

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



What's New in SD-Access?

Mahesh Nagireddy
Technical Marketing Engineering, Technical Leader
CCIE R&S
BRKENS-2566

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

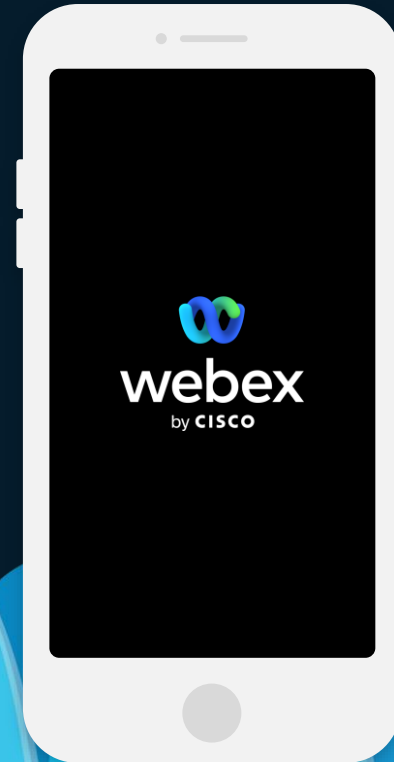
How

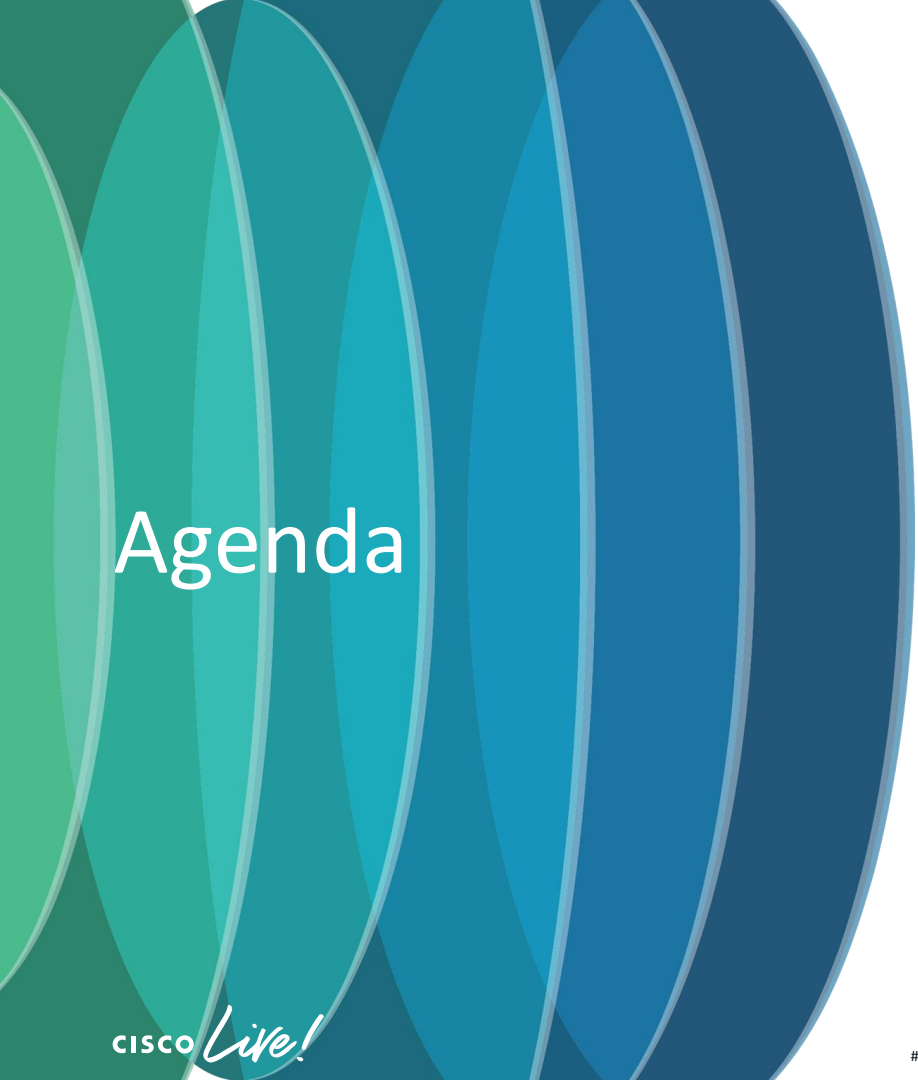
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2566>





Agenda

Cisco Catalyst Center (formerly Cisco DNA Center)

- Introduction
- Management Plane Enhancements
- Lan Automation
- Default Deny
- ISSU
- Mesh Support – 2.3.7.3

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

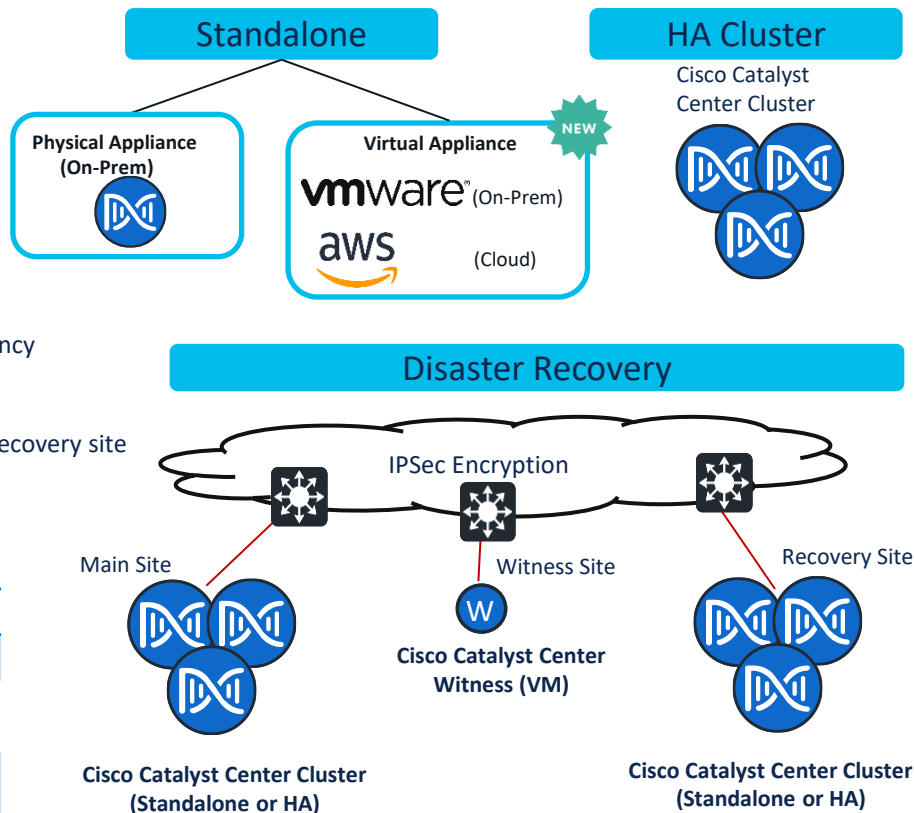
	High Availability	Disaster Recovery
Failure Detection time	5 minutes	3 minutes
Time taken to failover on failure detection	7-13 minutes	15-30 minutes
Failover time behavior	Service down up to 7 minutes	Service down up to 30 minutes

