cisco Live!

ALL IN

#CiscoLive

The bridge to possible

Deploying Large Scale Cisco SD-Access Campus Network

With Fabric Zone Feature Case Studies

Dhrumil Prajapati
Sr. Delivery Architect

BRKENS-3833

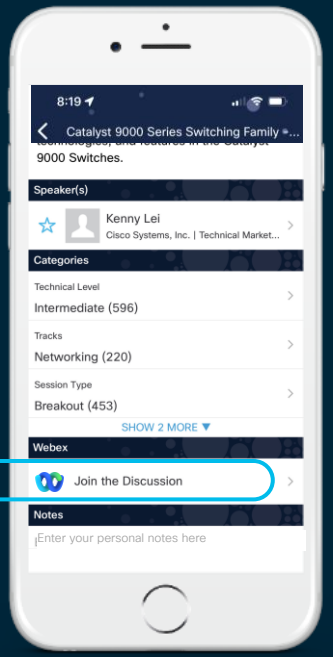
Cisco Webex App

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



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-3833

Webex spaces will be moderated by the speaker until June 17, 2022.

Who am I?

Dhrumil Prajapati

Sr. Delivery Architect

Technology and Transformation Group – CX

7+ Years @ Cisco

CCIE #28071 (R/S, SP)

CCDE #20210002

Specialized in: SD-Access, SD-WAN, MPLS, Enterprise Architecture

@DhruPrajapati

Special Thanks: Eddy Lee

Agenda

- Introduction
- Fabric Zone Considerations & Supported Use Cases
- Deploying Fabric Zone in Large Scale Campus Network Case Studies
- Creating Fabric Zone
- Troubleshoot Fabric Zone
- Conclusion

Introduction

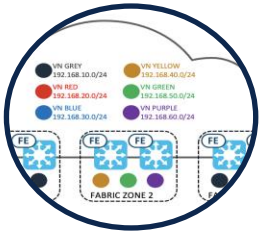
What is Fabric Zone (FZ) ?

Dividing a large single fabric site into smaller manageable micro sites

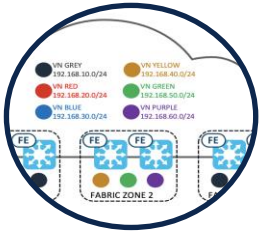
FZ uses Child Fabric Sites that are created and associated with the Parent Fabric Site

The Child Site inherits the properties of the Parent Site while allowing management of the network with fewer devices and segments

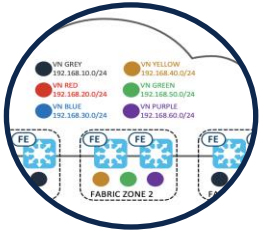
Why To Use & What Are The Benefits ?



Manageability: Customers who are having large-scale deployment of Fabric Edge Nodes in a single fabric site need a way to manage their network based on smaller location or zones (building, floors)



Security: Some customers require granular control of IP Pool provisioning scope within a site

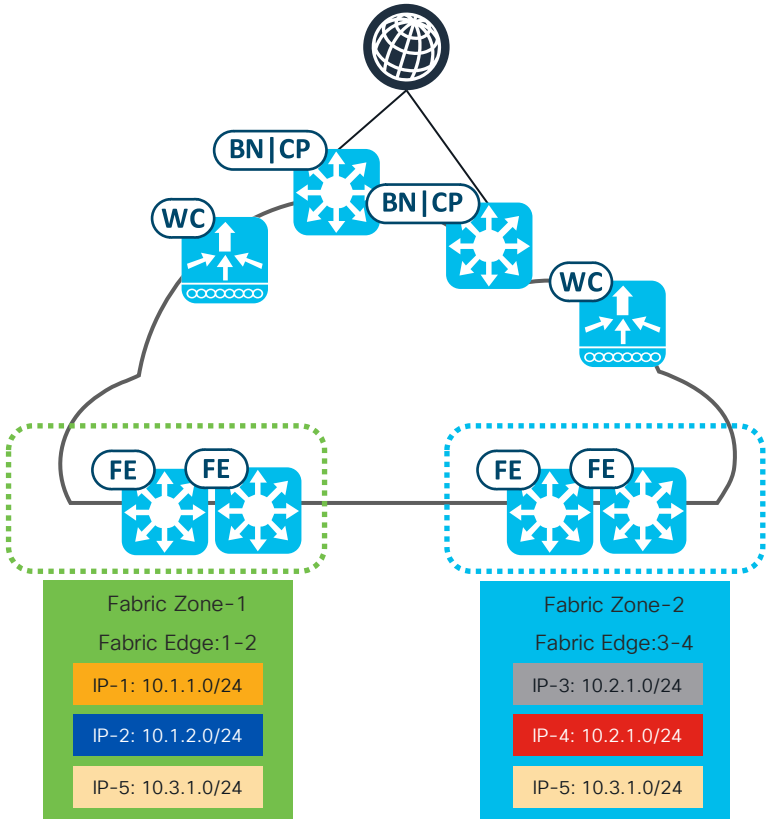


Scalability and Performance: Significant reduced provisioning time across the Fabric Edge nodes

