
cisco Live!
Let's go
#CiscoLive

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!

#CiscoLive

Cisco Webex App

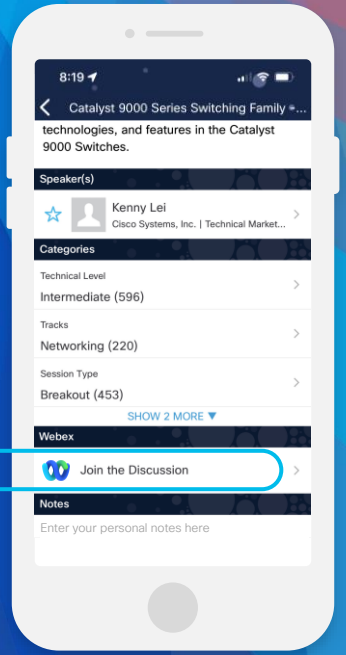
Questions?

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 9, 2023.



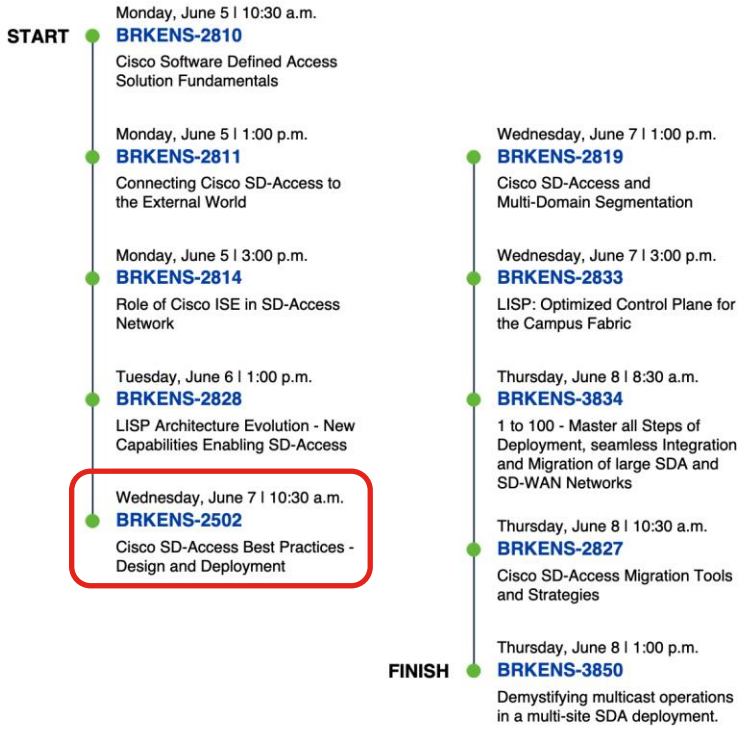
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2502

Cisco SD-Access Learning Map

Networking

SD-Access

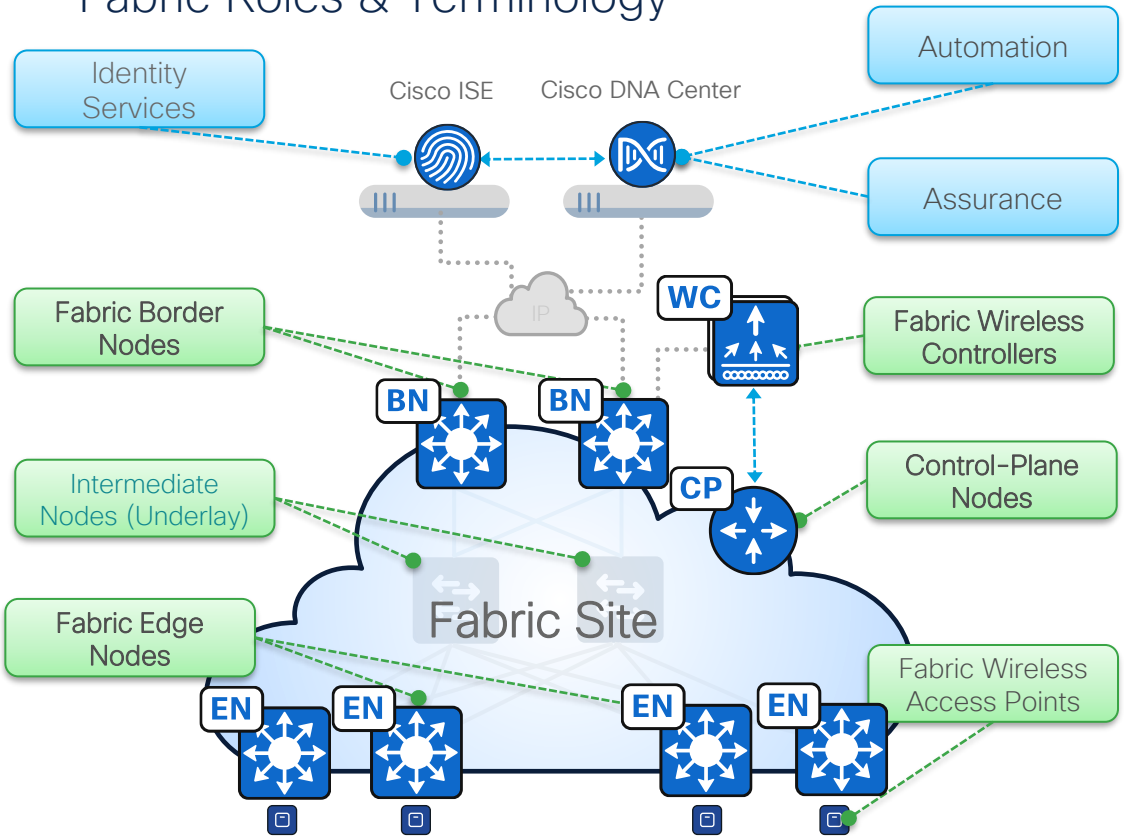
Learn about Cisco's Software Defined Access (SD-Access) solution that provides a secure, dynamic, and automated solution to meet the security and operational challenges faced by an ever-changing environment. The Cisco SD-Access sessions provide a comprehensive overview regarding best practices, design, deployment, migration, and monitoring of a Cisco SD-Access architecture.



Agenda

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

Cisco SD-Access
Fabric Roles & Terminology



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

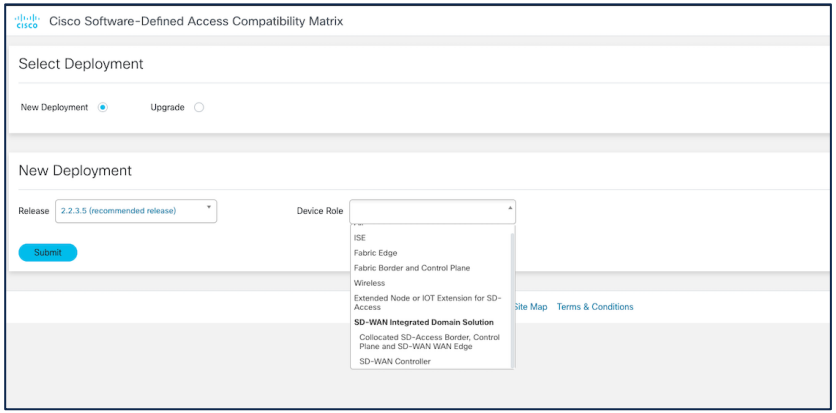
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

For your reference

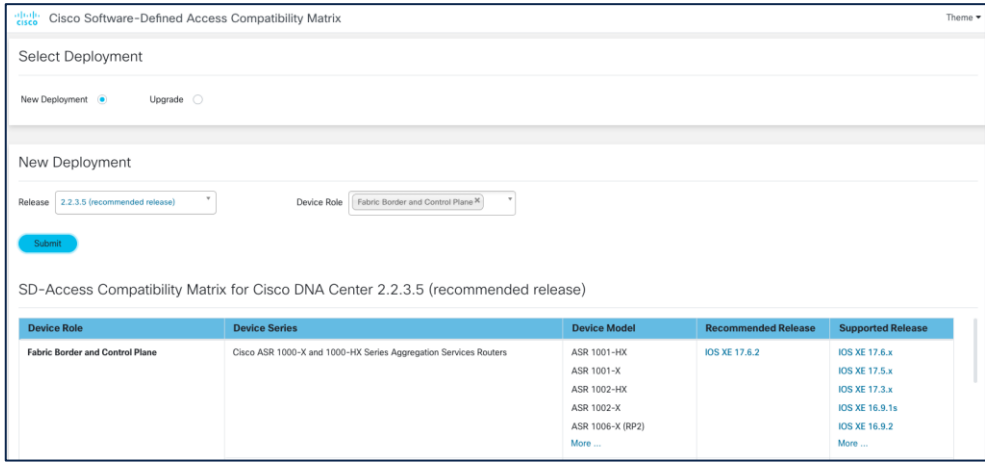
SD-Access Platform Support

Digital Platforms for your Cisco Digital Network Architecture

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



Platform support based on the Fabric Role



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

Cisco SD-Access Scale & Readiness

Cisco DNA Center 2.3.5 Data Sheet

Cisco DNA Center Fabric Readiness and Compliance Checks

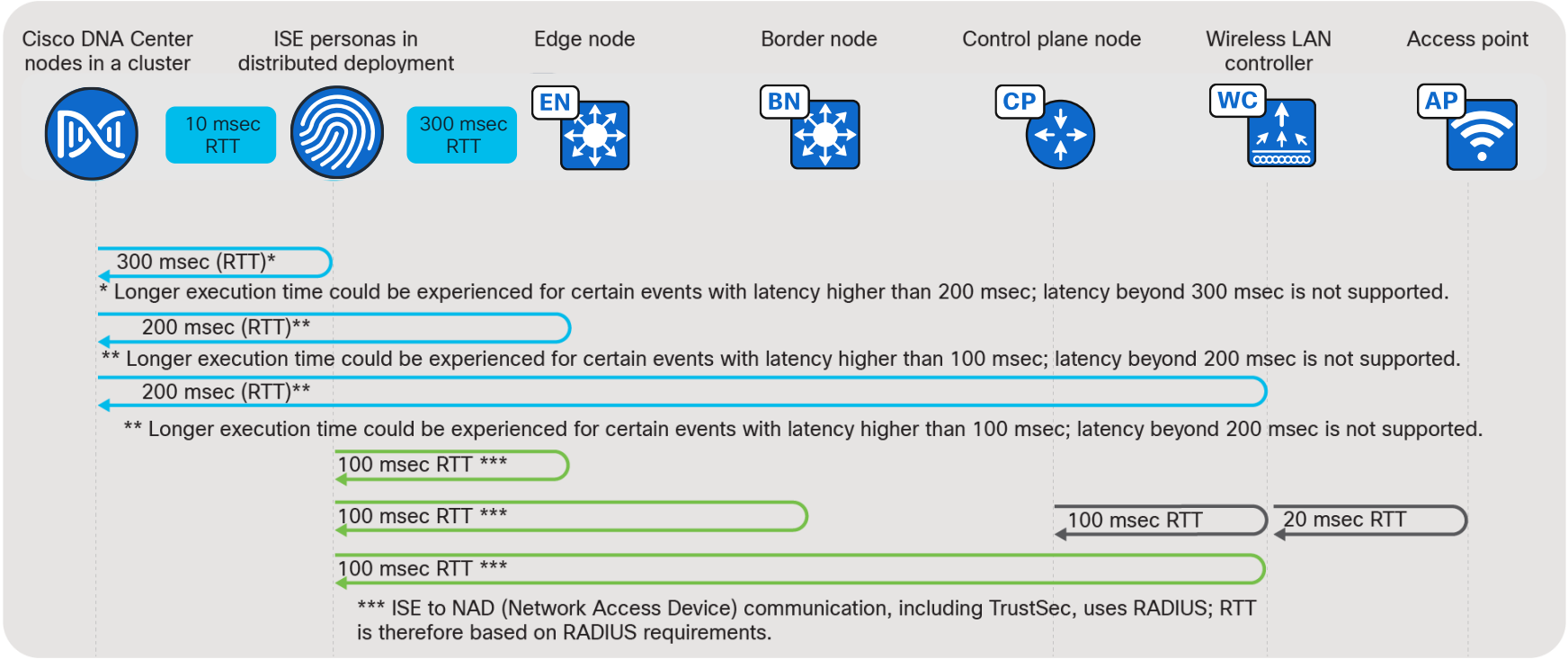
- Hardware Version
- Image Type
- Software Version
- Software Licenses

Cisco SD-Access Software Licensing

- Cisco DNA Advantage/Cisco DNA Premier License

Cisco DNA Center Security Best Practices Guide

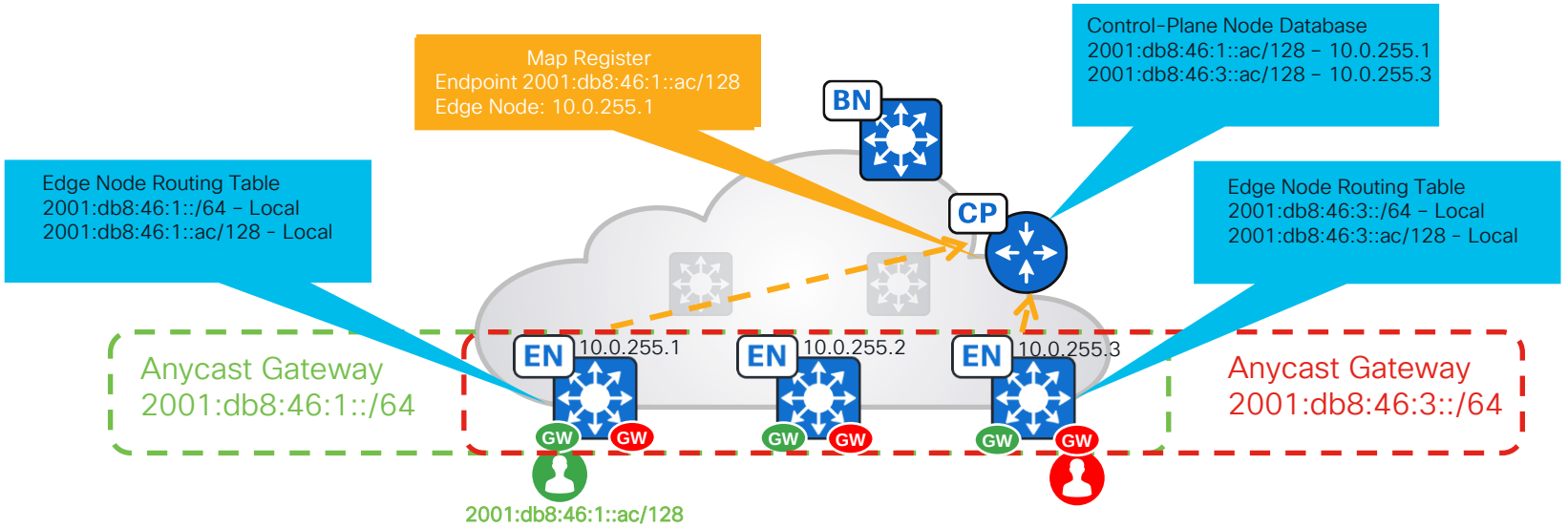
Cisco SD-Access
Latency Requirements



As of
DNA Center: 2.3.5.0
Cisco ISE: 3.2

V4 and V6 support in SD-Access

Cisco DNA 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 DNA Center to Cisco ISE	: V4 only



Cisco SD-Access
Cisco DNA Center Deployment

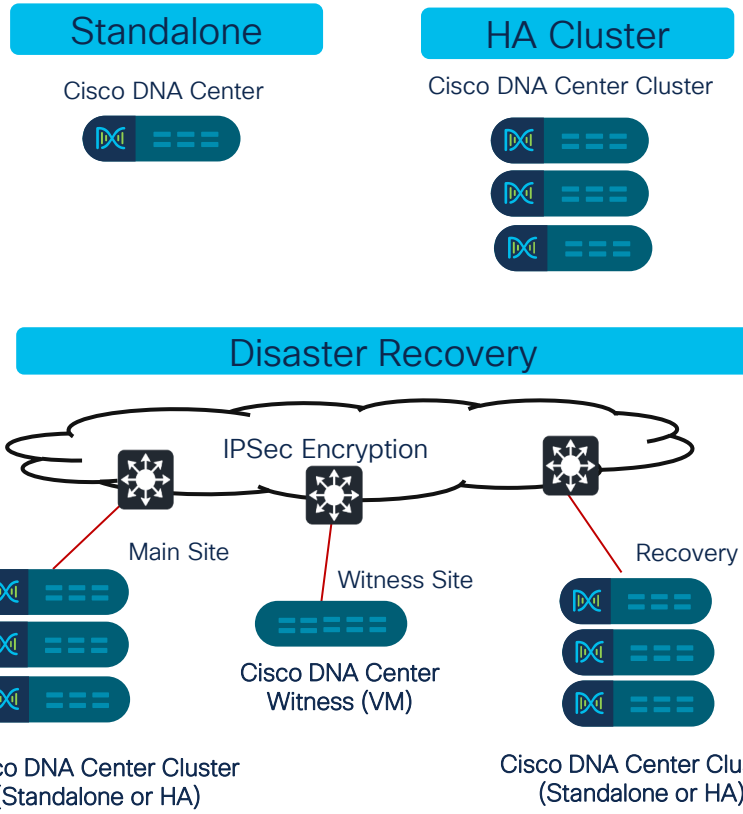
- **Deployment Types**
  - Standalone
  - Cluster for High Availability (HA)

    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

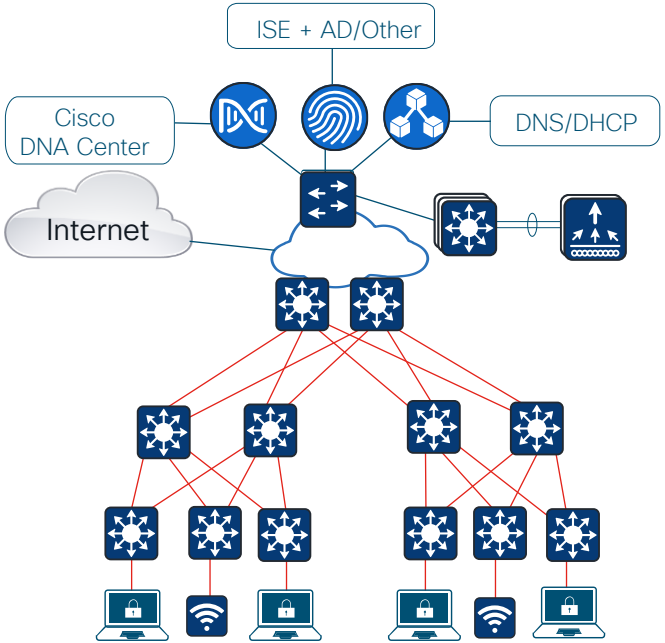
- Failure detection and recovery

	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 upto 7 minutes	Service down upto 30 minutes
Failback	Automatic	Manual

