Cisco Catalyst 9800 Configuration Best Practices

Ignacio Fité
Technical Marketing Engineer, Cisco Wireless

BRKEWN-2339

Cisco Webex App

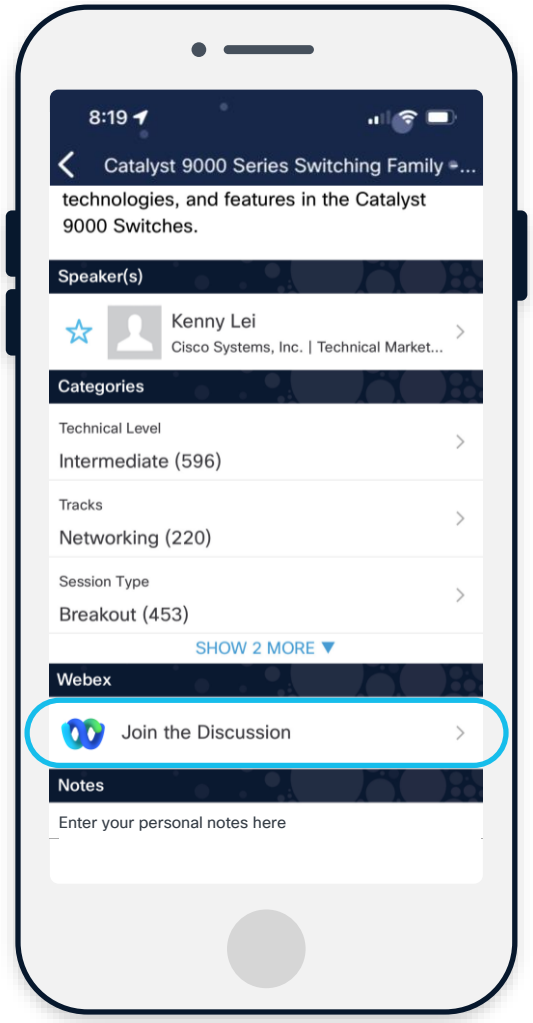
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 13, 2025.



Agenda

Day 0

01 C9800 Design and Deployment

02 Wi-Fi 6E/7 Migration Best Practices

Day 1

03 WLAN Configuration

04 Site Tag and WNCd Load Balancing

05 RF Tag Recommendations

Day 2

06 RF Monitoring

07 Optimization

08 Software Upgrades

Join at slido.com
#BRKEWN-2339

Beginning survey

Cisco Catalyst 9800 Series Configuration Best Practices

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/c9800-best-practices.html

Your speaker today...

Ignacio Fité

Technical Marketing Engineer (previously in sales)

6 years of experience with Cisco solutions

Wireless & Network Management Focus

What’s NOT covered in this session

- Catalyst Center
- Cloud Managed – Config Source: Device
- Troubleshooting of Cisco Catalyst 9800 Controllers
- RF Tips
- High density deployments

BRKEWN-2029, BRKEWN-2048, BRKEWN-2087, BRKEWN-2306,
BRKEWN-3413, BRKEWN-3628, BRKEWN-3002, [...]

For your reference

- There are slides in your PDF that will not be presented, or quickly presented.
- They are valuable, but included only “For your reference”.

For your reference

Agenda

Day 0

01 C9800 Design and Deployment

02 Wi-Fi 6E/7 Migration Best Practices

Day 1

03 WLAN Configuration

04 Site Tag and WNCd Load Balancing

05 RF Tag Recommendations

Day 2

06 RF Monitoring

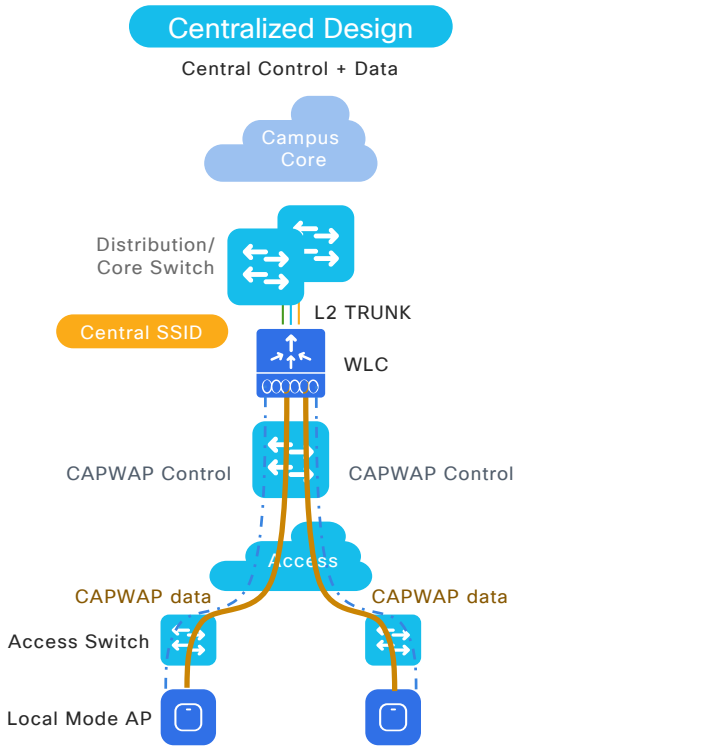
07 Optimization

08 Software Upgrades

Day 0

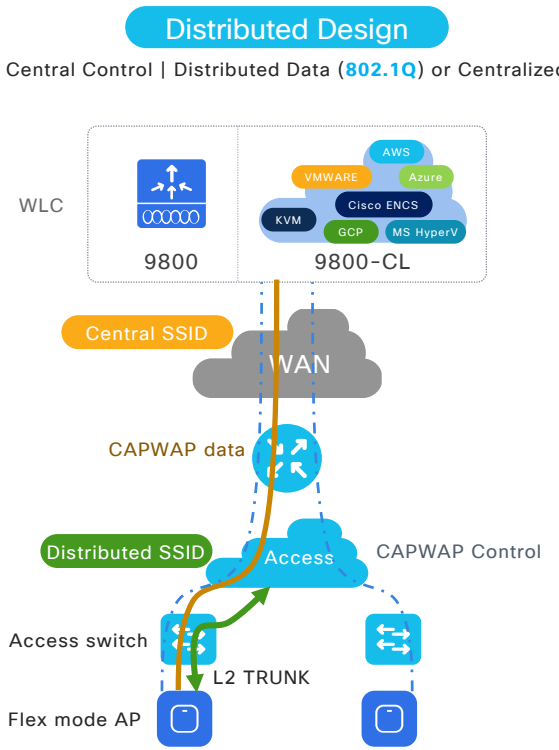
Cisco Catalyst 9800 On-Prem Deployment

Wireless Deployment Options



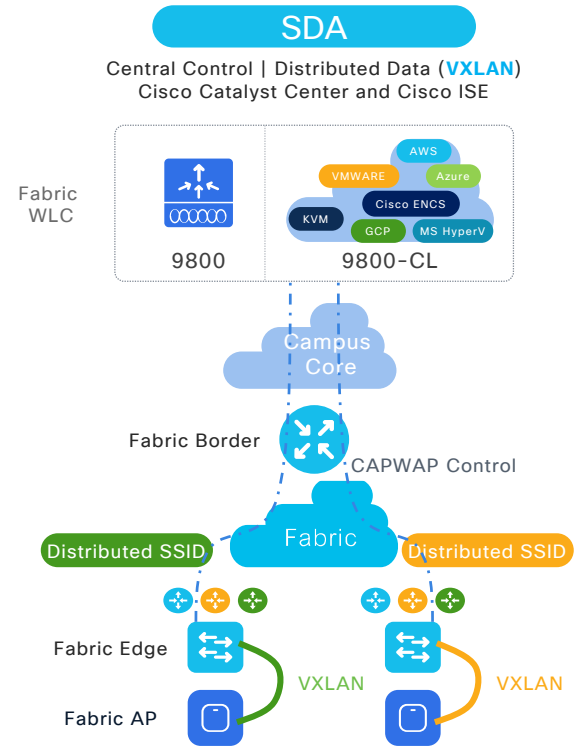
Local mode

- 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 CW9800M
3000 APs, 32,000 clients
50 Gbps

Cisco Catalyst CW9800H1 / CW9800H2
6000 APs, 64,000 clients,
100 Gbps

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

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

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

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
[4] End of Sale announced for December 31, 2025

What Deployment Mode to Choose?

For your reference

Campus / Enterprise

Size	WLC	Deployment Mode
Large	C9800-80, CW9800H1, CW9800H2	Local
Medium	C9800-40, CW9800M, C9800/CL	Local
Small	C9800-L, C9800-CL	Local

Branch or Distributed Enterprise

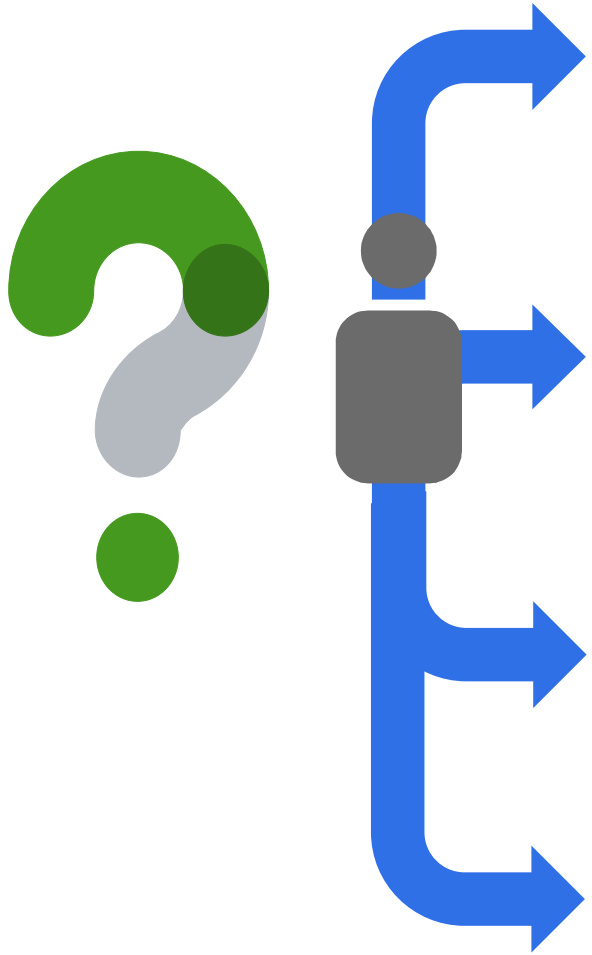
Size	WLC	Deployment Mode
Large	C9800-80, CW9800H1, CW9800H2, C9800-CL	FlexConnect, IaaS
	C9800-L, C9800-CL	Local
Medium	C9800-40, CW9800M, C9800-CL	FlexConnect, IaaS
Small	EWC[1], C9800-L, C9800-CL	FlexConnect, IaaS

[1] Embedded Wireless Controller in switch with SD-Access only.

Catalyst 9800 Recommended releases

What is the recommended release*?

no more “gold star” very soon



17.9.x:

- This release no longer receives software maintenance
- **17.9.7** was released in March 2025, recommended release for this train
- From 17.9.3, this train includes the code for **W1 APs** to ease the migration to C9800 & Wi-Fi 6E. **W1 APs** are **no longer supported**.
- **Recommended to upgrade to 17.12.x release train**

Move to 17.12.x:

- 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.)
- This train includes the code for **W1 APs** to ease the migration to C9800 & Wi-Fi 6E. **W1 APs** are **no longer supported**
- **17.12.5 is recommended gold star release for all deployments**

Move to 17.15.x:

- Adds support for 9172I, 9176I/D1 and 9178I
- **17.15.3 is the recommended release**

Will be gold star very soon, pending SMU for CSCwo80904

Move to 17.17.x:

- This is **not a long-lived maintenance release train**, avoid unless it is strictly necessary.
- Only if you need support for 9172H, new countries supporting 6GHz and the new features in this release (AP Certificate Auto-Renewal, AFC in the US and Canada)

* Always check TAC recommendations: https://cs.co/recommendediosxe
SMU = Software Maintenance Upgrade

Cisco Recommended Software Matrix*

For your reference

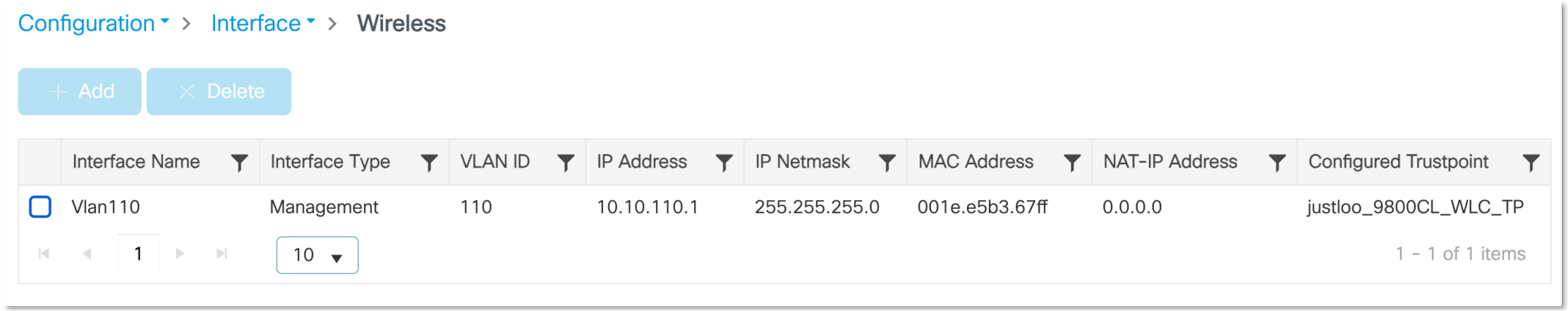
IOS-XE	AP	IRCM with Gen 1 AireOS	IRCM with Gen 2 AireOS	Catalyst Center	Prime	CMX	ISE
17.9.7	802.11ax 802.11ac W2	8.5.182.104	8.10.196.0	Matrix	3.10.2	11.1.0-21	3.3 3.2 3.1 [...]
17.12.5	802.11ax (Wi-Fi 6/6E) 802.11ac W1 and W2	8.5.182.104	8.10.196.0	Matrix	3.10.5	11.1.0-21	3.4 3.3 3.2 3.1 [...]
17.15.3	802.11be (Wi-Fi 7) 802.11ax (Wi-Fi 6/6E) 802.11ac W1 and W2	8.5.182.104	8.10.196.0	Matrix	3.10.6	11.1.0-21	3.4 3.3 3.2 3.1 [...]

(*) 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

Controller Settings

Wireless Management Interface

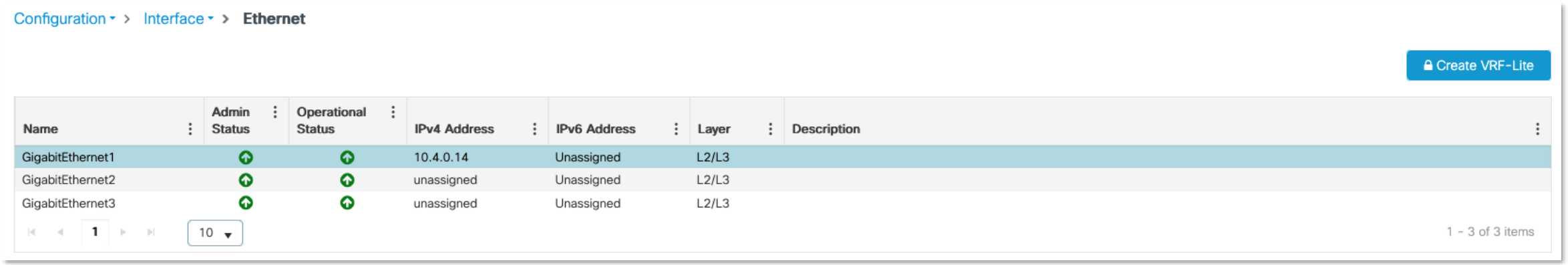
- A Single Layer 3 interface used for terminating CAPWAP traffic to APs and source any other management traffic
- For all C9800 appliances except C9800-CL in Public Cloud:
  - Configure as SVI
  - Tag with a VLAN

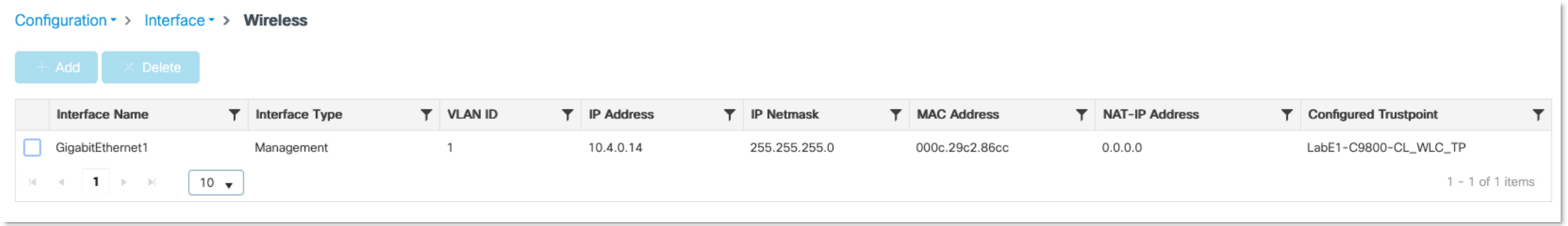


CAPWAP = Control and Provisioning of Wireless Access Points

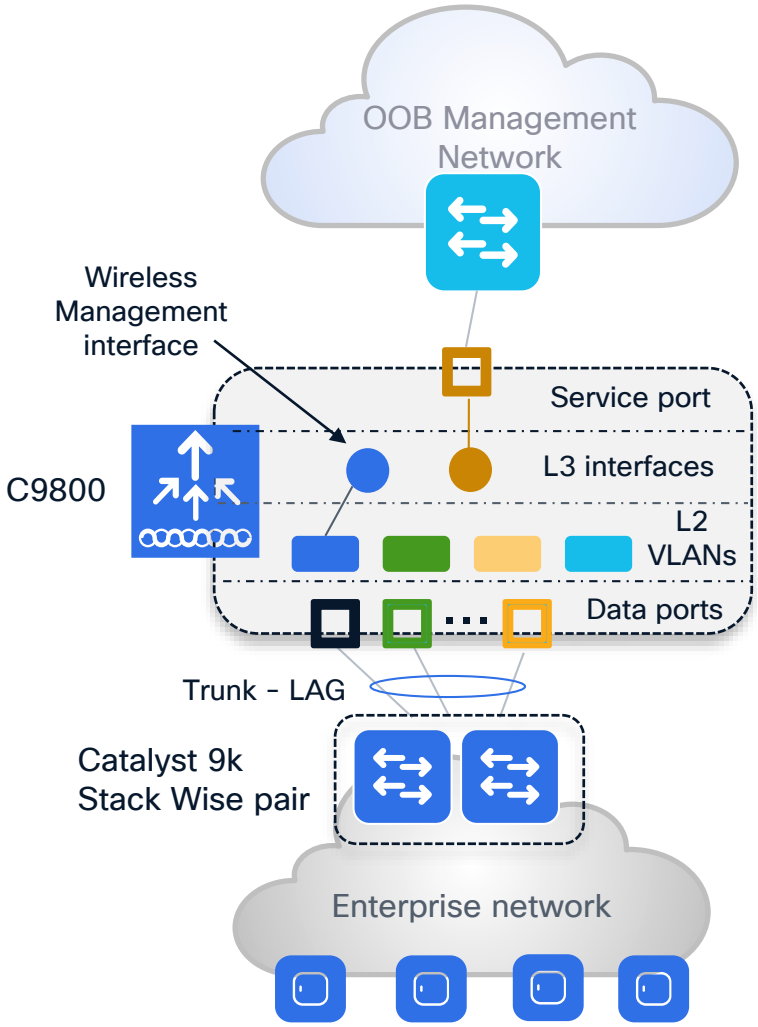
Wireless Management Interface

- For C9800-CL in Public Cloud:
  - Configure as L3 routed port





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**").
- For centrally switched SSID, it is **mandatory to configure a client L2 VLAN**

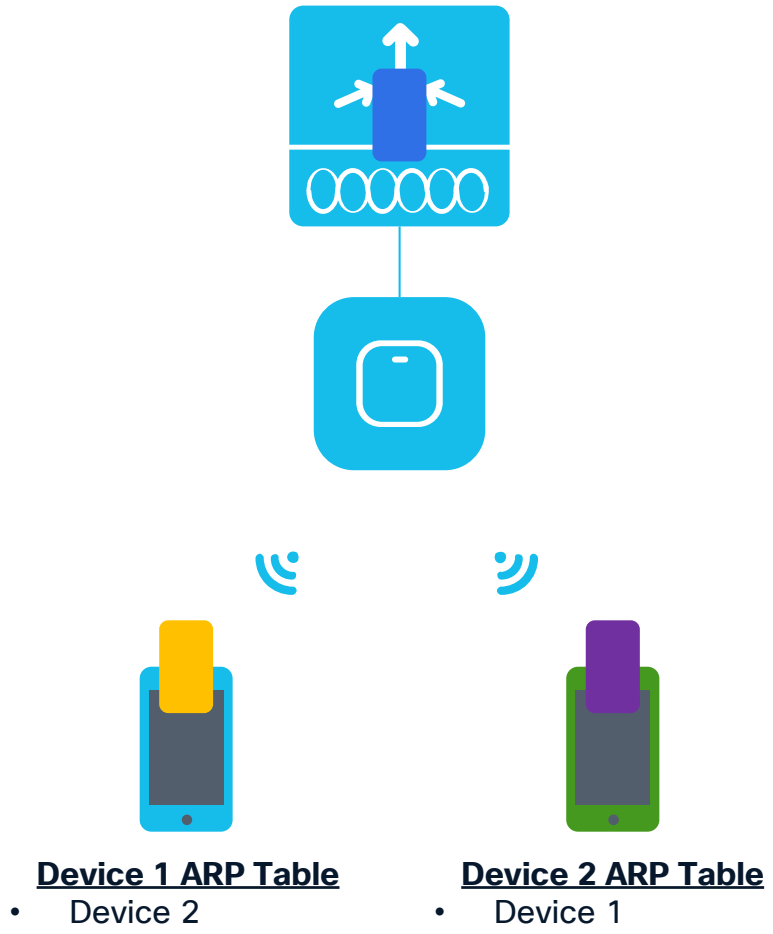
Best practices:

- 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

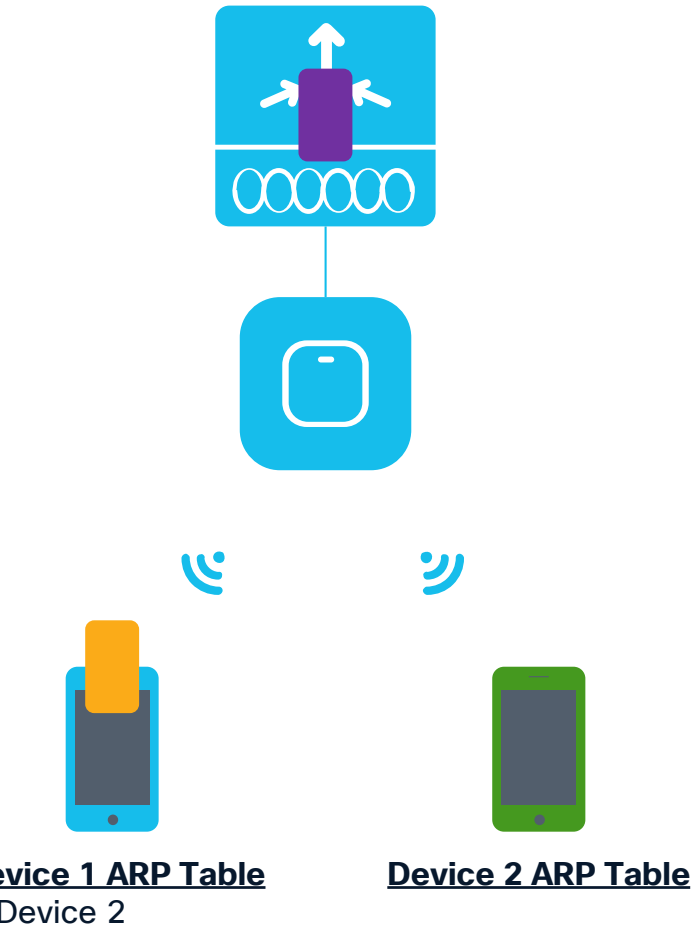
- **Default Behavior**
  - C9800 forwards ARP traffic by changing destination MAC from broadcast to unicast



