

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, triangular rays in various shades of blue and cyan, creating a sunburst effect that spreads across the right half of the image.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Cisco SD-Access Best Practices

Design and Deployment

Mahesh Nagireddy
Technical Marketing Engineering, Technical Leader
CCIE R&S
BRKENS-2502

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

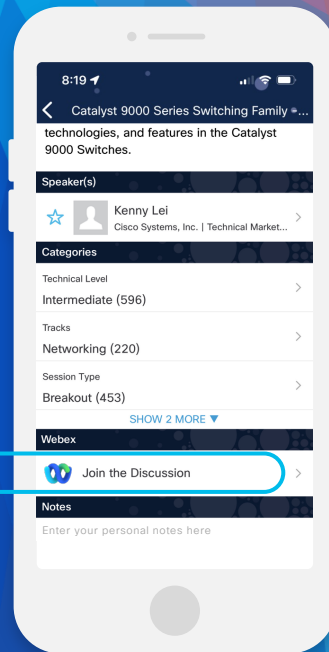
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2502>

Agenda

- Introduction
- SD-Access Scale & Readiness
- SD-Access Single-Site Design Options
- SD-Access Multi-Site Design Options
- SD-Access Policy Design Options

SD-Access Platform Support

Digital Platforms for your Cisco Digital Network Architecture



For more details: cs.co/sda-compatibility-matrix

Cisco Software-Defined Access Compatibility Matrix

Select Deployment

New Deployment ☒ Upgrade ☐

New Deployment

Release: 2.2.3.5 (recommended release)

Device Role:
 ISE
 Fabric Edge
 Fabric Border and Control Plane
 Wireless
 Extended Node or IOT Extension for SD-Access
 SD-WAN Integrated Domain Solution
 Collocated SD-Access Border, Control Plane and SD-WAN WAN Edge
 SD-WAN Controller

Submit

[Site Map](#) [Terms & Conditions](#)

Platform support based on the Fabric Role

Cisco Software-Defined Access Compatibility Matrix

Select Deployment

New Deployment ☒ Upgrade ☐

New Deployment

Release: 2.2.3.5 (recommended release)

Device Role: Fabric Border and Control Plane

Submit

SD-Access Compatibility Matrix for Cisco DNA Center 2.2.3.5 (recommended release)

Device Role	Device Series	Device Model	Recommended Release	Supported Release
Fabric Border and Control Plane	Cisco ASR 1000-X and 1000-HX Series Aggregation Services Routers	ASR 1001-HX ASR 1001-X ASR 1002-HX ASR 1002-X ASR 1006-X (RP2) More ...	IOS XE 17.6.2	IOS XE 17.6.x IOS XE 17.5.x IOS XE 17.3.x IOS XE 16.9.1s IOS XE 16.9.2 More ...

Supported Hardware, Software and Recommended Version for all Cisco SD-Access components

Cisco SD-Access Scale & Readiness

[Cisco DNA/Catalyst Center 2.3.5 Data Sheet](#)

Cisco Catalyst Center Fabric Readiness and Compliance Checks

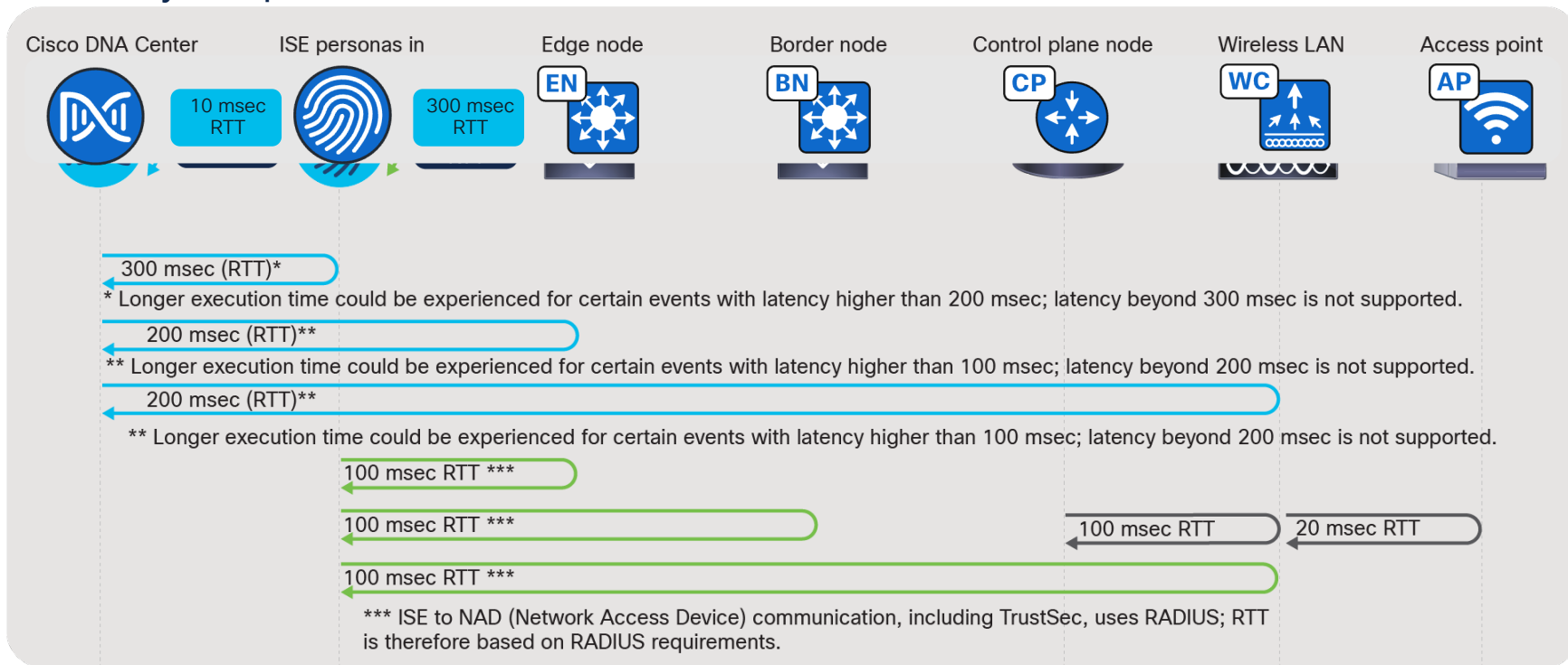
- Hardware Version
- Image Type
- Software Version
- Software Licenses

Software Licensing

- Cisco DNA Advantage/Cisco DNA Premier License

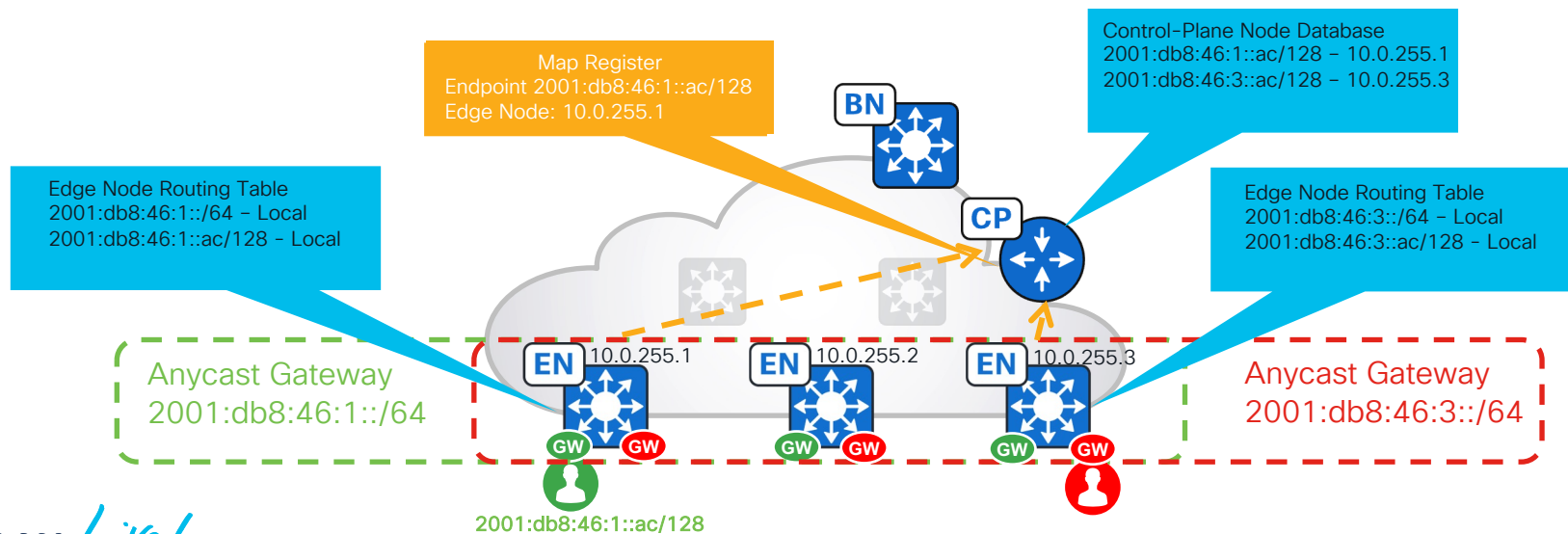
Cisco SD-Access

Latency Requirements



V4 and V6 support in SD-Access

Cisco Catalyst Center Physical Interfaces	: V4 / V6
Cisco Catalyst devices	: V4 / V6 / Dual-Stack
Cisco SD-Access Underlay Devices	: V4 only
Cisco SD-Access Overlay Clients	: V4 / V6 / Dual-Stack
Cisco ISE	: V4 / V6 / Dual-Stack
Cisco Catalyst Center to Cisco ISE	: V4 only



Cisco SD-Access

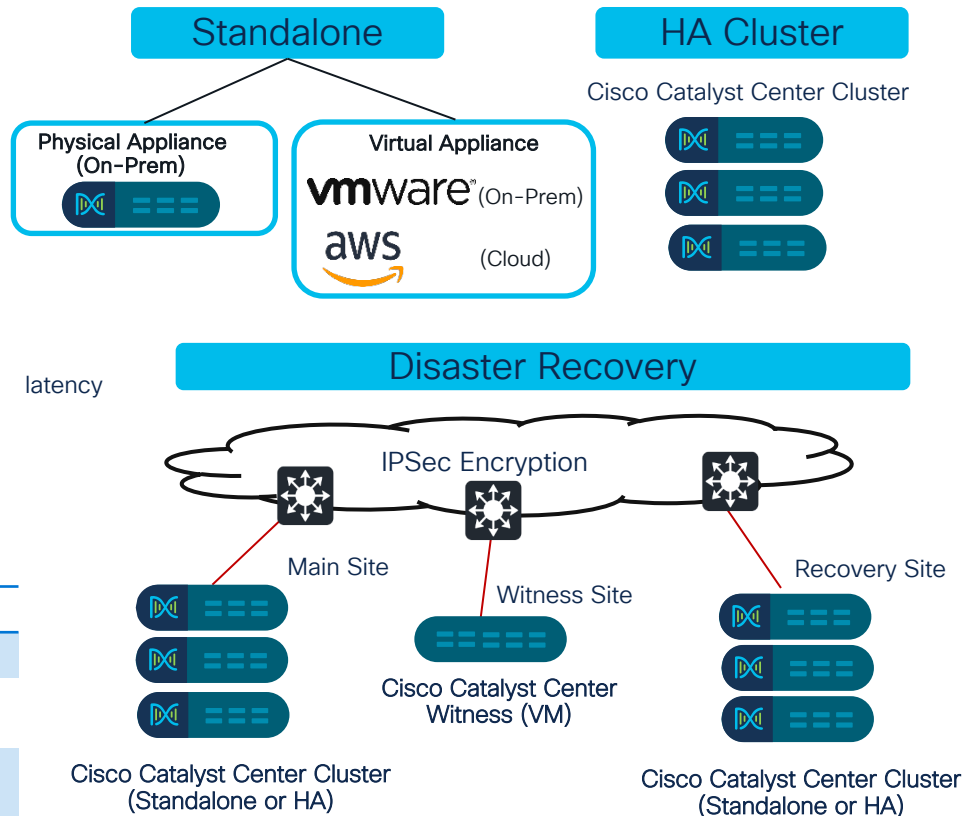
Cisco Catalyst Center Deployment

Deployment Types

- Standalone
 - On-Prem Physical Appliance
 - Virtual Appliance on Cloud(AWS)
 - On-Prem Virtual Appliance on ESXI(VMWare)
- Cluster for High Availability (HA)
 - Cluster interconnected with 10Gbps interface with <10msec latency
- Disaster Recovery (DR) for network downtime
 - Cluster connected with 1Gbps interface between main site and recovery site with <350 msec latency

Failure detection and recovery

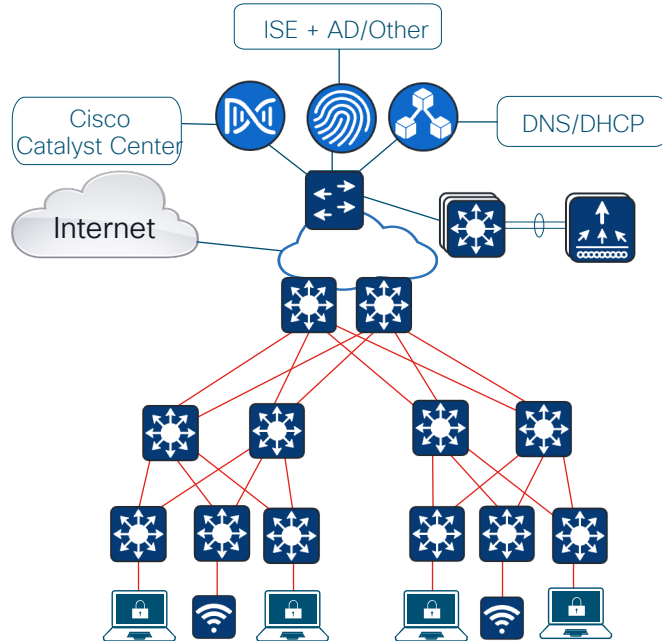
	High Availability	Disaster Recovery
Failure Detection time	5 minutes	3 minutes
Time taken to failover on failure detection	7-13 minutes	15-30 minutes
Failover time behavior	Service down up to 7 minutes	Service down up to 30 minutes
Failback	Automatic	Manual



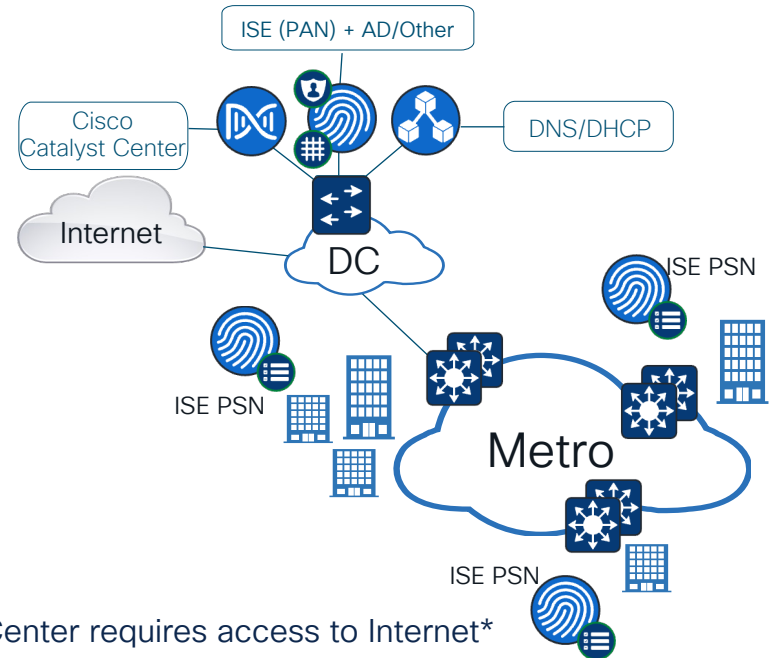
Cisco SD-Access Architecture

Where do I place Critical/Shared Services

Local DC or Services Block



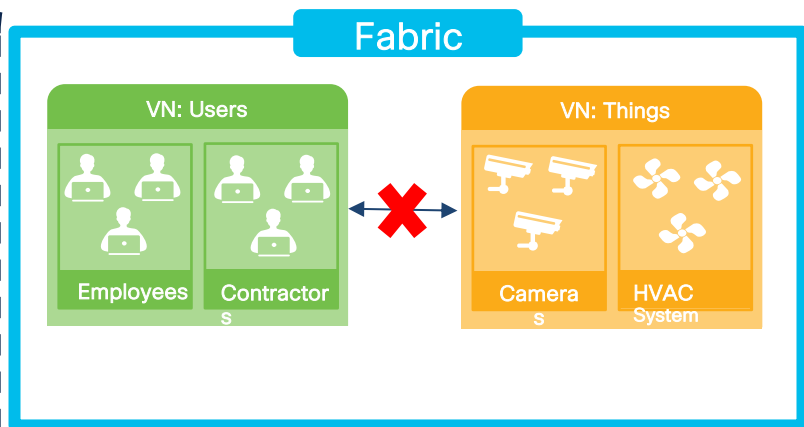
Remote DC



Cisco Catalyst Center requires access to Internet*

Cisco SD-Access Policy Segmentation Strategy

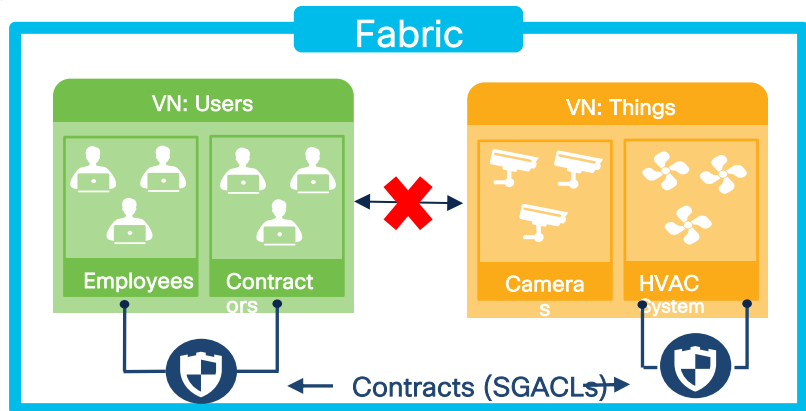
Macro Segmentation



Virtual Network (VN)