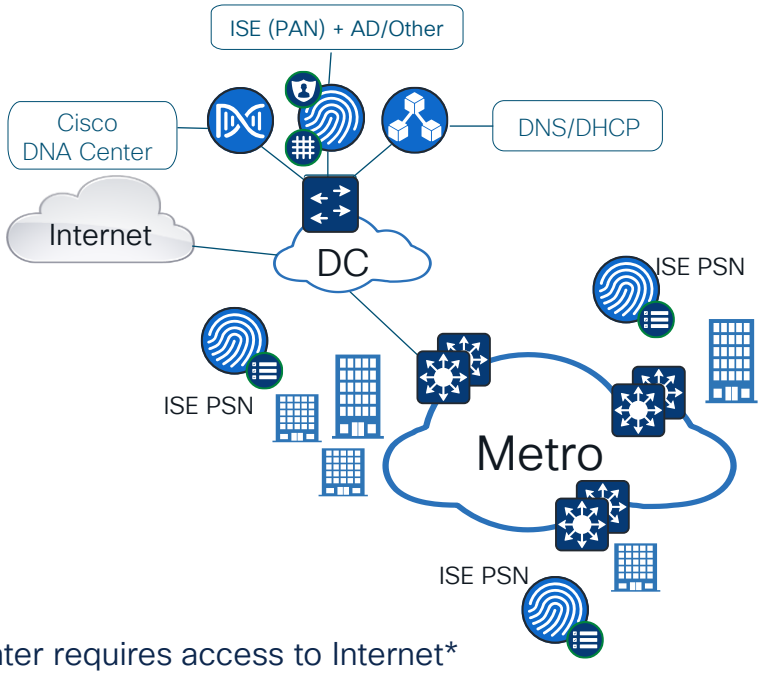


Cisco SD-Access Architecture
Where do I place Critical/Shared Services

Local DC or Services Block



Remote DC

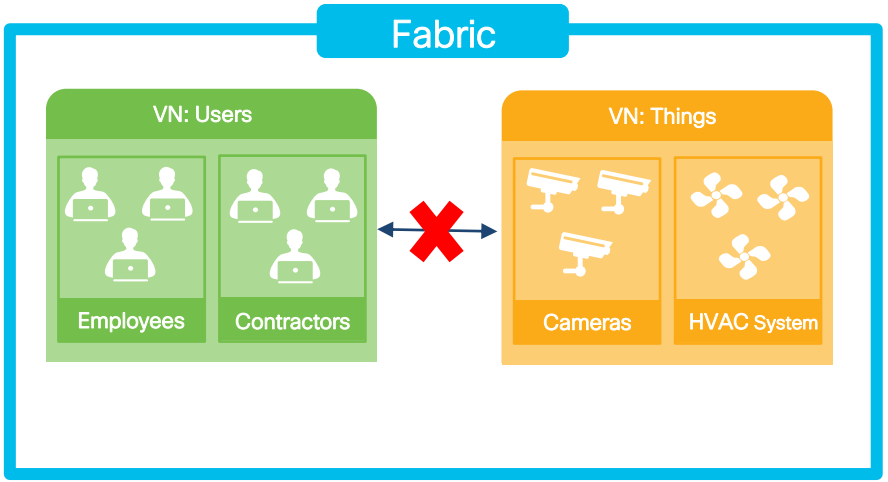


Cisco DNA Center requires access to Internet*

Cisco SD-Access Policy

Segmentation Strategy

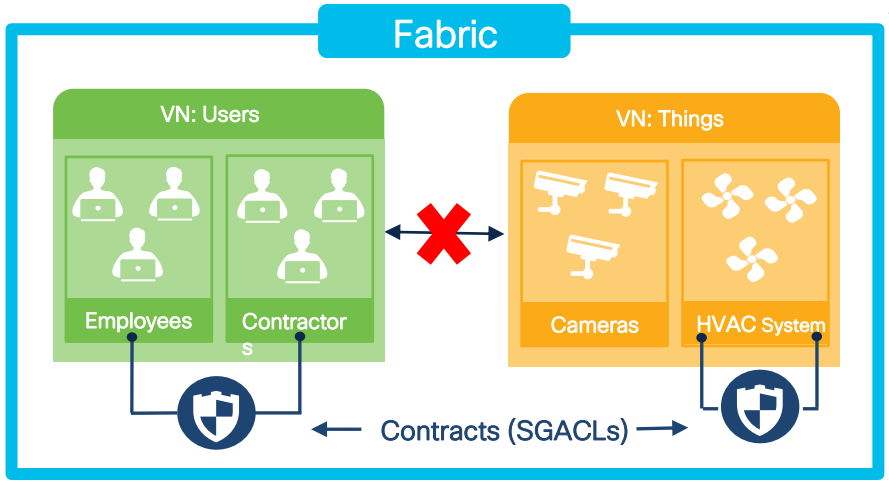
Macro Segmentation



Virtual Network (VN)

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

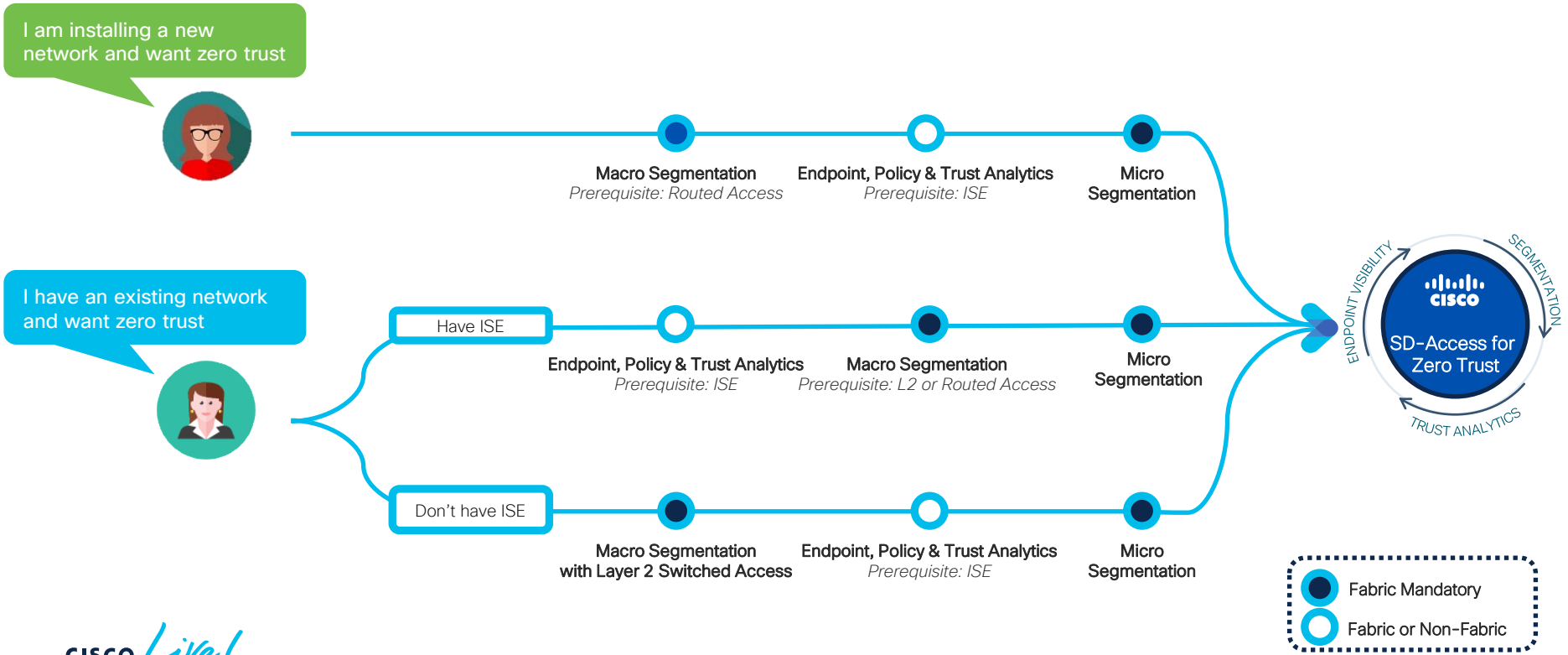
Micro Segmentation



Security Group Tag (SGT)

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

SD-Access Flexible Deployment Options



SD-Access Flexible Deployment Options

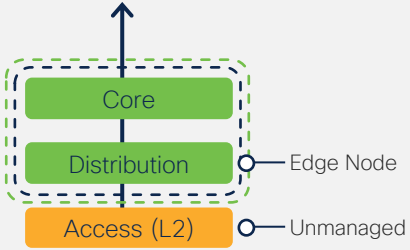
Migration Options

Macro segmentation

Micro segmentation

NEW

Fabric with unmanaged Layer 2 switched access*



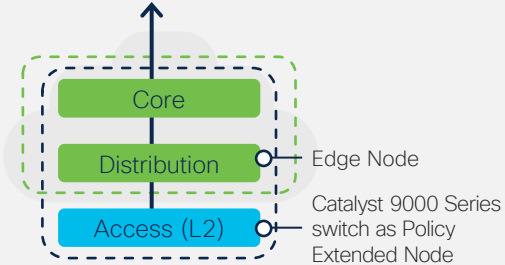
Use case: Keep your existing unmanaged switches

- 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



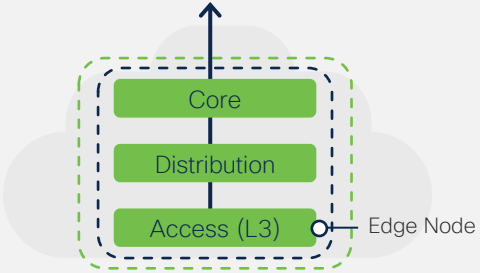
Use case: Retain Layer 2 access

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

Benefit: Security and automation at every layer

The Gold Standard

Fabric with Layer 3 routed access



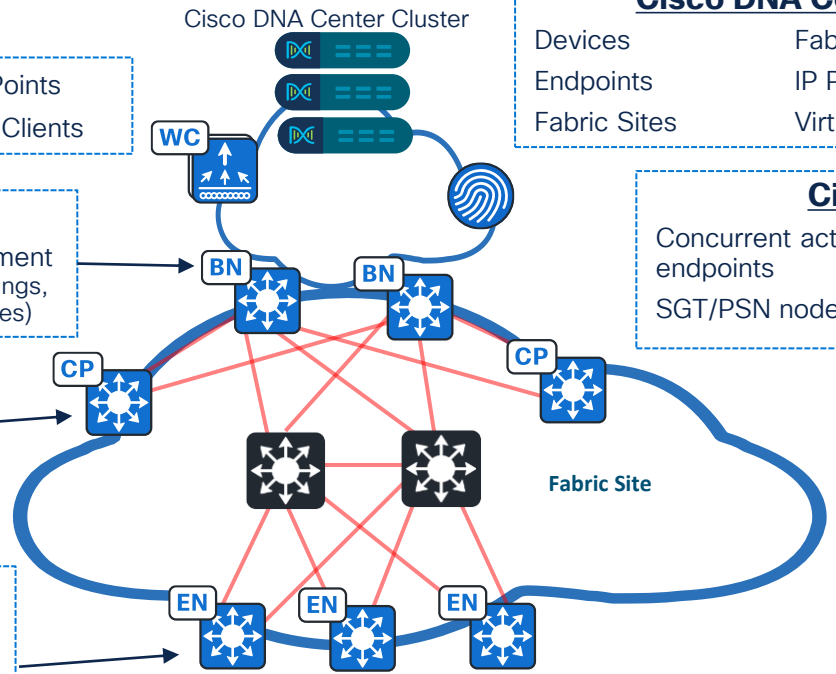
Use case: Full SD-Access

- 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 DNA Center release 2.2.1.0, generally available in late Q2 CY 2021

Cisco SD-Access Scale & Readiness



Cisco DNA Center

Devices	Fabric Devices/site
Endpoints	IP Pools/Site
Fabric Sites	Virtual Networks/site

Access Points
Wireless Clients

Virtual Networks
Anycast Gateways
Host Entries
External prefixes
Security Group Enforcement (SXP per VN, IP-SGT bindings, SG-ACEs, SGT/DGT Policies)

Cisco ISE

Concurrent active endpoints	SGACL
SGT/PSN node	SXP peering

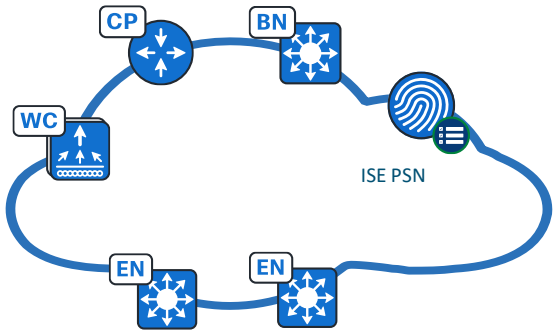
Virtual Networks
Fabric Host Entries

Virtual Networks
Anycast Gateways
Host Entries
Fabric access-tunnels
IP-SGT bindings
SGT/DGT Policies
SG-ACEs

Consider Individual Platform Scale and Performance

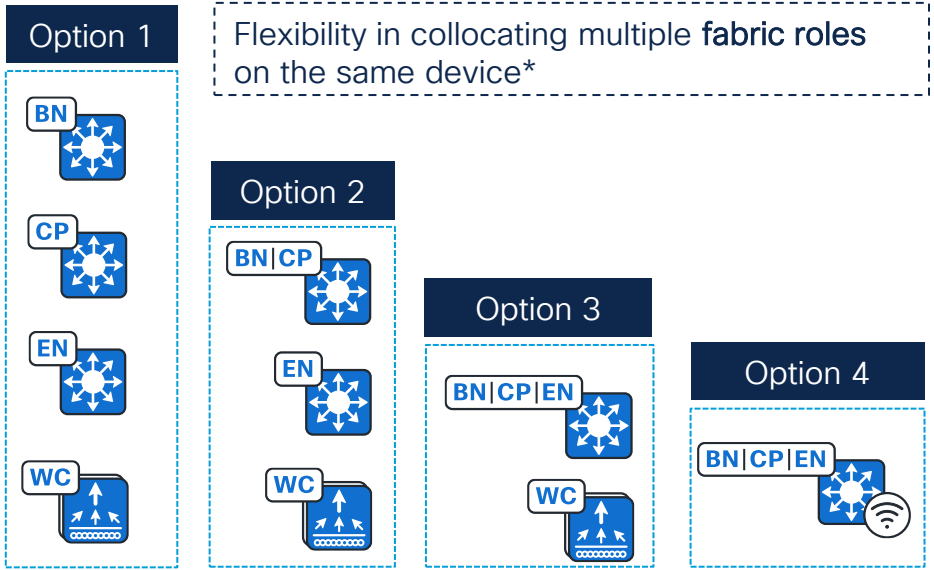
Least Common Denominator (LCD) across the solution elements

Cisco SD-Access Single-site Design Options
Fabric Site Design Options



Fabric Site

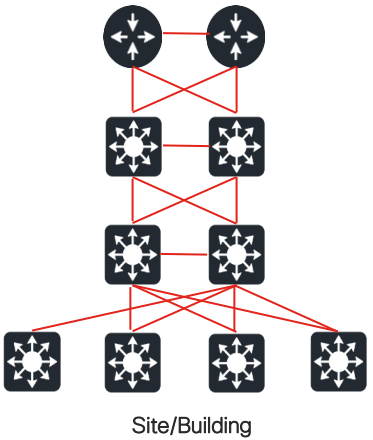
- Logical construct that contains:
  - Fabric Edge, Border, Control Plane
  - ISE PAN/PSN Node
  - (optional) Wireless LAN Controller, Access Points
  - (optional) Extended Nodes



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

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 to accommodate VXLAN encapsulation**
- Underlay multicast to optimize overlay subnet multicast/broadcast distribution



Manual | Semi-Automated Underlay

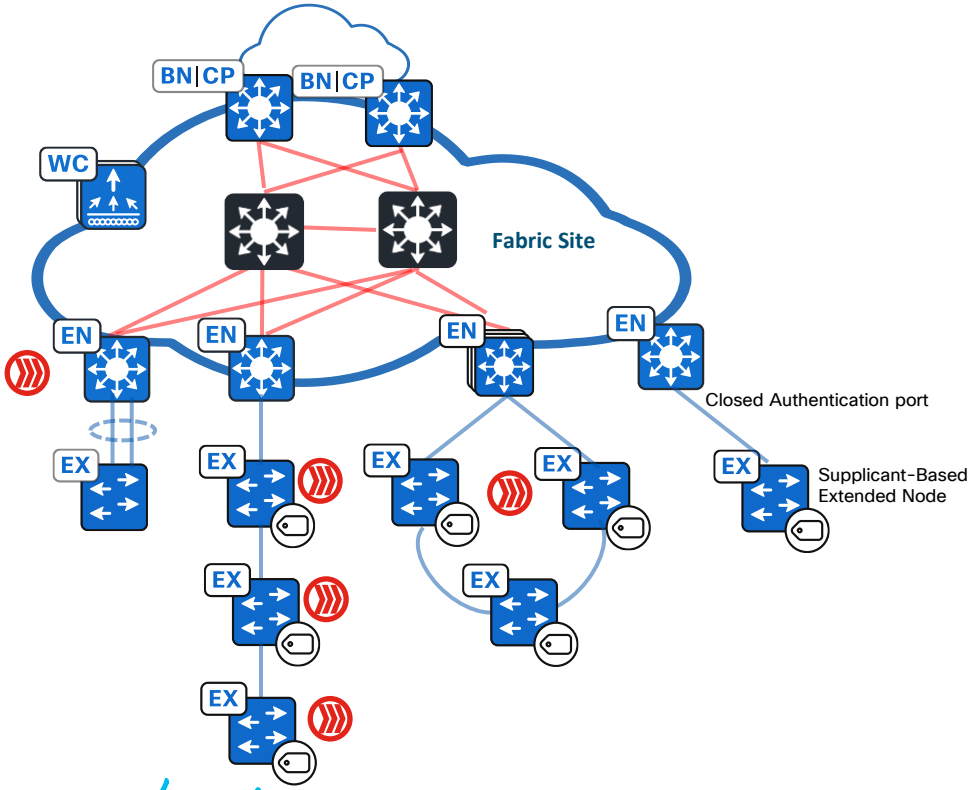
Device-by-Device onboarding and configuration either manually or through Cisco DNA Center Plug-and-Play.

