Cisco SD-Access Best Practices

Design and Deployment

Mahesh Nagireddy
Technical Marketing Engineering, Technical Leader
CCIE R&S

BRKENS-2502

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

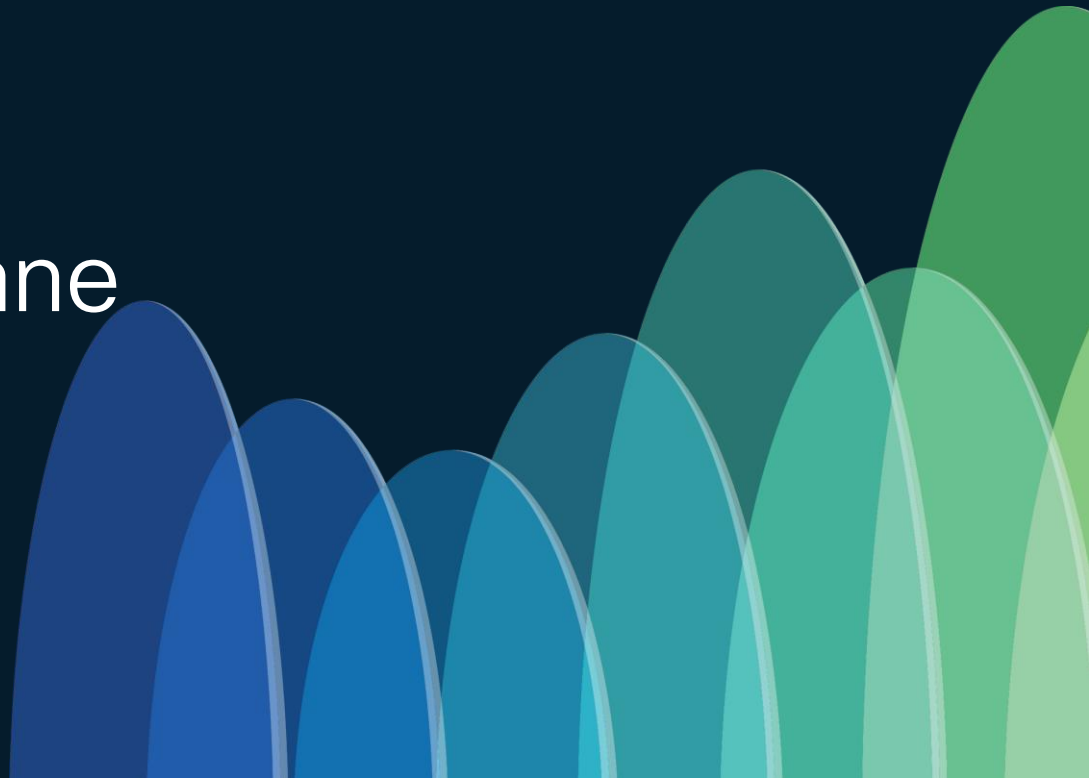
1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Agenda

- Introduction
- Cisco SD-Access Management Plane
- Cisco SD-Access Policy Plane
- Cisco SD-Access Fabric Design
- Cisco SD-Access Single/Multi-site Design
- Cisco SD-Access Services

SD-Access Management Plane

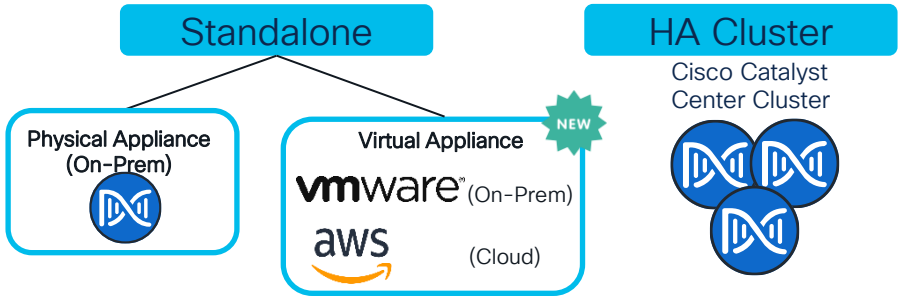


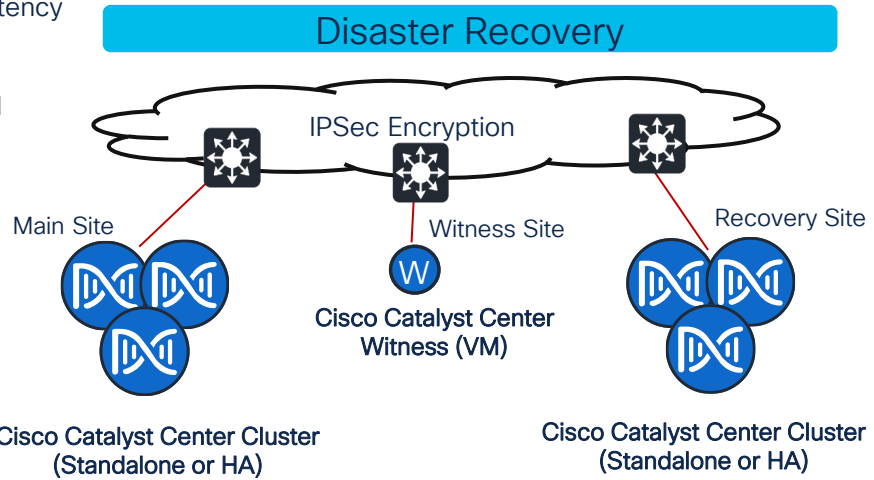
Cisco SD-Access
Cisco Catalyst Center Deployment

- **Deployment Options**
  - Standalone
    - On-Prem Physical Appliance(DN3 – C220 M6 HW)
    - Virtual Appliance on Cloud(AWS) *
    - On-Prem Virtual Appliance on VMWare ESXI *
  - 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



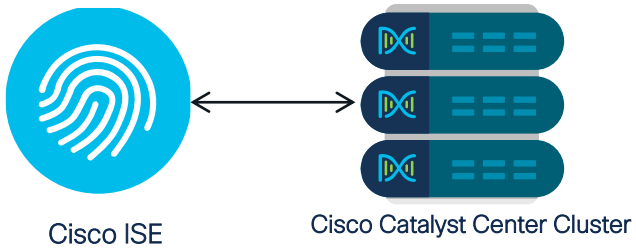


- Failure detection and recovery

	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

* - DN-SW-APL

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 CATC to ISE
Shared Transit + Extranet

Device Administration
TACACS

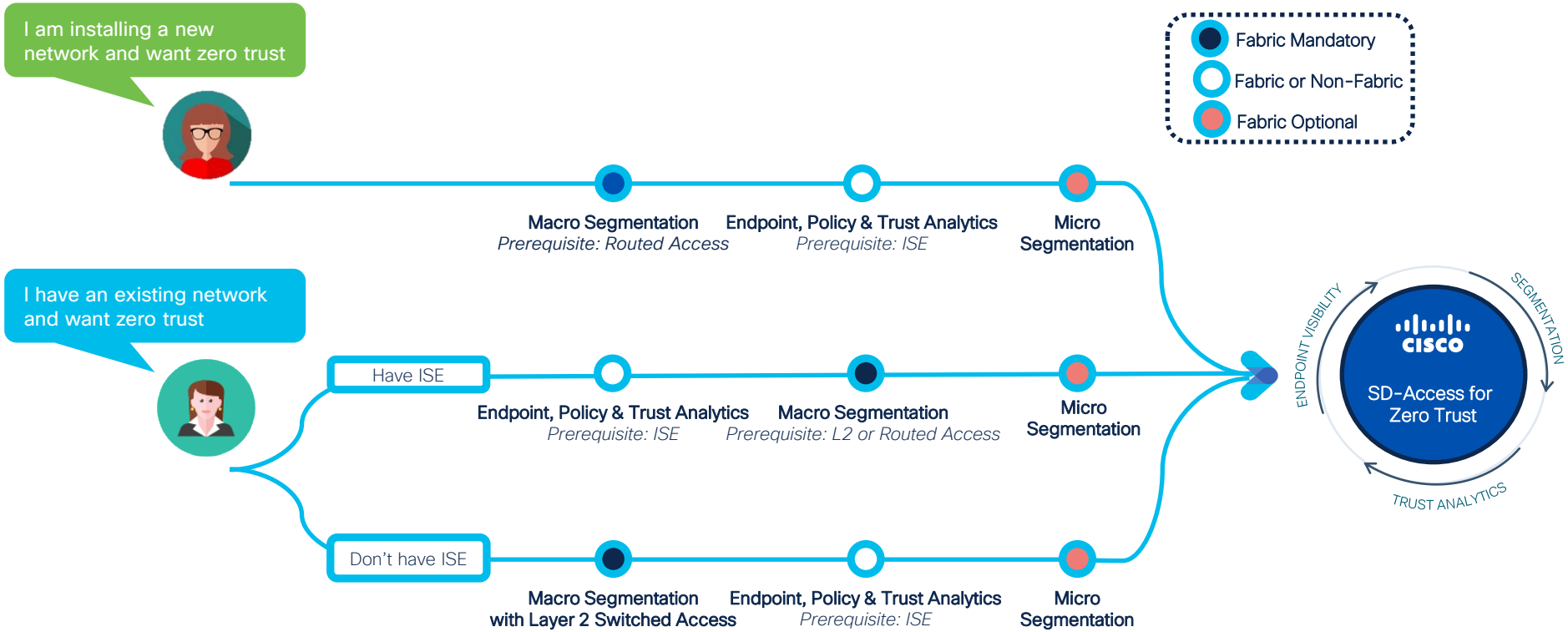
Asset Visibility
Everything & Everyone on Network

Policy Analytics
Group to Group Interaction with automated policy

Security Ecosystem Integration
Context Sharing

cisco Live!

SD-Access flexible deployment options



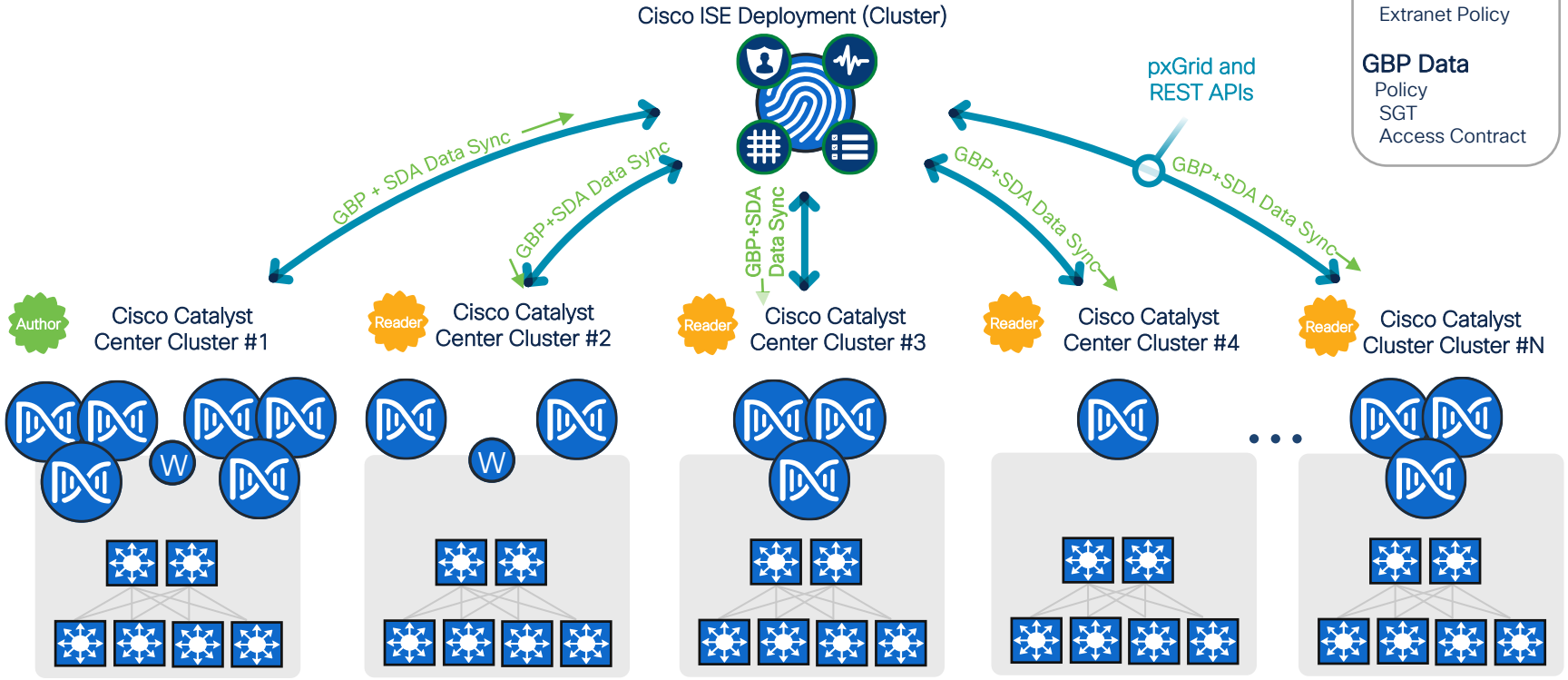
Integrating Cisco Catalyst Center with ISE

Multiple Cisco Catalyst Center Solution Overview

N=5 starting
Catalyst Center: 2.2.3.x

SD-Access Data
Virtual Network
Extranet Policy

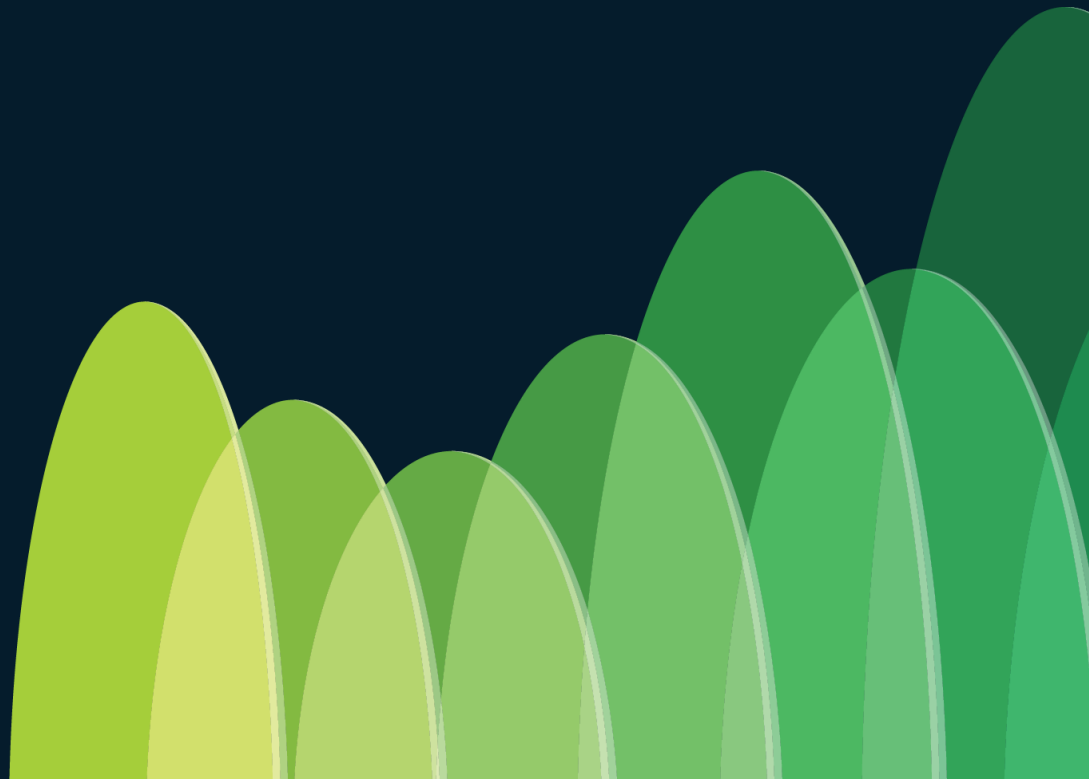
GBP Data
Policy
SGT
Access Contract



Intent-based Network Infrastructure

Multiple Cisco Catalyst Center to Single Cisco ISE PDG

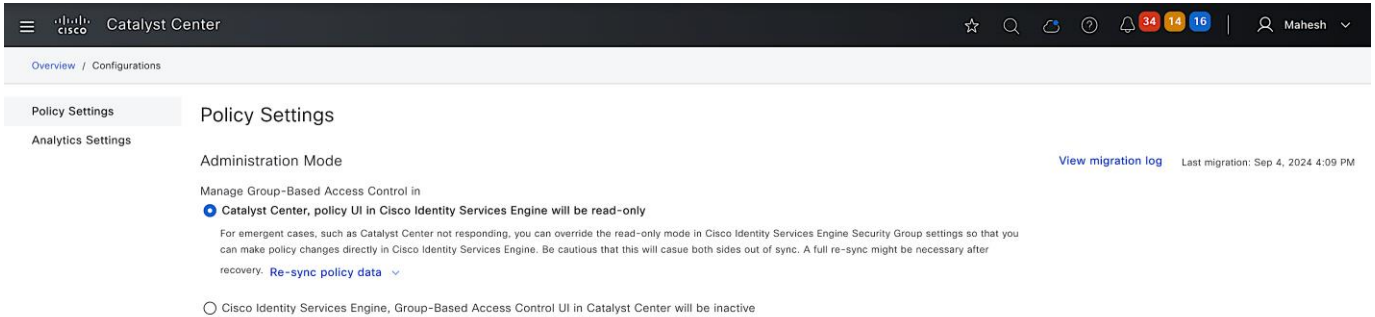
SD-Access Policy Plane



cisco Live!