- VN = VRF = LISP Instance ID
- Complete Isolation between VN's
- Default Policy: No communication

Micro Segmentation



Security Group Tag (SGT)

- Location Independent Policy
- Simple Permit/Deny/Contracts
- Default Policy: Permit/Deny

SD-Access Flexible Deployment Options

I am installing a new network and want zero trust

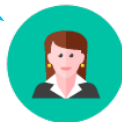


Macro Segmentation
Prerequisite: Routed Access

Endpoint, Policy & Trust Analytics
Prerequisite: ISE

Micro Segmentation

I have an existing network and want zero trust



Have ISE

Endpoint, Policy & Trust Analytics
Prerequisite: ISE

Macro Segmentation
Prerequisite: L2 or Routed Access

Micro Segmentation

Don't have ISE

Macro Segmentation with Layer 2 Switched Access

Endpoint, Policy & Trust Analytics
Prerequisite: ISE

Micro Segmentation



- Fabric Mandatory
- Fabric or Non-Fabric

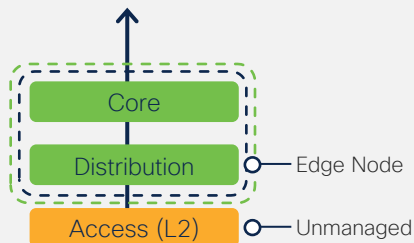
SD-Access Flexible Deployment Options

Migration Options

Macro segmentation
Micro segmentation

NEW

Fabric with unmanaged Layer 2 switched access*

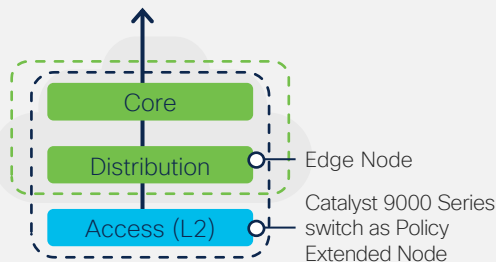


- Use case:** Keep your existing unmanaged switches
- Segmentation starts at distribution layer
 - Integrated wired and wireless

Benefit: Allow tenants to bring their own network.

NEW

Fabric with managed Layer 2 switched access

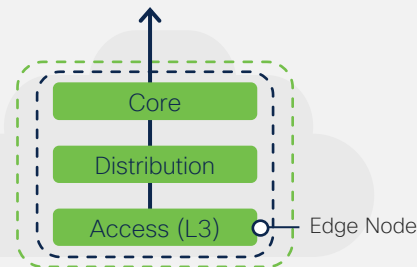


- Use case:** Retain Layer 2 access
- Extend segmentation down to Layer 2
 - Integrated wired and wireless

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 with Cisco Catalyst Center release 2.2.1.0, generally available in late Q2 CY 2021

Cisco Catalyst Center

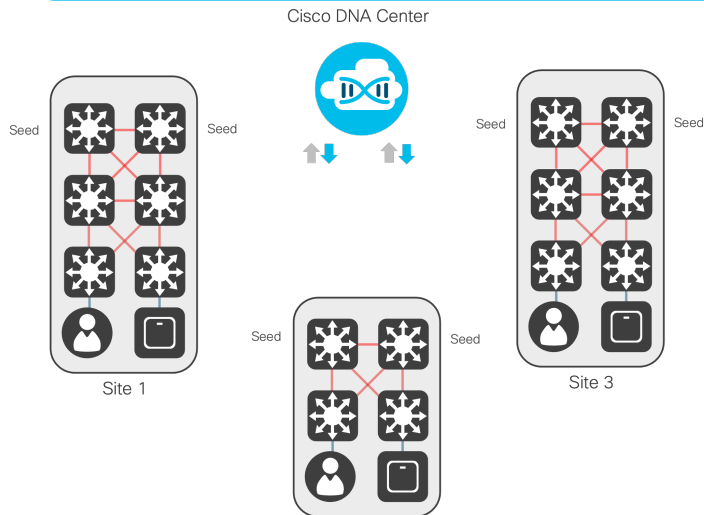
Device Onboarding options

Manual | Semi-Automated Underlay

Device-by-Device onboarding and configuration either manually or through Cisco Plug-and-Play.

Automated Underlay(Lan Automation)

Turnkey solution to onboard multiple switches with image management and best-practices configuration.



LAN Automation Enhancements 2.3.5.0

- Dedicated LAN Automation landing page
- 5 Simultaneous LAN Automation sessions with one session per site
- Day N Add or Delete L3 links

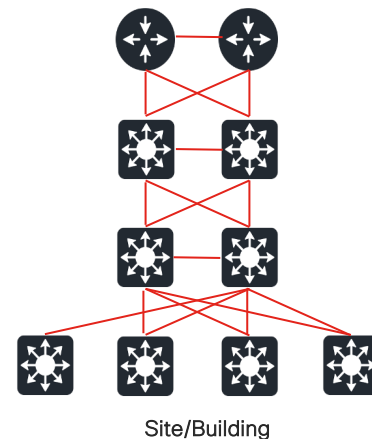
LAN Automation Enhancements 2.3.7.0

- Workflow now support /27,/28 and /29 LAN pools
- Deterministic of loopback IP addresses(Day 0 & Day N*)

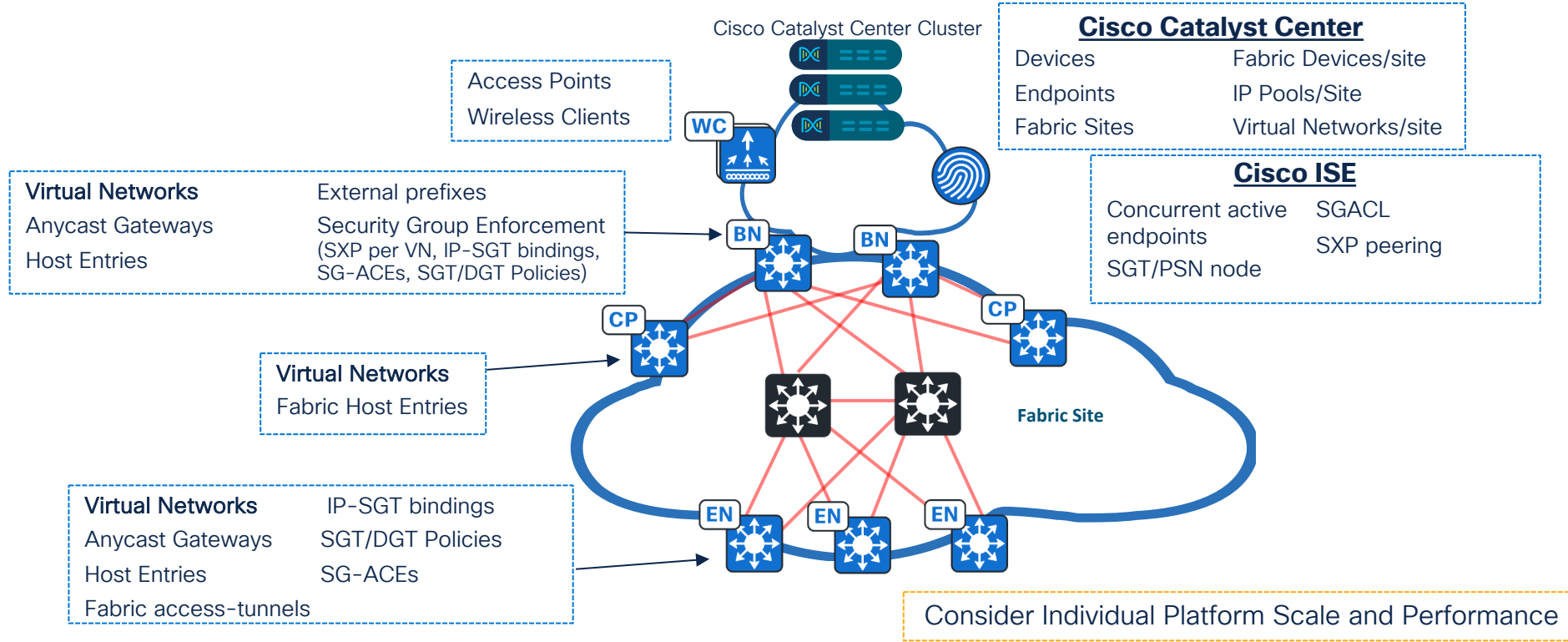
Fabric Network Infrastructure

Robust Underlay Infrastructure deployment

- Routed Access Network
- Any routing protocol
- Resilient and Redundant fast-converged connectivity with ECMP, BFD enabled.
- Loopback 0 with /32 host prefix.
- Higher MTU(Jumbo) to accommodate VXLAN encapsulation
 - Else use TCP-Adjust MSS
- Underlay multicast to optimize overlay subnet multicast/broadcast distribution



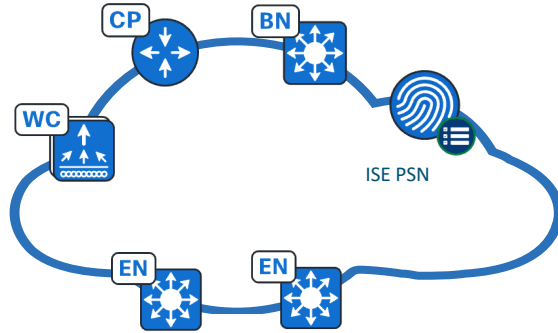
Cisco SD-Access Scale & Readiness



Least Common Denominator (LCD) across the solution elements

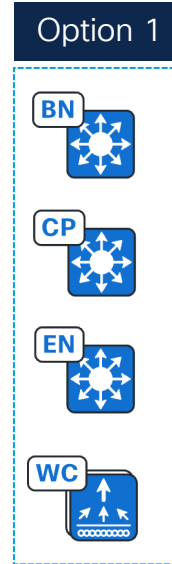
Cisco SD-Access Single-site Design Options

Fabric Site Design Options

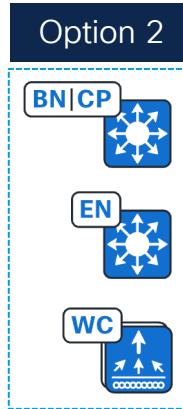
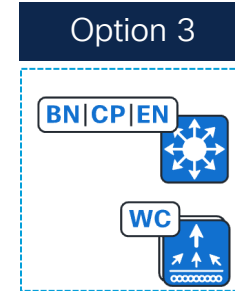
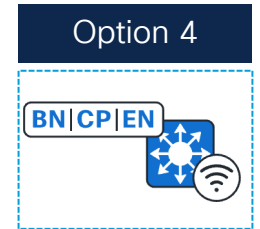


Fabric Site

- Logical construct that contains:
 - Fabric Edge, Border, Control Plane
 - ISE PAN/PSN Node
 - (optional) Wireless LAN Controller, Access Points
 - (optional) Extended Nodes



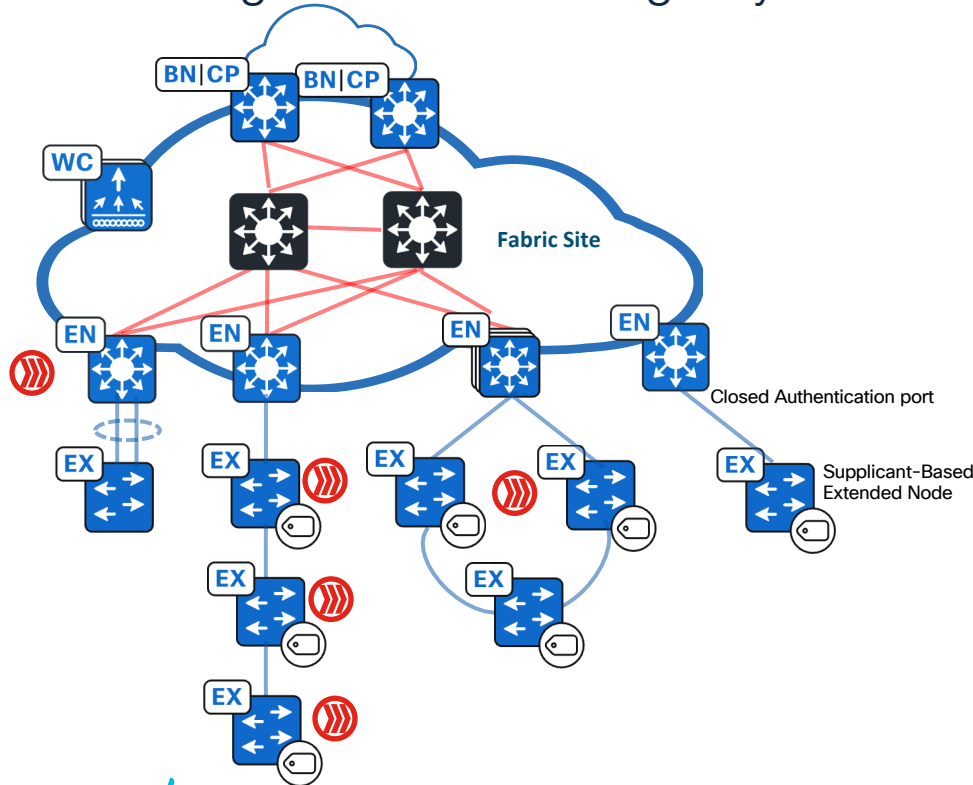
Flexibility in collocating multiple **fabric roles** on the same device*



* Refer to Cisco SD-Access compatibility matrix for latest information

Extended Enterprise

Extending the network using fully automated Layer 2 switch



Two Types

- Extended Node(EX)
- Policy Extended Node(PEN)

Supported devices

Extended Node

- IE3200
- IE3300
- IE4000
- IE4010
- IE5000
- Cat9K*(Ess License)
- ESS-9300
- CDB Series

Policy Extended Node

- IE3400
- IE3400H
- Cat9K*(Adv License)
- IE9300

Supported Topologies

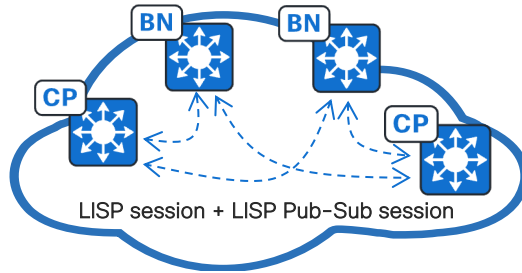
- Daisy Chain(Like device type) up to 18 Nodes
- Ring(Like device type)

Supplicant-Based Extended Node

* - Excluding C9600

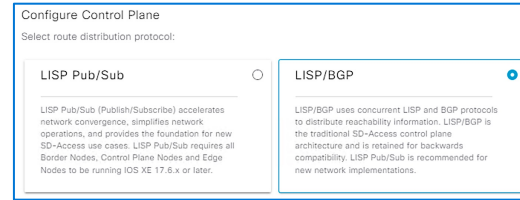
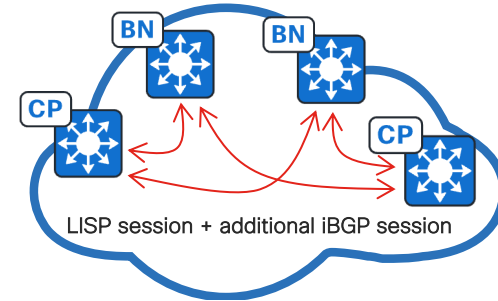
Cisco SD-Access Provision