Automated Underlay(**Lan Automation**)

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

Extended Enterprise

Extending the network using fully automated Layer 2 switch



Two Types

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

Supported devices

Extended Node	Policy Extended Node
• IE3300	• IE3400
• IE4000	• IE3400H
• IE4010	• Cat9K(Adv License)
• IE5000	• IE9300
• Cat9K(Ess License)	

Supported Topologies

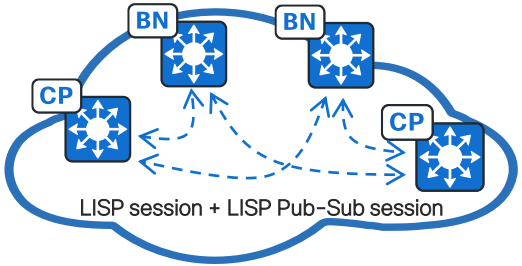
- Daisy Chain(Like device type) up to 18 Nodes
- Ring(Like device type)

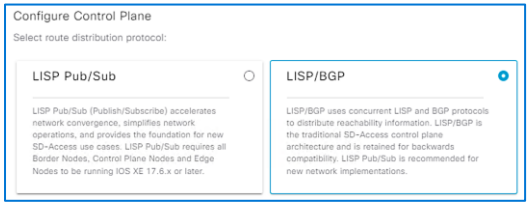
Supplicant-Based Extended Node

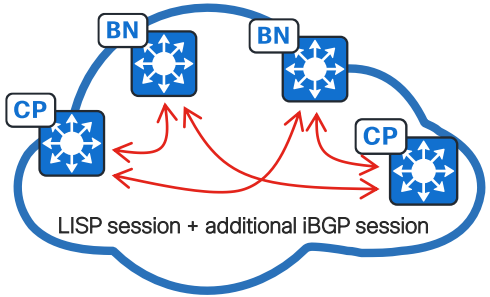
No support of Extended Node to C9200

DNA Center: 2.2.3.x
IOS-XE: ≥ 17.6.2

Cisco SD-Access Provision
Fabric Control Plane enhancements







LISP Pub/Sub

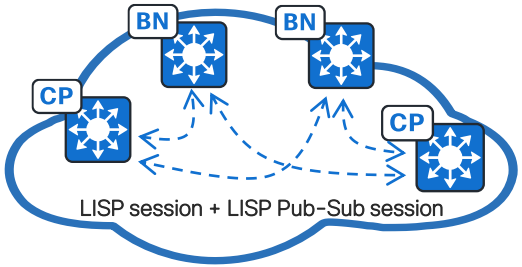
- Publisher-Subscriber model provides LISP Instance-ID table subscription from CP, TCP to Border nodes.
- Faster convergence within fabric site (N-S traffic) and across SD-Access transit.
- LISP Pub/Sub provides backbone for fabric innovations such as Dynamic-Default Border, Extranet, Active-Backup Internet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

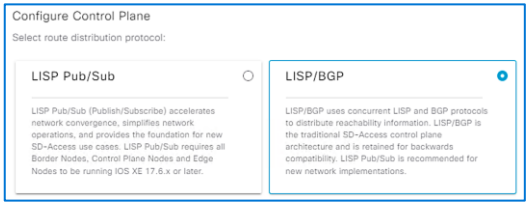
LISP / BGP

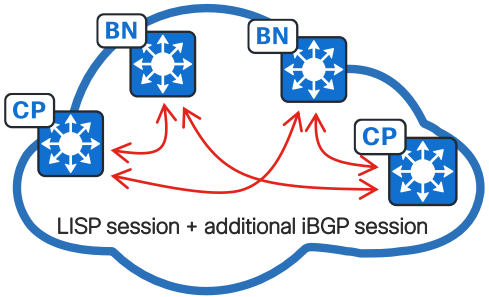
- iBGP session between B – CP and B – TCP node to share prefixes.
- Convergence overhead with additional protocol, redistribution and additional lookups
- Troubleshooting complexity with 2 Control-plane protocols
- Only supported Architecture with SD-WAN Integrated solution
- Only 2 TCP Node support

DNA Center: 2.2.3.x
IOS-XE: ≥ 17.6.2

Cisco SD-Access Provision
Fabric Control Plane enhancements Cont'd





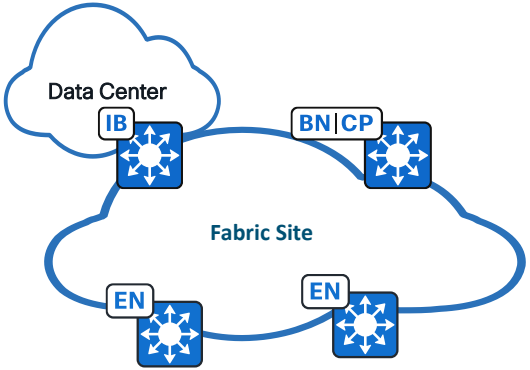


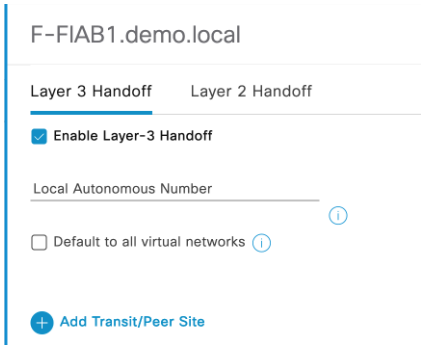
LISP Pub/Sub Benefits

- 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

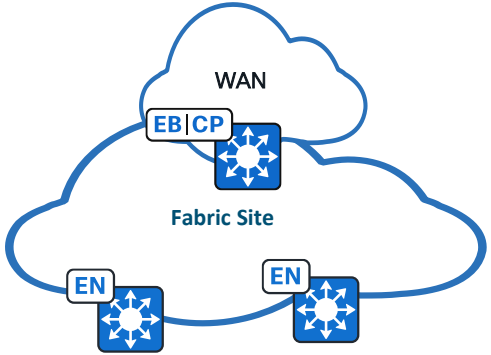
Cisco SD-Access Provision
Border Node Selection

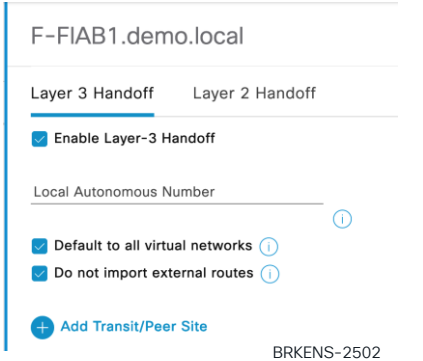
Internal Border (N)
(Rest of Company)



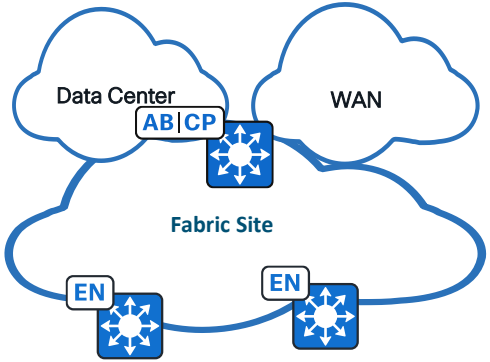


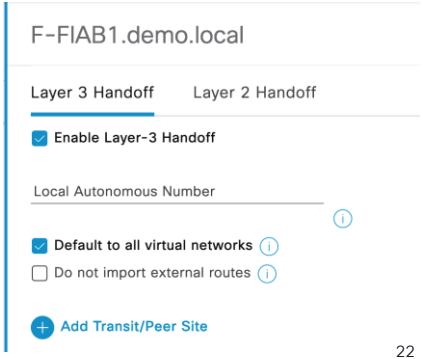
External Border (4 Max)
(Outside)



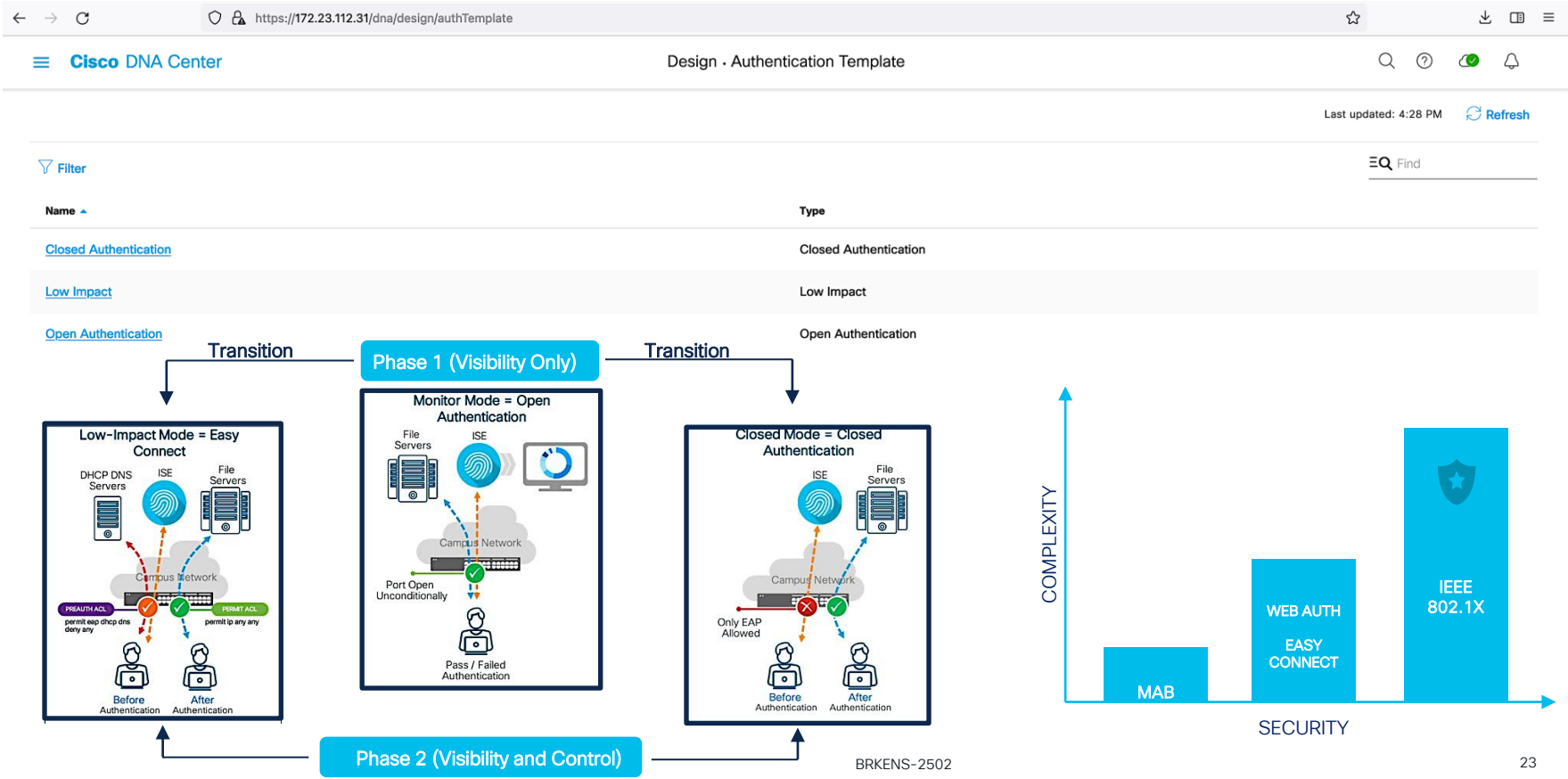


Internal + External Border (4 Max)
(Anywhere)

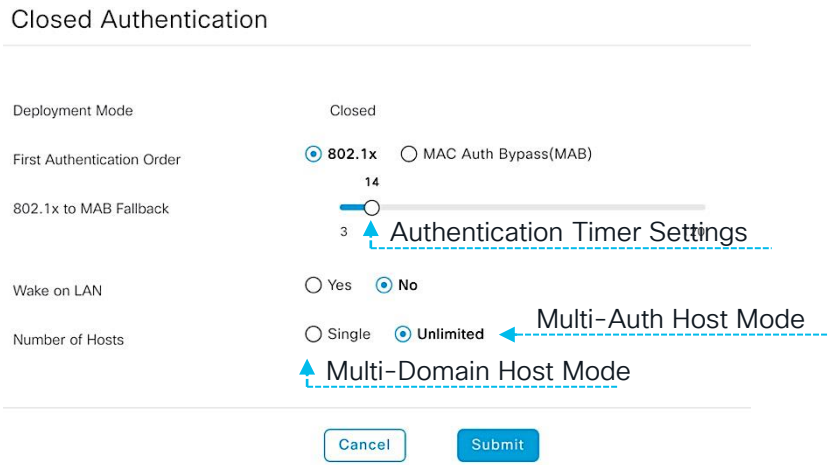


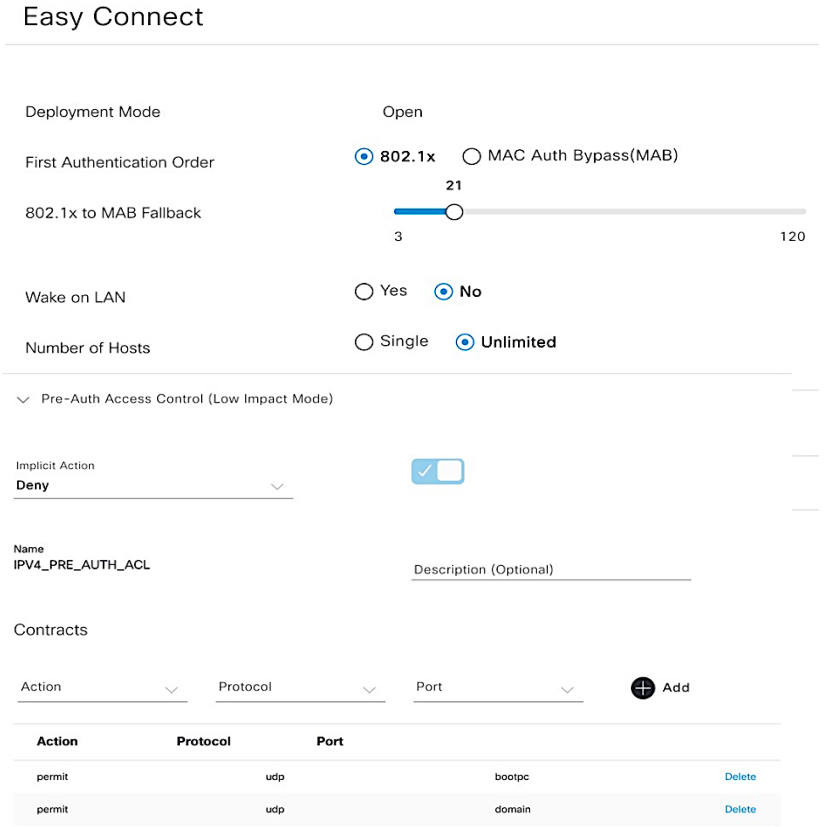


Cisco DNA Center Provision
Authentication Template



Cisco DNA Center Provision
Closed Authentication Template



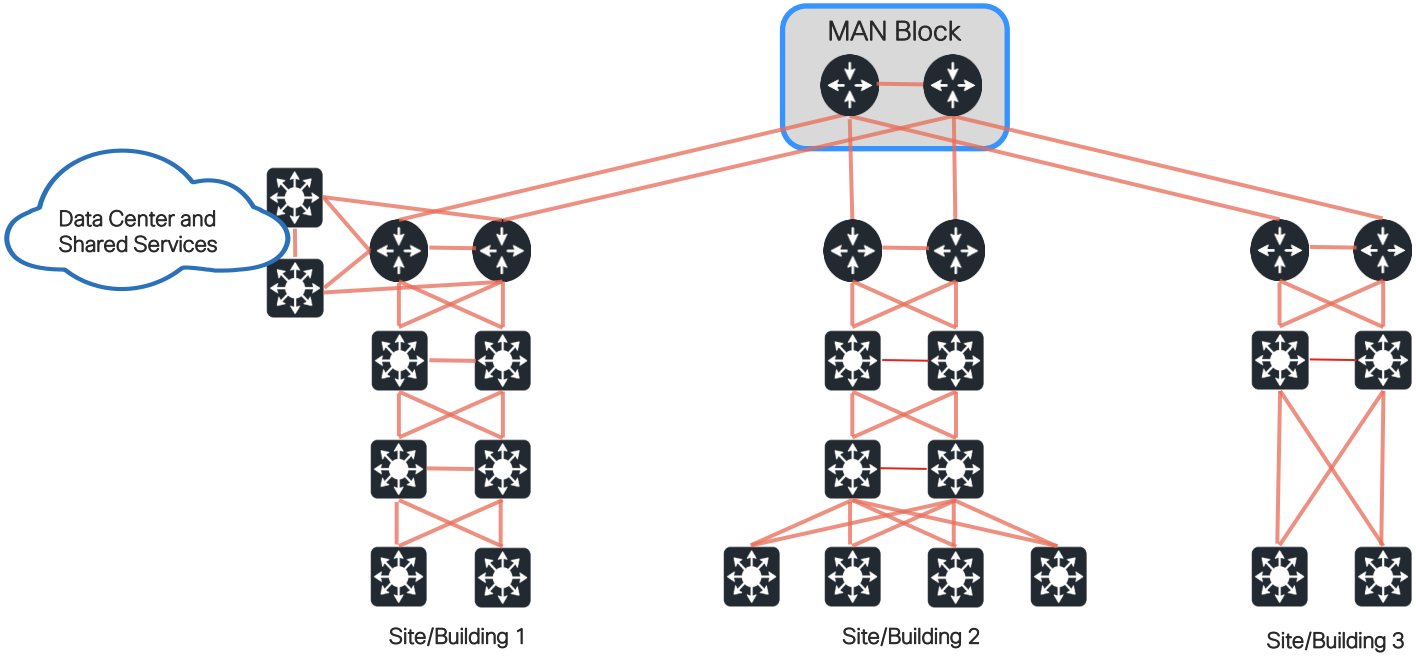


CLI's pushed with change in Fallback Timers

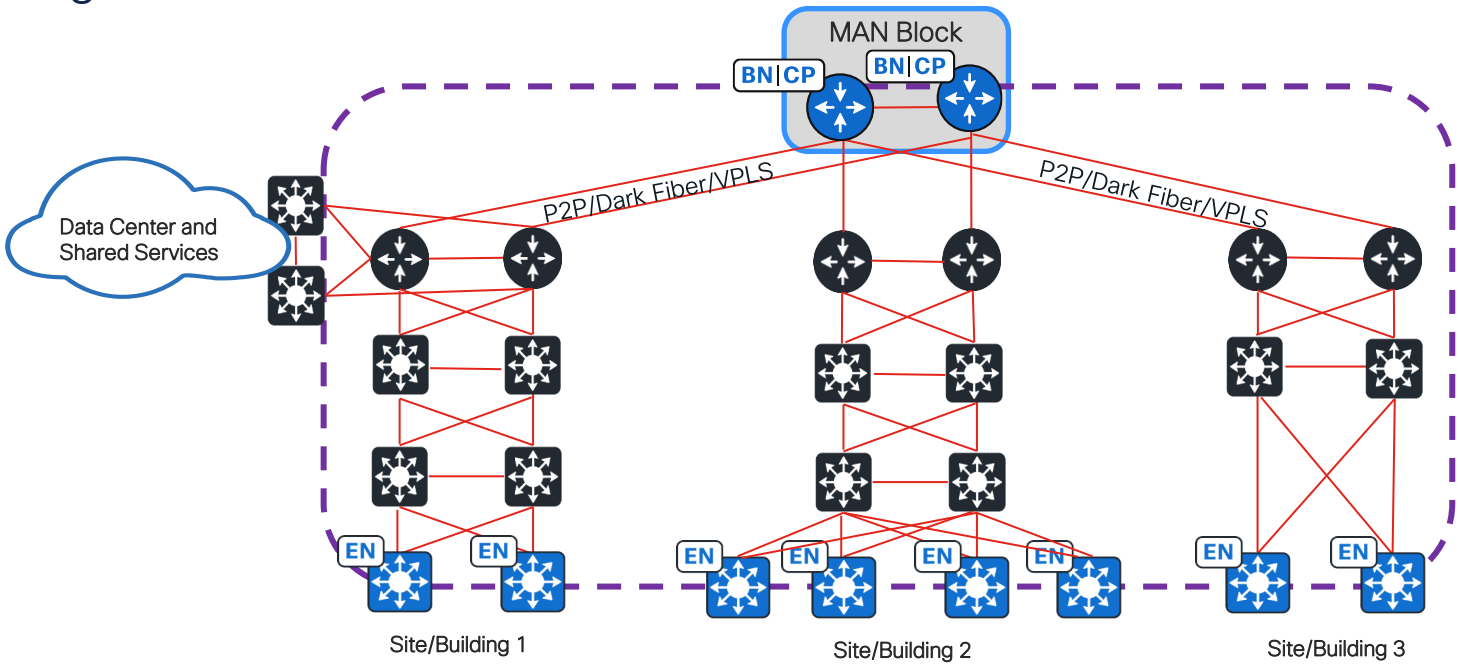
dot1x timeout tx-period 7

dot1x max-reauth-req 2

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

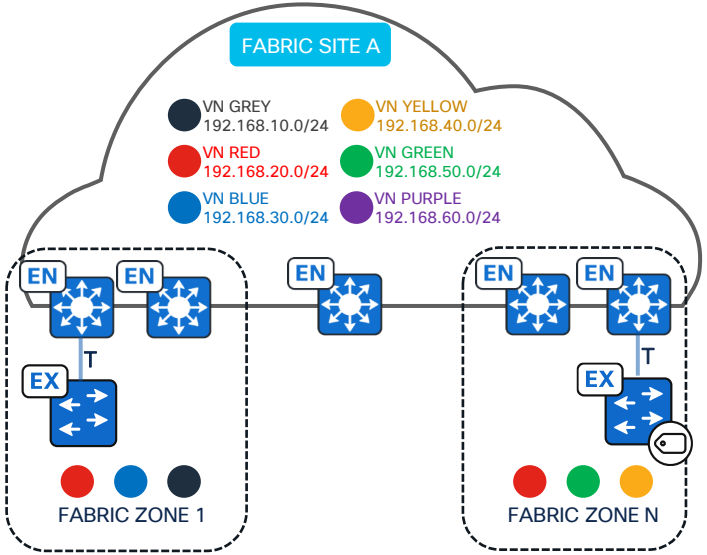
- Before 2.2.3.x, the provisioning scope of an IP Pool was the whole fabric site. For security and/or better fabric site scaling, some customers require granular control of IP Pool provisioning scope.

