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 Webex App

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

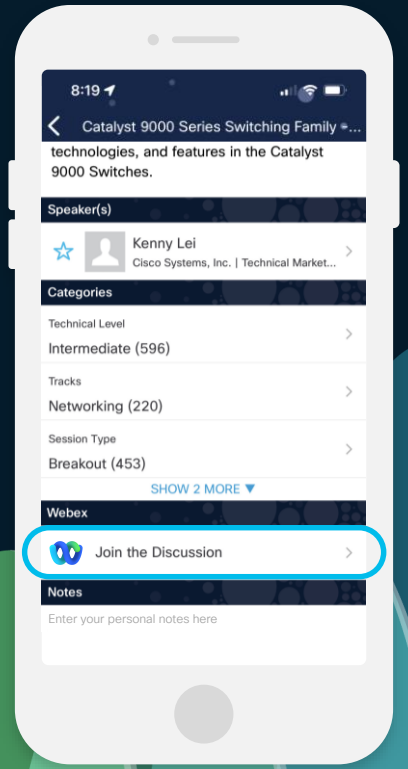
Questions?

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 7, 2024.



Cisco Live US SD-Access/ISE Learning Map

Sunday–2nd

TECENS-2820 9AM
Cisco Software-Defined Access LISP: Architecture Overview

Monday–3rd

BRKENS-2810 8:30AM
Cisco Software-Defined Access LISP Solution Fundamentals

BRKENS-2800 9:30AM
Cisco SD-Access Zero-Touch Provisioning Using LAN Automation

BRKENS-2811 1PM
Connecting Cisco SD-Access LISP to the World: Use Cases and Segmentation

LTRENS-2419 1PM
SD-Access LISP Pub/Sub Wired Lab

BRKENS-2816 3PM
Cisco SD-Access Transit: Advanced Design Principles

BRKSEC-2100 10:30AM
ISE Your Meraki Network with Group Based Adaptive Policy

BRKENS-1802 2:30PM
SD-Access Success Stories: Concept to Reality by Petrobras and Ford Motor

BRKSEC-2091 3PM
Cisco ISE Performance, Scalability and Best Practices

BRKENS-1852 4PM
TrustSec Refresh Reinforced with Latest Segmentation Innovations

Tuesday–4th

BRKENS-2502 10:30AM
Cisco SD-Access LISP VXLAN Fabric Best Practices: Design and Deployment

BRKENS-1801 4PM
SD-Access Success Stories: Concept to Reality by Stanford Health and Yale University

Wednesday–5th

BRKENS-2833 10:30AM
LISP: Optimized Control Plane for Software-Defined Access

BRKENS-2819 2:30PM
Cisco SD-Access and Multi-Domain Segmentation

CIUG-1003 2:30PM
Zero Trust with Software-Defined Access Roadmap Update

BRKENS-2821 4:00PM
Cisco SD-Access LISP VXLAN Fabric for Manufacturing Verticals

Thursday–6th

BRKENS-2827 11:00AM
Cisco SD-Access Migration Tools and Strategies

Catalyst Center

Cisco SD-Access LISP

ISE

Cisco ISE

BU-led sessions

Agenda

Cisco Catalyst Center (formerly Cisco DNA Center)

- 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 LISP Fabric

Industry Leading Campus Architecture

Miercom PERFORMANCE VERIFIED

Deployments

4050+

Momentum

40%

YoY growth in customers

Key use case

70%

Wireless

+ 66%

API (YoY)

Usage

24K+

Sites

1.8M+

Devices

Top verticals: Government, Finance, Professional services, and Manufacturing

Adopted by 31% of U.S. **Fortune 100** Companies

EMEA: 52%

Americas 29%

APJC 20%

Modern, Open and Scalable Fabrics

IETF Standard based Protocols

Cisco Catalyst Center

Cisco SD-Access

LISP VXLAN Fabric*

Cisco Catalyst 9000

BGP EVPN VXLAN Fabric

IETF

IETF

Enterprise | Healthcare | Education | Financial | Public Sector | Manufacturing | Hospitality | Media | Transportation | Retail

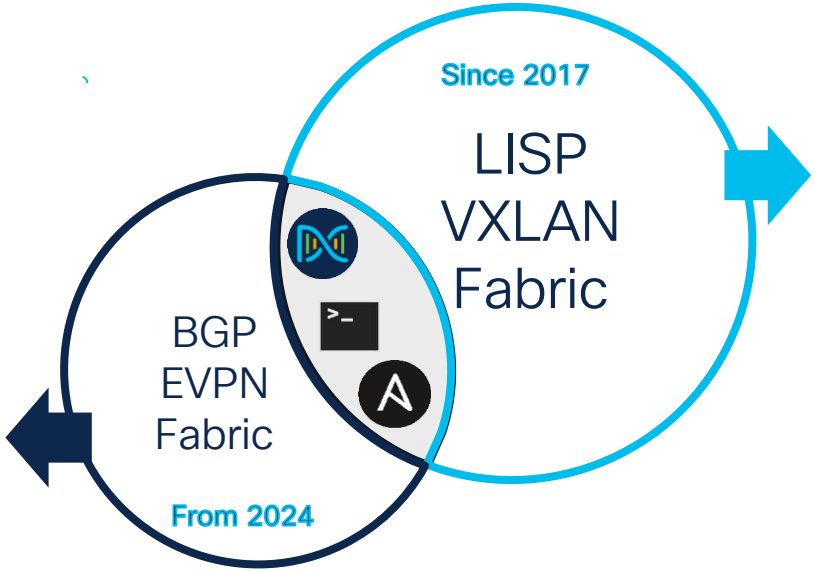
*Cisco's Lead Motion

Effortlessly Deploy Your Fabric of Choice

LISP Fabric is the leading choice for Enterprise customers!

EFT Ongoing

- Extend fabric across DC & Campus
- Multi-vendor deployment
- Wireless over the top
- Network segmentation



- **Simple**: Standards-based, Campus optimized BU recommended Control Plane
- **Efficient**: Lightweight, unparalleled scale & high performance due to rapid convergence time
- **Extensible**: Highly extensible to drive innovation (PubSub, Multi-site, Extranet)
- **Robust**: Integrated wireless w/ L2 mobility support campus wide

What is new and upcoming?

ISSU Support (9400) | API Automation

One Infrastructure | Single Data Plane | Consistent Zero-Trust Experience

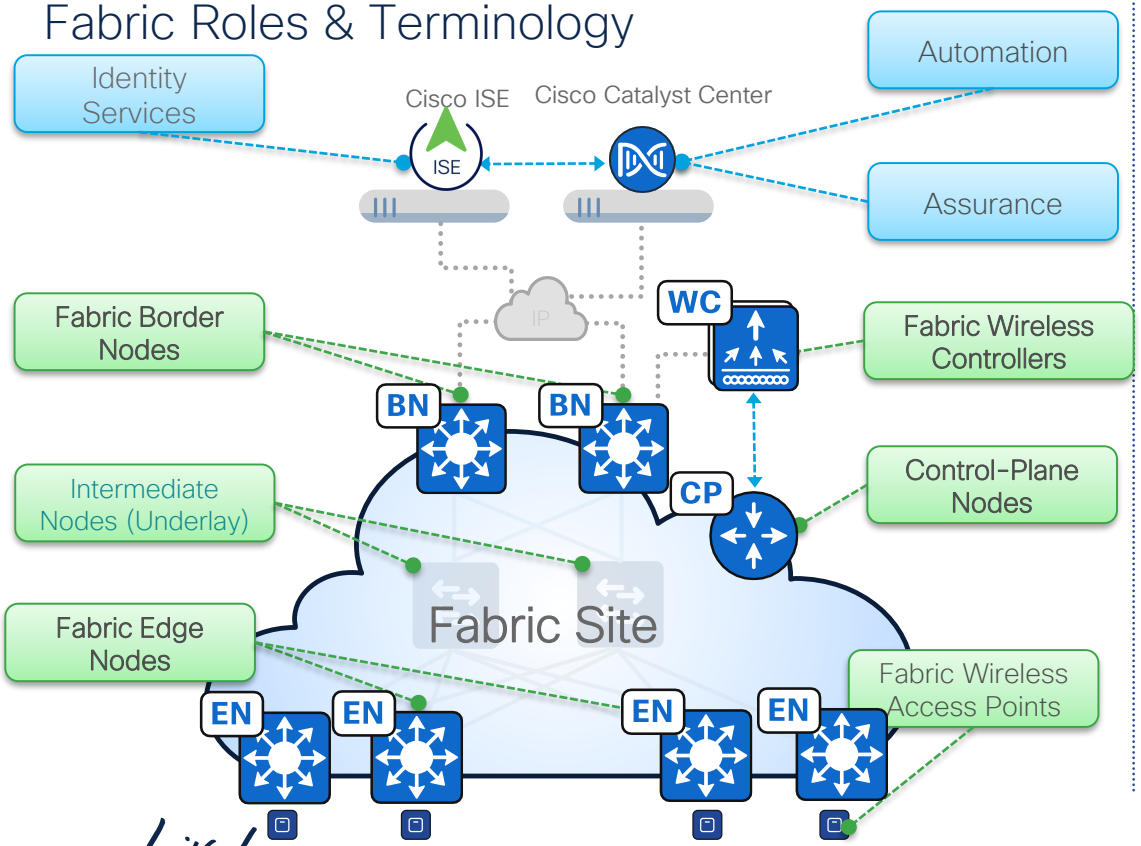
Cisco SD-Access Customer Success

	Healthcare	Education + Energy		Manufacturing
	Stanford HEALTH CARE	Yale	BR PETROBRAS	Ford
	Register - BRKENS-1801		On-Demand - BRKENS-1802	
SCALE	6200 devices 10K+endpoints	6500 devices 66K+endpoints	5300 devices 57K+endpoints	4500 devices 10K+endpoints
REQUIREMENTS	Zero-Trust Access Endpoint Profiling	API Tooling Resilient Network & Security Visibility		Secure, Highly Available network Hi Performance Scalable Wi-Fi

For your reference

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

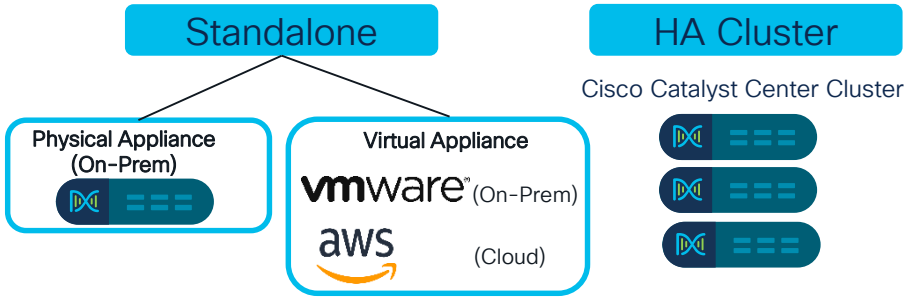
Cisco SD-Access

Cisco Catalyst Center Deployment

- **Deployment Types**
  - Standalone
    - On-Prem Physical Appliance
    - NEW Virtual Appliance on Cloud(AWS)
    - NEW On-Prem Virtual Appliance on ESXI(VMWare)
  - Cluster for High Availability (HA)

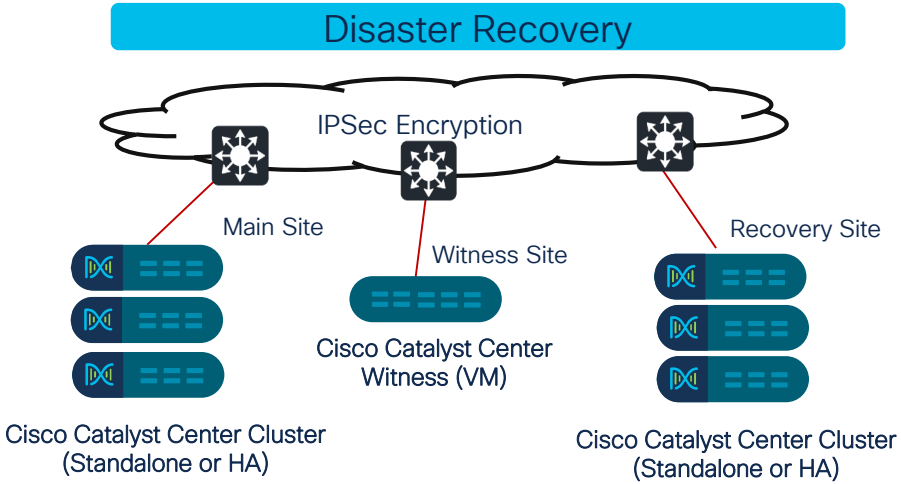
    Cluster interconnected with 10Gbps interface with <10msec latency
  - Disaster Recovery (DR) for network downtime

    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

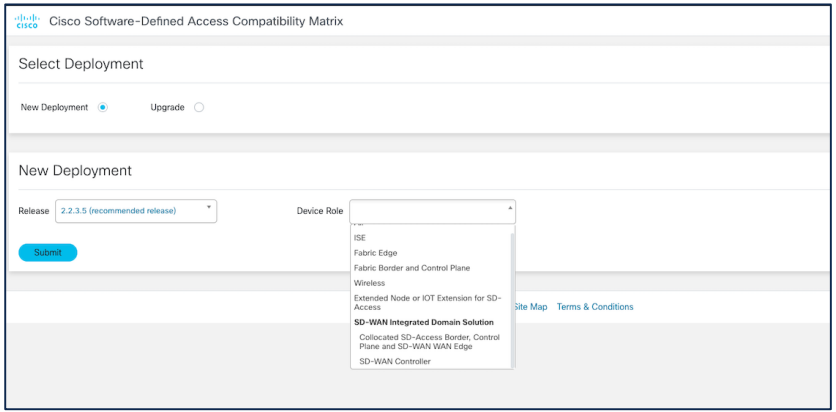


For your reference

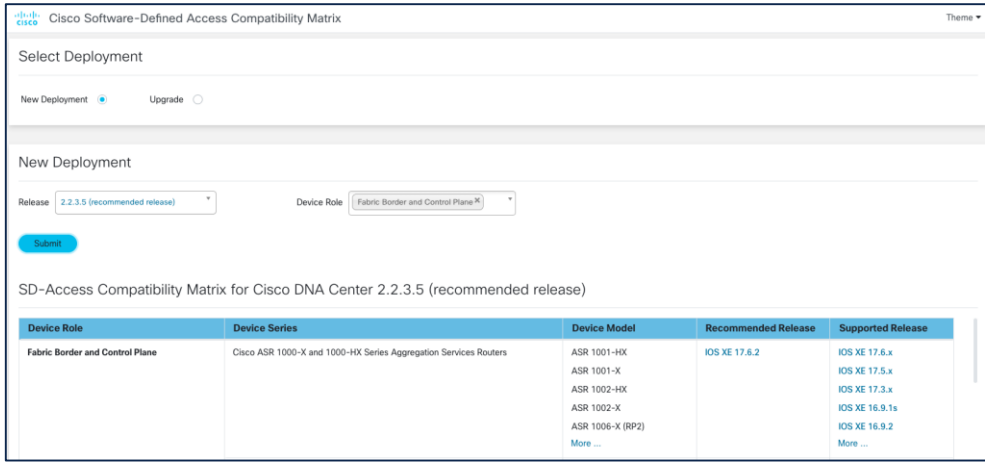
SD-Access Platform Support

- 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/Catalyst Center 2.3.5 Data Sheet]