Fabric Control Plane enhancements



LISP Pub/Sub

- Publisher-Subscriber model provides LISP Instance-ID table subscription from CP, TCP to Border nodes.
- Faster convergence within fabric site (N-S traffic) and across SD-Access transit.
- LISP Pub/Sub provides backbone for fabric innovations such as **Dynamic-Default Border**, **Extranet**, **Active-Backup Internet** (with SD-Transit) and more..
- 4 TCP(Transit Control Plane) Node support

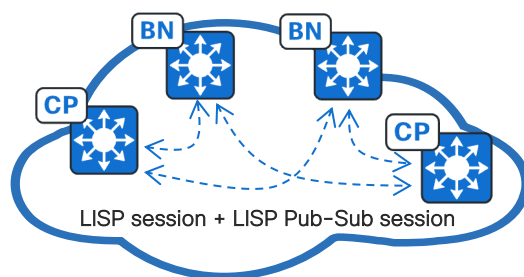
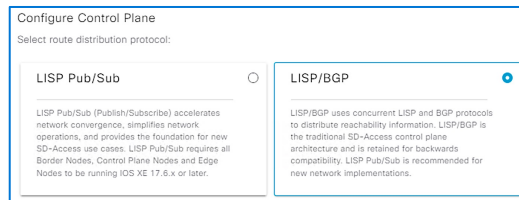
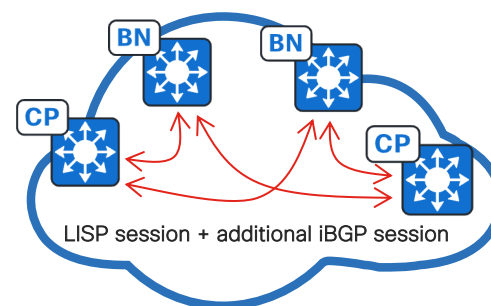


LISP / BGP

- iBGP session between B - CP and B - TCP node to share prefixes.
- Convergence overhead with additional protocol, redistribution and additional lookups
- Troubleshooting complexity with 2 Control-plane protocols
- Only supported Architecture with SD-WAN Integrated solution
- **Only 2 TCP Node support**

Cisco SD-Access Provision

Fabric Control Plane enhancements Cont'd



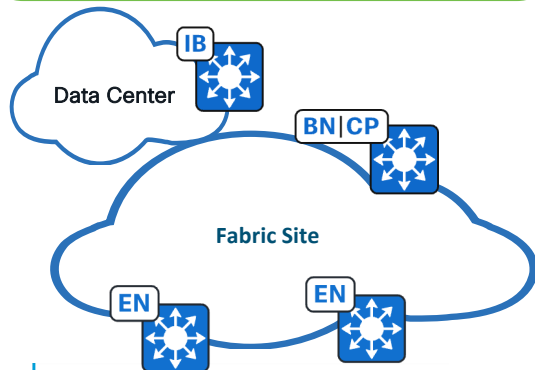
LISP Pub/Sub Benefits

- Remove dependency on BGP
- Simplified Border Routing Designs
- Faster Border Convergence due to faster mapping change updates
- Traffic Path Optimization with Dynamic Default Border
- Backup Internet Option
- Automated route leaking using LISP Extranet

Cisco SD-Access Provision

Border Node Selection

Internal Border (N)
(Rest of Company)



F-FIAB1.demo.local

Layer 3 Handoff Layer 2 Handoff

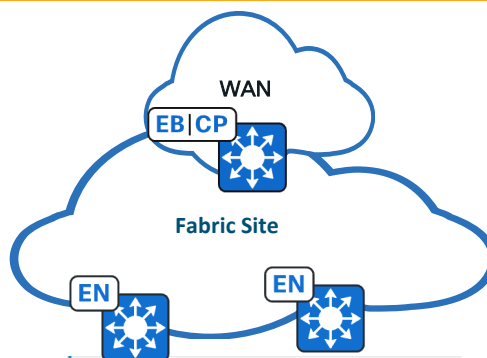
☒ Enable Layer-3 Handoff

Local Autonomous Number

☐ Default to all virtual networks ⓘ

[+ Add Transit/Peer Site](#)

External Border (4 Max)
(Outside)



F-FIAB1.demo.local

Layer 3 Handoff Layer 2 Handoff

☒ Enable Layer-3 Handoff

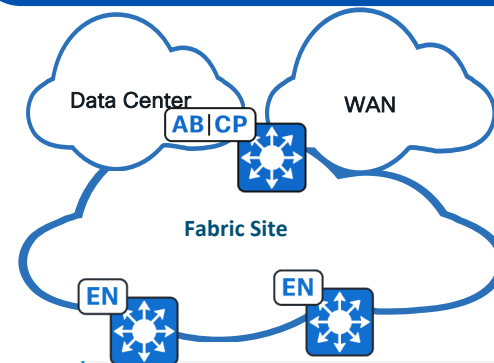
Local Autonomous Number

☒ Default to all virtual networks ⓘ

☒ Do not import external routes ⓘ

[+ Add Transit/Peer Site](#)

Internal + External Border (4 Max)
(Anywhere)



F-FIAB1.demo.local

Layer 3 Handoff Layer 2 Handoff

☒ Enable Layer-3 Handoff

Local Autonomous Number

☒ Default to all virtual networks ⓘ

☐ Do not import external routes ⓘ

[+ Add Transit/Peer Site](#)

Cisco Catalyst Center Provision Authentication Template

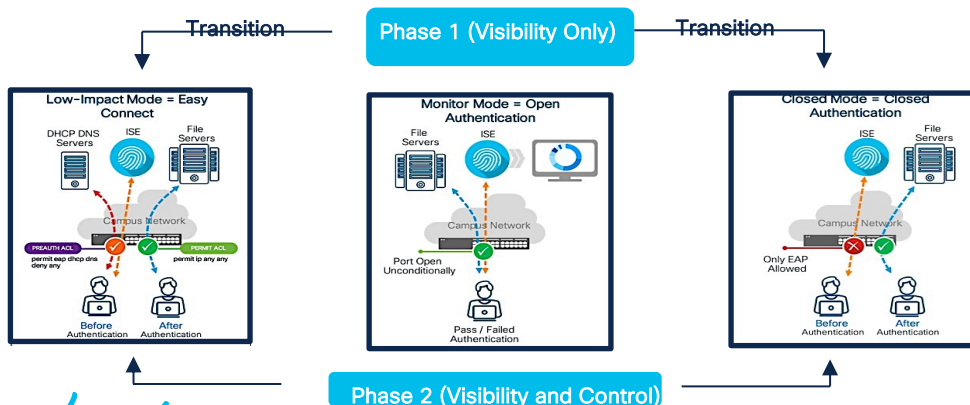
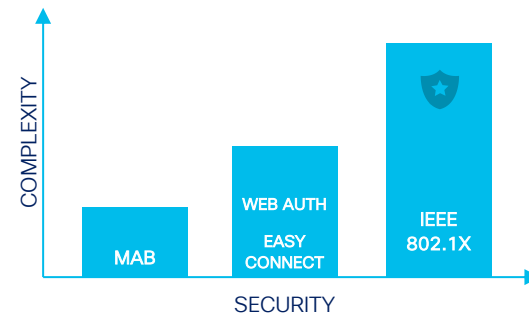
← → ↺ https://172.23.112.31/dna/design/authTemplate

☰ Cisco DNA Center Design · Authentication Template 🔍 ⓘ 🟢 🔔

Last updated: 4:28 PM Refresh

Filter

Name ▲	Type
Closed Authentication	Closed Authentication
Low Impact	Low Impact
Open Authentication	Open Authentication



Cisco Catalyst Center Provision

Closed Authentication Template

Closed Authentication

Deployment Mode: ☐ Open ☒ Closed

First Authentication Order: ☒ 802.1x ☐ MAC Auth Bypass(MAB)

802.1x to MAB Fallback: (3 to 120)

Wake on LAN: ☐ Yes ☒ No

Number of Hosts: ☐ Single ☒ Unlimited

Authentication Timer Settings

Multi-Auth Host Mode

Multi-Domain Host Mode

CLI's pushed with change in Fallback Timers

dot1x timeout tx-period 7

dot1x max-reauth-req 2

Easy Connect

Deployment Mode: ☐ Open ☒ Closed

First Authentication Order: ☒ 802.1x ☐ MAC Auth Bypass(MAB)

802.1x to MAB Fallback: (3 to 120)

Wake on LAN: ☐ Yes ☒ No

Number of Hosts: ☐ Single ☒ Unlimited

Pre-Auth Access Control (Low Impact Mode)

Implicit Action

Deny



Name

IPV4_PRE_AUTH_ACL

Description (Optional)

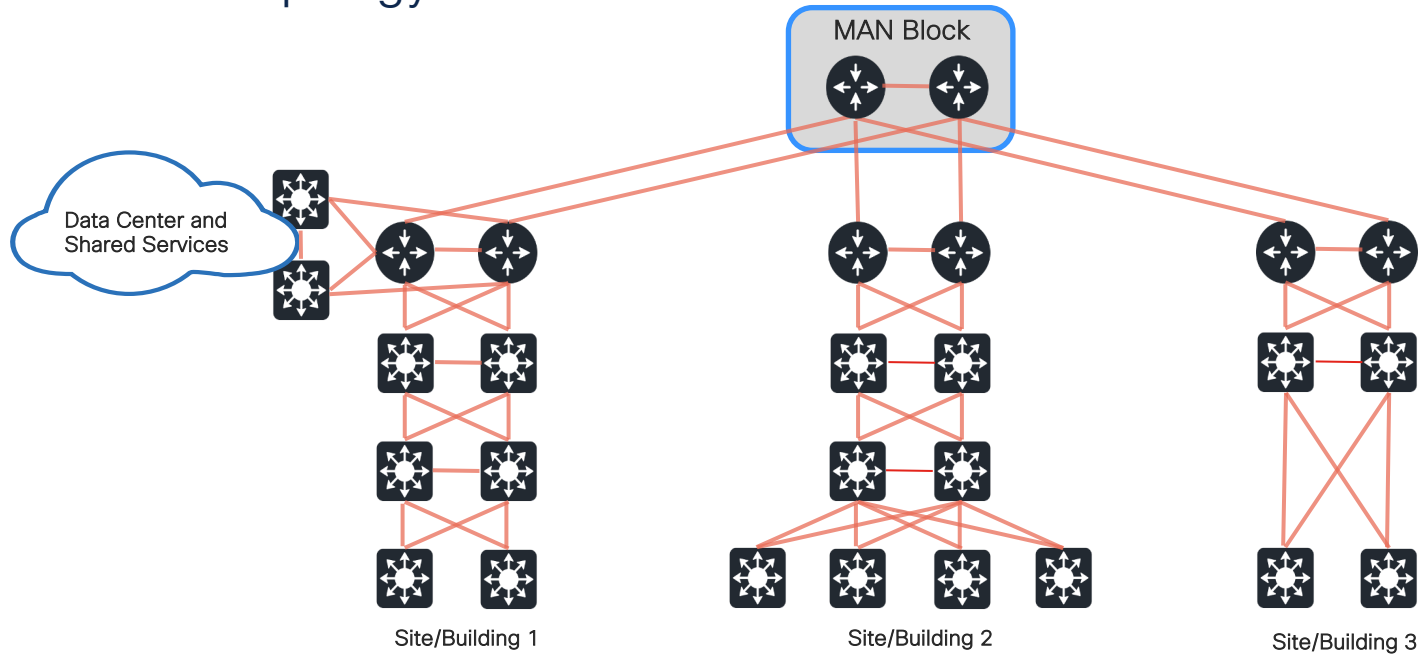
Contracts

Action Protocol Port

Action	Protocol	Port	
permit	udp	bootpc	Delete
permit	udp	domain	Delete

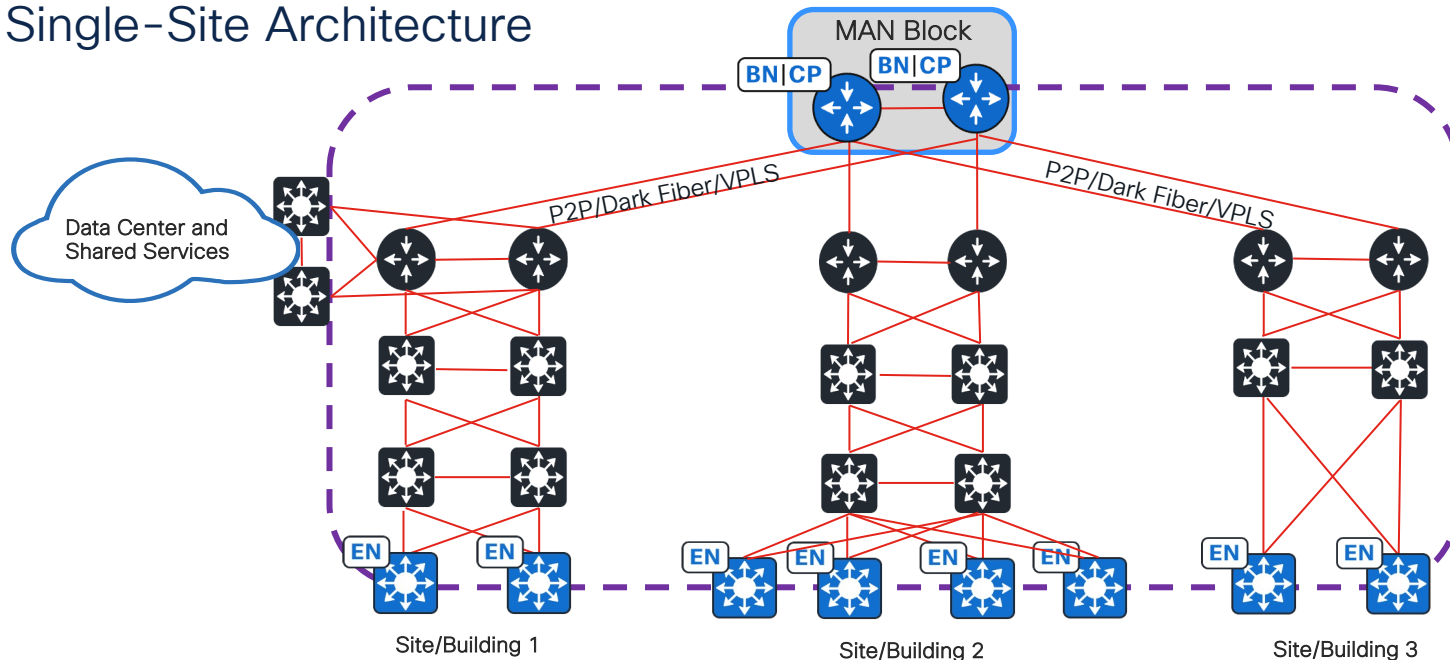
Cisco SD-Access Architecture

Current Topology



Cisco SD-Access Architecture

Single-Site Architecture



Challenges with Single Site Architecture

- One Subnet available across all buildings/Sites
- One Big Failure Domain
- Scale Limitations – IP Pools supported per site or Border/Control plane Scale

SD-Access Fabric Zones

Use Case

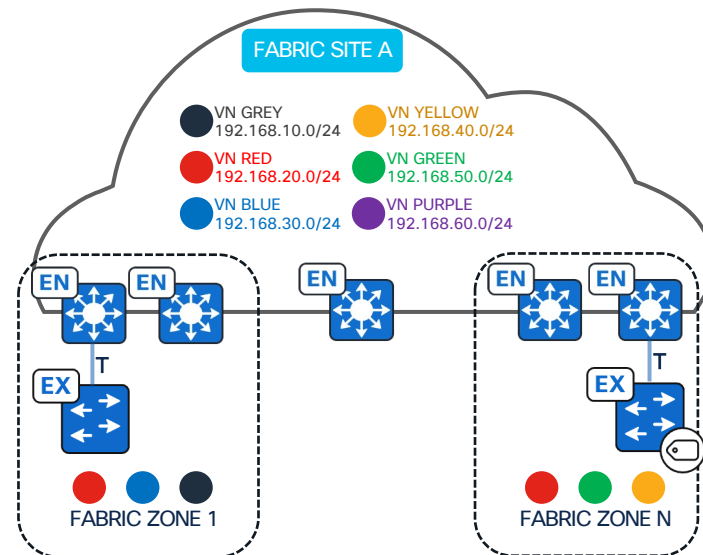
- Before 2.2.3.x, the provisioning scope of an IP Pool was the whole fabric site. For security and/or better fabric site scaling, some customers require granular control of IP Pool provisioning scope.

Details

- SD-Access Fabric Zones are *child sites* of a parent fabric site.
- Edge nodes (EN, EX, PEN) are added to Fabric Zones.
- L3VNs and IP pools are added and provisioned to one or more Fabric Zones.

