cisco Live!

ALL IN

#CiscoLive

The bridge to possible

SD-Access Wireless

Integrating wireless into SD-Access

Alex Tenenbaum, ENB TME

BRKEWN-2308

Cisco Webex App

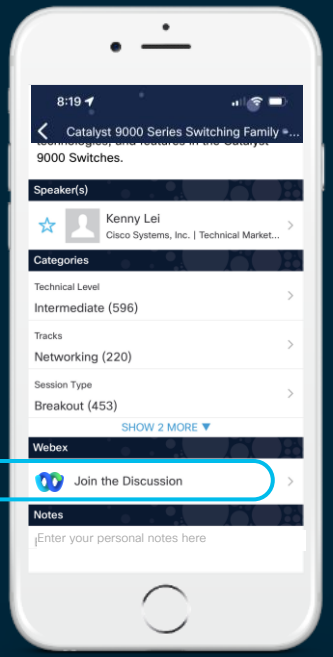
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 17, 2022.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2308

Software **Defined Access – Wireless Integration**

Agenda

1. **Why** Fabric and what does integrating wireless mean?
2. **How** does it really work?
3. **What** products make the solution?

SD-Access Fabric: Why Would You Care?

What is the Problem?

- Policy Model Today

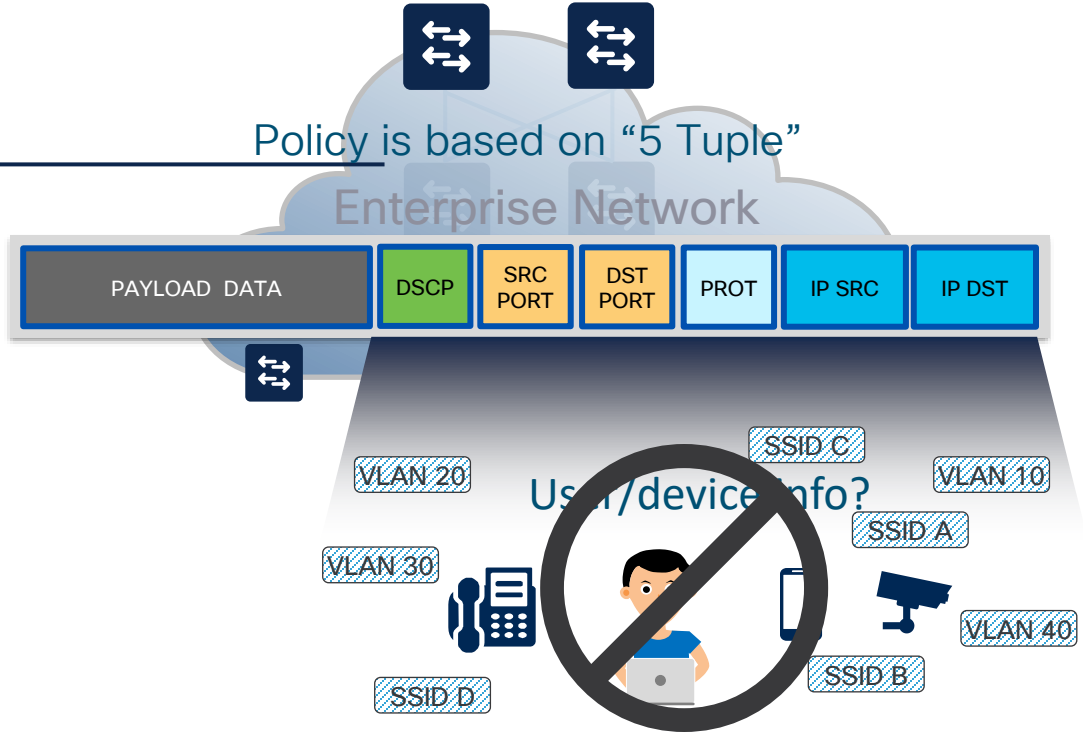
```
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 eq 639 122.201.132.164 0.0.31.255 gt 1511
access-list 102 deny tcp 247.54.117.116 0.0.0.127 gt 4437 136.68.158.104 0.0.1.255 gt 1945
access-list 102 permit icmp 136.196.101.101 0.0.0.255 lt 2361 90.186.112.213 0.0.31.255 eq 116
access-list 102 deny udp 242.4.189.142 0.0.1.255 eq 1112 19.94.101.166 0.0.0.127 eq 959
access-list 102 deny tcp 62.212.21.1 255.255.255.127 eq 2507 214.212.4.115 0.0.31.255 lt 993
access-list 102 deny tcp 103.10.93.140 255.255.255.255 eq 970 71.103.141.91 0.0.0.127 lt 848
access-list 102 deny ip 32.15.78.227 0.0.0.127 eq 1493 72.92.200.157 0.0.0.255 gt 4878
access-list 102 permit icmp 100.211.144.227 0.0.1.255 lt 4962 94.127.214.49 0.255.255.255 eq 1216
access-list 102 deny icmp 88.91.79.30 0.0.0.255 gt 26 207.4.250.132 0.0.1.255 gt 1111
access-list 102 deny ip 167.17.174.35 0.0.1.255 eq 3914 140.119.154.142 255.255.255.255 eq 4175
access-list 102 permit tcp 37.85.170.24 0.0.0.127 lt 3146 77.26.232.98 0.0.0.127 gt 1462
access-list 102 permit tcp 155.237.22.232 0.0.0.127 gt 1843 239.16.35.19 0.0.1.255 lt 4384
```

Network Policy

IP ADDRESSES

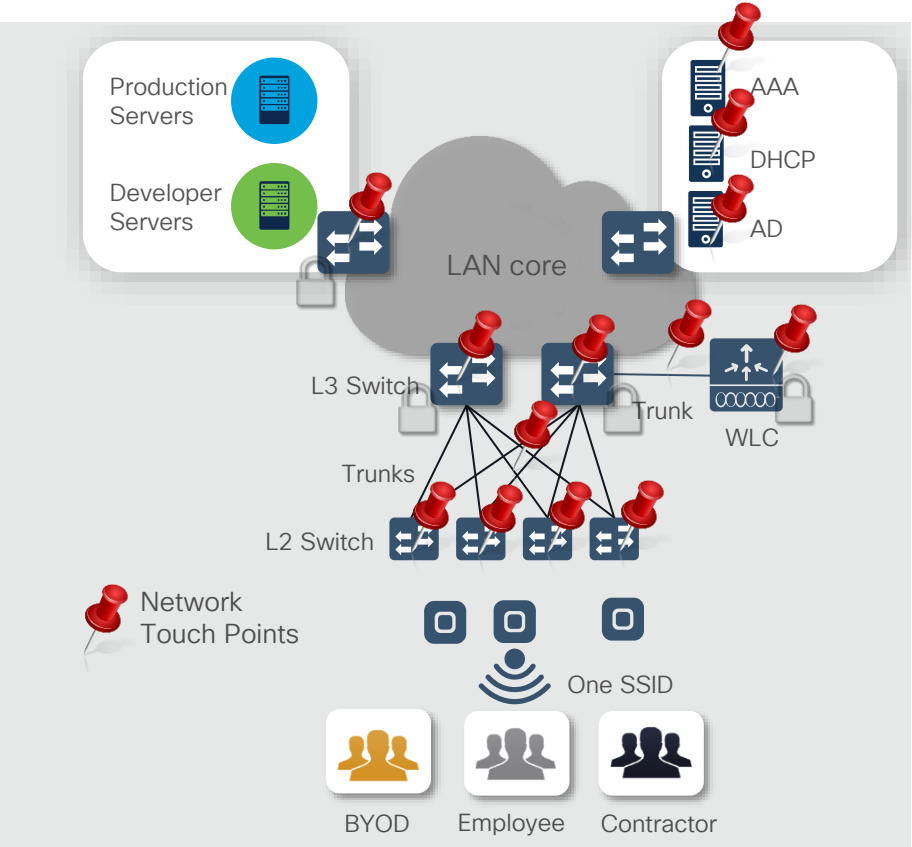
- Locate you
- Identify you
- Drive “treatment”
- Constrain you

Policy is based on “5 Tuple”

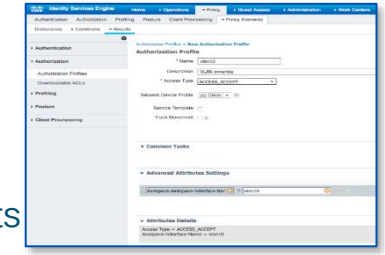


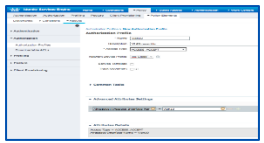
What is the Problem?

User Group policy rollout – Today



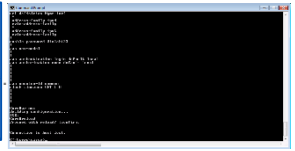
1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
   - Routing for new subnets
   - Map SSID to Interface/VLAN
4. Implement Policy
   - Define ACLs
   - Apply ACLs
5. Many different User Interfaces





AAA

WLC



Devices CLI

But What If …

… we could make **the IP address** or **MAC address** just be a **LOCATOR for you**, and provide **other ways to group users / devices to apply POLICY?**

Key Assertion

If we could **"break the dependence"** between IP addressing and policy, we could **greatly simplify** networks – and make networks **much more functional.**

Overlay uses **alternate forwarding** attributes to provide additional services

Policy is applied **irrespectively of network constructs** (VLAN, subnet, IP)

Easily implement **Network Segmentation** (w/o implementing MPLS)

Provide **L2 and L3 flexibility** (w/o stretching VLANs)

WITH A FABRIC…

… we could make **the IP address** just be a **LOCATOR for you**, and provide **other ways to group users / devices to apply POLICY?**

Key Assertion

If we could **"break the dependence"** between IP addressing and policy, we could **greatly simplify** networks – and make networks **much more functional.**

What exactly is a Fabric?