Cisco Catalyst Center policy

Manage group-based access control policy on Catalyst Center



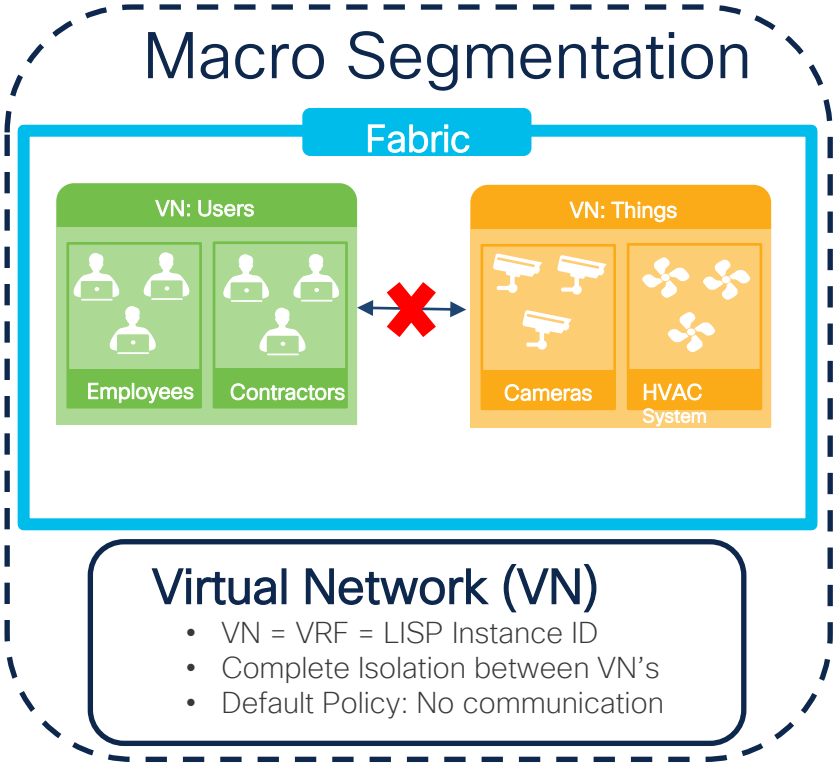
Managing Policy on Cisco Catalyst Center

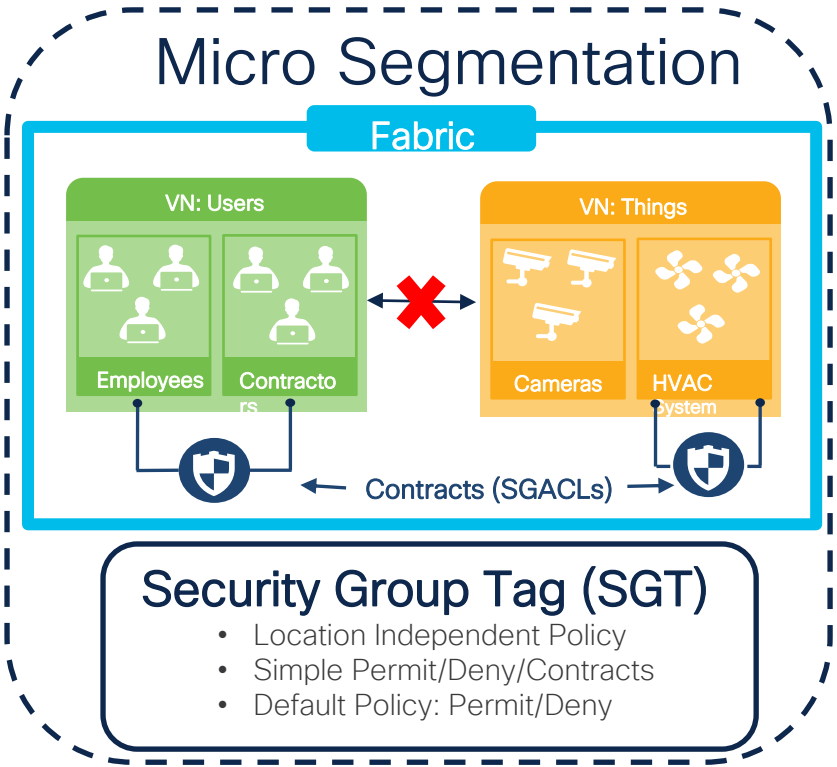
- Cisco ISE is Read-Only for Trustsec data
- Single Matrix support on Cisco ISE
- Default Permit/Deny applicable to all sites
- Single SGACL enforcement per policy

Managing Policy on Cisco ISE

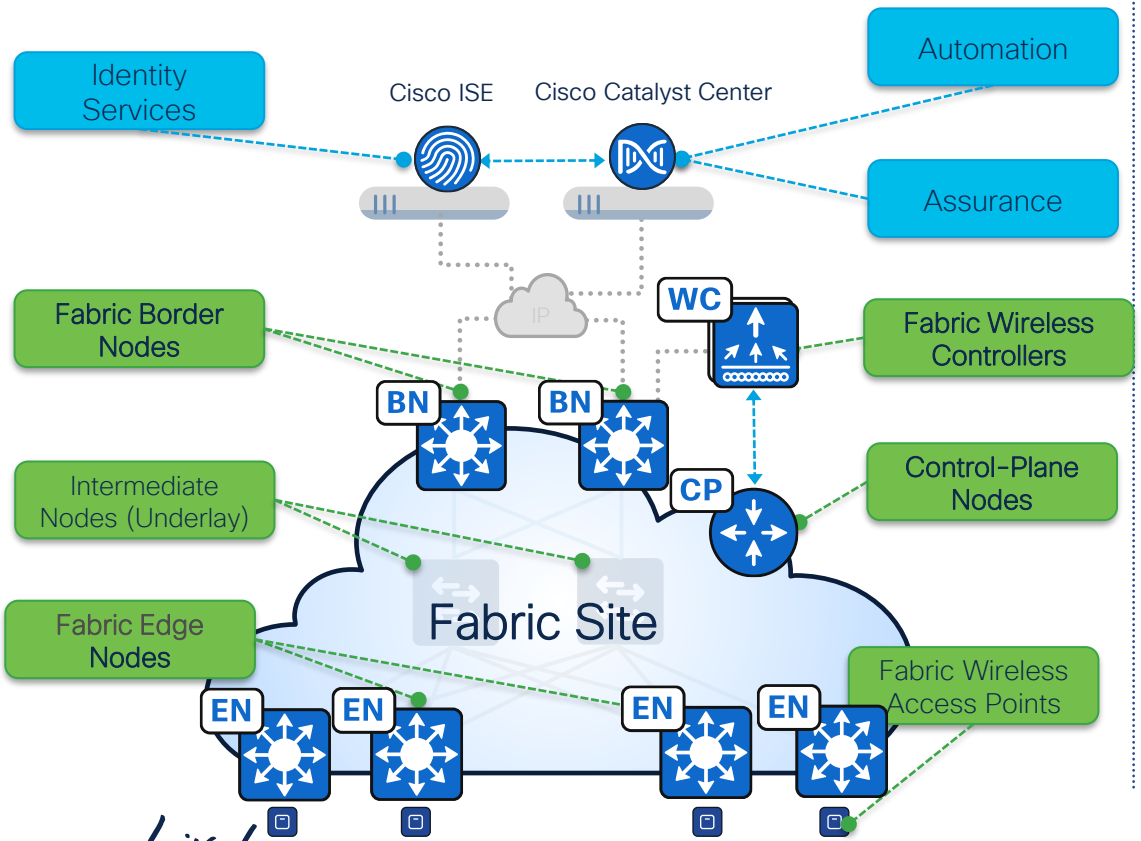
- No Matrix view on Catalyst Center
- **Multi-Matrix support on Cisco ISE**
- **Per Site Default Permit/Deny available with multi-Matrix**
- **Multi SGACL enforcement per policy**

Cisco SD-Access policy
Segmentation Strategy





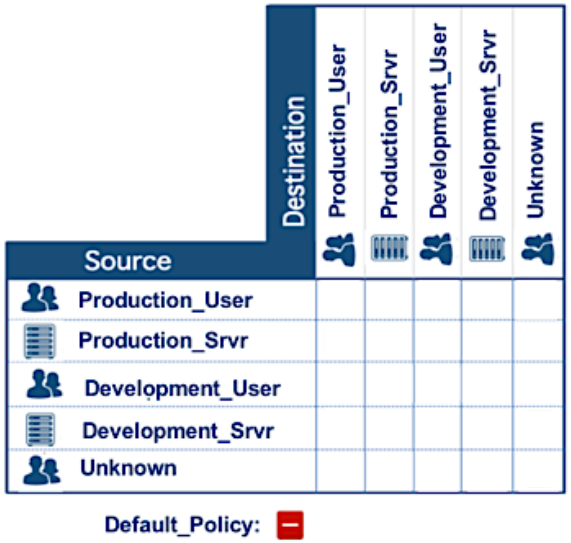
Cisco SD-Access
Fabric roles & terminology



- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyse 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 Catalyst Center policy
Default Permit vs Default Deny Model

Default DENY Model



- Default action is Deny IP
- Traffic should be explicitly permitted with the use of Security Group Access Lists (SGACLs).
- Fair understanding of traffic flows within their network.
- Lower TCAM Resource usage on switches
- Less Deny Policies(SGACL) to manage

Cons

- Detailed network study prior to implementation
- Fallback mechanism incase of Cisco ISE Nodes down

Cisco Catalyst Center Policy
Default Deny Automation Enhancements

Cisco Catalyst Center:

cts role-based enforcement ← BN + EN
cts role-based enforcement vlan-list 1023,1028 ←BN+ EN + PEN + SBEN

1. For Lan Automated Devices, disable CTS Role-based enforcement on L3 Uplinks immediately after the links are converted from L2 to L3 Interfaces. **Automated for New LAN Auto sessions starting Cisco Catalyst Center release 2.3.7.4**

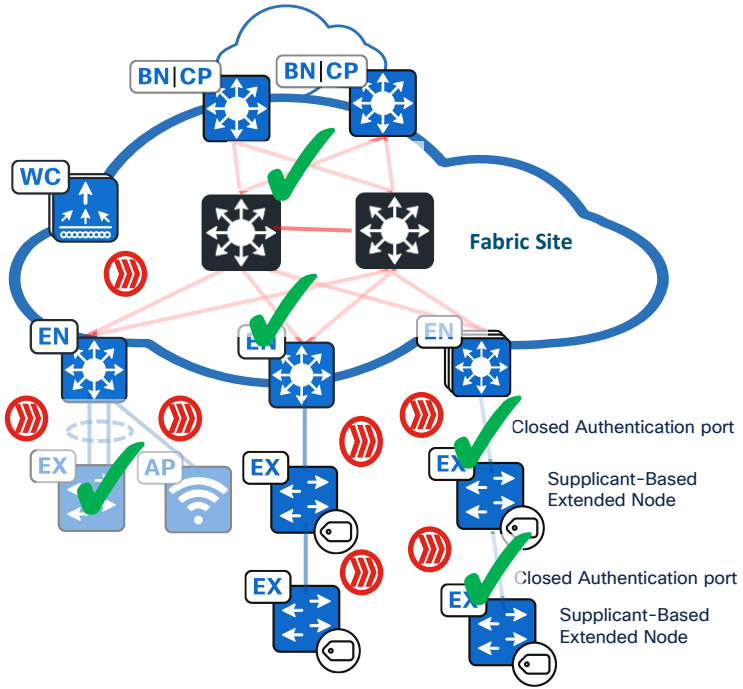
2. Use Template Editor to Disable CTS Role-based enforcement on AP, Extended node Vlans. **This is automated starting Cisco Catalyst Center release 2.3.7.6**

3. Disable CTS role-based enforcement on Edge Node downlinks facing **SBEN**. **This is automated starting Cisco Catalyst Center release 2.3.7.6**

4. Disable CTS Role-based enforcement on **SBEN** uplinks/downlinks connecting to Edge or **SBEN**. **This is automated starting Cisco Catalyst Center release 2.3.7.6**

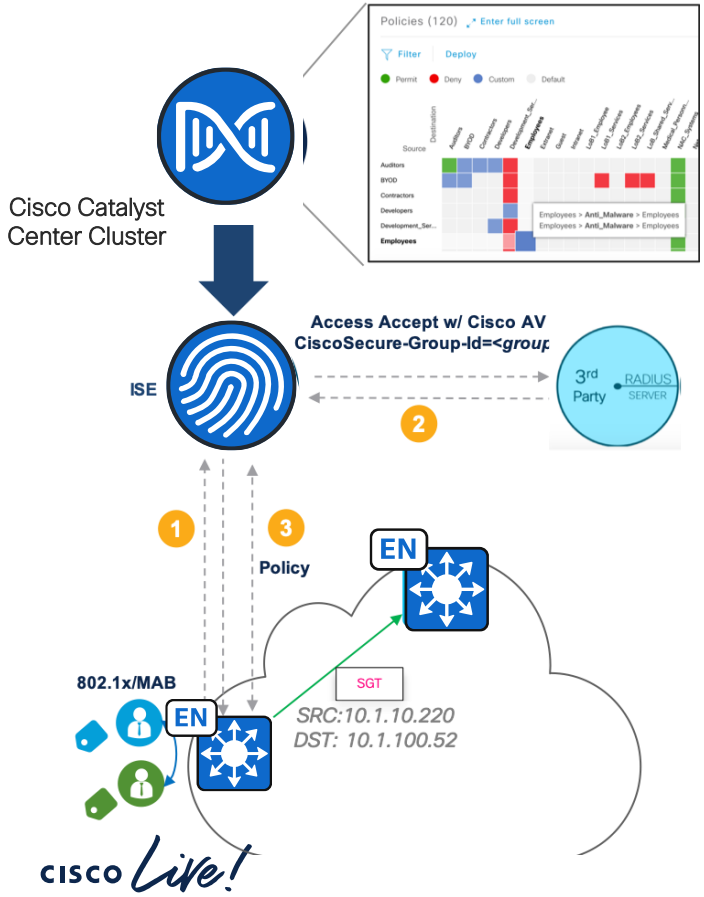
5. Disable CTS role-based enforcement on Edge Node downlinks facing PEN.

