cisco Live!

Let's go

The bridge to possible

Cisco Catalyst 9800 Configuration Best Practices

Justin Loo, Technical Marketing Engineer - Cisco Wireless

Justin Loo

Technical Marketing Engineer – Cisco Wireless

Fields of Expertise (4 Years at Cisco)

Cisco Catalyst 9800 Wireless LAN Controller, Cloud Monitoring for Catalyst Wireless

Personal Life

Born and raised in Southern California, University of California Los Angeles Alum

Hobbies

Traveling, Triathlon, Surfing, Trying new foods, Movies

Agenda

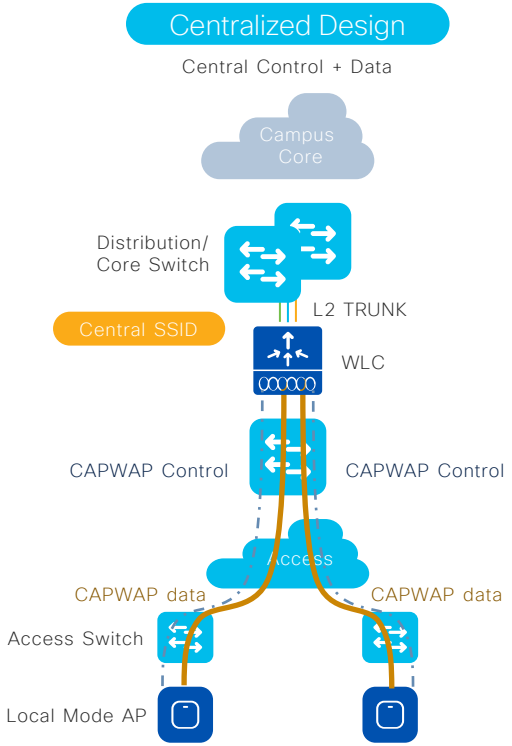
- Day 0
  - C9800 Design and Deployment
  - Wi-Fi 6E Migration Best Practices
- Day 1
  - WLAN Configuration
  - Site Tag and WNCd Load Balancing
  - RF Tag Recommendations
- Day 2
  - RF Monitoring
  - Optimization
  - Software Upgrades

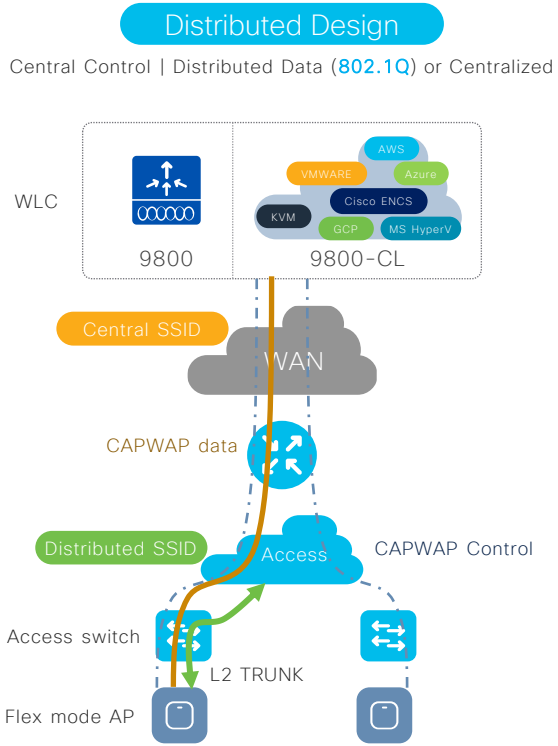
Day 0

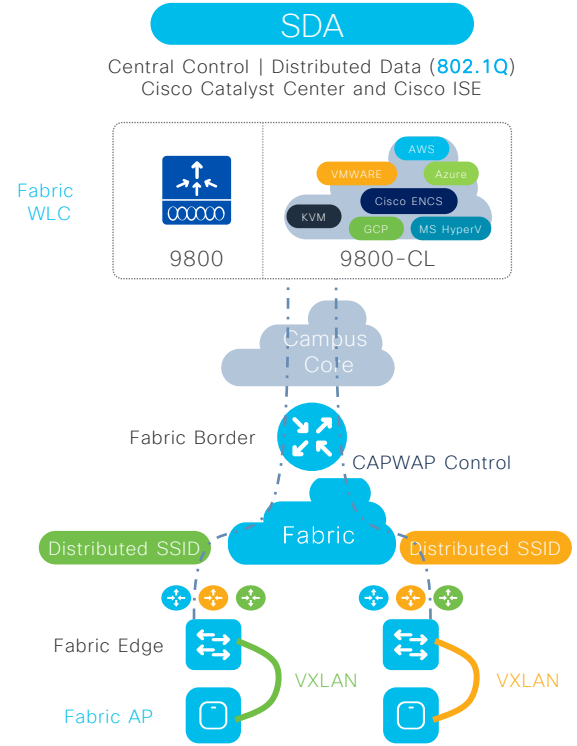
Cisco Catalyst 9800 On-Prem Deployment

Wireless Deployment Options

On-Prem Design







Local mode

- Mid to Large size Campus
- APs are in local mode
- Client traffic bridged at WLC in a L2 trunk
- Single point of entry into wired network
- Roaming is supported across all APs
- Latency < 20ms between AP and WLC

FlexConnect

- Distributed Enterprise design choice
- APs in Flex mode, across a WAN from WLC
- Per SSID: Client traffic is distributed at AP in L2 trunk or centralized via CAPWAP
- Roaming limited to APs in a Flex domain

Software Defined Access (SDA)

- Mid to Large size Campus
- APs are in Fabric mode
- Traffic distributed at AP via VXLAN
- Roaming is supported across all APs
- Latency < 20ms between AP and WLC

Next-generation wireless infrastructure for any scale

Cisco® Catalyst® 9800 embedded wireless[1]
200 APs, 4000 clients

Cisco Catalyst 9800-L
250 APs, 5000 clients,
5 Gbps

Cisco Catalyst 9800-L[2]
500 APs, 10000 clients,
9 Gbps

Cisco Catalyst 9800-40
2000 APs, 32,000 clients,
40 Gbps

Cisco Catalyst 9800-80
6000 APs,
64,000 clients
80 Gbps

Azure aws Microsoft Hyper-v KVM vmware Google Cloud Platform

Cisco Catalyst 9800-CL[3]
1000, 3000, or 6000 APs
10,000, 32,000, or 64,000 clients

Up to 200 APs | Up to 250 APs | Up to 1000 APs | Up to 2000 APs | Up to 6000 APs

Distributed branch and small campus | Medium campus | Large campus

[1] SD-Access only.
[2] Requires Performance License
[3] Cisco Catalyst 9800-CL for public cloud: Cisco FlexConnect® only

What Deployment Mode to Choose?

For your reference

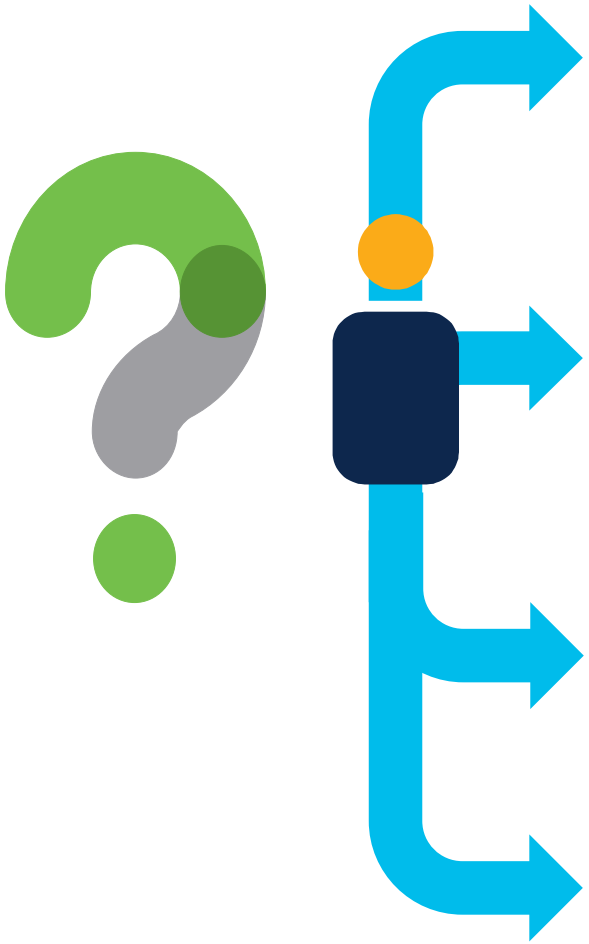
Campus / Enterprise		
Size	WLC	Deployment Mode
Large	Catalyst 9800-80	Local
Medium	Catalyst 9800-40	Local
Small	Catalyst 9800-L, Catalyst 9800-CL	Local

Branch or Distributed Enterprise		
Size	WLC	Deployment Mode
Large	Catalyst 9800-80, Catalyst 9800-CL	FlexConnect, IaaS
	Catalyst 9800-L, Catalyst 9800-CL	Local
Medium	Catalyst 9800-40, Catalyst 9800-CL	FlexConnect, IaaS
	Catalyst 9800-L, Catalyst 9800-CL	Local
Small	EWC, Catalyst 9800-L, Catalyst 9800-CL	FlexConnect, IaaS

Catalyst 9800 Recommended releases

What is the recommended release?

no more “gold star”



Go with 17.3.x:

- If you need support for 802.11ac W1 APs (IOS based APs)
- If you want the image with the “star”, with the most soak time in the field
- 17.3.8 has been released in September, recommended release for this train
- Recommended to upgrade to 17.9.x release train

Go with 17.6.x:

- If you want the most stable train for Wi-Fi 6 Catalyst Access Points without support for W1 APs (1700/2700/3700/1572)
- 17.6.6 has been released in September, recommended release for this train
- Recommended to upgrade to 17.9.x release train

Go with 17.9.x:

- If need support for newest Catalyst Wireless Wi-Fi 6E APs
- From 17.9.3, this train includes support for W1 APs to ease the migration to C9800 & Wi-Fi 6E
- 17.9.4a + APSP is recommended gold star release for all deployments

Go with 17.12.x:

- Only if you need support for 9166D and IW9167I, new countries supporting 6GHz, FIPS 140-3 compliance, and the new features in this release (VRF, Mesh on SDA, RF based load balance, etc.)
- 17.12.x supports 802.11ac W1 APs to ease the migration to C9800 & Wi-Fi 6E
- 17.12.2 is the recommended release

(*) Always check TAC recommendations: http://cs.co/recommendediosxe

Cisco Recommended Software Matrix*

Reference

IOS-XE	AP	IRCM with Gen 1 AireOS	IRCM with Gen 2 AireOS	Catalyst Center	Prime	CMX	Spaces	ISE
17.6.5	802.11ax 802.11ac W2	8.5.182.104	8.10.185	Matrix	3.10.1	10.6.3	2.3.1	3.1 3.0 2.7
17.9.4a	802.11ax (Wi-Fi 6/6E) 802.11ac W1 and W2	8.5.182.104	8.10.183	Matrix	3.10.2	10.6.3	2.3.1	3.2 3.1 3.0 2.7
17.12.2	802.11ax (Wi-Fi 6/6E) 802.11ac W1 and W2	8.5.182.104	8.10.190	Matrix	3.10.4 Update 1	10.6.3	3, May 2023 2.3.4	3.2 3.1 3.0 2.7

(*) Please bookmark and check these links for the latest info:
http://cs.co/compatibilitymatrix
http://cs.co/recommendediosxe
Catalyst Center Matrix https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/catalyst_center_compatibility_matrix/index.html

Wave1 AP support in 17.9.X & 17.12.X

Disruption free upgrade path to Wi-Fi6/6E

AP 1700, 2700, 3700
EOVSS/LDOS Apr 30,2024

AP 1572
EOVSS/LDOS Nov 30,2025

Why are we doing this?

To simplify migration of legacy APs (Wave1) to current generation Wi-Fi 6/6E APs for customer impacted by supply chain delays, **no extension in life cycle**

What is supported?

- Wave1 APs would operate with 17.9.3 & 17.12.x based WLC
- Solution matrix will be compatible with 17.9 release

What is new?

- EOVSS extended to LDOS . No change in LDOS dates
- Wave1 APs support in 17.9 release train starting 17.9.3
- Wave1 APs support extended to 17.12.x

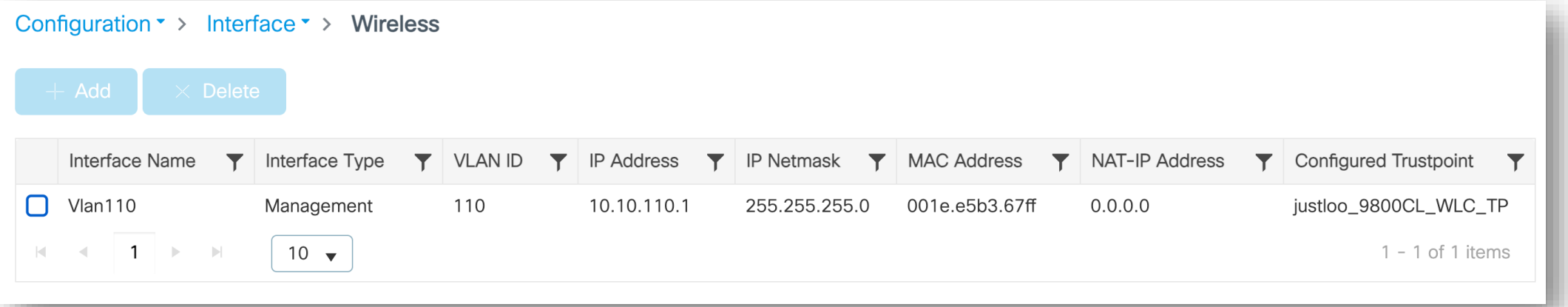
What is unchanged?

- Wave1 AP EOSM & LDOS dates
- Wave1 feature support (same as 17.3)
- April 2024 is LDOS, **need to continue update plans**

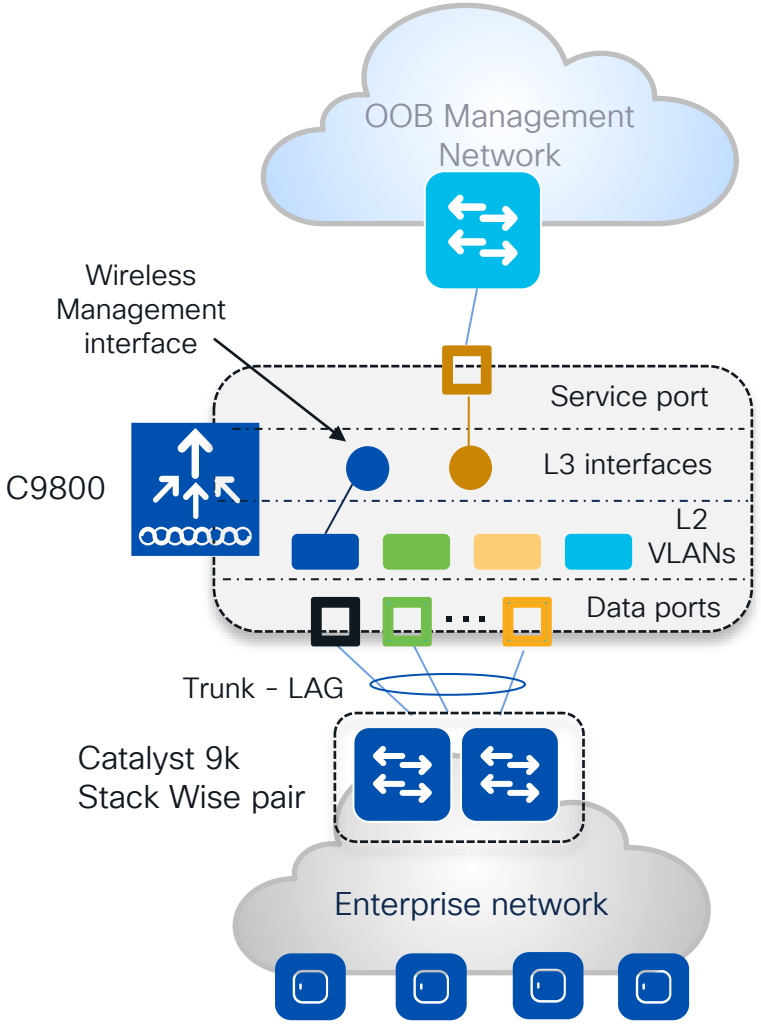
Controller Settings

Wireless Management Interface

- A Single Layer 3 interface used for terminating CAPWP traffic to APs and source any other management traffic
- Recommendations:
  - Configure as SVI for all C9800 appliances except C9800-CL Public Cloud
  - Tag with a VLAN



Port, VLAN, SVI interfaces considerations



Facts:

- It's mandatory to have one L3 interface configured as wireless management interface (WMI)
- CAPWAP traffic is terminated to the wireless management interface. There is only one wireless management interface
- Service port on the appliance belongs to the Management VRF ("Mgmt-intf"). On the C9800-CL the support for VRF is in the roadmap
- For centrally switched SSID, it is mandatory to configure a client L2 VLAN

Best practices:

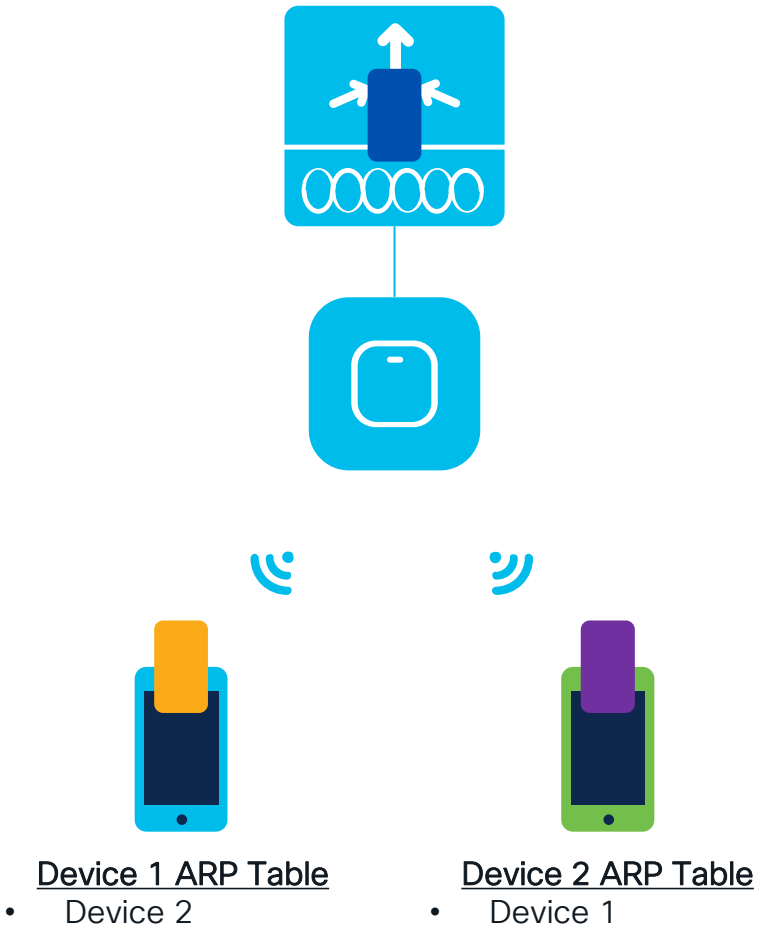
- Switch Virtual Interface (SVI) for wireless management interface is recommended.
- Do not configure SVIs for client VLANs, unless really needed (e.g., DHCP relay) – this is different from AireOS where Dynamic interface is required.
- Connect the uplink ports in a port-channel, configured as trunk to a pair of switches in Stack Wise virtual or similar technologies. Same AireOS best practice
- C9800-CL in public cloud must use a single L3 port (not SVI) and hence has the following feature limitation: no support for sniffer mode AP and HyperLocation

DHCP = Dynamic Host Configuration Protocol
VRF = Virtual Route Forwarding | VLAN = Virtual Local Area Network

Best Practice – Address Resolution Protocol (ARP) Proxy

- **Default Behavior**
  - C9800 forwards ARP traffic by changing destination MAC from broadcast to unicast
- **ARP Proxy**
  - Starting 17.3.1, C9800 can be configured to act as a proxy and respond on behalf of a registered client

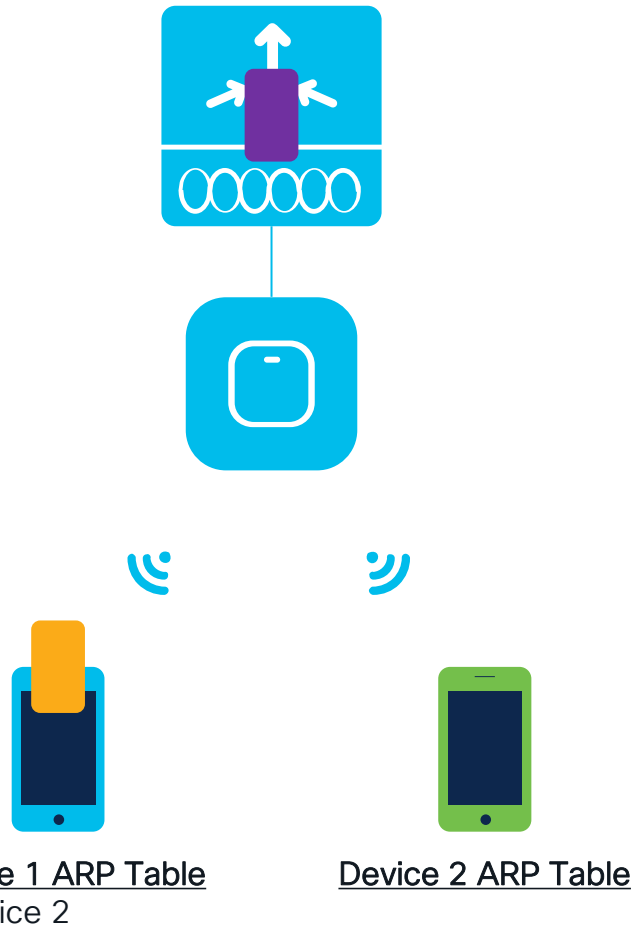
```
C9800# conf t
C9800(config)# wireless profile policy <name>
C9800(config-wireless)# ipv4 arp-proxy
```



Best Practice – Address Resolution Protocol (ARP) Proxy

- **Default Behavior**
  - C9800 forwards ARP traffic by changing destination MAC from broadcast to unicast
- **ARP Proxy**
  - Starting 17.3.1, C9800 can be configured to act as a proxy and respond on behalf of a registered client

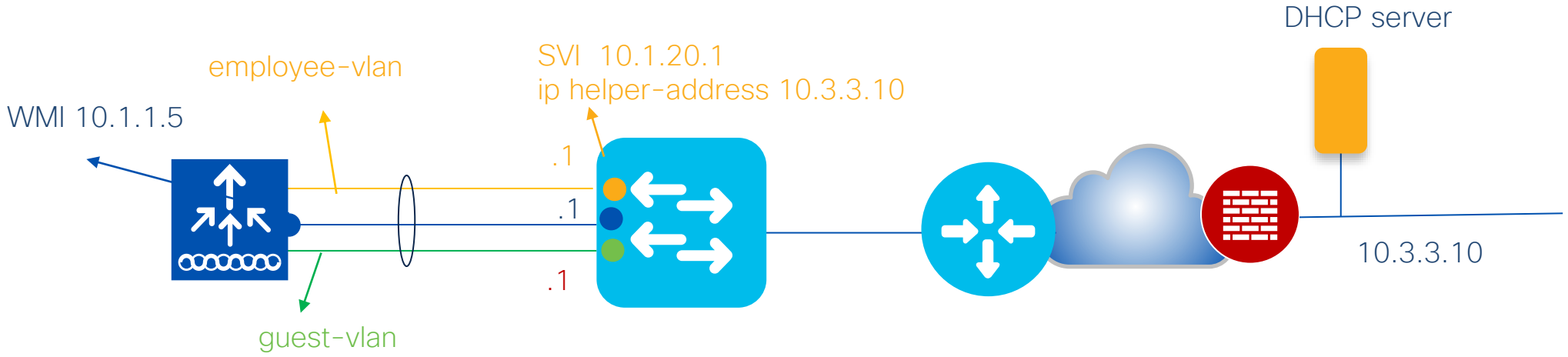
```
C9800# conf t
C9800(config)# wireless profile policy <name>
C9800(config-wireless)# ipv4 arp-proxy
```



- Device 2

Best Practice – DHCP proxy/relay

- **DHCP Proxy mode:**
  - In AireOS, enabling DHCP Proxy for wireless clients is a best practice
  - In C9800 DHCP proxy is not needed as IOS-XE has embedded security features like DHCP snooping, ARP inspection, etc. that don't require a L3 interface
- **DHCP relay or bridging mode?**
  - DHCP bridging is the **recommended mode** and should be used if DHCP relay can be configured on the upstream switch or if the DHCP server is on the client VLAN

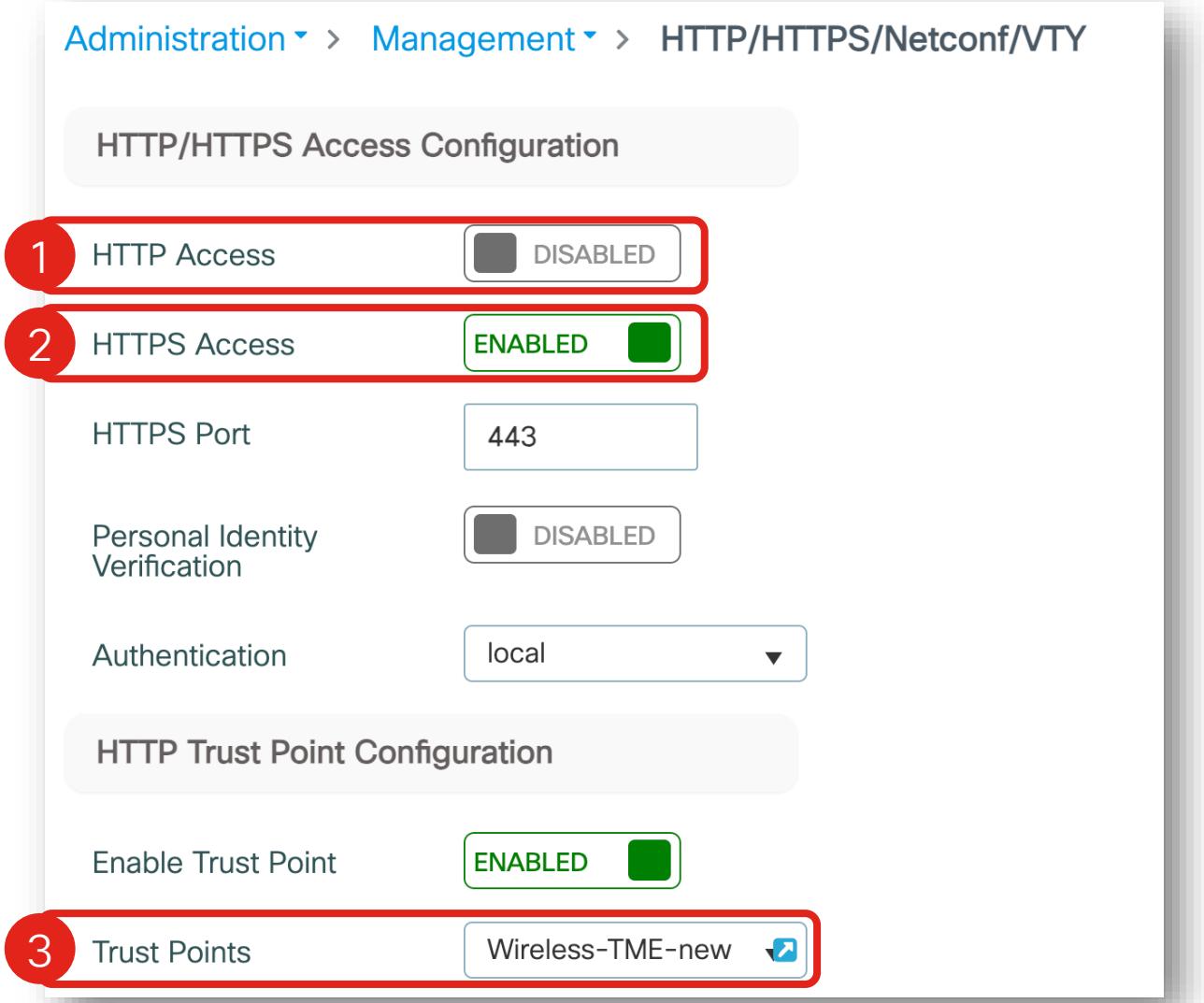


Using C9800 Internal DHCP Server

- Best practice is to use an external DHCP server
- Internal DHCP server – tested and supported across all platforms for a maximum of 20% of the box's maximum client scale.
  - For example, for a 9800-80 that supports 64,000 clients, the maximum DHCP bindings supported is around 14,000.
- Guidelines:
  - Configure SVI for the client VLAN and set the IP address as the DHCP server's IP address.
  - IP addresses are not preserved across reboots → Multiple clients can be assigned to the same IP address

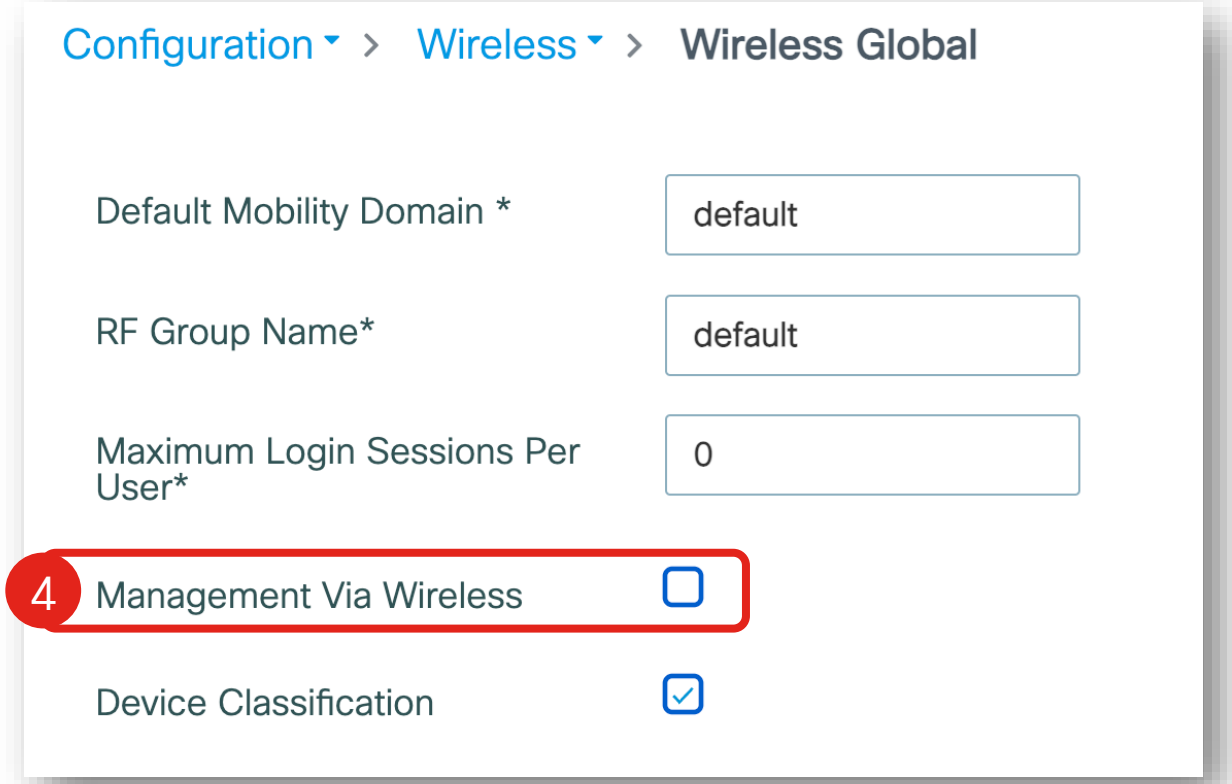
Enable Secure Web Management Access

1. Disable HTTP
2. Enable HTTPs
3. Manually configure trustpoint
4. Disable Management via Wireless (optional)



Enable Secure Web Management Access

1. Disable HTTP
2. Enable HTTPs
3. Manually configure trustpoint
4. Disable Management via Wireless (optional)



Password Encryption

Cisco IOS XE allows you to encrypt all passwords used on the box

Step 1: Define encryption key

```
C9800# configure terminal
C9800(config)# key config-key password-encrypt <key>
```

Step 2: Enable password Encryption

```
C9800(config)# password encryption aes
```

Note: There is no mechanism to decrypt passwords.

High Availability

High Availability

Reducing downtime for Upgrades and Unplanned Events

Unplanned Events
Device and network interruptions

- SSO Stateful Switchover
- N+1 High Availability
- LACP/PAGP w/ SSO
- Multi-chassis LAG
- AP Link Redundancy w/ C9136

Controller Software Update
Software Maintenance updates (SMU)

- Hot Patch (No Wireless Controller reboot) Auto Install on Standby
- Cold Patch HA install on SSO Pair

Access Point Updates
AP Updates and new AP models

- Rolling AP Update (No Wireless Controller Reboot)
- AP Device Pack New AP Model
- Flexible Per-Site, Per-Model Updates

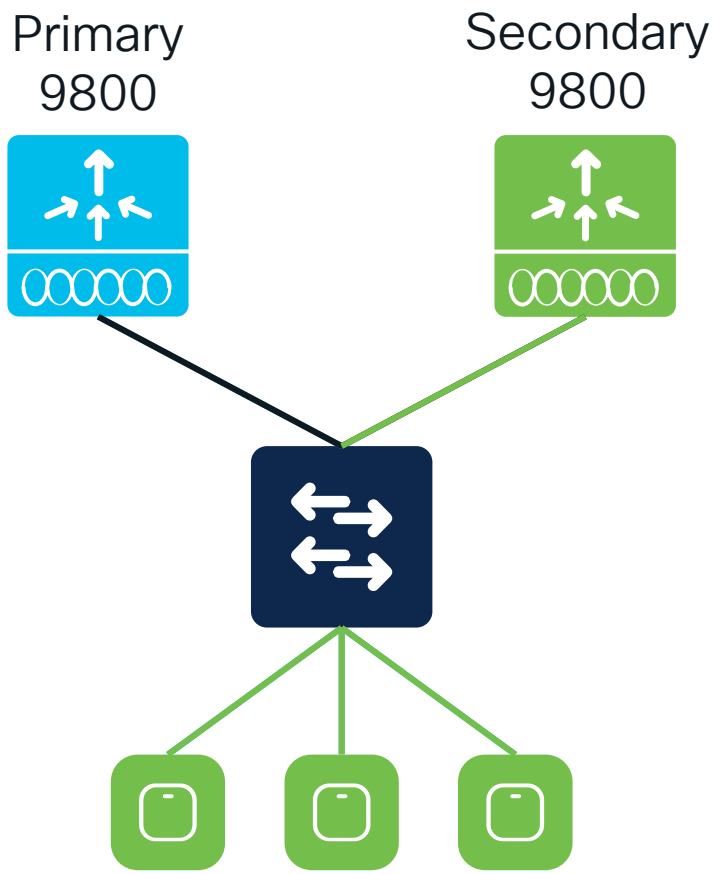
Software Image Upgrades
Wireless controller image upgrades

- N+1 Hitless Rolling AP Upgrade (All Sites or Site Based)
- In Service Software Upgrade (ISSU)

N+1 Redundancy

N+1 Redundancy

- Single C9800 serve as backup for N number of controllers
- Secondary WLC can be different model and software version
- Secondary WLC can be on different subnet
- Upon failover, APs will need to join the Secondary, and clients re-authenticate
- APs can be configured to automatically fallback to Primary
- Stateless Redundancy → Need to keep configurations between Primary and Secondary in synch



AP failover takes ~45-60 seconds

N+1 best practices

Primary and Secondary WLC should run the same software version → No AP Image Download

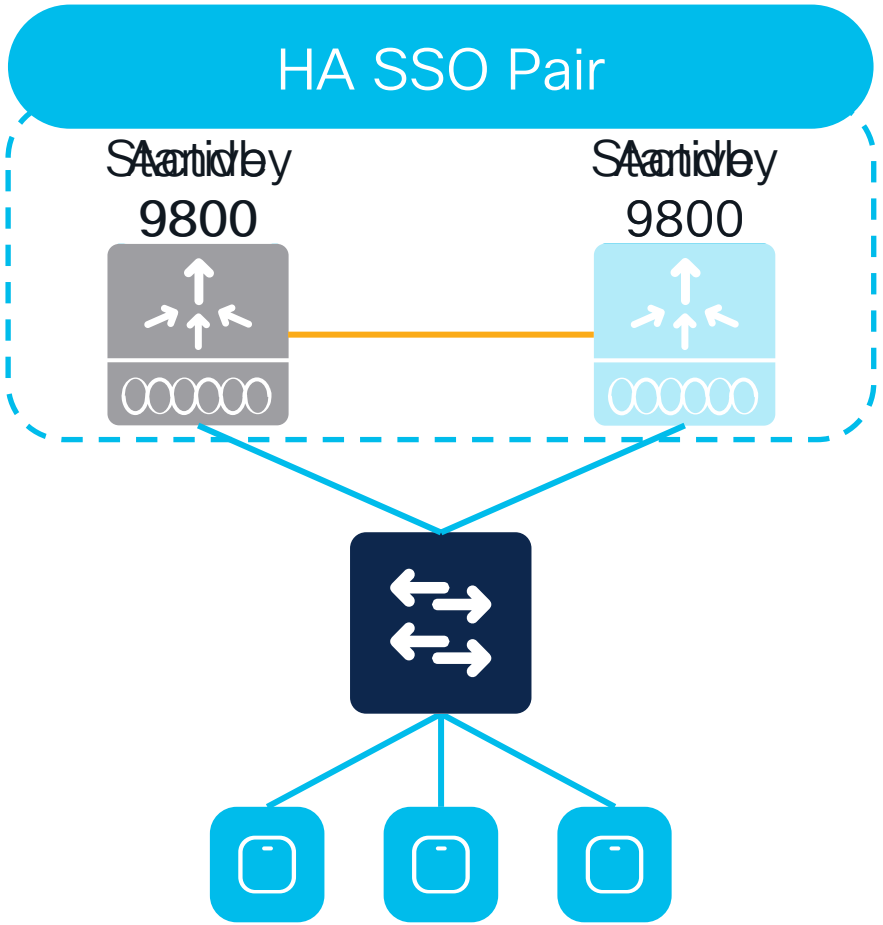
Configurations should be consistent across the Primary, Secondary, and Tertiary controllers (Use Cisco Catalyst Center to automate)

- WLANs
- Profiles and Policies
- Mobility Group
- Policy Tag
- Site Tag
- RF Tag
- AP-to-Tag Mappings

High Availability Stateful Switchover (HA SSO)

High Availability Stateful Switchover (HA SSO)

- Pair of 9800 in Active and Hot-Standby appear as a single WLC to the network
- All configuration synced between the pair for seamless, stateful switchover
- Clients and APs do not disconnect