Failback

Automatic

Manual

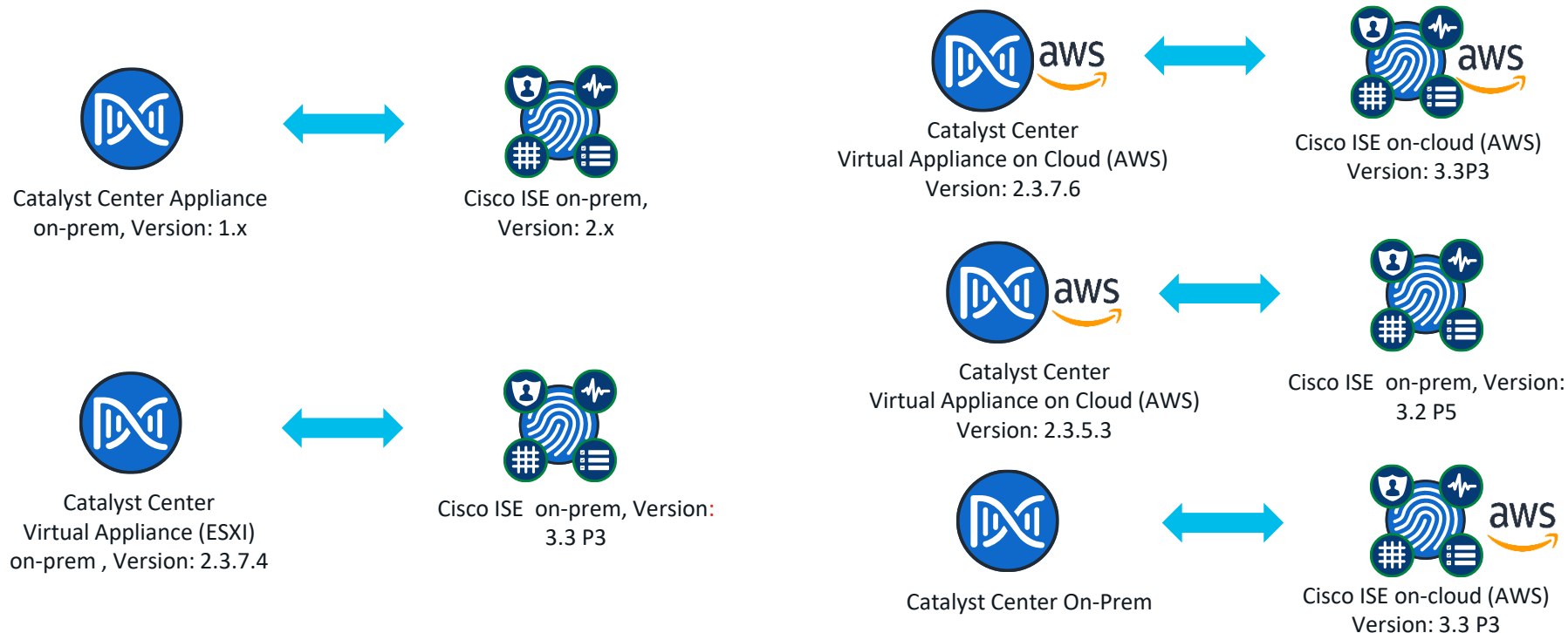
CISCO *Live!*



* - DN-SW-APL

Cisco SD-Access

On-Prem and Cloud supported models



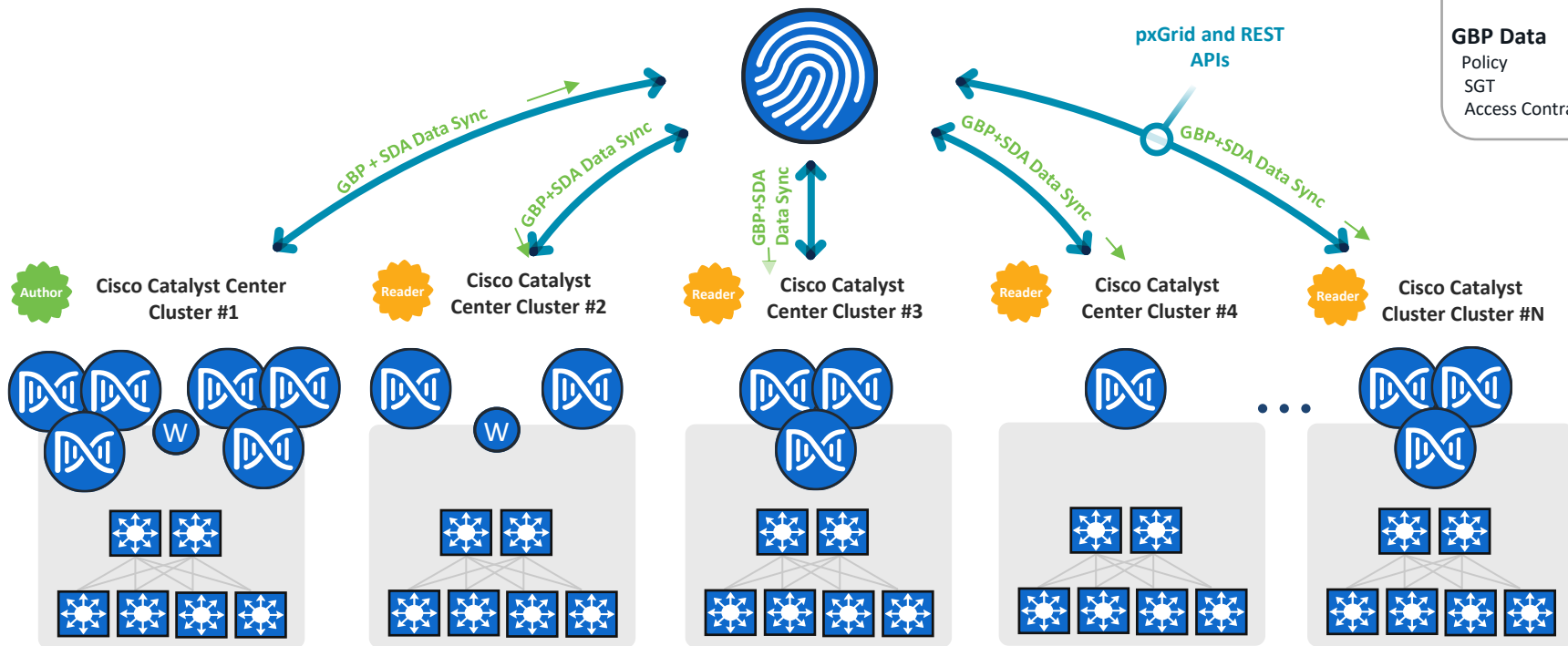
Multiple Catalyst Center Feature supported on all above options