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.

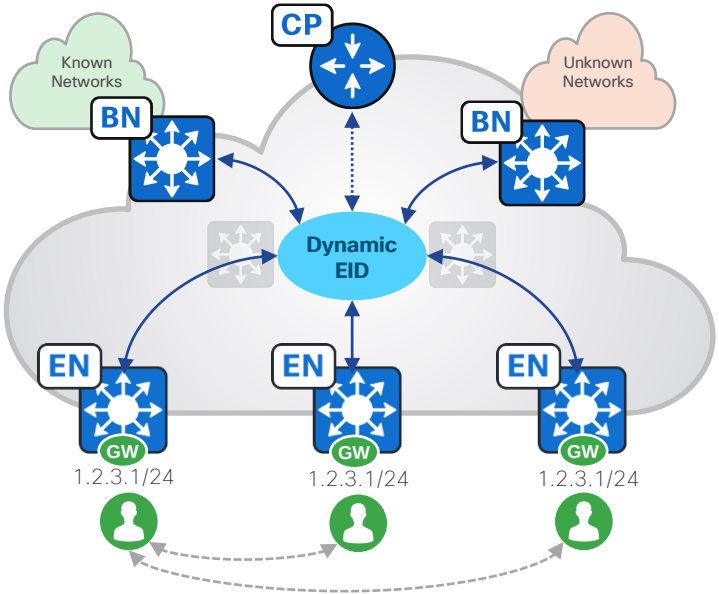
Considerations

- 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.

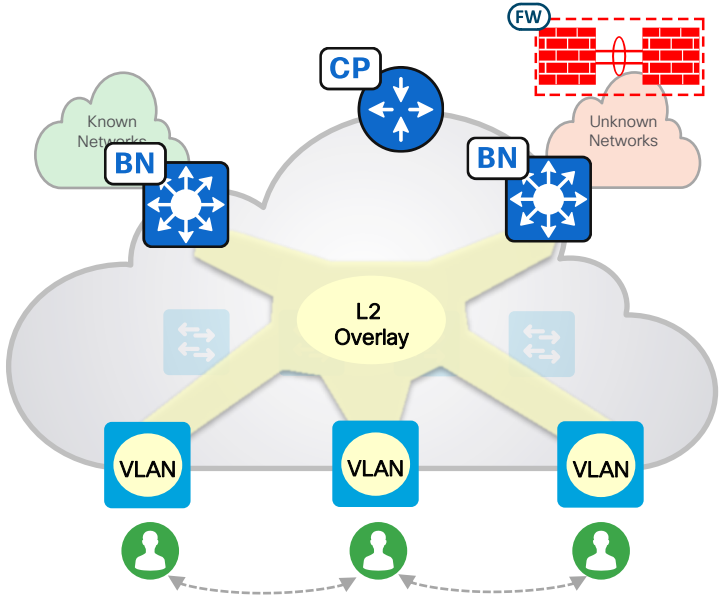


SD-Access Fabric
L3/L2 Overlays

Layer 3 Overlay
Stretched Subnets



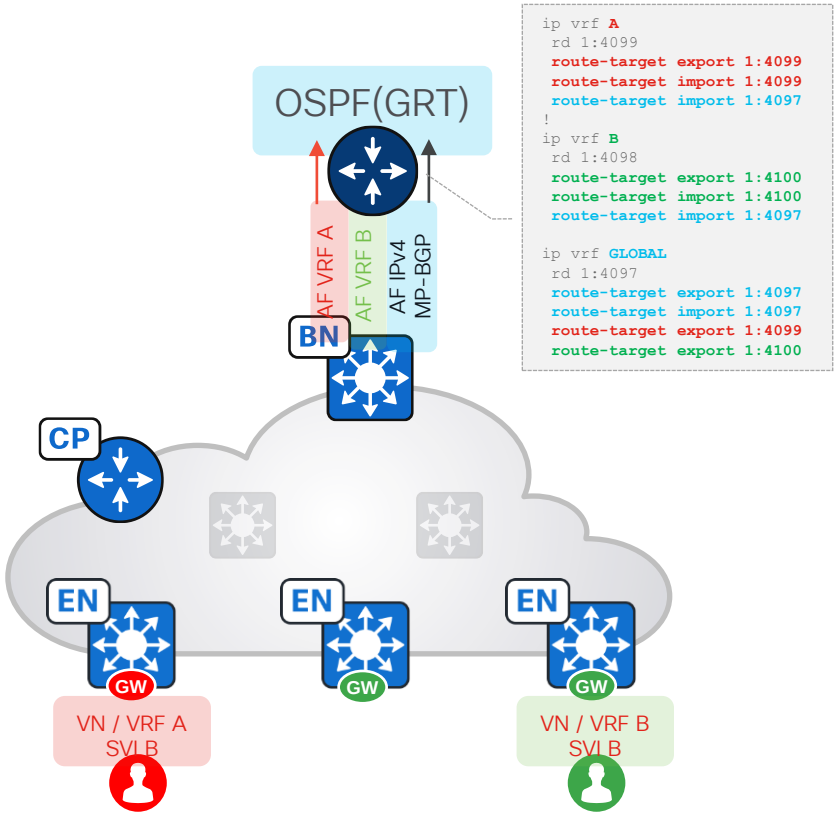
Layer 2 Overlay / GW outside Fabric



SD-Access Fabric

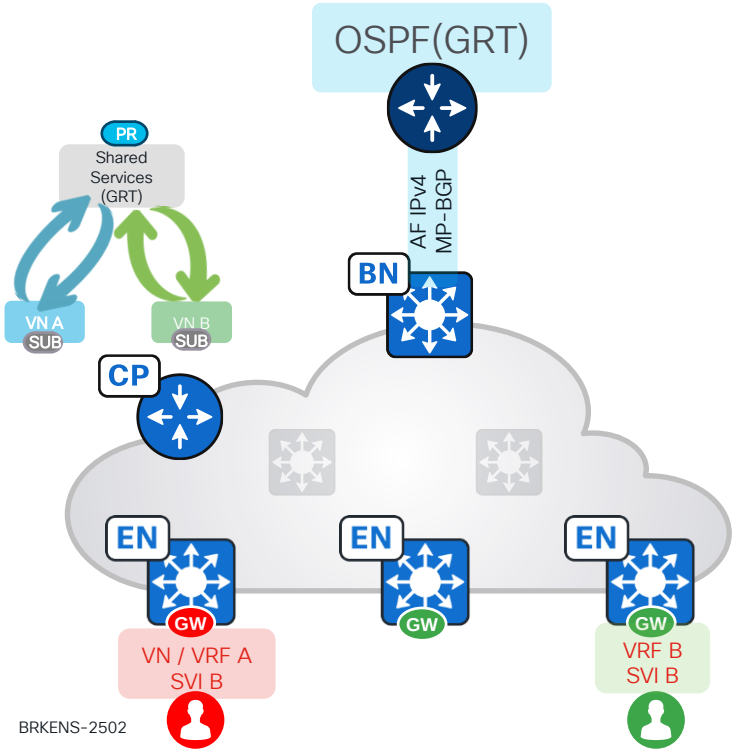
Border Handoff with Route Leaking

Traditional Route Leaking



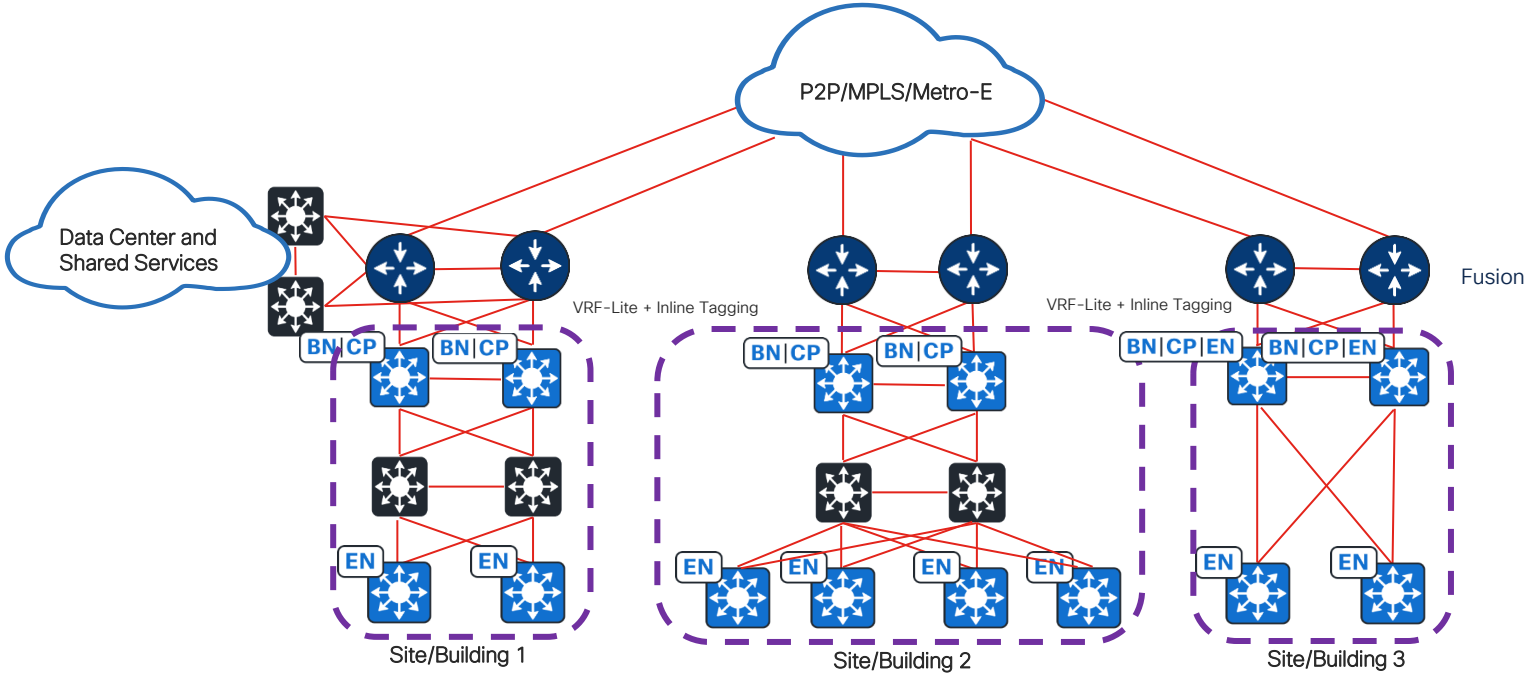

```
ip vrf A
 rd 1:4099
 route-target export 1:4099
 route-target import 1:4099
 route-target import 1:4097
!
ip vrf B
 rd 1:4098
 route-target export 1:4100
 route-target import 1:4100
 route-target import 1:4097

ip vrf GLOBAL
 rd 1:4097
 route-target export 1:4097
 route-target import 1:4097
 route-target export 1:4099
 route-target export 1:4100
```

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

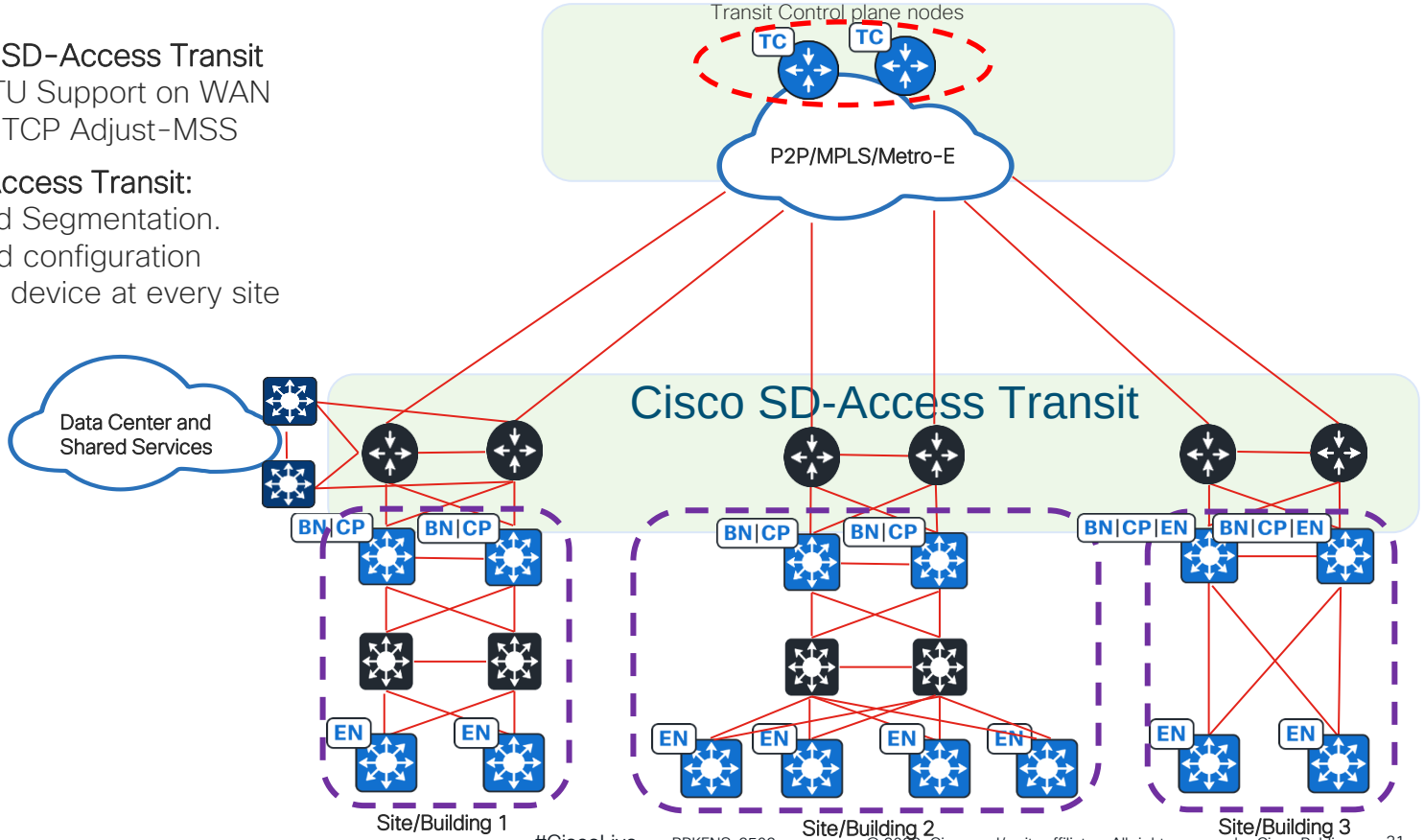
Multisite Architecture with SD-Access Transit

Pre-Requisite with SD-Access Transit

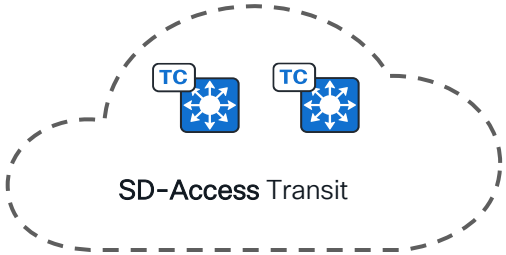
- Higher MTU Support on WAN
- *Else use TCP Adjust-MSS

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



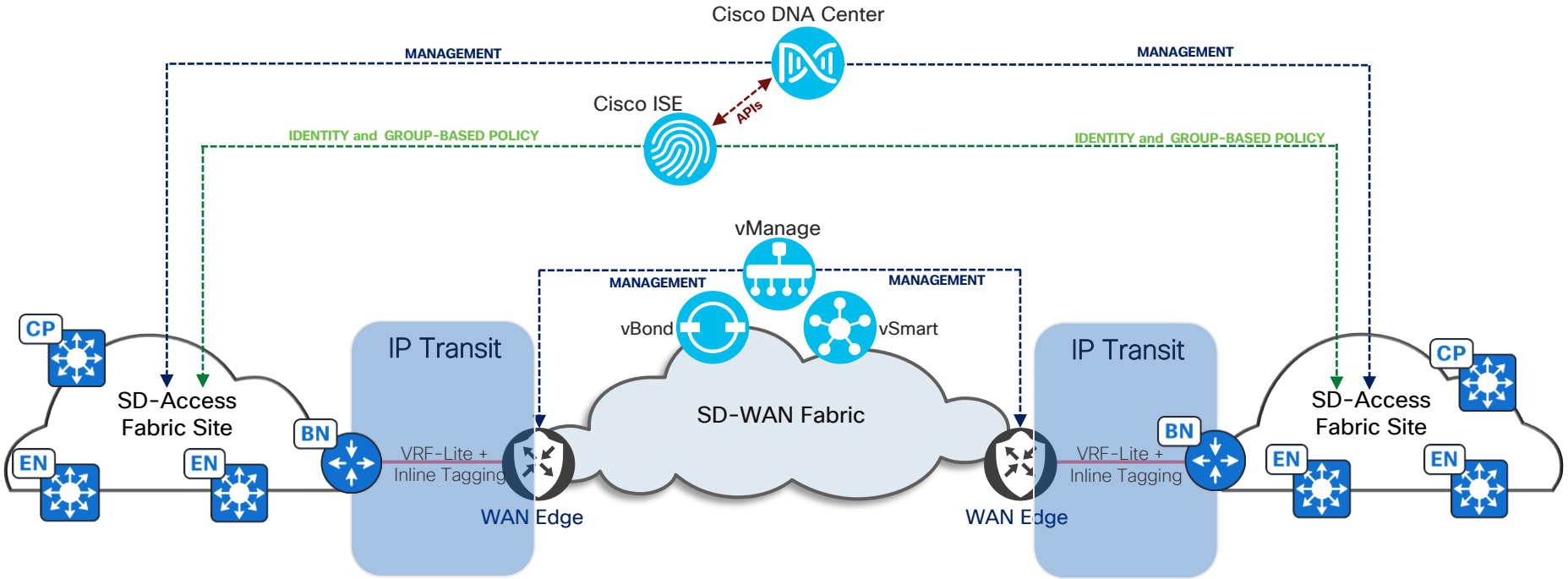
SD-Access Transit is a native solution carrying VN and SGT between Fabric sites.