Considerations

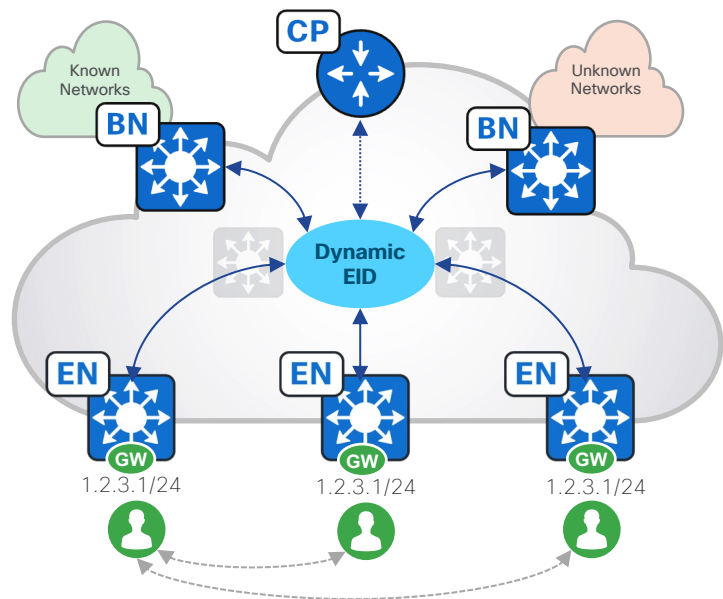
- L3VNs and IP Pools must be assigned to the parent fabric site before assigning to one or more Fabric Zone.
- Only edge nodes (EN, EX, PEN) can be provisioned to a Fabric Zone. Collocated fabric roles (e.g., EN+B, EN + Embedded WLC, etc.) cannot be provisioned to a Fabric Zone.
- EX/PEN must be in same Fabric Zone as parent EN.



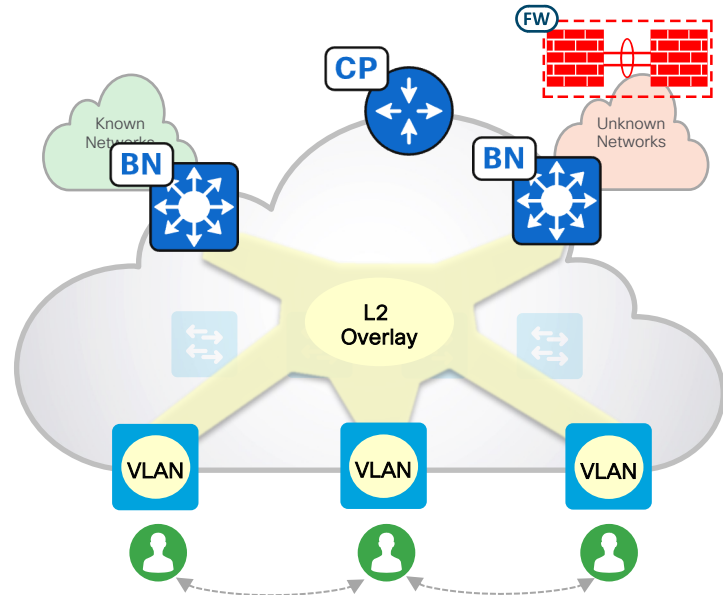
SD-Access Fabric

L3/L2 Overlays

Layer 3 Overlay Stretched Subnets



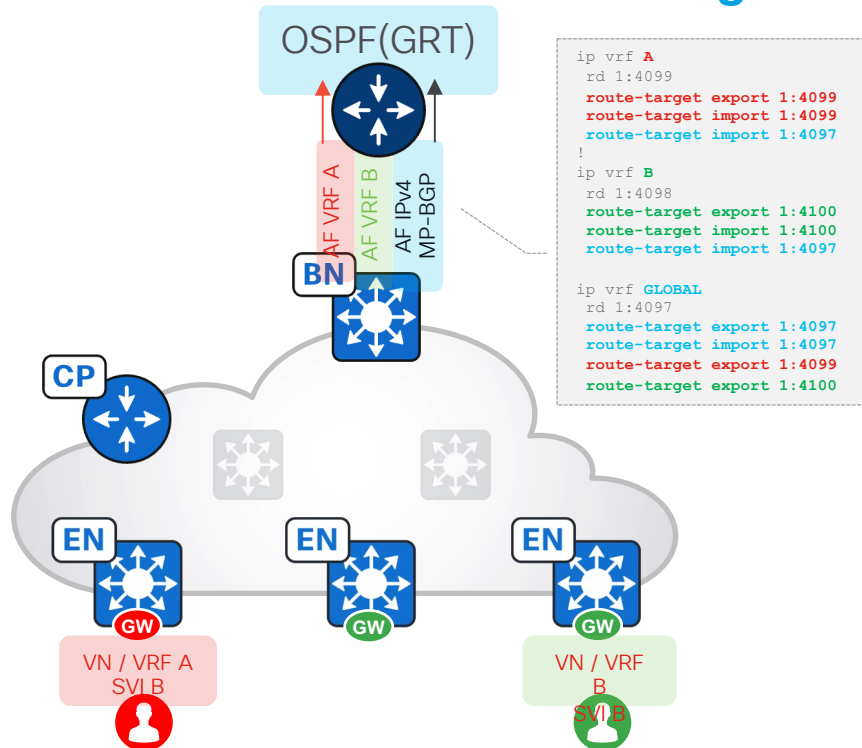
Layer 2 Overlay / GW outside Fabric



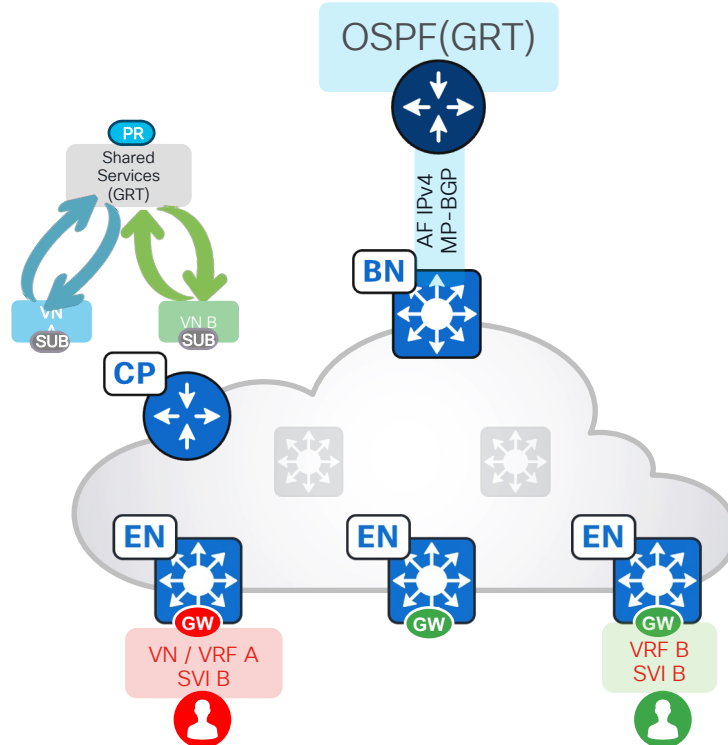
SD-Access Fabric

Border Handoff with Route Leaking

Traditional Route Leaking

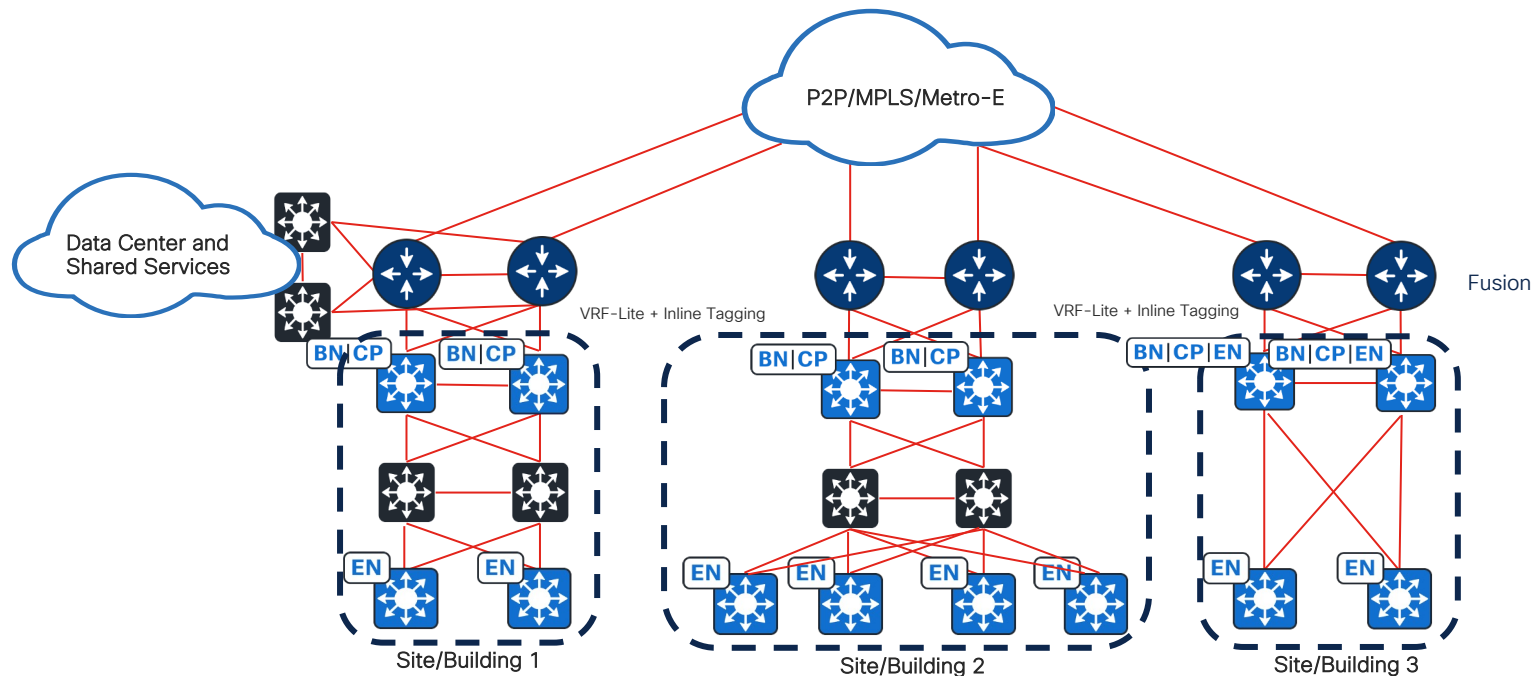


LISP Extranet



Cisco SD-Access Architecture

Multisite Architecture with IP TRANSIT



Challenges with Multisite IP Transit

- No End to End Segmentation.
- Fusion Routers at every site
- No Automation on Fusion device

Cisco SD-Access Architecture

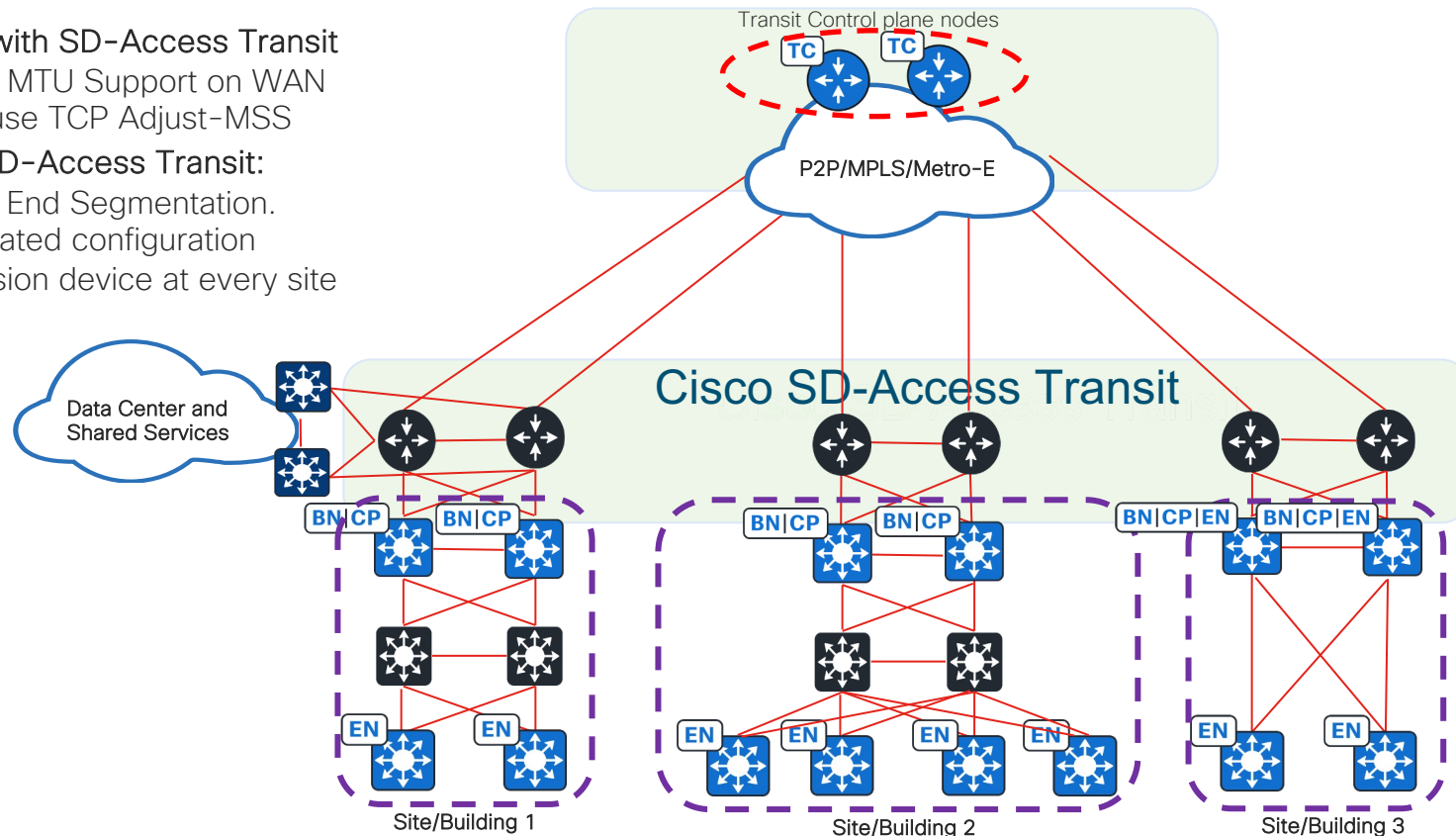
Multisite Architecture with SD-Access Transit

Pre-Requisite with SD-Access Transit

- Higher MTU Support on WAN
- *Else use TCP Adjust-MSS

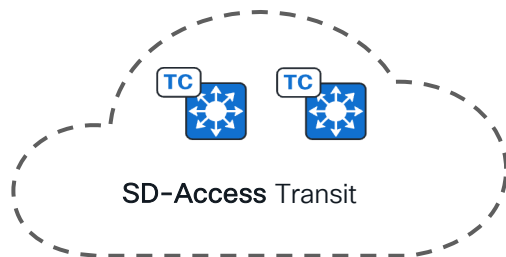
Benefits with SD-Access Transit:

- End to End Segmentation.
- Automated configuration
- No Fusion device at every site



Cisco SD-Access Deployment

Multisite Deployment with SD-Access Transit



SD-Access Transit is a native solution carrying VN and SGT between Fabric sites.