Integrating Cisco Catalyst Center with ISE

Multiple Cisco Catalyst Center Solution Overview

N=5 starting
Catalyst Center: 2.2.3.x

Cisco ISE Deployment (Cluster)



SD-Access Data

Virtual Network
Extranet Policy

GBP Data

Policy
SGT
Access Contract

Intent-based Network Infrastructure

CISCO *Live!*

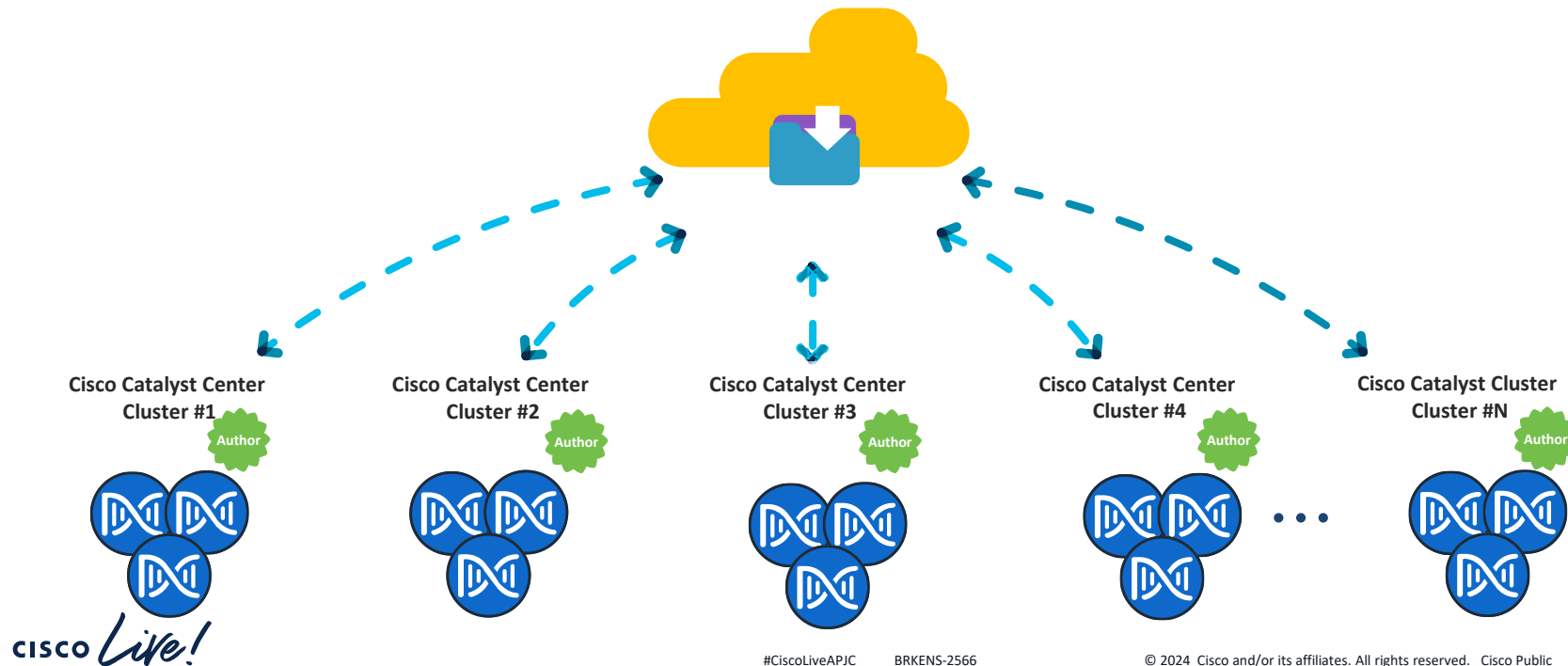
Multiple Cisco Catalyst Center

Multiple Cisco Catalyst Center Package and Installation

Package required if
Catalyst Center release < 2.3.6.x
Cisco ISE release < 3.2

Connect with your Cisco Sales Representative or Channel Partner for:

- High-Level Design review
- Multiple Cisco Catalyst Center Package release



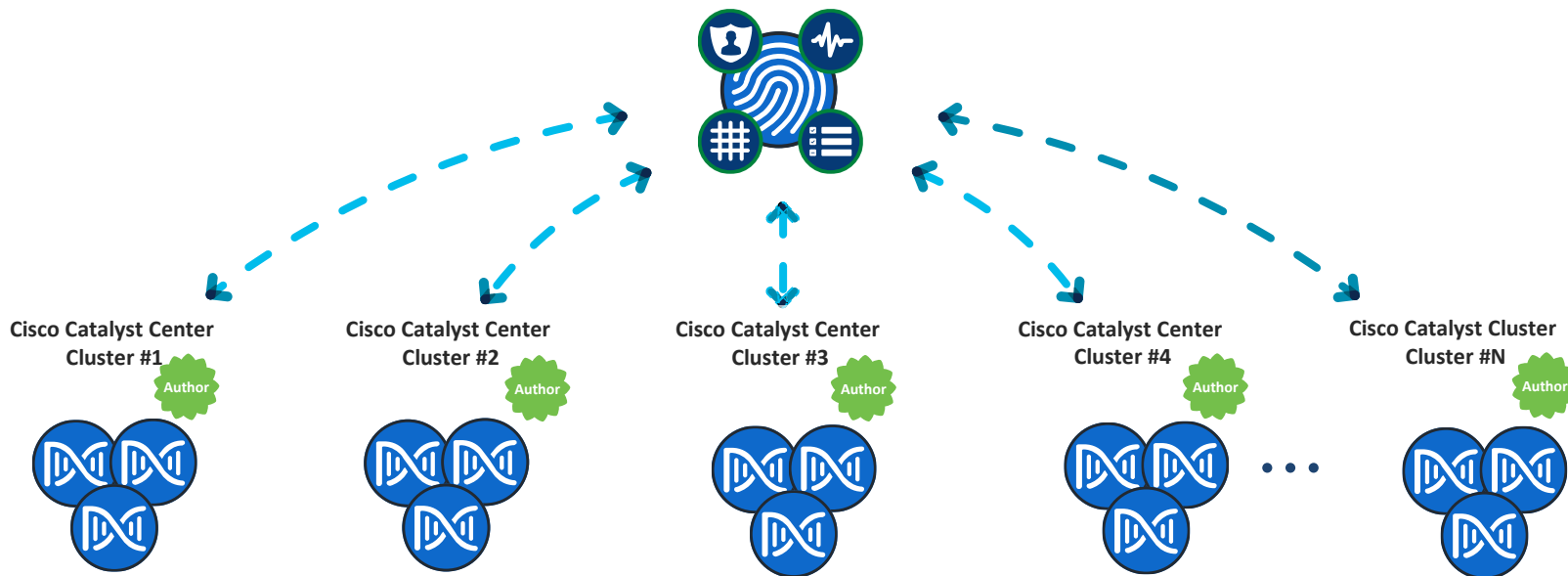
Multiple Cisco Catalyst Center

Multiple Cisco Catalyst Center Enhancements(Package part of ISO)