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**

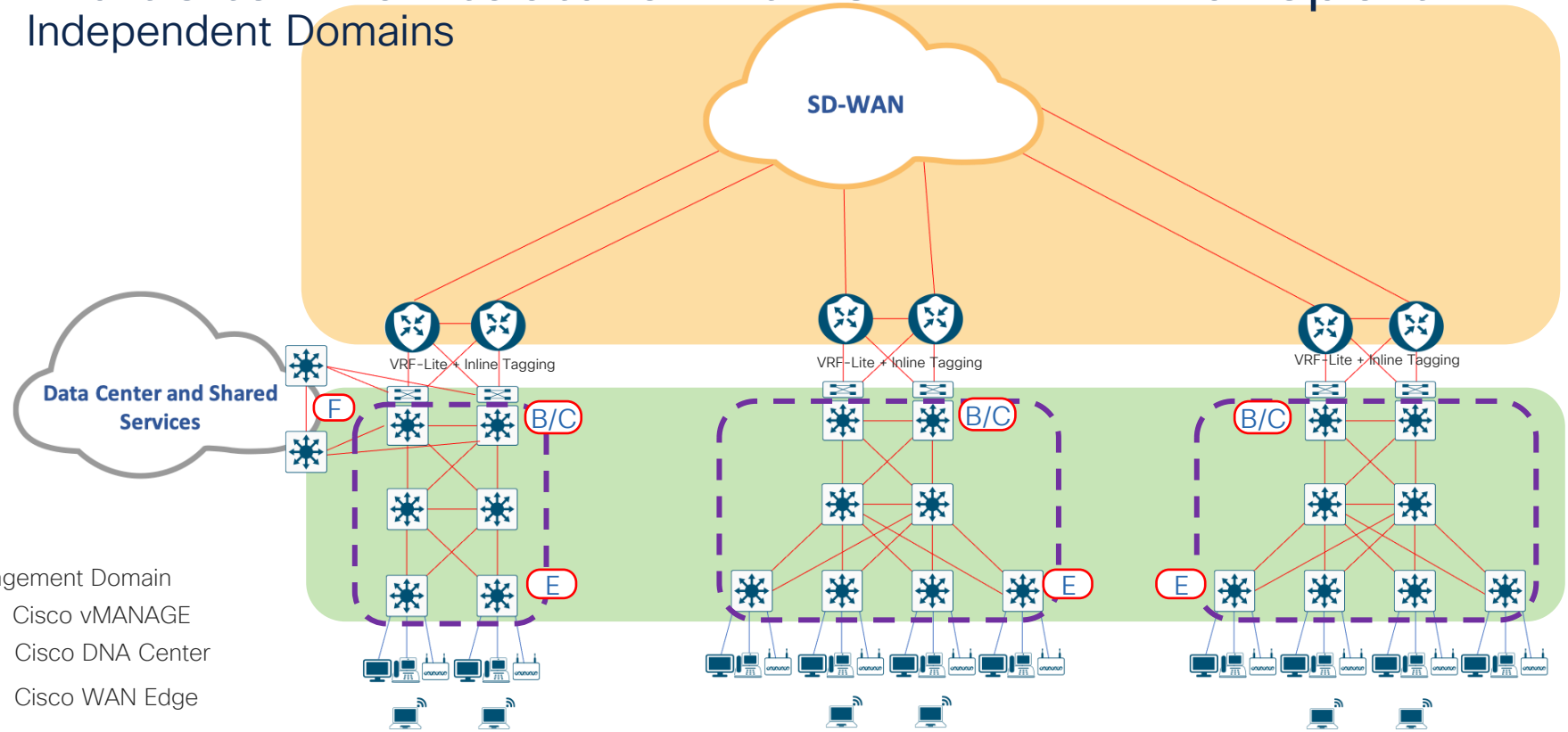
Multisite Architecture with SD-WAN Transport
Independent Domains



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

Multisite Architecture with SD-WAN Transport

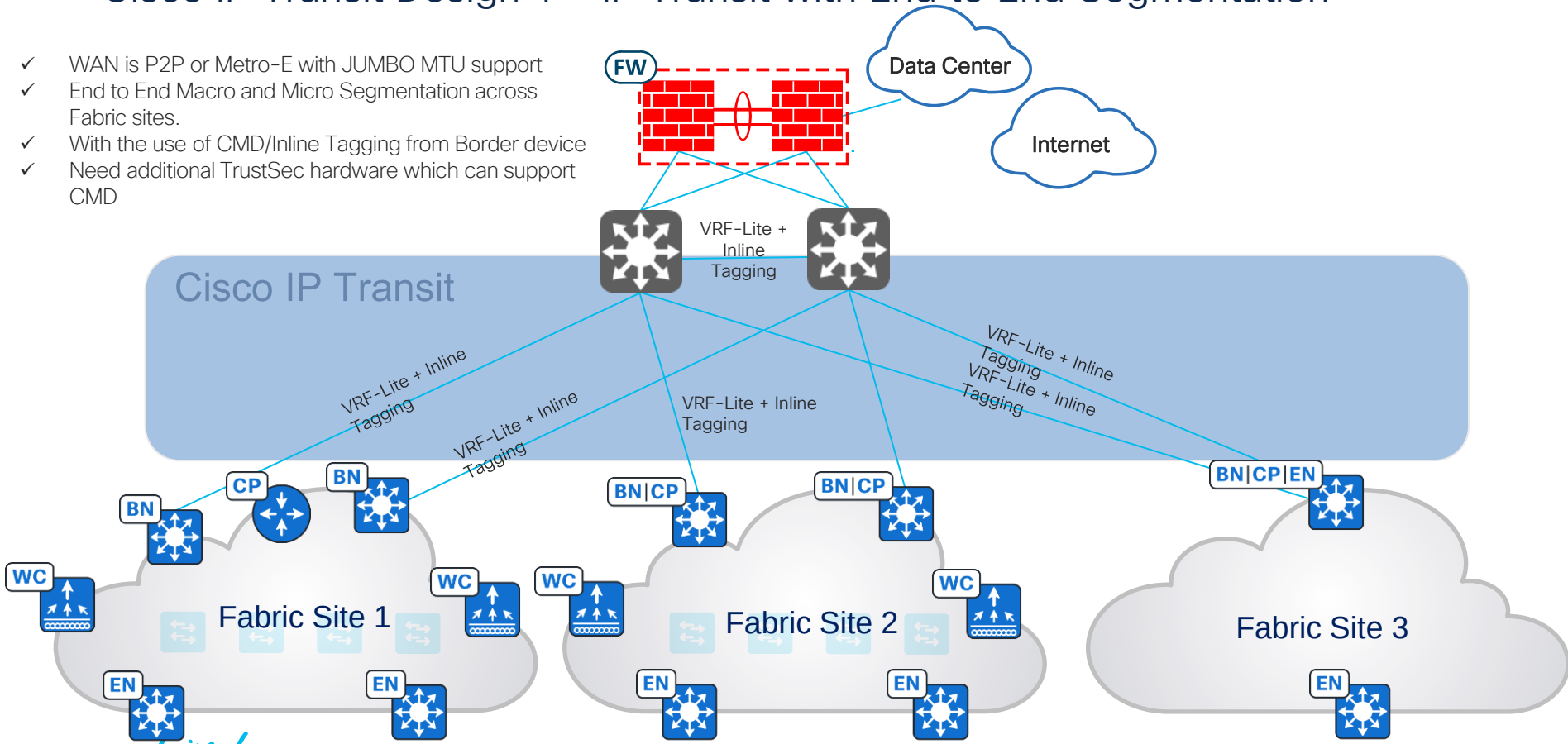
Independent Domains



Cisco SD-Access Multisite

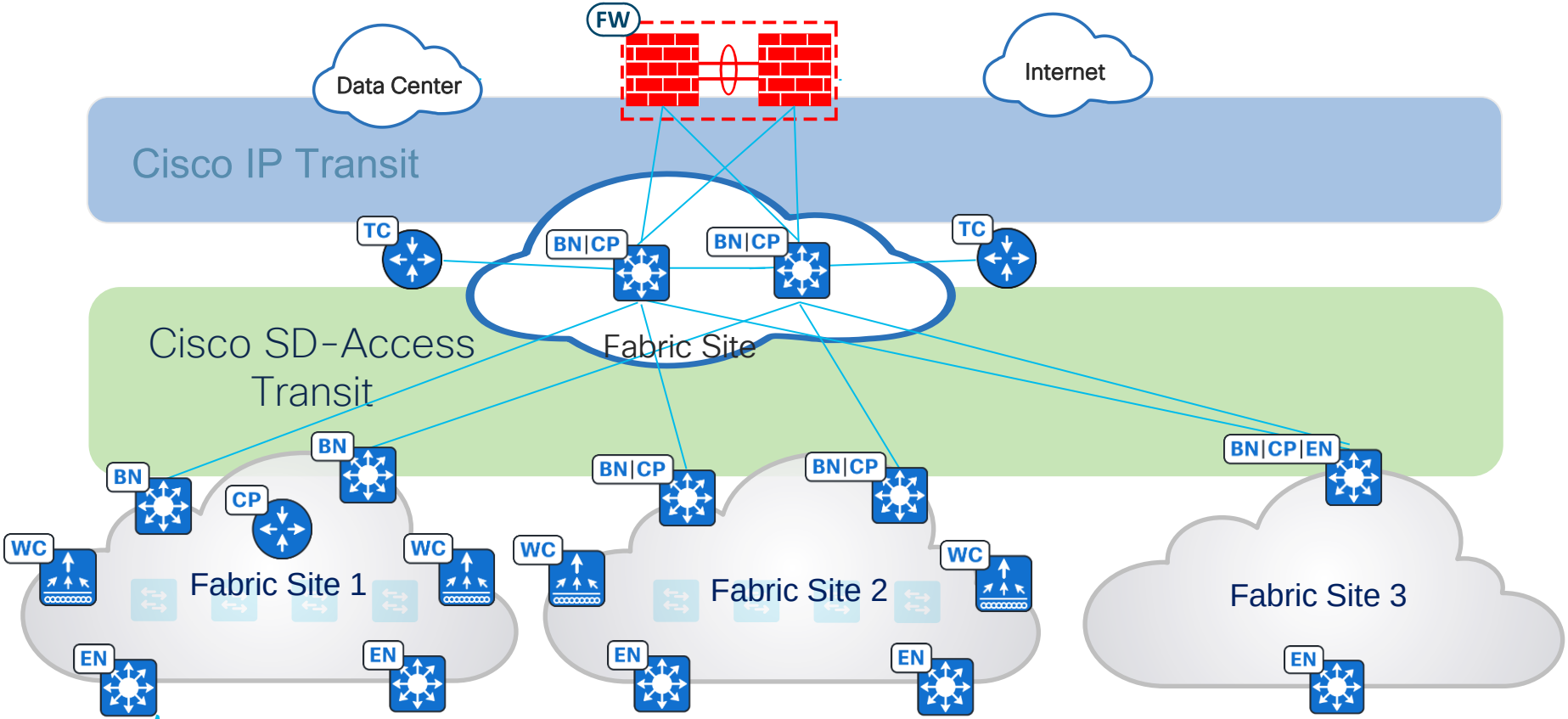
Cisco IP Transit Design 1 – IP Transit with End to End Segmentation

- ✓ 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



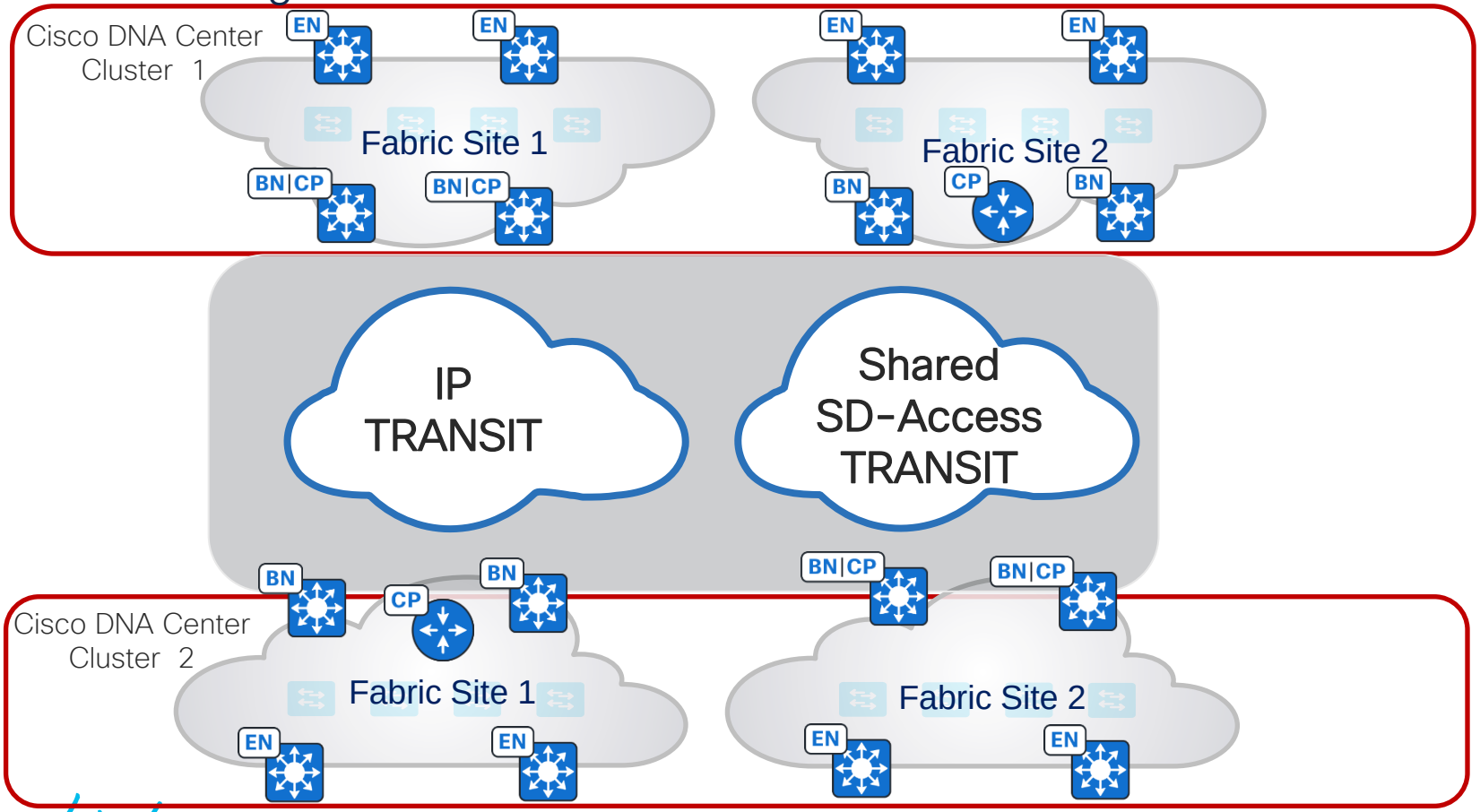
Cisco SD-Access Multisite

Cisco SD-Access Transit Design 1



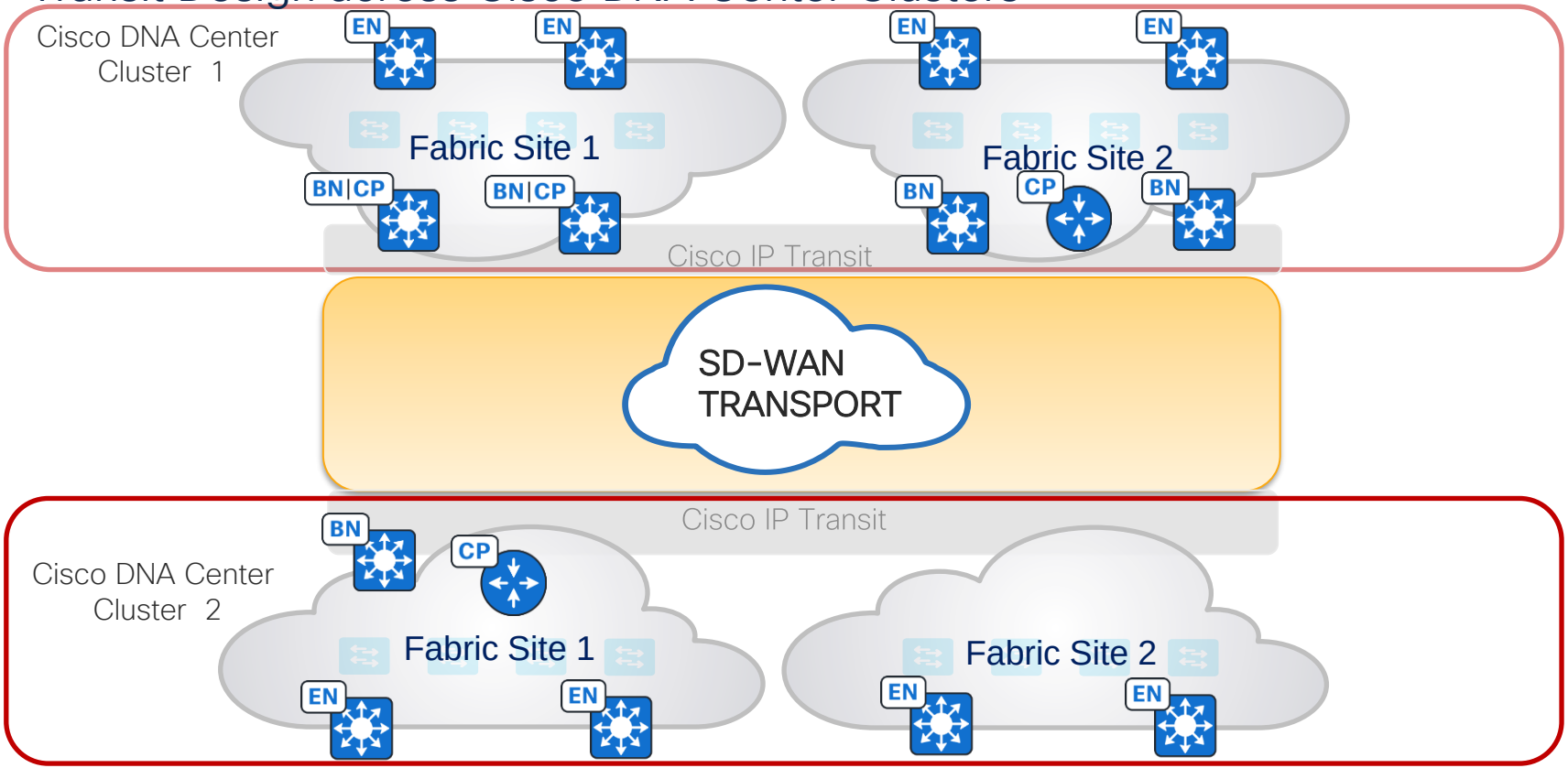
Cisco SD-Access Multisite

Transit Design across Cisco DNA Center Clusters



Cisco SD-Access Multisite

Transit Design across Cisco DNA Center Clusters



Cisco SD-Access Multicast

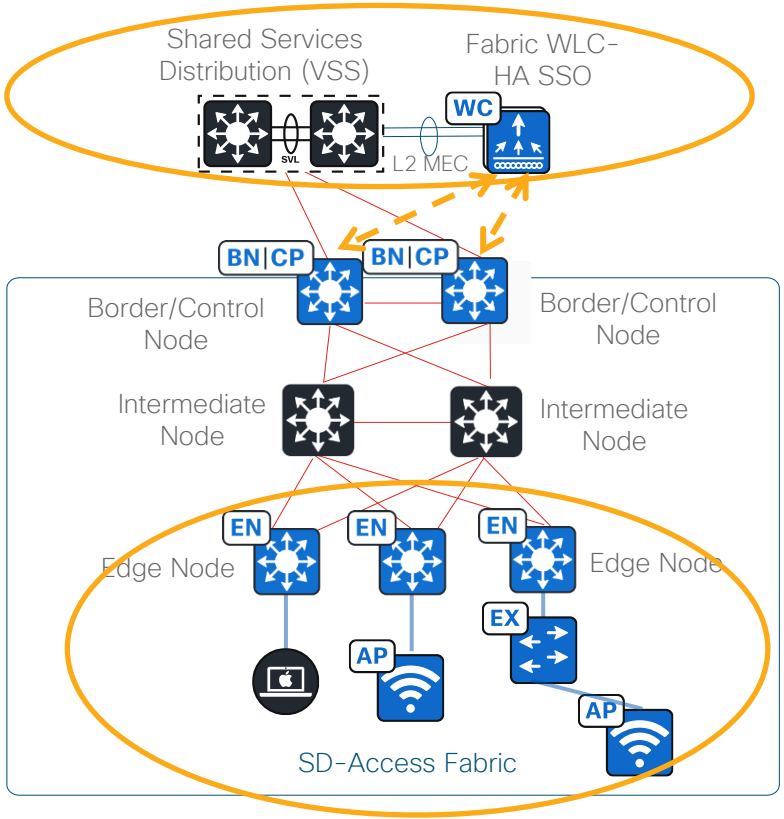
Supported Modes(Overlay)	: ASM, SSM
RP Overlay Placement (ASM)	: Inside/Outside Fabric
Source/Receiver Placement	: Inside/Outside Fabric
Multicast Configuration	: Automated by Cisco DNA Center
Per VN RP support	: Supported
Multi-site with SD-A Transit	: Supported with LISP PUB/SUB
Multiple RP per VN	: Supported
Group to RP Mappings	: Supported
Concurrent ASM/SSM	: 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