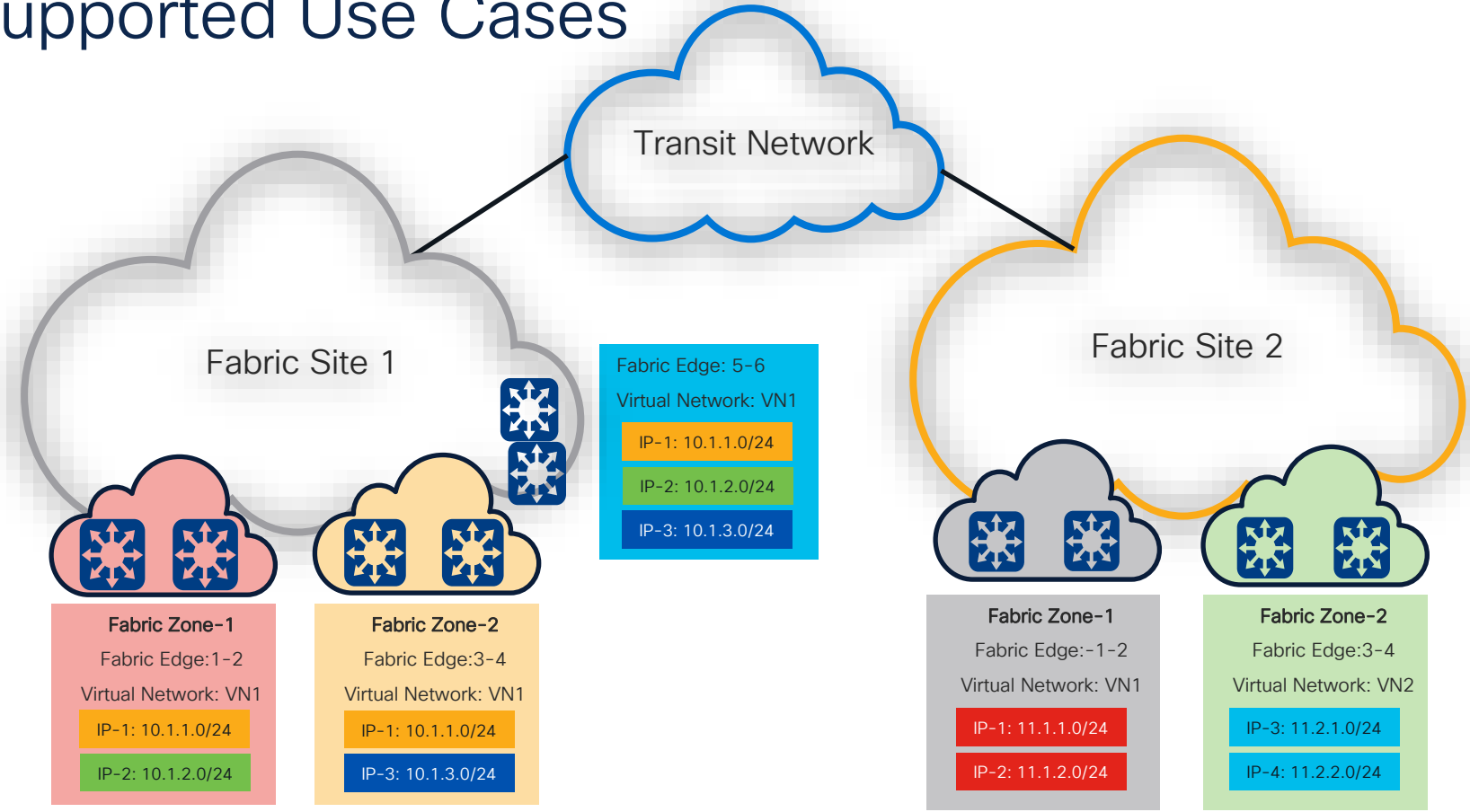
Fabric Zone Considerations & Supported Use Cases

Fabric Zone Considerations

- Addition of Control-plane, Border and WLC is only supported at the Parent Fabric Site.
- VN/Gateways must be assigned to fabric site (Parent) first before assigning to Fabric Zone (Child)
- Only edge nodes (FE, EN, PEN) can be provisioned to a Fabric Zone. EN/PEN must in the same FZ as Parent FE
- Collocated fabric roles (e.g., FE+B, FE + Embedded WLC, etc.) cannot be provisioned to a Fabric Zone.



Supported Use Cases



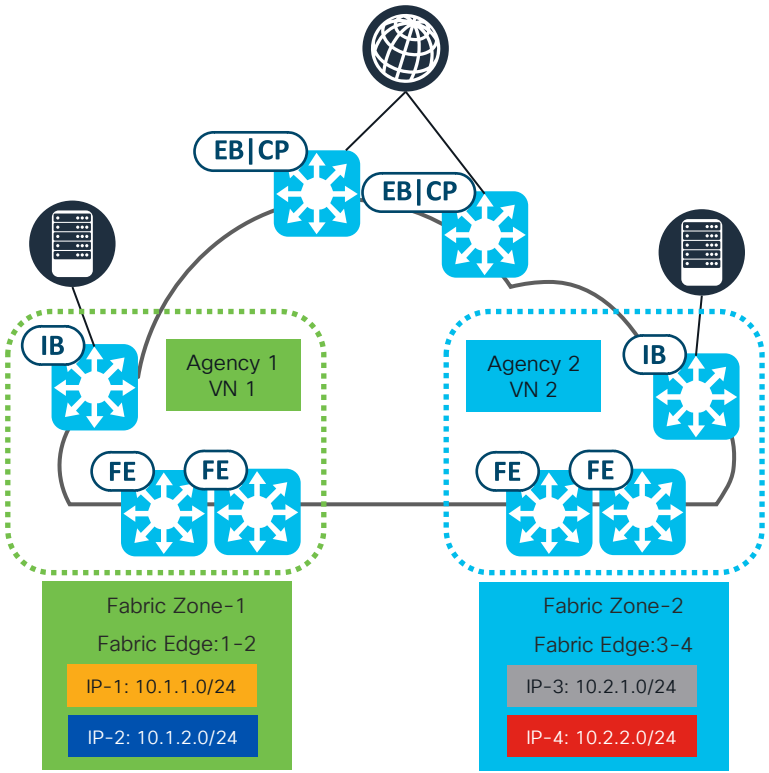
Fabric Performance Data Without Fabric Zone in a Single Site

- Good NEWS! Cisco Engineering has done some comprehensive performance testing without Fabric Zones and details of the results can be found on CCO Article:
- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/Cisco-Validated-Solution-Profiles/b_cisco_validated_solution_profile_enterprise_government.html