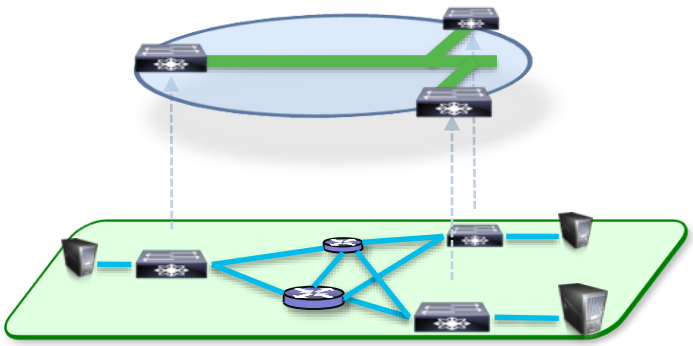
A **Fabric** provides an **Overlay network**

An *Overlay* is a *logical topology* used to *virtually connect* devices, built *on top* of some arbitrary physical *Underlay* topology.

An *Overlay* network often uses *alternate forwarding attributes* to provide *additional services,* not provided by the *Underlay*.

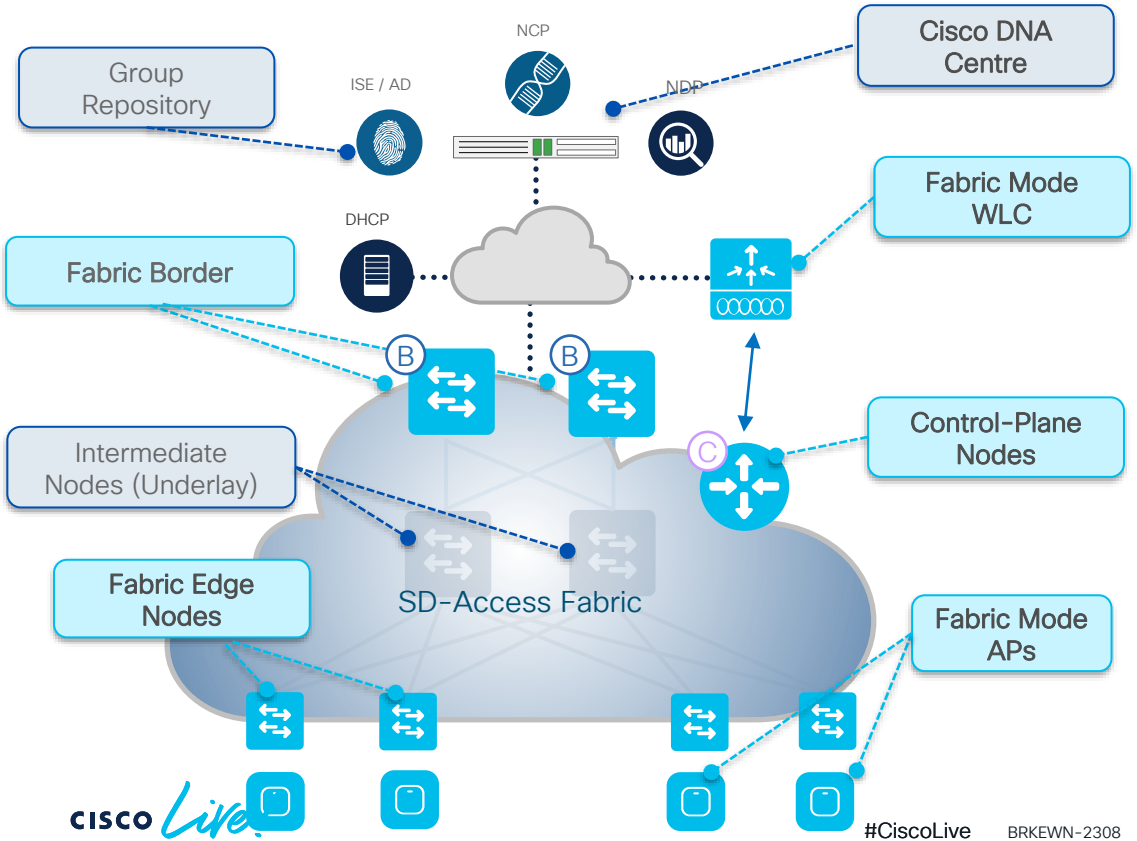
Examples of Network Overlays

- GRE or mGRE
- MPLS or VPLS
- IPSec or DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI



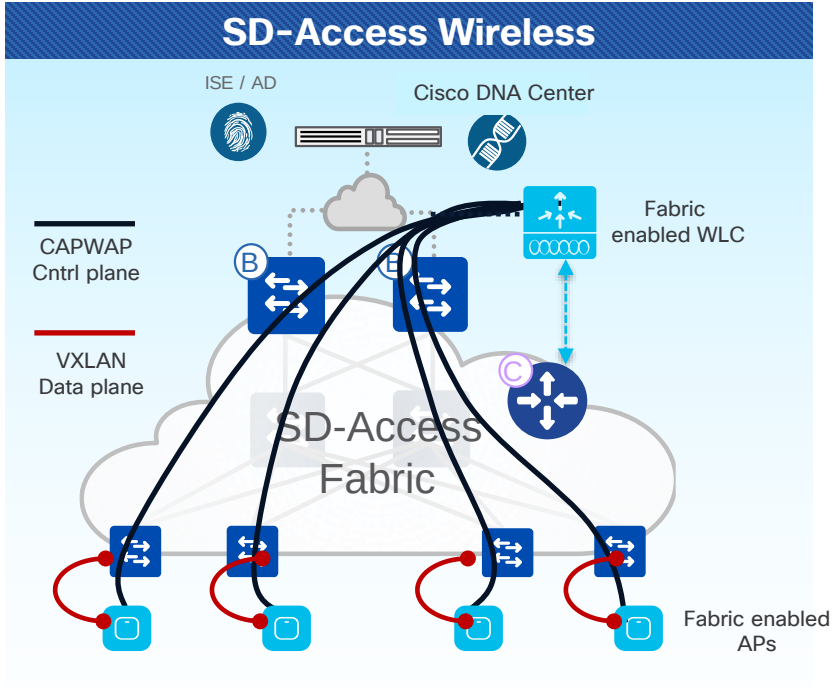
SD-Access Fabric Architecture

Roles and Terminology



- **Cisco DNA Controller** – Enterprise SDN Controller provides GUI management abstraction via multiple Service Apps, which share information
- **Group Repository** – External ID Services (e.g.. ISE) is leveraged for dynamic User or Device to Group mapping and policy definition
- **Control-Plane (CP) Node** – Map System that manages Endpoint ID to Location relationships. Also known as Host Tracking DB (HTDB)
- **Border Nodes** – A Fabric device (e.g.. Core) that connects External L3 network(s) to the SDA Fabric
- **Edge Nodes** – A Fabric device (e.g.. Access or Distribution) that connects wired endpoints to the SDA Fabric
- **Fabric Wireless Controller** – Wireless Controller (WLC) fabric-enabled, participate in LISP control plane
- **Fabric Mode APs** – Access Points that are fabric-enabled. Wireless traffic is VXLAN encapsulated at AP

SD-Access Wireless: true integration in Fabric

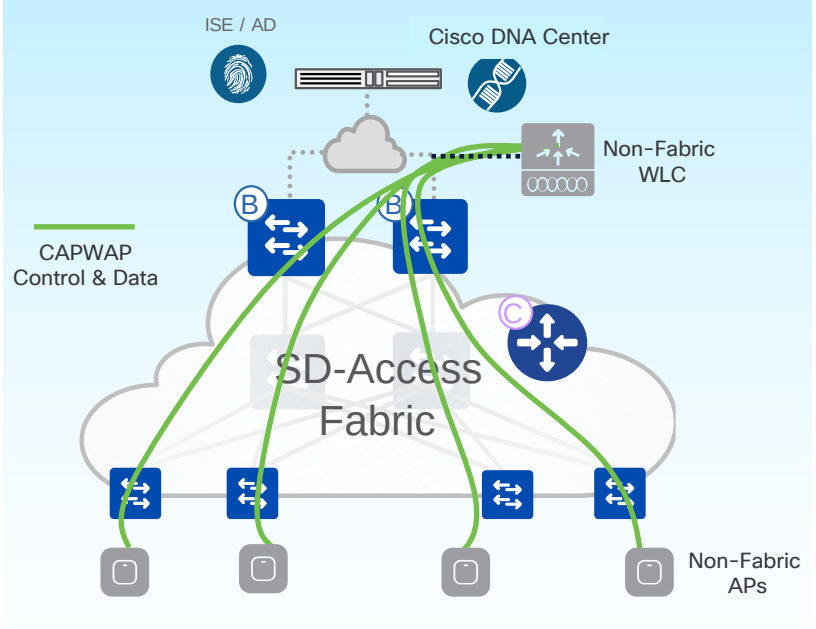


- CAPWAP Control Plane, VXLAN Data plane
- WLC/APs integrated in Fabric, SD-Access advantages
- Requires software upgrade (8.5+)
- Optimized for 802.11ac Wave 2 and 11ax APs

- True wireless integration with Fabric
- Provides all the advantages of SDA for wireless clients:
  - Full automation with Cisco DNA Center
  - Hierarchical segmentation (VRF and SGT)
  - Same policy as wired
  - Distributed Data Plane with no drawbacks
  - Optimized traffic path for Guest
- Recommended option

