

CISCO *Live!*



#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 *Live!*

#CiscoLive

# 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 17, 2022.



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

# 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) ?

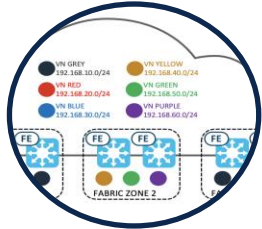
Dividing a large single fabric site into smaller manageable micro sites

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

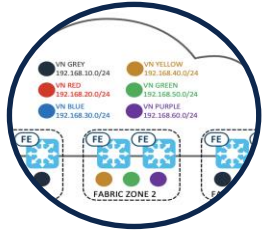
The Child Site inherits the properties of the Parent Site while allowing management of the network with fewer devices and segments



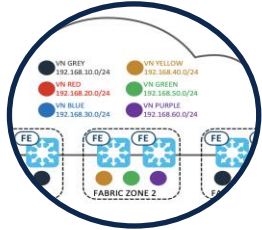
# Why To Use & What Are The Benefits ?



**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



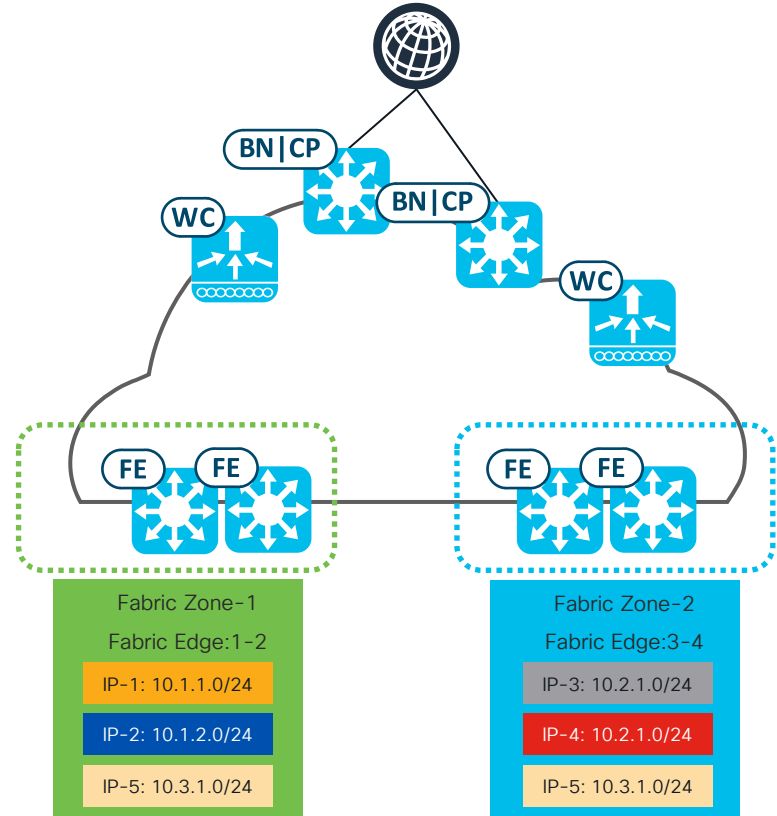
**Scalability and Performance:** Significant reduced provisioning time across the Fabric Edge nodes