Large Scale Deployment Case Studies

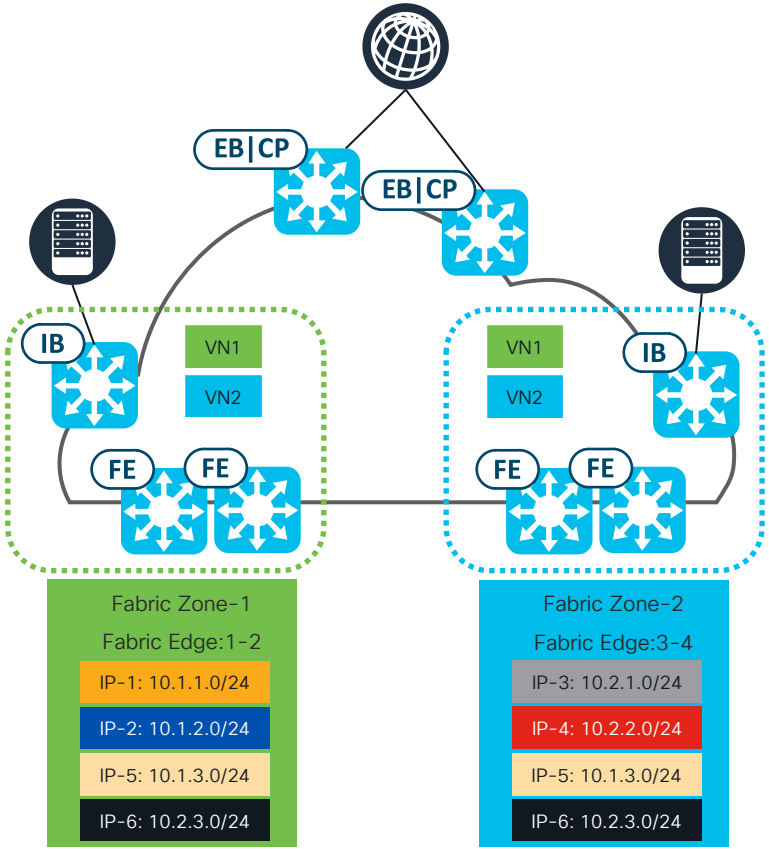
Case Study 1 – Zones per VN

- Customer A has a large single site SDA Fabric campus network with over 1000 FEs and 1000 IP pools
- Macro segmentation: One Agency per VN , the campus network supports total of over 100 government agencies/VNs
- Each agency owns their dedicated fabric edge nodes which have multiple local IP pools residing their own buildings and local breakout access to their own Data Centers



Case Study 1 – Other Requirements

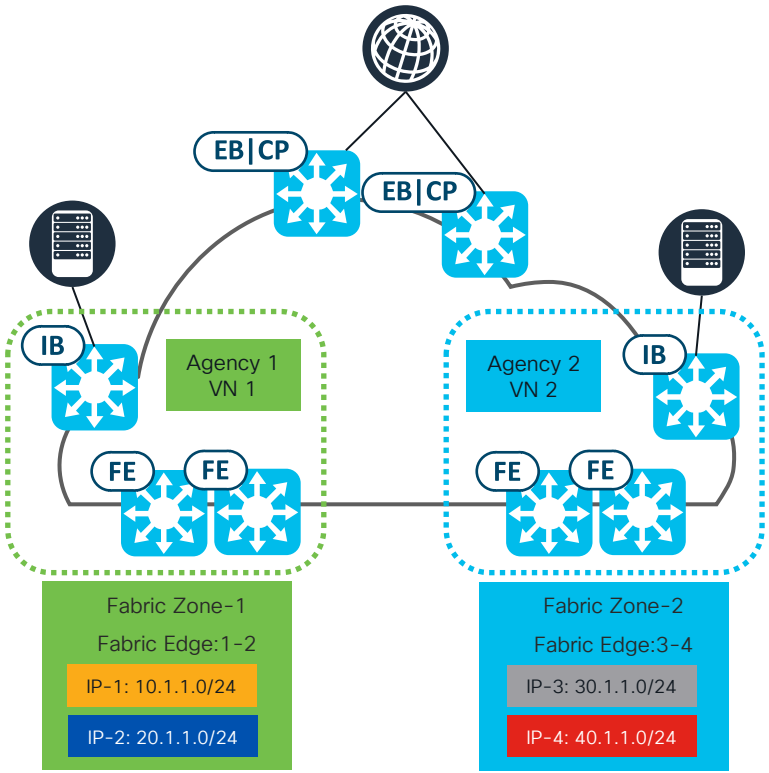
- What if the customer has the requirements such as roaming between Agencies ?
- Create one roaming pool per VN across different buildings owned by respective Agency
- With Fabric Zone feature, IP Pools optimized at local agency level with additional administrative efforts



Case Study 2 - Requirements

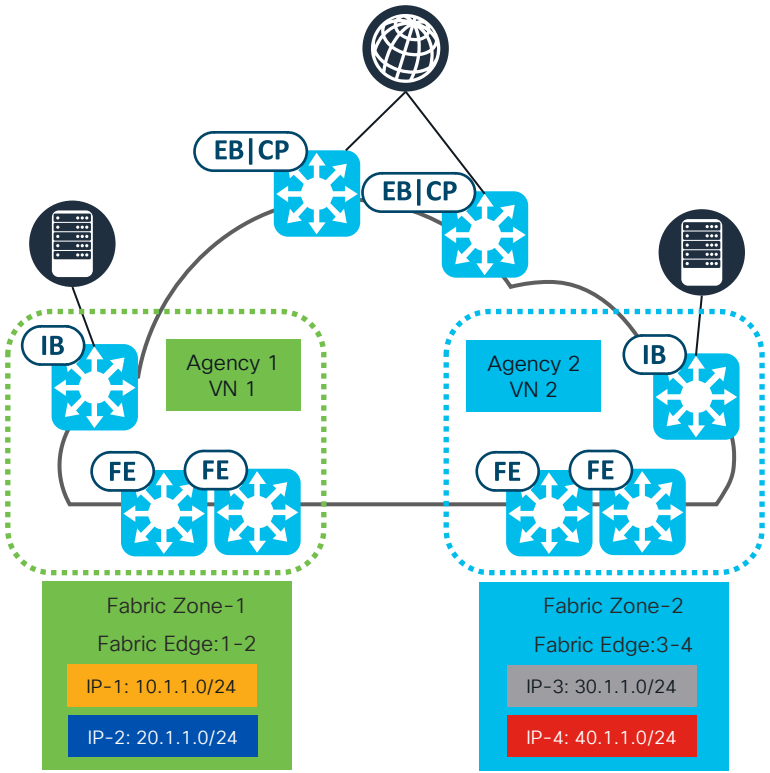
- Customer B requires Critical VLAN per VN instead of one critical VLAN for all Virtual Networks (VNs) from current DNAC automation due to security concerns between VNs