Wireless on top of SDA Fabric

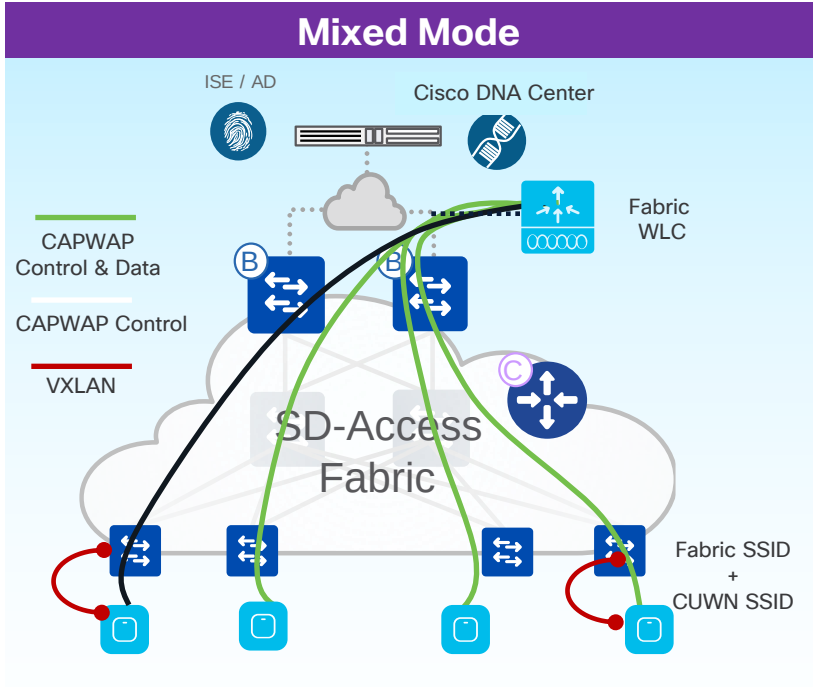
CUWN wireless Over The Top (OTT)



- CAPWAP for Control Plane and Data Plane
- SDA Fabric is just a transport
- Supported on any WLC/AP software and hardware

- **No SDA advantages for wireless**
- Migration step to full SD-Access
- Customer wants/need to first migrate wired (different Ops teams managing wired and wireless, get familiar with Fabric, different buying cycles, etc.) and leave wireless “as it is”
- Customer cannot migrate to Fabric yet (older APs, need to certify the new software, etc.)

Wireless Integration in SDA Fabric

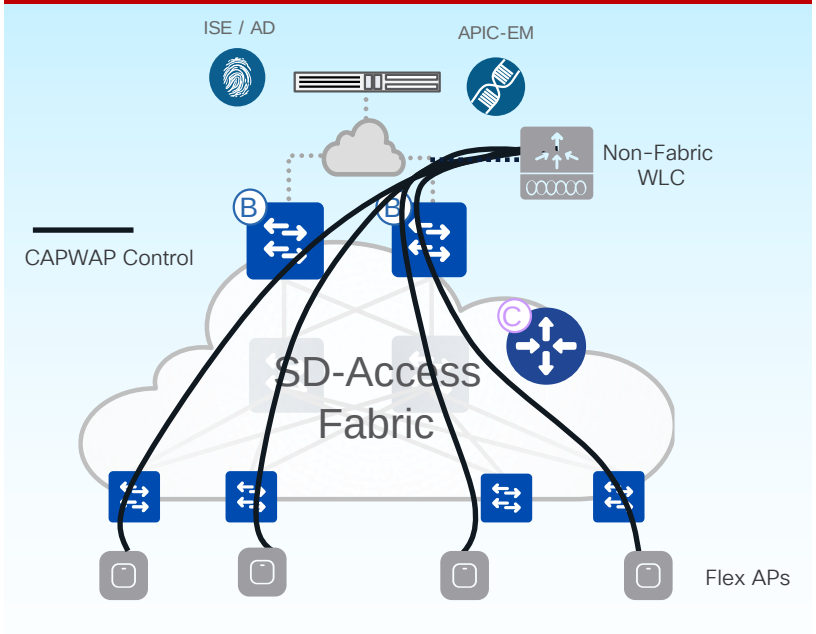


- non-Fabric SSID: client traffic is CAPWAP encapsulated to WLC
- Fabric SSID: client traffic is VXLAN encapsulated

- Mixed mode: mix of Fabric and non-Fabric (centralized) SSIDs
- Mixed mode is supported both on the same AP or different APs

Wireless on top of SDA Fabric

FlexConnect Over The Top (OTT)

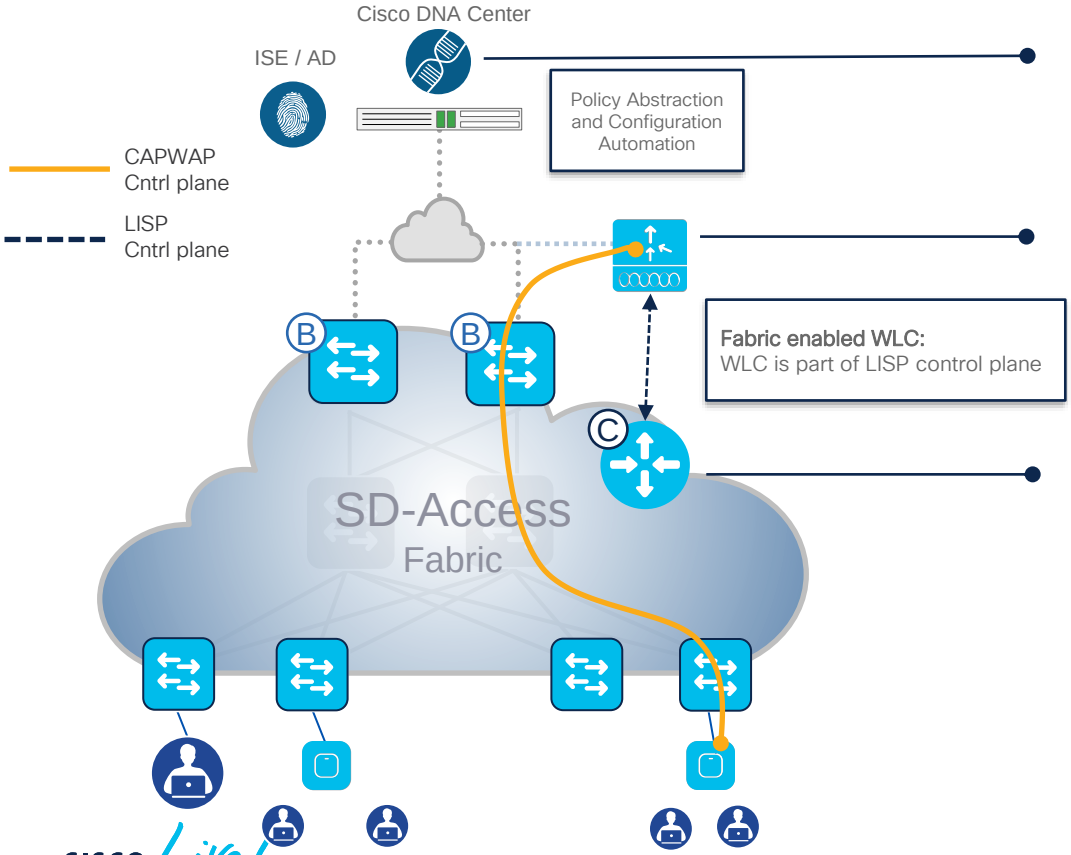


- CAPWAP for Control Plane
- Data plane is locally switched. Wireless traffic is treated like wired traffic.

- FlexConnect local switching is supported with Design council approval.
- This applies also to 3rd party wireless solution that bridges traffic at the AP

SD-Access Wireless Architecture

Simplifying the Control Plane



Automation
- Cisco DNA Center simplifies the Fabric deployment,
- Including the wireless integration component

Centralized Wireless Control Plane
- WLC still provides client session management
- AP Mgmt, Mobility, RRM, etc.
- Same operational advantages of non-SDA WLC

LISP control plane Management
- WLC integrates with LISP control plane
- WLC updates the CP for wireless clients
- Mobility is integrated in Fabric thanks to LISP CP

SD-Access Wireless Architecture

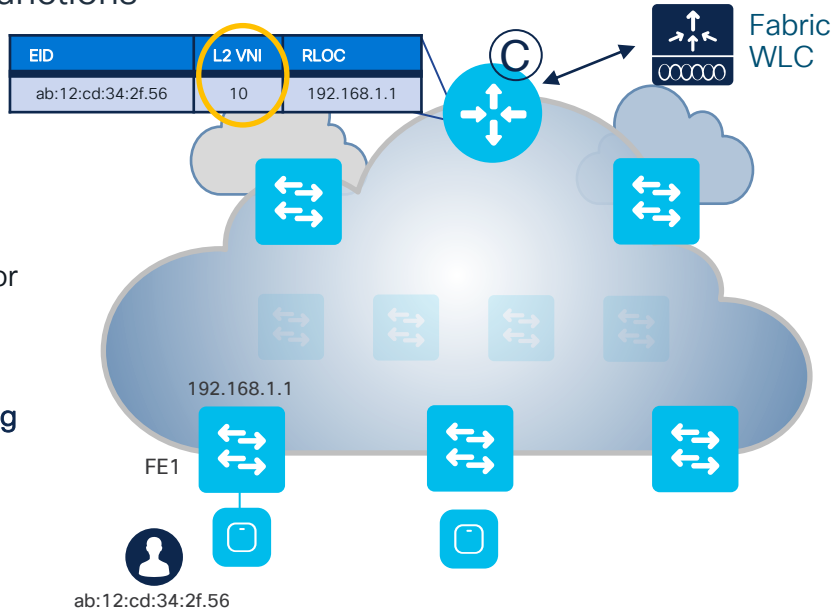
Fabric WLC- A Closer Look

Fabric Mode WLC integrates with the LISP Control Plane

Control Plane is centralized at the WLC for all Wireless functions

- WLC is still responsible for : AP image/config, Radio Resource Management (RRM) and client session management and roaming