Max Cluster : 5
Catalyst Center : >2.3.6.x(LA+)
Cisco ISE. : >3.2

Connect with your Cisco Sales Representative or Channel Partner for:

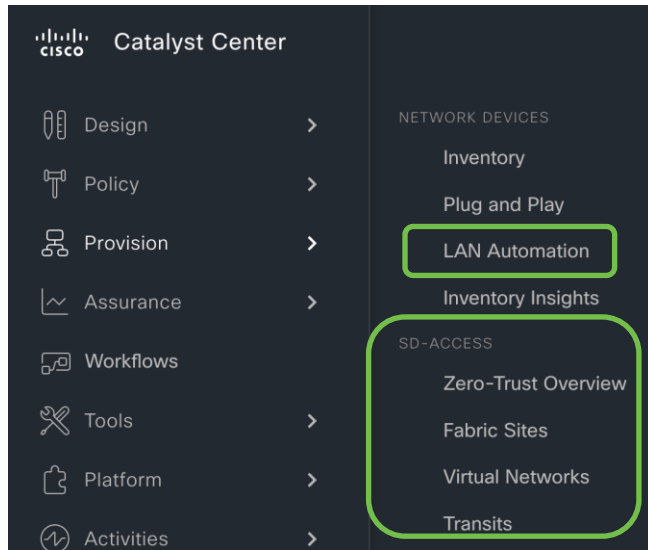
- **High-Level Design review**



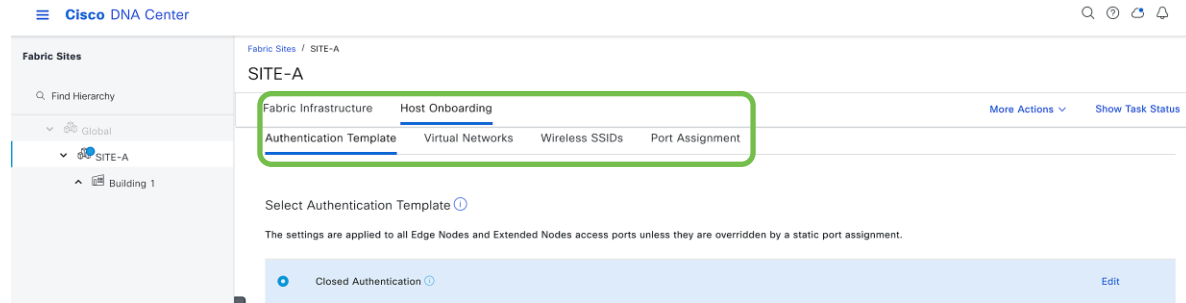
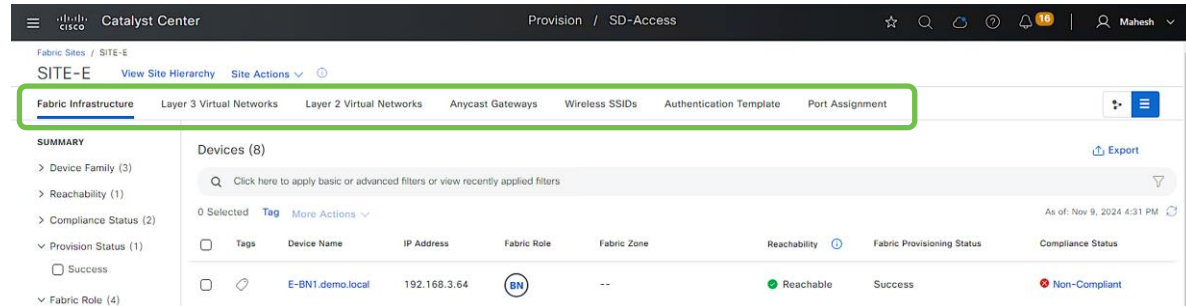
Cisco SD-Access

UI/UX Enhancements

Direct Navigation to SD-Access Building Blocks and Workflows



Original UI navigational architecture has been preserved and refreshed, nesting Virtual Networks and Anycast Gateways under Fabric Sites.



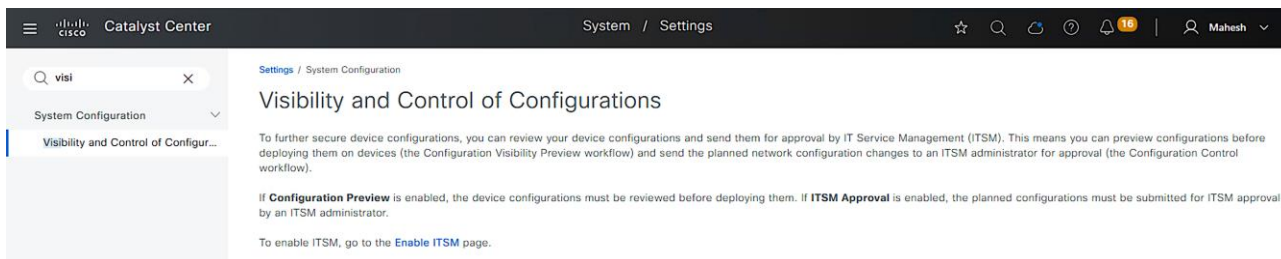
Visibility and Control of SD-Access

Details

- The configuration preview step will be made mandatory to display the CLI commands generated for all provisioning operations.
- The system provides visibility into the exact CLI commands being sent to devices for all operations.
- Generate device specific config preview rather than all config at once
- The control feature allows you to submit planned fabric configurations to ITSM for approval prior to deploying them on the fabric devices.

Considerations

- Visibility is supported from Cisco Catalyst Center 2.3.6.x and Control from 2.3.7.x release.
- New Visibility is enabled by default, but this can be disabled via a toggle
- There can only one active provisioning task.



Visibility and Control Demo



Visibility and Control of SD-Access ITSM Workflow

- The control feature allows you to submit planned fabric configurations to ITSM for approval prior to deploying them on the fabric devices.

Settings / System Configuration

Visibility and Control of Configurations

To further secure device configurations, you can review your device configurations and send them for approval by IT Service Management (ITSM). This means you can preview configurations before deploying them on devices (the Configuration Visibility Preview workflow) and send the planned network configuration changes to an ITSM administrator for approval (the Configuration Control workflow).

If **Configuration Preview** is enabled, the device configurations must be reviewed before deploying them. If **ITSM Approval** is enabled, the planned configurations must be submitted for ITSM approval by an ITSM administrator.

To enable ITSM, go to the **Enable ITSM** page.