AP failover takes order of sub seconds

SSO best practices

Forming SSO Pair

Appliance Type

- Physical Appliances: Use exact same hardware model
  - C9800-L-C cannot pair with C9800-L-F
- C9800-CL Private Cloud: Pick same scale (Large, Medium, or Small) and throughput (Normal or High) template for both VMs

Software

- Both boxes are running the same software and in the same boot mode
- **Install mode is recommend**

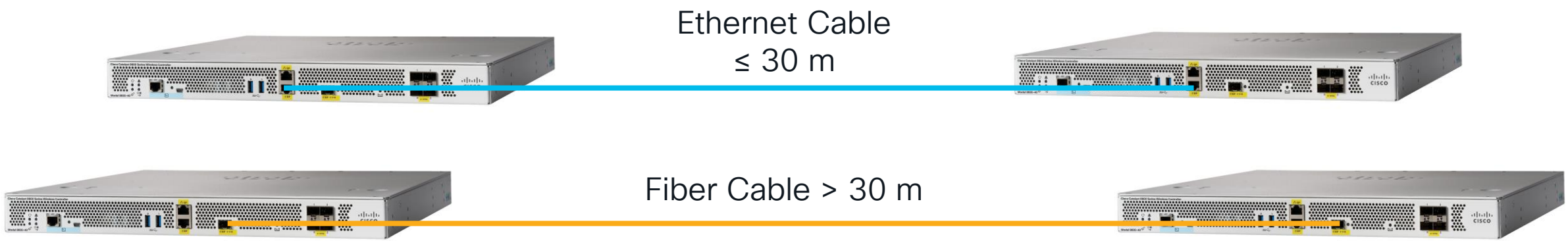
Configurations

- Configure using RMI+RP for dual active detection
- Set keep-alive retries to 5
- Set the higher priority (2) on the chassis that should be active
- For RMI+RP, renumber chassis prior to configuring to avoid Active-Active

SSO best practices

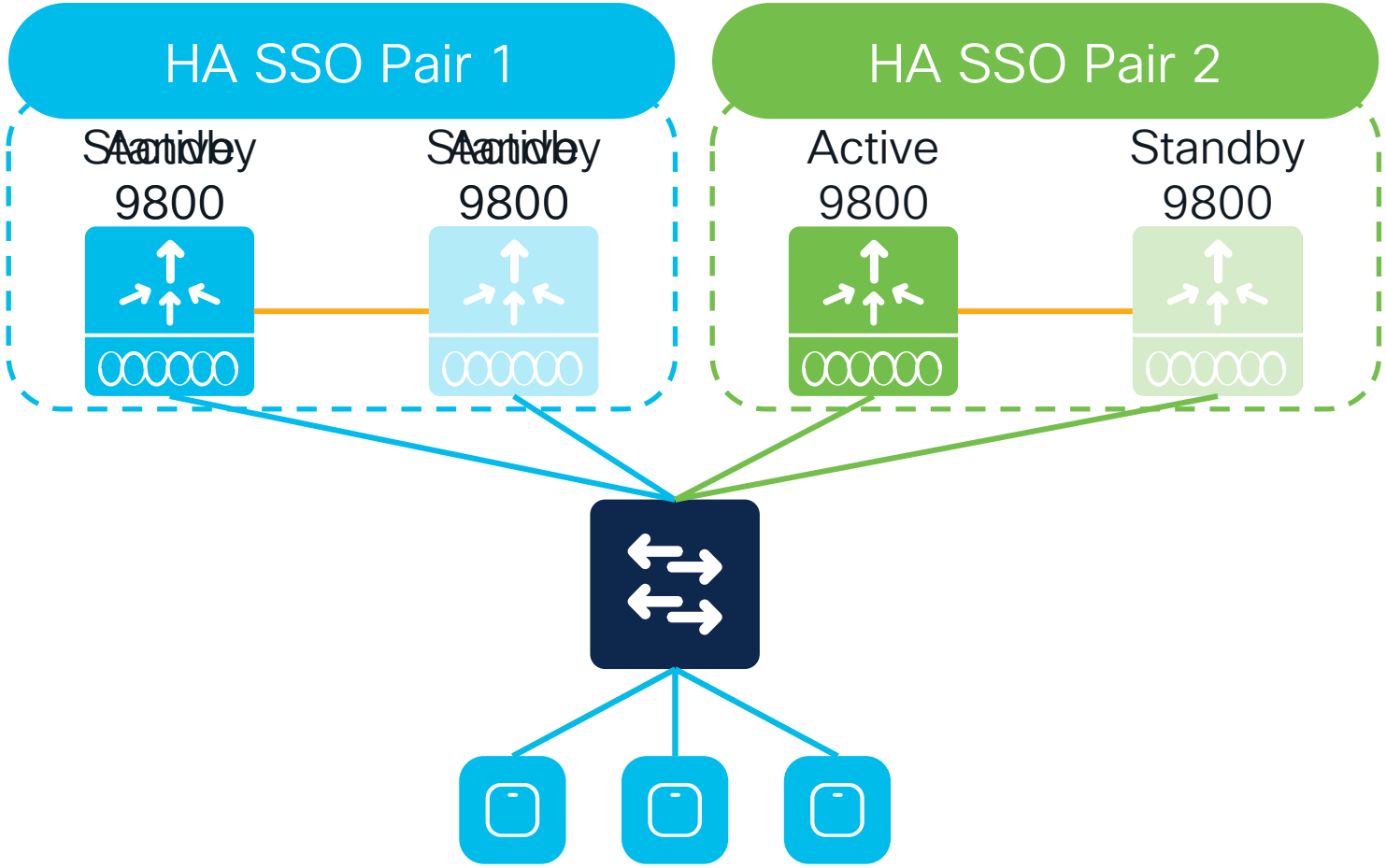
Back-to-Back Redundancy Port Connections

- For back-to-back RP connections on C9800-40/80:
  - 30 meters or Less (~100 feet): Use copper cable
  - Greater than 30 meters: Use fiber cable

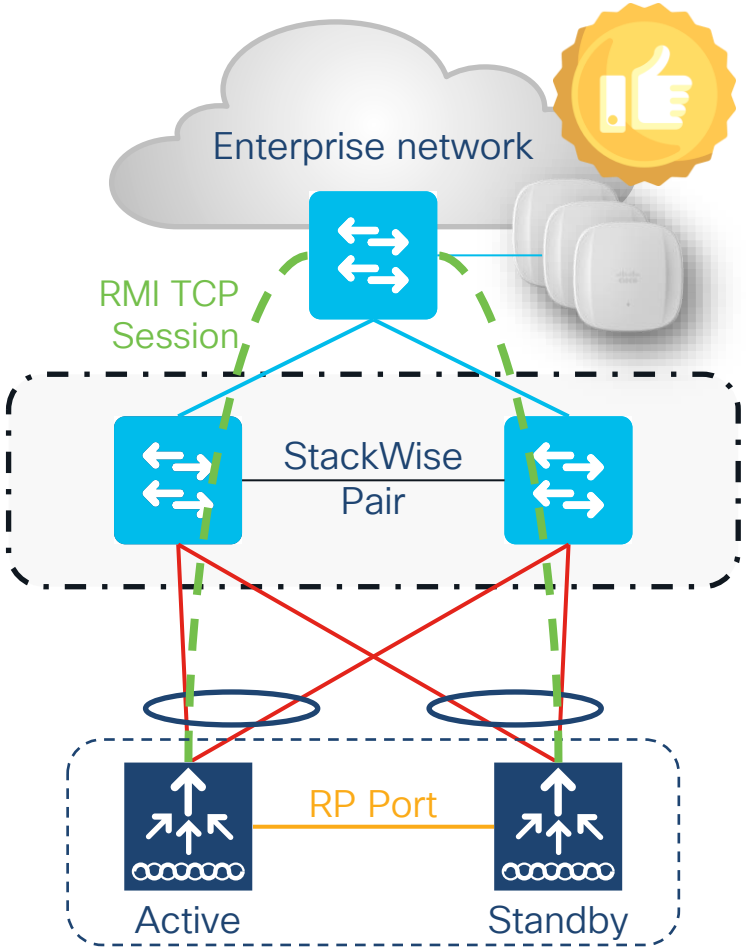


Redundancy with HA SSO and N+1

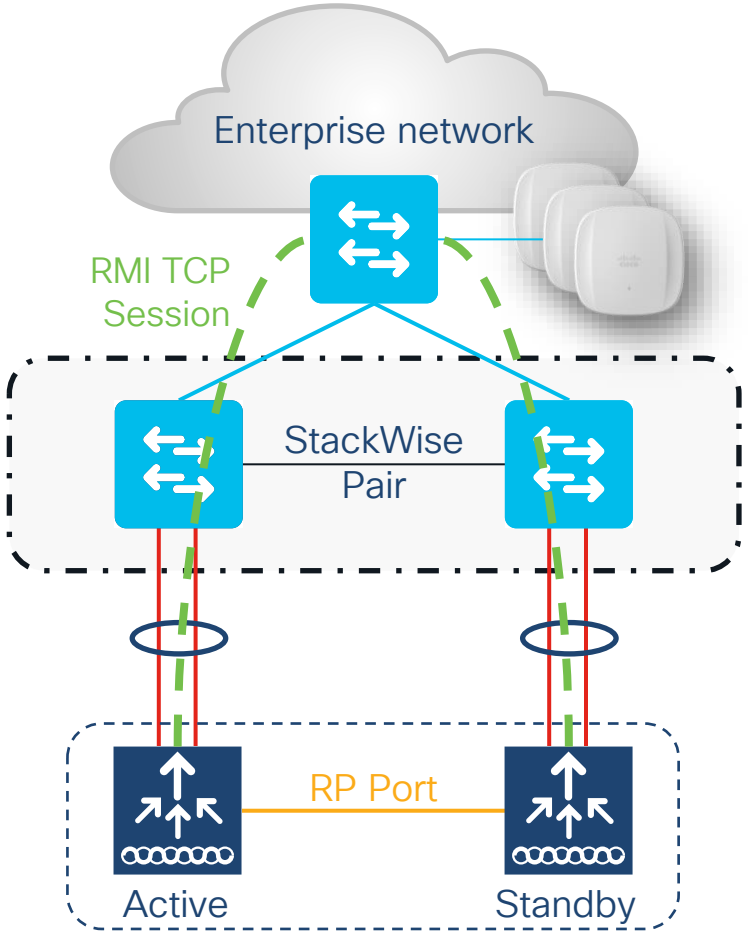
- Highest redundancy model
- Take advantage of sub-second failover
- Redundancy in the event SSO New-Active fails before the Old-Active is recovered
- Hitless upgrades for non-ISSU releases



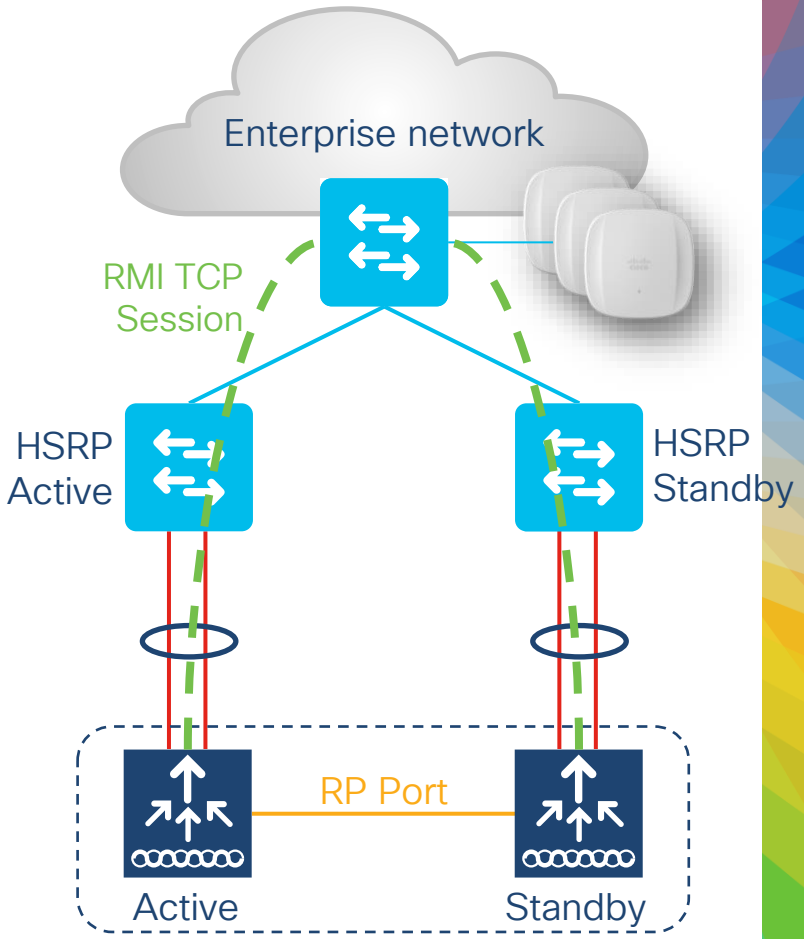
Connecting WLCs to Rest of Network



StackWise Pair with Split links



StackWise Pair without Split links



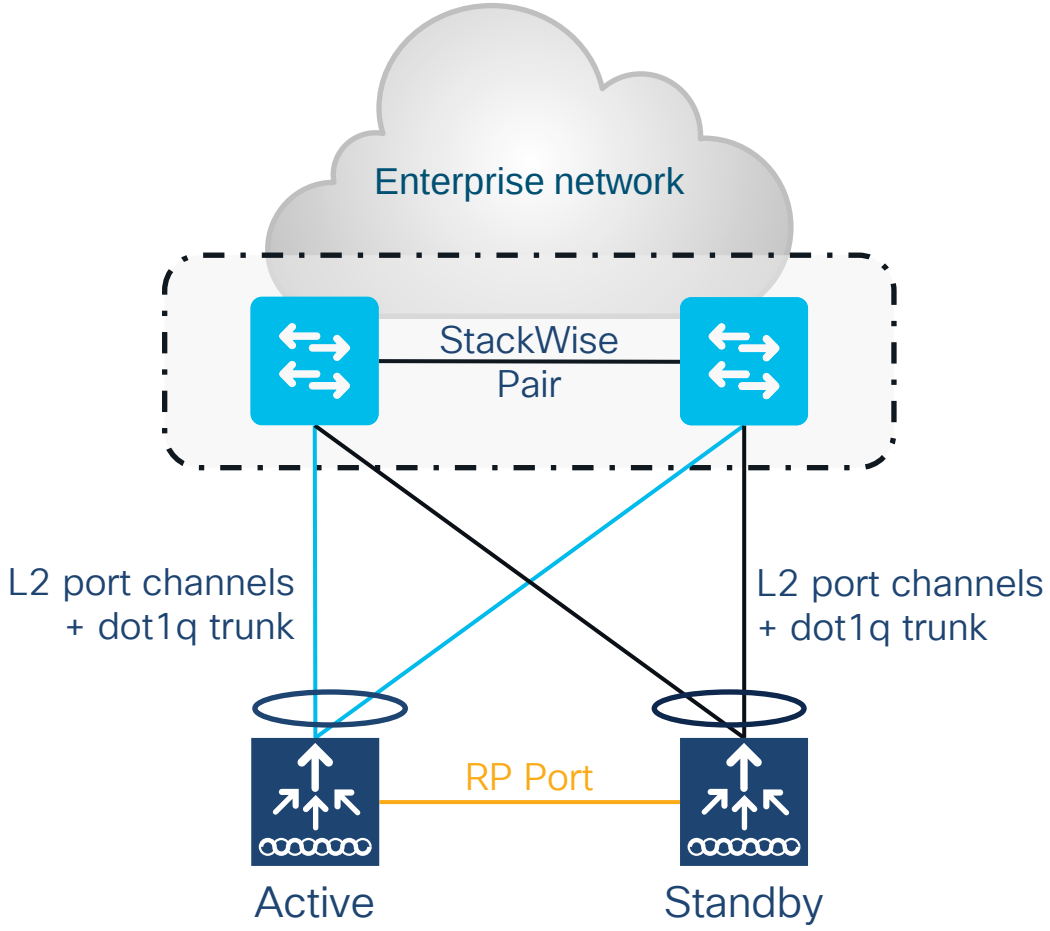
HSRP

Note: RP can be connected back-to-back or via L2 switches

StackWise Pair with split links

SSO HA Pair

Recommended



- For SSO HA, connect the Standby in the same way (same ports)
- Single L2 port-channel on each box. Ports connected to Active, and ports connected to Standby must be put in different port-channel
- Enable dot1q to carry multiple VLANs
- Make sure that switch can scale in terms of ARP and MAC table entries

Note: Spread the uplinks across the StackWise pair and connect the RP back-to-back (no L2 network in between)

Wi-Fi 6E: what’s the impact on migration?

Industry's best & broadest Wi-Fi 6E portfolio

9162

9164

9166D1

9166I

9136

MR57

9163E

Indoor Access Points

Outdoor Access Points

Management mode can be changed

What if I still have older controllers?

Configuration Migration Tool

- Migration tool managed by CX/TAC: https://cway.cisco.com/wlc-config-converter/

Cisco TAC Tool - WLC Config Converter

WLC Config Converter

Migrating wireless controllers to or from across any of these platforms: 2500/5500/7500/8500/WISM2/3650/3850/4500 S8E/5760/Catalyst 9800 controller

Please upload the following:
AireOS: "show run-config startup-commands" output or TFTP config backup
Converged Access: "show running-config" output

Details

TFTP config backup or 'show run-config startup-commands' output from AireOS WLC.

5520_config.txt
13.6 KB

Platform Conversion Type

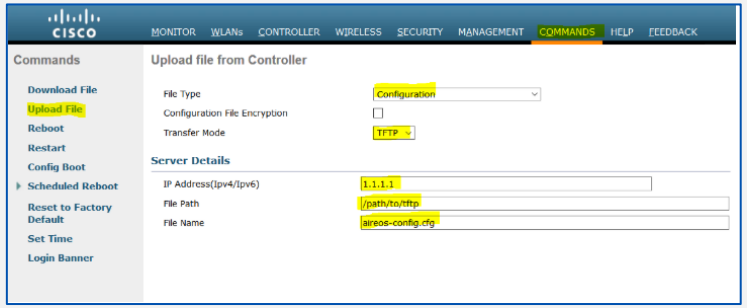
AireOS-->Catalyst 9800

Run

Choose the AireOS to C9800 converter and click Run

Drop the AireOS config file:

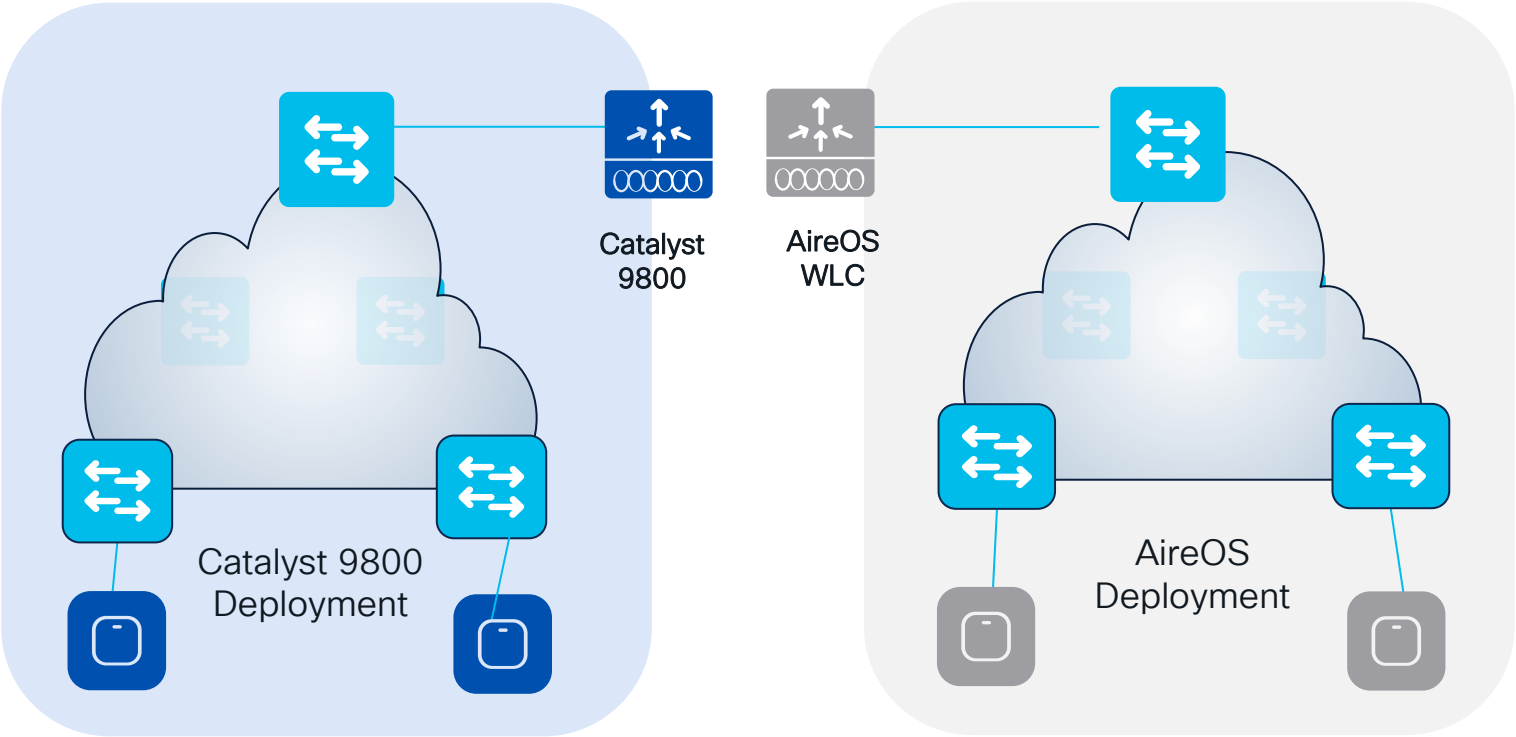
- Upload it directly from GUI:



- Or use the “show run-config command” output and put it in a .txt file

CX = Customer eXperience
TAC = Technical Assistance Center

AireOS and IOS-XE coexistence



Primary questions:

- Is **seamless roaming** needed?
- Is **Guest Anchor** deployed?
- Is a unique Dynamic Channel and Power plan needed across Controllers (Cisco **RRM**)?

Inter Release Controller Mobility (IRCM) is your friend!

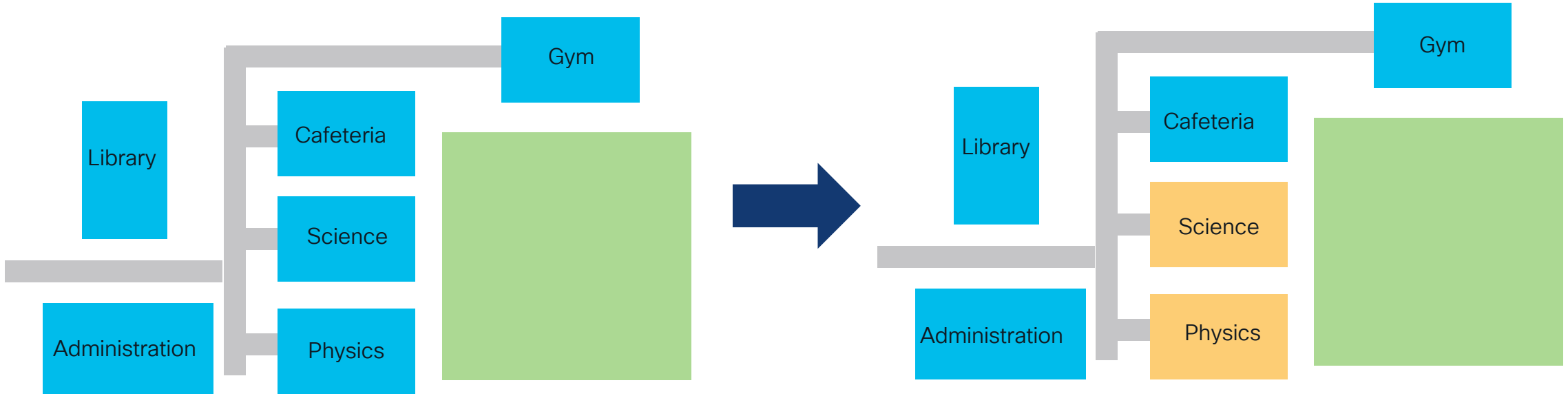
RRM = Radio Resource Management

Customer Migration Scenario

2.4/5 GHz

2.4/5/6 GHz

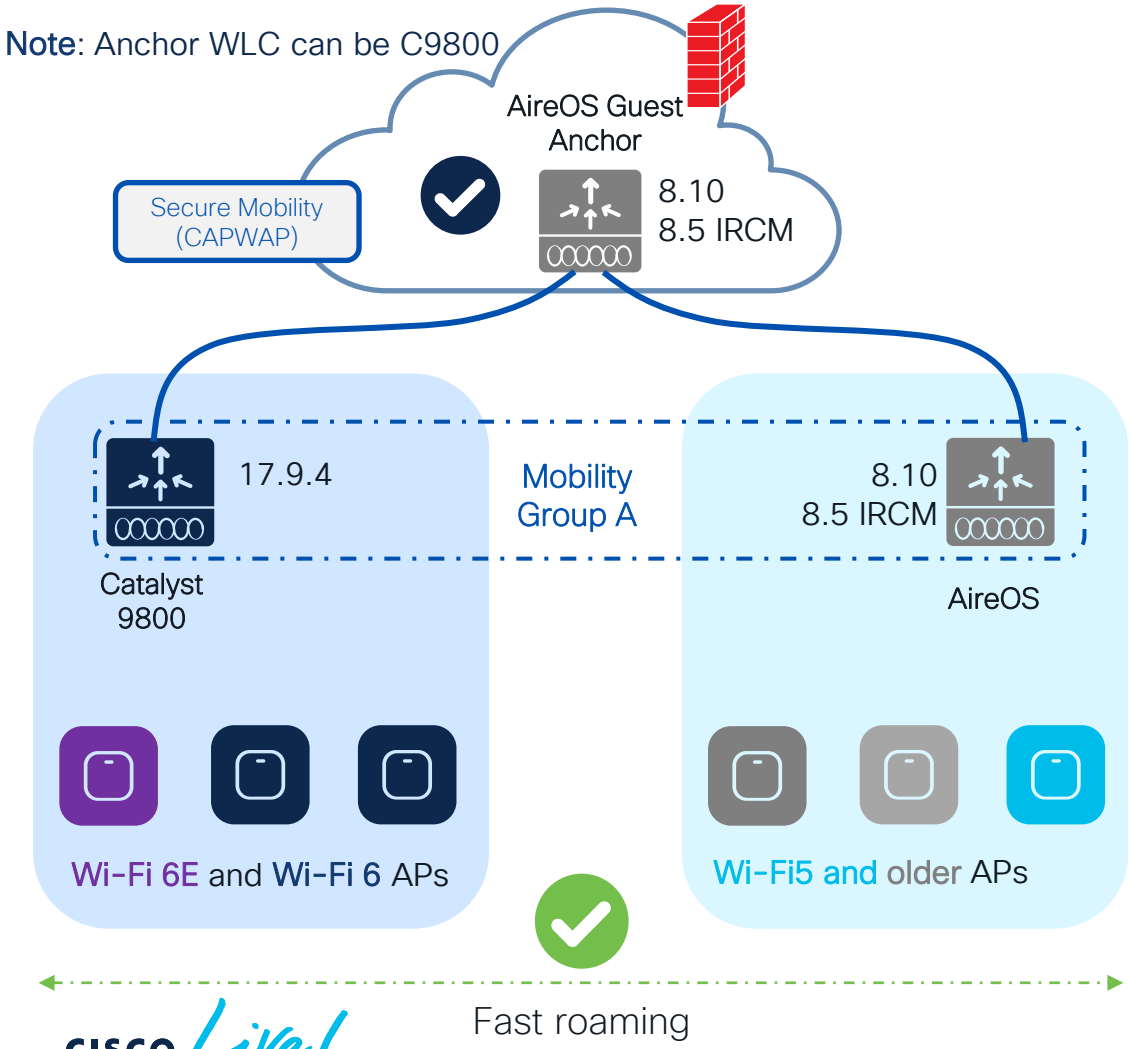
- Move “per RF blocks”
- Move a building or complete floor into the new hardware and software



Avoid “Sale & Pepper” deployments. Do not mix APs on different WLCs at same time.

How do I start adopting 6GHz?

Answer: Inter Release Controller Mobility (IRCM)

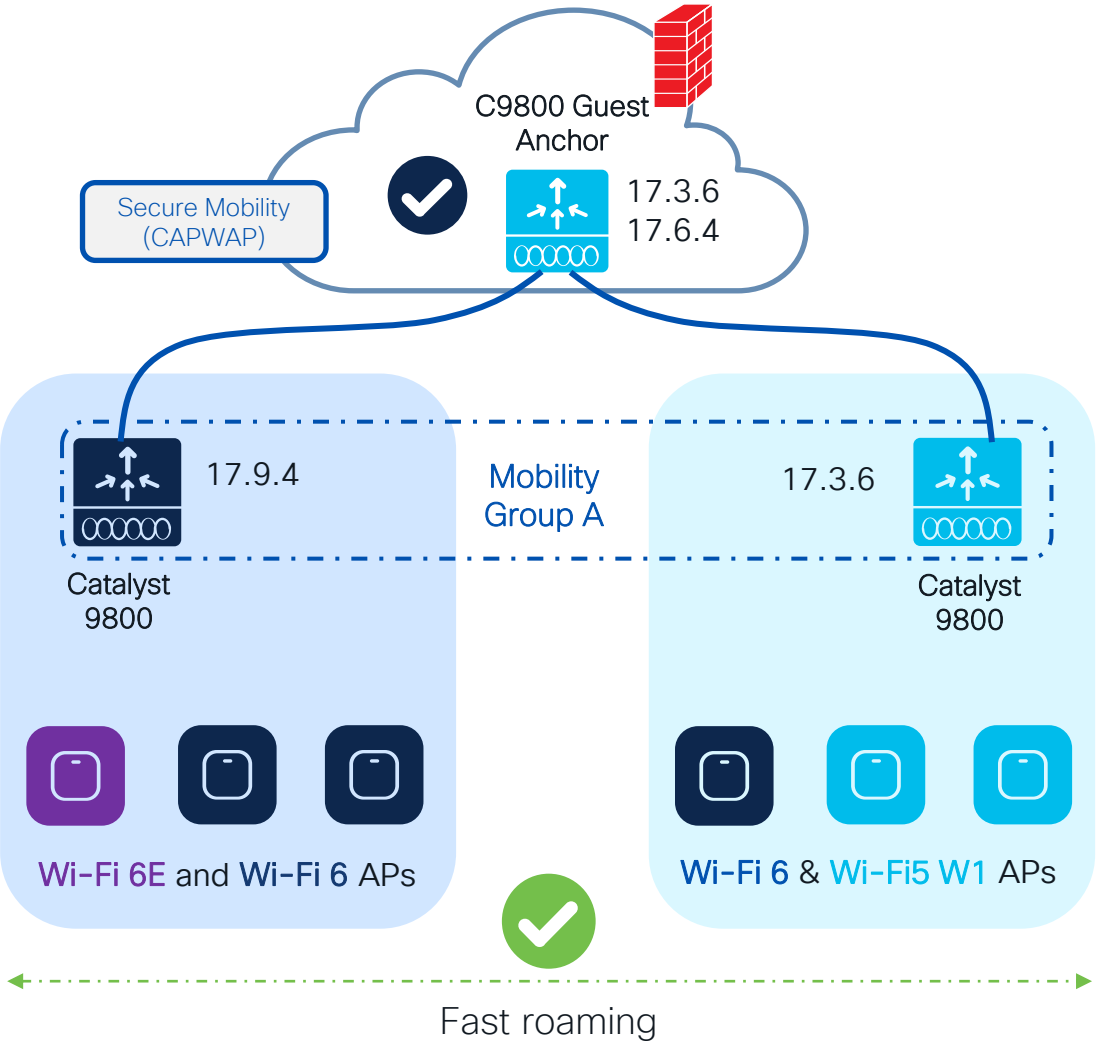


Scenario 1: AireOS WLC supports IRCM

- Introduce new 6/6E AP hadware on the new C9800 and support seamless roaming and Guest Anchor with existing networks
- This method allows the smooth coexistence of both WLCs, with RF areas migrated as needed, without any overnight switchover.
- Things to consider:
  - If the controller is limited to 8.5 (5508, 8510), we will need a special IRCM version (8.5.182.104), to connect them to IOS-XE
  - TIP: Always configure the primary/secondary WLC in APs. The new WLC will reject unsupported APs, but if any AP could work in both controller types, this will avoid APs joining the wrong one, or flip-flopping between them, until the migration is ready to proceed
  - Fast & secure roam will only be supported if the WLAN profile is the same on the two WLCs

How do I start adopting 6GHz?

Answer: Inter Release Controller Mobility (IRCM)



Scenario 2: Catalyst network with W1 APs

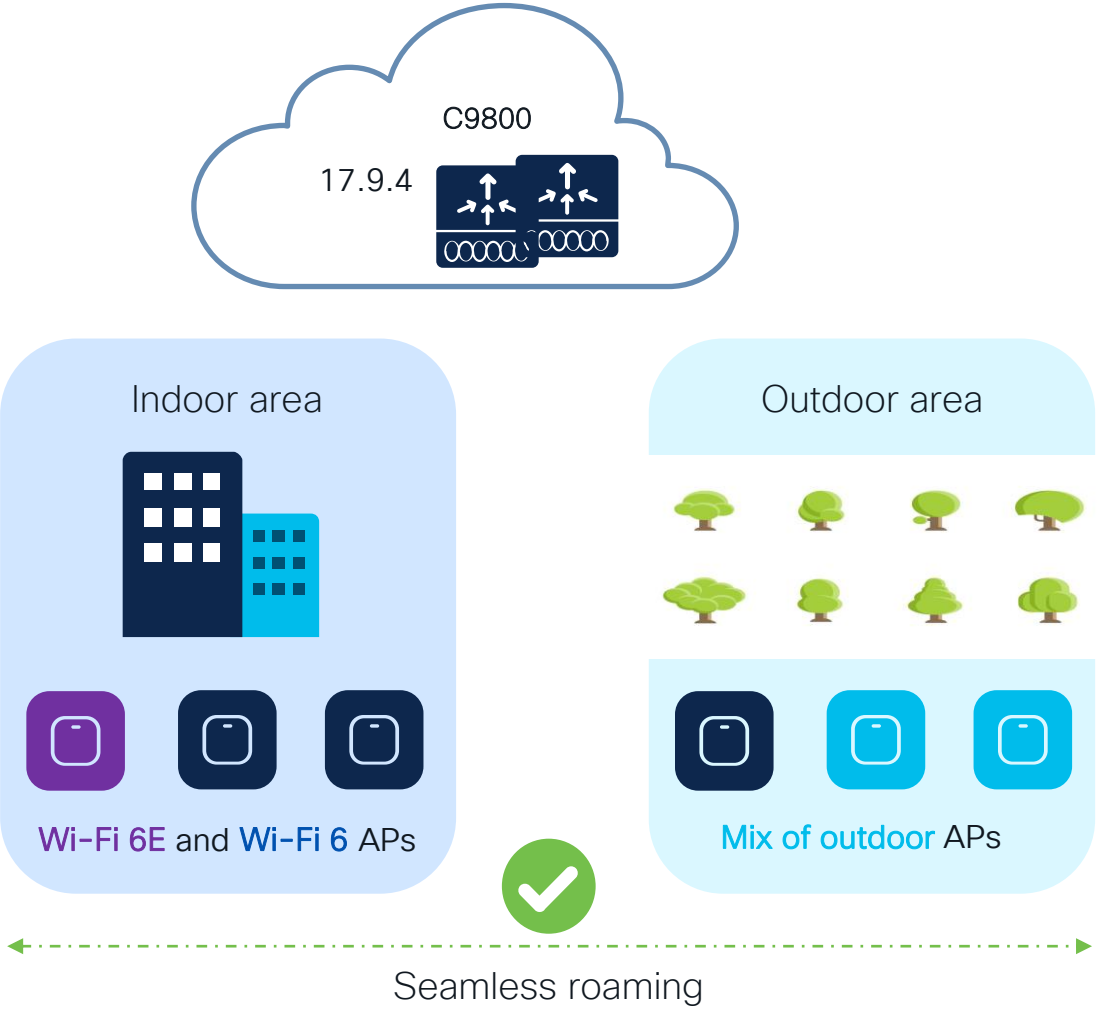
If you have already started your C9800 journey but Wave 1 APs are still present (1700/2700/3700).

- Introduce new AP hadware on the new supported IOS XE release and support seamless roaming and Guest Anchor with exsiting C9800 networks
- The release combination shown have been tested at scale, check IRCM deployment guide*
- Fast & secure roam will only be supported if the WLAN profile is the same on the two WLCs
- Pace your migration by moving APs when ready
- **Note**: Anchor can be on AireOS as well (8.10 or 8.5 IRCM latest

(*) https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller-aireos_ircm_dg.html

How do I start adopting 6GHz?

What about outdoor areas?