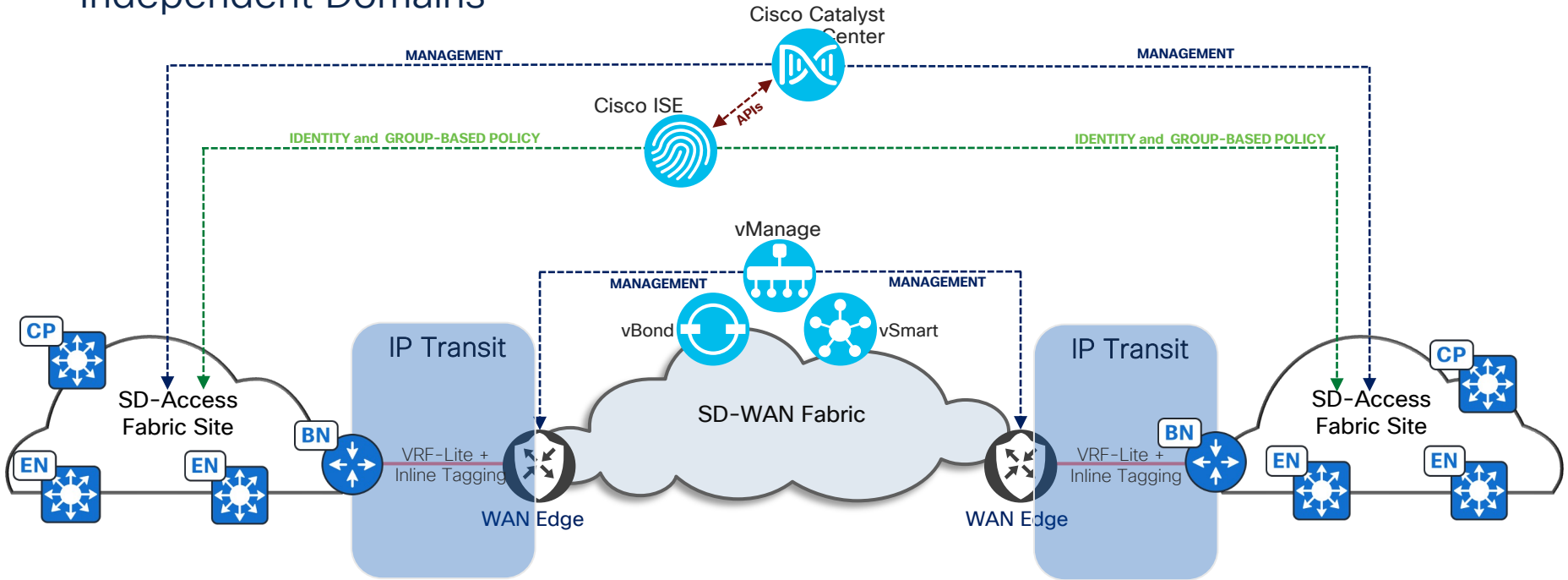
Key Considerations:

- Higher MTU support

- Transit Control Plane nodes are **dedicated devices** with IP reachability to every fabric site's Border nodes
- Transit Control Plane nodes is **not required to be in data forwarding path**
- Transit Control Plane nodes maintains aggregate prefixes of all Fabric sites
- Fabric site Border node should be either External or Anywhere border type to connect to SD-Access Transit.
- SD-Access Transit can be deployed with LISP-BGP or **LISP Pub/Sub**

Multisite Architecture with SD-WAN Transport

Independent Domains

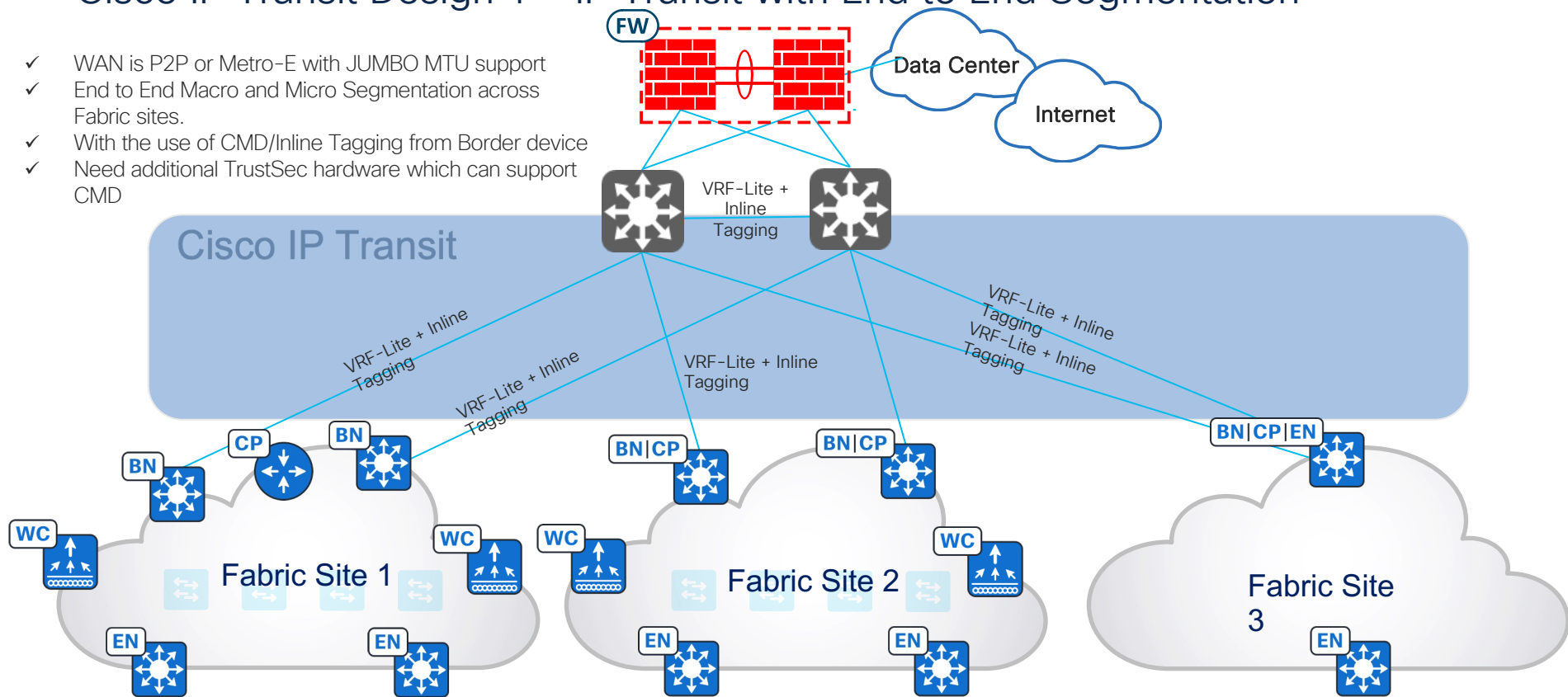


[Cisco SD-Access | SD-WAN Independent Domain Pairwise Integration PDG](#)

Cisco SD-Access Multisite

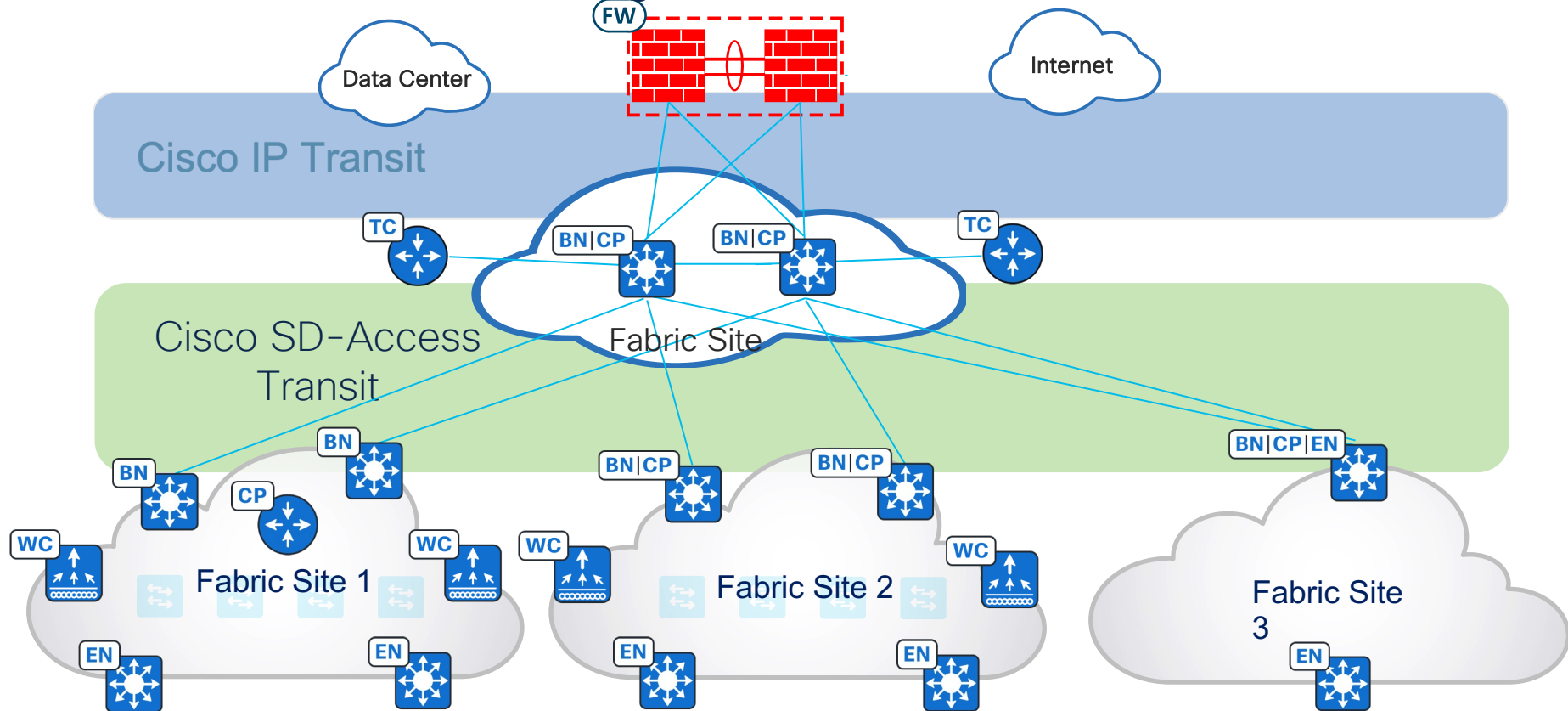
Cisco IP Transit Design 1 - IP Transit with End to End Segmentation

- ✓ WAN is P2P or Metro-E with JUMBO MTU support
- ✓ End to End Macro and Micro Segmentation across Fabric sites.
- ✓ With the use of CMD/Inline Tagging from Border device
- ✓ Need additional TrustSec hardware which can support CMD



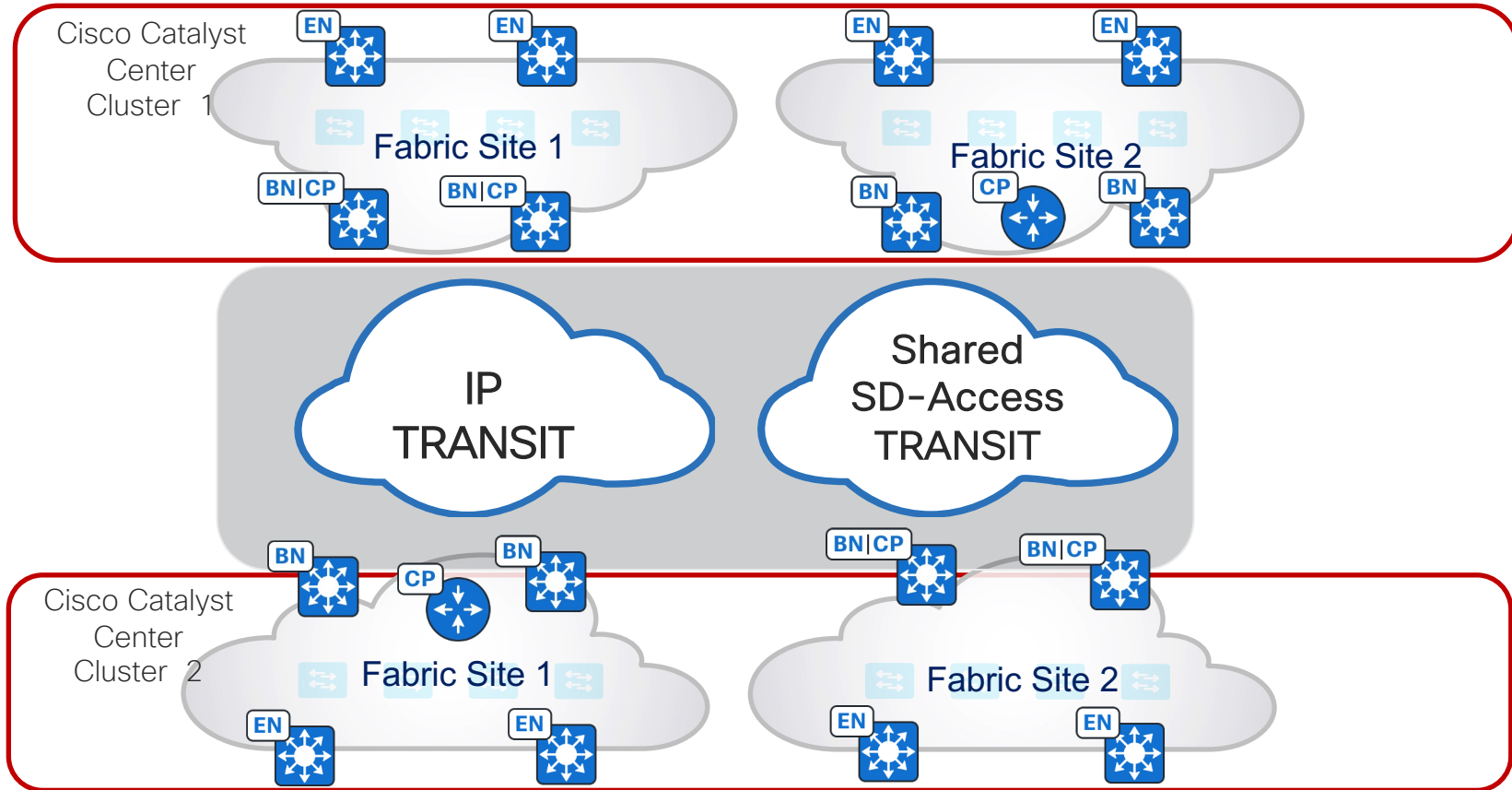
Cisco SD-Access Multisite

Cisco SD-Access Transit Design 1



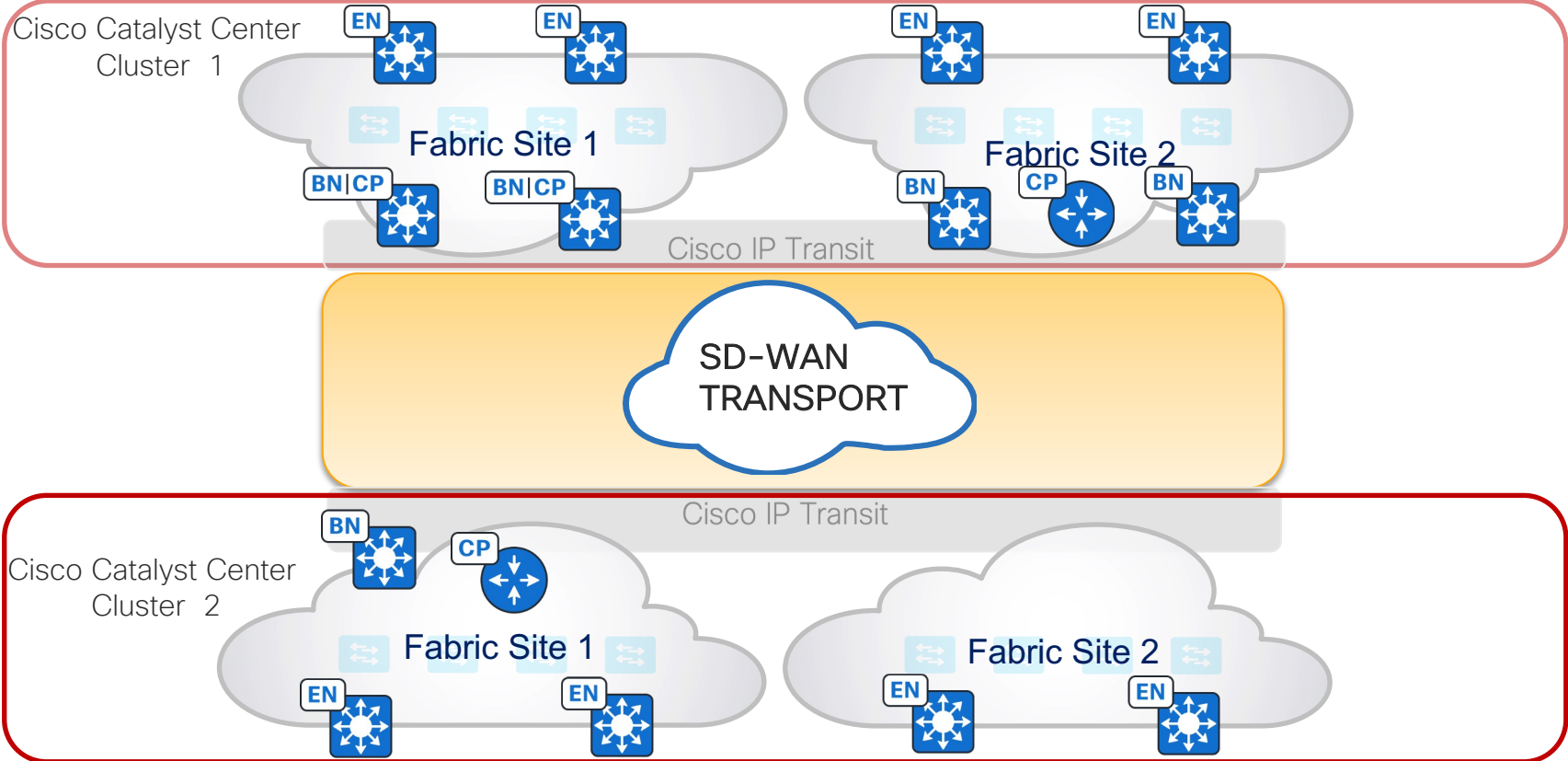
Cisco SD-Access Multisite

Transit Design across Cisco Catalyst Center Clusters



Cisco SD-Access Multisite

Transit Design across Cisco Catalyst Center Clusters



Cisco SD-Access Multicast

Supported Modes(Overlay)
RP Overlay Placement (ASM)
Source/Receiver Placement
Multicast Configuration
Per VN RP support
Multi-site with SD-A Transit
Multiple RP per VN
Group to RP Mappings
Concurrent ASM/SSM