- Each VN needs to elect one critical IP pool for local DC and internet access in the event of all PSNs are not available for the NADs

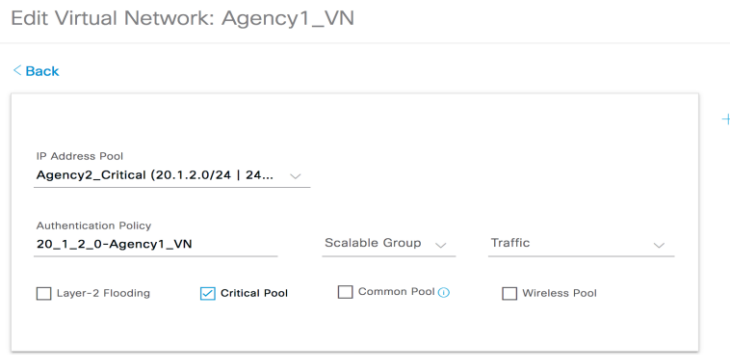


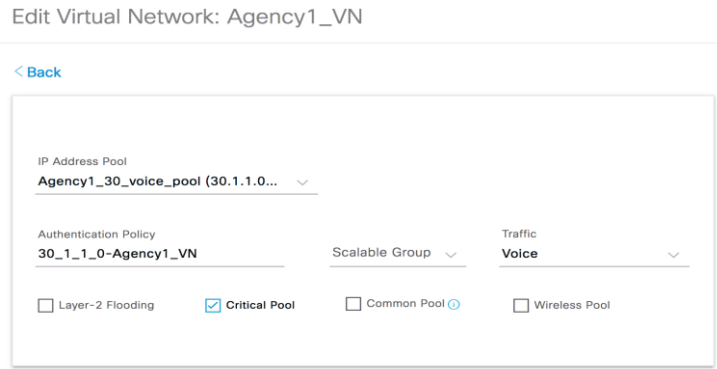
Case Study 2 - Requirements

- Leverage fabric zone feature with dedicated edge nodes belongs to the same VN and assign this critical IP pool across all edge nodes belongs to this VN
- Using DNAC Template to modify existing critical VLAN (e.g 2047) in Agency 1 FEs to critical IP pool SVI VLAN (e.g 1021) for VN1 edge nodes
- Using DNAC Template to modify existing critical VLAN (e.g 2047) in Agency 2 FEs to critical IP pool SVI VLAN (e.g 1022) for VN2 edge nodes



Case Study 2 - Critical VLAN (Data/Voice)





- Current DNAC release supports Critical VLAN for Data and Voice being enabled at VN level
- But it is only allowed per Fabric Domain
- We will need to extend this capability per VN base

Case Study 2 – Current DNAC Release CVLAN Creation Behavior

Classification	CLI

Network VLAN	Global VLAN:
	`vlan 2047`
	` name CRITICAL_VLAN`

Service Templates	`service-template DefaultCriticalAuthVlan_SRV_TEMPLATE` `  vlan 2047`

Policy Maps (Closed)	`10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure`
	` 10 activate service-template DefaultCriticalAuthVlan SRV_TEMPLATE`
	` 20 activate service-template DefaultCriticalVoice SRV_TEMPLATE`
	` 30 authorize`
	` 40 pause reauthentication`

Deployment Case Study 2 – CVLAN Creation

DNAC pushes Critical VLAN for Data and Voice per VN/VRF

```
interface Vlan2047
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f85e
 vrf forwarding Agency1_VN
 ip address 20.1.1.1 255.255.255.0
 ip helper-address 172.16.10.28
 ip helper-address 172.16.20.28
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 20_1_1_0-Agency1_VN-IPV4
 lisp mobility 20_1_1_0-Agency1_VN-IPV6
 ipv6 address 2402:1234:1::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
end
```

```
interface Vlan2046
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f85d
 vrf forwarding Agency1_VN
 ip address 30.1.1.1 255.255.255.0
 ip helper-address 172.16.10.28
 ip helper-address 172.16.20.28
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 30_1_1_0-Agency1_VN-IPV4
 lisp mobility 30_1_1_0-Agency1_VN-IPV6
 ipv6 address 2402:1234:3::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
end
```

Deployment Case Study 2 – CVLAN Creation

```
template DefaultWiredDot1xClosedAuth
 dot1x pae authenticator
 switchport access vlan 2047
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
!
template DefaultWiredDot1xLowImpactAuth
 dot1x pae authenticator
 switchport access vlan 2047
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_1X_MAB
!
```

```
template DefaultWiredDot1xOpenAuth
 dot1x pae authenticator
 switchport access vlan 2047
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber PMAP_DefaultWiredDot1xOpenAuth_1X_MAB
!
```

```
service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
 sgt 30
 vlan 2047
```

Deployment Case Study 2 – Critical Data & Voice VLANs Modification

```
template DefaultWiredDot1xClosedAuth
 dot1x pae authenticator
 switchport access vlan 2047-> 1021
 switchport mode access
 switchport voice vlan 2046-> 1022
 mab
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate
server
 service-policy type control subscriber
PMAP_DefaultWiredDot1xClosedAuth_1X_MAB



service-template
DefaultCriticalAuthVlan_SRV_TEMPLATE
 sgt 30
 vlan 2047 -> 1021
```