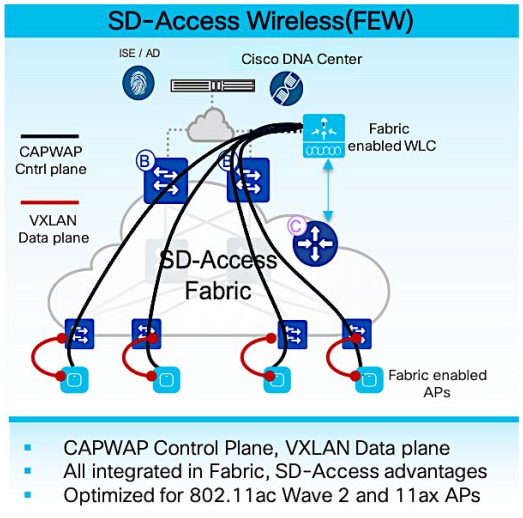
SD-Access Wireless Connectivity

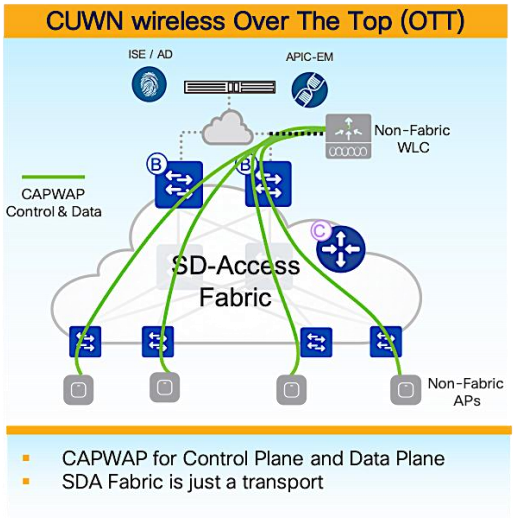


- WLC typically connect to a “shared services” Distribution Block
  - VSS/Stack is the preferred topology
  - Management IP address in Global Routing Table
  - Specific route to advertise WLC’s IP in the underlay
- WLC can talk to only #2 Enterprise CP nodes
- Access Points connect to Fabric Edge
  - 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	: FEW , OTT , Mixed Mode
Supported Platforms	: C9800, EWC,3504,5520,8540
AP Mode	: Local, Flex*
Control-Plane Node support	: 2(AireOS) , 8(C9800)*



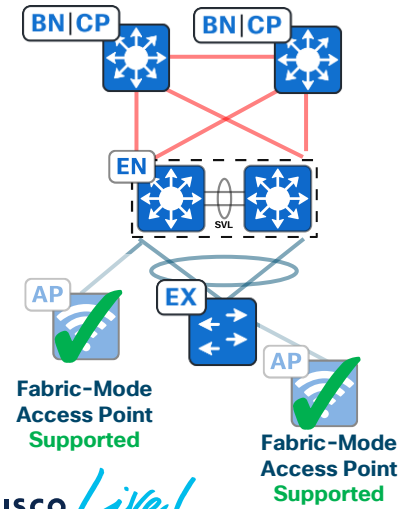


SD-Access Wireless Design Best Practices

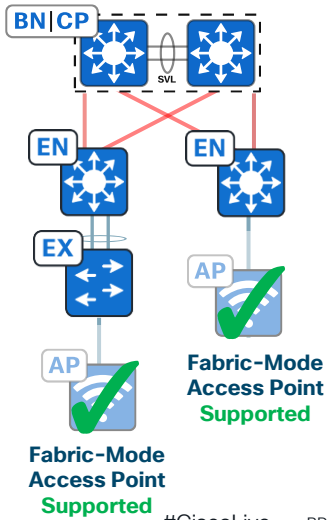
SVL in Fabric Topology Examples

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

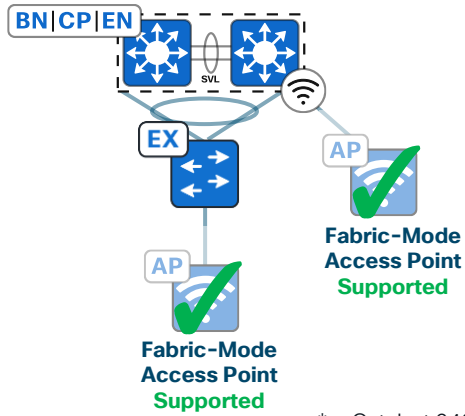
Fabric AP to SVL Edge Node



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

DNA Center: 2.1.2.0

Redundancy Comparison

Stateless Redundancy with N+1 HA

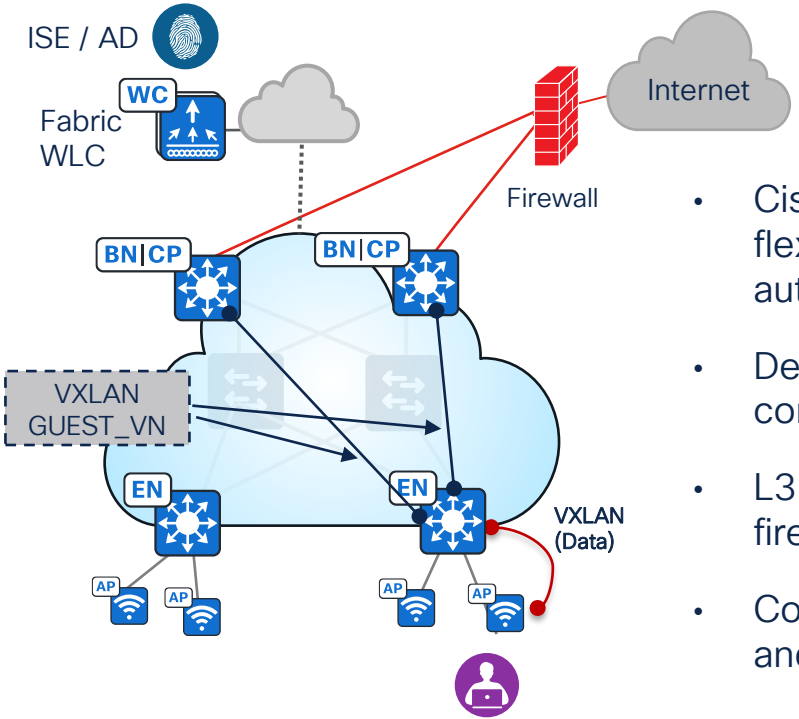
- WLCs remain independent of each other. Cisco DNA Center and SD-Access fabric sees them as two separate WLCs.
- For each location there is a primary and a secondary WLC.
- Both WLCs communicate with the control plane nodes.
- In a failover event, the CAPWAP tunnel is broken between AP and Primary WLC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

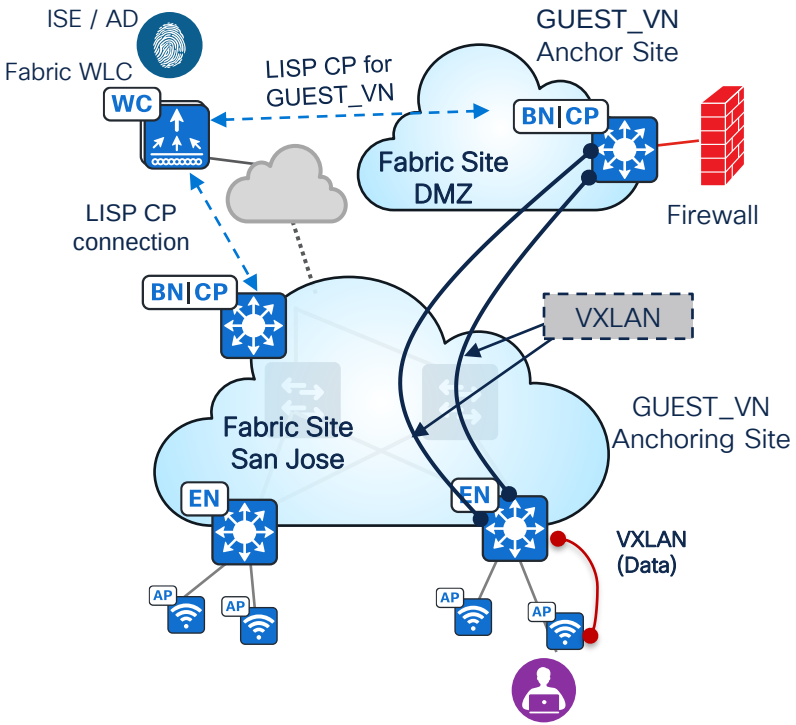
Wireless Guest Design – Dedicated Virtual Network



- Cisco DNA 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

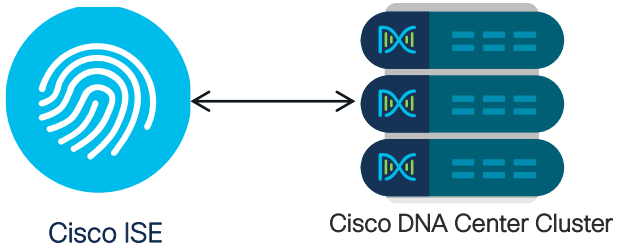
Cisco SD-Access Wireless

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

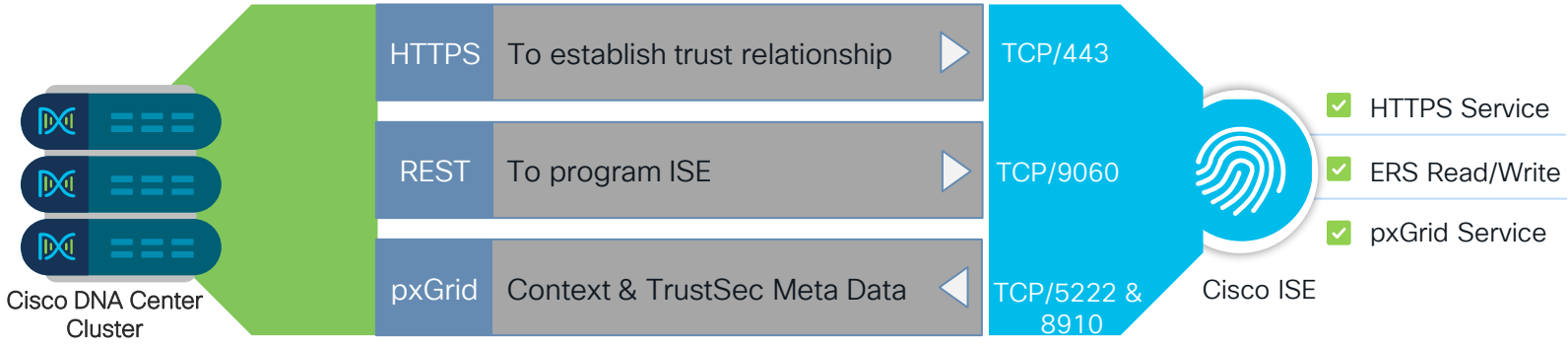
Device Administration
TACACS

Asset Visibility
Everything & Everyone on Network

Policy Analytics
Group to Group Interaction with automated policy

Security Ecosystem Integration
Context Sharing

Cisco DNA Center & ISE Communication



Cisco ISE: Enable below ISE Services

Administration > System >Deployment > Select ISE Host Name

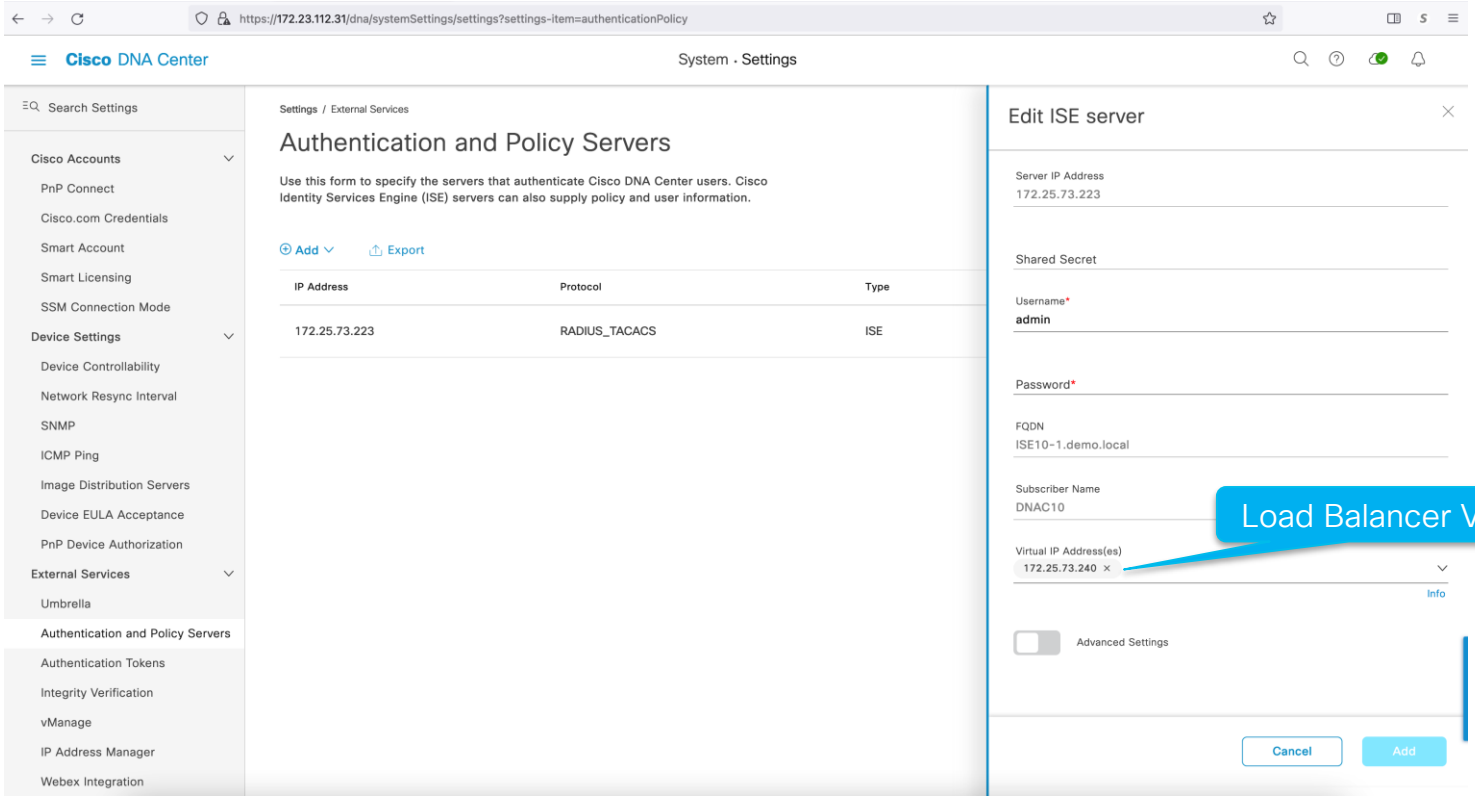
Enable pxGrid Services

Administration > Settings > ERS Settings

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

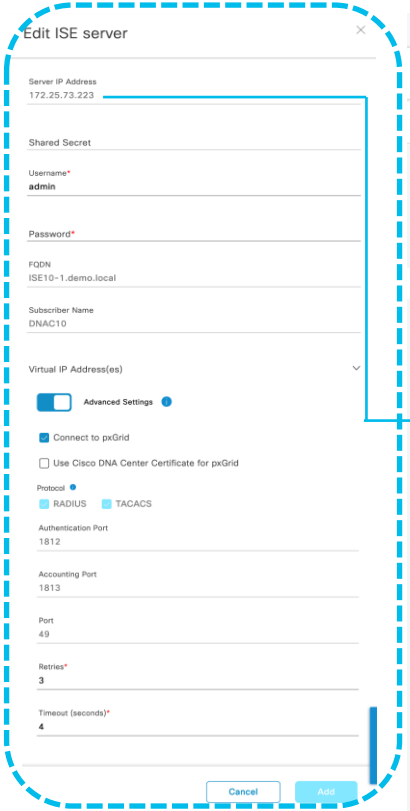
Enable *ERS for Read on* ***All other Nodes*** *incase of Distributed model*

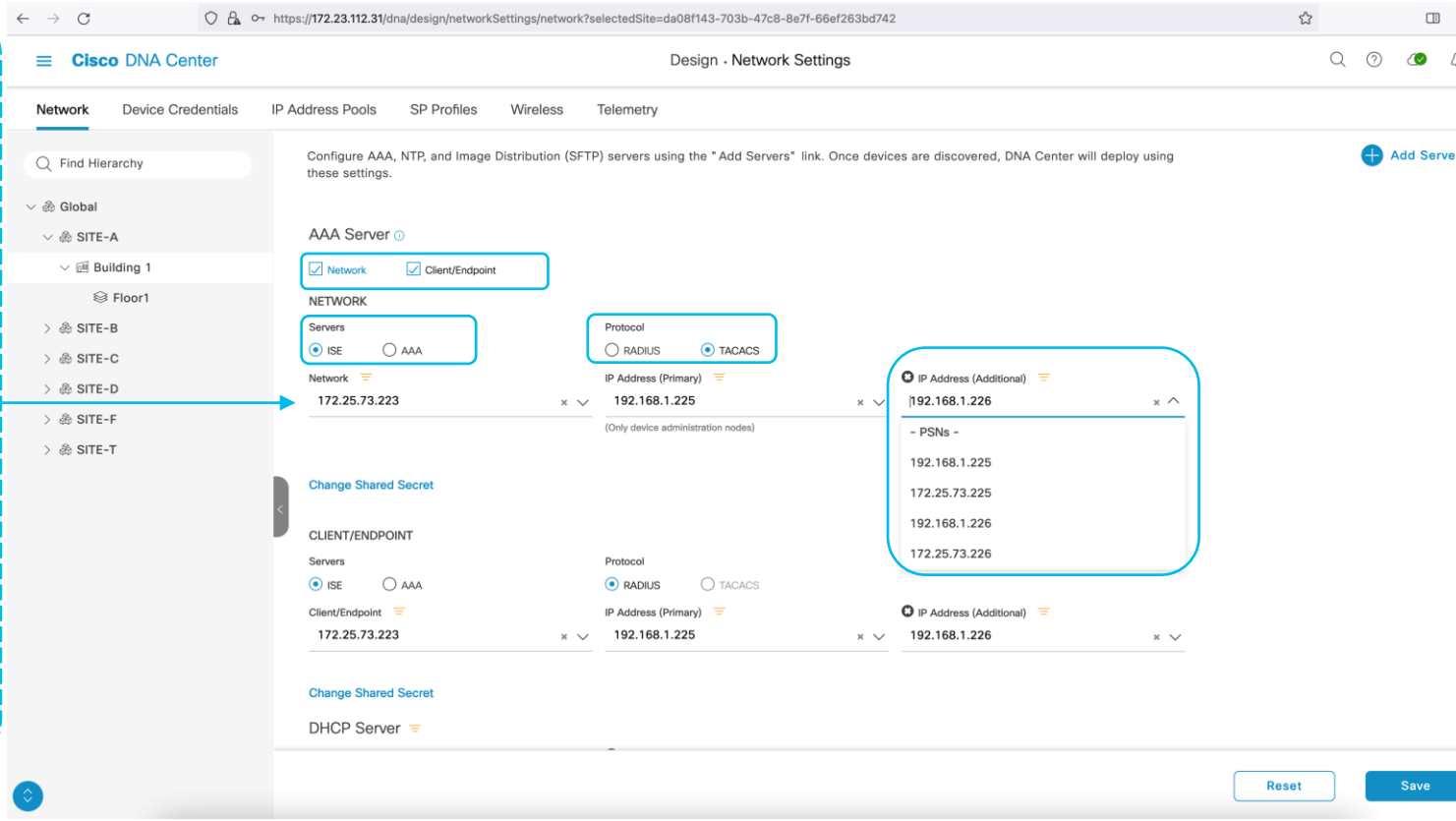
Cisco DNA Center Settings
Cisco ISE + Load Balancer