- For Fabric integration:
  - For wireless, **client MAC address is used as EID**
  - WLC interacts with the Host Tracking DB on Control-Plane node for Client **MAC address registration** with SGT and L2 VNI
  - The VN information is a **Layer 2 VN (L2 VNID)** information and it's mapped to a VLAN on the FEs
  - WLC is responsible for **updating the Host Tracking DB with roaming** information for wireless clients
  - Fabric enabled WLC needs to be co-located at the same site with APs (latency between AP and WLC needs to be < 20 ms)



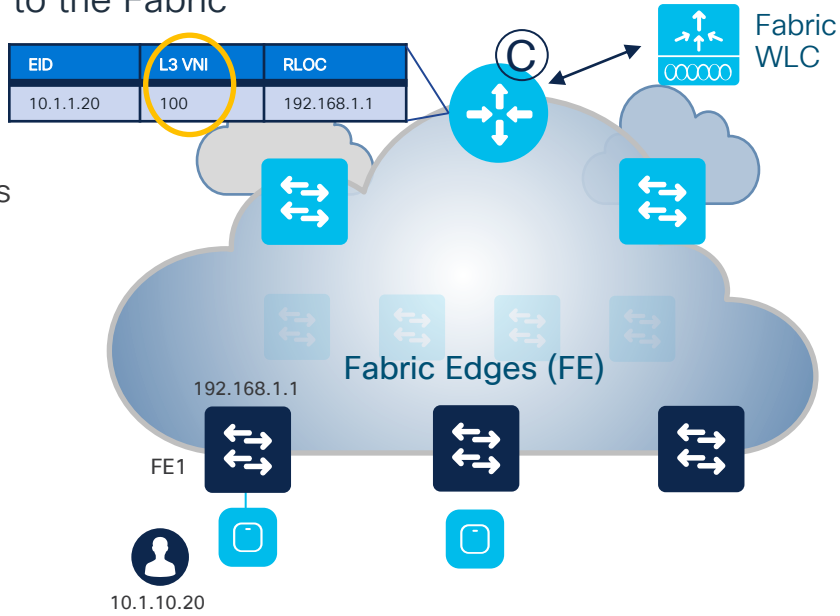
SD-Access Wireless Architecture

Optimizing the Data Plane: Fabric Edge – A Closer Look

Fabric Edge Node is based on a LISP Tunnel Router

Provides connectivity for Users and Devices connected to the Fabric

- Responsible for Identifying and Authenticating wired Endpoints
- **Registers Endpoint ID** info with the Control-Plane Node(s)
- Provide VN services for Wireless Clients (**L3 VNID**)
- **Onboard APs into fabric and form VXLAN tunnels with APs**
- Provides **Anycast L3 Gateway** for connected Endpoints



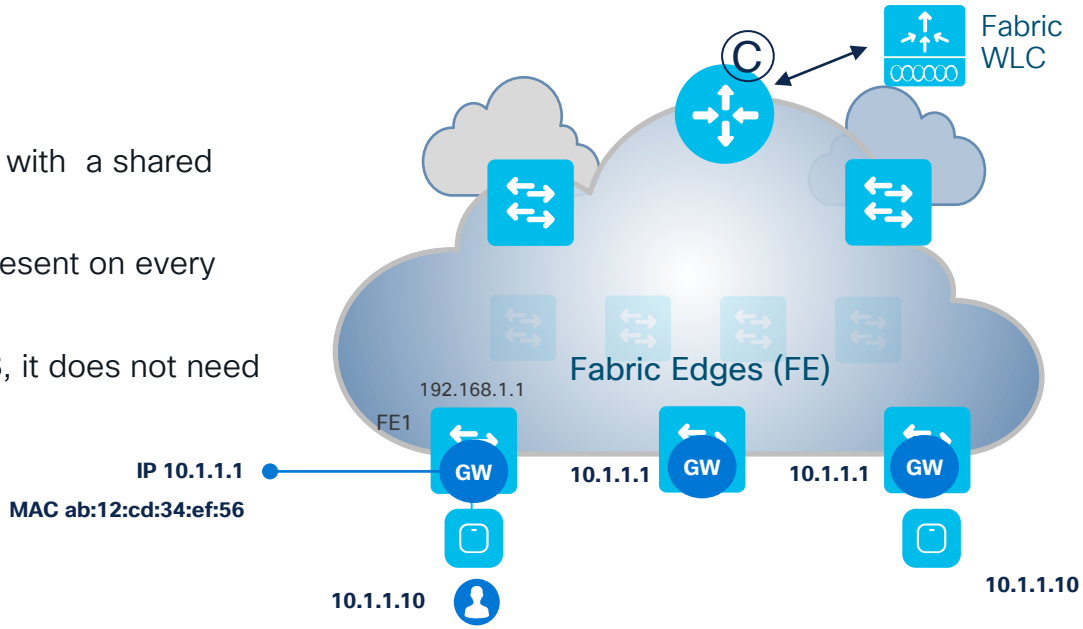
SD-Access Wireless Architecture

Optimizing the Data Plane: Anycast Gateway – A Closer Look

Anycast GW provides a single L3 Default Gateway

Based on Virtual IP address (VIP)

- Similar principle and behavior as HSRP / VRRP with a shared Virtual IP and MAC address
- The same Switched Virtual Interface (SVI) is present on every Edge, with the same Virtual IP and MAC
- If (when) a Host moves from Edge A to Edge B, it does not need to change it's (L3) Default Gateway!



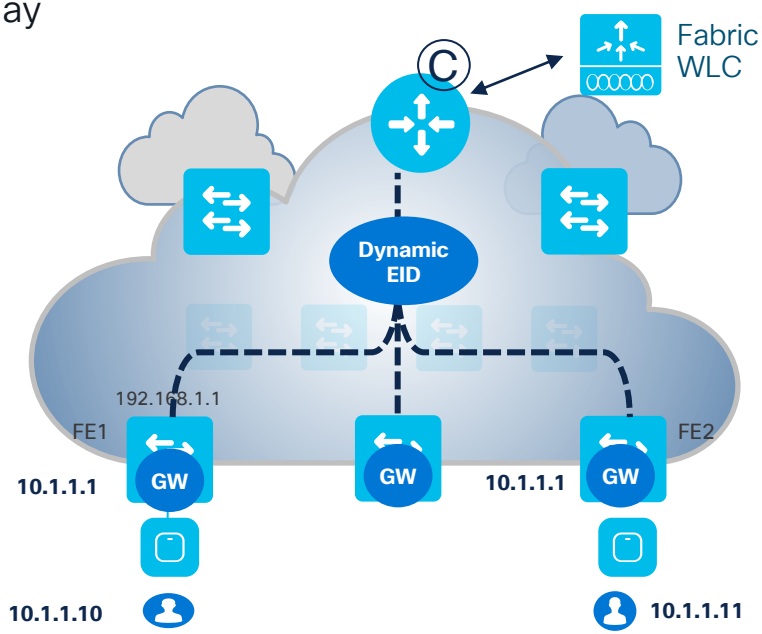
SD-Access Wireless Architecture

Optimizing the Data Plane: Stretched subnets – A Closer Look

Stretched subnets allow an IP subnet to be "stretched" via the overlay

Based on a Anycast GW + LISP Dynamic EID + VXLAN overlay

- Host IP based traffic arrives on the local Fabric Edge SVI, and is then transferred by LISP
- LISP Dynamic EID allows Host-specific (/32, /128, MAC) advertisement and mobility
- **No longer need to stretch a VLAN** across access layer switches to connect Host 1 and 2 to get L2 adjacency
- Client 1 connected to Fabric Edge 1 (FE1) can talk to client B on FE2 as they are on the same IP subnet.



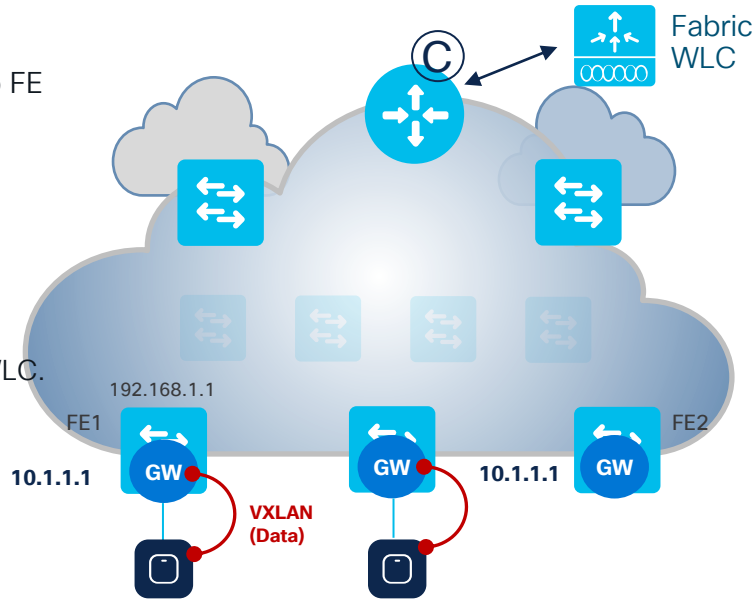
SD-Access Wireless Architecture

Optimizing the Data Plane: Fabric Mode AP – A Closer Look

Fabric Mode AP integrates with the VXLAN Data Plane

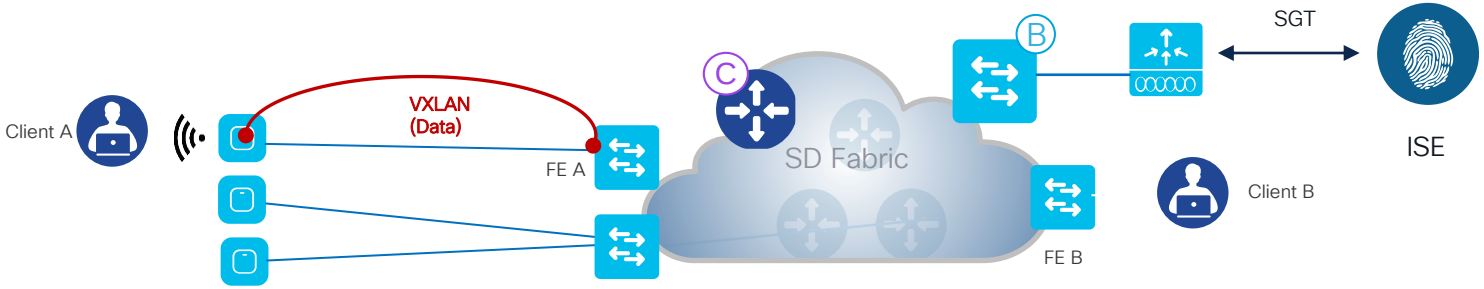
Wireless Data Plane is distributed at the AP

