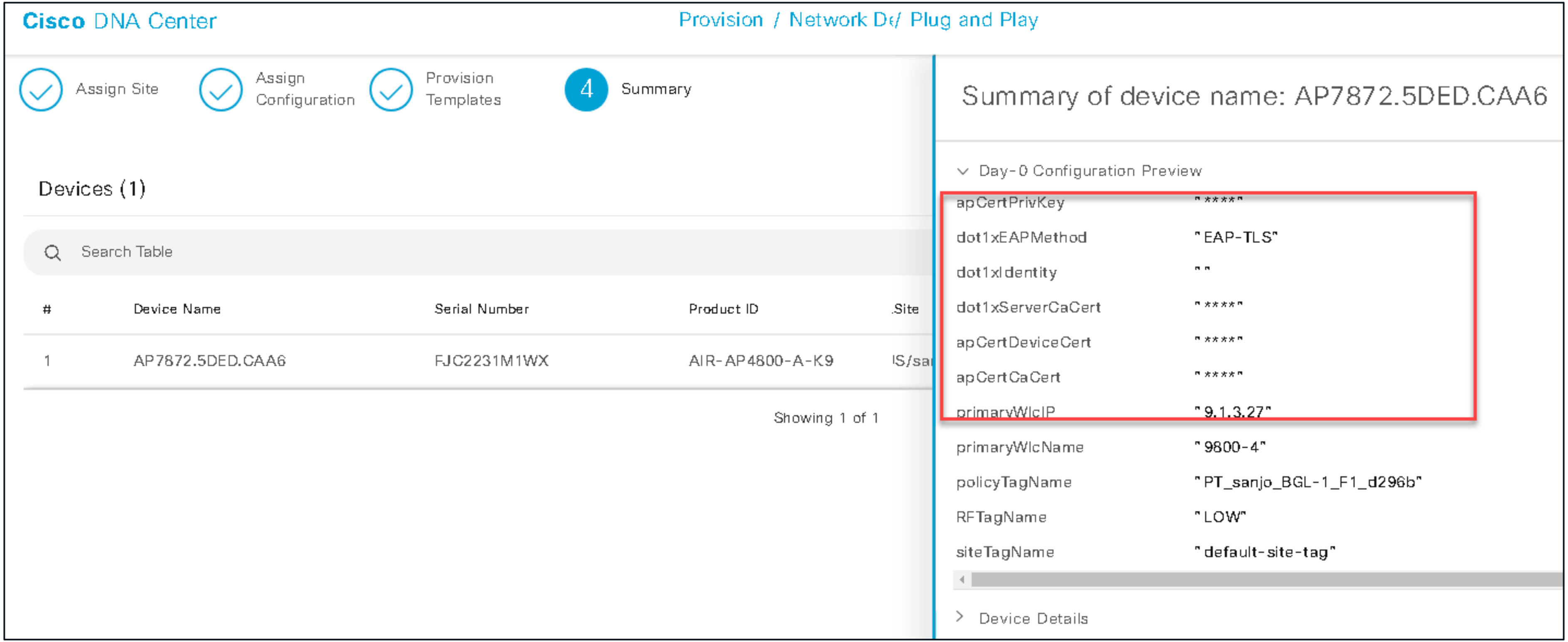
Location Services

No servers available

Secure AP Onboarding

Onboarding Process

The PnP workflow is enhanced to send the dot1x configuration to the access point.