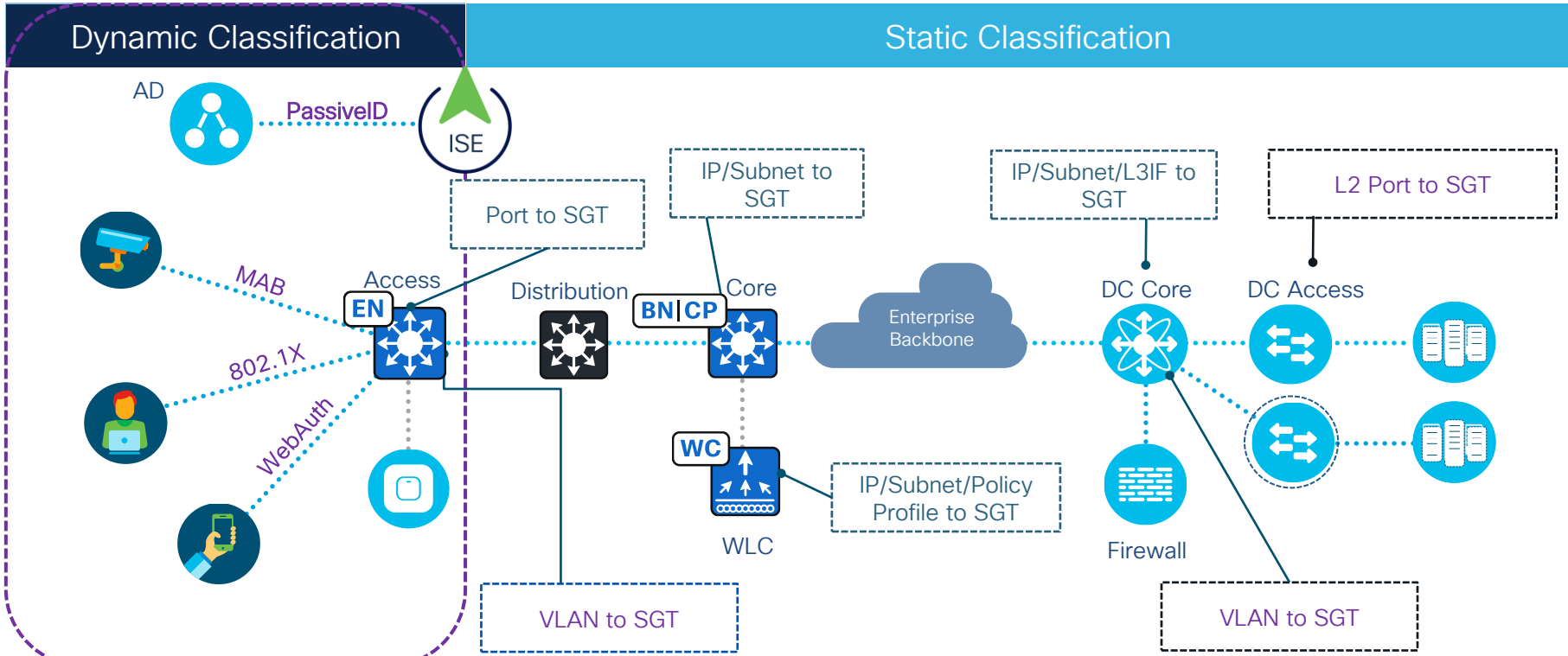
Cisco DNA Center Design

ISE as AAA Server for Client and Network





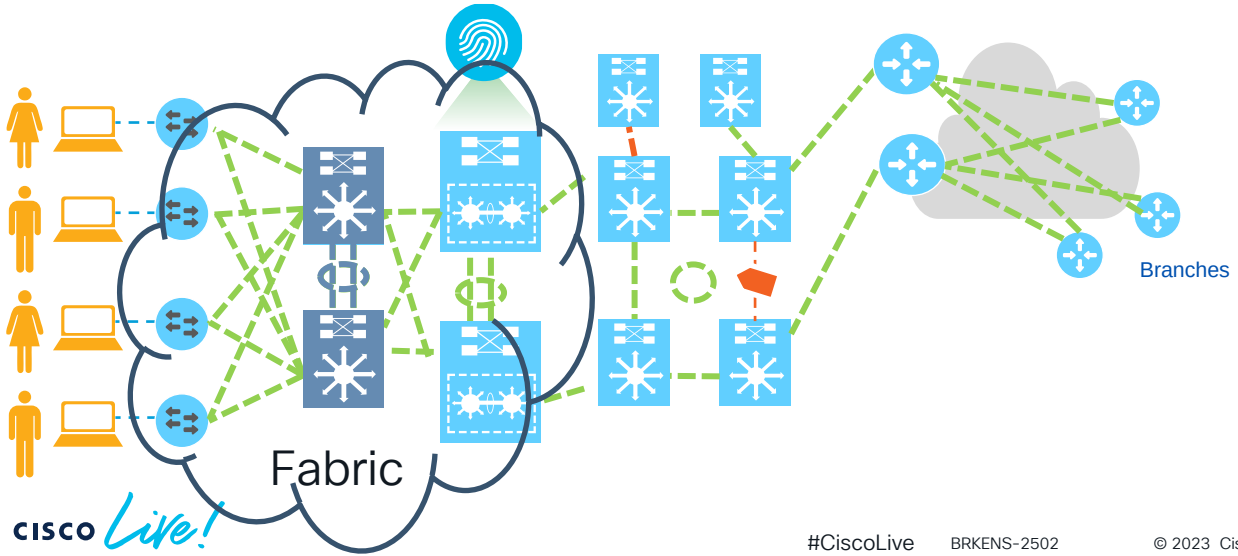
Security Group Tags(SGT)
Classification Mechanism



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

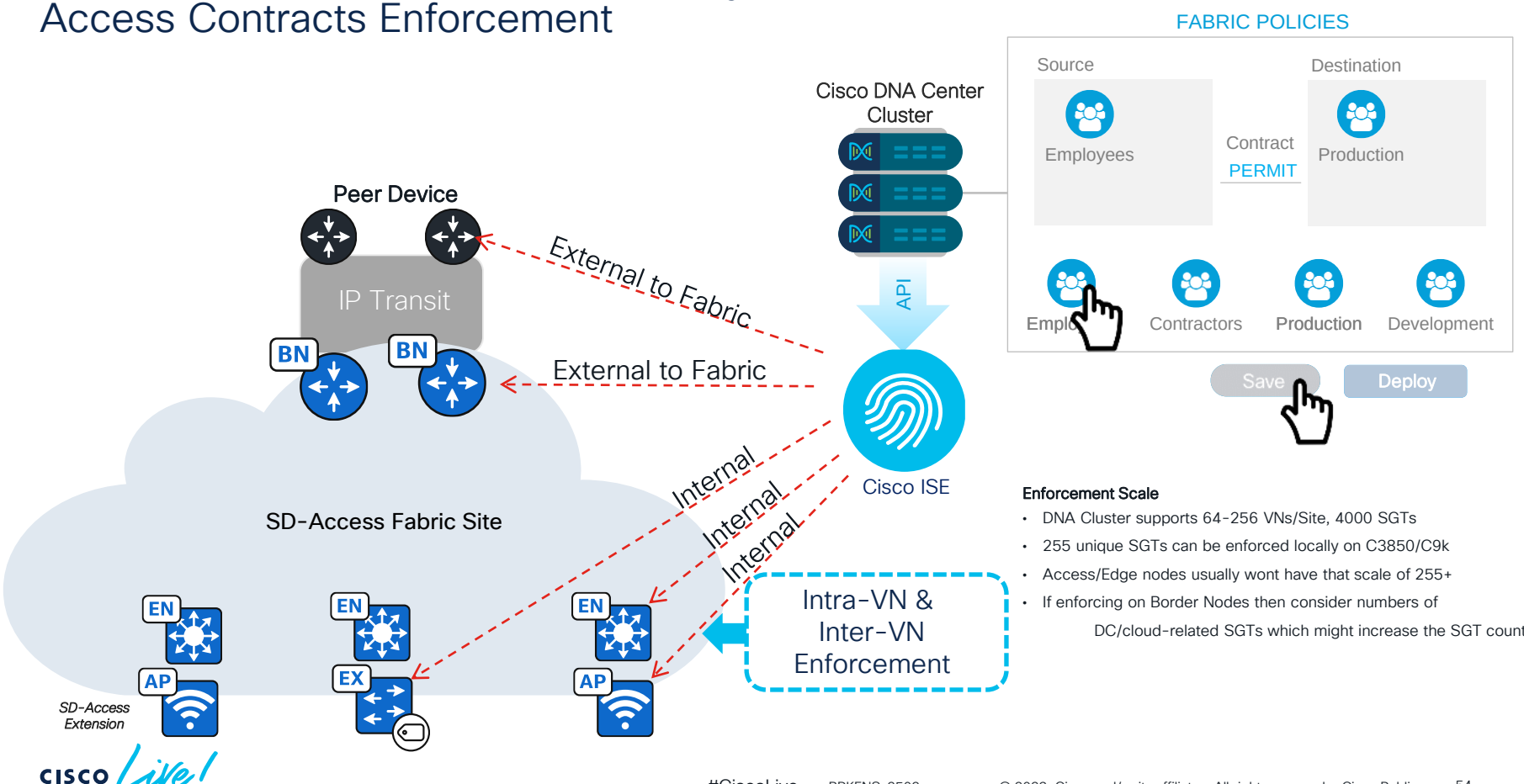
- Cisco MetaData (CMD)
- Ethernet
- MACsec
- IPsec
- DM-VPN
- GET-VPN
- **VXLAN**

Supporting devices

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

Cisco DNA Center Policy

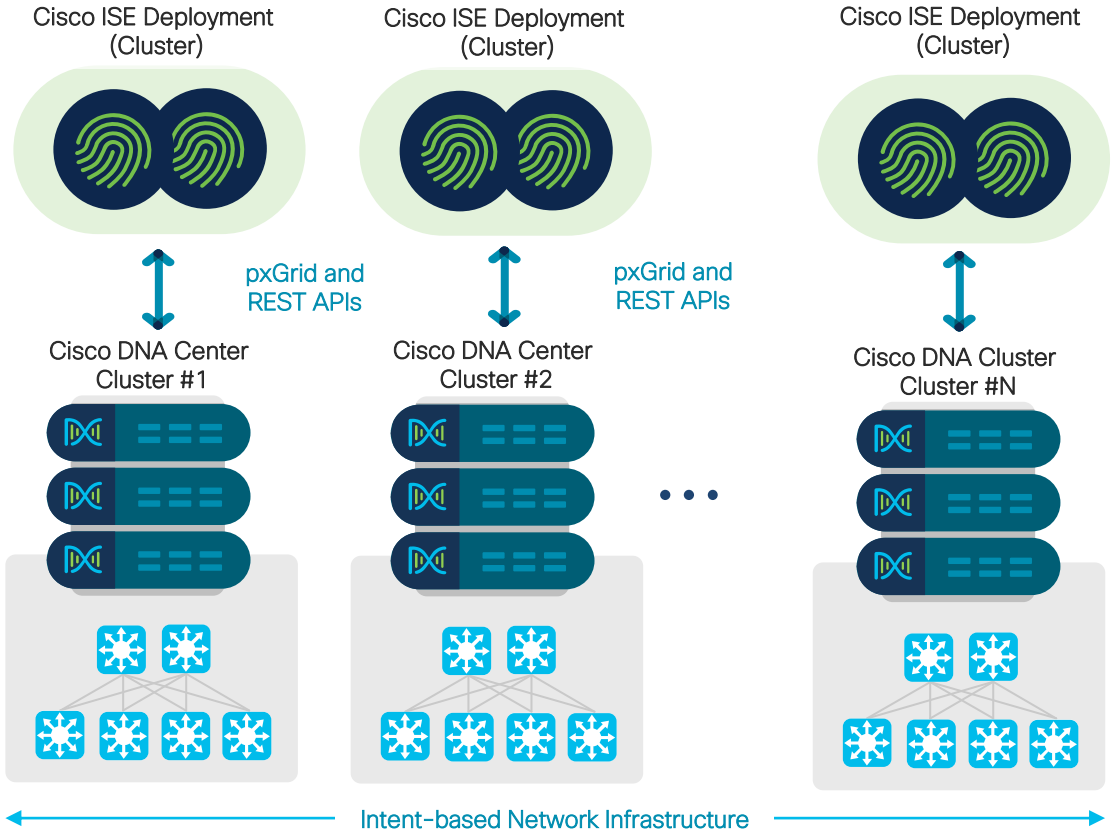
Access Contracts Enforcement



Enforcement Scale

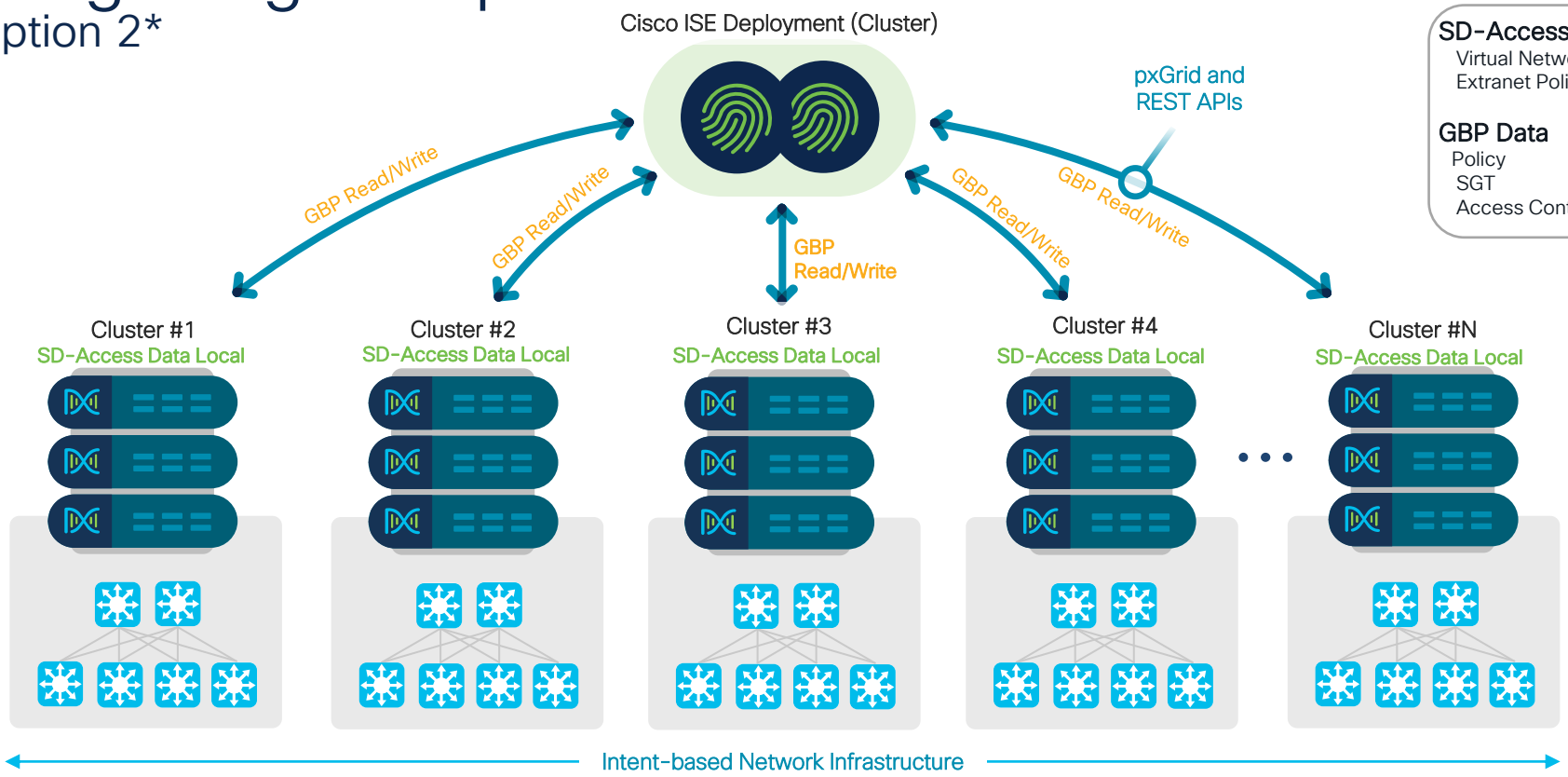
- DNA Cluster supports 64-256 VNs/Site, 4000 SGTs
- 255 unique SGTs can be enforced locally on C3850/C9k
- Access/Edge nodes usually wont have that scale of 255+
- If enforcing on Border Nodes then consider numbers of DC/cloud-related SGTs which might increase the SGT counts