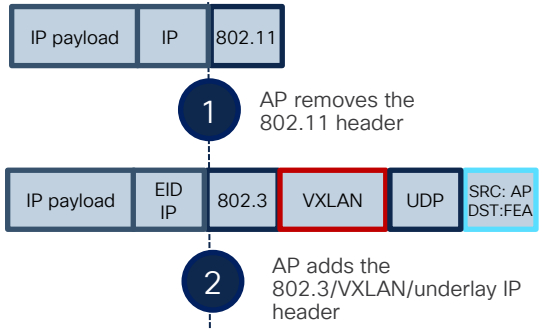
- Fabric mode AP is a local mode AP and needs to be **directly connected** to FE or to an extended node
- CAPWAP control plane goes to the WLC using Fabric
- **Fabric is enabled per SSID**:
  - For Fabric enabled SSID, AP converts 802.11 traffic to 802.3 and encapsulates it into VXLAN encoding VNI and SGT info of the client
  - Forwards client traffic based on forwarding table as programmed by the WLC. Usualy VXLAN DST is first hop switch.
- AP applies all wireless specific feature like SSID policies, AVC, QoS, etc.



SD-Access Wireless Architecture

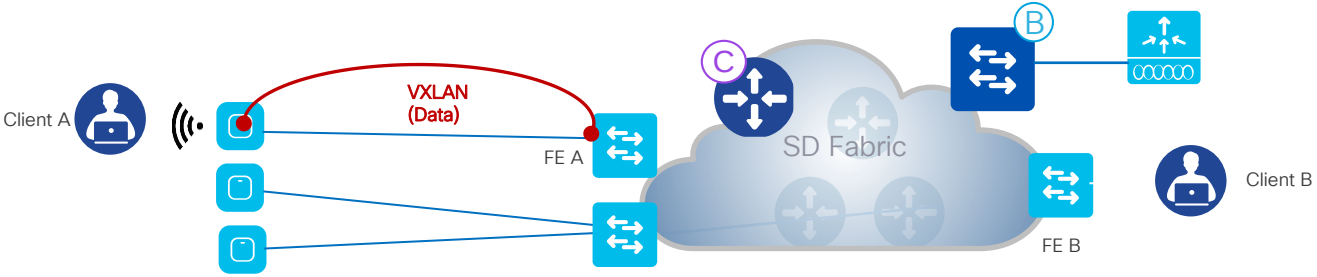
Simplifying policy and Segmentation

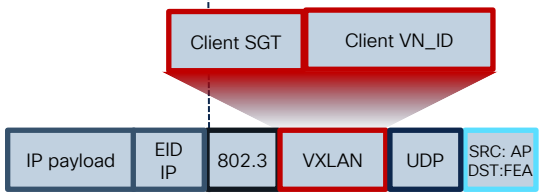




SD-Access Wireless Architecture

Simplifying policy and Segmentation





2

APs embed the Policy information in the VXLAN header and forwards it

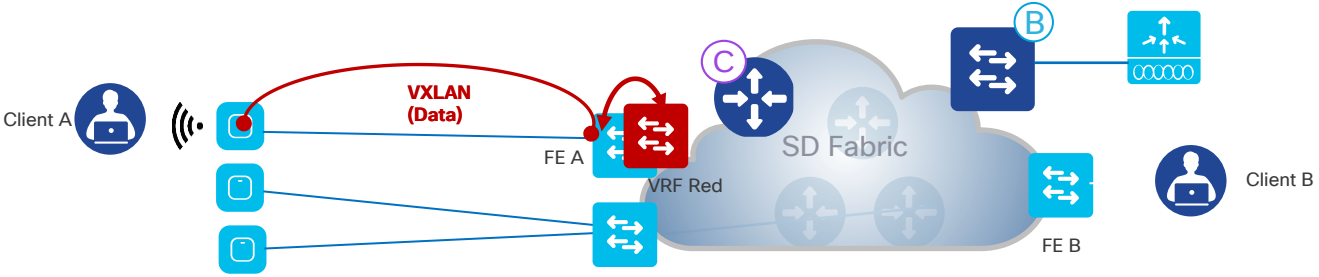
The client VRF is represented by the Layer 2 Virtual Network (L2 VNID)

Hierarchical Segmentation:

1. Virtual Network (VN) == VRF - isolated routing Control Plane + Data Plane
2. Scalable Group Tag (SGT) - User Group identifier

SD-Access Wireless Architecture

Simplifying policy and Segmentation



FEA does a lookup to CP to locate client B

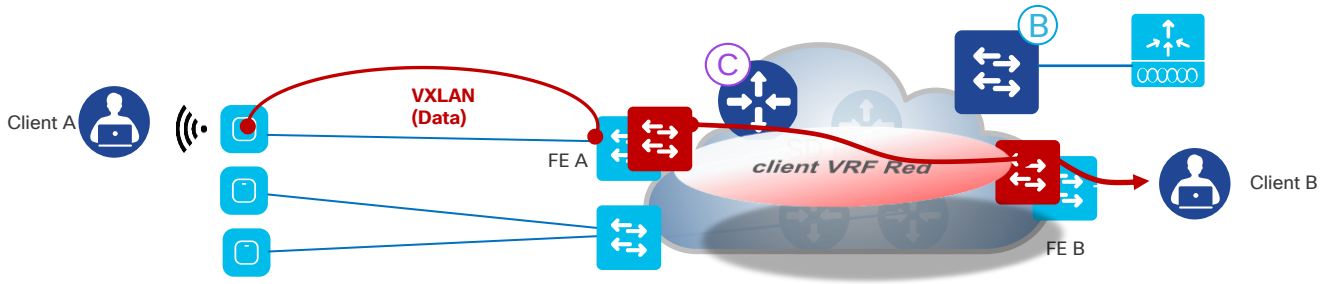
IP payload	EID IP	802.3	VXLAN	UDP	SRC:FEA DST:FEB

3 FE decapsulates the VXLAN header, looks at the L2 VNID and maps it to the VLAN and L2 LISP instance.

Then FE A does the lookup and rebuild the VXLAN encapsulates to the destination FE B

SD-Access Wireless Architecture

Simplifying policy and Segmentation



Mapped to VRF
SGT policy is applied

IP payload	EID IP	802.3	VXLAN	UDP	SRC:FEA DST:FEB

4

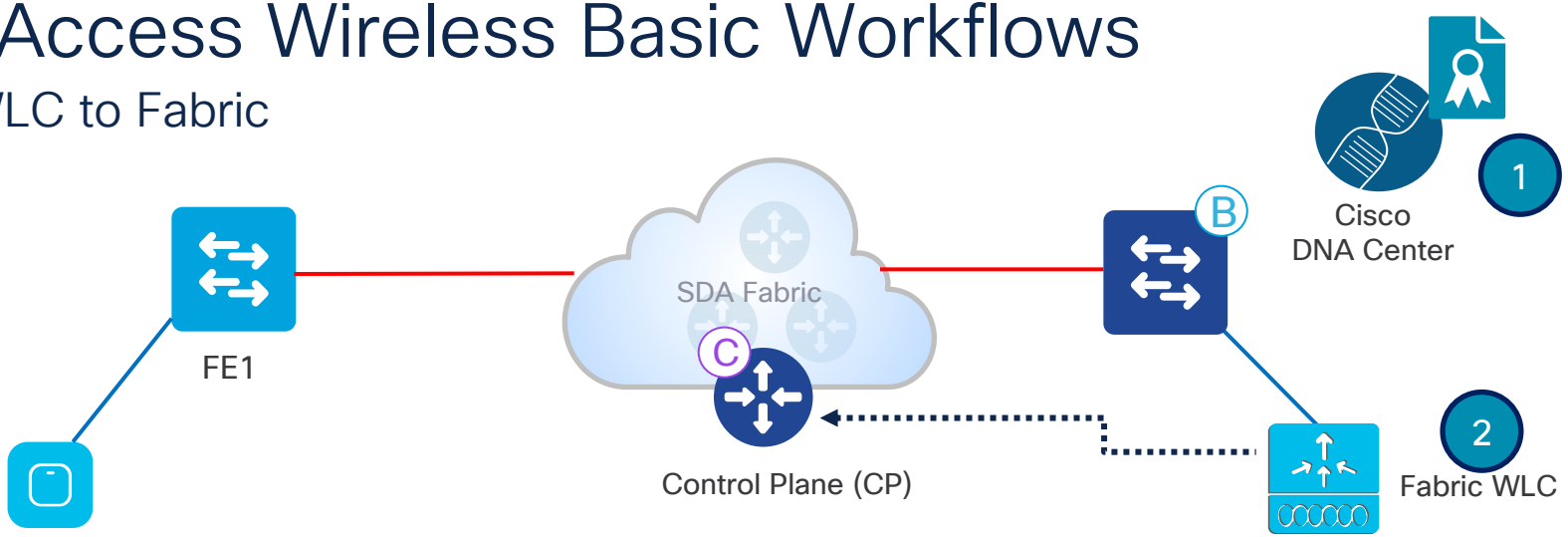
FE removes the outer IP header, looks at the VNID maps it to the VLAN.