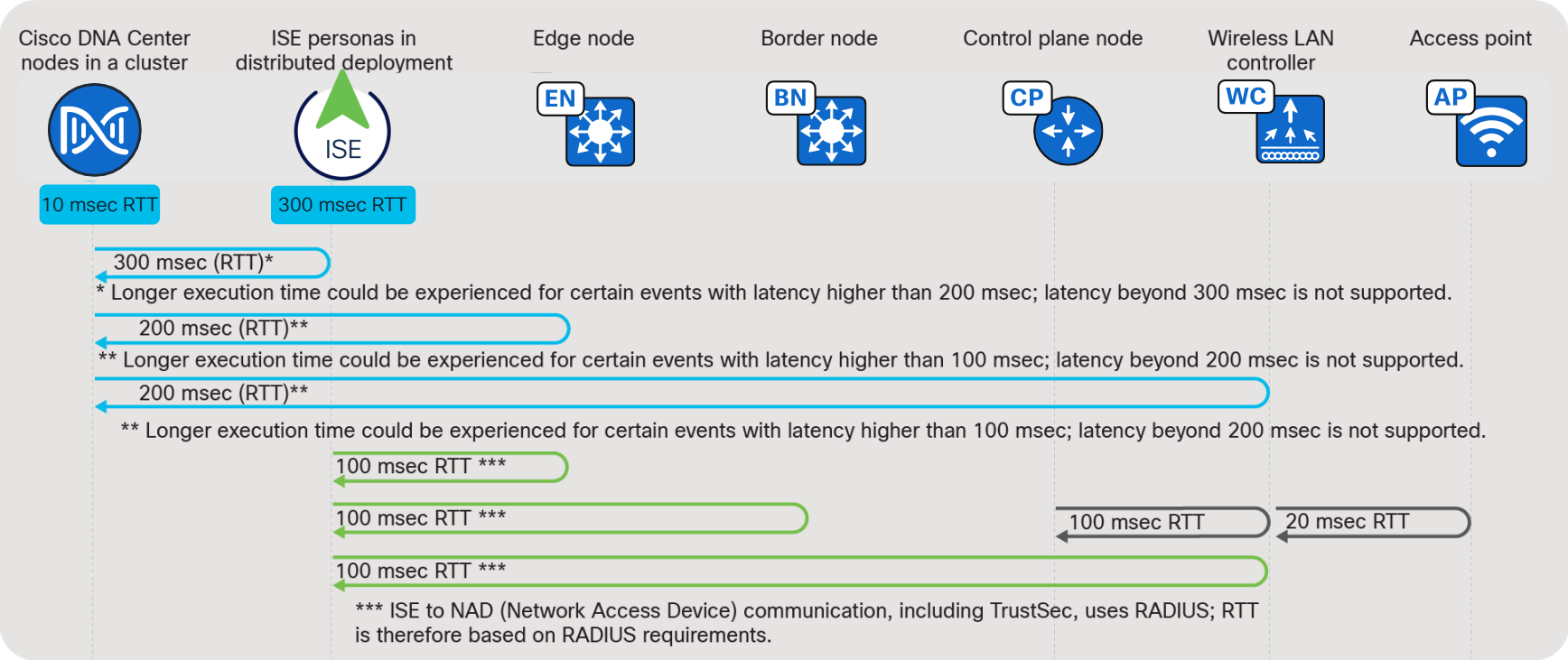
Cisco Catalyst Center Fabric Readiness and Compliance Checks

- Hardware Version
- Image Type
- Software Version
- Software Licenses
- Loopback 0

Software Licensing

- Network Advantage & DNA Advantage/Cisco DNA Premier License

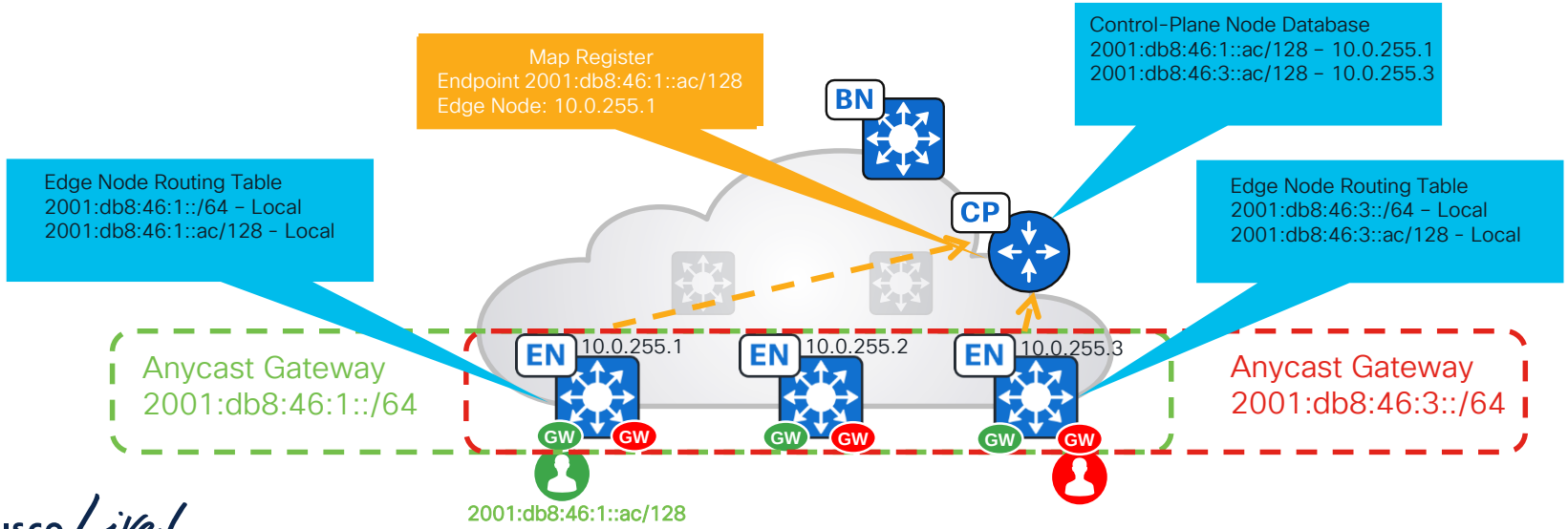
Cisco SD-Access
Latency Requirements



As of
Catalyst Center: 2.3.7.0
Cisco ISE: 3.2

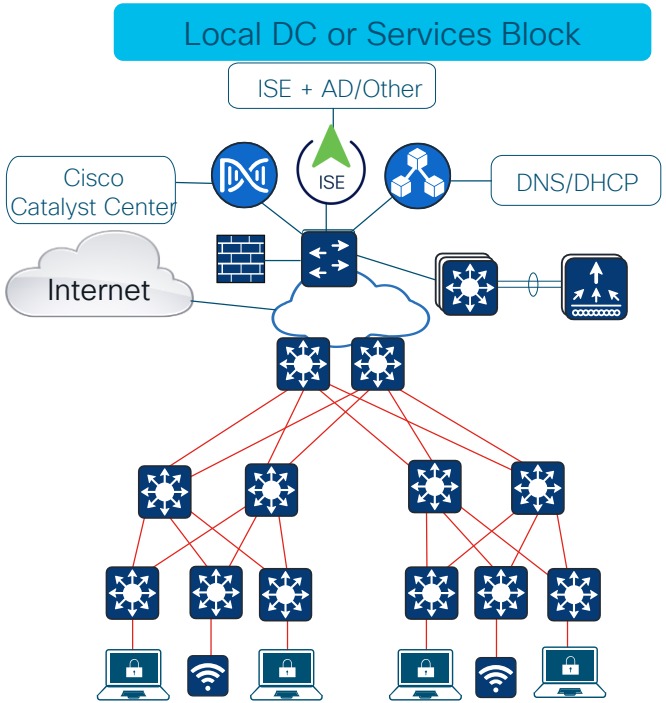
V4 and V6 support in SD-Access

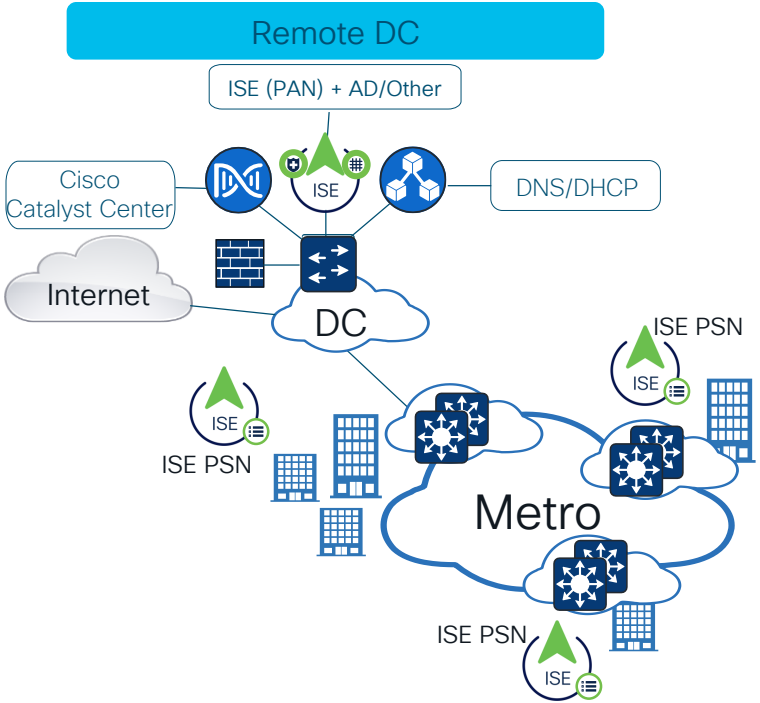
Cisco Catalyst Center Physical Interfaces	: V4 / V6
Cisco Catalyst devices	: V4 / V6 / Dual-Stack
Cisco SD-Access Underlay Devices	: V4 only
Cisco SD-Access Overlay Clients	: V4 / Dual-Stack
Cisco ISE	: V4 / V6 / Dual-Stack
Cisco Catalyst Center to Cisco ISE	: V4 only



Cisco SD-Access Architecture

Where do I place Critical/Shared Services





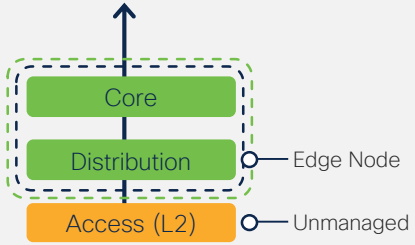
Cisco Catalyst Center Security Best Practices Guide

SD-Access Flexible Deployment Options

Migration Options

Macro segmentation
Micro segmentation

Fabric with unmanaged Layer 2 switched access*

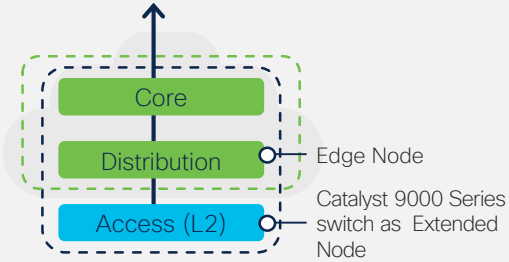


Use case: Keep your existing unmanaged switches

- Segmentation starts at distribution layer
- Integrated wired and wireless

Benefit: Allow tenants to bring their own network.

Fabric with managed Layer 2 switched access



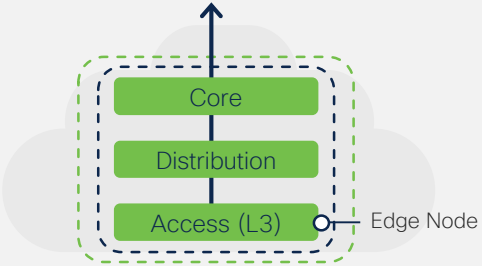
Use case: Retain Layer 2 access

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

Benefit: Security and automation at every layer

Fabric with Layer 3 routed access

The Gold Standard



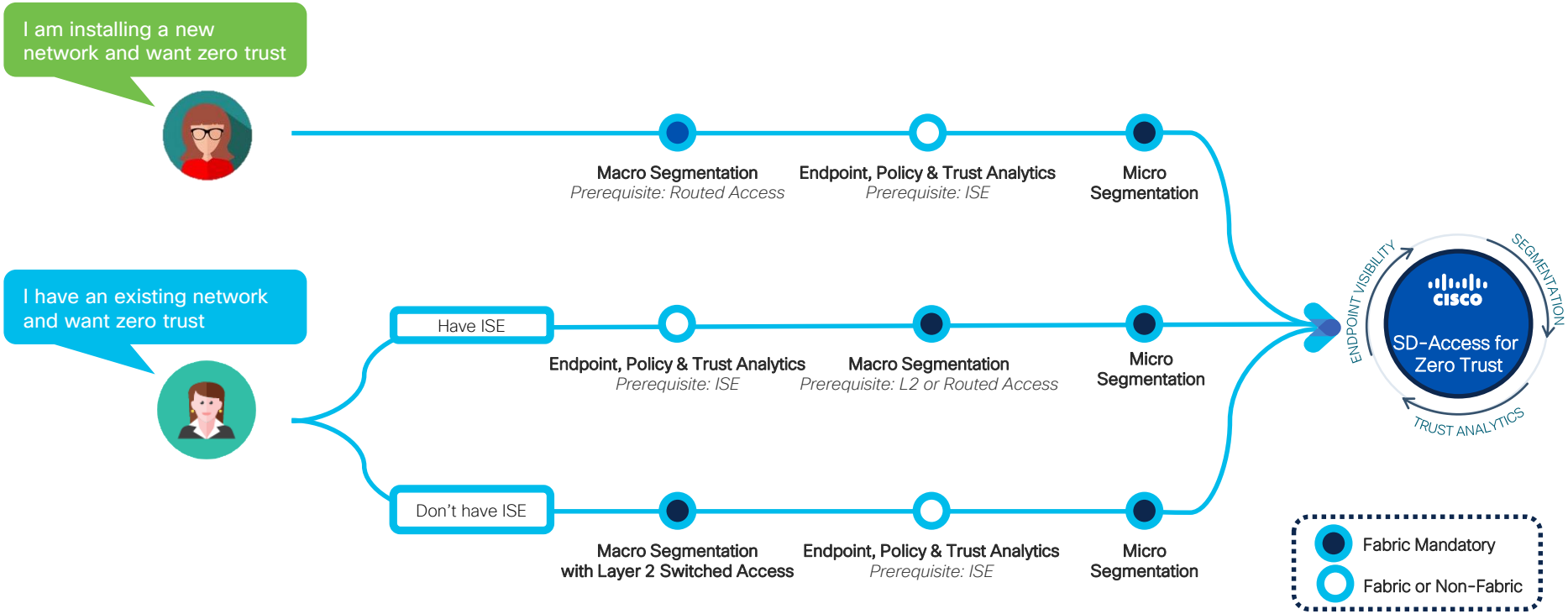
Use case: Full SD-Access

- 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

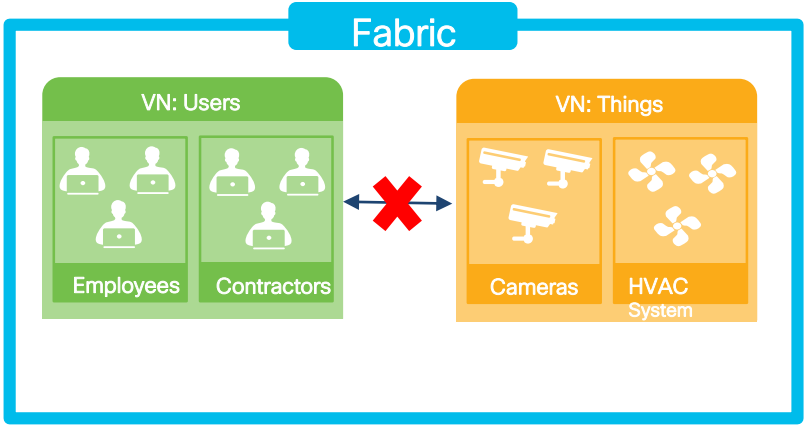
SD-Access Flexible Deployment Options



Cisco SD-Access Policy

Segmentation Strategy

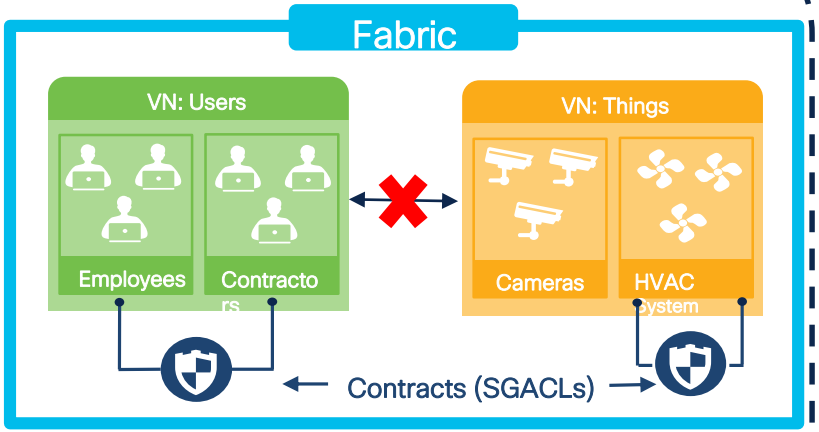
Macro Segmentation



Virtual Network (VN)