Integrating Multiple Cisco DNA Center with ISE
Option 1



Integrating Multiple Cisco DNA Center with ISE

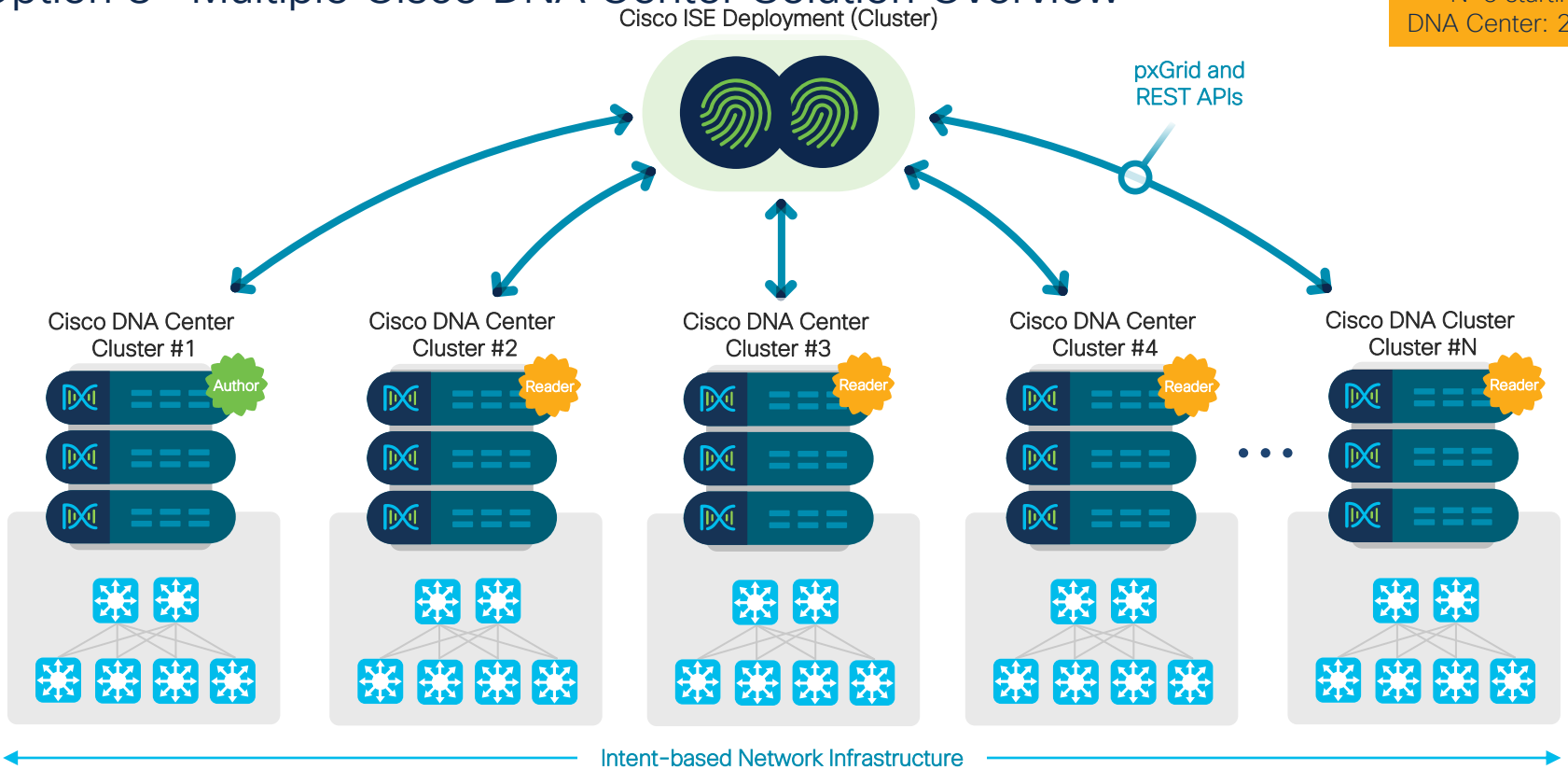
Option 2*



Integrating Multiple Cisco DNA Center with ISE

Option 3- Multiple Cisco DNA Center Solution Overview

N=5 starting
DNA Center: 2.2.3.x

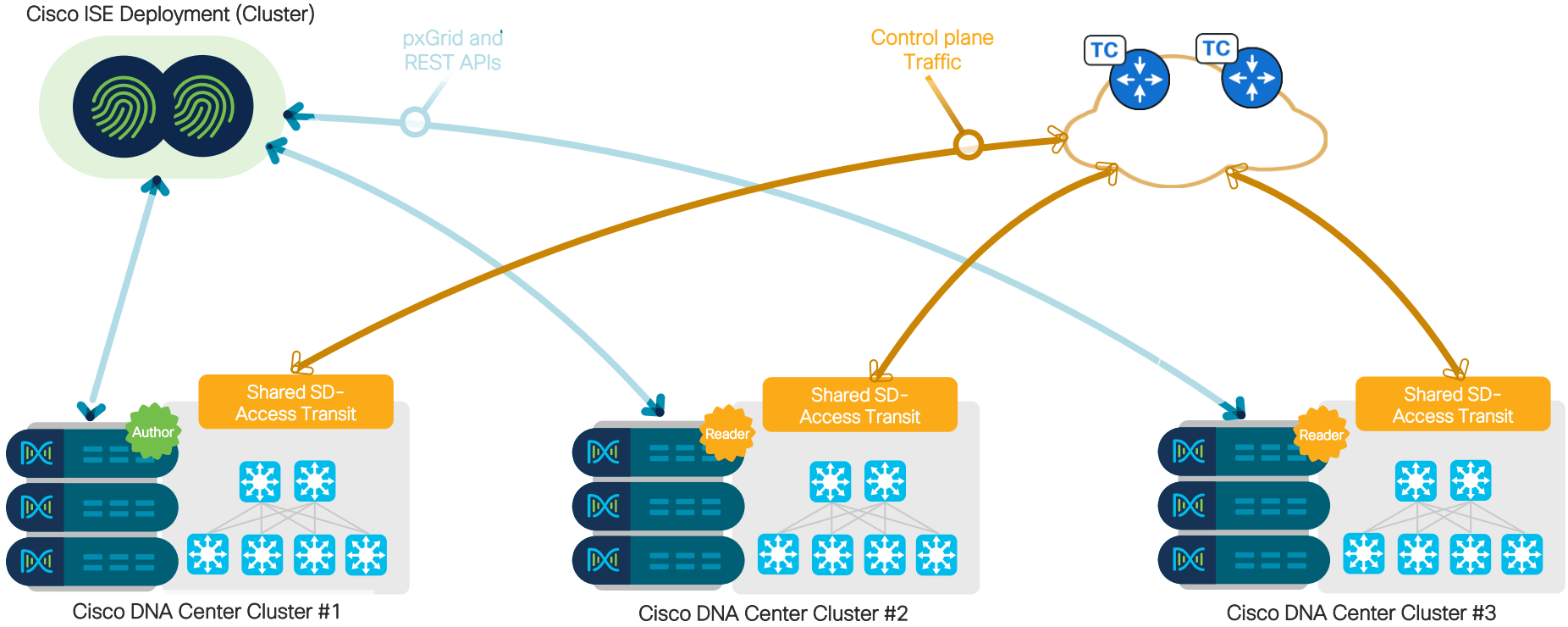


Multiple Cisco DNA Center to Single Cisco ISE PDG

Multiple Cisco DNA Center Use Case
Shared SD-Access Transit

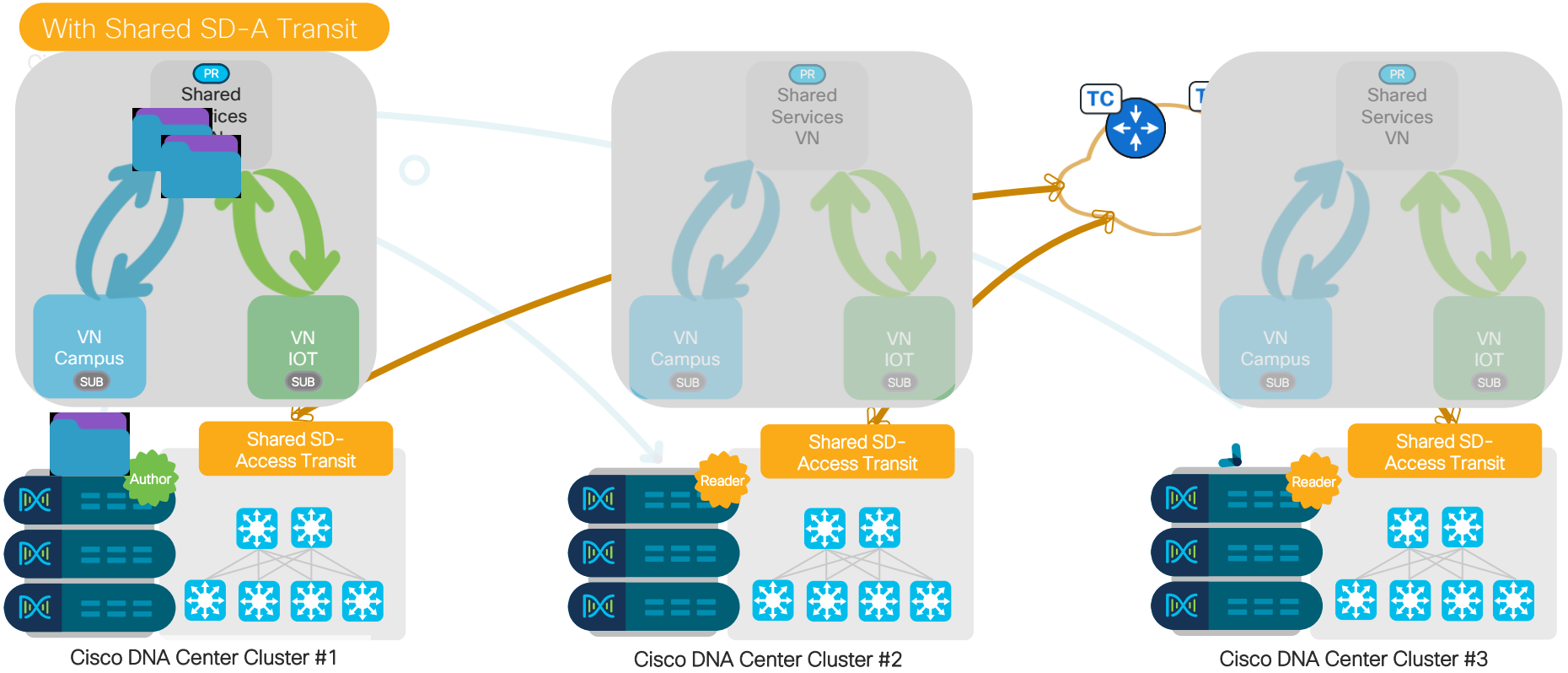
Shared SD-Access Transit starting DNA Center: 2.2.3.x

4 TCP Node supported Starting DNA Center : 2.3.3.0



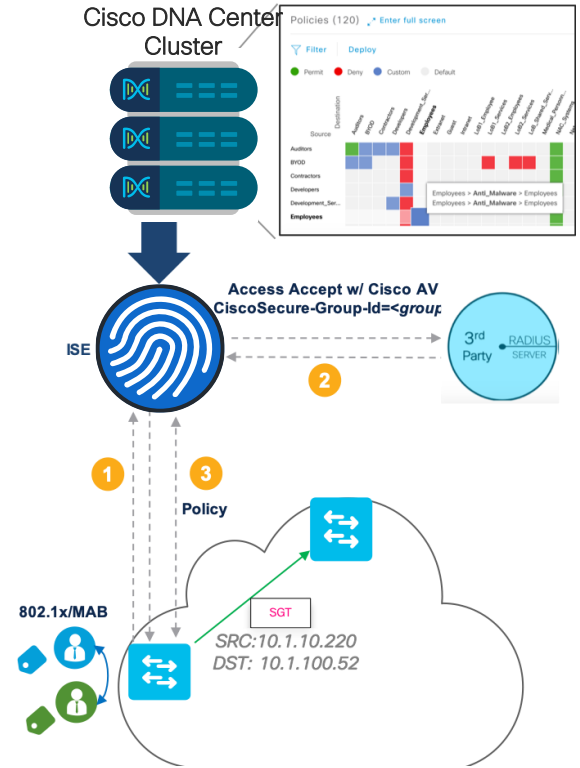
SD-Access Transit shared across multiple Cisco DNA Center Clusters

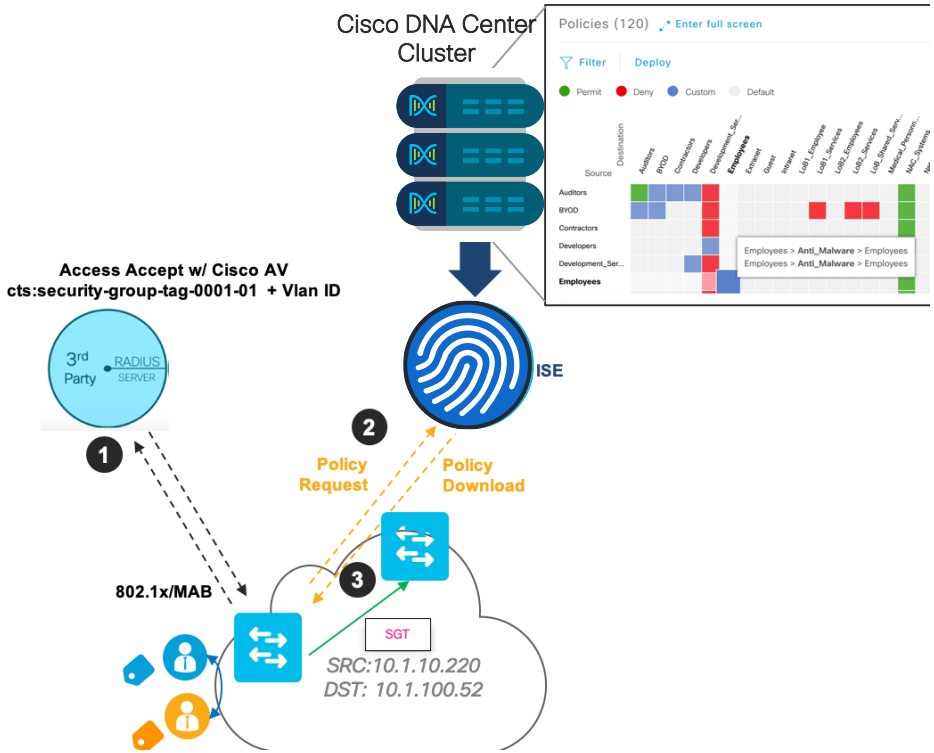
Multiple Cisco DNA Center
LISP Extranet Policy- Scenario 1(Shared Policy)



SD-Access Transit shared across multiple Cisco DNA Center Clusters

Cisco DNA Center Policy
Third-Party AAA/RADIUS Server support

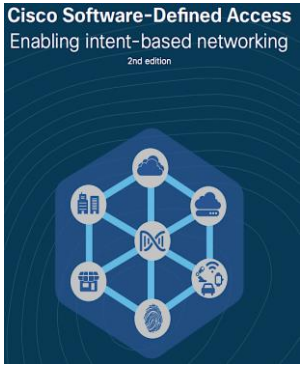




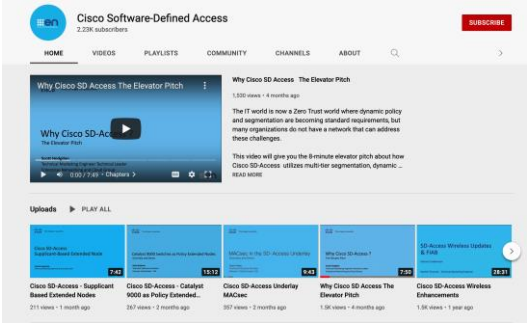
Cisco SD-Access Collaterals

[Cisco Software-Defined Access for Industry Verticals]

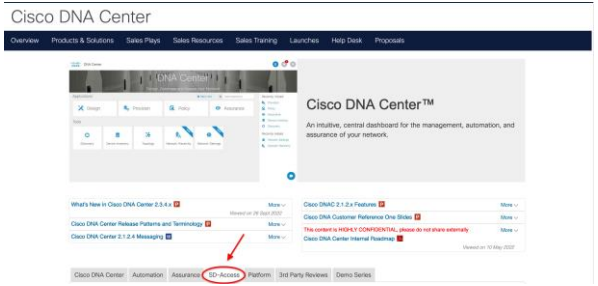
[Cisco Software-Defined Access]
[Enabling intent-based networking]



[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]

Options for deployment

- Cisco DNA Center automated configuration of a Cisco LISP Fabric which includes Macro and Micro Segmentation
  - Includes SDA Automation Workflows and Integrations
  - Best practice standardized configurations
  - Includes SDA Assurance

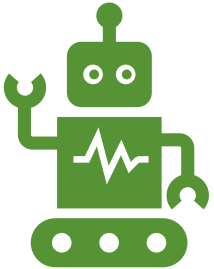
OR

- CLI Configuration of Cisco LISP Fabric which includes Macro and Micro Segmentation
  - Open integration with heterogenous tooling (CLI, Ansible, NSO, etc)
  - Agile customization within the parameters of the LISP Fabric validated design
  - Can support DNAC Device and Client Assurance
  - Subset of features supported compared to what is available with Cisco DNA Center.

Raise of Hands!!

- How many of you use automation systems to orchestrate network configurations today on the network devices?
- Example of automation systems (Ansible playbooks, NSO)

- How many of you would be interested in deploying LISP VXLAN Fabric in your networks via the above automation systems?



Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

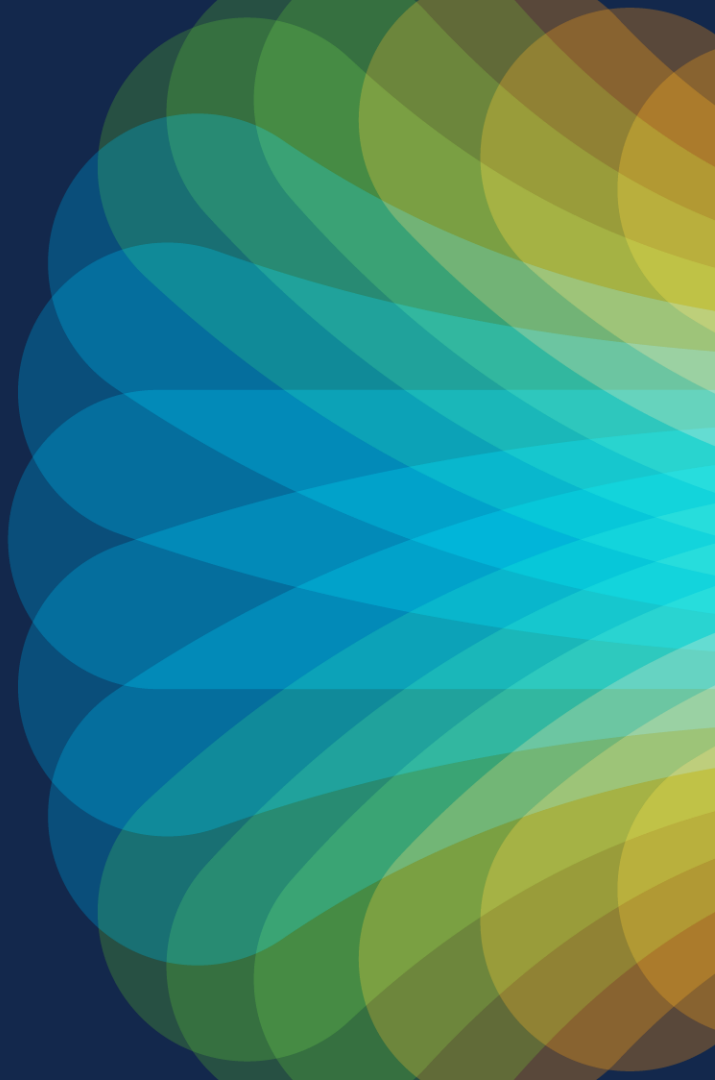
These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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

The bridge to possible

Thank you



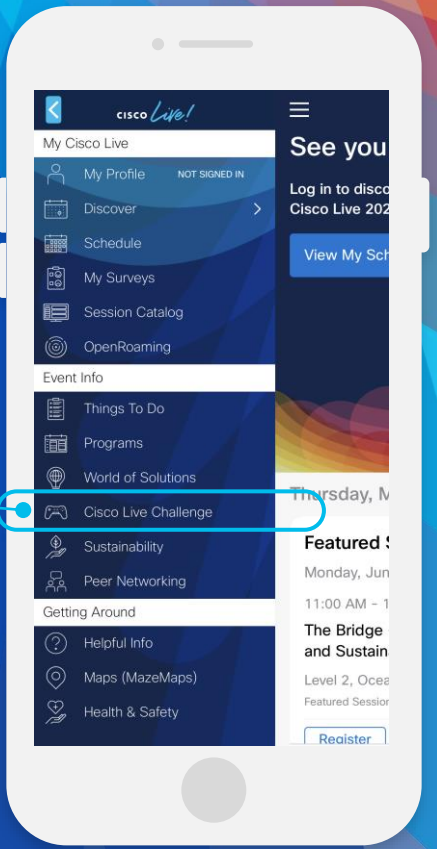
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:




cisco Live!
Let's go
#CiscoLive