☒ Configuration Preview

☒ ITSM Approval

Preview Configuration - Modifying Port Assignment for device(s) at Cisco-building-9

As of: Oct 4, 2023 4:54:43 PM [Refresh](#)

Status: ● Ready

If you do not wish to wait for this process to complete, you can leave this page at any time by clicking "Exit and Preview Later" button. The process will continue in the background and can be viewed in the **Activities > Work Items** window.

Search by device name: Device IP: 2.3.60.2 Site: Global/San Jose/Cisco-... [ⓘ](#)

Config Sourced From: All [⌵](#)

```
1 no macro auto trigger CISCO_CUSTOM_EVENT
2 no macro auto trigger CISCO_DMG_EVENT
3 no macro auto trigger CISCO_IPV6_EVENT
4 no macro auto trigger CISCO_LAST_RESORT_EVENT
5 no macro auto trigger CISCO_LIGHT_EVENT
6 no macro auto trigger CISCO_ML_VCF_EVENT
7 no macro auto trigger CISCO_PHONE_EVENT
8 no macro auto trigger CISCO_ROUTER_EVENT
9 no macro auto trigger CISCO_WIRELESS_AP_EVENT
10 interface GigabitEthernet1/0/17
11 no dot1x max-remote-req
12 no dot1x timeout tx-period
13 no source template DefaultNredDot1xClosedAuth
14 no swportport vlan 4005
15 no macro auto processing
16 access-session inherit disable outaocf
17 access-session inherit disable interface-template-sticky
18 swportport access vlan 4005
19 load-interval 30
20 exit
```

[ⓘ Generation Status Legend](#) [Exit and Preview Later](#) [Discard](#) [Submit for Approval](#)

Activities / Work Items

[Audit Logs](#) [Tasks](#) [Work Items](#)

SUMMARY

▼ Status (5)

- ☐ In Progress
- ☐ Failed
- ☐ Ready
- ☐ Discard Failed
- ☐ Resource Discard Failed

[Work Item](#)

Modifying Port Assignment for device(s) at Cisco-building-9

Oct 4, 2023 4:54 PM | Status: ● Ready | Submitted for ITSM approval

Submit for Approval

Clicking submit will submit all of the devices in this workflow for approval. Once approved the devices will deploy at the time specified below. Add notes to summarize the activity for the approval. You may want to schedule this during a maintenance window. Once approved, the progress and relevant information can be tracked from the **Activities > Tasks** window.

Task Name*
Modifying Port Assignment for device(s) at Cisco

Start Date/Time
Oct 4, 2023 [⌵](#)

Time Zone
America/Los_Angeles [⌵](#)

Notes*
port assignment

[Cancel](#) [Submit](#)

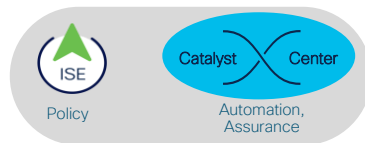
Device	Work Item Description	Type	Status	Planned start date	Planned end date	Assigned to	Updated
CISCO-BU-9-001	Modifying Port Assignment for device(s) at Cisco-building-9	Standard	Completed	2023-10-04 17:00:00	2023-10-04 17:00:00	maglev	2023-10-04 17:00:00
CISCO-BU-9-002	Group Resource Policy	Standard	Completed	2023-10-04 17:00:00	2023-10-04 17:00:00	maglev	2023-10-04 17:00:00
CISCO-BU-9-003	Group Resource Policy	Standard	Completed	2023-10-04 17:00:00	2023-10-04 17:00:00	maglev	2023-10-04 17:00:00
CISCO-BU-9-004	Group Resource Policy	Standard	Completed	2023-10-04 17:00:00	2023-10-04 17:00:00	maglev	2023-10-04 17:00:00
CISCO-BU-9-005	Group Resource Policy	Standard	Completed	2023-10-04 17:00:00	2023-10-04 17:00:00	maglev	2023-10-04 17:00:00
CISCO-BU-9-006	Group Resource Policy	Standard	Completed	2023-10-04 17:00:00	2023-10-04 17:00:00	maglev	2023-10-04 17:00:00
CISCO-BU-9-007	Group Resource Policy	Standard	Completed	2023-10-04 17:00:00	2023-10-04 17:00:00	maglev	2023-10-04 17:00:00
CISCO-BU-9-008	Group Resource Policy	Standard	Completed	2023-10-04 17:00:00	2023-10-04 17:00:00	maglev	2023-10-04 17:00:00
CISCO-BU-9-009	Group Resource Policy	Standard	Completed	2023-10-04 17:00:00	2023-10-04 17:00:00	maglev	2023-10-04 17:00:00
CISCO-BU-9-010	Group Resource Policy	Standard	Completed	2023-10-04 17:00:00	2023-10-04 17:00:00	maglev	2023-10-04 17:00:00

cisco Live!