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

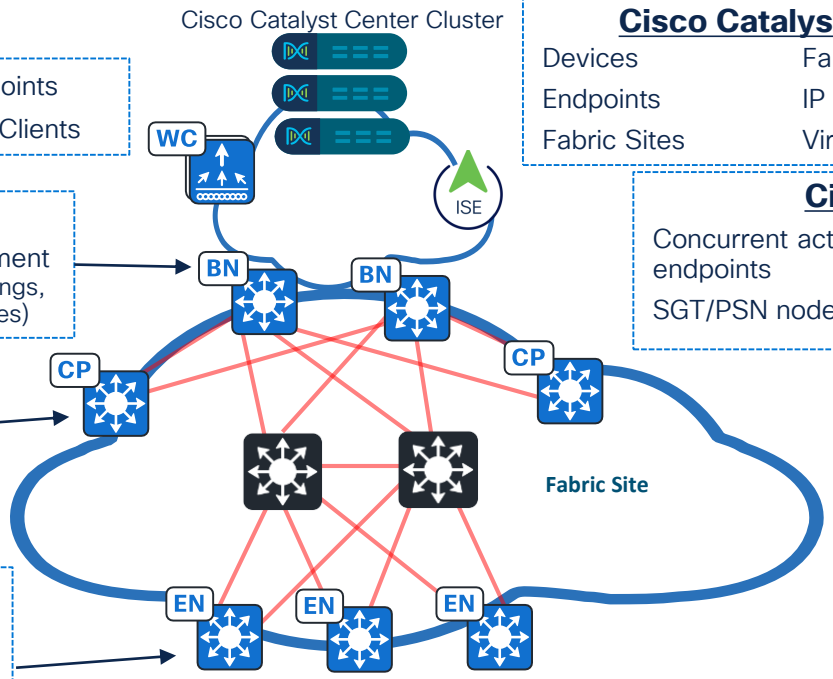
Micro Segmentation



Security Group Tag (SGT)

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

Cisco SD-Access Scale & Readiness



Cisco Catalyst Center

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

Cisco ISE

Concurrent active endpoints	SGACL
	SXP peering
SGT/PSN node	

Access Points
Wireless Clients

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

Virtual Networks
Fabric Host Entries

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

Consider Individual Platform Scale and Performance

Least Common Denominator (LCD) across the solution elements

Cisco Catalyst Center

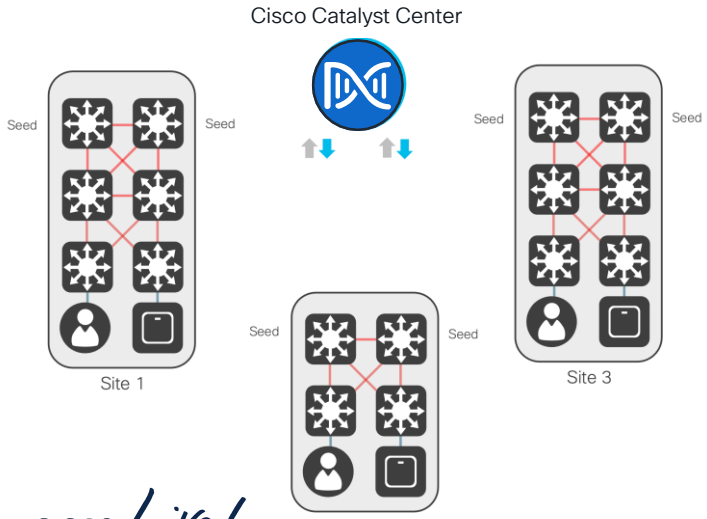
Device Onboarding options

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.
Underlay multicast to optimize overlay subnet multicast/broadcast distribution



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

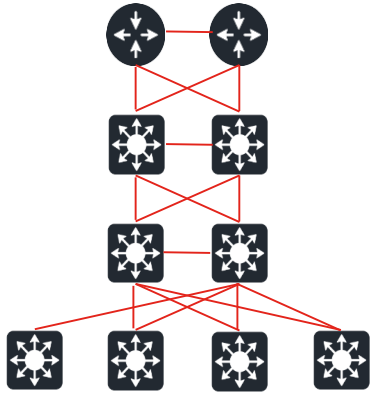
LAN Automation Enhancements 2.3.7.0

- 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

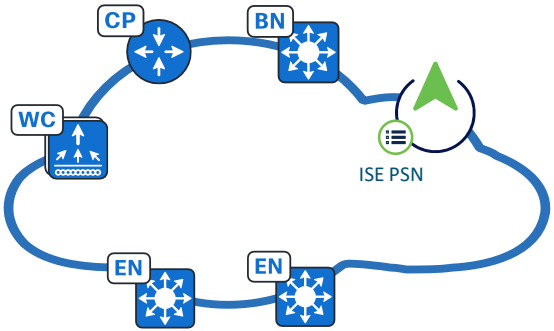
- **Routed Access Network**
- Manual Underlay: Any routing protocol
- Resilient and Redundant fast-converged connectivity with **ECMP, BFD enabled.**
- Loopback 0 with /32 host prefix.
- **Higher MTU(Jumbo) to accommodate VXLAN encapsulation**
  - Else use TCP-Adjust MSS



Site/Building

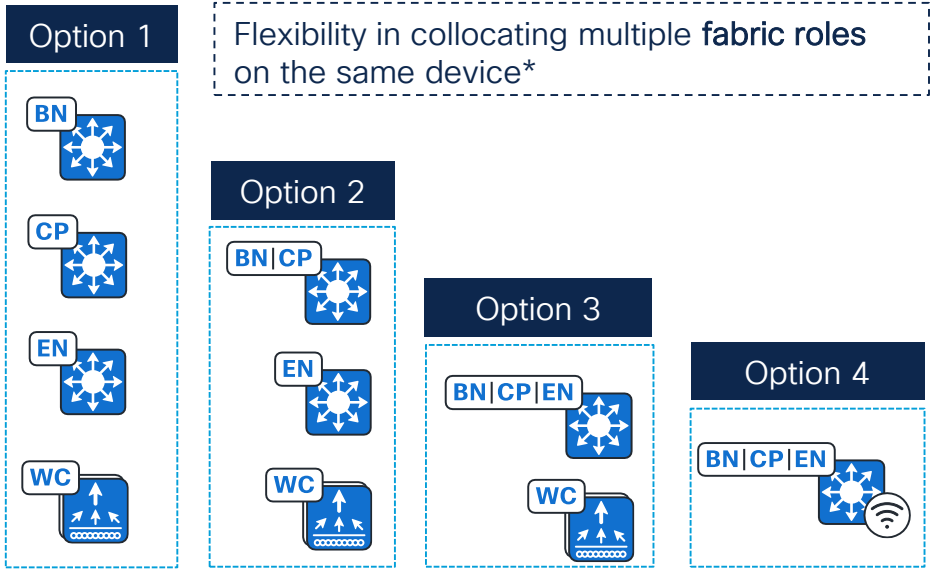
Cisco SD-Access Fabric Site Design Options

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



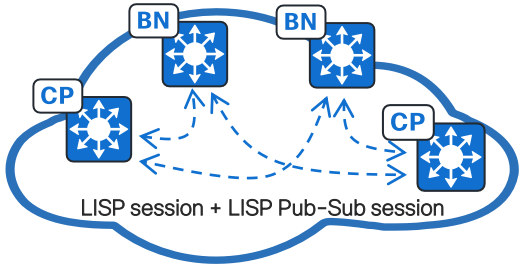
Flexibility in collocating multiple **fabric roles** on the same device*

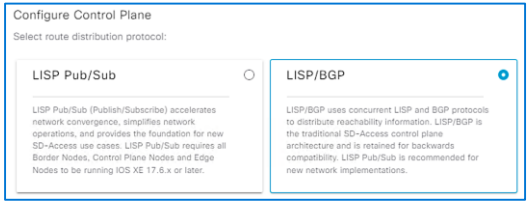
* Refer to Cisco SD-Access compatibility matrix for latest information

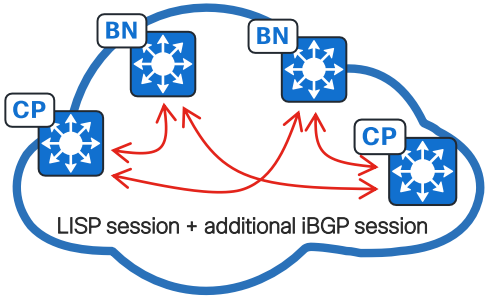
Starting
Catalyst Center: 2.2.3.x
IOS-XE: ≥ 17.6.2

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

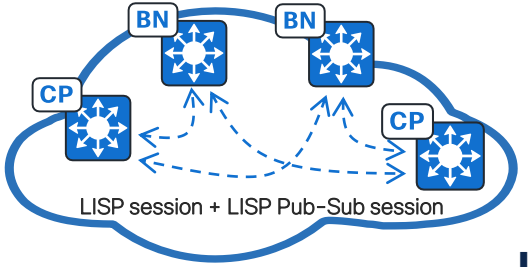
LISP / BGP

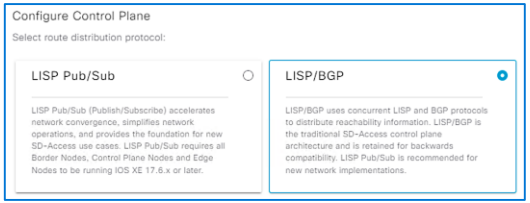
- iBGP session between B – CP and B – TCP node to share prefixes.
- Convergence overhead with additional protocol, redistribution and additional lookups
- Troubleshooting complexity with 2 Control-plane protocols
- Only supported Architecture with SD-WAN Integrated solution
- Only 2 TCP Node support

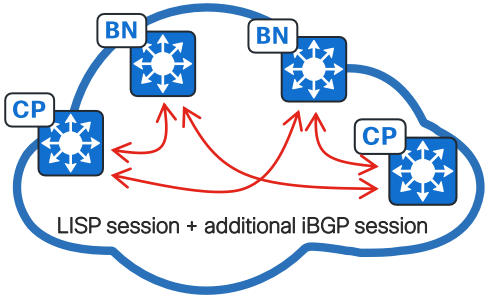
Starting
Catalyst Center: 2.2.3.x
IOS-XE: ≥ 17.6.2

Cisco SD-Access Provision

Fabric Control Plane enhancements Cont'd







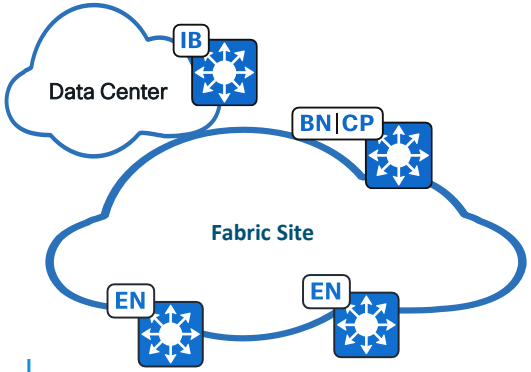
LISP Pub/Sub Benefits

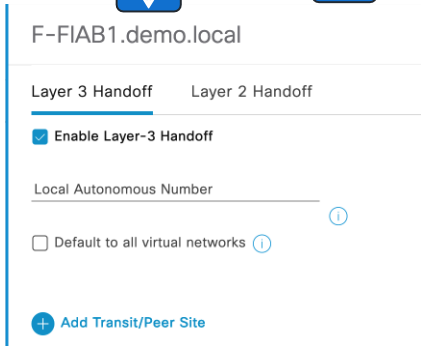
- Remove dependency on BGP
- Simplified Border Routing Designs
- Faster Border Convergence due to faster mapping change updates
- Traffic Path Optimization with Dynamic Default Border
- Backup Internet Option
- Automated route leaking using LISP Extranet

Cisco SD-Access Fabric Site Design Options

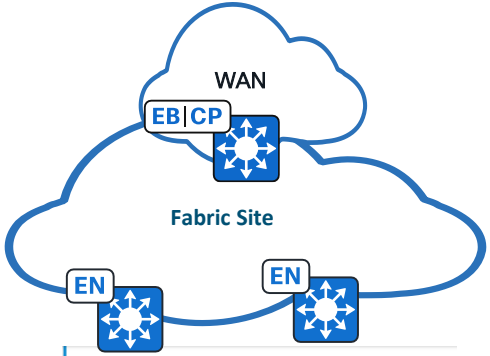
Border Node Selection

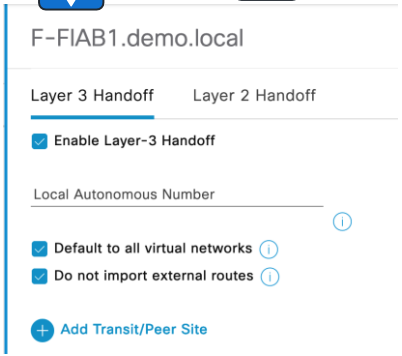
Internal Border (N) (Rest of Company)



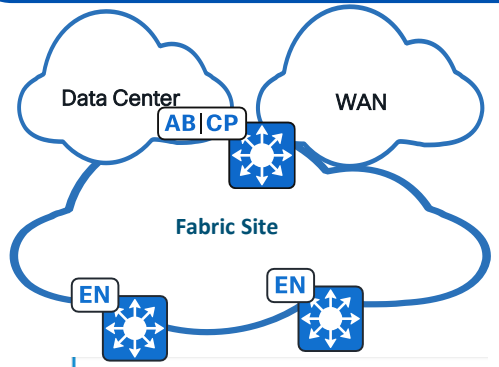


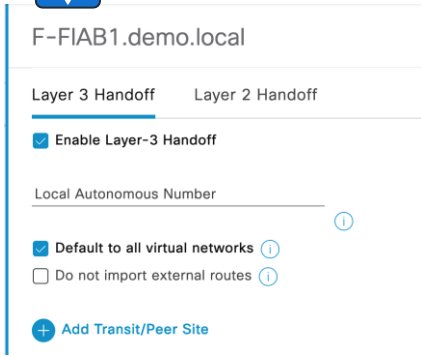
External Border (4 Max) (Outside)





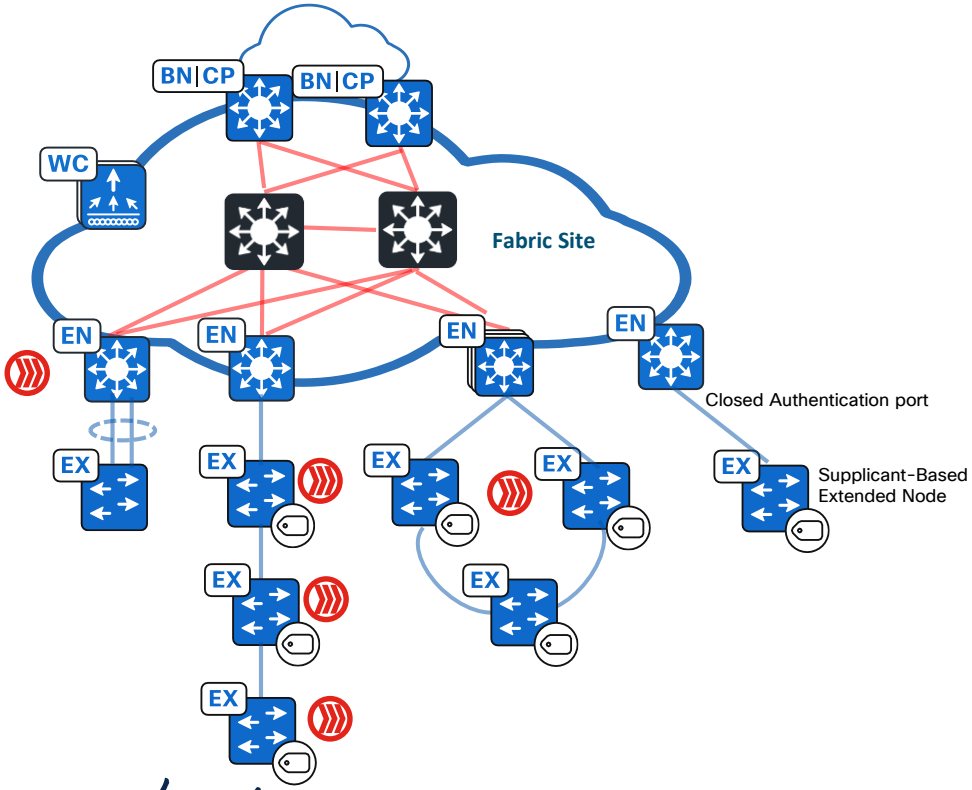
Internal + External Border (4 Max) (Anywhere)