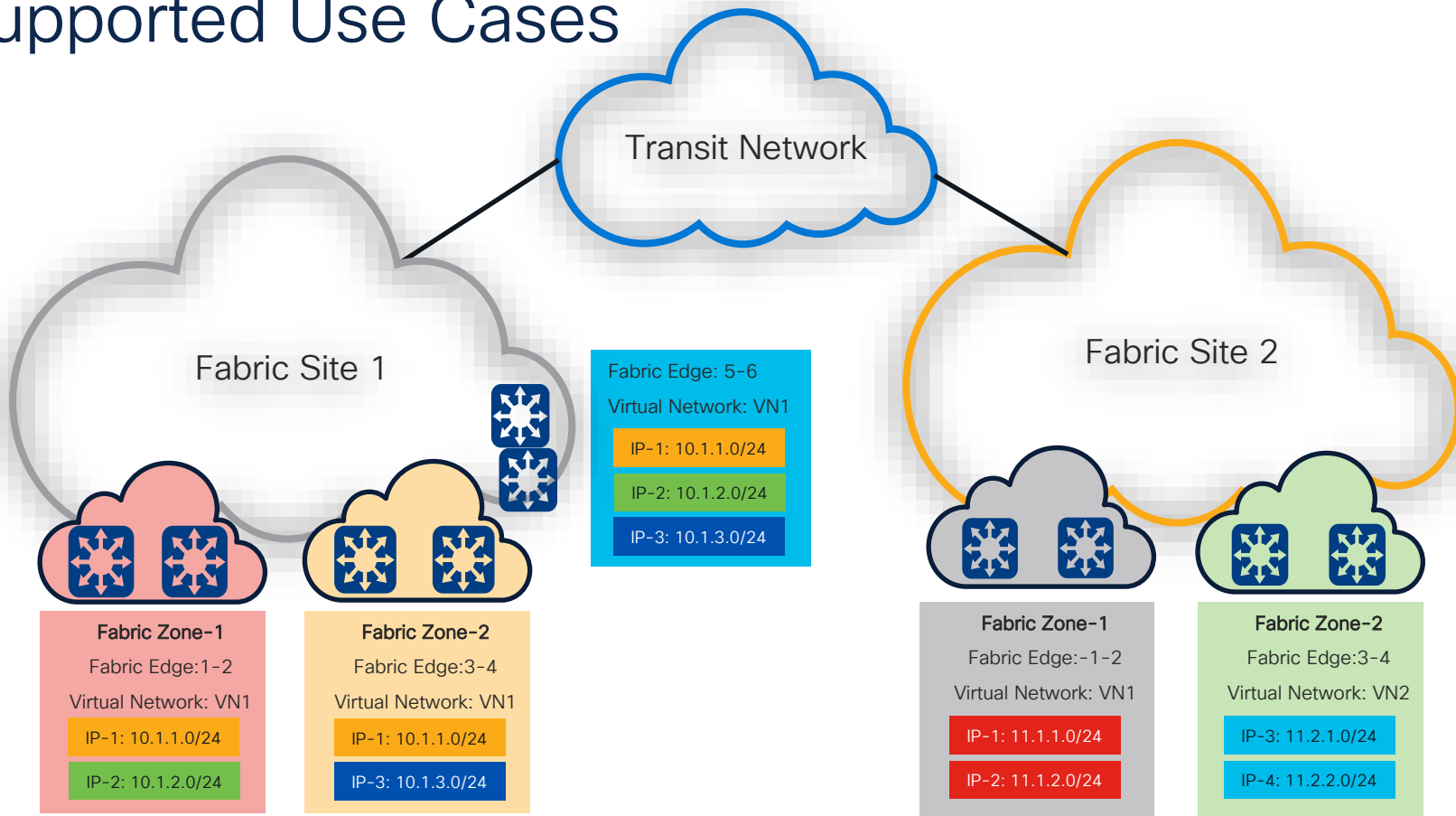
# Fabric Zone Considerations & Supported Use Cases

# 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



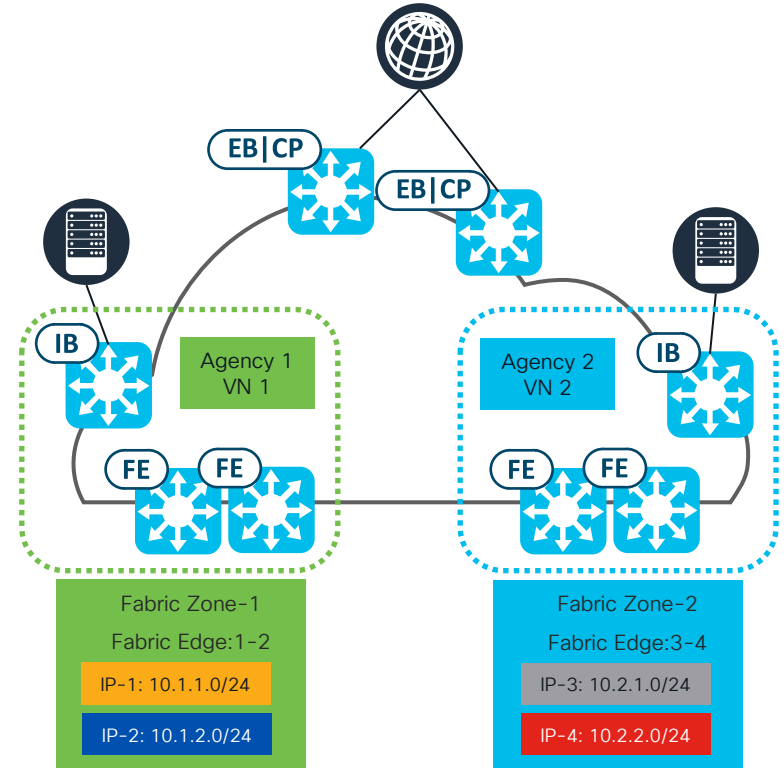
# Fabric Performance Data Without Fabric Zone in a Single Site