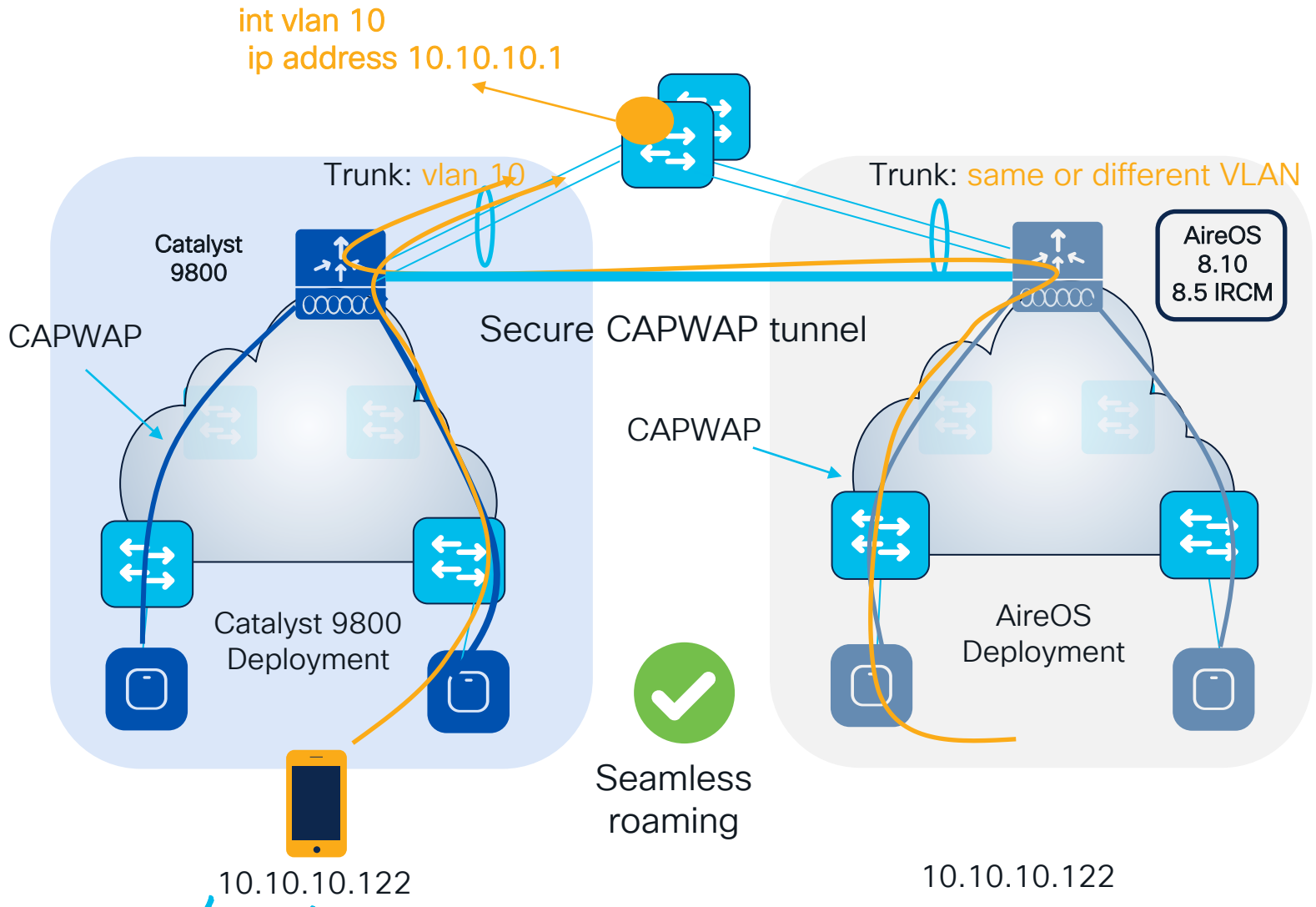


Scenario 3: Mixed indoor and outdoor areas

- Wi-Fi 6E is not available outdoor yet
- Wi-Fi 6E SSIDs will not be broadcasted outdoor
- WLAN Design*:
  - Define a new WLAN/SSID with support for 6Ghz and WPA3 in all bands. This will give you the possibility to have fast & secure roaming between indoor and outdoor
  - Configure two WLANs with same SSID, one with support for 6Ghz and one only 2.4 and 5 Ghz. This would support slow roam only (client will authenticate again and start fresh on roam-to WLC). The roaming can still be seamless (same client IP is maintained)

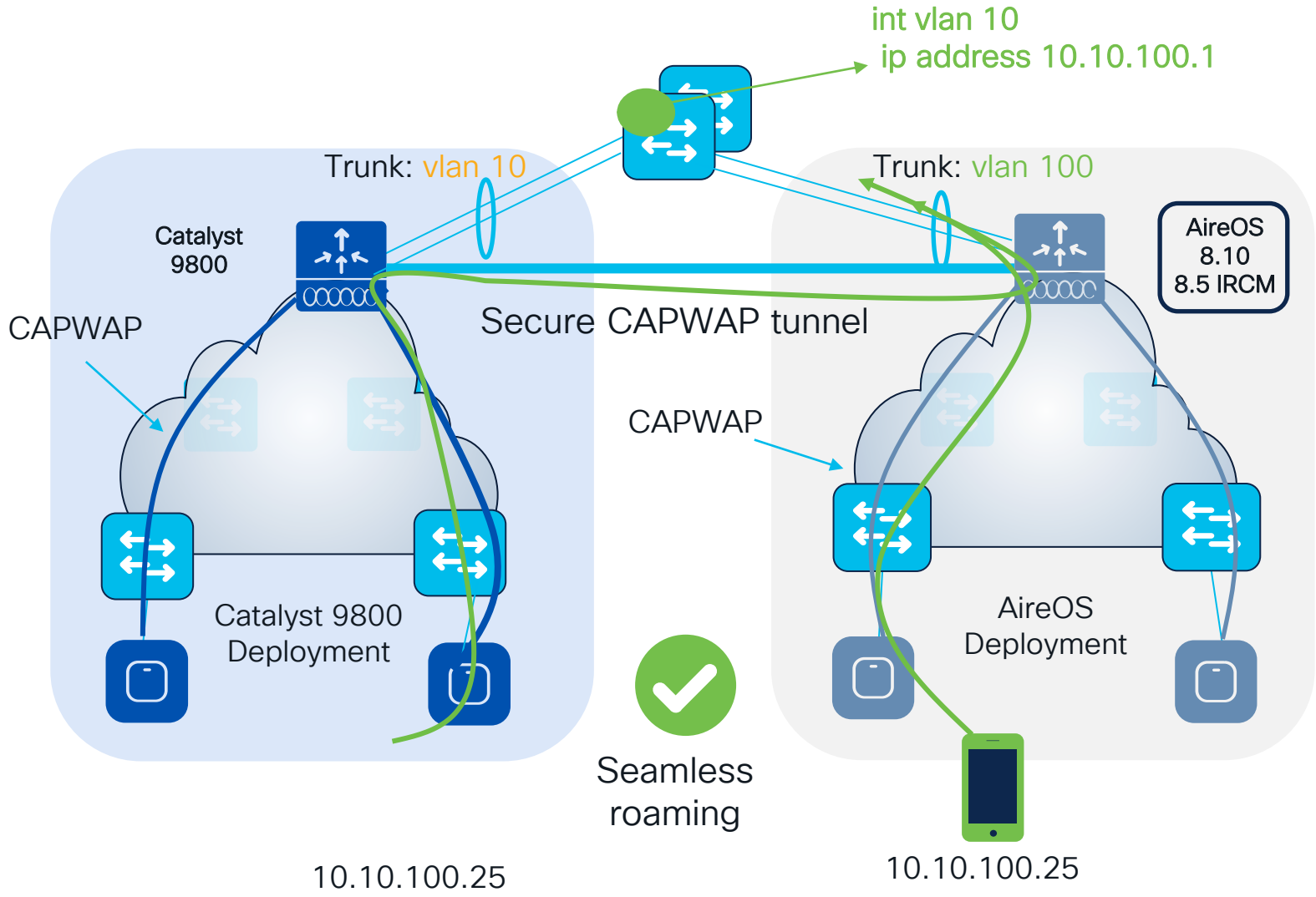
(*) for more details on WLAN Design, please refer to “Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points” - BRKEWN-2024

AireOS and IOS-XE coexistence – Roaming



- All client roaming between AireOS WLC and C9800 are **L3 roaming**
- The client session will be anchored to the first WLC that the client has joined
- **The point of attachment to the wired network doesn't change** when roaming between C9800 and AireOS and vice versa
- This is independent of the VLAN mapped to the SSID on the wired side

AireOS and IOS-XE coexistence – Roaming

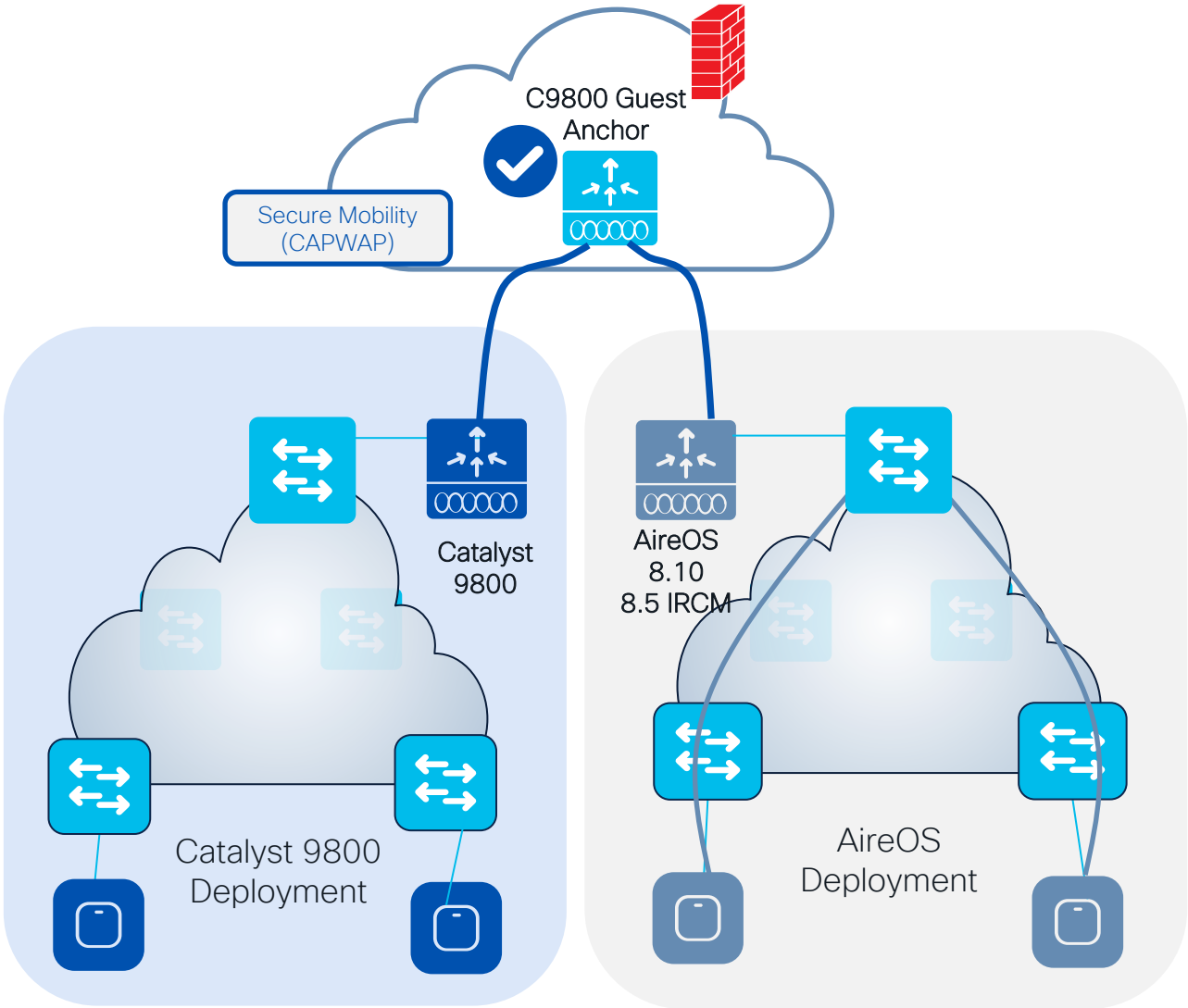


Recommendations:

- In the Design Migration phase, whenever possible, **use different VLAN IDs and use different subnets**
- Consequence: clients will get a different IP whether it joins first 9800 or AireOS; seamless roaming is anyway guaranteed
- When this might not be possible:
  - Customer is not willing to change the VLAN design when adding C9800 (this might include AAA and Firewall changes)
  - Customer leverages Public IP subnets so they don't have another subnet to assign
  - Customer leverages Static IPs

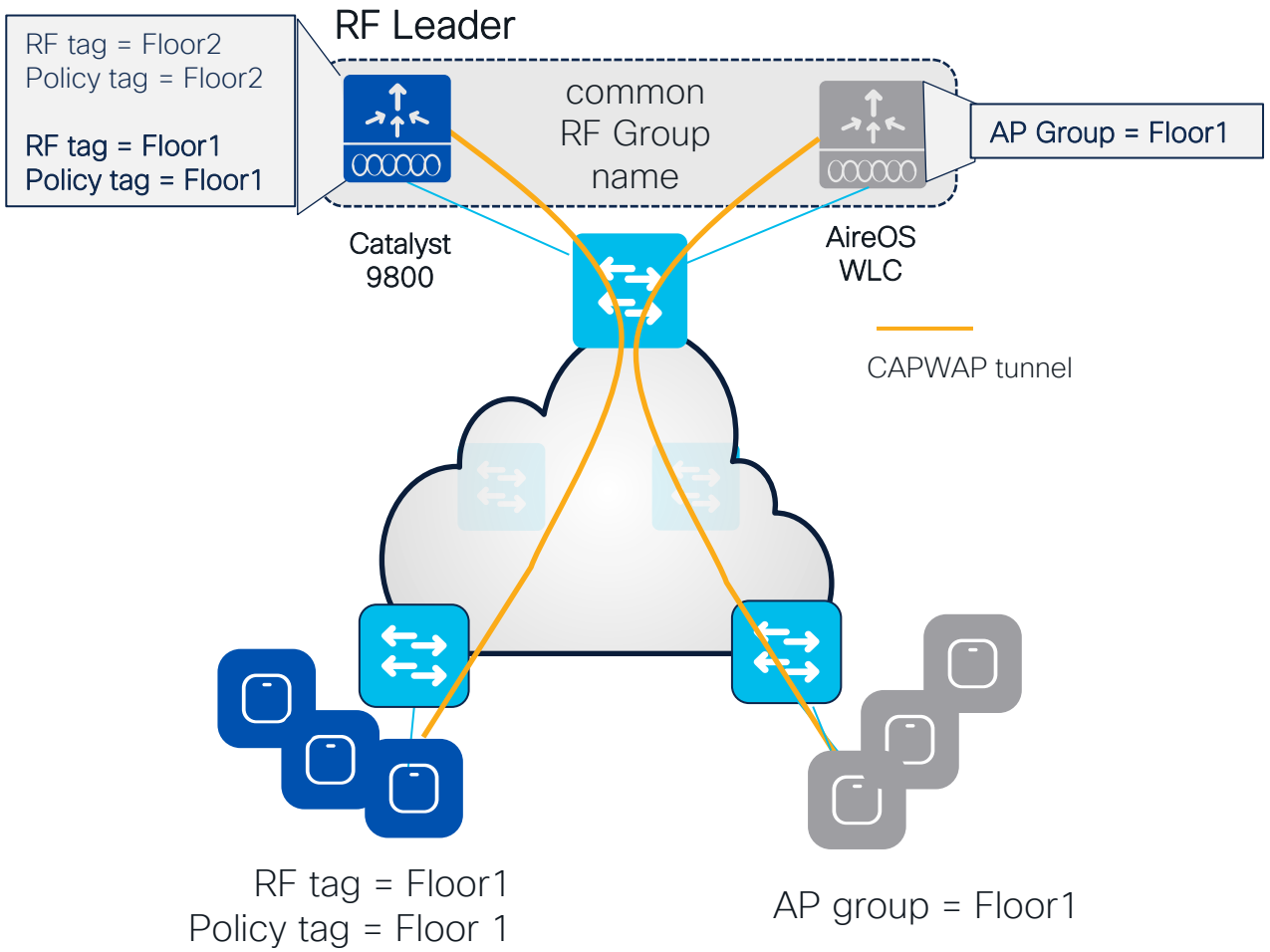
AireOS and IOS XE IRCM – Guest Anchor

- For software compatibility, follow IRCM rule of N+/-2 (with N = your release)
- List of parameters that must match between Foreign and Anchor:
  - WLAN and Policy profiles names
  - WLAN profile > security settings
  - Policy profile > DHCP settings need to match
  - WebAuth parameter-map name and type
- **Note:** When anchoring to and from AireOS, use the 8.10 or 8.5 IRCM image and match WLAN profile name, security and DHCP settings



AireOS to C9800 migration – common RF Group

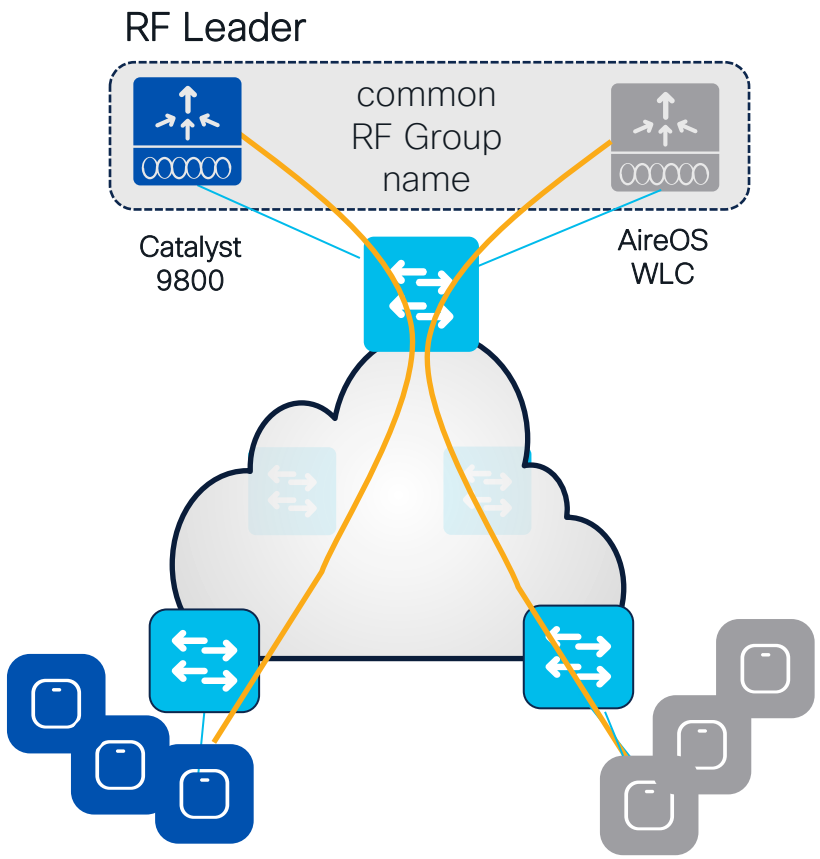
RRM works in a mixed controller environment and we can have one RF master:



- C9800 and AireOS controllers can create one RF domain and share a common RF plan
- The RF group name on both AireOS and C9800 controllers needs to match
- 8.8 is required on AireOS
  - A RF leader is elected (based on controller capacity) and common channel and power plan will be used for all APs
  - APs will be not show up as rogue on the other controller
- NOTE: in a scenario where you want to have custom RF profiles or enable FRA, then the leader (e.g., C9800 controller) needs to have Policy and RF tags matching the names of the AP Group names on AireOS WLC. Of course, the settings of RF profiles on both controllers need to match as well.

AireOS to C9800 migration - common RF Group

RRM works in a mixed controller environment and we can have one RF master:



Lower priority

Higher priority

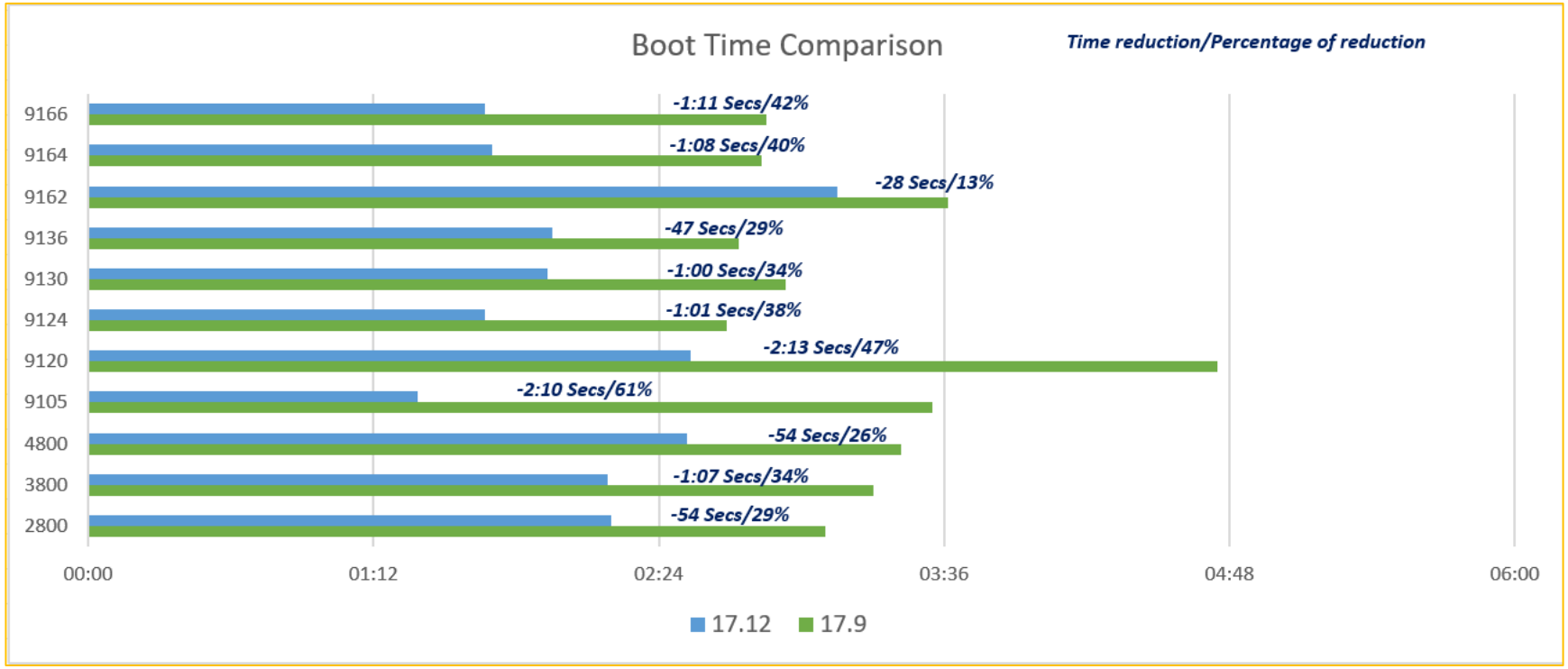
- RF Leader election happens according to this table

Group Leader order	Maximum AP's	Maximum AP /RF Group
3504	150	500
C9800-L	250	500
5508	500	1000
C9800-CL (Small)	1000	2000
5520	1500	3000
C9800-40	2000	4000
C9800-CL (Medium)	3000	6000
8510/8540	6000	6000
C9800-CL (Large)	6000	12000
C9800-80	6000	12000

Optimizations

AP Boot Time Optimization

- ✓ AP booting involves initialization of many modules and the total bootup time is the aggregation of each boot components
- ✓ In 17.12.1, we have done some optimizations in these modules' initialization
- ✓ With this optimization we could achieve a drastic reduction(up to ~40%) in bootup time in all AP Platforms



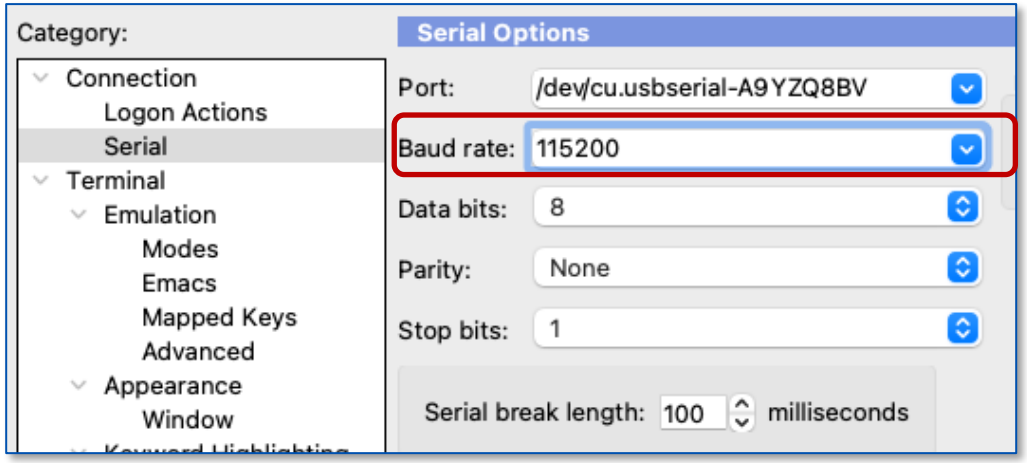
Boot Time Verification

Method to Measure

- ✓ To measure the bootup time of the Access Point, SSID beacon packets are captured from the AP
- ✓ The Access Point is tagged to broadcast a single <TEST SSID>
- ✓ A reboot of AP is initiated from the AP console
- ✓ Continuous Packet Capture is triggered on the respective channel
- ✓ Packet captures are terminated once the AP joins the controller and beaconing the SSID
- ✓ The bootup time is derived based on the packet captures - Time between the last beacon before reload until the first beacon after re-join

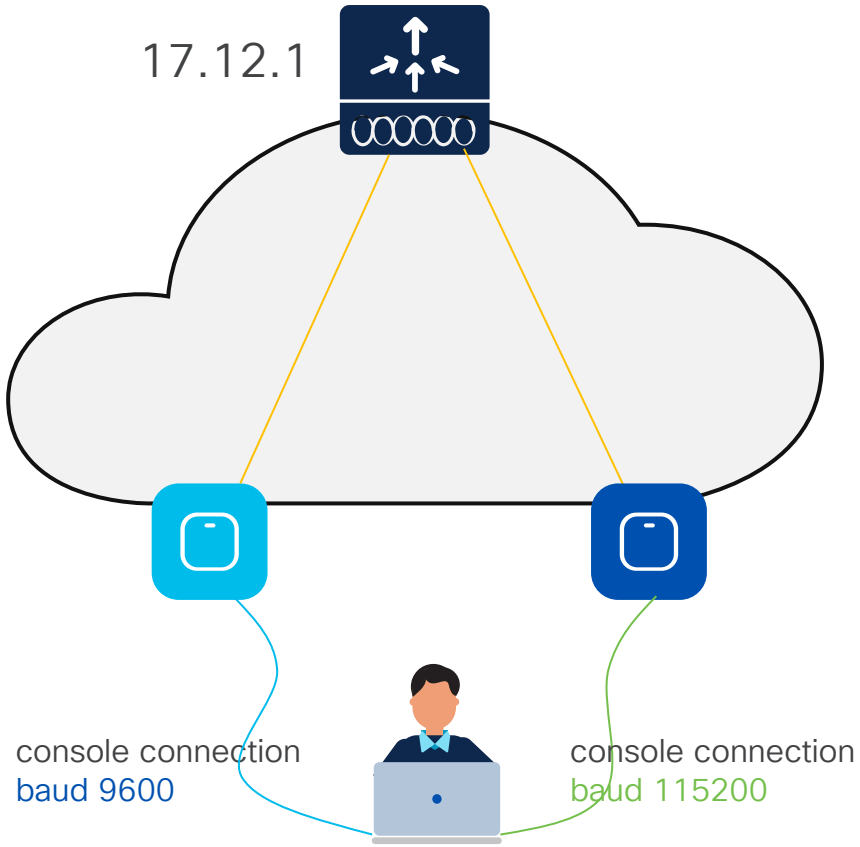
AP Console baud rate change

- Change the baud rate from 9600 to 115200 to get the console back:



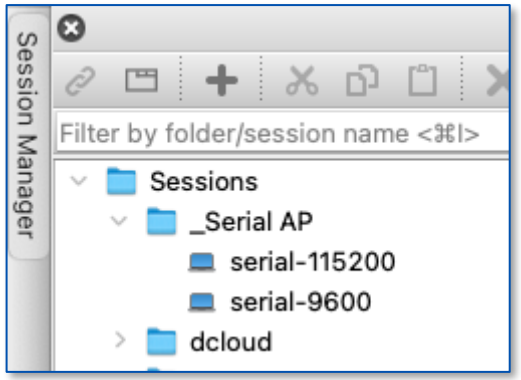
- Why? To improve boot time; depending on the AP model, you get up to 30s reduction in boot time
- How: By increasing the baud rate to 115200, the kernel and radio driver/firmware logs are printed faster and hence the AP boots faster (more info in CSCwe88390)

AP Console baud rate change



Why would you care?

- Customer is on 17.9.4, admin is connected to AP via console with baud rate of 9600. All good
- C9800 is upgraded to 17.12.1. Existing AP still reachable with same console connection. All good
- New AP is added to the network > baud rate on new AP is automatically set to 115200
- Admin needs separate settings to connect to new AP
- Admin can clear AP config on existing APs to change the baud rate and have one way to console to all APs
- Or:



Wireless Product Analytics

Wireless Product Analytics

Knowing product usage to serve customers better

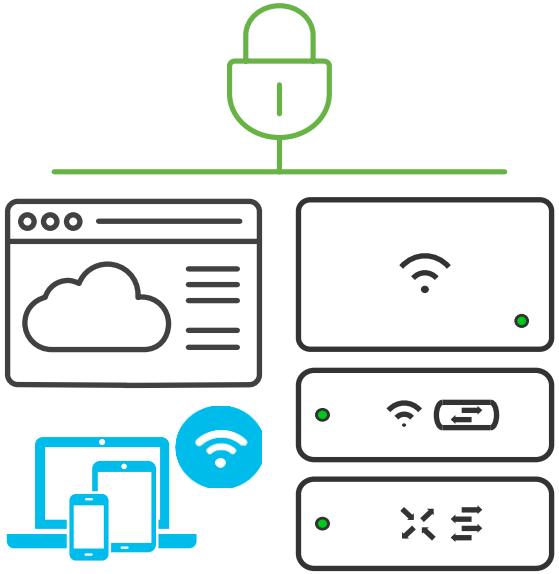
Product Decisions for Customer benefit

- SW version, feature & scale usage
- Introduction on New APs on best software release
- Continued product and feature improvements

Better Product Experiences for Customers

- SW version and critical Security Advisories
- Recommendation to avoid security issues
- Risk scoring
- Best practice recommendations

Wireless Product Analytics – New proposal



- Release Notes (Existing)
- Product Analytics FAQ (New)
- Download Banner (New)
- Data Privacy sheet (Upcoming)

Currently available (via CLI)	Auto Enabled
17.9.4+ 17.10+	**Shipping** - 17.10.1 (SM),17.11.1(SM) **Planned** -17.9.5 (EM)& 17.12.2(EM)

In 17.9.5 and 17.12.2 – Functionality is auto enabled
No data collected or sent for 7 days after upgrade providing time to disable

The data collected is non-PII data. CLI is present to view the report collected/ sent for transparency

All the information is sent in a secure format (HTTPS) and stored in a secure & encrypted format

All the data processed is compliant to **GDPR** , Cisco EULA and Cisco Privacy agreement . More details in FAQ

Options to disable :
Use no-form of 'pae' command - no pae
Block the URL https://dnaservices.cisco.com

Wireless Product Analytics - Documentation

Products & Services | Support | How to Buy | Training & Events | Partners | Employees | Sarath Gorthi Subrahmanya

Software Download

Downloads Home / Wireless / Wireless LAN Controller / Standalone Controllers / Catalyst 9800 Series Wireless Controllers /

Search...

Expand All | Collapse All

Bengaluru-17.6.5(MD)

All Release

17

Dublin-17.11

Dublin-17.10

Dublin-17.10.1(ED)

Cupertino-17.9

Cupertino-17.8

Cupertino-17.7

Catalyst 9800-40 Wireless Cont

Release Dublin-17.10.1 **ED**

My Notifications

This version of software had Device Telemetry (Prod
for more details

File Information

Cisco Catalyst 9800-40 Wireless Controller
C9800-40-universalk9_wlc.17.10.01.SPA.bin
Advisories

Banner on software download

cisco.com/c/en/us/td/docs/wireless/controller/9800/tech-notes/Wireless_Product_Analytics_FAQ.html

Products and Services | Solutions | Support | Learn

... / Cisco Catalyst 9800 Series Wireless Controllers / Technical References /

Wireless Product Analytics FAQ

Save | Download | Print

Updated: July 18, 2023

Bias-Free Language

Product Analytics / Device Telemetry on
Cisco Catalyst 9800 Wireless Controllers
IOS-XE 17.9.4+ / IOS-XE 17.10+

Contents

FAQs

Device Telemetry	This feature allows for the collection of non-personal usage device systems information for Cisco products, which helps in continuous product improvements. This feature is enabled by default. Use the **no** form of the **pae** command to disable this feature. The following commands are introduced as part of this feature: • **pae** • **show product-analytics kpi** • **show product-analytics report** • **show product-analytics stats** **Note** Turning off Smart Licensing Device Systems Information does not impact other Systems Information collection including from Cisco DNA Center or vManage. **Important**: Cisco is constantly striving to advance our products and services. Knowing how you use our products is key to accomplishing this goal. To that end, Cisco will collect device and licensing Systems Information through Cisco Smart Software Manager (CSSM) for product and customer experience improvement, analytics, and adoption. Cisco processes your data in accordance with the Cisco End User License Agreement, the Cisco Privacy Statement and any other applicable agreement with Cisco. To modify your organization's preferences for device and licensing systems information, use the **pae**command. See Cisco Catalyst 9800 Series Wireless Controller Command Reference → **pae**.

Release Notes

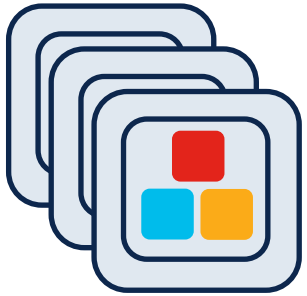
FAQ: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/tech-notes/Wireless_Product_Analytics_FAQ.html?

Day 1: C9800 Configurations

Design with Tags in Mind

C9800 Configuration Model (Profiles & Tags)

Access Points



RF Tag

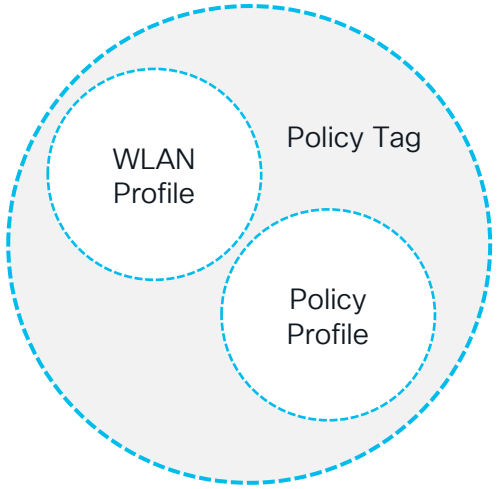
Policy Pag

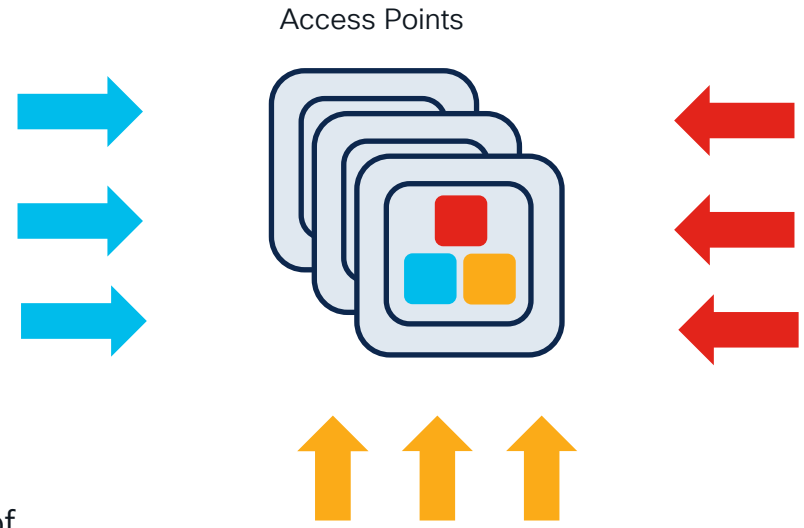
Site Tag

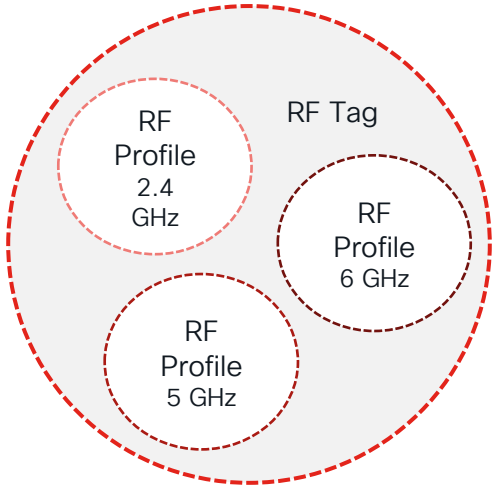
Important to remember:

- Profiles (Policy, AP Join and Radio Frequency (RF)) and tags are the new configuration constructs
- Profiles are assigned via tags. Every AP needs to be assigned to the three AP tags (Policy, Site, RF)
- Advantages of the new configuration models:
  - Modular and reusable config constructs
  - Flexible to assign configuration to a group of APs
  - Easier to manage site specific configuration across geo-distributed locations
  - No reboot needed when applying config changes via tags (remember AP groups?)

Tag Breakdown

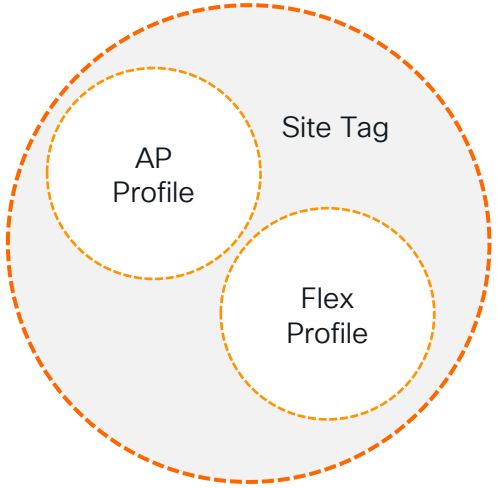






- Defines the Broadcast domain (list of WLANs to be broadcasted) with the policies of the respective SSIDs
- “Equivalent” to AP Group in AireOS

- Defines the Radio Frequency (RF) properties of the group of APs per radio



- Defines the properties of the site (central or remote)
- For FlexConnect site:
  - Defines the fast-roaming domain
  - “Equivalent” to Flex Groups in AireOS

SSID = Service Set IDentifier

Policy Tag

WLAN Design Updates

Wi-Fi 6E Security (Recap)

Wi-Fi 6E uplevels security.

WPA3 L2 Security: OWE, SAE*, 802.1x-SHA256

WPA3 and Enhanced Open Security made mandatory for Wi-Fi 6E certification.

No backward compatibility with Open and WPA2 Security.

Requires Protected Management Frame (PMF) in both AP and Clients.

*Only SAE-H2E (Hash to Element) Method Supported.
SAE (Hunting N Pecking) – Not Supported

AKM = Authentication and Key Management
OWE = Opportunistic Wireless Encryption
SAE = Simultaneous Authentication of Equals
SHA-256 = Secure Hash Algorithm (SHA) 256 bit

WLAN/SSID Design

6GHz WLAN Design Considerations

What options would you have?

1. ”All-In” Option: Reconfigure the existing WLAN to WPA3, one SSID for all radio policies (2.4/5/6 GHz) – Most unlikely

2. “One SSID” Option: Configure multiple WLANs with same SSID name, different security settings – Most conservative

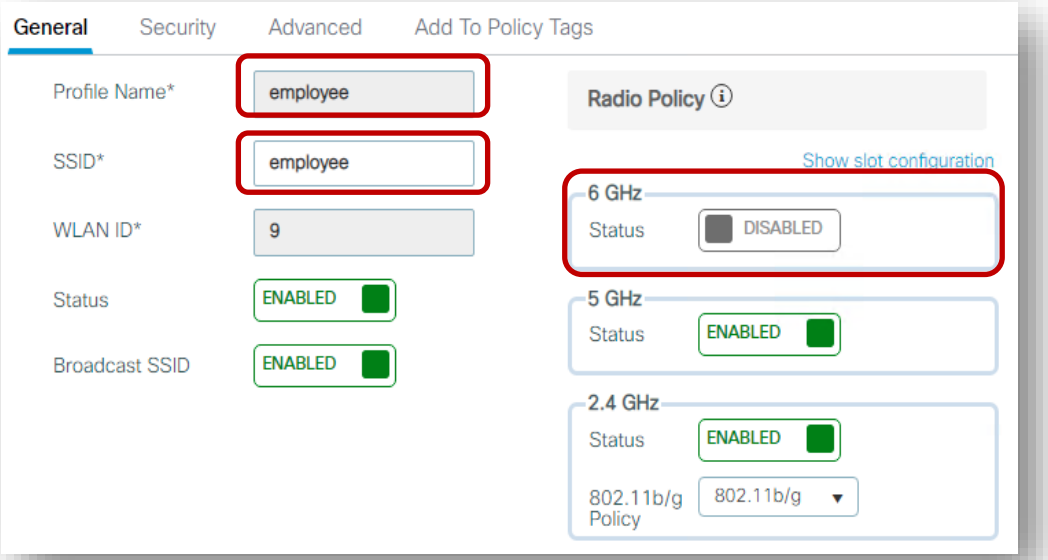
3. “Multiple SSIDs” Option: Redesign your SSIDs, adding specific SSID/WLAN with specific security settings – Most flexible

Most likely your current SSID configuration would prevent it from being broadcasted on 6GHz
Note: as 17.9.3, there is a limit of 8 SSIDs broadcasted on 6GHz radio

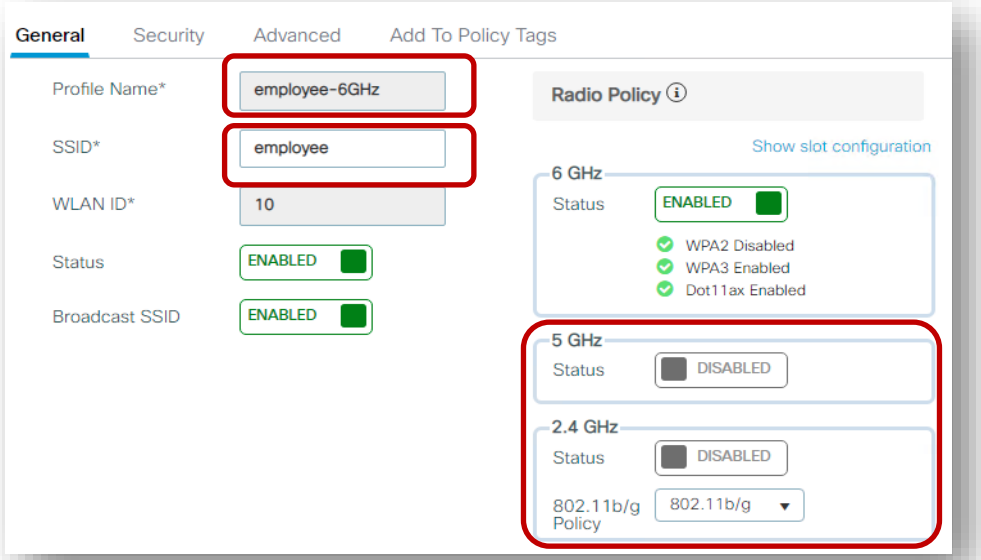
WLAN design considerations

- **Option 2**: Single SSID but different AKM per band. For Cisco today, this means creating an additional WLAN for 6GHz, with same SSID name but different WLAN profile name and security settings (AKM):

Existing WLAN serving 2.4 and 5GHz



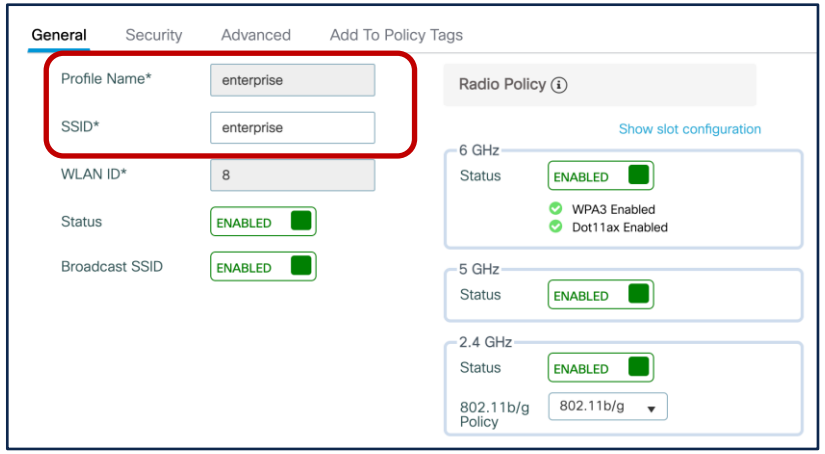
New WLAN, same SSID name serving 6GHz

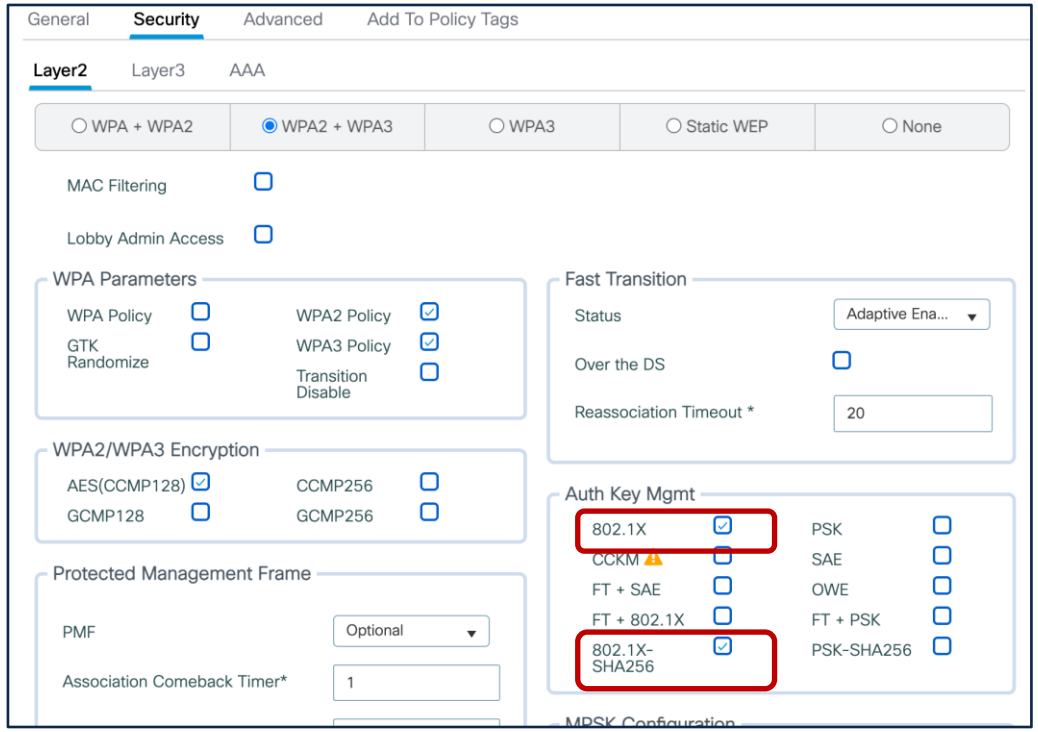


AKM = Authentication and Key Management

Going Forward … (IOS-XE 17.12.1)

Single WLAN Profile for 2.4/5 and 6 GHz





- L2 Security would be WPA2+ WPA3.
- AKM should be set to **802.1x-SHA256** and **802.1x** (SHA1) for Enterprise; SAE and PSK for Personal.
- PMF as **Optional**

- How to configure the client side?
  - For clients that don't support 6 GHz, configure a **WPA2 profile or WPA3 Enterprise with PMF as Optional** depending on the client support.
  - For clients that support 6 GHz, configure **WPA3 Enterprise**. They will use these settings to connect to both 2.4/5 GHz and 6GHz

WFA = Wi-Fi Alliance

How does a SSID look like?

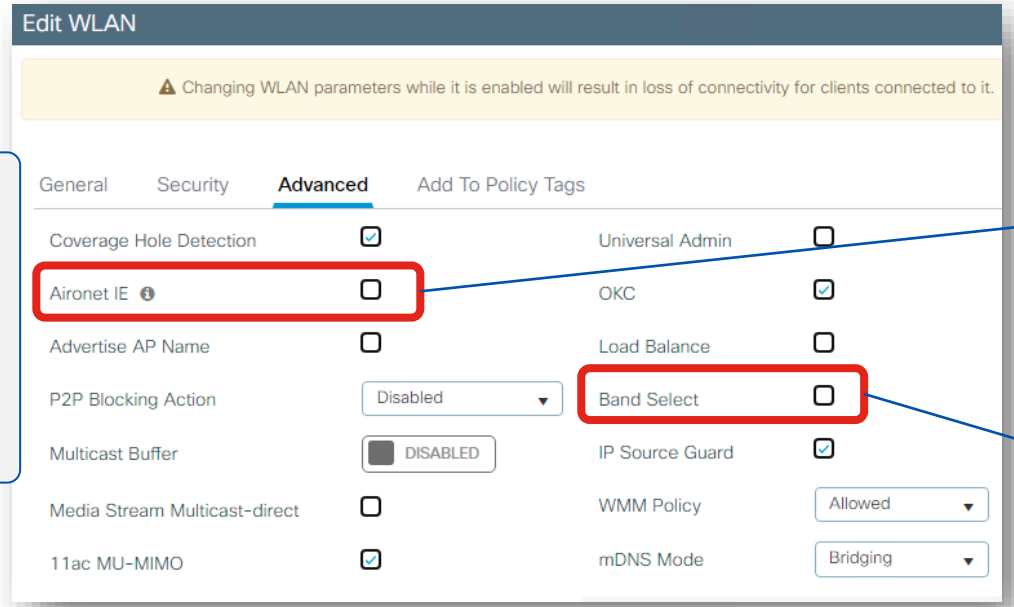
As shown below, individual configurations for 2.4/5GHz and 6GHz with their Security combination

```
C9800#show wlan name Blizzard
Security-2.4GHz/5GHz
         802.11 Authentication                    : Open System
Wi-Fi Protected Access (WPA/WPA2/WPA3)            : Enabled
          WPA2 (RSN IE)                          : Enabled
          AES Cipher                                : Enabled
          WPA3 (WPA3 IE)                        : Enabled
              AES Cipher                                : Enabled
          Auth Key Management
                 802.1x                                 : Enabled
.........
 Security-6GHz
             WPA3 (WPA3 IE)                                : Enabled
                 AES Cipher                                : Enabled
Auth Key Management
          Dot1x-SHA256                              : Enabled
```

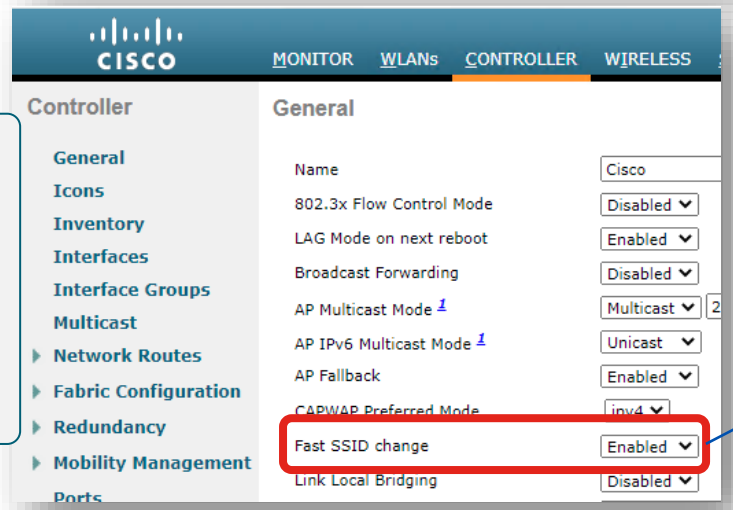
WLAN settings

WLAN settings

C9800-80



8540



We used to have these commands in AireOS, shall we keep them in IOS XE WLC?

Q: Do we still need Aironet IE?

A: No, unless you are running Cisco specific devices like IP phones and WGBs

Q: Do we still need Band Select?

A: Not on this SSID as you have voice traffic, and it might affect fast roaming. In other SSIDs is fine.

Q: What happened to Fast SSID change?

A: No need to enable the feature explicitly, this is taken care automatically on C9800

Webauth Configuration

Webauth configuration

Problem:

Wireless client unable to pop up the captive portal page automatically. If client goes to any website, it gets certificate warning message.

Solution:

Need to enable WebAuth on HTTP. In C9800 you don't need to enable HTTP for the entire box (GUI access), but only for WebAuth client connections.

Add webauth-http-enable command under the definition of parameter-map:

```
parameter-map type webauth global
    virtual-ip ipv4 192.0.2.1 virtual-host <name>
    webauth-http-enable
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Webauth Global Configuration
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! config interface address virtual 192.0.2.1
! config interface hostname virtual <name>
! config custom-web webauth-type external
! config custom-web ext-webauth-url <url>
! config custom-web redirecturl <https url>
!% Note: parameter-map configuration follow interactive-mode
when it get configure first time.
!% Please enter prompt option while configuring parameter-map.
!% e.g. : This operation will permanently convert all relevant
authentication commands to their CPL control-policy equivalents.
As this conversion is irreversible and will disable the conversion CLI
'authentication display [legacy|new-style]', you are strongly
advised to back up your current configuration before proceeding.
!% Do you wish to continue? [yes]: yes
parameter-map type webauth global
  virtual-ip ipv4 192.0.2.1 virtual-host <name>
parameter-map type webauth global
  type webauth
  redirect for-login <http url>
  redirect on-success <https url>
```

mDNS Configuration

mDNS configuration

Scenario:

AireOS configuration was correctly translated and hence Location Services were not enabled on the mDNS service policy.

Recommendation:

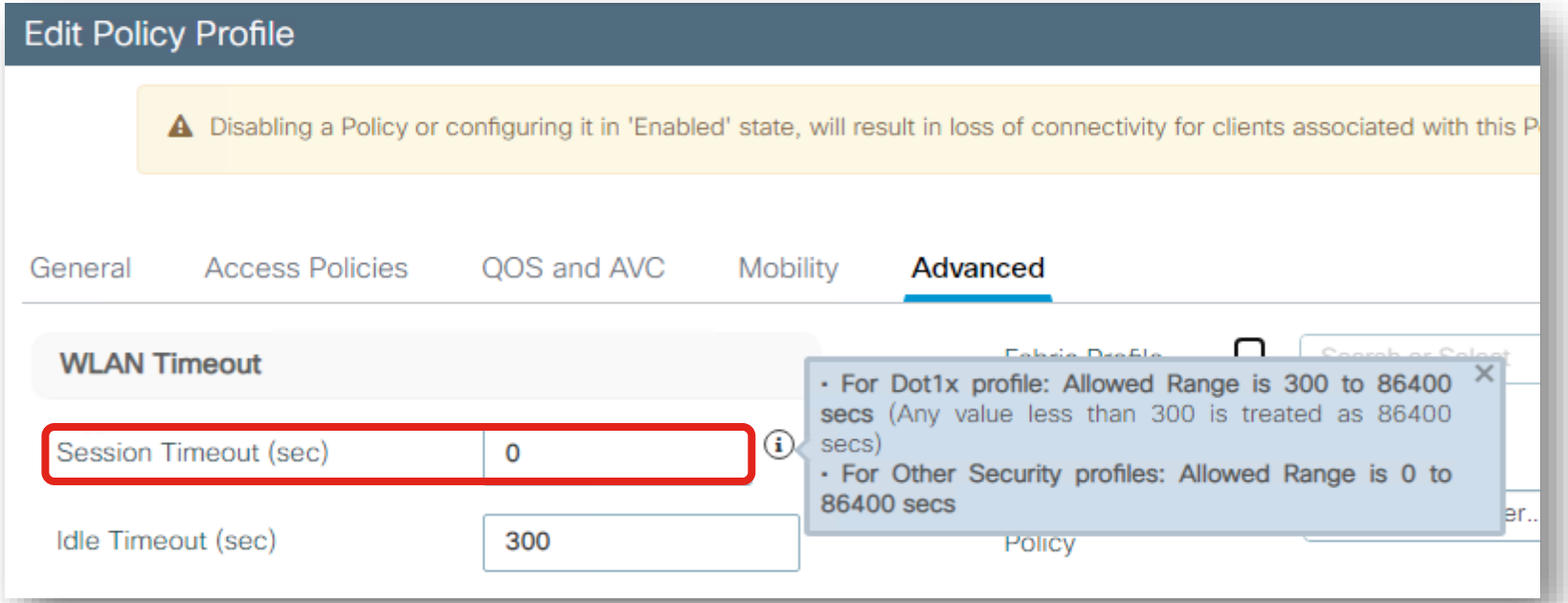
Configure the mDNS policy to use Location Specific Services (LSS) to optimize mDNS responses to clients:

```
mdns-sd service-policy aireos-default-mdns-profile
  […]
  location lss
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! mdns profile and service mapping
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[skip]
mdns-sd service-list aireos-default-mdns-profile-out OUT
  match AirTunes
  match Printer-IPPS
  match Printer-SOCKET
  match HP_Photosmart_Printer_2
  match HomeSharing
  match HP_Photosmart_Printer_1
  match Airplay
mdns-sd service-policy aireos-default-mdns-profile
  service-list aireos-default-mdns-profile-in IN
  service-list aireos-default-mdns-profile-out OUT
  !% "location lss" skipped since it is disabled in any of
"mdns service" mapped under "mdns profile".
```

Policy Profile settings

Policy Profile settings



Q: In AireOS we set the value to "0" to have max timeout, does it apply the same to C9800?

A: In C9800, before 17.4.1 if it is set to 0, then session timeout is disabled > all roams are SLOW. Starting 17.4.1, for 802.1x SSID if you set it to zero, it's reconfigured to max allowed

Q: can we use the default policy profile as a "normal" profile

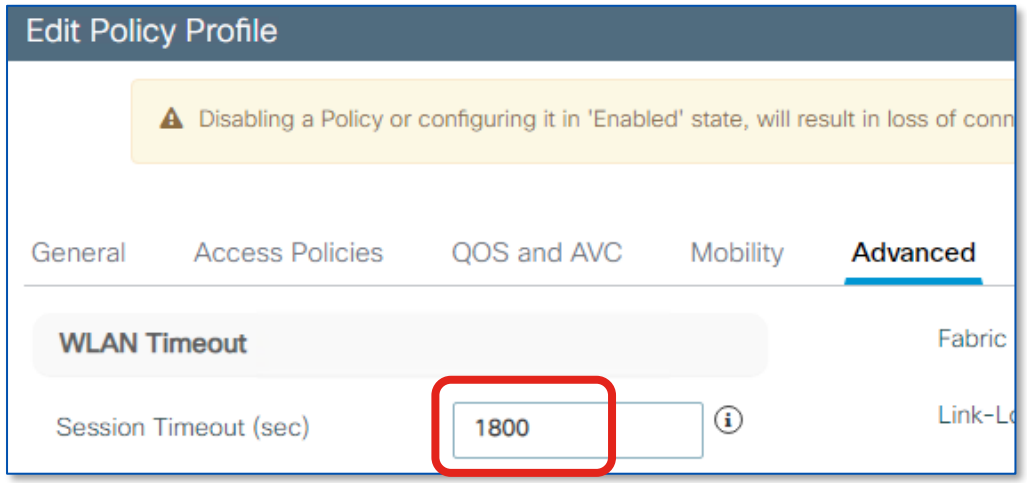
A: Yes, absolutely

Default session timeout to 8 hours

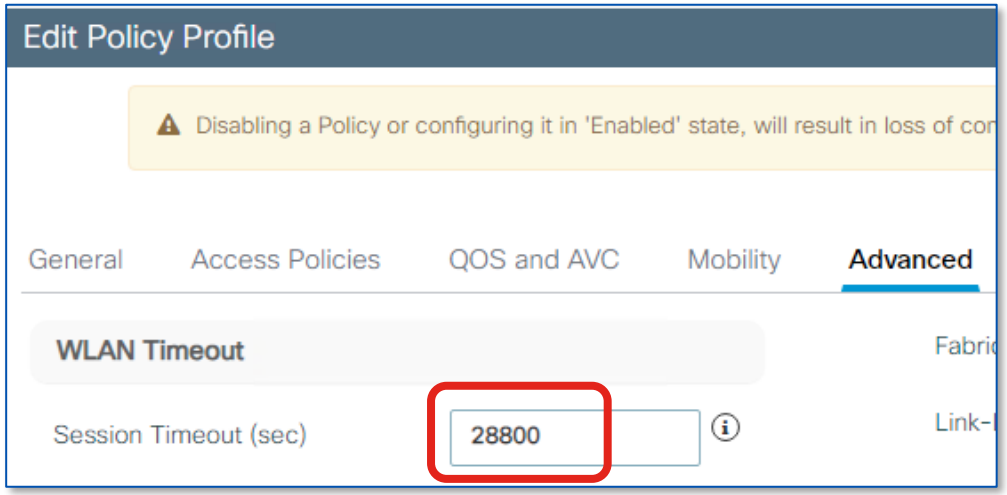
What it is?

- The default session timeout in policy profile is changed from 30 mins to 8 hours
- Why? Some clients don't like frequent re-auth and re-keying and there have been multiple TAC cases related to this, solved with longer session time out
- This new would help relieve the pressure on AAA servers

Before 17.12 > timeout is 30 mins

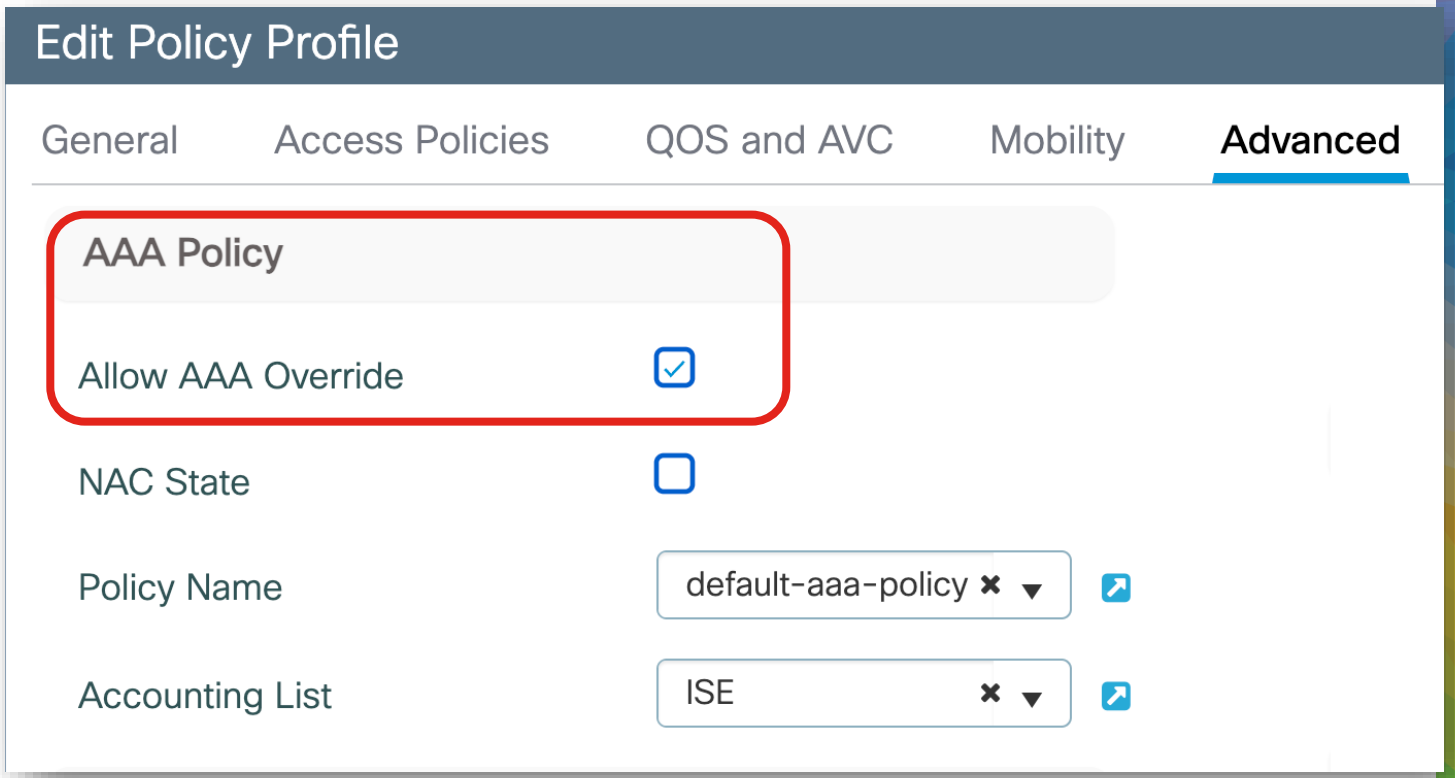


Starting 17.12 > timeout is 8 hours



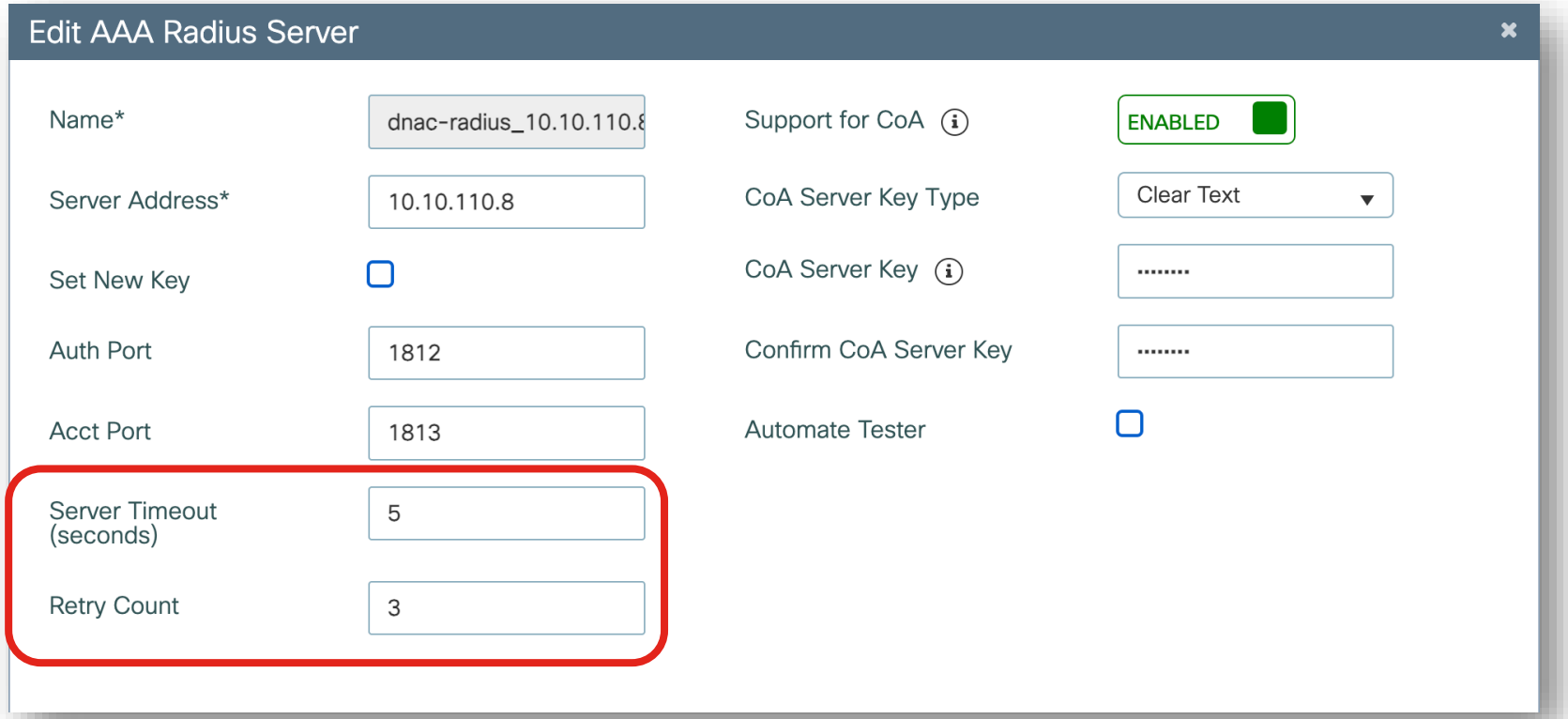
AAA Override

- Use a single common SSID to apply per-user attributes
- Example
  - VLANs
  - Security Group Tags (SGT)



RADIUS Server Timeout

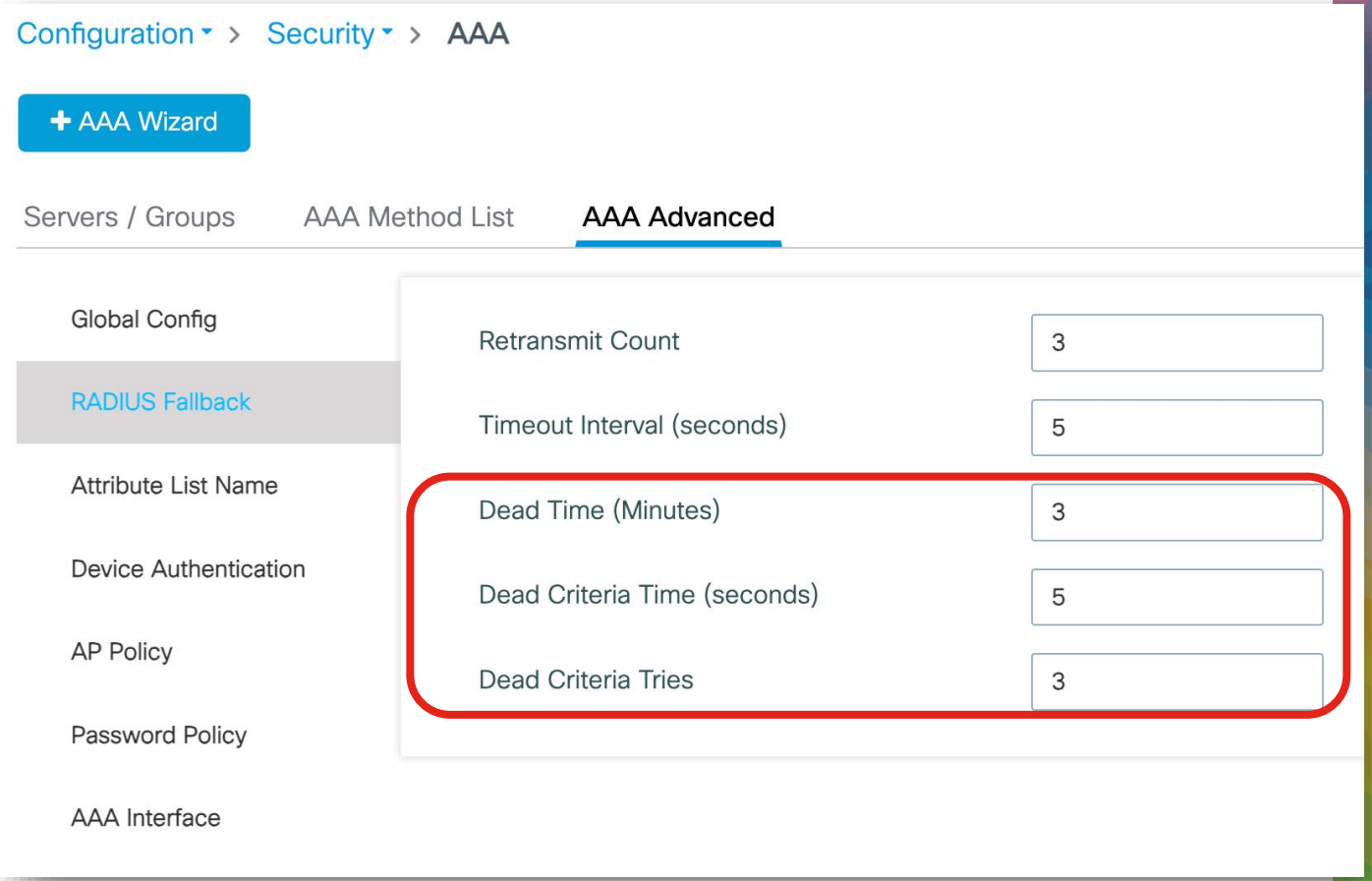
- Minimum of 5 seconds for timeout
- Minimizes early expiration of the authentication process



RADIUS Server Timeout

Dead-Criteria and Deadtime Timers

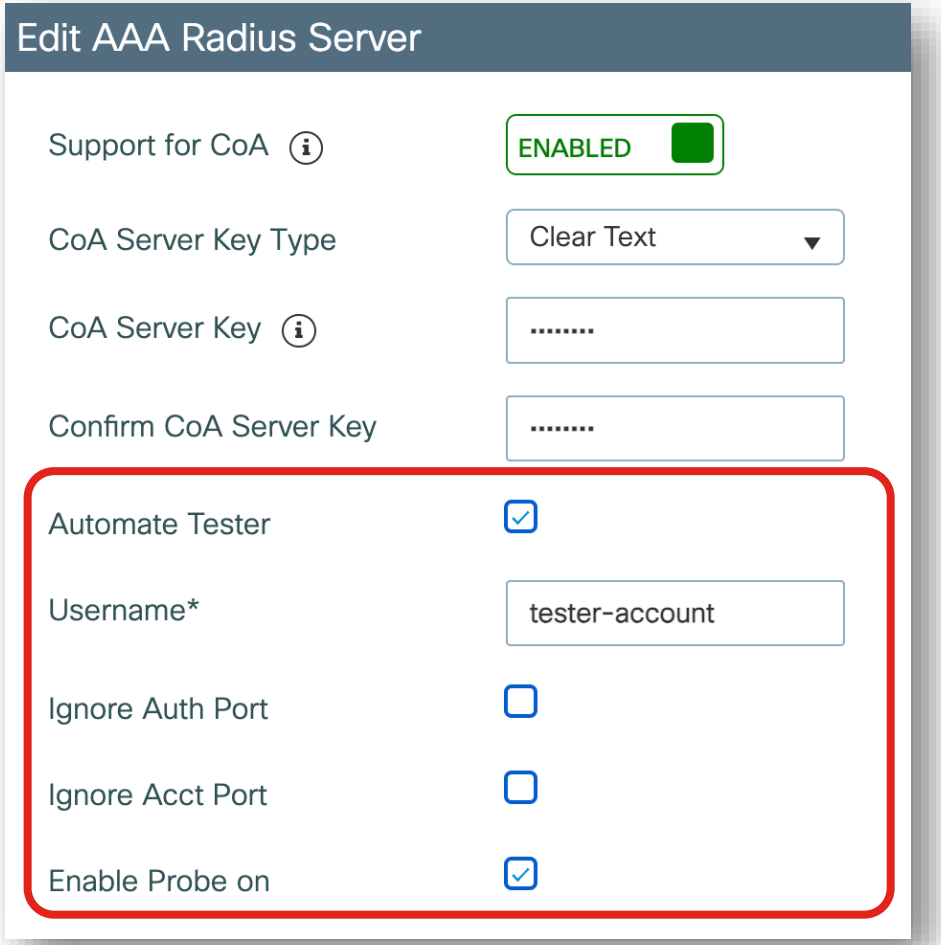
- Important for use with multiple AAA servers and load balancing
- Specifies when to mark server dead and move to next one
- Use probes to monitor status of server



RADIUS Server Timeout

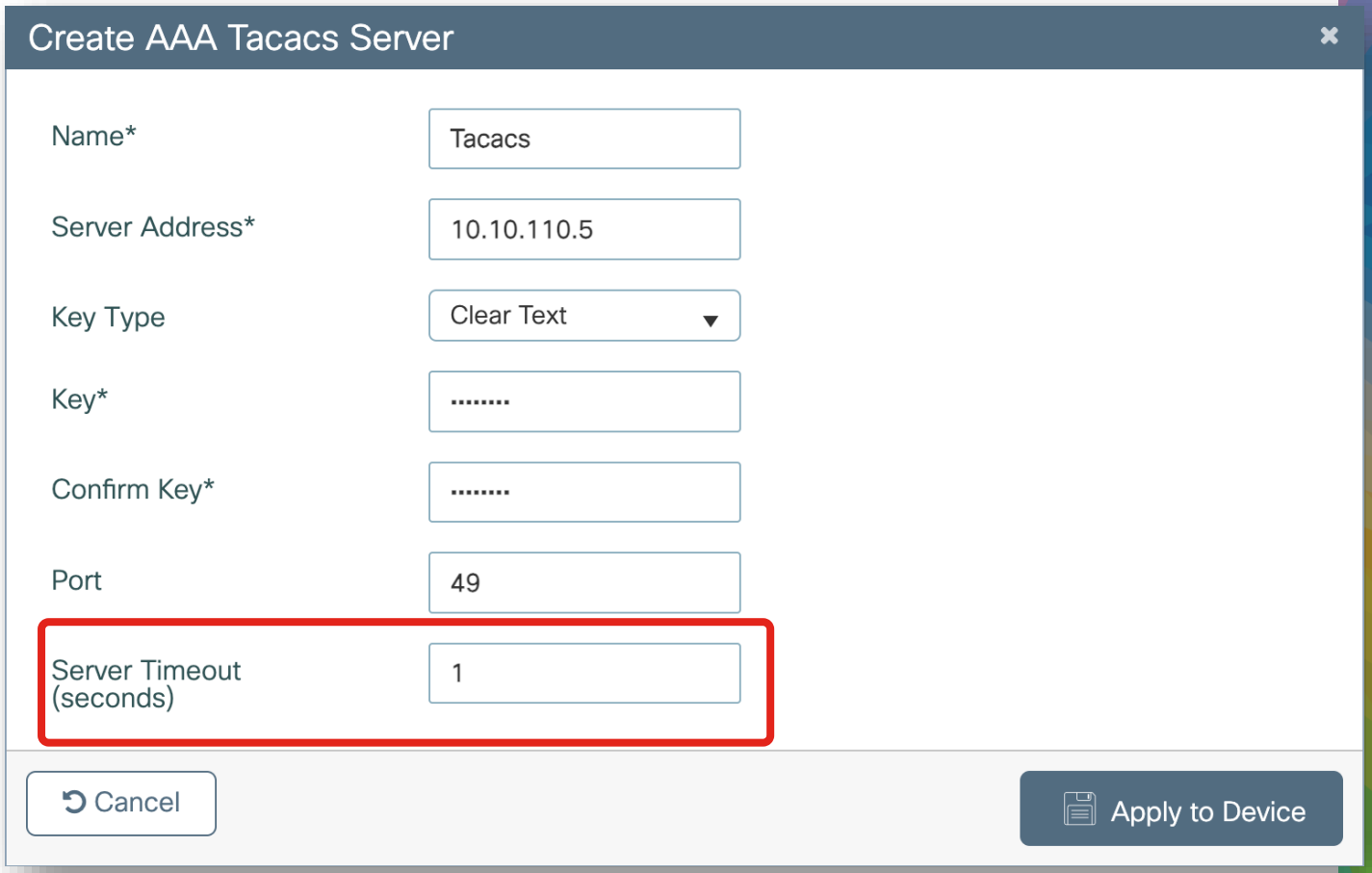
Dead-Criteria and Deadtime Timers

- Important for use with multiple AAA servers and load balancing
- Specifies when to mark server dead and move to next one
- Use probes to monitor status of server

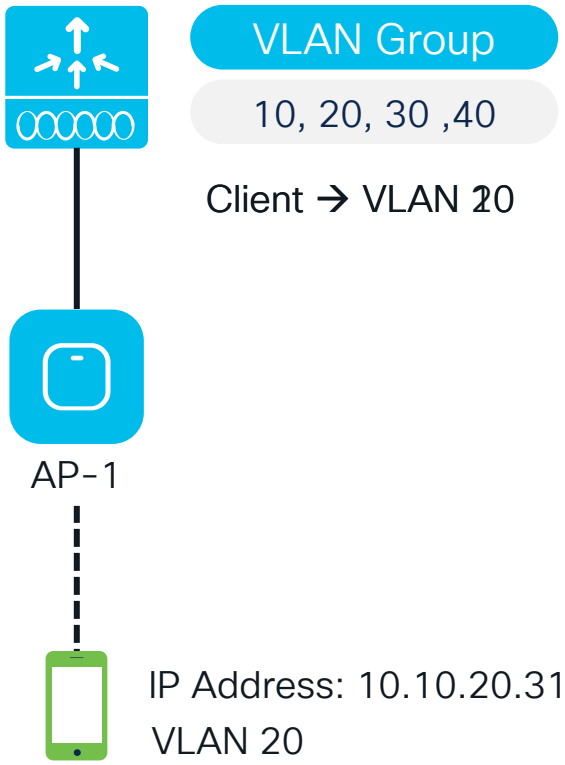


TACACS+ Management Timeout

- Increase retransmit timeout if:
  1. Repeated reauthentication requests
  2. Controller falls back to the backup server when primary is still up and reachable
- Recommended value of 1 second



VLAN Group Support for DHCP and Static IP Clients



9800 assigns a VLAN to clients upon joining the network

Client has a static IP in a different VLAN than the one assigned

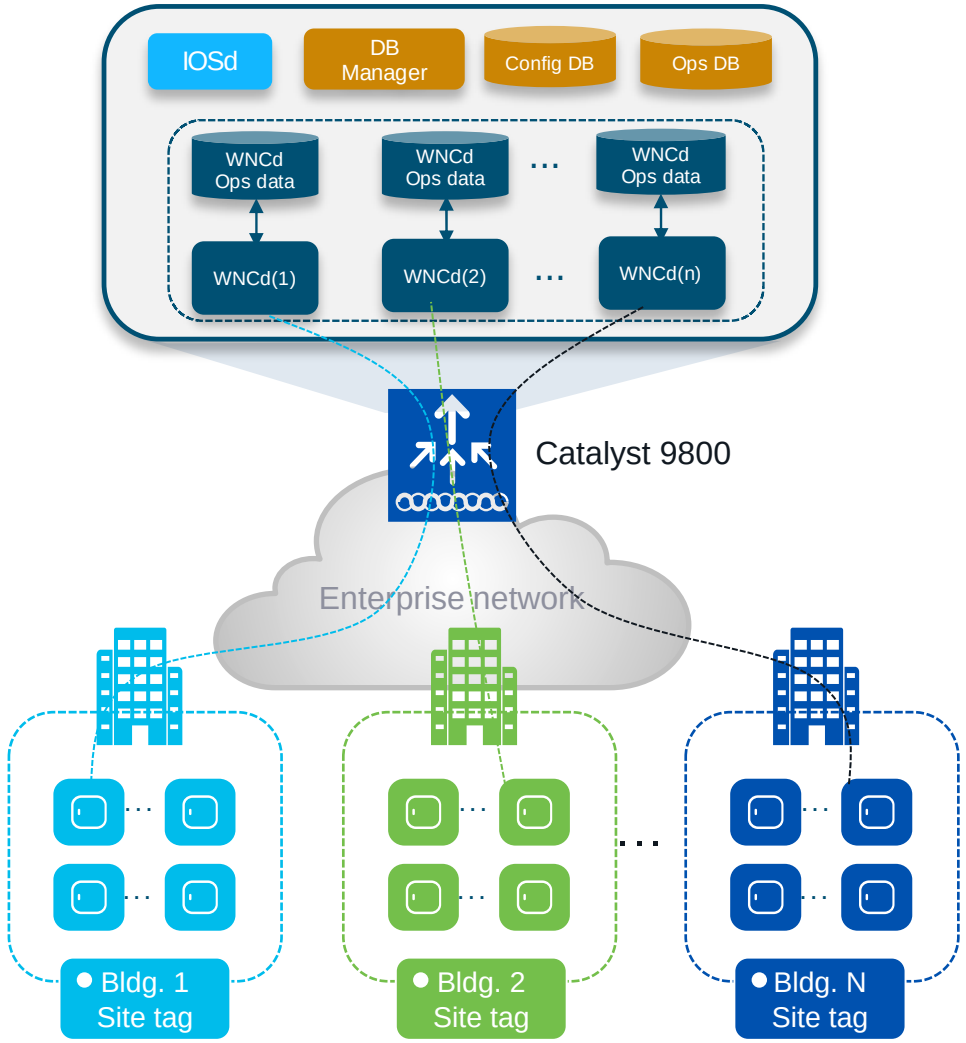
If VLAN exists in the group, client is assigned to that VLAN

If VLAN does not exist, use Static IP Mobility

Site Tag Design

Site Tags – Design considerations

Refresher!



Important facts:

- C9800 has a multi-process software architecture
- APs are distributed across Wireless Network Controller processes (WNCd) within a C9800
- Distributing APs (and clients) across WNCd processes gives better scale and performance
- The number of WNCd varies from platform to platform:

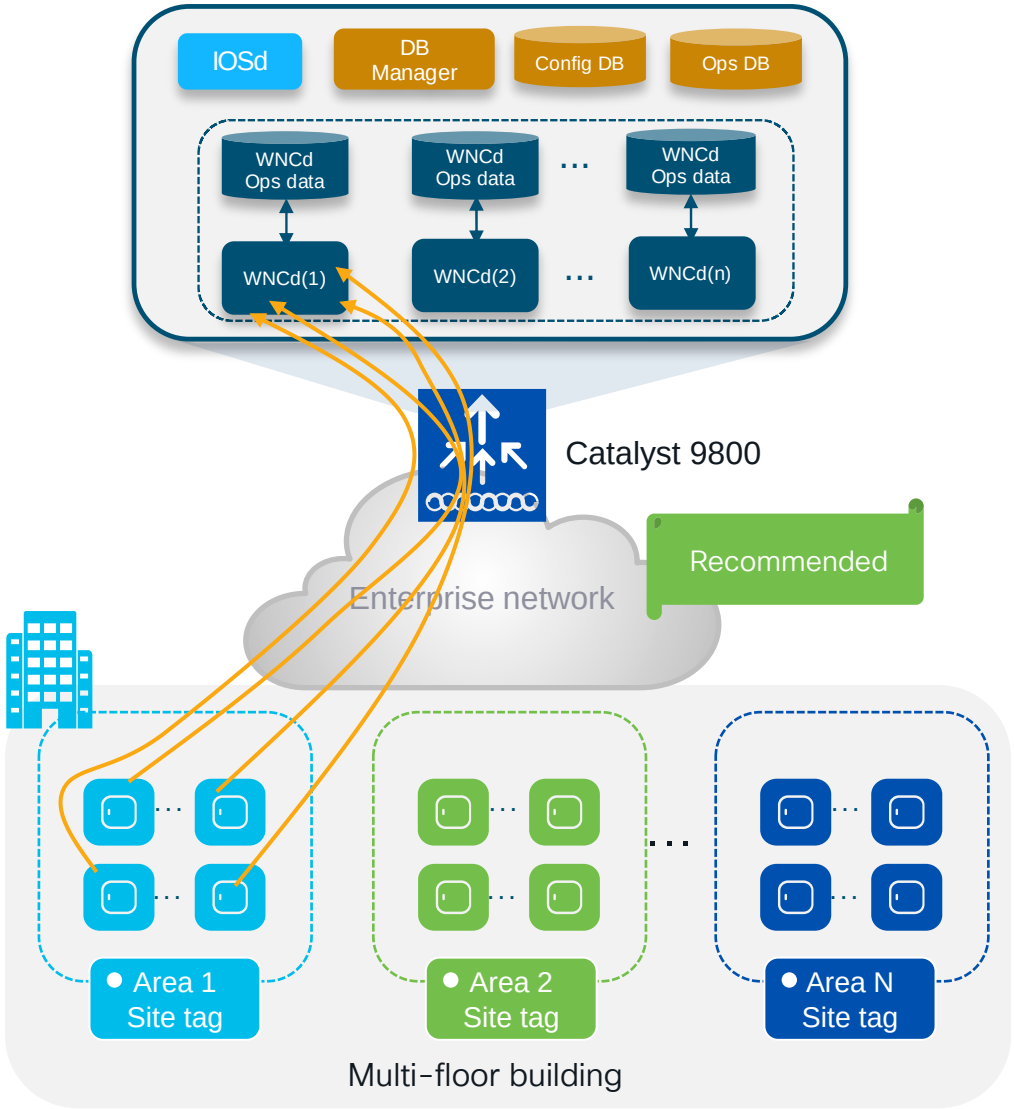
Platform	# of WNCD instances
EWC (on AP or C9k switch)	1
C9800-L	1
C9800-CL (small)	1
C9800-CL (medium)	3
C9800-40	5
C9800-CL (large)	7
C9800-80	8

Following command shows the # of WNCDs processes:

```
9800#sh processes platform | inc wncd
```

Site Tags – AP to WNCd distribution

Refresher!



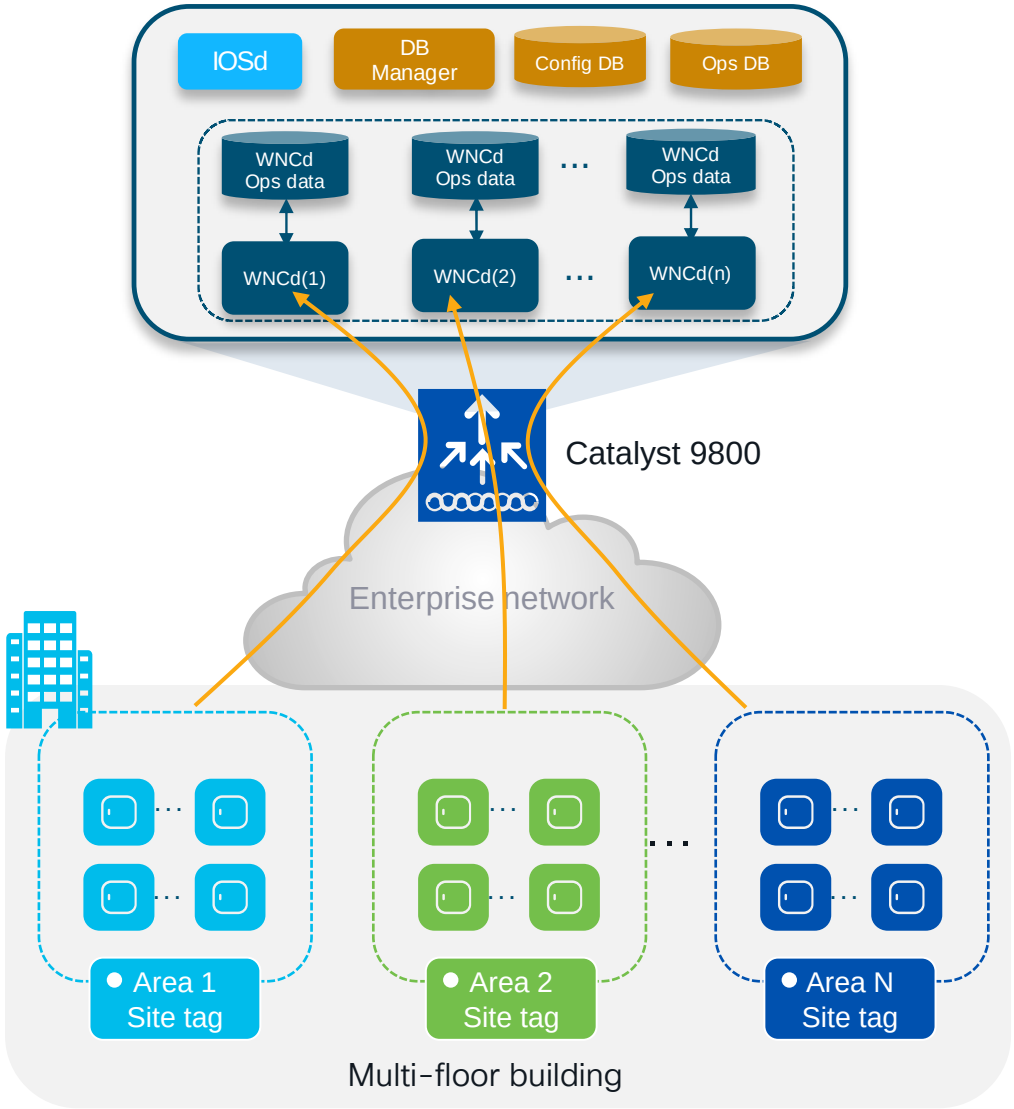
How AP distribution across WNCds works:

- AP distribution to WNCd processes is based on Site Tag: APs with the same site-tag are managed by the same WNCd
- Site tags are distributed among WNCds using the least loaded criteria based on the number of site tags (not the # of APs)
- APs to WNCd mapping happens at AP joining time. Mapping is considered only for the first AP joining with the new site tag
- For best performance: use custom site tag and group APs at a roaming domain level > Site Tag = Roaming Domain
- IMPORTANT: the site tag doesn't have to coincide with a geographical physical site. The site tag is a logical group of access points
- To show how APs are distributed across WNCds:

```
c9800#sh wireless loadbalance ap affinity wncd
```

Site Tags – AP to WNCd distribution

Refresher!



Recommendations:

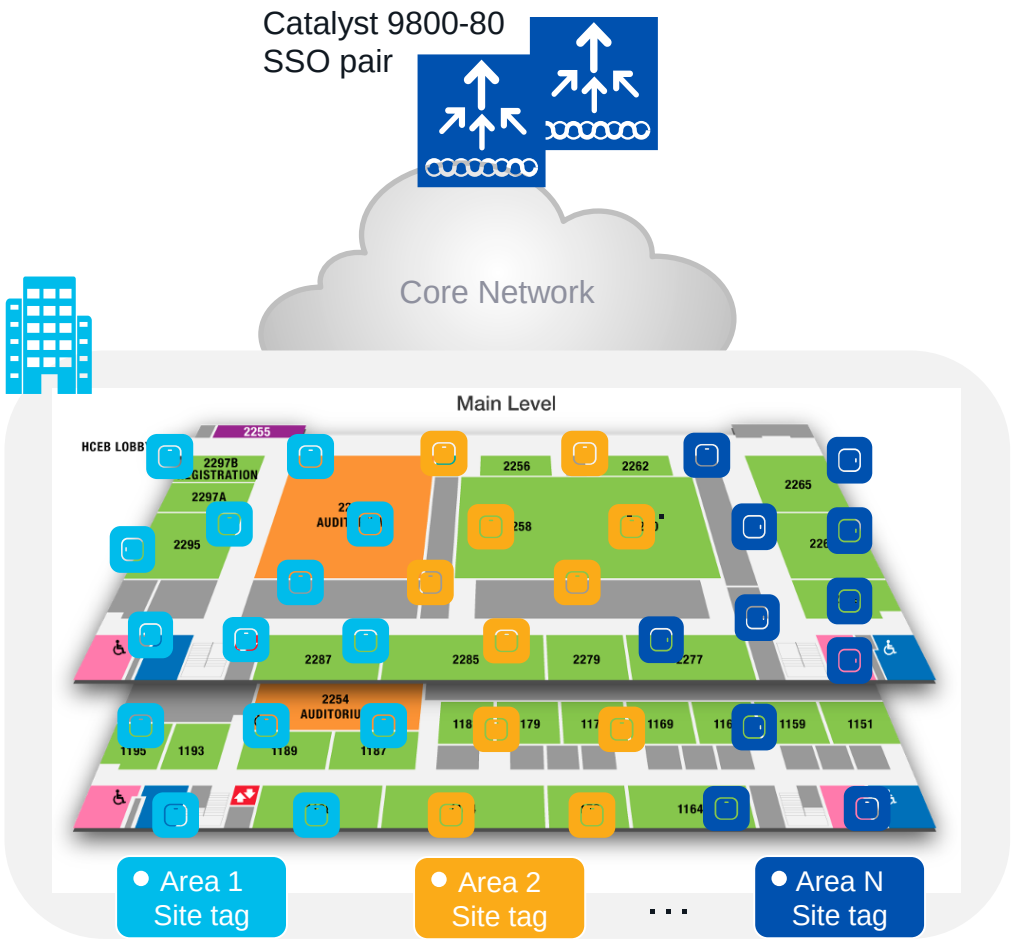
- Use custom site tags
- Whenever possible, have less than 500 APs per site tag
- Do not overwhelm a site-tag and WNCd. Do not exceed the following max number of APs per site tag:

Platform	Max APs per site tag
9800-80, 9800-CL (Medium and Large)	1600
9800-40	800
Any other 9800 form factor	Max AP supported

- Evenly distribute APs among site tags and use the recommended number of site tags per platform:

Platform	Recommended # of site tags
C9800-80	8 or a multiple (16, 24, ...)
C9800-CL (large)	7 or a multiple (14, 21,..)
C9800-40	5 or a multiple (10, 15, ...)
C9800-CL (Medium)	3 or a multiple (6, 9,..)

Site Tags Design – Large venue deployment



Scenario#1: Large venue deployment

- Conference center, stadium, large venue, where you have a lot of clients, and these clients can roam seamlessly everywhere > Large roaming domain

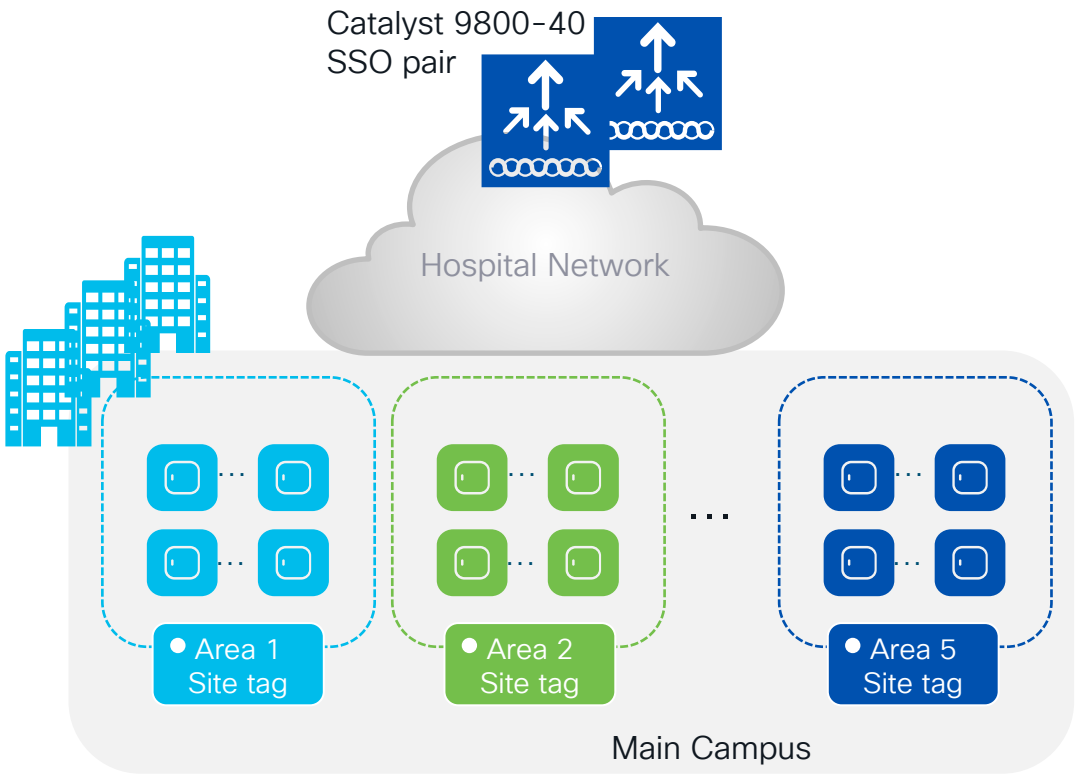
What are the recommendations in this case?

- Use custom site tags and evenly distribute APs among these
- Recommendation: Have the number of site tags match the number of WNCds on that platform:

Platform	# site tag
C9800-80	8
C9800-CL (large)	7
C9800-40	5
C9800-CL (Medium)	3

- This is to minimize the number of inter-WNCd roaming events and reduce any inter-process communication performance penalty

Site Tags – AP to WNCd distribution



Customer design

- Main campus, multiple buildings, one single roaming domain
- 1200 APs in local mode, with high density of roaming clients
- Pair of C9800-40 running 17.6

Recommendations:

- Go with custom site tags
- Since 1200 AP exceeds the recommended number of APs per site tag > use #5 site tags (grouping buildings together in five virtual areas).
- Assign APs to area tags so that you have around 200 APs per site tag. Perfectly load balanced system with #240 APs per site tag and per WNCd.
- Remember: 802.11r is fully supported across WNCds; it's only 802.11k/v neighbor info that will not be shared. This is fixed in 17.6 and optimized in 17.7 and later

Wireless Config Analyzer Express (WCAE)

The wireless engineer trowel

- Do I have a problem with WNCd load balancing?
- WCAE is your friend! Run the WCAE > you get a report like this:

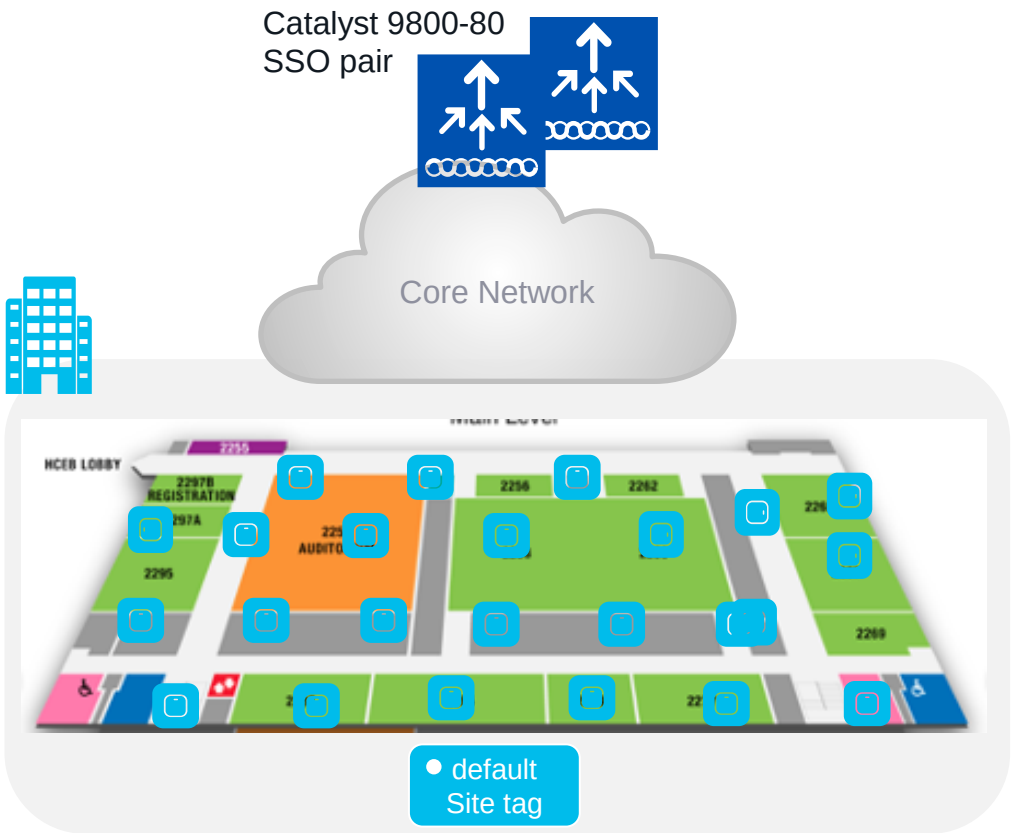
starting 17.9

Back to Content Tab

WNCD ID	Tags Count	Tags Assigned	AP Count	Client Count	CPU load	Percentage Aps	Percentage Clients
0	1	(Click on + sign to expand)	153	217	7	13.40	14.73
1	1	(Click on + sign to expand)	218	358	7	19.09	24.30
2	1	(Click on + sign to expand)	168	1	3	14.71	0.07
3	1	(Click on + sign to expand)	195	50	4	17.08	3.39
4	1	(Click on + sign to expand)	8	4	1	0.70	0.27
5	1	(Click on + sign to expand)	171	7	3	14.97	0.48
6	1	(Click on + sign to expand)	154	735	8	13.49	49.90
7	1	(Click on + sign to expand)	75	101	2	6.57	6.86
		Totals:	1142	1473			

- This is not a balanced system, but CPU is low > IMPORTANT: No need to redesign!
- WCAE is here: https://developer.cisco.com/docs/wireless-troubleshooting-tools

Site Tags Design – Special case



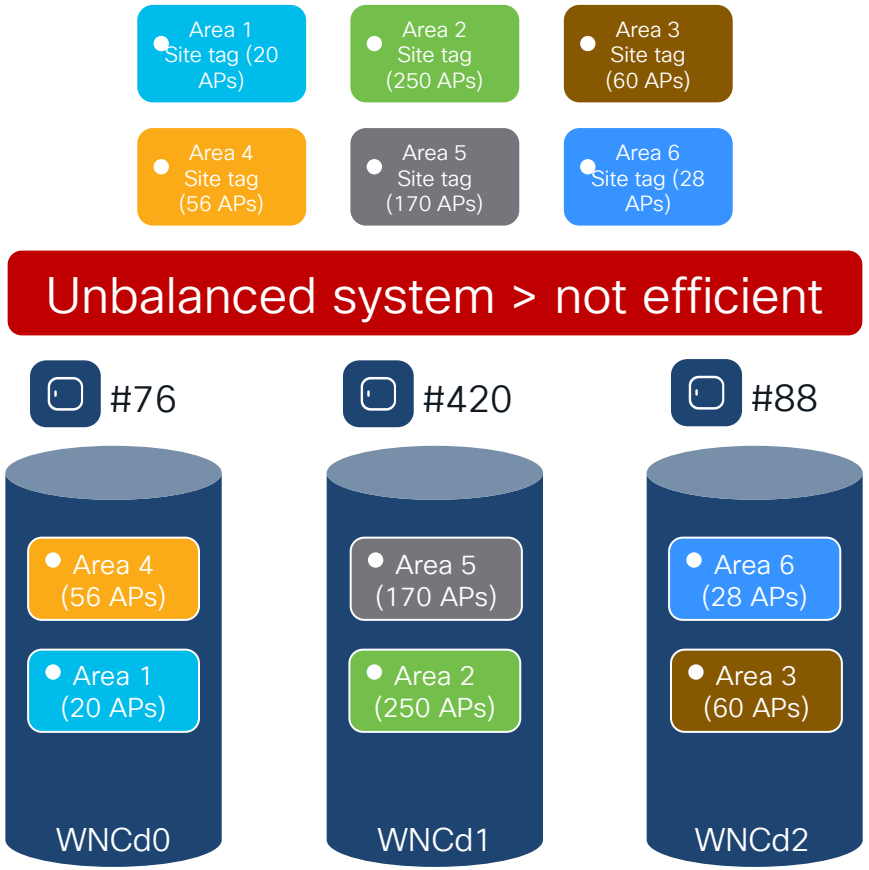
Scenario #2: Large warehouse

- Large warehouse = one single roaming domain. Local mode AP deployment
- Customer cannot design with custom site tags: No AP names, no APs on maps, difficult to identify AP areas, and simply too much operational cost…

Can I use the default-site-tag?

- Default-site-tag: APs will be distributed in round robin across the WNCds, and this may result in inter-WNCd roaming
- Assumption: If the system is not heavely loaded > clients and/or AP scale is 30-40% of the max scale supported on the C9800
- Design option: it's ok to put all APs in the default-site-tag
  - Fast roaming (11r, OKC, etc.) is supported across WNCds
  - 802.11k/v is also supported across WNCds starting 17.7
- This recommandation is valid for all authentication types

Site Tags – AP to WNCd distribution

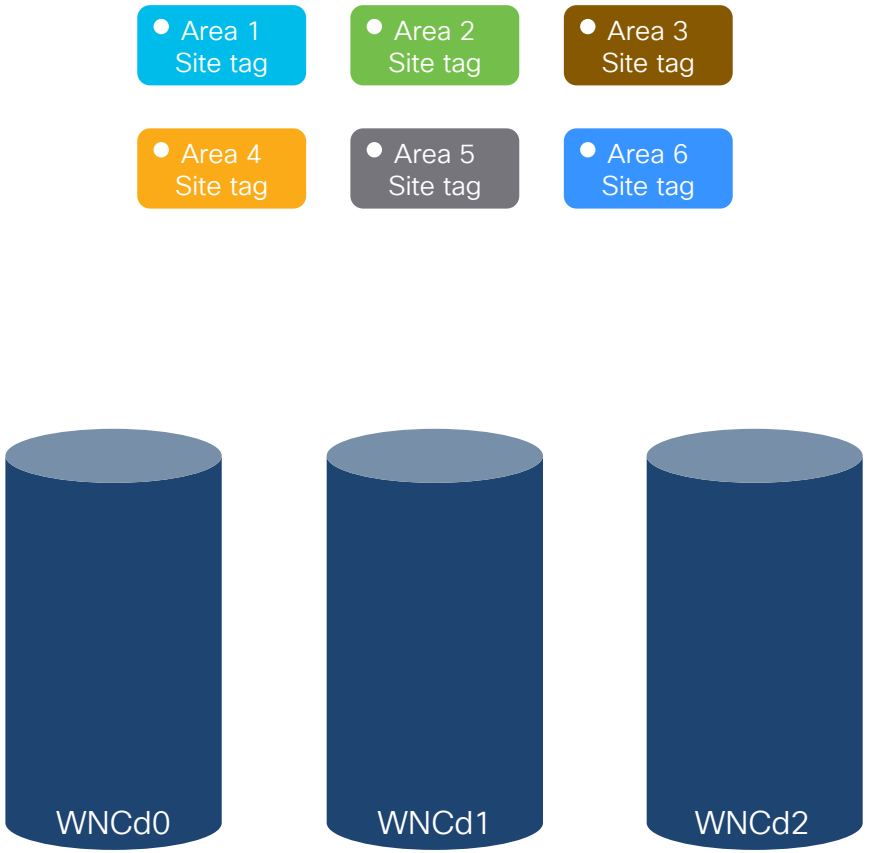


Until 17.9.1, site tags are distributed among WNCds using the least loaded criteria based on the number of site tags. The algorithm doesn't take into considerations the number of APs or clients per site tag

Problem: Current algorithm can result in uneven WNCd load, as it depends on the number of APs per site tag and the order of AP joining

- Example: C9800-CL medium (#3 WNCd), six custom site tags and APs joining in this order:
  - Area1 : #20 APs > WNCd0
  - Area2 : #250 AP > WNCd1
  - Area3 : #60 AP > WNCd2
  - Area4 : #56 APs > WNCd0 (all WNCd has #1 tag, starting again from WNCd0)
  - Area5 : #170 APs > WNCd1 (as WNCd0 has already #2 tags)
  - Area6 : #28 APs > WNCd2 (as WNCd2 as it's the least loaded for # of tags)
- The resulting AP to WNCds mapping is the askew:
  - WNCd0 > site tags: area1, area4 > #76 (20+56) APs
  - WNCd1 > site tags: area2, area5 > #420 (250+170) APs
  - WNCd2 > site tags: area3, area6 > #88 (60+28) APs

Site Tags – New load balancing Algorithm

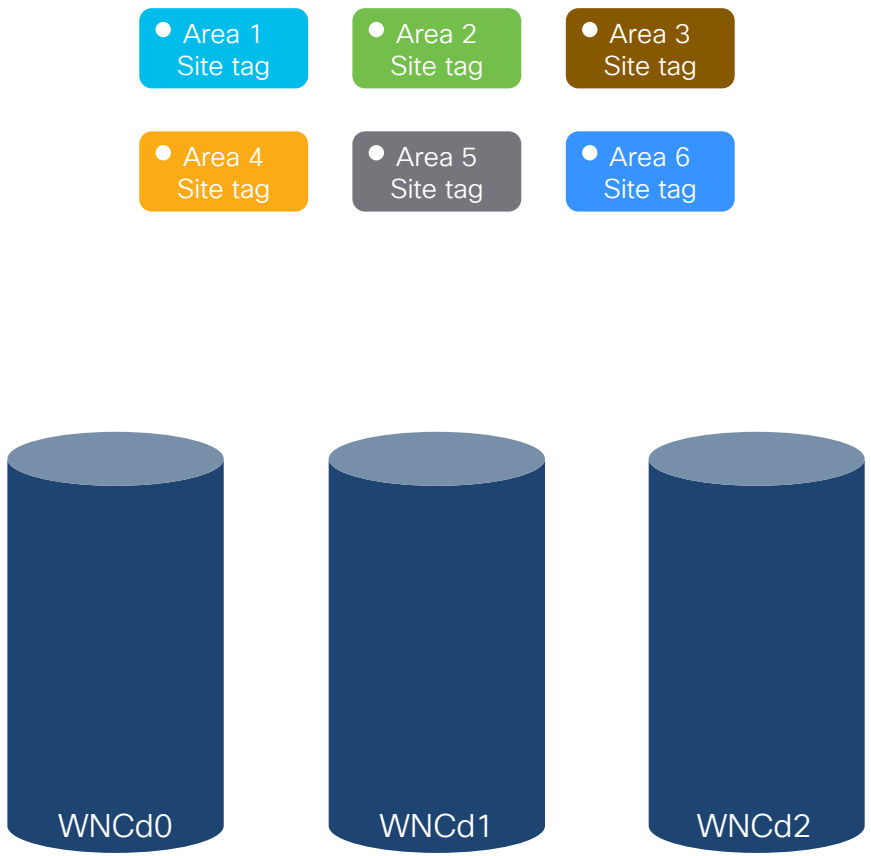


- Starting 17.9.2 and 17.10, the algorithm to distribute APs among WNCds may use the load parameter configured under the site tag:

```
C9800(config)#wireless tag site <site-tag-name>
C9800(config-site-tag)#load <num> (0 to 1000)
```

- Load is an estimate of the relative WNCd capacity reserved for that site tag. It's about reserving a part of the WNCd for a site
- What contributes to the load of the WNCd: all control plane activities > client joining, authentication, roaming, client probes, but also features like mDNS that require CPU time
- IMPORTANT: For load balancing to be efficient it is expected to configure "load" for all the custom site tags

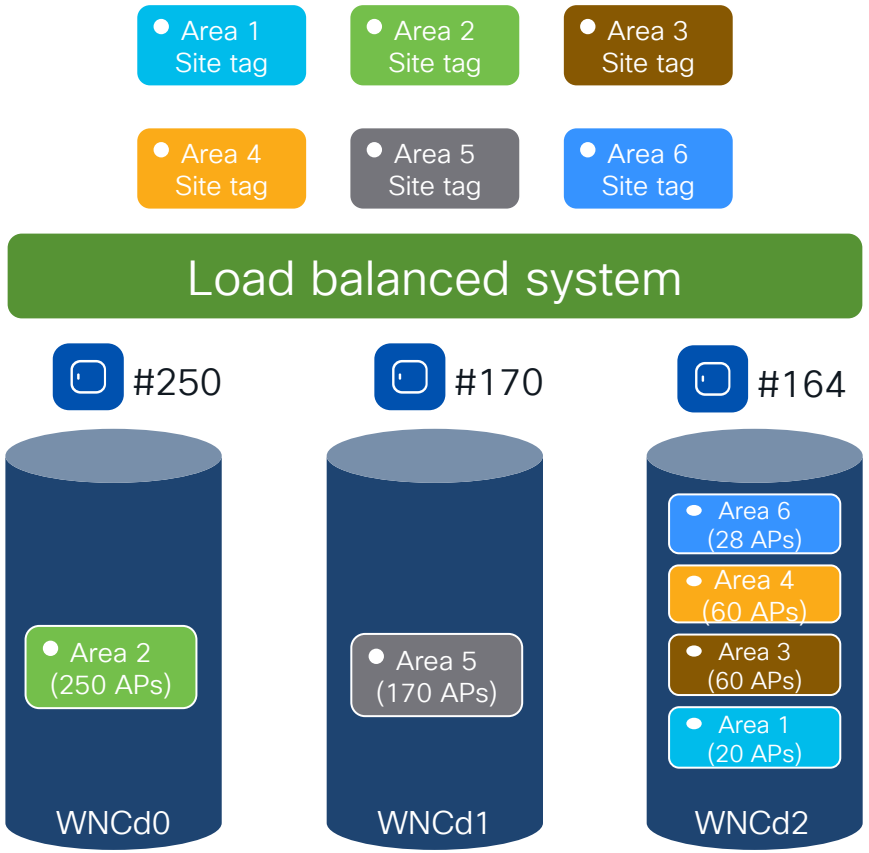
Site Tags – New load balancing Algorithm



How to choose the load?

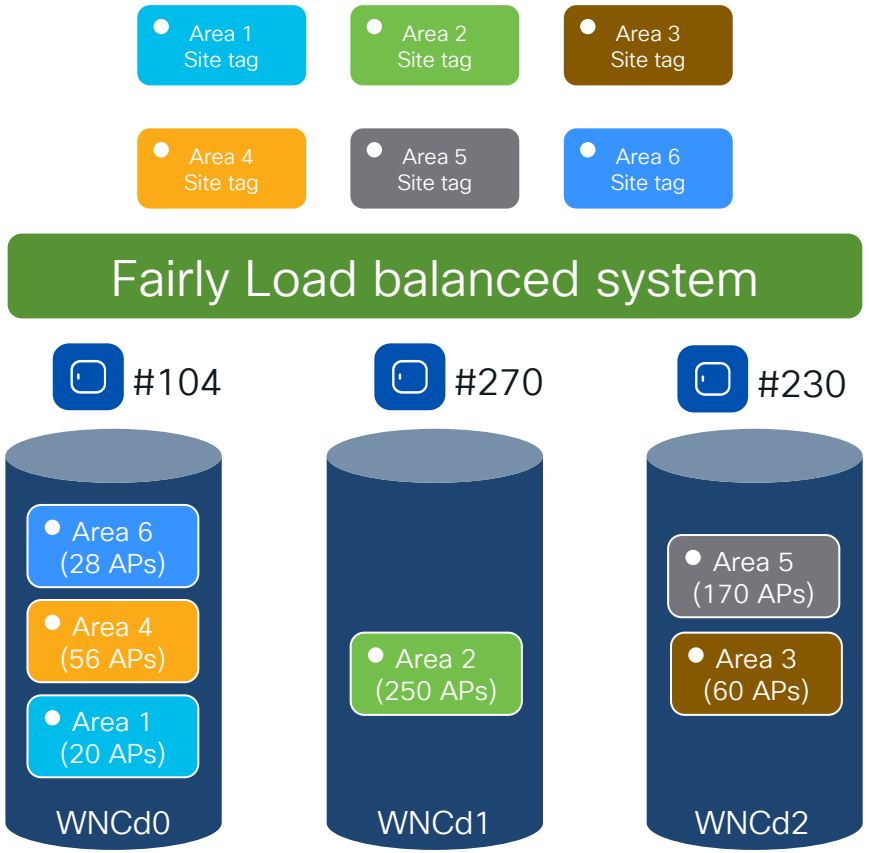
- The default value 0 means no load indication for the site tag. Nothing changes, the algorithm is the same as in 17.9.1 and previous releases
- **Most common option**: Office building with multiple floors/areas. Each floor/area is one site tag. If you estimate similar client/traffic load on each floor/area > **set the "load" equal the # of APs for each site**
- **Weighted option**: In the building one of the floor/area has a conference/training center with a higher expected activity (e.g., lot of clients joining, leaving and roaming) > set a higher weighted "load" that specific site tag. For instance, if #10 APs are present at the conference center area, configure the load to be 20

Site Tags – New load balancing Algorithm



- Let's go back to previous example: C9800-CL (#3 WNCd), six site tags configured with the load = number of APs:
  - Area1 : #20 APs > site-tag load = 20
  - Area2 : #250 AP > site-tag load = 250
  - Area3 : #60 AP > site-tag load = 60
  - Area4 : #56 APs > site-tag load = 56
  - Area5 : #170 APs > site-tag load = 170
  - Area6 : #28 APs > site-tag load = 28
- With the new load balance algorithm, the resulting AP to WNCds mapping would be the following:
  - WNCd0 > site tags: area2 > **#250** APs
  - WNCd1 > site tags: area5 > **#170** APs
  - WNCd2 > site tags: area1, area3, area4, area 6 > **#164** (20+60+56+28) APs
- The result is a load balanced and more efficient system
- Note: For the new load balance algorithm to take into consideration the load, and be independent of AP joining order (this example), configure the load parameter under the site tag and reboot the C9800 so that the algorithm can run on saved data

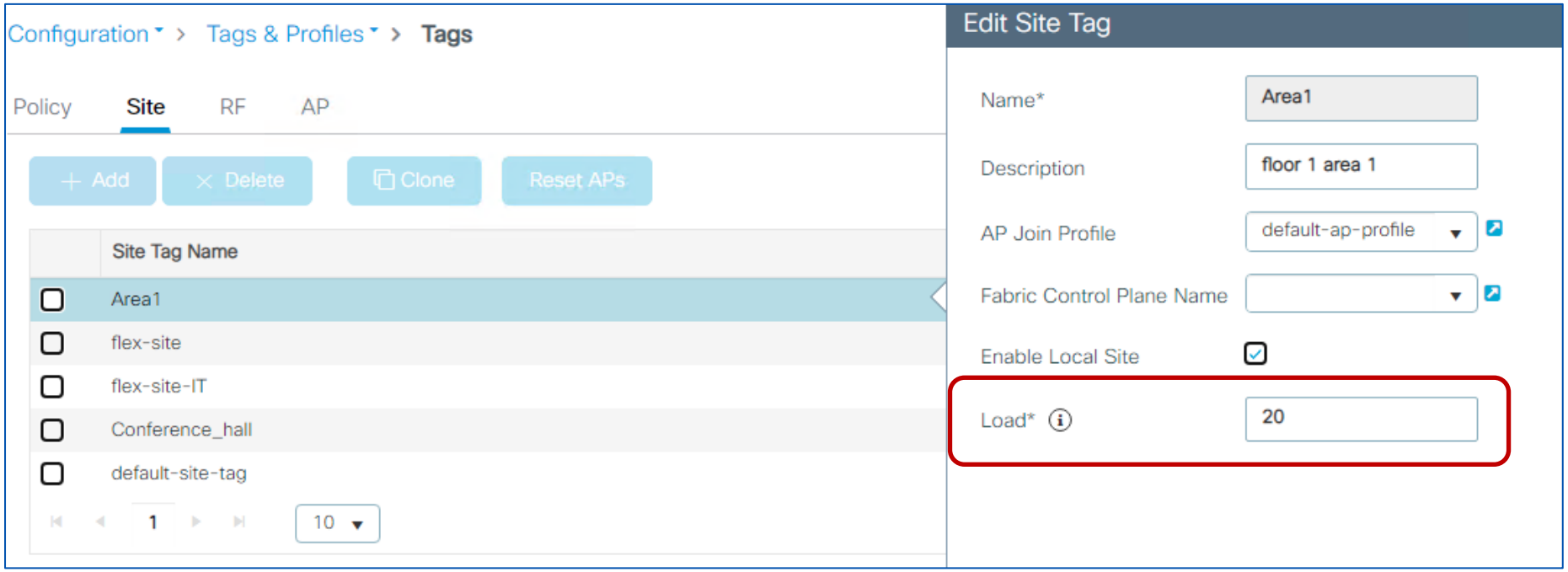
Site Tags – New load balancing Algorithm



- If the C9800 is not rebooted, the load balance algorithm still takes into consideration the site load with the configured load parameter, but it's going to be dependent on the order of AP joining
- Same example: C9800-CL (#3 WNCd), six site tags configured with the following load = number of APs:
  - Area1 : #20 APs > site-tag load = 20
  - Area2 : #250 AP > site-tag load = 250
  - Area3 : #60 AP > site-tag load = 60
  - Area4 : #56 APs > site-tag load = 56
  - Area5 : #170 APs > site-tag load = 170
  - Area6 : #28 APs > site-tag load = 28
- If APs are de-registered and register again, the resulting AP to WNCds mapping would be the following:
  - Area1 : #20 APs > WNCd0
  - Area2 : #250 AP > WNCd1
  - Area3 : #60 AP > WNCd2
  - Area4 : #56 APs > WNCd0 (least loaded in terms of AP count)
  - Area5 : #170 APs > WNCd2 (least loaded in terms of AP count)
  - Area6 : #28 APs > WNCd0 (least loaded in terms of AP count)
- The result is a fairly load balanced and efficient system

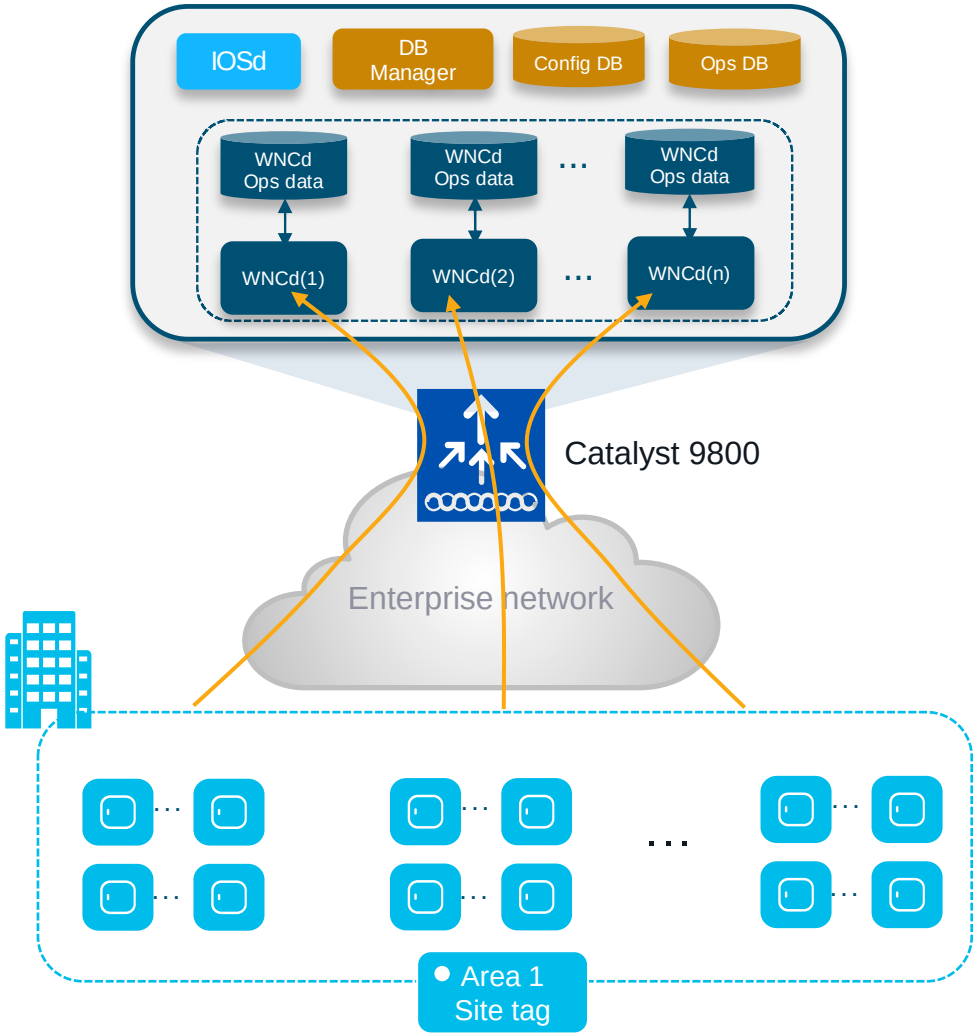
Configuring the site tag Load- WebUI

Configuration > Tags & Profiles > Tags -> Site



Load* = Estimate of the relative load contributed by this group of APs (site-tag).
AP count can be used as a good approximation.

Site Tags – AP to WNCd distribution



What if?

- Customer cannot define named site tags (no AP names, no APs on maps) or simply doesn't want to do it
- Customer has already configured a site tag with a lot of APs (e.g., 600 APs on a 9800-40), so the load cannot help

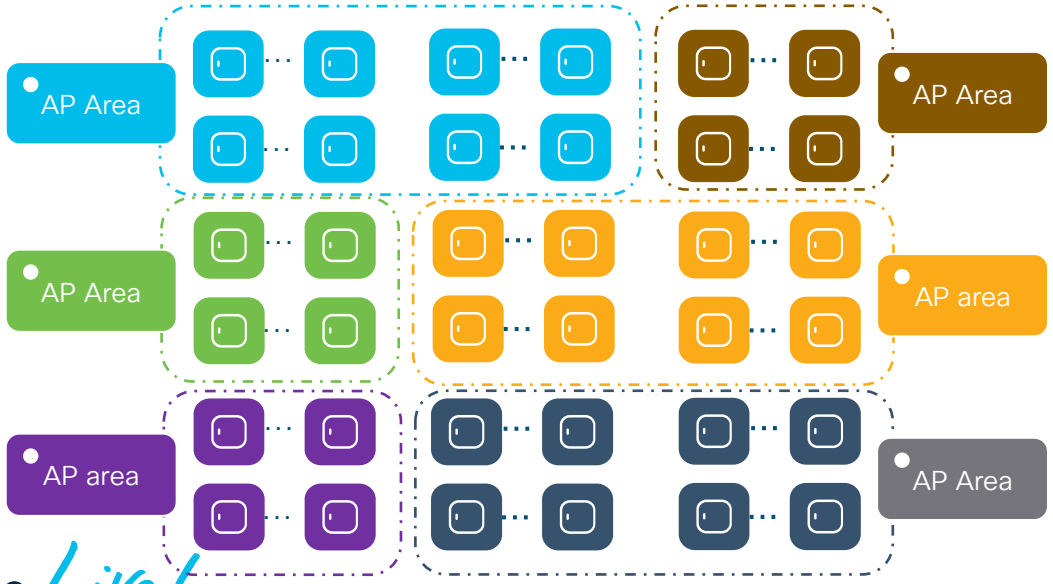
Starting 17.12.1, we have a solution!

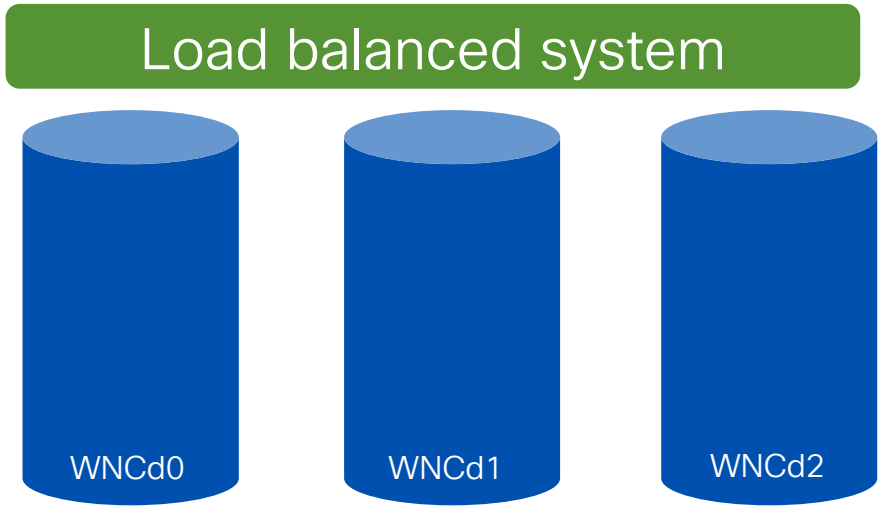
(RRM based) Auto WNCd load balancing

RRM based Auto WNCd load balancing

What is it?

- RRM-based, automatic way of clustering APs and evenly distribute them across WNCds.
- RF based clusters (AP Areas) are formed using RSSI info received from RRM AP neighbour reports
- The algorithm can be run on demand or scheduled. It's off by default and it requires the APs deployed and a stable RF (APs have their neighbours discovered). Works with any site tag configuration.
- The resulting AP load balancing is applied upon WLC reboot or admin trigger which causes AP CAPWAP restart
- When applied, it overwrites any other load balancing based on site tag and load

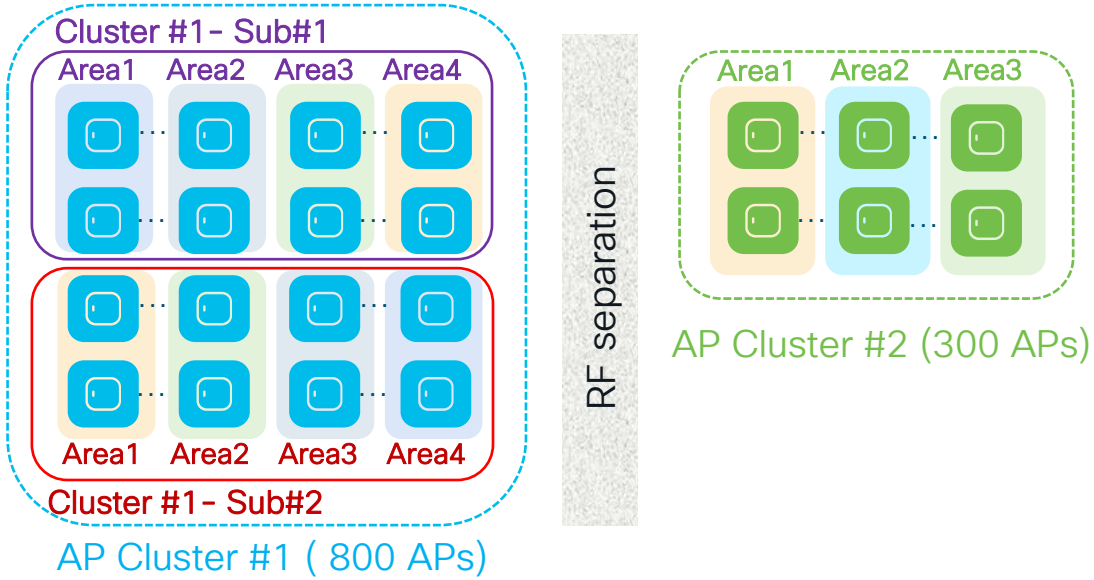




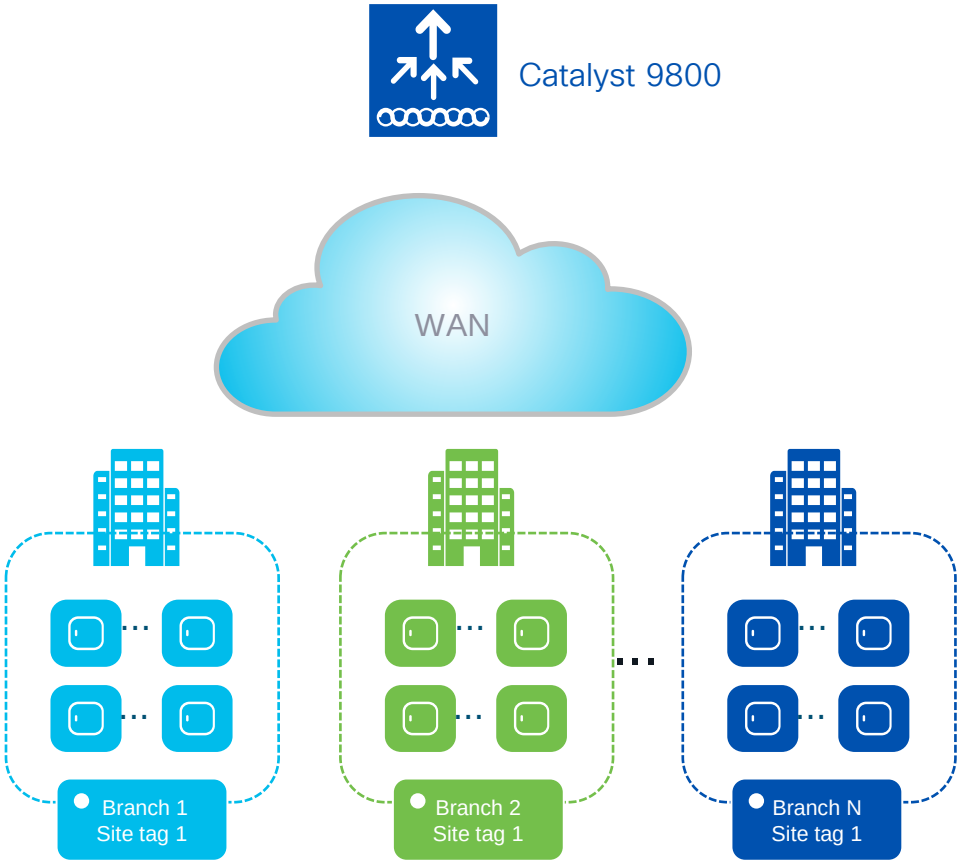
RRM based auto WNCd load balancing

How does the auto load balancing algorithm work?

- Form the AP clusters (neighbourhood) based on RSSI received from AP neighbour report on 5 GHz
- Further divide AP clusters into sub-neighbourhoods if the # of APs goes above a defined size (400)
- Create areas from each sub-neighbourhood. Each area size will be MAX 100 AP. A sub-neighbourhood can have up to 4 areas.
- Assign areas to WNCd processes to optimize APs to WNCd load balancing



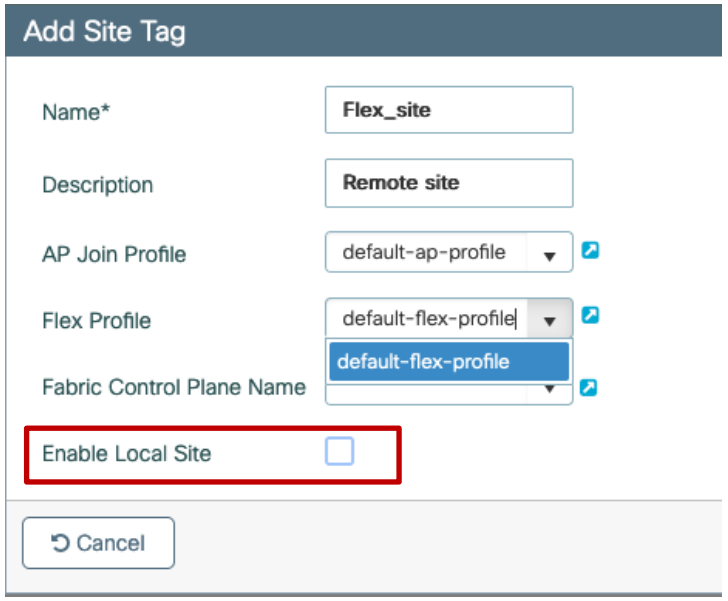
Site Tag for FlexConnect Deployments



FlexConnect APs

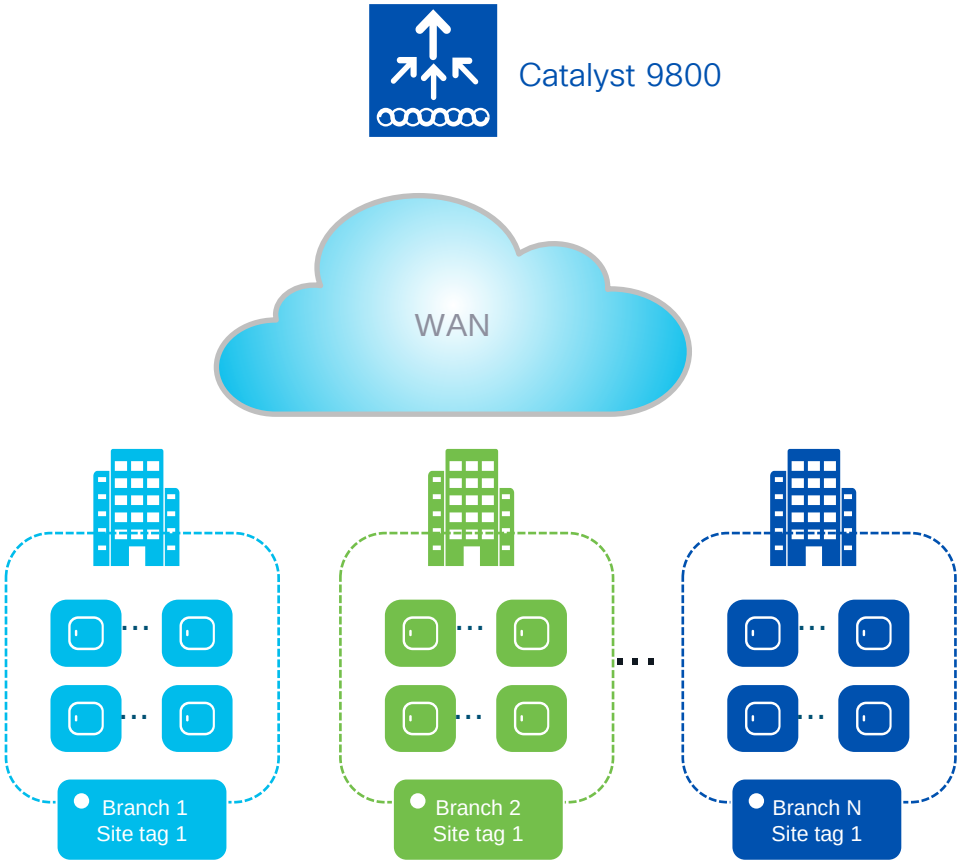
Important facts:

- For a site with FlexConnect APs, configure the Site Tag to be a non-Local Site (disable Local site)



- In this case the Site Tag is equivalent to the FlexConnect Group in AireOS

Site Tag for FlexConnect Deployments



Important facts:

- For FlexConnect, **fast roaming domain = site tag**. The clients' keys are distributed only to the APs in the same site tag
- Roaming across site tags for Flex APs will result in a client full re-authentication
- **Fast roaming is not supported on the default-site-tag** when configured as Flex (PMKs are not distributed) > always use a custom site tag
- As with AireOS, there is a limit of **100 APs** per **Flex Site Tag** for supporting seamless roaming (< 17.8)
- Starting 17.8, the limit is extended to 300 APs and 3000 clients

PMK = Pairwise Master Key

For your reference

Design- Recommended use of AP Site Tags

1. For **Local mode APs**, the recommended number is **500 APs per Site Tag**. But it should not exceed the following limit:

Platform	Max APs per site tag
9800-80, 9800-CL (Medium and Large)	1600
9800-40	800
Any other 9800 form factor	Max AP supported

2. Use the recommended number of site tags per platform and **evenly distribute APs among site tags**:

Platform	Tags per platform
C9800-80	8 or a multiple (16, 24, ...)
C9800-CL (large)	7 or a multiple (14, 21,..)
C9800-40	5 or a multiple (10, 15, ...)
C9800-CL (Medium)	3 or a multiple (6, 9,..)

RF Tag

First – a handy (free!) tool: WCAE

- **Wireless Config Analyzer Express** (WCAE) is an extremely valuable tool when validating and optimizing a Cisco Wi-Fi deployment
- Feed your WLC config output to WCAE and it will help you:
  - Find and troubleshoot problems quickly
  - Identify top areas for RF optimization
  - Check configs against best practices
  - RRM overview with the RF Summary

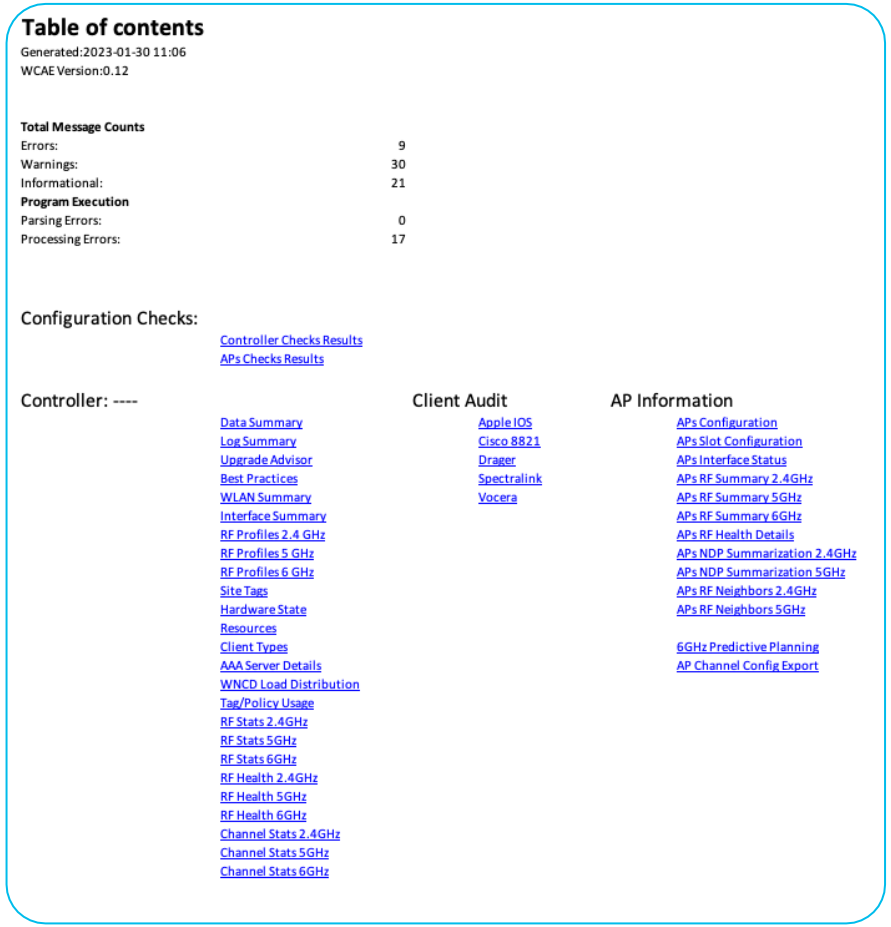


Table of contents

Generated:2023-01-30 11:06
WCAE Version:0.12

Total Message Counts

Errors:	9
Warnings:	30
Informational:	21
Program Execution	
Parsing Errors:	0
Processing Errors:	17

Configuration Checks:

Controller Checks Results
APs Checks Results

Controller: ----

Data Summary
Log Summary
Upgrade Advisor
Best Practices
WLAN Summary
Interface Summary
RF Profiles 2.4 GHz
RF Profiles 5 GHz
RF Profiles 6 GHz
Site Tags
Hardware State
Resources
Client Types
AAA Server Details
WNCD Load Distribution
Tag/Policy Usage
RF Stats 2.4GHz
RF Stats 5GHz
RF Stats 6GHz
RF Health 2.4GHz
RF Health 5GHz
RF Health 6GHz
Channel Stats 2.4GHz
Channel Stats 5GHz
Channel Stats 6GHz

Client Audit

Apple IOS
Cisco 8821
Drager
Spectralink
Vocera

AP Information

APs Configuration
APs Slot Configuration
APs Interface Status
APs RF Summary 2.4GHz
APs RF Summary 5GHz
APs RF Summary 6GHz
APs RF Health Details
APs NDP Summarization 2.4GHz
APs NDP Summarization 5GHz
APs RF Neighbors 2.4GHz
APs RF Neighbors 5GHz

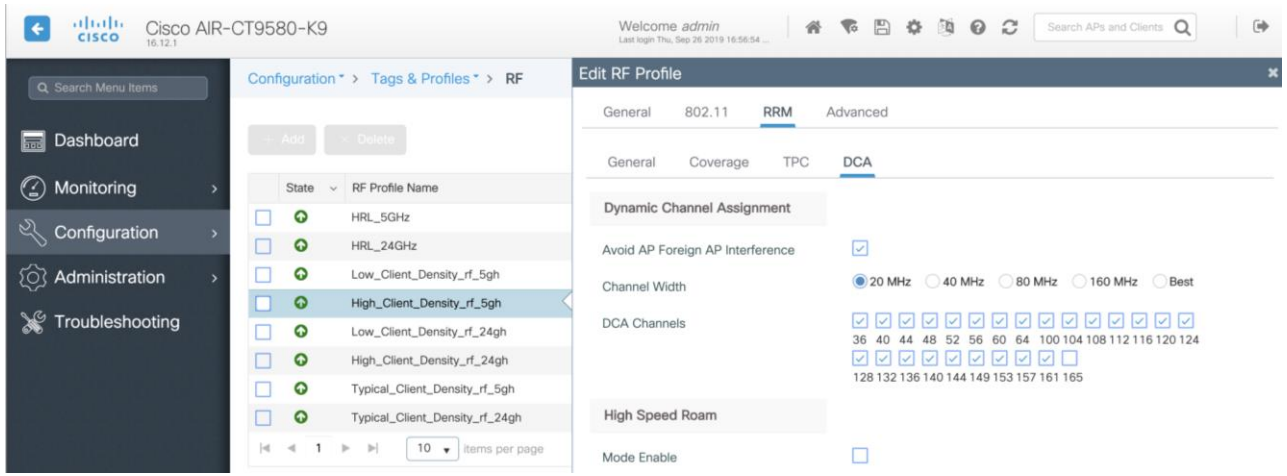
6GHz Predictive Planning
AP Channel Config Export

Download: https://developer.cisco.com/docs/wireless-troubleshooting-tools/

More info: Cisco Live US 2022 – BRKEWN-3006

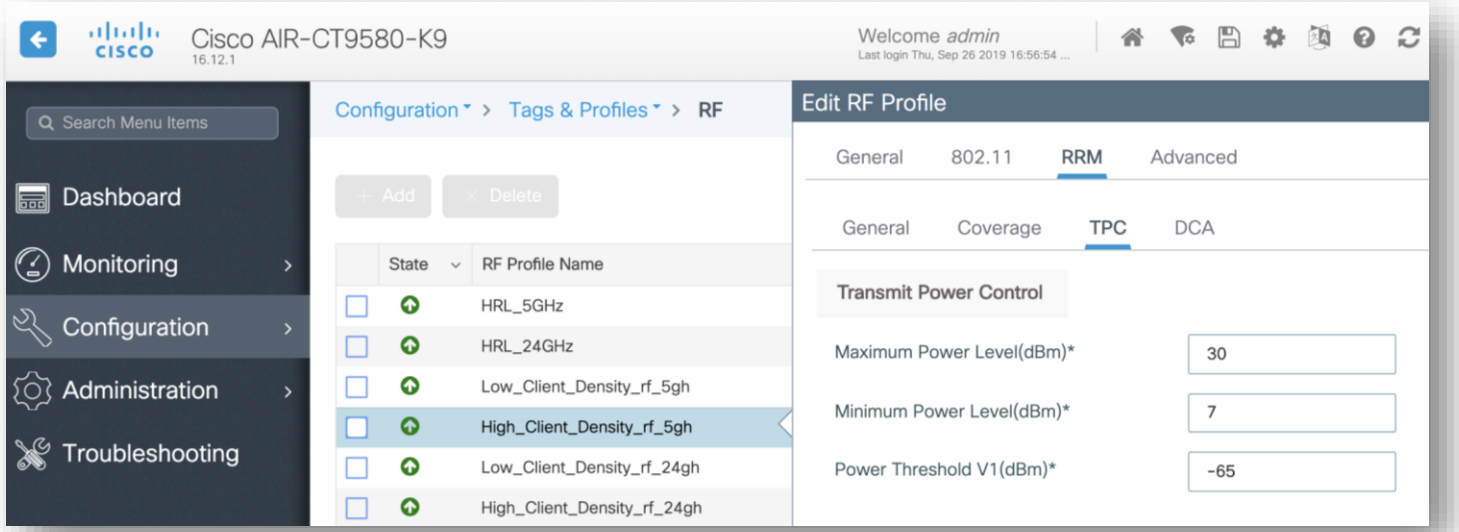
Channel Planning with RF Profiles

- Plan channels with Dynamic Channel Allocation (Catalyst) via RF Profile
- If needed – **eliminate unusable channels** for business-critical areas (DFS, etc)
- Reserve channels for use by other systems

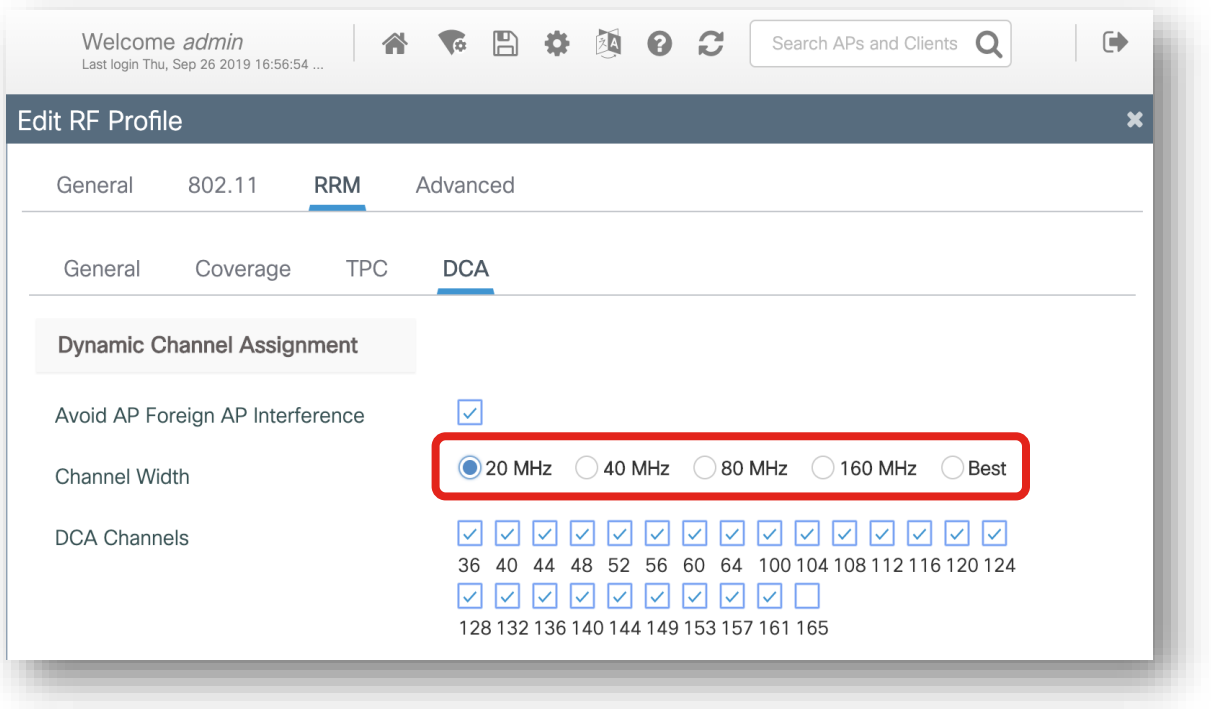


Balancing Transmit Power with RF Profiles

- **Ensures AP-to-AP consistency** (no “client magnets”) and 2.4GHz to 5GHz balance (5GHz hotter, 2.4GHz cooler)
- **TPC/AutoPower Min** – lower power limit specified for a given radio. TPC/AutoPower will never adjust power below this level.
- **TPC/AutoPower Max** – upper power limit specified for a given radio. TPC/AutoPower will never adjust power above this level.



Selecting Channel Width with RF Profiles



5GHz

- Recommendation is **40MHz channel**
  - Balances performance and non-overlapping channel
- Use **20 MHz** in high density environments
  - Provides most channel reuse (capacity)
- **Wider channels may be used selectively** in more isolated areas – smaller classrooms, lobbies, conference rooms, etc.

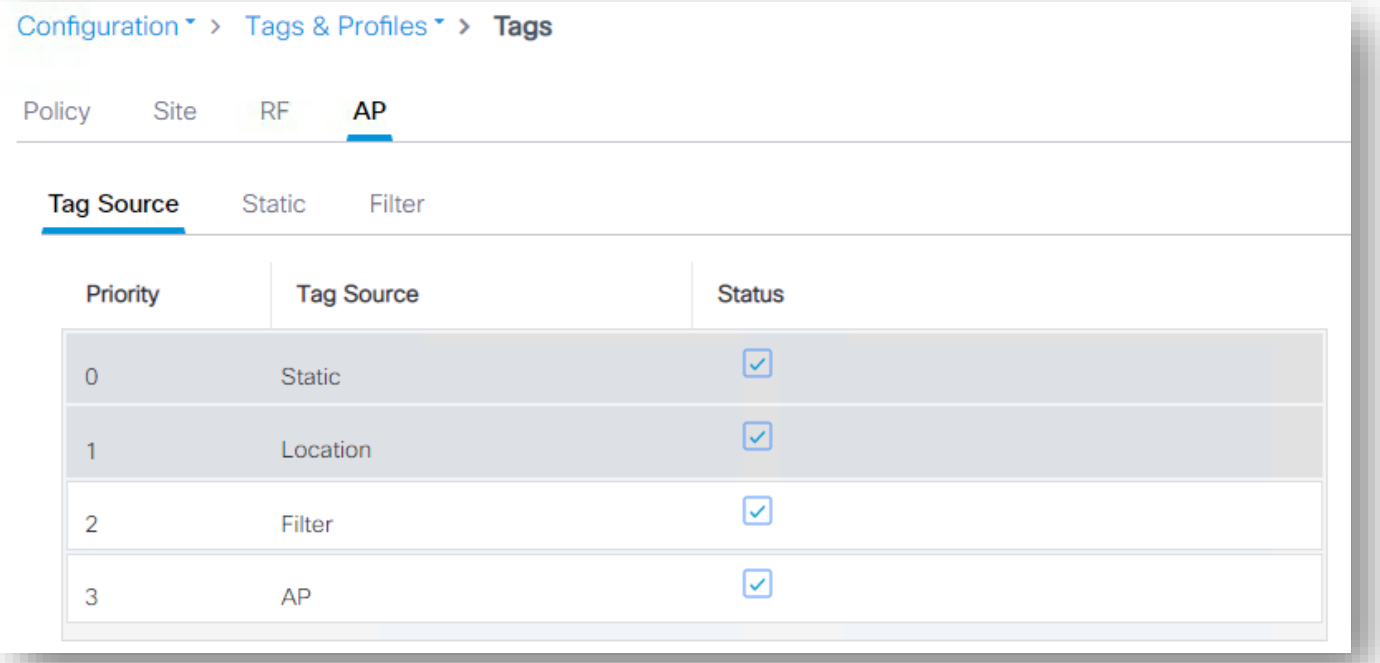
6GHz

- Heavily dependent on regulatory domain
- Note! Higher channel width results in higher max Tx power for data frames (but not beacons – remember when surveying!)

APs to Tags mapping

AP to Tags assignment

- Without an existing configuration, when the AP joins the C9800 it gets assigned the default tags: namely the **default-policy-tag**, **default-site-tag** and **default-rf-tag**
- The AP <> tags mapping can have multiple tag sources:

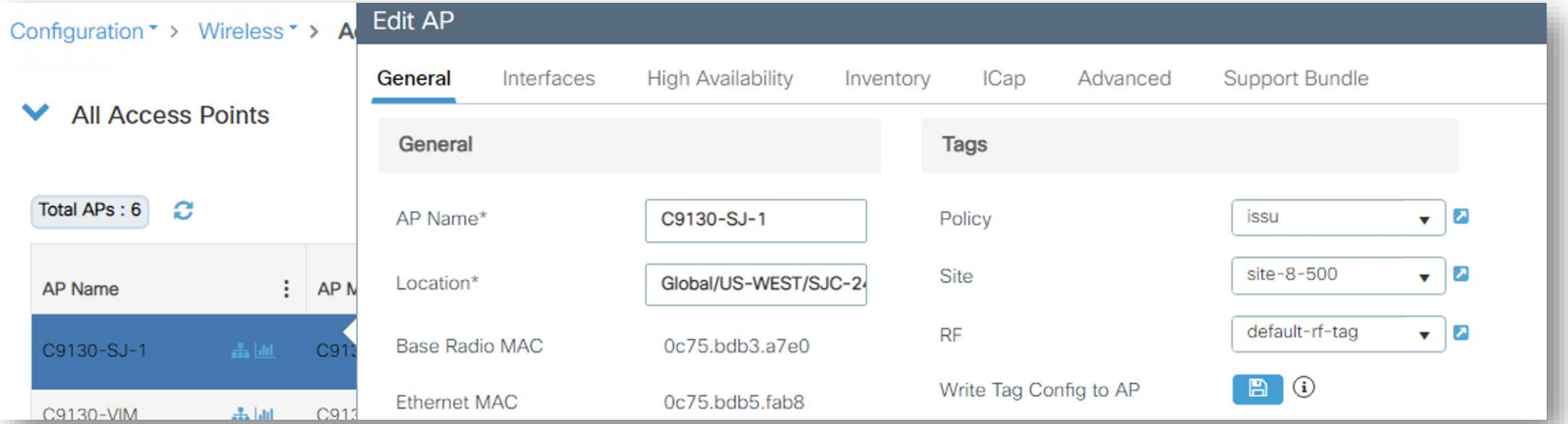


- Static: admin configuration
- Location: Basic Setup flow
- Filter: regular expression
- AP: the tags are saved on AP

These are in order of priority. You can only change the priority order of Filter and AP source

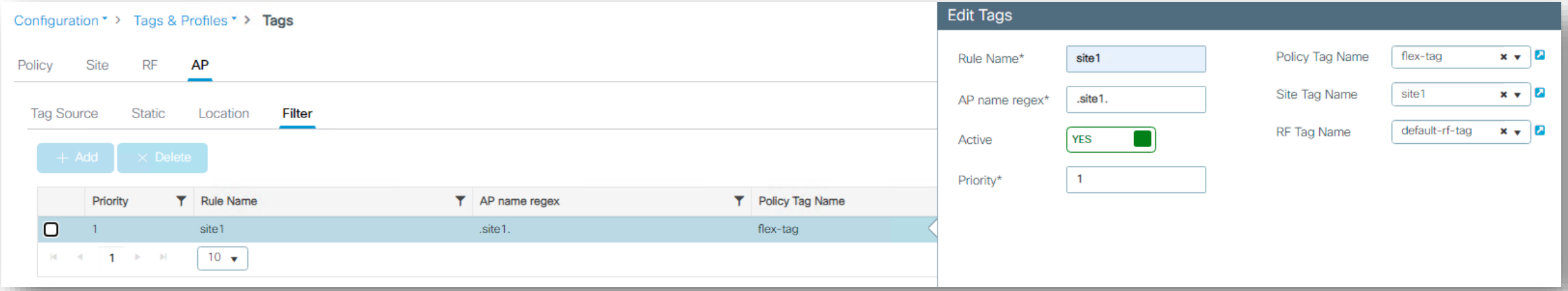
AP to Tags assignment – Source: Static

- The **static** Tag <> AP binding is based on AP's Ethernet MAC and it's a configuration on the Controller: upon joining the C9800, the configuration is applied and AP gets assigned to the selected tags
- Go to Configuration > Wireless > Access Points



AP to Tags assignment – Source: Filter

- Filter: You need an AP naming convention (ex., AP_<#>_<site>, where site can be building, floor, area) and your APs have already been named correctly
- Configuration>Tags & Profiles>Tags go to AP>Filter: add a rule with a regex expression to match APs with e.g., “site1” in the name and assign them to the desired tags



- When the AP with name containing “site1” joins the C9800 or it’s renamed, it’s assigned to the tags specified in the filter. Since this is an AP tag change, a CAPWAP restart is triggered automatically, the AP will disjoin and join back (less than 30s)

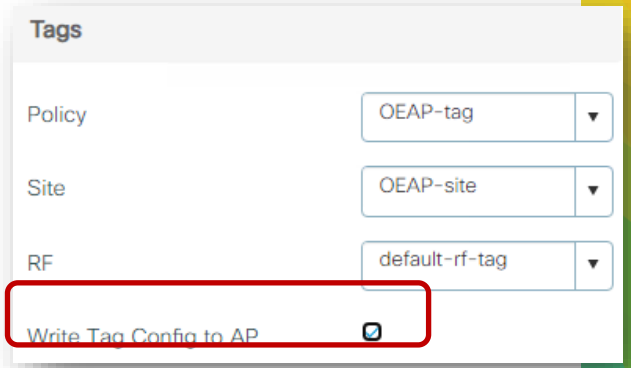
CAPWAP = Control and Provisioning of Wireless Access Points

AP to Tags assignment – Source: AP

- The AP present the tags upon joining, no mapping is needed on C9800
- The AP retains its tags when joining a new WLC, if the tags are defined on the new WLC and there is no higher priority mapping (e.g., static)
- Before 17.6, to push the tags information to the AP, you need to use a CLI command in exec mode:

```
C9800#ap name <APname> write tag-config
```

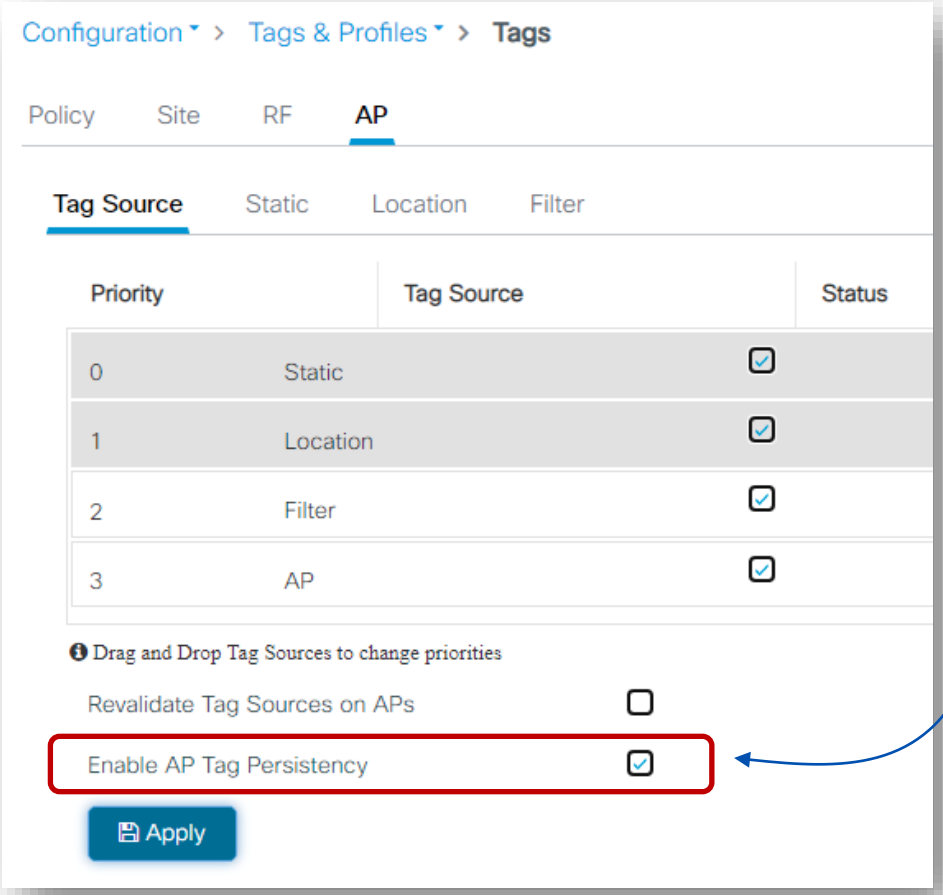
- Using the CLI command could be cumbersome, we have solutions:
  - Event Manager Script (useful for 17.3.x release)
  - Graphical user interface (GUI) settings in 17.4.1 and later
  - Starting 17.6. new feature called AP Tag Persistency



AP to Tags assignment – AP (SW >17.6)

Configuring AP Tag Persistency

Configuration > Tags & Profiles > Tags:



- From 17.6.1 this is supported in CLI in global configuration mode:
  `C9800(config)#ap tag persistency enable`
- 17.6.2 and 17.7 adds support from GUI

Note: This will enable writing tags to the AP as it joins. For this to be applied to existing APs joined to the C9800, they will need to rejoin the WLC (CAPWAP restart)

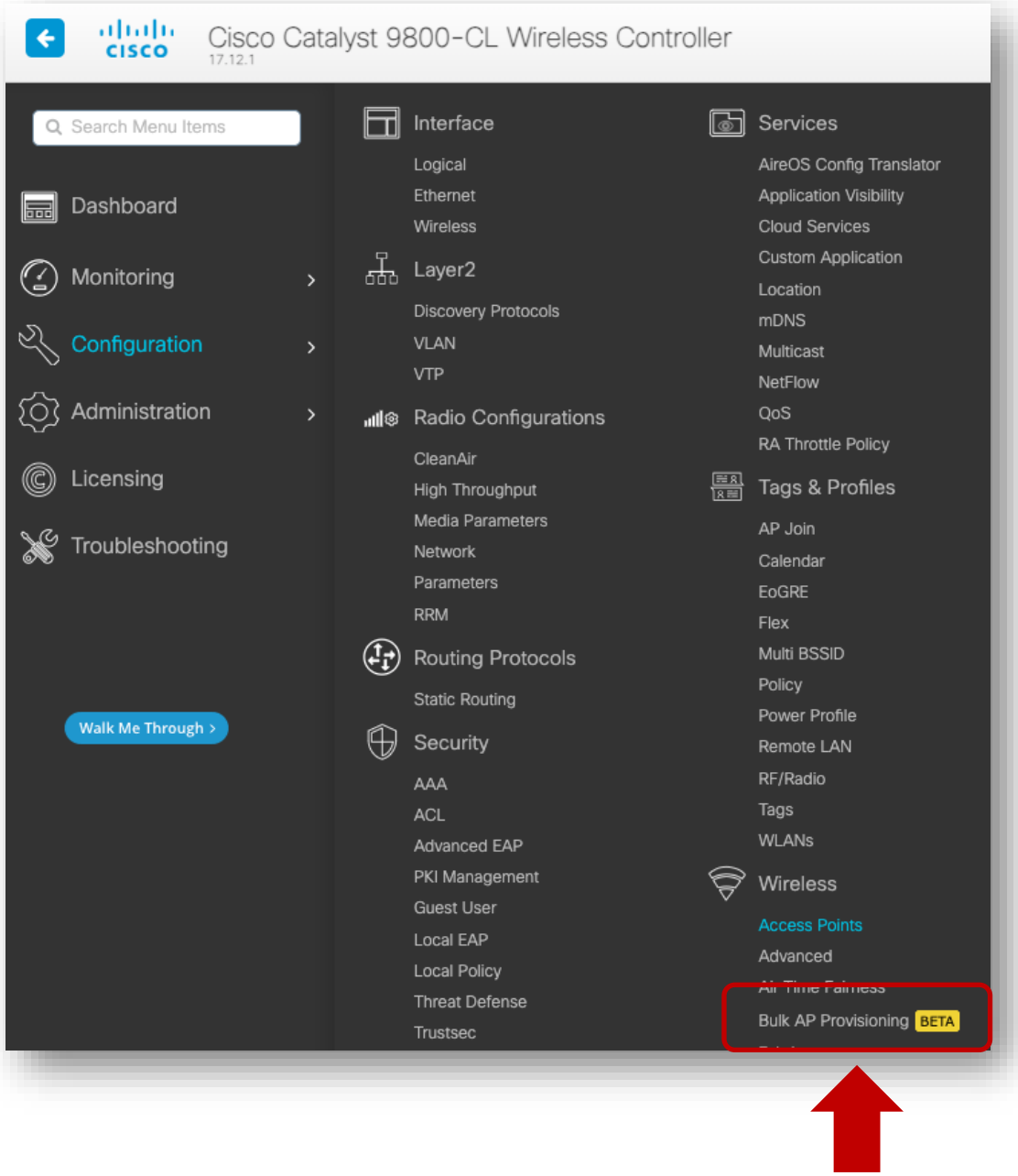
Verifying AP Tag source

- Run the show command below:

```
C9800#show ap tag summary

Number of APs: 1

AP Name    AP Mac    Site Tag Name    Policy Tag Name    RF Tag Name    Misconfigured   Tag Source

-------------------------------------------------------------------------------------------
AP1       <MAC>       flex-site1         flex-tag         default-rf-tag      No           AP
AP2       <MAC>       site-8-500         issu             default-rf-tag      No           Static
```

- For Persistency mapping, ensure that the Tag Source shows AP, indicating that the tags were successfully written to the AP and learnt/used by the WLC.

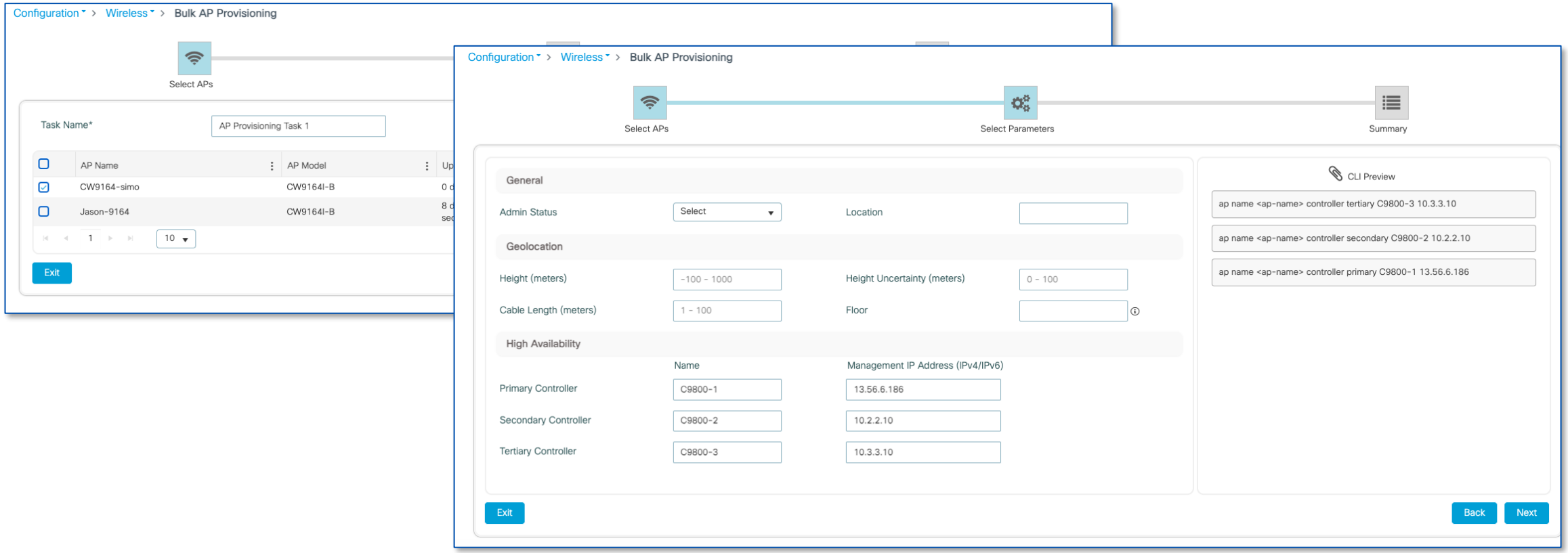
AP Bulk Provisioning



AP Bulk Provisioning

Why would you care?

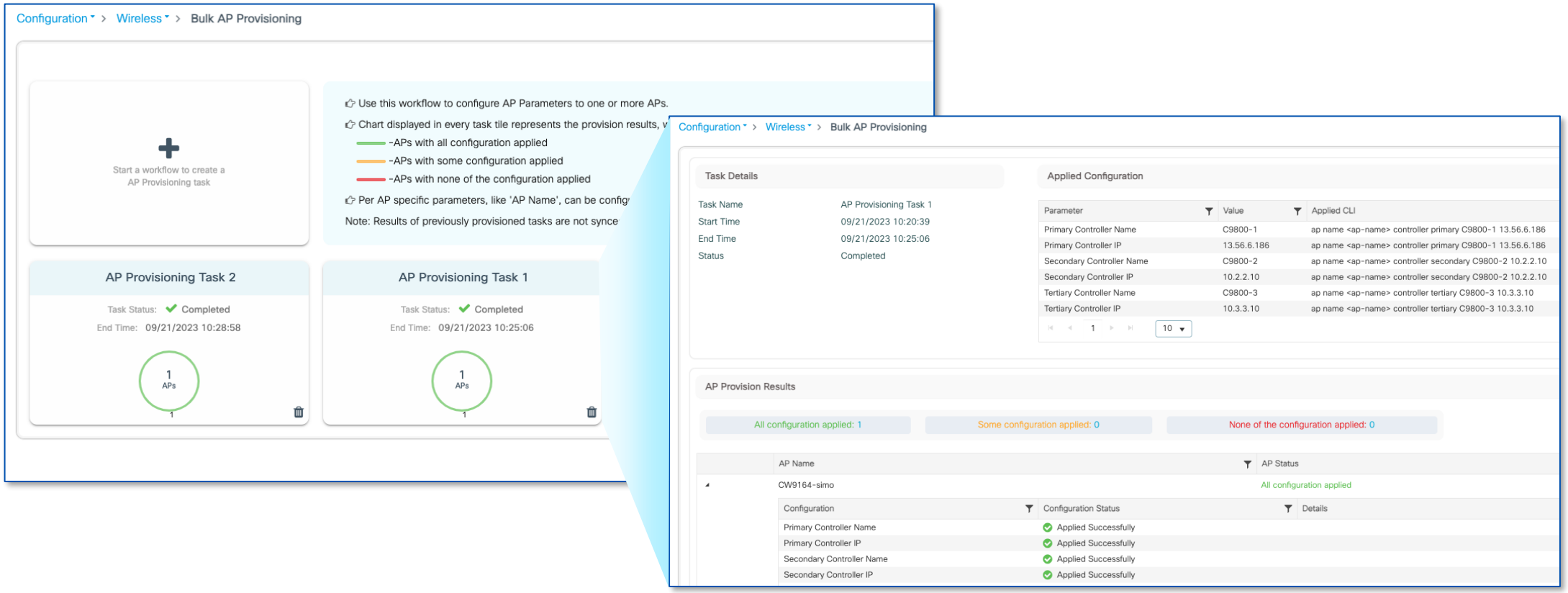
- Change few AP settings…in bulk!
- One of the most requested is changing the Primary (Secondary/Tertiary), to move APs between WLCs



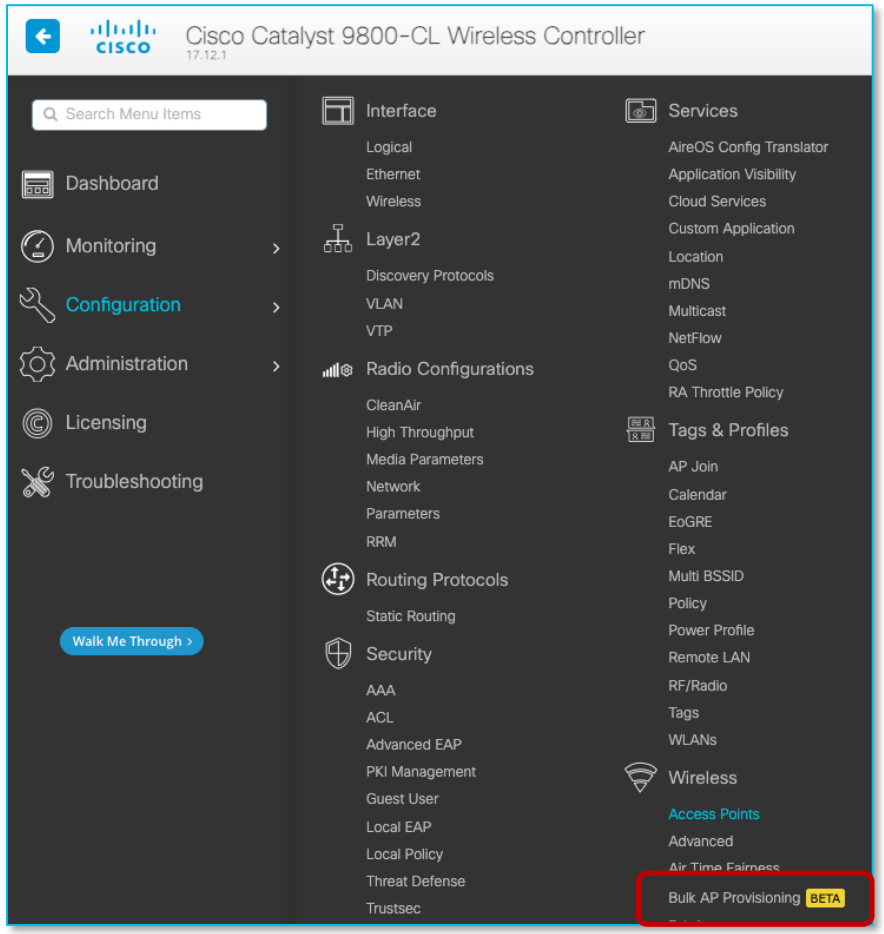
AP Bulk Provisioning

Why would you care?

- Change few AP settings…in bulk!
- One of the most requested is changing the Primary (Secondary/Tertiary), to move APs between WLCs



AP Bulk Provisioning – what's next?



- BETA tag removed in 17.12.2 and 17.13
- Additional filters to select APs (e.g., AP tags) coming in 17.13
- Any other ideas? LET US KNOW!

Day 2

AI-Enhanced RRM

AI-Enhanced RRM key customer benefits

Better RF, better insights, reduced operational costs and time

AI-driven self-optimizing RF

Leverages machine learning to find patterns and optimize your RF before issues happen.

Performance visibility

Provides per-building visibility into RF health using Wireless Config Analyzer algorithm.

Complete historical context

Understand exactly what RRM changes occurred at a per-AP level, and how they benefit the network.

Measured Improvements in RF KPIs!

- CCI Reduction: Up to 40%
- SNR Downlink Gain: Up to 7 dB
- RRM Changes Reduction: Up to 75% at busy hours

Actionable insights

AI-derived recommendations on RRM setting changes for a more optimal performance.

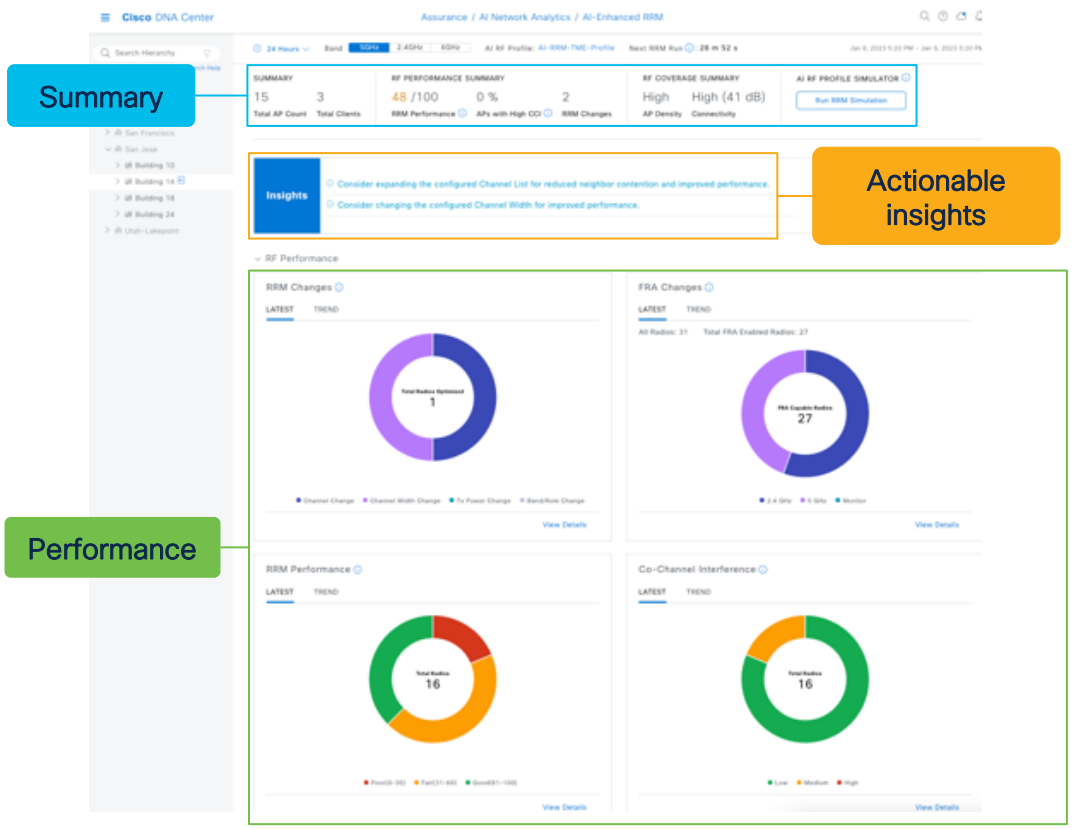
Simplified RRM configuration

Complicated traditional RRM configurations are simplified, with policy toggles and thresholds.

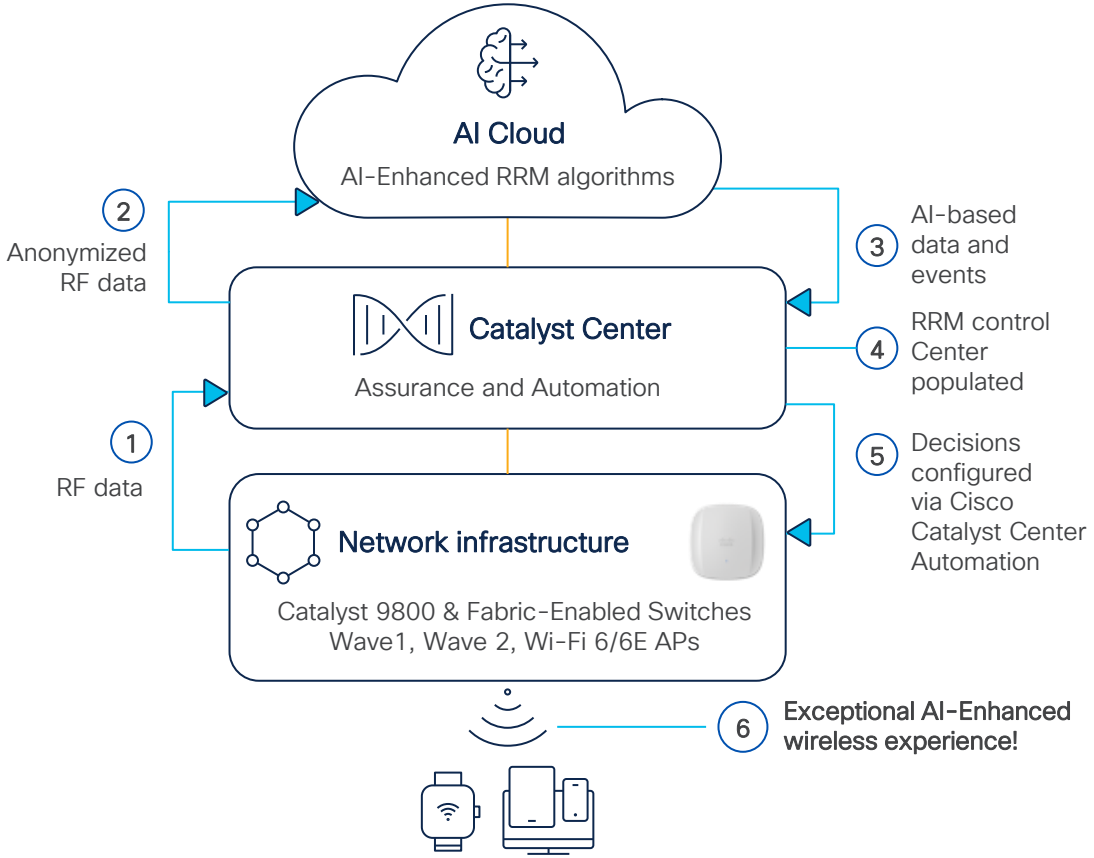
AI-Enhanced RRM is AI that Powers RF Optimization

Provides Users with Better Wi-Fi and Admins with a Better RF Management Experience!

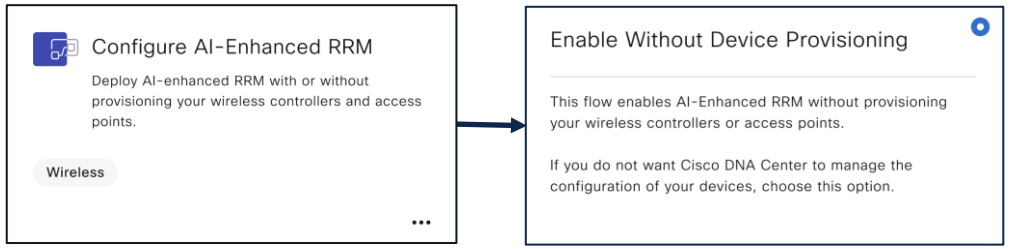
Instantaneous visibility



Proactive optimizations



What mitigates these pain points?



New AI-Enhanced RRM Workflow for Assurance Only Customers!

For More Information

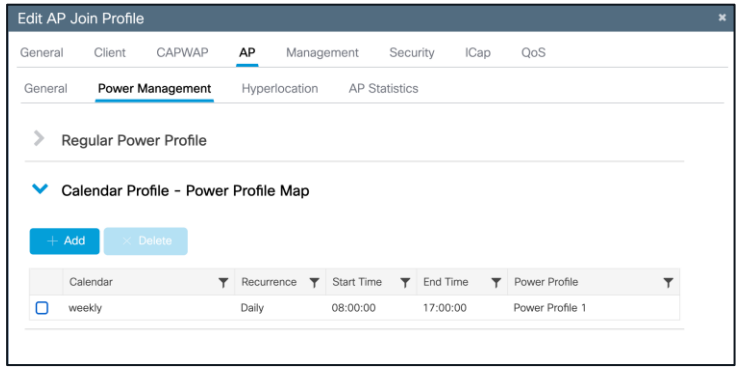
AP Power Optimization

AP Power Optimizations Feature Suite

Save Power, Reallocate Power, and Visibility into Savings

AP Power Save Mode
Lower AP Power Usage

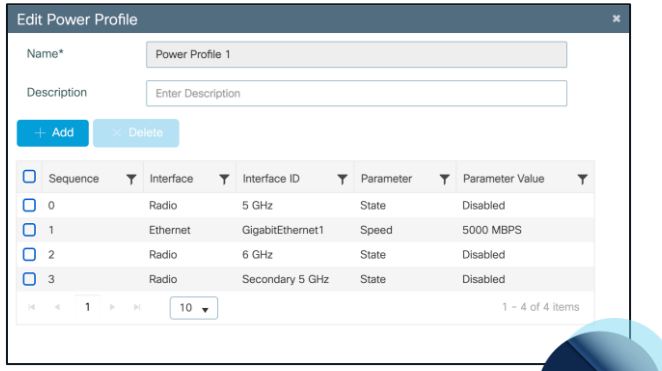
- Create a calendar profile for off-peak hours.
- Create a power profile to lower the power consumption budget during off-peak hours.
- Power Profile: Shut AP Radio or lower spatial Stream, lower port speed, disable USB port.



IOS-XE 17.8

AP Power Distribution
Control over how power is

- Reallocate extra AP Power to different radios while operating on PoE+ (30W).
- Customization of your PoE power budget.
- Example: Disable 2.4 GHz radio -> use extra power for 6 GHz radio.



IOS-XE 17.10

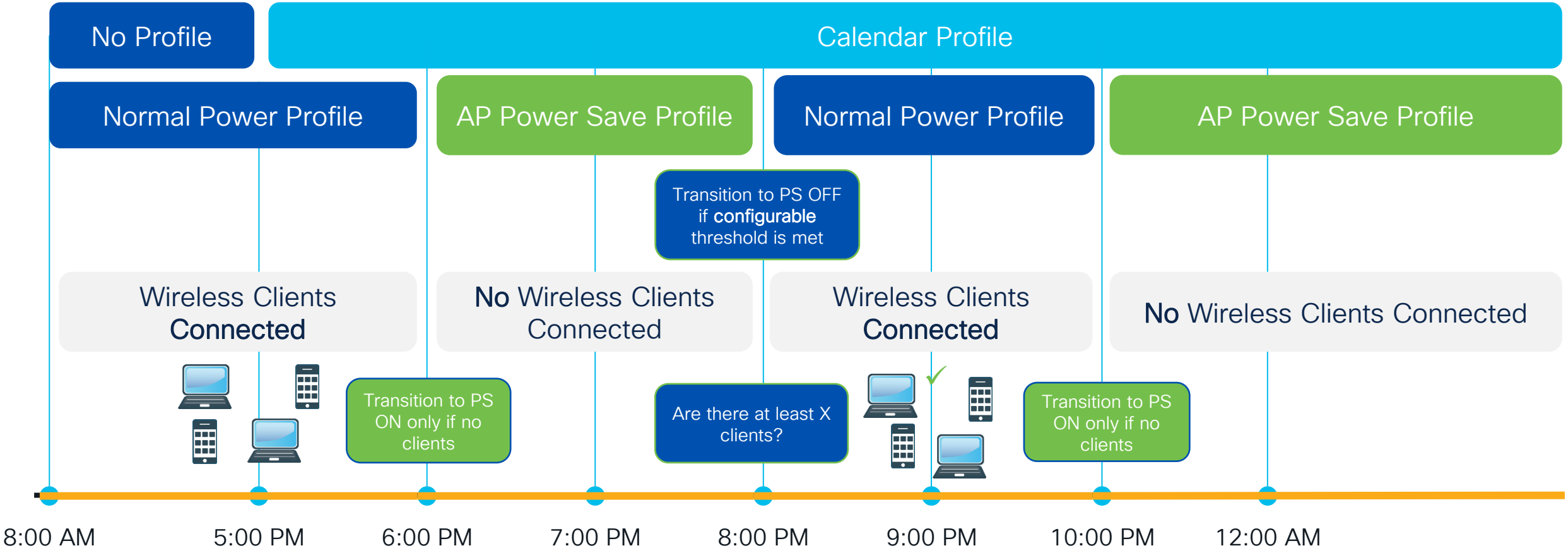
NEW

AP Power Savings Insight
Power, Money, and Emissions Savings on Cisco Catalyst Center

- Cisco Catalyst Center PoE dashboard integration.
- Power Savings, Money Savings, Emissions Reductions.
- Visibility into trends and insights.
- Both site level and AP level view.

Catalyst AP Power Save (PS): Client logic change

From 17.12.1! (originally was coming in 17.13)!!

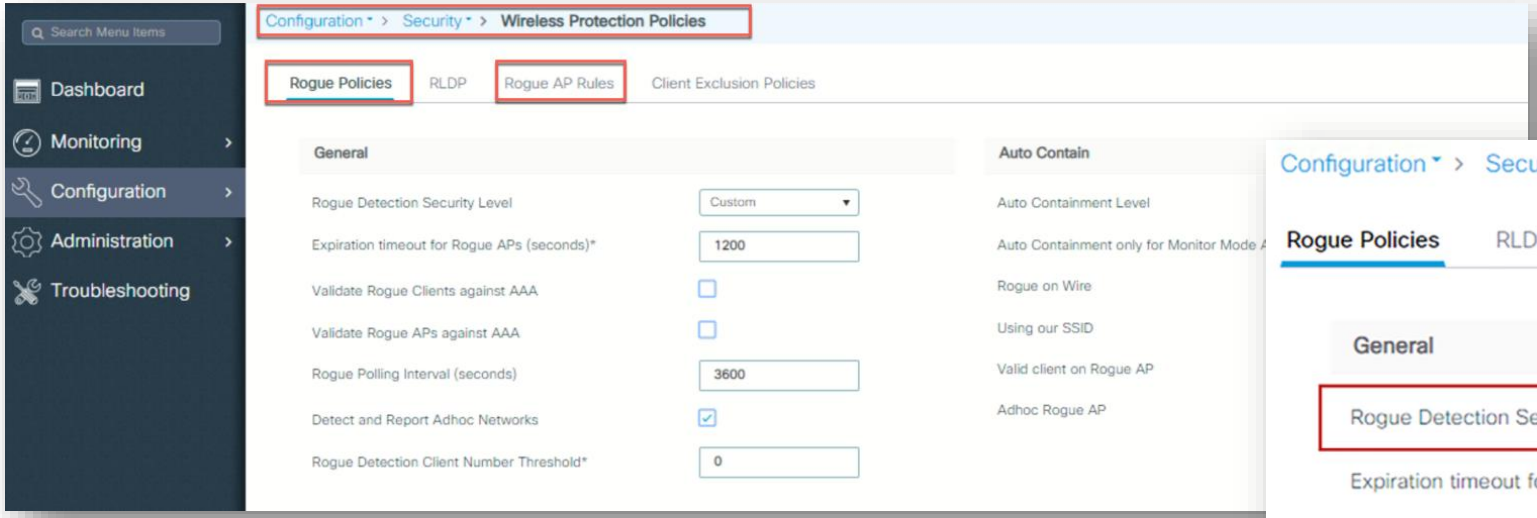


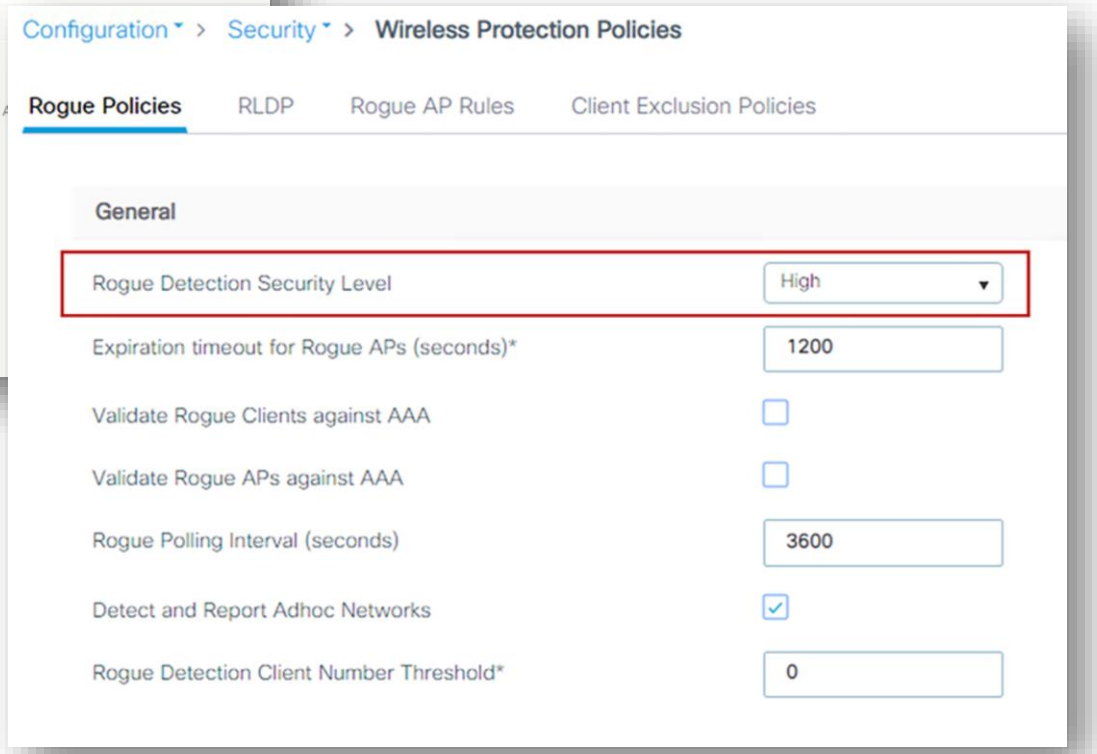
Rogues

Rogue rules on C9800

Rogue rules can be configured on C9800 to classify and contain rogues and set thresholds.

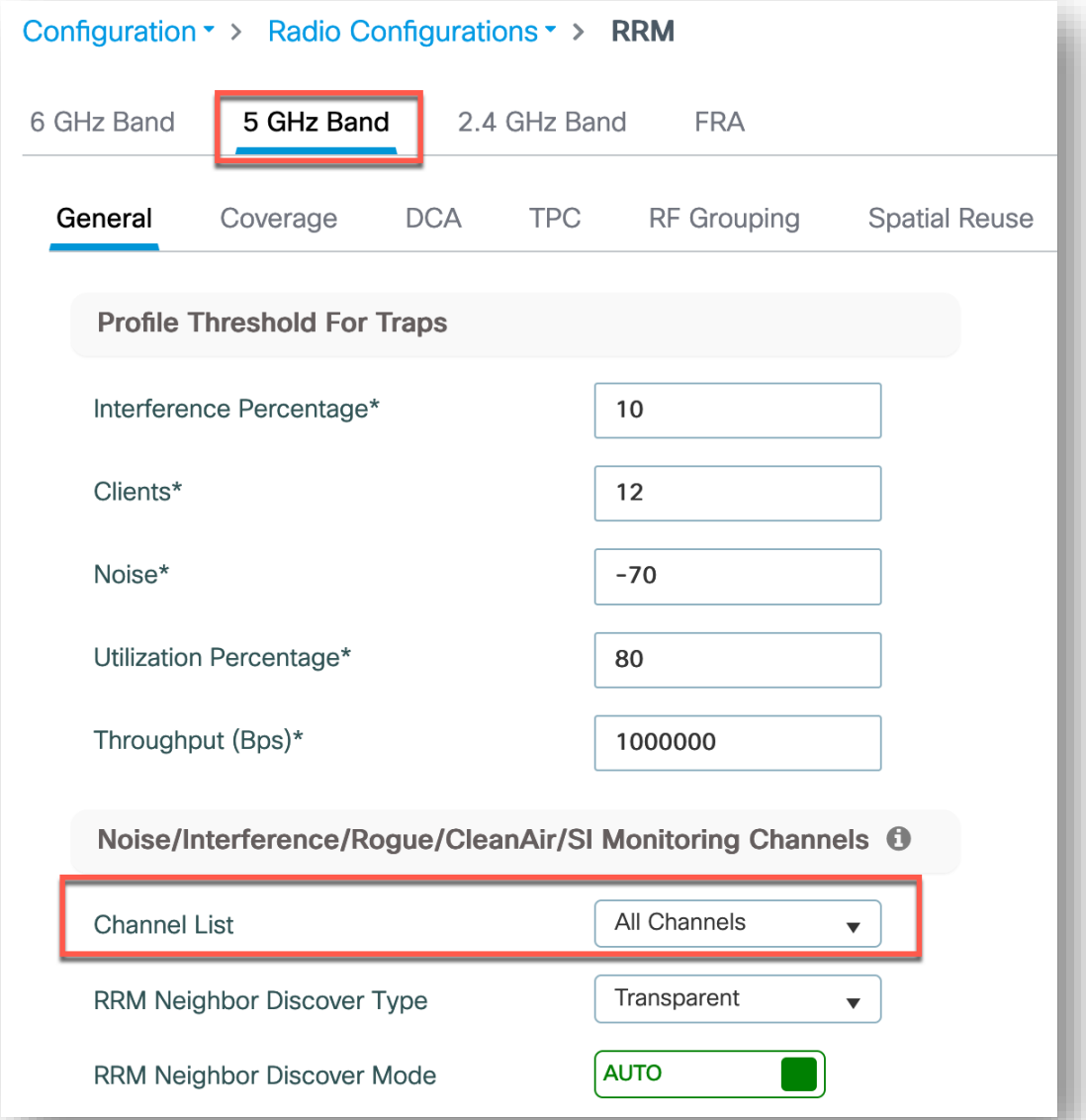
At a minimum, the security level should be set to **High**





Rogue Monitoring Channels

- For higher security, choose to scan all channels.
- Choose DCA channels for higher performance, as the system will scan the least number of channels.
- For a balance of performance and security, choose the country channel option.



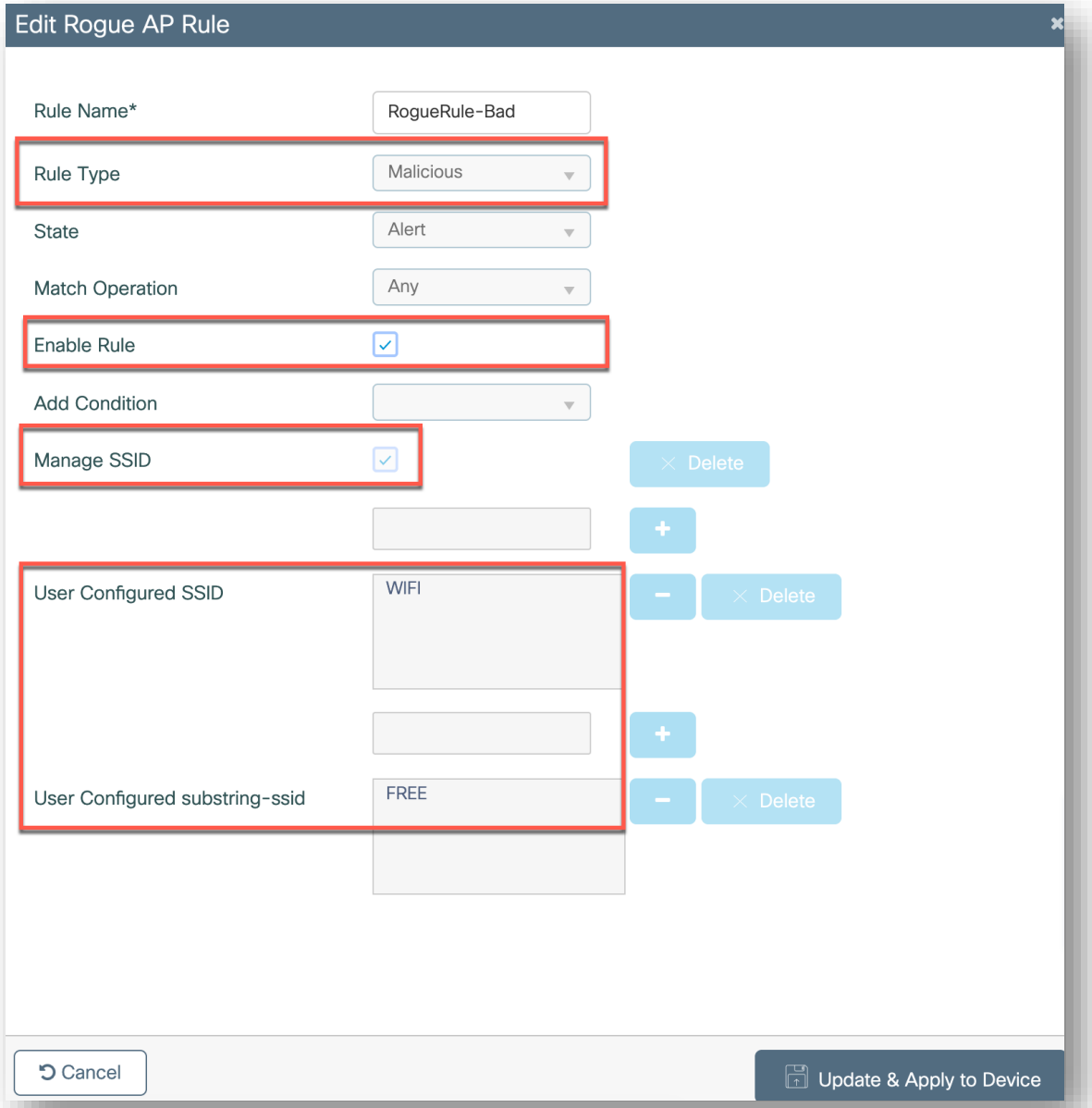
Rogue AP rules

Recommended malicious rogue AP rules

Managed SSIDs: Any rogue APs using managed SSIDs, like your wireless infrastructure, must be marked as malicious.

Minimum RSSI >-70 dBm: For Enterprise deployments

User-configured SSID/substring SSIDs: Monitor any SSIDs that use different variations.



CleanAir Pro™

Introducing Cisco CleanAir Pro™

15 years of innovations and excellence carried forward

Cisco CleanAir®

RF ASIC-based excellence

Purpose built for 2.4- and 5-GHz wireless

Cisco CleanAir™ Pro

Evolving Wi-Fi excellence into 6 GHz

- Full 2.4-, 5-, and 6-GHz band support
- Multiradio architecture
- AI/ML-driven scanning radio decoding HE frames
- ML-based interferer classification, on AP

CleanAir Pro™ ML Based Classification

- ML-based
  - Train classifier based on the collected metrics/statistics
  - Data set includes both cabled and OTA data, mixed/unmixed with WiFi
    - Thousands of samples per device type
- Data Collection
  - Built-in command that triggers saving off raw spectrogram data for later offline retraining of classifier
  - Enhancements can be distributed back through WLC or Catalyst Center

Cisco CleanAir Pro™

Detect/Classify

- CleanAir Pro =CA-Pro
- 5 GHz Video Camera is on Channel 157
- All the CleanAir and CleanAir Pro radios agree – channel 157 is messed up and it is severe.
- Some Disagreement on device type
- All agree on the Duty Cycle

Monitoring > Wireless > CleanAir Statistics

5 GHz Band | 2.4 GHz Band

CleanAir Interference Devices | SI Interference Devices | Air Quality Report | Worst Air Quality Report

Cluster ID	Interferer Type	AP Name	Version	Severity	RSSI (dBm)	Duty Cycle (%)	Affected Channel
d500.0000.00ea	Continuous TX	C9130i_9f.6e.a0	CA	5	-93	100	157
d500.0000.00ea	Continuous TX	C9130i_9f.6e.a0	CA	4	-93	100	157
d500.0000.00ea	Video camera	Marlin_4_91.4260	CA	88	-65	100	157
~~d500.0000.00c9~~	~~WiFi Inv. Ch~~	~~Marlin_4_91.4260~~	~~CA~~	~~2~~	~~-81~~	~~1~~	~~144~~
d500.0000.00ea	Video camera	C9120_E-a2:9d:c0	CA	35	-86	100	157
d500.0000.00ea	Continuous TX	C9120_E-a2:9d:c0	CA	--	-80	100	157
d500.0000.010f	Video camera	CW9166i_Fe.0e20	CA-Pro	3	-76	100	157
d500.0000.011c	Continuous TX	CW9166i_Fe.0e20	CA-Pro	100	-52	100	157
d500.0000.011c	Continuous TX	C9136.5F:09e0	CA-Pro	100	-55	100	157
d500.0000.011c	Continuous TX	C9136_5f.f1.a0	CA-Pro	3	-74	100	157

Cisco CleanAir Pro™

Detect/Classify

- CleanAir Pro =CA-Pro
- 5 GHz Video Camera is on Channel 157
- C9130i_9f.6e.a0 see's 100% DC at -93 dBm and a minor severity of 5 (meh..)
- C9136 and CW9166 see it at -52 to - 55 dBm with a high severity of 100 (very bad)

Monitoring > Wireless > CleanAir Statistics

5 GHz Band | 2.4 GHz Band

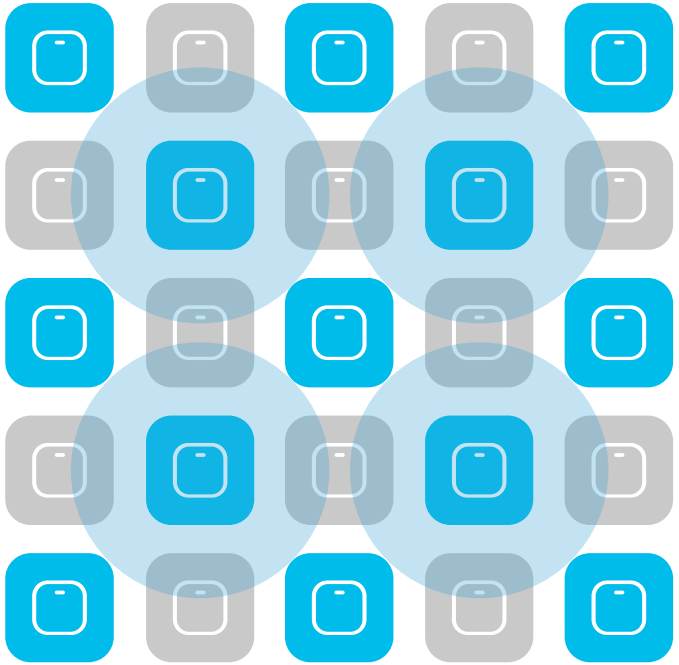
CleanAir Interference Devices | SI Interference Devices | Air Quality Report | Worst Air Quality Report

Cluster ID	Interferer Type	AP Name	Version	Severity	RSSI (dBm)	Duty Cycle (%)	Affected Channel
d500.0000.00ea	Continuous TX	C9130i_9f.6e.a0	CA	5	-93	100	157
d500.0000.00ea	Continuous TX	C9130i_9f.6e.a0	CA	4	-93	100	157
d500.0000.00ea	Video camera	Marlin_4_91.4260	CA	88	-65	100	157
d500.0000.00c9	WiFi Inv. Ch	Marlin_4_91.4260	CA	2	-81	1	144
d500.0000.00ea	Video camera	C9120_E-a2:9d:c0	CA	35	-86	100	157
d500.0000.00ea	Continuous TX	C9120_E-a2:9d:c0	CA	--	-80	100	157
d500.0000.010f	Video camera	CW9166i_Fe.0e20	CA-Pro	3	-76	100	157
d500.0000.011c	Continuous TX	CW9166i_Fe.0e20	CA-Pro	100	-52	100	157
d500.0000.011c	Continuous TX	C9136.5F:09e0	CA-Pro	100	-55	100	157
d500.0000.011c	Continuous TX	C9136_5f.f1.a0	CA-Pro	3	-74	100	157

Software Updates

Rolling AP Update/Upgrade Infrastructure

Rolling AP Upgrade: Neighbor AP marking

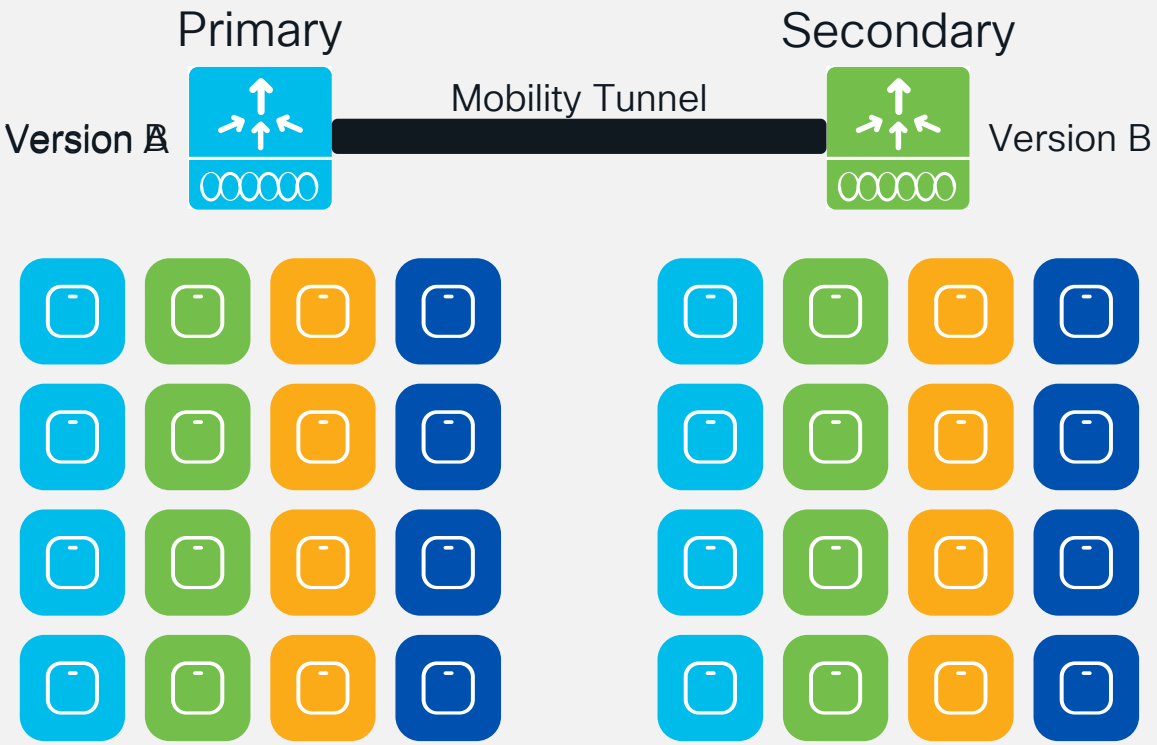


How does it work?

- Group APs into multiple groups and upgrade one group at a time.
- Grouping is done based on RF neighbors
- Admin user can control the impact and determines the number of iterations taken and the Rolling Upgrade time
- Candidate AP selection
  - With N = 4: If the AP in blue is selected and 4 of its best neighbours marked unavailable for selection. The resultant selection will be about P = 50% of APs
  - For P = 25%, N = 6, expected iterations all ap upgrade ~ 5 > ~1h
  - For P = 15%, N = 12, expected iterations all ap upgrade ~ 12 > ~2h
  - For P = 5%, N= 24, expected iterations all ap upgrade ~ 22 > ~4h
  - APs reload and re-join (AP image pre-download is used) determines the Rolling AP Upgrade time

N+1 Site Based Hitless Upgrade

N+1 Site Based Hitless Upgrade



- Use new Site Filters for per-site image upgrades of APs in N+1 scenarios
- Like the previous N+1 Hitless Upgrades, APs will pre-download the images
- During site upgrades, APs will upgrade to new image in rolling fashion
- After the primary controller is upgraded, APs can move back in similar fashion

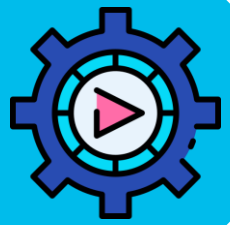
In-Service Software Upgrade (ISSU)

Why ISSU?

Eliminate network downtime during controller upgrade process

Eliminate the need for a dedicated N+1 controller in the upgrade process

Automate the process of upgrade without manual intervention



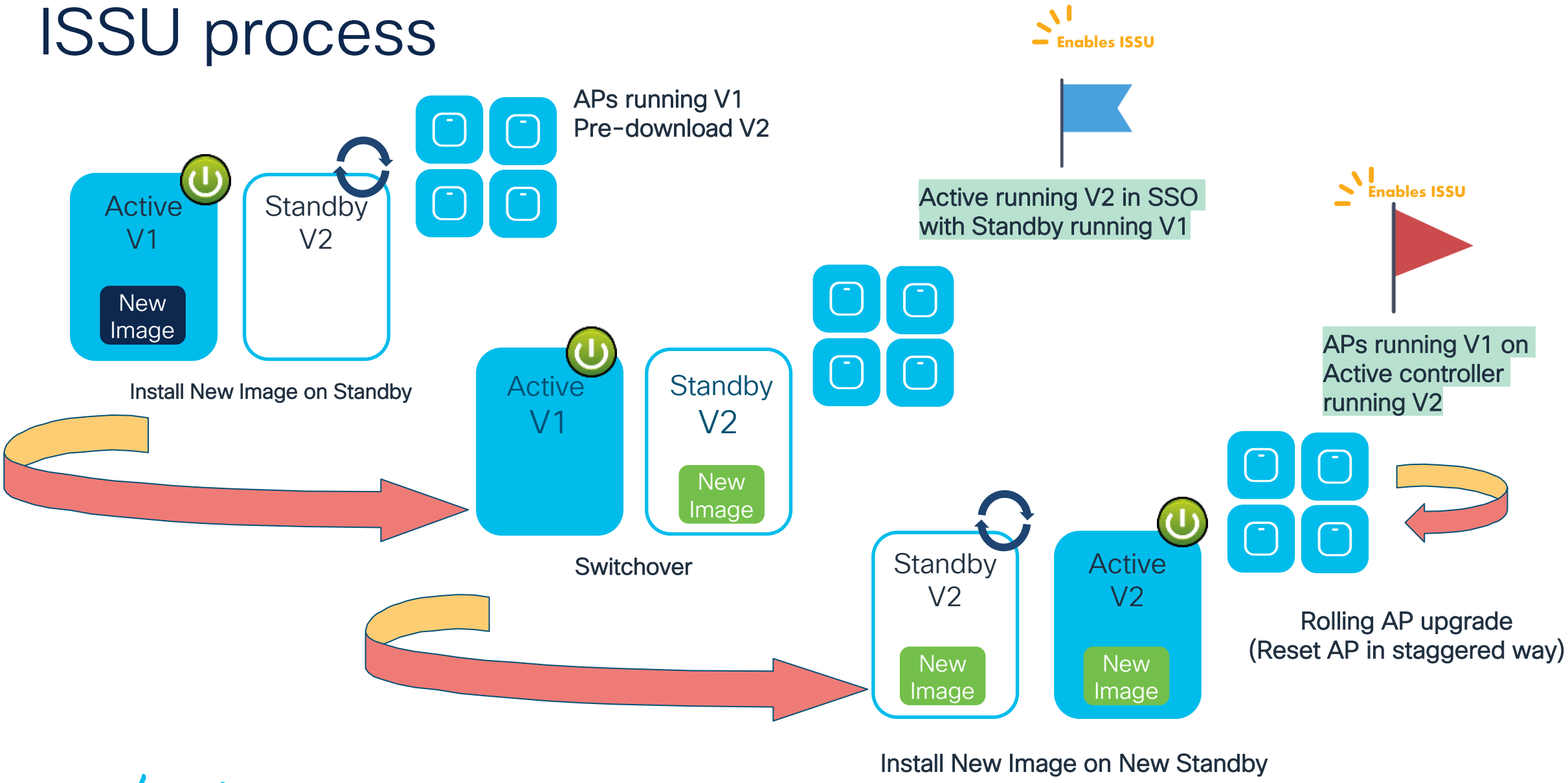
What is ISSU ?

Complete image upgrade from one image to another while traffic forwarding continues

All AP/Client sessions are retained during upgrade process

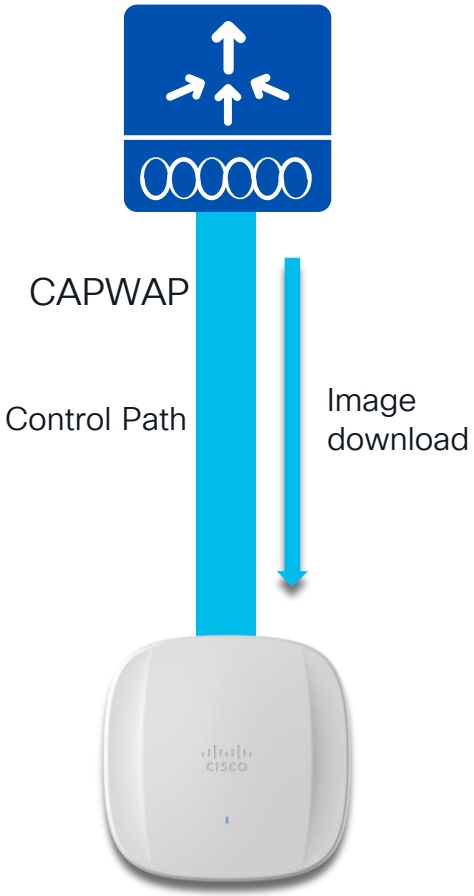
Pre-requisites:
- ✓ Base image is ISSU capable
- ✓ SSO pair in Active-Hot Standby
- ✓ Controllers in INSTALL mode

ISSU process



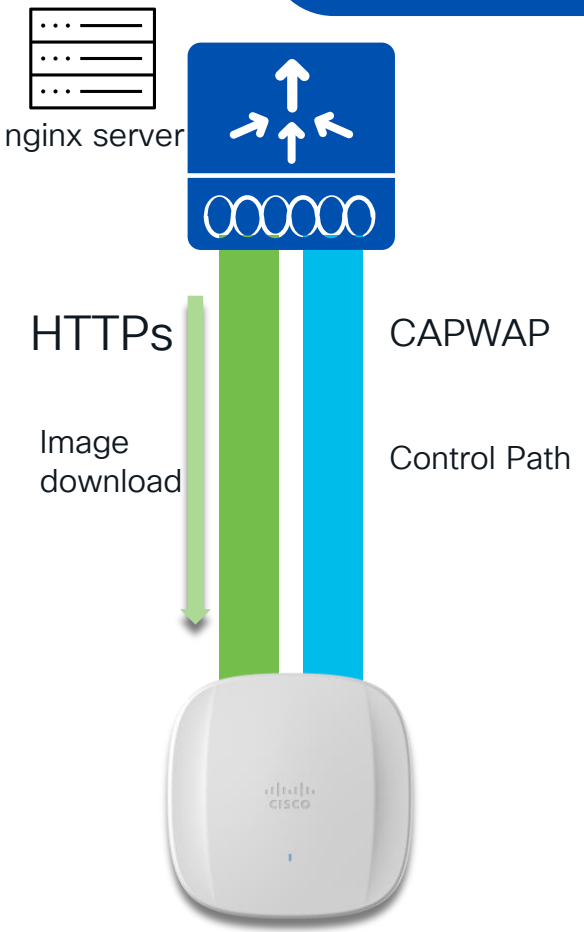
How can I improve AP image download time?

Before IOS XE 17.11.1



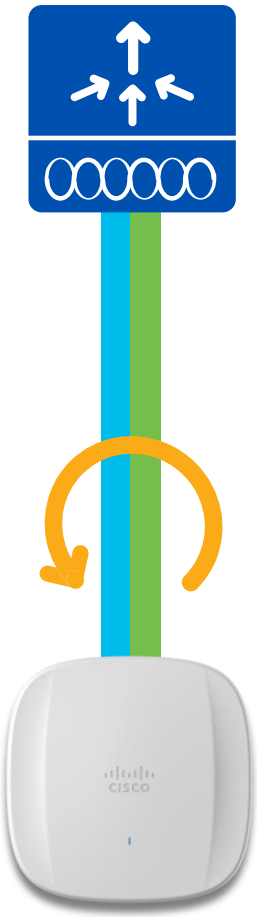
- AP image download happens over CAPWAP Control Path
- Slow by limitation with CAPWAP window size
- Image downloads WNCd process increases CPU work-load

After IOS XE 17.11.1



- AP image download happens over HTTPs
- Fast download speed
- Reduce CPU load and frees up CAPWAP

Fallback to CAPWAP if HTTPs Failure



If any failure happens in image download over http, it will fall back to CAPWAP method to keep the upgrade functionality.

Wireless Controller SMU (Software Maintenance Update)

Controller SMU

Standalone vs Redundant Wireless Controller

	Hot Patch (No Wireless Controller reboot) Auto Install on Standby	Cold Patch Wireless Controller Reboot
Standalone box	No reload of Controller. AP & Client session won't be affected.	Reload controller. AP & Client sessions would be affected.
Redundant box	SMU activation applies patch on Active & Standby. There is no controller reload and there is no impact to AP and Client sessions.	Follows ISSU path and both Standby & Active controller reloaded but there is no impact to AP and Client session. CLI required for ISSU

Per-site & Per-AP Model AP Service Pack

APSP workflow

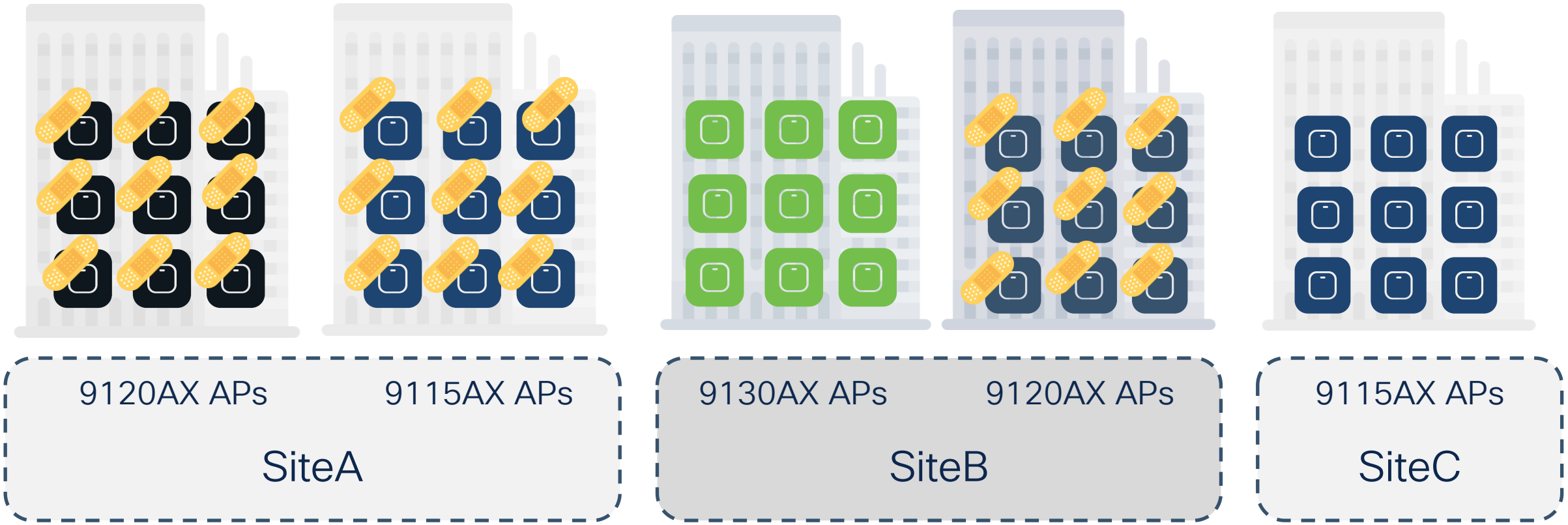
Applying APSP for 9115/9120 APs on per-site and per-model basis

ap image site-filter file APSP1 add SiteA
Install prepare activate
Install activate
Install commit

Apply on Site A in rolling AP fashion

ap image site-filter file APSP1 add Site B
ap image file APSP1 site-filter apply

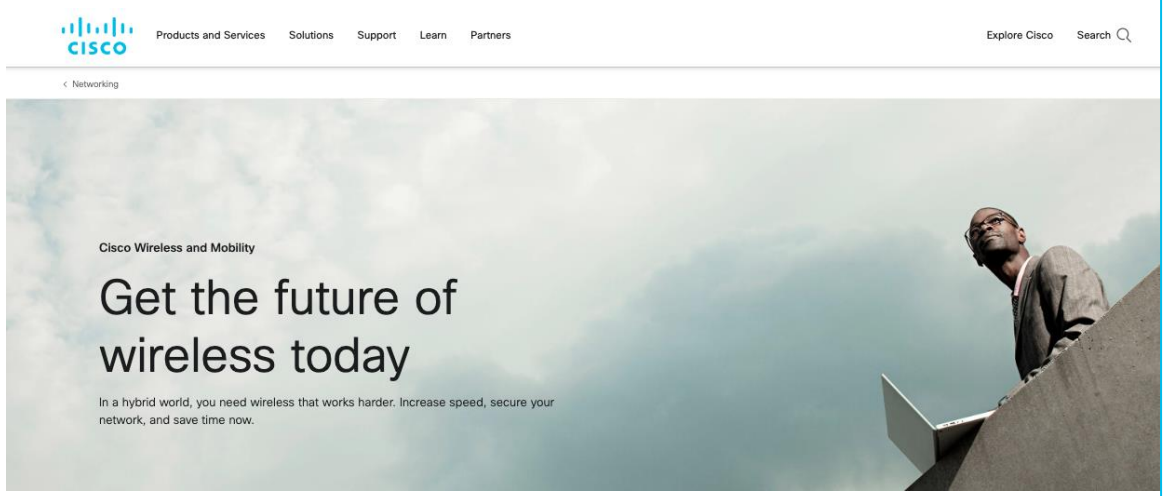
Not applicable for building with 9130AX



More info?

Where can I find more info?

Wireless and Mobility page on CCO:
https://www.cisco.com/c/en/us/products/wireless/index.html



Other links on CCO:

- C9800 Best Practices:
  https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html
- Wireless Migration Tech guide (Partners only):
  https://salesconnect.cisco.com/open.html?c=2afc6956-71cd-4562-aab3-2728d3d48d0f
- C9800 YouTube channel:
  https://www.youtube.com/results?search_query=ciscowlan
- IRCM Development Guide:
  https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller-aireos_ircm_dg.html

Networking

Wi-Fi 6/6E

Learn from experts on wireless topics such as WiFi6 and WiFi6E standards enhancements. You will understand what you need to know about designing for 6GHz, migrating from AireOS to Catalyst 9800 or to Cloud management with Meraki. You will understand how to design your enterprise wireless network using Cisco on-premise, cloud or hybrid portfolio.

START

Monday, February 5 I 8:45 a.m.
TECEWN-2234
Demystify Wi-Fi : because fundamentals matter

Tuesday, February 6 I 11:30 a.m.
BRKEWN-2339
Catalyst 9800 Configuration Best Practices

Tuesday, February 6 I 1:30 p.m.
BRKEWN-1742
7 Ways to Fail - on Wi-Fi 6(E)

Tuesday, February 6 I 2:45 p.m.
BRKEWN-2094
Successfully Configuring Catalyst 9800 Wireless on Your First Shot

Wednesday, February 7 I 8:30 a.m.
BRKEWN-2087
High Density Wi-Fi Design, Deployment, and Optimization

Wednesday, February 7 I 10:30 a.m.
BRKEWN-2024
Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points

Thursday, February 8 I 10:30 a.m.
BRKEWN-1538
Internet of Things on the Next Generation Cisco Catalyst Wireless Wi-Fi 6E Access Points

Thursday, February 8 I 3:00 p.m.
BRKEWN-3413
Advanced RF Tuning for Wi-Fi6E with Catalyst Wireless: Become an Expert, while getting a little help from AI

FINISH

Networking

Wireless Automation & Troubleshooting

Learn from experts on wireless topics such as automation and analytics for enterprise wireless networks, and best practice in troubleshooting wireless networks from speakers who are at the forefront of wireless innovation. You will understand our AI/ML strategy for Cisco Wireless.

START

Monday, February 5 I 2:15 p.m.
TECEWN-3369
TAC stories : WiFi networks that save lives...and your job

Tuesday, February 6 I 8:00 a.m.
BRKEWN-2014
Meraki Wireless AIOps - An Intuitive AI Solution to Optimize Wi-Fi at Scale !

Tuesday, February 6 I 4:45 p.m.
BRKEWN-2029
Cisco Wireless AIOps

Wednesday, February 7 I 4:00 p.m.
BRKEWN-2097
Monitoring Catalyst Wireless with the Meraki Dashboard

Thursday, February 8 I 10:45 a.m.
BRKEWN-2667
Cisco Wireless Supercharged by Cisco Catalyst Center - The Ultimate Guide to Bring Your Wireless Operation to the Next Level

Thursday, February 8 I 1:30 p.m.
BRKEWN-2043
Saving Energy and Money with Your Cisco Wireless Network

Friday, February 9 I 9:00 a.m.
BRKEWN-3628
Troubleshoot Catalyst 9800 Wireless Controllers

Friday, February 9 I 11:00 a.m.
BRKEWN-2399
Meraki Wireless from a Troubleshooter Perspective

FINISH

Friday, February 9 I 11:00 a.m.
BRKEWN-3006
Keep your Catalyst 9800 & AP-COS Wireless Network Healthy, with Wireless Config Analyzer Express and other Advanced Tools

Networking

Wireless Securely Designed Solutions

Learn about design best practices for Cisco wireless solution, including many security optimizations. You will also learn about energy optimizations for Cisco Wireless deployments. Finally you will learn how to enable Smart Workspaces and locations based services that leverage your Cisco Wireless and BLE solution.

START

Monday, February 5 I 8:30 a.m.
TECEWN-2005
Secure, Scalable, Enterprise Wi-Fi Deployment using Meraki Cloud

Tuesday, February 6 I 11:45 a.m.
IBOEWN-2031
The Inner Workings of QoS for Modern Wireless Networks

Tuesday, February 6 I 1:15 p.m.
BRKEWN-2926
Tune your Cisco Wi-Fi designs for the most demanding clients and applications, boosted with applied AI

Tuesday, February 6 I 2:00 p.m.
IBOEWN-2000
Design/Deployment and tuning of Outdoor Wi-Fi & Workgroup Bridges (WGBs)

Tuesday, February 6 I 4:45 p.m.
BRKEWN-2035
Meraki Wireless: Ready for Enterprise

Wednesday, February 7 I 2:15 p.m.
BRKEWN-2042
Cisco Spaces: How to Turn your Wi-Fi Network into Location Based Intelligence

Wednesday, February 7 I 2:15 p.m.
IBOEWN-2349
An Open Discussion on Shaping the Future of Buildings with Cisco Spaces

Thursday, February 8 I 8:30 a.m.
BRKEWN-3004
Understanding Wireless Security and the Implications for Secure Wireless Network Design

Thursday, February 8 I 8:45 a.m.
BRKOPS-2402
Automate the Deployment of a Wireless Network with the Help of Cisco Catalyst Center

Thursday, February 8 I 5:00 p.m.
FINISH
BRKEWN-2037
Open Roaming under the hood

The bridge to possible

Thank you

cisco Live!

cisco Live!

Let's go