Solutions to OT Challenges

Environmental and Connectivity



Two Types

- Extended Node(EX)
- Policy Extended Node(PEN)
- Supplicant-based Extended Node(SBEN)

Supported devices

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

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

SBEN Node
- C9200
- C9300
- C9400
- C9500

Supported Topologies

- Daisy Chain(Like device type)**
  - Max of 18 IE switches
  - Max of 3 Cat9k switches
- Ring(Like device type)
  - Max of 18 IE switches

Enforcement

*- Excluding C9600
** EX and PEN Only

Starting Catalyst Center release : 2.2.3.x

SD-Access Fabric Zones

Use Case

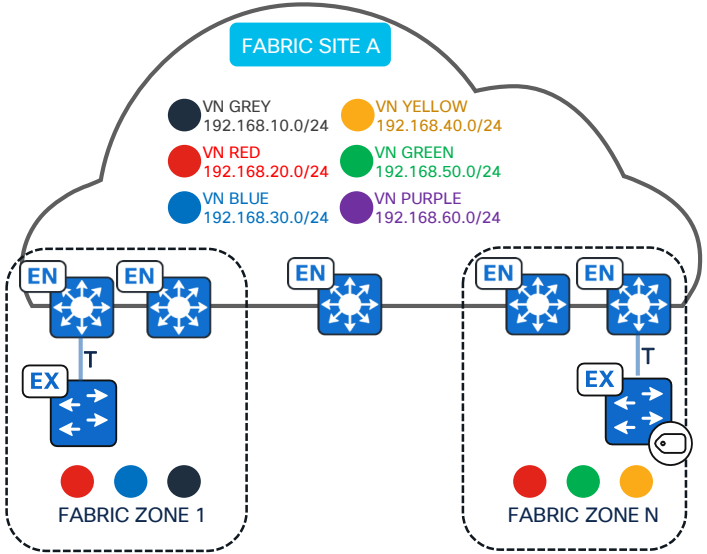
- Before 2.2.3.x, the provisioning scope of an IP Pool was the whole fabric site. For security and/or better fabric site scaling, some customers require granular control of IP Pool provisioning scope.

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

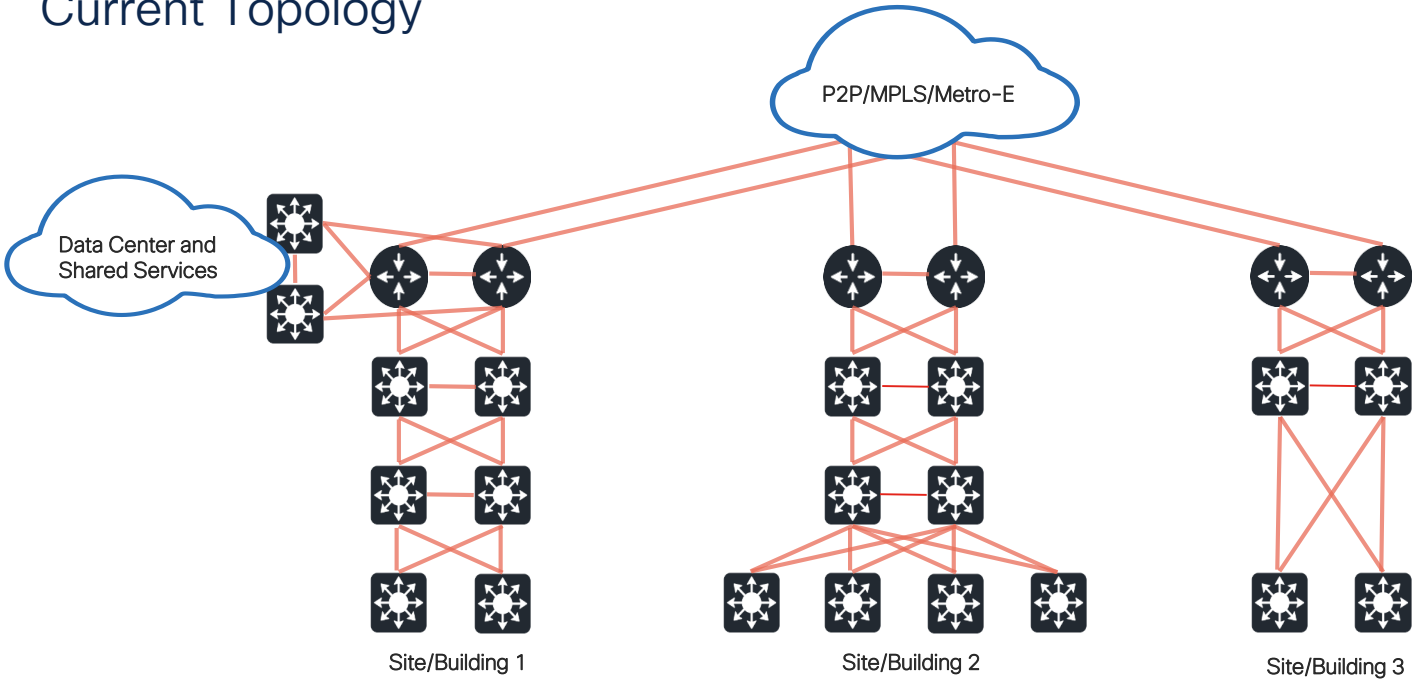
- L3VNs and IP Pools must be assigned to the parent fabric site before assigning to one or more Fabric Zone.
- Only edge nodes (EN, EX, PEN) can be provisioned to a Fabric Zone. Collocated fabric roles (e.g., EN+B, EN + Embedded WLC, etc.) cannot be provisioned to a Fabric Zone.
- EX/PEN must be in same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



SD-Access Single-Site Design Options

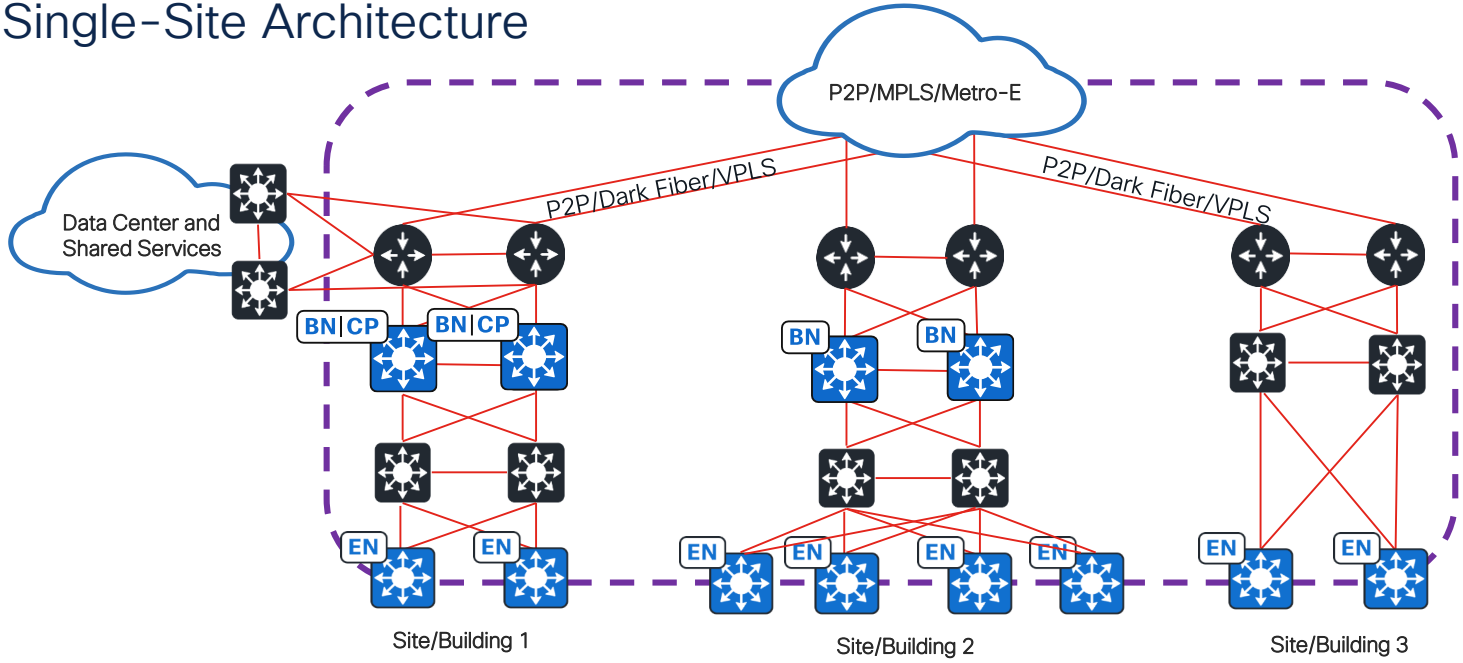
Cisco SD-Access Architecture

Current Topology



Cisco SD-Access Architecture

Single-Site Architecture

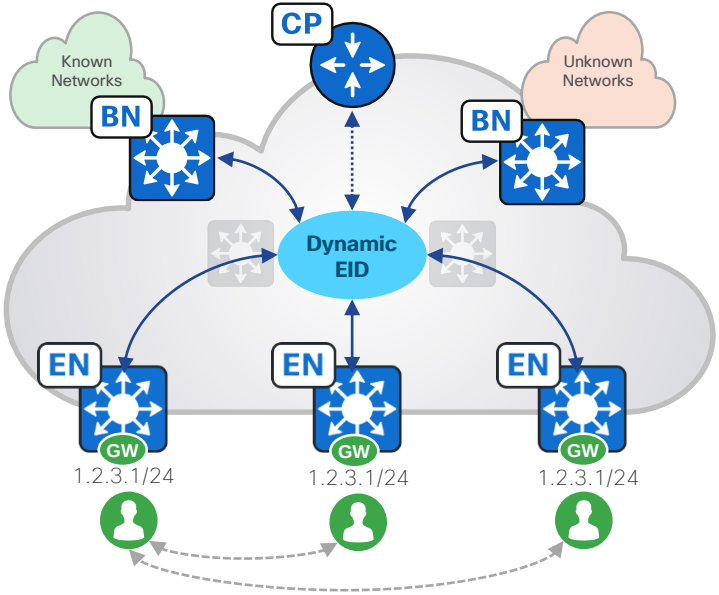


Challenges with Single Site Architecture

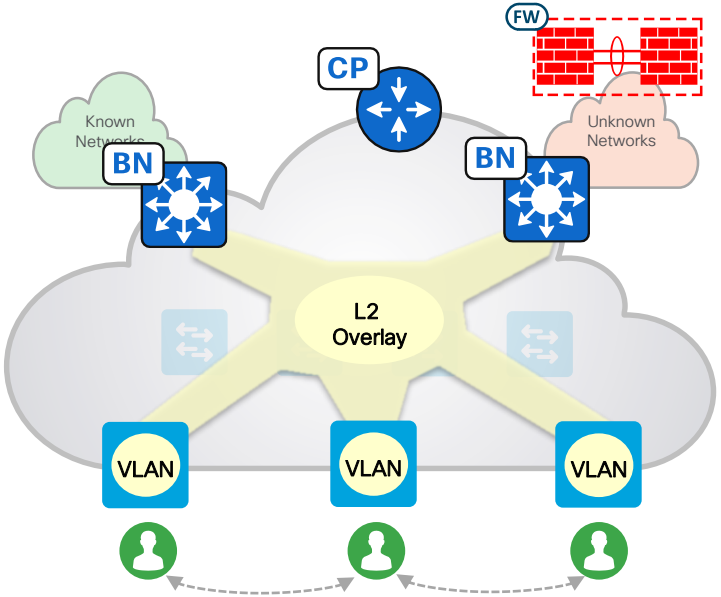
- One Subnet available across all buildings/Sites
- One Big Failure Domain
- Scale Limitations – IP Pools supported per site or Border/Control plane Scale