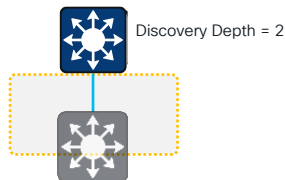
Lan Automation Enhancements

Lan Automation – Planning

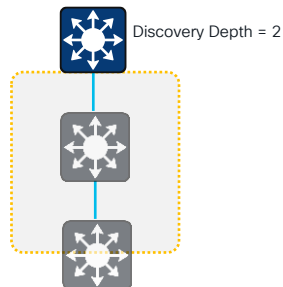
Automation Boundary



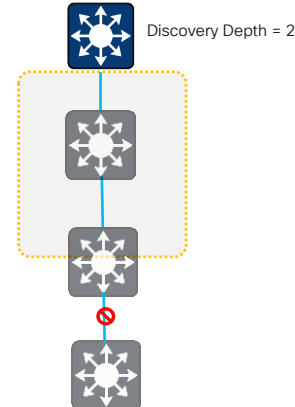
2 Tier – Collapsed Core Design



3 Tier – Campus Design

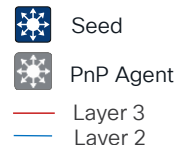


Extended Campus Design



Underlay Automation Boundary

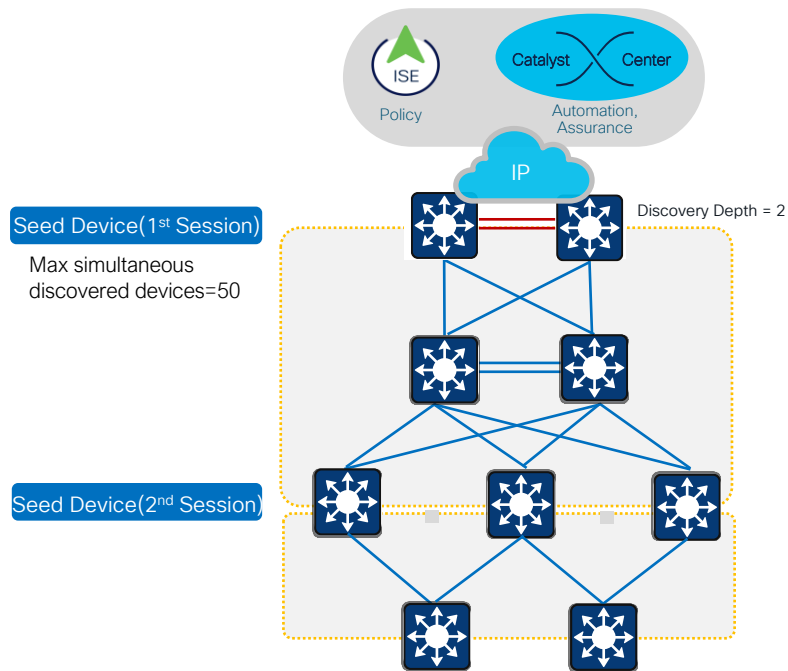
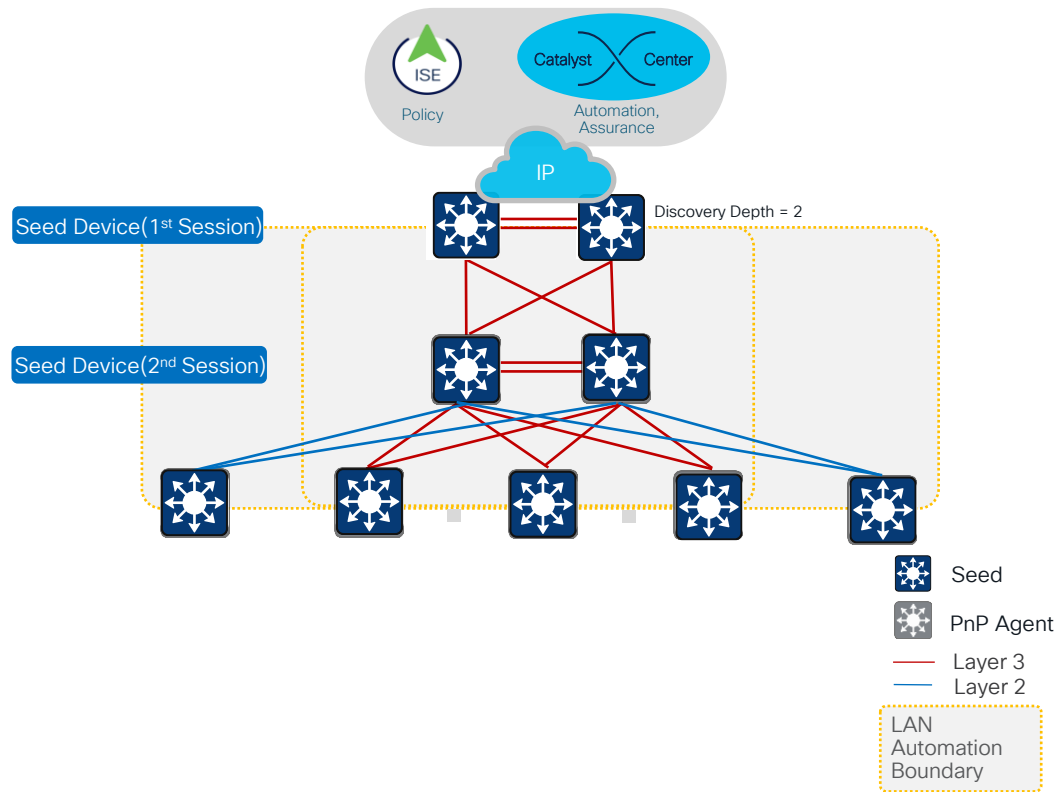
Maximum Automation boundary(Discovery Depth) from Seed Device: 1 to 5 (Default: 2)*
Supporting common hierarchical and structured Enterprise network designs



LAN
Automation
Boundary

Lan Automation – Planning

Multistep for Large Topologies



Lan Automation Enhancements

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*)

LAN Automation Enhancements 2.3.7.5

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

Lan Automation – Planning

IP Pool Planning

IP Pool Type and Usage

Roles	Mandatory	Pool Type	Usage
Main/Principal IP Pool	Yes	LAN	Temp DHCP Pool* Loopback(/32) P2P L3 Links(/31)* Multicast
Link Overlapping IP Pool	No	LAN	Temp DHCP Pool P2P L3 Links(/31)

IP Pool Allocation Logic

Allocation Logic	TEMP Pool	Rest of the Pool
Less than /21	/23(512 IPs)	Loopback(/32) P2P L3 Links(/31)* Multicast
/24	/26(64 IPs)	Loopback(/32) P2P L3 Links(/31)* Multicast

* – Link Overlapping IP Pool not provided

Lan Automation – Planning

IP Pool Planning

IP Pool Usage Example (Recommended to use Overlapping IP Pool for P2P Links for /26 & lower)

Allocated Pool	Total Devices to Automate	No of Uplinks	TEMP DHCP Range	Loopback Range	P2P Range	Total IP's
Main/Principal IP Pool 192.168.13.0/24	10	2 (one each to Primary and Secondary Seed)	First /26 (192.168.13.1 to 63)	Next /27 (192.168.13.64 to 94)	Remaining IPs (192.168.13.96 to 254)	10 – Temp DHCP(Released upon completion) 10 – Loopback 40 – P2P Uplinks
Main/Principal IP Pool 192.168.13.0/26	Max 6,if no overlapping pool Max : 29 with Overlapping Pool	2 (one each to Primary and Secondary Seed)	First half (/27) (192.168.13.0 to 31)	Next /29 (192.168.13.32 to 36)	Remaining IPs (192.168.13.40 to 63)	/37 for Anycast RP
Main/Principal IP Pool 192.168.13.0/28	Max 1 if no overlapping pool Max: 5 with Overlapping Pool	2 (one each to Primary and Secondary Seed)	First half (/29) (192.168.13.0 to 7)	Next /31 (192.168.13.8 to 9)	Next /30 (192.168.13.12 to 15)	

Demo Video



Default Deny

Cisco Catalyst Center Policy

Default Permit vs Default Deny Model

Default Permit Model

		Destination				
Source		Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
	Production_User					
	Production_Srvr					
	Development_User					
	Development_Srvr					
	Unknown					

Default_Policy:

Details

- Default action is Permit IP
- Restrictions should be explicitly configured with the use of Security Group Access Lists (SGACLs).
- No complete understanding of traffic flows within their network.
- Fairly easy to implement.

Cons

- More Deny Policies (SGACL) to manage
- More TCAM resources
- Multiple Policy Distribution to switches

Cisco Catalyst Center Policy

Default Permit vs Default Deny Model

Default DENY Model

		Destination				
Source		Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
 Production_User						
 Production_Srvr						
 Development_User						
 Development_Srvr						
 Unknown						

Default_Policy: 

Details

- 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
- Degrade Wireless roaming performance till policy download
- Fallback mechanism incase of Cisco ISE Nodes down

Cisco Catalyst Center Policy

Default Deny Automation Enhancements

Cisco Catalyst Center:

1. 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
2. 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
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

Default Deny Automation Enhancements

Fabric Configuration Updates

1 Ready Updates

Ready Updates (1) [Apply All](#)

Group-Based Policy Enforcement Update For Supplicant Based Extended Nodes

The configuration standards for Supplicant-Based Extended Nodes have been revised to explicitly disable Group-Based Policy Enforcement on the uplink interfaces. This modification will improve the reliability of the onboarding process for these nodes. Apply changes?