- **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](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

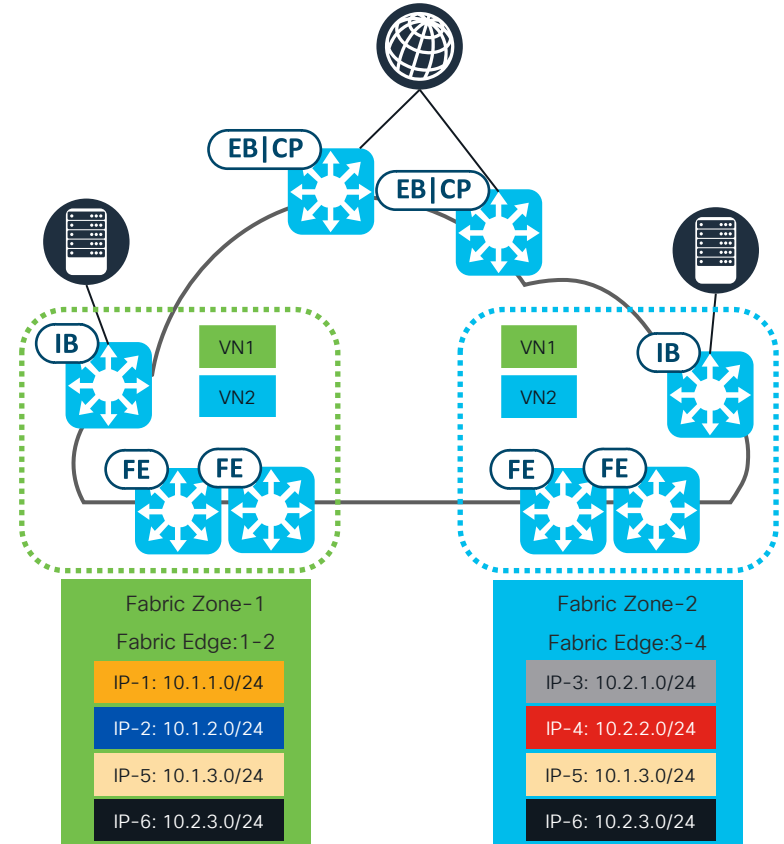
# Case Study 1 – Zones per VN

- 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



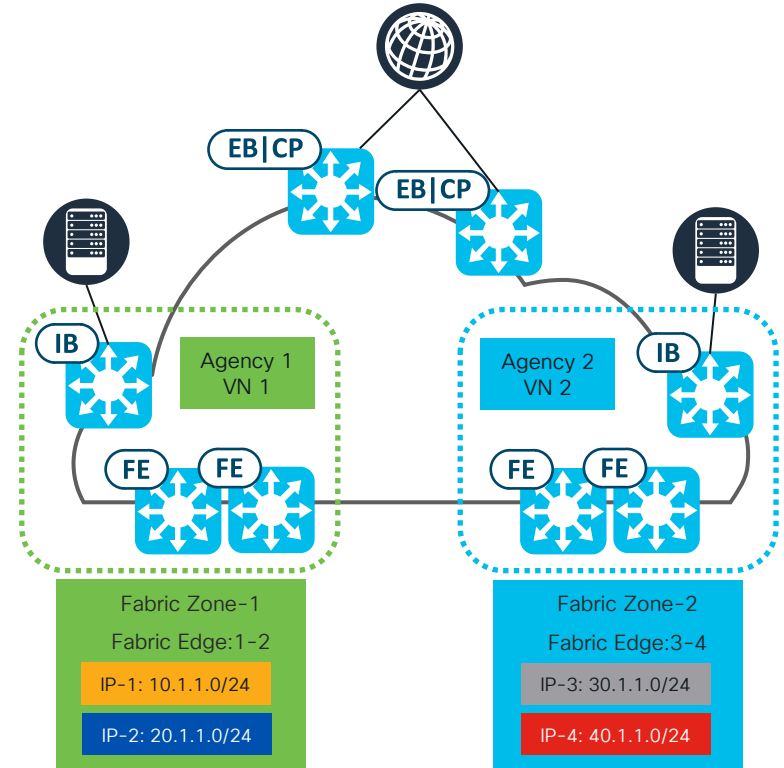
# Case Study 1 – Other Requirements

- 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

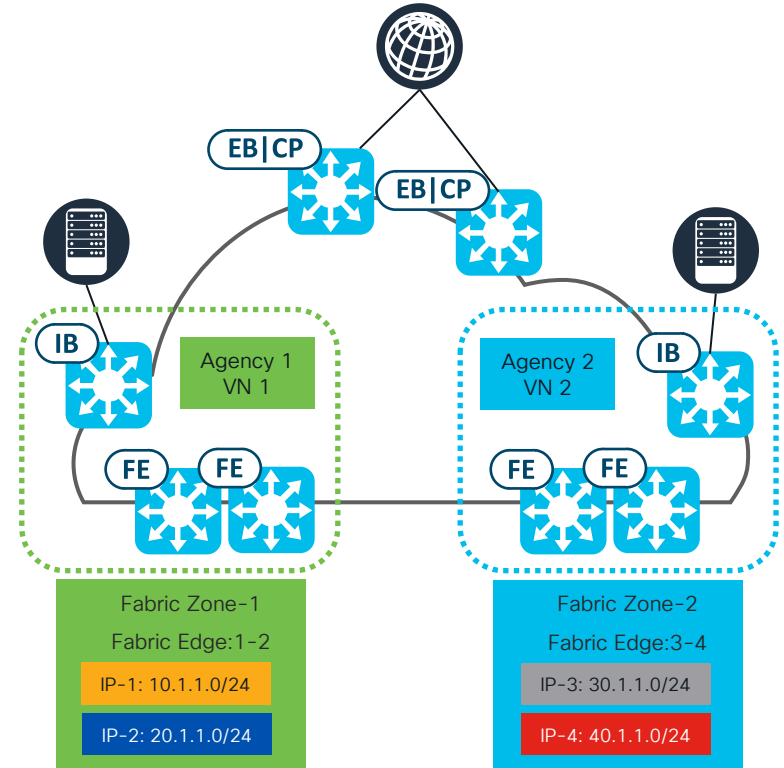
- Customer B requires Critical VLAN per VN instead of one critical VLAN for all Virtual Networks (VNs) from current DNAC automation due to security concerns between VNs
- Each VN needs to elect one critical IP pool for local DC and internet access in the event of all PSNs are not available for the NADs





# 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)

Edit Virtual Network: Agency1\_VN

[< Back](#)

IP Address Pool  
**Agency2\_Critical** (20.1.2.0/24 | 24...

Authentication Policy  
**20\_1\_2\_0-Agency1\_VN**

Scalable Group Traffic

☐ Layer-2 Flooding ☒ Critical Pool ☐ Common Pool ☐ Wireless Pool

Edit Virtual Network: Agency1\_VN

[< Back](#)

IP Address Pool  
**Agency1\_30\_voice\_pool** (30.1.1.0...