SD-Access Fabric
L3/L2 Overlays

Layer 3 Overlay
Stretched Subnets



Layer 2 Overlay / Vlan based L2 VNI

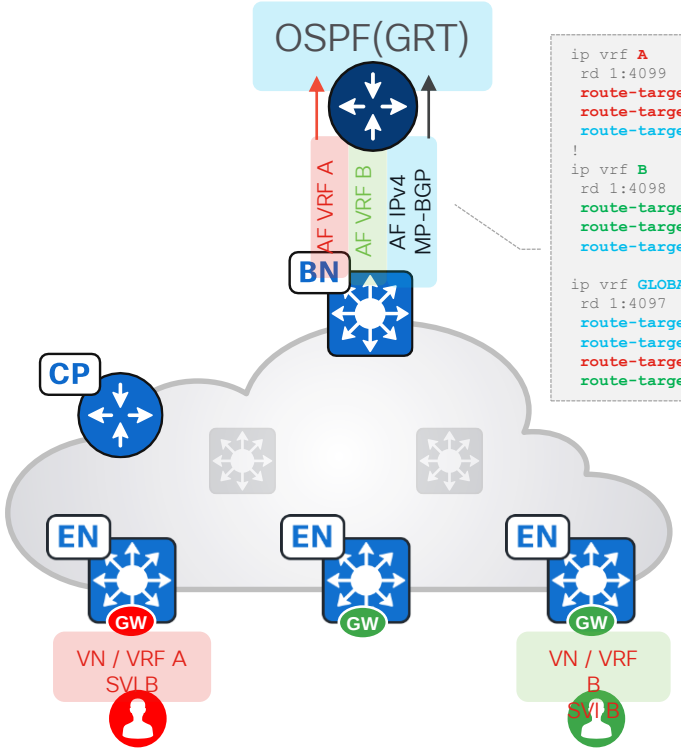


Starting Catalyst Center release: 2.3.4.0

SD-Access Fabric

Border Handoff with Route Leaking

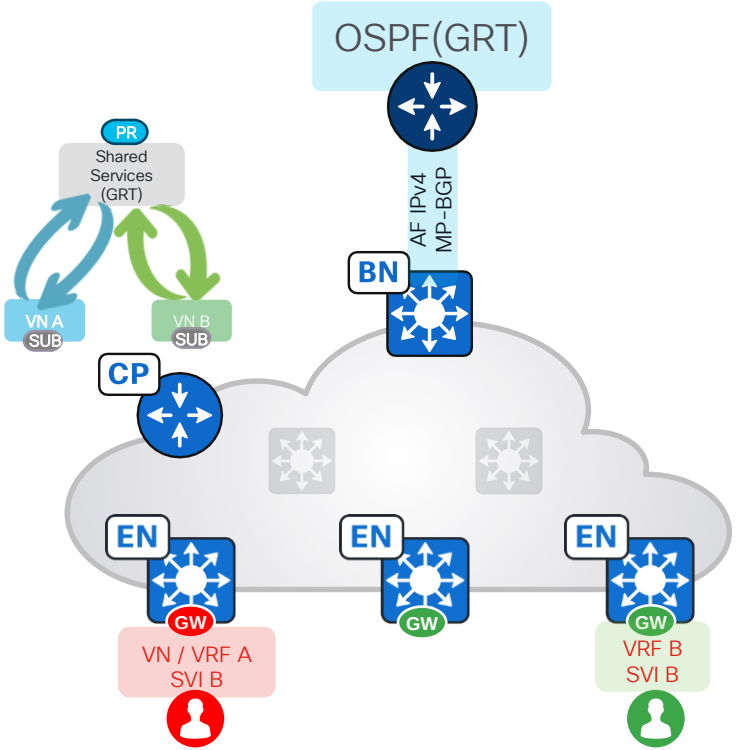
Traditional Route Leaking




```
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



Starting Cisco Catalyst Center release 2.3.5.0

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 Catalyst 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

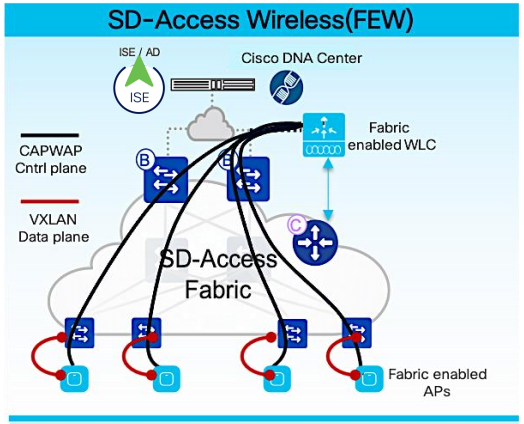
Cisco SD-Access Multicast

Fabric Multicast Deployment Modes

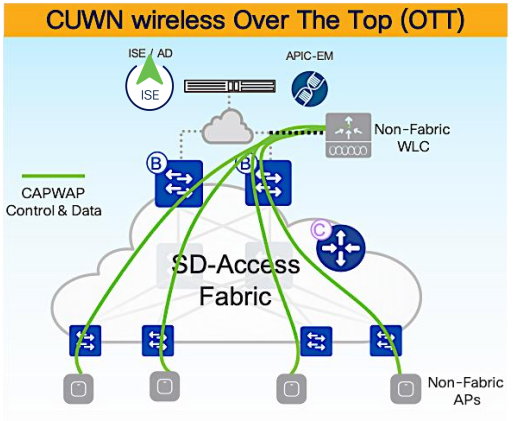
Head-End Replication	Native Multicast
No Underlay Multicast	Underlay Multicast required
Preferred for lesser Edge nodes in FS	Preferred option for Large number of Edge nodes in FS
Replication Load on Head-End device	Reduces replication Load at the Head-End
V4 and V6 support	No V6 support

Cisco SD-Access Wireless

Deployment types	: FEW , OTT , Mixed Mode
Supported Platforms	: C9800, eWLC,3504,5520,8540
AP Mode	: Local, Flex*
Control-Plane Node support	: 1 Pair (2 CP)(AireOS) , 16 Pairs(32 CP)(C9800)**



- CAPWAP Control Plane, VXLAN Data plane
- All integrated in Fabric, SD-Access advantages
- Optimized for 802.11ac Wave 2 and 11ax APs



- CAPWAP for Control Plane and Data Plane
- SDA Fabric is just a transport

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

Starting Catalyst Center release 2.1.2.0

SD-Access Wireless Design Best Practices

SD-Access Wireless – N+1 HA vs SSO

Redundancy Comparison

Stateless Redundancy with N+1 HA

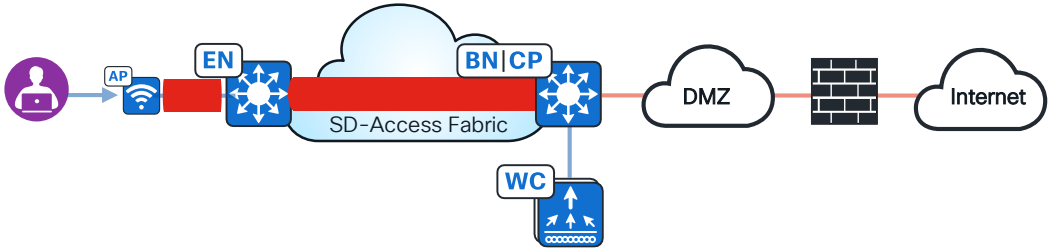
- WLCs remain independent of each other. Cisco Catalyst Center and SD-Access fabric sees them as two separate WLCs.
- For each location there is a primary and a secondary WLC.
- Both WLCs communicate with the control plane nodes.
- In a failover event, the CAPWAP tunnel is broken between AP and Primary 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

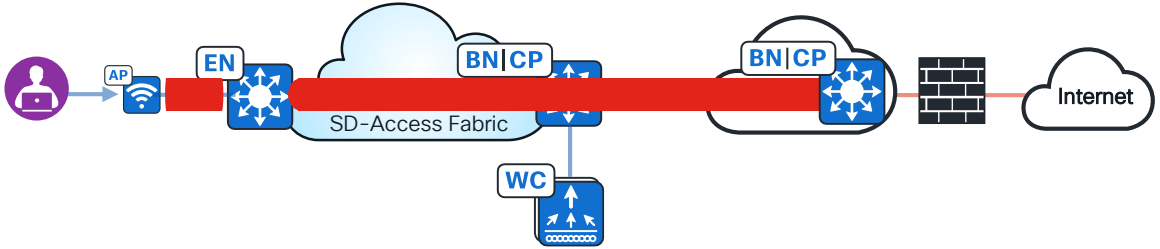
- WLC SSO is seen as a single entity.
- Only active WLC communicates with the control plane nodes.
- APs and clients stay connected during a failover event.
- In a failover event, the new Active WLC will bulk update the control plane node regarding the wireless hosts.
- For Embedded Wireless on Catalyst 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 Guest VN



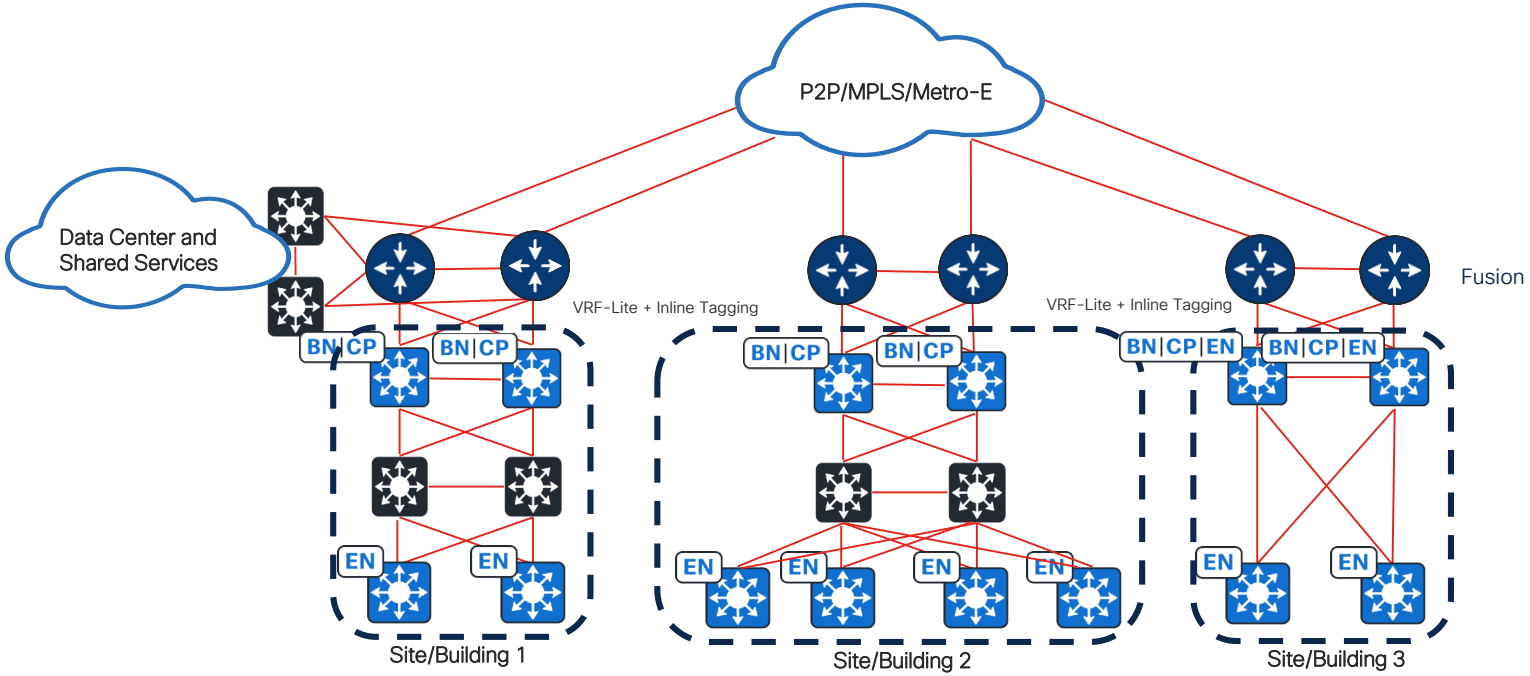
Dedicated Guest VN with MSRB



SD-Access Multi-Site Design/Transit Options