6. Disable CTS Role-based enforcement on **PEN** uplinks/downlinks connecting to Edge or **PEN**



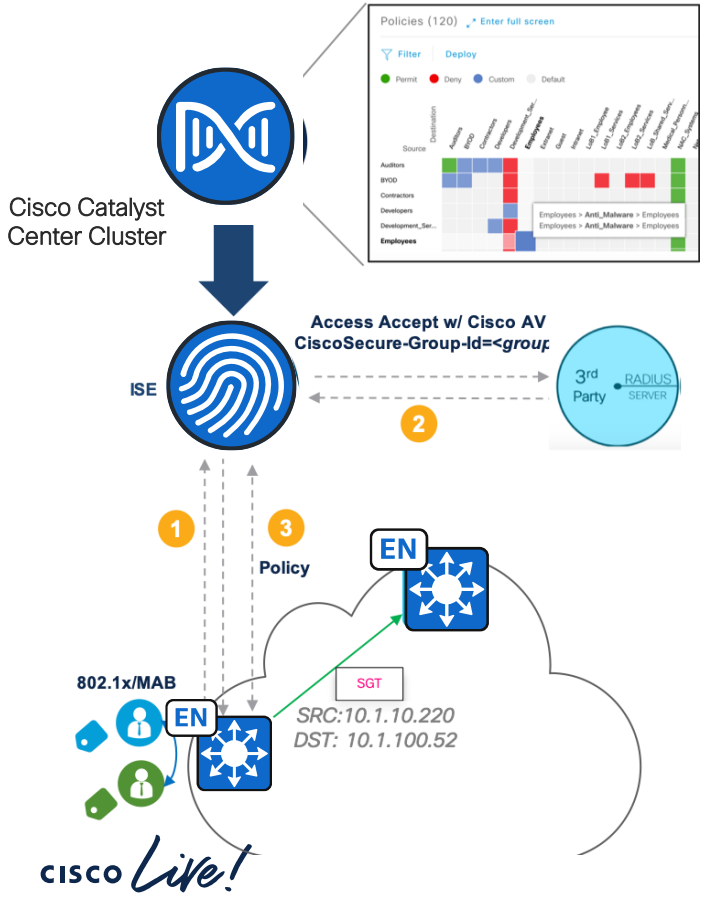
Cisco Catalyst Center policy

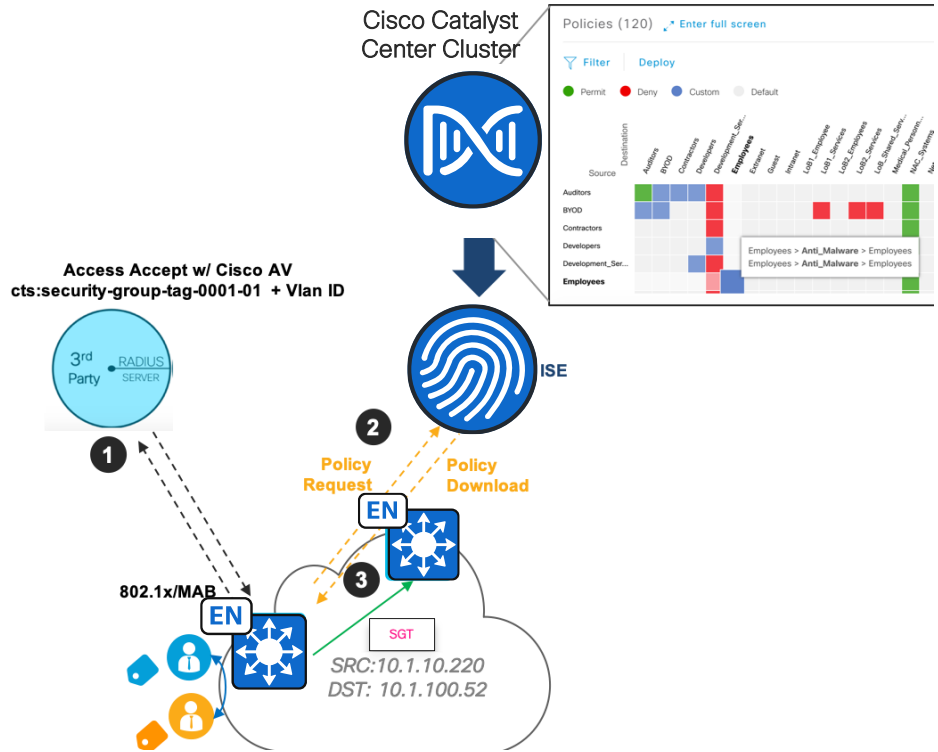
Third-Party AAA/RADIUS Server support



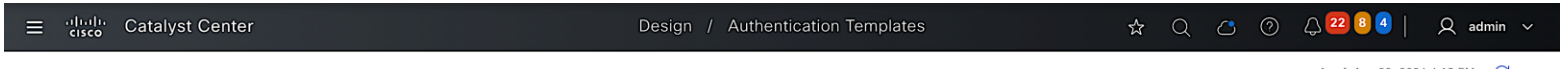
Cisco Catalyst Center policy

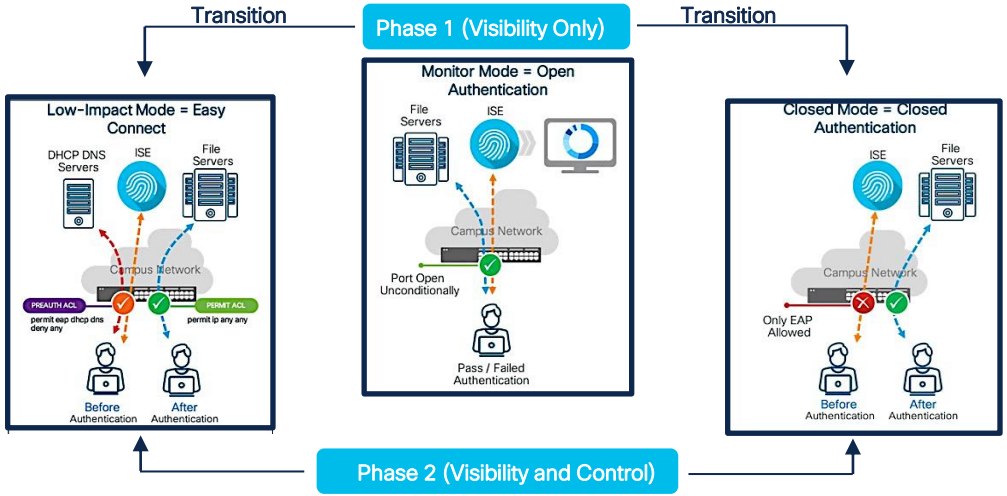
Third-Party AAA/RADIUS Server support

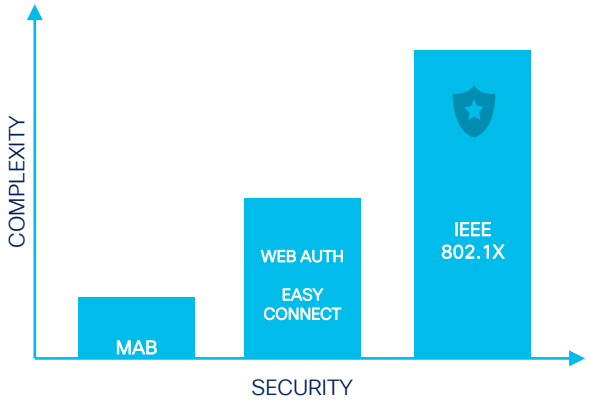




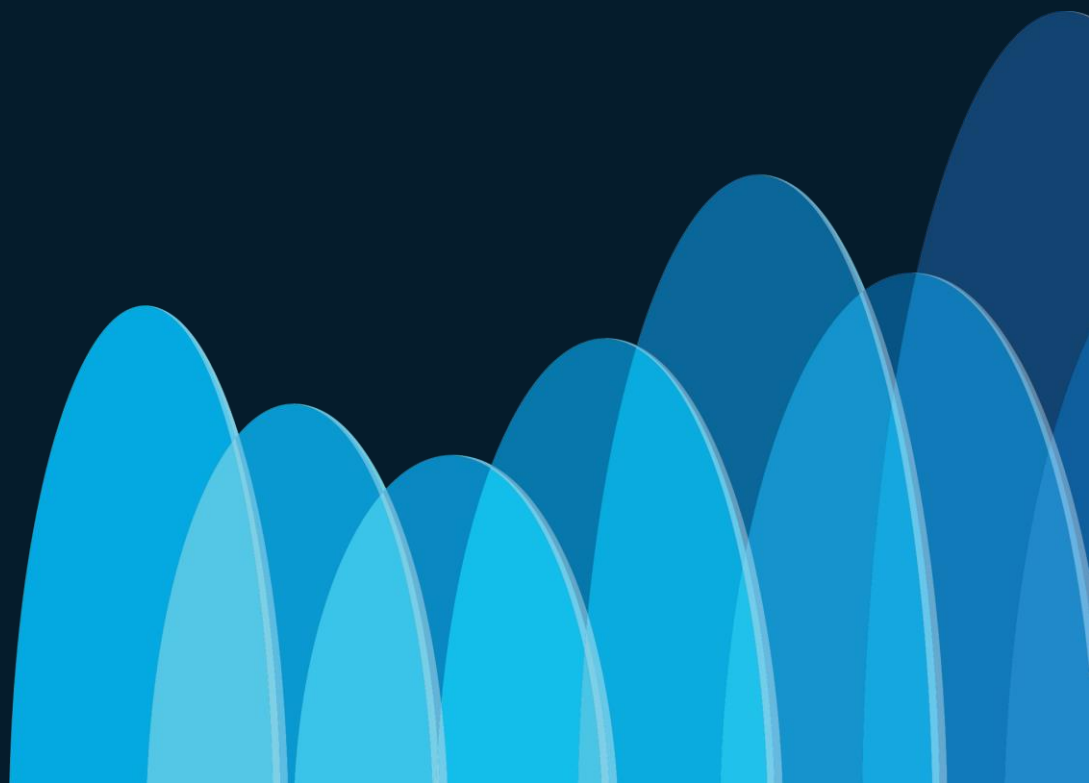
Cisco Catalyst Center provision
Authentication template







Fabric Design



cisco Live!

Cisco SD-Access underlay
Readiness and compliance

Cisco Catalyst Center 2.3.7 Data Sheet

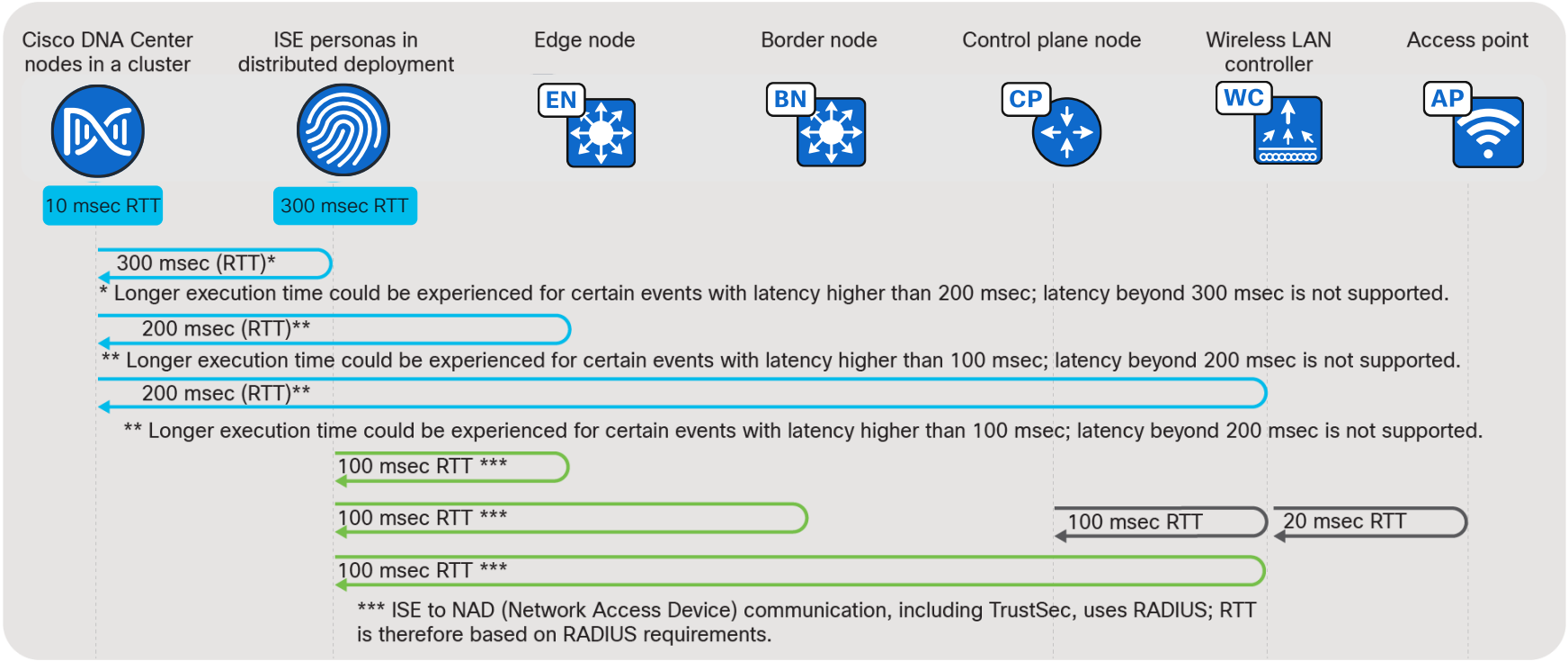
Cisco Catalyst Center Fabric Readiness and Compliance Checks

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

Software Licensing

- Network Advantage & DNA Advantage/Cisco DNA Premier License

Cisco SD-Access underlay
Latency requirements



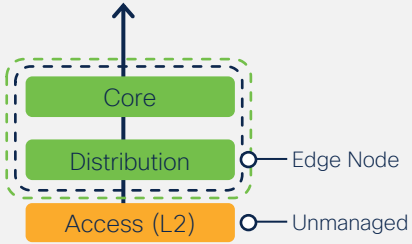
SD-Access flexible deployment options

Migration options

Macro segmentation

Micro segmentation

Fabric with unmanaged Layer 2 switched access*

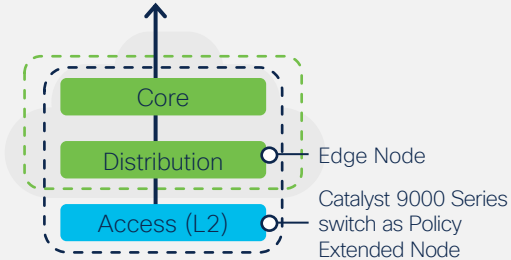


Use case: Keep your existing unmanaged switches

- Segmentation starts at distribution layer
- Integrated wired and wireless

Benefit: Allow tenants to bring their own network.

Fabric with managed Layer 2 switched access



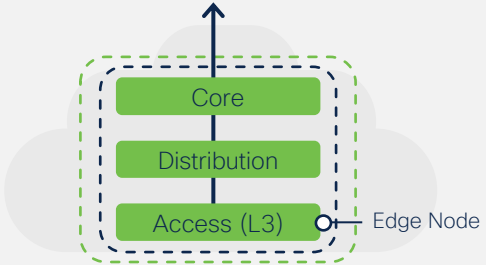
Use case: Retain Layer 2 access

- 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

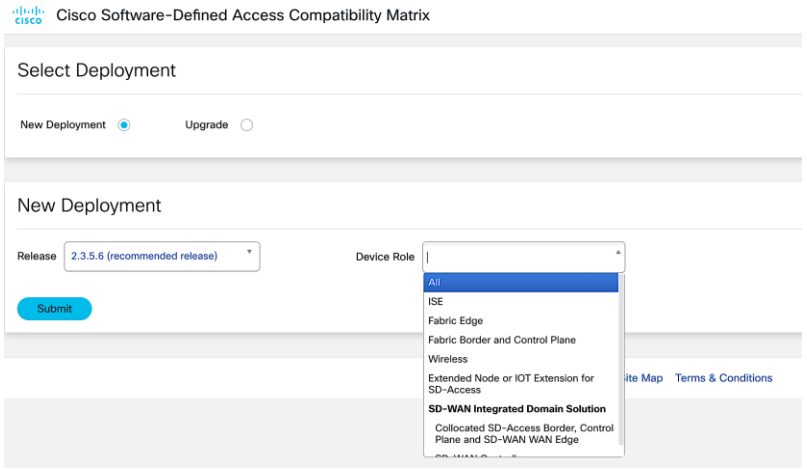
- Full stack macro and micro segmentation
- Integrated wired and wireless
- Policy-based traffic steering
- Topology independence

Benefit: Experience all that SD-Access offers

* Supported starting Cisco Catalyst Center release 2.2.1

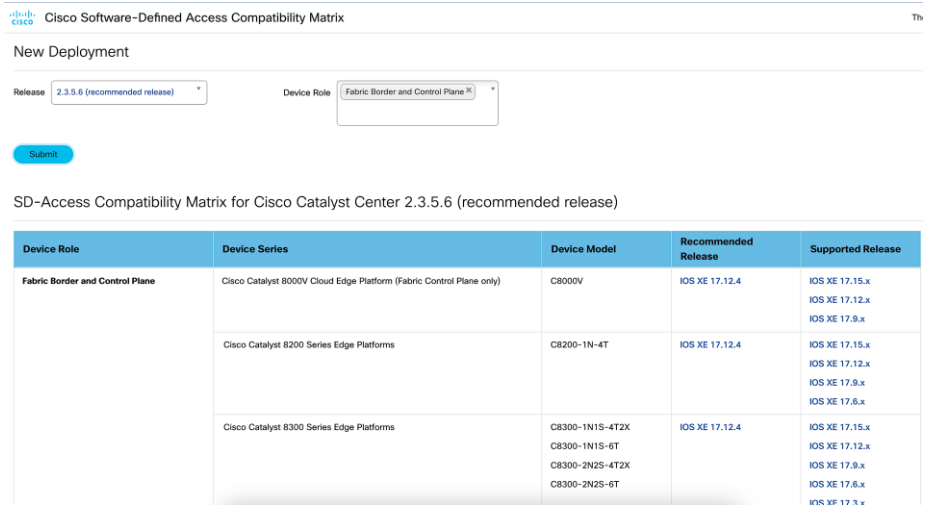
For your reference

Cisco SD-Access underlay
Platform and software recommendations



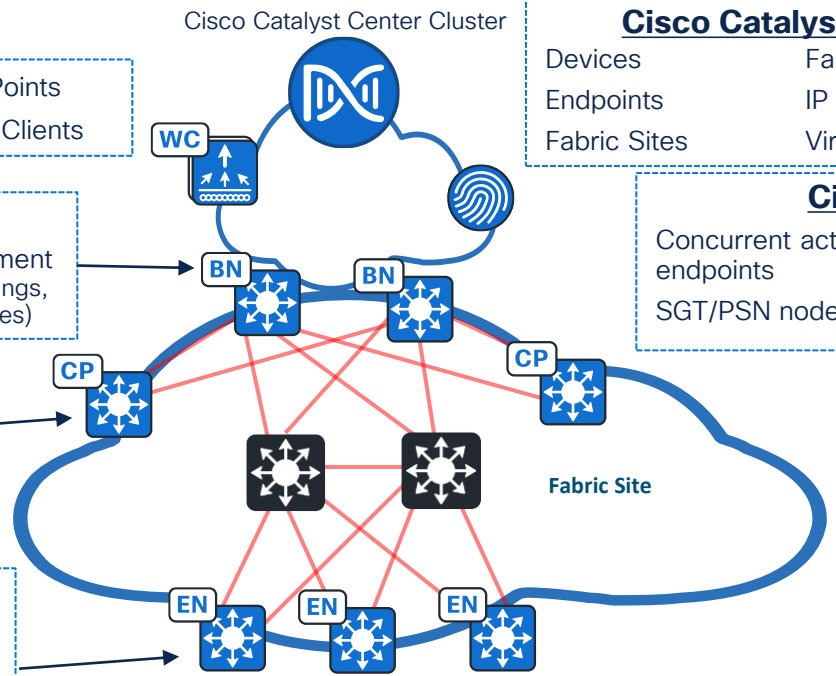
Platform support based on the Fabric Role

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



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

Cisco SD-Access underlay
Platform scale



Cisco Catalyst Center

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

Access Points
Wireless Clients

Cisco ISE

Concurrent active endpoints	SGACL
	SXP peering
SGT/PSN node	

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

Virtual Networks
Fabric Host Entries

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

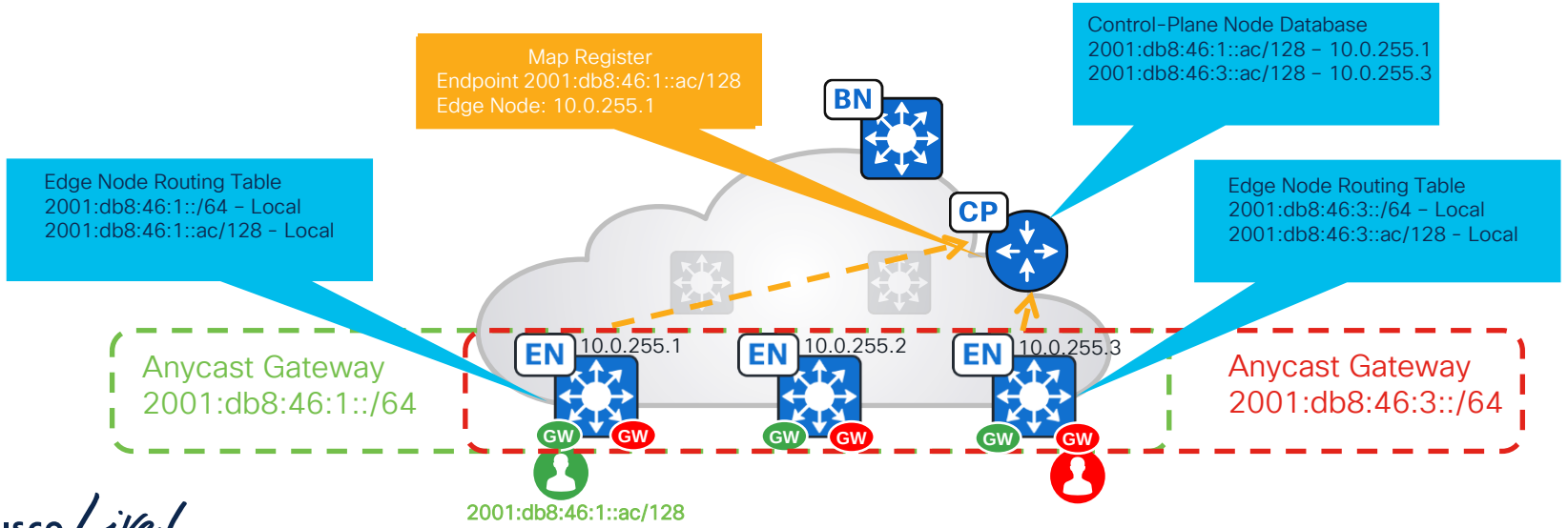
Consider Individual Platform Scale and Performance