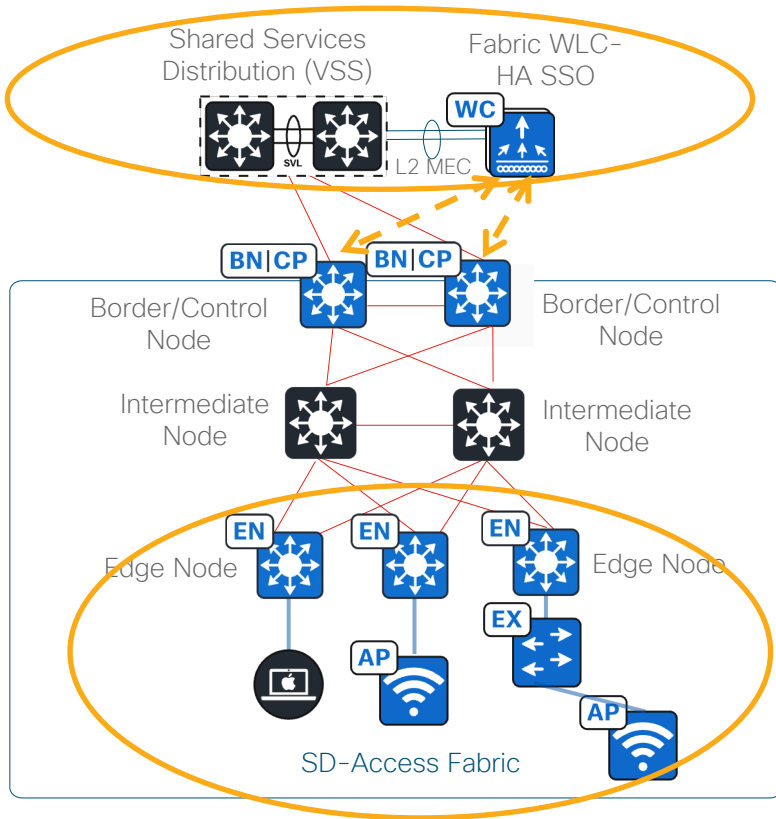
: ASM, SSM
: Inside/Outside Fabric
: Inside/Outside Fabric
: Automated by Cisco Catalyst Center
: Supported
: Supported with LISP PUB/SUB
: Supported
: Supported
: Supported

Cisco SD-Access Multicast

Fabric Multicast Deployment Modes

Head-End Replication	Native Multicast
No Underlay Multicast	Underlay Multicast required
Preferred for lesser Edge nodes in FS	Preferred option for Large number of Edge nodes in FS
Replication Load on Head-End device	Reduces replication Load at the Head-End
V4 and V6 support	No V6 support

SD-Access Wireless Connectivity



- WLC typically connect to a “shared services” Distribution Block
 - VSS/Stack is the preferred topology
 - Management IP address in Global Routing Table
 - Specific route to advertise WLC’s IP in the underlay
- WLC can talk to only #2 Enterprise CP nodes
- Access Points connect to Fabric Edge
 - APs reside in INFRA_VN (GRT) and form CAPWAP connection to WLC. No need for VRF leaking
 - AP can be connected to an extended node
 - APs are connected in Local mode

Cisco SD-Access Wireless

Deployment types

Supported Platforms

AP Mode

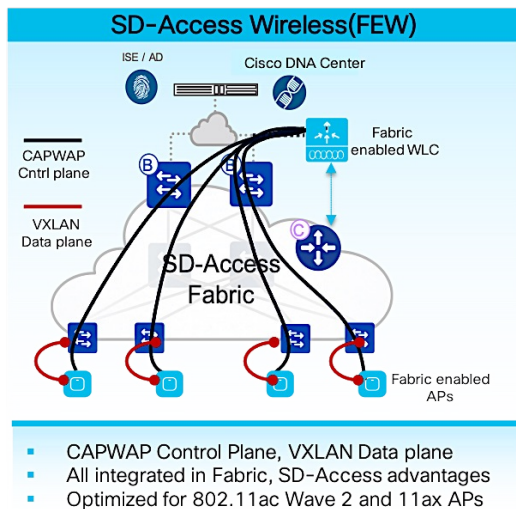
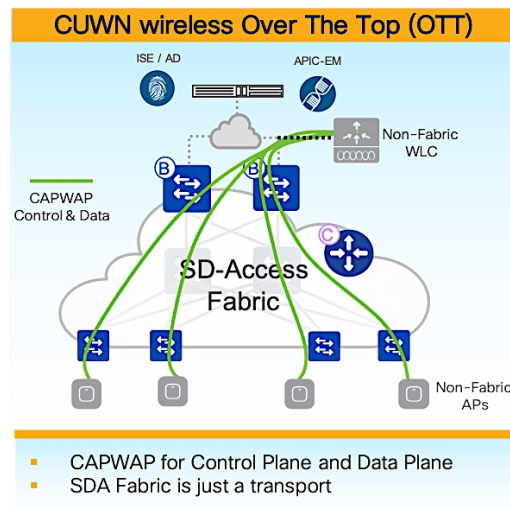
Control-Plane Node support

: FEW , OTT , Mixed Mode

: C9800, EWC,3504,5520,8540

: Local, Flex*

: 2(AireOS) , 8(C9800)*

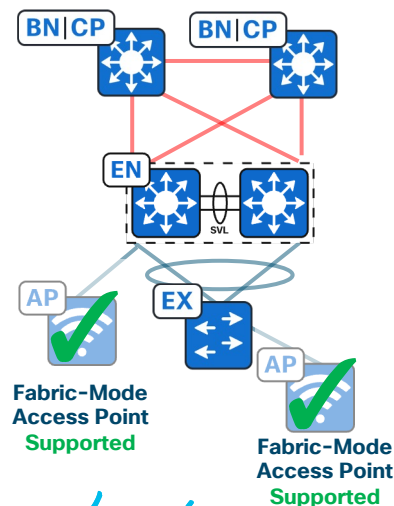


SD-Access Wireless Design Best Practices

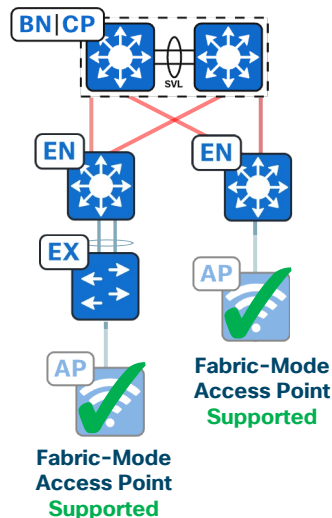
SVL in Fabric Topology Examples

Device Family	BP	CP	EN	BN+CP	FIAB	FIAB+eWL C	SVL as Seed
C9400/C9500	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C9600	Yes	Yes	No	Yes	No	No	Yes

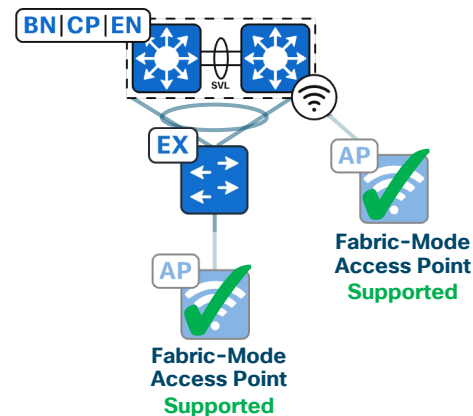
Fabric AP to SVL Edge Node



Fabric AP to EX/PEN



Embedded Wireless support on SVL *



* - Catalyst 9400 and 9500

SD-Access Wireless Design Best Practices

Fabric Wireless Recommendations

SD-Access – WLC Scale

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

SD-Access – Embedded Wireless

Platform	Number of APs	Number of Clients
Catalyst 9200/L	Not Supported	Not Supported
Catalyst 9300/L	50	1000
Catalyst 9300 (Single Switch)	100	2000
Catalyst 9300 (Switch Stack)	200	4000
Catalyst 9400/9500/9500H	200	4000

SD-Access Wireless Design Best Practices

SD-Access Wireless – N+1 HA vs SSO

Redundancy Comparison

Stateless Redundancy with N+1 HA

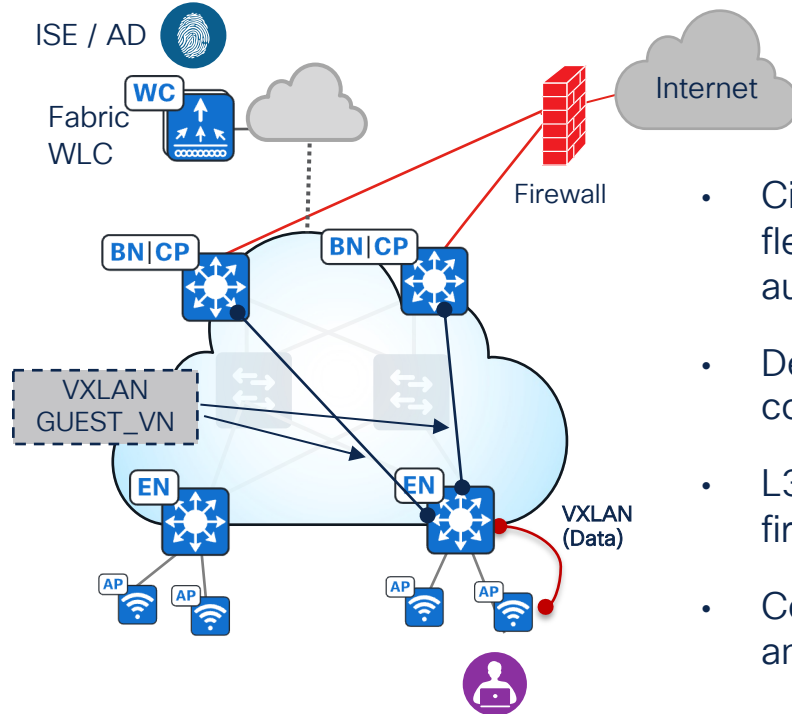
- WLCs remain independent of each other. Cisco Catalyst Center and SD-Access fabric sees them as two separate WLCs.
- For each location there is a primary and a secondary WLC.
- Both WLCs communicate with the control plane nodes.
- In a failover event, the CAPWAP tunnel is broken between AP and Primary WLC and is reinitiated with the Secondary WLC.
- APs and clients move to the Secondary WLC.
- AP rolling upgrade support(Catalyst Center 2.1.2.0 onwards)

Stateful Redundancy with SSO

- WLC SSO is seen as a single entity.
- Only active WLC communicates with the control plane nodes.
- APs and clients stay connected during a failover event.
- In a failover event, the new Active WLC will bulk update the control plane node regarding the wireless hosts.
- For Embedded Wireless on Catalyst 9000 switches, SSO is achieved through hardware stacking on Catalyst 9300/L switches and through redundant supervisors on Catalyst 9400 switches and Catalyst 9500 SVL

Cisco SD-Access Wireless

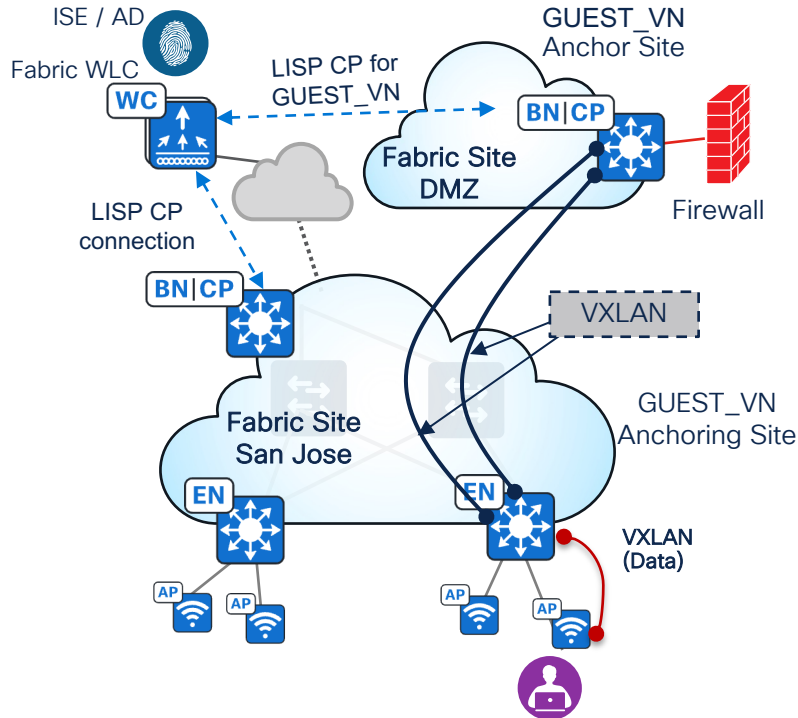
Wireless Guest Design – Dedicated Virtual Network



- Cisco Catalyst Center Guest-SSID workflow provides flexibility to create custom Guest portal with ISE authorization policies.
- Dedicated Virtual Networks for segmentation provides control plane and data plane isolation
- L3 Handoff with BGP peering between Border and firewall.
- Consistent network and policy deployment for wired and wireless infrastructure

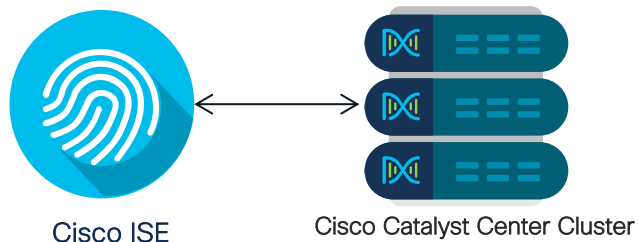
Cisco SD-Access Wireless

Wireless Guest Design – Dedicated Virtual Network with MSRB



- Multisite Remote Border (MSRB) allows a Virtual Network to be anchored to a different fabric site's Border, Control Plane nodes providing traffic egress point flexibility.
- Edge node (Anchoring site) encapsulates VXLAN with destination as remote-site Border (Anchor site) for the VN.
- VXLAN cannot be fragmented, higher MTU must be supported across the sites
- Catalyst 9800 can support up to 8 Control Plane node pairs.
- AireOS WLCs can support maximum 2x Control Plane node pairs

Cisco ISE Use Cases in SD-Access



Guest Access

Guest network automation

Host On-boarding

User authentication

Group Based Policies

SDA Segmentation

Assurance

Client 360

Multiple DNAC to ISE

Shared Transit + Extranet

Device Administration

TACACS

Asset Visibility

Everything & Everyone on
Network

Policy Analytics

Group to Group Interaction
with automated policy

Security Ecosystem

Integration

Context Sharing

Cisco Catalyst Center Settings

Cisco ISE + Load Balancer

The screenshot shows the Cisco DNA Center web interface. The left sidebar contains a search bar and a navigation menu with categories like Cisco Accounts, Device Settings, External Services, and Authentication and Policy Servers. The main content area is titled 'Authentication and Policy Servers' and includes a table of configured servers. A modal window titled 'Edit ISE server' is open on the right, showing fields for Server IP Address, Shared Secret, Username, Password, FQDN, Subscriber Name, and Virtual IP Address(es). A blue callout bubble points to the 'Virtual IP Address(es)' field, which contains the value '172.25.73.240'.

Settings / External Services

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.

[Add](#) [Export](#)

IP Address	Protocol	Type
172.25.73.223	RADIUS_TACACS	ISE

Edit ISE server

Server IP Address
172.25.73.223

Shared Secret

Username*
admin

Password*

FQDN
ISE10-1.demo.local

Subscriber Name
DNAC10

Virtual IP Address(es)
172.25.73.240

Advanced Settings

Cancel Add

Load Balancer VIP

Cisco Catalyst Center Design

ISE as AAA Server for Client and Network

The screenshot displays the Cisco Catalyst Center Design interface, specifically the 'Network Settings' page. The interface is divided into two main sections: a left sidebar for navigation and a main content area for configuration.