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

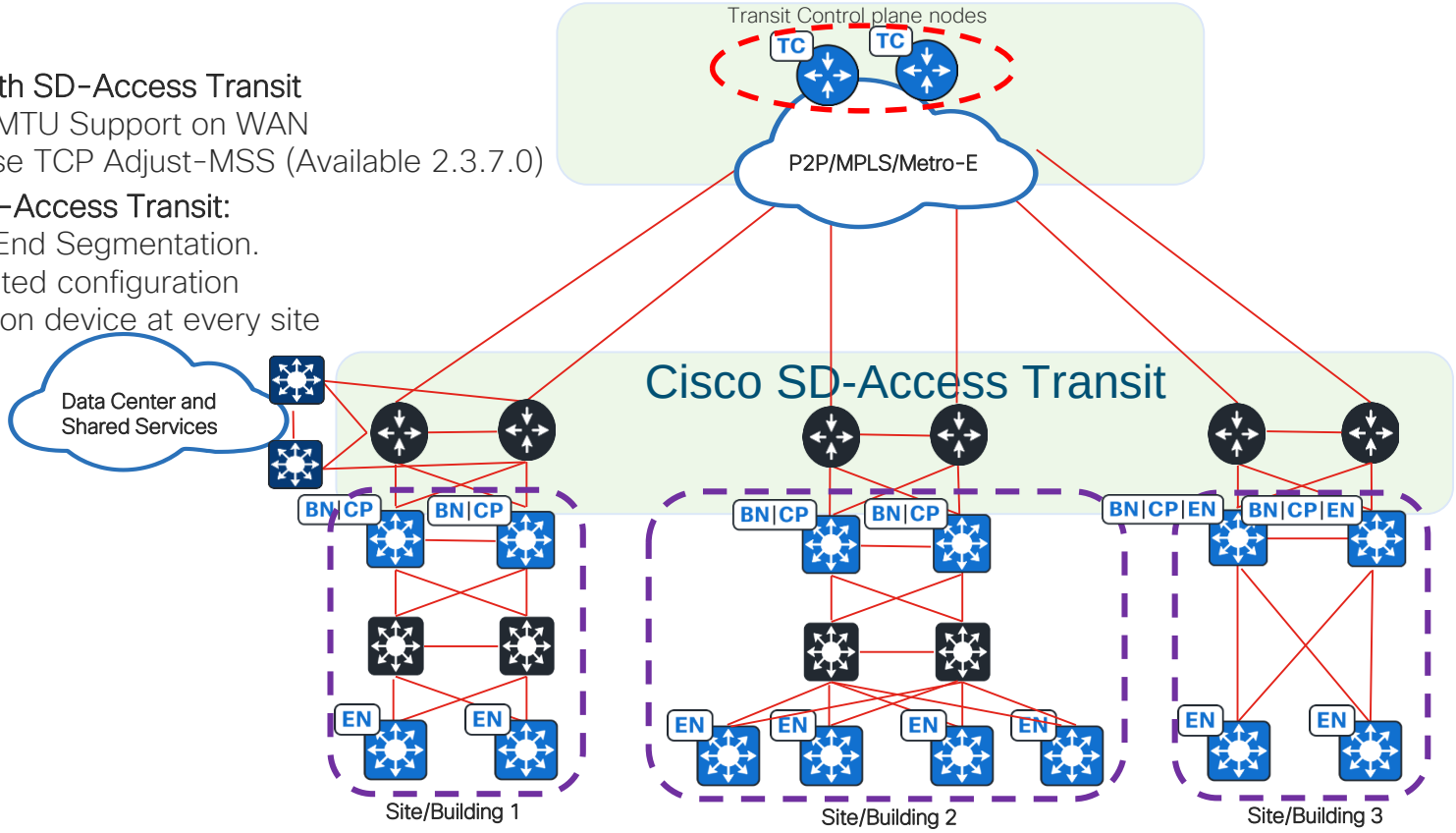
Multisite Architecture with SD-Access Transit

Pre-Requisite with SD-Access Transit

- Higher MTU Support on WAN
- *Else use TCP Adjust-MSS (Available 2.3.7.0)

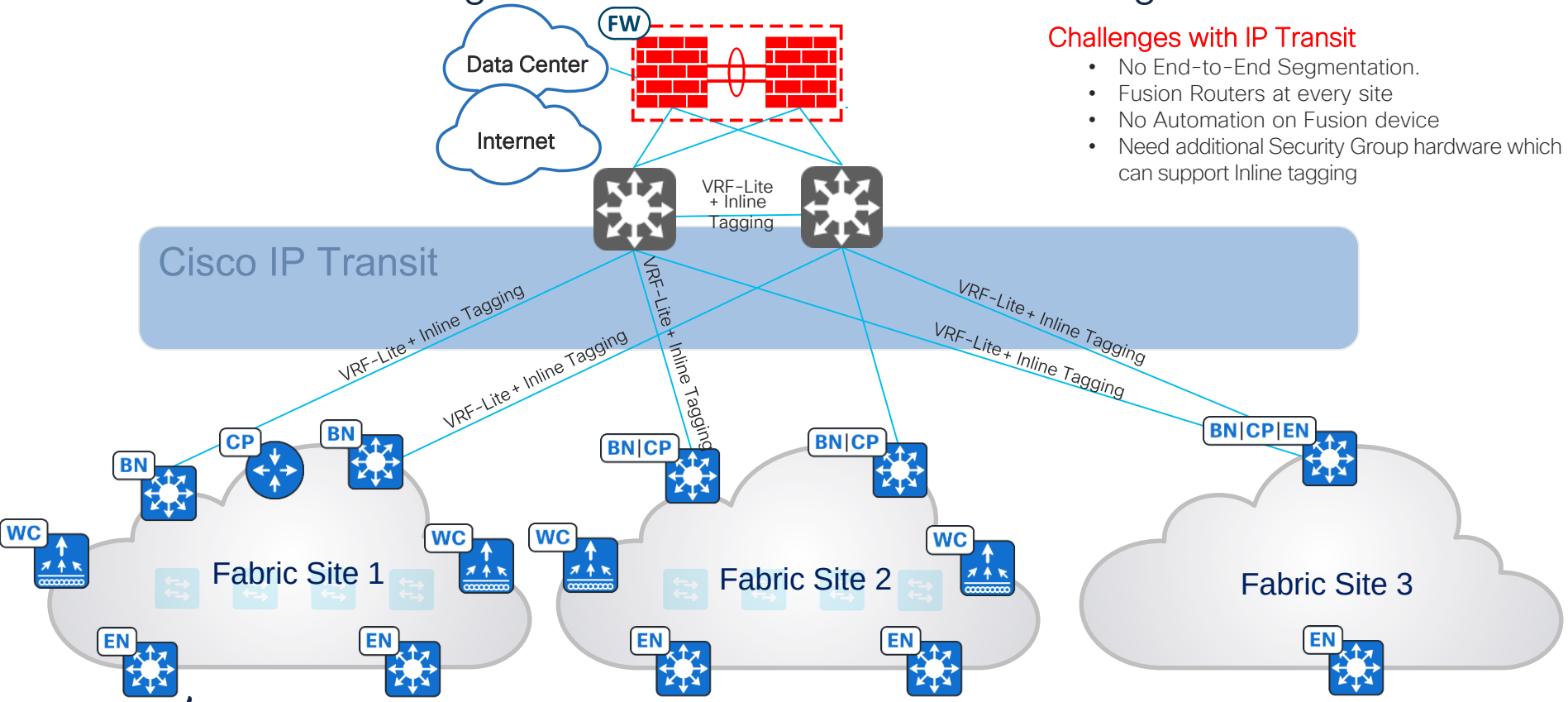
Benefits with SD-Access Transit:

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



Cisco SD-Access Multi-site

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

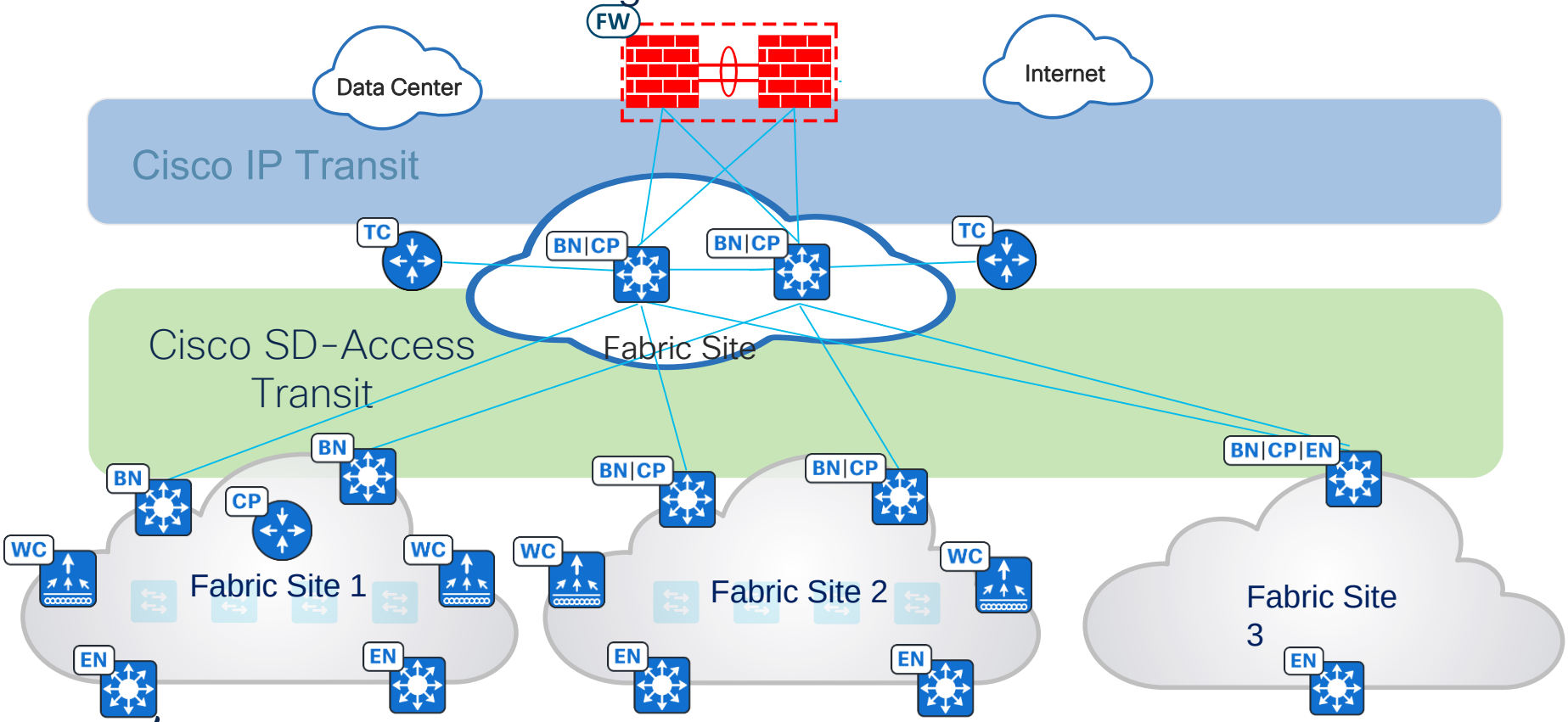


Challenges with IP Transit

- No End-to-End Segmentation.
- Fusion Routers at every site
- No Automation on Fusion device
- Need additional Security Group hardware which can support Inline tagging

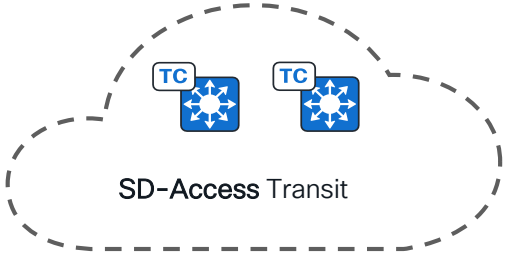
Cisco SD-Access Multi-site

Cisco SD-Access Transit Design 1



Cisco SD-Access Deployment

Multisite Deployment with SD-Access Transit



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

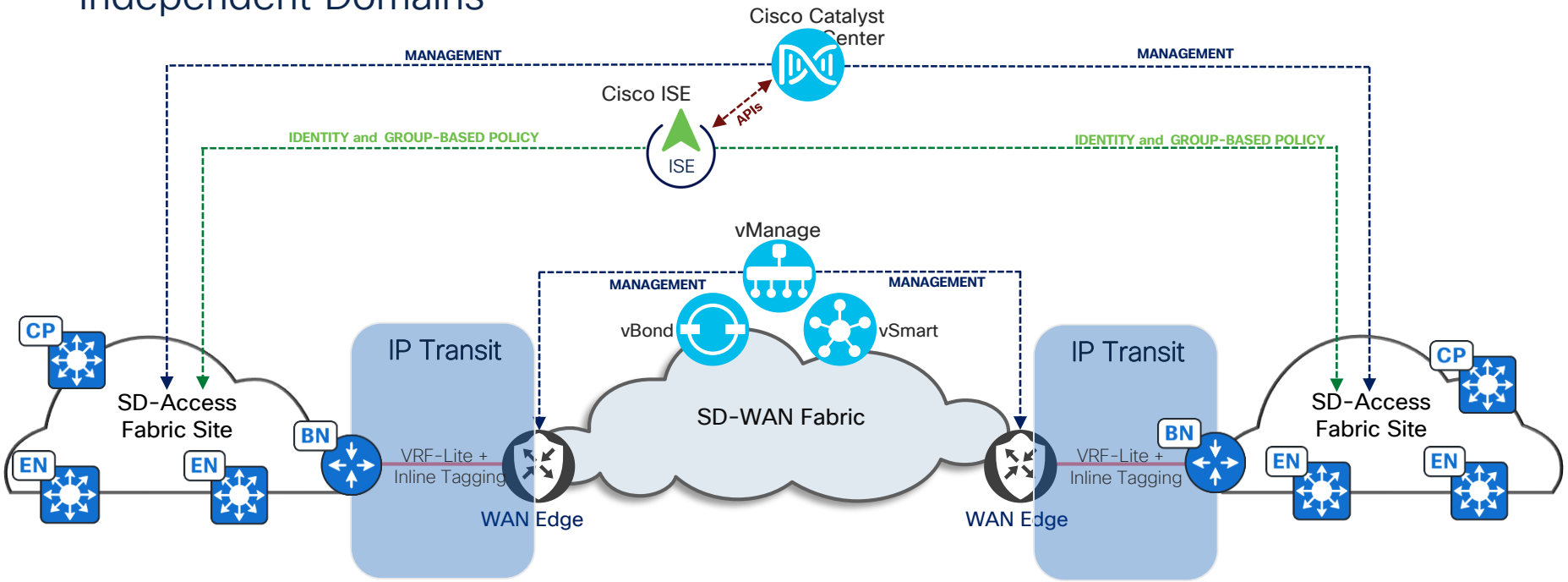
Key Considerations:

- 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

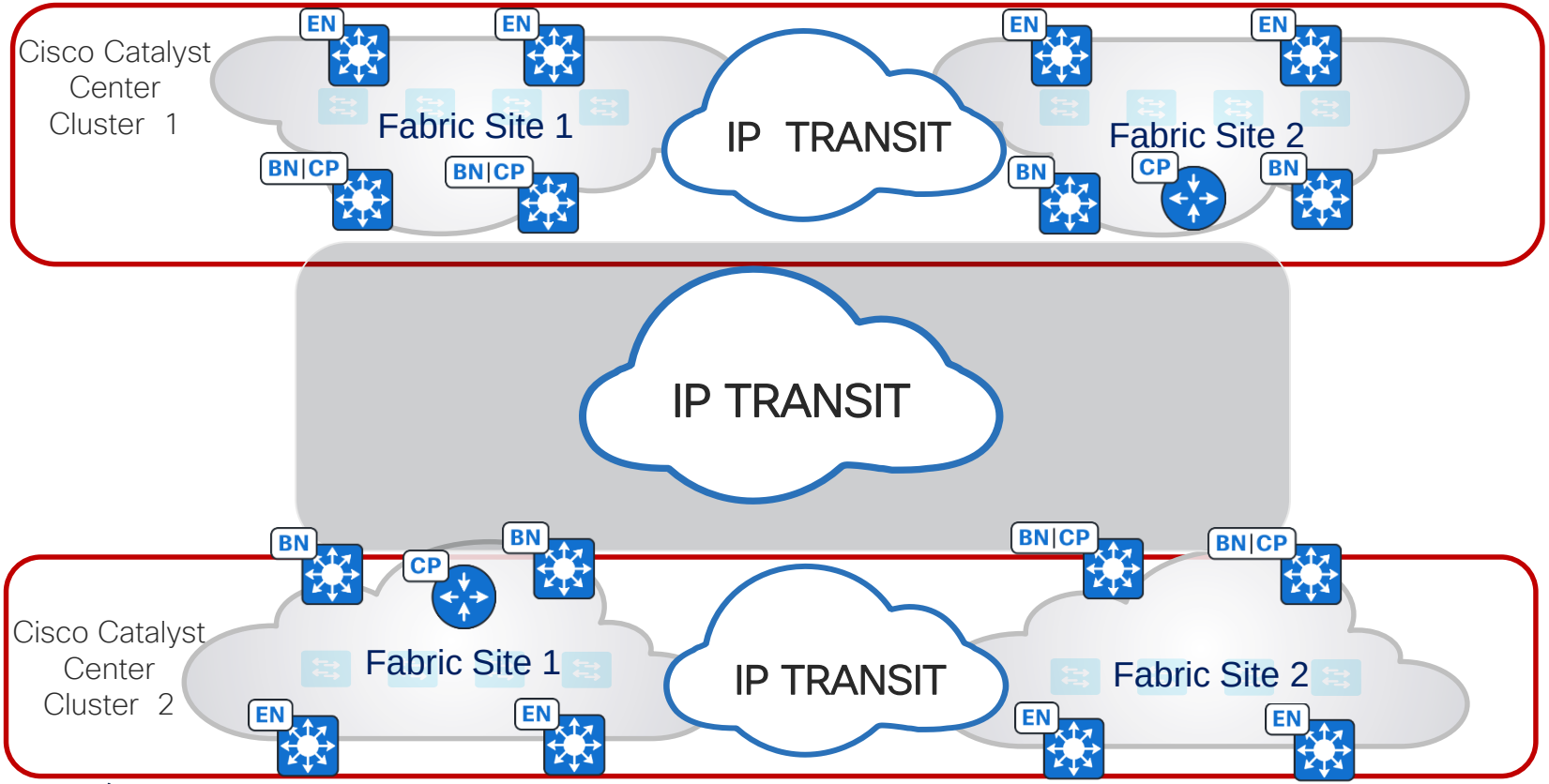
Independent Domains



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

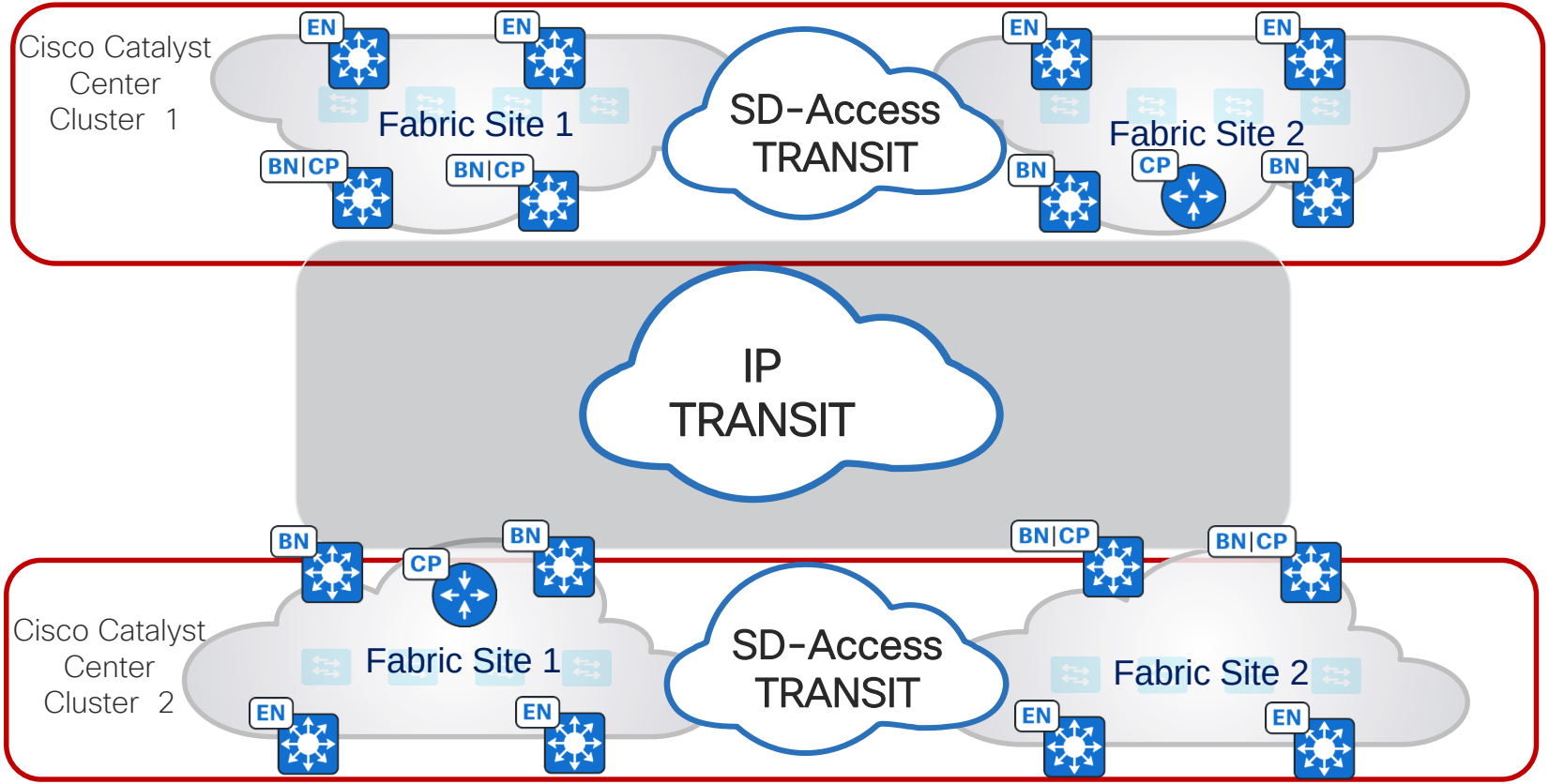
Cisco SD-Access Multi-site

Transit Design across Cisco Catalyst Center Clusters



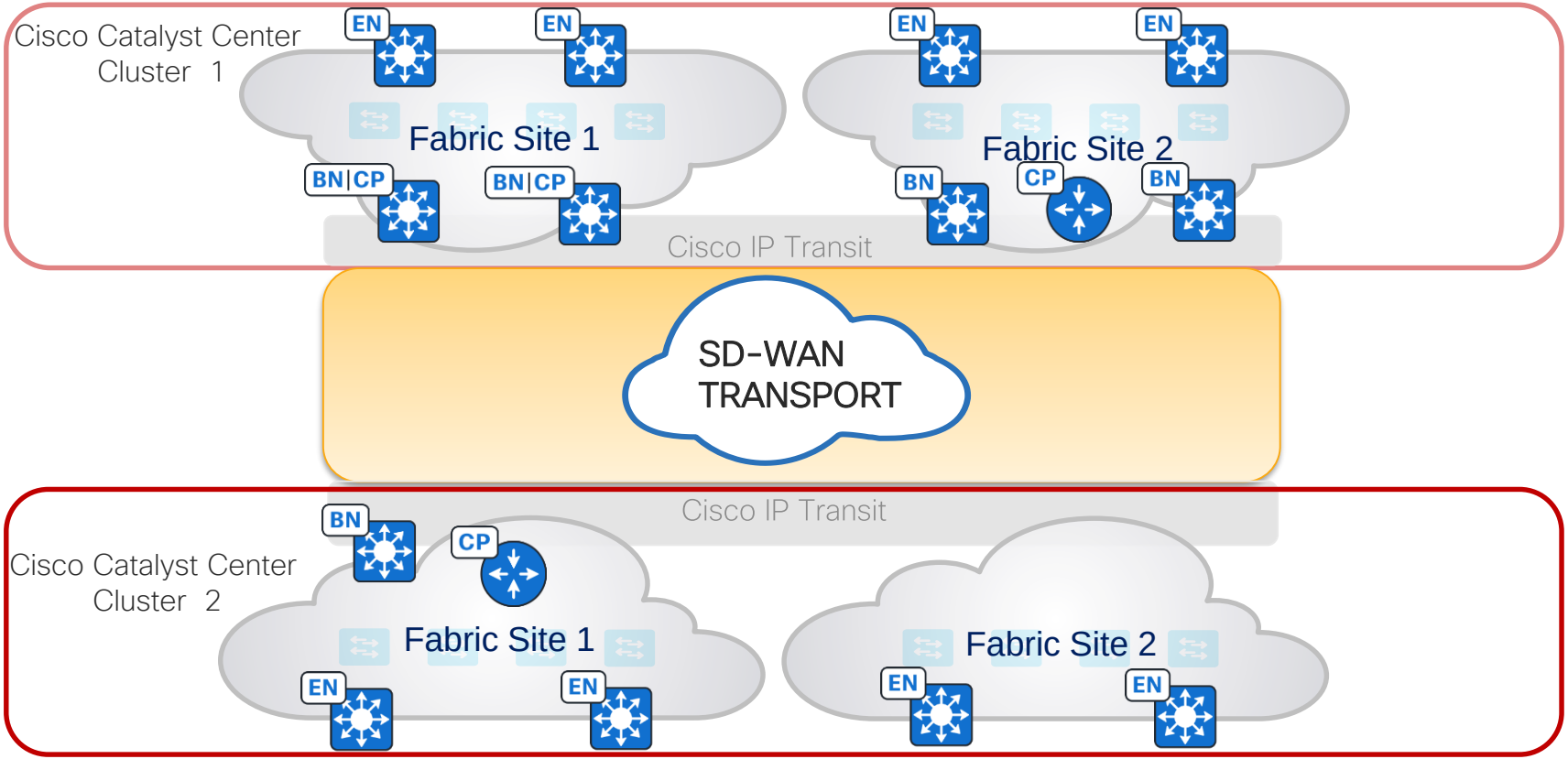
Cisco SD-Access Multi-site

Transit Design across Cisco Catalyst Center Clusters



Cisco SD-Access Multi-site

Transit Design across Cisco Catalyst Center Clusters



SD-Access Policy Design Options

Cisco Catalyst Center Provision
Authentication Template

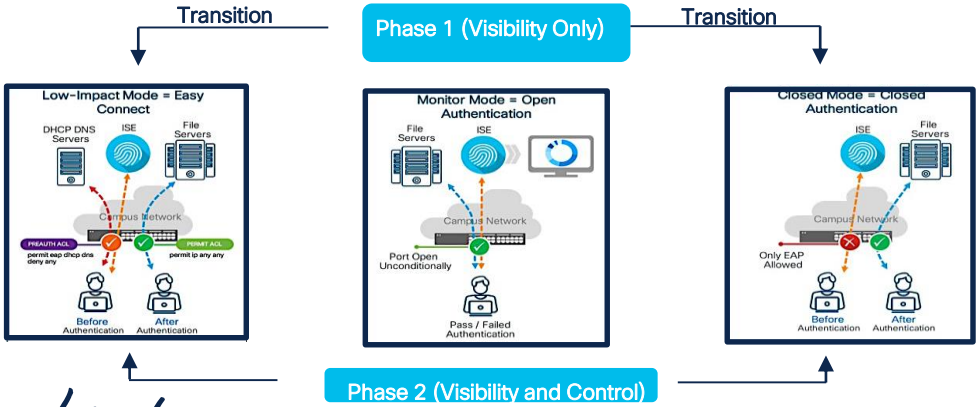
https://172.23.112.31/dna/design/authTemplate

Cisco DNA Center — Design · Authentication Template

Last updated: 4:28 PM — Refresh

Filter — Find

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



Cisco Catalyst Center Policy

Manage Group-Based Access Control policy

Cisco DNA Center

Overview / Configurations

Policy Settings

Analytics Settings

Policy Settings

Administration Mode

Manage Group-Based Access Control in

- (●) **Cisco DNA Center, policy UI in Cisco Identity Services Engine will be read-only**

  For emergent cases, such as Cisco DNA Center not responding, you can override the read-only mode in Cisco Identity Services Engine Security Group settings so that you can make policy changes directly in Cisco Identity Services Engine. Be cautious that this will casue both sides out of sync. A full re-sync might be necessary after recovery.

  Re-sync policy data