Authentication Policy  
**30\_1\_1\_0-Agency1\_VN**

Scalable Group Traffic  
**Voice**

☐ Layer-2 Flooding ☒ Critical Pool ☐ Common Pool ☐ Wireless Pool

- 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
```

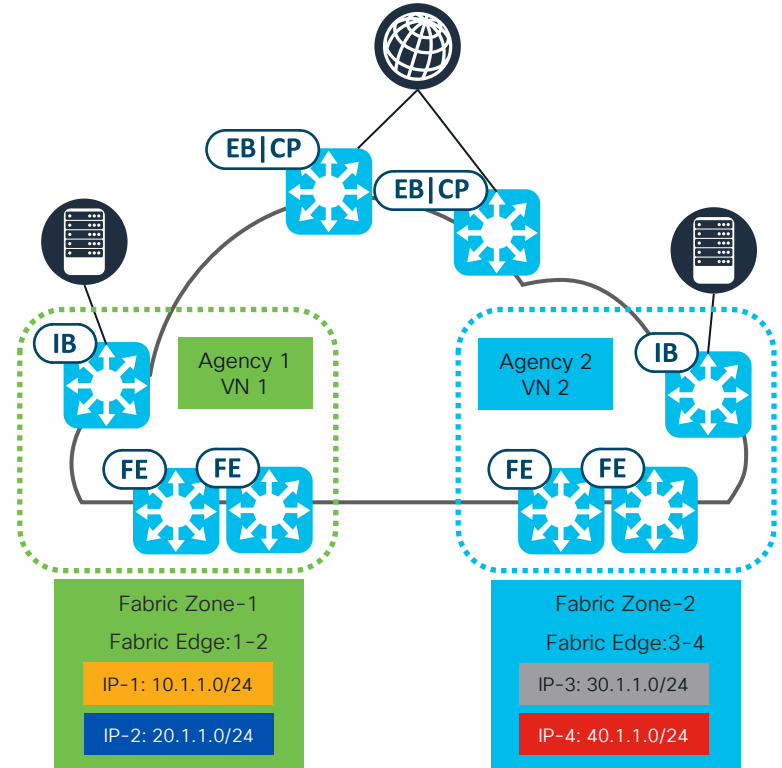
```
interface Vlan1021
description Configured from Cisco DNAC
mac-address 0000.0c9f.f85e
vrf forwarding Agency1_VN
ip address 20.1.1.1 255.255.255.0
ip helper-address 172.16.10.28
ip helper-address 172.16.20.28
no ip redirects
ip route-cache same-interface
no lisp mobility liveness test
lisp mobility 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

**1** Cisco DNA Center

Fabric Sites > SJ1

SJ1 View site hierarchy

SITE SUMMARY

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

Fabric Infrastructure Host Onboarding

**2** More Actions

**3** Edit Fabric Zone

The Internet

SJ1\_CB.ma.com

SJ1\_IN1.ma.com

SJ1\_E1.ma.com

SJ1\_E2.ma.com

SJ1\_E3.ma.com

# SDA: Fabric Zone in Brownfield

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

☰ Cisco DNA Center

Create a Fabric site and Fabric Zones

⌂

### 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

LEGEND Fabric Site

Find Hierarchy

4

Global (2)

San\_Jose (3)

✓

SJ1 (2)

☒ SJ1\_F1

☒ SJ1\_F2

Exit

Review

Back

Next

# SDA: Fabric Zone in Brownfield

## ❑ Step 3: Select Fabric Zone Virtual Network

➤ Provision → Virtual Networks → Select Fabric Site

5

Cisco DNA Center

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

6

Select Fabric Site

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

Find Hierarchy

▼ Global

▼ San Jose

7

SJ1

SJ1\_F1 FZ

SJ1\_F2 FZ

# 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
<a href="#">CAMPUS_VN</a>	4099	--	1:4099	2	2/3	-- (0/2 Fabric Sites)	🟢 (1/2 Fabric Sites)	--	⋮
<a href="#">DEFAULT_VN</a>	4098	--	1:4098	0	0/3	-- (0/0 Fabric Sites)	-- (0/0 Fabric Sites)	--	⋮
<a href="#">GUEST_VN</a>	4100	--	1:4100	0	2/3	-- (0/2 Fabric Sites)	-- (0/2 Fabric Sites)	--	⋮
<a href="#">INFRA_VN</a>	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