Also looks at the SGT and apply the policy before forwarding the packet

Client Policy is carried end to end in the overlay

SD-Access Wireless Basic Workflows

Add WLC to Fabric

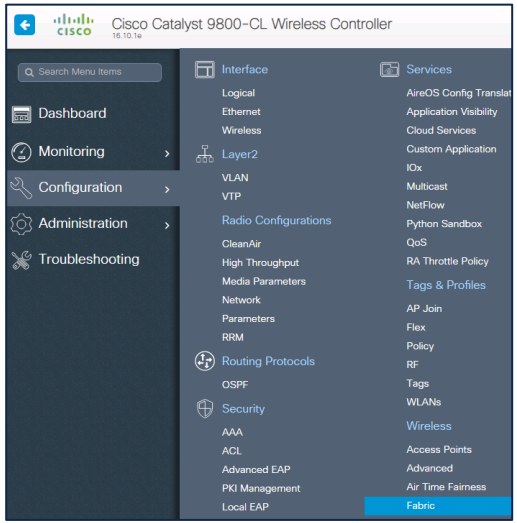


1. In Cisco DNA Center, first provision the WLC and then add it to the Fabric site
2. Fabric configuration is pushed to WLC. WLC becomes Fabric aware. Most importantly WLC is configured with credentials to established a secure connection to CP
3. WLC is ready to participate in SD-Access Wireless

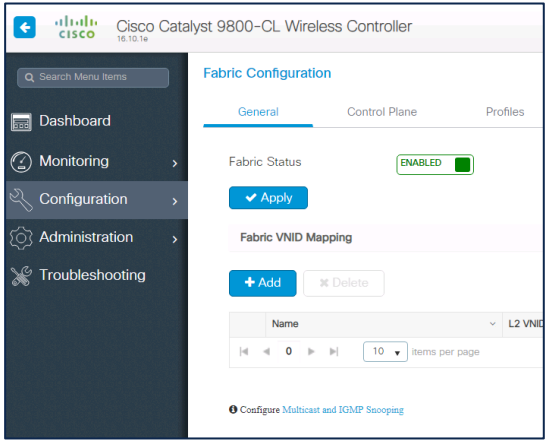
SD-Access Wireless Basic Workflows

Add WLC to Fabric – verify settings

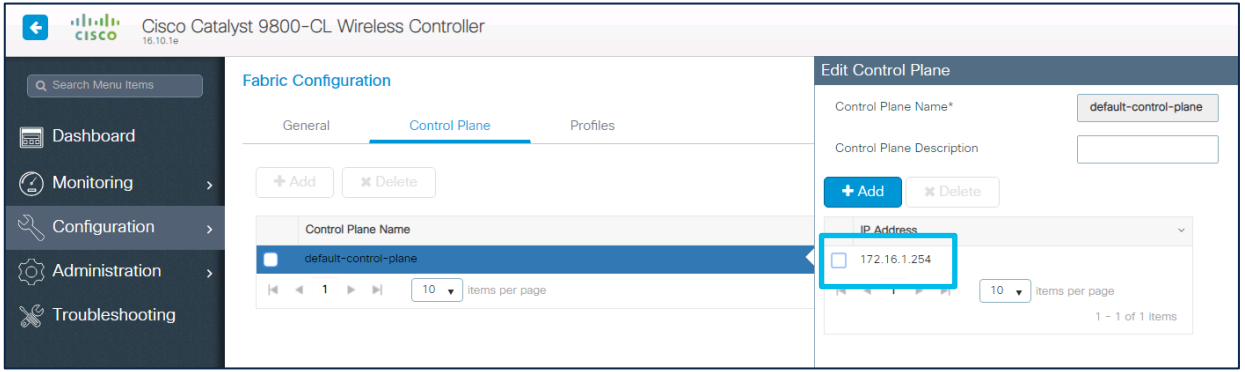
Configuration > Wireless > Fabric



Fabric status is enabled



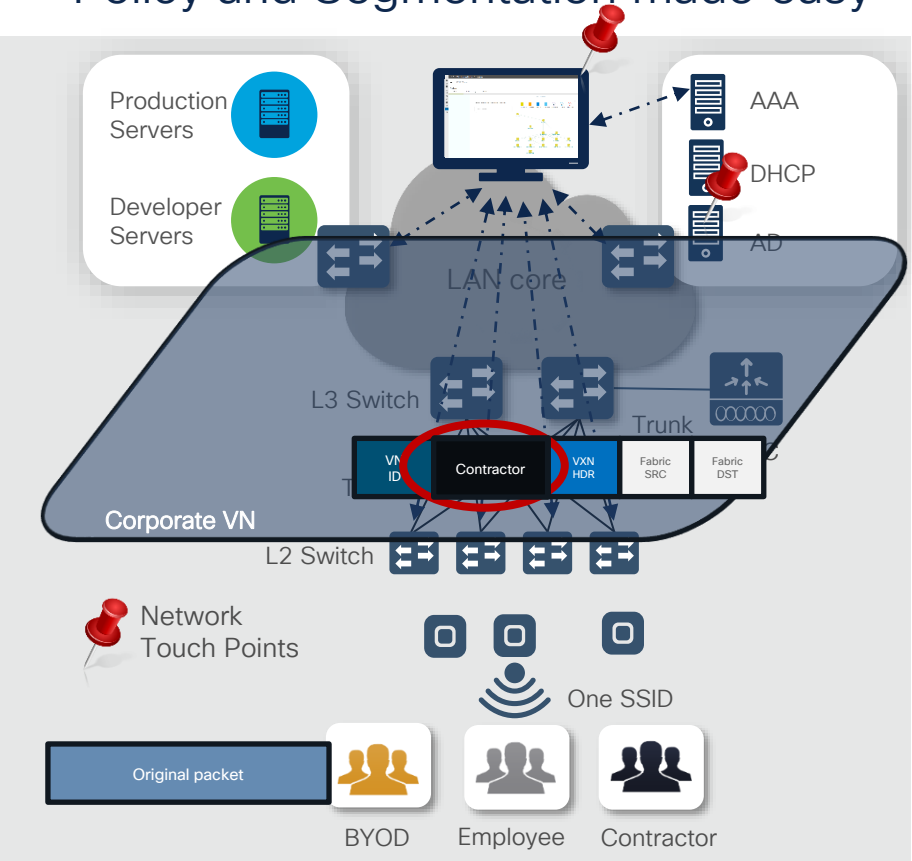
CP is correctly configured



Benefits of SD-Access Wireless

Benefit of SD-Access Wireless

Policy and Segmentation made easy



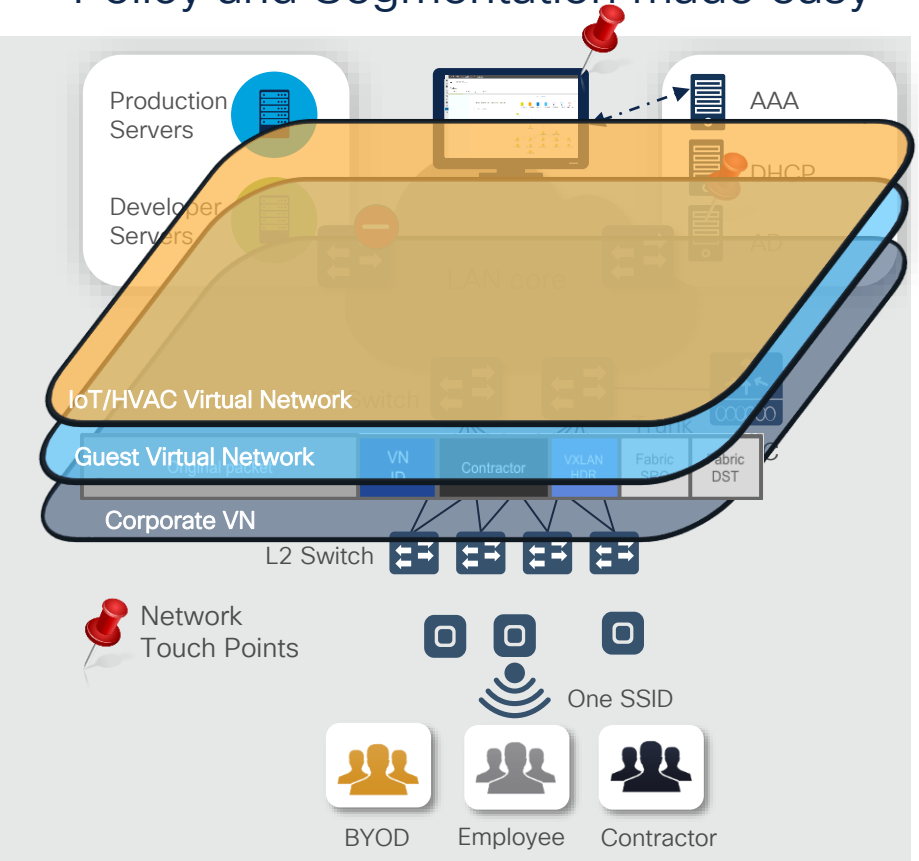
1. Define Groups in AD
2. Design and Deploy in Cisco DNA-C
   - Create Virtual Network for Corporate
   - Define Policies
     - Role/Group based
   - Apply Policies
     - SGT based