Least Common Denominator (LCD) across the solution elements

Cisco SD-Access underlay
V4 and V6 support

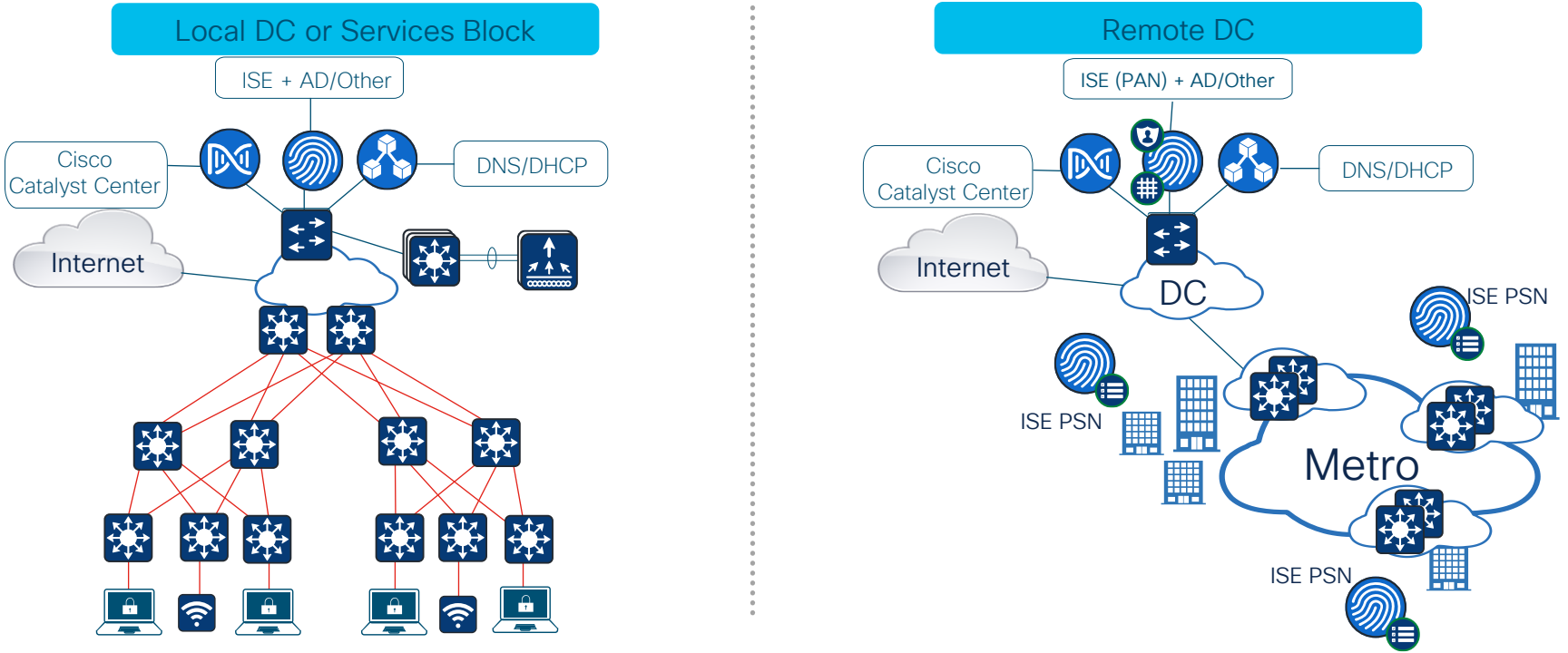
As of
Catalyst Center: 2.3.7.0
Cisco ISE: 3.4

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 / Dual-Stack
Cisco Catalyst Center to Cisco ISE	: V4 only



Cisco SD-Access underlay

Where do I place Critical/Shared Services



Cisco Catalyst Center requires access to Internet*

Cisco SD-Access underlay

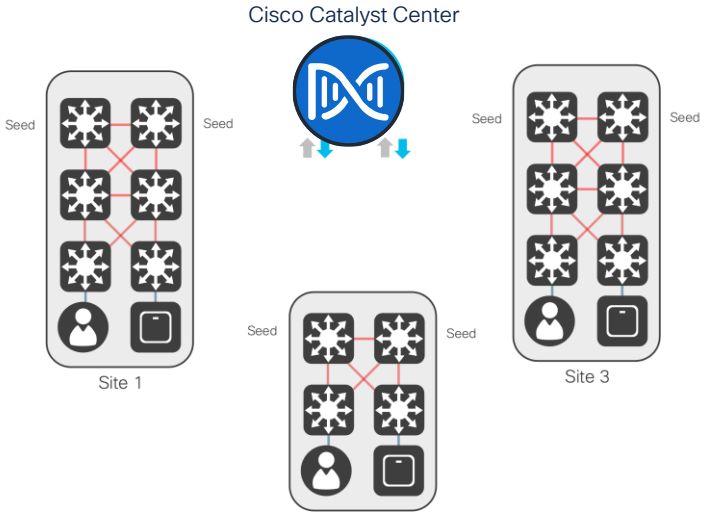
Device onboarding options

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

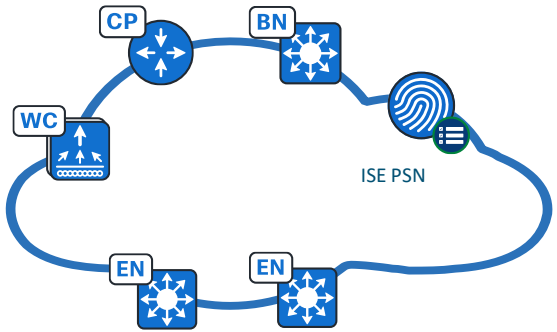
LAN Automation Enhancements 2.3.7.X

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

LAN Automation Enhancements 2.3.7.5

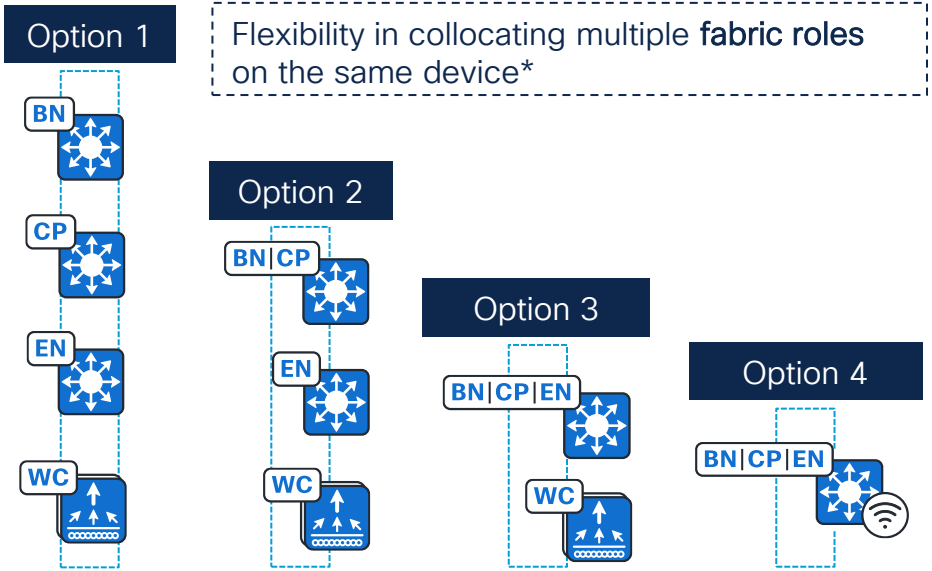
- Discovery depth level for LAN automation(Default depth=2)
- Session Attributes
  - Session Timeout
  - Device Matching
    - Relaxed
    - Strict

Cisco SD-Access overlay
Fabric device roles



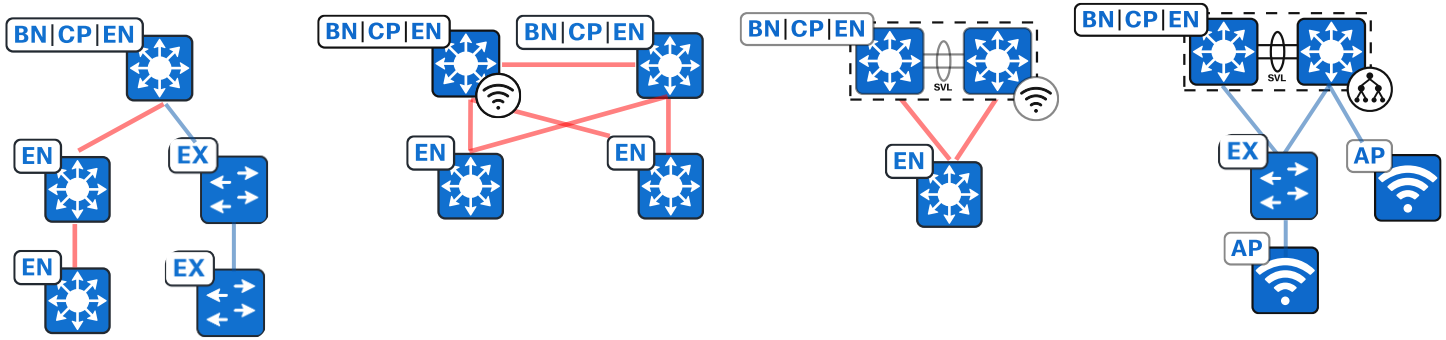
Fabric Site

- 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

Cisco SD-Access overlay
Fabric in a Box design



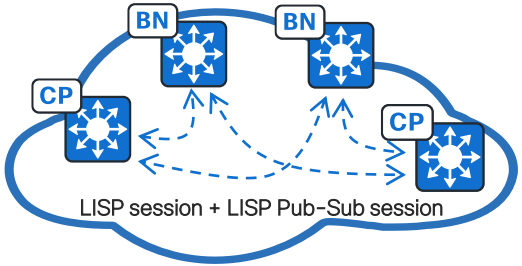
Fabric in a Box site guidelines

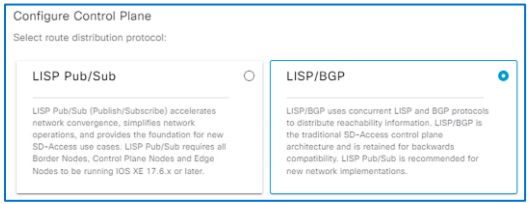
SVL Platform	Fabric in a Box
Endpoints, target fewer than	1000
Access Points	50*

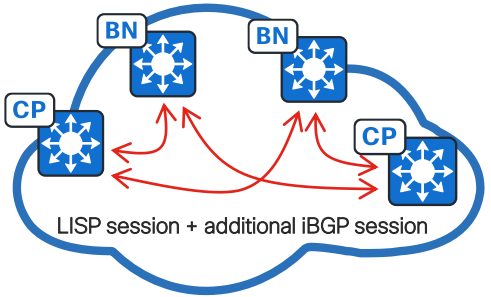
* - C9300

Cisco SD-Access overlay
Fabric control plane enhancements

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







LISP Pub/Sub

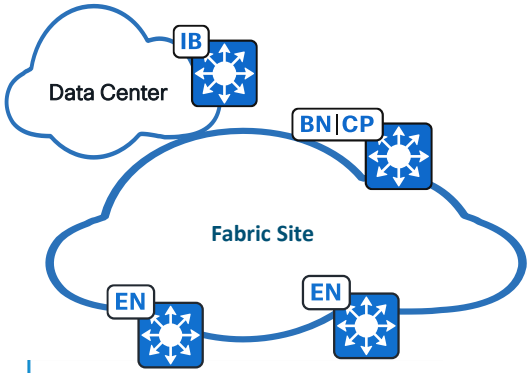
- Publisher-Subscriber model provides LISP Instance-ID table subscription from CP, TCP to Border nodes.
- Faster convergence within fabric site (N-S traffic) and across SD-Access transit.
- LISP Pub/Sub provides backbone for fabric innovations such as Dynamic-Default Border, Extranet, Active-Backup Internet (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 2 TCP Node support

Cisco SD-Access overlay
Border node design options

Internal Border (N)
(Rest of Company)



F-FIAB1.demo.local

Layer 3 Handoff | Layer 2 Handoff

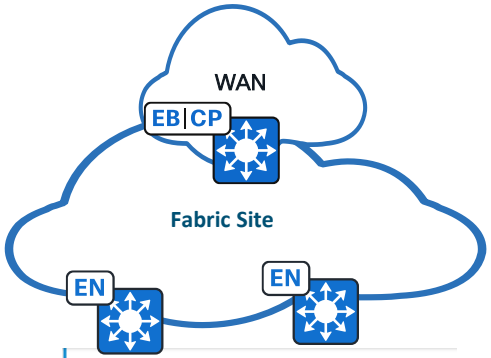
Enable Layer-3 Handoff

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

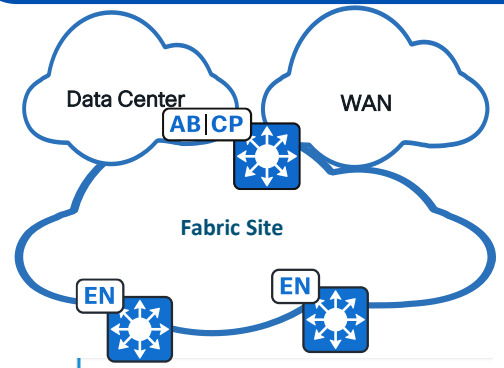
Local Autonomous Number

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

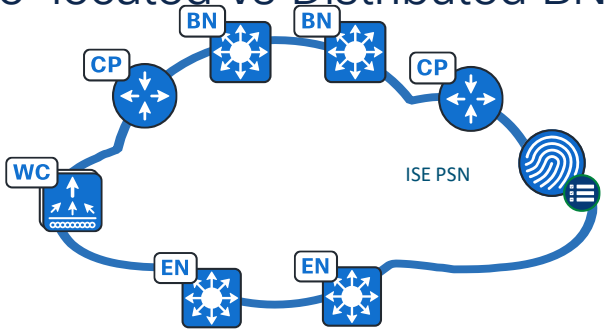
Default to all virtual networks

Do not import external routes

Add Transit/Peer Site

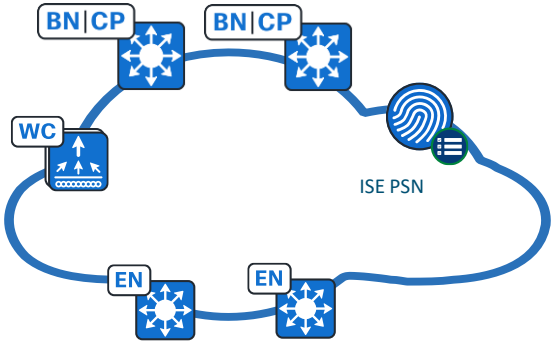
Cisco SD-Access overlay

Co-located vs Distributed BN/CP



Distributed Control Plane Node and Border Node

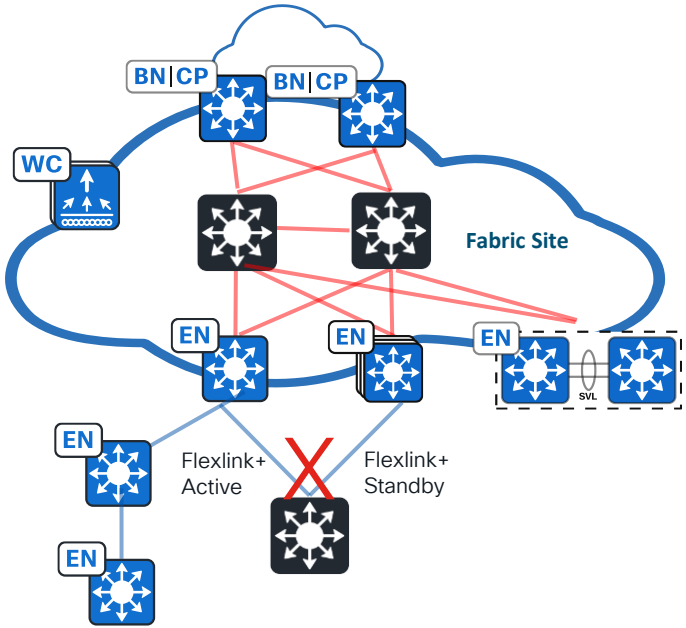
- Improved network stability
- CP ample available memory
- **Best fit for High-frequency roam environments**
- Resilient design when it comes to upgrades, reboots and configs changes



Co-located Control Plane Node and Border Node

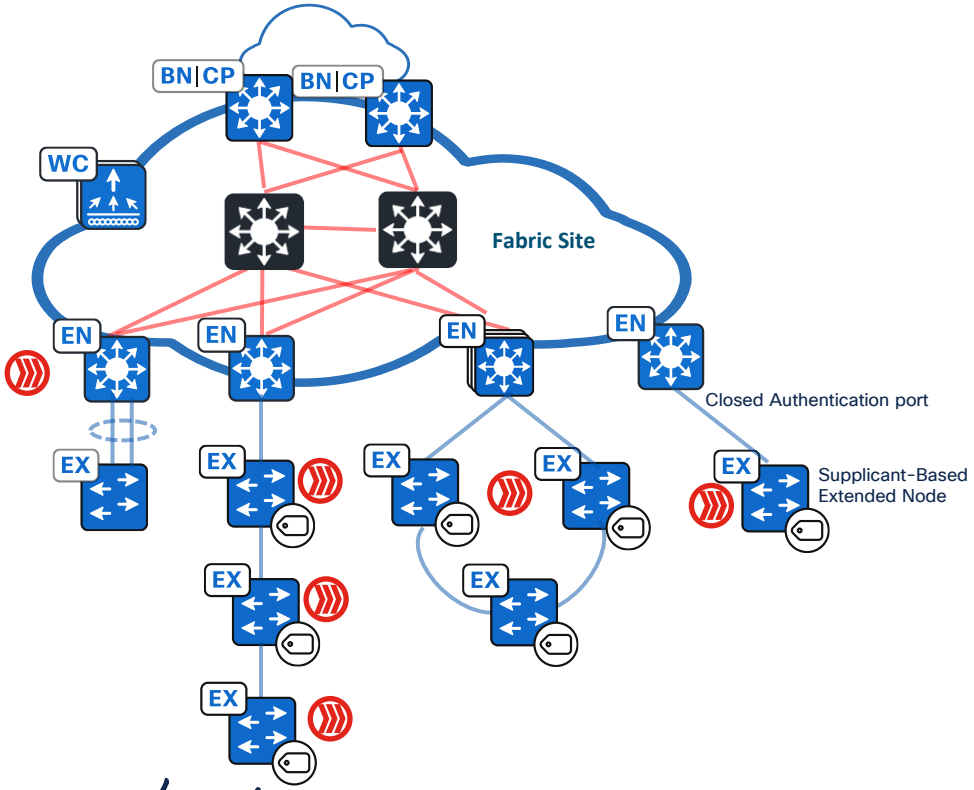
- Simplest Design with lower Capex
- Supports anticipated endpoint, throughput, and scale requirements
- **Not more than 2 CPs if collocating with FEW**

Cisco SD-Access overlay
Edge node design options



- Switch deployment modes supported
  Standalone, Switch Stack, Modular & SVL
- Daisy chain of Edge Node
- Dual homing L2 switch to Edge Node supported with Flexlink+

Cisco SD-Access overlay
Extended enterprise



Three Types
- Extended Node(EX)
- Policy Extended Node(PEN)
- Supplicant-Based Extended Node(SBEN)

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

Supplicant-Based
- Cat9K*(Adv License)

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

*- Excluding C9600

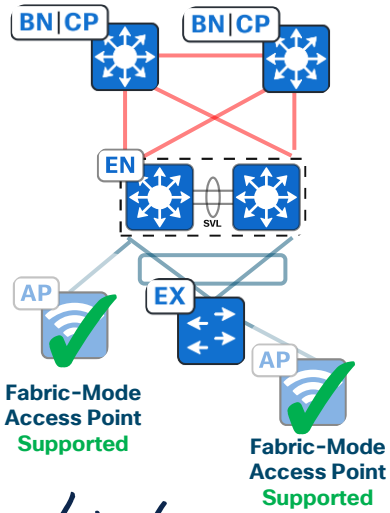
Starting Catalyst Center release 2.2.2.5