- ( ) Cisco Identity Services Engine, Group-Based Access Control UI in Cisco DNA Center will be inactive

Managing Policy on Cisco Catalyst Center

- Cisco ISE is Read-Only
- Single Matrix support on Cisco ISE
- Default Permit/Deny applicable to all sites
- Single SGACL enforcement per policy

Managing Policy on Cisco ISE

- No Matrix view on Catalyst Center
- Multi-Matrix support on Cisco ISE
- Per Site Default Permit/Deny available with multi-Matrix
- Multi SGACL enforcement per policy

Cisco Catalyst Center Policy

Default Permit vs Default Deny Model

Default Permit Model

Source \ Destination	Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
Production_User		⊖	⊖	⊖	⊖
Production_Srvr	⊖		⊖	⊖	⊖
Development_User	⊖	⊖		⊖	⊖
Development_Srvr	⊖	⊖	⊖		
Unknown	⊖	⊖	⊖		

Default_Policy: ✓

Default Deny Model

Source \ Destination	Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
Production_User	✓				
Production_Srvr		✓			
Development_User			✓		
Development_Srvr				✓	✓
Unknown				✓	✓

Default_Policy: ⊖

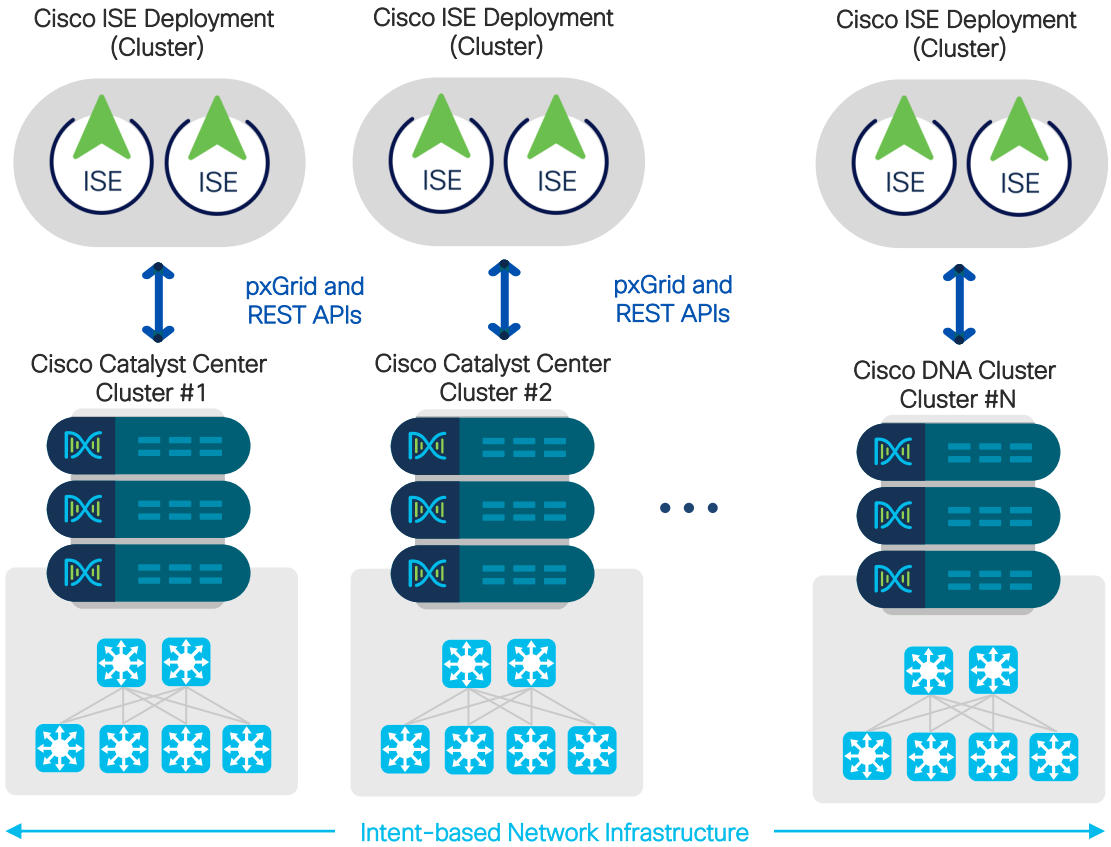
Source \ Destination	Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
Production_User					✓
Production_Srvr					✓
Development_User					✓
Development_Srvr					✓
Unknown	✓	✓	✓	✓	✓

Default_Policy: ⊖

Initial Brownfield Deployment

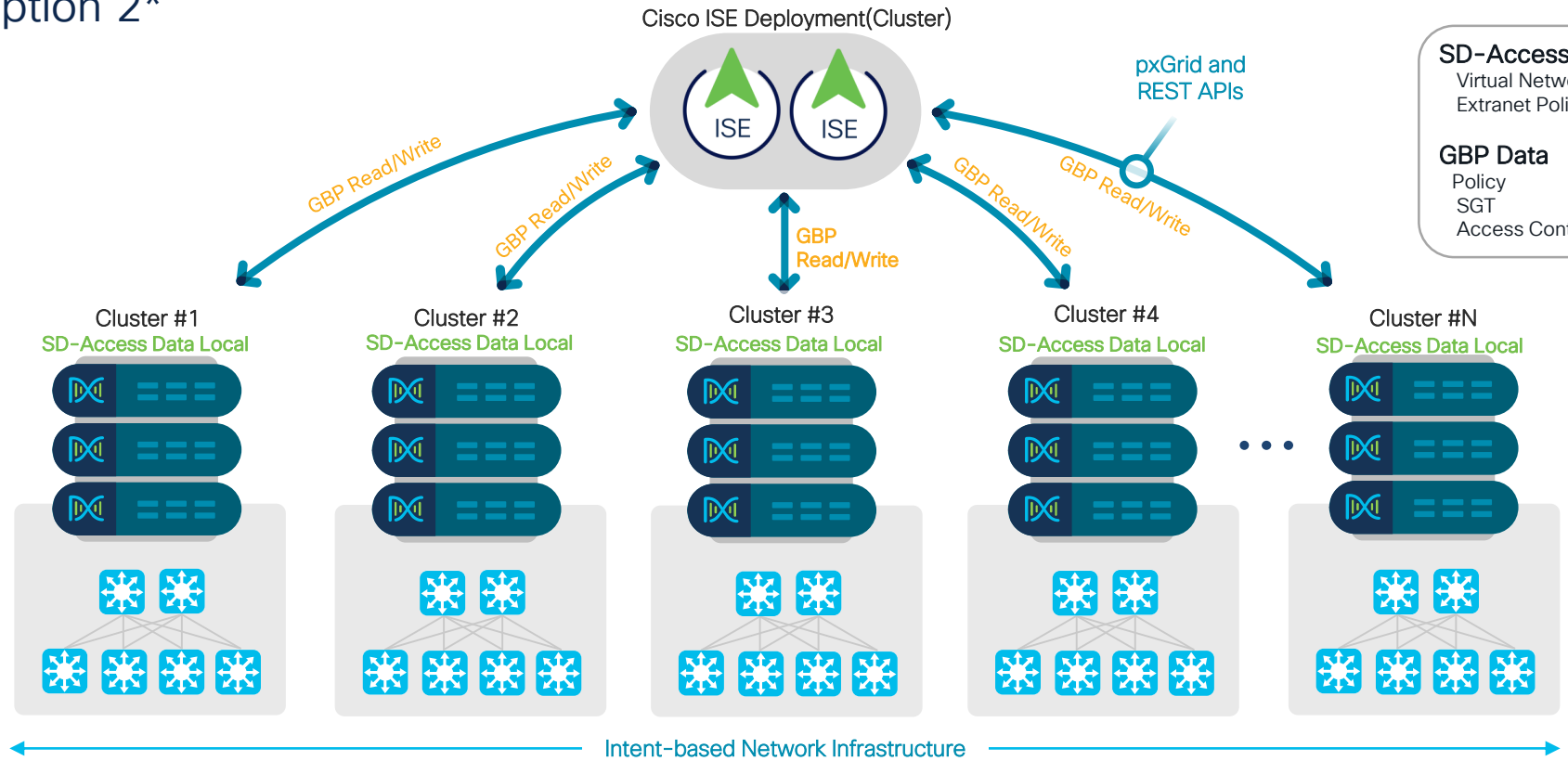
Integrating Multiple Cisco Catalyst Center with ISE

Option 1



Integrating Multiple Cisco Catalyst Center with ISE

Option 2*



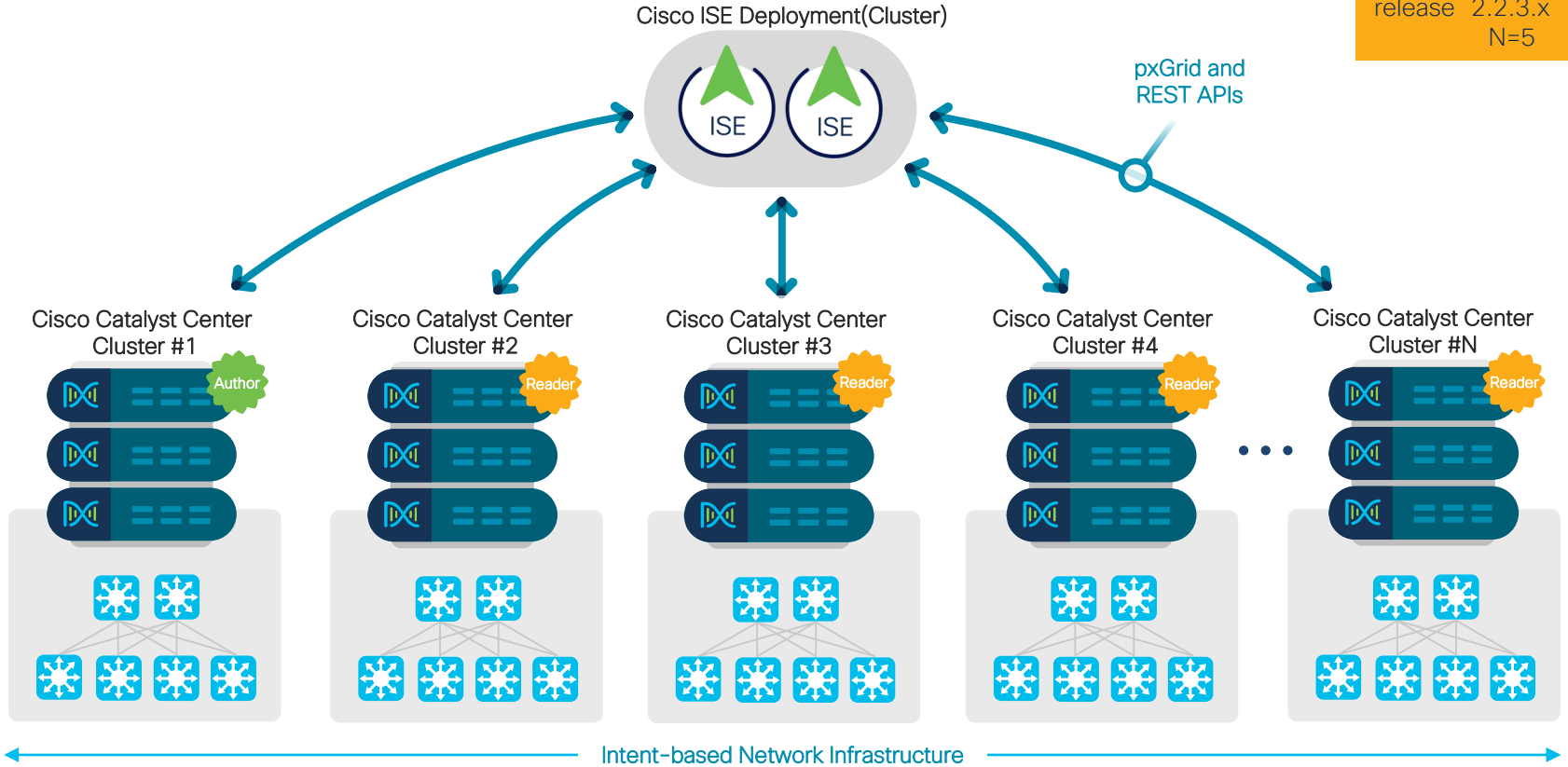
SD-Access Data
- Virtual Network
- Extranet Policy

GBP Data
- Policy
- SGT
- Access Contract

Integrating Multiple Cisco Catalyst Center with ISE

Option 3- Multiple Cisco Catalyst Center Solution Overview

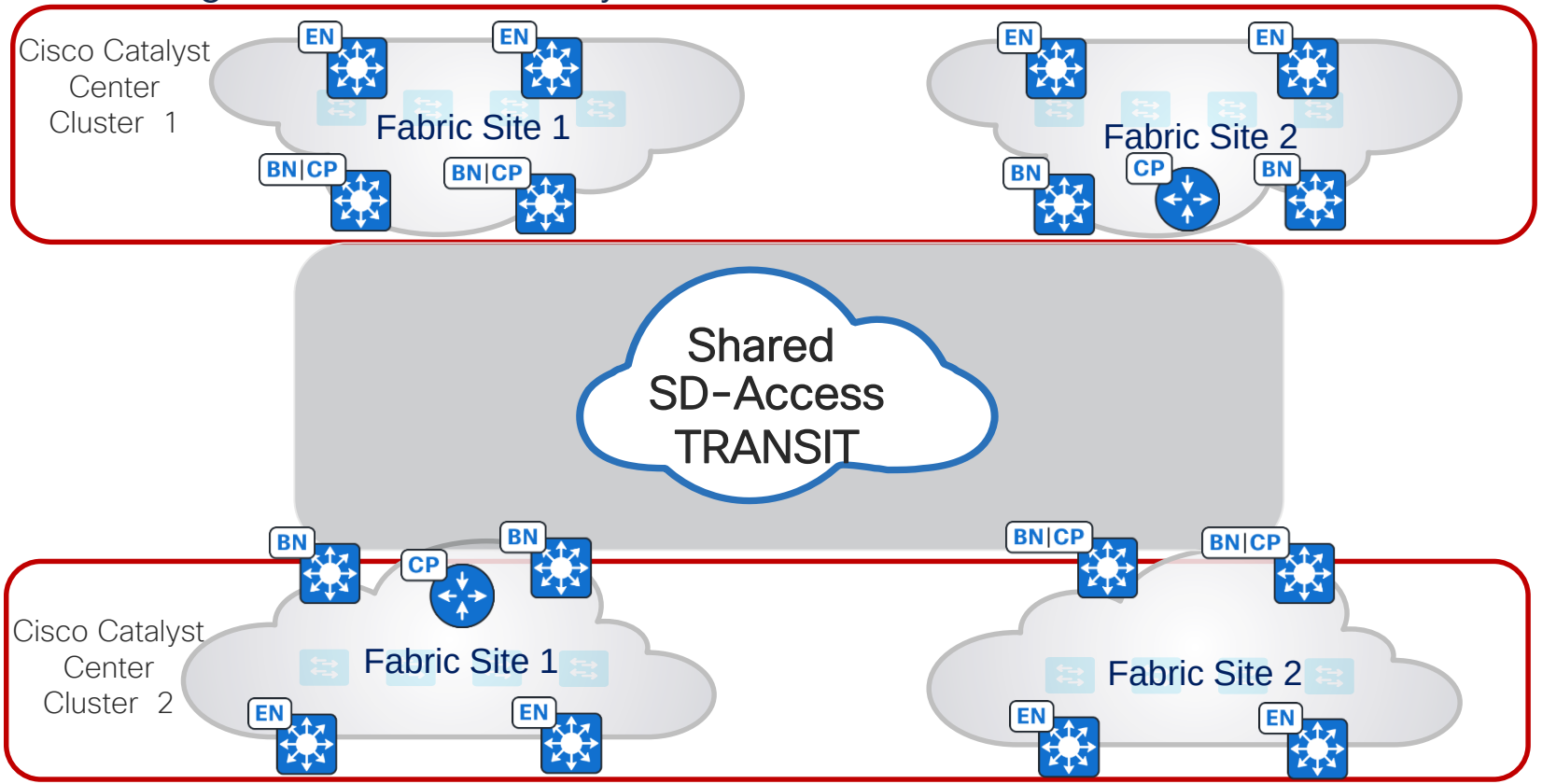
Starting Catalyst Center release 2.2.3.x
N=5



Multiple Cisco Catalyst Centerenter to Single Cisco ISE PDG

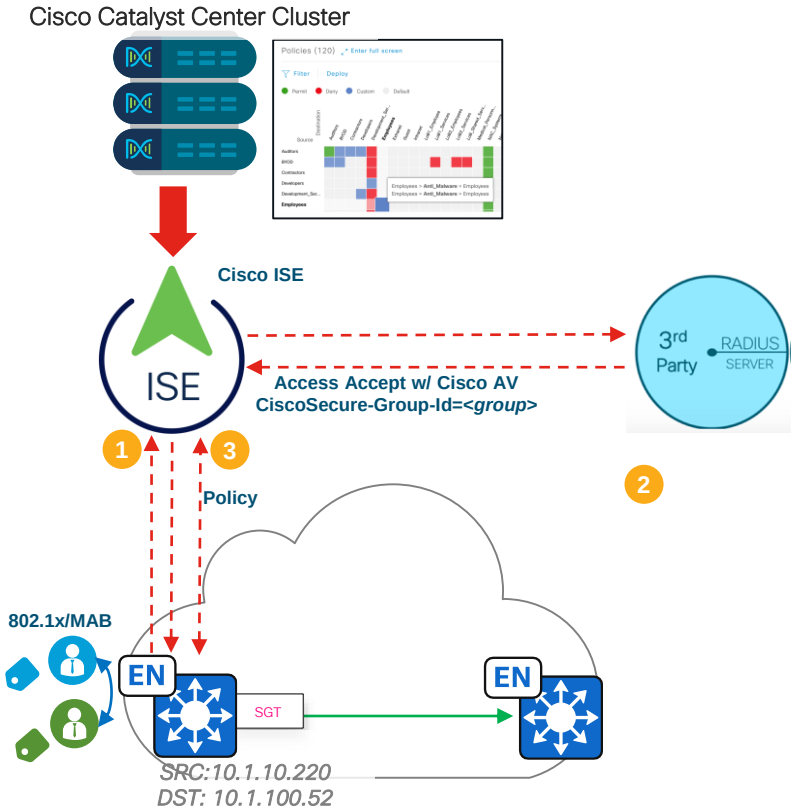
Cisco SD-Access Multi-site

Transit Design across Cisco Catalyst Center Clusters



Cisco Catalyst Center Policy

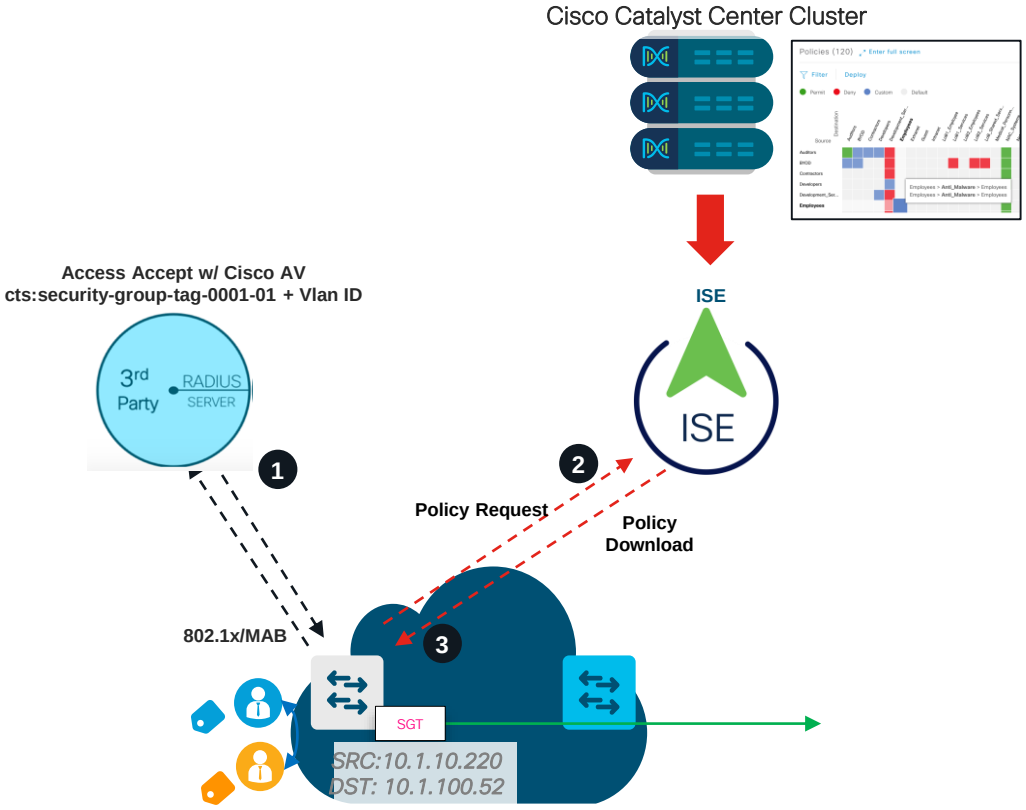
Third-Party AAA/RADIUS Server support – Option 1



- 3rd Party Radius server is configured as external Radius server to Cisco ISE.
- Cisco ISE acts as a proxy for all Authentication request
- 3rd Party Radius server to pass the Authorization results via Cisco AV Pair Attributes

Cisco Catalyst Center Policy

Third-Party AAA/RADIUS Server support – Option 2



- 3rd Party Radius server is configured as external Radius server to Cisco ISE.
- Cisco ISE acts as a proxy for all Authentication request
- 3rd Party Radius server to pass the Authorization results via Cisco AV Pair Attributes