#	Device Name	Serial Number	Product ID	Site
1	AP7872.5DED.CAA6	FJC2231M1WX	AIR-AP4800-A-K9	S/sa

Summary of device name: AP7872.5DED.CAA6

apCertPrivKey	"*****"
dot1xEAPMethod	"EAP-TLS"
dot1xIdentity	" "
dot1xServerCaCert	"*****"
apCertDeviceCert	"*****"
apCertCaCert	"*****"
primaryWlcIP	"9.1.3.27"
primaryWlcName	"9800-4"
policyTagName	"PT_sanjo_BGL-1_F1_d296b"
RFTagName	"LOW"
siteTagName	"default-site-tag"

Secure AP Onboarding

Onboarding Process

Access Point initially goes through a MAB authentication on switchport

```
fabric_edget#sh access-session interface gi 1/0/12 details
            Interface:  GigabitEthernet1/0/12
               IIF-ID:  0x186C3CD7
          MAC Address:  7872.5ded.caa6
         <snip>


Server Policies:
           Vlan Group:  Vlan: 1027
              ACS ACL: xACSACLx-IP-DACL_AP_limited_access-624e6cc4


Method status list:
       Method           State
        dot1x           Stopped
          mab           Authc Success
```

Secure AP Onboarding

Onboarding Process

Access Point after completion of the PnP process reboots and starts dot1x with the switchport

```
Fabric_edget#sh access-session interface gi 1/0/12 details
            Interface:  GigabitEthernet1/0/12
               IIF-ID:  0x1984EC50
          MAC Address:  7872.5ded.caa6
         <snip>


Local Policies:

Server Policies:
     Interface Template:  ApAutzTemplate


Method status list:
       Method                State
        dot1x                Authc Success
```

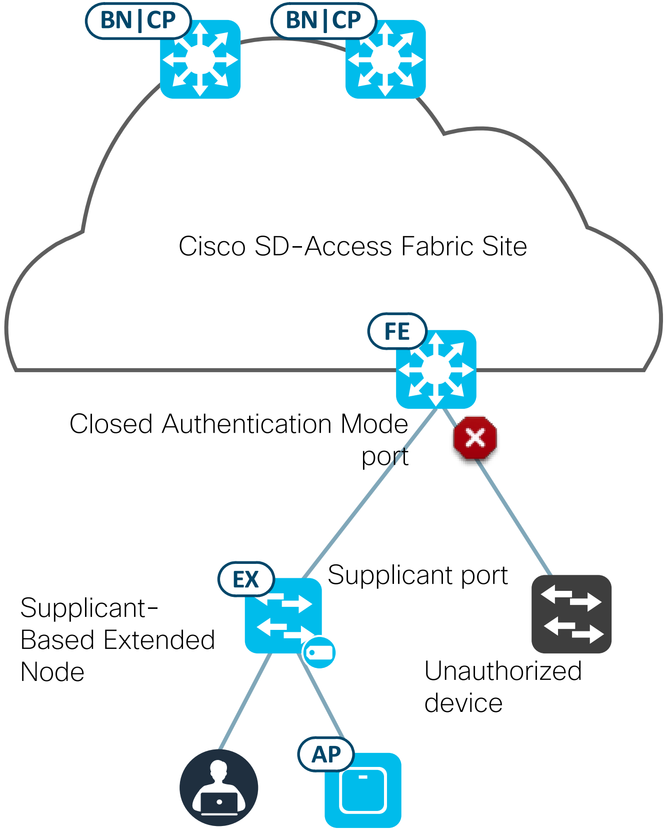
Zero Trust Capabilities

(Supplicant-Based Extended Nodes)