Cisco SD-Access overlay

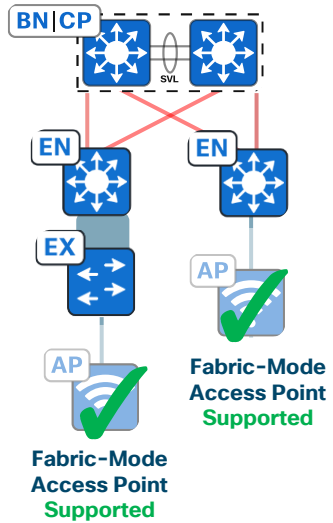
SVL in fabric topology examples

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

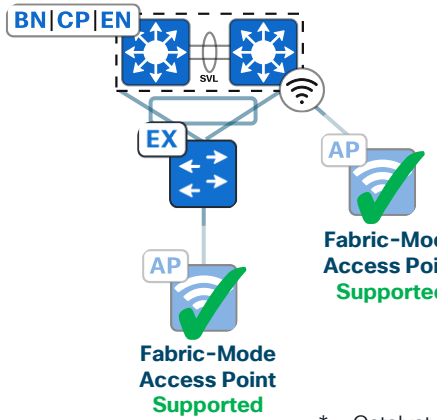
Fabric AP to SVL Edge Node



Fabric AP to EX/PEN



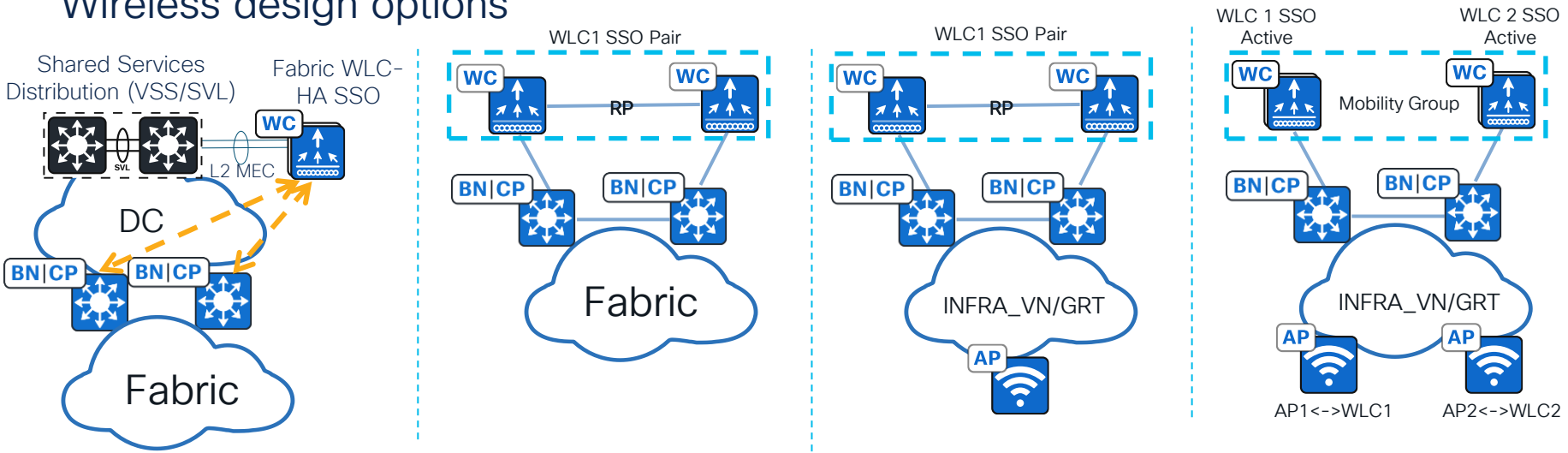
Embedded Wireless support on SVL*



* - Catalyst 9400 and 9500

Cisco SD-Access overlay

Wireless design options



WLC connect to a “shared services” Distribution Block

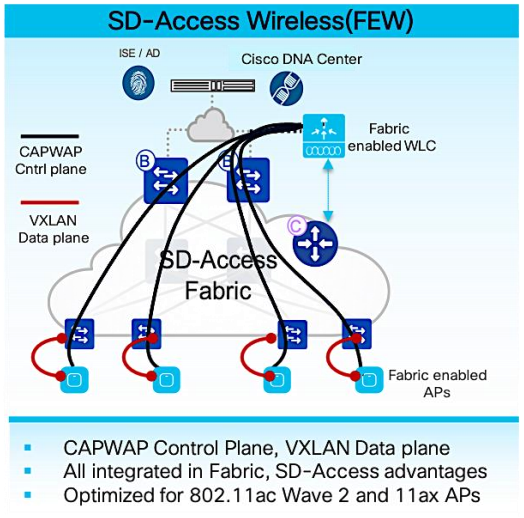
- VSS/SVL/VPC/Stack is the preferred topology
- Management IP address in Global Routing Table
- Specific route to advertise WLC’s IP in the underlay
- WLC can talk to only #2 Enterprise CP nodes

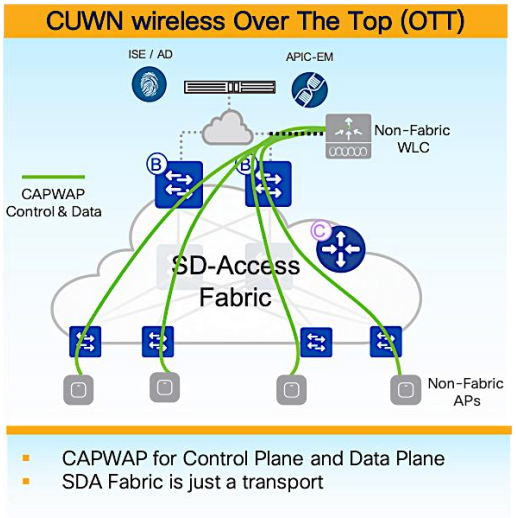
Access Points connect to EN/EX

- APs reside in INFRA_VN (GRT) and form CAPWAP connection to WLC. No need for VRF leaking
- APs are connected in Local mode

Cisco SD-Access overlay
Wireless design options

Deployment types	: FEW , OTT , Mixed Mode
Supported Platforms	: C9800, eWLC,3504,5520,8540
AP Mode	: Local, Flexconnect*
Control-Plane Node Support	: AireOS, C9800





Cisco SD-Access overlay
Which controller to choose?

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

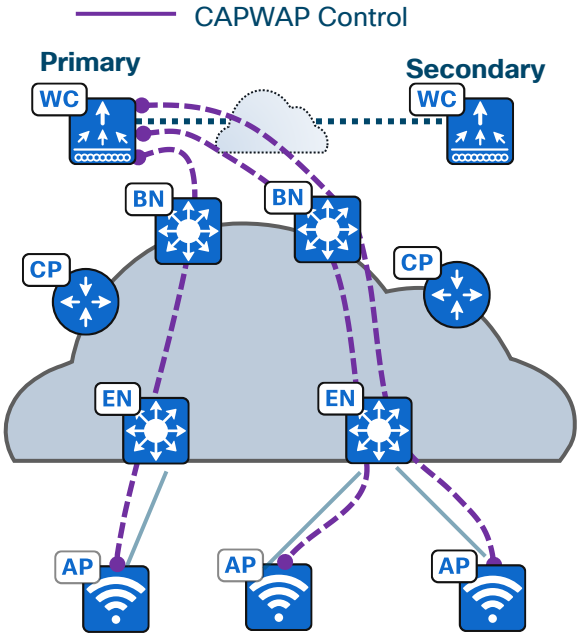
Platform	Number of APs	Number of Clients
Catalyst 9200/L	Not Supported	Not Supported
Catalyst 9300 L	50	1000
Catalyst 9300 (Single Switch)	200	4000
Catalyst 9300 (Switch Stack)	200	4000
Catalyst 9400/9500/9500H	200	4000

Cisco SD-Access overlay

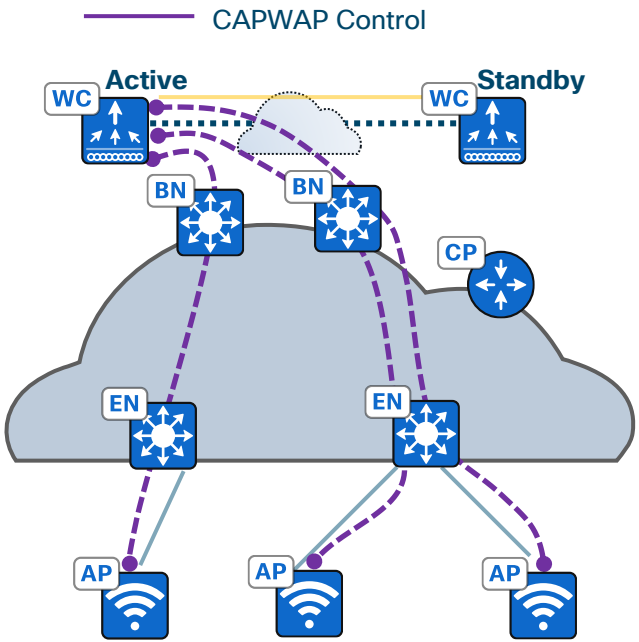
Fabric enabled wireless– N+1 HA vs SSO

Redundancy Comparison

Stateless Redundancy with N+1 HA



Stateful Redundancy with SSO



Starting Catalyst Center release 2.1.2.0

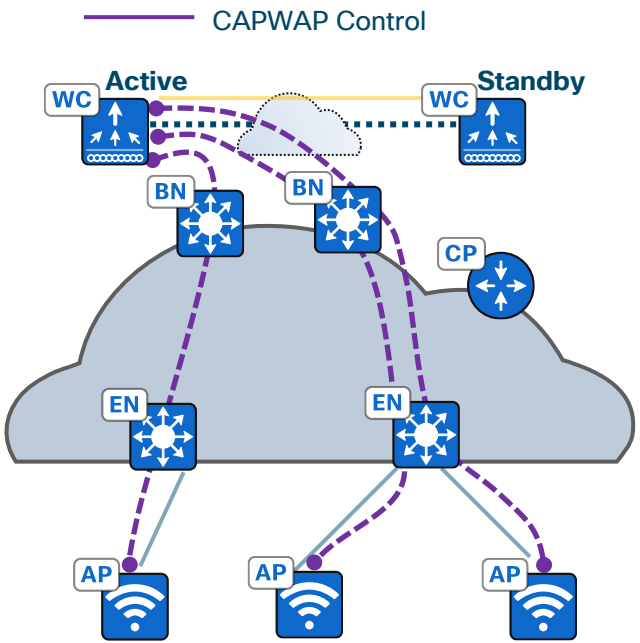
Cisco SD-Access overlay
Fabric enabled wireless– N+1 HA vs SSO

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



cisco Live!

Starting Catalyst Center release 2.1.2.0

Cisco SD-Access overlay

Fabric enabled wireless– N+1 HA vs SSO

Redundancy Comparison

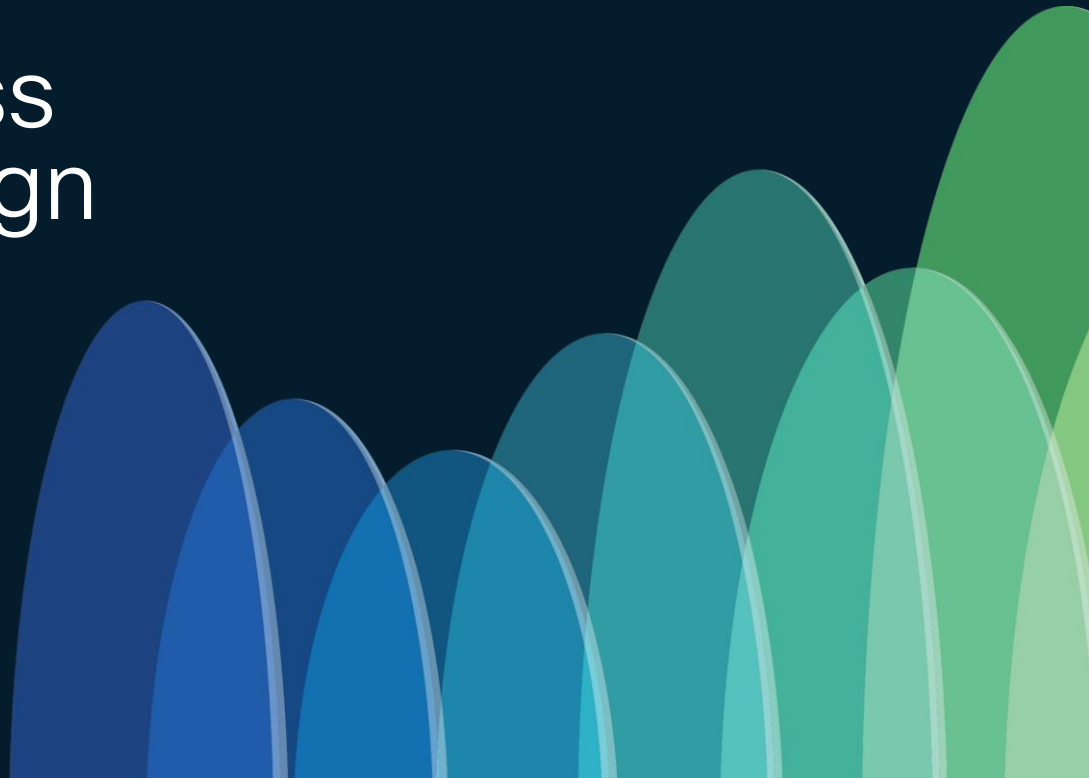
Stateless Redundancy with N+1 HA

- 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

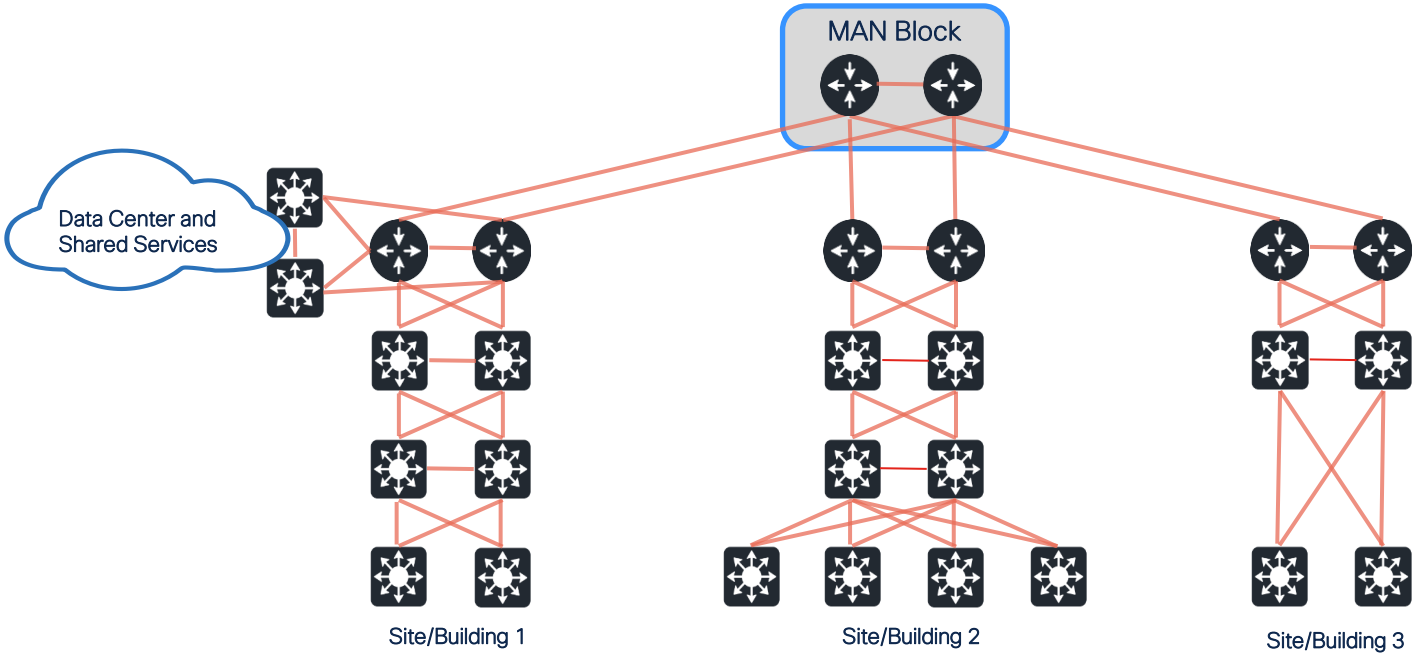
- WLC SSO is seen as a single entity.
- Only active WLC communicates with the control plane nodes.
- APs and clients stay connected during a failover event.
- In a failover event, the new Active WLC will bulk update the control plane node regarding the wireless hosts.
- For Embedded Wireless on Catalyst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

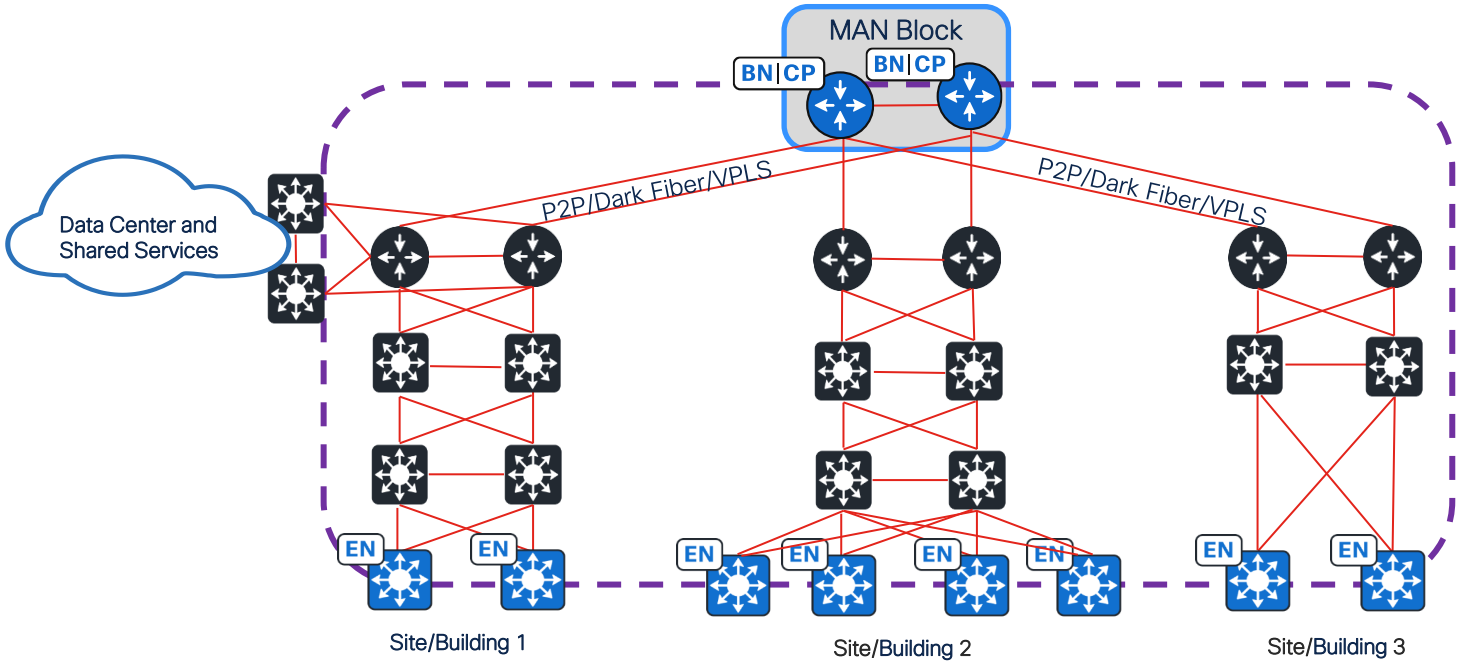


cisco Live!