1

Cisco DNA Center

Fabric Sites > All Fabric Sites

All Fabric Sites

Summary

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

2

Search Table

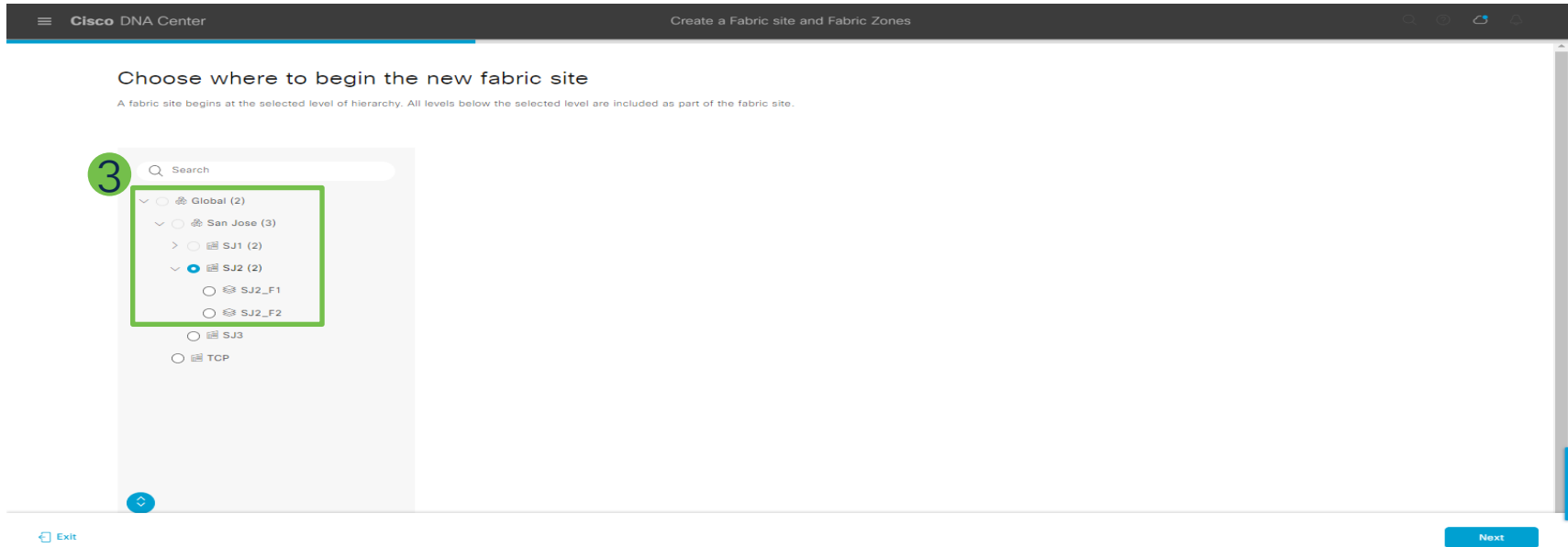
+ Add Fabric site

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

# 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

Cisco DNA Center

Create a Fabric site and Fabric Zones

### Optional: 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.

☐ 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

LEGEND

Fabric Site

Global (2)

San Jose (3)

SJ2 (2)

☒ SJ2\_F1

☒ SJ2\_F2

Exit

Review

Back

Next

CISCO Live!