Zero Trust Capabilities

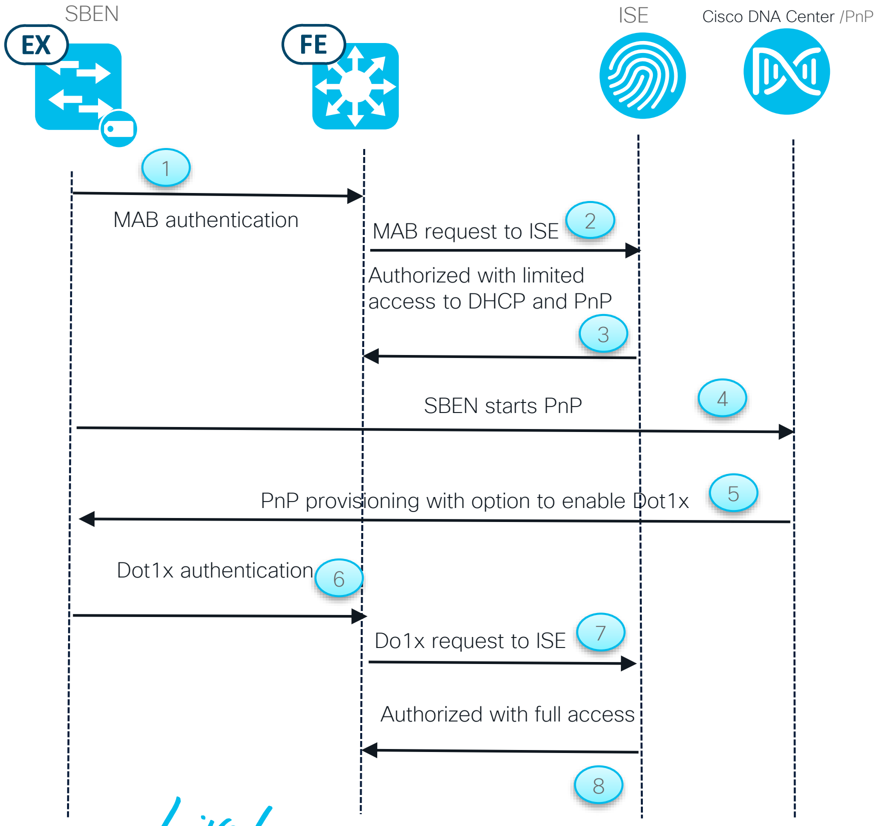
Supplicant-Based Extended Node (SBEN)

- Automatically onboard supported factory default switches connected to Fabric Edge (FE) node closed authentication ports.
- Protect the network from attachment of unauthorized devices by maintaining closed authentication on all Edge Node access ports
- Supplicant-Based Extended Nodes (SBEN) onboarding is designed to onboard EN using PNP in a zero-trust environment.
- Supplicant-Based Extended Nodes (SBEN) are provisioned by Cisco DNA Center to have a supplicant with EAP-TLS authentication on their uplink to the Edge Node. The EAP-TLS certificate is provisioned by Cisco DNA Center from Cisco DNA Center Certificate Authority (CA).
- After successful onboarding, access to the port is purely based on authentication status. If device/port goes down, authentication session is cleared, and traffic is not allowed on the port. When the port comes back, it goes through dot1x authentication to regain access to the Cisco SD-Access network.
- Supplicant-Based Extended Nodes (SBEN) are provisioned as Policy Extended Nodes. Thus, they use SGTs for micro-segmentation on access ports.


BN|CP
BN|CP
Cisco SD-Access Fabric Site
FE
Closed Authentication Mode port
EX
Supplicant port
Supplicant-Based Extended Node
Unauthorized device
AP

Supplicant-Based Extended Node

Workflow



Flow	Event
1	Extended node out of factory connects to a closed auth port on the fabric edge. The FE is configured for dot1x followed by MAB. The FE starts MAB after dot1x timeout.
2	FE forwards the MAB request to Cisco ISE for authentication and authorization
3	Cisco ISE authorizes the MAB request with limited access, only providing access to DHCP and PnP. Cisco DNA Center provisions the ACL and interface template on fabric devices for providing limited access.
4	SBEN starts PnP with the Cisco DNA Center.
5	Cisco DNA Center as part of the PnP workflow provisions dot1x credentials and enables dot1x supplicant on the extended node.
6	SBEN stars dot1x authentication after the PnP provisioning
7	FE forwards the Dot1x request to Cisco ISE for authentication and authorization
8	Cisco ISE authorizes the dot1x request providing full access. Cisco DNA Center provisions the required interface template for full access which can be referred in the authorization profile.