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

Starting Catalyst Center release : 2.2.3.x

Use Case

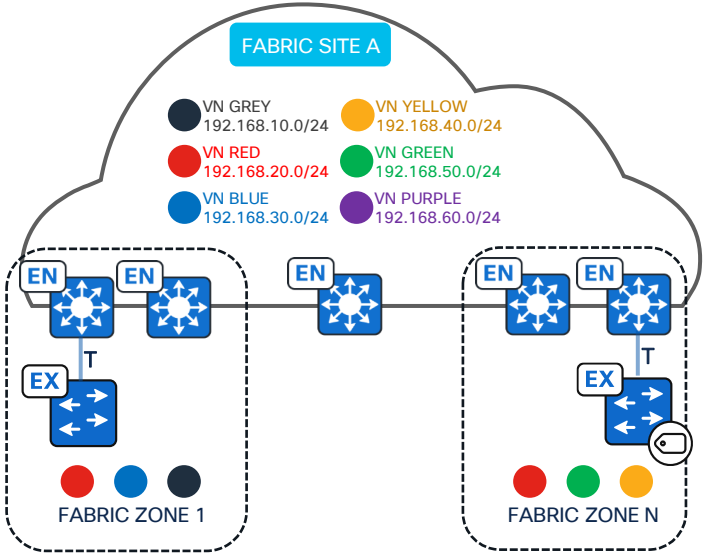
- Before 2.2.3.x, the provisioning scope of an IP Pool was the whole fabric site. For security and/or better fabric site scaling, some customers require granular control of IP Pool provisioning scope.

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.

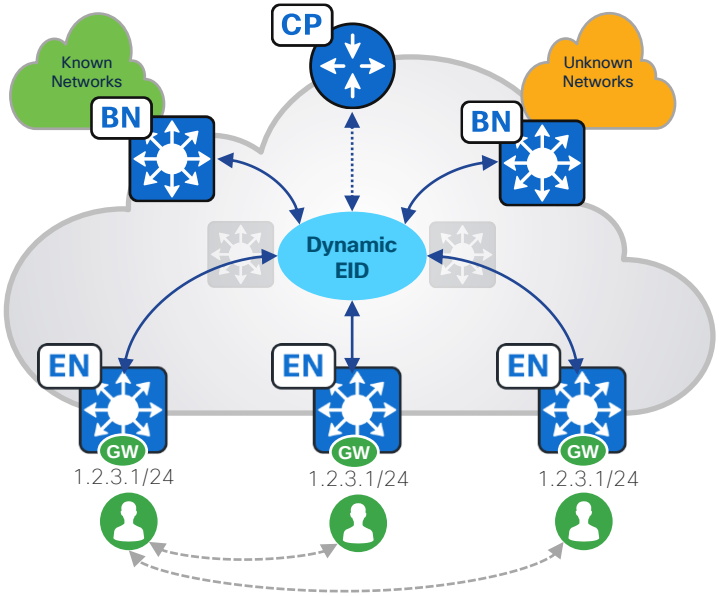
Considerations

- 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.

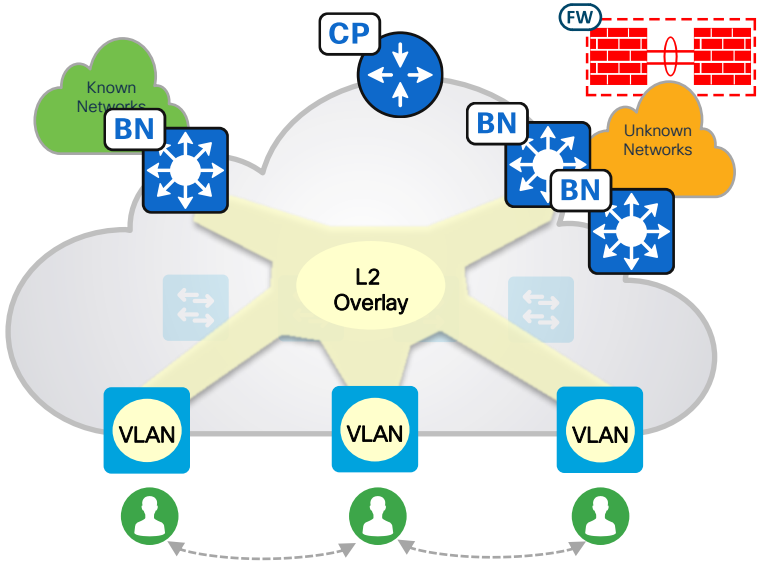


SD-Access Fabric
L3/L2 overlays

Layer 3 Overlay
Stretched Subnets

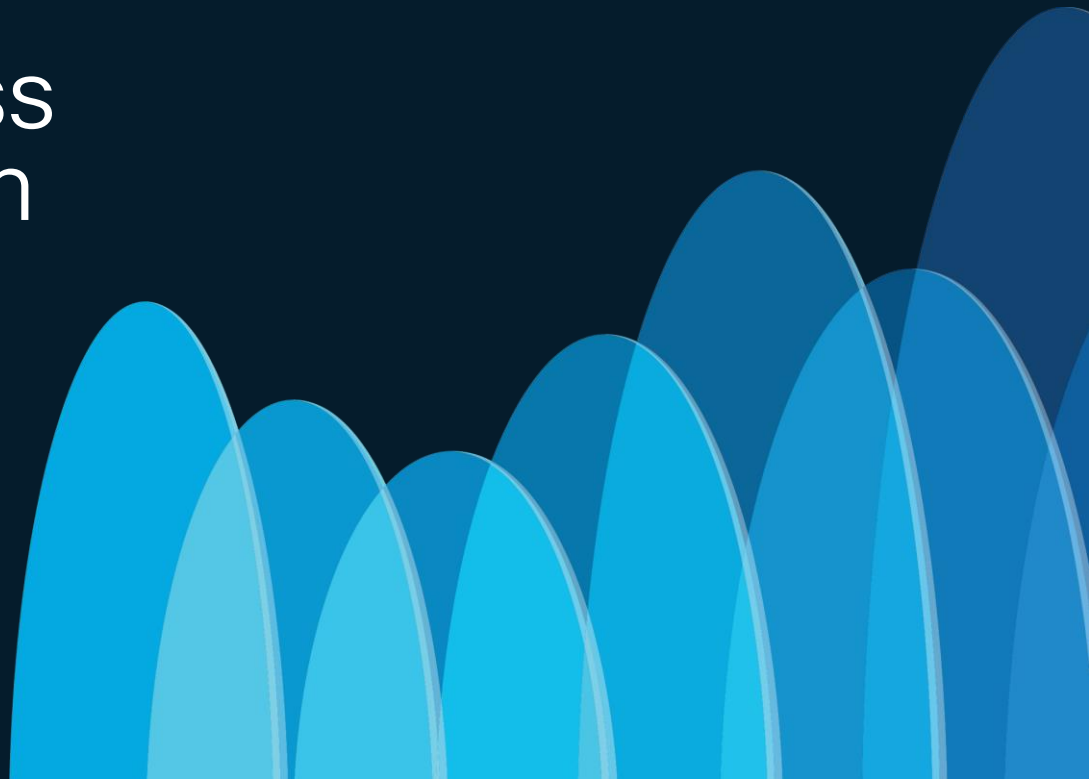


Layer 2 Overlay / GW outside Fabric



- L2 Loop during Handoff?
- Vlan based L2 VNI Pool Size?

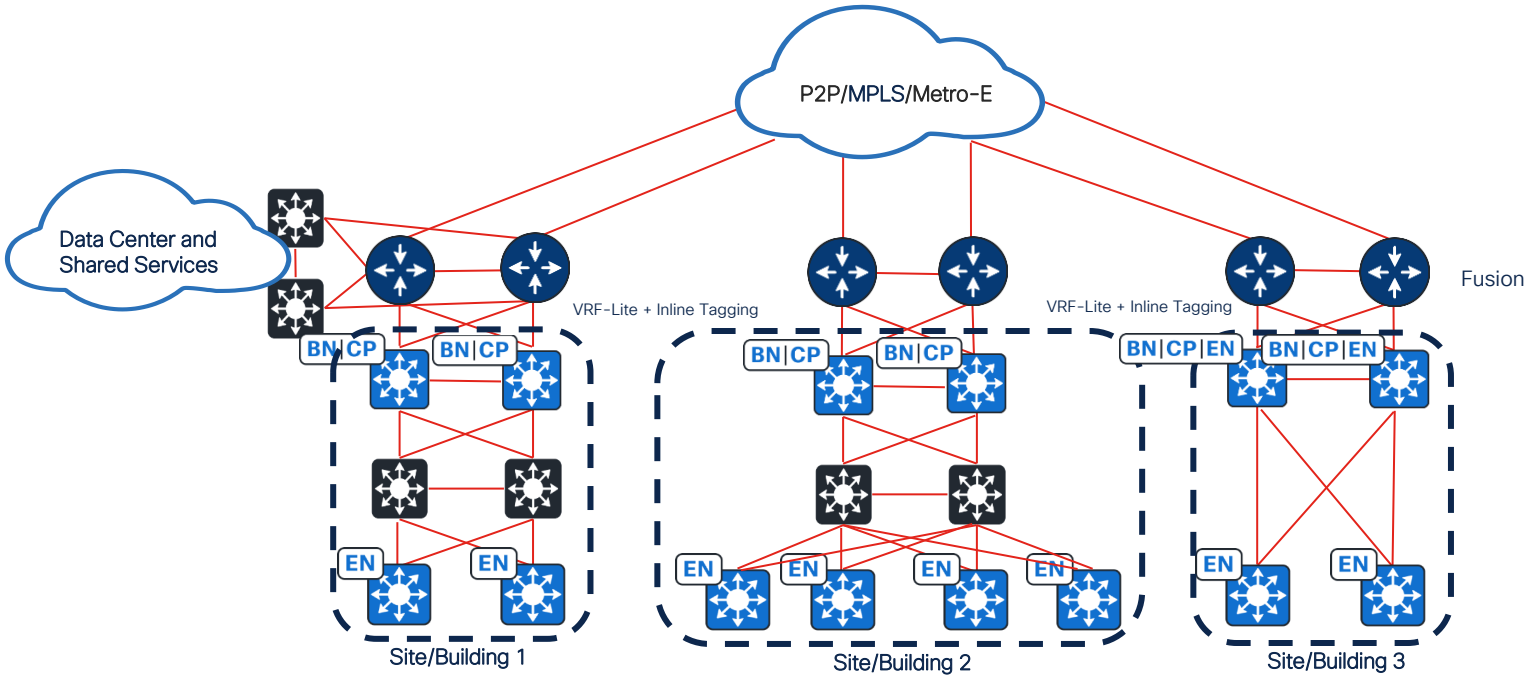
Cisco SD-Access Multi-Site Design Options



cisco Live!

Cisco SD-Access multi-site

Multisite architecture with IP TRANSIT



Cisco SD-Access Multi-Site

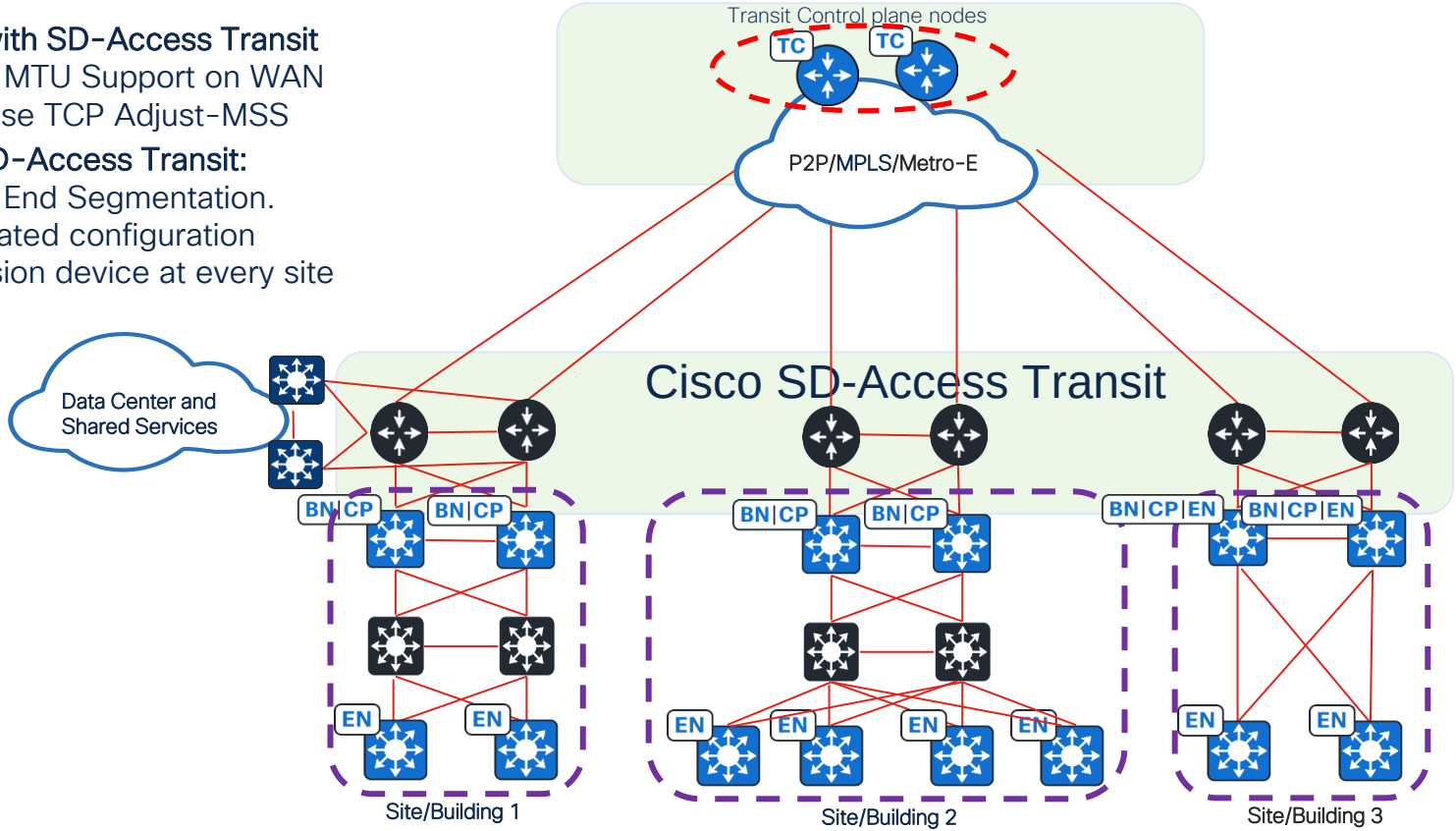
Multisite Architecture with SD-Access Transit

Pre-Requisite with SD-Access Transit

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

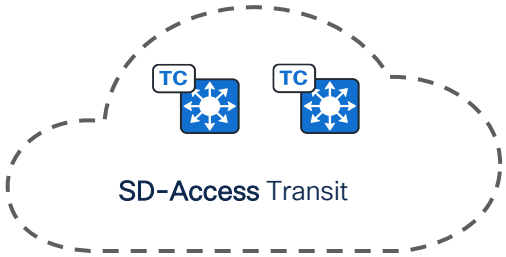
Benefits with SD-Access Transit:

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



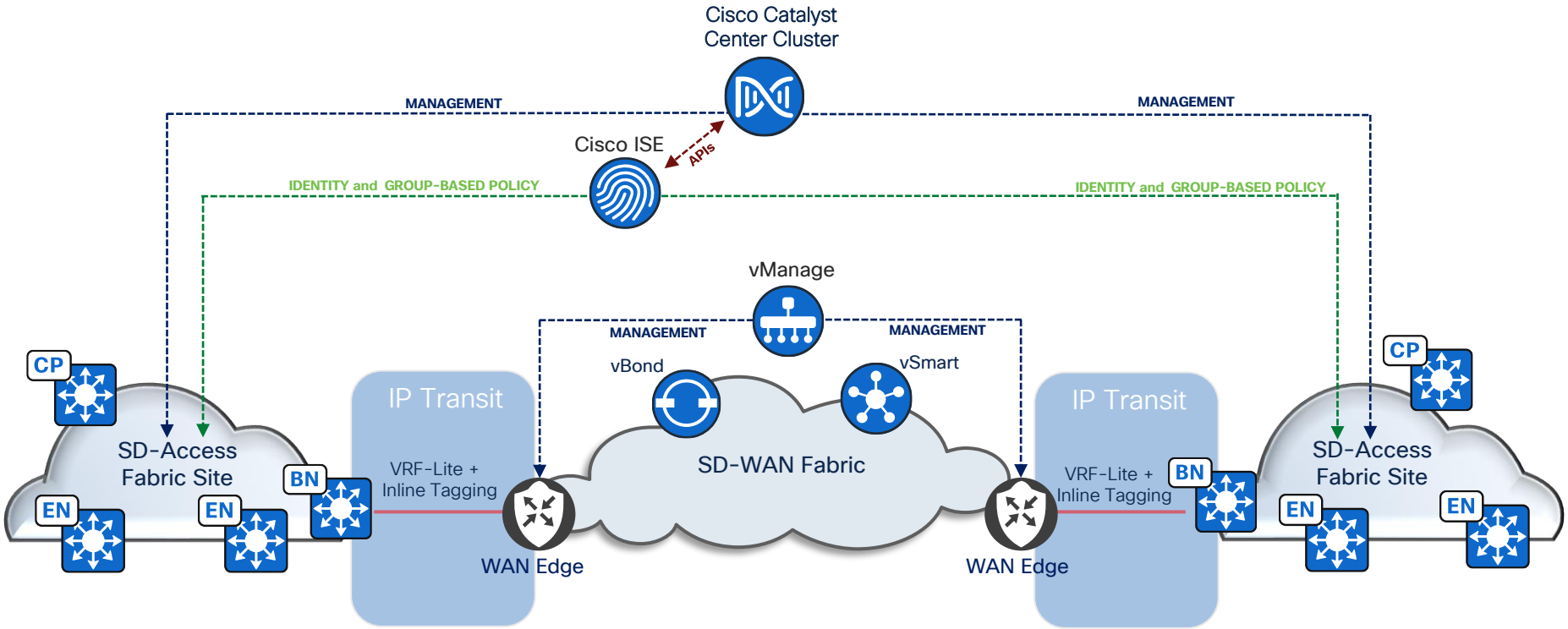
Cisco SD-Access multi-site

Multisite deployment with SD-Access transit



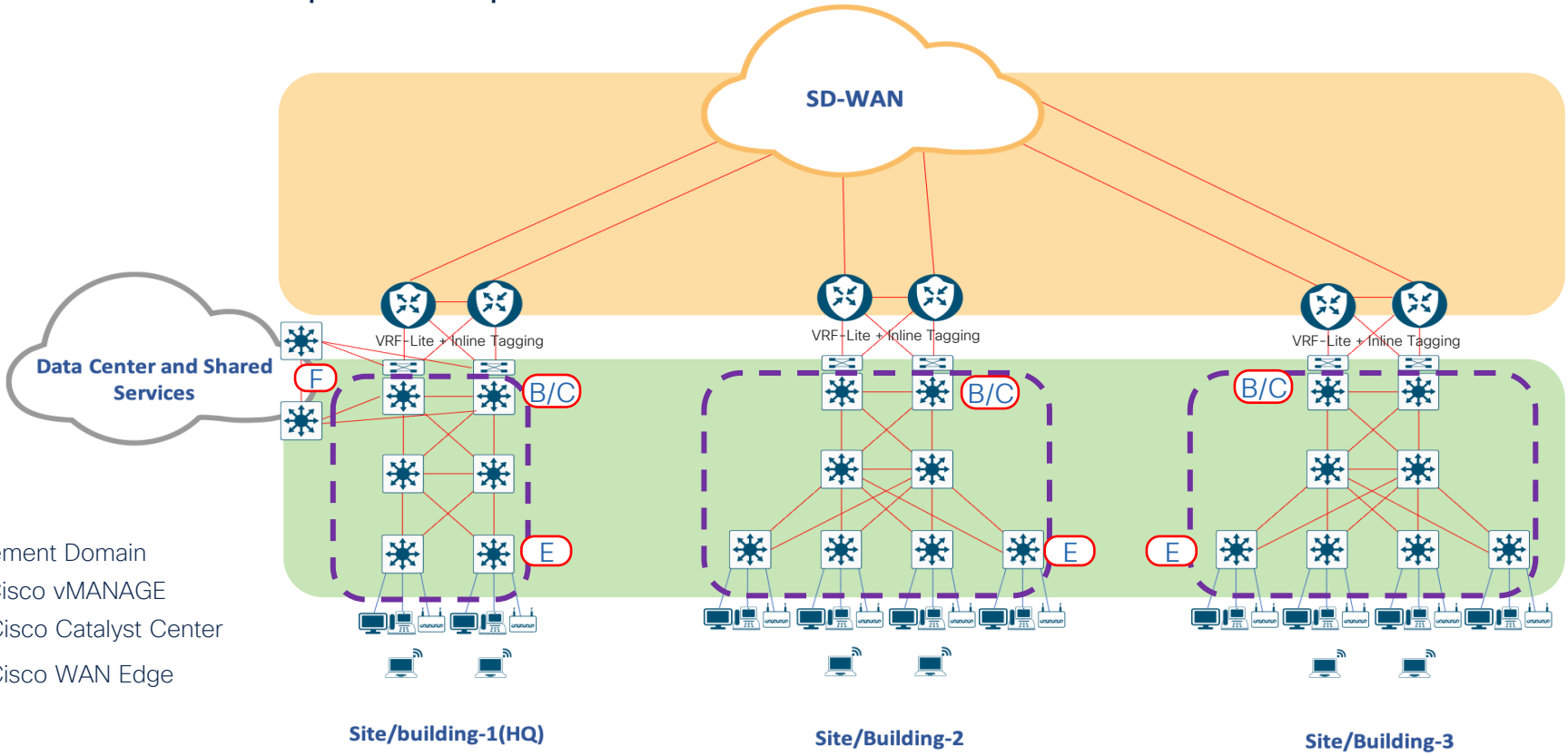
- Transit Control Plane nodes are **dedicated devices** with IP reachability to every fabric site's Border nodes
- Transit Control Plane nodes is **not required to be in data forwarding path**
- Transit Control Plane nodes maintains aggregate prefixes of all Fabric sites
- Fabric site Border node should 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**

Cisco SD-Access Multi-Site
SD-WAN Transport/Independent Domains



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

Cisco SD-Access Multi-Site
SD-WAN Transport/Independent Domains

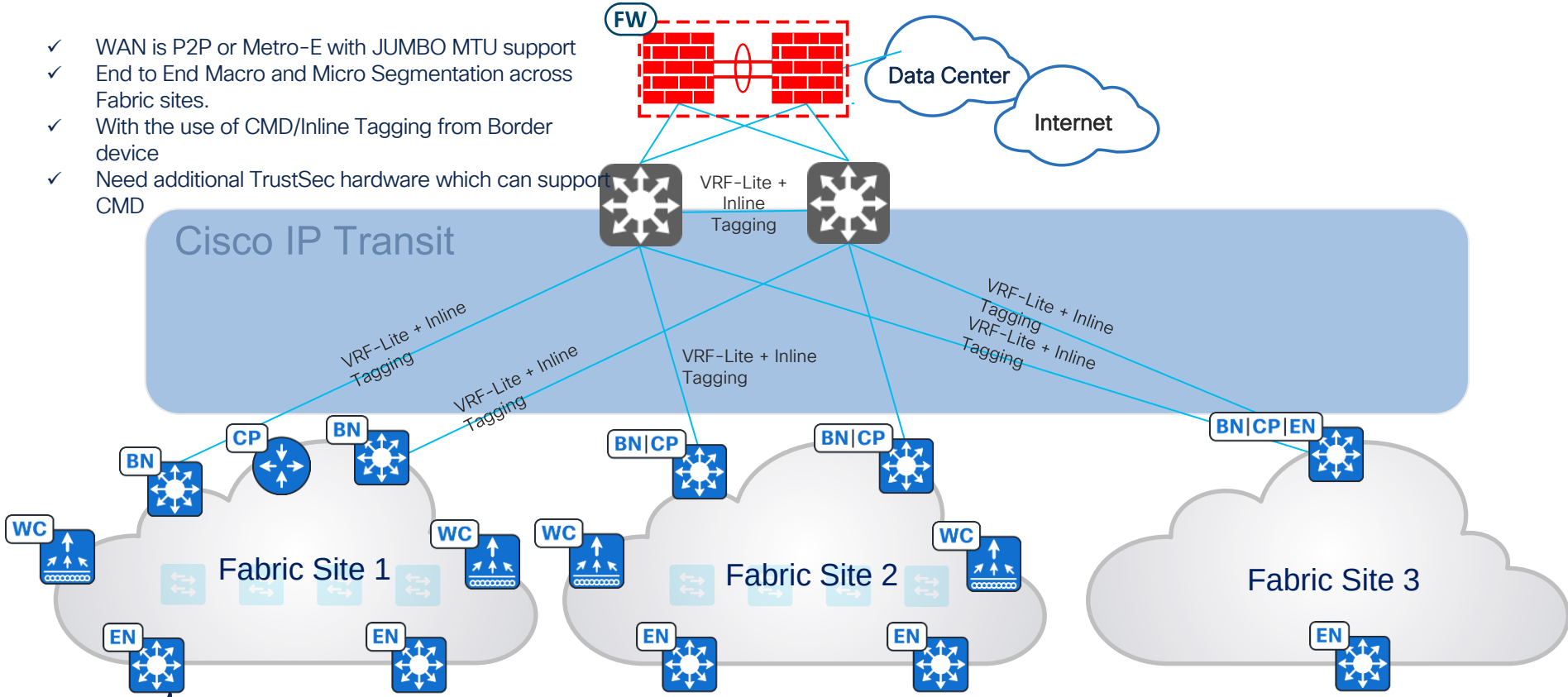


Management Domain
- Cisco vMANAGE
- Cisco Catalyst Center
- Cisco WAN Edge

Cisco SD-Access Multi-Site

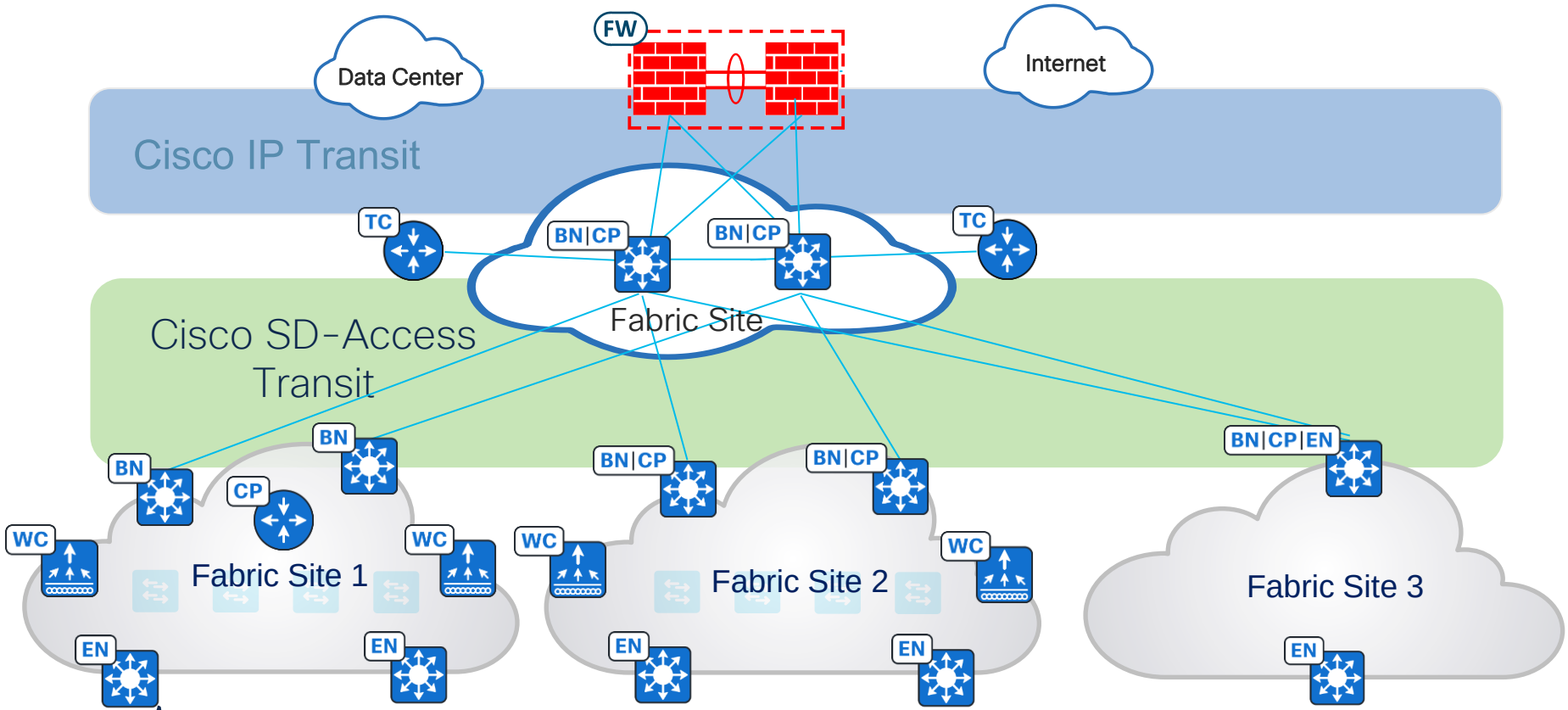
Cisco IP Transit Design 1 – IP Transit with End to End Segmentation