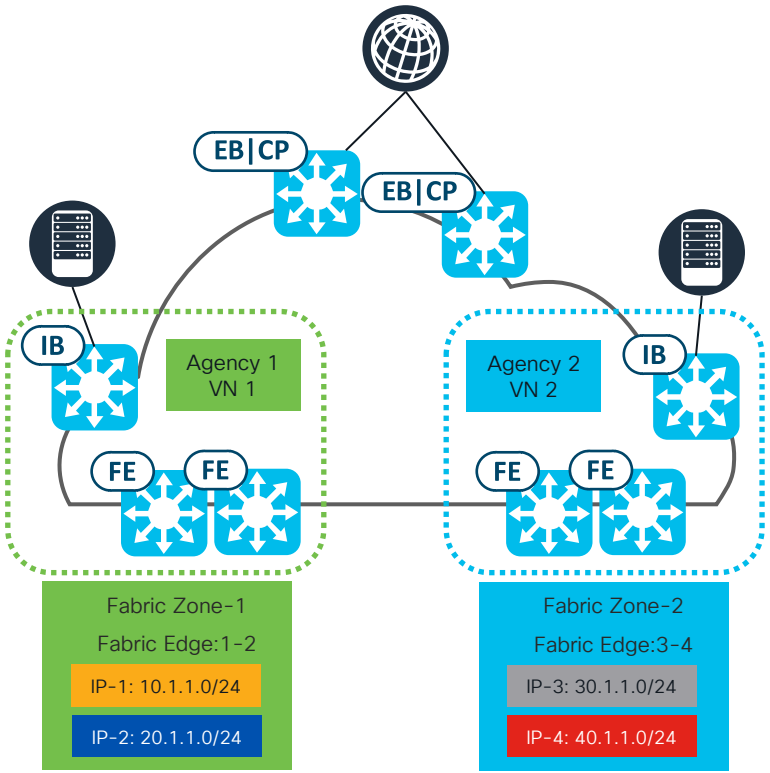
```
interface Vlan1021
 description Configured from Cisco DNAC
 mac-address 0000.0c9f.f85e
 vrf forwarding Agency1_VN
 ip address 20.1.1.1 255.255.255.0
 ip helper-address 172.16.10.28
 ip helper-address 172.16.20.28
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 20_1_1_0-Agency1_VN-IPV4
 lisp mobility 20_1_1_0-Agency1_VN-IPV6
 ipv6 address 2402:1234:1::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
end
```

```
interface Vlan1022
 description Configured from Cisco DNAC
 mac-address 0000.0c9f.f85d
 vrf forwarding Agency2_VN
 ip address 30.1.1.1 255.255.255.0
 ip helper-address 172.16.10.28
 ip helper-address 172.16.20.28
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 30_1_1_0-Agency2_VN-IPV4
 lisp mobility 30_1_1_0-Agency2_VN-IPV6
 ipv6 address 2402:1234:3::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
end
```

Case Study 2 - Considerations

- One FE or group of FEs belong to one VN only via DNAC provisioning
- Different VNs can not share the same FE with this solution since DNAC will push the critical VLANs based on the building or floor level where the VN belongs to which is practical for most of customers
- No L3 mobility if users are moving into different buildings which belong to different VN.

Note: These considerations are only applied when Critical VLANs (Data & Voice) being enabled. When AAA servers are restored or available, these conditions will be removed, the SD-Access network is back to normal operation.