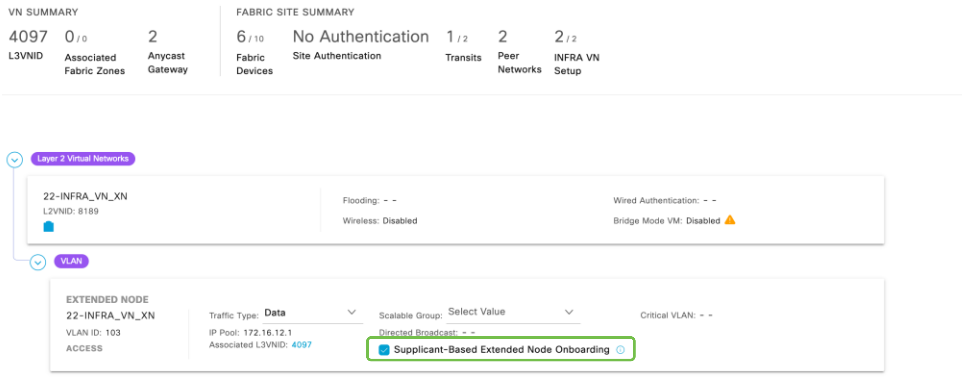
Supplicant-Based Extended Node

Considerations

Considerations

- Upstream Edge Nodes must be 9300/L, 9400 or 9500/H Series Switches.
- SBENs must be Catalyst 9200/L/CX, 9300/L, 9400, or 9500/H Series Switches.
- Both the Edge Nodes and their connected SBENs must use IOS XE 17.7.x ,ISE 3.1 or later .
- SBEN supports a maximum of one physical uplink port. EtherChannel is not supported.
- Configuration on ISE for providing limited access /policy authorization must be done manually out of band.
- Daisy chain of SBEN not supported.

First Method to enable SBEN from Cisco DNA Center UI



VN SUMMARY

4097 L3VNID · 0 / 0 Associated Fabric Zones · 2 Anycast Gateway

FABRIC SITE SUMMARY

6 / 10 Fabric Devices · No Authentication Site Authentication · 1 / 2 Transits · 2 Peer Networks · 2 / 2 INFRA VN Setup

Layer 2 Virtual Networks

22-INFRA_VN_XN
L2VNID: 8189

Flooding: - -
Wireless: Disabled

Wired Authentication: - -
Bridge Mode VM: Disabled ⚠

VLAN

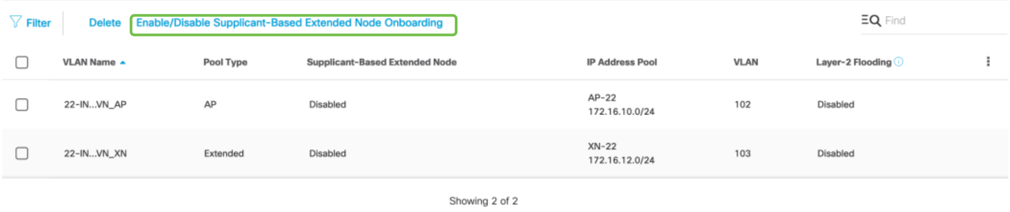
EXTENDED NODE
22-INFRA_VN_XN
VLAN ID: 103
ACCESS

Traffic Type: Data
IP Pool: 172.16.12.1
Associated L3VNID: 4097

Scalable Group: Select Value
Directed Broadcast: - -
☑ Supplicant-Based Extended Node Onboarding

Critical VLAN: - -

Second method to enable SBEN from Cisco DNA Center UI



Filter | Delete | Enable/Disable Supplicant-Based Extended Node Onboarding | Find

□	VLAN Name ▲	Pool Type	Supplicant-Based Extended Node	IP Address Pool	VLAN	Layer-2 Flooding
□	22-IN...VN_AP	AP	Disabled	AP-22 172.16.10.0/24	102	Disabled
□	22-IN...VN_XN	Extended	Disabled	XN-22 172.16.12.0/24	103	Disabled

Showing 2 of 2

Complete your Session Survey

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

Continue Your Education

- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

The bridge to possible

Thank you

cisco Live!