- ✓ 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



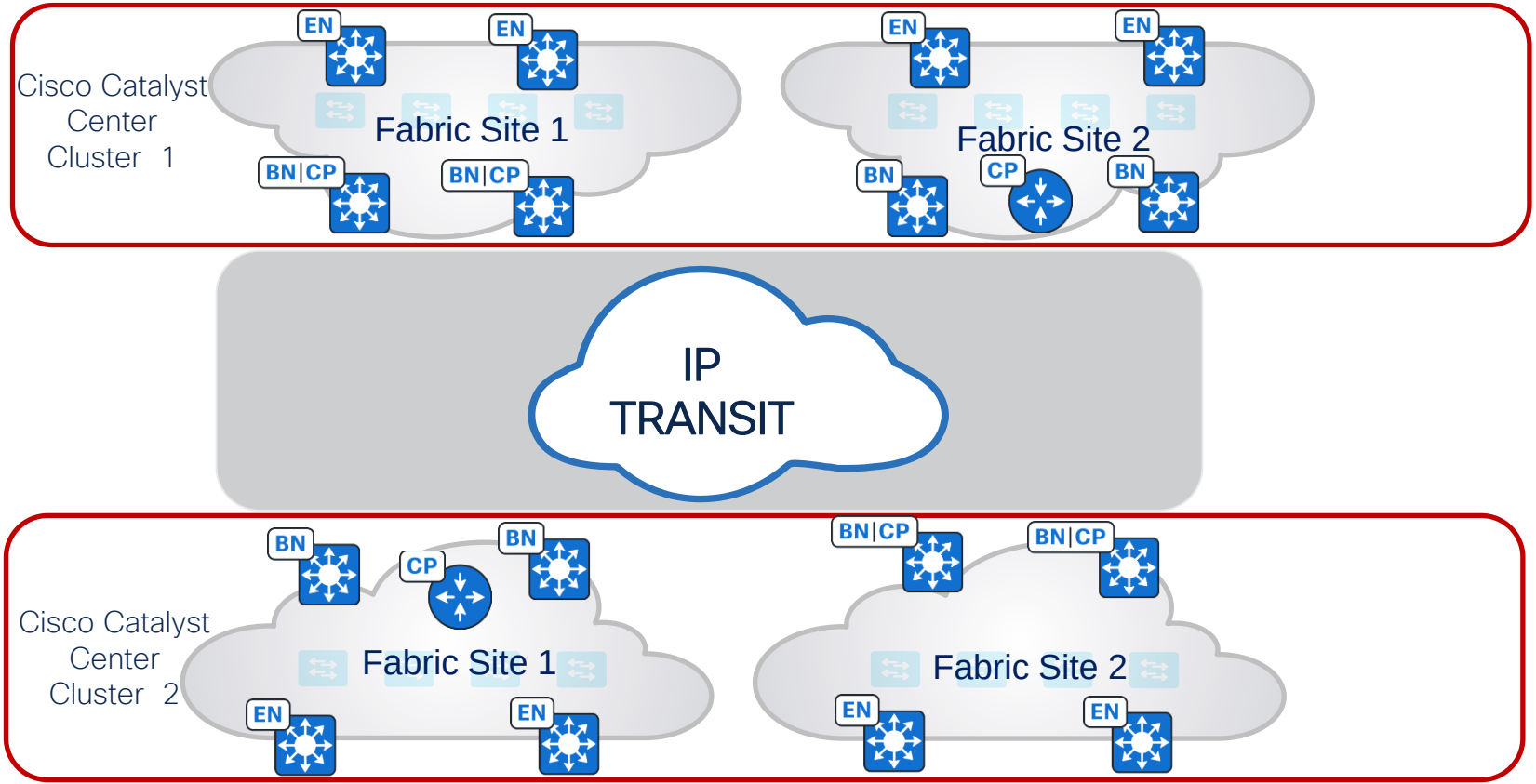
Cisco SD-Access Multi-Site

Cisco SD-Access Transit Design 1



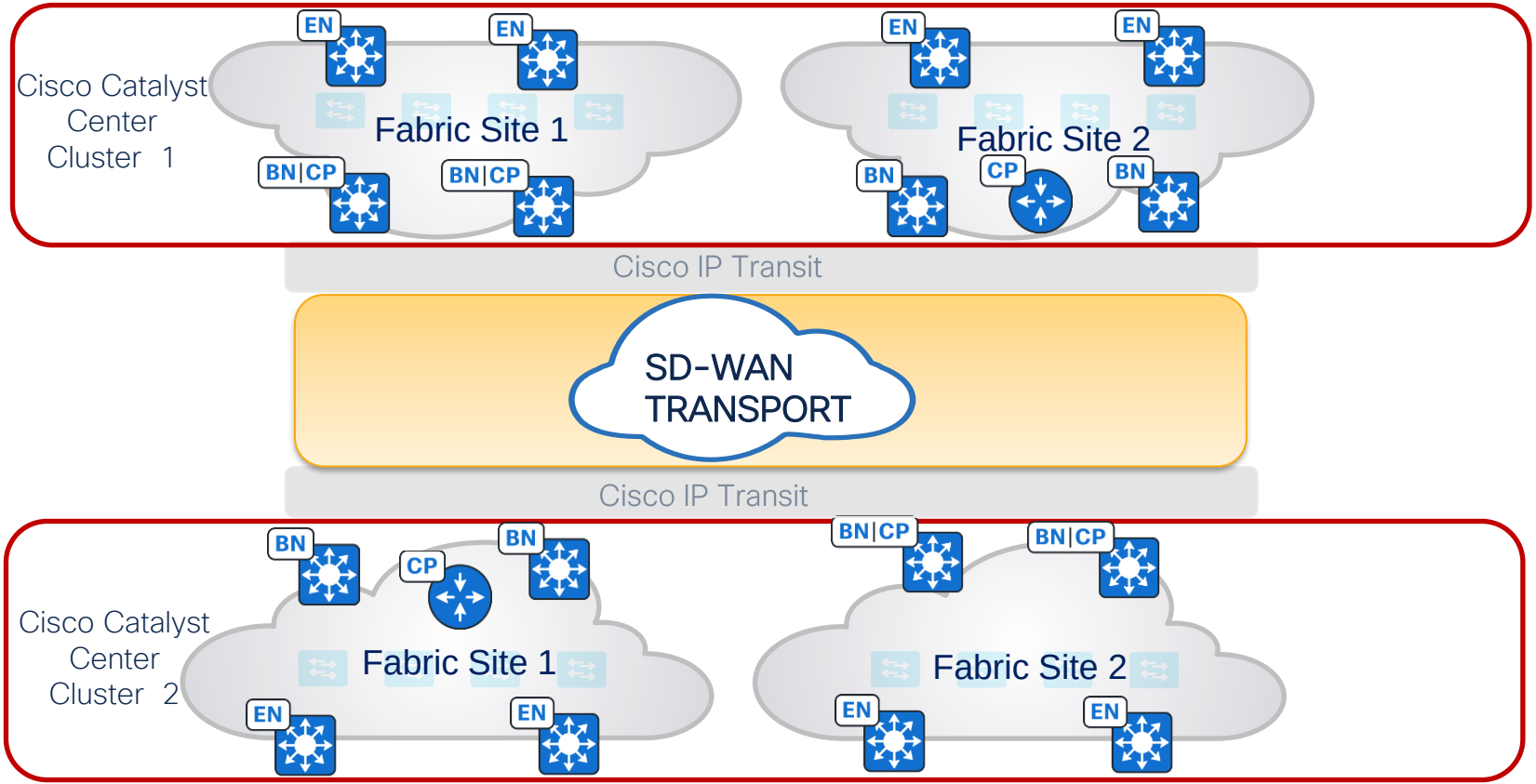
Cisco SD-Access Multi-Site

Transit design across Cisco Catalyst Center clusters



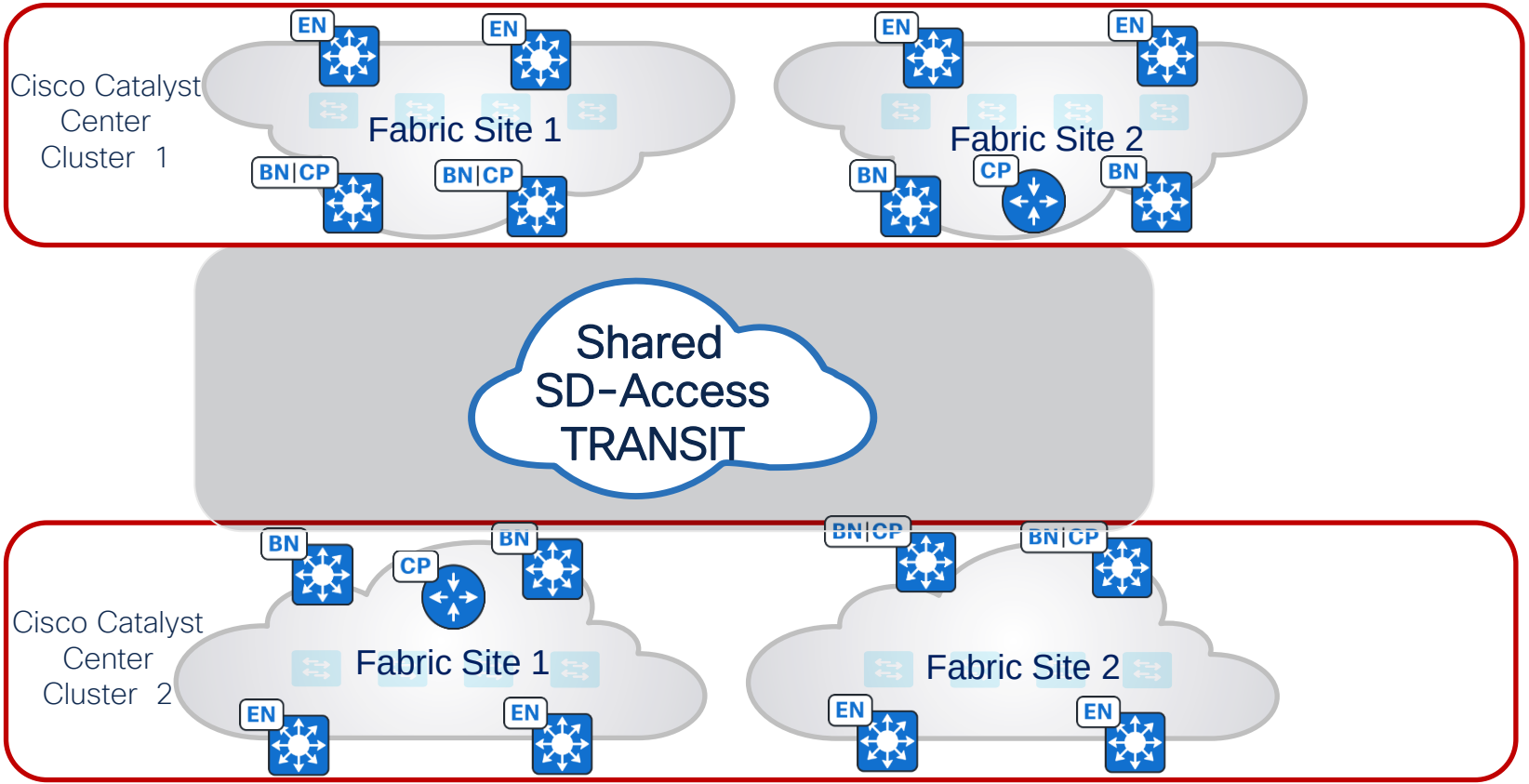
Cisco SD-Access Multi-Site

Transit design across Cisco Catalyst Center clusters



Cisco SD-Access Multi-Site

Transit design across Cisco Catalyst Center clusters



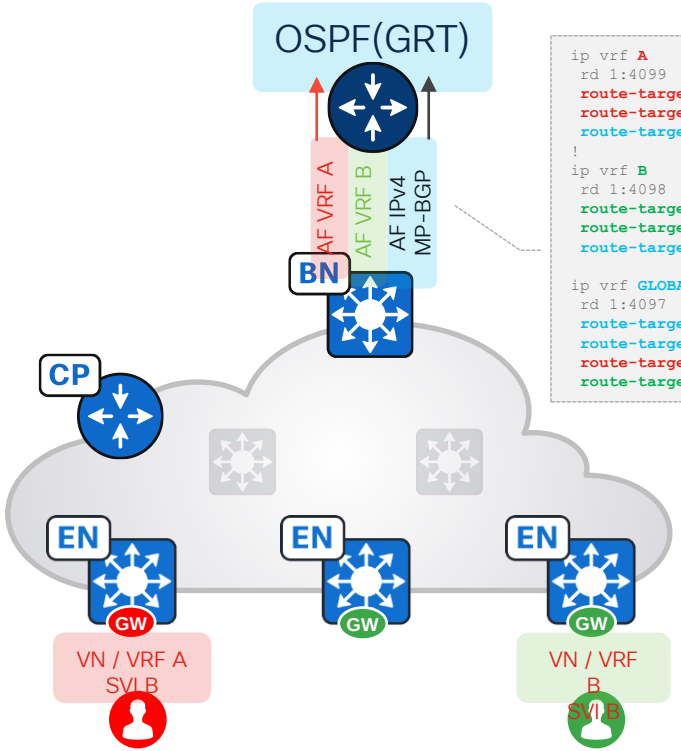
Cisco SD-Access Services

cisco Live!

Cisco SD-Access services

Traditional route leaking vs LISP extranet

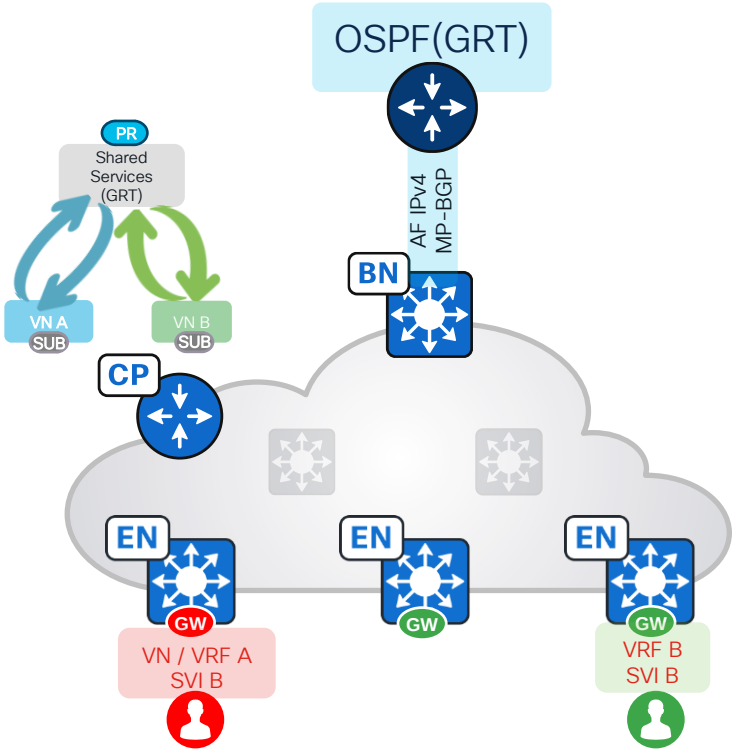
Traditional Route Leaking




```
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 services
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**

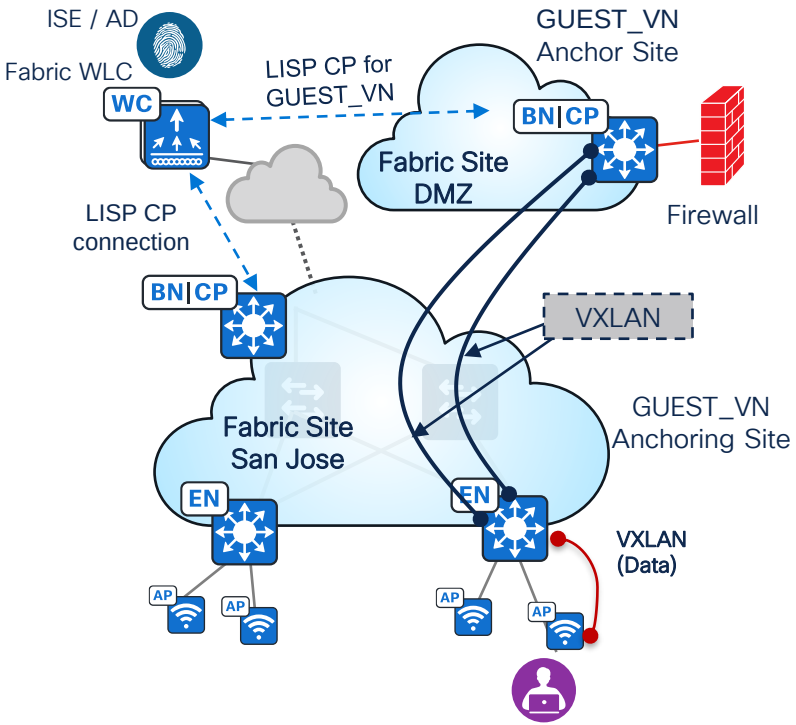
Source	Receiver	RP Placement
Fabric	Fabric	Borders
Outside Fabric	In Fabric	Borders/External
Outside Fabric	Multi-Site Fabric	External

Cisco SD-Access services
Multicast forwarding options

Head-End Replication	Native Multicast
No Underlay Multicast(uses Overlay only)	Underlay Multicast required
Replication Load(CPU & Bandwidth) on FHR	Reduces replication Load on FHR
Deployments where multicast cannot be enabled in underlay	Preferred option due to efficiency and reduction of load on FHR
V4 and V6 support	No V6 support

Cisco SD-Access services

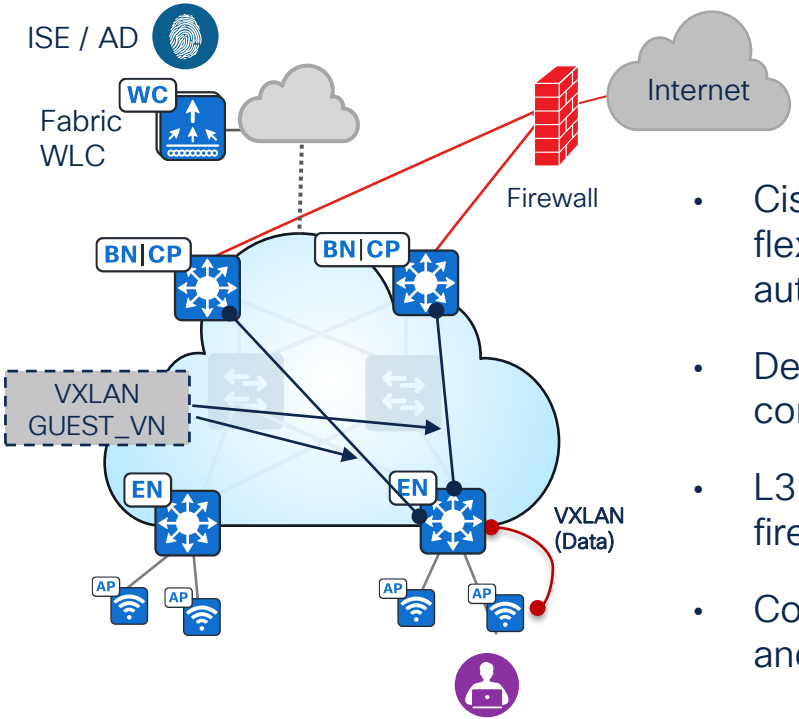
Wireless guest design – Dedicated Virtual Network with MSRB



- 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 SD-Access services

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

As of Catalyst Center release 2.3.7.5

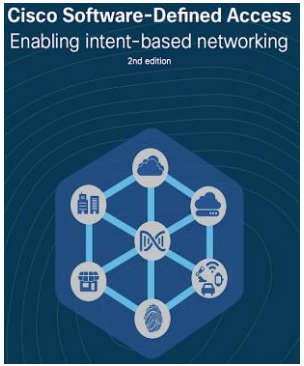
Cisco SD-Access
Unsupported Designs/options

- MPLS Termination on Border Node
- MACsec between Switch to Host
- PTP packet processing on Fabric Nodes
- SSO not support across eWC controllers.
- ISSU support on Fabric nodes
- Fabric Site/Node move from one Catalyst Center Cluster to another Cluster.
- Dual homing endpoint to multiple Fabric Edge
- Day N Fabric role addition/deletion not supported
- Changing Subnets/Subnet size once deployed

Cisco SD-Access collaterals

Cisco Software-Defined Access for Industry Verticals

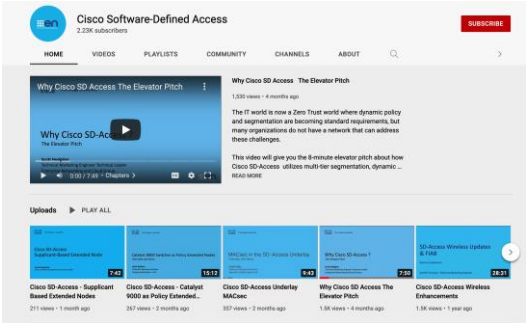
Cisco Software-Defined Access
Enabling intent-based networking



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 Catalyst Center to ISE

Cisco SD-Access Design Tool

EN&C Validated Designs

The Latest SD-Access Guides

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

Continue your education

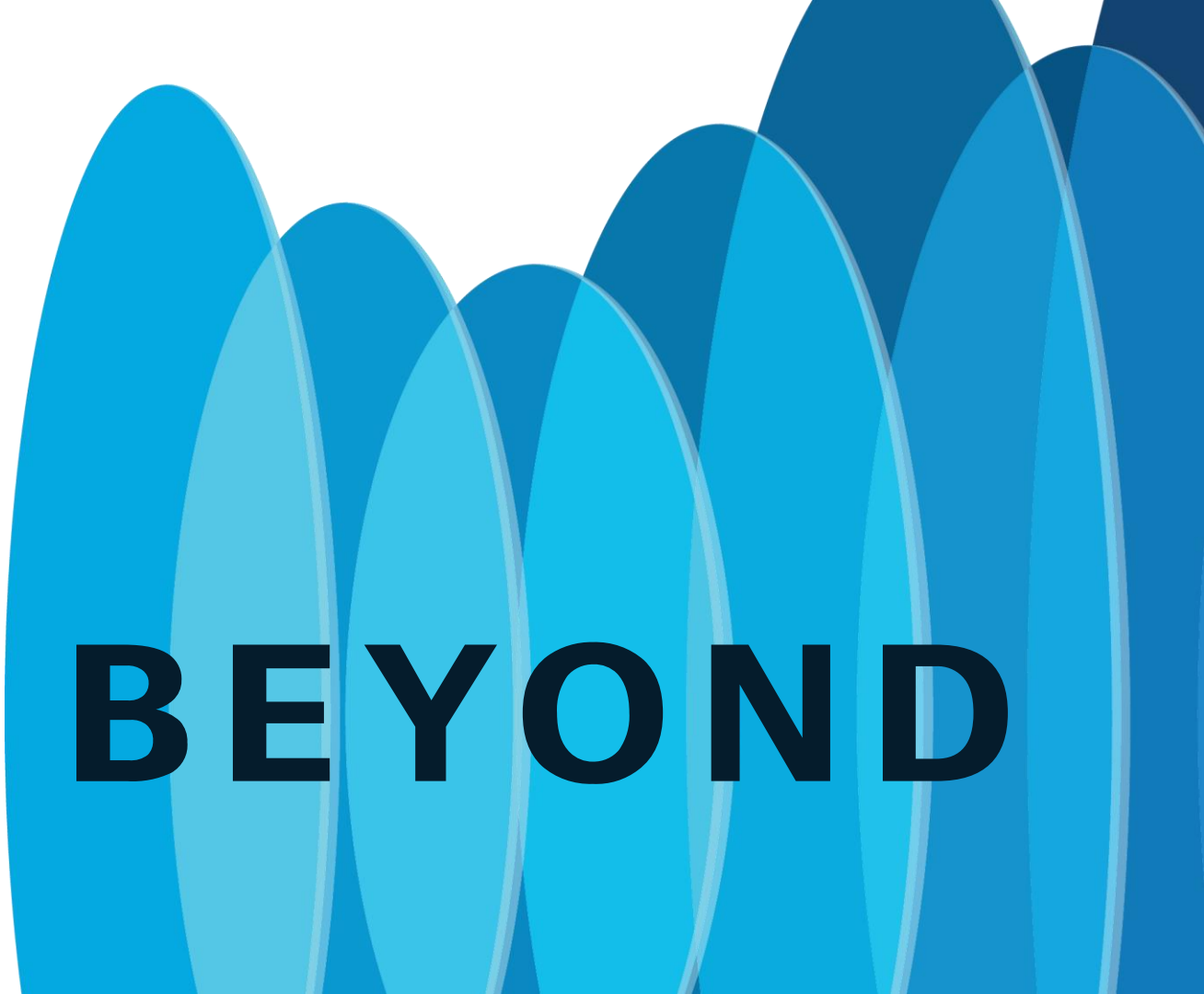
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.


cisco
Thank you
cisco Live!

Thank you

cisco Live!

cisco Live!



GO BEYOND