- Small HA Cisco ISE Deployment

New Feature
Enhanced

Catalyst Leadership in Enterprise Networks

A Platform based Approach

Catalyst Center and Meraki Dashboard

28M Network Devices Managed

50% Y/Y

19M APs | 6M Switches | 2.5M Routers | 830M Clients

13M
Devices on Catalyst Center

15.3M
Devices on Meraki Dashboard

Catalyst 9000 Family

100,000+ Customers, Millions of Switches

"Catalyst 9K continues to be the fastest ramping product in the company's history"

- Chuck Robbins, CEO Cisco Systems

Secure Networking

- Common Policy
- Secure Equipment Access
- SD-Access (LISP & EVPN)
- High-speed Encryption

Digital Experience

- Campus Automation
- AI Endpoint Analytics
- Digital Experience ThousandEyes
- AI Ops & Assurance

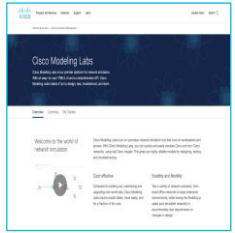
Operational Simplicity

- Cloud Managed Catalyst
- Infrastructure as a Code
- S3 & CloudWatch Integration
- Visibility, Control & Rollback

Cisco Validated Profiles (CVP)

Industry Validated Reports

Industry Certifications



Cisco Modeling Labs

Global Partner Solution Advisors

- *NEW* - Fully Virtualized, SD-Access Secure Campus Lab

Virtualized SD-Access Lab

- Fully Customizable Topology with virtualized 9kv's and 8kv's
- Access on dCloud or build on your existing Data Center
- Fraction of the cost
- GPSA mentored lab buildout support available!

CTF Mission

- Experience the SD-Access Virtual Lab at Capture the Flag in The World of Solutions
- Use Cases – Fabric Sites and Virtual Network Provisioning, Fusion Automation, Extranet, Micro Segmentation, and more!

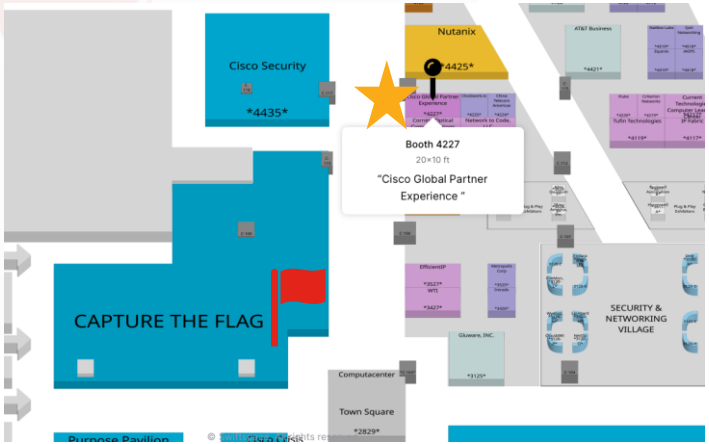
Contact

- GPSA is your source for no-cost, partner enabment and practice building!
- Visit the Global Partner Experience booth (4227) across from Capture the Flag, for more information.

Virtual SD-Access Lab on dCloud

GPSA Sales Connect Page

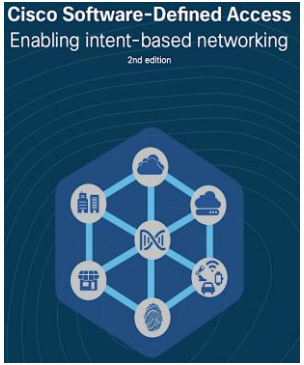
CTF at Cisco Live
Check out Secure Campus Section



Cisco SD-Access LISP Fabric Collaterals

Cisco Software-Defined Access for Industry Verticals

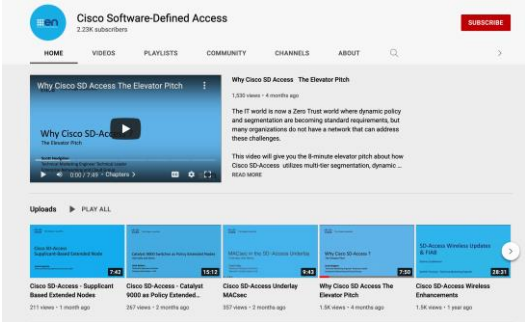
Cisco Software-Defined Access
Enabling intent-based networking



Cisco Solution Validated Profiles (CVPs)

- Cisco Large Enterprise and Government Profile
- Healthcare Vertical
- Financial Vertical
- Healthcare Vertical
- Manufacturing Vertical
- Retail Vertical
- University Vertical

Cisco SD-Access YouTube Link



Multiple Cisco DNA Center to ISE

Cisco SD-Access Design Tool

EN&C Validated Designs

The Latest SD-Access Guides

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you