Cisco

Catalyst Center

Edit Anycast Gateways

☆ 🔍 🔄 📢 10 👤 maglev

Configuration Attributes

Each Layer 3 Virtual Network can be assigned one or more Anycast Gateways. An Anycast Gateway has an associated VLAN and Layer 2 Virtual Network. Each of these has multiple configuration parameters and attributes.

Q Search

LAYER 3 VIRTUAL NETWORKS

🏠 .../Mpl...o-building-23

INFRA_VN

ANYCAST GATEWAY

IP Address Pool
110.5.120.0/24

☐ TCP MSS Adjustment

VLAN

VLAN Name
110_5_120_0-INFRA_VN

VLAN ID
1021

Pool Type
☒ Fabric APs ☐ Extended Nodes

Group-Based Policy
☒ Enforcement

☐ Auto generate VLAN name

ANYCAST GATEWAY

IP Address Pool
110.5.60.0/24

☐ TCP MSS Adjustment

VLAN

VLAN Name
110_5_60_0-INFRA_VN

VLAN ID
1022

Pool Type
☐ Fabric APs ☒ Extended Nodes

Group-Based Policy
☒ Enforcement

☐ Auto generate VLAN name ☒ Supplicant-Based Extended Node Onboarding

Exit

Review

Back

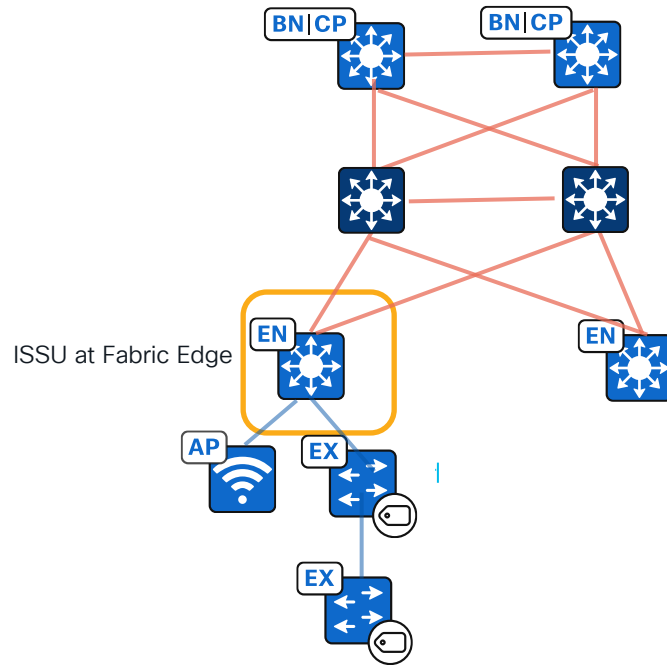
Next

Existing Deployments of
EN/PEN/SBEN

SD-Access ISSU Support

In-Service Software Upgrade

Support in SD-Access LISP Fabric



- Considerations

- ✓ Device model matches C9404R, C9407R, C9410R with dual sup
- ✓ Fabric role: Edge Node(EN) only
- ✓ IOS XE Version: 17.15.1
- ✓ Source and Destination images part of the supported ISSU matrix

WGB support on Cisco SD-Access



WGB support on SD-Access

Intro

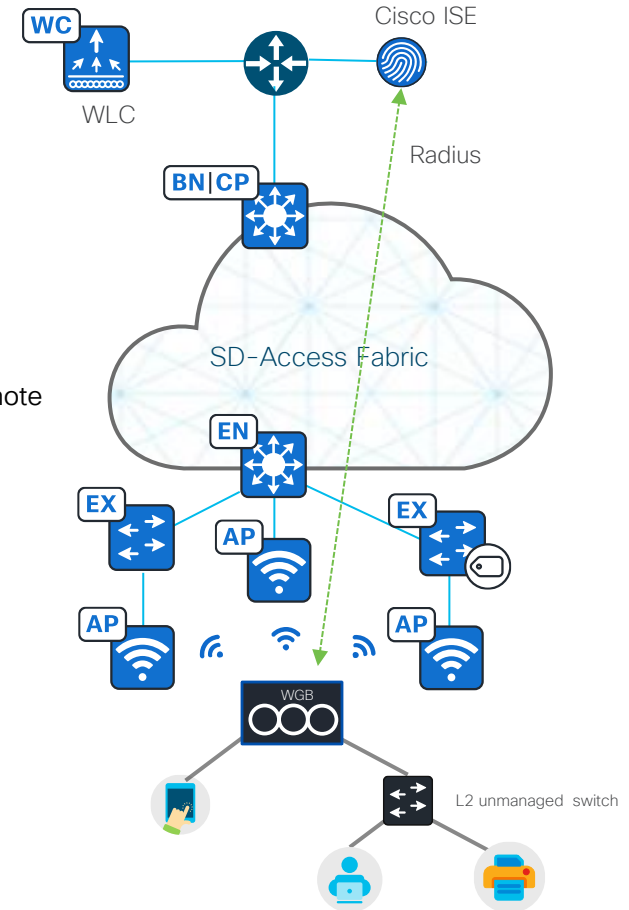
- A workgroup bridge (WGB) is a Cisco access point that is configured to act as a wireless client towards the wireless infrastructure, and to provide Layer 2 connectivity for the devices connected to its ethernet interface

Use Case

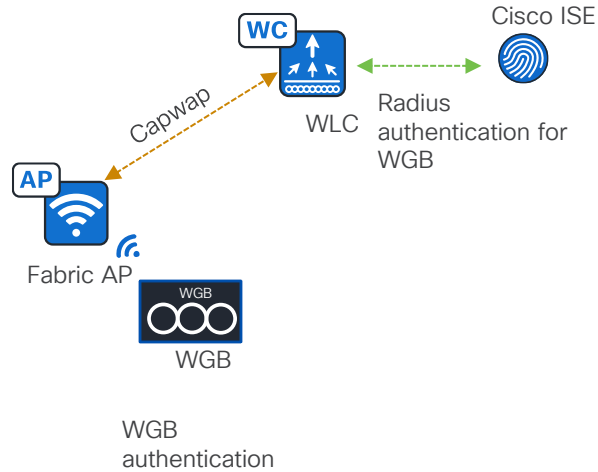
- A WGB support in SD-Access allows the extension of the fabric connectivity to remote sites where fabric EN/EX/PEN can't be deployed.