#CiscoLive

BRKENS-3833

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

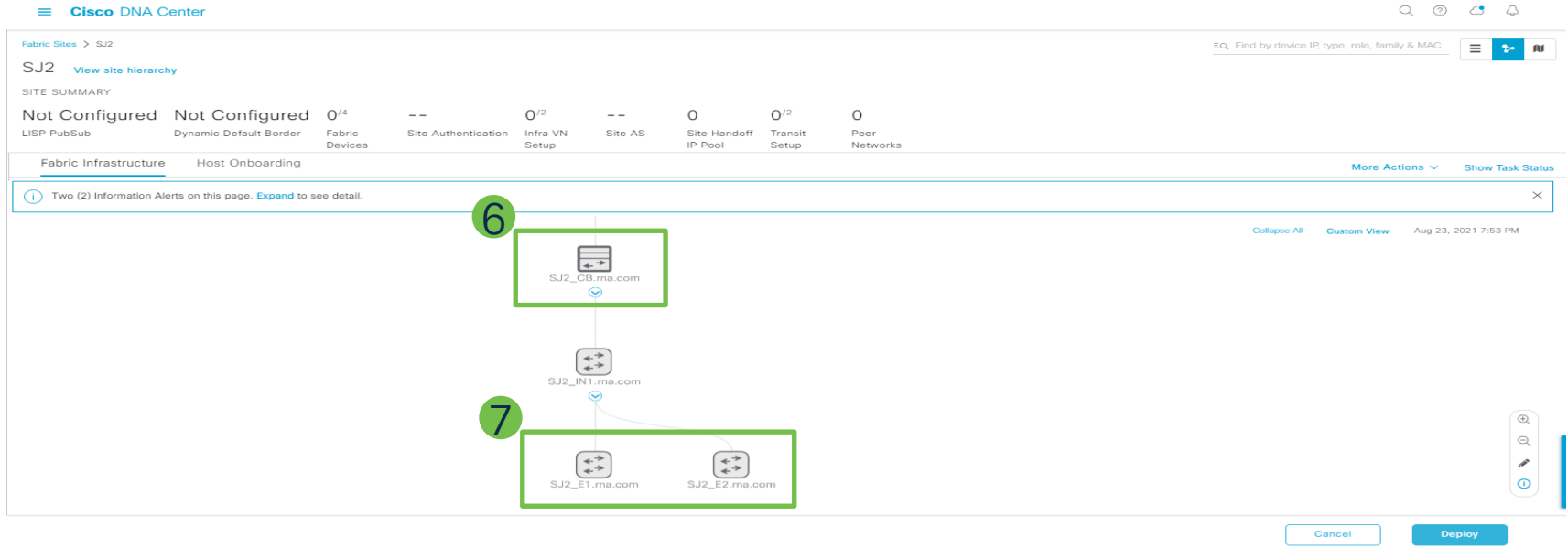
32



# 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

The screenshot shows the Cisco DNA Center interface for managing Virtual Networks. The page title is 'Virtual Networks' with a sub-header 'Fabric Site: SJ1/SJ1\_F1 FZ'. Below the title, there are tabs for 'Layer 3 (1)' and 'Layer 2 (3)'. A sidebar on the left shows a 'SUMMARY' section with a 'Multicast (2)' dropdown and checkboxes for 'Configured' and 'Not Configured'. A green circle with the number '8' is next to the 'Configured' checkbox. The main area contains a table with columns: Name, L3VNID, Gateways, Multicast, Remote Exit, and Actions. The table has one row with the name 'VN1', L3VNID '4100', Gateways '3', Multicast 'Not Configured', and Remote Exit '--'. A green box highlights the 'VN1' cell. Another green circle with the number '9' is next to the 'Actions' column, which contains a dropdown menu with options 'Create Gateways' and 'Delete gateways'. A green box highlights this dropdown menu.

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

# 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

## 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



## 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



## 4 Enablement Workflow

DNAC UI friendly workflow support both brownfield and greenfield migration



## 3 Deployment Case Studies

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



# 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](https://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

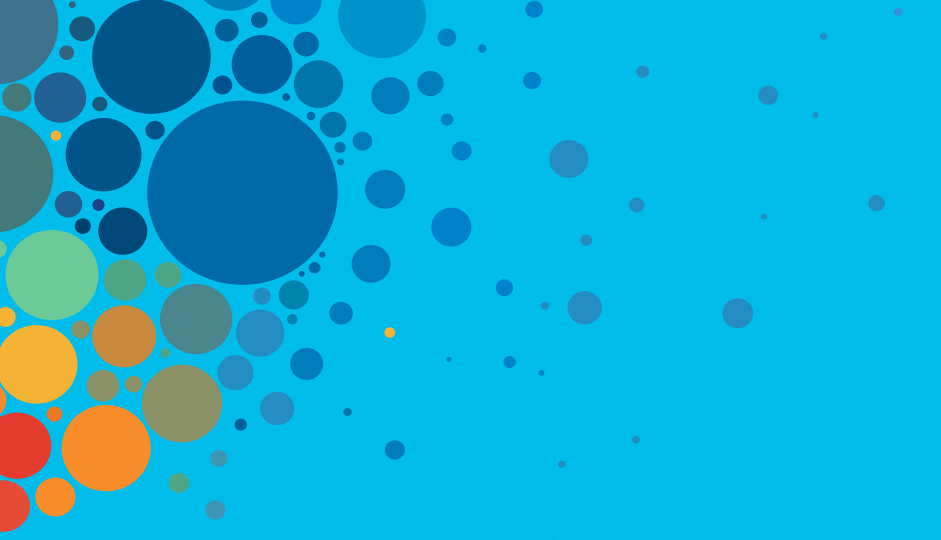
180-day certification prep program with learning and support

### 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](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*



#CiscoLive