	Production Serv. **SGT 10**	Developer Serv. **SGT 20**
Employee **SGT 100**		
BYOD **SGT 200**		
Contractor **SGT 300**		

3. Upon user authentication, Policy is automatically applied and carried end to end

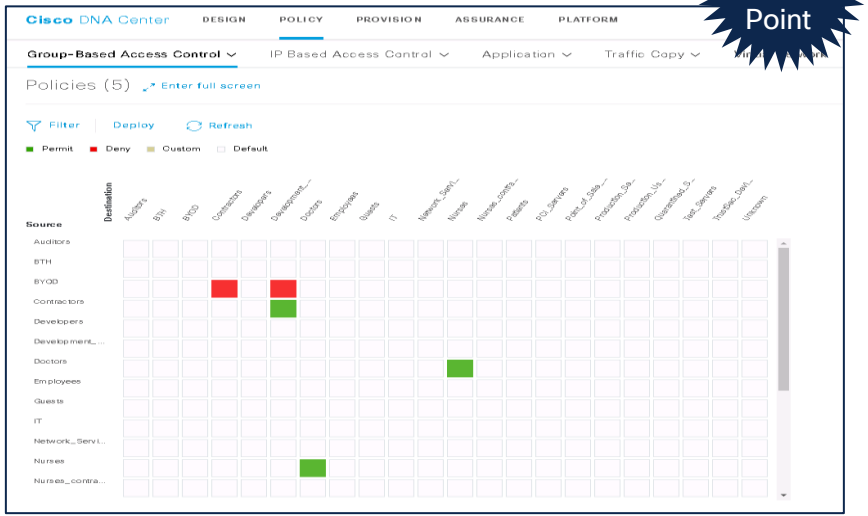
Benefit of SD-Access Wireless

Policy and Segmentation made easy



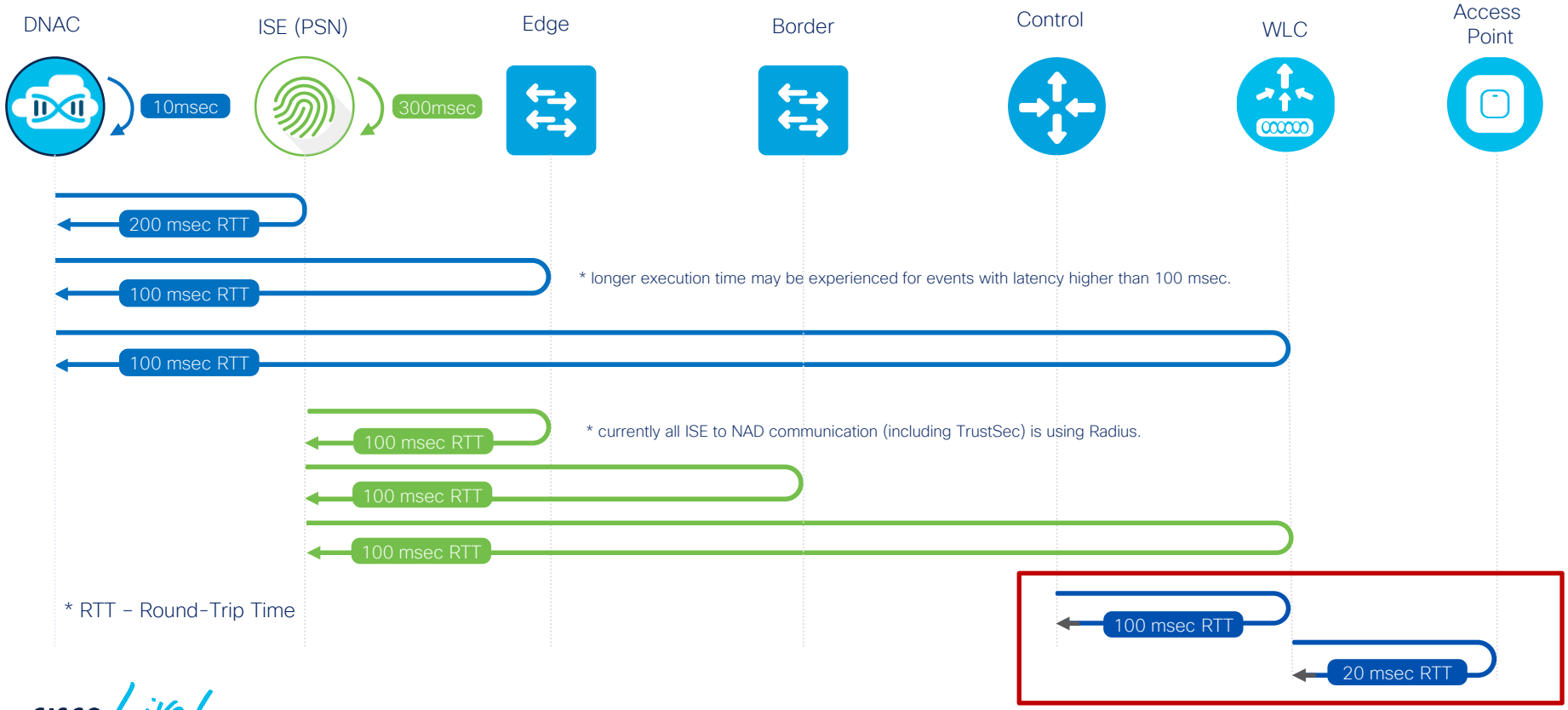
1. Define Groups in AD
2. Design and Deploy in Cisco DNA-C
   - Create Virtual Network for Corporate
   - Define Policies
     - Role/Group based
   - Apply Policies
     - SGT based

One Touch Point



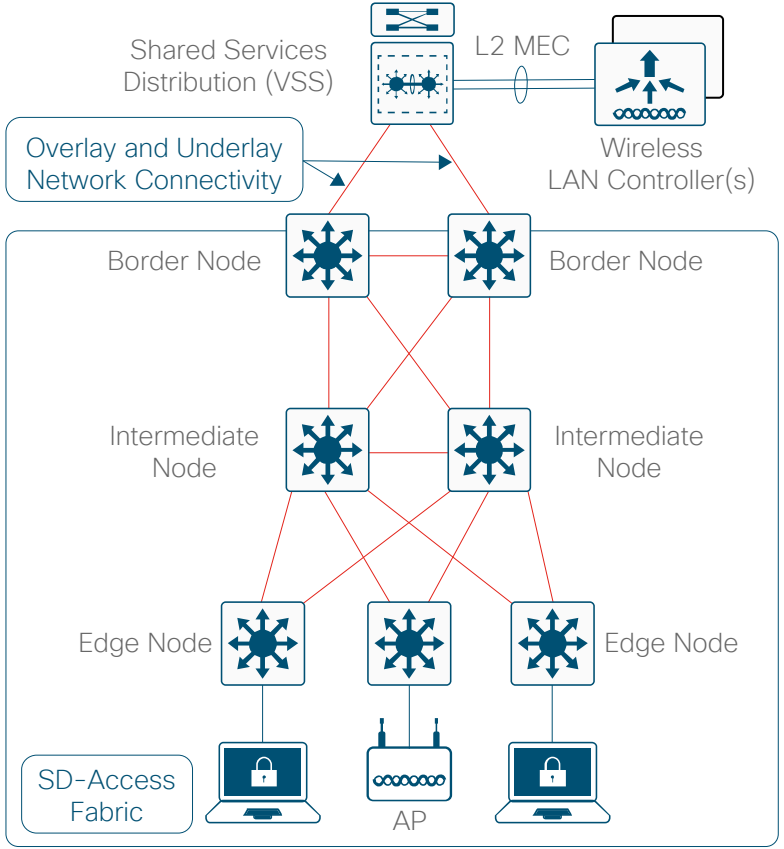
Cisco SD-Access Network Requirements

Latency Requirements (RTT)



SD-Access Wireless Connectivity

What you need to know

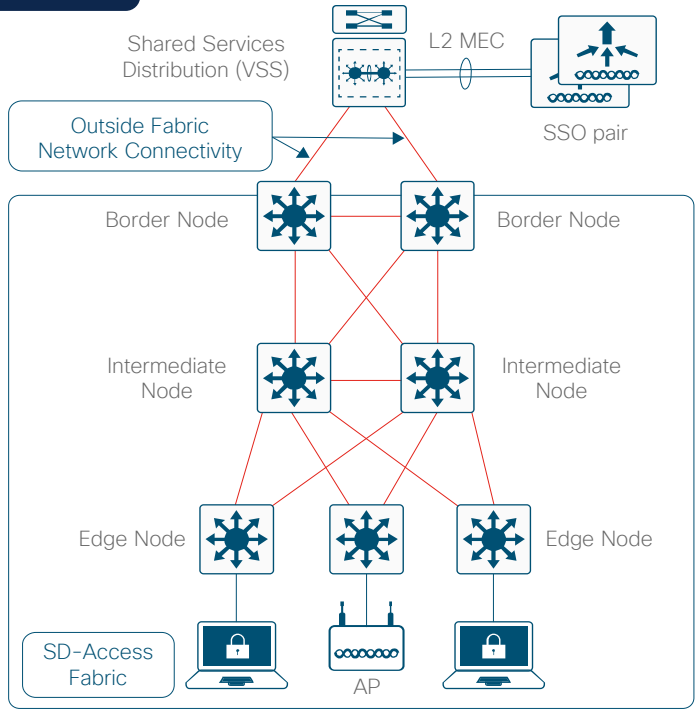


- WLC typically connect to a “shared services” Distribution Block
  - VSS/Stack is the preferred topology
  - Management IP address in Global Routing Table
  - Specific route to advertise WLC’s IP in the underlay
- WLC can talk to only #2 Enterprise CP nodes
- Access Points connect to Fabric Edge
  -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