Left Sidebar (Navigation):

- Global**
- SITE-A**
- Building 1**
- Floor1**
- SITE-B**
- SITE-C**
- SITE-D**
- SITE-F**
- SITE-T**

Main Content Area (Configuration):

AAA Server Configuration:

- Network:** Configured with ISE as the AAA Server. The IP Address (Primary) is 172.25.73.223. The Shared Secret is 172.25.73.223.
- Client/Endpoint:** Configured with ISE as the AAA Server. The IP Address (Primary) is 192.168.1.225. The Shared Secret is 192.168.1.225.

Advanced Settings (Left Panel):

- Server IP Address:** 172.25.73.223
- Shared Secret:**
- Username:** admin
- Password:**
- FQDN:** ISE10-1.demo.local
- Subscriber Name:** DNAC10
- Virtual IP Address(es):**
- Advanced Settings:** ☒ Connect to pxGrid, ☐ Use Cisco DNA Center Certificate for pxGrid
- Protocol:** ☒ RADIUS, ☐ TACACS
- Authentication Port:** 1812
- Accounting Port:** 1813
- Port:** 49
- Retries:** 3
- Timeout (seconds):** 4

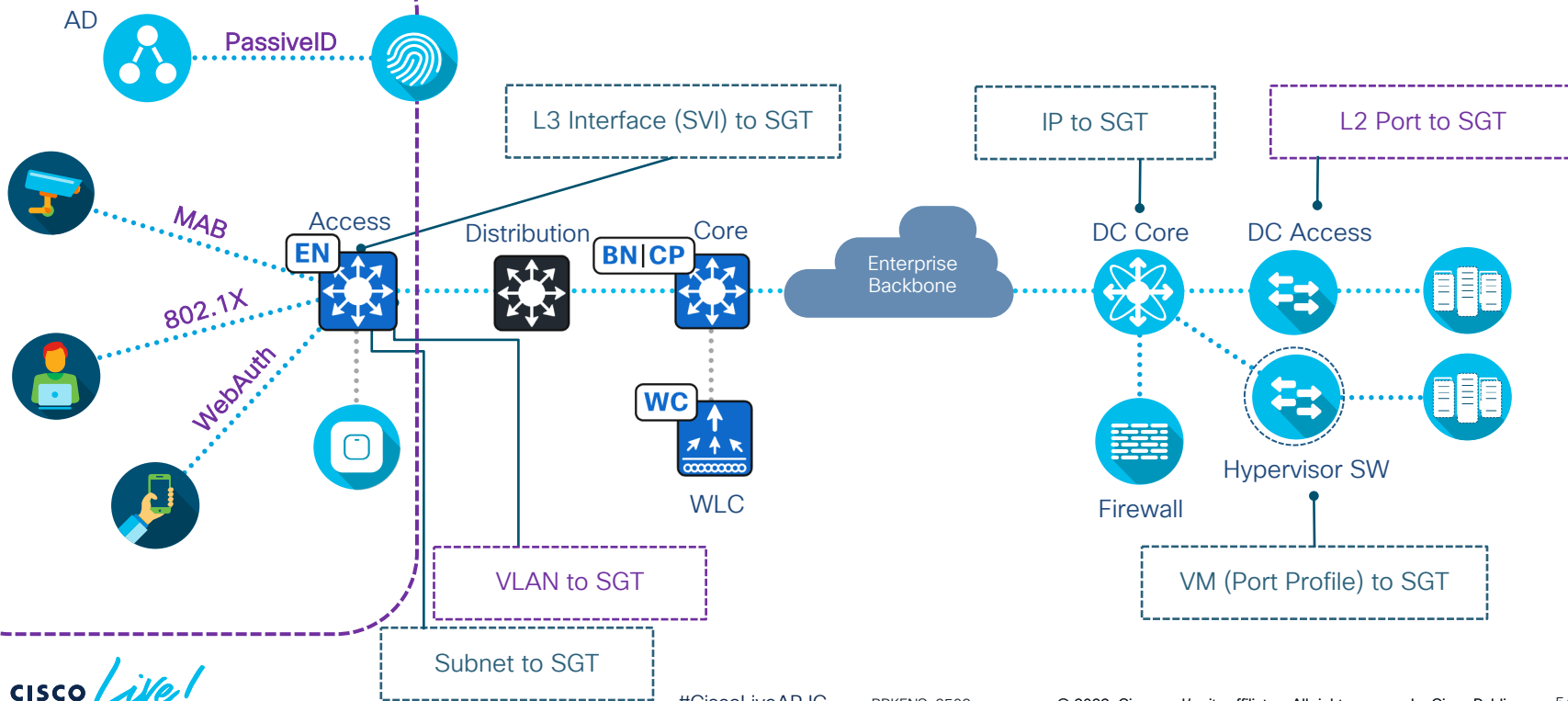
Buttons: Cancel, Add, Reset, Save

Security Group Tags(SGT)

Classification Mechanism

Dynamic Classification

Static Classification

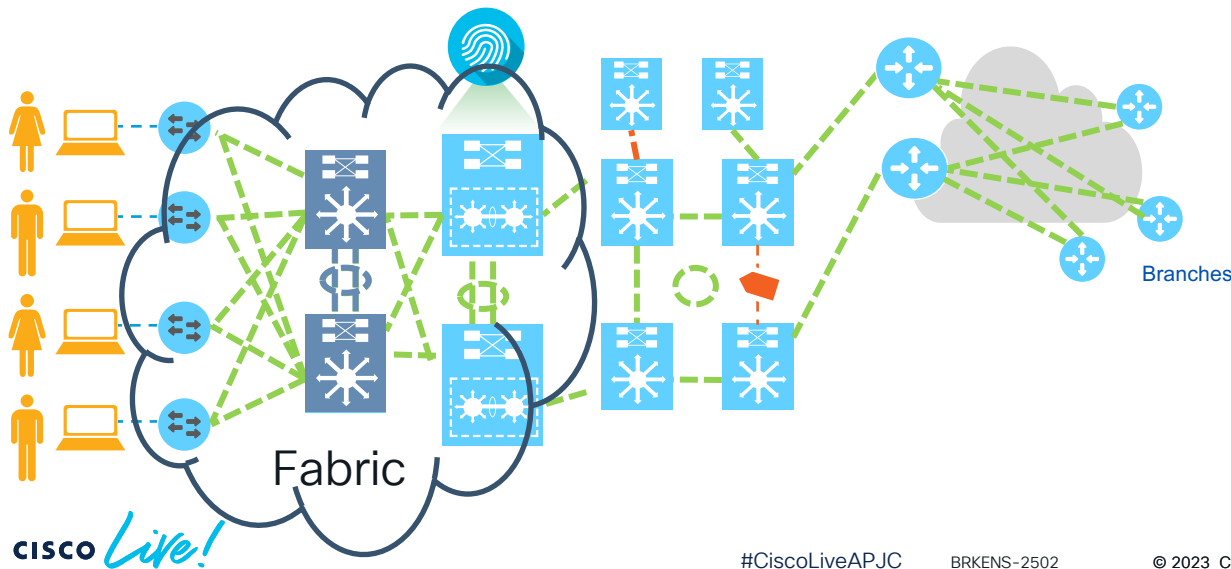


Security Group Tags(SGT)

Propagation Mechanism

Inline Tagging Methods

- **Ethernet Inline Tagging:** (EtherType:0x8909) 16-Bit SGT encapsulated within Cisco Meta Data (CMD) payload.
- **IPSec / L3 Crypto:** Cisco Meta Data (CMD) uses protocol 99, and is inserted to the beginning of the ESP/AH payload.
- **LISP:** SGT (16 bit) insertion in the Nonce field (24 bit)
- **VXLAN:** SGT (16 bit) inserted into Segment ID of VXLAN Header



Propagation options

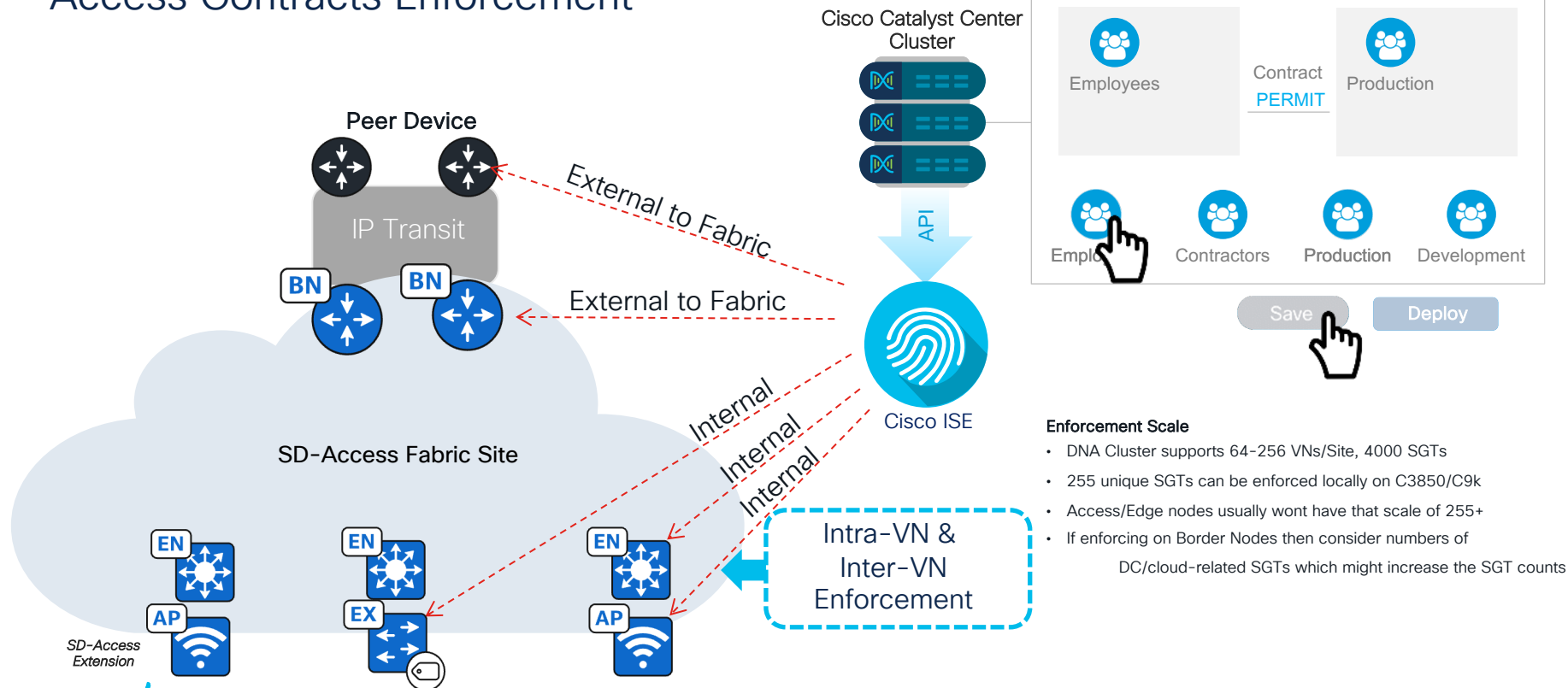
- Cisco MetaData (CMD)
- Ethernet
- MACsec
- IPSec
- DM-VPN
- GET-VPN
- VXLAN

Supporting devices

- Catalyst switches
- WLAN controllers
- Nexus switches
- Integrated Service Routers
- Industrial Ethernet Switches
- ASR 1000
- ASA 5500-x
- Firepower Threat Defense

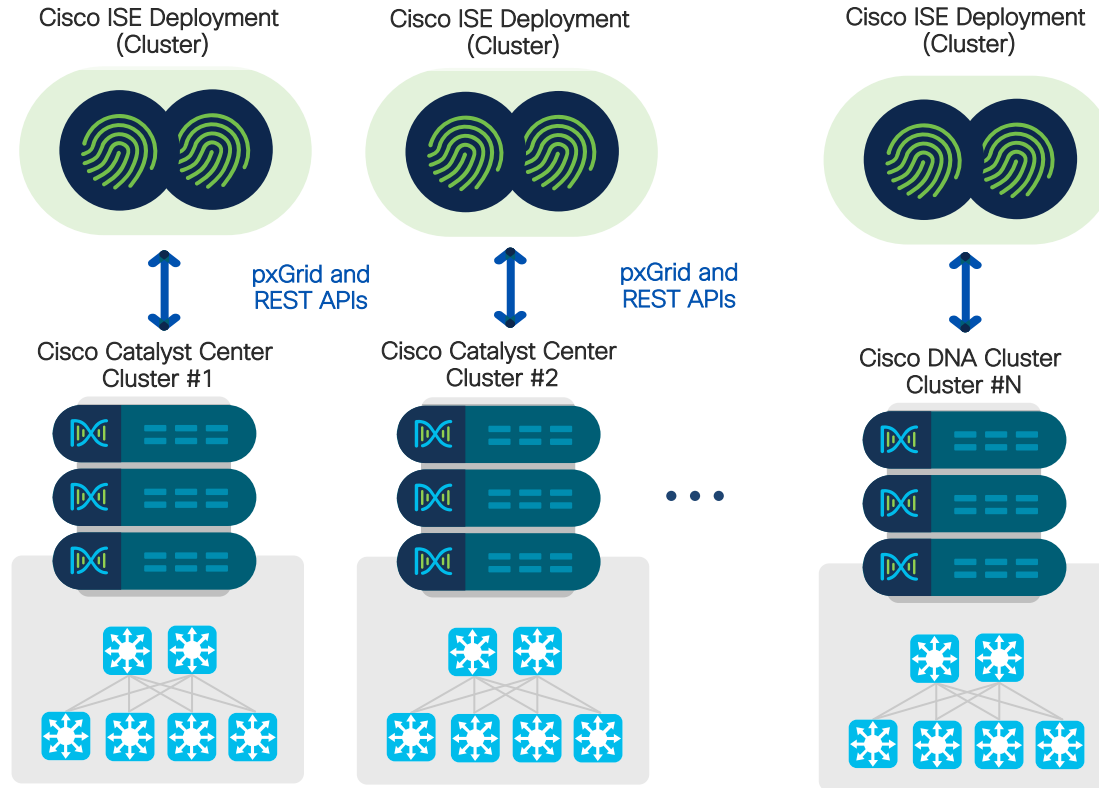
Cisco Catalyst Center Policy

Access Contracts Enforcement



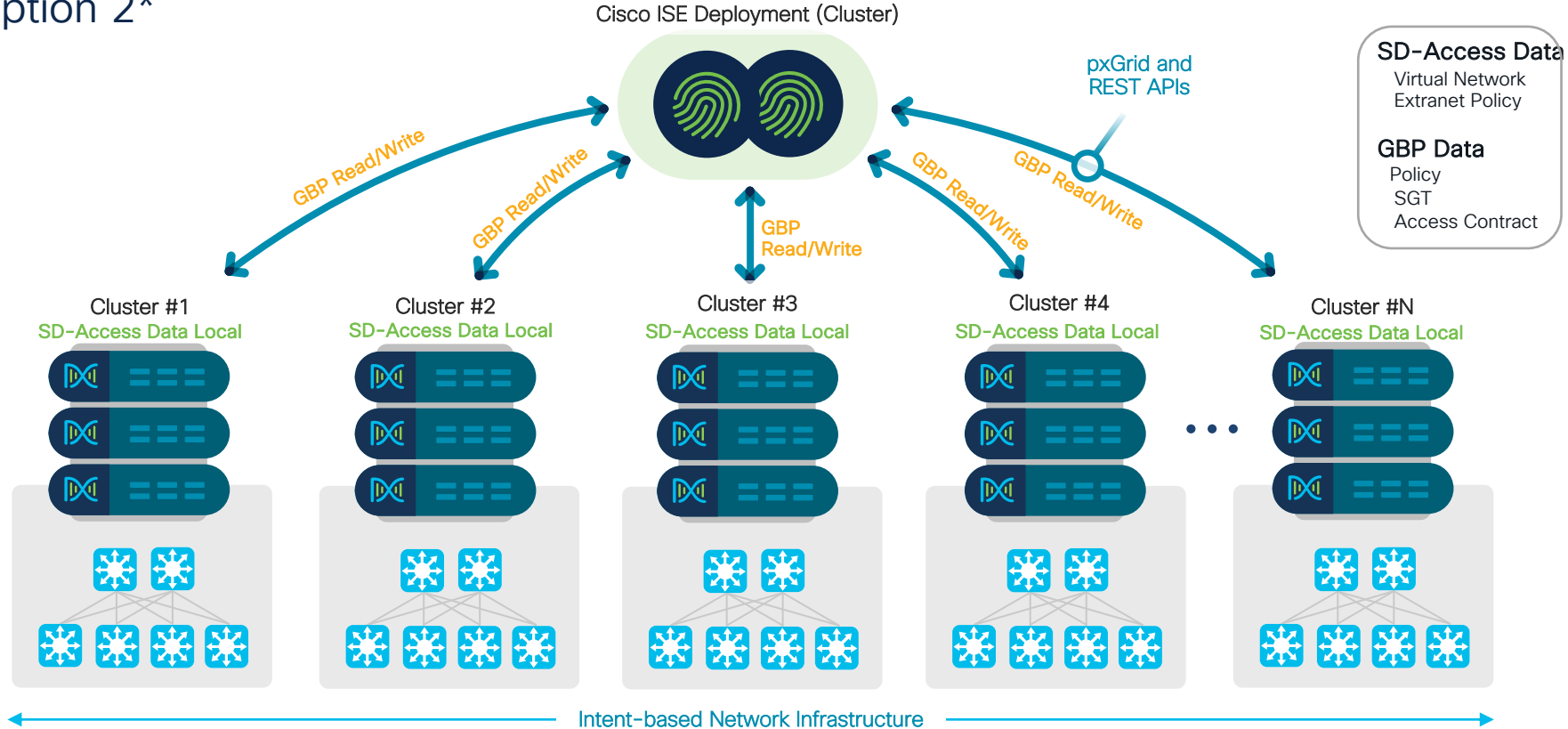
Integrating Multiple Cisco Catalyst Center with ISE