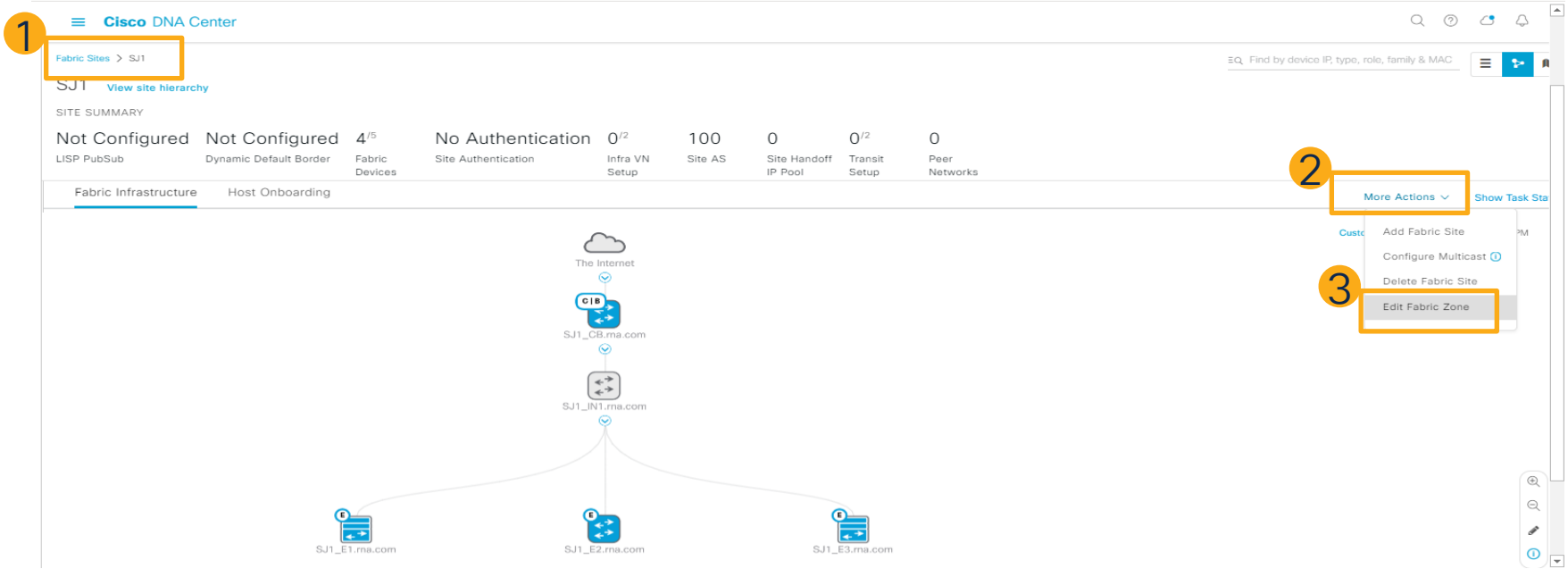
Creating Fabric Zones

DNAC Workflow

1. Creating FZ in Brownfield
2. Creating FZ in Greenfield

SDA: Fabric Zone in Brownfield

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

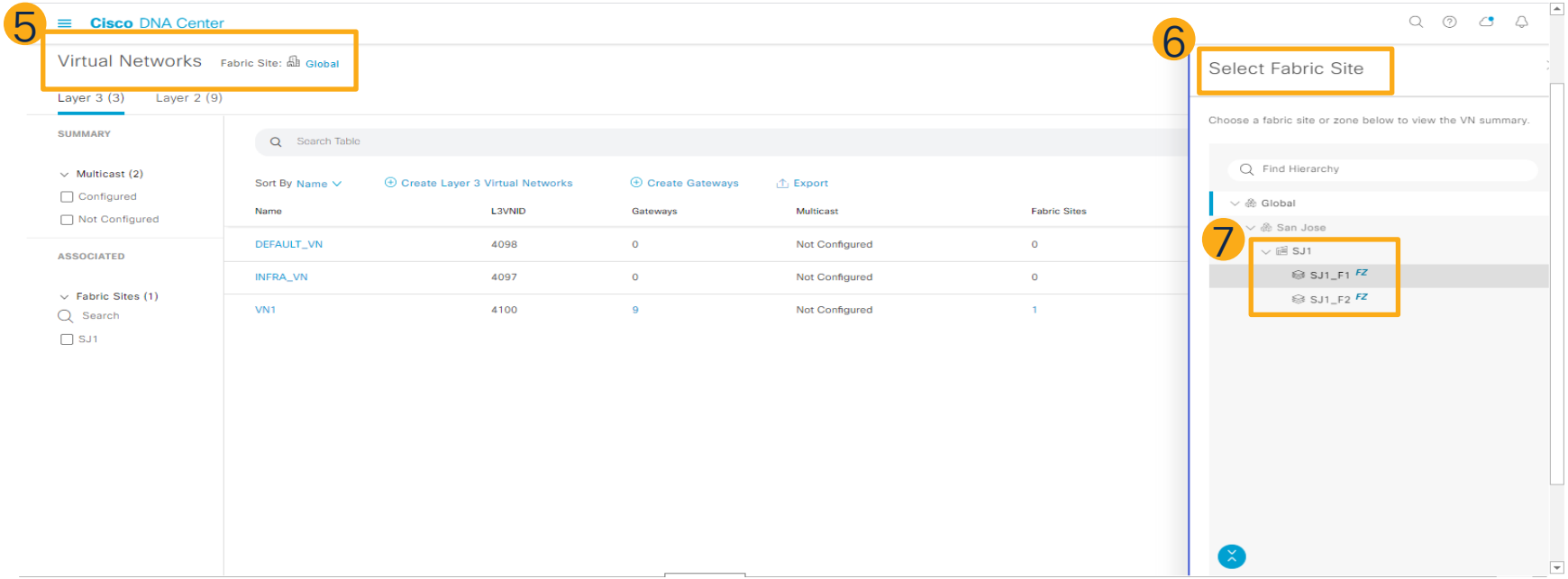


SDA: Fabric Zone in Brownfield

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

SDA: Fabric Zone in Brownfield

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



SDA: Fabric Zone in Brownfield

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

Cisco DNA Center

Preview New SD-Access BETA

Virtual Networks | Fabric Sites | Transits and Peer Networks

Virtual Networks Fabric Site: Global

Layer 3 | Layer 2

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 8 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)	- -	•••