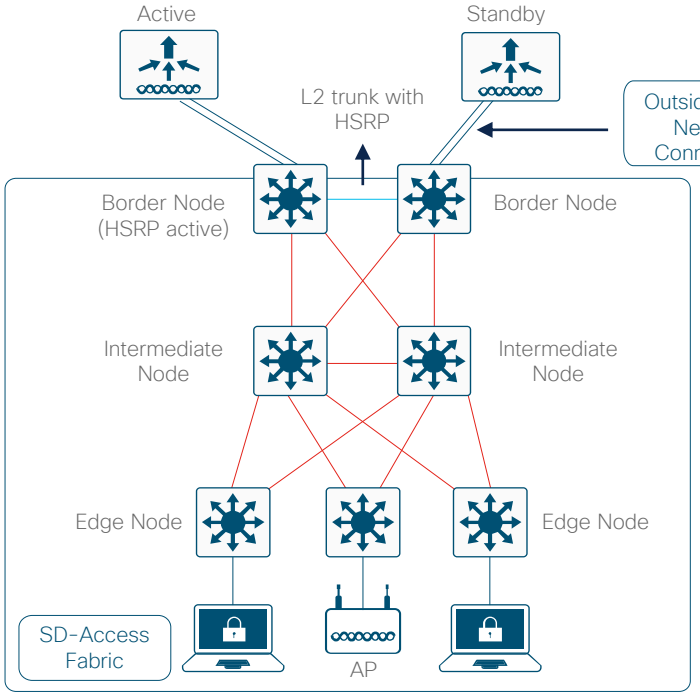
SD-Access Wireless Connectivity

How to connect an SSO pair of Fabric WLCs?

To a shared Service block



Directly to the pair of FBs



What products make SD-Access Wireless

SD-Access Support

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

- Digital Platforms for your Cisco Digital Network Architecture

Switching

Catalyst 9600

Catalyst 9400

Catalyst 9500

Catalyst 9300

Catalyst 9200

Catalyst 4500E

Catalyst 6800

Nexus 7700

Catalyst 3650 & 3850

Routing

ASR-1000-HX

ASR-1000-X

ISR 4451

ISR 4430

ISR 4330

ENCS 5400

Wireless

Catalyst 9800

Catalyst APs

AIR-CT8540

AIR-CT3504

AIR-CT5520

AireOS
Wave 2 APs

C9K EWC

IoT Extension

Cisco Digital Building

Catalyst 3560-CX

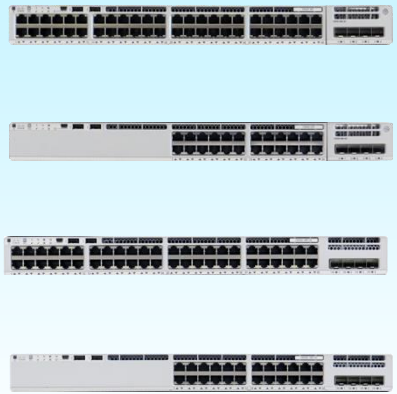
Cisco IE 3300, 3400, 3400H, 4000, 5000 series

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

SD-Access Platforms

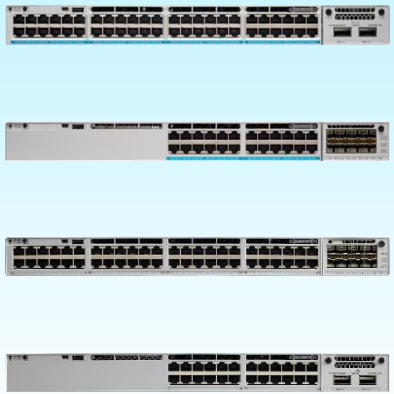
Fabric Edge Node for SD-Access Wireless

Catalyst 9200



- Catalyst 9200/L
- 1/mG RJ45
- 1G SFP (Uplinks)

Catalyst 9300

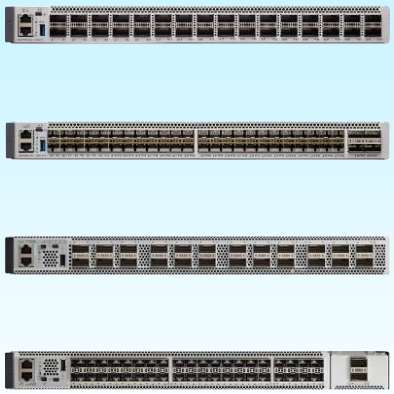


- Catalyst 9300
- 1/mG RJ45
- 10/25/40/mG NM

Catalyst 9400

- Catalyst 9400
- Sup1/Sup1XL
- 9400 Cards

Catalyst 9500



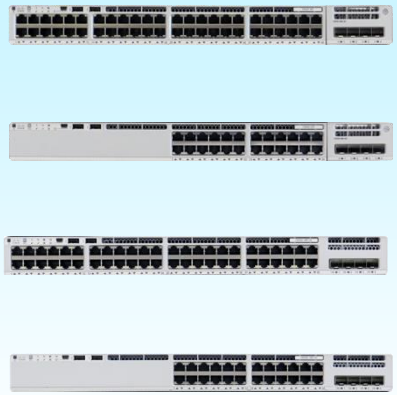
- Catalyst 9500
- 1/10/25G SFP
- 40/100G QSFP

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

SD-Access Platforms

Fabric Edge Node for SD-Access Wireless

Catalyst 9200



- Catalyst 9200/L
- 1/mG RJ45
- 1G SFP (Uplinks)

Catalyst 9300

- Catalyst 9300
- 1/mG RJ45
- 10/25/40/mG NM

Catalyst 9400

- Catalyst 9400
- Sup1/Sup1XL
- 9400 Cards

Catalyst 9500

- Catalyst 9500
- 1/10/25G SFP
- 40/100G QSFP

- Catalyst 9200 supports max 25 APs (# of VXLAN tunnels) and total 500 clients (both Wired and Wireless)
- Catalyst 9200L is not supported as a Fabric Edge for SD-Access Wireless
- Catalyst 9200 and 9200L do not support SD-Access Embedded Wireless controller

SD-Access Platforms

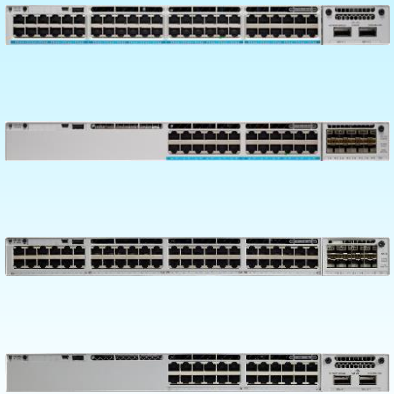
Fabric Edge Node for SD-Access Wireless

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

Catalyst 9200

- Catalyst 9200/L
- 1/mG RJ45
- 1G SFP (Uplinks)

Catalyst 9300



- Catalyst 9300
- 1/mG RJ45
- 10/25/40/mG NM

Catalyst 9400

- Catalyst 9400
- Sup1/Sup1XL
- 9400 Cards

Catalyst 9500

- Catalyst 9500
- 1/10/25G SFP
- 40/100G QSFP

- Catalyst 9300 is supported with full scale
- Catalyst 9300L is limited to 50 APs and total 1k clients (both Wired and Wireless)
- Same numbers for Fabric Edge and with Wireless Embedded Controller

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

SD-Access Platforms

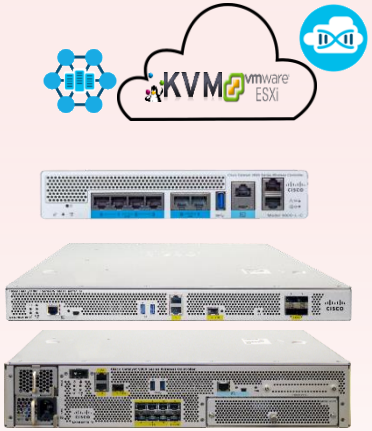
Fabric Enabled Wireless

* No IPv6, AVC, FNF

AireOS WLC

- AIR-CT3504
- AIR-CT5520
- AIR-CT8540

Catalyst 9800



- Catalyst 9800-40/80/L
- Catalyst 9800-CL

Wi-Fi 6, 11ac W2 APs

Catalyst APs

Outdoor APs (local mode) IW6300

- Wi-Fi 6 APs 802.11ax Cat 9105/9115/9120/9130/9136
- 11ac Wave2 Aps 1800/2800/3800 and 4800
- IW6300 Heavy Duty series

Catalyst 9800 for SD-Access Wireless

Optimized for Distributed Braches → Small and Medium Campus → Medium and Large Campus

For Switch

- Catalyst 9800 embedded wireless on Catalyst 9300
- 200 AP, 4k Clients
- Software Package activation
- Indirect AP Support
- Cisco IOS® XE Software
- Optimized for mobility
- Centralized Control Plane
- Always on Fabric with robust HA

For Private Cloud

- Catalyst 9800 for Private Cloud
  - 1k AP, 10k Clients
  - 3k AP, 32k Clients
  - 6k AP, 64k Clients
- Cisco IOS® XE Software
- Optimized for mobility
- Designed for IoT
- Always on Fabric with robust HA
- Scale on demand

On Appliance

- Catalyst 9800-L
- Catalyst 9800-4
- Catalyst 9800-80
- Cisco IOS® XE Software
- Optimized for mobility
- Designed for IoT
- Always on Fabric with robust HA

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

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

cisco Live!

ALL IN

#CiscoLive