Option 1



Integrating Multiple Cisco Catalyst Center with ISE

Option 2*



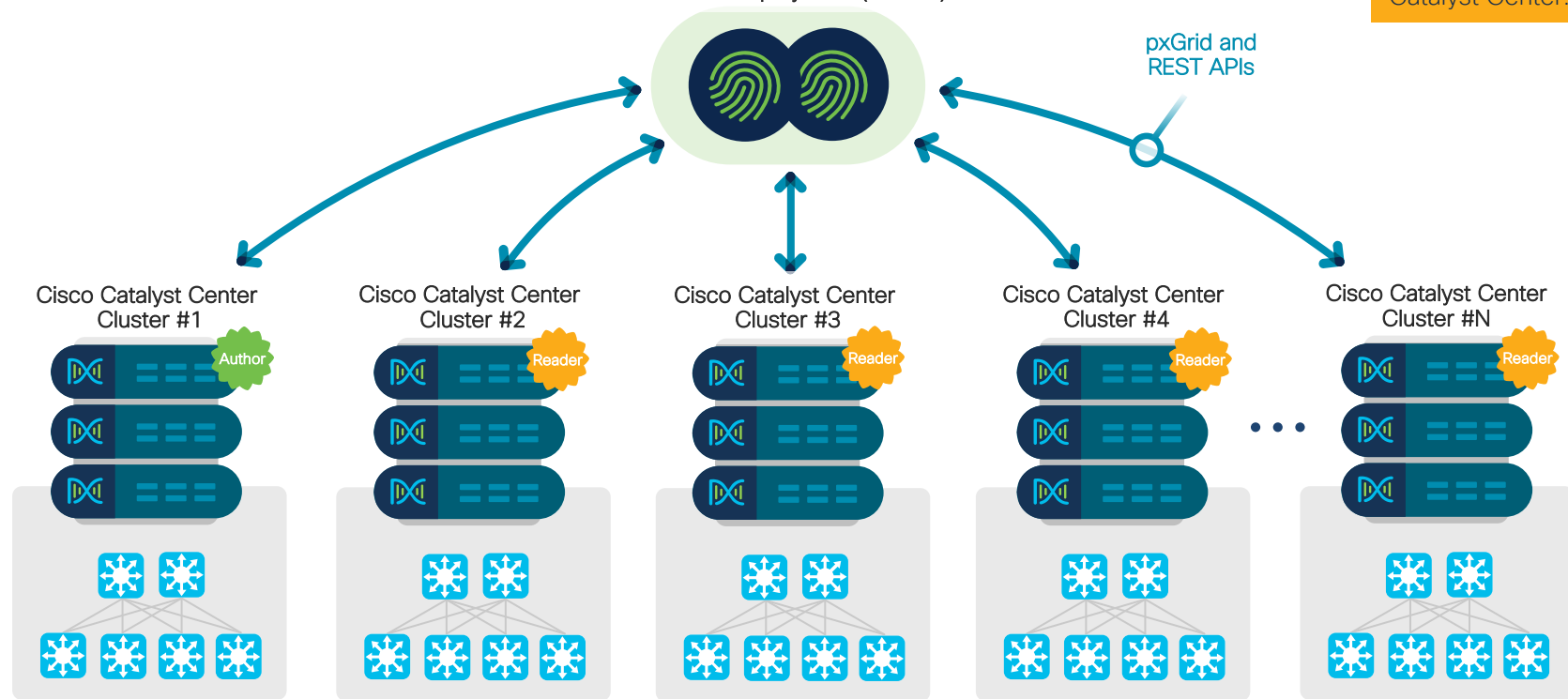
Integrating Multiple Cisco Catalyst Center with ISE

Option 3- Multiple Cisco Catalyst Center Solution Overview

N=5 starting
Catalyst Center: 2.2.3.x

Cisco ISE Deployment (Cluster)

pxGrid and
REST APIs

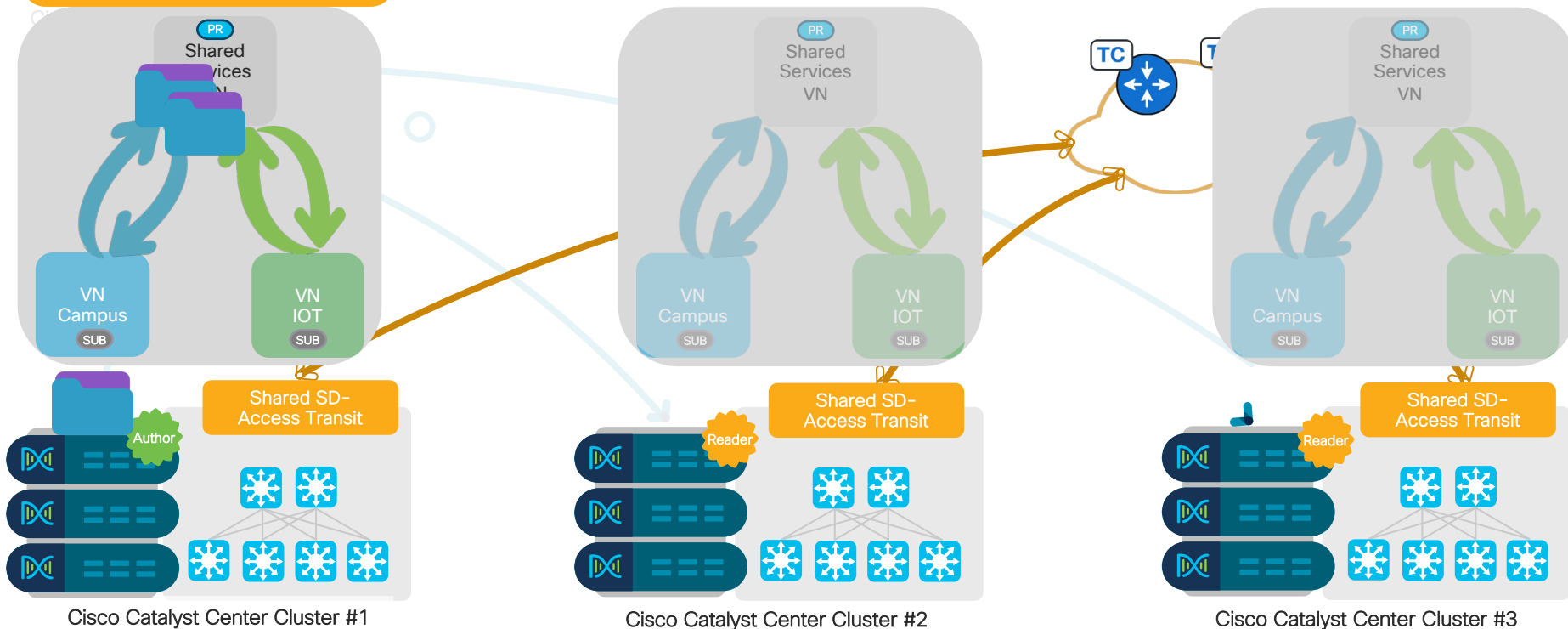


Intent-based Network Infrastructure

Multiple Cisco Catalyst Center

LISP Extranet Policy- Scenario 1(Shared Policy)

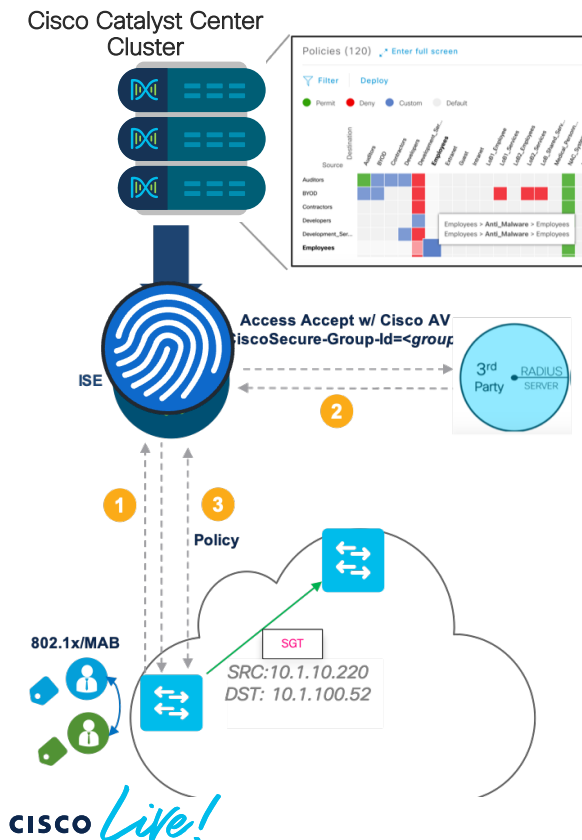
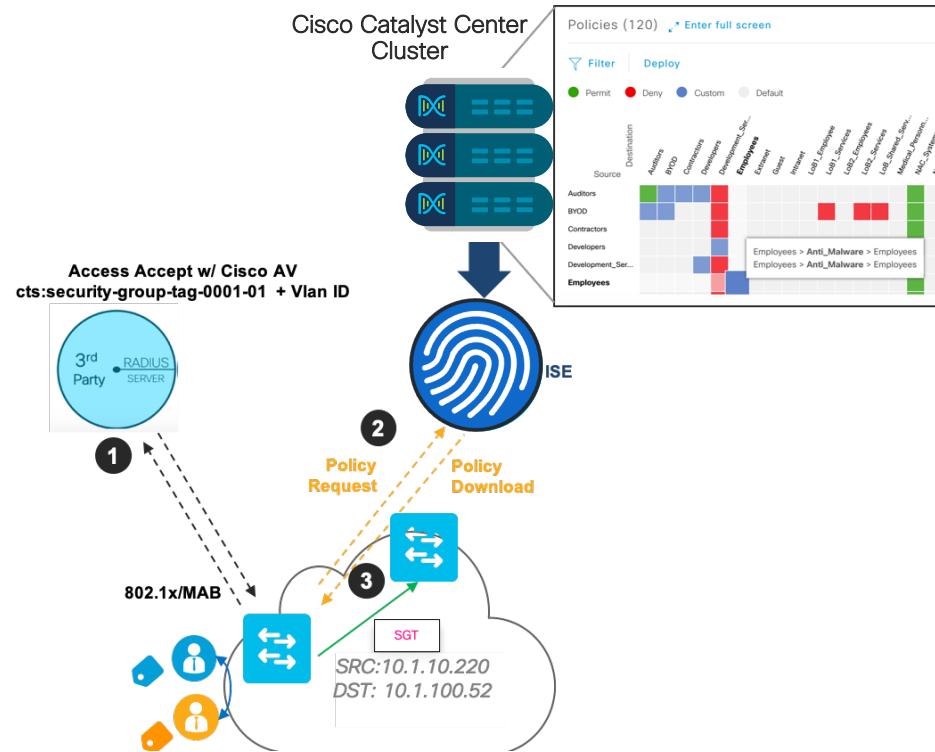
With Shared SD-A Transit



SD-Access Transit shared across multiple Cisco Catalyst Center Clusters

Cisco Catalyst Center Policy

Third-Party AAA/RADIUS Server support



Cisco SD-Access Collaterals



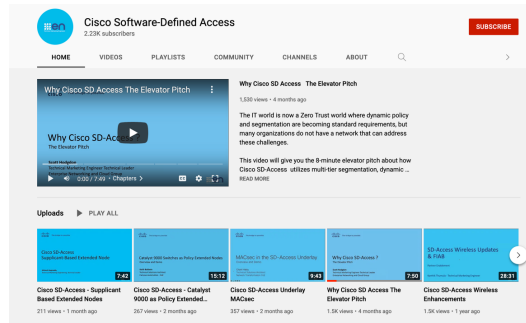
Cisco Software-Defined Access for Industry Verticals



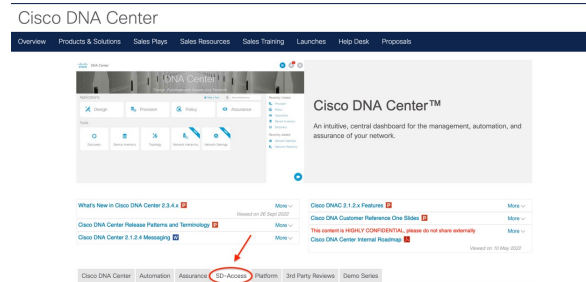
Cisco Software-Defined Access Enabling intent-based networking



Cisco SD-Access YouTube Link



Cisco SD-Access SalesConnect Link



SD-Access BU Engagement Form

SD-Access BU Design Council Form

Multiple Cisco DNA Center LA Form

Cisco SD-Access Design Tool

EN&C Validated Designs



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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

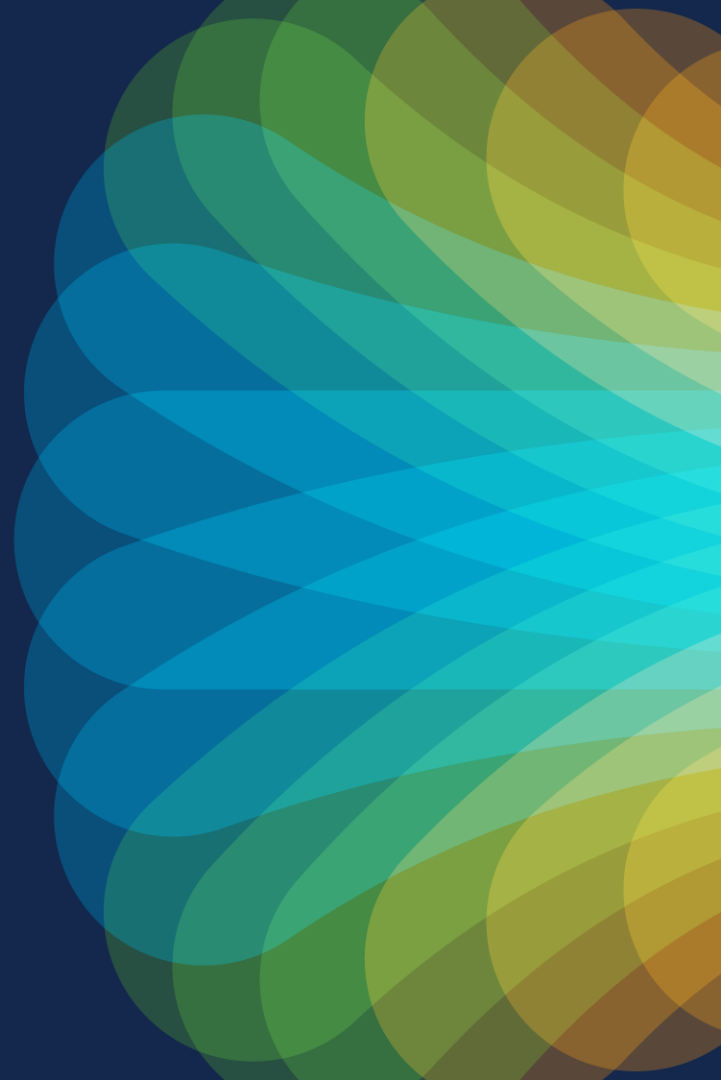


The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC



The background is a vibrant, abstract graphic featuring a rainbow color palette. On the left, there are horizontal, wavy bands of color transitioning from red at the top to blue at the bottom. On the right, a bright white light source emits a series of sharp, radiating lines in various colors, creating a sunburst or starburst effect that blends into the wavy bands.

cisco *Live!*

Let's go

#CiscoLiveAPJC