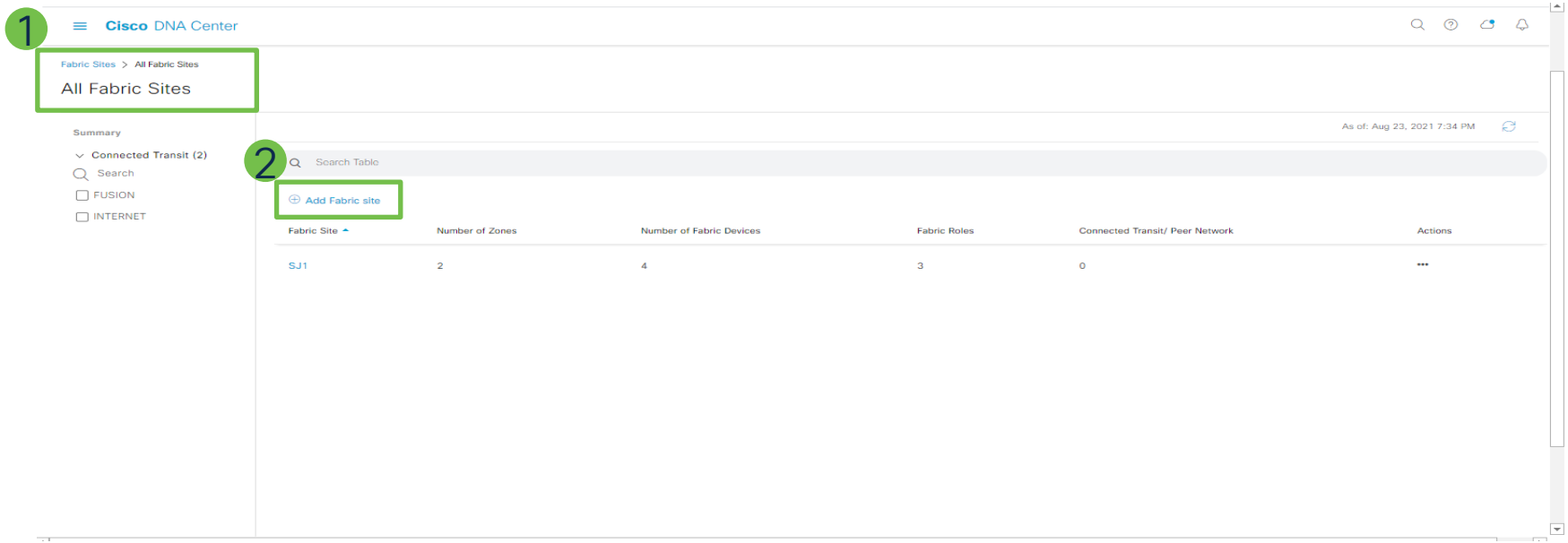
Create Anycast Gateways

Add to fabric site

Delete gateways

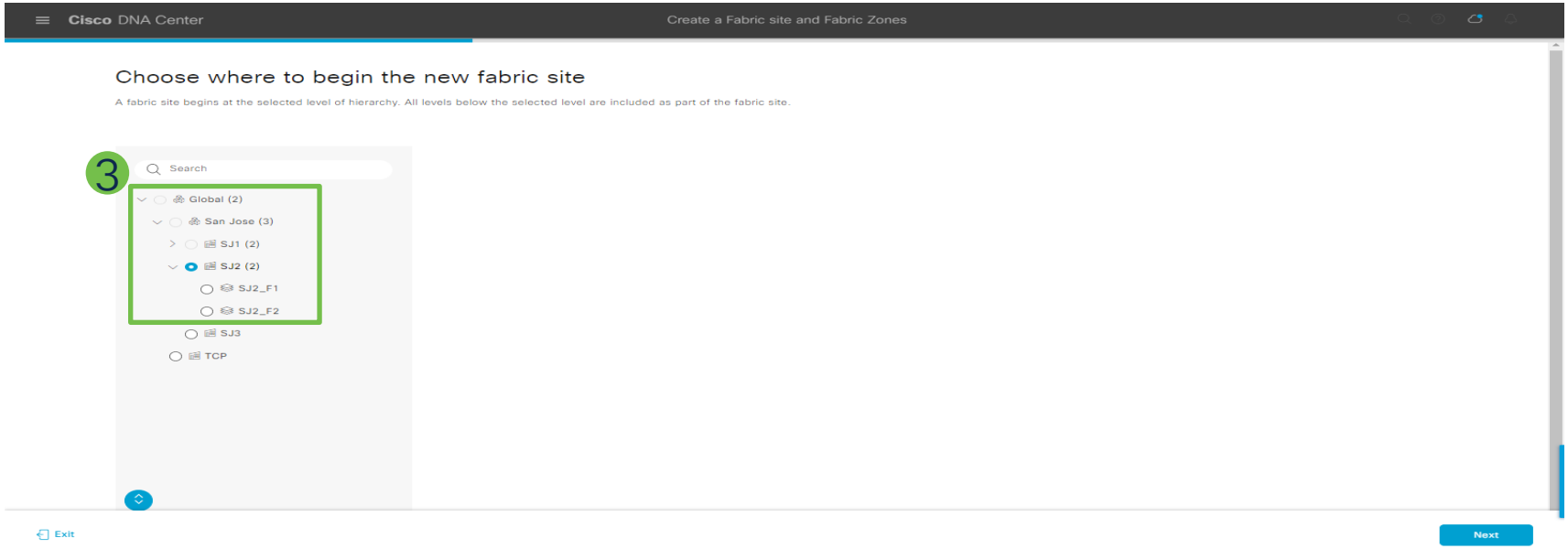
SDA: Fabric Zone in Greenfield

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



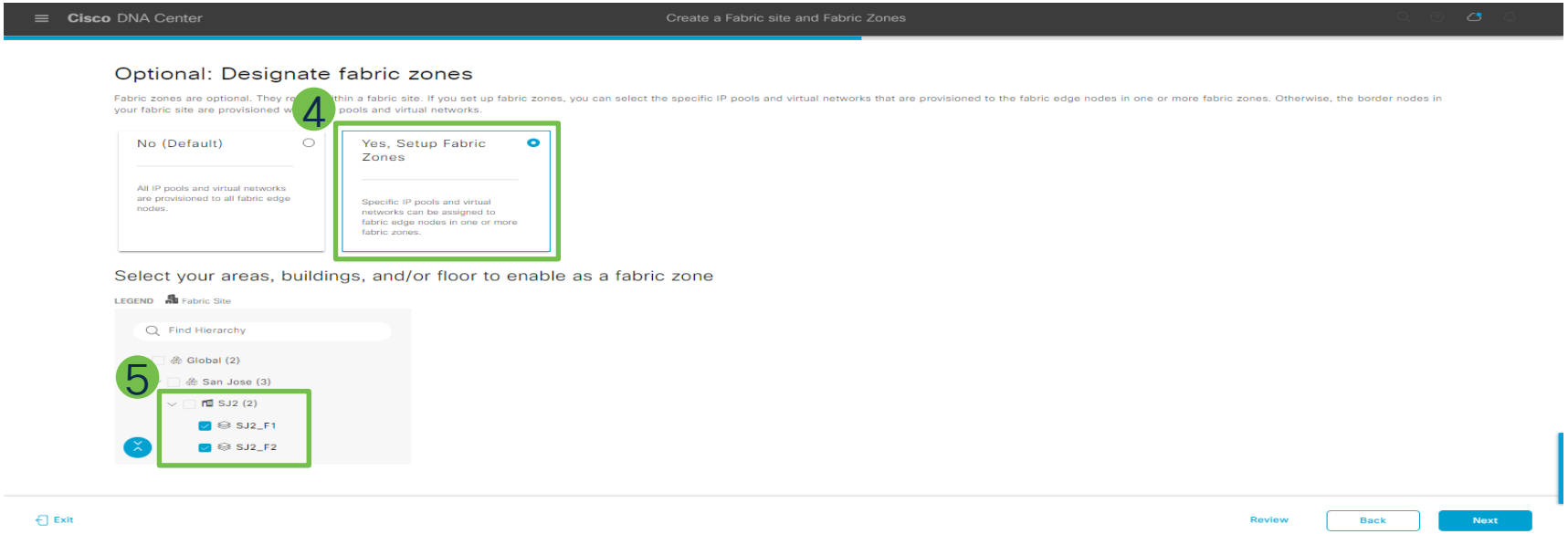
SDA: Fabric Zone in Greenfield

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



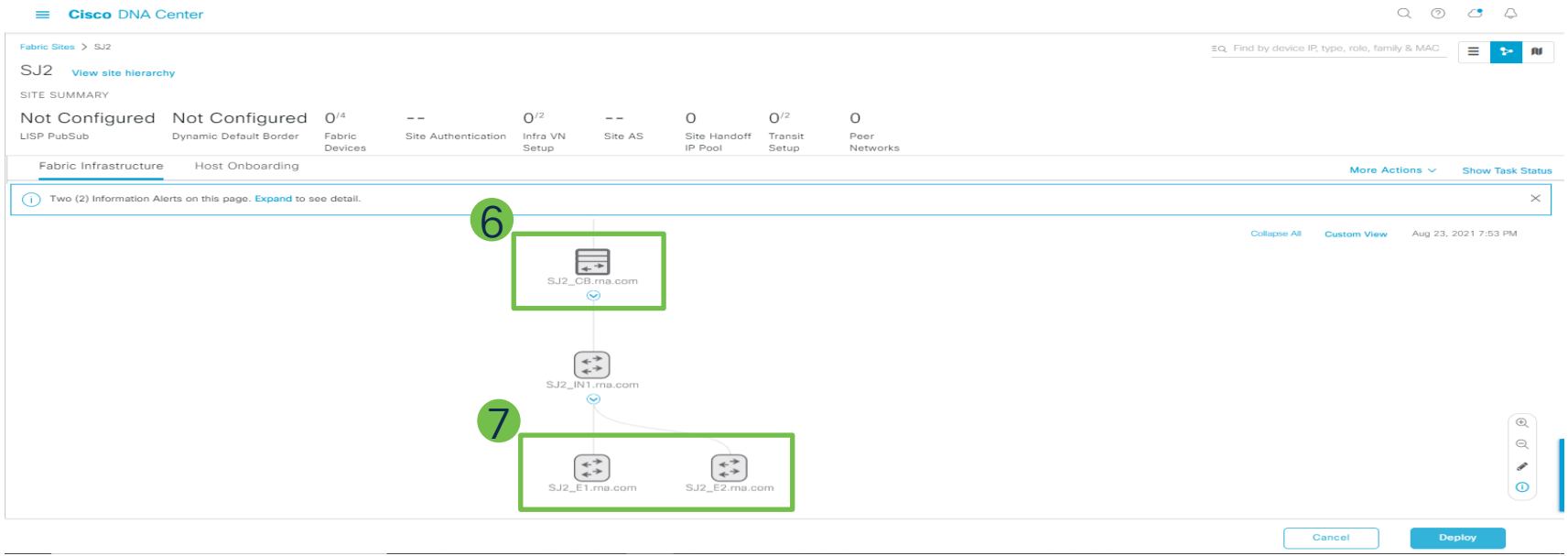
SDA: Fabric Zone in Greenfield

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



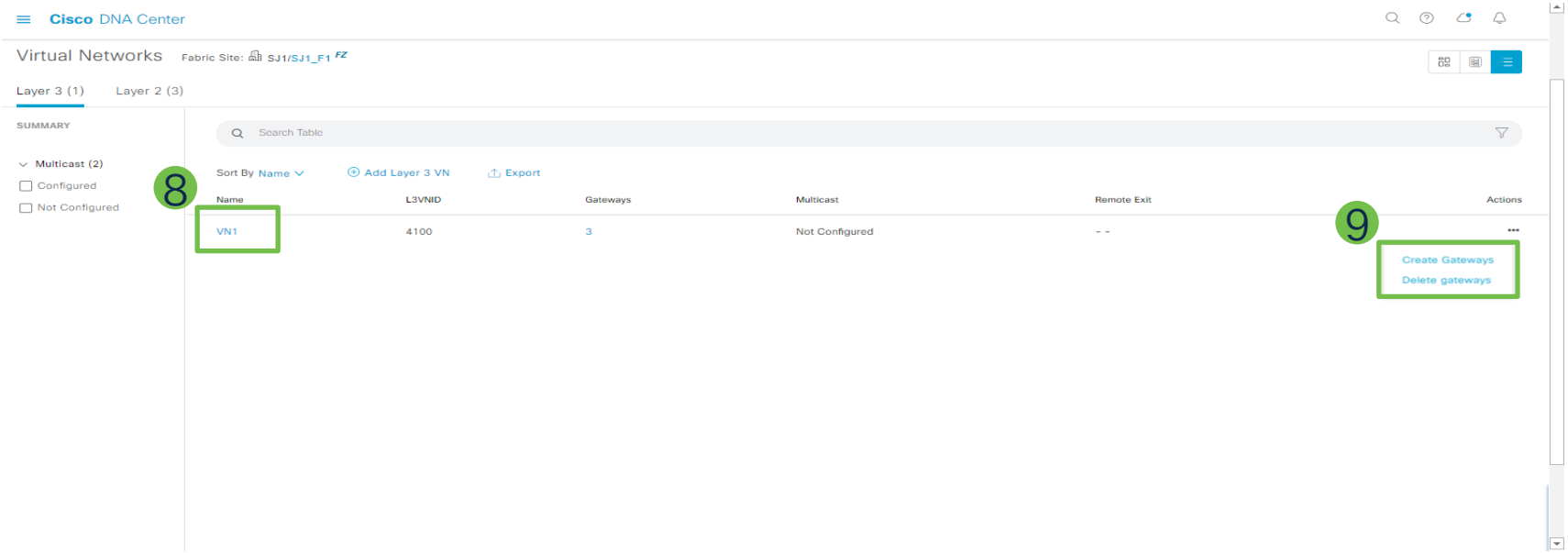
SDA: Fabric Zone in Greenfield

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



SDA: Fabric Zone in Greenfield

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



Troubleshoot Fabric Zone

Troubleshoot Fabric Zone (FZ)

If Fabric Zone configuration or provisioning is missed in Fabric Edge or other devices,

Check DNAC CLI logs using below commands:

```
$ magctl service logs -rf apic-em-network
$ magctl service logs -rf spf-service-manager
```

Conclusion

Conclusion/Key Takeaways

1 Fabric Zone Feature

Available since DNAC 2.2.3.x and IOS-XE 17.5/17.6+ releases

2 Supported Use Cases

Brownfield and Greenfield are supported

3 Deployment Case Studies

Large Scale SDA single site optimization
Security and manageability enhancement
Leverage FZ for Critical VLAN per VN support

4 Enablement Workflow

DNAC UI friendly workflow support both brownfield and greenfield migration

5 Unlock Fabric Zone Potential

Leverage Fabric Zone feature in SDA to support large scale SDA customer deployment
Better scaling and security support
Deploy it with confidence

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

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

Thank you

cisco Live!

ALL IN

#CiscoLive