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
```



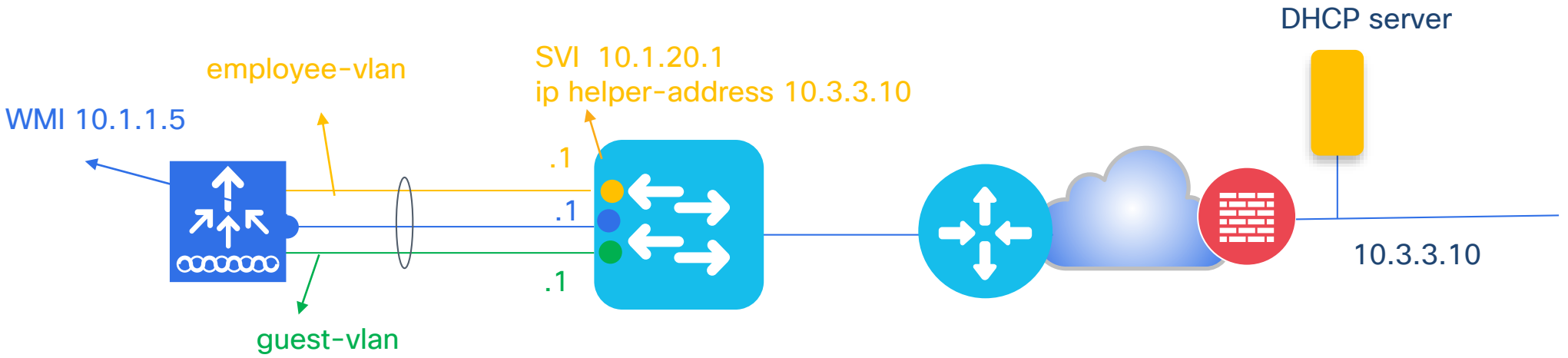
Device 1 ARP Table

- Device 2

Device 2 ARP Table

Best Practice – DHCP proxy/relay

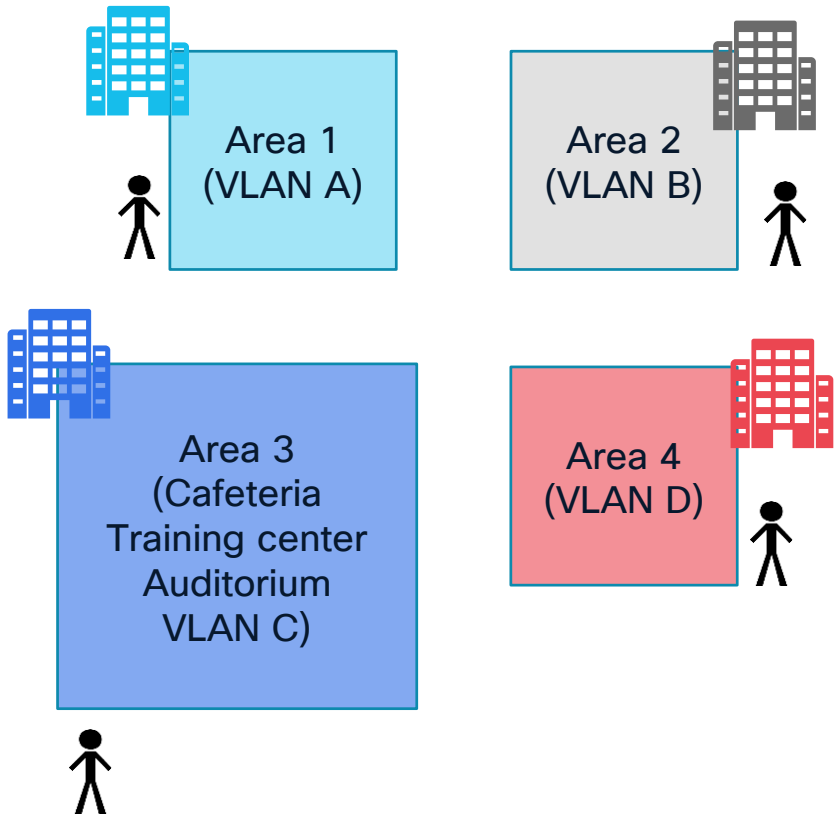
- **DHCP Proxy mode:**
  - In AireOS, enabling DHCP Proxy for wireless clients is a best practice
  - In C9800 DHCP proxy is **not needed** as IOS-XE has embedded security features like DHCP snooping, ARP inspection, etc. that don't require a L3 interface
- **DHCP relay or bridging mode?**
  - DHCP bridging 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

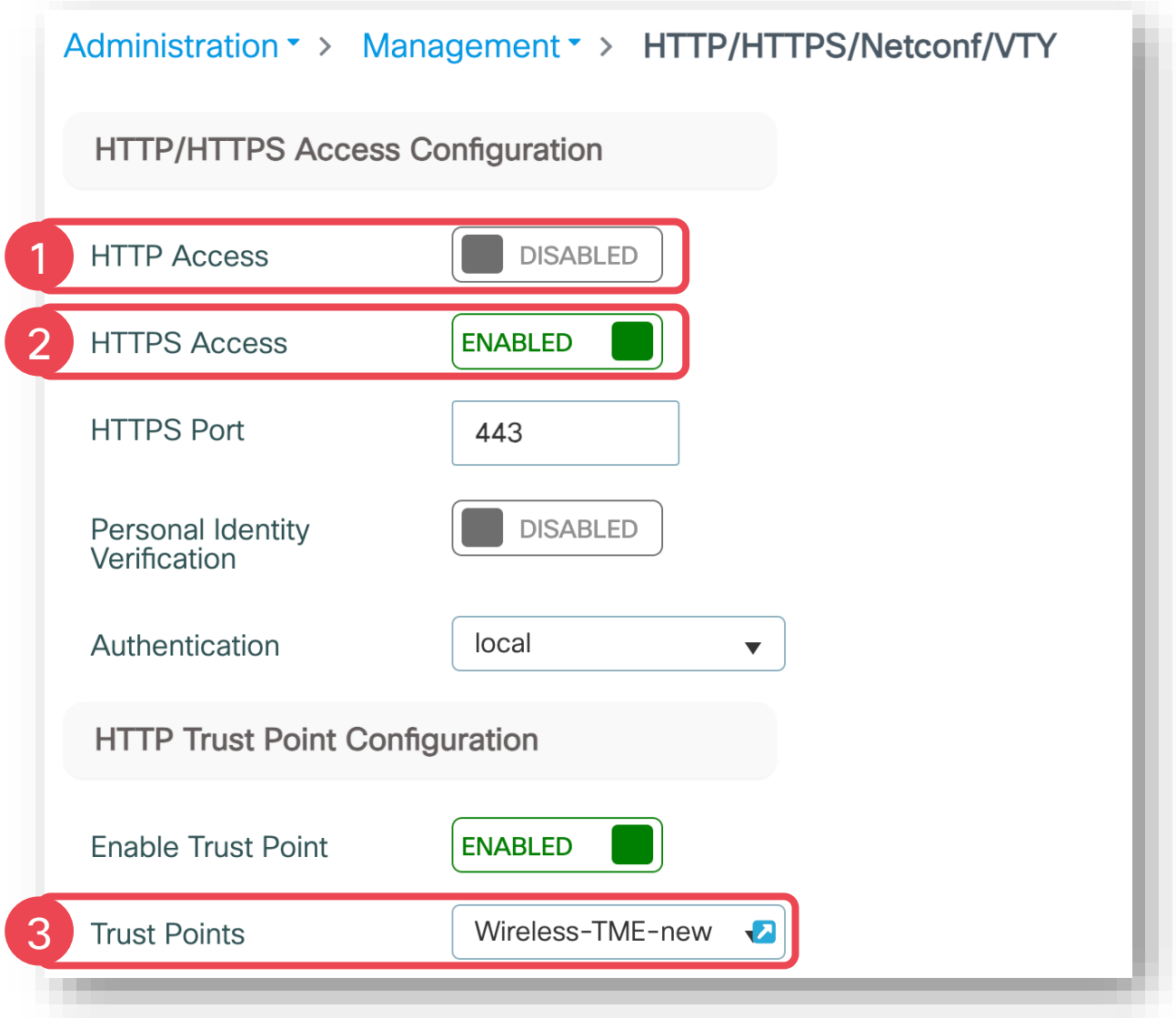
DHCP Scope and Lease design considerations



- Size your **DHCP scope** considering all the possible devices that could join that area to prevent DHCP scope starvation: stationary but also roaming devices from other areas
- **DHCP Lease** is very important to reduce the load on DHCP server, prevent starvation and security issues.
- The **recommendation** for DHCP lease: align it to the the average dwell time in that environment. For example:
  - Set it to 12 hours for normal office deployments
  - Set it to 8 hours for Universities
  - Set it to 1 hour for Retailers
  - Set it very low (e.g., 30 mins) for security reasons (reduced unauthorized time) but there is an impact on the DHCP server. Also consider Random MAC > keep DHCP lease lower to avoid starvation

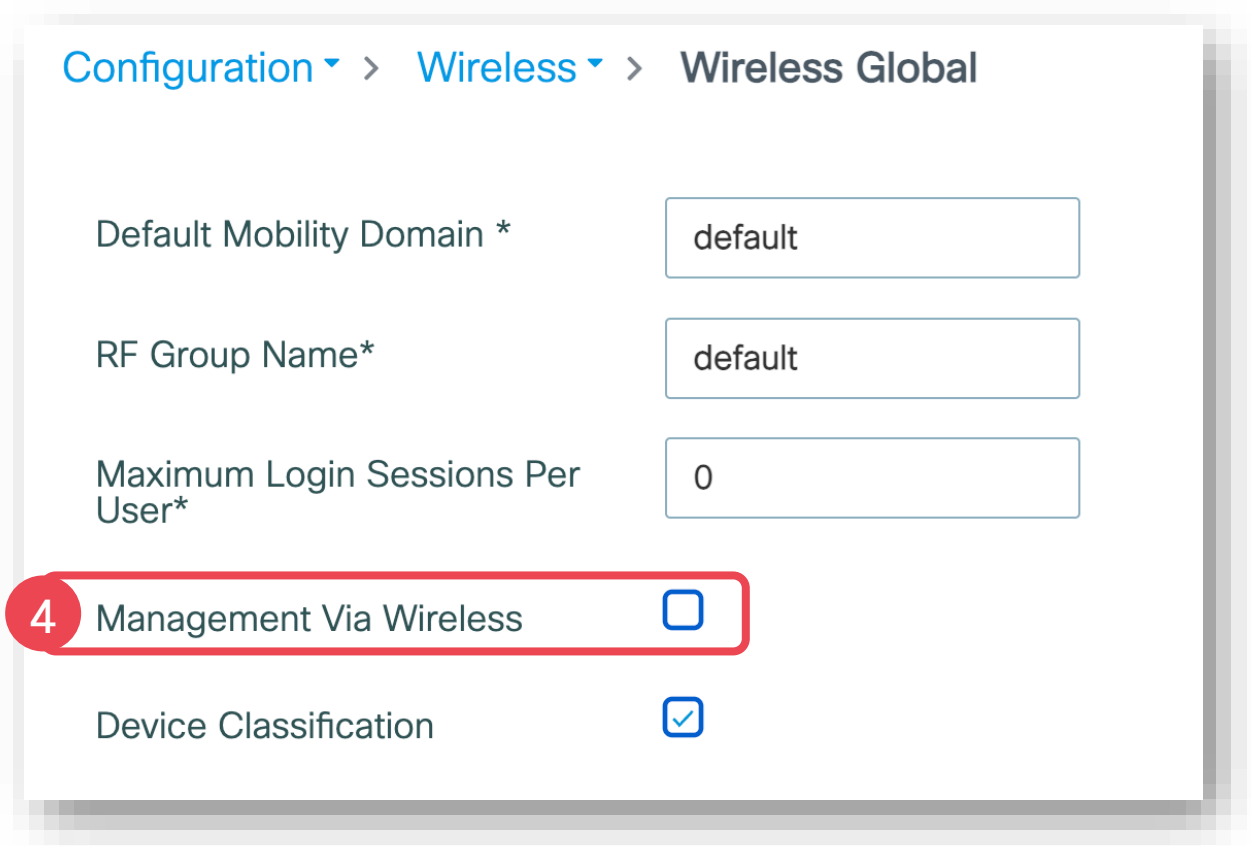
Enable Secure Web Management Access

1. Disable HTTP
2. Enable HTTPs
3. Manually configure trustpoint



Enable Secure Web Management Access

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



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/ CW9178

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

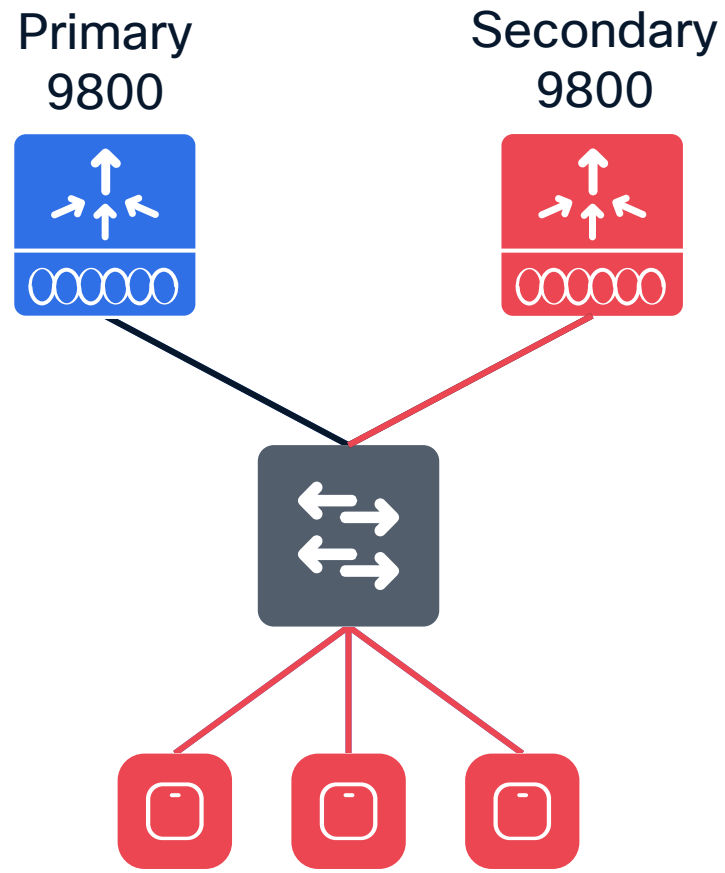
Software Image Upgrades
Wireless controller image upgrades

- 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

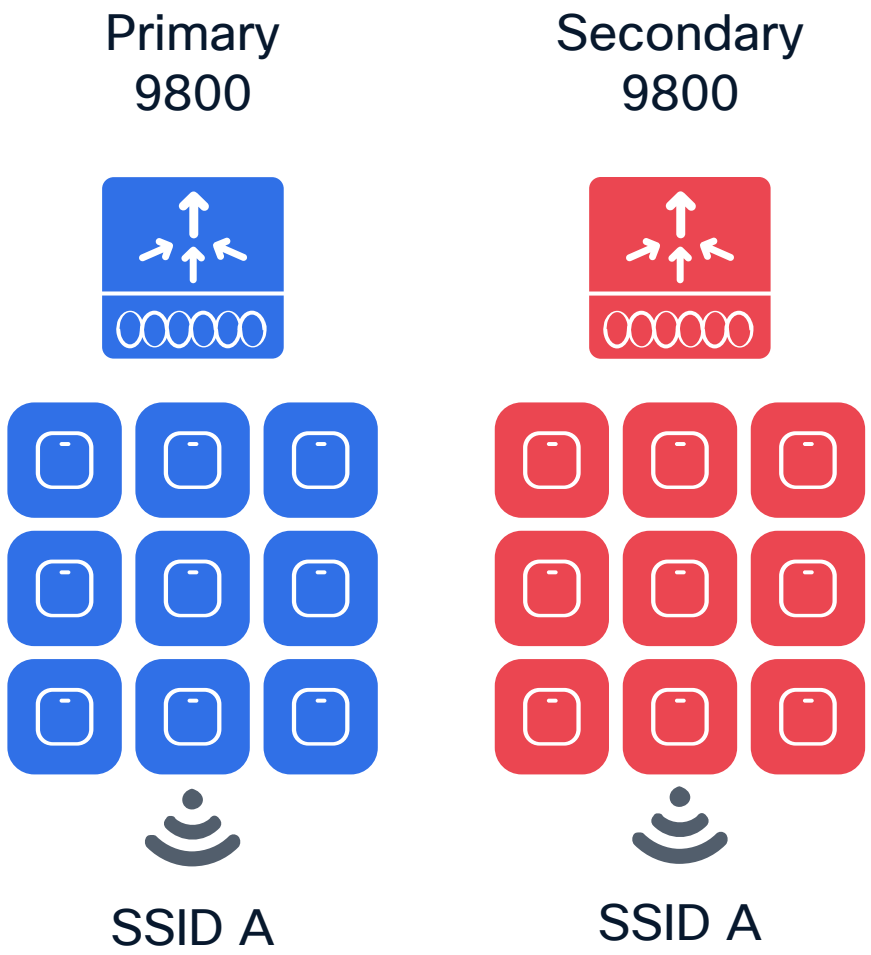
N+1 best practices

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

N+1 best practices: Saving AP to Tag Mappings



Define tag mappings via static mappings or REGEX based on AP name / location

Save tag mapping to the AP and define tags on secondary controller

Pre-17.6.1: Manually write the tags to each AP

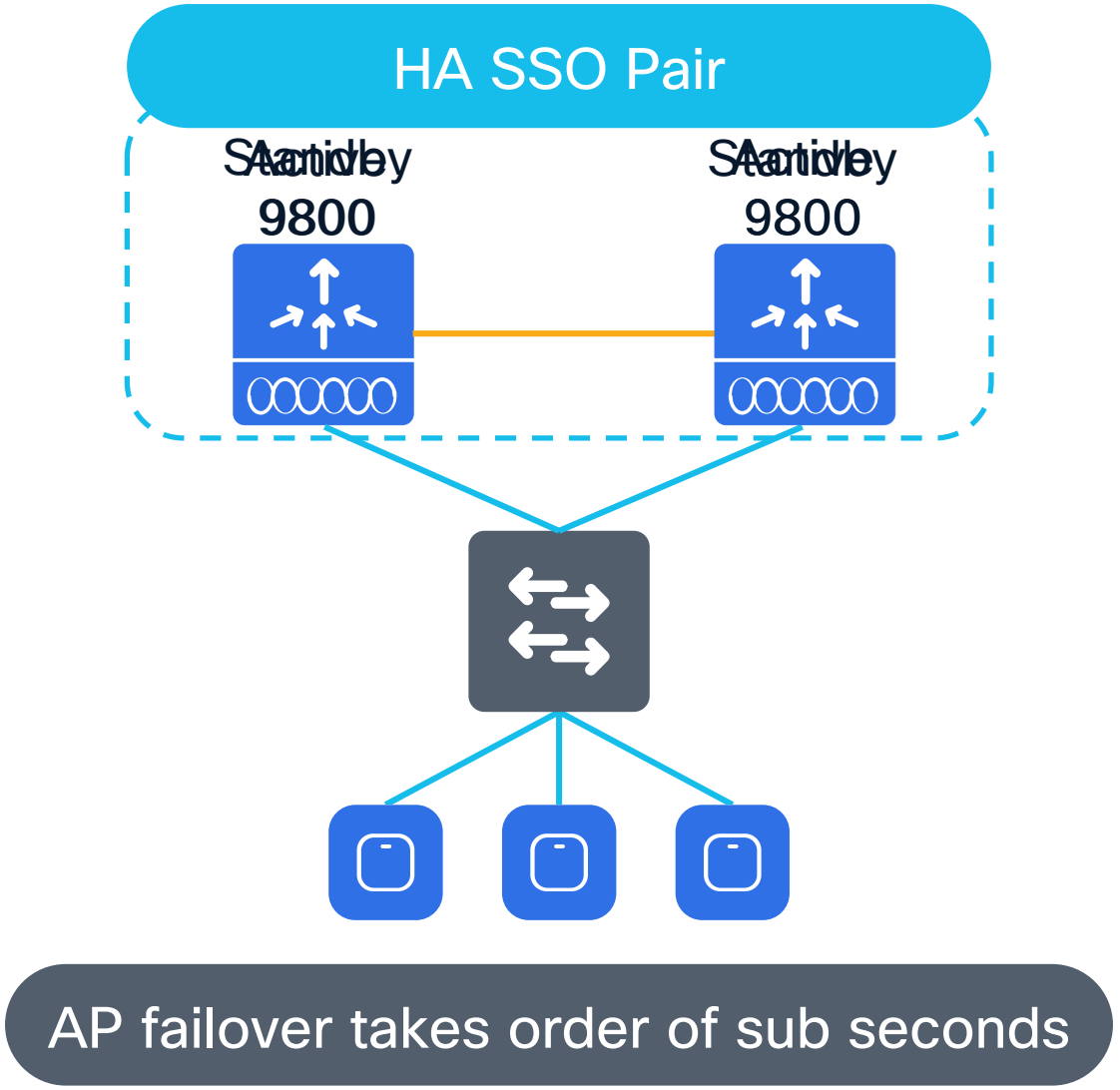
17.6.1 and Later: Automatically write tags to the APs via AP Tag Persistency*

* Not enabled by default, how to enable.

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



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**

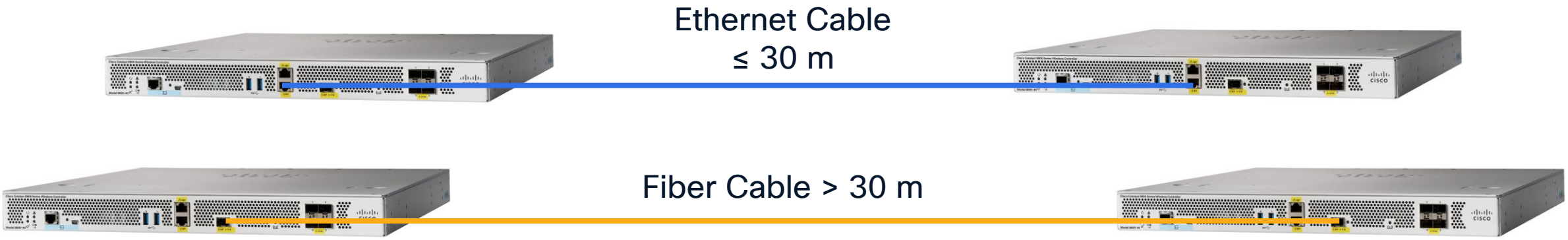
Configurations

- 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

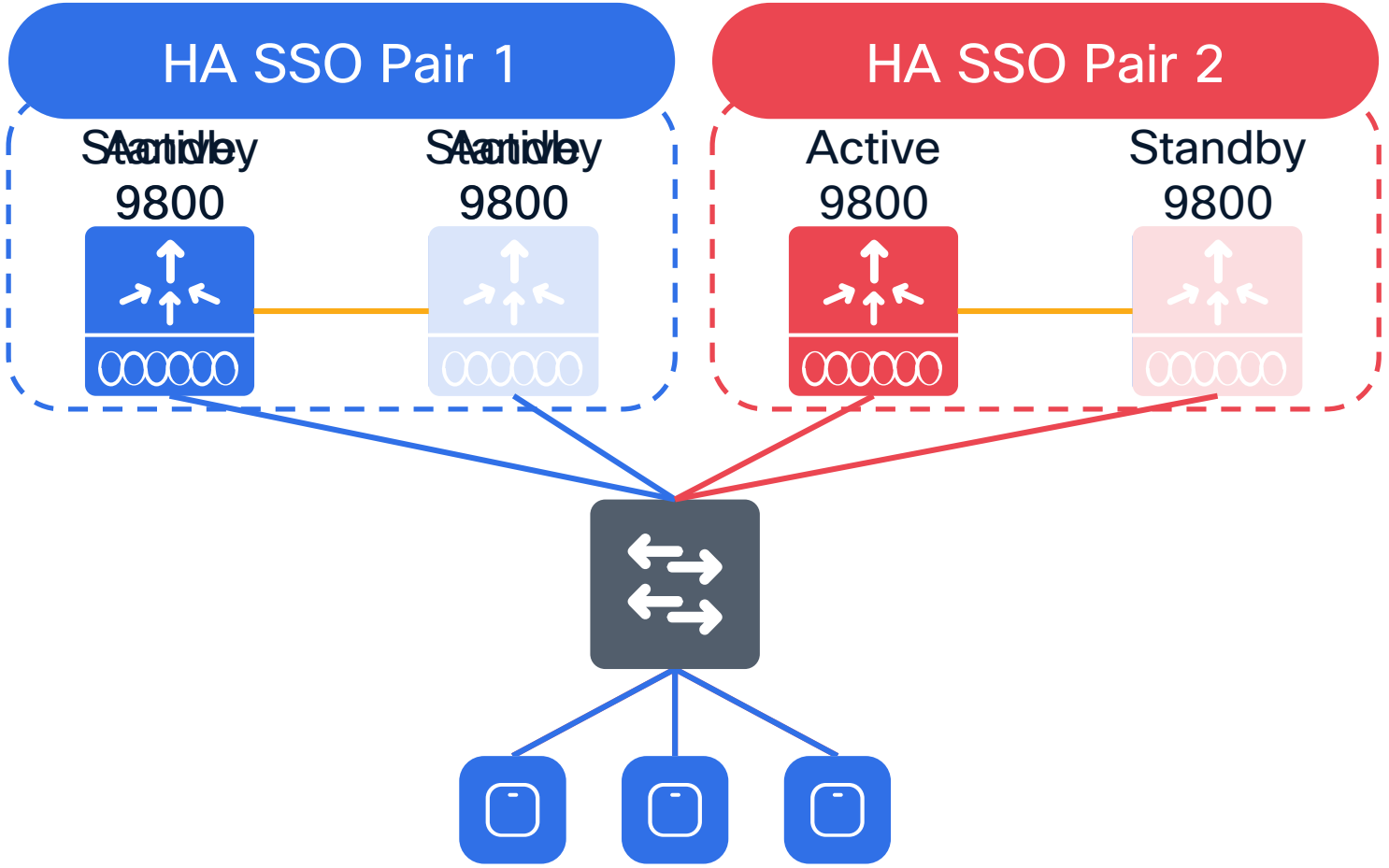
Back-to-Back Redundancy Port Connections

- For back-to-back RP connections on C9800-40/80 & CW9800M/H1/H2:
  - 30 meters or less (~100 feet): Use copper cable
  - Greater than 30 meters: Use fiber cable

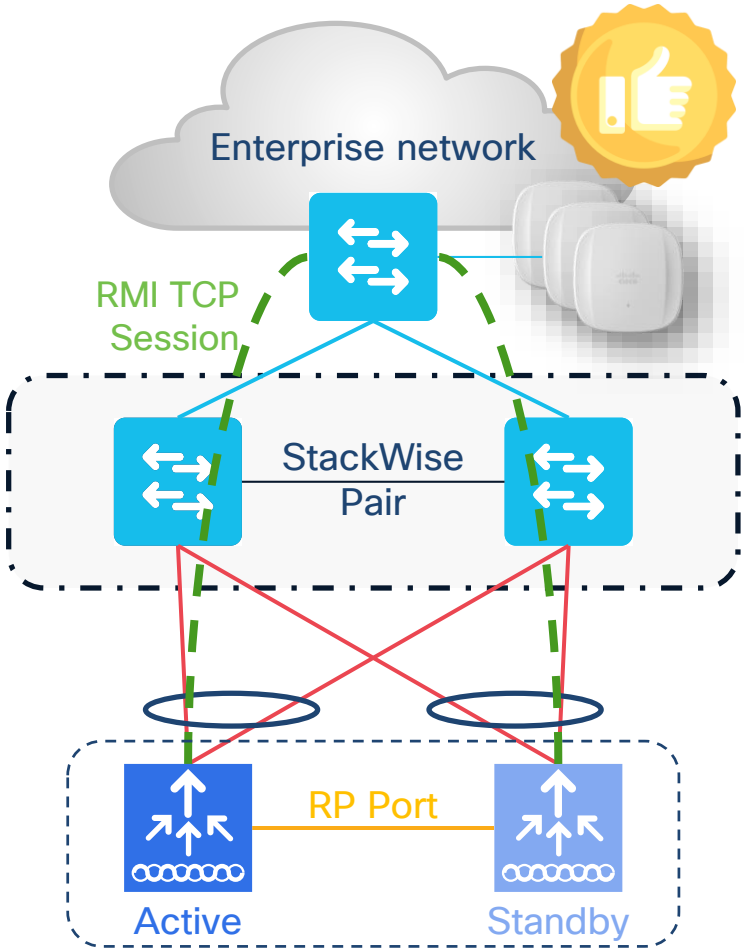


Redundancy with HA SSO and N+1

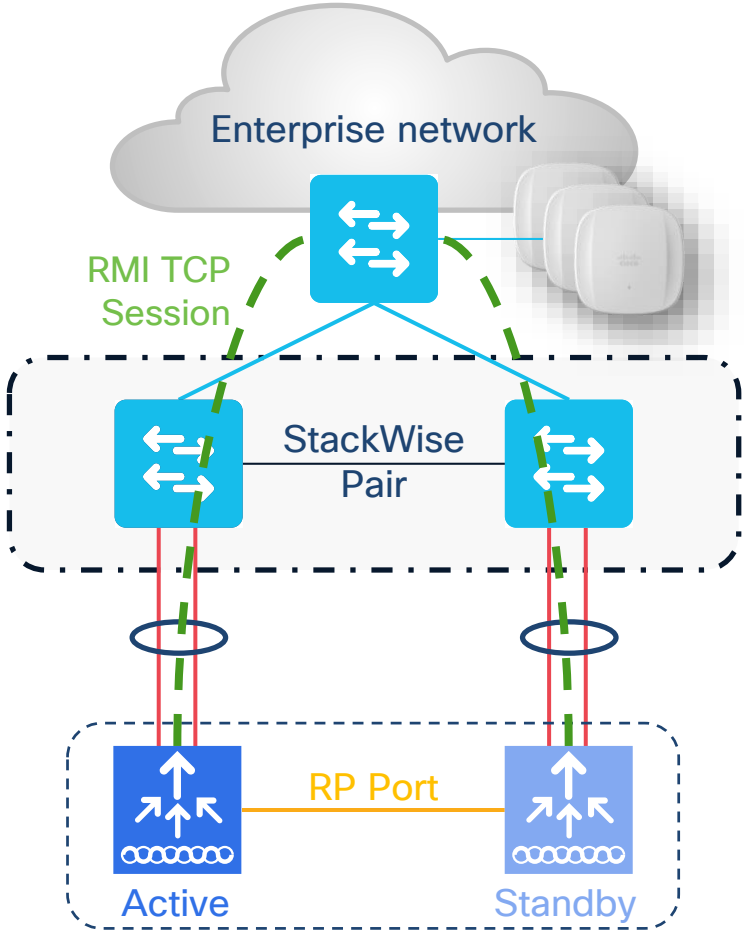
- Highest redundancy model
- Take advantage of sub-second failover
- Redundancy in the event SSO New-Active fails before the Old-Active is recovered
- Hitless upgrades for non-ISSU releases



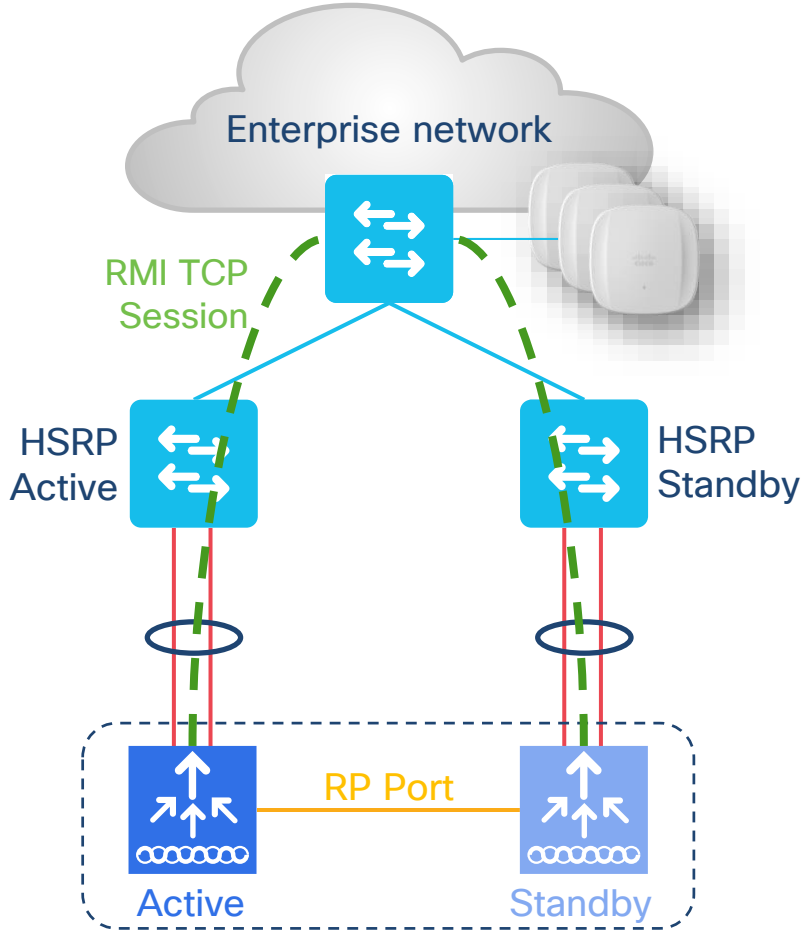
Connecting WLCs to Rest of Network



StackWise Pair with Split links



StackWise Pair without Split links

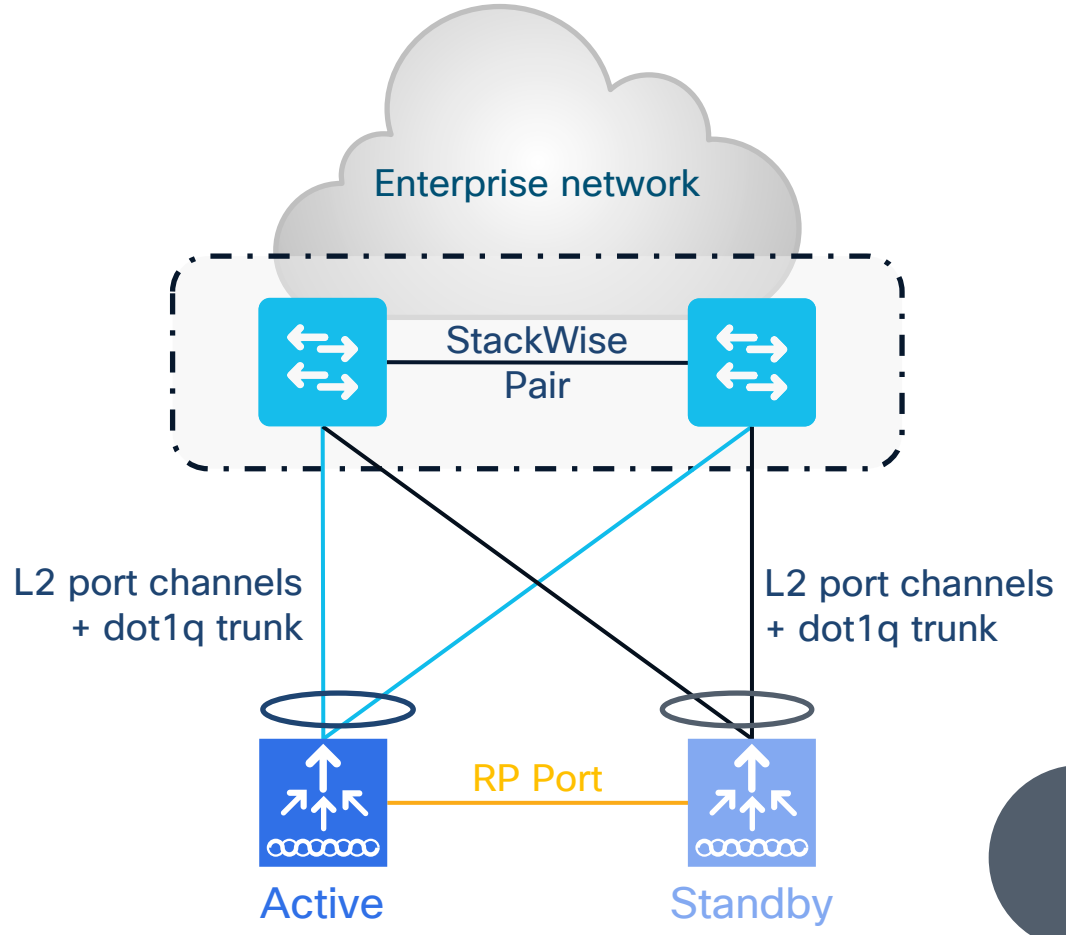


HSRP

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

StackWise Pair with split links

SSO HA Pair



Recommended

- For HA SSO, 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 (optionally L2 network in between)

Wi-Fi 6E/7: what's the impact on migration?

Complete Wi-Fi 6E & 7 portfolio

CleanAir® **Pro**
in all APs

9172 I/H

9176 I/D

9178

9179F

9162

9164

9166 I/D

9136

MR57

9163E

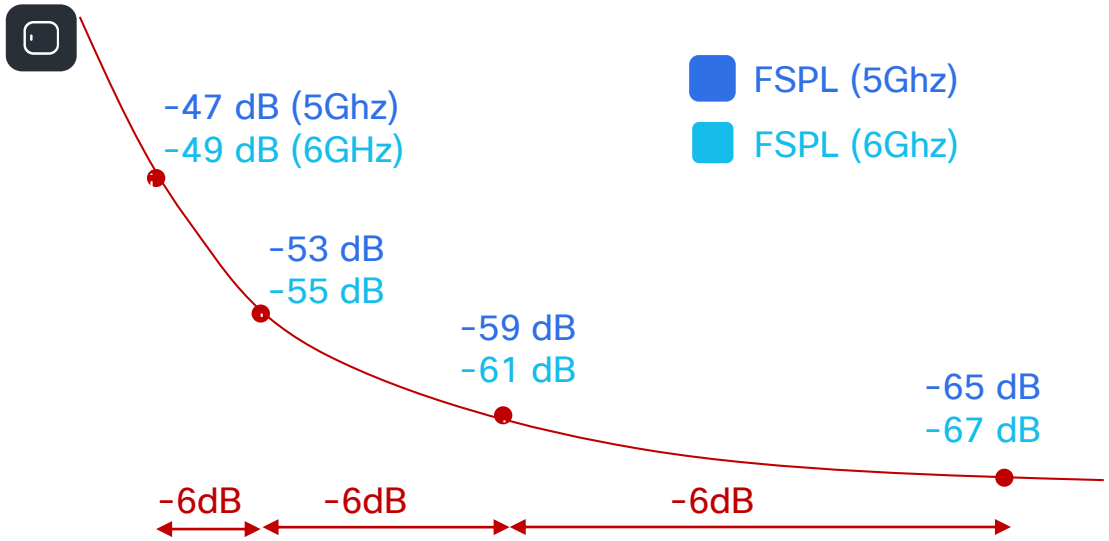
Indoor | Hybrid | Outdoor

Management mode can be changed

6GHz RF Design

What you need to consider?

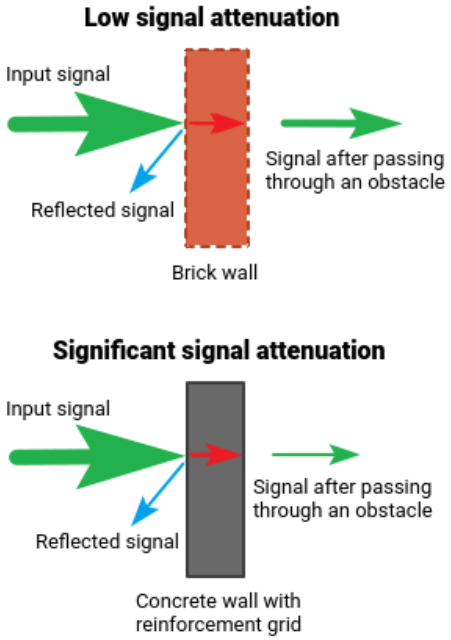
- Path Loss (FSPL) – Path loss in the first meter is on average 2dB higher at 6GHz vs. 5GHz. After that, the 6 dB rule applies: doubling the distance results in a 6 dB loss, regardless of the frequency
- Cell Size – At 6 GHz @ same power level cell is smaller vs. cell size at 5 GHz



FSPL = Free Space Path Loss: https://en.wikipedia.org/wiki/Free-space_path_loss

What you need to consider?

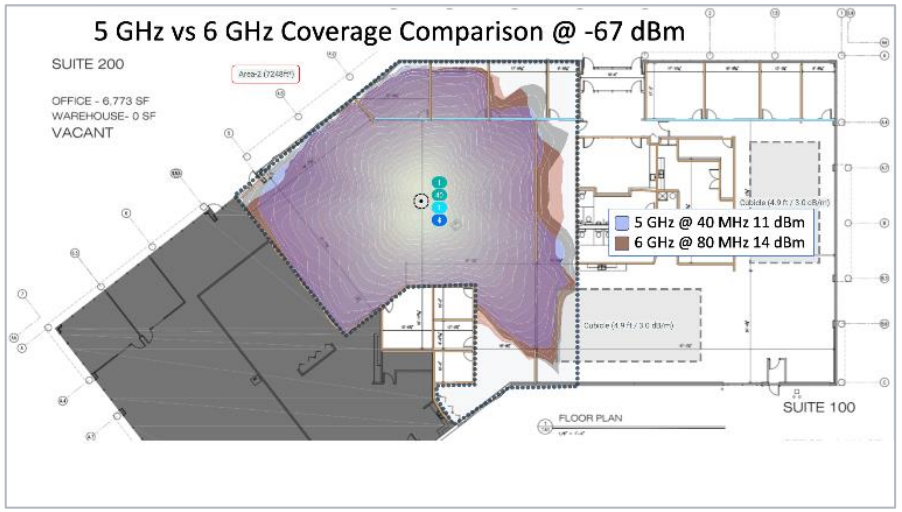
- Path Loss (FSPL) – Path loss in the first meter is on average 2dB higher at 6GHz vs. 5GHz. After that, the 6 dB rule applies: doubling the distance results in a 6 dB loss, regardless of the frequency
- Cell Size – At 6 GHz @ same power level cell is smaller vs. cell size at 5 GHz
- Absorption/Reflectance – 6 GHz will be attenuated more through wall or other surfaces
- Noise floor at 6 GHz is much lower than 5 GHz, at least for some time ☺
- Downstream (from AP to client) / Upstream (from client to AP): expecting upstream to be your cell limiting factor
- Coverage type: today 6GHz is indoor only unless US/Canada with AFC



FSPL = Free Space Path Loss: https://en.wikipedia.org/wiki/Free-space_path_loss
Image taken from https://help.keenetic.com/hc/en-us/articles/213968869-Wi-Fi-signal-attenuation-coefficients-when-passing-through-different-materials

RF Design considerations

- AP antenna patterns at 6GHz are similar to 5GHz
- AP coverage between 5GHz and 6GHz will be similar, especially in open spaces BUT it does require to compensate with power > 3dB higher in 6GHz



5GHz @40 MHz 11dBm

6GHz @80 MHz 14 dBm

- With brick walls, elevator and other environments, you would probably need to measure and add few APs

RF Design considerations

- 1:1 AP replacement for Existing Deployments:
  - Cell size 140 – 190 m^2 with 3-4 m ceiling height
  - If power level average is 3-4 > 1:1 AP replacement is possible > similar coverage level between 5 and 6 GHz
  - If the power level is 1-2, then you may need to add APs, around 10 to 20% additional access points

- For new deployments, a site survey is recommended: leverage the new site survey mode on Cisco Wi-Fi 6E/7 APs
- Mixing Wi-Fi 6E/7 APs with existing APs in the same area is not recommended > avoid “salt & pepper” design if you can

Cisco Wireless AP: Site Survey mode configuration steps

1. Change AP to site survey mode > exec command “ap site-survey”

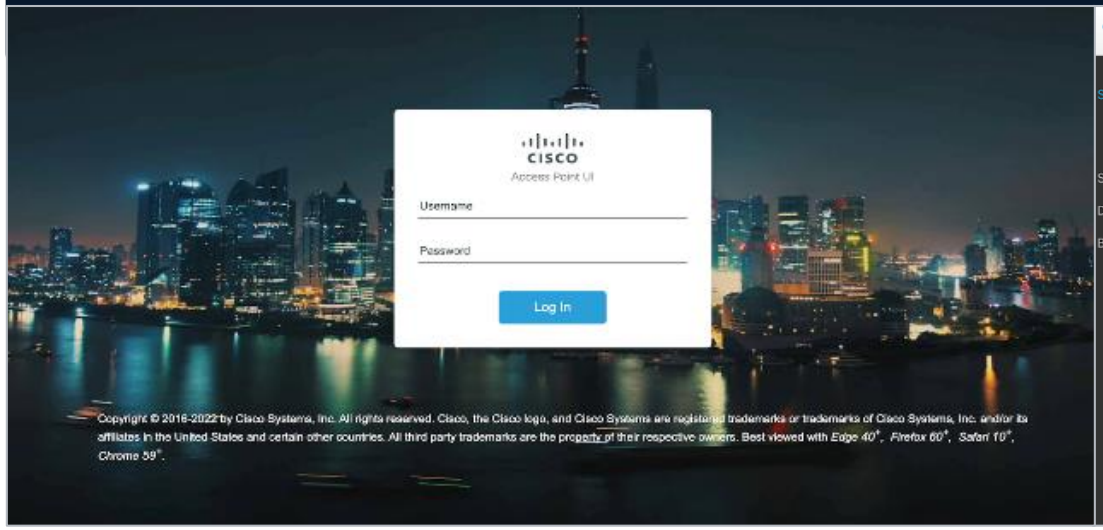
```
CW9176#ap ?
  capwap       Switch to CAPWAP AP type
  site-survey  Switch to Site Survey AP type
```

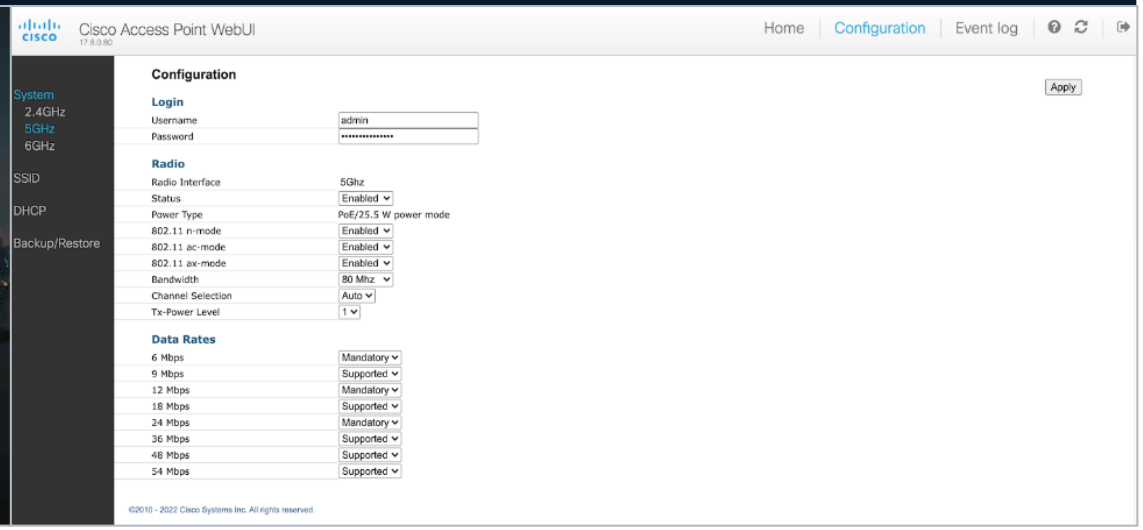
2. After bootup, the AP is automatically assigned a static IP of 10.0.23.1. CLI prompt changes

```
site-survey-AP#
```

(default credentials Cisco/Cisco)

3. AP will start broadcasting the C9176_site_survey* SSID with open authentication security
4. Connect your wireless client with the C9176_site_survey* SSID and it’ll receive a DHCP IP from 10.0.23.0/24.
5. Access the Catalyst Site Survey WebUI via 10.0.23.1 (*default credentials admin/admin*)



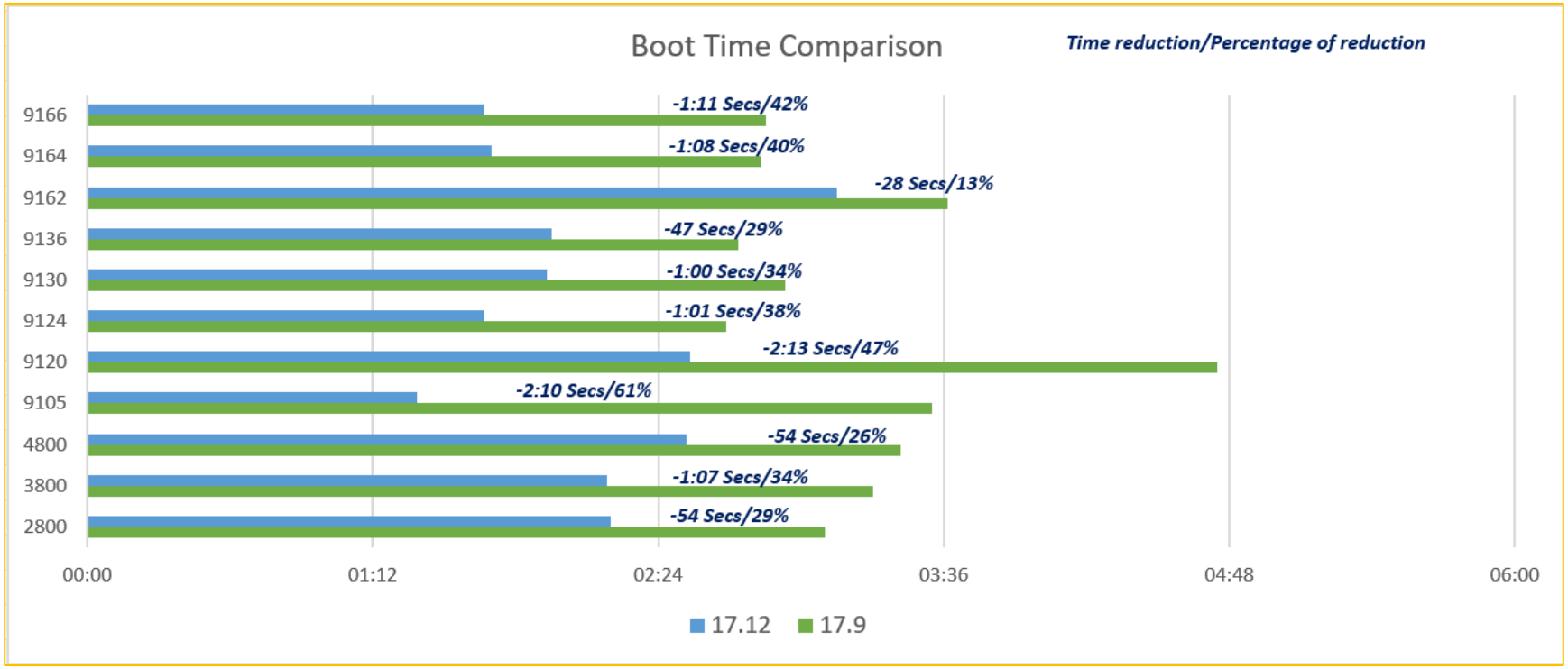


* SSID exact name depends on AP model

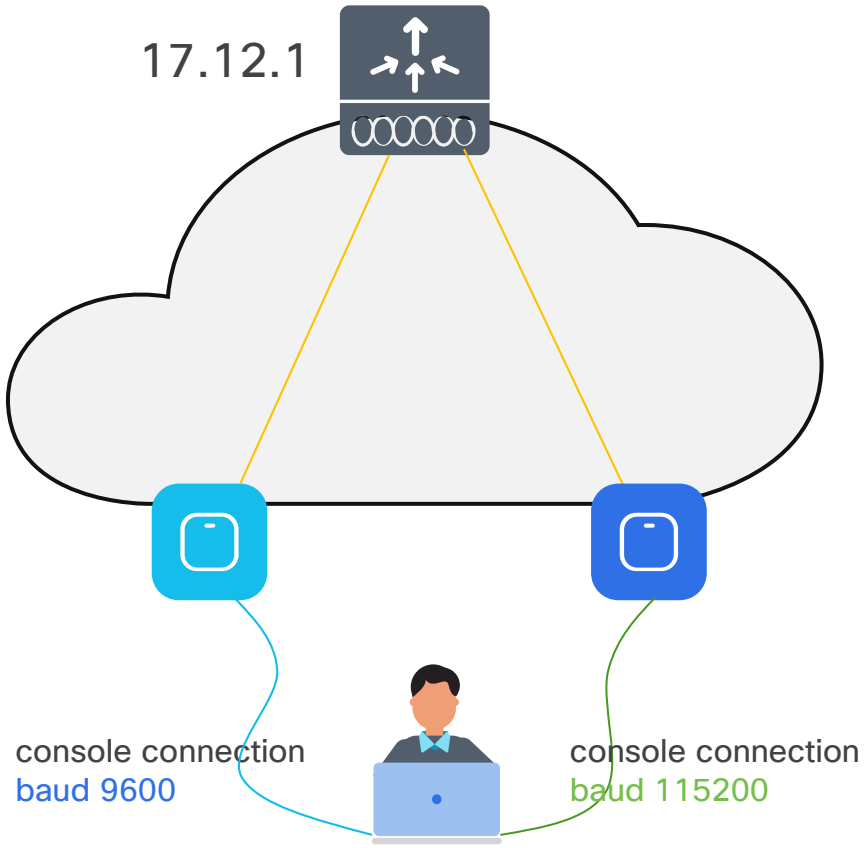
Optimizations

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

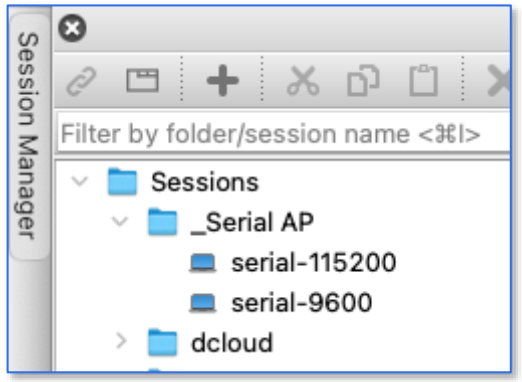


AP Console baud rate change



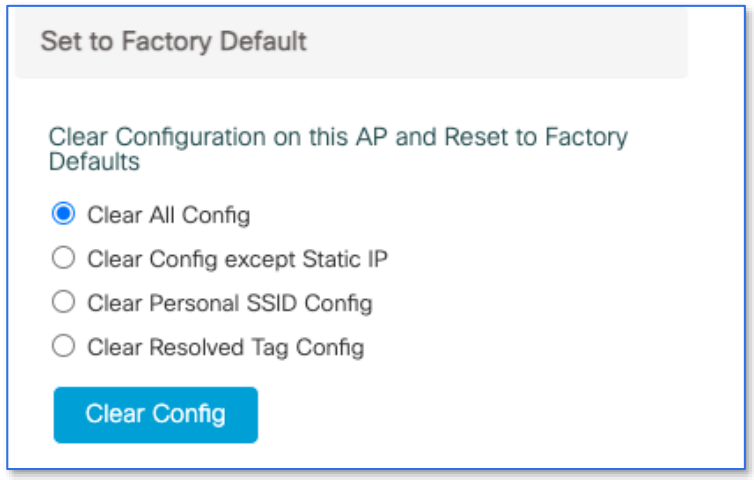
Why would you care?

- Customer is on 17.9.7, 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:

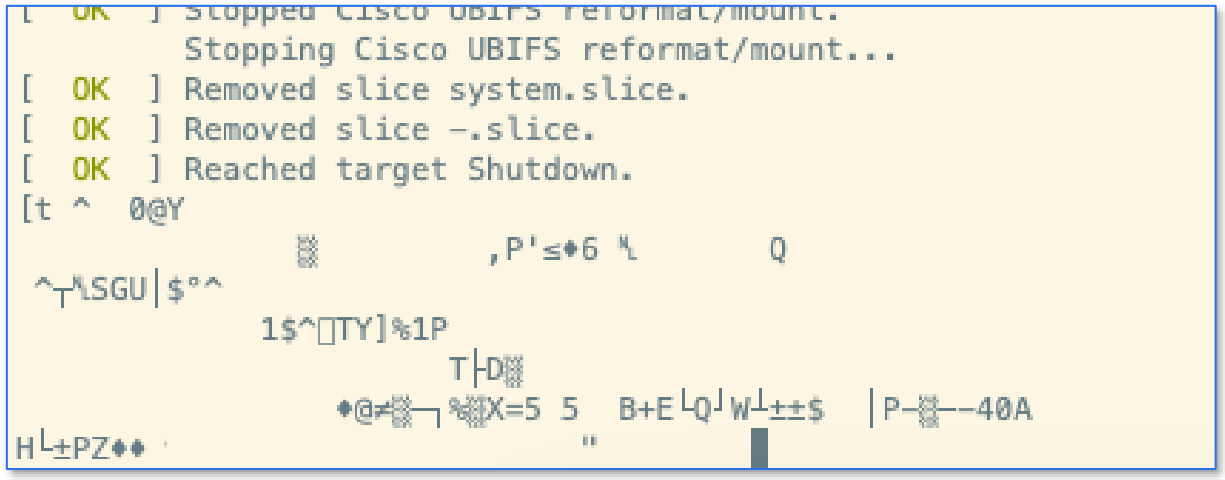


AP Console baud rate change

- WPA2 should be disabled while WPA3, PMF and dot11ax are enabled to broadcast WLAN exclusively on 6-GHz band. WPA2 ca
- The inner MAC filtering feature of Embedded Packet Capture (EPC), captures CAPWAP data fragments and CAPWAP control no
- When wireless interface is not available, the RMI +RP configuration on the Web UI is disabled.
- From this release, the **bssid-neighbor-stats interval** value has been changed from 1 to180 seconds to 30 to 600 seconds. The
- From this release, the default console baud rate of the 802.11AX APs is changed from 9600 bps to 115200 bps.

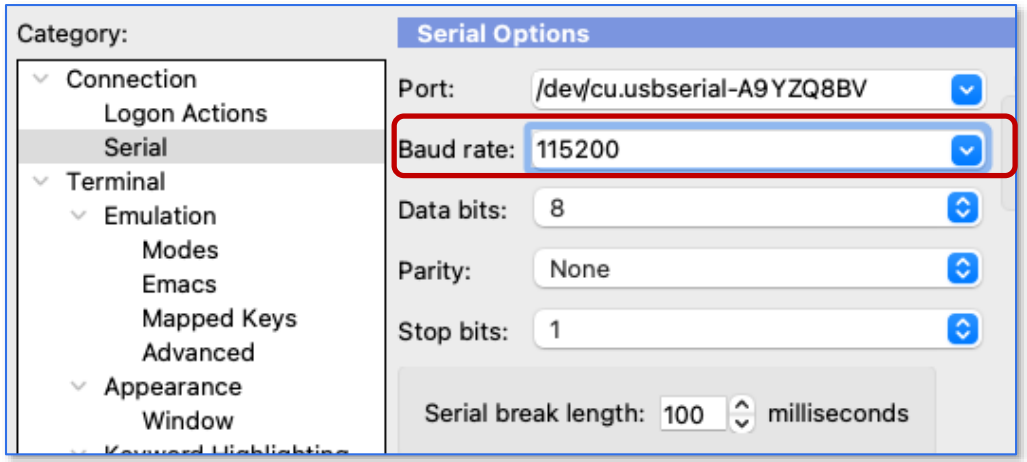


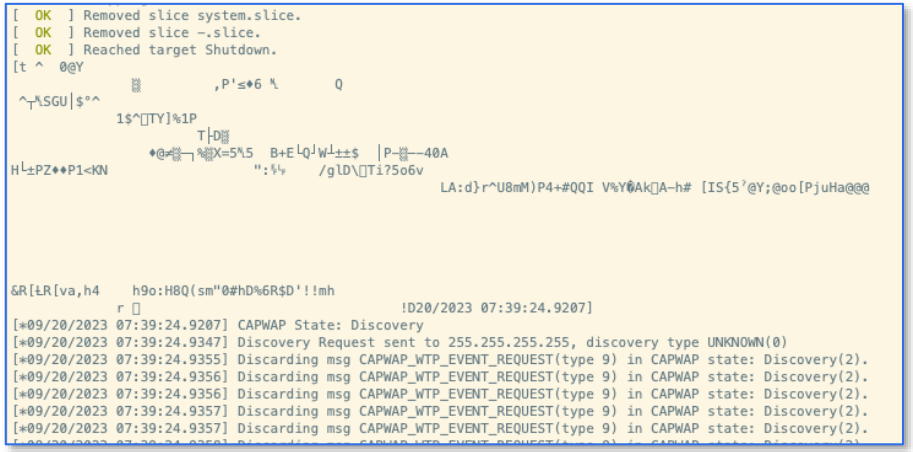
after AP reboot



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)

Wireless Product Analytics

Wireless Product Analytics

Knowing product usage to serve customers better

Product decisions for customer benefit

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

Better product experiences for customers

- Software version and critical security advisories
- Recommendation to avoid security issues
- Risk scoring
- Best practice recommendations

Wireless Product Analytics

- Release Notes
- Product Analytics FAQ
- Data Privacy sheet

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

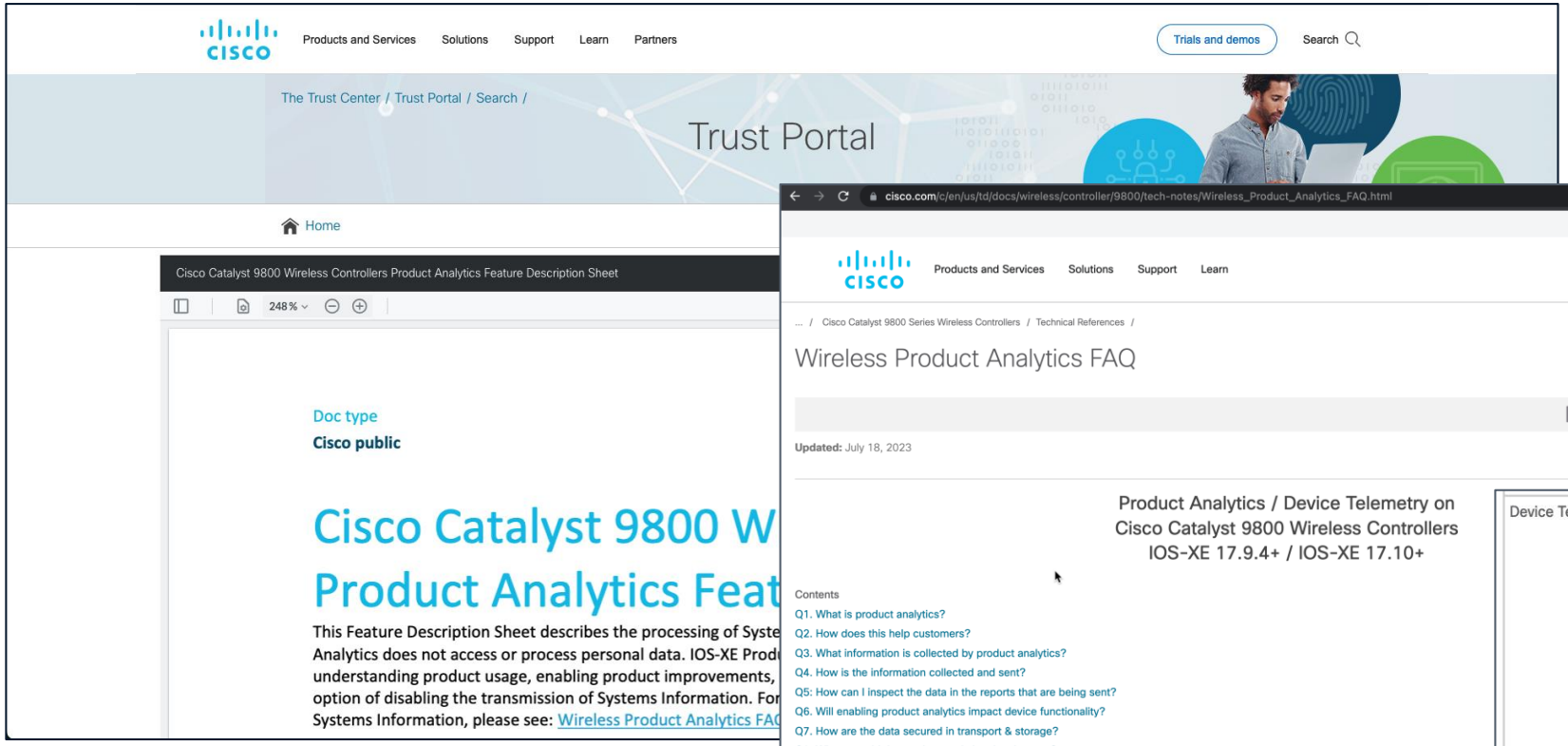
The data collected is non-PII data. CLI is present to view the report collected/ sent for transparency

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

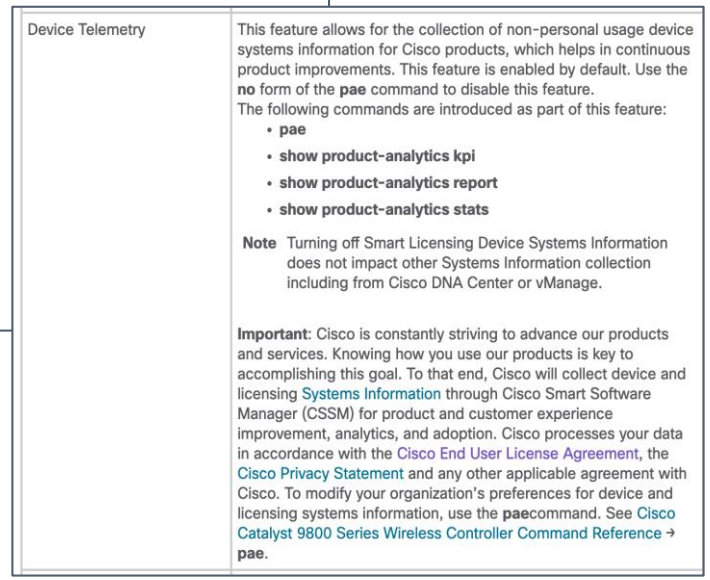
Options to disable :
Use no-form of 'pae' command - no pae
Block the URL https://dnaservices.cisco.com

Wireless Product Analytics - Documentation



Data privacy sheet

FAQs



Release notes

Agenda

Day 0

01 C9800 Design and Deployment

02 Wi-Fi 6E/7 Migration Best Practices

Day 1

03 WLAN Configuration

04 Site Tag and WNCd Load Balancing

05 RF Tag Recommendations

Day 2

06 RF Monitoring

07 Optimization

08 Software Upgrades

Agenda

Day 0

01 C9800 Design and Deployment

02 Wi-Fi 6E/7 Migration Best Practices

Day 1

03 **WLAN Configuration**

04 **Site Tag and WNCd Load Balancing**

05 **RF Tag Recommendations**

Day 2

06 RF Monitoring

07 Optimization

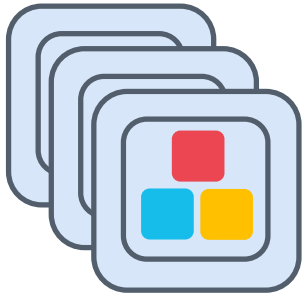
08 Software Upgrades

Day 1:
C9800 Configurations

Design with Tags in Mind

C9800 Configuration Model (Profiles & Tags)

Access Points



RF Tag

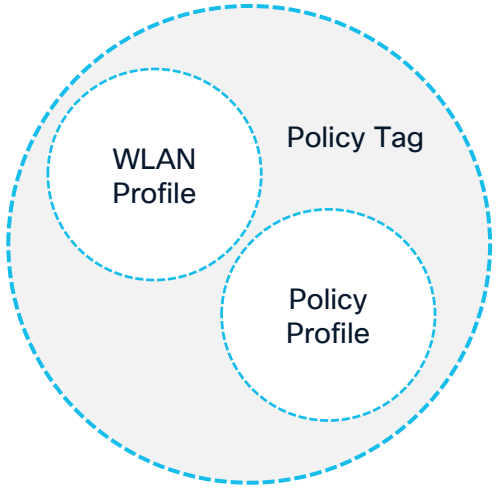
Policy Pag

Site Tag

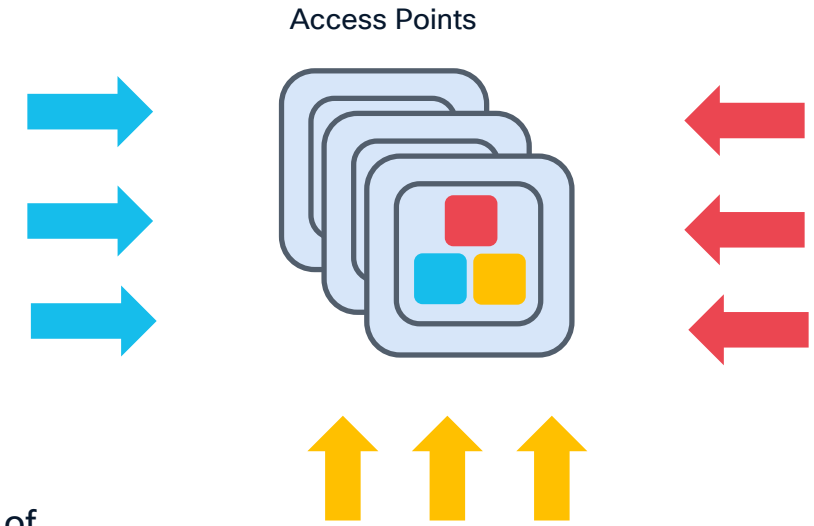
Important to remember:

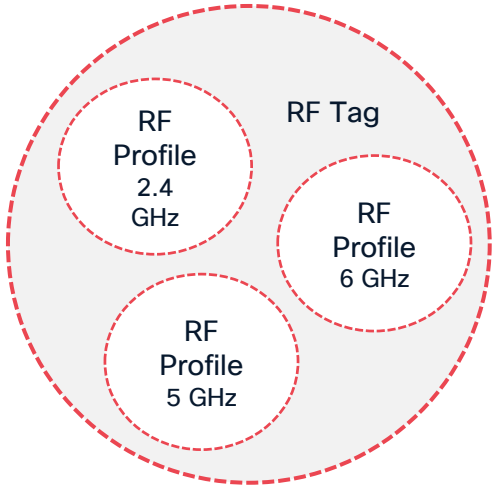
- Profiles (Policy, AP Join and Radio Frequency (RF)) and tags are the new configuration constructs
- Profiles are assigned via tags. Every AP needs to be assigned to the three AP tags (Policy, Site, RF)
- Advantages of the new configuration models:
  - Modular and reusable config constructs
  - Flexible 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

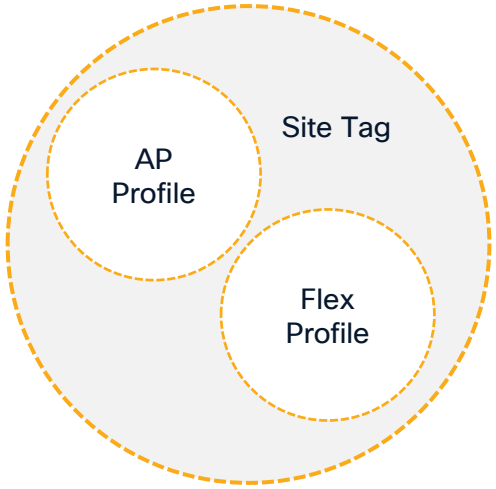


- Defines the Broadcast domain (list of WLANs to be broadcasted) with the policies of the respective SSIDs
- “Equivalent” to AP Group in AireOS





- 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

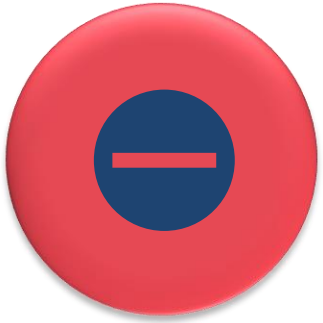
Wi-Fi 6E Security (Recap)

Wi-Fi 6E uplevels security.

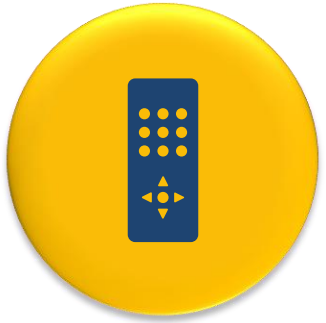
WPA3

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

Wi Fi™
WPA3



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

Wi-Fi 7 Security

WPA3 Requires WPA3 on all frequencies

 Requires Beacon Protection

 Requires GCMP-256 as a cipher*

 Requires Protected Management Frame (PMF)

*see next slides for further details on how this applies to IOS-XE 17.15 and 17.18

Wi-Fi 6E & 7 Security

Enterprise

For your reference

WPA type*	AKM[s]	Fast transition	PMF	AES-128	GCMP-256***	Compatibility	Notes
WPA3 Enterp.	802.1X-SHA256	All	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	GCMP-256 future
WPA3 Enterp.	FT + 802.1X**	Enabled	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	GCMP-256 future
WPA3 Enterp.	802.1X-SHA256 FT + 802.1X**	Enabled	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	GCMP-256 future
WPA3 Enterp.	SUITEB192-1X	Disabled	✓	✗	✓	Wi-Fi 6E Wi-Fi 7	
WPA2 Enterp. WPA3 Enterp.	802.1X 802.1X-SHA256	All	Optional	✓	✓	Legacy Wi-Fi 6E^ Wi-Fi 7^	GCMP-256 future Allows legacy clients on 2.4/5 GHz ^^ in 6GHz PMF is broadcasted as mandatory 🏆 Compatibility Focus
WPA2 Enterp.	802.1X	Adaptive Disabled	✗	✓	✗	Legacy (No 6E & 7)	No 802.11be, no 6GHz

* Enable beacon protection
** still uses SHA256, even if not explicit in its naming
*** GCMP256 not supported in C9105, C9115 and C9120

AKM = Authentication and Key Management
SHA-256 = Secure Hash Algorithm (SHA) 256 bit
PMF = Protected Management Frame

Wi-Fi 6E & 7 Security

For your reference

Personal

WPA type*	AKM[s]**	Fast transition	PMF	AES-128	GCMP-256***	Compatibility	Notes
WPA3 Pers.	SAE-EXT-KEY	Disabled	✓	✓	✓	No legacy Wi-Fi 7	AES-128 allowed in 17.15 GCMP-256 mandatory in 17.18
WPA3 Pers.	SAE-EXT-KEY FT + SAE-EXT-KEY	Enabled	✓	✓	✓	No legacy Wi-Fi 7	AES-128 allowed in 17.15 GCMP-256 mandatory in 17.18
WPA3 Pers.	SAE SAE-EXT-KEY	Disabled	✓	✓	✓	Wi-Fi 6 Wi-Fi 6E Wi-Fi 7	SAE “transition”, “transition” may need H2E/HPN Support for clients without SAE-EXT-KEY
WPA2 Pers. WPA3 Pers.	PSK SAE SAE-EXT-KEY	Disabled	Optional	✓	✓	Legacy Wi-Fi 6E Wi-Fi 7	Transition may need H2E/HPN AES-128 allowed in 17.15 GCMP-256 mandatory in 17.18
WPA2 Pers. WPA3 Pers.	PSK SAE SAE-EXT-KEY FT-SAE-EXT-KEY FT-SAE	Enabled	Optional	✓	✓	Legacy Wi-Fi 6E Wi-Fi 7	FT support Transition may need H2E/HPN AES-128 allowed in 17.15 GCMP-256 mandatory in 17.18
WPA2 Pers. WPA3 Pers.	PSK SAE	Disabled	✓	✓	✗	Legacy Wi-Fi 6E No Wi-Fi 7	No 802.11be, but 6GHz supported
WPA2 Pers.	PSK	Disabled	✗	✓	✗	Legacy (No 6E & 7)	No 802.11be, no 6GHz

* Enable beacon protection
** SAE hash to element (H2E) is required for Wi-Fi 6E & 7
*** GCMP256 not supported in C9105, C9115 and C9120

AKM = Authentication and Key Management
SAE = Simultaneous Authentication of Equals
PMF = Protected Management Frame
H2E = Hash to Element
HPN = Hunting and Pecking

Wi-Fi 6E & 7 Security

Enhanced Open

For your reference

WPA type	AKM[s]	Fast transition	PMF	AES-128	GCMP-256*	Compatibility	Notes
Enhanced Open	OWE	Disabled	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	AES-128 allowed in 17.15 GCMP-256 mandatory in 17.18
Enhanced Open	OWE	Disabled	✓	✓	✗	Wi-Fi 6E No Wi-Fi 7	No 802.11be, but 6GHz supported
Enhanced Open	OWE-Transition	Disabled	N/A	✓	✗	Legacy No Wi-Fi 6E No Wi-Fi 7	No 802.11be, no 6GHz supported Requires 2 SSIDs**

* GCMP256 not supported in C9105, C9115 and C9120
** see https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217737-configure-enhanced-open-ssid-with-transi.html

AKM = Authentication and Key Management
OWE = Opportunistic Wireless Encryption
PMF = Protected Management Frame

WLAN/SSID Design

6GHz WLAN Design Considerations

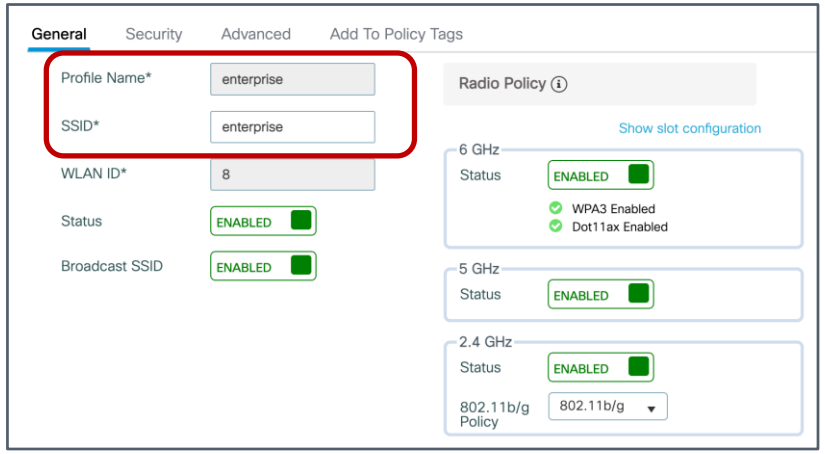
What options would you have?

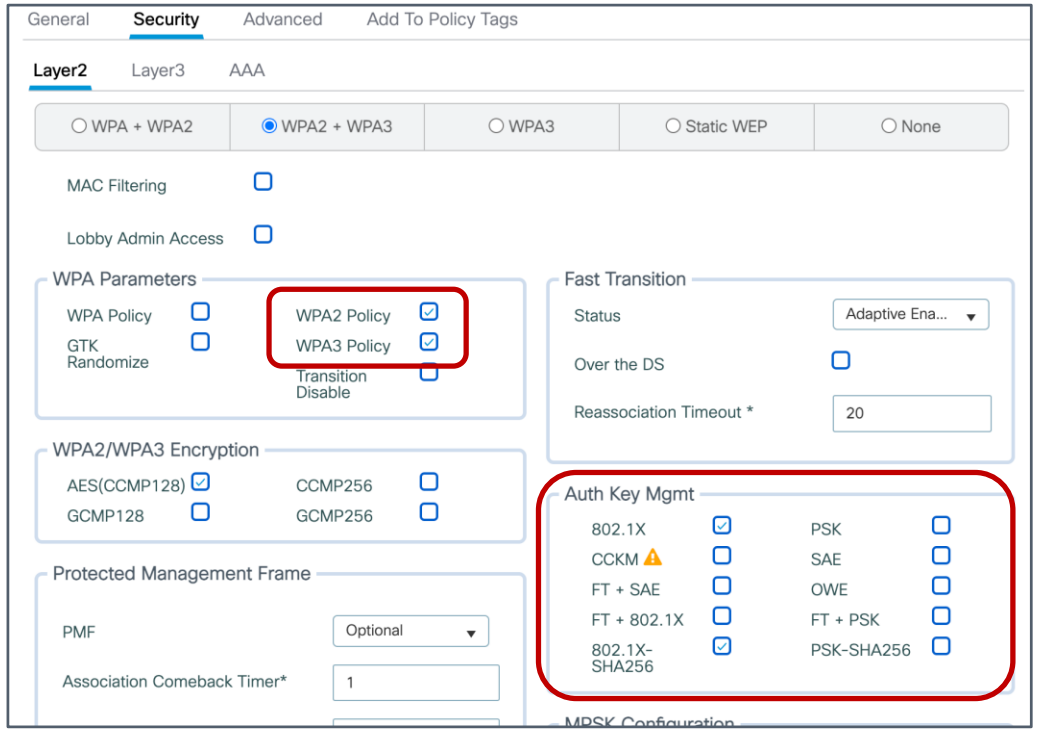
1. "All-In" Option: Reconfigure the existing WLAN to WPA3, one SSID for all radio policies (2.4/5/6 GHz) – Most unlikely
2. "One SSID" Option: Configure multiple WLANs with same SSID name, different security settings – Most conservative
3. "Multiple SSIDs" Option: Redesign your SSIDs, adding specific 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

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 **depending on the compatibility desired**

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
```

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

Recommendation:

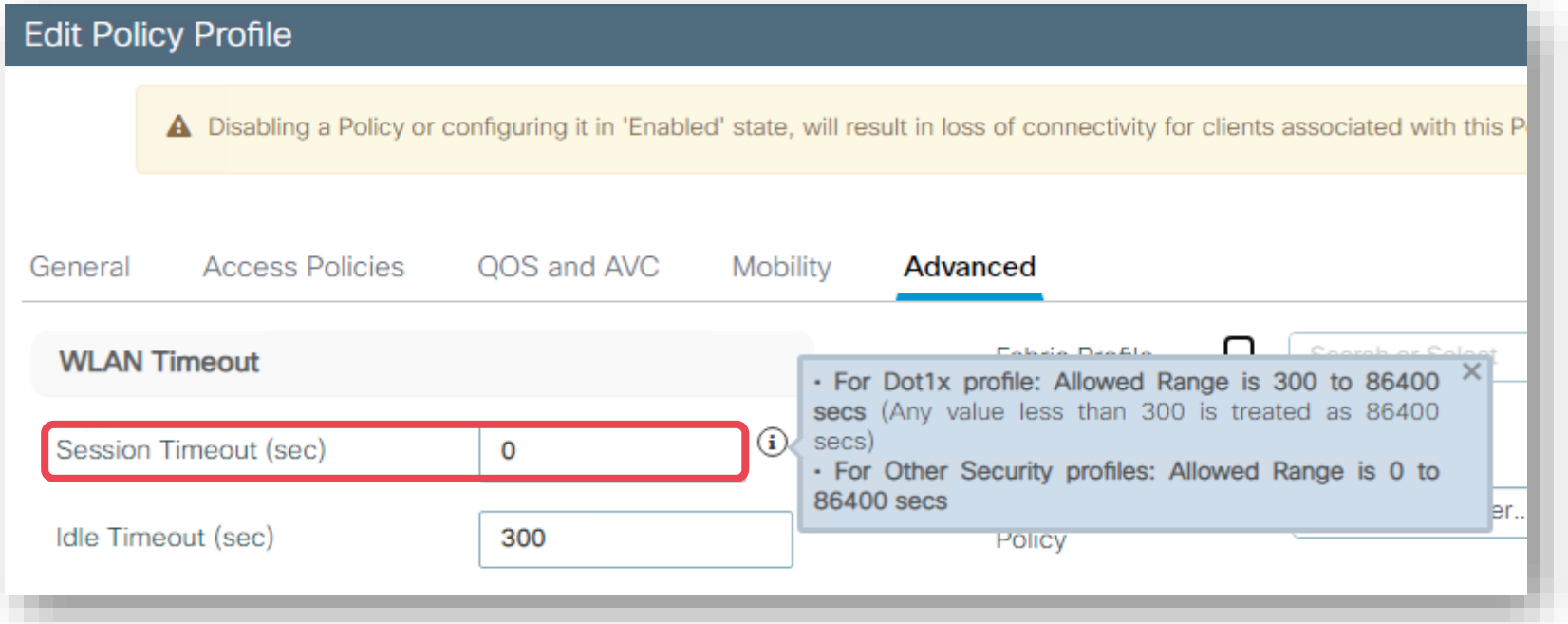
Configure the mDNS policy to use Location Specific Services (LSS) to optimize mDNS responses to clients:

```
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?

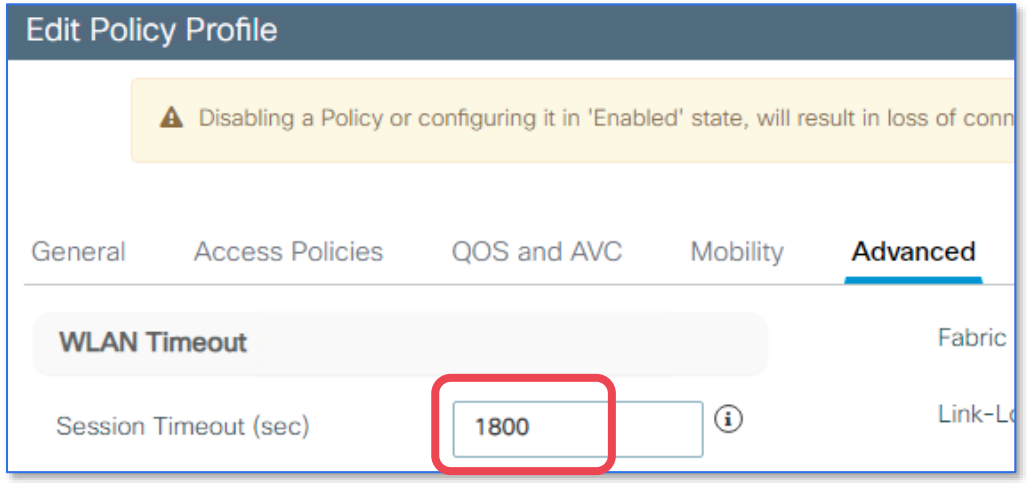
A: Yes, absolutely.

Default session timeout to 8 hours

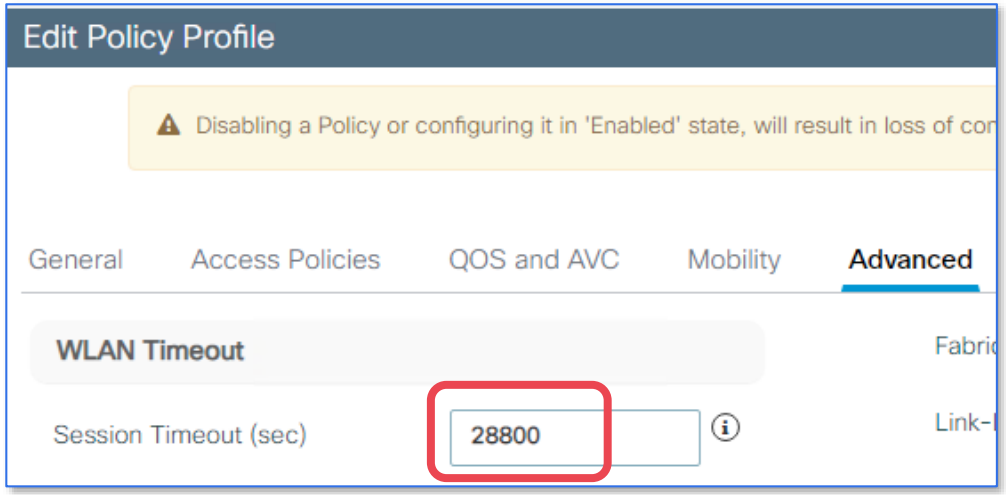
What it is?

- The default session timeout in policy profile has been 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

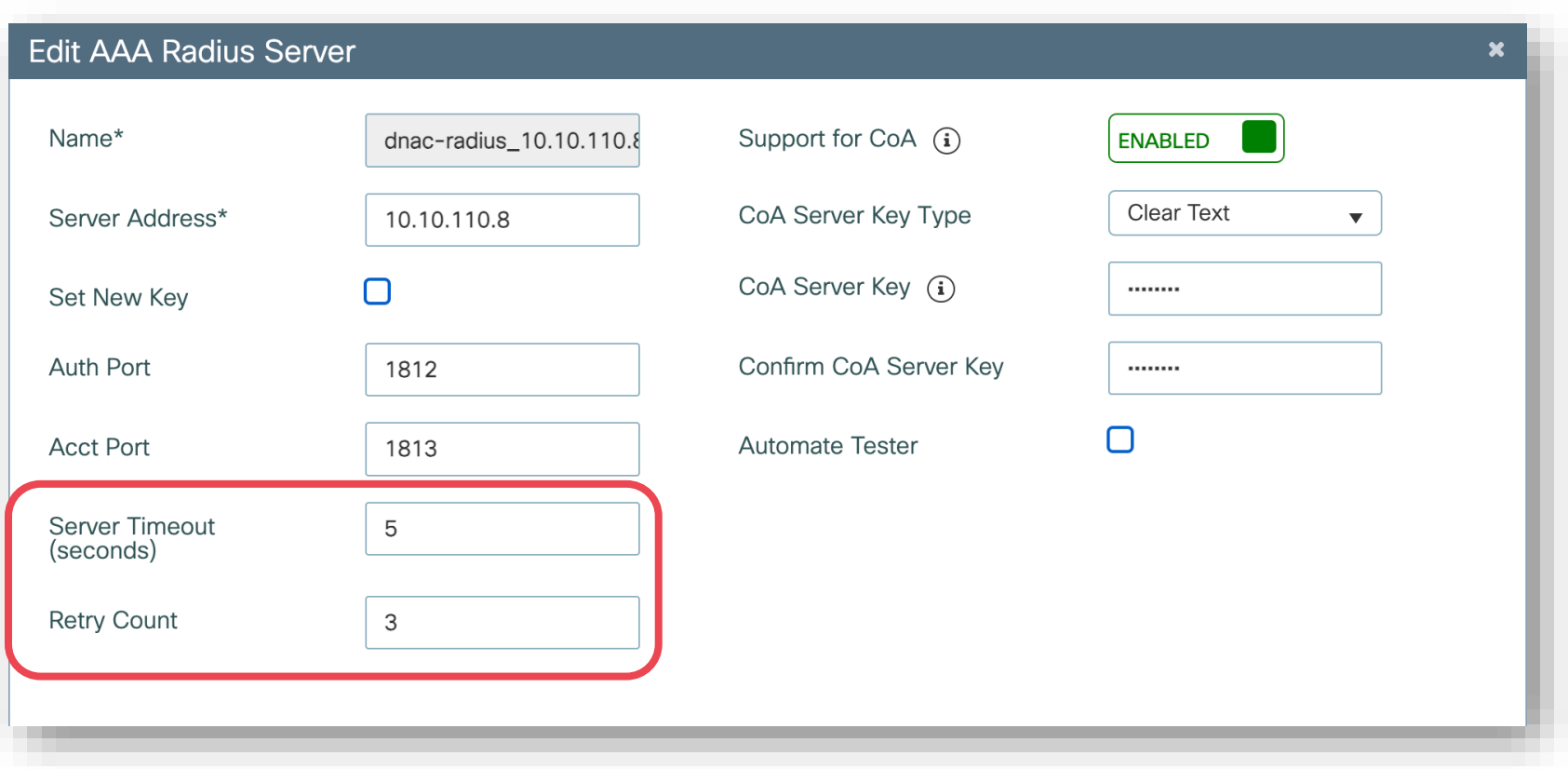


AAA Override

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

RADIUS Server Timeout

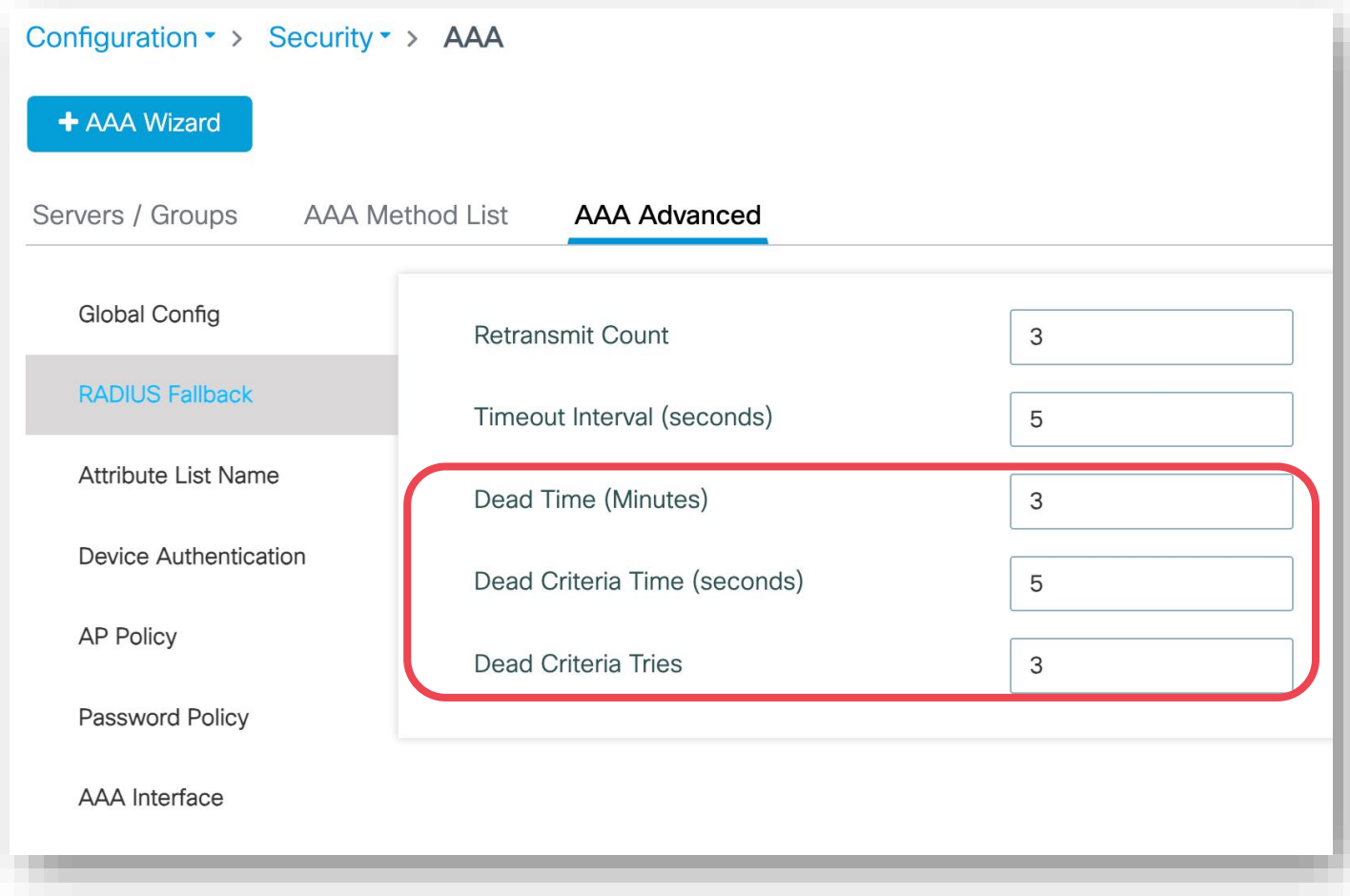
- Minimum of 5 seconds for timeout
- Minimizes early expiration of the authentication process



RADIUS Server Timeout

Dead-Criteria and Deadtime Timers

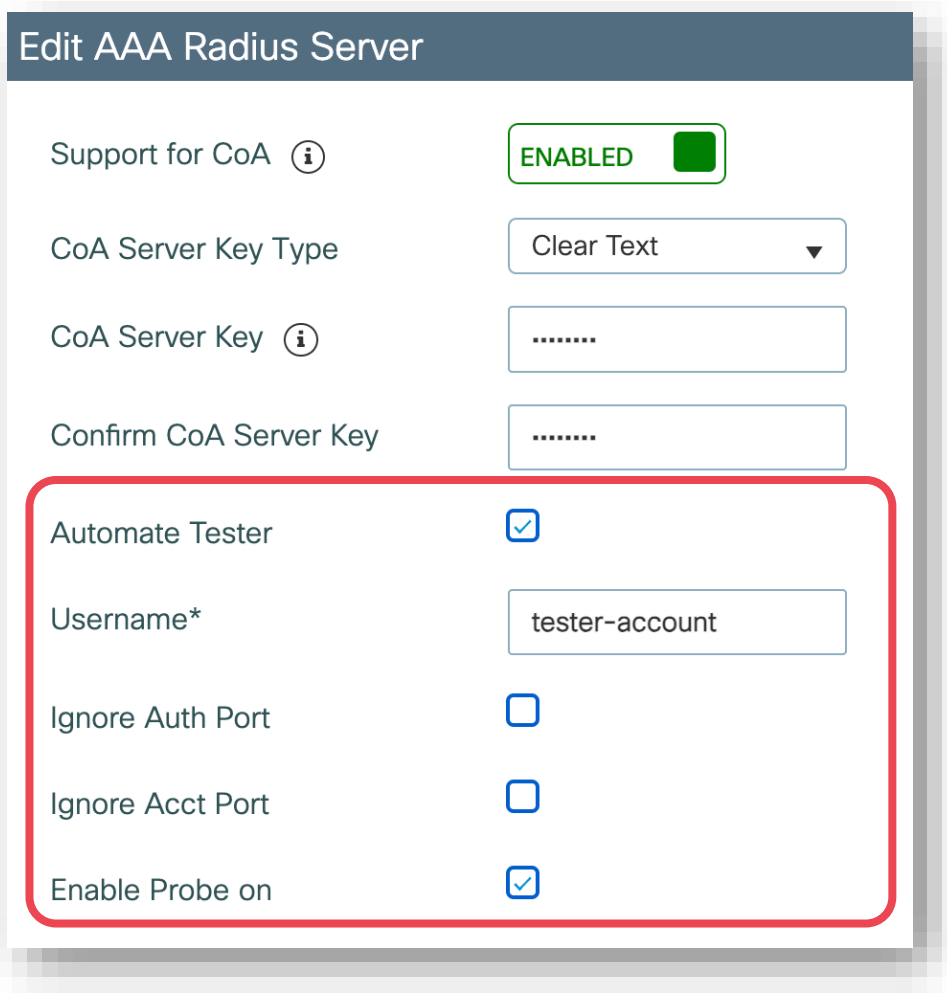
- Important for use with multiple AAA servers and load balancing
- Specifies when to mark server dead and move to next one
- Use probes to monitor status of server



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

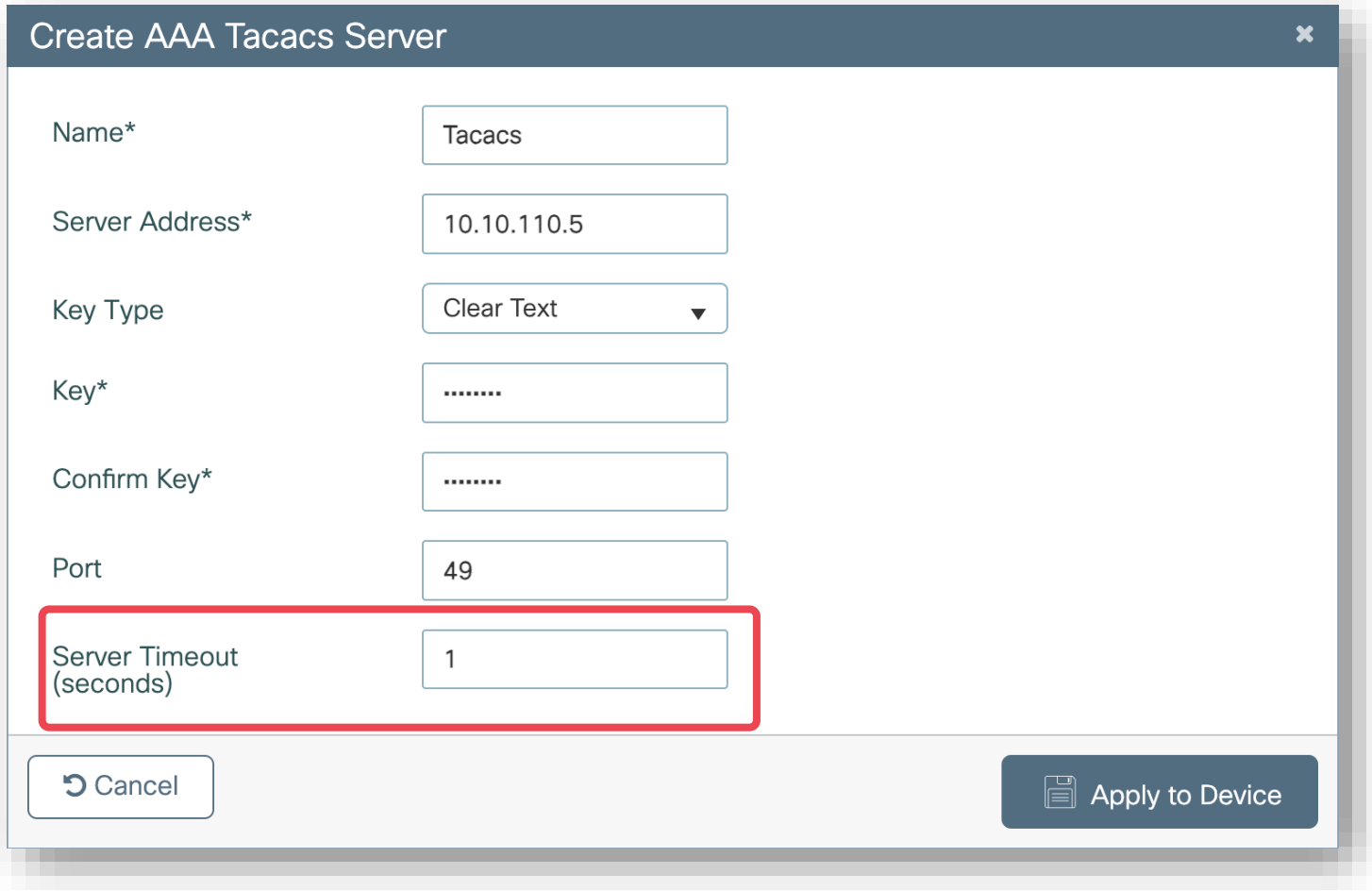


TACACS+ Management Timeout

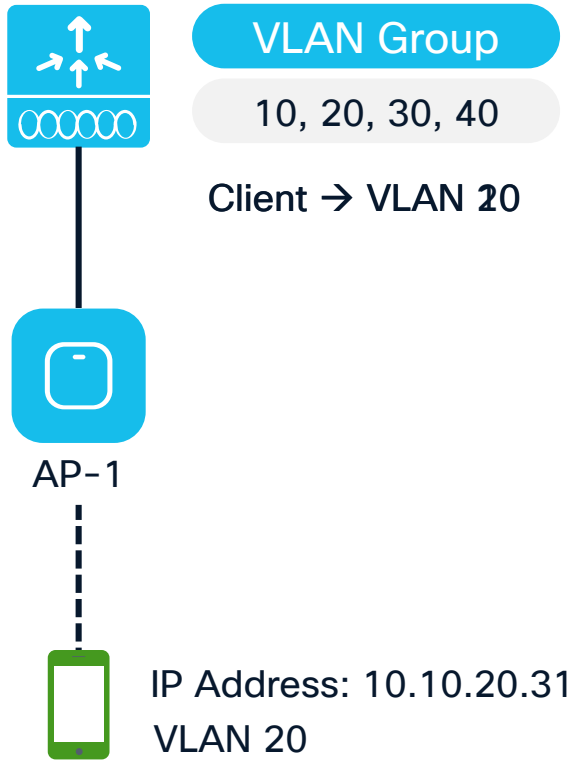
Increase retransmit timeout if:

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

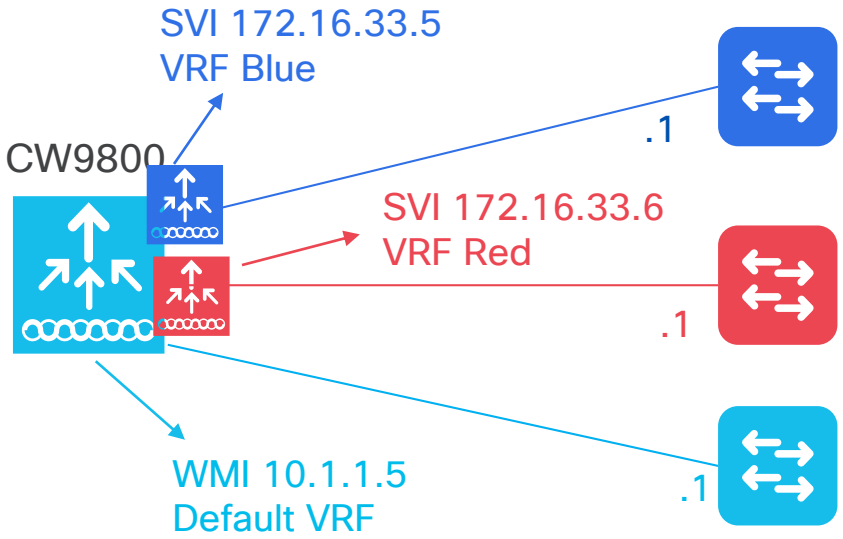
Client has a static IP in a different VLAN than the one assigned

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

If VLAN does not exist, use Static IP Mobility

Virtual Routing and Forwarding (VRF) support

- VRF refers to a technology that allows multiple instances of a routing table to co-exist within the same router... but CW9800 is not a router, so what does it really mean?
- VRF support for CW9800 refers to the capability of splitting the control plane and data plane into multiple segregated instances within the same CW9800 platform and make these planes VRF aware



Why? Use cases:

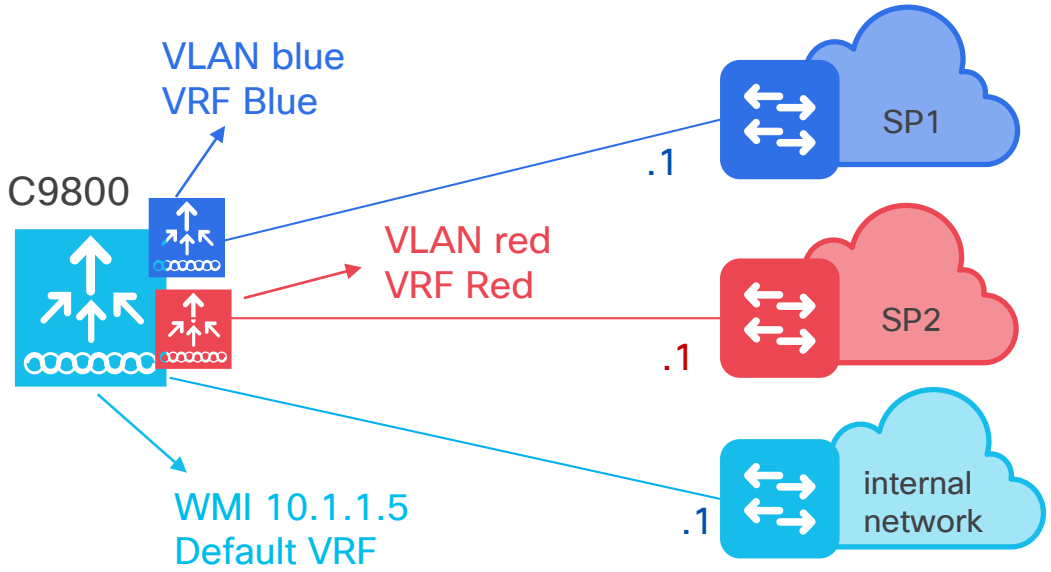
1. Client overlapping IP support, in local mode and Flex central switching*
2. Flexible forwarding of locally originated traffic to external Services like DHCP, AAA, Syslog servers, etc.
3. Increased security with isolation between client VLANs.

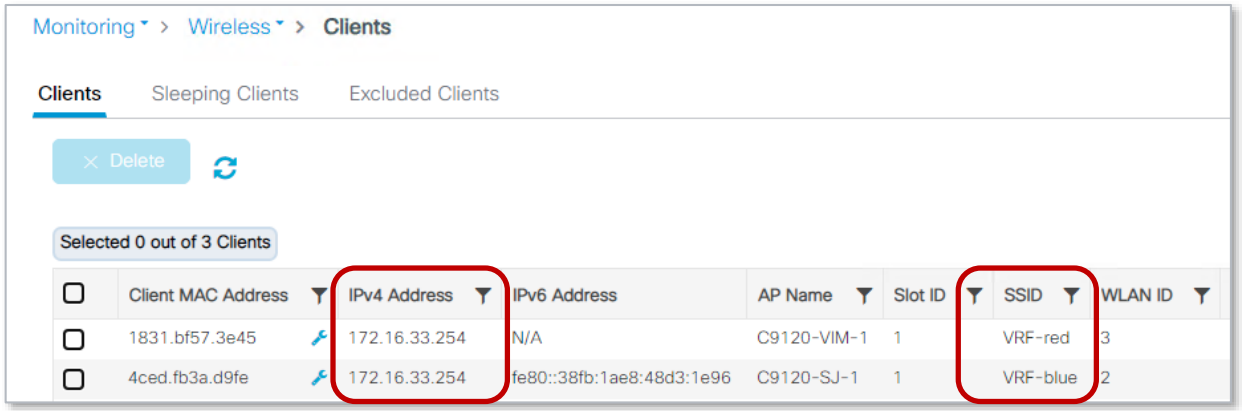
* IP overlapping in Flex Local switching is supported from 17.4.1 with different site tags

VRF support > Client Overlapping IPs

IP-overlapping use case:

- Multi-dwelling facility (e.g., airport). CW9800-based network is part of the infrastructure service
- Each customer/tenant gets an SSID, and traffic is offloaded to a different SP
- No control on SP network and IP assignment > need support for client overlapping IP address

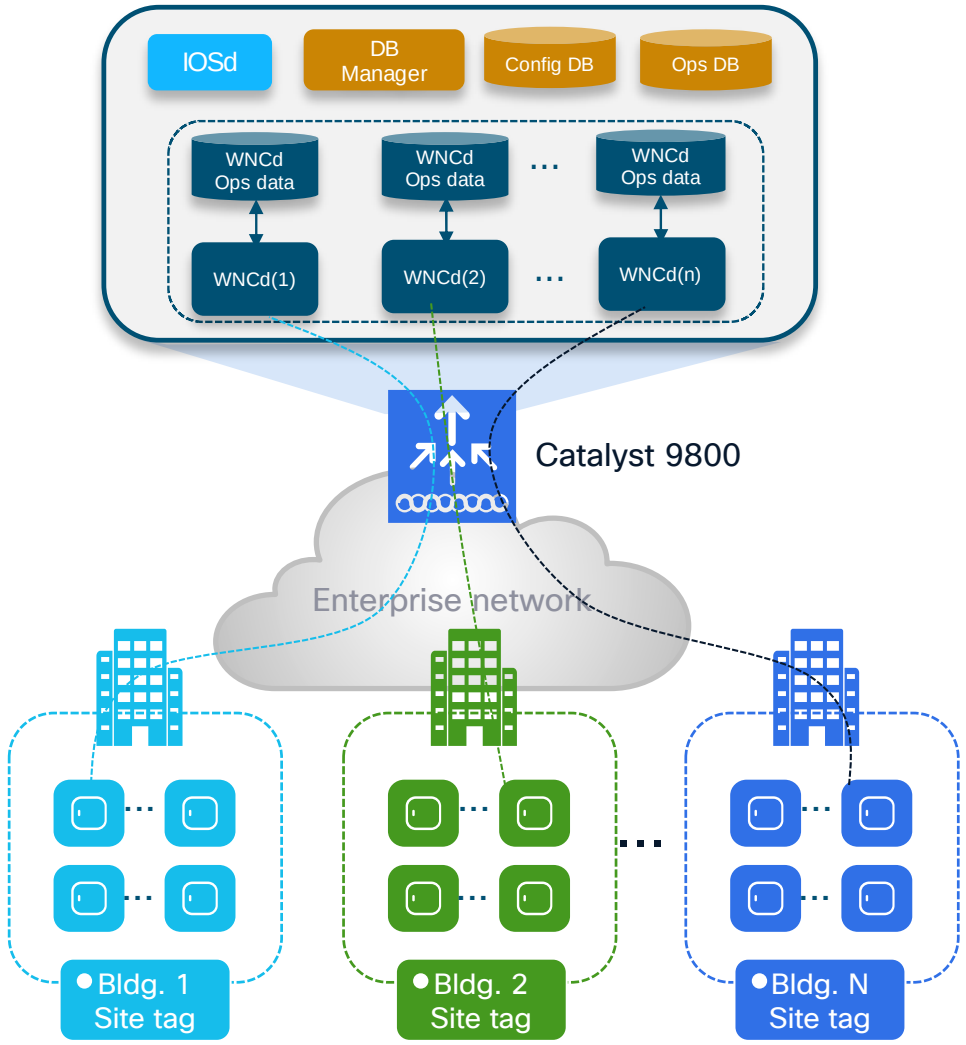




- Without VRF support, this would result in IP theft
- Pure bridging on CW9800, no need for client SVI

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:

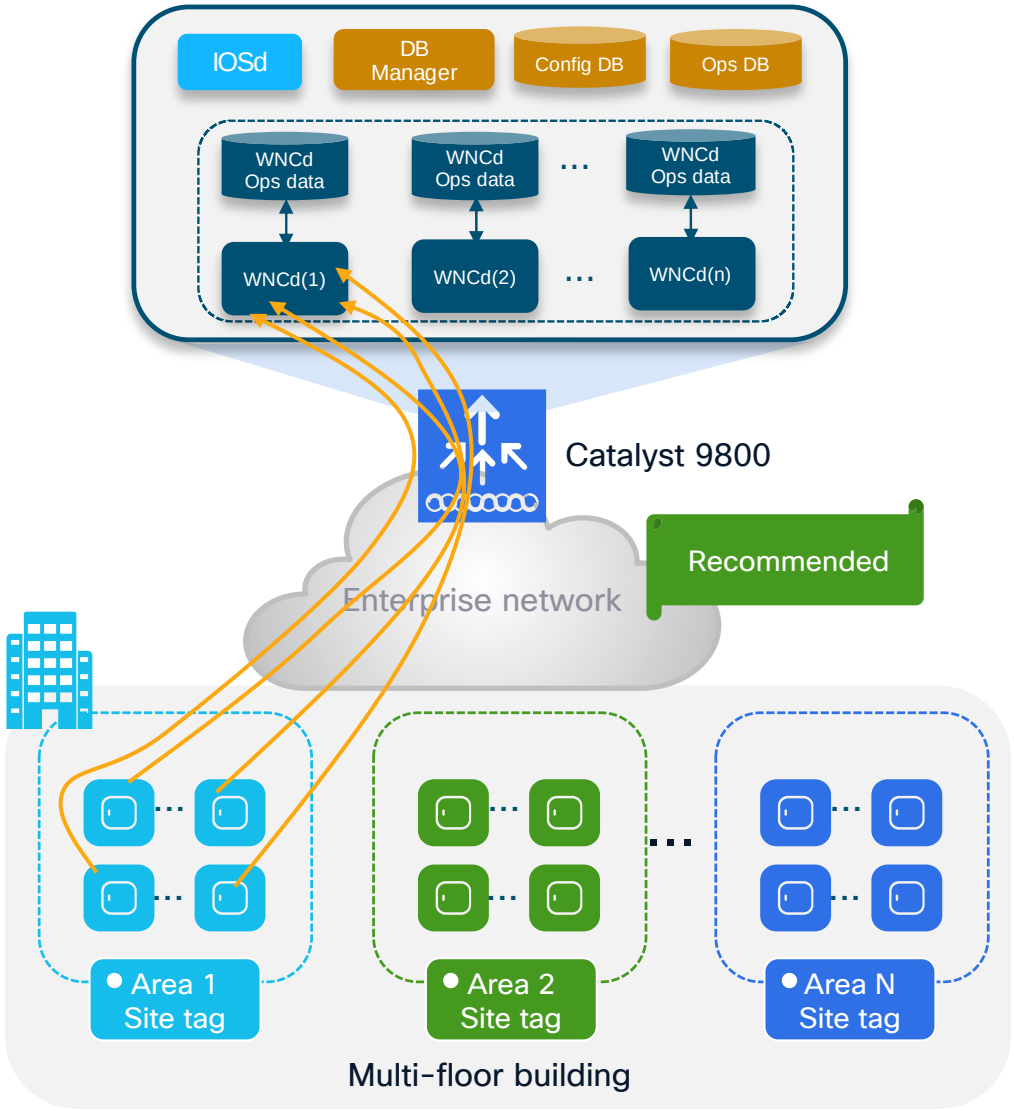
Platform	# of WNCD instances
EWC (on AP or C9k switch)	1
C9800-L	1
C9800-CL (small)	1
C9800-CL (medium)	3
C9800-40, CW9800M	5
C9800-CL (large)	7
C9800-80, CW9800H1, CW9800H2	8

Following command shows the # of WNCDs processes:

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

Site Tags – AP to WNCd distribution

Refresher!



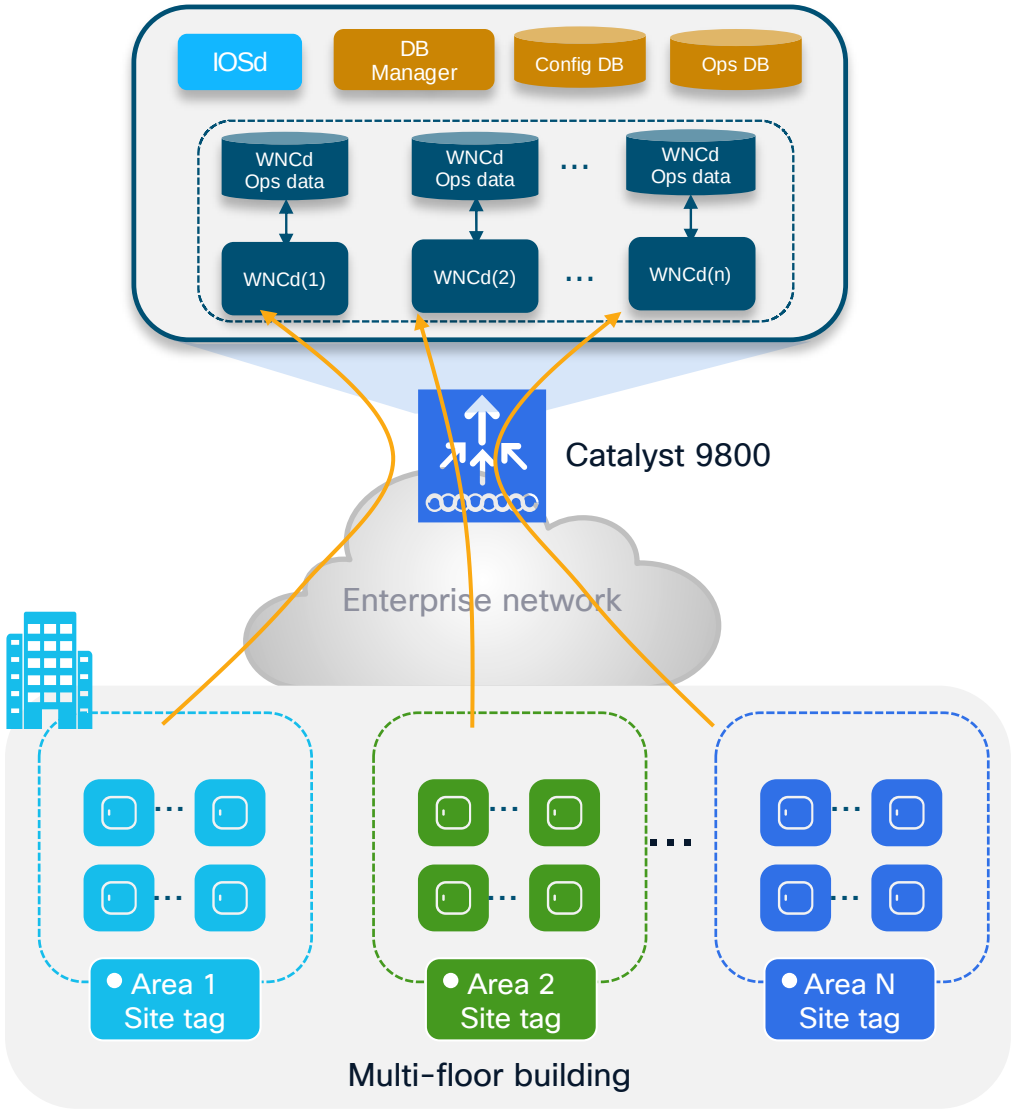
How AP distribution across WNCds works:

- **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:

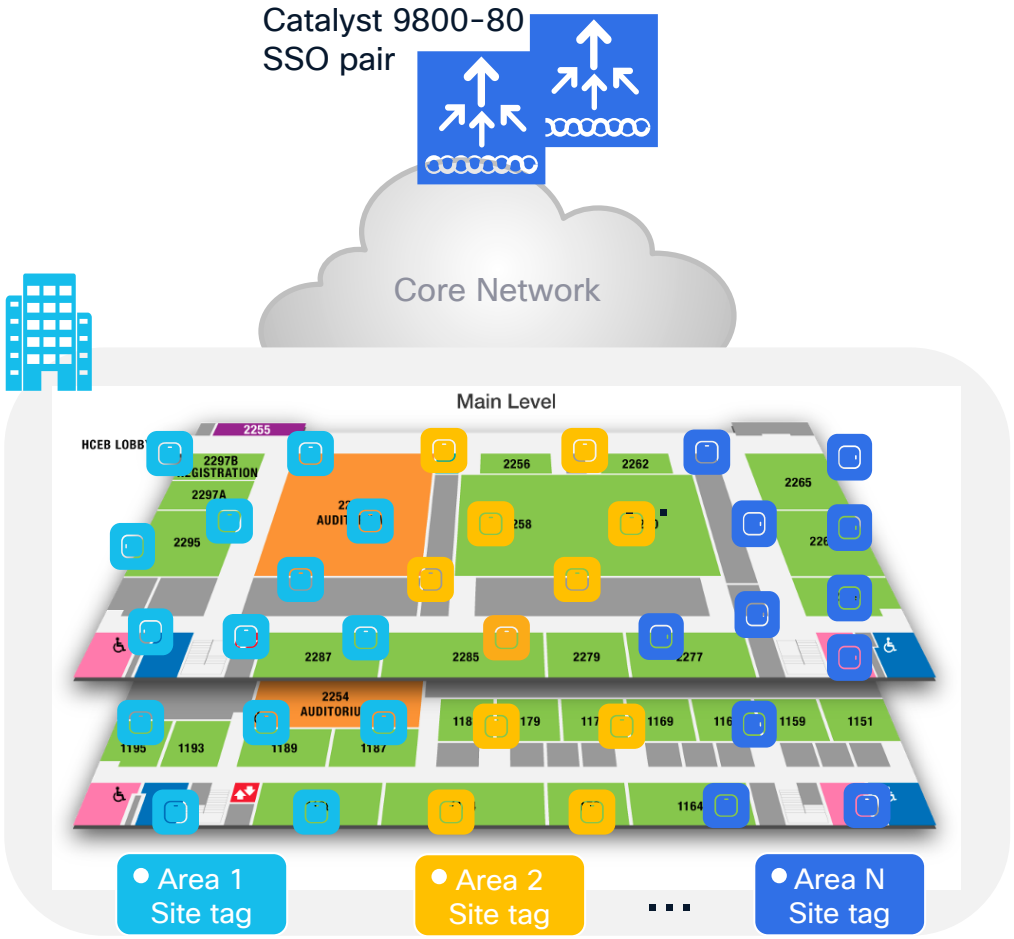
- Use **custom site tags**
- Whenever possible, have **less than 500 APs per site tag**
- **Do not overwhelm a site-tag and WNCd.** Do not exceed the following max number of APs per site tag:

Platform	Max APs per site tag
9800-80, CW9800H1, CW9800H2, 9800-CL (M & L)	1600
9800-40, CW9800M	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, CW9800H1, CW9800H2	8 or a multiple (16, 24, ...)
C9800-CL (large)	7 or a multiple (14, 21,..)
C9800-40, CW9800M	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**

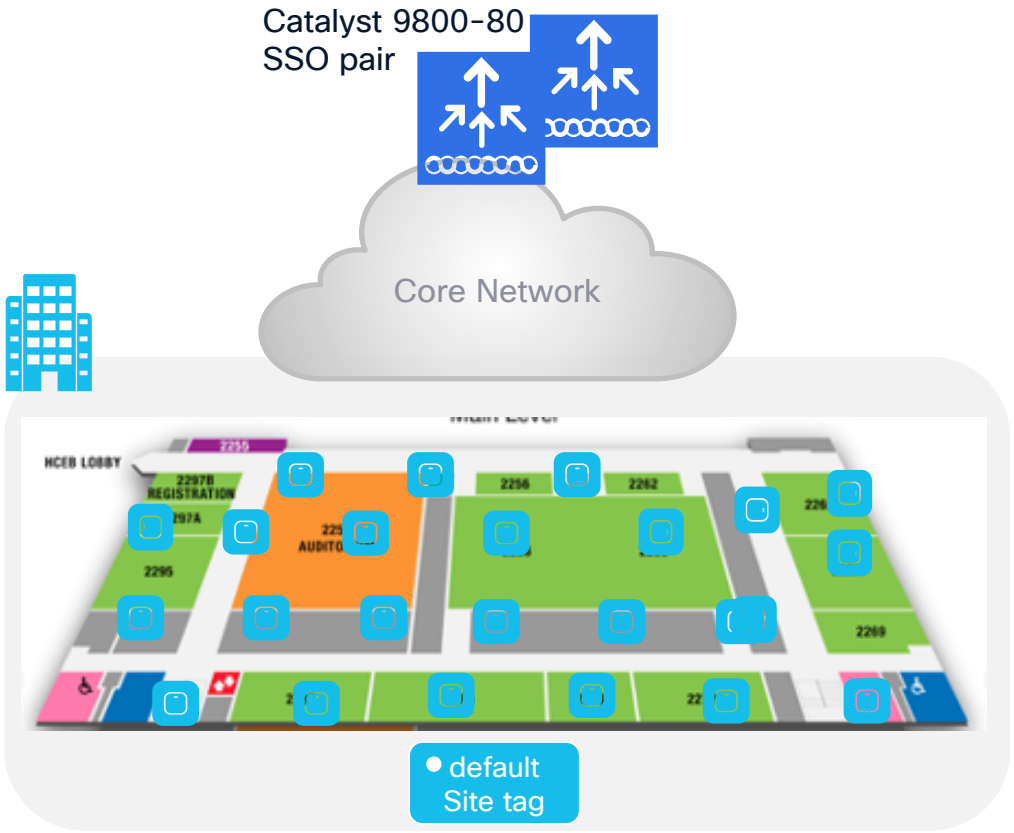
What are the recommendations in this case?

- 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, CW9800H1, CW9800H2	8
C9800-CL (large)	7
C9800-40, CW9800M	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 Design – Special case



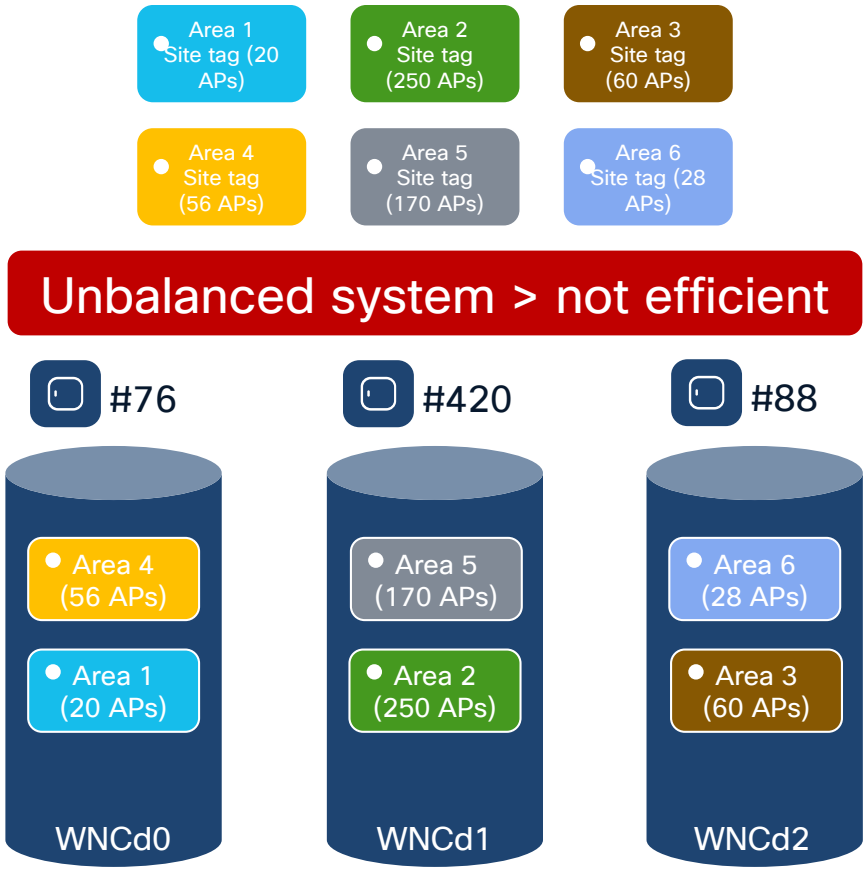
Scenario #2: Large warehouse

- 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 heavily 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

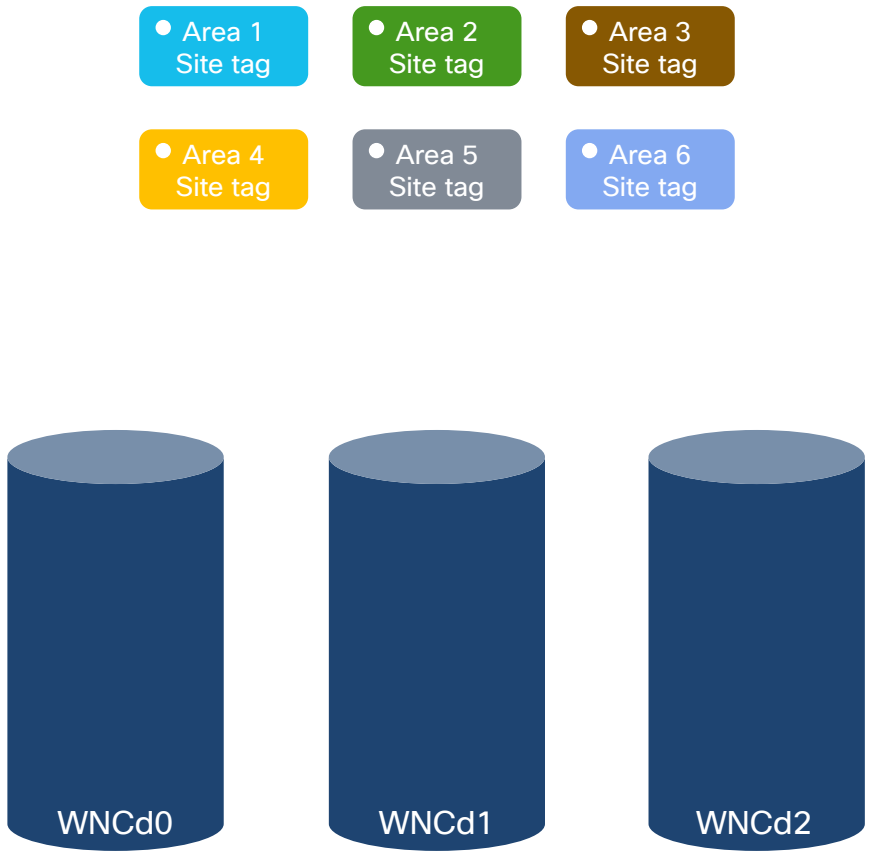


Until 17.9.1, site tags are distributed among WNCds using the **least loaded criteria** based on the **number of site tags.** The algorithm doesn't take into considerations the number of APs or clients per site tag

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

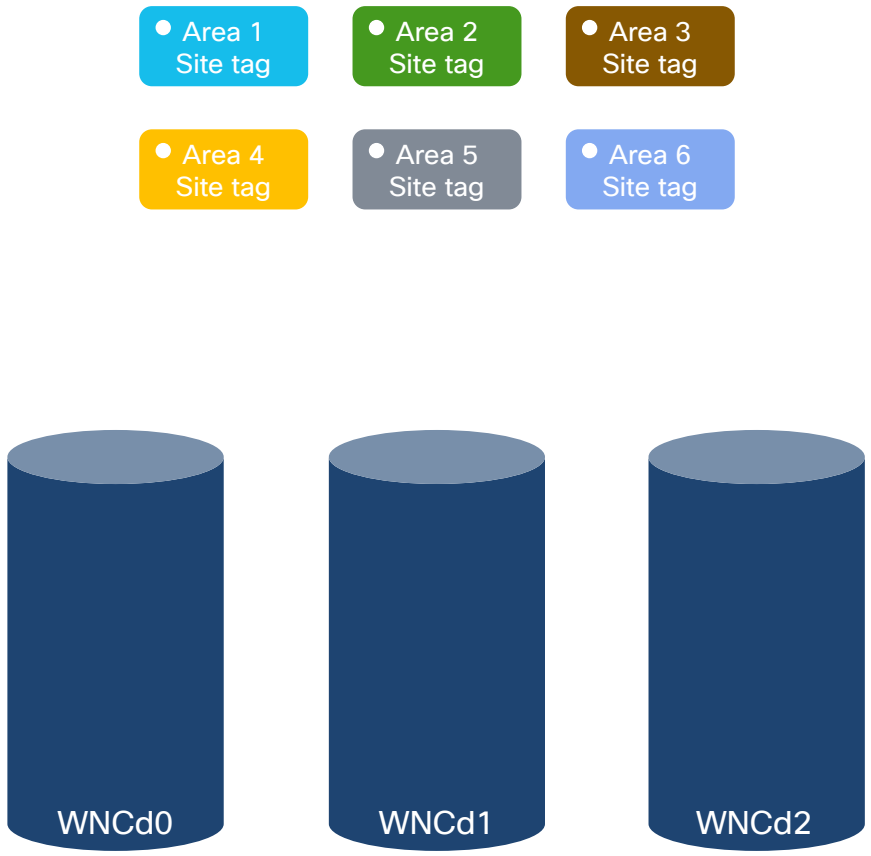


- **Starting 17.9.2 and 17.10**, the algorithm to distribute APs among WNCds may use the **load** parameter configured under the site tag:

```
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**

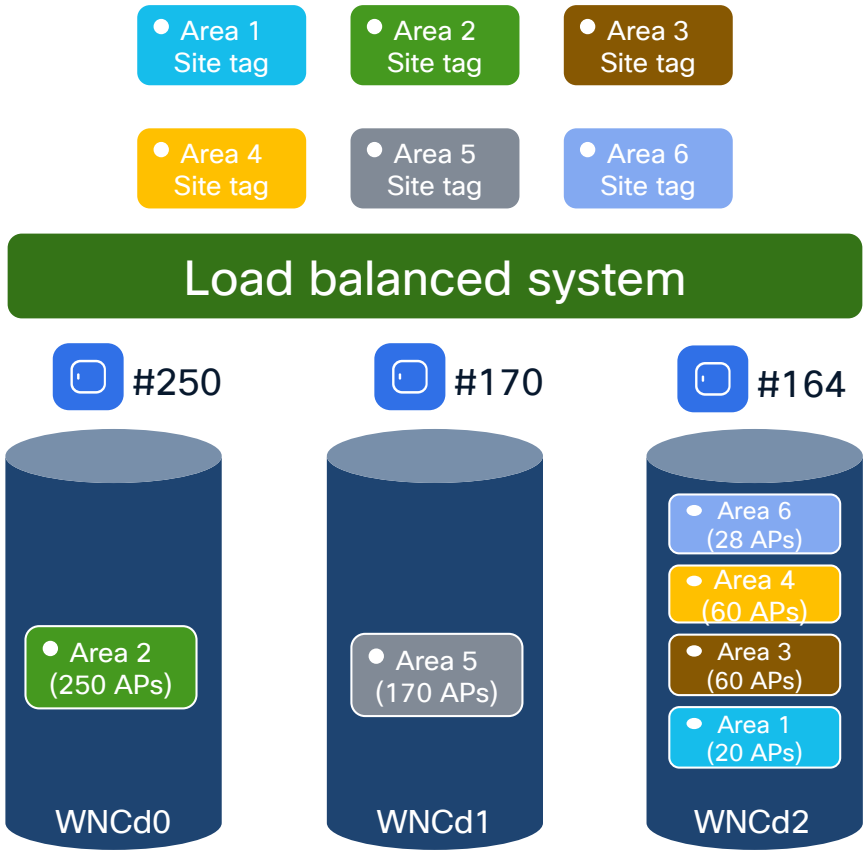
Site Tags – New load balancing Algorithm



How to choose the load?

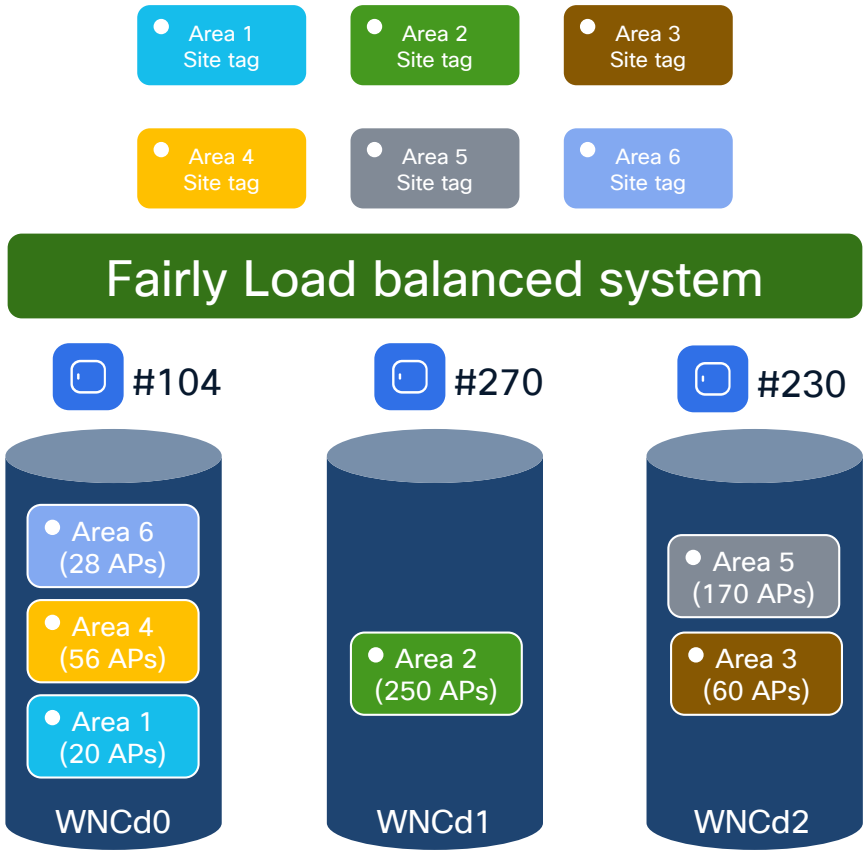
- The default value 0 means no load indication for the site tag. Nothing changes, the algorithm is the same as in 17.9.1 and previous releases
- **Most common option**: Office building with multiple floors/areas. Each floor/area is one site tag. If you estimate similar client/traffic load on each floor/area > 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

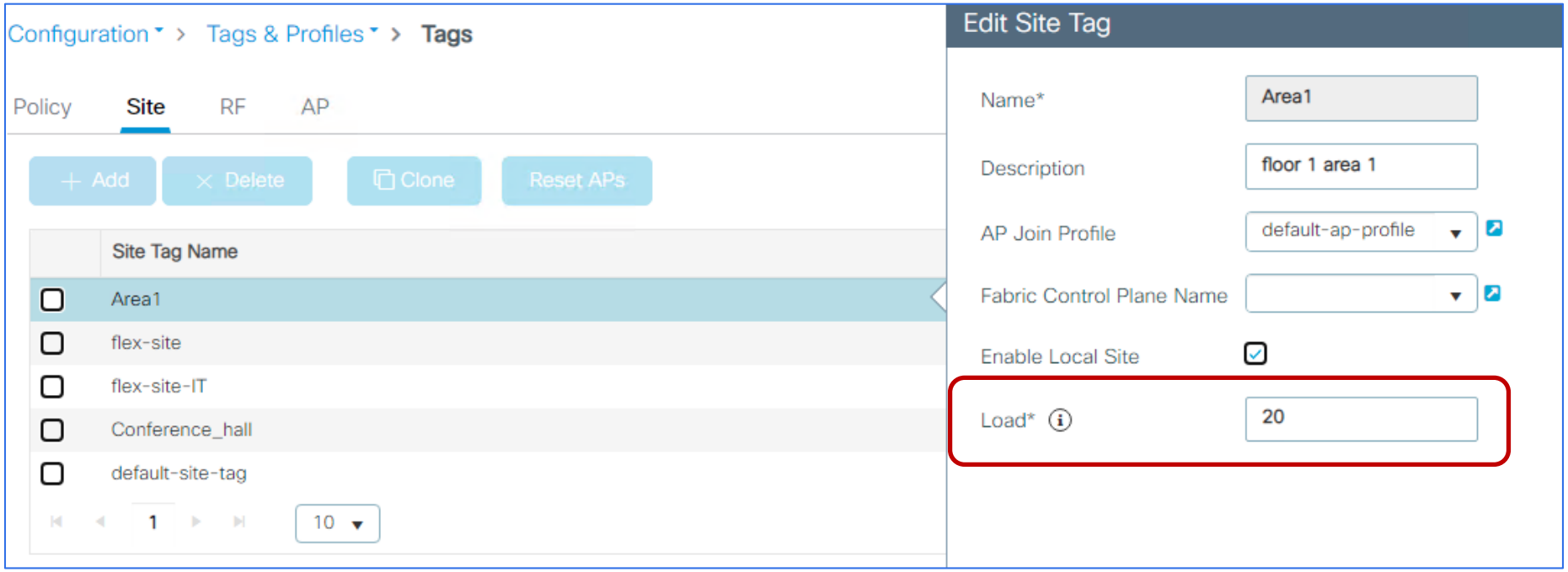
Site Tags – New load balancing Algorithm



- **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

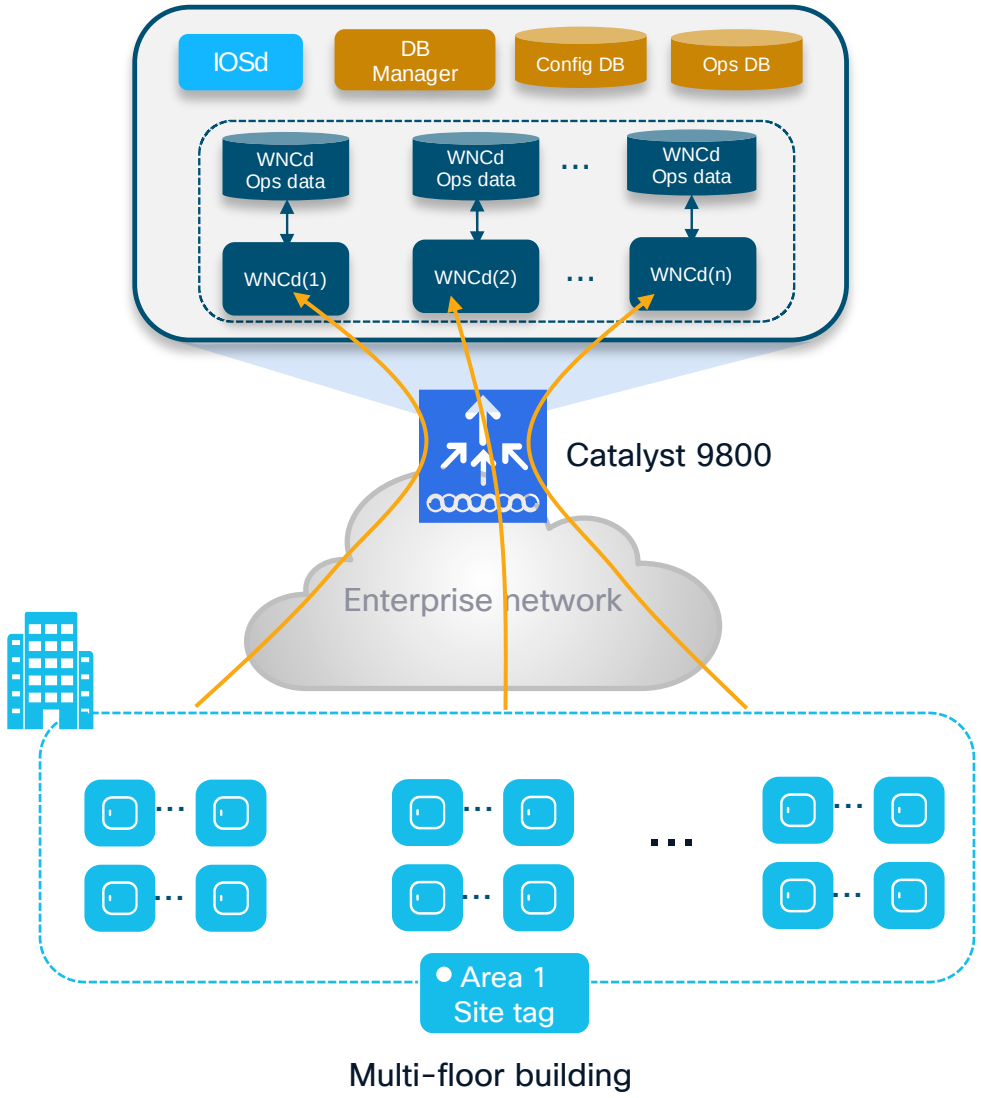
Configuring the site tag Load- WebUI

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

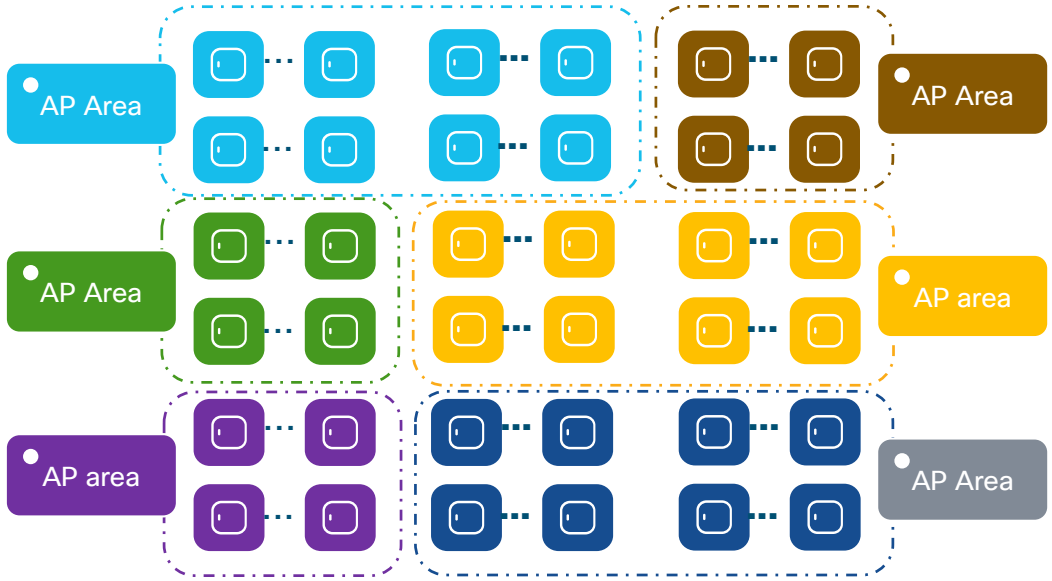
Starting 17.12.1, we have a solution!

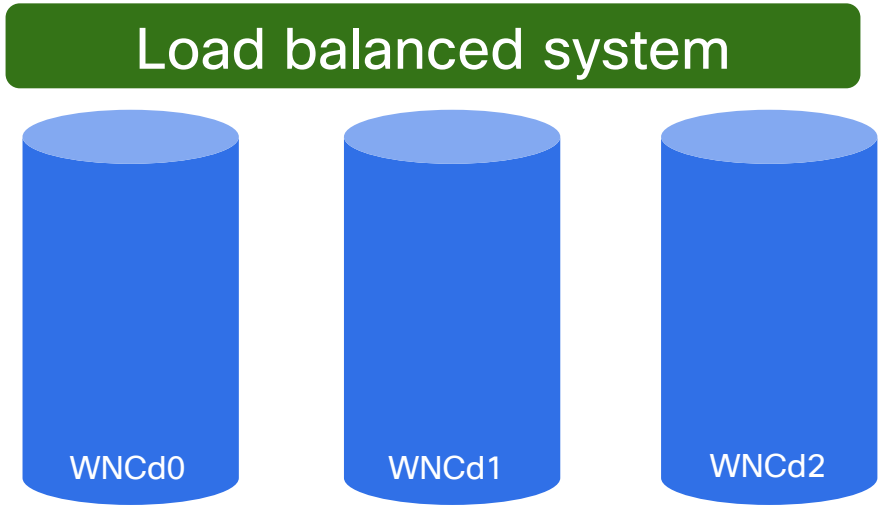
(RRM based) Auto WNCd load balancing

RRM based Auto WNCd load balancing

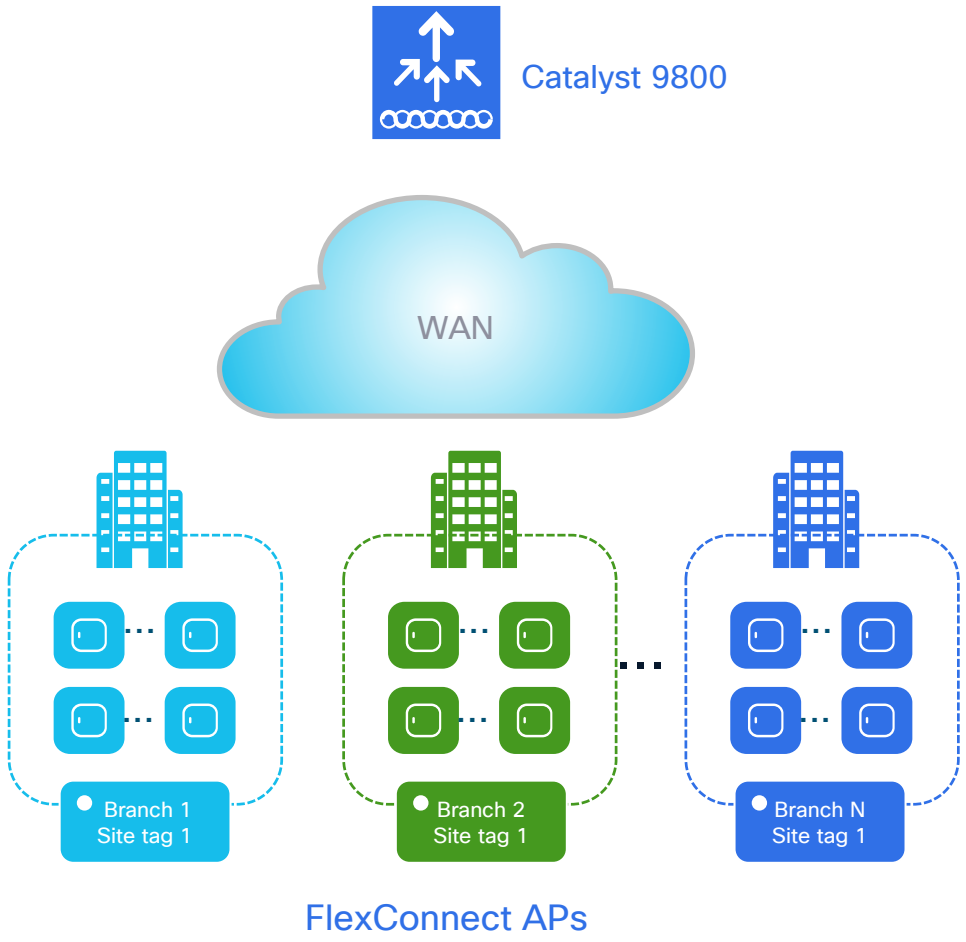
What is it?

- 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



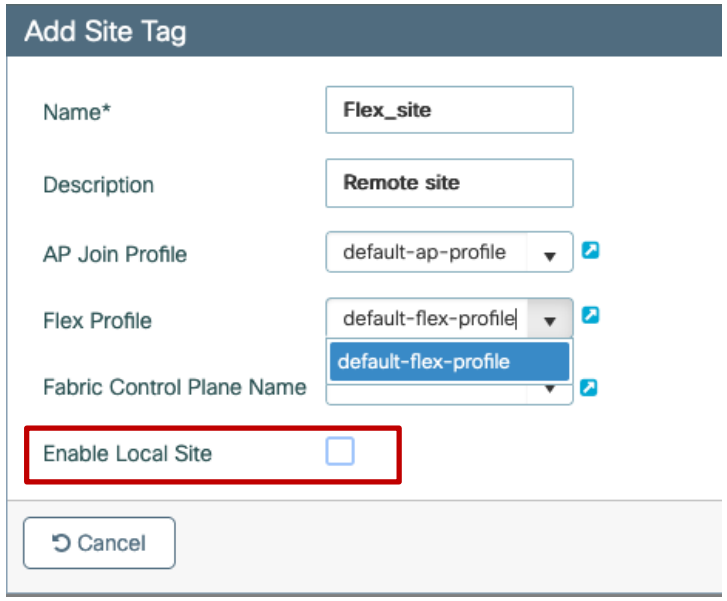


Site Tag for FlexConnect Deployments



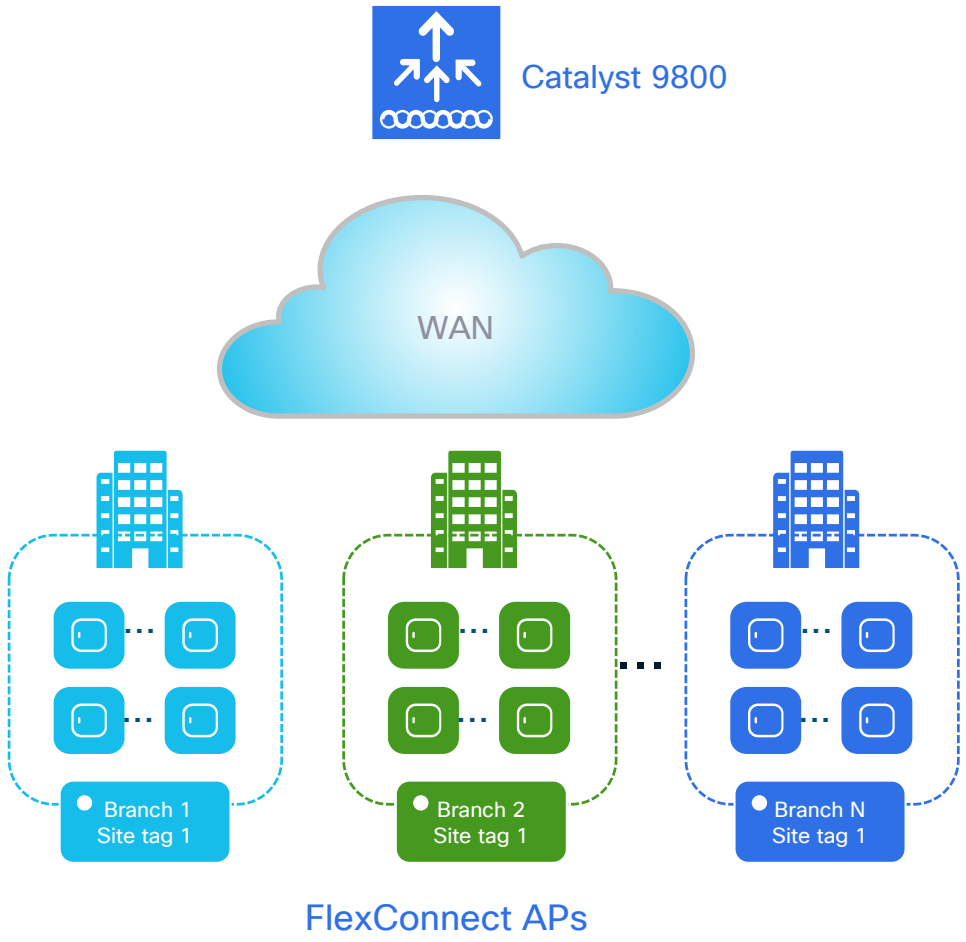
Important facts:

- 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

Design – Recommended use of AP Site Tags

For your reference

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,..)

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

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

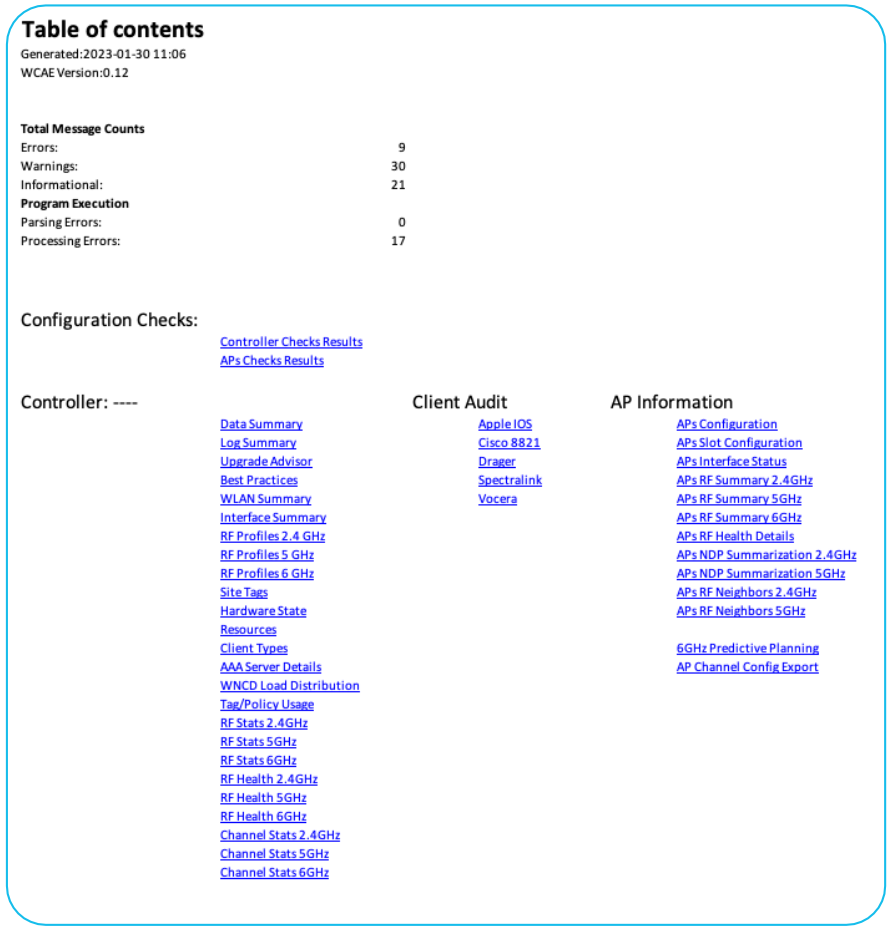


Table of contents

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

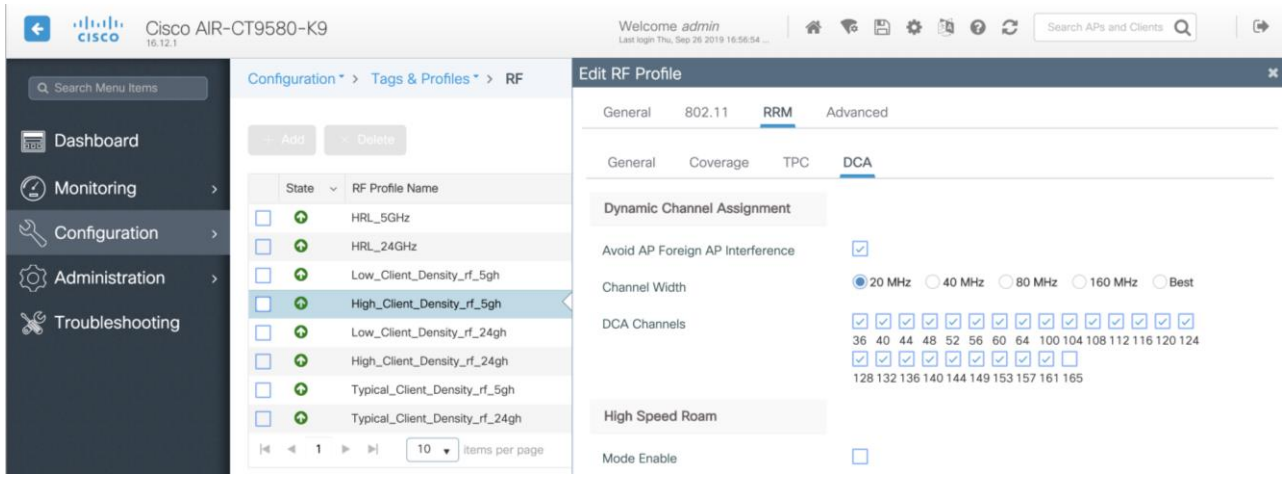
6GHz Predictive Planning
AP Channel Config Export

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

More info: Cisco Live US 2022 – BRKEWN-3006

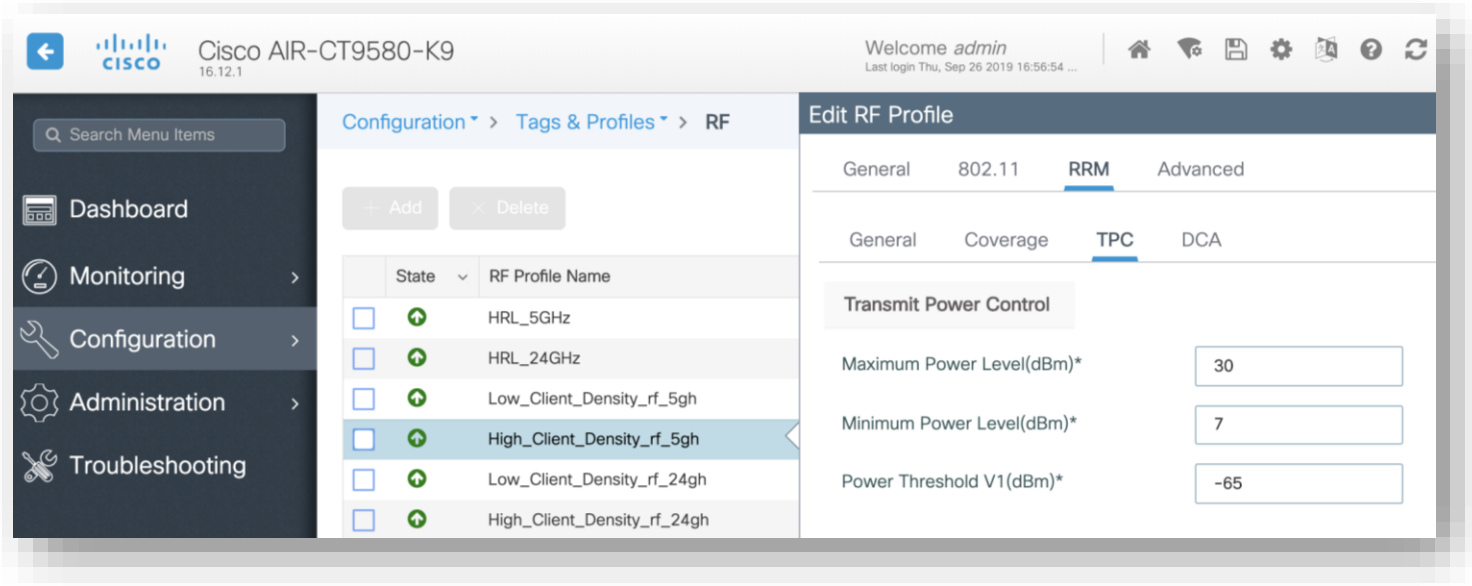
Channel Planning with RF Profiles

- 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

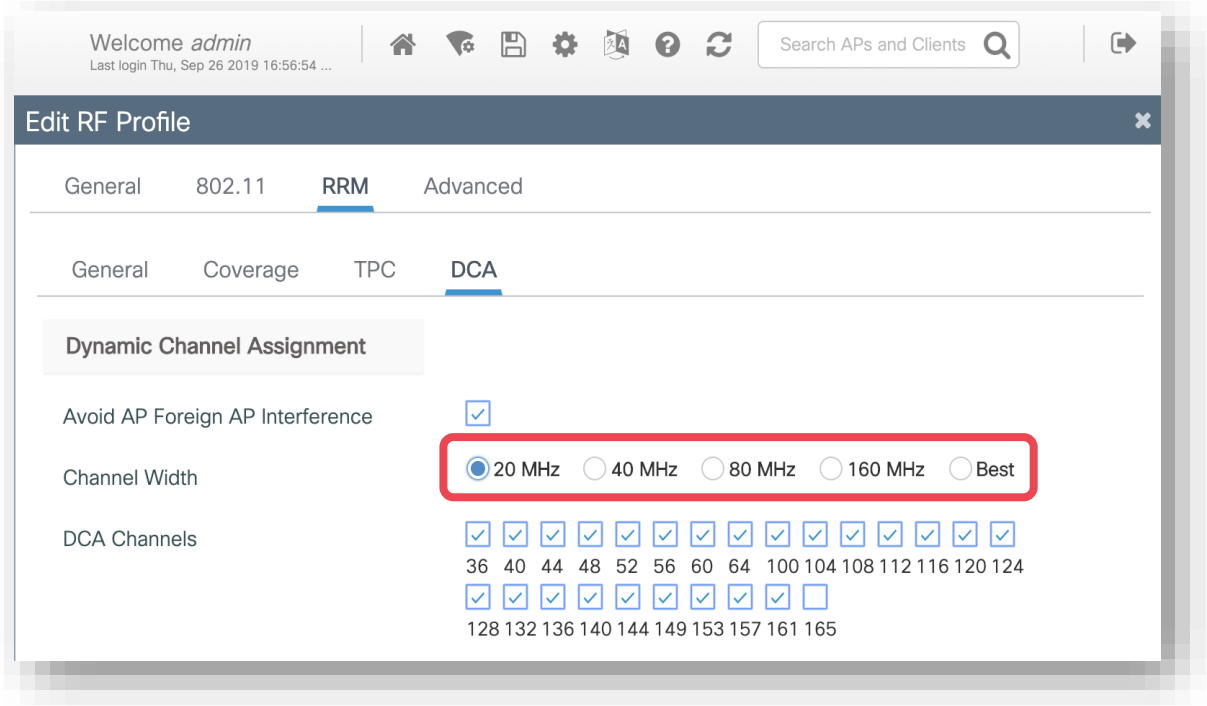


Balancing Transmit Power with RF Profiles

- **Ensures AP-to-AP consistency** (no “client magnets”) and 2.4GHz to 5GHz/6GHz balance (5GHz/6GHz 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.

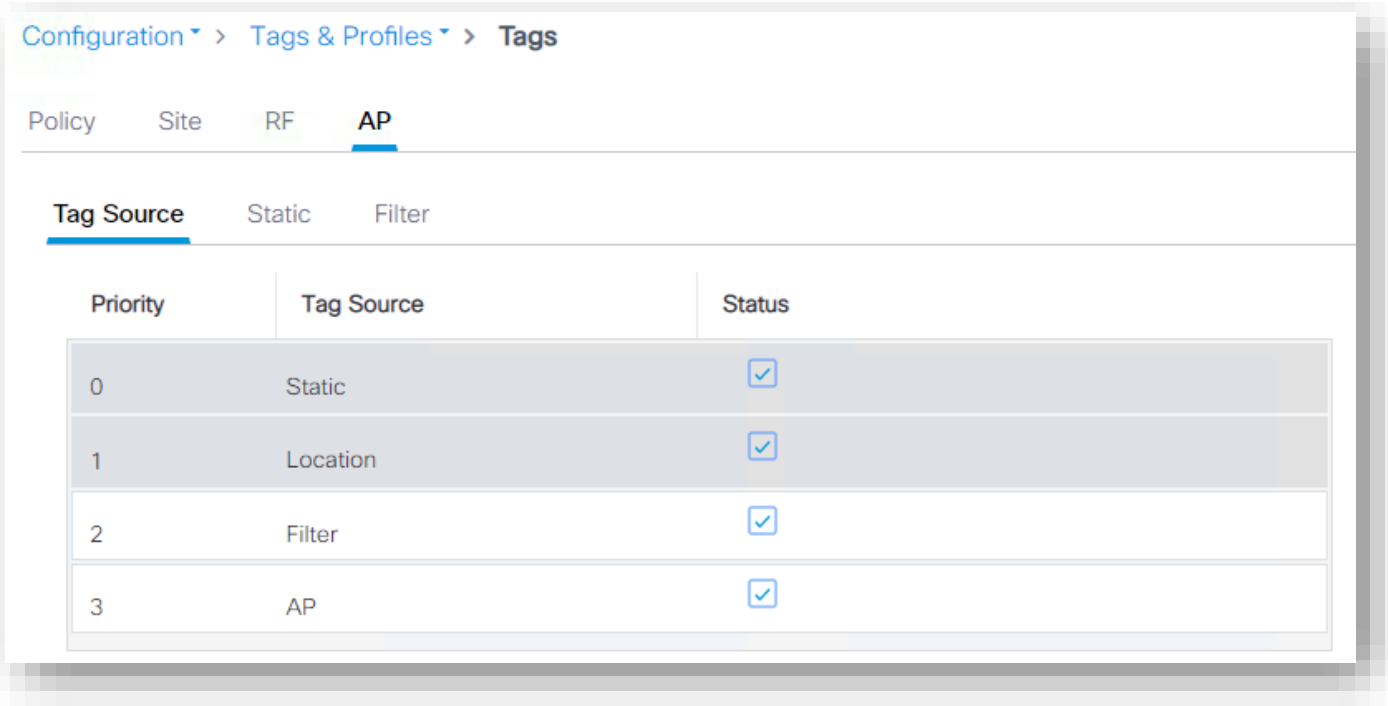
6GHz

- 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:

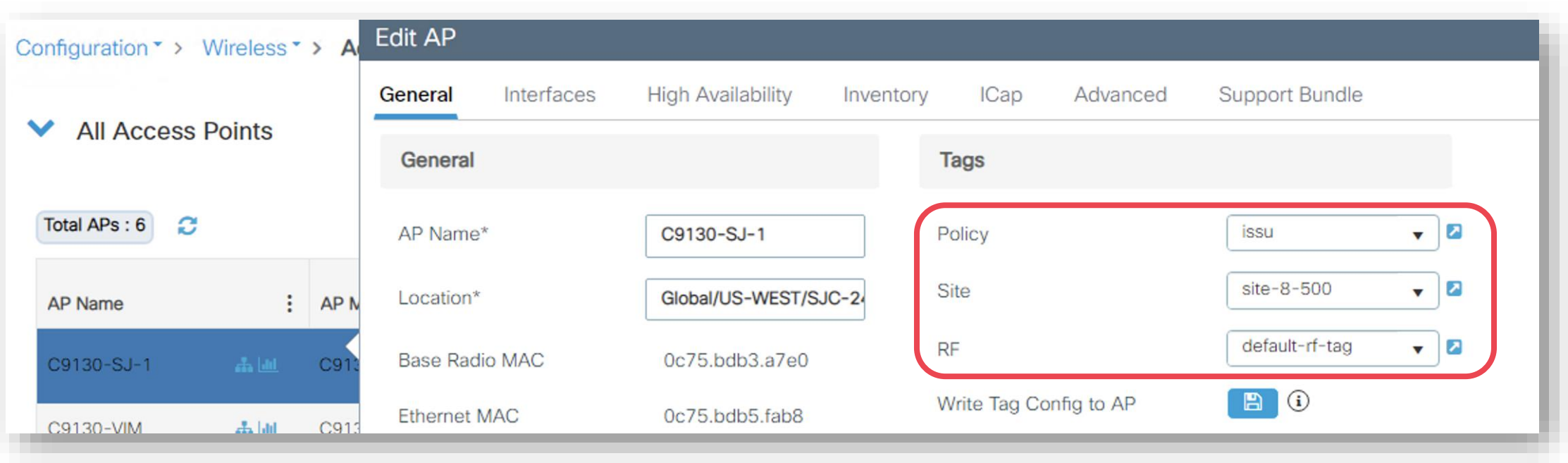


- Static: admin configuration
- Location: Basic Setup flow
- Filter: regular expression
- AP: the tags are saved on AP

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

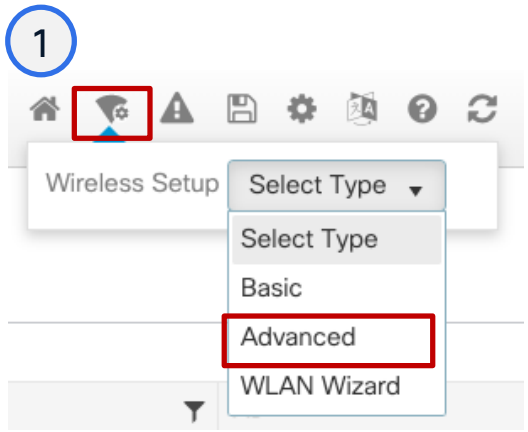
AP to Tags assignment – Source: Static

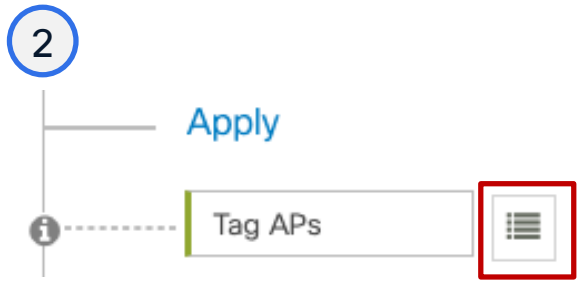
- The static Tag <> AP binding is based on AP's Ethernet MAC and it's a configuration on the Controller: upon joining the C9800, the configuration is applied, and the AP gets assigned to the selected tags
- Go to Configuration > Wireless > Access Points

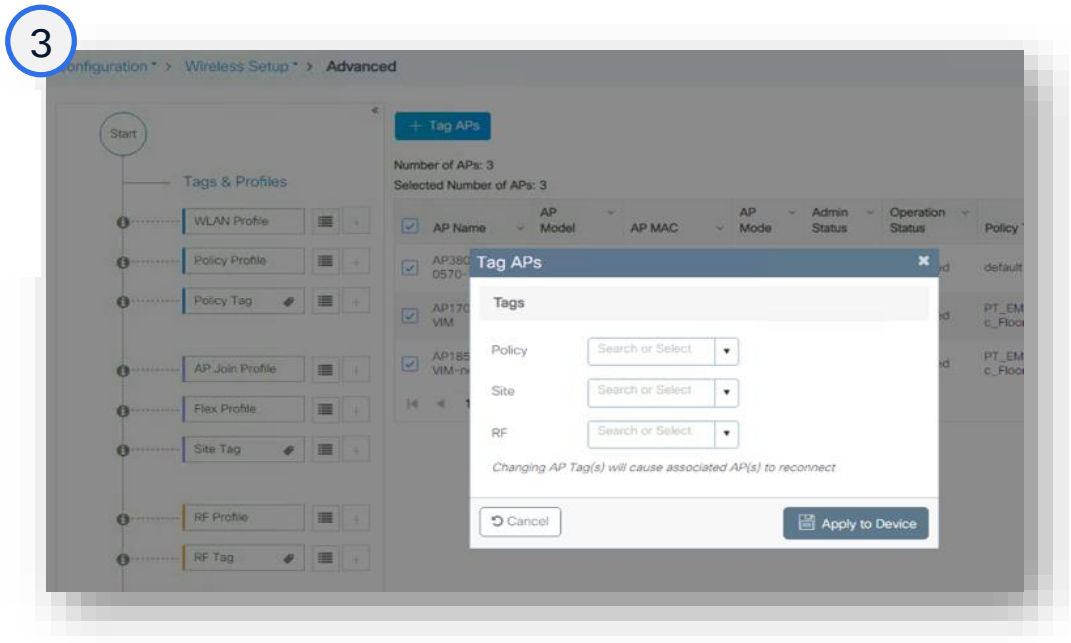


AP to Tags assignment – Source: Static

- To statically assign Tags to multiple APs, you can use the Advanced Wireless Setup > Click on Start Now and select "Tag APs" and select the APs you wish to map:

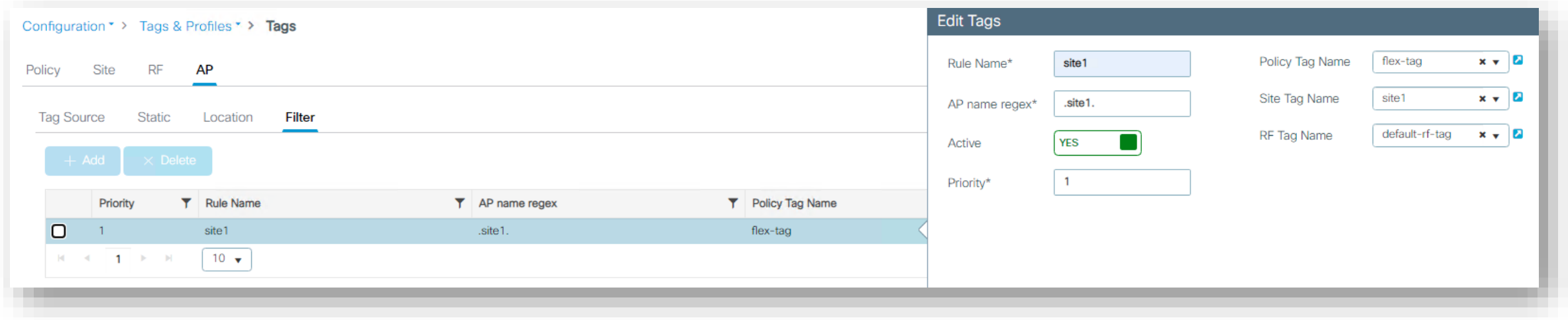






AP to Tags assignment – Source: Filter

- 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)

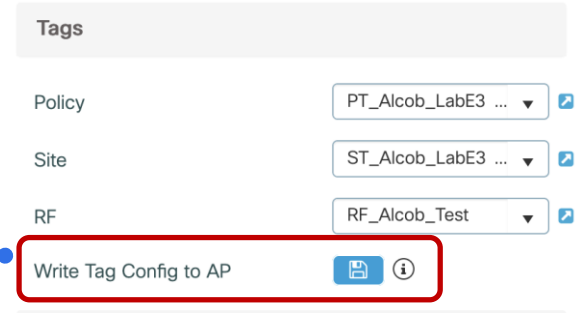
CAPWAP = Control and Provisioning of Wireless Access Points

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
```

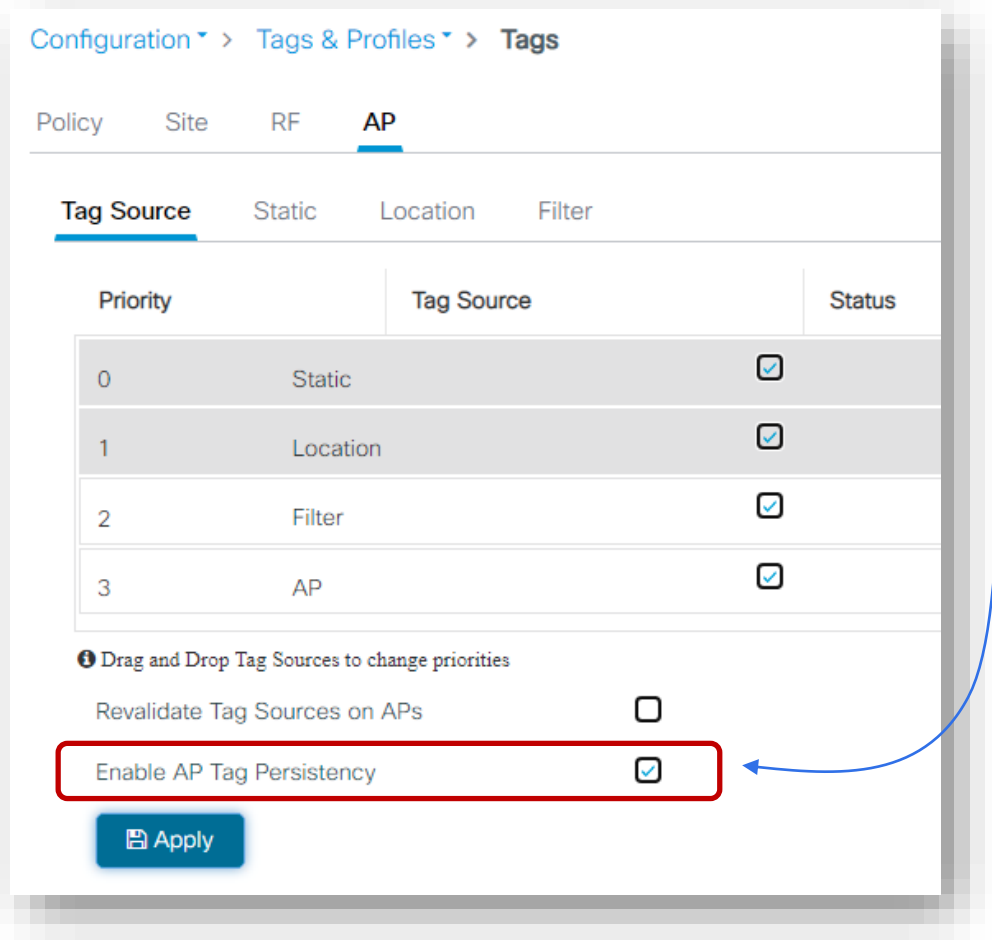
- Using the CLI command could be cumbersome, we have solutions:
  - Event Manager Script (useful for 17.3.x release)
  - Graphical user interface (GUI) settings in 17.4.1 and later
  - Starting 17.6 new feature called AP Tag Persistency



AP to Tags assignment – AP

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

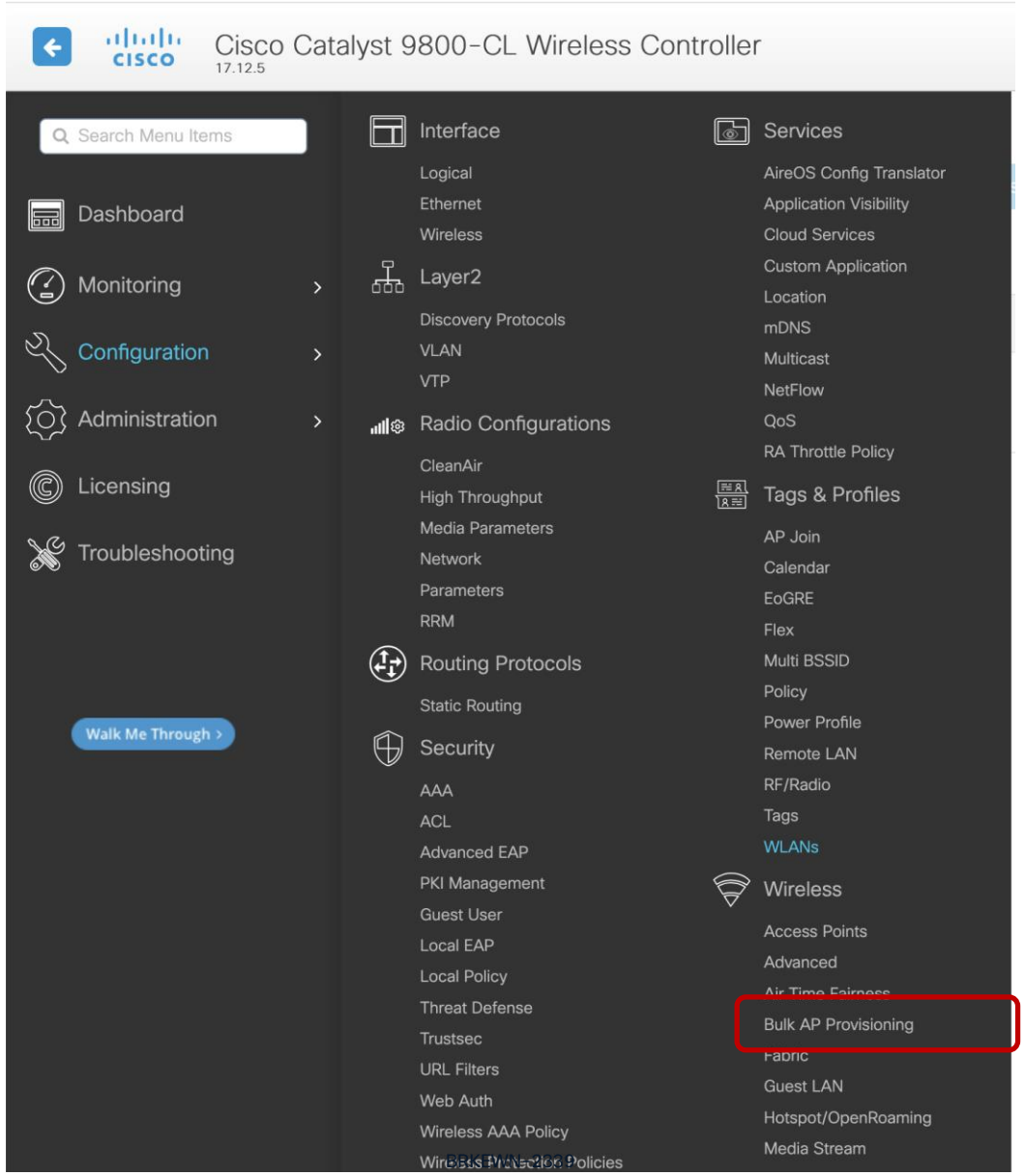
- Run the show command below:

```
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

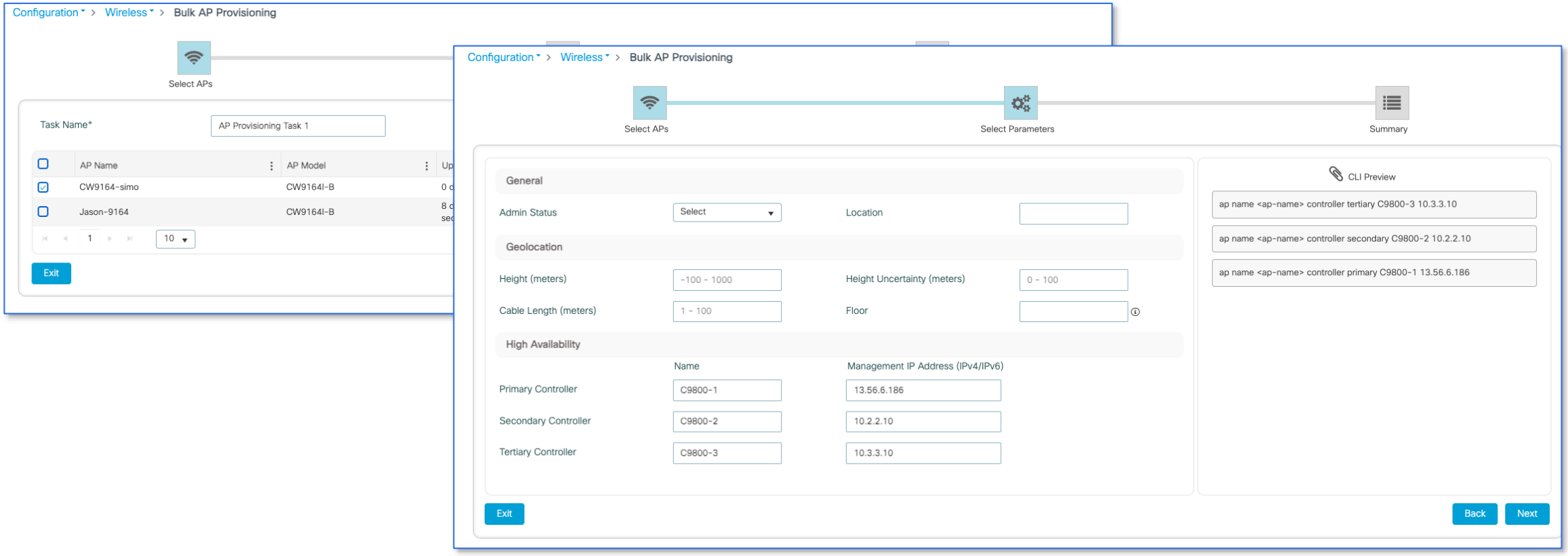
AP Bulk Provisioning



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



Agenda

Day 0

01 C9800 Design and Deployment

02 Wi-Fi 6E/7 Migration Best Practices

Day 1

03 **WLAN Configuration**

04 **Site Tag and WNCd Load Balancing**

05 **RF Tag Recommendations**

Day 2

06 RF Monitoring

07 Optimization

08 Software Upgrades

Agenda

Day 0

01 C9800 Design and Deployment

02 Wi-Fi 6E/7 Migration Best Practices

Day 1

03 WLAN Configuration

04 Site Tag and WNCd Load Balancing

05 RF Tag Recommendations

Day 2

06 **RF Monitoring**

07 **Optimization**

08 **Software Upgrades**

Day 2

AI-Enhanced RRM

AI-Enhanced RRM key customer benefits

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.

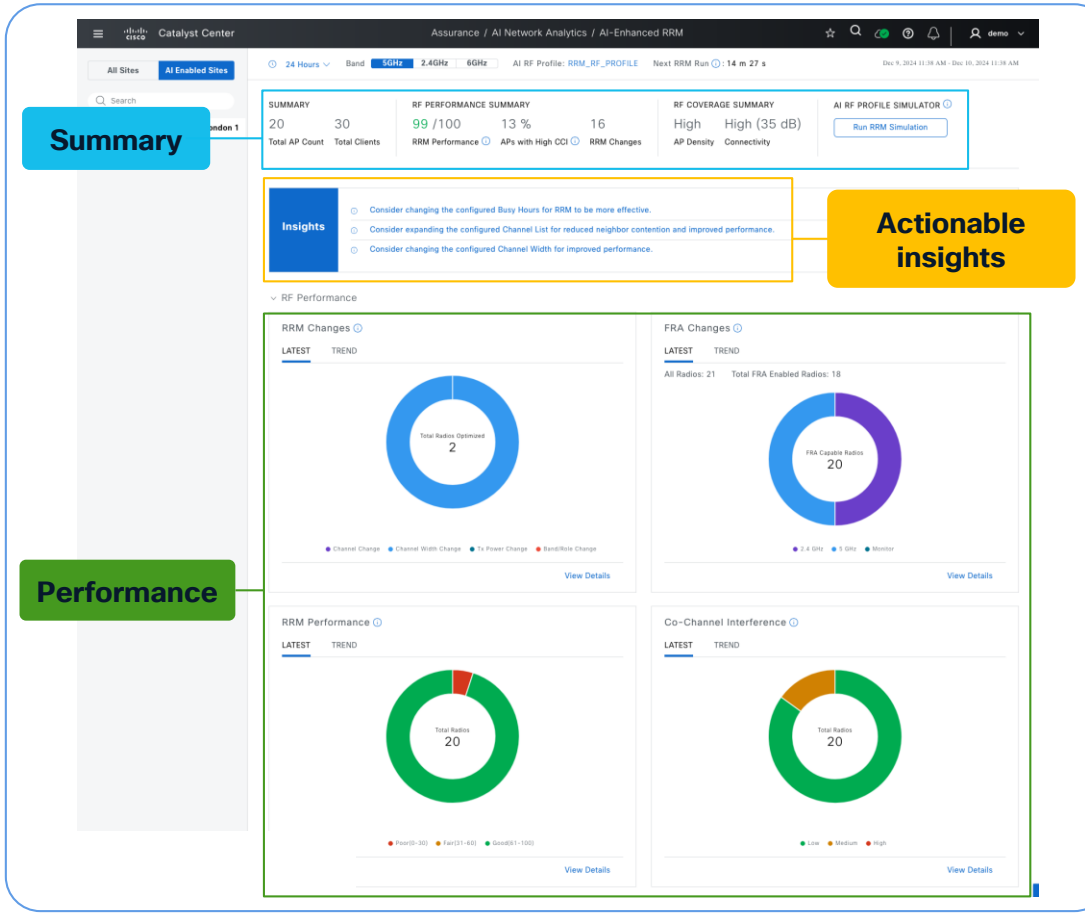
Simplified RRM configuration

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

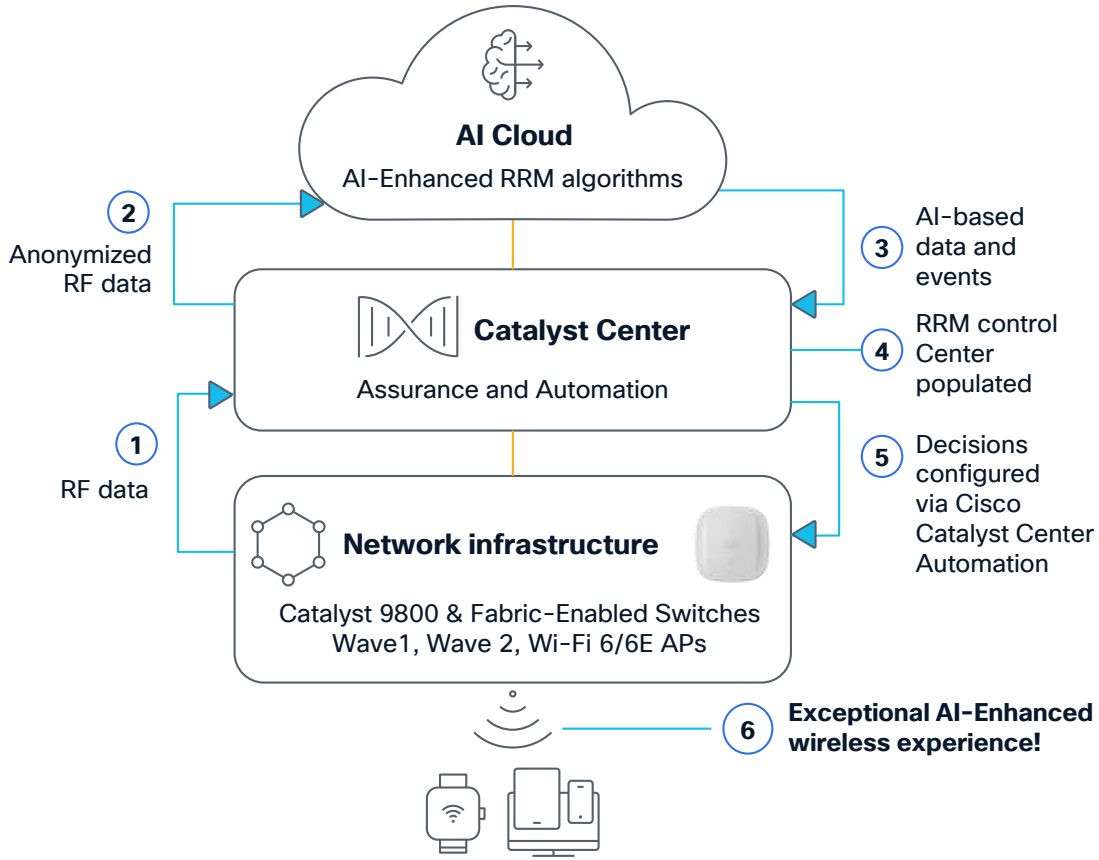
AI-Enhanced RRM is AI that Powers RF Optimization

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

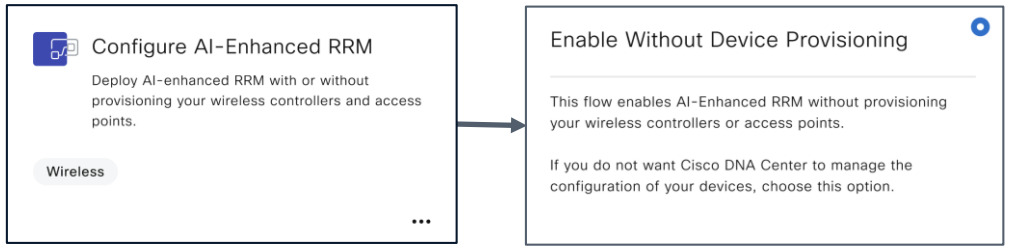
Instantaneous visibility



Proactive optimizations



What mitigates these pain points?



New AI-Enhanced RRM Workflow for Assurance Only Customers!

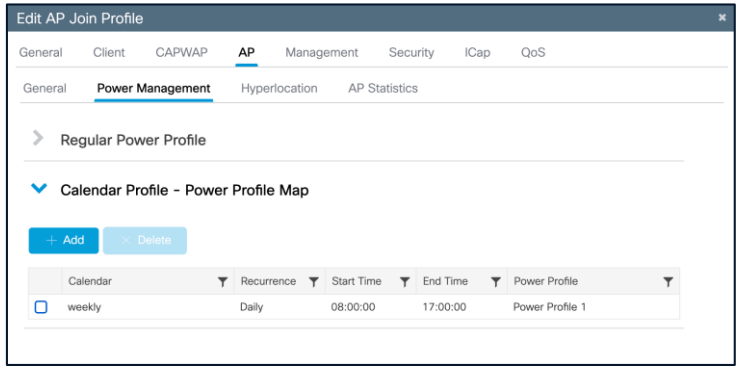
AP Power Optimization

AP Power Optimizations Feature Suite

Save Power, Reallocate Power, and Visibility into Savings

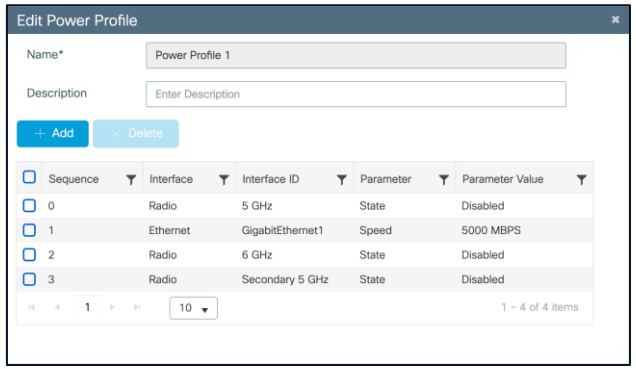
AP Power Save Mode
Lower AP Power Usage

- 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.



AP Power Distribution
Control over how power is used

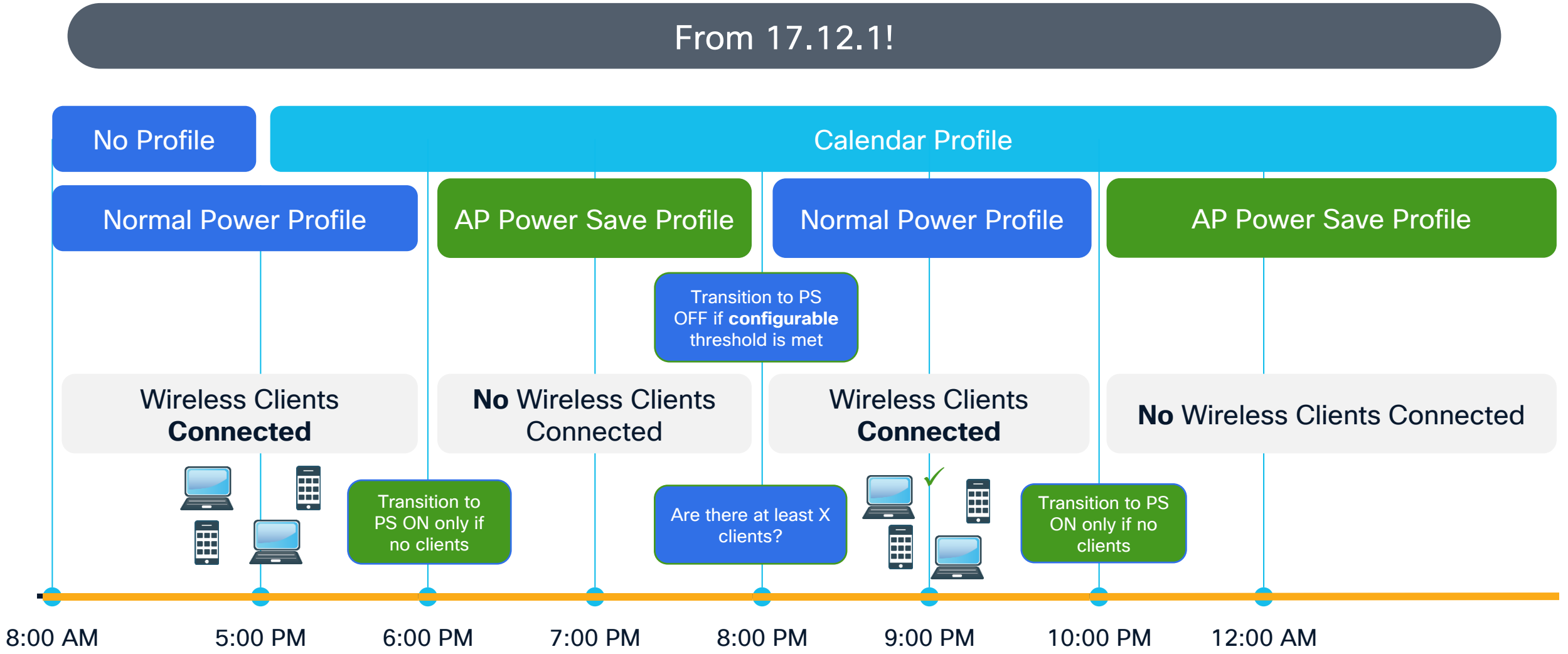
- Reallocate extra AP Power to different radios while operating on PoE+ (30W).
- Customization of your PoE power budget.
- Example: Disable 2.4 GHz radio -> use extra power for 6 GHz radio.



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.

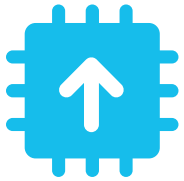
Catalyst AP Power Save (PS): Client logic change



CleanAir Pro™

Introducing Cisco CleanAir Pro™

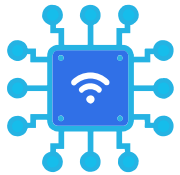
15 years of innovations and excellence carried forward



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

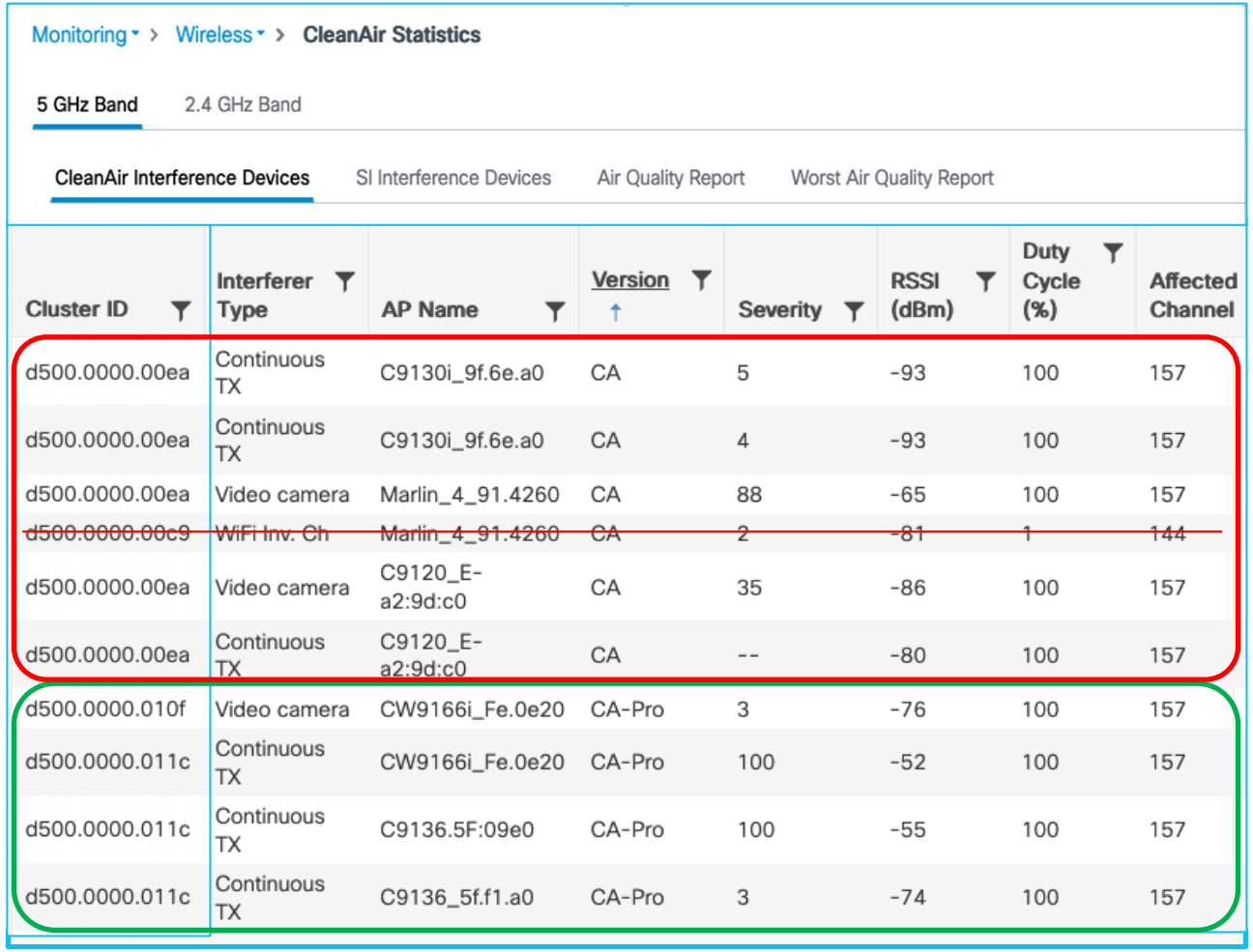
CleanAir Pro™ ML Based Classification

- 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

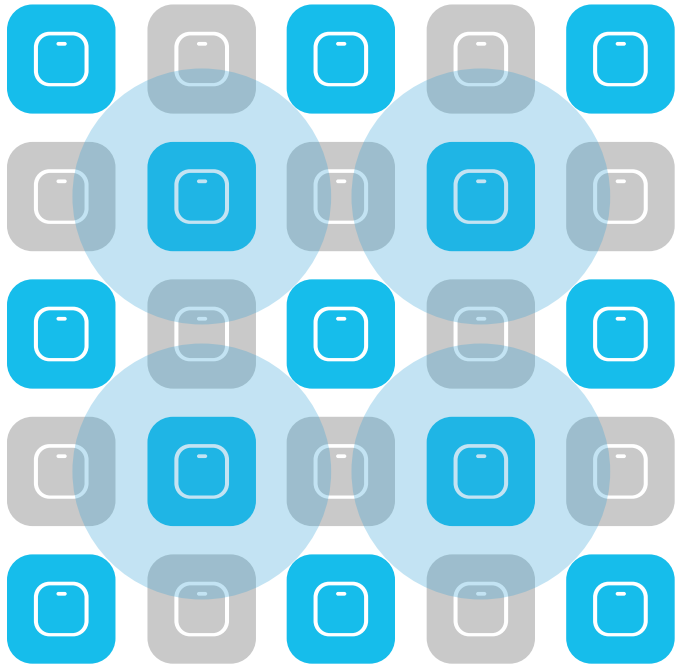


Cluster ID	Interferer Type	AP Name	Version	Severity	RSSI (dBm)	Duty Cycle (%)	Affected Channel
d500.0000.00ea	Continuous TX	C9130i_9f.6e.a0	CA	5	-93	100	157
d500.0000.00ea	Continuous TX	C9130i_9f.6e.a0	CA	4	-93	100	157
d500.0000.00ea	Video camera	Marlin_4_91.4260	CA	88	-65	100	157
d500.0000.00c9	WiFi 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



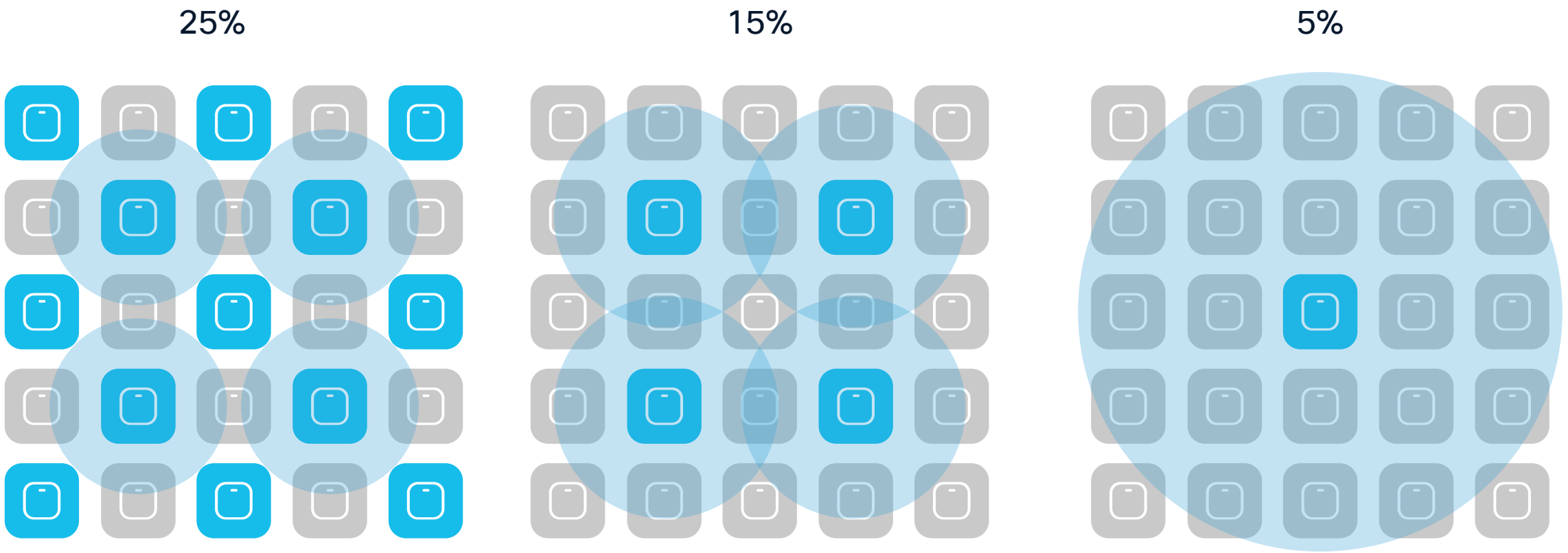
How does it work?

- 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

What can it be used for?

- APSP installation
- With N+1 Hitless upgrade
- With ISSU in HA SSO

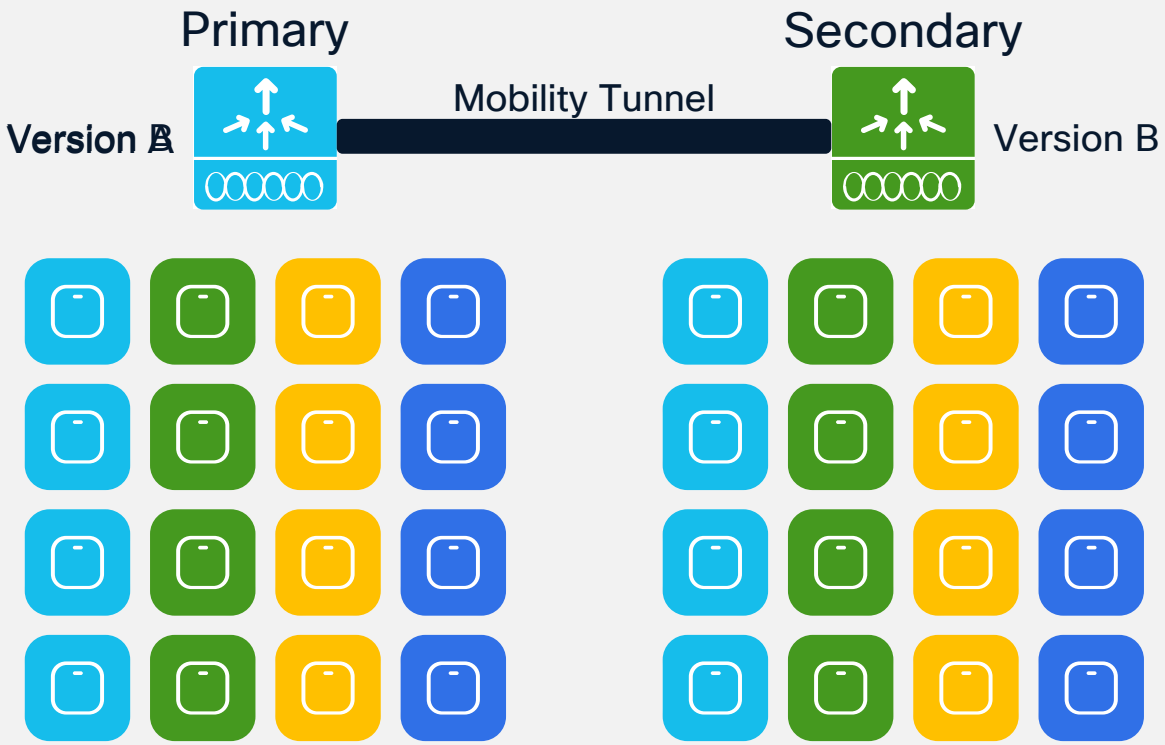
Rolling AP Upgrade: Neighbor AP marking



User selects % of APs to upgrade in one go [5, 15, 25]
For 25%, Neighbors marked = 6 [Expected number of iterations ~ 5]
For 15%, Neighbors marked = 12 [Expected number of iterations ~ 12]
For 5%, Neighbors marked = 24 [Expected number of iterations ~ 22]

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

AP upgrade workflow

Site Filter

Site 1

Site 2

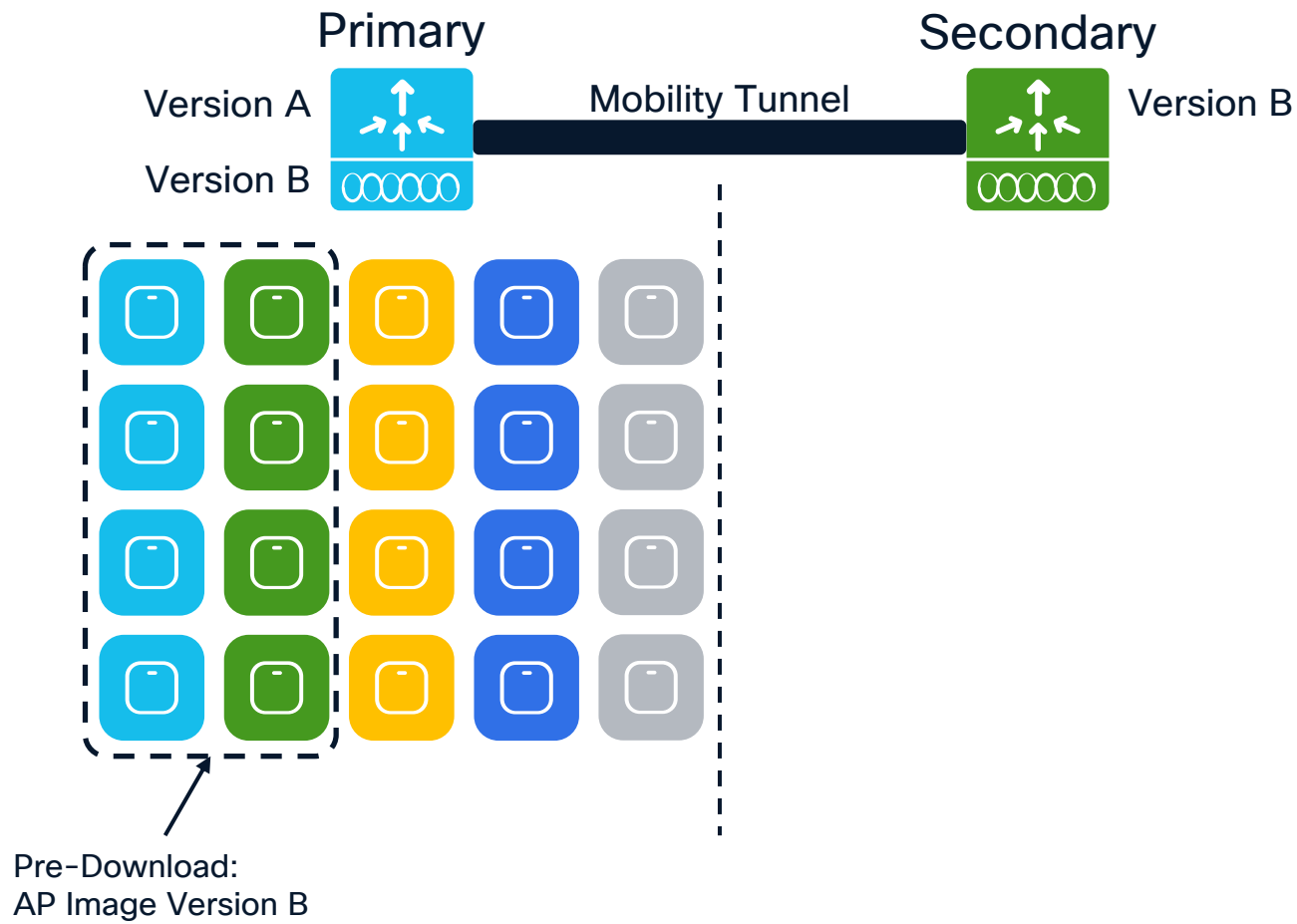
1. Add the new IOS-XE image to the controller:
   `install add file <Path to Image>`

```
install add file bootflash:IOS-VersionB.bin
```

2. Add the sites that will be upgraded first to the site filter:
   `ap image site-filter any-image add <Site Tag Name>`

```
ap image site-filter any-image add Site1
ap image site-filter any-image add Site2
```

3. Pre-download image to the APs:
   `ap image predownload`



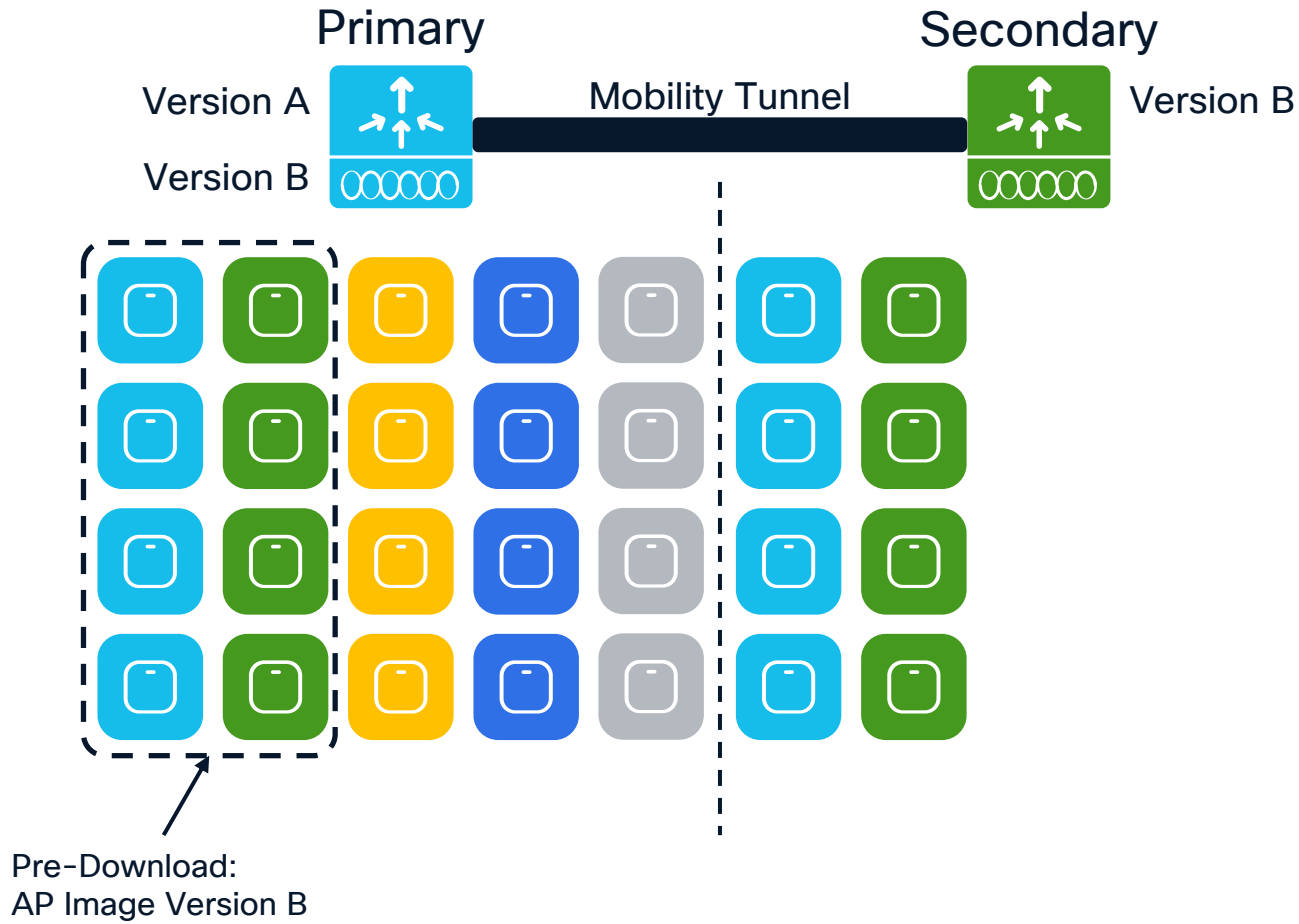
AP upgrade workflow

4 Move APs to the new destination WLC:
ap image upgrade destination <Destination WLC Name> <Destination WLC IP>

```
ap image upgrade destination Secondary-WLC 10.10.110.4
```

5 APs will reload with the new image and join the Secondary WLC on a rolling basis

6 As the APs successfully join the Secondary WLC, the Secondary will update the Primary WLC.



AP upgrade workflow

Site Filter

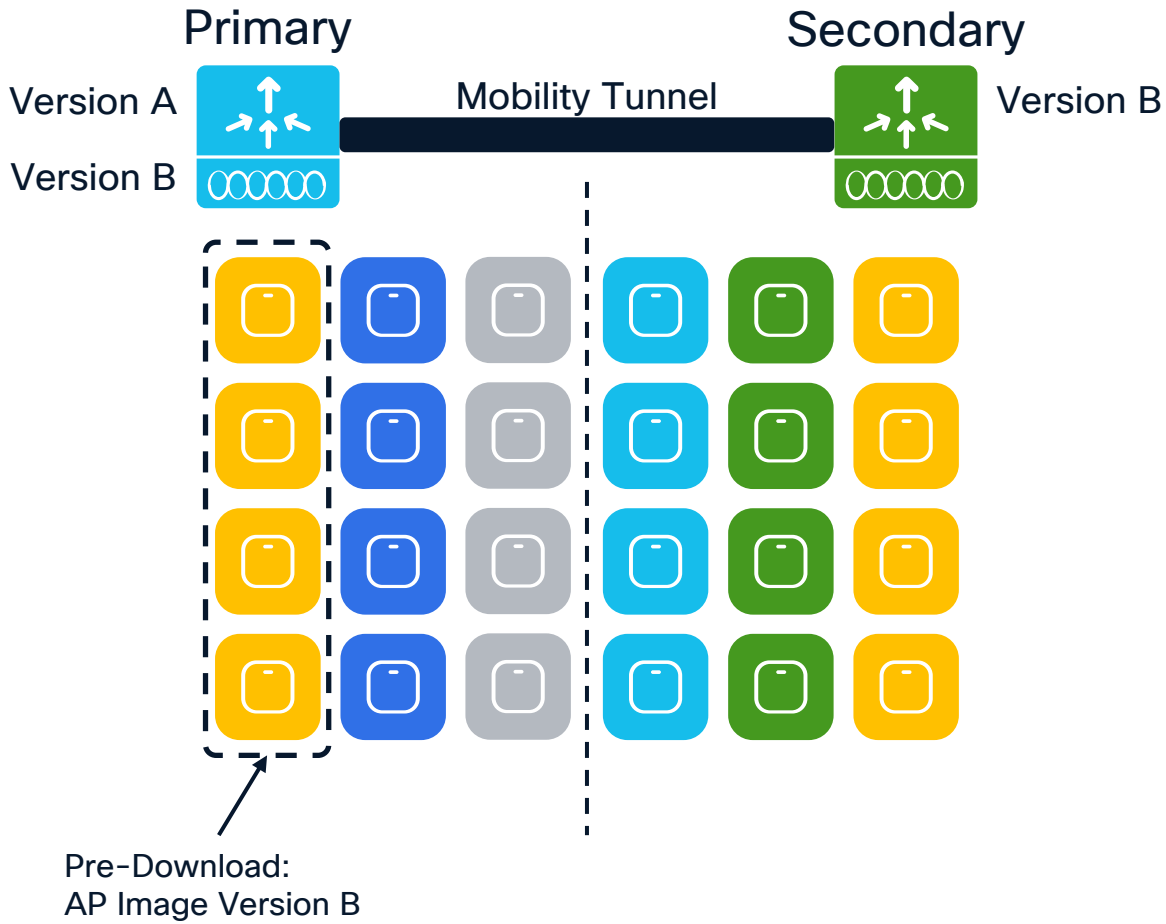
- Site 1
- Site 2
- Site 3

7 Add further sites to the site filter:
ap image site-filter any-image add <Site Tag Name>

```
ap image site-filter any-image add Site3
```

8 Initiate the AP image pre-download, reload with the new image, and join to the Secondary WLC in rolling fashion:
ap image site-filter any-image apply

9 As the APs successfully join the Secondary WLC, the Secondary will update the Primary WLC.



AP upgrade workflow

Site Filter

Site 1

Site 2

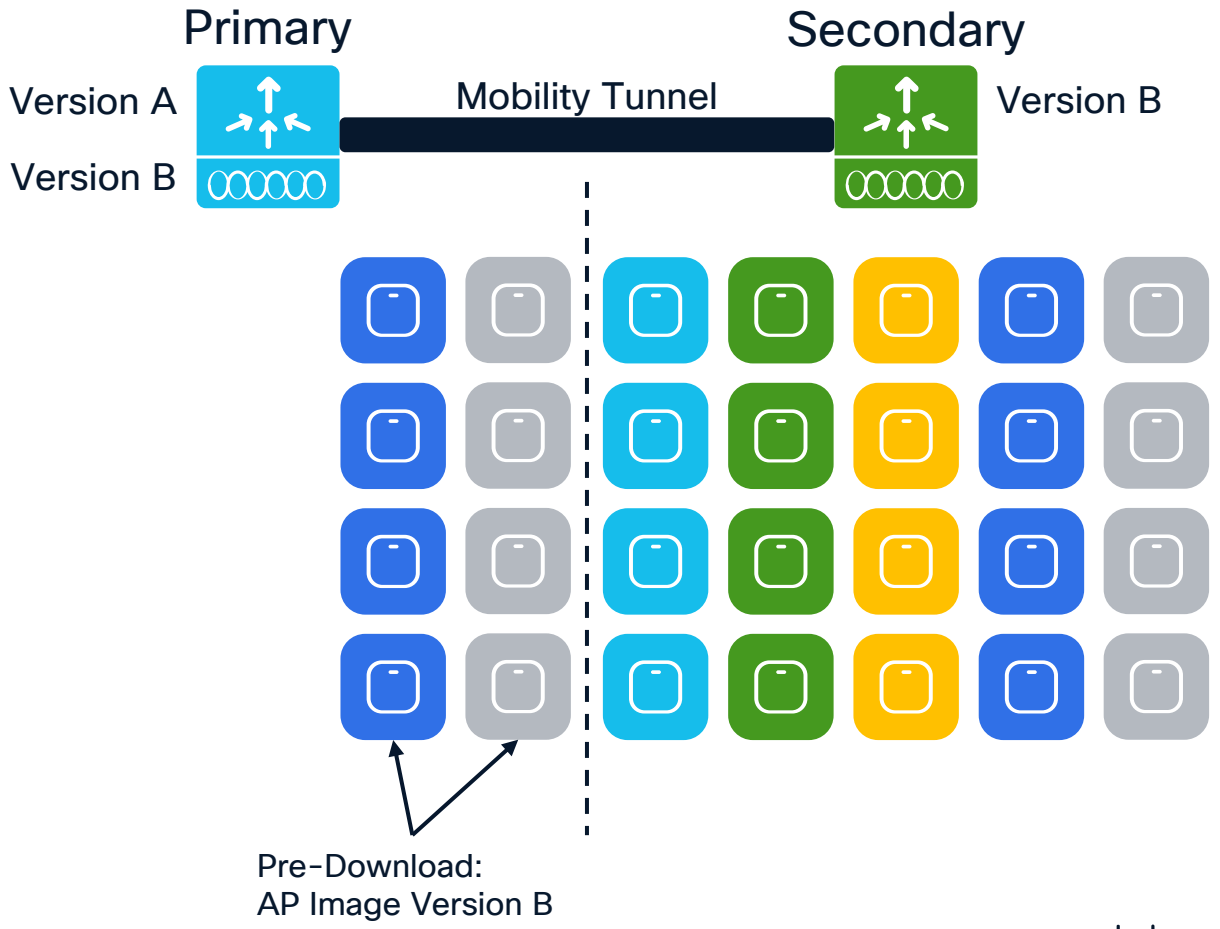
Site 3

10 Upgrade the rest of the sites by clearing the site filter:
`ap image site-filter any-image clear`

11 APs at the remaining sites will pre-download the image, reload with the new image, and join to the Secondary WLC in rolling fashion.

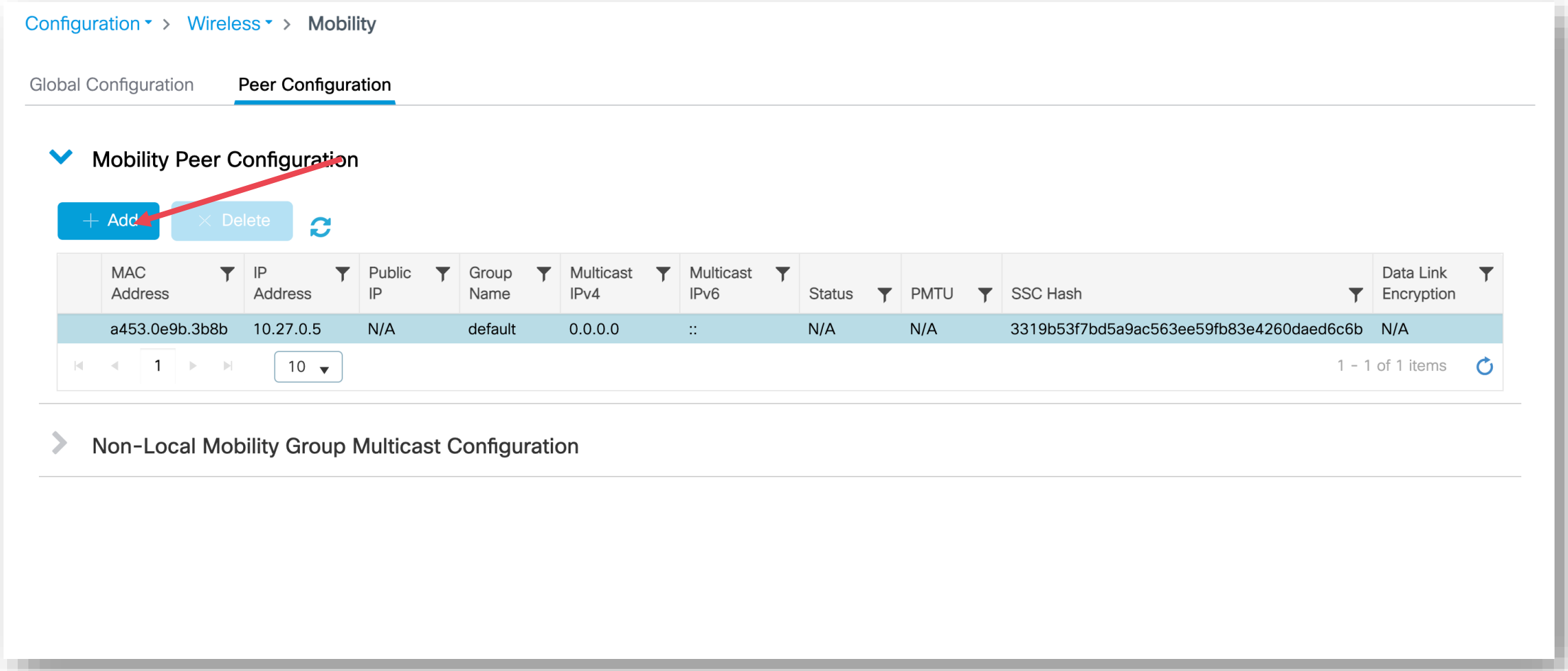
12 As the APs successfully join the Secondary WLC, the Secondary will update the Primary WLC.

13 Activate the new IOS XE image on the Primary WLC.



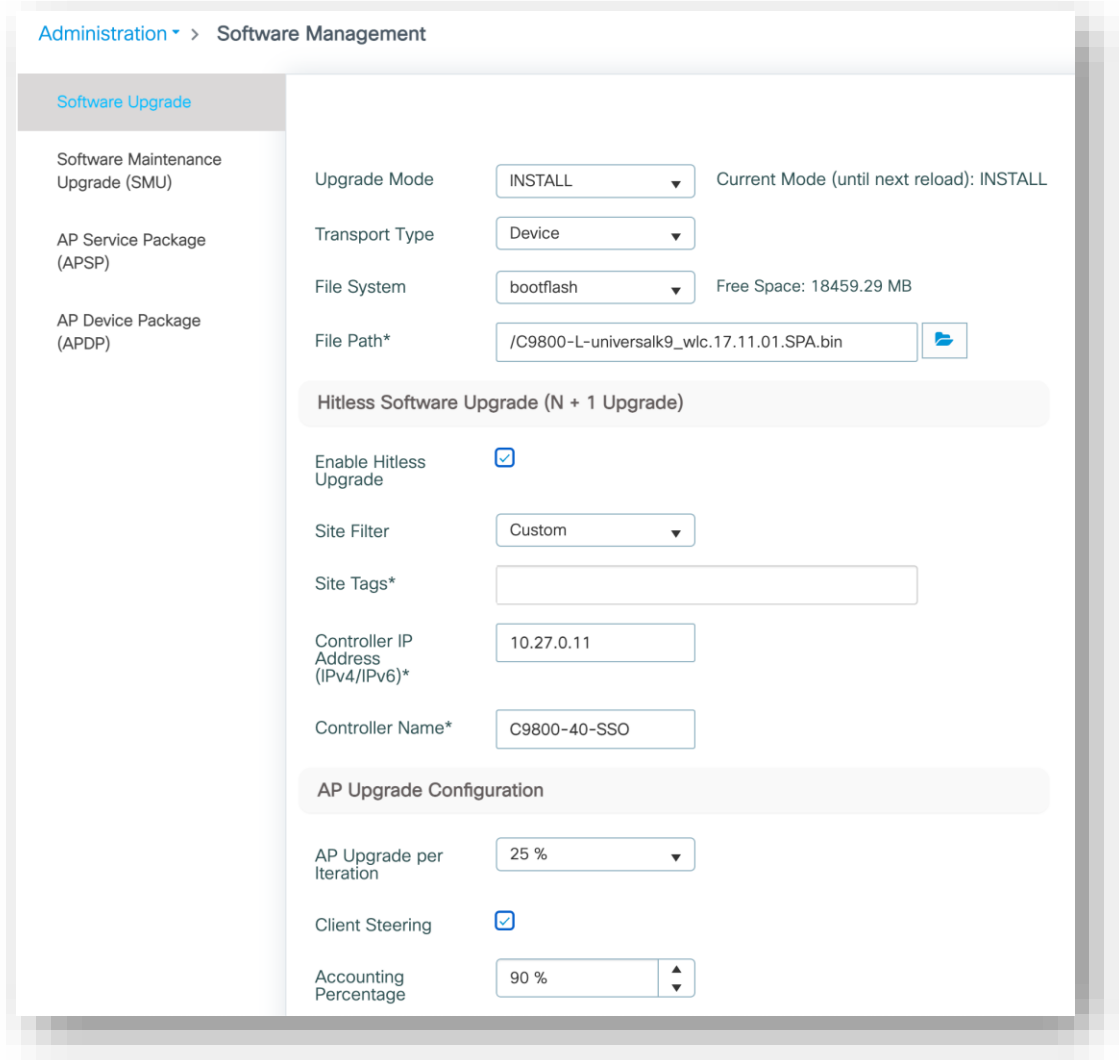
Configuration via WebUI Mobility Tunnel

For your reference



N+1 Site Based Hitless Upgrade with WebUI

For your reference



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

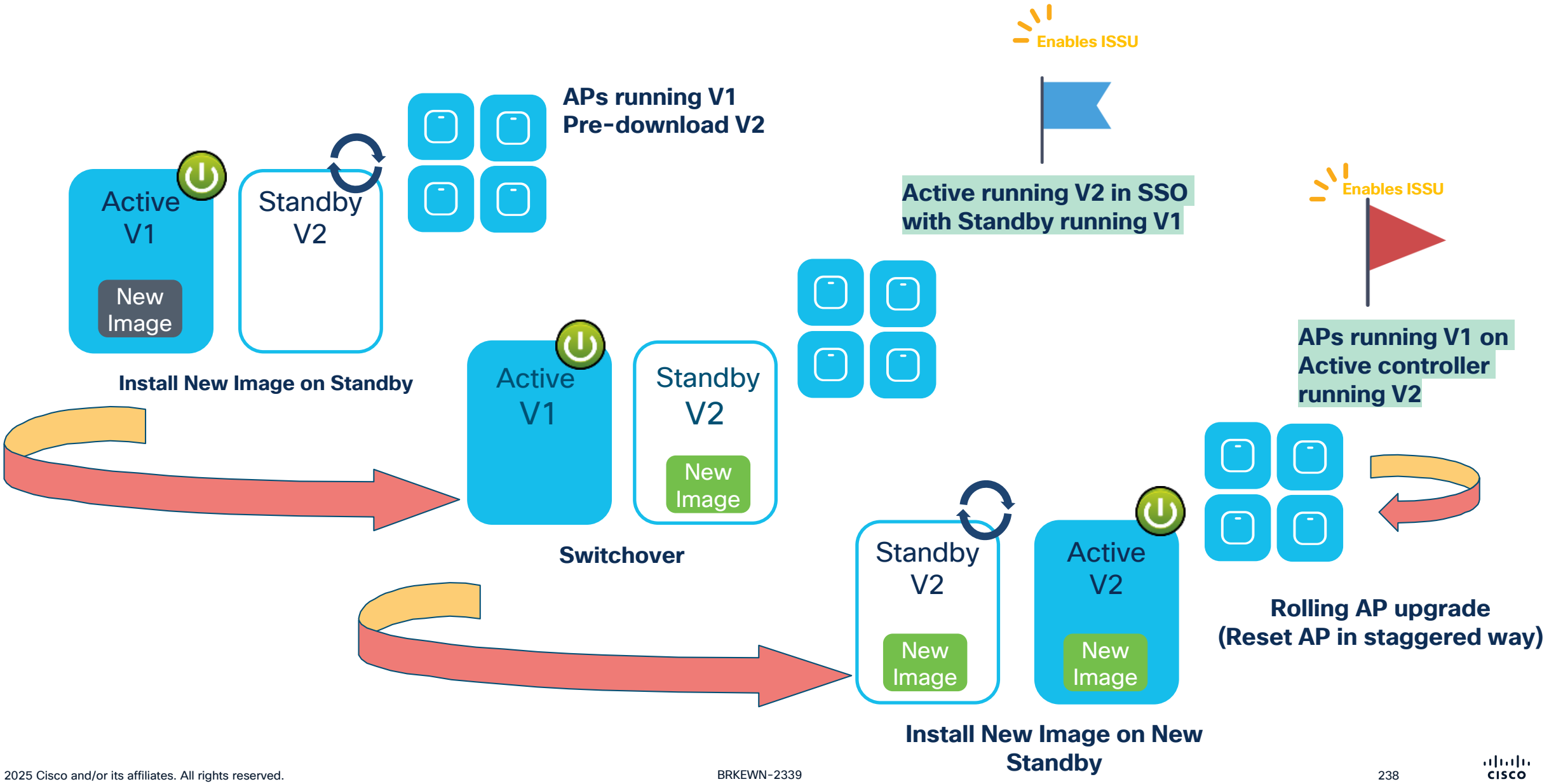
What is ISSU ?

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

All AP/Client sessions are retained during upgrade process

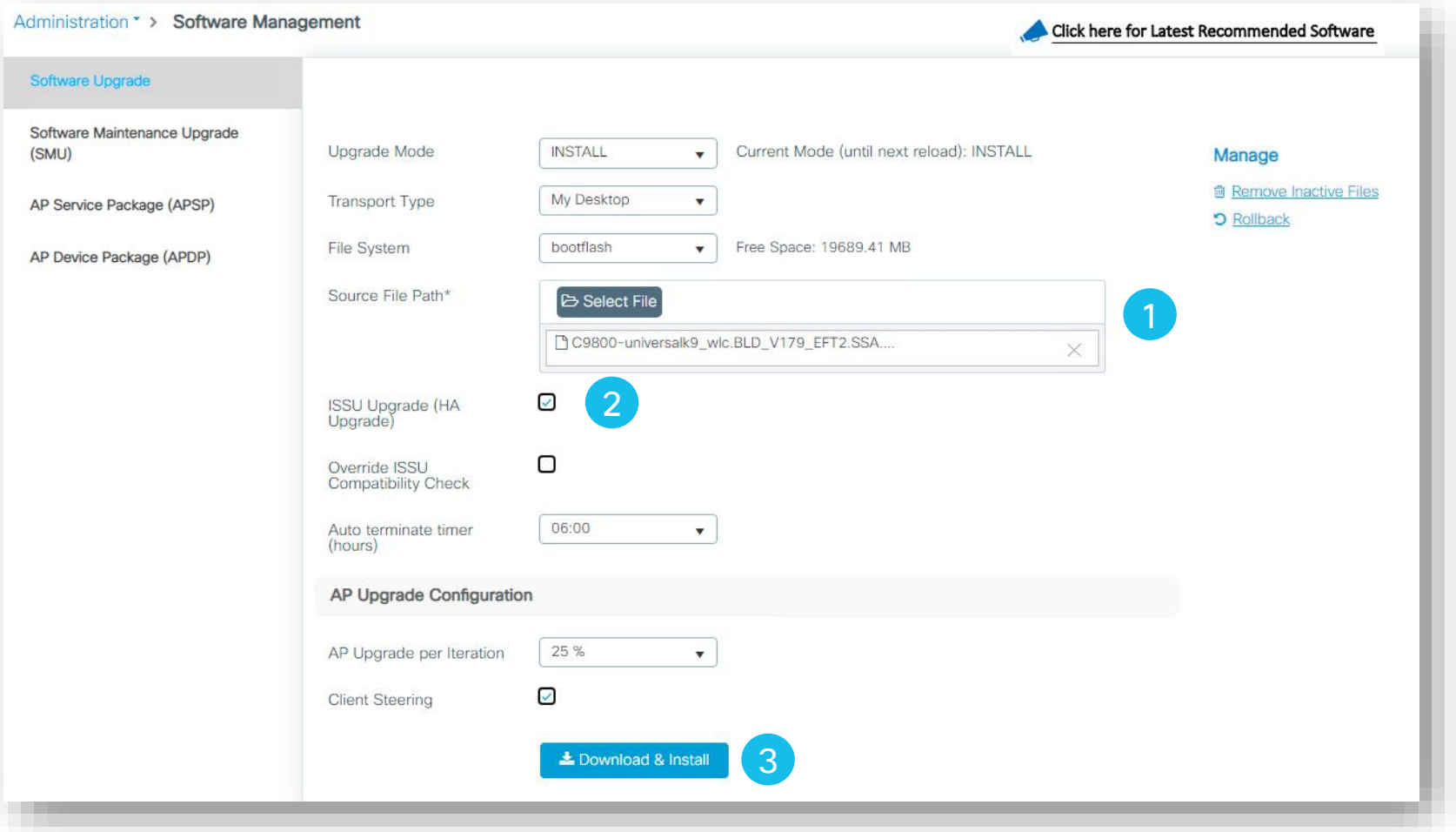
Pre-requisites:
- ✓ Base image is ISSU capable
- ✓ SSO pair in Active-Hot Standby
- ✓ Controllers in INSTALL mode

ISSU process



Easy ISSU upgrade with WebUI!

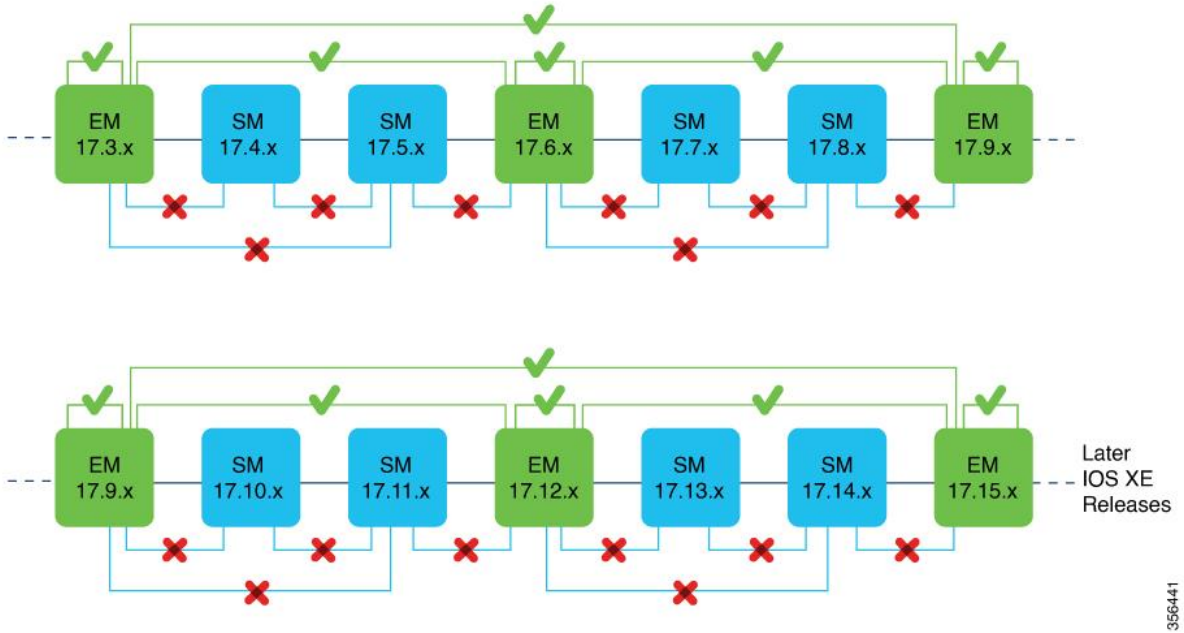
For your reference



1. Select the image you want to upgrade to
2. Enable ISSU and select % for Rolling AP upgrade
3. Click Download and Install

ISSU official support Matrix

For your reference

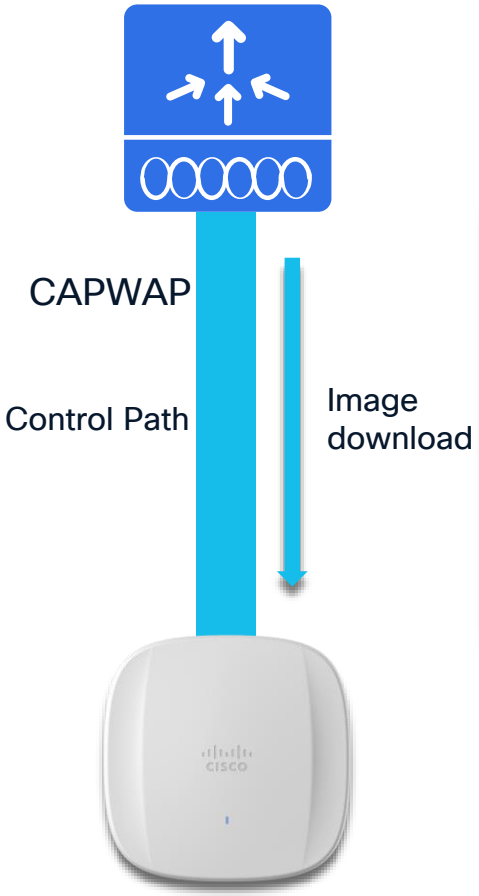


Supported	Not Supported
• N +2 – Within EM release (17.9.1 <> 17.9.3) • N +2 – Across EM release (17.3.X <> 17.9.X) ***EM*** *= Extended Maintenance release* ***SM*** *= Standard Maintenance release*	• Within EM release beyond +2 release • Across EM release beyond +2 release • Across software release trains (e.g., 17.12 to 18.1) • Within SM release (17.1.1 <> 17.1.2) • Across SM release • EM <> SM release • Downgrade from any release to any release • No support on Engineering Special (ES) releases

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_standalones/b-in-service-software-upgrade-issu.html

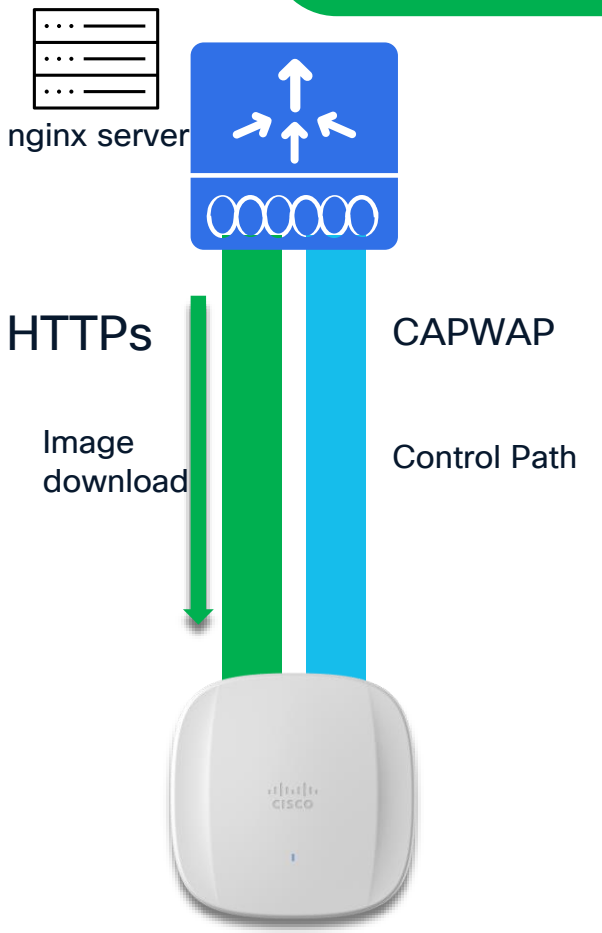
How can I improve AP image download time?

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

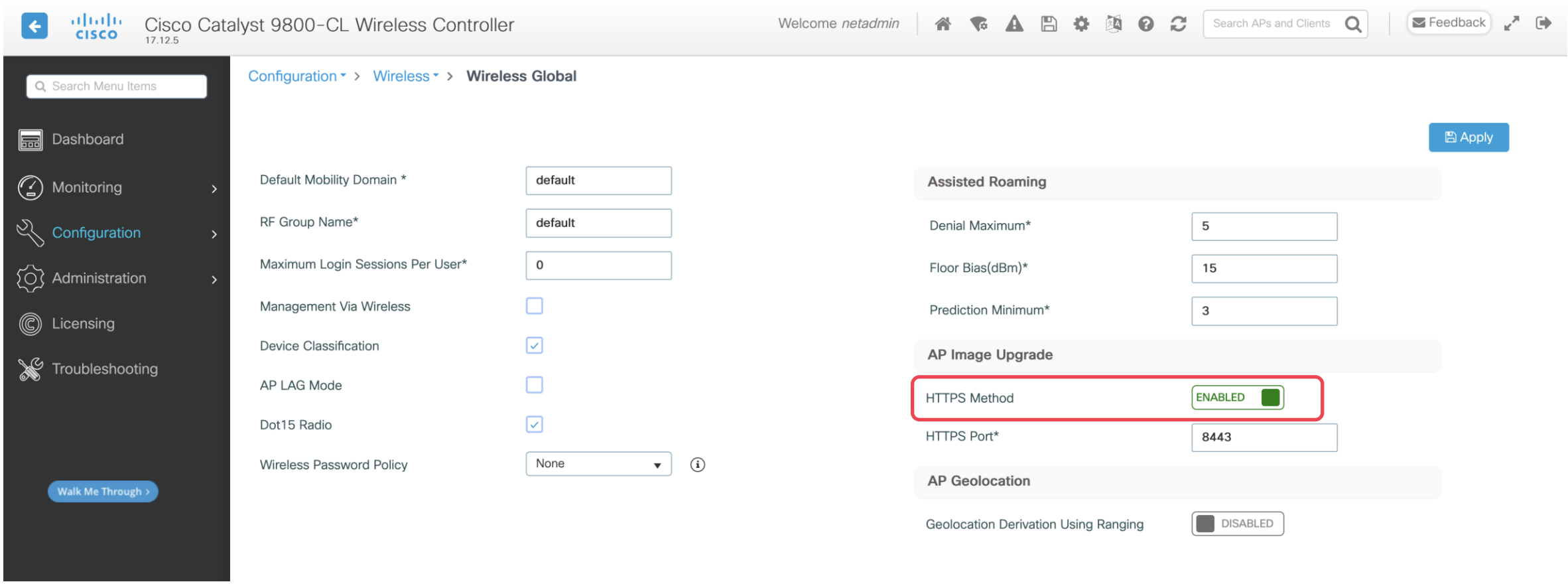


- AP image download happens over HTTPs
- Fast download speed
- Reduce CPU load and frees up CAPWAP

Efficient AP Image Upgrade

How to enable

Configuration > Wireless > Wireless Global



https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_eff_image_upgrade_ewlc.html

Wireless Controller SMU (Software Maintenance Update)

Controller Software Maintenance Upgrade (SMU)

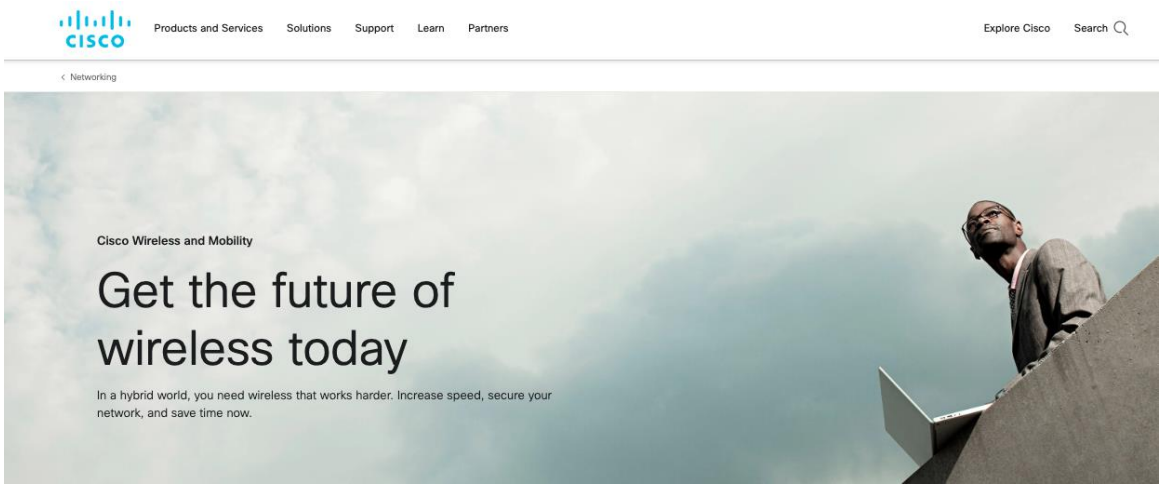
Standalone vs Redundant Wireless Controller

	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

More info?

Where can I find more info?

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



Other links on cisco.com:

- C9800 Best Practices:
  https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html
- 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

Complete your session evaluations

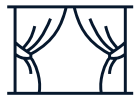
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

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

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: nfitelop@cisco.com

Thank you

cisco Live !


CISCO