Details

- Supported from Cisco Catalyst Center 2.3.7.x release .
- The WGB/Fabric wireless should be running Cisco IOS_XE 17.12.1 and upwards.
- The WGB associates with a fabric SSID, extending the fabric network to the Ethernet ports of the WGB
- The endpoints behind the WGB are in the same Layer 2 extension as the WGB itself.
- The WGB can associate with an open/PSK and dot1x-based SSID.
- The WGB can act as an authenticator and talk radius protocol to allow endpoints on its ethernet ports to be authenticated



WGB support on SD-Access



Considerations

- The endpoints behind WGB get the same policy attributes as a WGB, such as the VNID/SGT
- The WGB communicates using EAP with endpoints and RADIUS with the AAA server, and there is no provision to modify the timers for these protocols
- Ensure that the latency between the WGB and the RADIUS server is within acceptable limits to avoid triggering re-transmissions.
- WGB configurations are *not* automated by the Cisco Catalyst Center; the configuration needs to be manually provisioned using the CLI
- The fabric SSID needs to be enabled for CCX Aironet for the WGB to associate. The CCX attribute can be automated with the Cisco Catalyst Center using the model config generator.
- No support for *wireless endpoints* behind WGB

Mesh support on Cisco SD-Access



Mesh support on SD-Access

Use Case

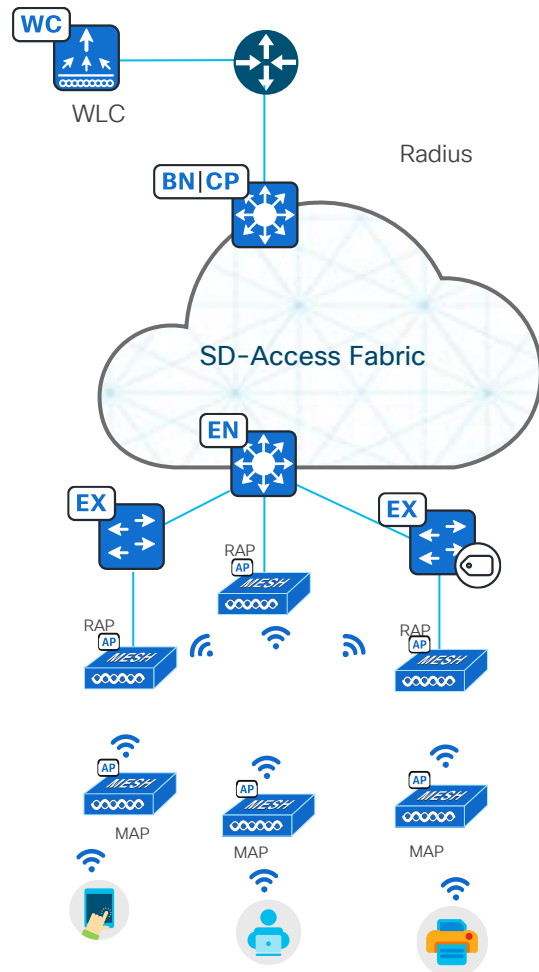
- To support Mesh deployment on the Software-Defined Access fabric, enabling the extension of the fabric's SSID from indoor to outdoor environments
- Maintain segmentation on the mesh network

Details

- Supported from Cisco Catalyst Center 2.3.7.x release .
- The Fabric wireless network should be running Cisco IOS_XE 17.12.1 and upwards.
- Fully automated workflow using the Cisco Catalyst center
- The wireless endpoints connected to the RAP, or the MAP receives the same segmentation as connected to a fabric SSID on a fabric AP
- MAP and RAP is in bridge mode but gets classified as a fabric AP, very similar to the local mode AP.

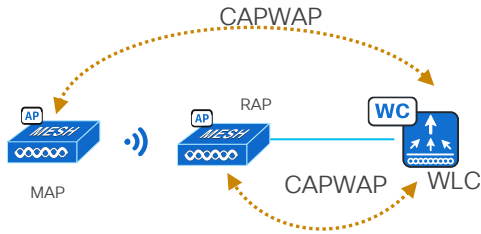
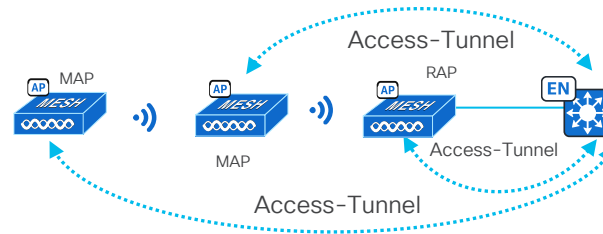
Platforms

- WLC : All hardware and virtual form factors of the C9800 series. Embedded Wireless on Catalyst 9000 switches is not supported.
- AP: Wave2 and Catalyst Access Points that are compatible with mesh functionality.



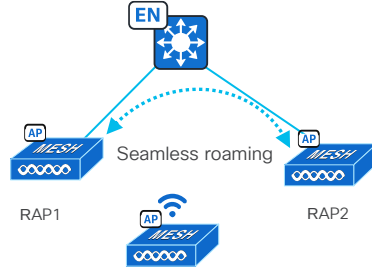
Mesh support on SD-Access

Details



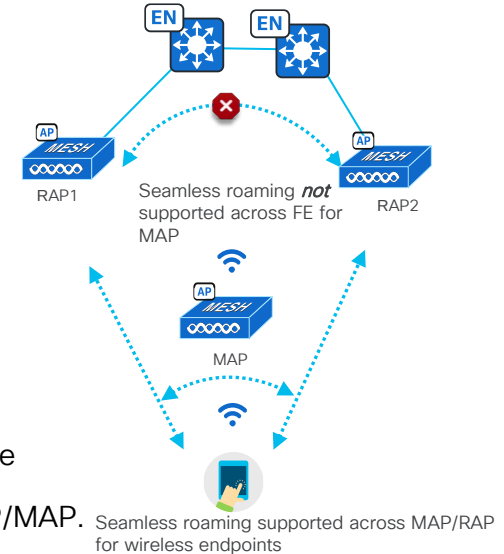
- MAP and RAP establishes a CAPWAP session with the Wireless LAN Controller and uses the regular CAPWAP discovery methods
- The wireless endpoints can be associated to the MAP and RAP and support seamless roaming across the MAP and RAP
- The RAP and MAP has an Access-tunnel (VxLAN) established to the respective fabric edge.
- The MAP creates a tunnel to a fabric edge where the parent RAP is attached to.
- MAP and the fabric edge has a layer2 connectivity, traffic from a wireless endpoint gets converted from 802.11 to 802.3 and goes through VxLAN encapsulation destined to the fabric edge.

Roaming support for MAP



Roaming

- In mesh network a RAP is uplinked to a fabric edge directly or through a EN/PEN node
- A MAP gets attached to a network using the backhaul radio network of a parent RAP/MAP.
- A MAP can roam if it finds a better parent node which could either be a MAP or a RAP.
- MAP operating in fabric mode can only roam across RAP/MAP if it attached to the same parent fabric edge node.
- MAP roaming to another MAP/RAP attached to a different fabric edges are not supported
- A wireless client can roam across RAP/MAP on different fabric edges.



Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



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



Continue your education



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



Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC