The bridge to possible

Cisco Catalyst 9800 Configuration Best Practices

Justin Loo
Technical Marketing Engineer - Cisco Wireless
BRKEWN-2339

cisco Live!

#CiscoLive

Cisco Webex App

Questions?

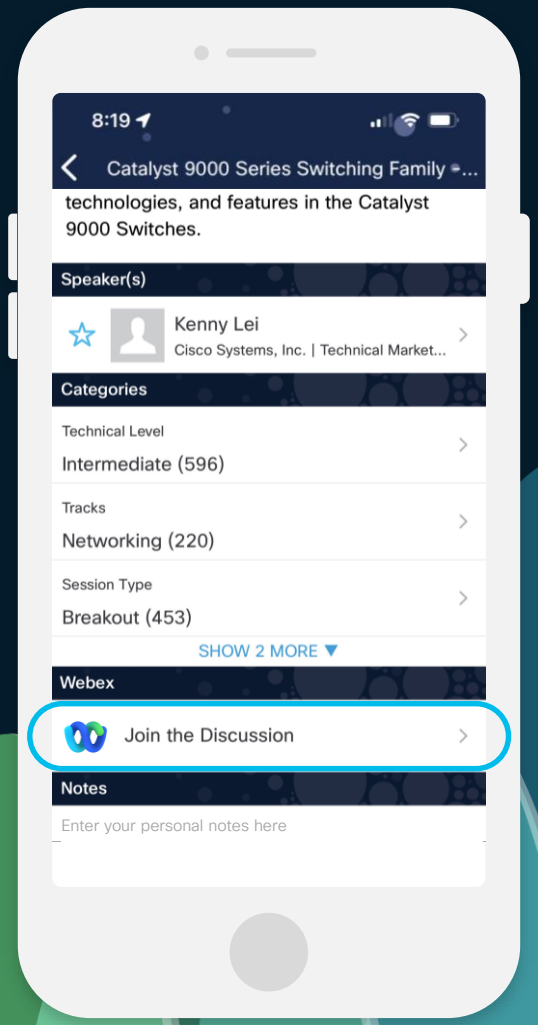
Use Cisco Webex App to chat
with the speaker after the session

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 7, 2024.

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2339



Justin Loo

Technical Marketing Engineer – Cisco Wireless

Fields of Expertise (4 Years at Cisco)

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

Personal Life

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

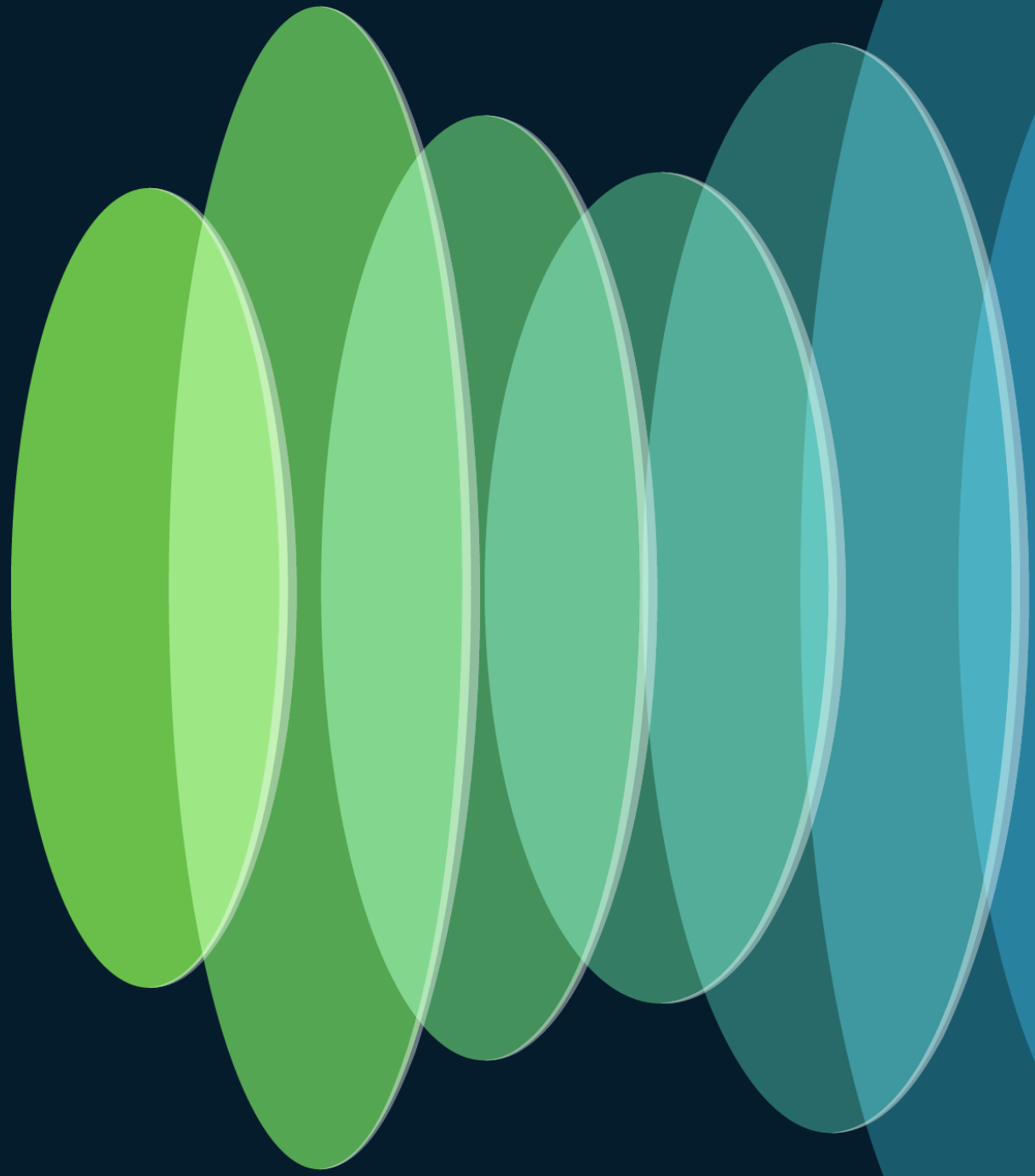
Hobbies

Traveling, Triathlon, Surfing, Trying new foods, Movies

Agenda

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

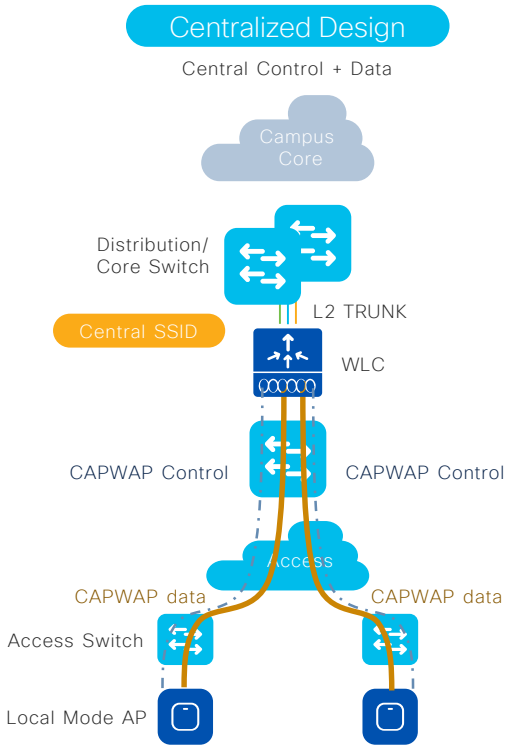
Day 0

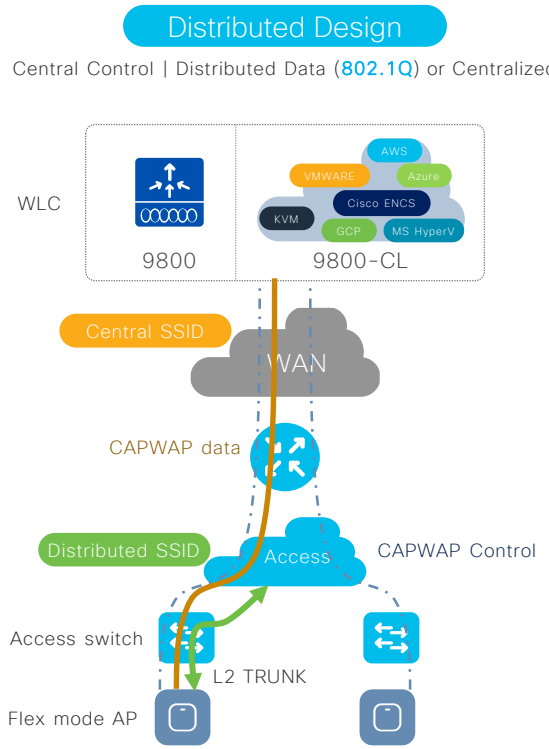


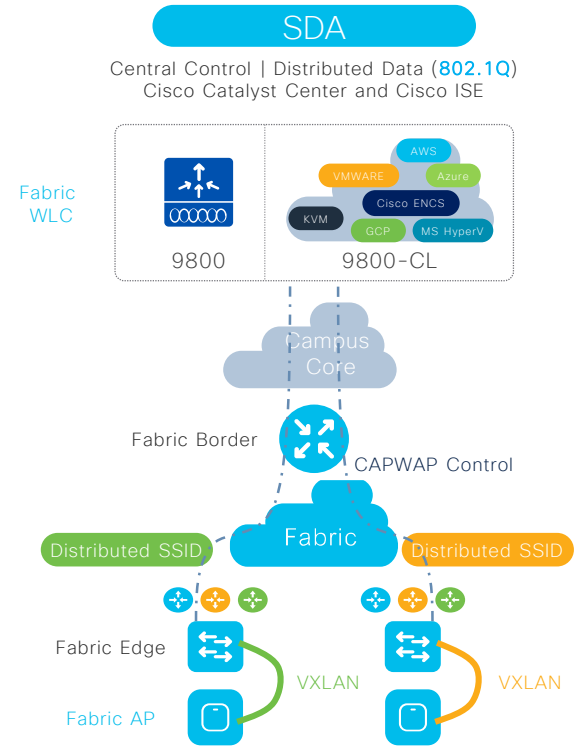
Cisco Catalyst 9800 On-Prem Deployment

cisco Live!

Wireless Deployment Options
On-Prem Design







Local mode

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

FlexConnect

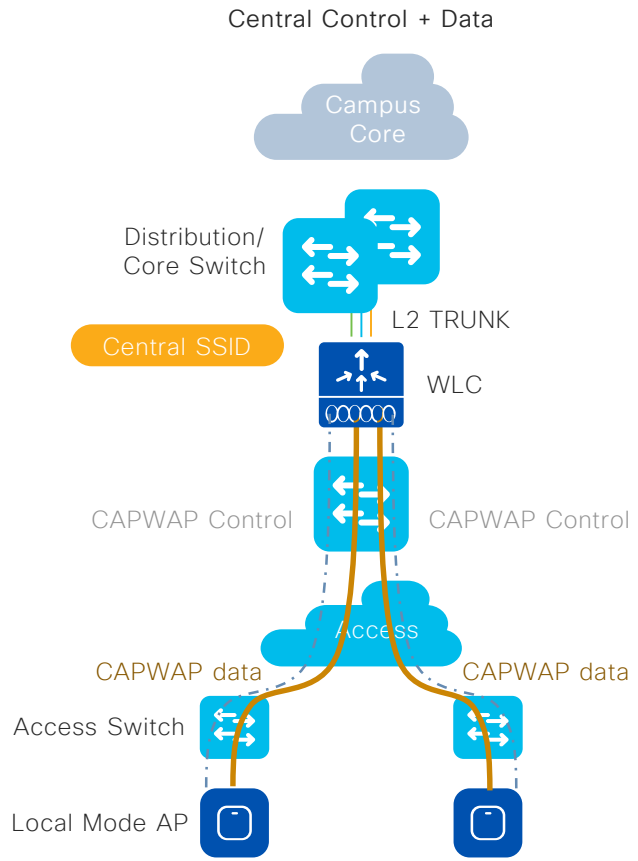
- Distributed Enterprise design choice
- APs in Flex mode, across a WAN from WLC
- Per SSID: Client traffic is distributed at AP in L2 trunk or centralized via CAPWAP
- Roaming limited to APs in a Flex domain

Software Defined Access (SDA)

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

Why Central Mode Deployment?

- **Simple IP Addressing and mobility**
  - All wireless client traffic is switched at the WLC
  - Client IP addressing & VLAN(s) defined on the WLC
  - Client Layer 3 roaming without reassigning an address
- **Single point of connection to the wired network**
  - Easier to apply security & QoS policies for wireless users
- **Simplified Overlay Design**
  - Traffic is tunnelled (using CAPWAP Protocol) from AP to WLC
  - Can be deployed on top of any wired infrastructure

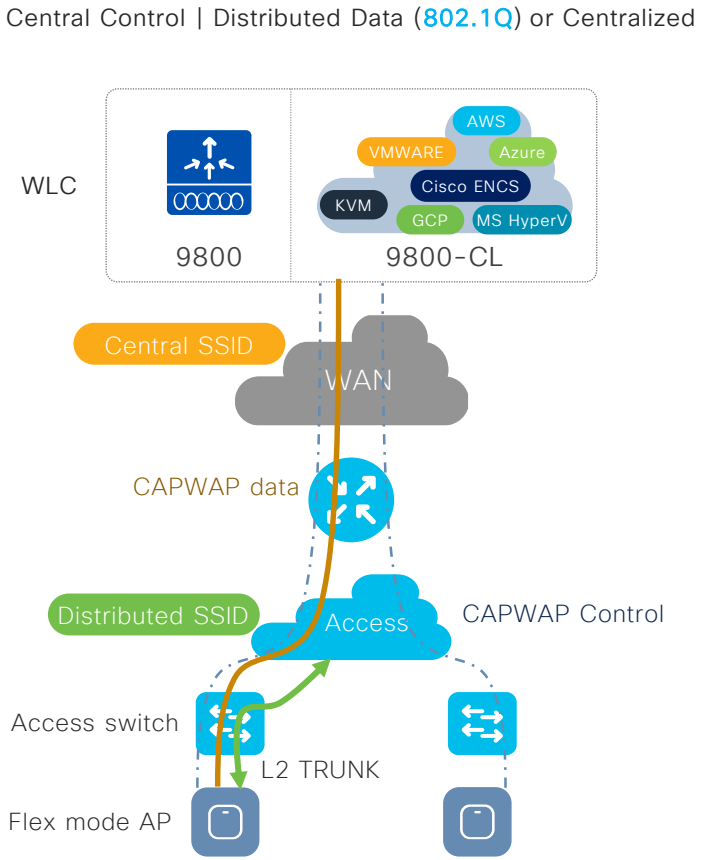


Examples –

- Enterprises
- Campus/ Universities
- Hospitals

Why FlexConnect Mode Deployment?

- **Optimized Control and Data Planes**
  - Throughput does not rely on central WLC
- **WAN Failure Survivability in Branch Offices**
  - Flexconnect AP will go to “Standalone Mode”-
    - No impact on locally switched SSIDs
    - Disconnection of centrally switched SSIDs clients
  - Authenticates new clients with locally defined RADIUS server
- **Efficient AP Upgrade across WAN**
  - With the Smart Image Upgrade, software only sent to Master AP, reducing WAN bandwidth requirements

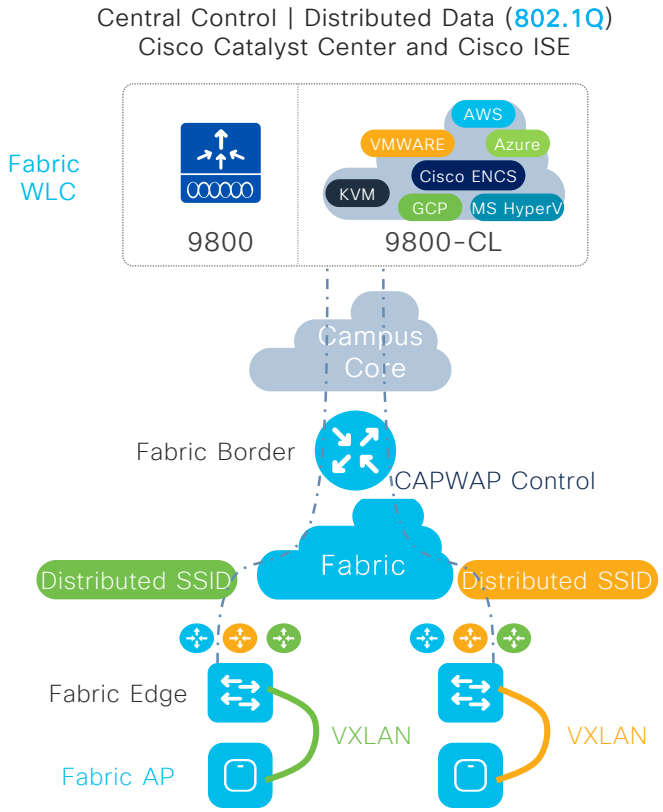


Examples –

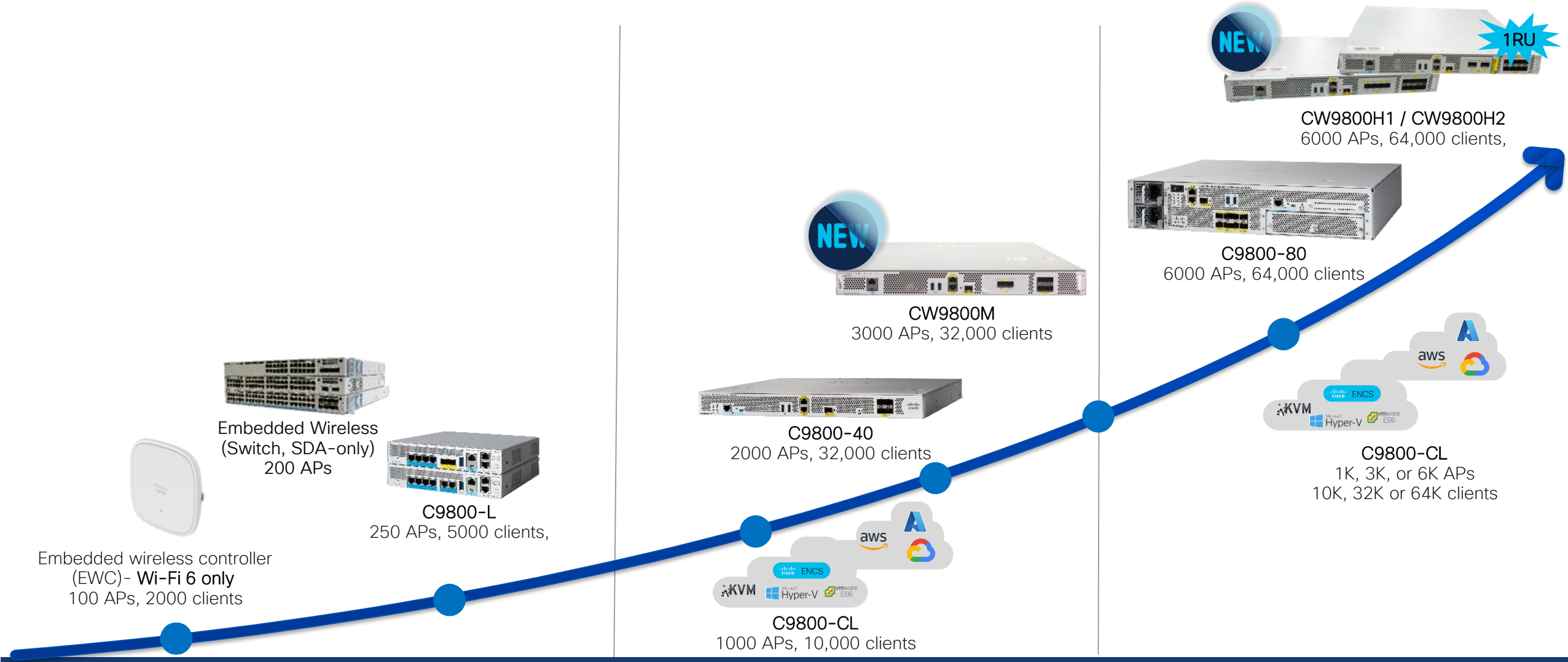
- Branch Offices
- Small/ Medium Stores/ Retail

Why SD-Access Wireless Deployment?

- **Automation**
  - Unified Wired-Wireless automation for design and deployment
- **Simplifying Data, Control and Management Planes**
  - Control Plane centralized at WLC
  - Distributed data plane for Wireless (No restriction with Wireless Controller Data throughput)
  - Single touchpoint for management with Cisco Catalyst Center
- **Seamless Layer 2 roaming**
  - Stretch client subnet without extending same VLAN everywhere
- **Segmentation**
  - Macro-Micro Segmentation for enhanced security (Common policies for Wired-Wireless)



Cisco 9800 Wireless Infrastructure



Cisco Catalyst CW9800H1 & CW9800H2 Wireless Controllers

The only difference between H1/H2:
CW9800H1 = 4x 25G
CW9800H2 = 2x 40G

1/10G & [25G or 40G] Uplinks

Up to 100 Gbps Backhaul

64,000 Clients

6,000 APs

1RU

Up to 36% faster than C9800-80, while using up to 40% less power!

Simple

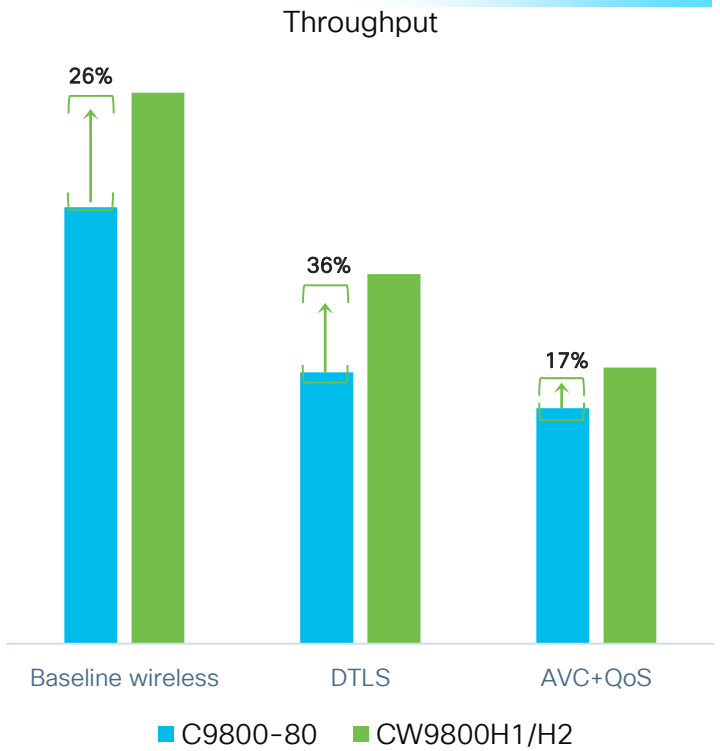
- Familiar WebUI and config structure reduces upgrade friction
- 10G HA port allows for easier deployments in modern data centers

Secure

- Designed for WPA3 and beyond
  - Line rate encryption with HW offload eliminates performance degradation from enabling advanced encryption

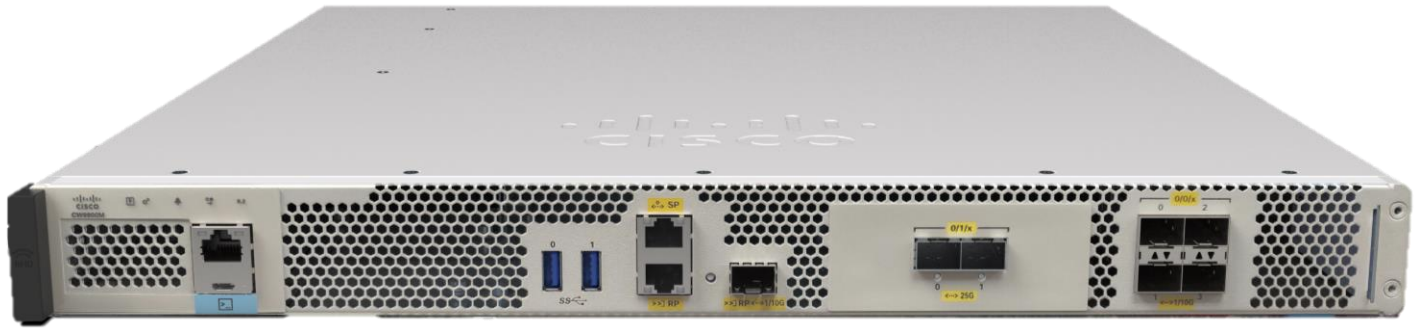
Sustainable

- Up to 40% more power efficient
- $1310 in power savings over 5 years @ $0.169/kWh
- New 1RU design saves space, allowing for more efficient data centers



Performance tests consist of bi-directional (simultaneous 50% up/down) “IMIX” real-world traffic

Cisco Catalyst CW9800M Wireless Controller



Up to 50 Gbps Backhaul

1/10/25G Uplinks

32,000 Clients

3,000 APs

Up to 53% faster than C9800-40, while using up to 18% less power!

Simple

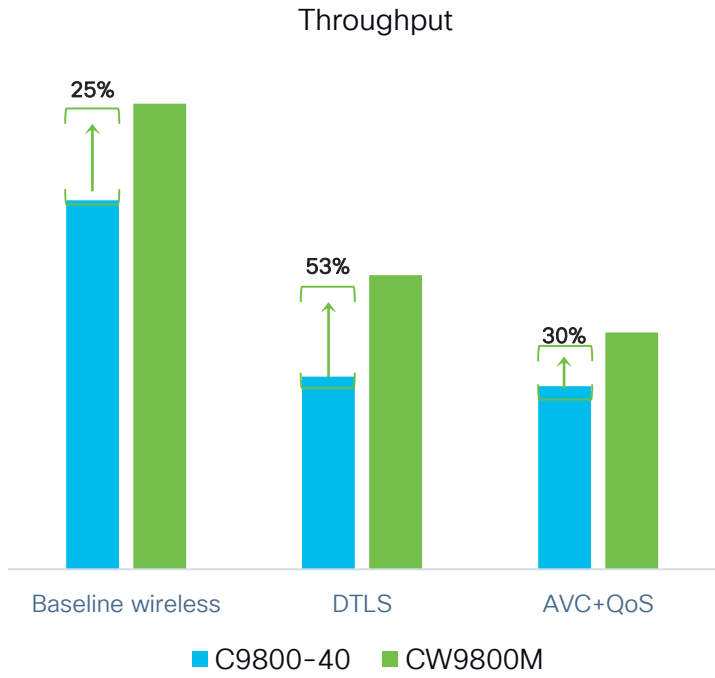
- Familiar WebUI and config structure reduces upgrade friction
- 10G HA port allows for easier deployments in modern data centers

Secure

- Designed for WPA3 and beyond
  - Line rate encryption with HW offload eliminates performance degradation from enabling advanced encryption

Sustainable

- Up to 18% more power efficient than C9800-40
- Increased AP scale by 1.5x allows for future growth



Performance tests consist of bi-directional (simultaneous 50% up/down) “IMIX” real-world traffic

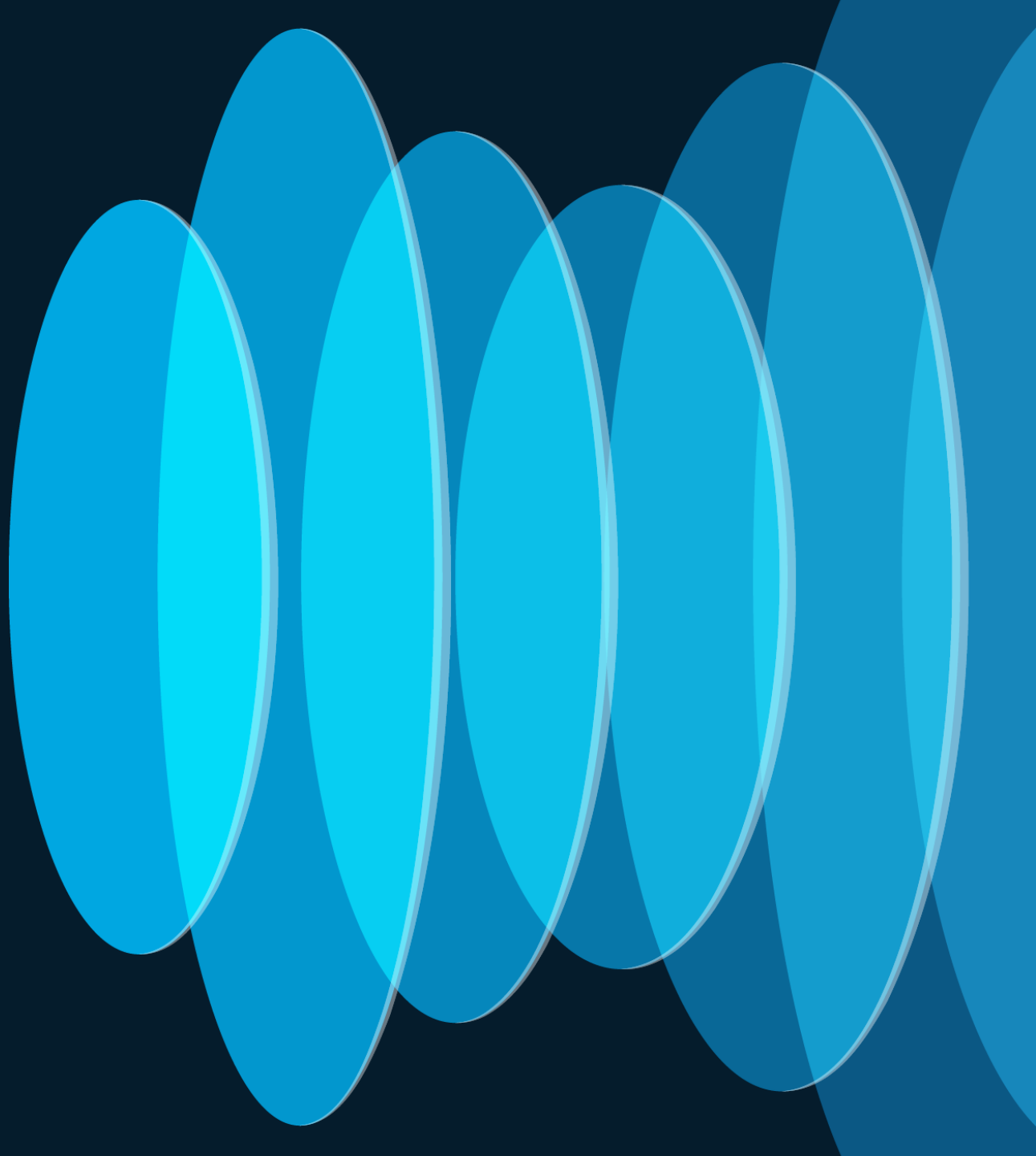
What Deployment Mode to Choose?

For your reference

Campus / Enterprise		
Size	**WLC**	**Deployment Mode**
Large	Catalyst 9800-80 CW9800H1/H2	Local
Medium	Catalyst 9800-40 CW9800M	Local
Small	Catalyst 9800-L, Catalyst 9800-CL	Local

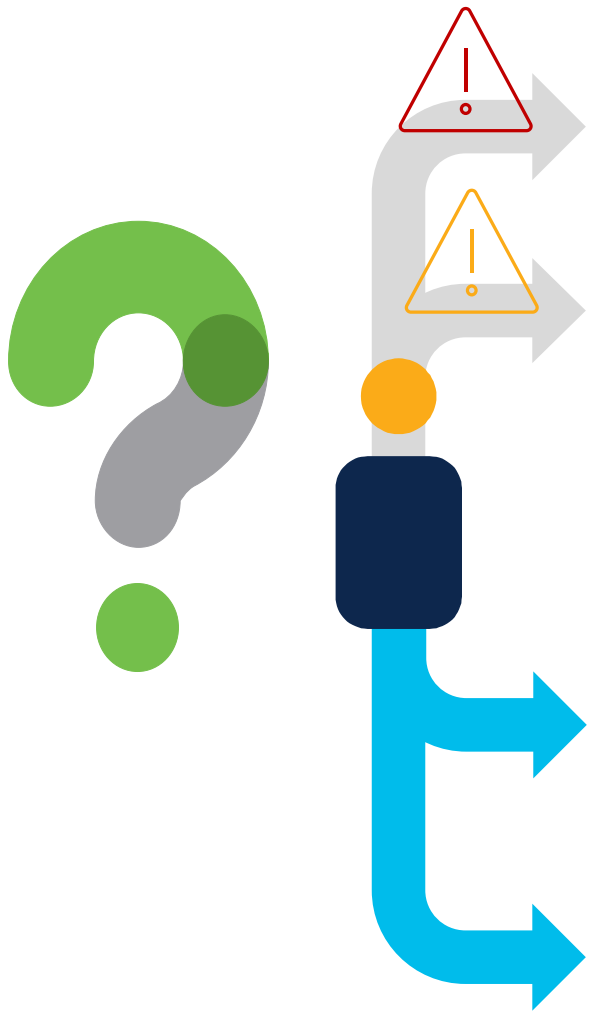
Branch or Distributed Enterprise		
Size	**WLC**	**Deployment Mode**
Large	Catalyst 9800-80, Catalyst 9800-CL CW9800H1/H2	FlexConnect, IaaS
	Catalyst 9800-L, Catalyst 9800-CL	Local
Medium	Catalyst 9800-40, Catalyst 9800-CL CW9800M	FlexConnect, IaaS
	Catalyst 9800-L, Catalyst 9800-CL	Local
Small	EWC, Catalyst 9800-L, Catalyst 9800-CL	FlexConnect, IaaS

Catalyst 9800 Recommended releases



cisco Live!

What is the recommended release?



17.3.x is End of Vulnerability support

- If you are already on 17.3.x train, go with 17.3.8a as it has the fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

Go with 17.6.x:

no more "gold star"

- If you want the most stable train for Wi-Fi 6 Catalyst Access Points without support for W1 APs (1700/2700/3700/1572)
- 17.6.7 has been released in April 2024, recommended release for this train

Go with 17.9.x:

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

Go with 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 support, Mesh on SDA, RF-based AP load balance, etc.)
- 17.12.x supports 802.11ac W1 APs to ease the migration to C9800 & Wi-Fi 6E
- 17.12.3 released in April 24 and it's the gold star candidate

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

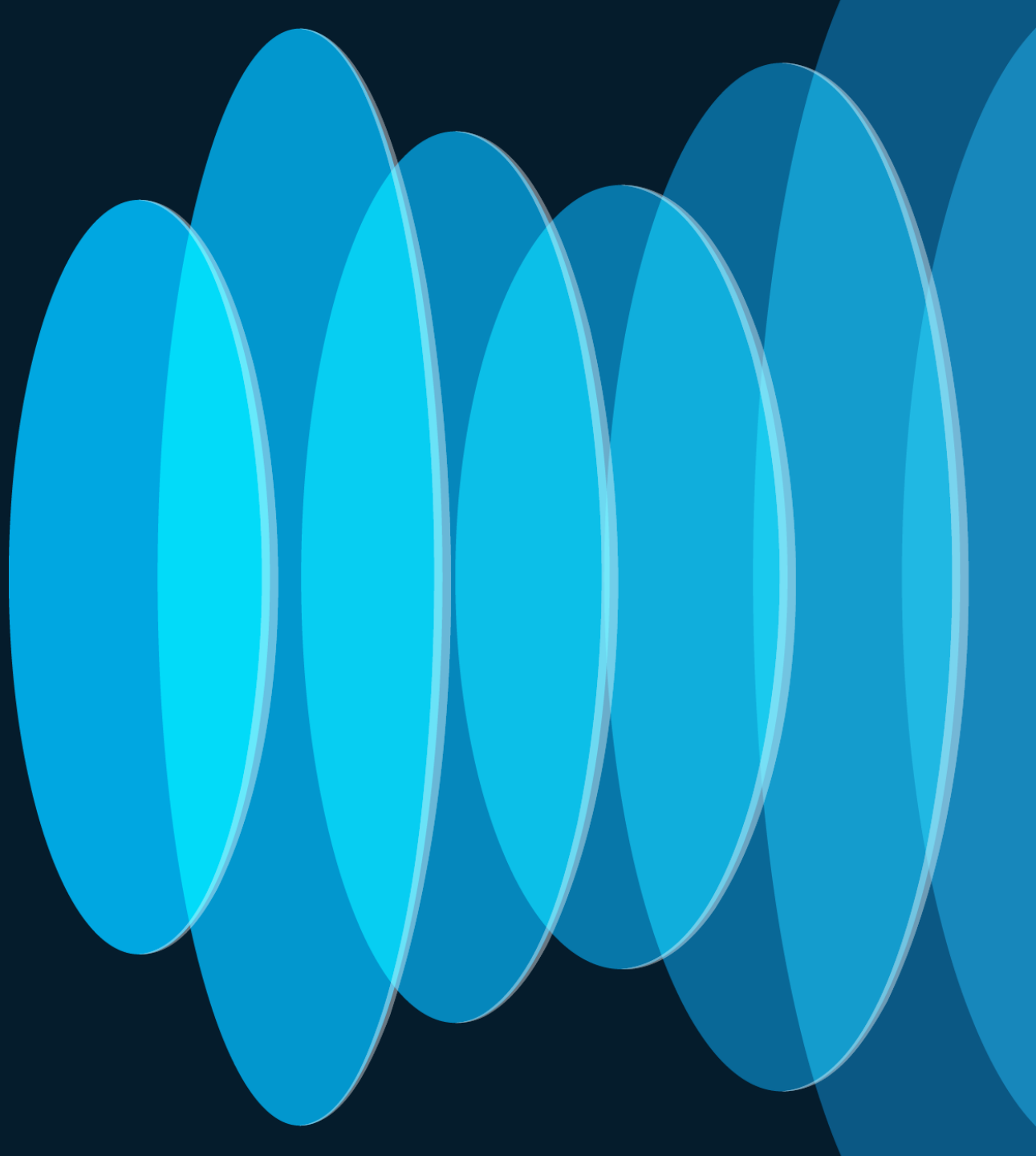
Cisco Recommended Software Matrix*


Reference

IOS-XE	AP	IRCM with Gen 1 AireOS	IRCM with Gen 2 AireOS	Catalyst Center	Prime	CMX	ISE
17.3.8a	802.11ax 802.11ac W1 & W2	8.5.182.104	8.10.190.0	Matrix	3.10.1	10.6.2	3.1 3.0 2.7 2.6 2.4
17.6.7	802.11ax 802.11ac W2	8.5.182.104	8.10.190.0	Matrix	3.10.1	10.6.2	
17.9.5	802.11ax (Wi-Fi 6/6E) 802.11ac W1 & W2	8.5.182.104	8.10.190.0	Matrix	3.10.2	10.6.3	3.2 3.1 3.0 2.7
17.12.3	802.11ax (Wi-Fi 6/6E) 802.11ac W1 & W2	8.5.182.104	8.10.190.0	Matrix	3.10.4 update1 3.10.3		

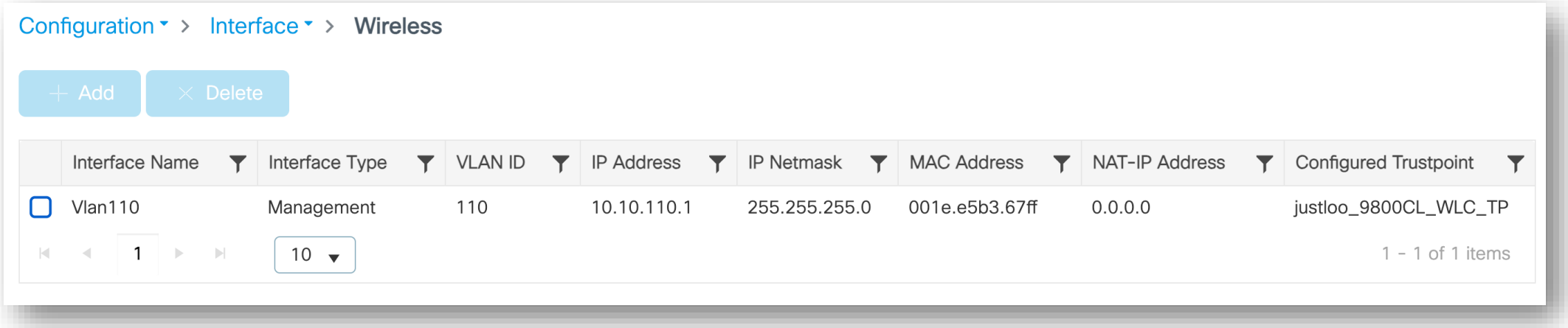
(*) Please bookmark and check these links for the latest info:
http://cs.co/compatibilitymatrix
http://cs.co/recommendediosxe
Catalyst Center: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

Controller Settings

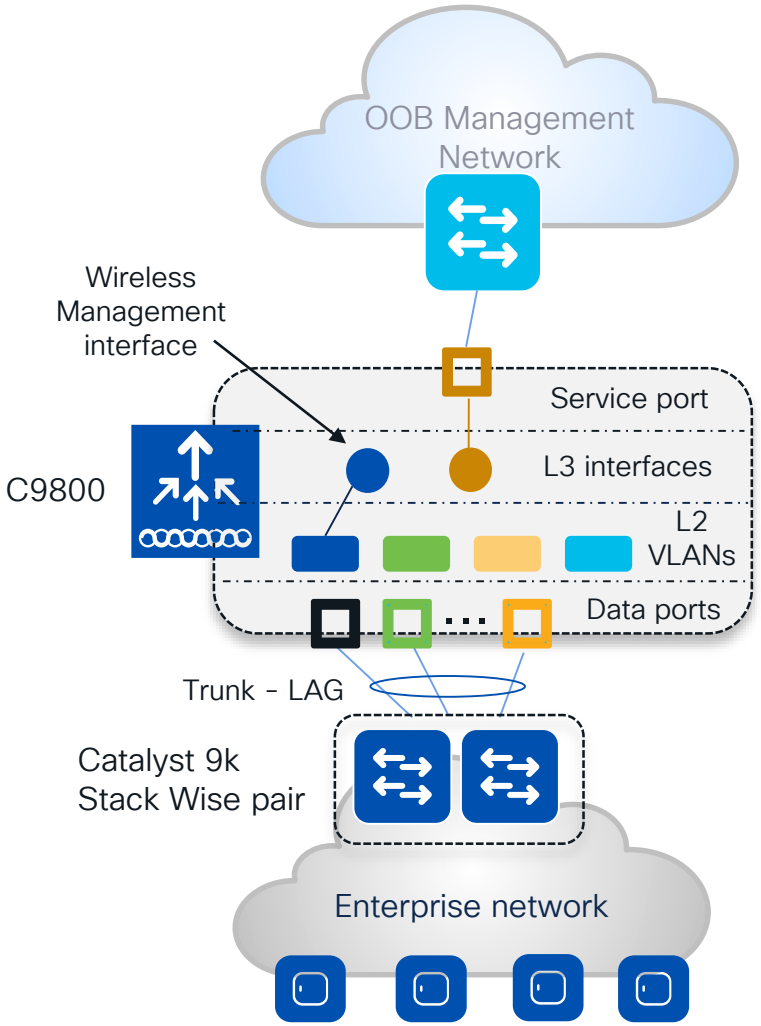


Wireless Management Interface

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



Port, VLAN, SVI interfaces considerations



Facts:

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

Best practices:

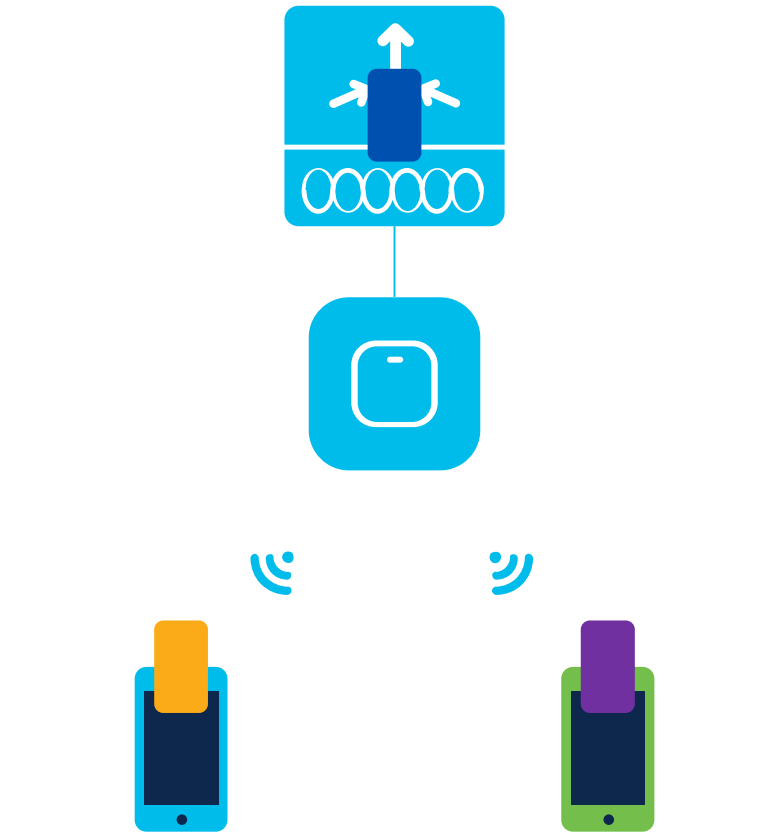
- Switch Virtual Interface (SVI) for wireless management interface is recommended.
- Do not configure SVIs for client VLANs, unless really needed (e.g., DHCP relay) – this is different from AireOS where Dynamic interface is required.
- Connect the uplink ports in a port-channel, configured as trunk to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

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

Best Practice – Address Resolution Protocol (ARP) Proxy

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

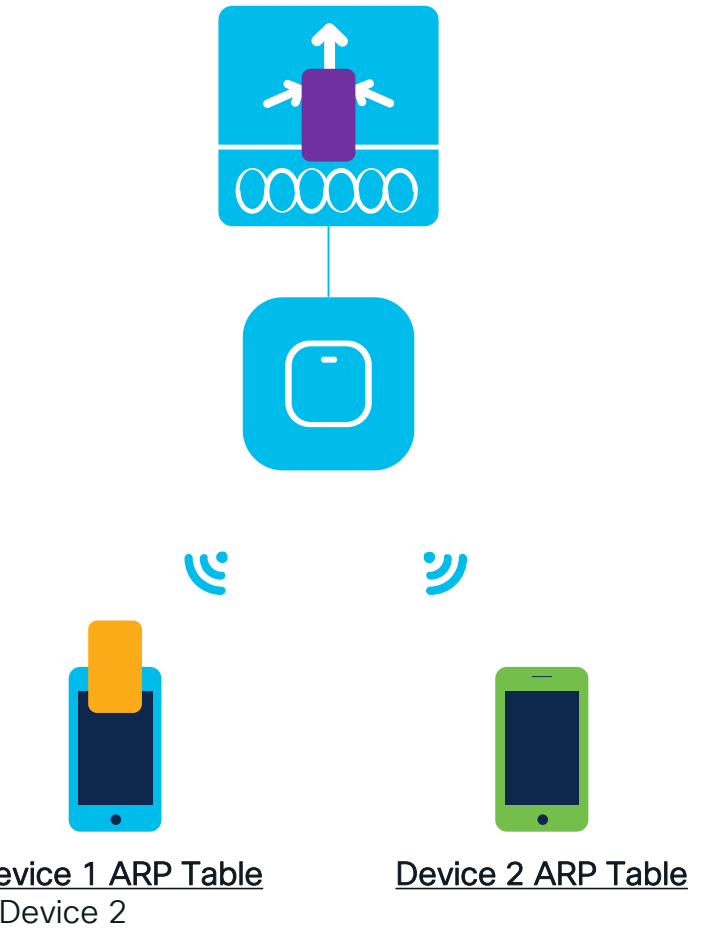
```
C9800# conf t
C9800(config)# wireless profile policy <name>
C9800(config-wireless)# ipv4 arp-proxy
```



Best Practice – Address Resolution Protocol (ARP) Proxy

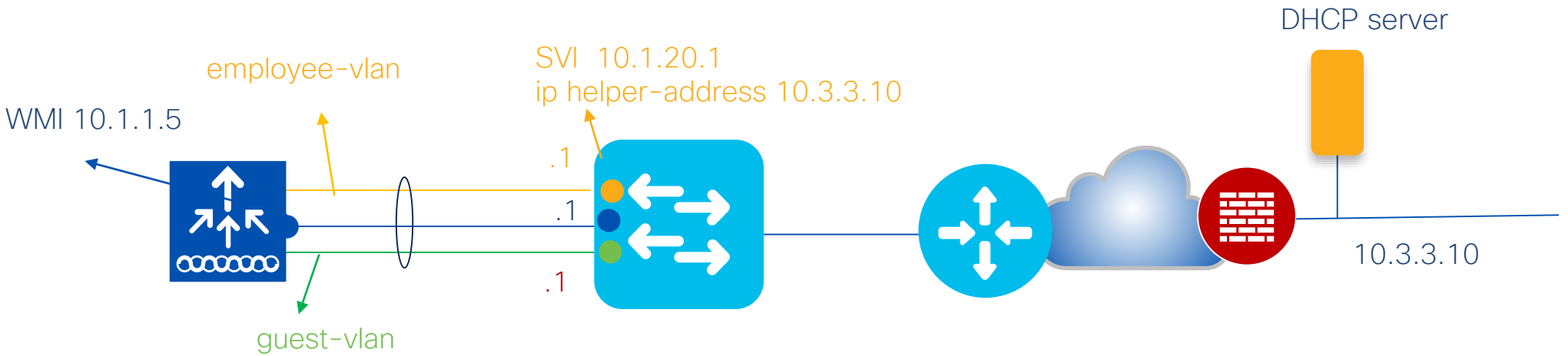
- **Default Behavior**
  - C9800 forwards ARP traffic by changing destination MAC from broadcast to unicast
- **ARP Proxy**
  - Starting 17.3.1, C9800 can be configured to act as a proxy and respond on behalf of a registered client

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



Best Practice – DHCP proxy/relay

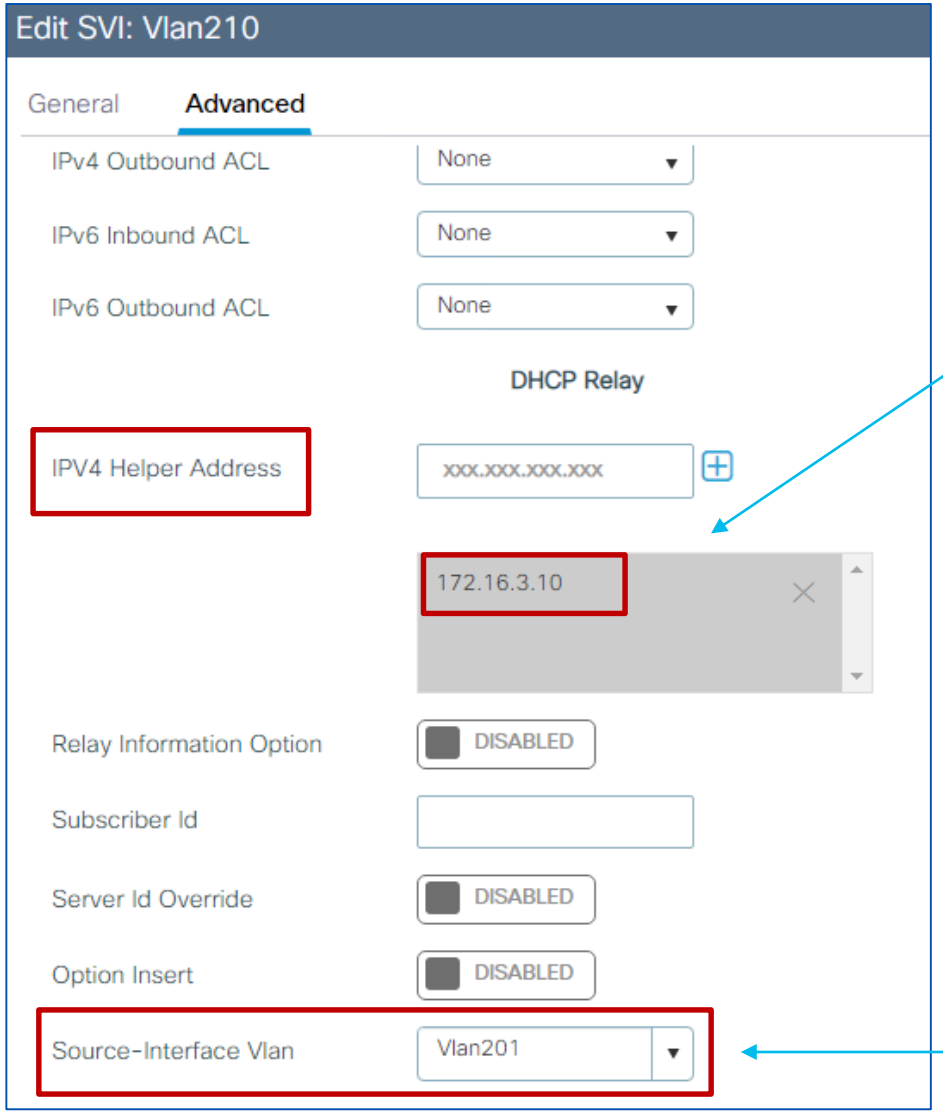
- **DHCP Proxy mode:**
  - In AireOS, enabling DHCP Proxy for wireless clients is a best practice
  - In C9800 DHCP proxy is not needed as IOS-XE has embedded security features like DHCP snooping, ARP inspection, etc. that don't require a L3 interface
- **DHCP relay or bridging mode?**
  - DHCP bridging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



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
  - DHCP relay on C9800 should be configured if customer wants to add option 82 info
  - On box DHCP relay can be configured on the client interface VLAN (SVI) or the WLAN basis
    - In both cases you still need the SVI to be configured with an IP address
    - The outgoing interface for DHCP traffic will be determined by routing table lookup for DHCP server's IP
  - DHCP relay mode: the real IP of the DHCP server is hidden from the client but the IP of the controller is exposed, so you may want to consider any security implications

C9800 as DHCP relay for client VLAN



- Create an SVI for the client VLAN (e.g. “Vlan210” in this case)
- Add the DHCP Server IP > this configures the ip helper command under the interface:

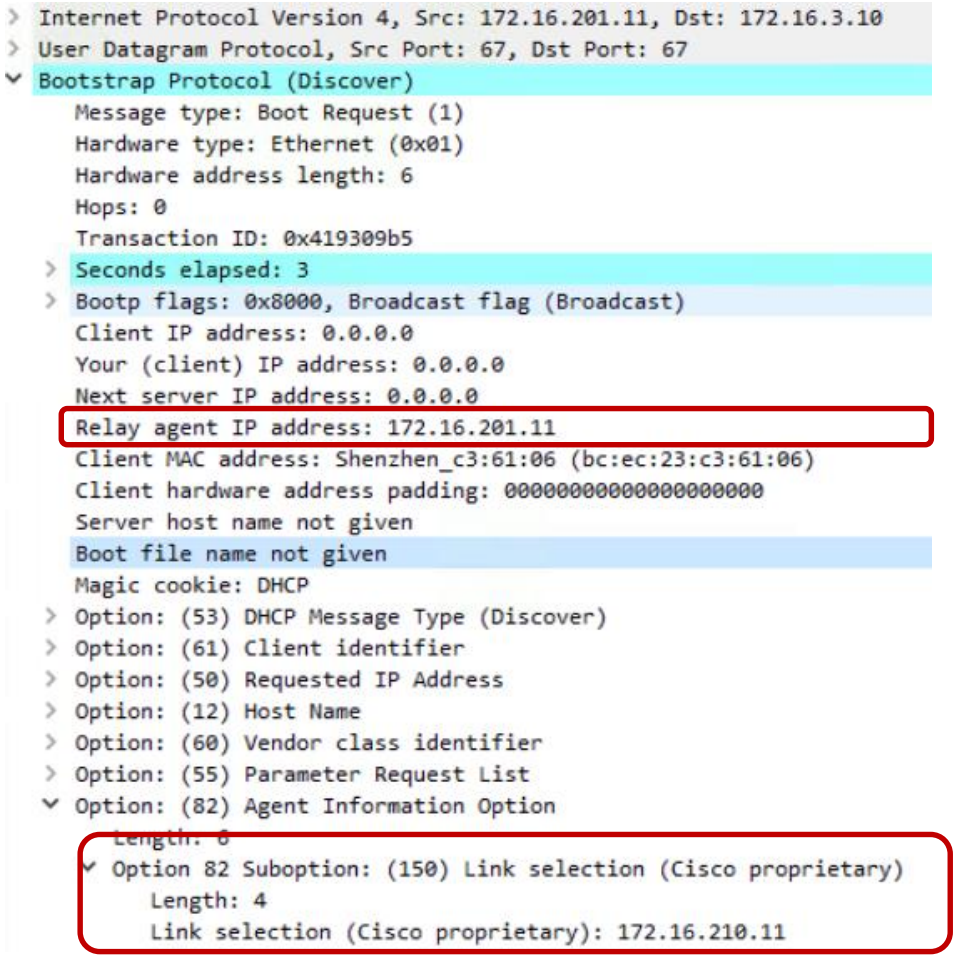
```
interface Vlan210
 description Employee-SVI
 ip address 172.16.210.21 255.255.255.0
 ip helper-address 172.16.3.10
```

- The DHCP relay packet is sourced from this SVI and the GIADDR is also set to the IP of Vlan210.
- The outgoing interface is chosen with an IP routing table lookup, so the outgoing interface/vlan could be a different one. Likely it will wireless management interface (WMI) as you have the default gateway on this VLAN. This can result in asymmetric traffic and in Reverse Path Forwarding (RPF) failures on the first hop switch/firewall
- To avoid this, the first step is to configure a specific interface as source for DHCP packets > in this case we want DHCP traffic to be sourced from WMI (e.g., Vlan 201 > IP 172.16.201.11):

```
interface Vlan210
 description Employee-SVI
 ip address 172.16.210.21 255.255.255.0
 ip helper-address 172.16.3.10
 ip dhcp relay source-interface vlan 201
```

C9800 as DHCP relay for client VLAN

- In this case the source of the DHCP packets and the GIADDR are set to the interface specified in the DHCP relay command (172.16.201.11 in this case)
- How does the DHCP server know how to assign the IP from the right client pool?
- When the “ip dhcp relay source-interface” command is used, C9800 automatically adds the client subnet information in a proprietary suboption 150 of option 82 (called “link selection”), as you can see from the capture
- You need to configure your DHCP server to assign IP addresses based on the link selection information, as this indicates the right client pool…

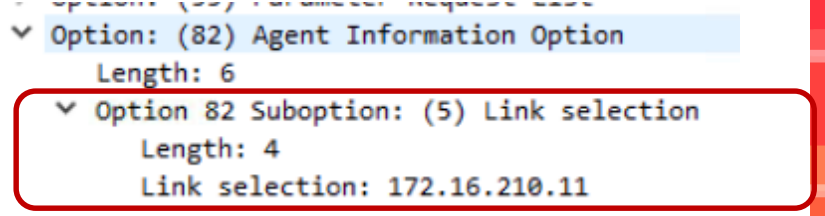


C9800 as DHCP relay for client VLAN

- The recommendation is to change the C9800 configuration to use the standard suboption 5 to send the link selection info. You can do this by configuring the following global command:

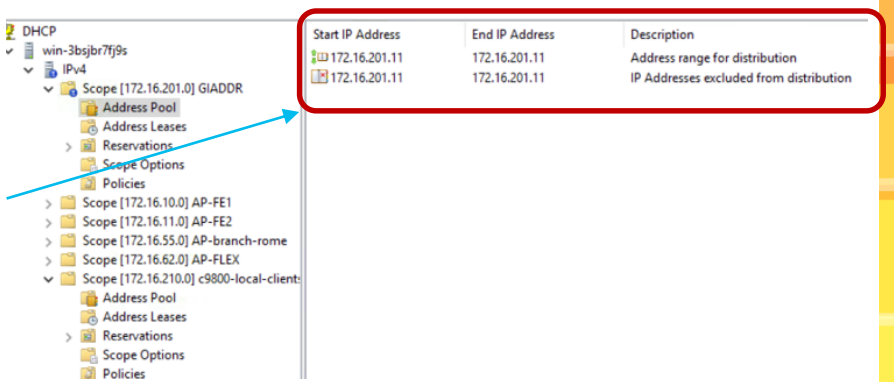
```
ip dhcp compatibility suboption link-selection standard
```

As you can see the option for link selection has changed



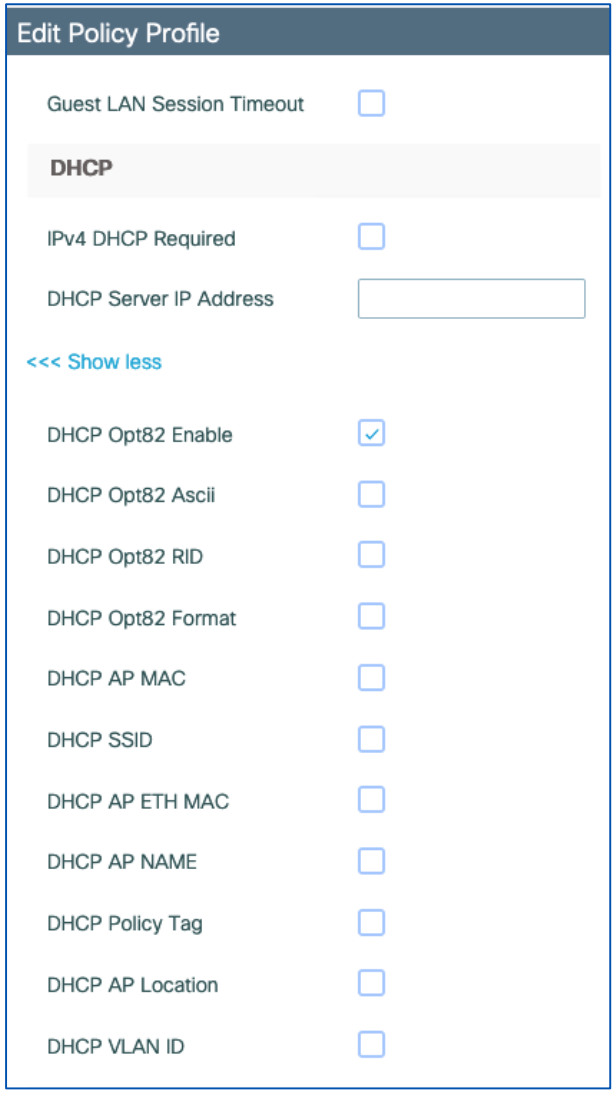
- What do you have to do on the DHCP server? For example, Windows 2016 the instructions are here: https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-subnet-options

- You have to create a dummy scope to “authorize” the IP of the relay agent. In our example, it’s the IP of the VLAN 201, the WMI (172.16.201.11). You have to add the IP to the scope and then exclude it from the distribution



C9800 DHCP Relay – option 82

- If you want to add other relay information, DHCP option 82 is enabled under the Policy profile
- Starting 17.4. C9800 has parity with AireOS in terms of what information can be sent
- Important note: the command "ip source DHCP source-interface" will not take effect if option 82 settings are configured under the policy profile. In other words, option 82 settings work only if the source interface for the DHCP packets is taken from the routing table. This is fixed starting 17.3.3 and 17.4

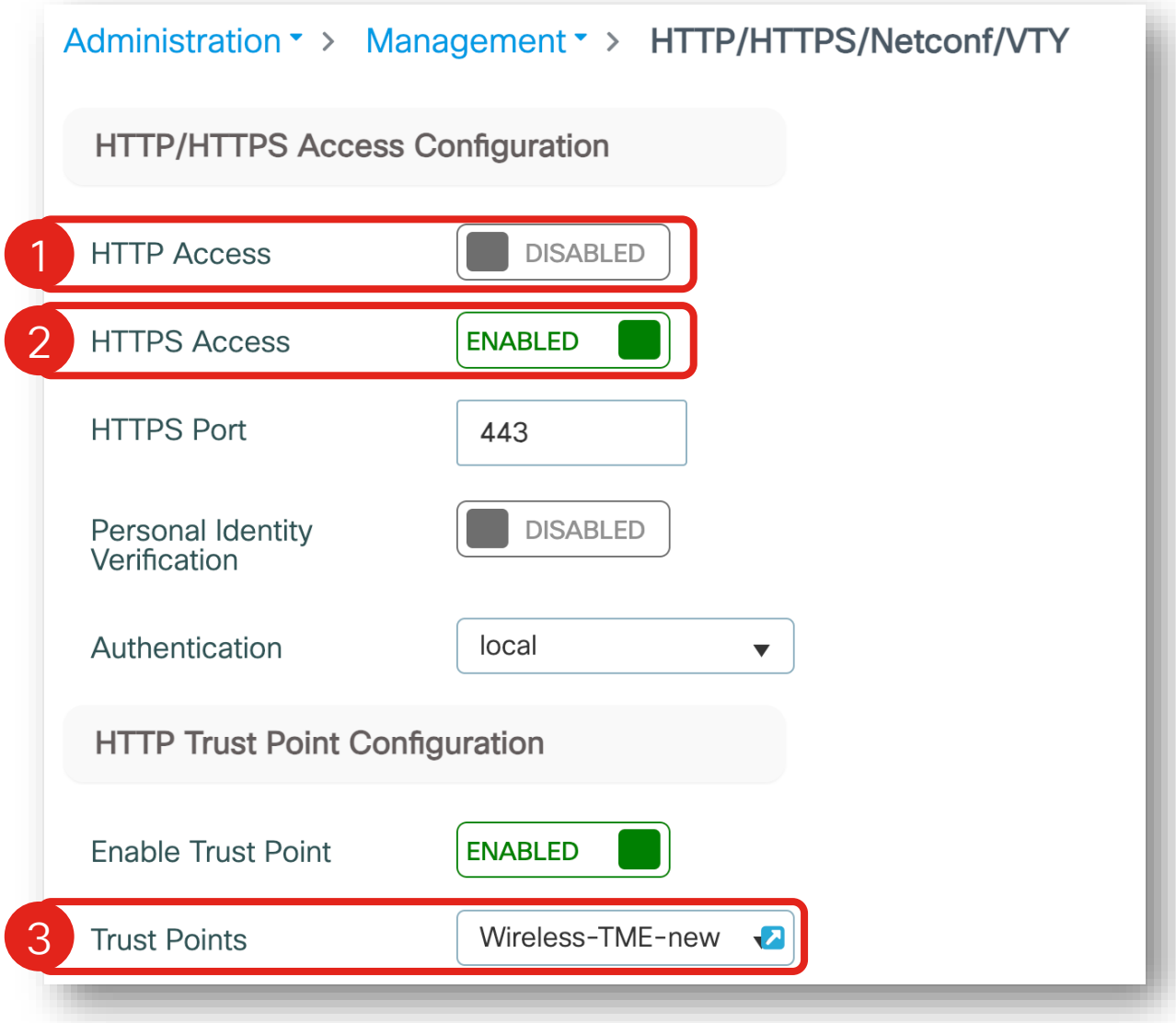


Using C9800 Internal DHCP Server

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

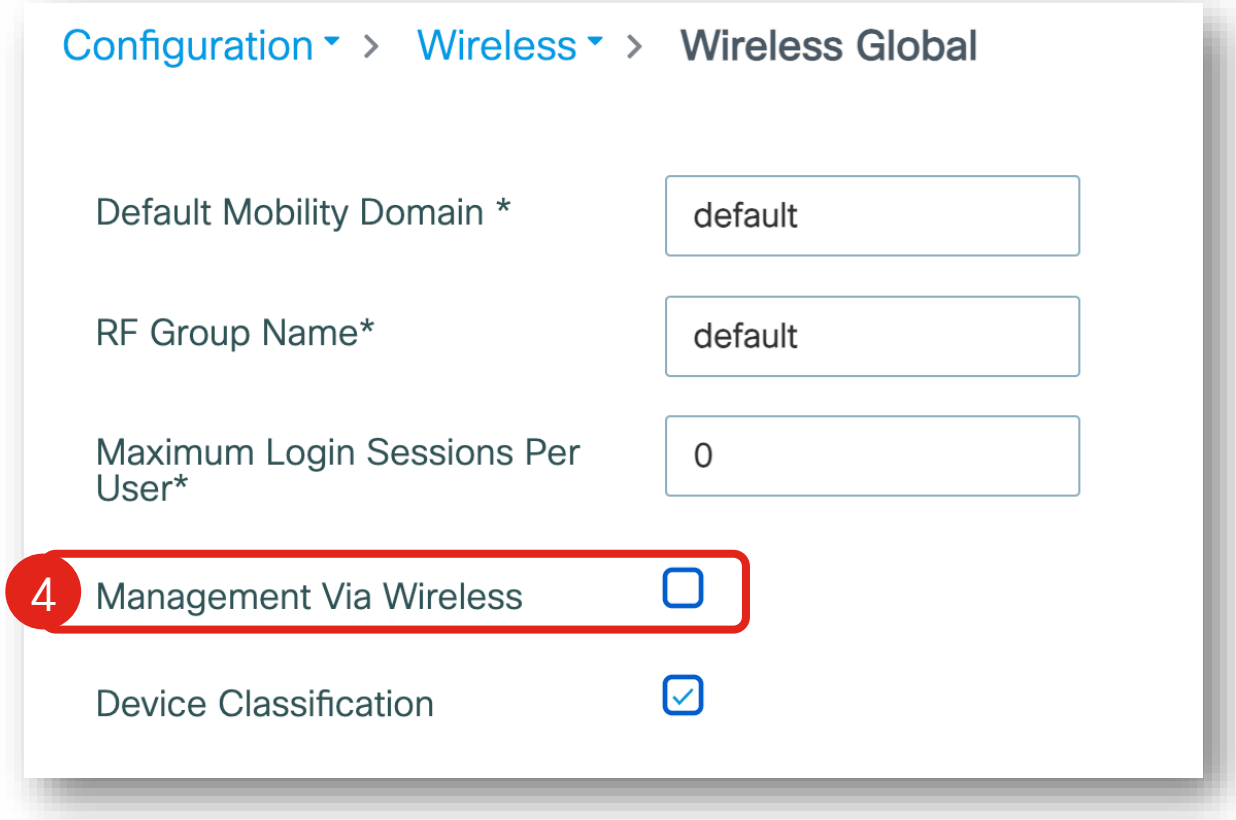
Enable Secure Web Management Access

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



Enable Secure Web Management Access

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



Password Encryption

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

Step 1: Define encryption key

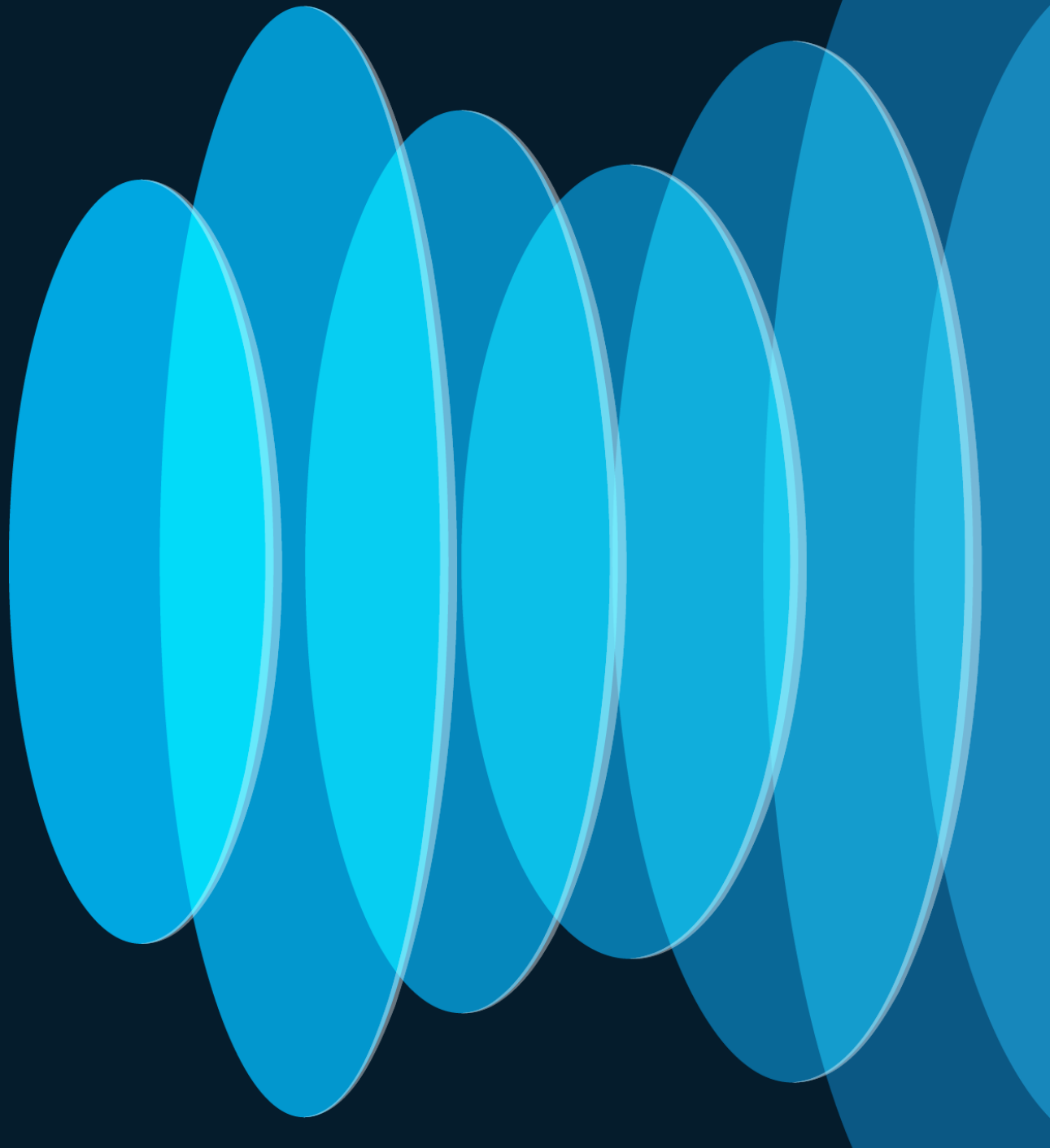
```
C9800# configure terminal
C9800(config)# key config-key password-encrypt <key>
```

Step 2: Enable password Encryption

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

Note: There is no mechanism to decrypt passwords.

High Availability



High Availability
Reducing downtime for Upgrades and Unplanned Events

Unplanned Events
Device and network interruptions

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

Controller Software Update
Software Maintenance updates (SMU)

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

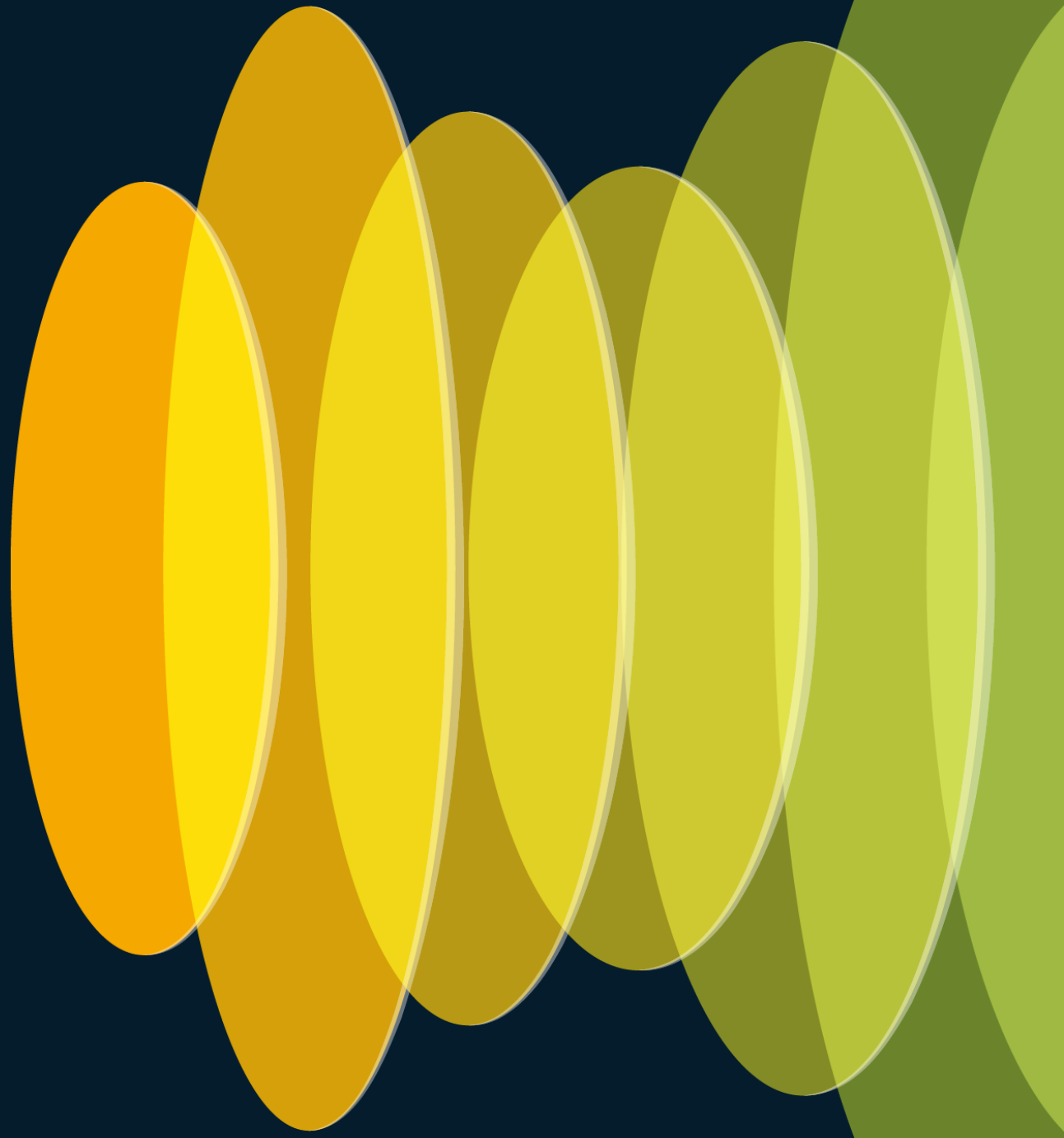
Access Point Updates
AP Updates and new AP models

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

Software Image Upgrades
Wireless controller image upgrades

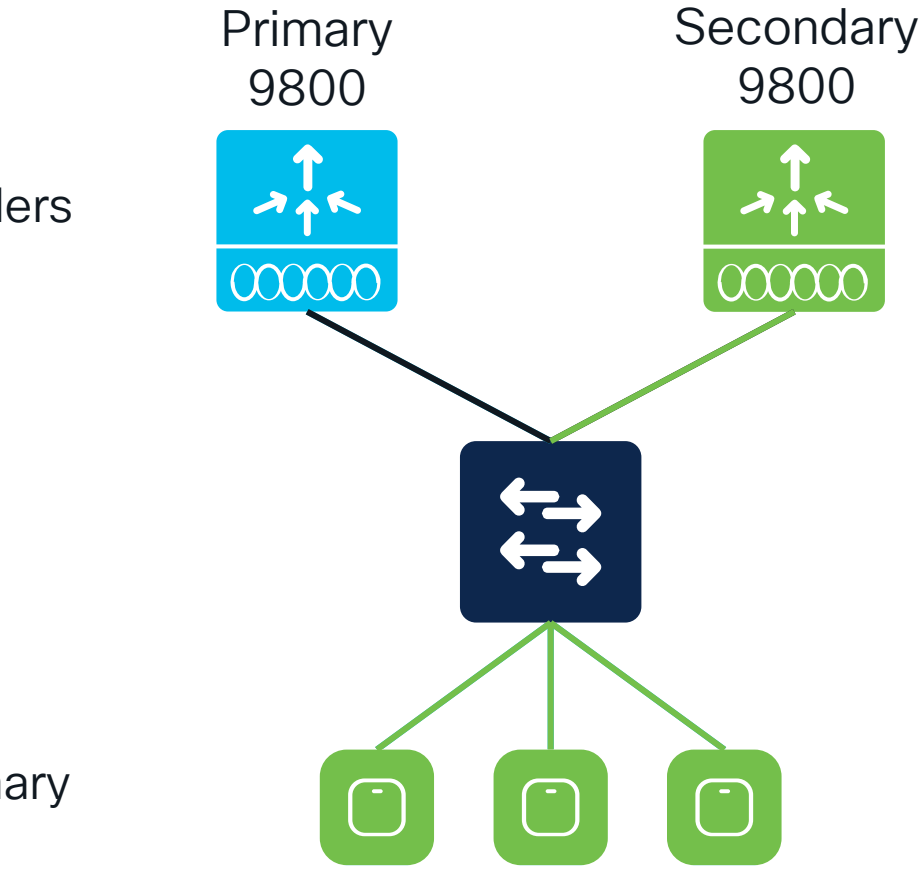
- N+1 Hitless Rolling AP Upgrade (All Sites or Site Based)
- In Service Software Upgrade (ISSU)

N+1 Redundancy



N+1 Redundancy

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



AP failover takes ~45-60 seconds

N+1 Redundancy Configuration

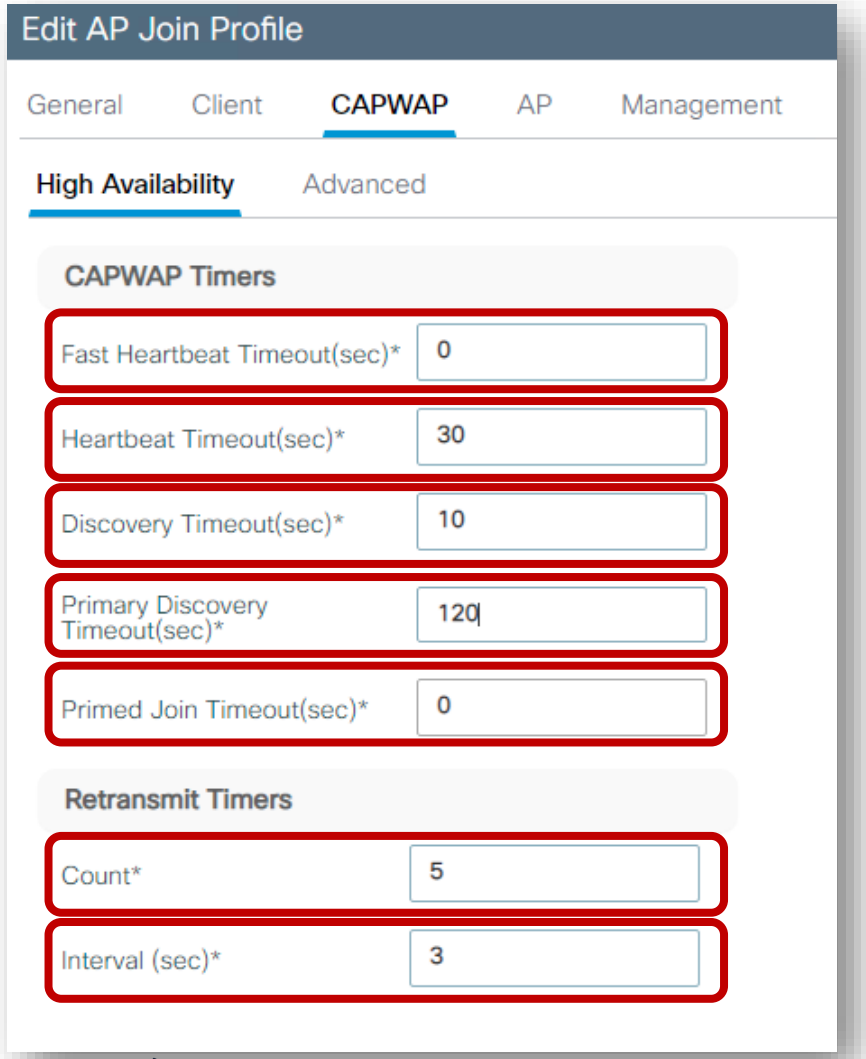
Can be configured via 2 methods

AP Join Profile

Statically on the APs

Recommended to use ONLY ONE of the methods

N+1 Redundancy: Timers



Fast heartbeats are dedicated packets to check the availability of Primary WLC and accelerate the failure detection and hence AP failover > 30-45 sec

- 1-10s (default is 0 = disabled). Dedicated keepalives to detect WLC failure
- 1-30s (default is 30). Regular CAPWAP keepalives
- 1-10s (default is 10). Time AP waits to process received discoveries
- 30-3000s (default is 120). Time AP would check on the Primary
- 120-43200s (default is 0 = disabled). Time AP tries to join only P/S/T

- 3-8 (default is 5)
- 2-5s (default is 3)

Bulk Priming APs in Large Scale Deployments

Pre-IOS XE 17.10.1

- Manually enter Primary, Secondary, and Tertiary for each AP
- Not scalable to enter console of each AP and configure this

IOS XE 17.10.1 or Later

- Create an AP Priming Profile on the C9800 that automatically applies to APs when joining
- Scales to large numbers of APs joining the controller

AP Priming Profile and AP Priming Filter

AP Priming Profile

- Contains the hostname and IP address of the Primary, Secondary, and Tertiary controllers
- Primary and Secondary controllers are mandatory
- Mapped to an AP Priming Filter

AP Priming Filter

- Similar structure as the AP filter for tag mapping
- Uses RegEx string mappings to match APs based on their configured names
- Applies the mapped AP Priming Profile to the matched APs

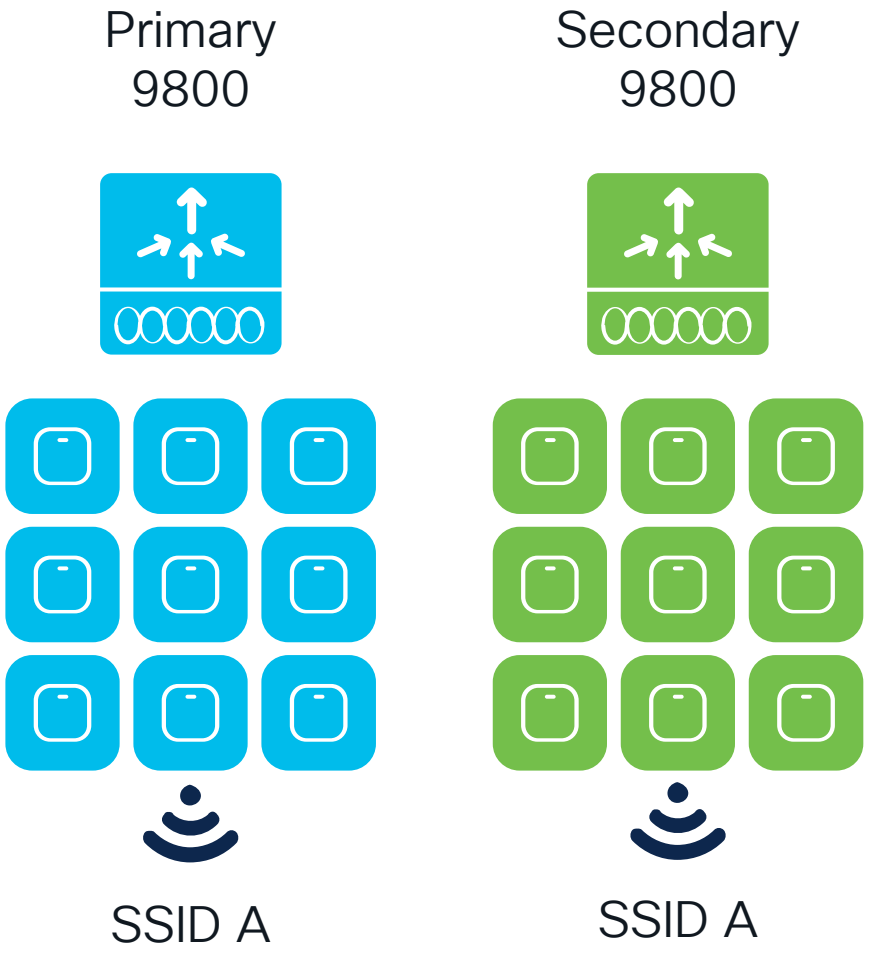
N+1 best practices

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



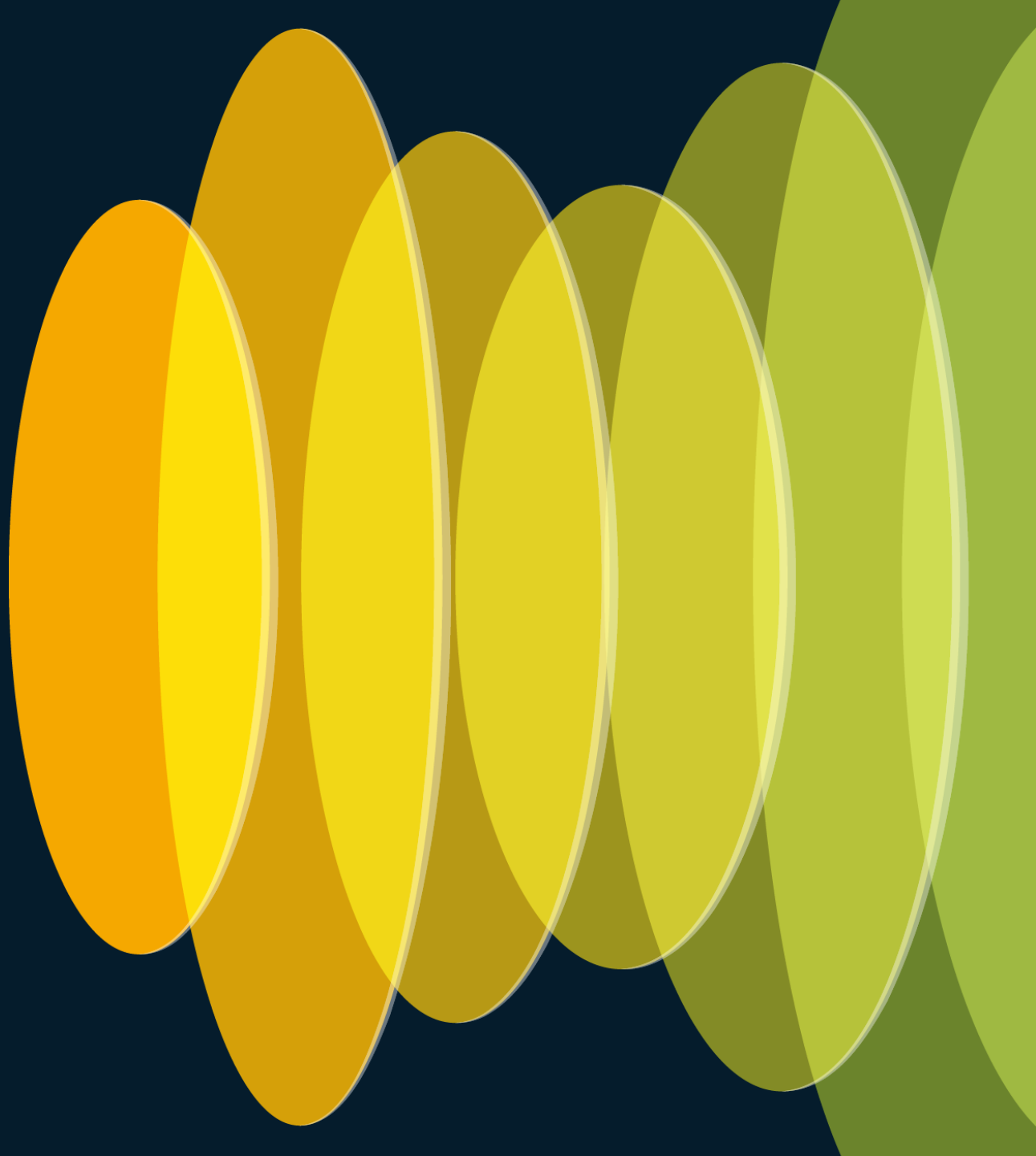
Define tag mappings via static mappings or REGEX based on AP name / location

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

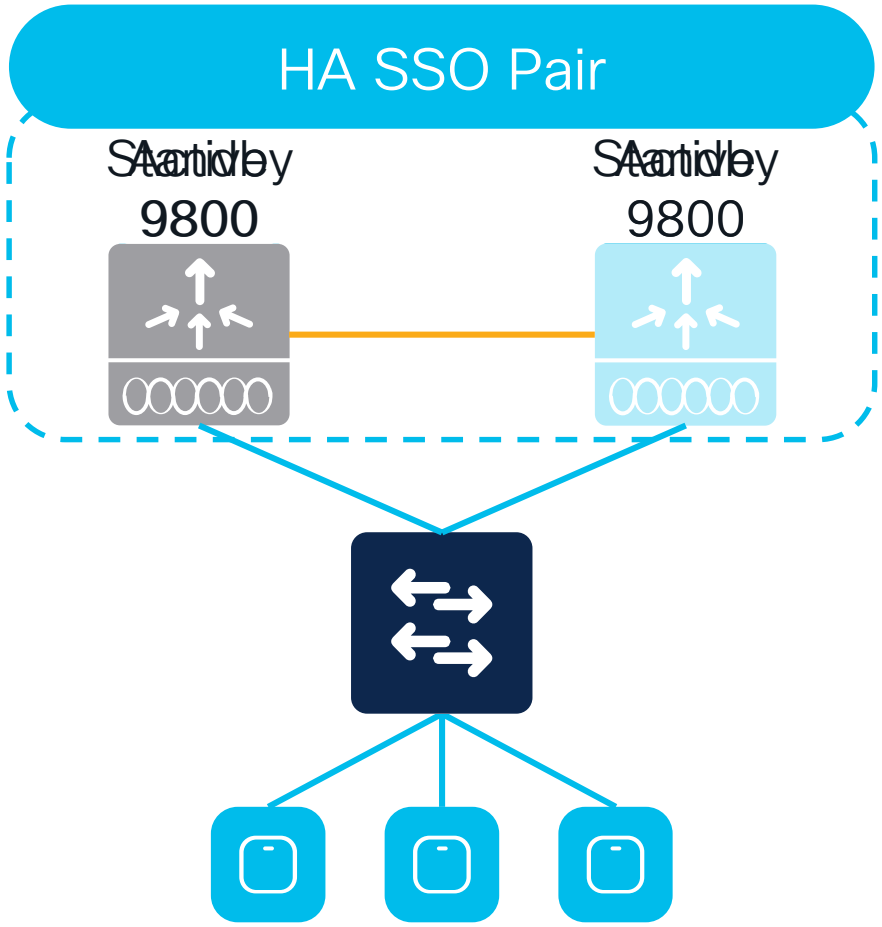
High Availability Stateful Switchover (HA SSO)



cisco Live!

High Availability Stateful Switchover (HA SSO)

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

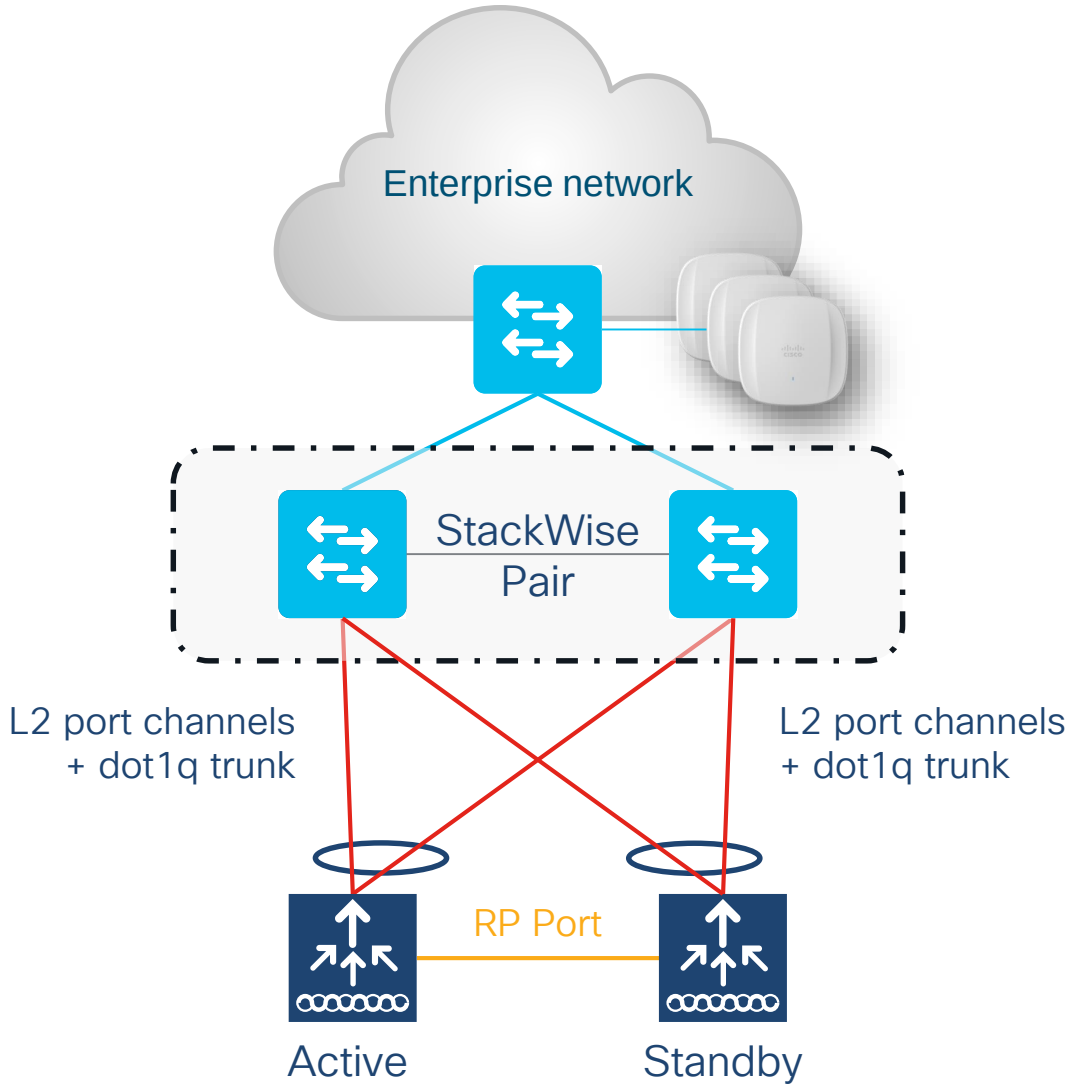


AP failover takes order of sub seconds

HA SSO behavior
Redundancy Port (RP)

Redundancy Port (RP)

- Syncs configuration and AP/Client databases between Active and Standby
- Monitors status of the chassis
- Possible single point of failure

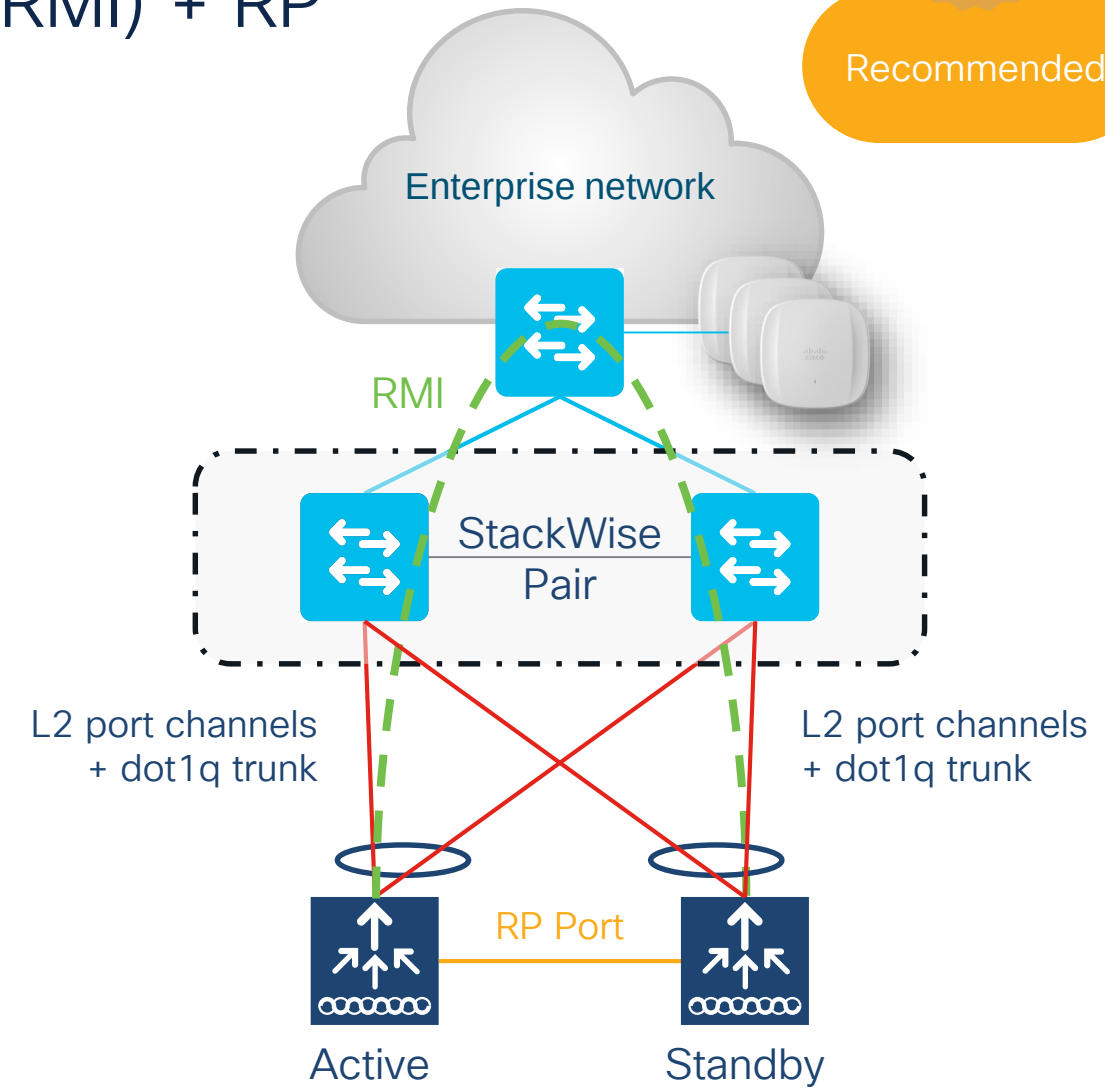


HA SSO behavior
Redundancy Management Interface (RMI) + RP

Recommended

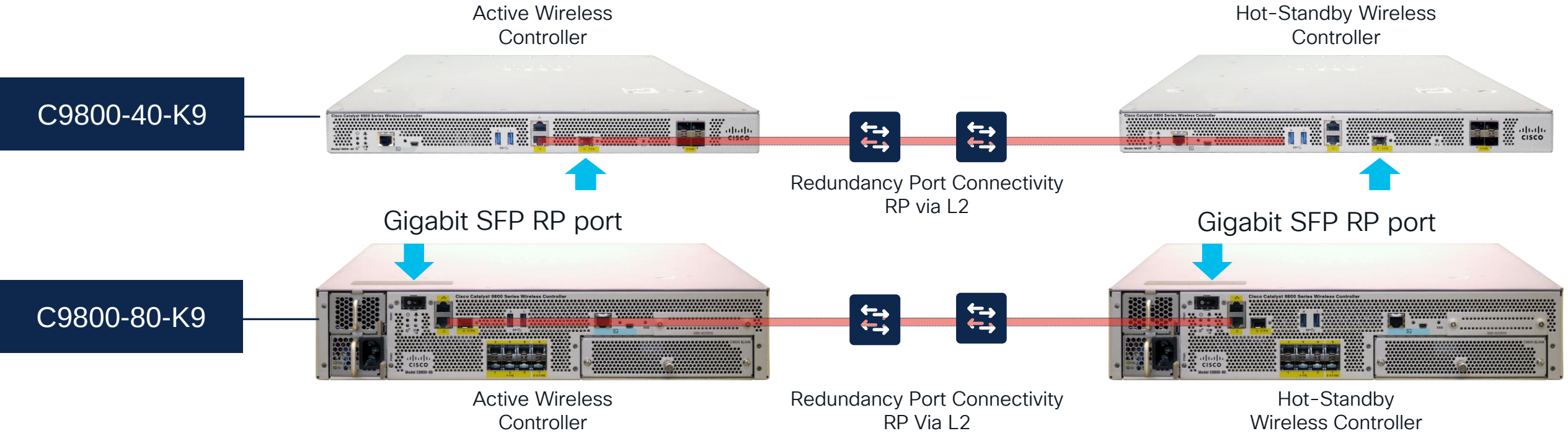
RMI + RP

- With RP only, there is no way to know if the peer is down or there is a link issue
- RMI is introduced for:
  - Default Gateway check
  - Status of peer through the network
  - Dual Active Detection
- Configure it in same subnet as the Wireless Management Interface (WMI)
- RMI can be used for remote management of the standby (SSH, Programmability)
- IPv6 support introduced in 17.3.2



High Availability (SSO) on C9800-40/80

A direct physical connection between Active and Standby Redundant Ports or Layer 2 connectivity is required to provide stateful redundancy within or across datacenters



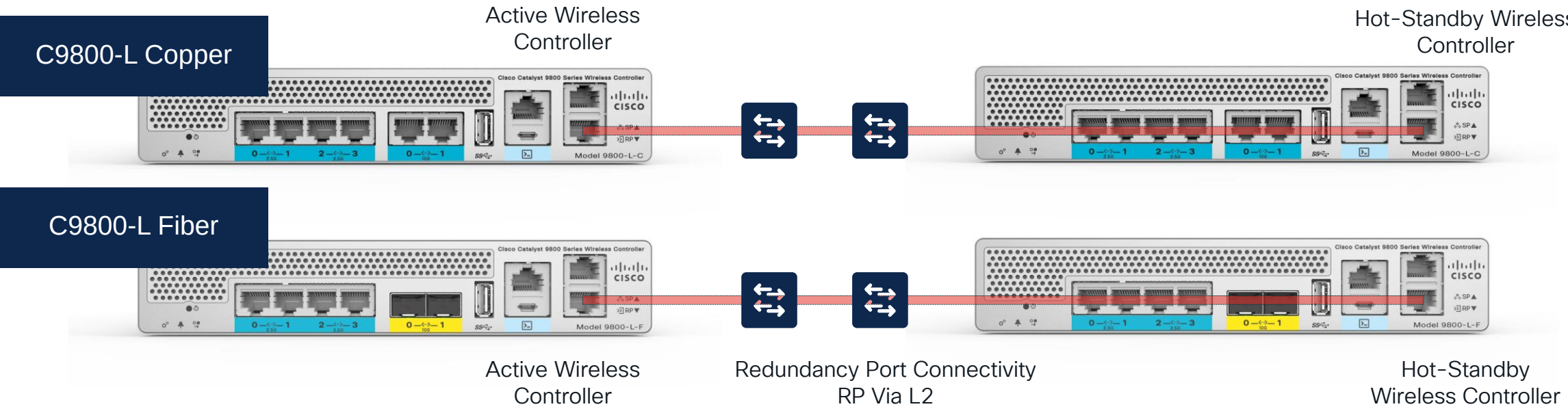
Sub-second failover and zero SSID outage

The only supported SFPs on Gigabit RP port are : GLC-SX-MMD and GLC-LH-SMD

High Availability (Client SSO) on Catalyst 9800-L

A direct physical connection between Active and Standby Redundant Ports or Layer 2 connectivity is required to provide stateful redundancy within or across datacenters.

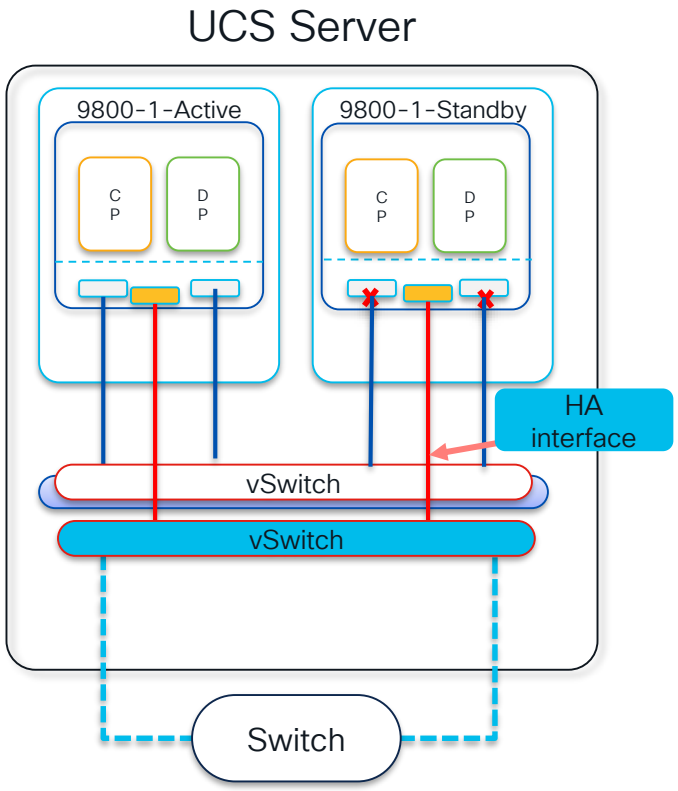
Note: There is no Fiber RP Port on 9800-L.



Sub-second failover and zero SSID outage

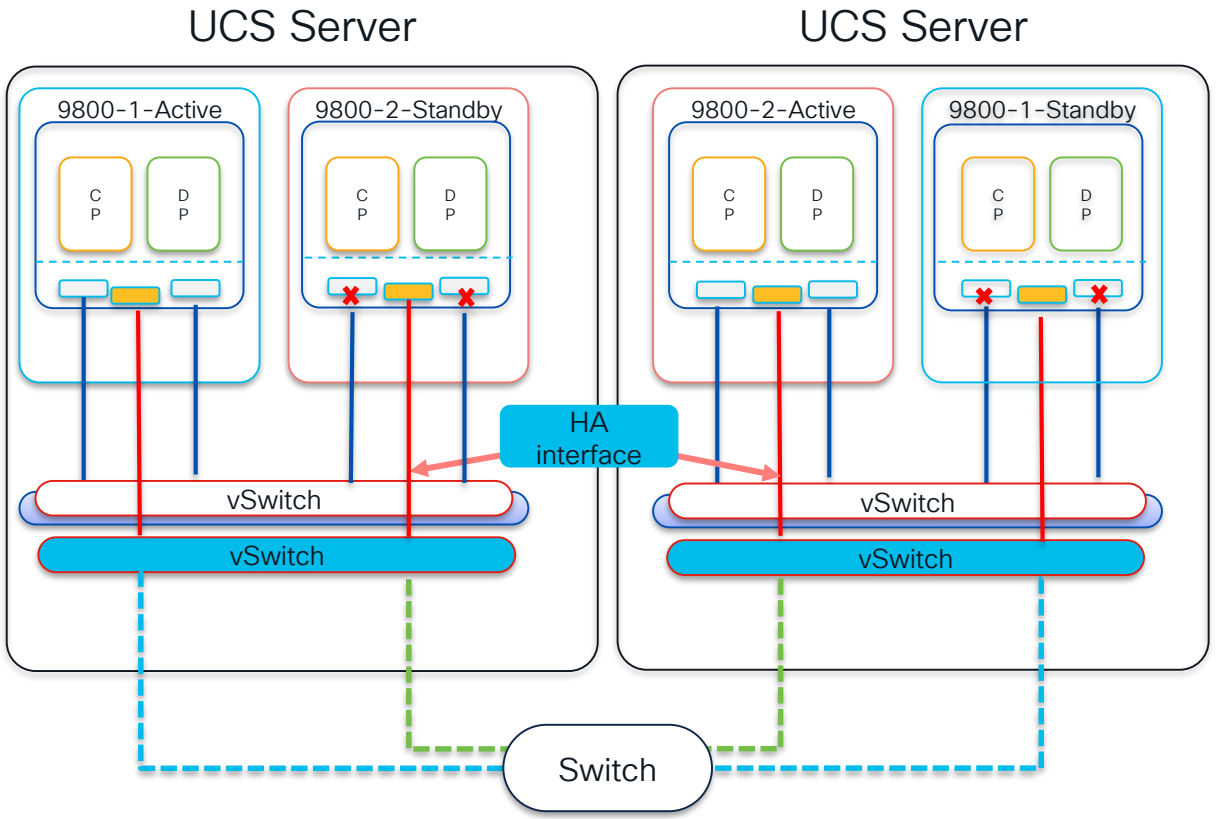
High Availability (SSO) on Catalyst 9800-CL

Intra-Host Redundancy



Redundancy Port Connectivity

Inter-Host Redundancy



Redundancy Port Connectivity
RP via L2

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

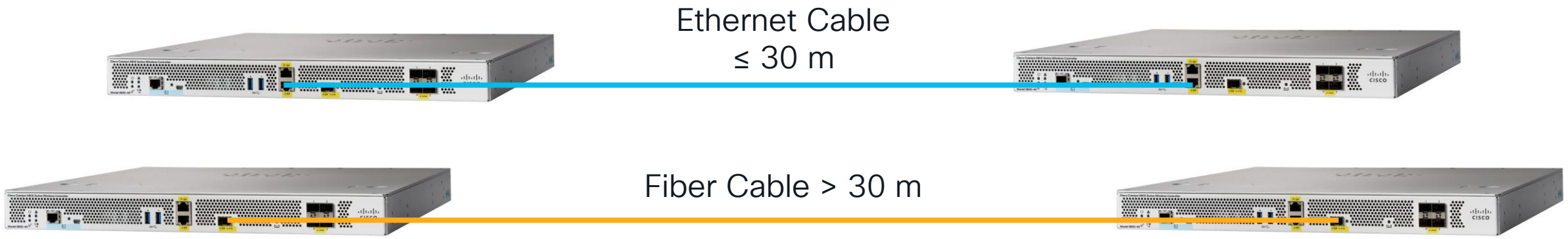
- Both boxes are running the same software and in the same boot mode
- **Install mode is recommend**

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

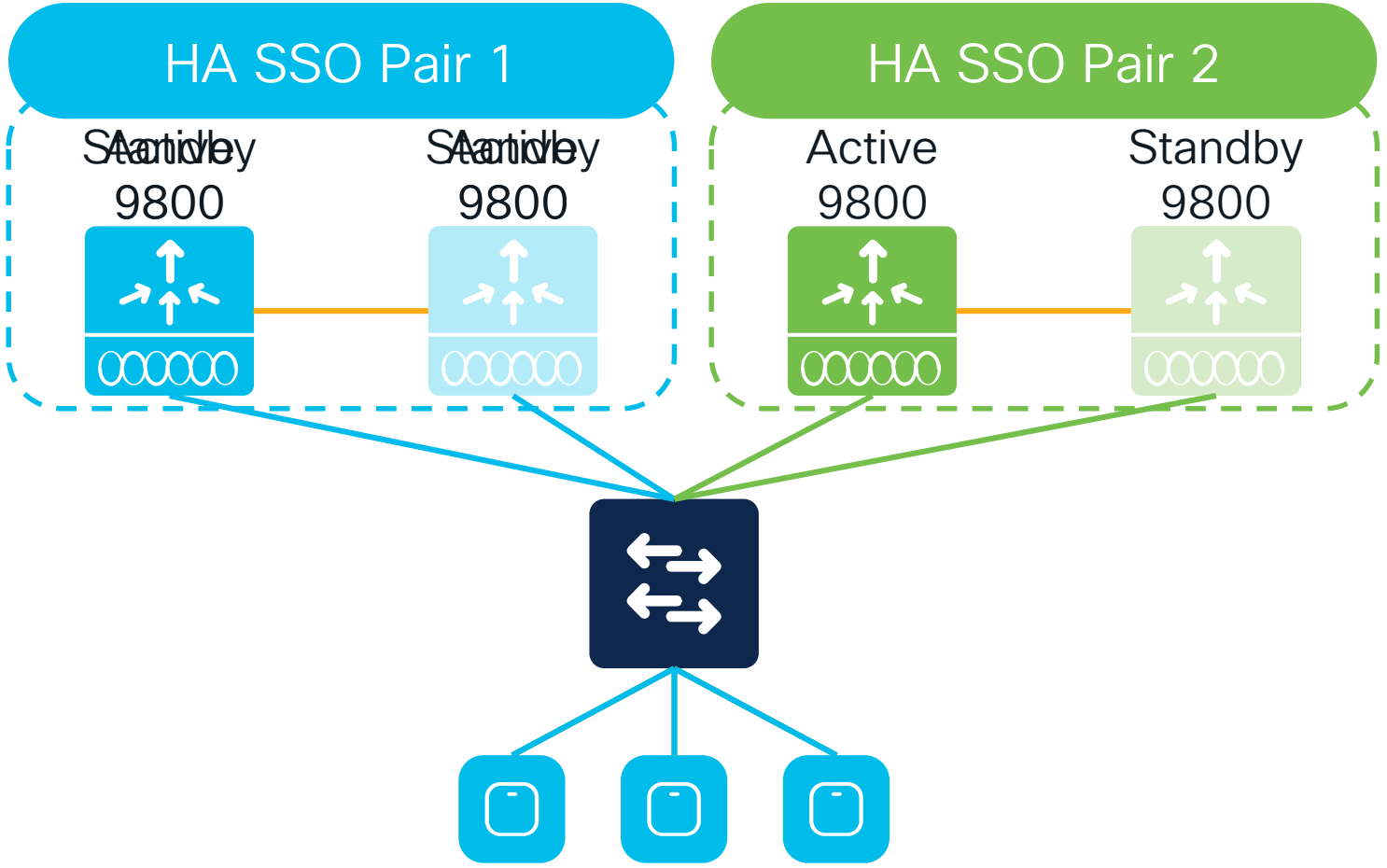
SSO best practices
Back-to-Back Redundancy Port Connections

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

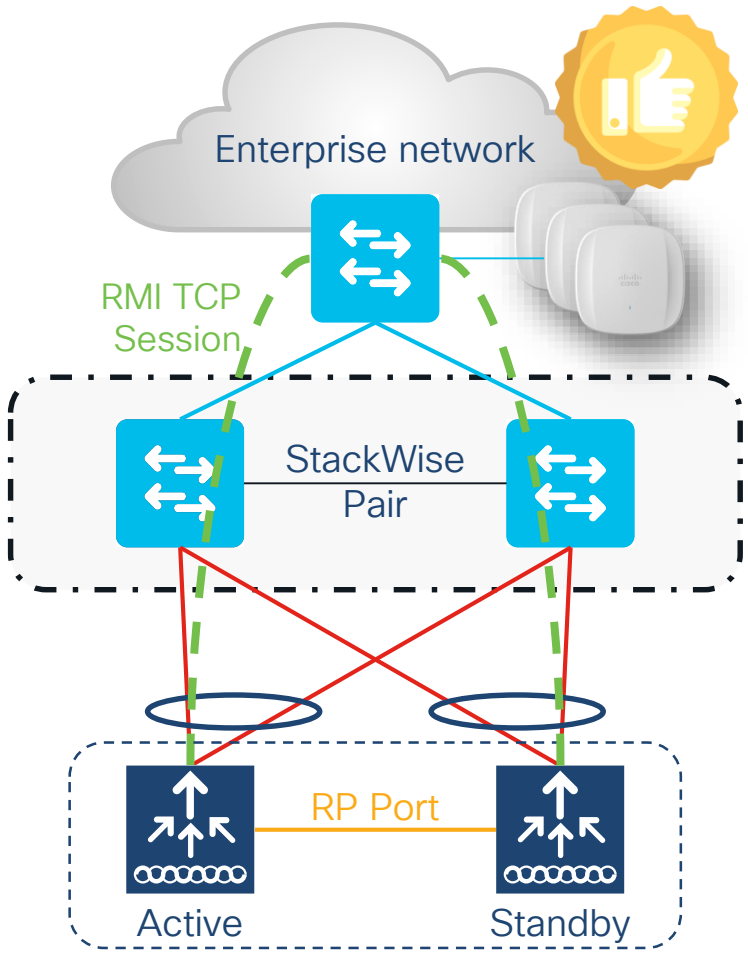


Redundancy with HA SSO and N+1

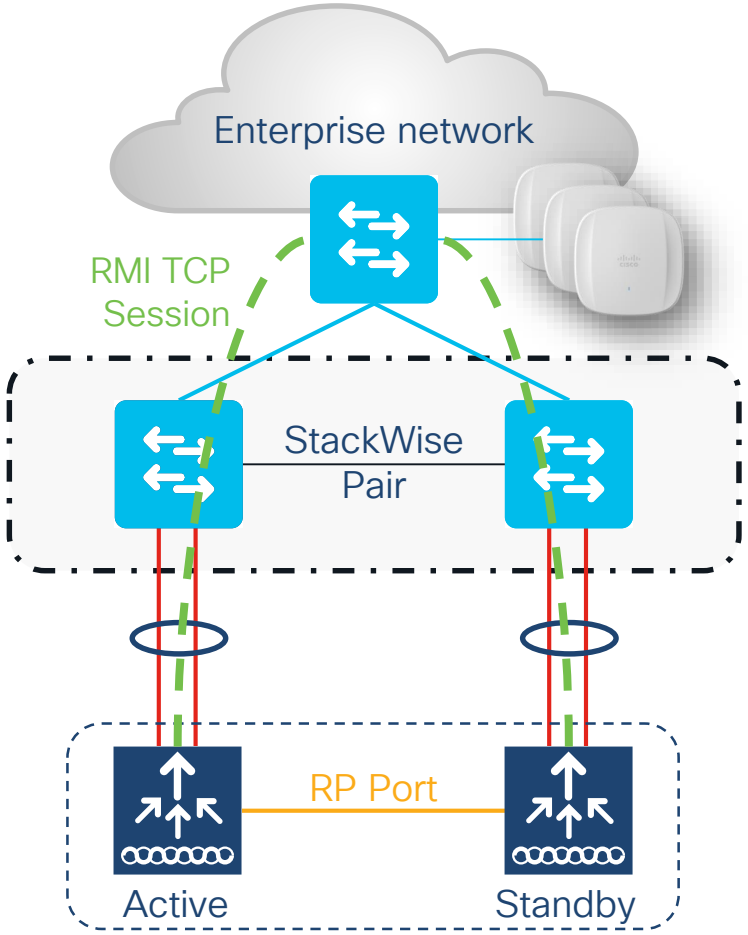
- Highest redundancy model
- Take advantage of sub-second failover
- Redundancy in the event SSO New-Active fails before the Old-Active is recovered
- Hitless upgrades for non-ISSU releases



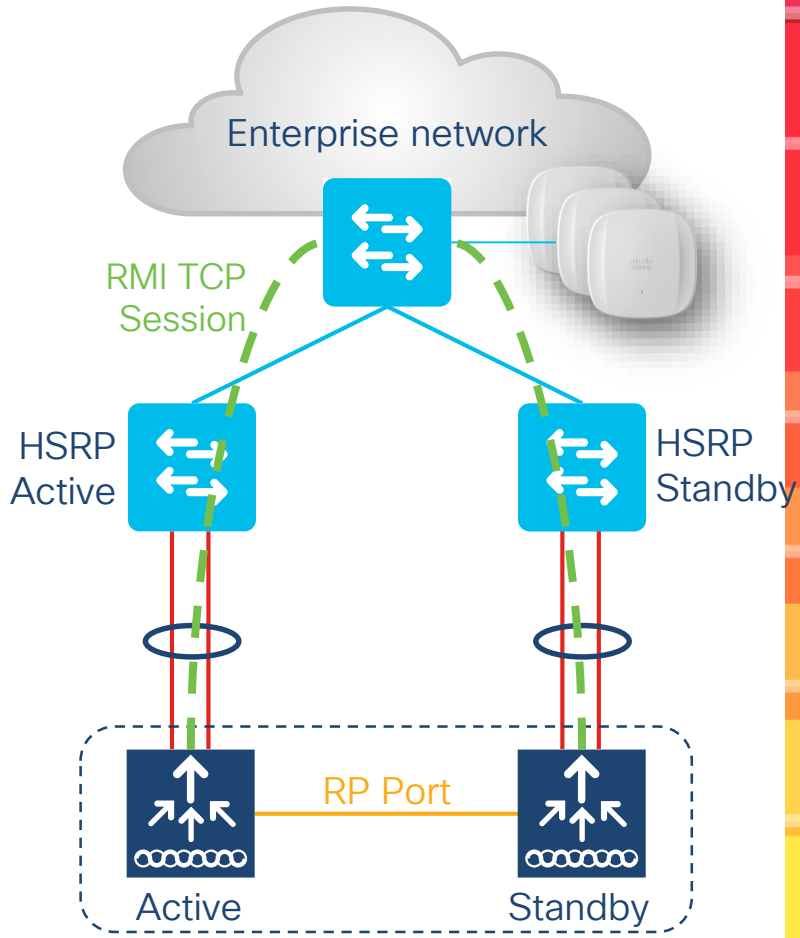
Connecting WLCs to Rest of Network



StackWise Pair with Split links



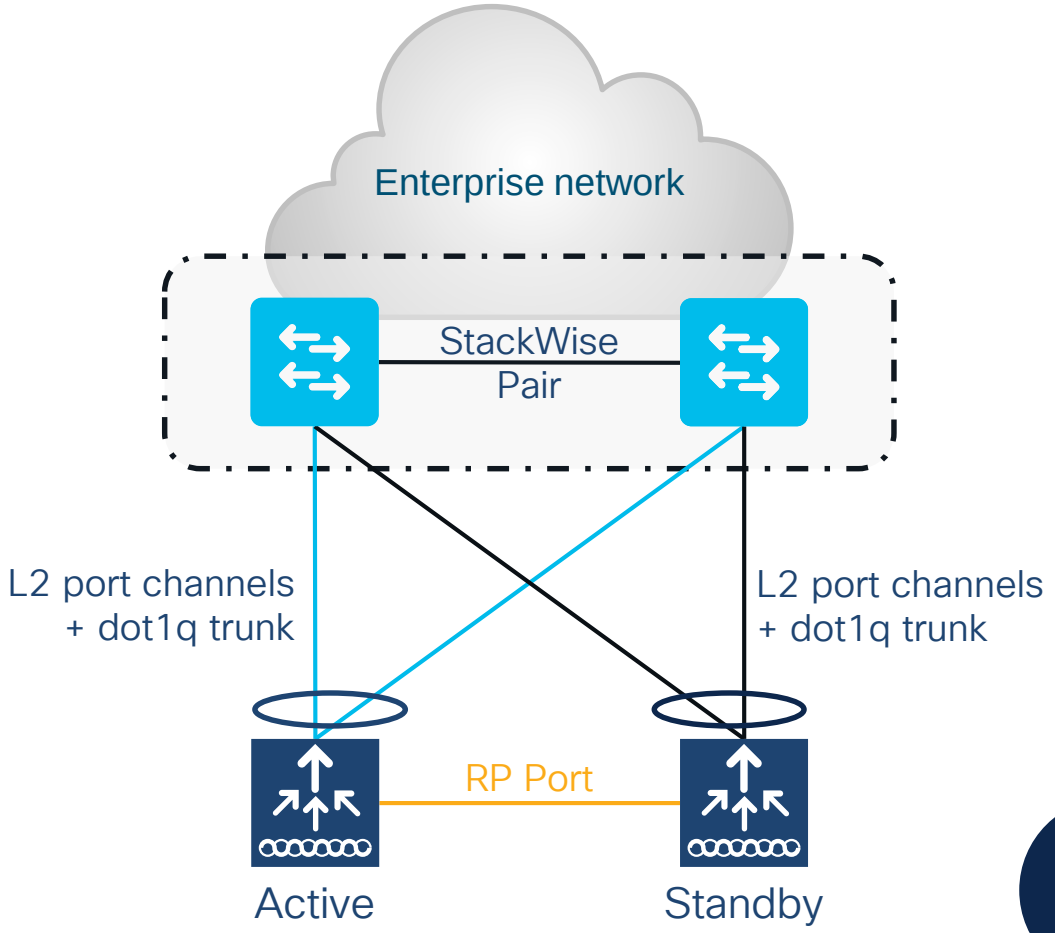
StackWise Pair without Split links



HSRP

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

StackWise Pair with split links
SSO HA Pair



Recommended

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

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

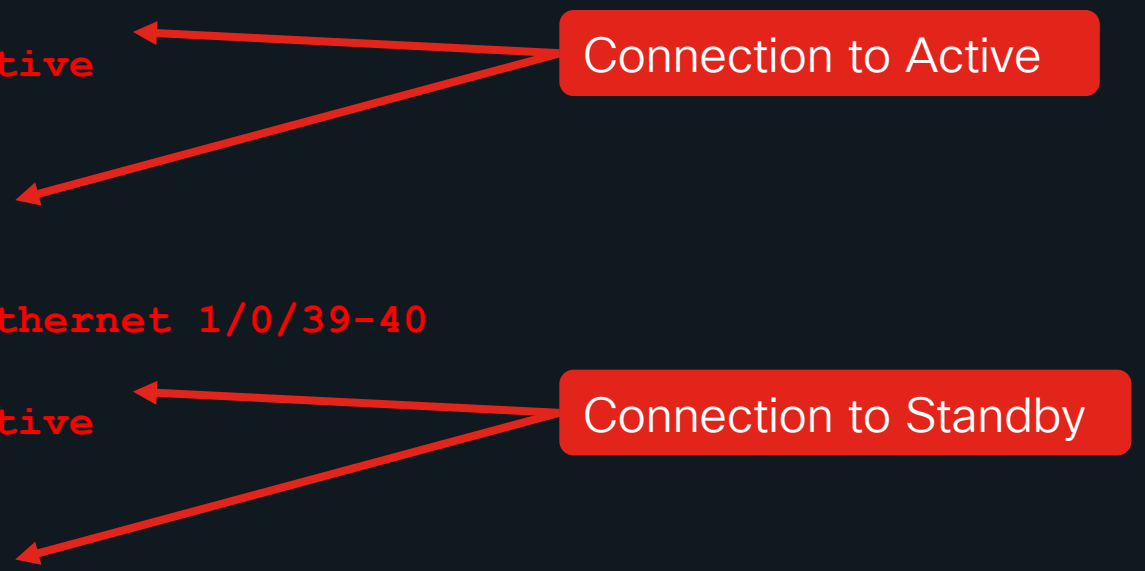
Configuring the Port Channel on C9800 HA SSO
Example

```
C9800# configure terminal
C9800(config)# interface TenGigabitEthernet0/0/0
C9800(config-if)# switchport mode trunk
C9800(config-if)# channel-group 1 mode active

C9800(config)# interface TenGigabitEthernet0/0/0
C9800(config-if)# switchport mode trunk
C9800(config-if)# channel-group 1 mode active

C9800(config)# interface Port-channel 1
C9800(config-if)# switchport mode trunk
```

Configurations on active and standby are synced and will be identical

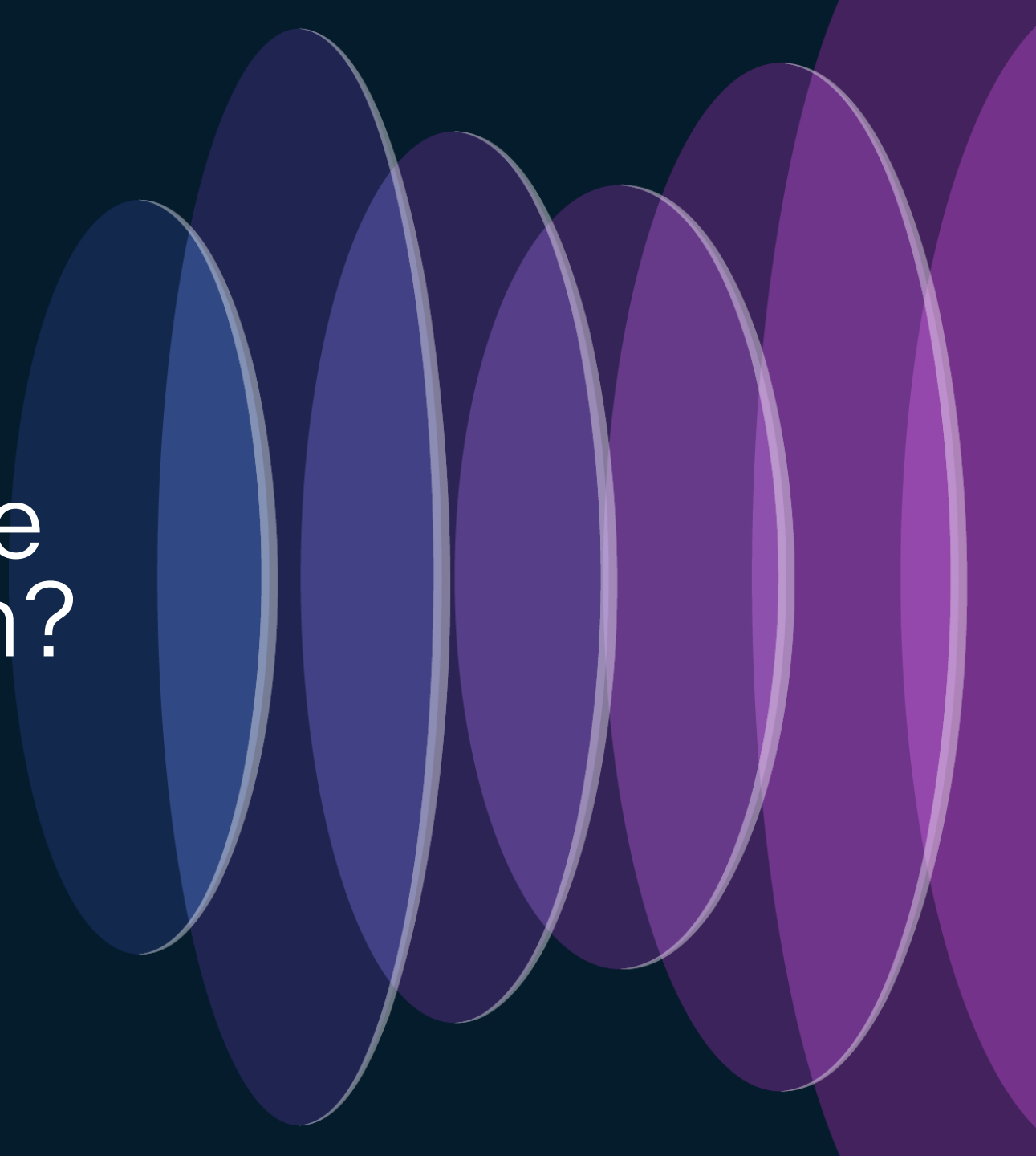
Configuring the Port Channel on Upstream Switch
Example

```
Switch# configure terminal
Switch(config)# interface range TenGigabitEthernet 1/0/37-38
Switch(config-if)# switchport mode trunk
Switch(config-if)# channel-group 11 mode Active

Switch(config)# interface Port-channel 11
Switch(config-if)# switchport mode trunk

Switch(config)# interface range TenGigabitEthernet 1/0/39-40
Switch(config-if)# switchport mode trunk
Switch(config-if)# channel-group 12 mode Active

Switch(config)# interface Port-channel 12
Switch(config-if)# switchport mode trunk
```



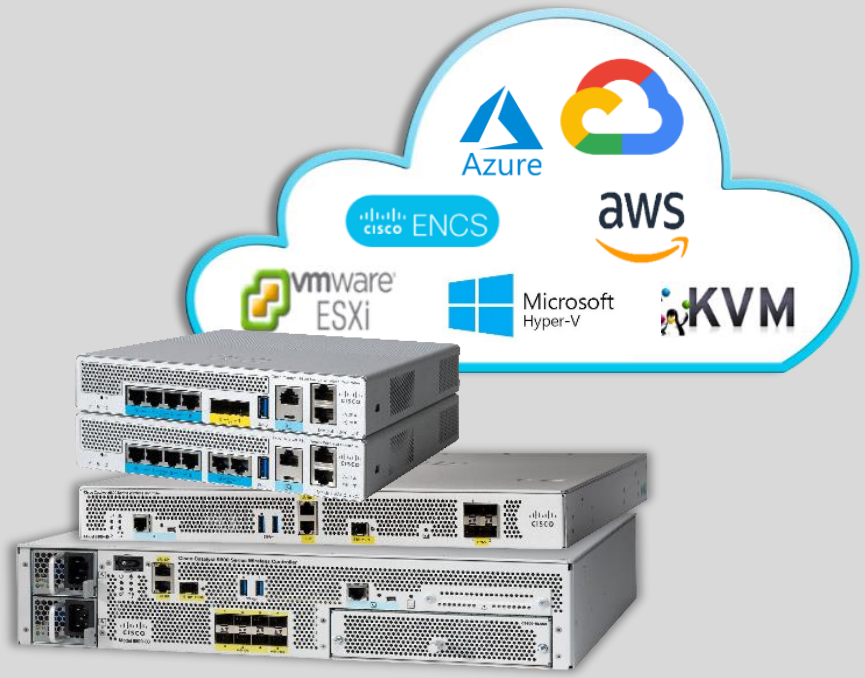
Connections to the Active and Standby Chassis must be kept on separate Port Channels (stack or not)

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



cisco Live!

Wi-Fi 6/6E runs on Cisco Catalyst Wireless



Catalyst 9800
Wireless LAN Controller (WLC)

Supported Access Points

Wi-Fi 6/6E

C9136

CW9166/64

CW9162

Wi-Fi 6

9130

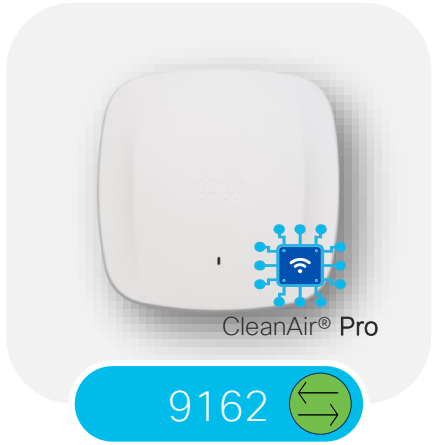
9124

9120

9115

9105

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



Indoor Access Points

Outdoor Access Points

Management mode can be changed

Catalyst 6E Access Points
Enabling New Experiences

Cisco CleanAir® Pro

Dedicated tri-band radio for intelligent packet capture and spectrum analysis for rapid troubleshooting

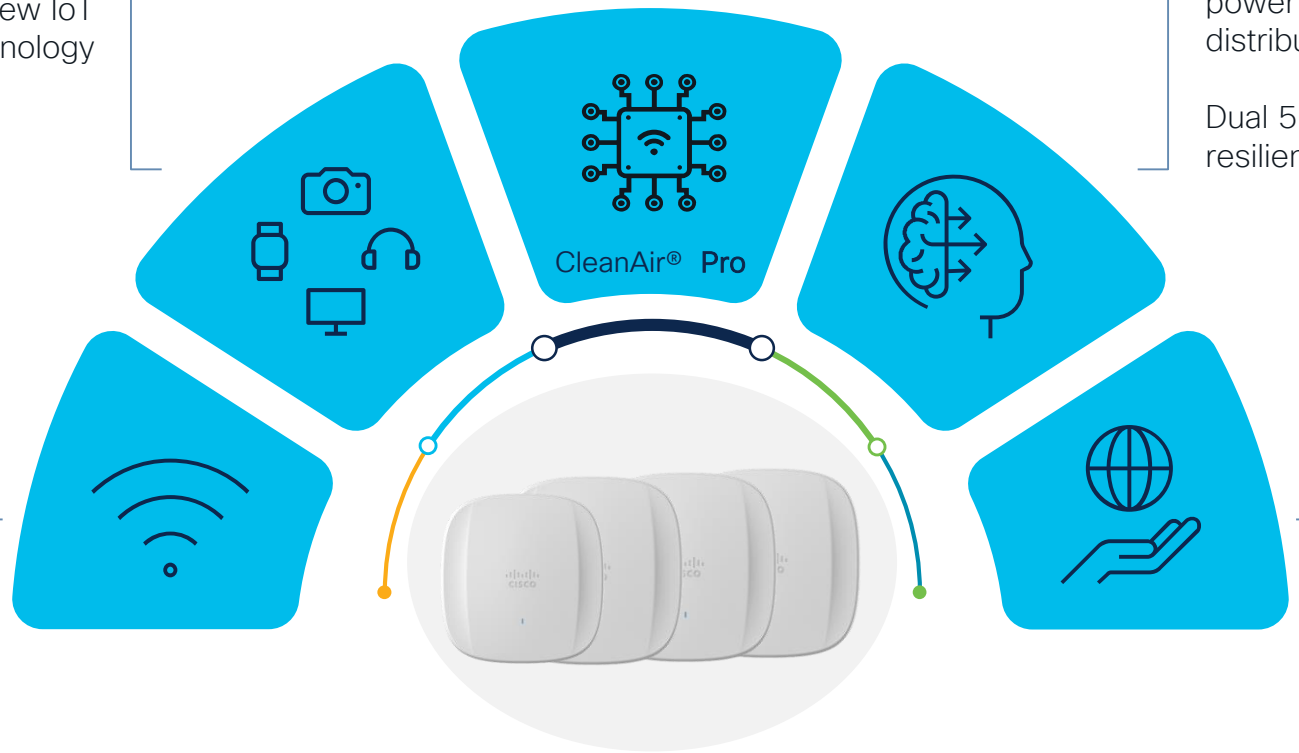
Multilingual IoT radios

Third-generation IoT 802.15.4 radio USB with up to 9W for new IoT technology

Smart, resilient infrastructure

AP power optimizations for power savings and distribution

Dual 5-Gbps uplink ports for resiliency (9136)



Unmatched Wi-Fi experience

Up to 16-stream tri-band concurrent

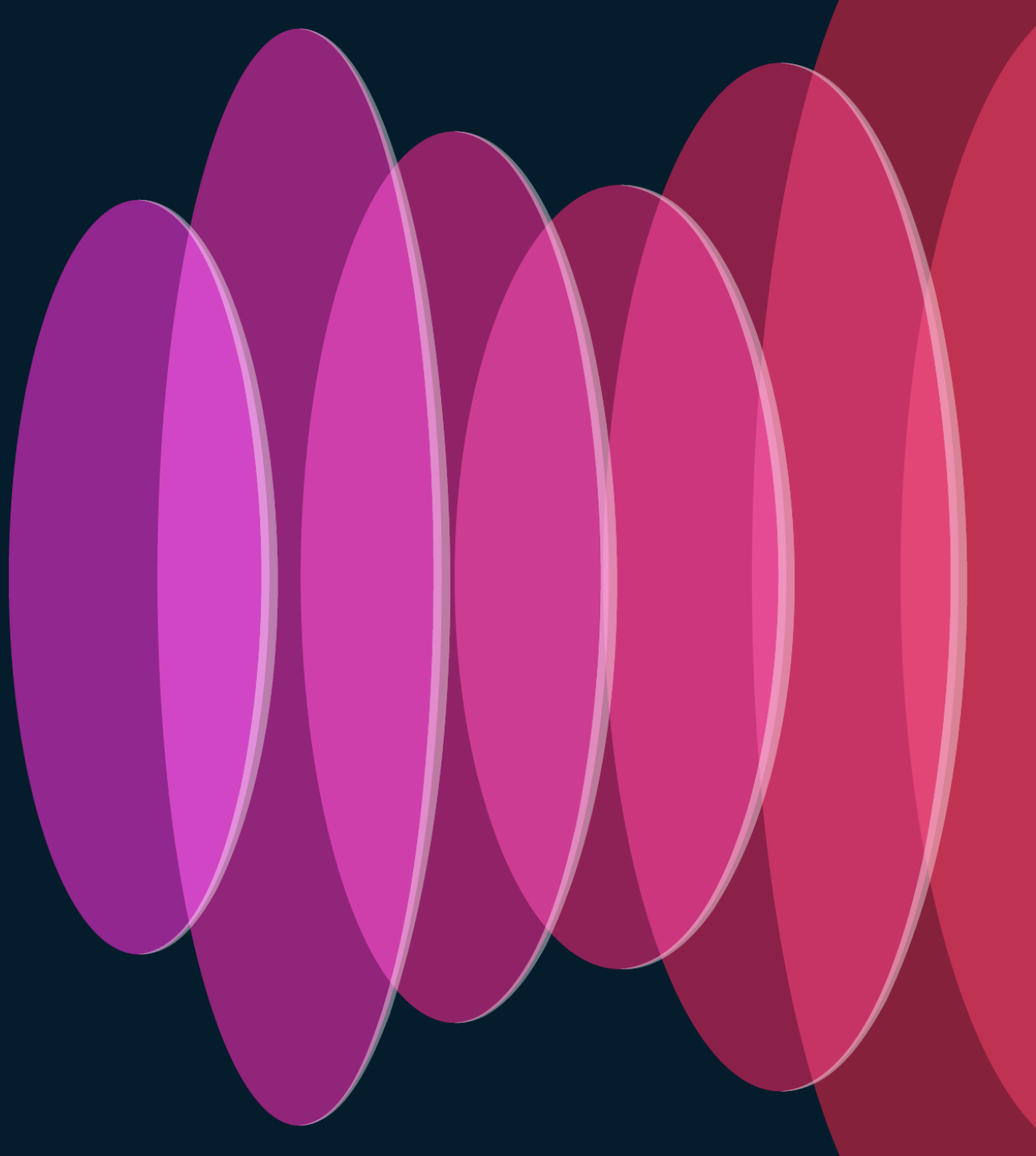
XOR and Flexible Radio Assignment (FRA) for changing needs

WPA3 security

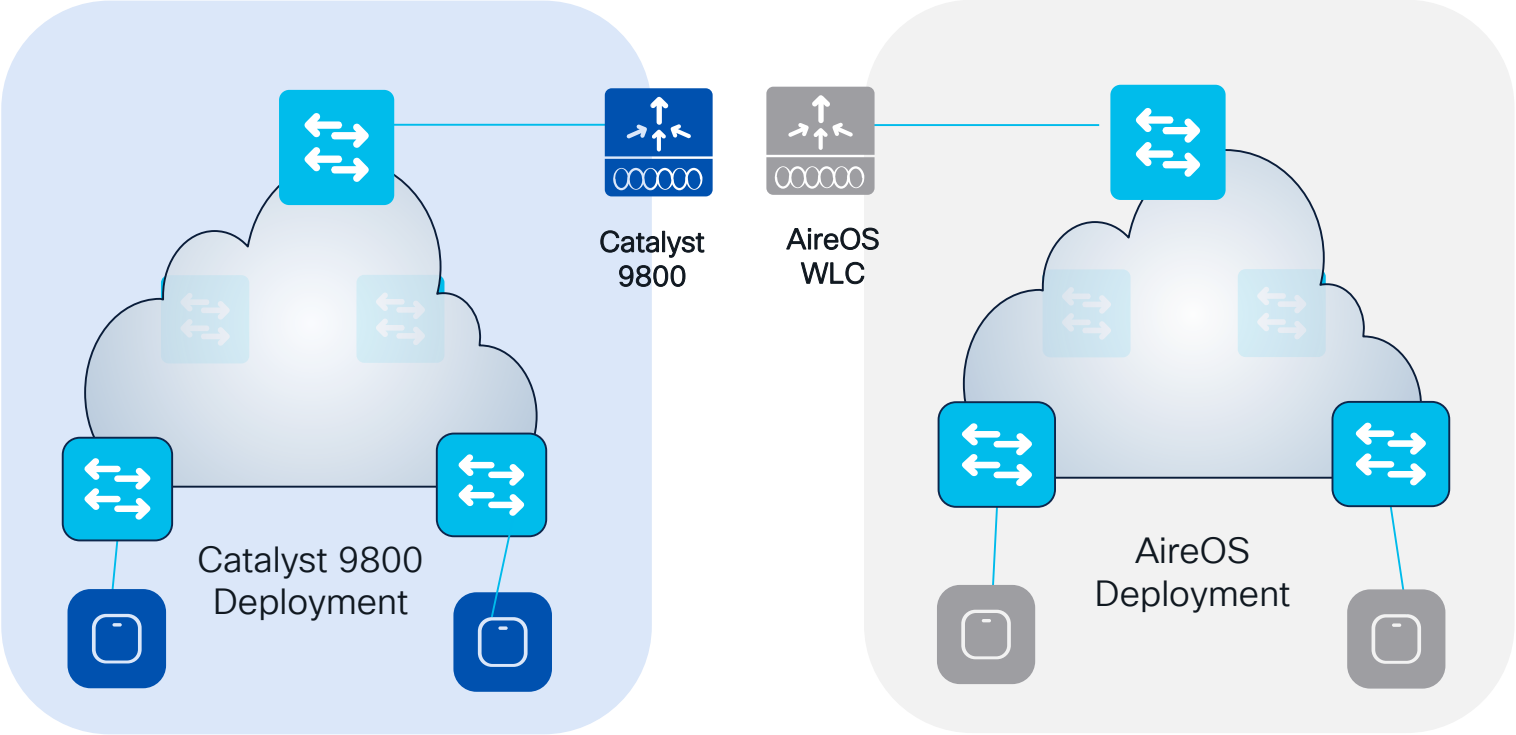
Environmental sensors

Air quality sensor for HVAC integration
Temperature, humidity sensors

What if I still have older controllers?



AireOS and IOS-XE coexistence



Primary questions:

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

Inter Release Controller Mobility (IRCM) is your friend!

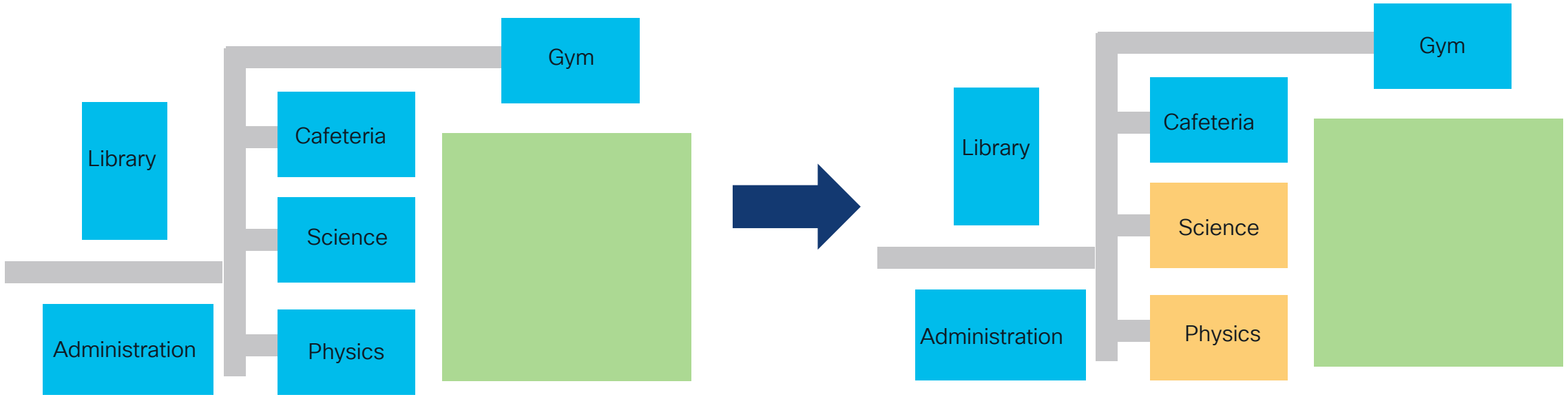
RRM = Radio Resource Management

Customer Migration Scenario

2.4/5 GHz

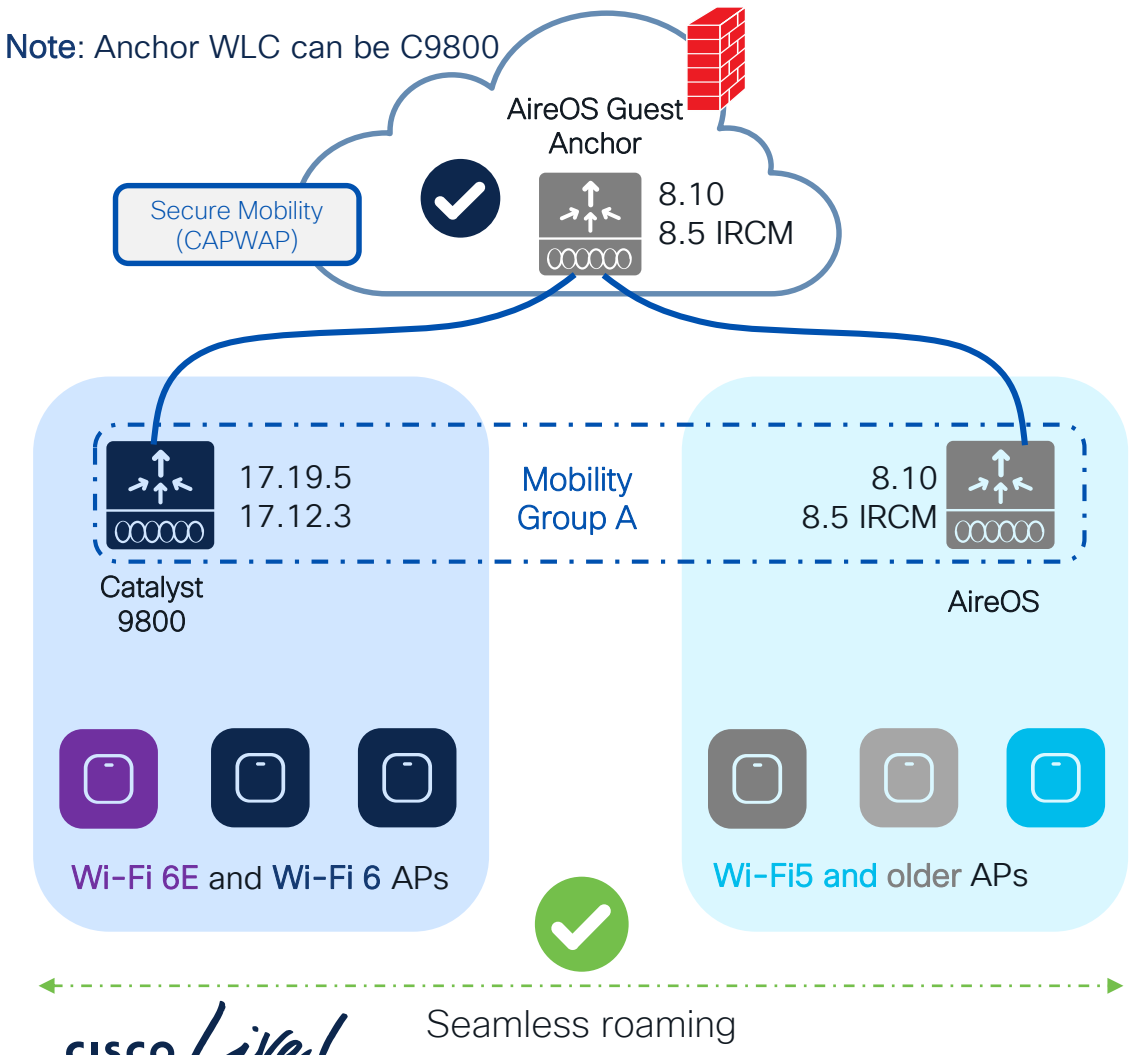
2.4/5/6 GHz

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



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

How do I start adopting 6GHz?
Answer: Inter Release Controller Mobility (IRCM)

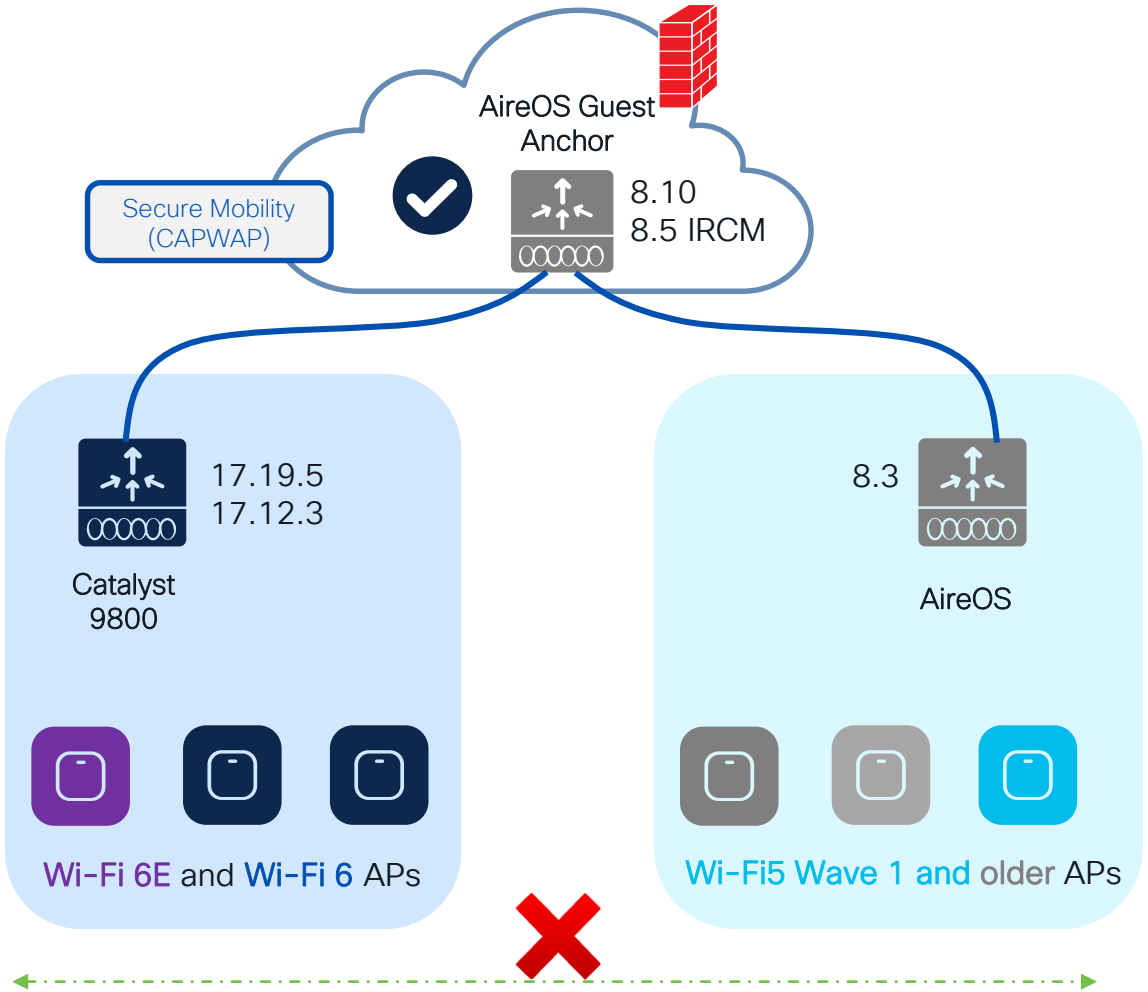


Scenario 1: Legacy Controller Supports IRCM

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

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

How do I start adopting 6GHz?
Answer: Inter Release Controller Mobility (IRCM)

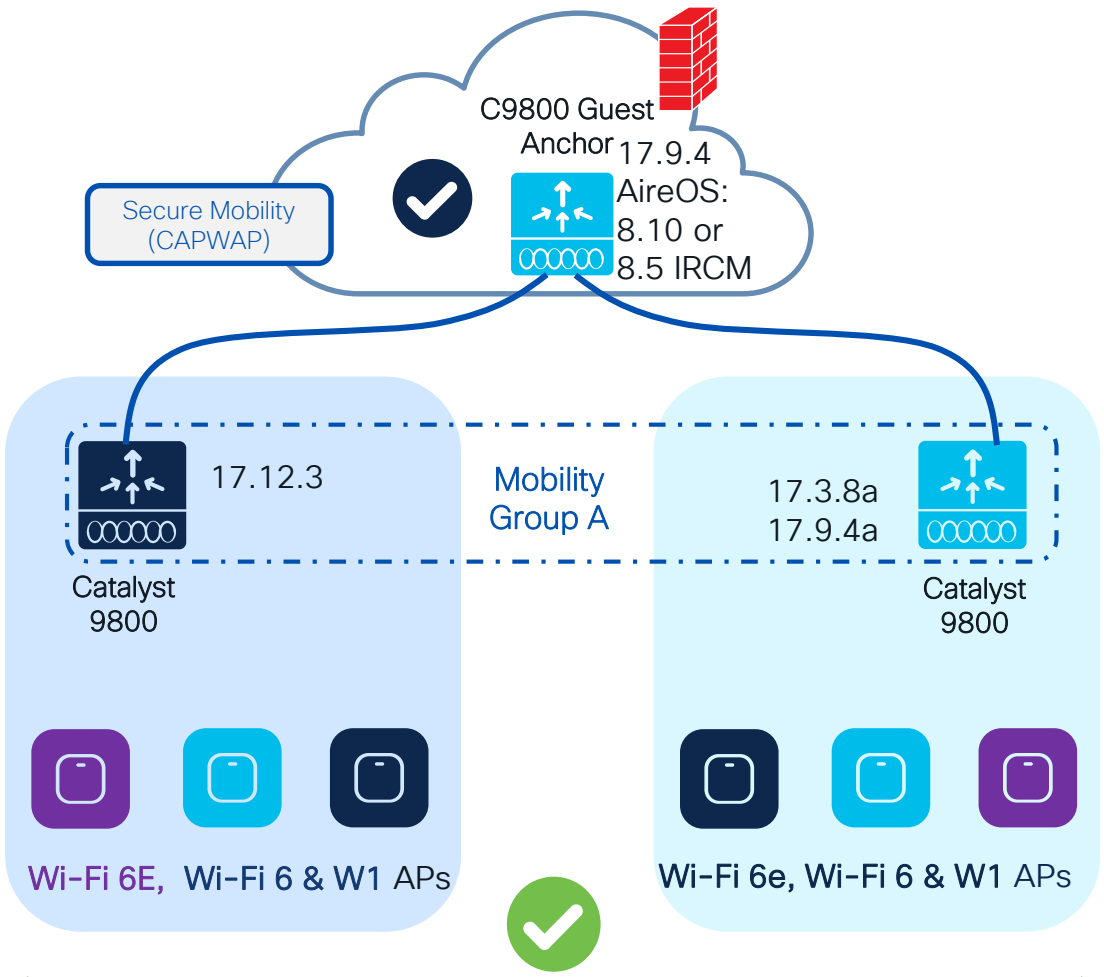


Scenario 2: Legacy Controller not supporting IRCM

- Not possible to establish IRCM between old controller and new 9800 handling 6E Aps
- Limits options available. Forces more aggressive migration process.
- Migration alternatives:
  - Keep the two networks separated ; migrate physical RF areas as new Aps are added.
  - Roaming is not possible.
  - Avoid migrations “per floor” as in most building types, it is normal to see clients roaming between Aps on different floor.
  - Temporarily, replace the legacy controller with one that supports IRCM.
- The release combinations shown have been tested at scale, check IRCM deployment guide*

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

How do I start adopting 6GHz?
Answer: Inter Release Controller Mobility (IRCM)

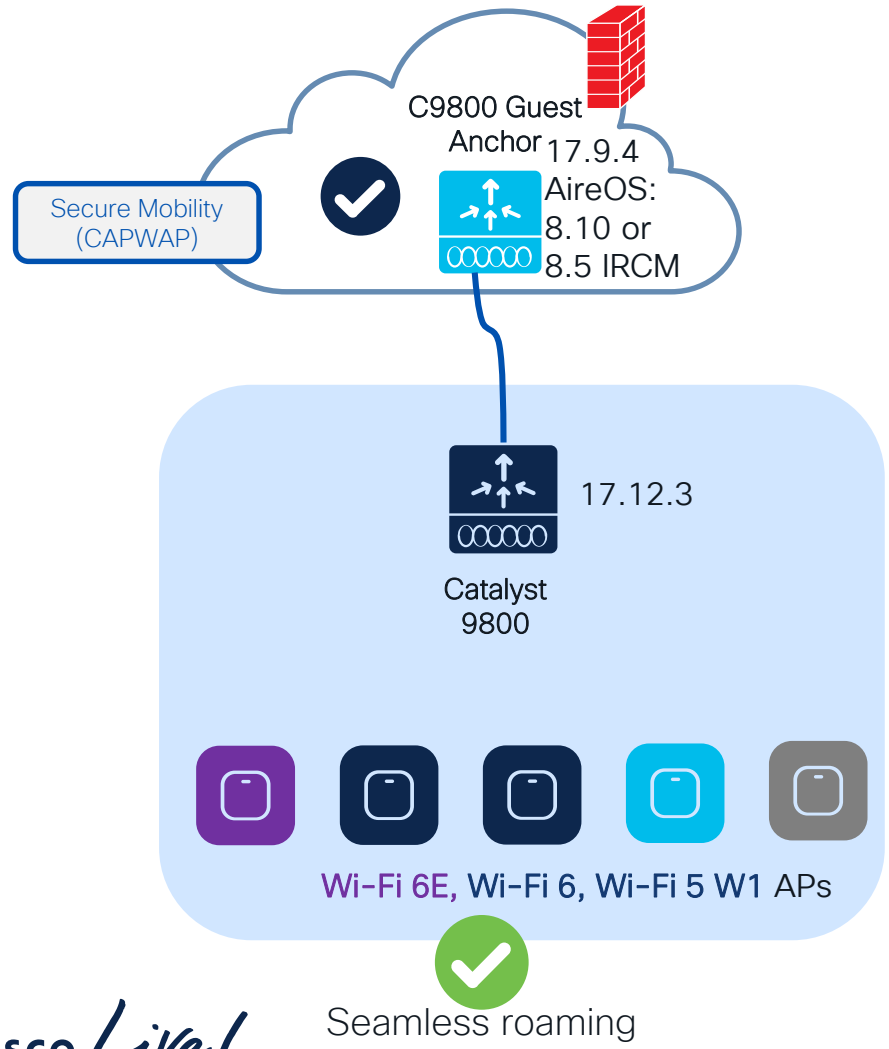


Scenario 2: If you're in IOS-XE 17.3.x, 17.6.x, 17.9.x code

- If you have already started your C9800 journey… & need to introduce CW9166D1
- Introduce new AP hardware on the new supported IOS XE release and support seamless roaming and Guest Anchor with existing C9800 networks
- The release combinations shown have been tested at scale, check IRCM deployment guide*
- Fast & secure roam will only be supported if the WLAN profile is the same on the two WLCs
- Note: Anchor can be on AireOS as well (8.10 or 8.5 IRCM latest

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

How do I start adopting 6GHz?
Answer: Inter Release Controller Mobility (IRCM)

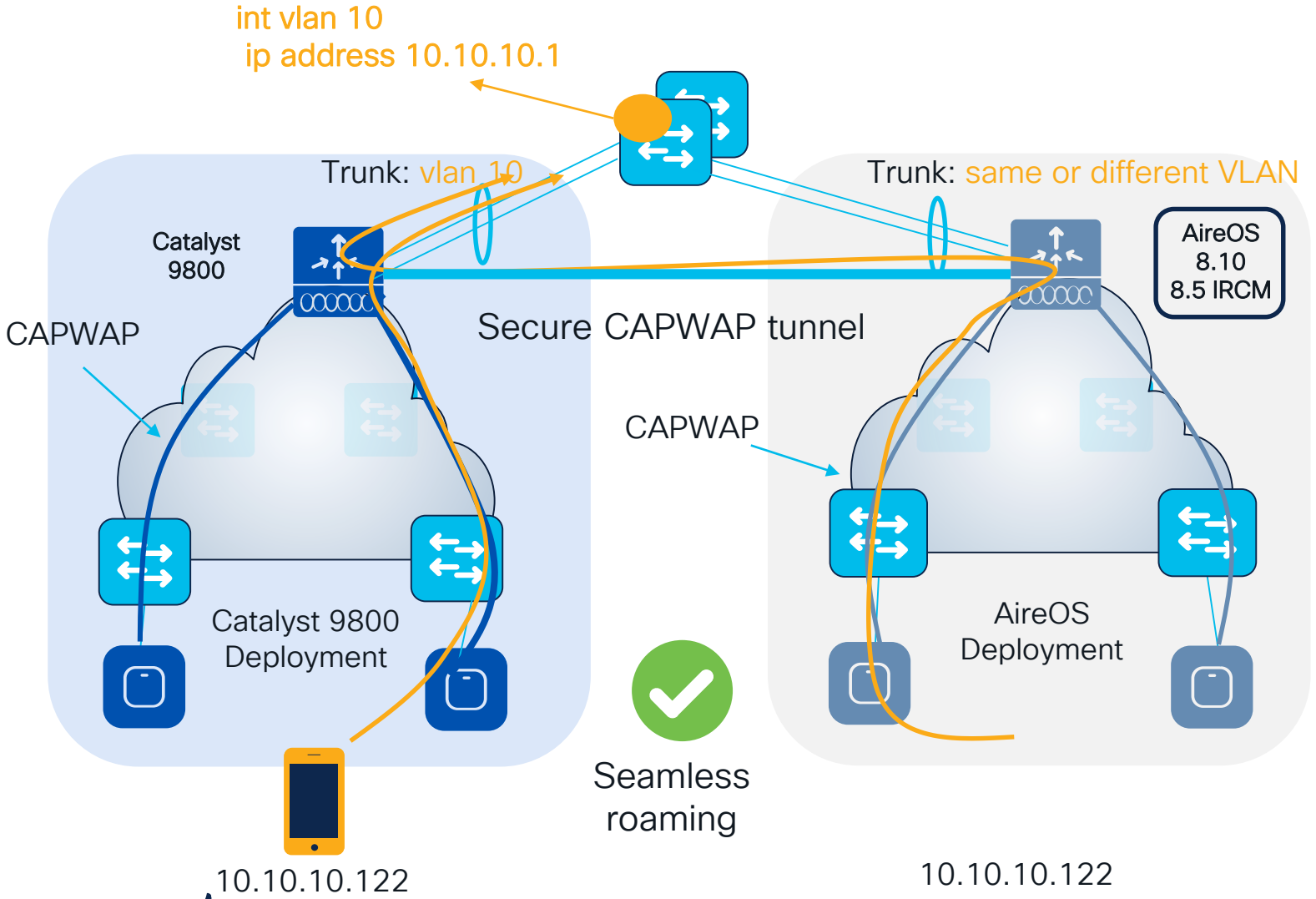


Scenario 3: If you have already started your C9800 journey

- Controller code is 17.12.3
- Wave 1 Aps support added (1700/2700/3700).
- Note: Anchor can be on AireOS as well (8.10 or 8.5 IRCM latest
- Note: 17.12.1 for APJ Countries

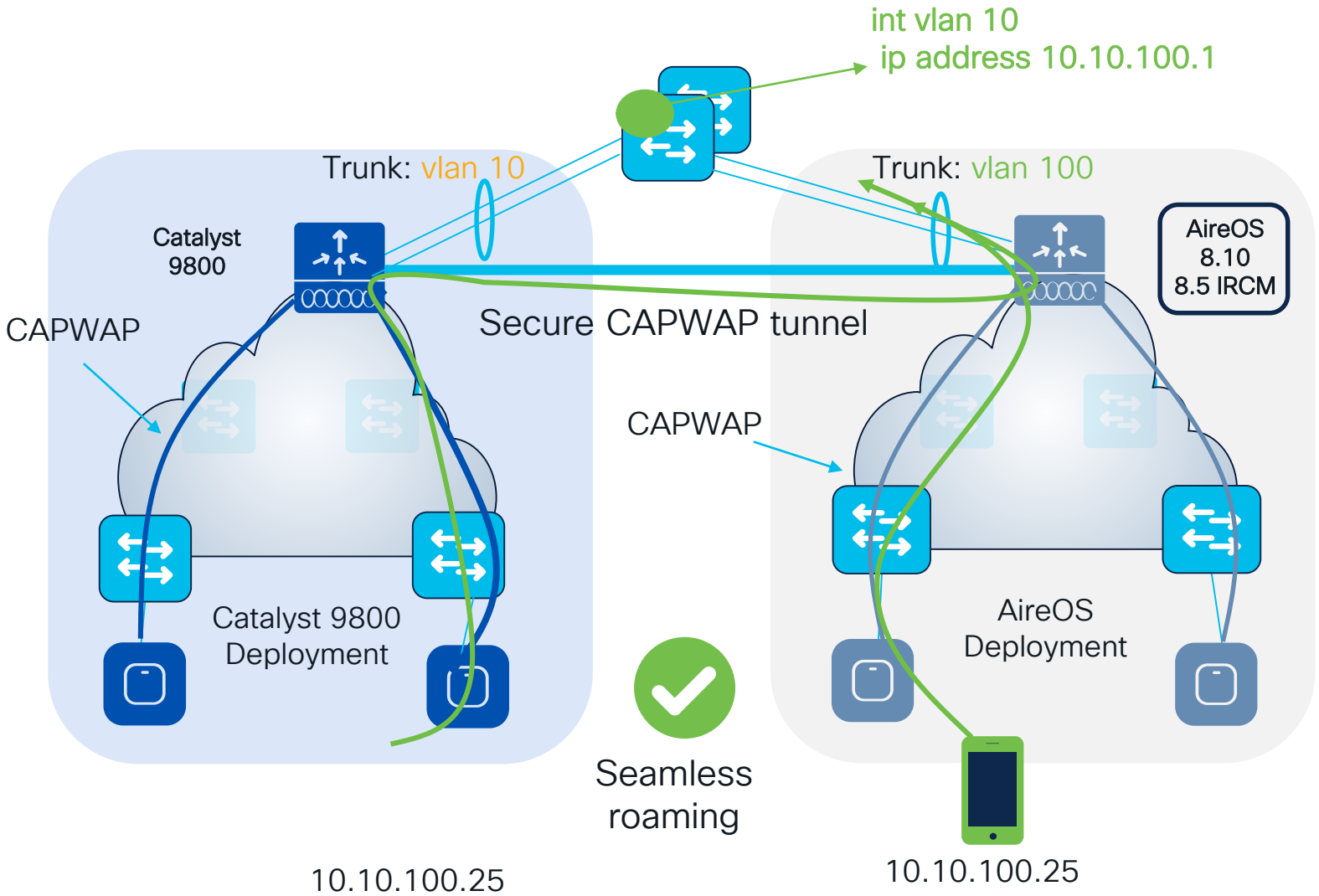
(*) https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller-aireos_ircm_dg.html

AireOS and IOS-XE coexistence – Roaming



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

AireOS and IOS-XE coexistence – Roaming

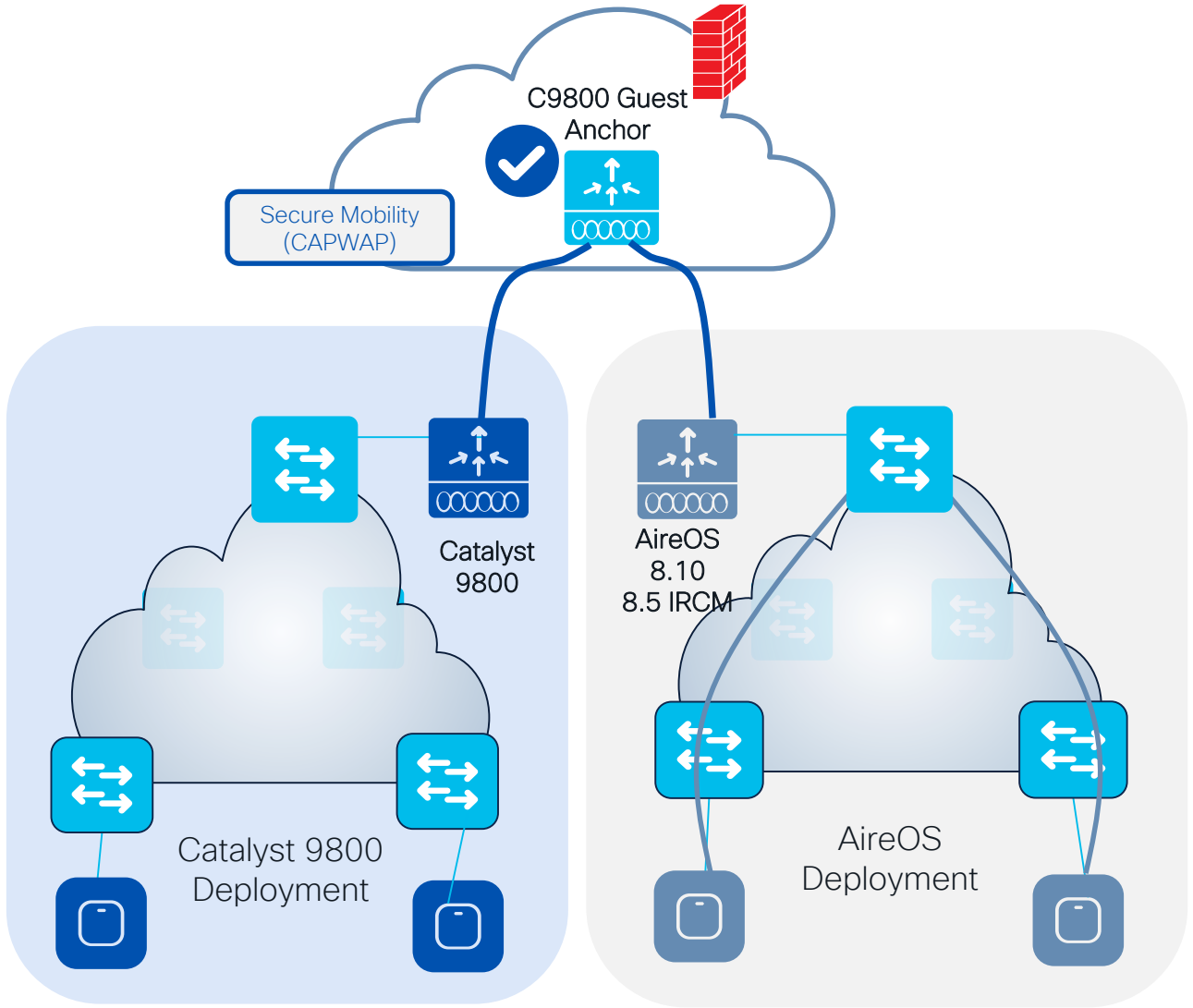


Recommendations:

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

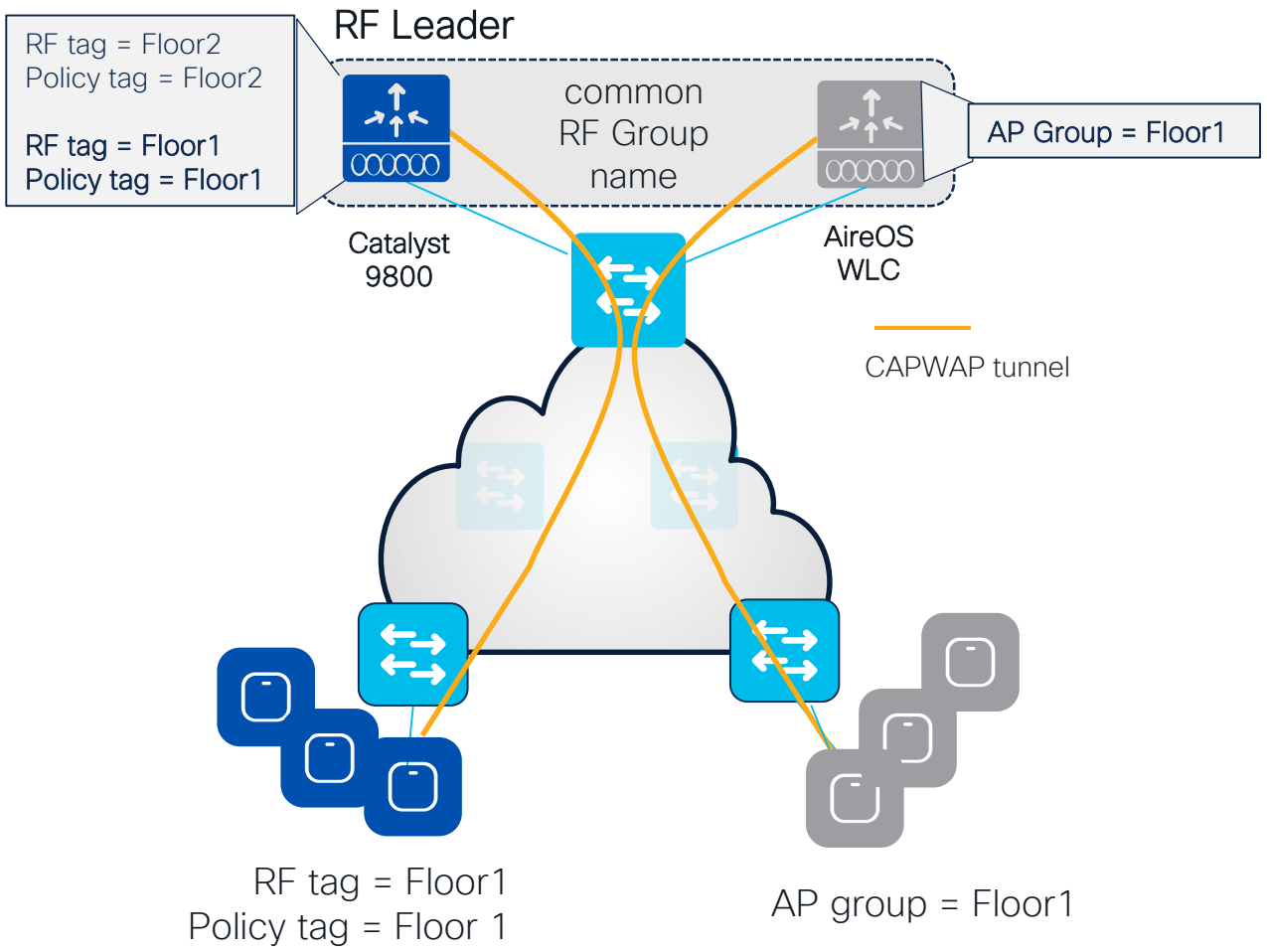
AireOS and IOS XE IRCM – Guest Anchor

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



AireOS to C9800 migration – common RF Group

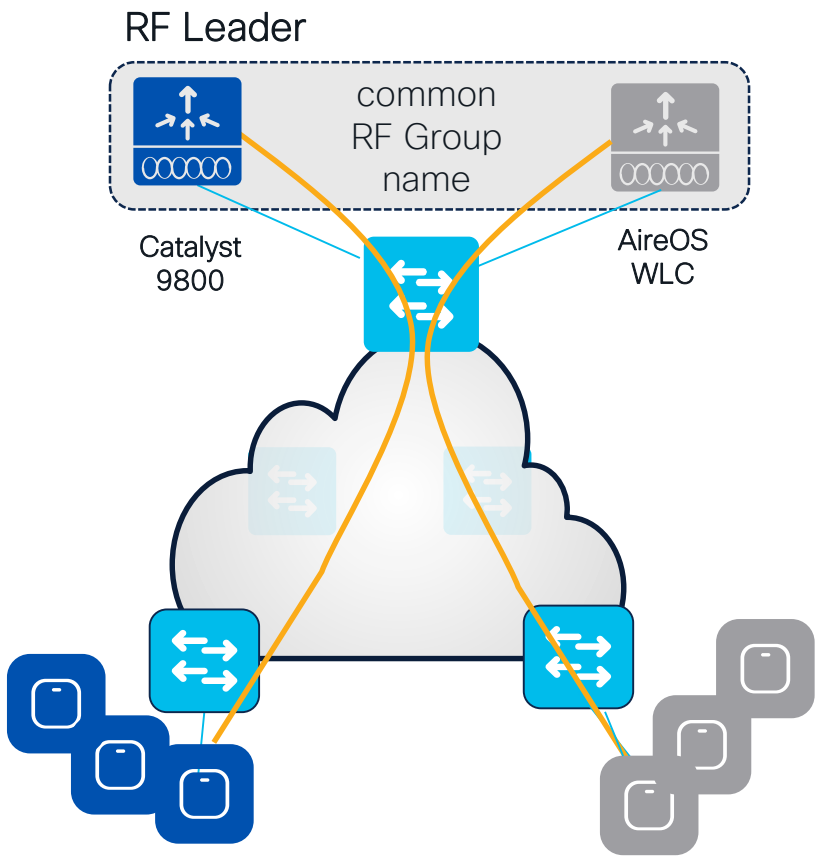
RRM works in a mixed controller environment and we can have one RF master:



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

AireOS to C9800 migration – common RF Group

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



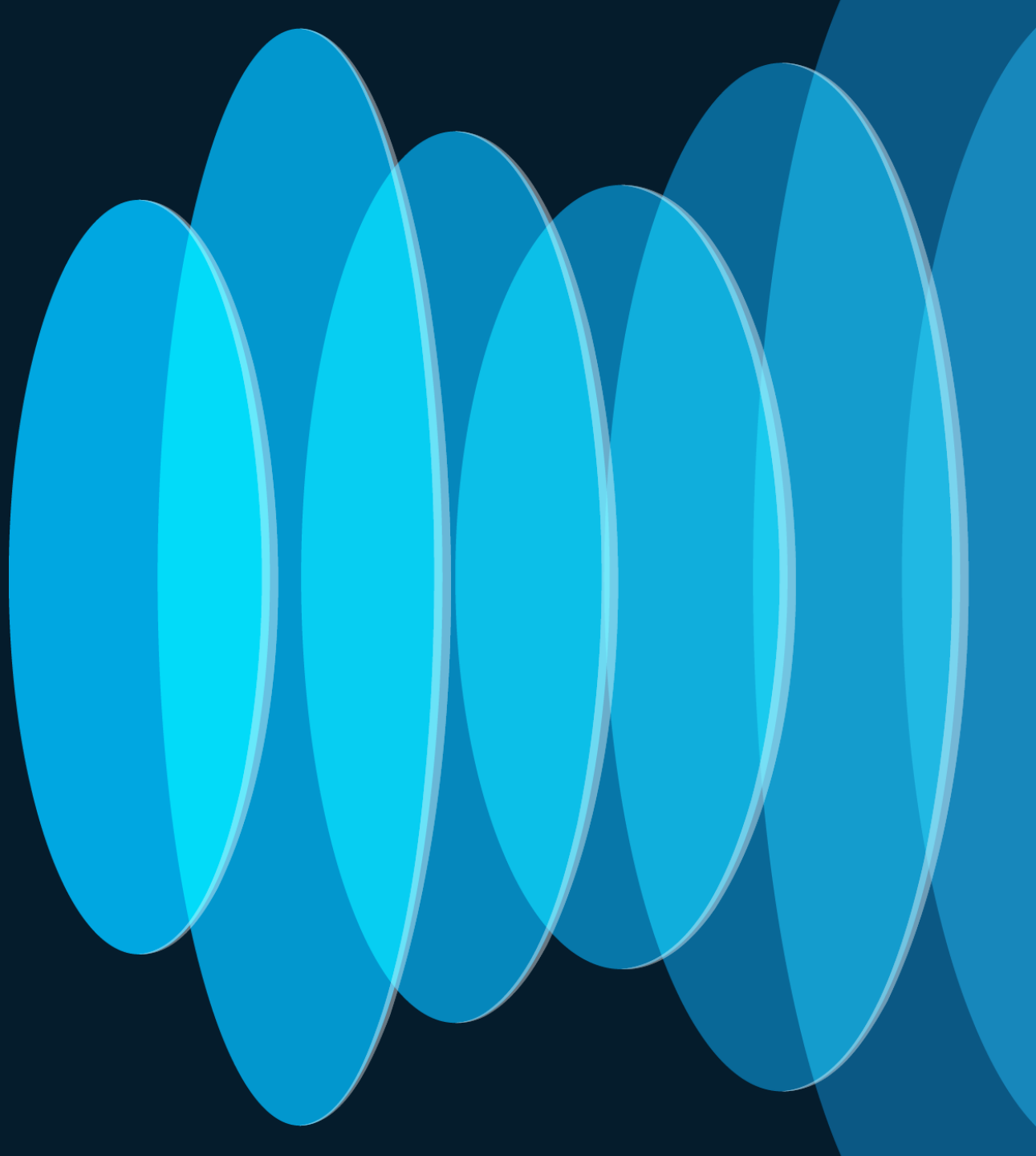
Lower priority

Higher priority

- RF Leader election happens according to this table

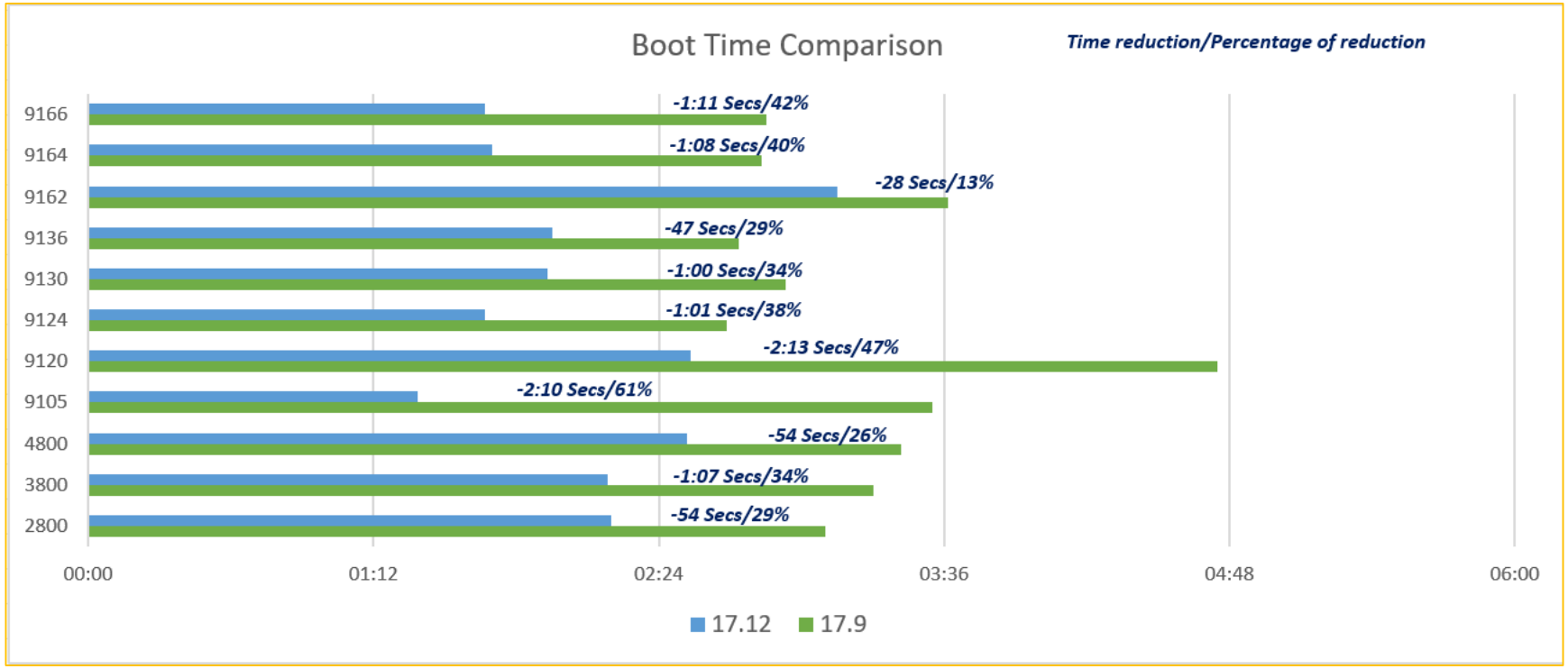
Group Leader order	Maximum AP's	Maximum AP /RF Group
3504	150	500
C9800-L	250	500
5508	500	1000
C9800-CL (Small)	1000	2000
5520	1500	3000
C9800-40	2000	4000
C9800-CL (Medium)	3000	6000
CW9800M	3000	6000
8510/8540	6000	6000
C9800-CL (Large)	6000	12000
C9800-80 CW9800H1/H2	6000	12000

Optimizations



AP Boot Time Optimization

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



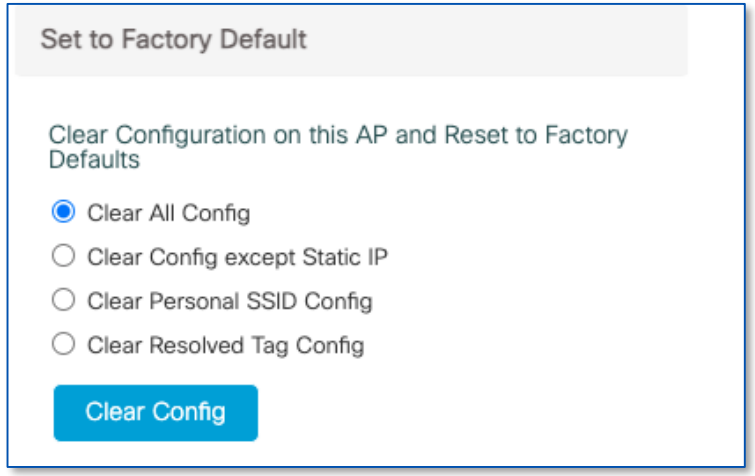
Boot Time Verification

Method to Measure

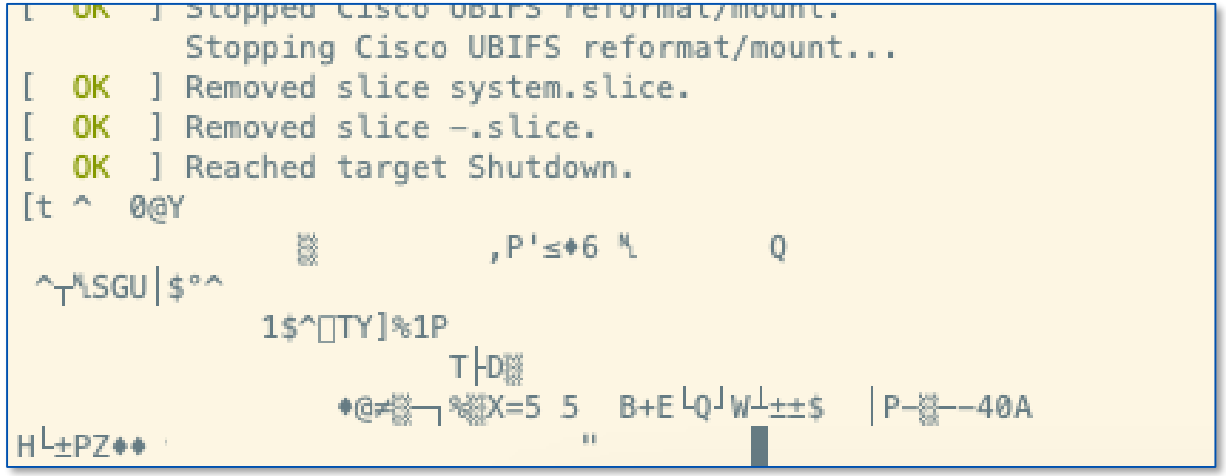
- ✓ To measure the bootup time of the Access Point, SSID beacon packets are captured from the AP
- ✓ The Access Point is tagged to broadcast a single <TEST SSID>
- ✓ A reboot of AP is initiated from the AP console
- ✓ Continuous Packet Capture is triggered on the respective channel
- ✓ Packet captures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

AP Console baud rate change

- 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.

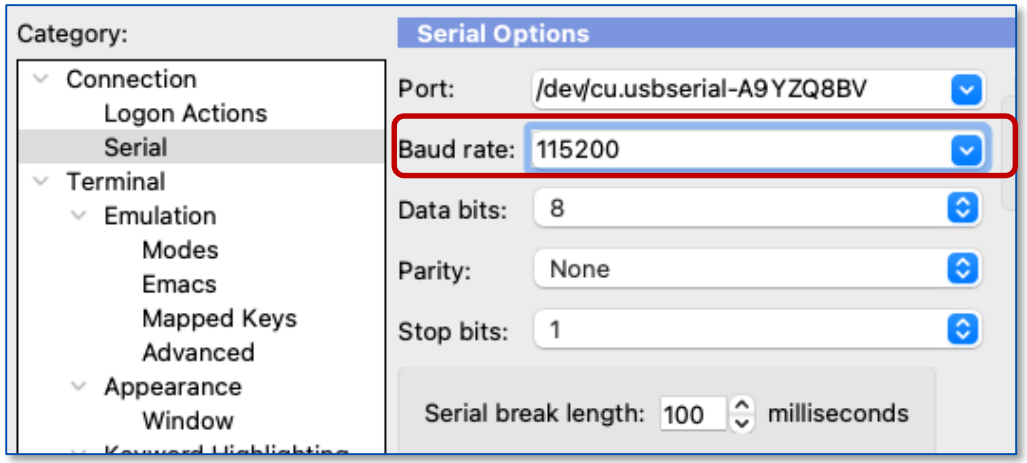


after AP reboot



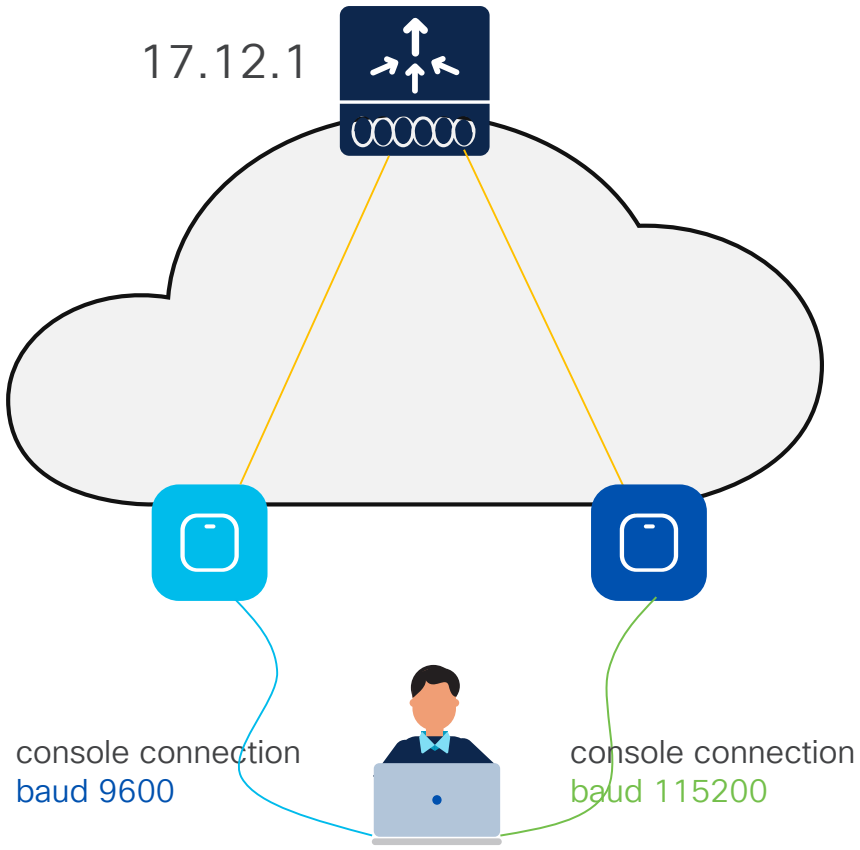
AP Console baud rate change

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



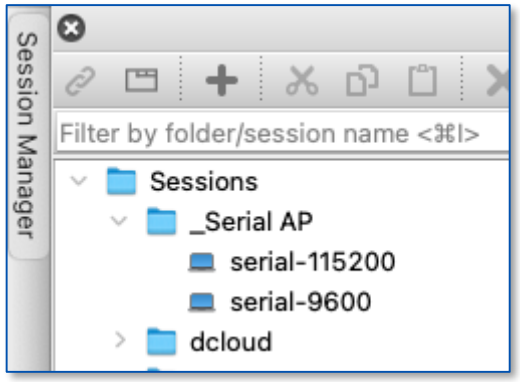
- Why? To improve boot time; depending on the AP model, you get up to 30s reduction in boot time
- How: By increasing the baud rate to 115200, the kernel and radio driver/firmware logs are printed faster and hence the AP boots faster (more info in CSCwe88390)

AP Console baud rate change



Why would you care?

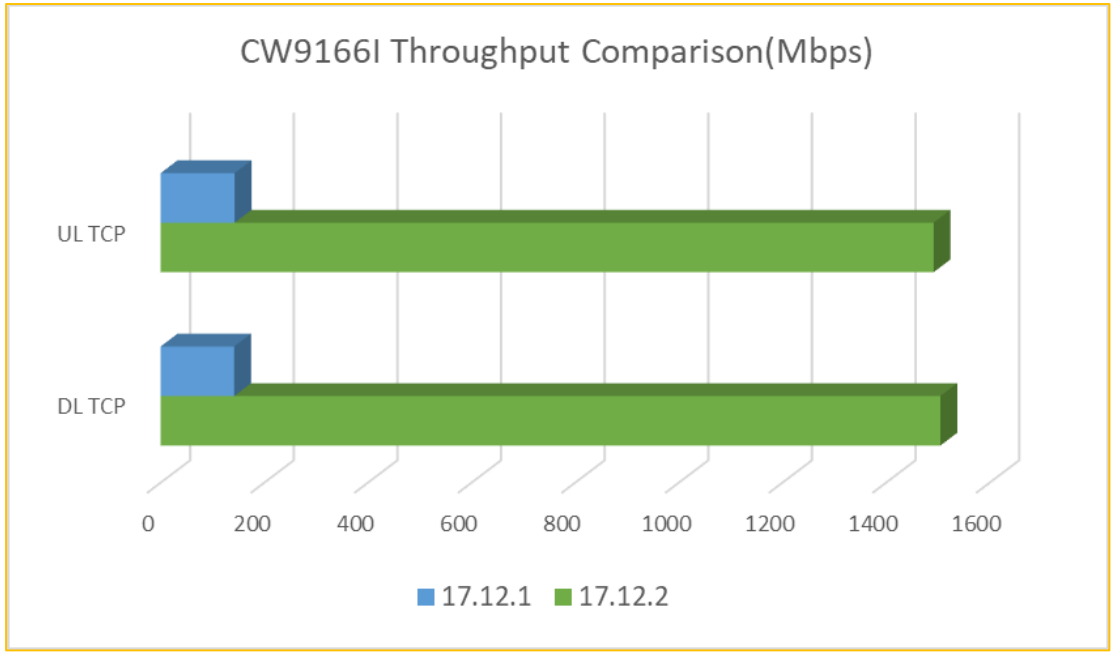
- Customer is on 17.9.4, admin is connected to AP via console with baud rate of 9600. All good
- C9800 is upgraded to 17.12.1. Existing AP still reachable with same console connection. All good
- New AP is added to the network > baud rate on new AP is automatically set to 115200
- Admin needs separate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



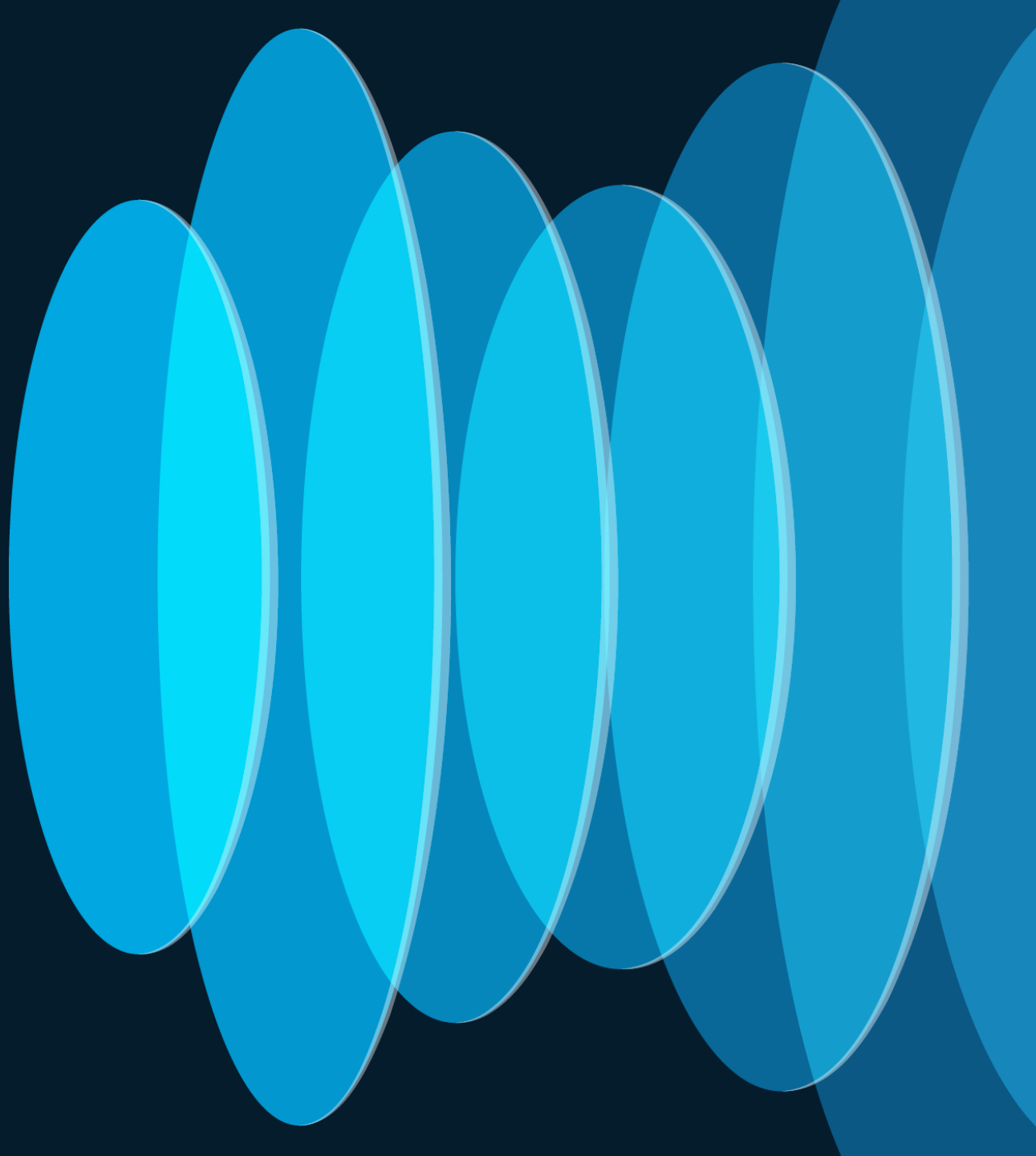
Data DTLS Performance Improvement

- ✓ For better security we can enable Data DTLS to encrypt the CAPWAP data packets between C9800 and the Access Points
- ✓ Due to the nature of the overhead involved in Data Encryption and Decryption, there will always be a slight performance degradation when enabling Data DTLS in the network
- ✓ With the optimization in 17.12.2 (17.9.4 too), the throughput results are improved with the encryption ON
- ✓ In GCM cipher, we could achieve around 10X performance increase in latest releases
- ✓ With this, the Customers can see huge raise in throughput numbers in the following ciphers

  I. ECDHE-ECDSA-AES128-GCM-SHA256
  II. ECDHE-RSA-AES128-GCM-SHA256
  III. ECDHE-ECDSA-AES256-GCM-SHA384



Wireless Product Analytics



cisco Live!

Wireless Product Analytics
Knowing product usage to serve customers better

Product Decisions for Customer benefit

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

Better Product Experiences for Customers

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

Wireless Product Analytics

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

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

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

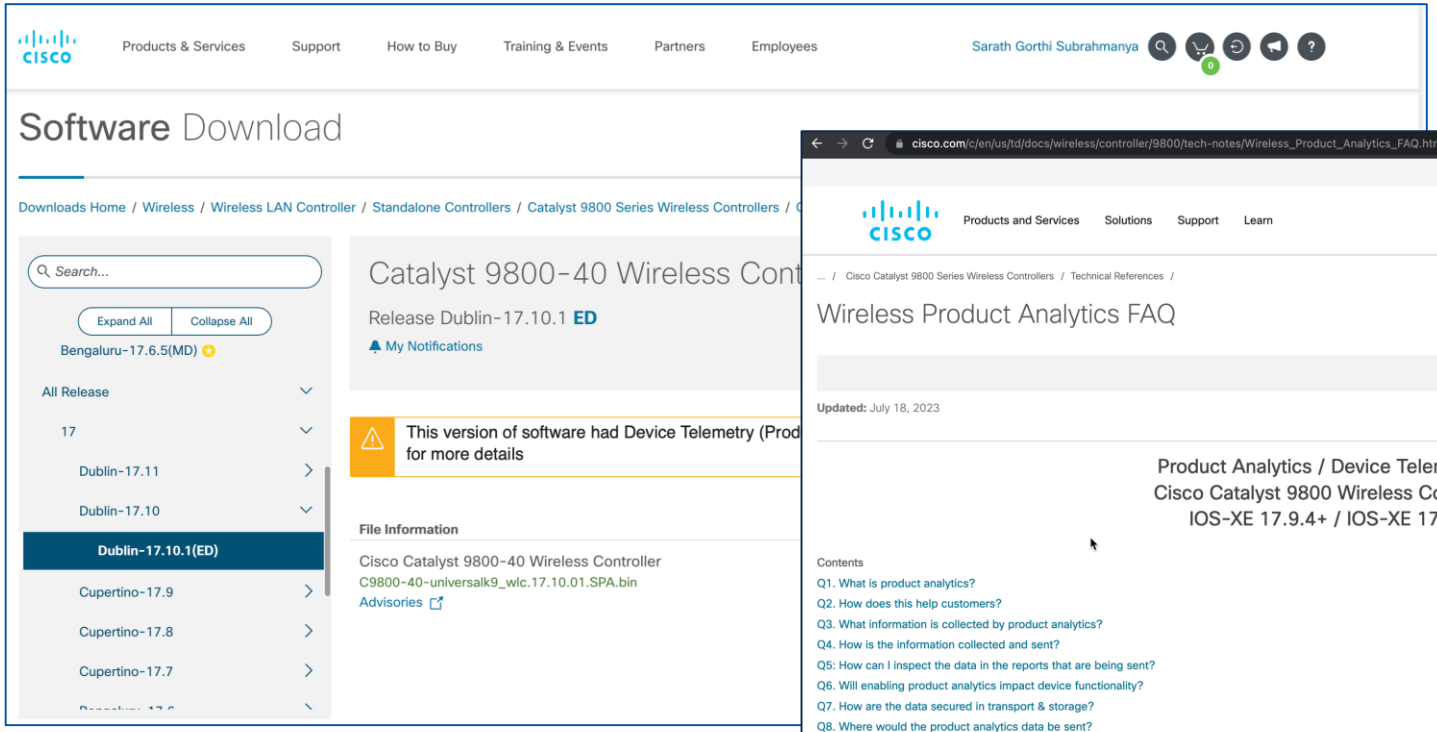
The data collected is non-PII data. CLI is present to view the report collected/ sent for transparency

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

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

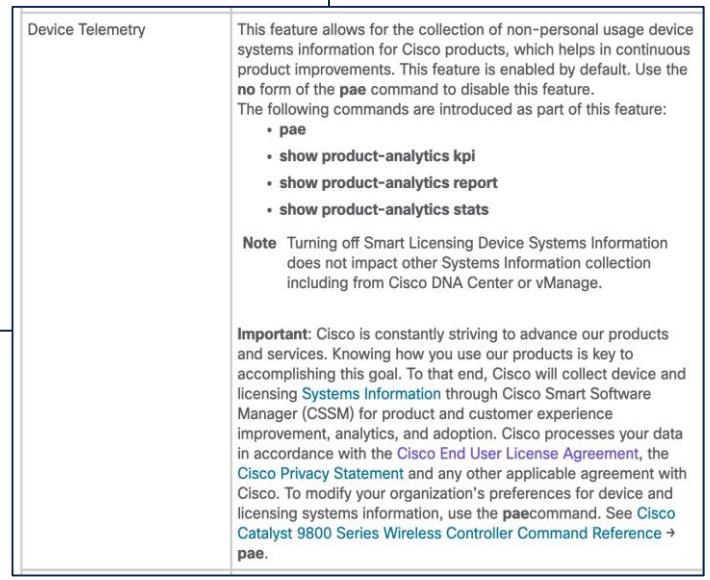
Options to disable :
Use no-form of 'pae' command - no pae
Block the URL https://dnaservices.cisco.com

Wireless Product Analytics - Documentation



Banner on software download

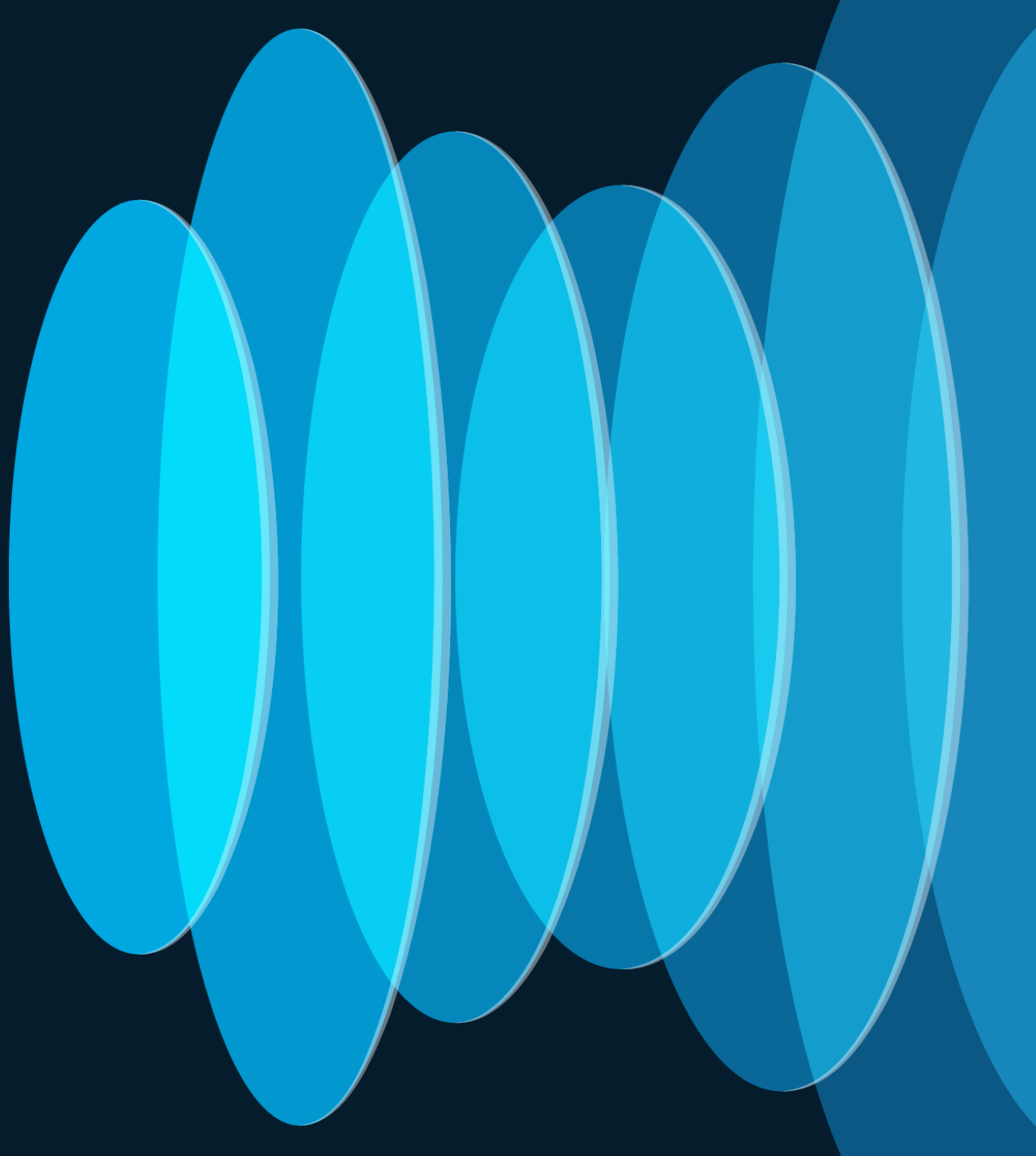
FAQs



Release Notes

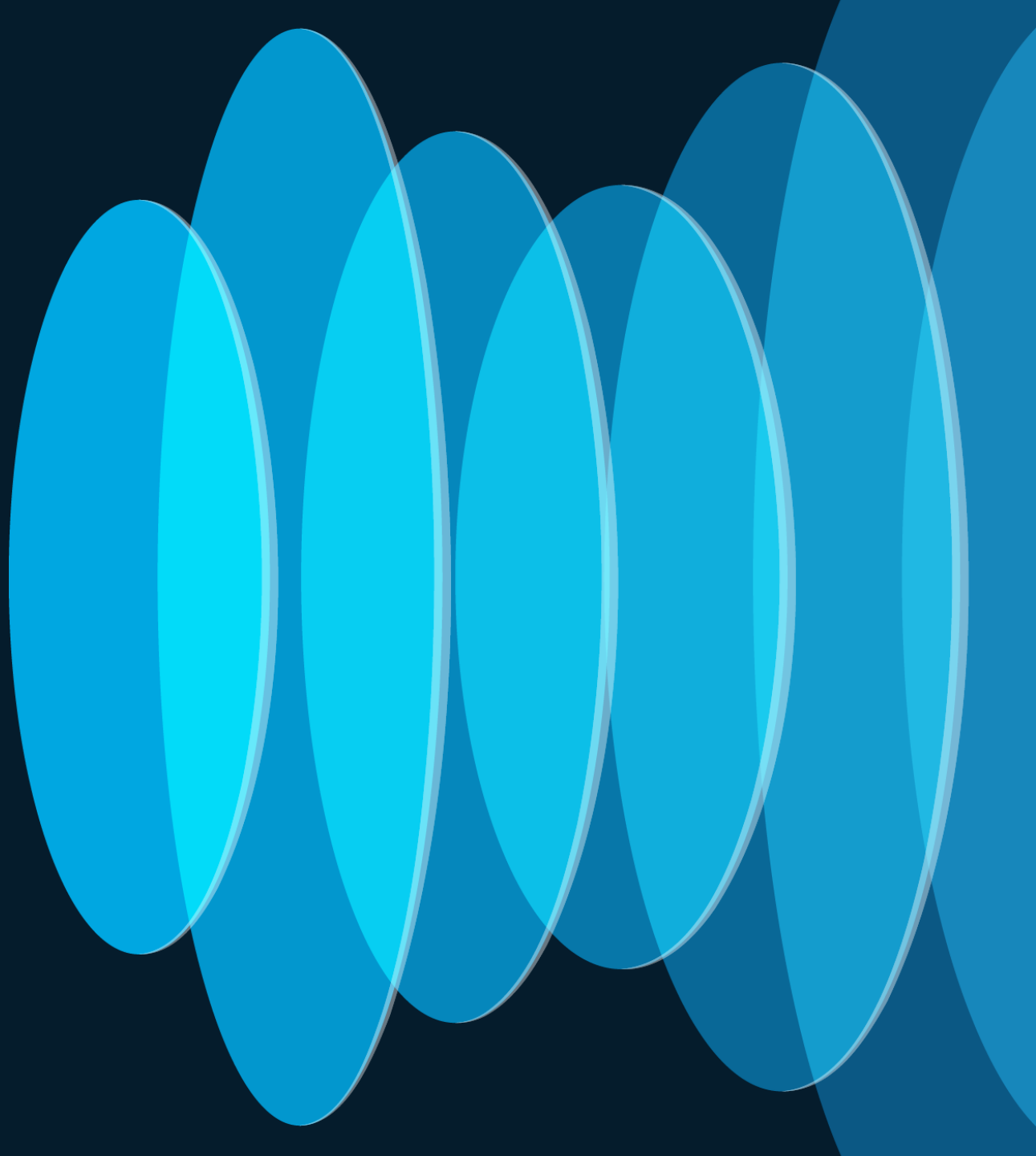
FAQ: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/tech-notes/Wireless_Product_Analytics_FAQ.html?

Day 1: C9800 Configurations



cisco Live!

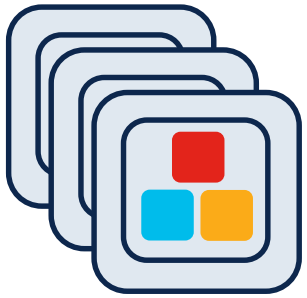
Design with Tags in Mind



cisco Live!

C9800 Configuration Model (Profiles & Tags)

Access Points



RF Tag

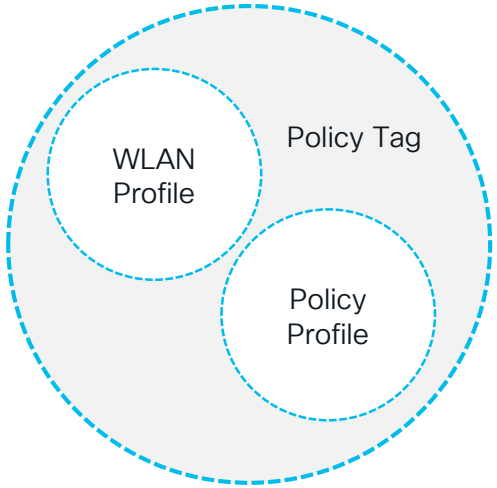
Policy Tag

Site Tag

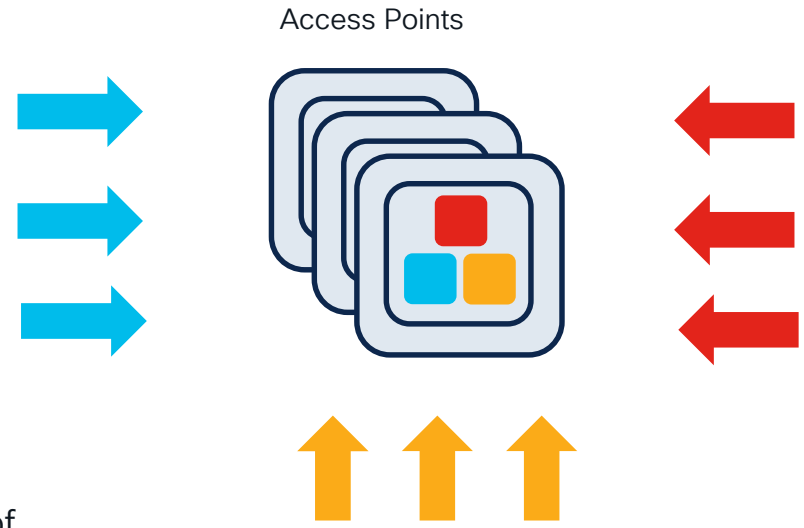
Important to remember:

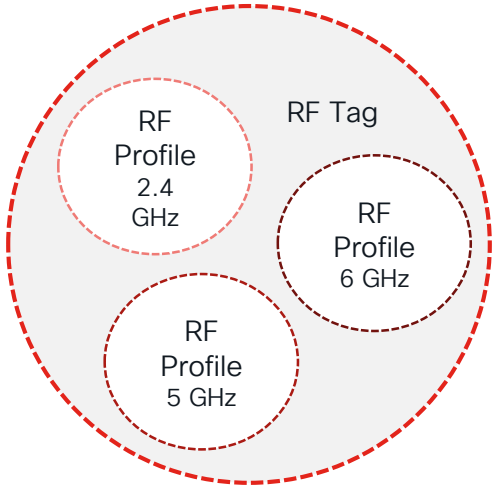
- Profiles (Policy, AP Join and Radio Frequency (RF)) and tags are the new configuration constructs
- Profiles are assigned via tags. Every AP needs to be assigned to the three AP tags (Policy, Site, RF)
- Advantages of the new configuration models:
  - Modular and reusable config constructs
  - Flexible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

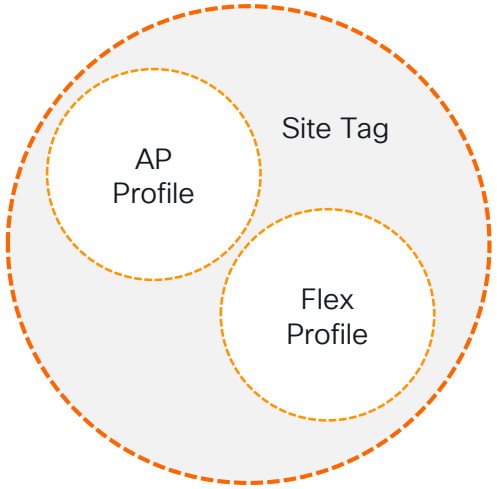


- Defines the Broadcast domain (list of WLANs to be broadcasted) with the policies of the respective SSIDs
- “Equivalent” to AP Group in AireOS





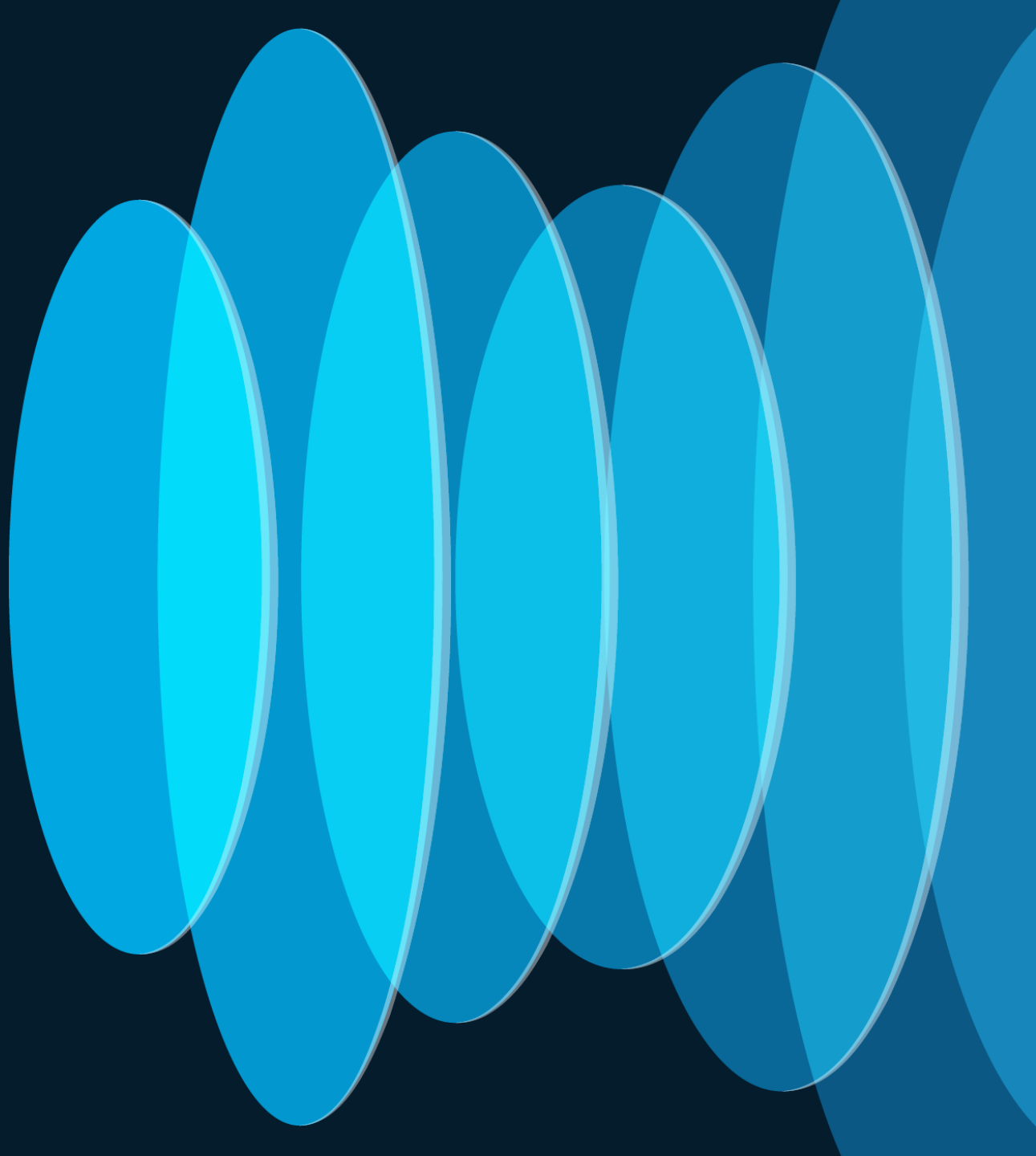
- Defines the Radio Frequency (RF) properties of the group of APs per radio



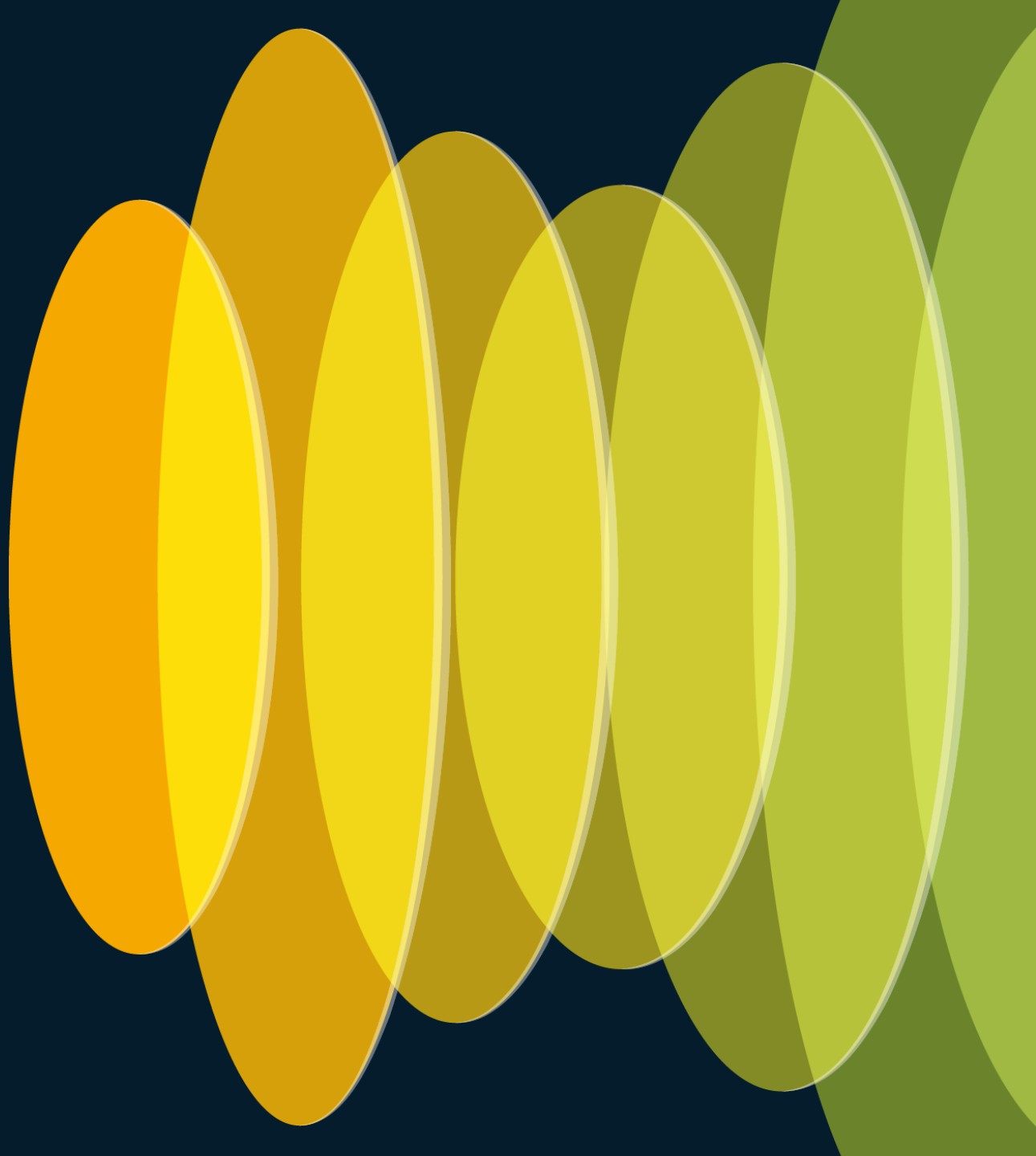
- Defines the properties of the site (central or remote)
- For FlexConnect site:
  - Defines the fast-roaming domain
  - “Equivalent” to Flex Groups in AireOS

SSID = Service Set IDentifier

Policy Tag



WLAN Design Updates



cisco Live!

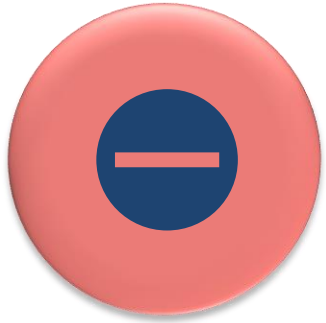
Wi-Fi 6E Security (Recap)

Wi-Fi 6E uplevels security.

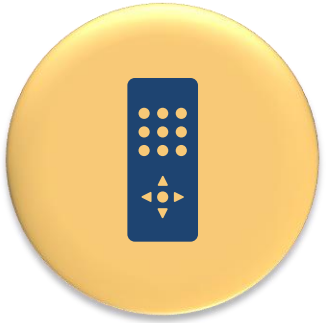
WPA3 L2 Security: OWE, SAE*, 802.1x-SHA256

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

Wi Fi™ WPA3



No backward compatibility with Open and WPA2 Security.

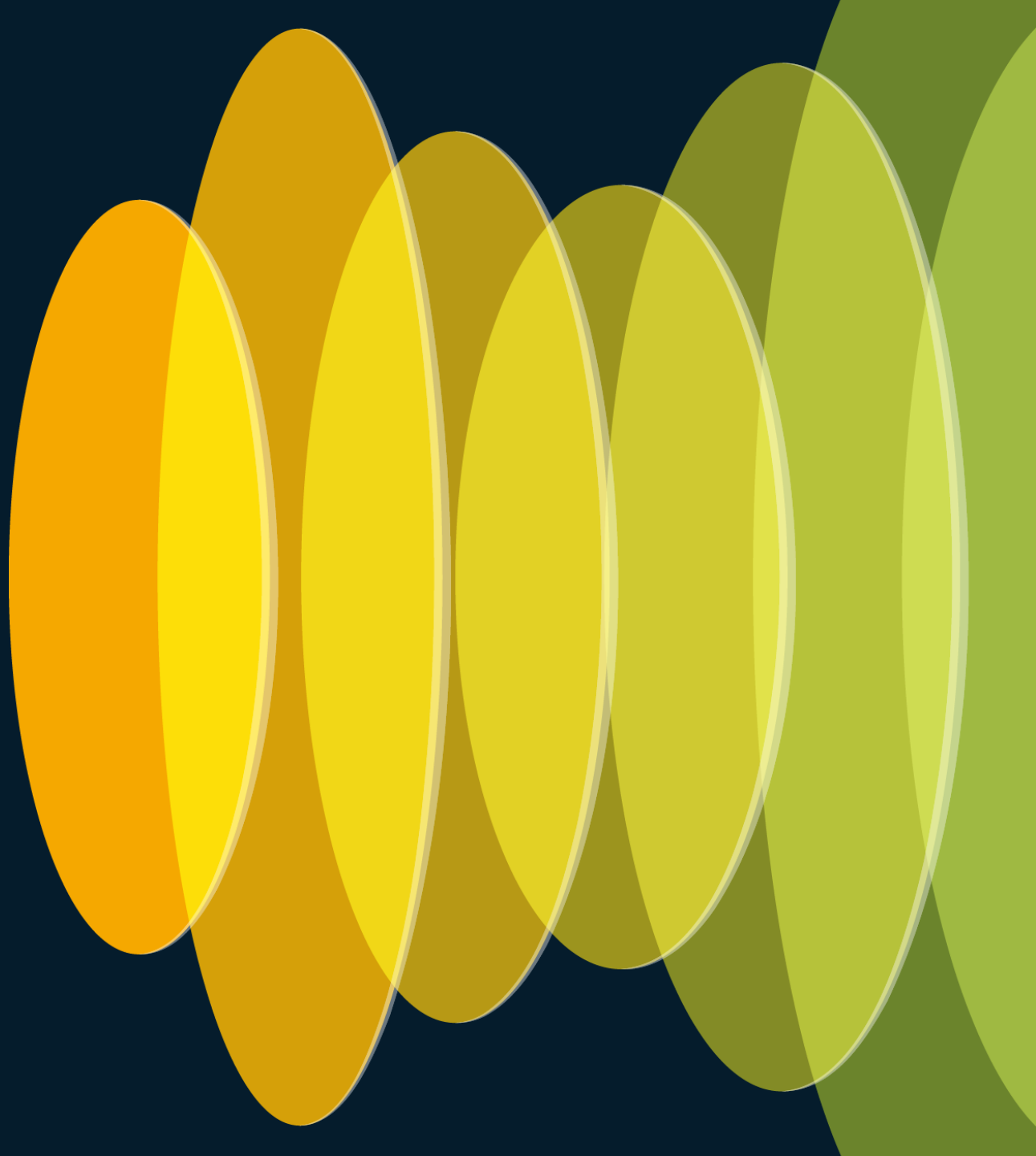


Requires Protected Management Frame (PMF) in both AP and Clients.

*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

WLAN/SSID Design



cisco Live!

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

Option 2 sub-options for 2.4/5 GHz
Pre IOS XE 17.12.1

Two options for WLAN security settings in 2.4/5GHz band:

a) WPA3 Transition mode

b) WPA/WPA2

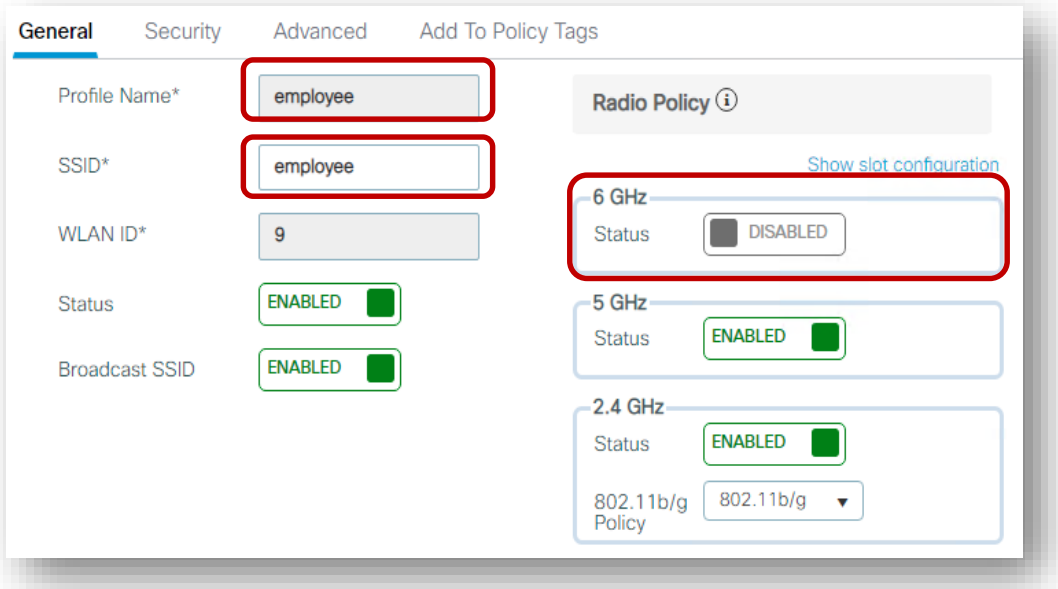
Things to keep in mind:

- From the initial testing done, some older drivers clients may have issues in connecting to a WPA3 transition mode
- **Today Cisco doesn't support seamless roaming across WLANs, so for both options it will be a hard roam across bands.**

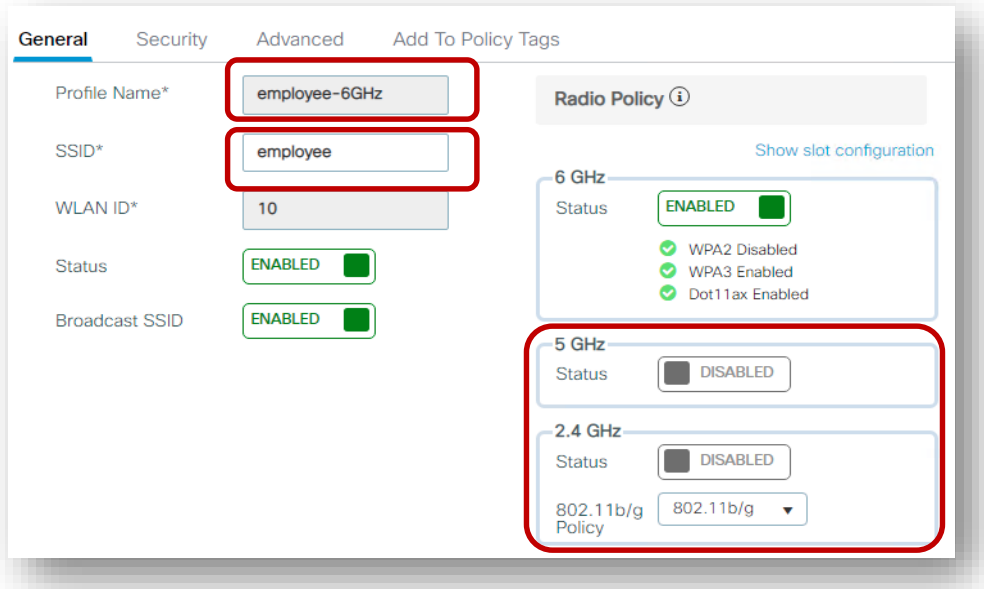
WLAN design considerations

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

Existing WLAN serving 2.4 and 5GHz



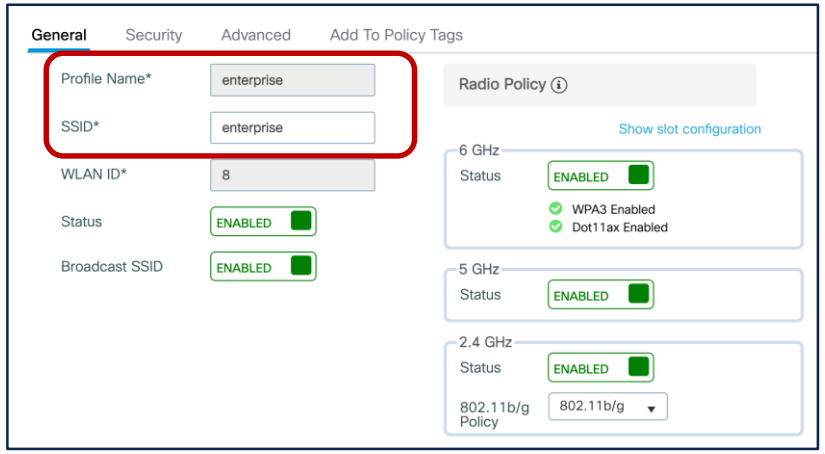
New WLAN, same SSID name serving 6GHz

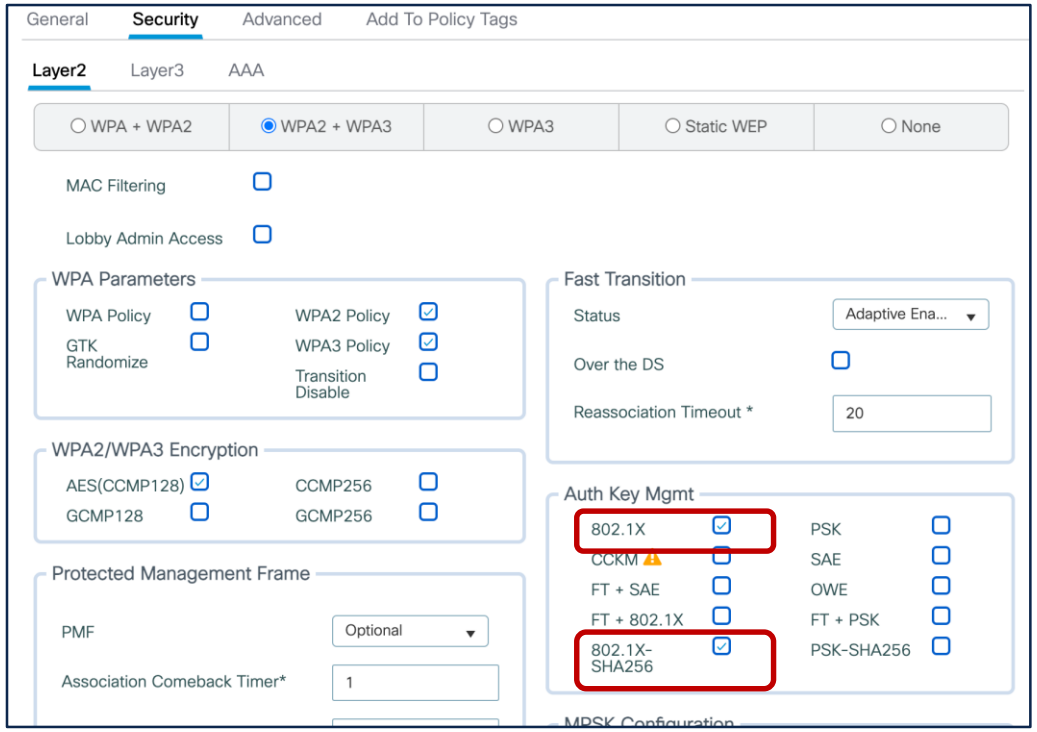


AKM = Authentication and Key Management

Going Forward … (IOS-XE 17.12.1)

Single WLAN Profile for 2.4/5 and 6 GHz





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

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

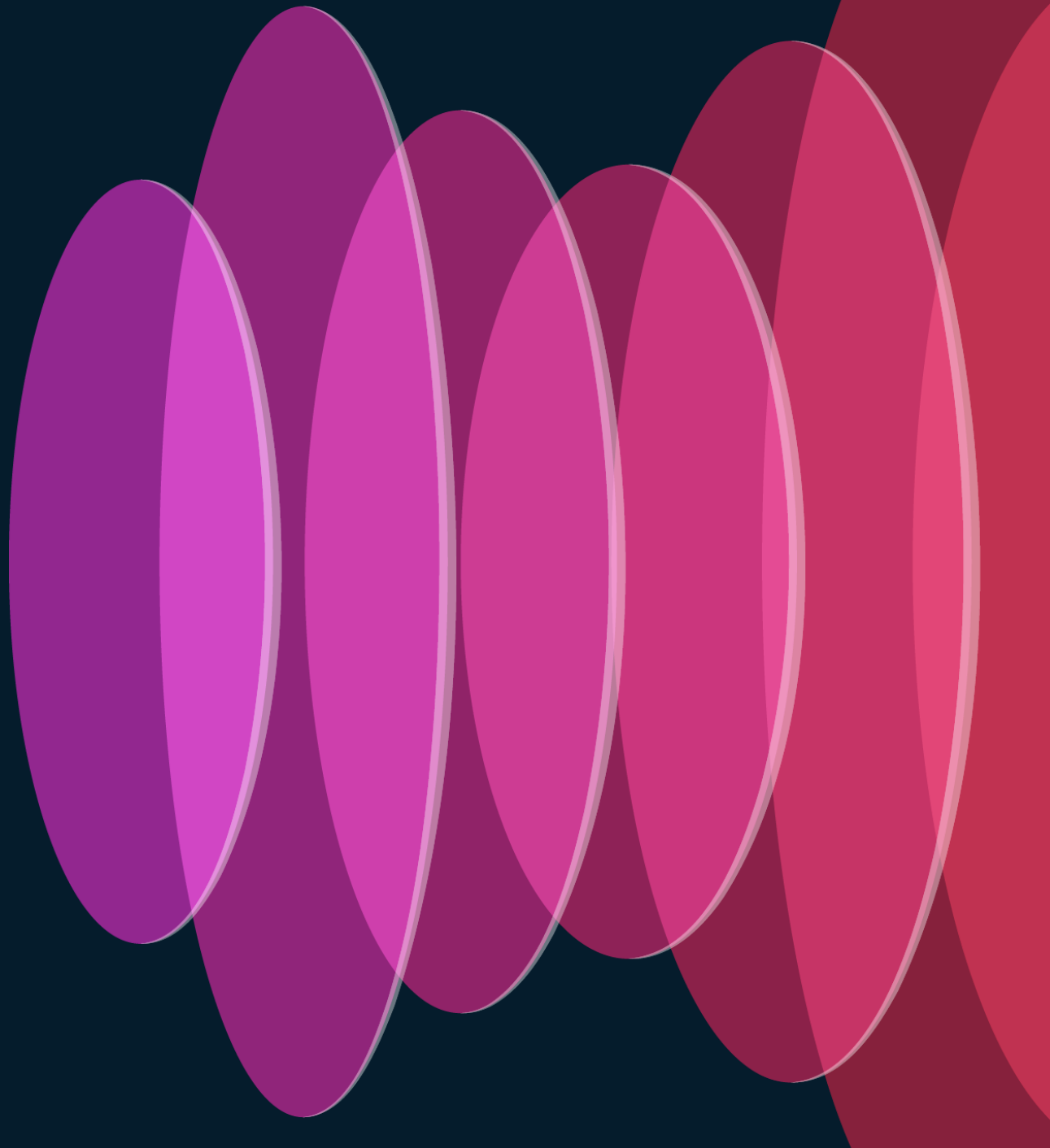
WFA = Wi-Fi Alliance

How does a SSID look like?

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

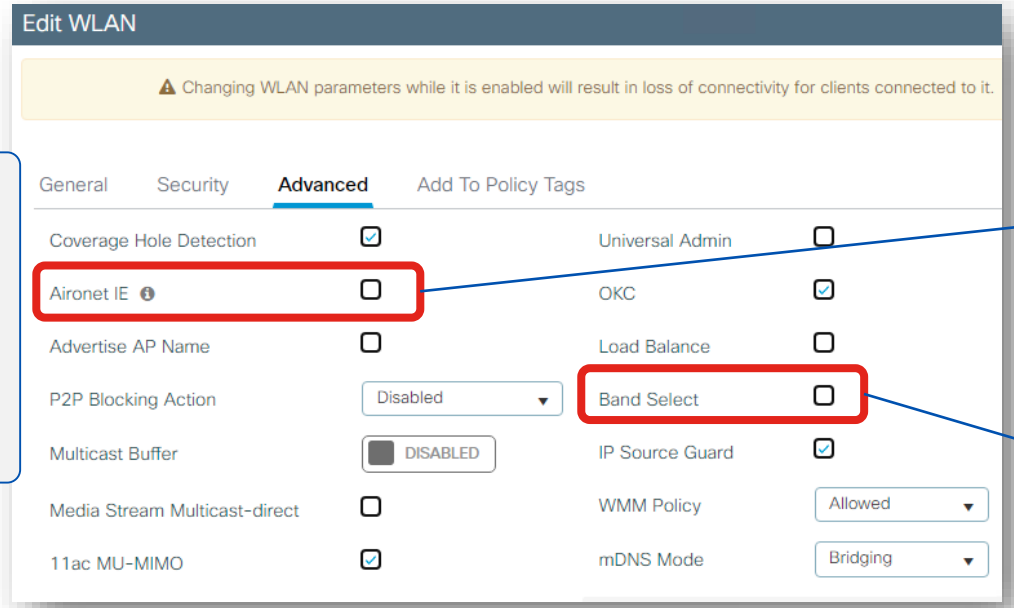
```
C9800#show wlan name Blizzard
Security-2.4GHz/5GHz
          802.11 Authentication                  : Open System
Wi-Fi Protected Access (WPA/WPA2/WPA3)           : Enabled
           WPA2 (RSN IE)                       : Enabled
           AES Cipher                             : Enabled
      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

WLAN settings

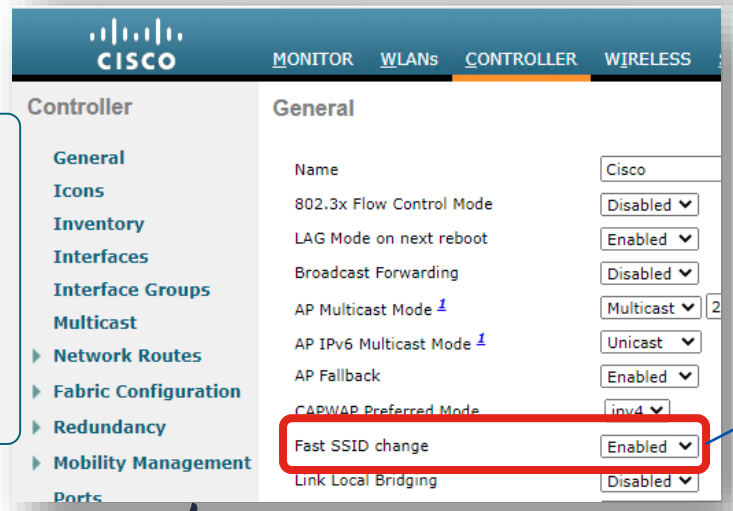


WLAN settings

C9800-80



8540



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

Q: Do we still need Aironet IE?

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

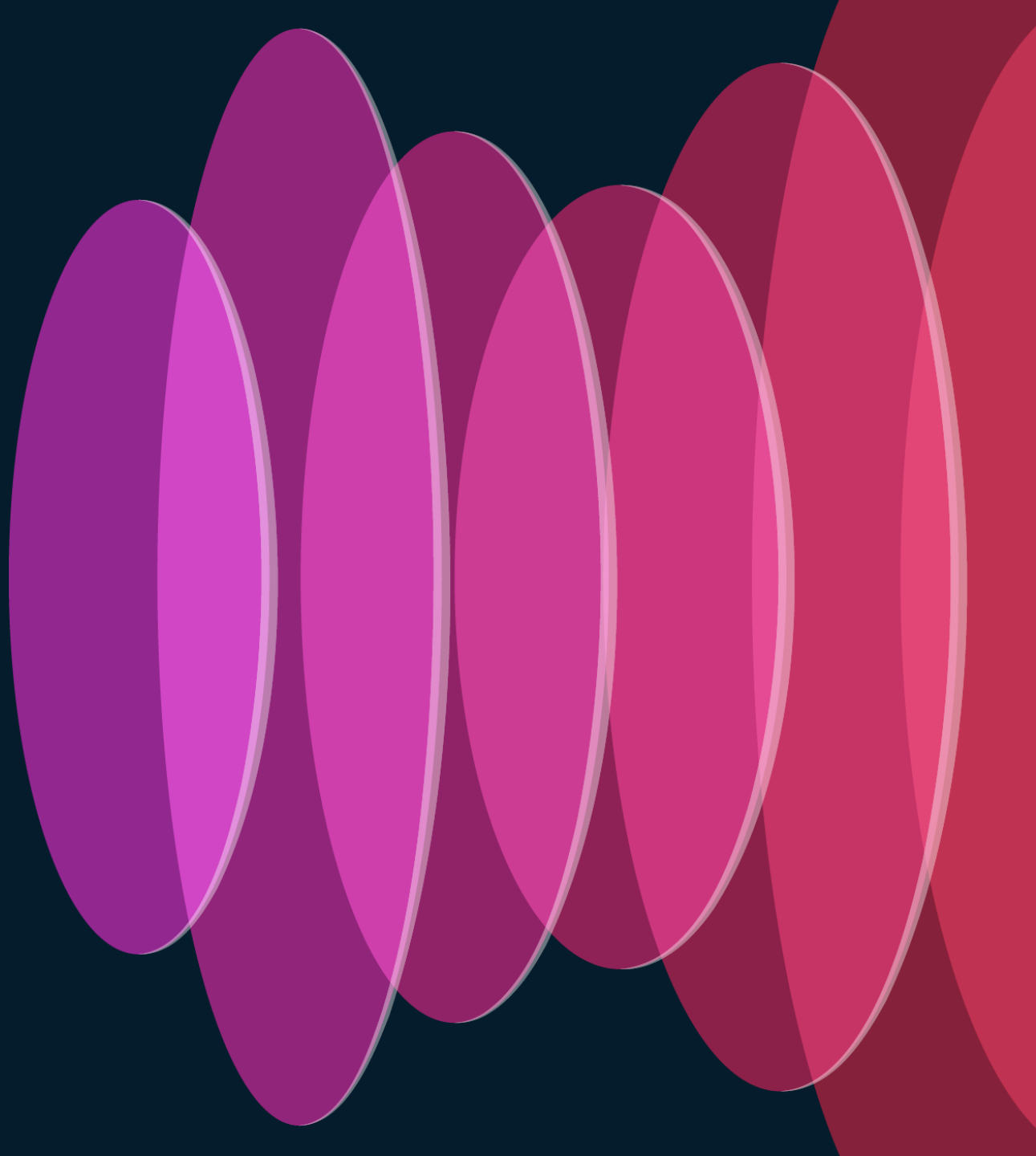
Q: Do we still need Band Select?

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

Q: What happened to Fast SSID change?

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

Webauth Configuration



Webauth configuration

Problem:

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

Solution:

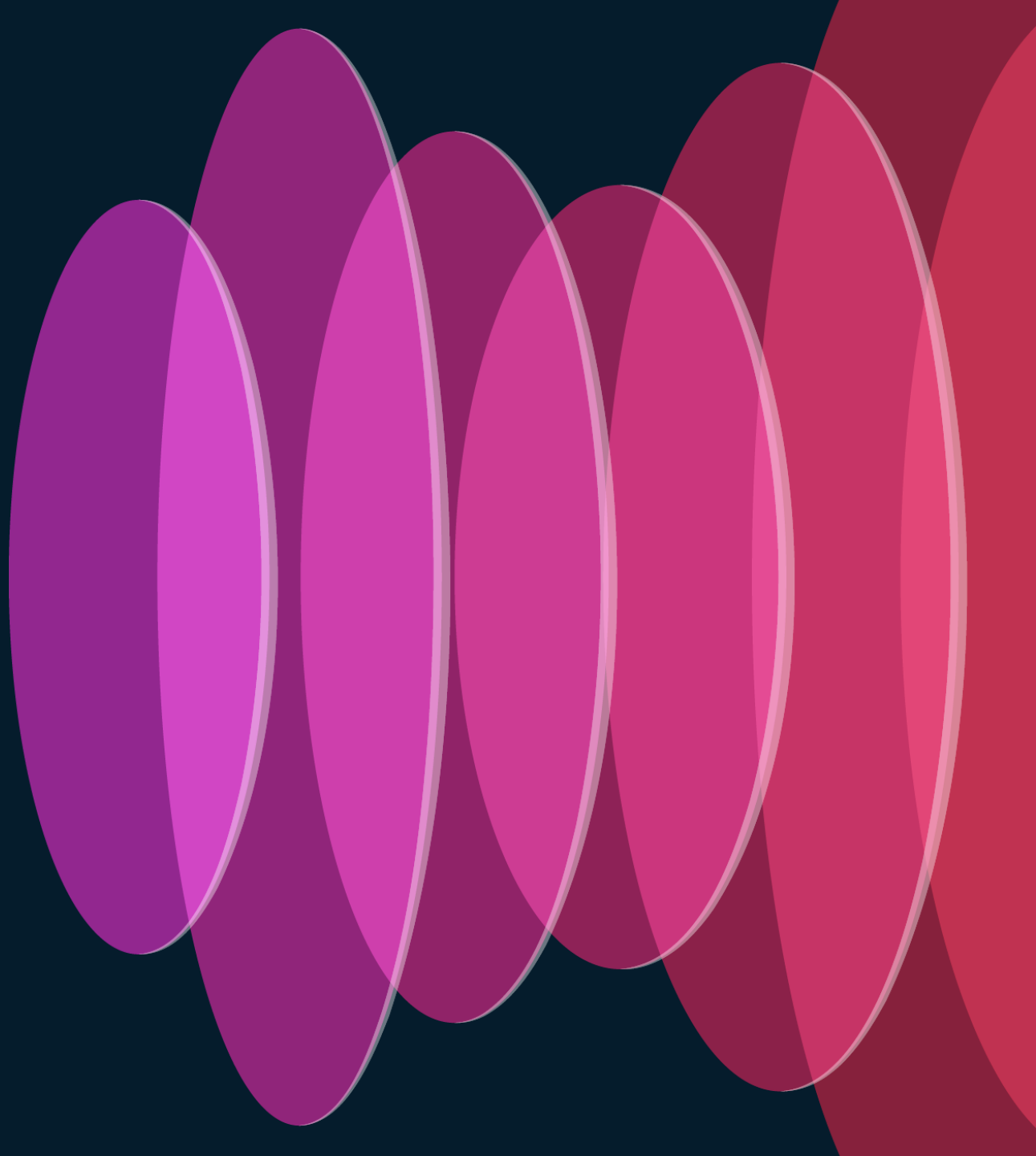
Need to enable WebAuth on HTTP. In C9800 you don't need to enable HTTP for the entire box (GUI access), but only for WebAuth client connections.

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

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

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

mDNS Configuration



cisco Live!

mDNS configuration

Scenario:

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

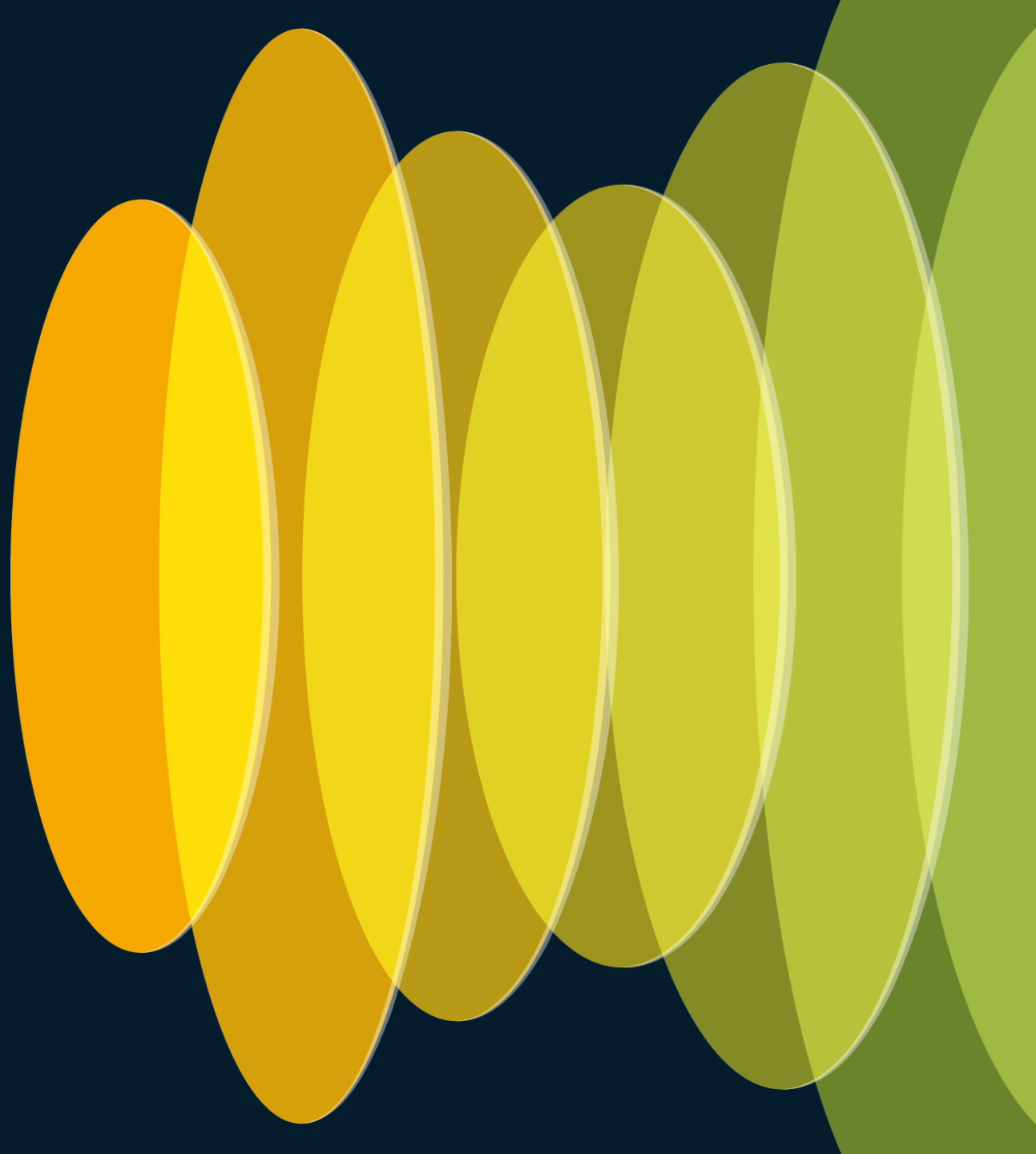
Recommendation:

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

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

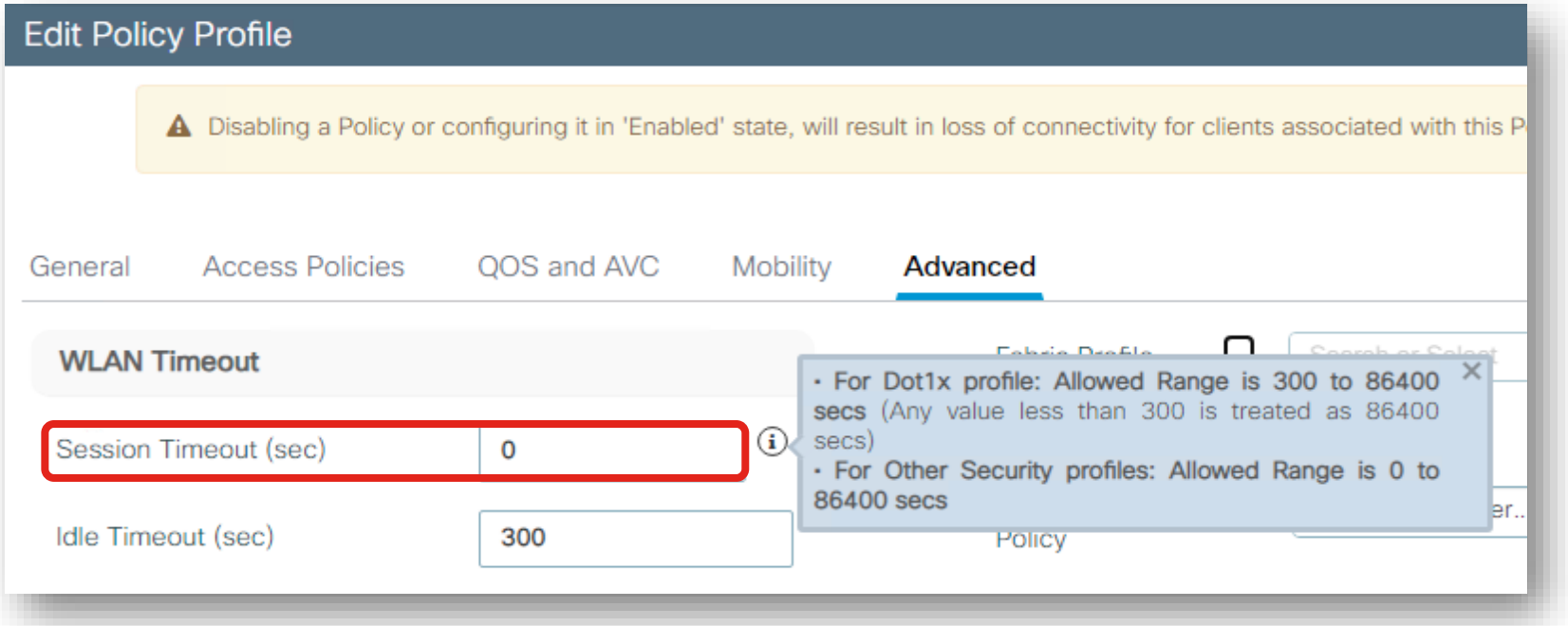
```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! mdns profile and service mapping
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[skip]
mdns-sd service-list aireos-default-mdns-profile-out OUT
    match AirTunes
    match Printer-IPPS
 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

Policy Profile settings



cisco Live!

Policy Profile settings



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

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

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

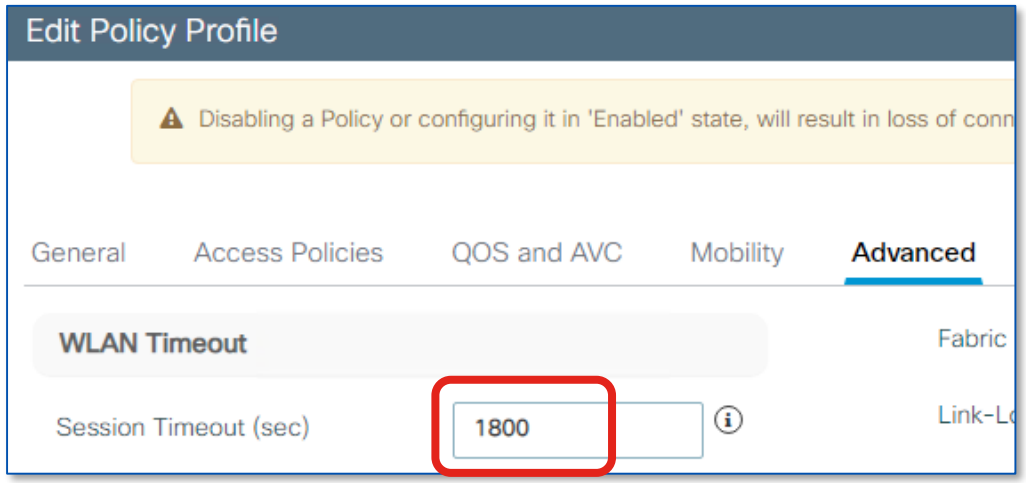
A: Yes, absolutely

Default session timeout to 8 hours

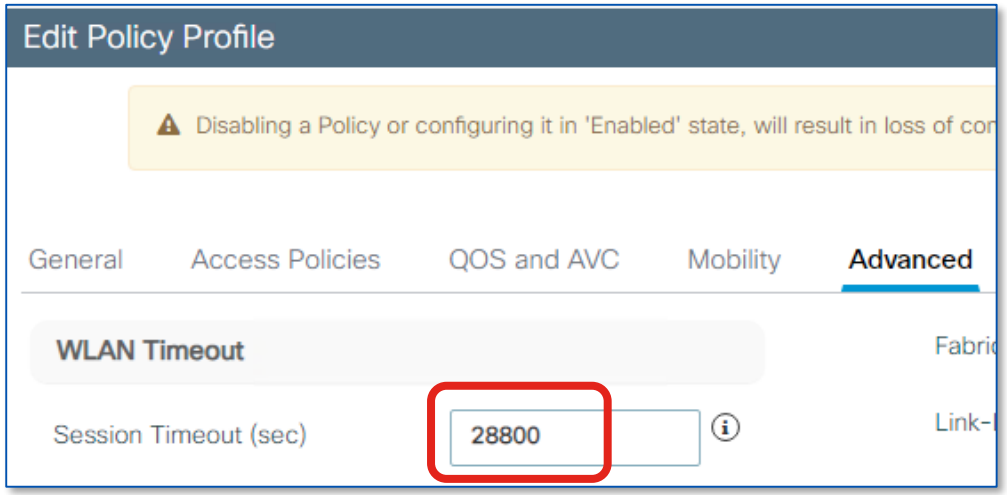
What it is?

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

Before 17.12 > timeout is 30 mins

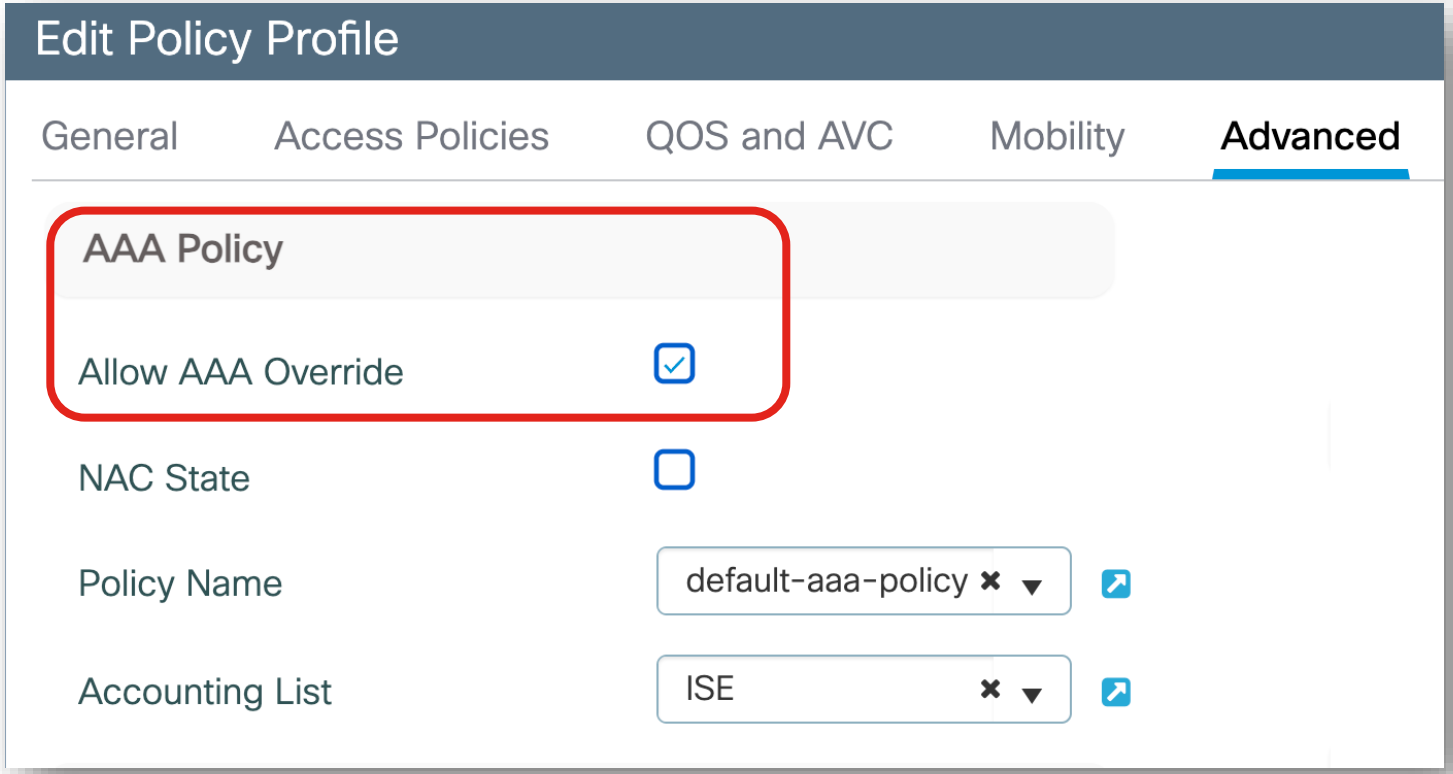


Starting 17.12 > timeout is 8 hours

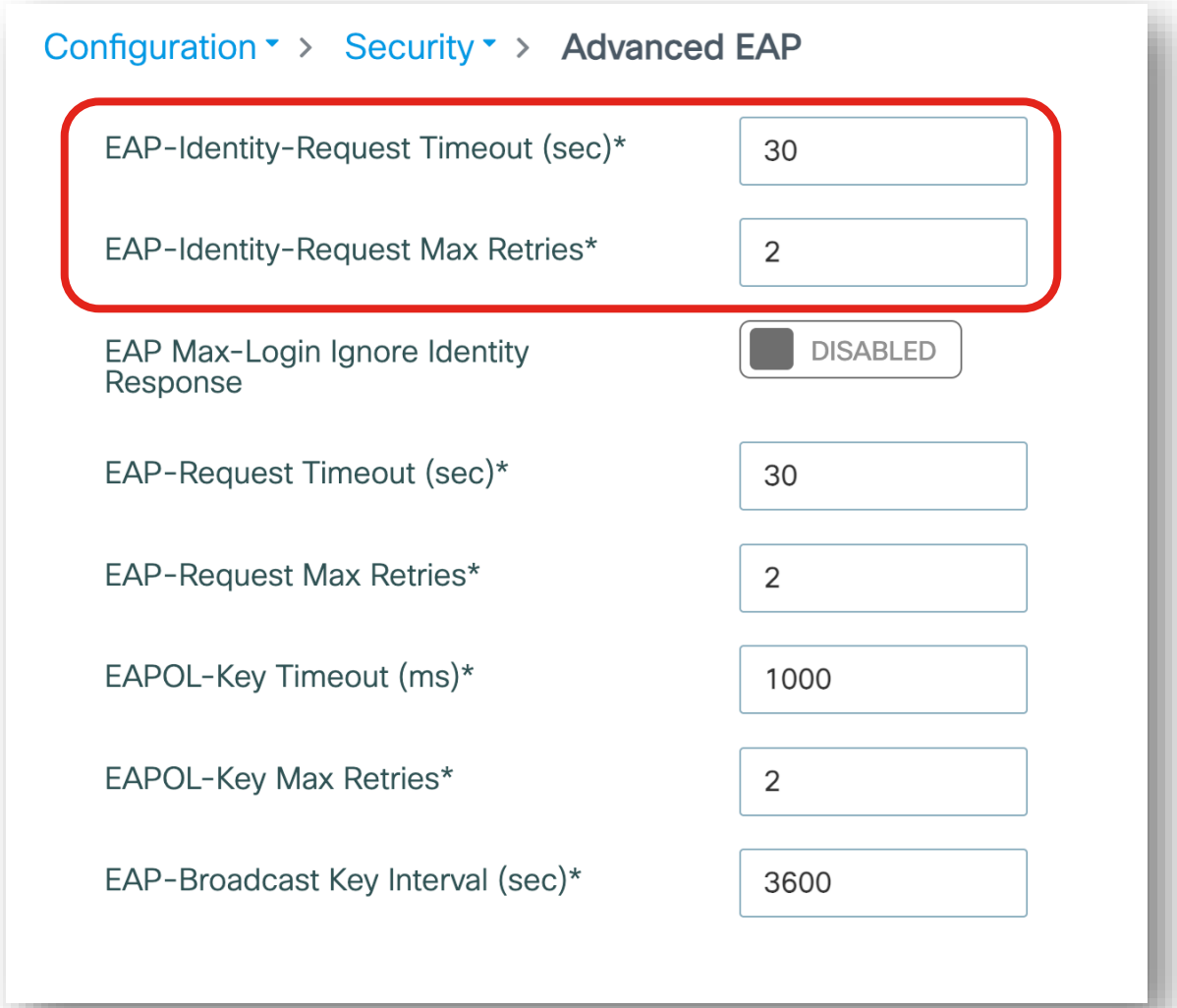


AAA Override

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

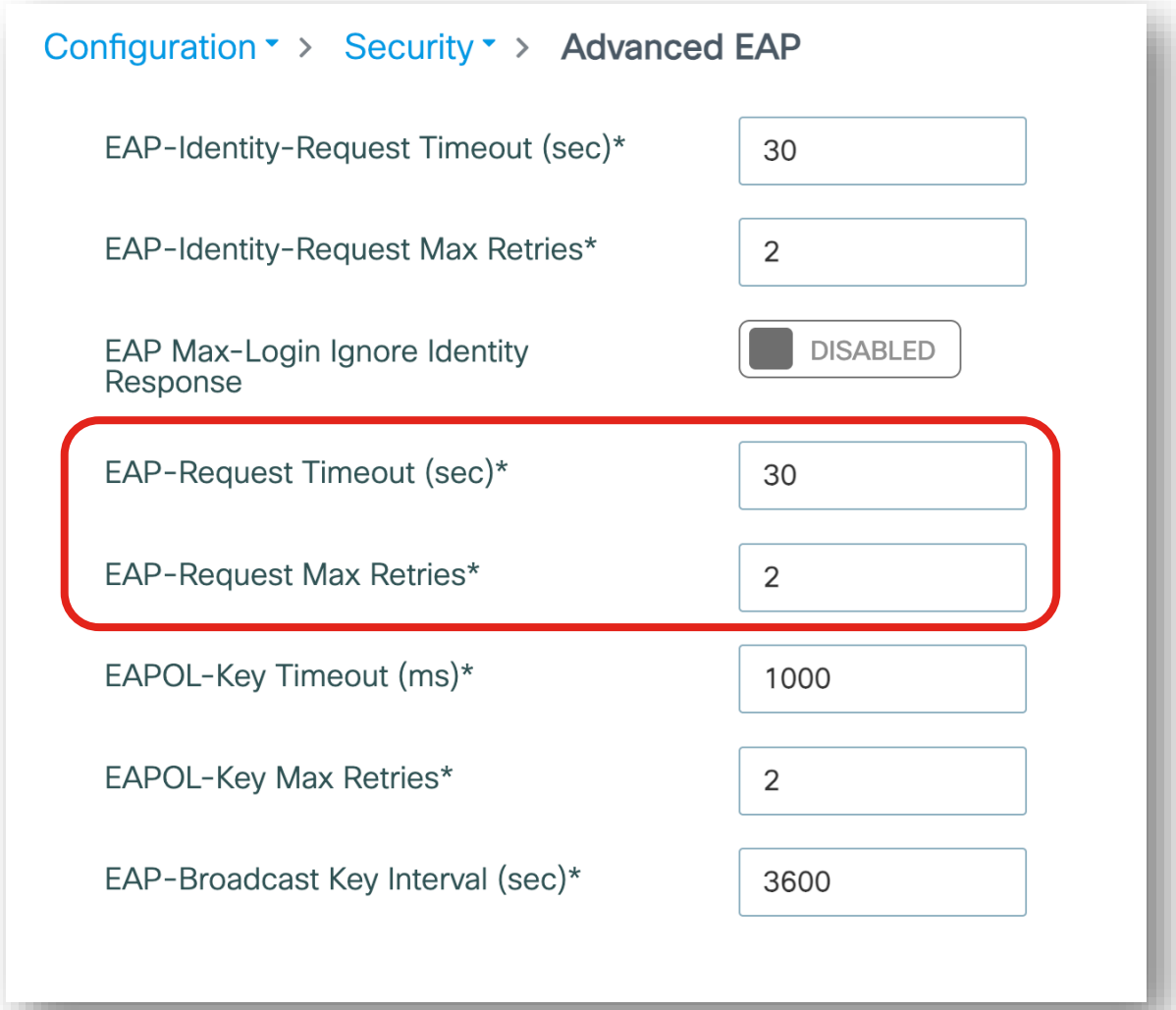


EAP Timeout



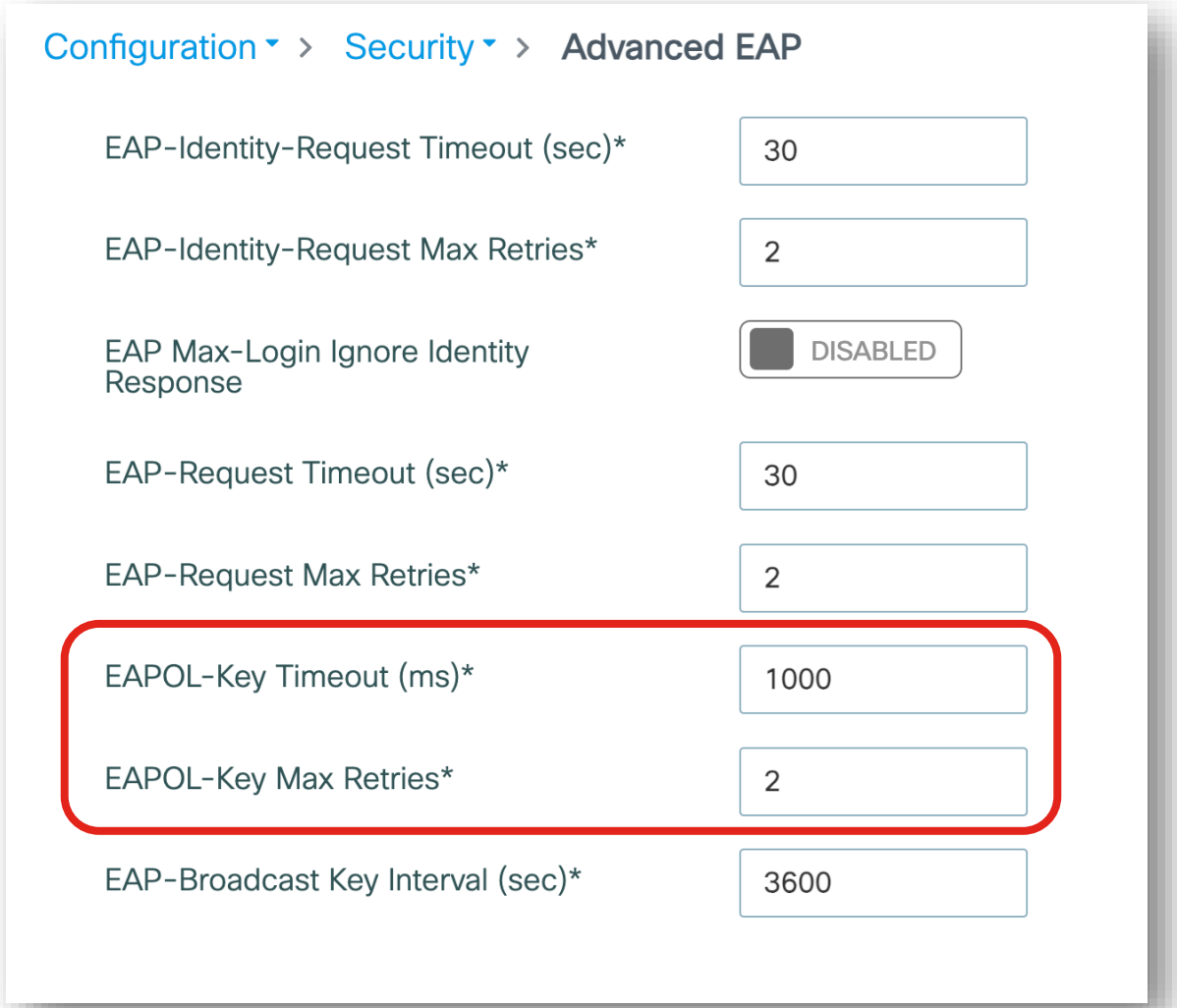
- Default timeout and retries fit the majority of use cases
- May need increase if:
  - Implement one-time passwords on smart card
  - User interaction required
- Be careful of increasing too high
  - Trade-off of client experience in case of authentication failure

EAP Timeout



- Clients may not properly handle fast retry timers
- Acceptable values:
  - 2 seconds in most cases
  - Up to 30 seconds for slow clients (phones)

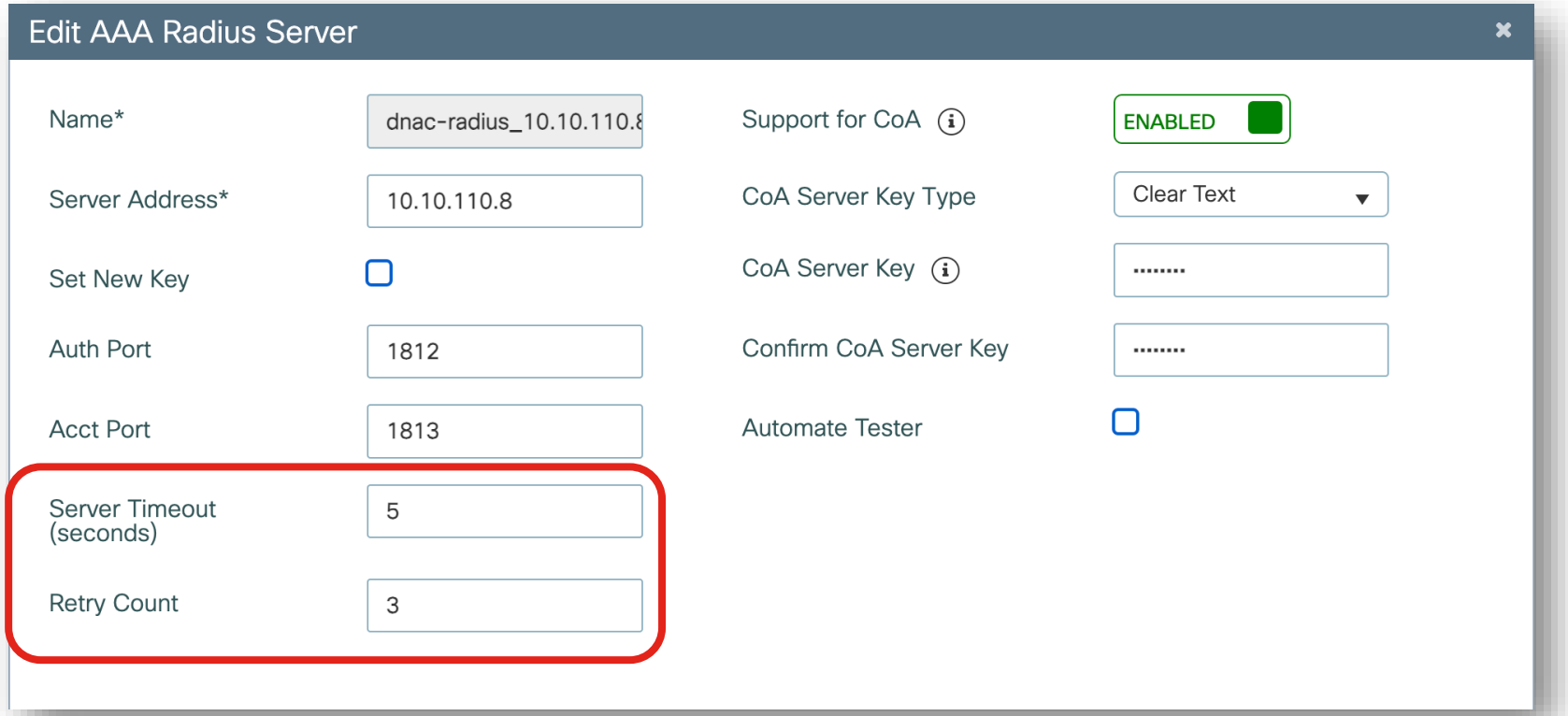
EAP Timeout



- Timeout set as minimal as possible for voice clients
  - ~400-1000 ms
- Retries has direct implication for several of the KRACK attacks in 2017
  - For maximum security, set to 0
  - Validate in environment as it may result in failed authentication in bad RF environments

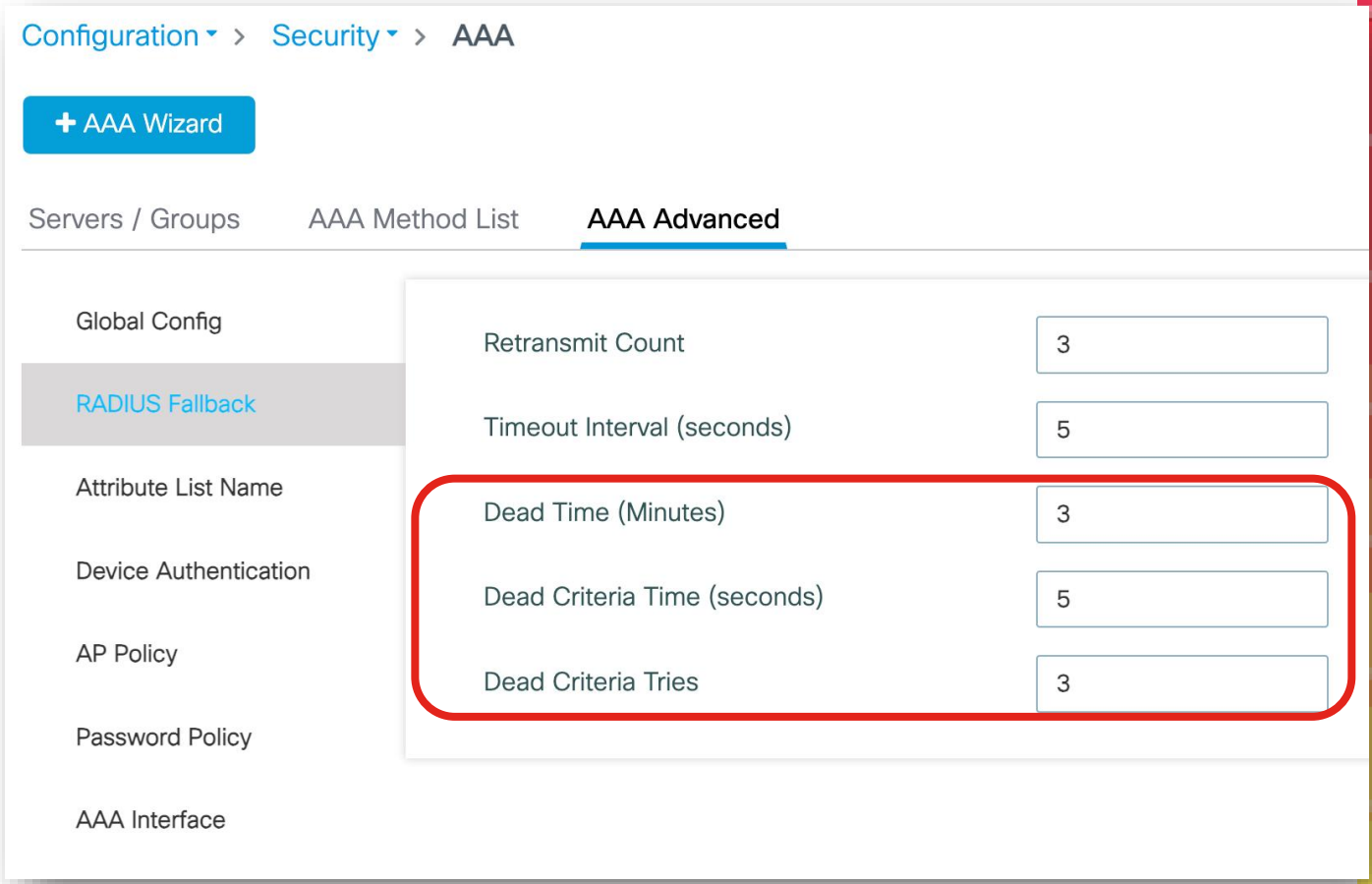
RADIUS Server Timeout

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



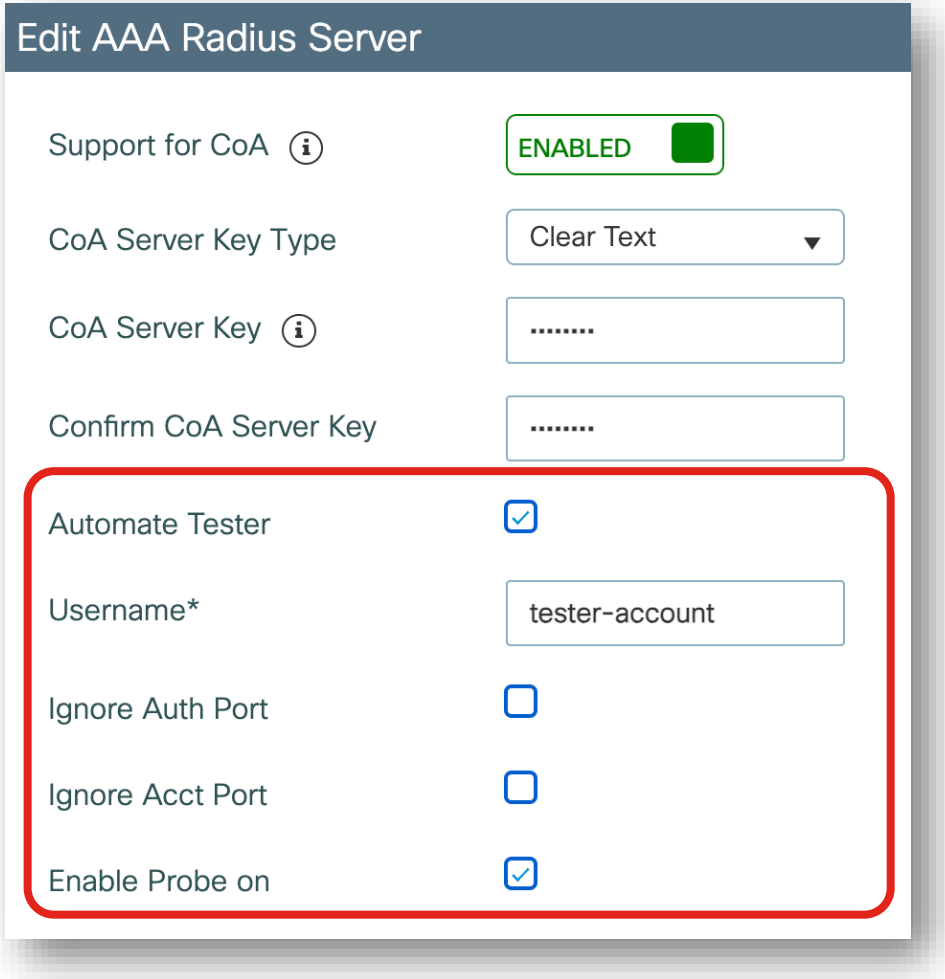
RADIUS Server Timeout
Dead-Criteria and Deadtime Timers

- 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



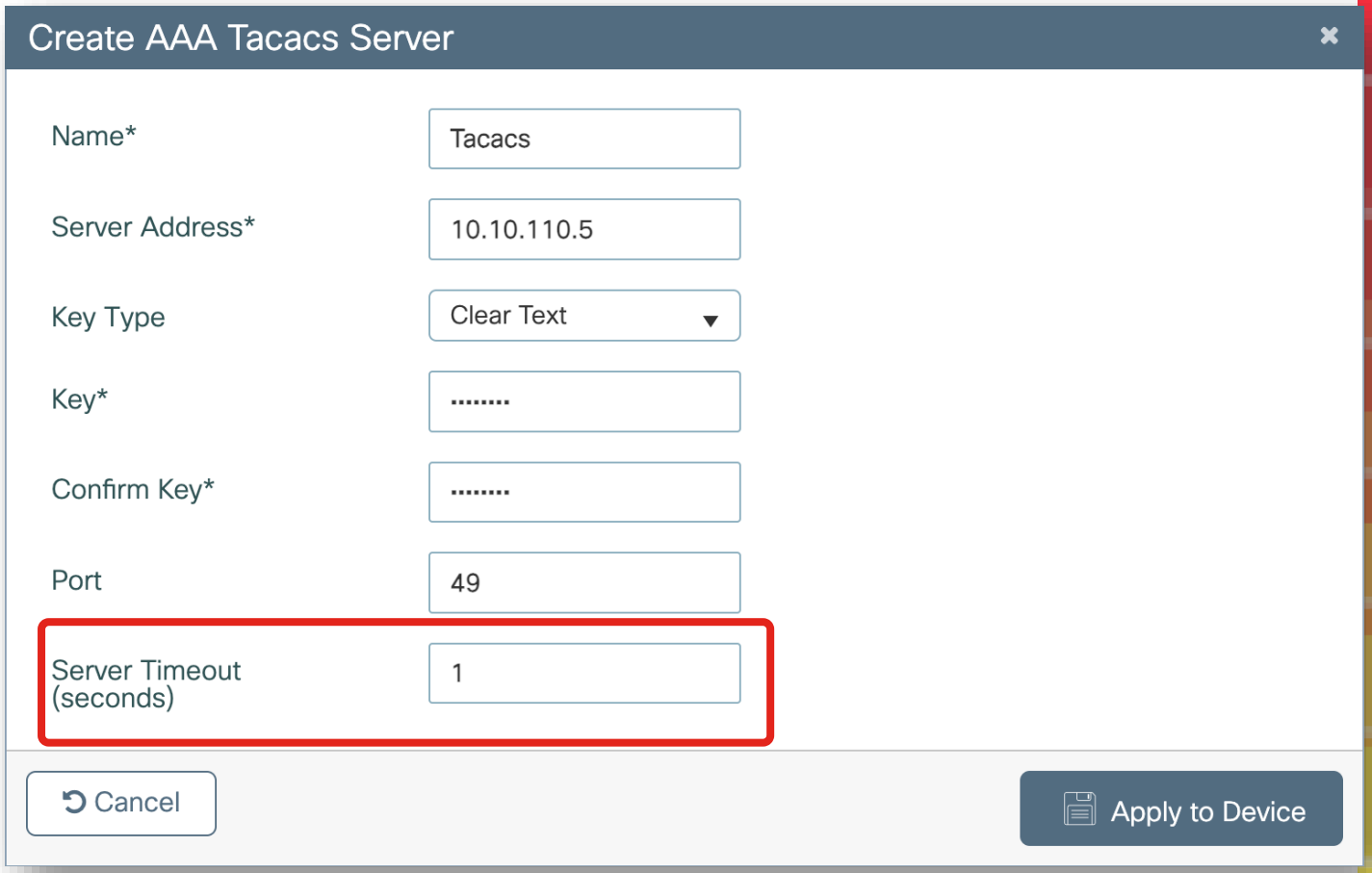
RADIUS Server Timeout
Dead-Criteria and Deadtime Timers

- 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

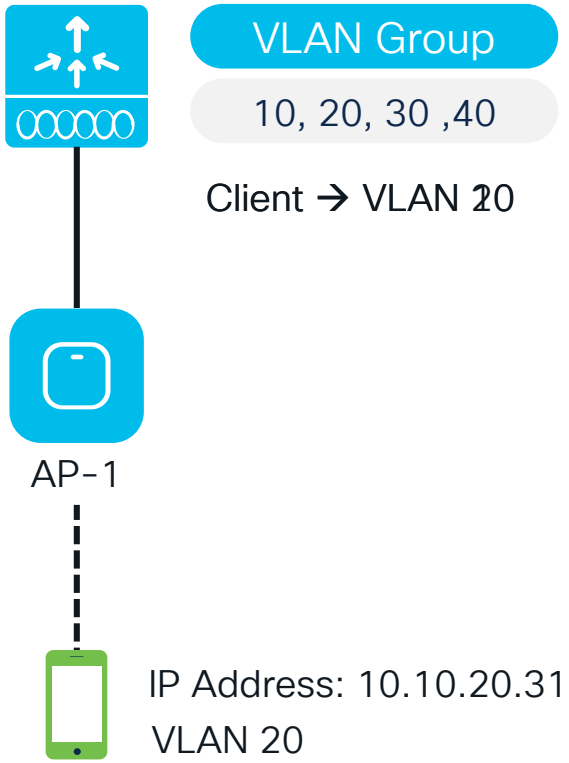


TACACS+ Management Timeout

- 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



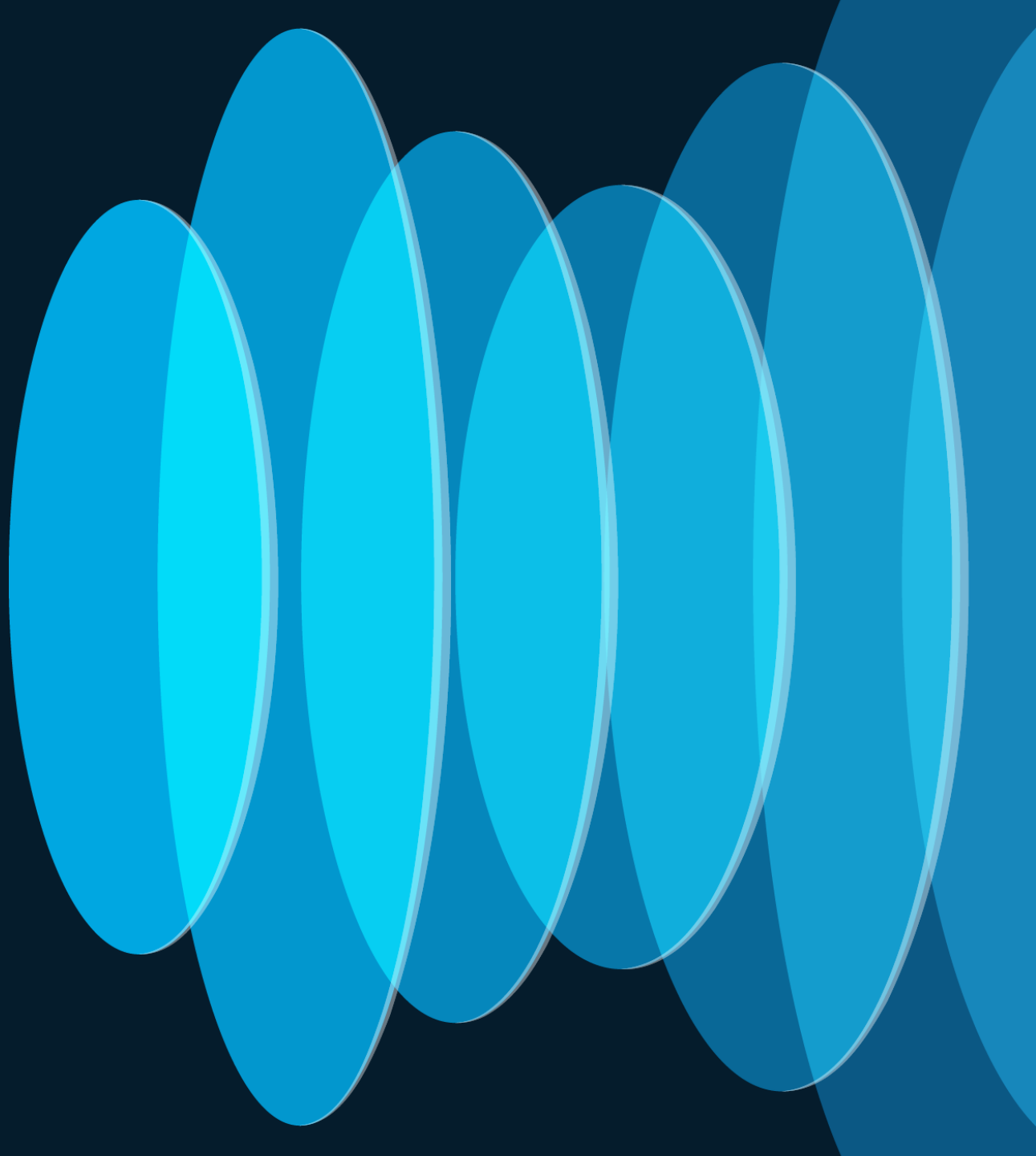
9800 assigns a VLAN to clients upon joining the network

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

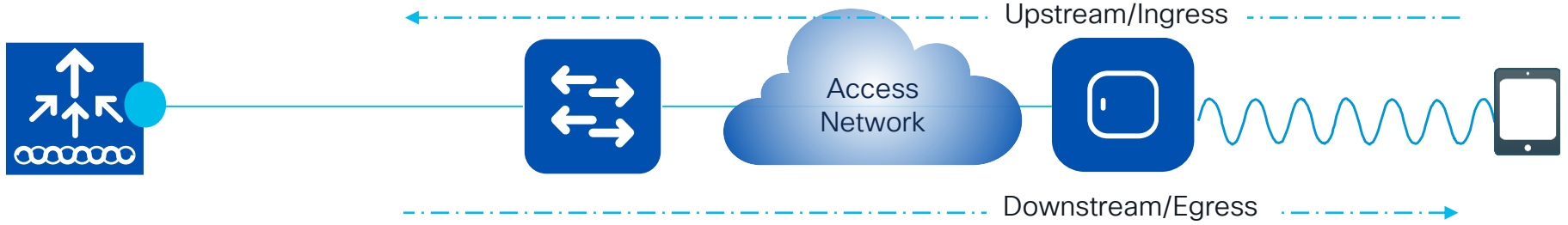
If VLAN does not exist, use Static IP Mobility

QoS



Catalyst 9800 Wireless QoS – Policy targets

- A target is the entity where policy is applied. C9800 supports #3 targets: SSID, client and port.
- Wireless QoS policies are applied in the upstream and (or) downstream direction.
  - Downstream: The flow of traffic from a wired source to a wireless destination
  - Upstream: The flow of traffic from a wireless source to a wired destination
- SSID Policies: You can create QoS policies on SSID in both the ingress (upstream) and egress (downstream) directions. The policy is applicable per AP per SSID. You can configure policing and marking policies on SSID.
- Client Policies: applicable both the ingress (upstream) and egress (downstream) directions. You can configure policing and marking policies on clients. AAA override is also supported.



Catalyst 9800 Wireless QoS – Modular QoS

- Catalyst QoS model is based on **Modular QoS CLI (MQC)**
- In IOS-XE, **MQC** is used to implement the Differentiated Service model QoS
- The main MQC constructs:
  - **Class-map:** to classify traffic
  - **Policy-map:** to bind traffic class to actions
  - **Service-policy:** to attach policy-map to target/direction

Classification ACL

```
ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C
 10 permit udp any eq 5246 16666 any
```

Class-map definition

```
class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class
 match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C
class-map match-any AutoQos-4.0-Output-Voice-Class
 match dscp ef
```

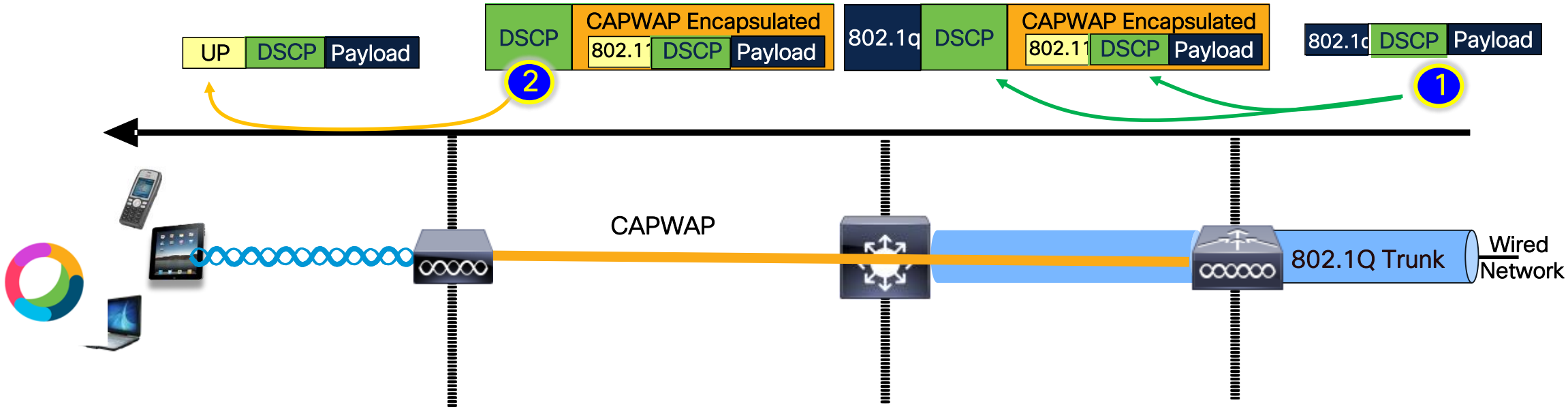
Policy-map definition

```
policy-map AutoQos-4.0-wlan-Port-Output-Policy
 class AutoQos-4.0-Output-CAPWAP-C-Class
  priority level 1
 class AutoQos-4.0-Output-Voice-Class
  priority level 2
 class class-default
```

Service-policy attachment

```
interface TenGigabitEthernet0/0/0
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
```

Downstream QoS Model

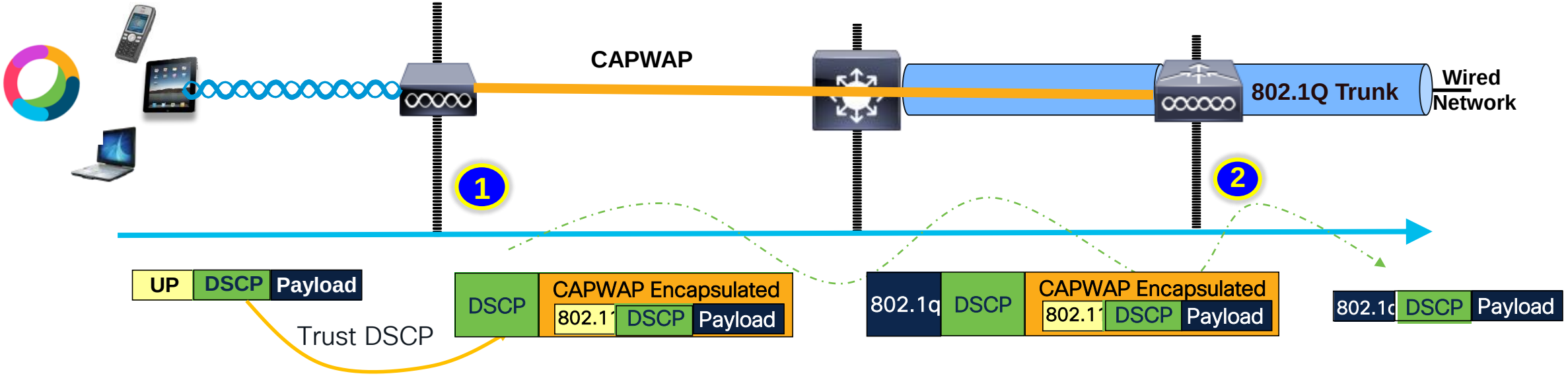


1. The client packet is received over an 802.1q trunk by the WLC. The WLC uses the DSCP value of the original IP packet and maps it to the outer DSCP of the CAPWAP tunnel (assuming no ceiling value is applied via Metal QoS at the WLC)

2. The AP leverages the the DSCP value from CAPWAP header for internal QoS processing and queuing The DSCP value is mapped to the 802.11e UP value in the egress wireless frame to the client

Upstream QoS Model

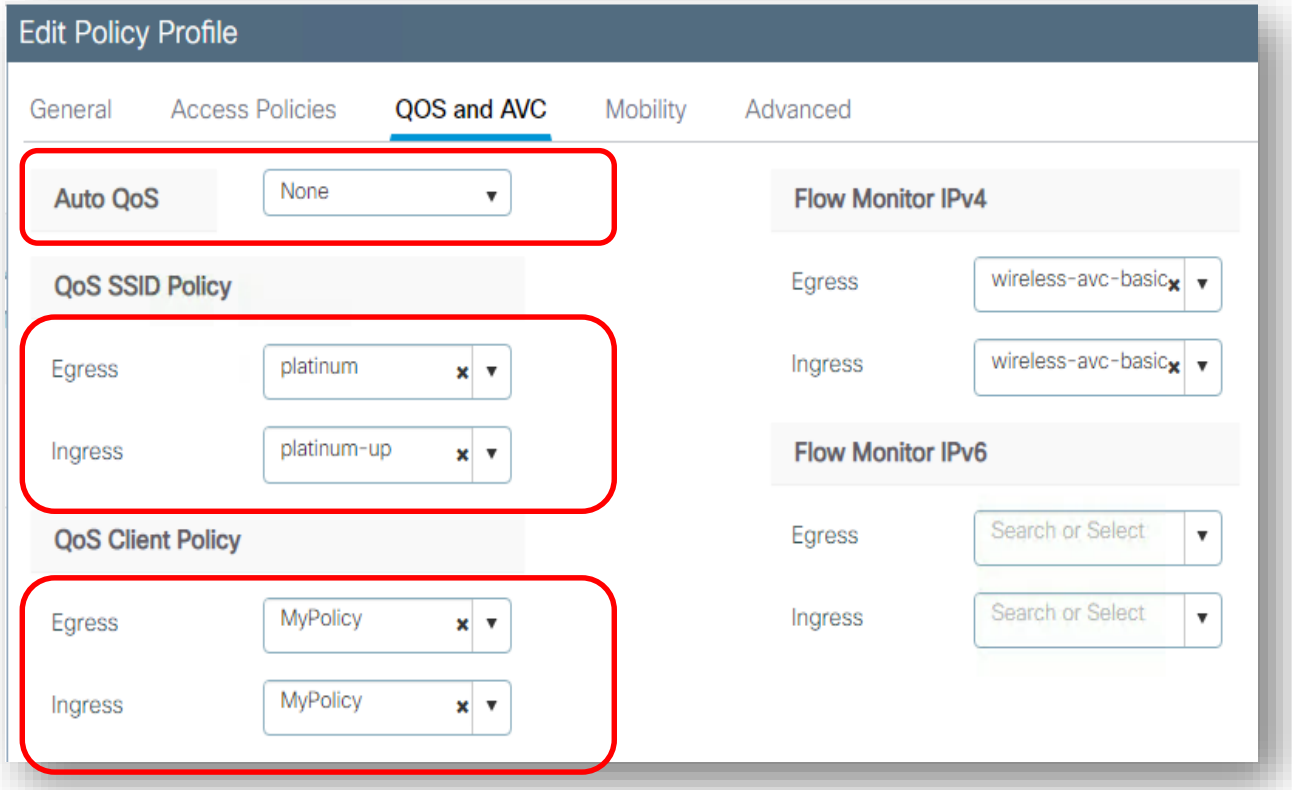
1. The client 802.11e frame is received by the AP. The AP utilizes the DSCP value in the original packet for internal QoS processing and then maps it to the outer CAPWAP IP header, (assuming no ceiling value is applied via Metal QoS at the WLC)(*)



2. This allow preservation of the DSCP value from the client all the way through the network, emerging untouched from the WLC (assuming no Metal QoS or AVC policy is applied to remark DSCP)

(*) Before release 17.4, you need to explicitly configure “qos-map trust-dscp-upstream” under the AP join profile. If this setting is not there, the AP will use the UP value in the received frame to derive the outer DSCP value of the CAPWAP header

QoS Workflow

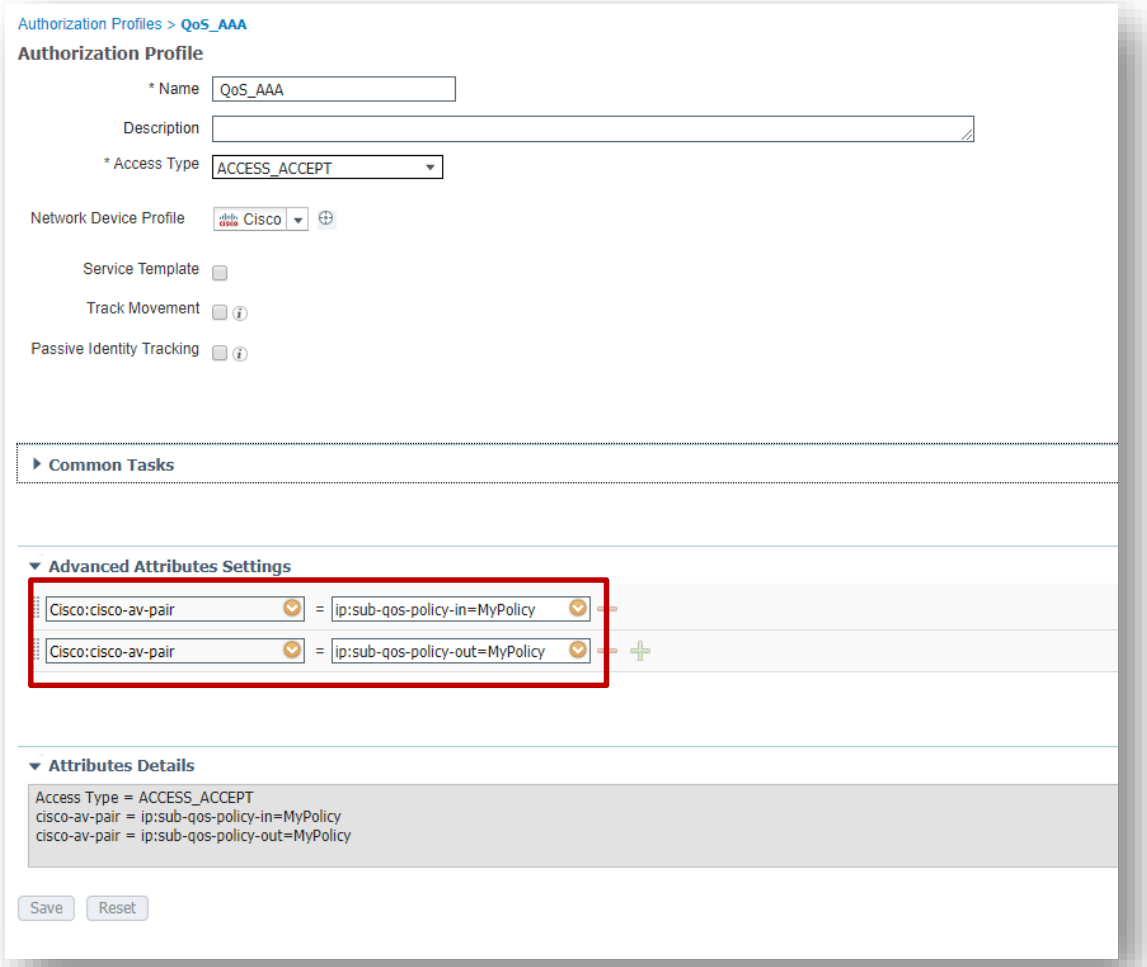


QoS Policy can be applied at multiple level:

- Auto QoS: this is a set of predefined policies automatically applied at the SSID, radio and controller port level
- SSID: it gets applied per AP to the aggregate traffic for all clients on that SSID
- Client level: it's per client policy
- Both SSID and client: client policy is applied first and then the SSID policy
- Custom or Metal QoS policy can be applied per client via "aaa override"

QoS Workflow – AAA override

- QoS Policy override is available per user policies not per SSID
- Return the policy name in cisco av-pair
  - cisco-av-pair = ip:sub-qos-policy-in=MyPolicy
  - cisco-av-pair = ip:sub-qos-policy-out=MyPolicy
- Can also return a Metal policy
- Supported for Local and Flex/Fabric APs



Catalyst 9800 QoS

General restrictions:

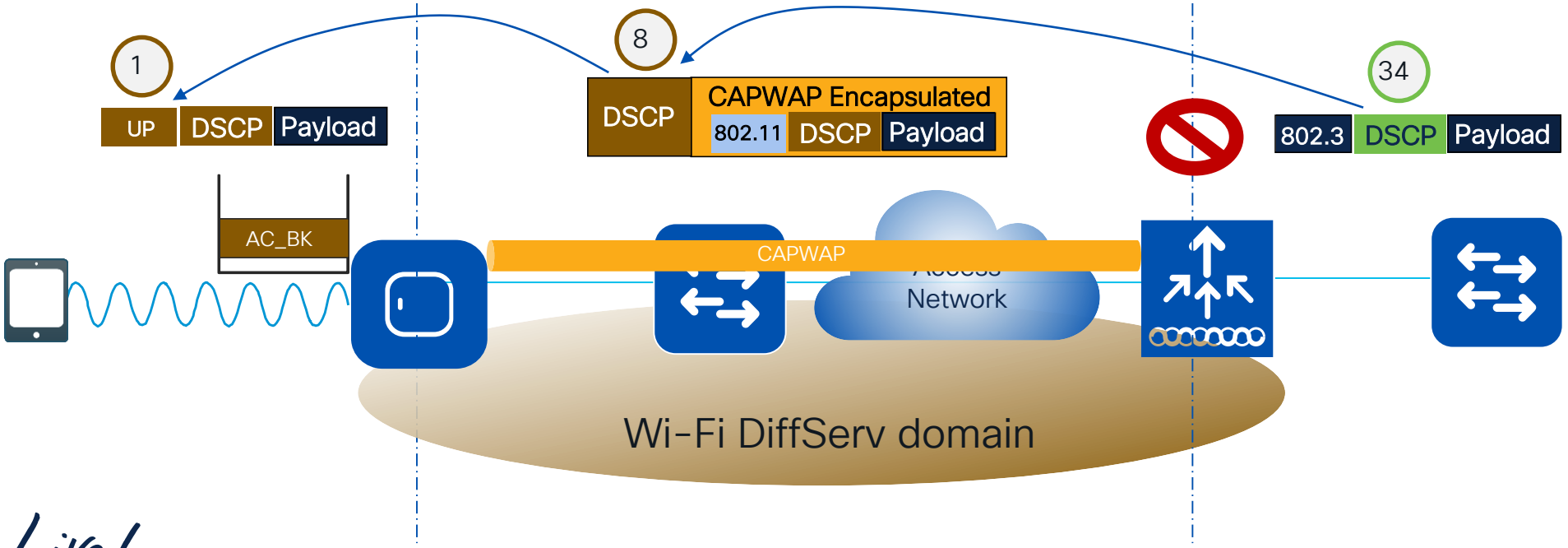
- SSID and client targets can be configured only with marking and policing policies
- One policy per target per direction is supported
- Class maps in a policy map can have different types of filters. However, only one set action per class is supported.

AP side restrictions:

- For FlexConnect local switching and Fabric, the QoS policies are applied at the AP and “police” actions are only enforced at a per flow (5-tuple) level (e.g., rate limiting is per flow)

Catalyst 9800 QoS – Metal QoS

- There are four QoS profiles: Platinum, Gold, Silver and Bronze
- The main purpose of the QoS profile is to **limit the maximum DSCP allowed** on a wireless network **and** thus limit the **802.11 UP value**
- Example with Bronze profile: max DSCP allowed = 8 <> UP = 1

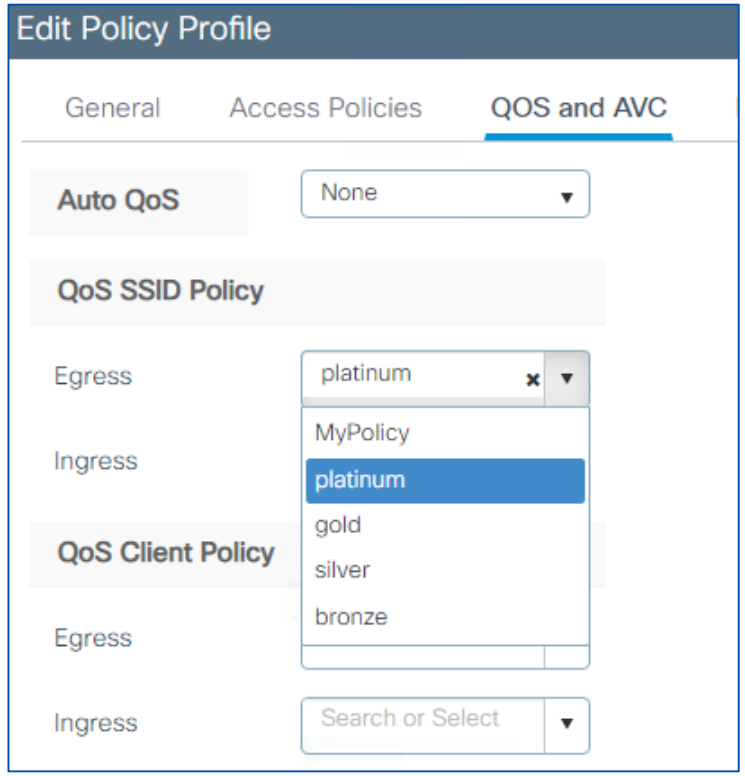


Downstream

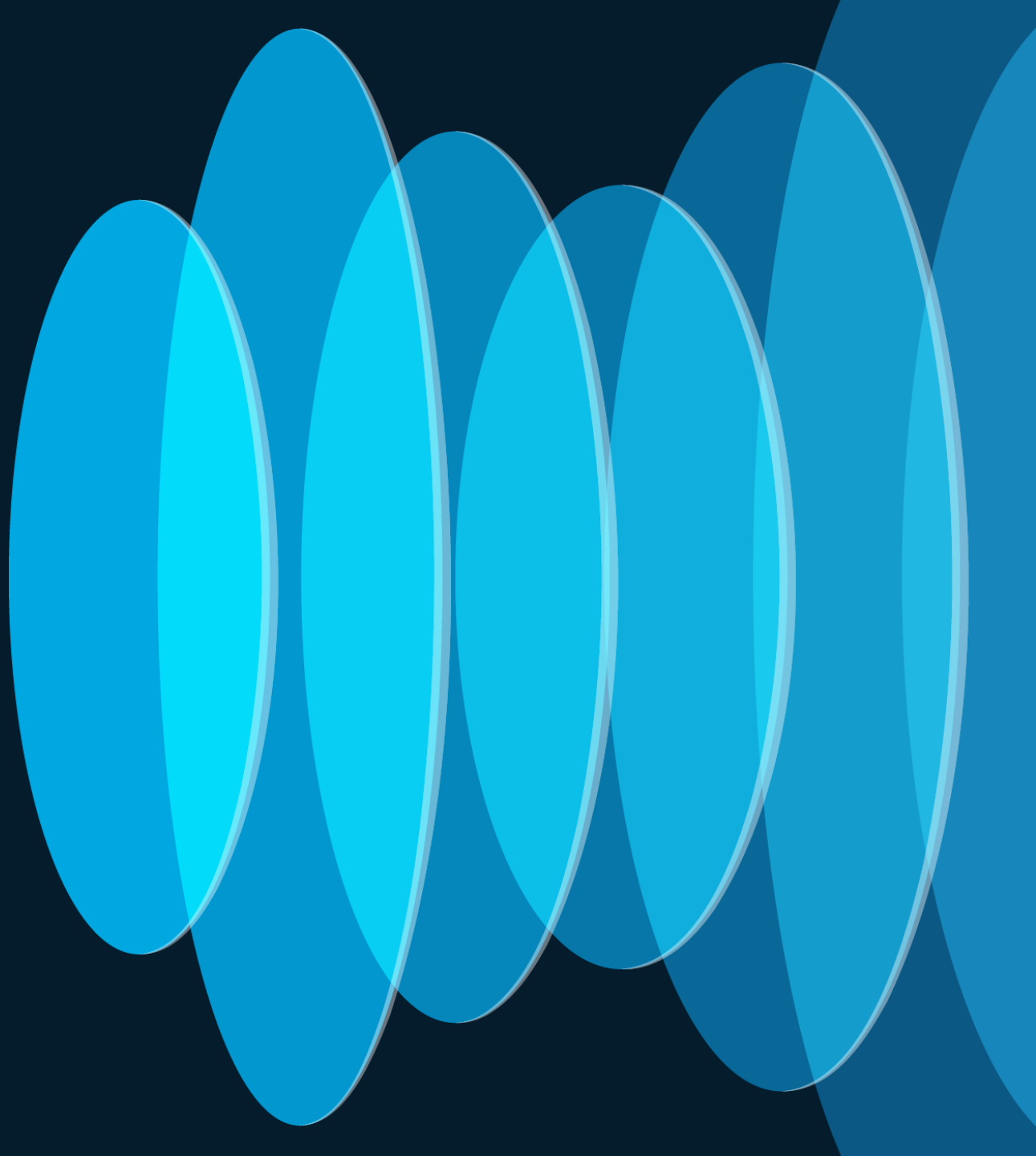
Catalyst 9800 – Metal QoS Profiles

- QoS Metal Profiles in C9800:
  - The inner DSCP value may also be re-written
  - For C9800 you can apply Metal QOS on Egress and Ingress direction separately
  - On the GUI, you can only set the Metal QoS per SSID. On CLI you can also configure it on client target
  - For each profile, there is a max DCSP setting that will be used to remark traffic:

Qos Profile	Max DSCP
Bronze	8
Silver	0
Gold	34
Platinum	46



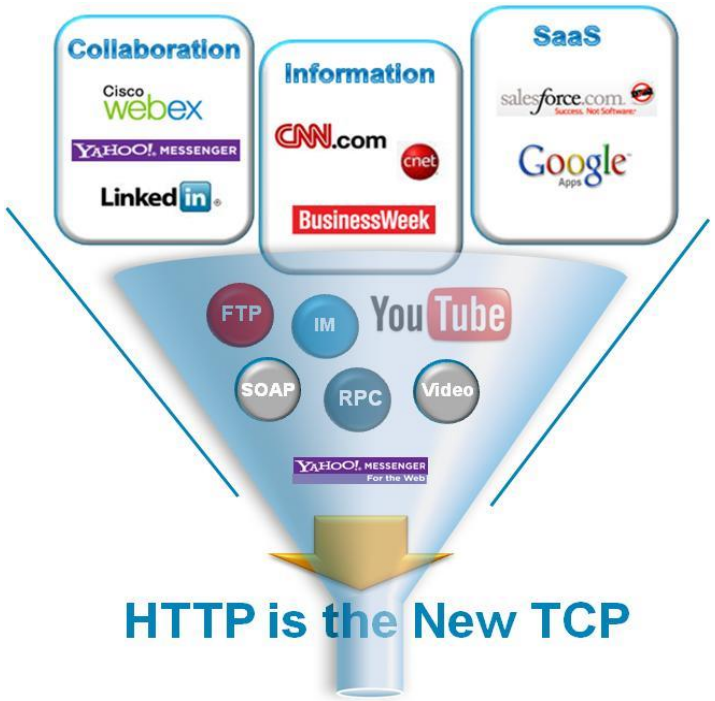
Application Visibility & Control (AVC)



cisco Live!

Application Visibility & Control (AVC)

- Deep Packet Inspection in the wireless controller – allows application identification, remarking, rate limiting, and dropping of unwanted traffic
- Leverages the IOS NBAR2 Engine

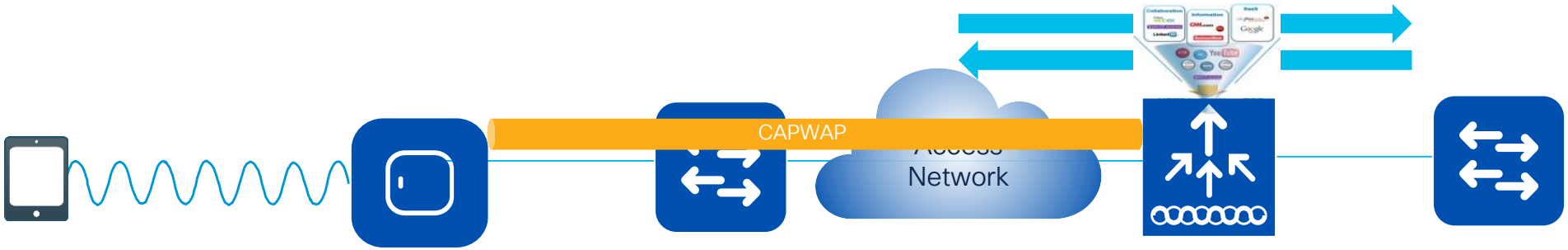


AVC In The Wireless LAN Controller

- Discover which applications are running on your corporate and guest WLANs
- Prioritize critical wireless apps and de-prioritize non-business apps
- Monitor voice and video performance on the WLAN

Application Visibility & Control (AVC)

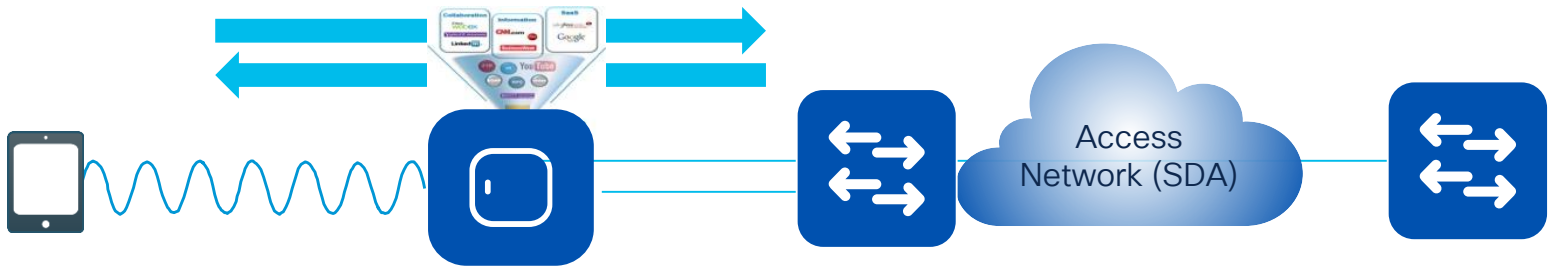
- Central switching: AVC policy is applied at the WLC for downstream and upstream
- AVC can be applied in a specific direction (upstream or downstream or both)
- The “C” in AVC may modify the inner DSCP value, thus influencing the CAPWAP DSCP and wireless UP values; it can also drop or rate limit traffic



Local mode or FlexConnect Central switching

Application Visibility & Control (AVC)

- Local switching: AVC policy is applied at the AP for downstream and upstream
- AVC can be applied in a specific direction (upstream or downstream or both)
- The “C” in AVC may modify the inner DSCP value, thus influencing the CAPWAP DSCP and wireless UP values; it can also drop or rate limit traffic



FlexConnect local switching or Fabric

Custom AVC (cool new feature!)

- New custom apps and attributes can be defined by the user

Custom IP, Port, DSCP

```
eWLC-AVC(config)#ip nbar custom customapp transport udp
eWLC-AVC(config-custom)#?
Custom protocol commands:
  direction  Flow direction
  dscp       DSCP in IPv4 and IPv6 packets
  exit       Exit from custom configuration mode
  ip         ip address
  ipv6       ipv6 address
  no         Negate a command or set its defaults
  port       ports
```

Example:

C9800(config)#ip nbar custom my_app **transport** udp

C9800(config-custom)# **ip address** 9.9.71.50 9.9.71.11 9.9.71.14

C9800(config-custom)# **port** 1111

C9800(config-custom)# **dscp** 0

C9800(config-custom)# **direction** any

Custom HTTP Host and URL

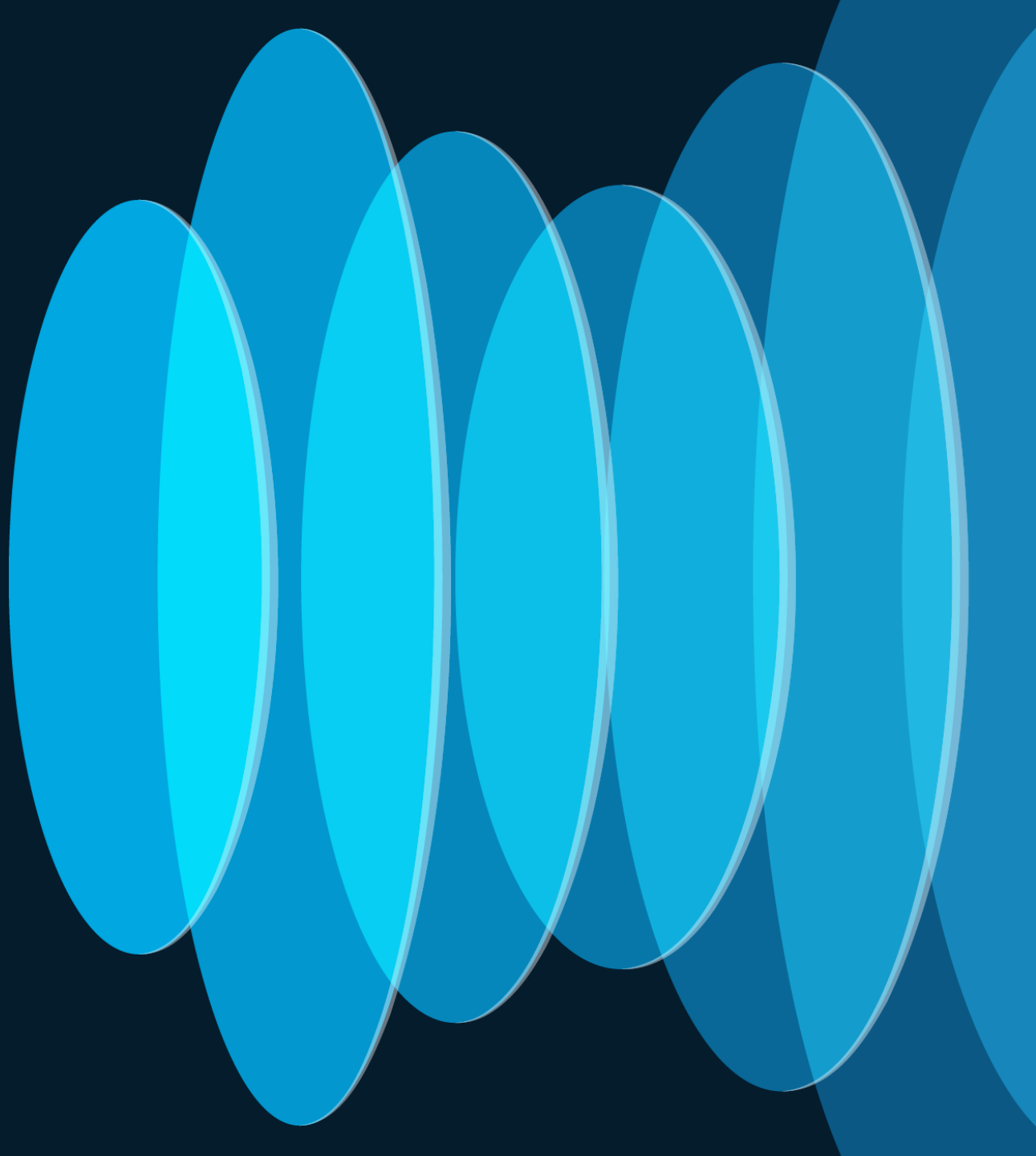
C9800(config)#ip nbar custom my_http http **url** “latest/whatsnew.html”

C9800(config)#ip nbar custom my_http http **host** “www.anydomain.com”

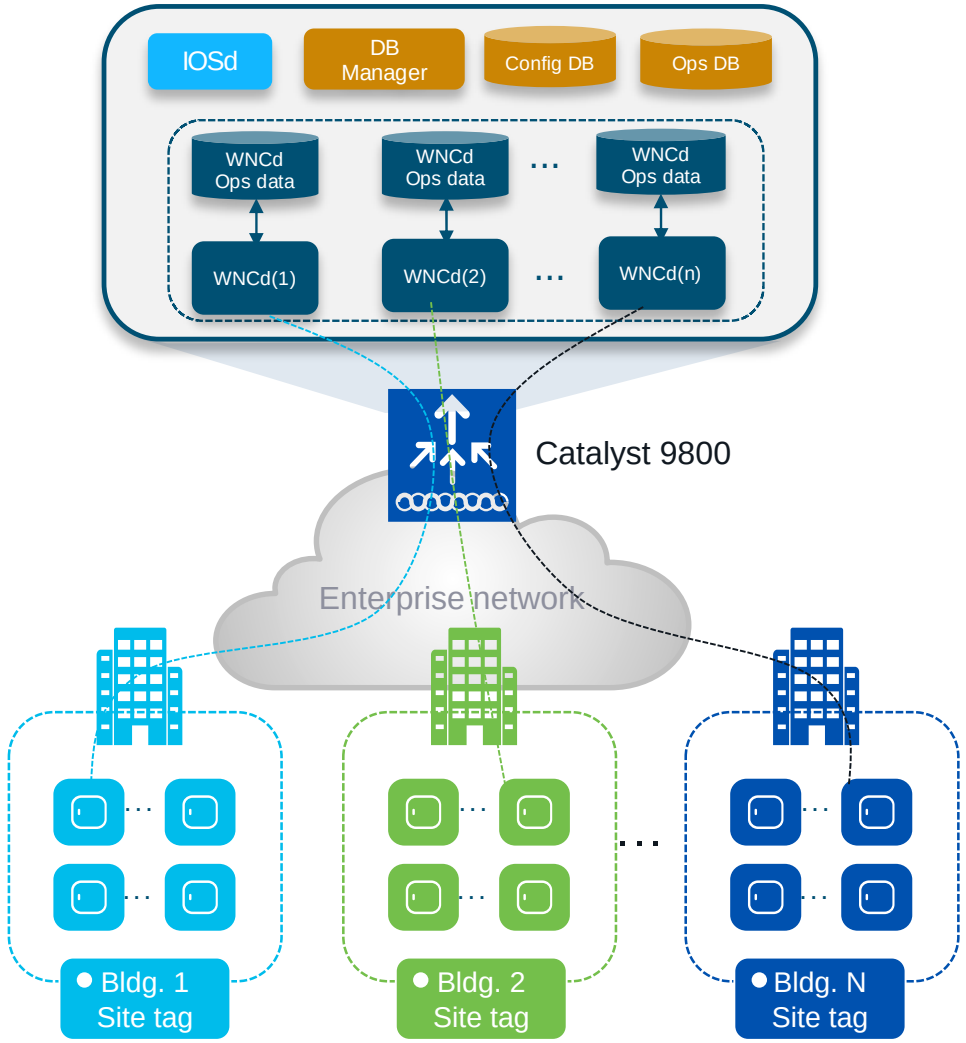
C9800(config)#ip nbar custom my_http http **url** “latest/whatsnew” **host** “www.anydomain.com”

The URL or host specification strings can take the form of a **regular expressions**

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:

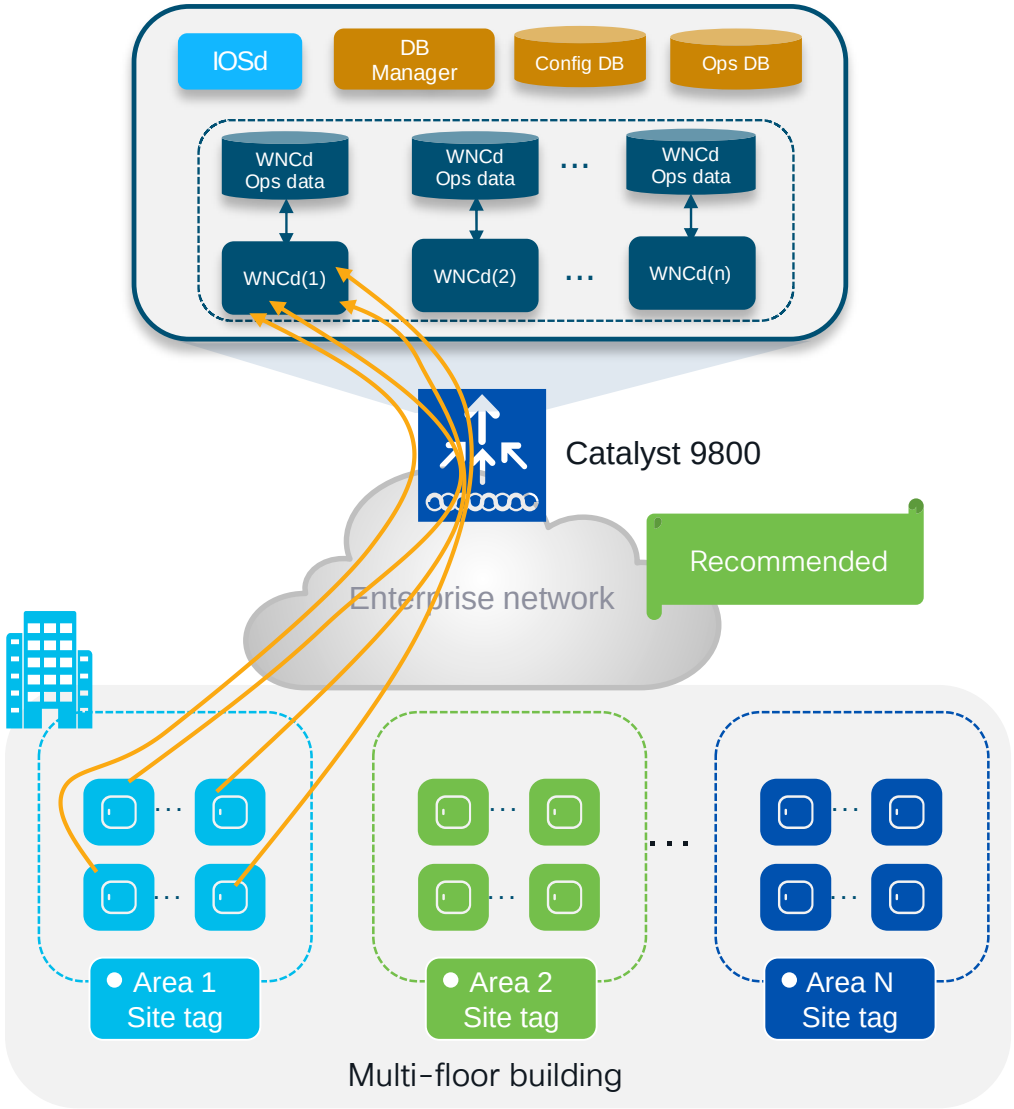
Platform	# of WNCD instances
EWC (on AP or C9k switch)	1
C9800-L	1
C9800-CL (small)	1
C9800-CL (medium)	3
C9800-40 / CW9800M	5
C9800-CL (large)	7
C9800-80 / CW9800H1/H2	8

Following command shows the # of WNCDs processes:

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

Site Tags – AP to WNCd distribution

Refresher!



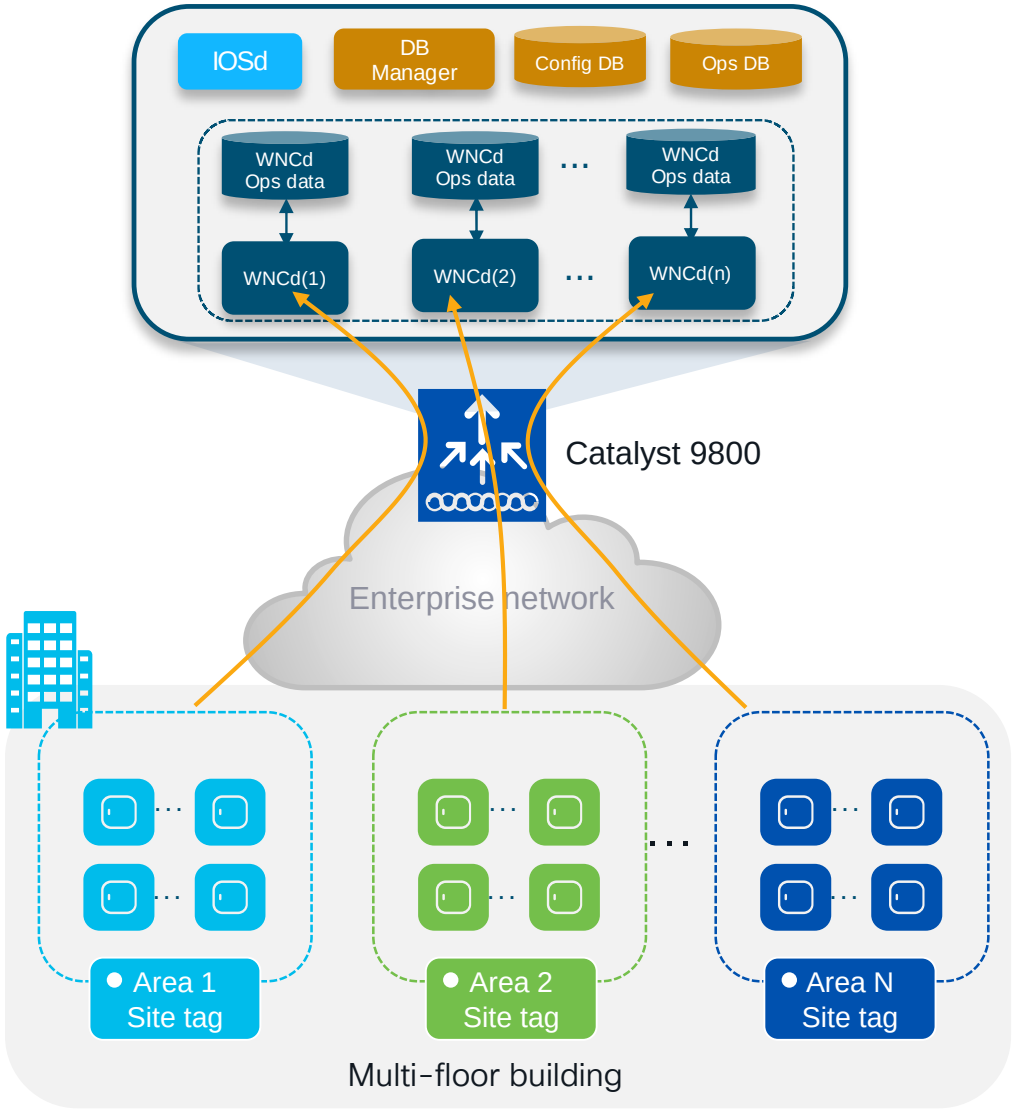
How AP distribution across WNCds works:

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

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

Site Tags – AP to WNCd distribution

Refresher!



Recommendations:

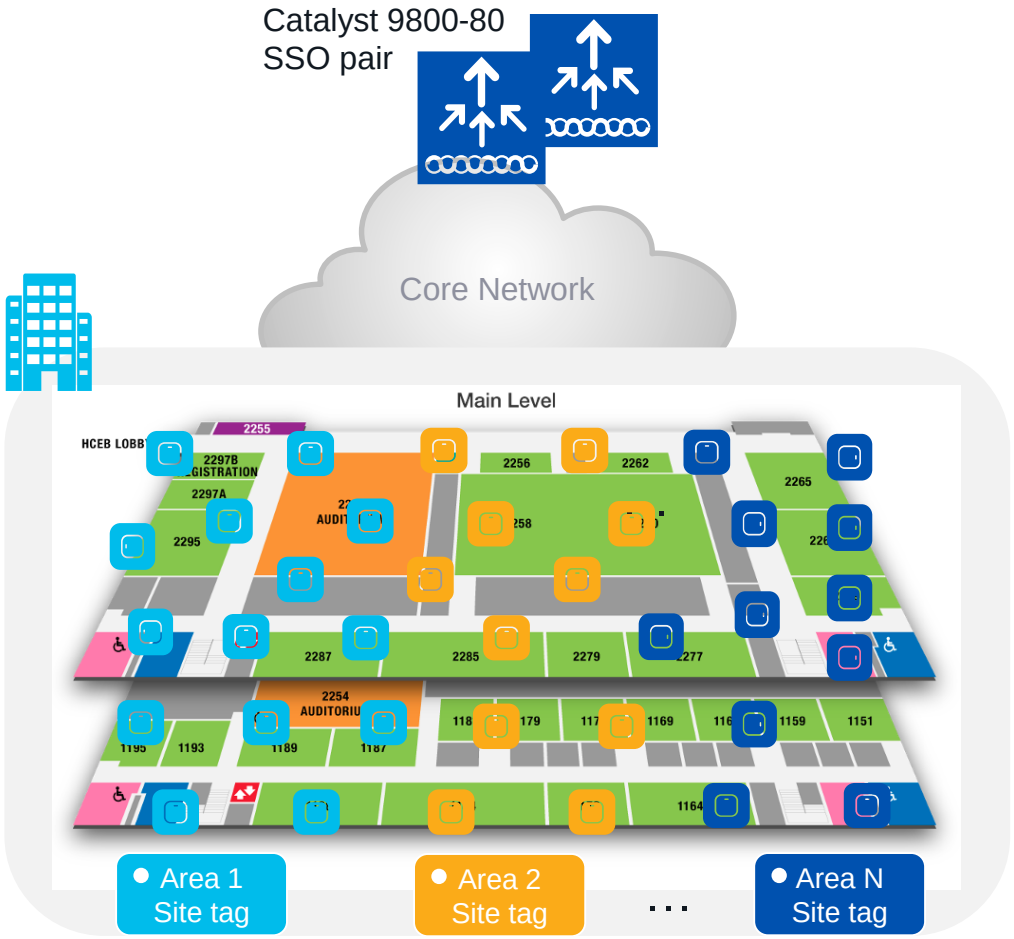
- Use **custom site tags**
- Whenever possible, have **less than 500 APs per site tag**
- **Do not overwhelm a site-tag and WNCd.** Do not exceed the following max number of APs per site tag:

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

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

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

Site Tags Design – Large venue deployment



Scenario#1: Large venue deployment

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

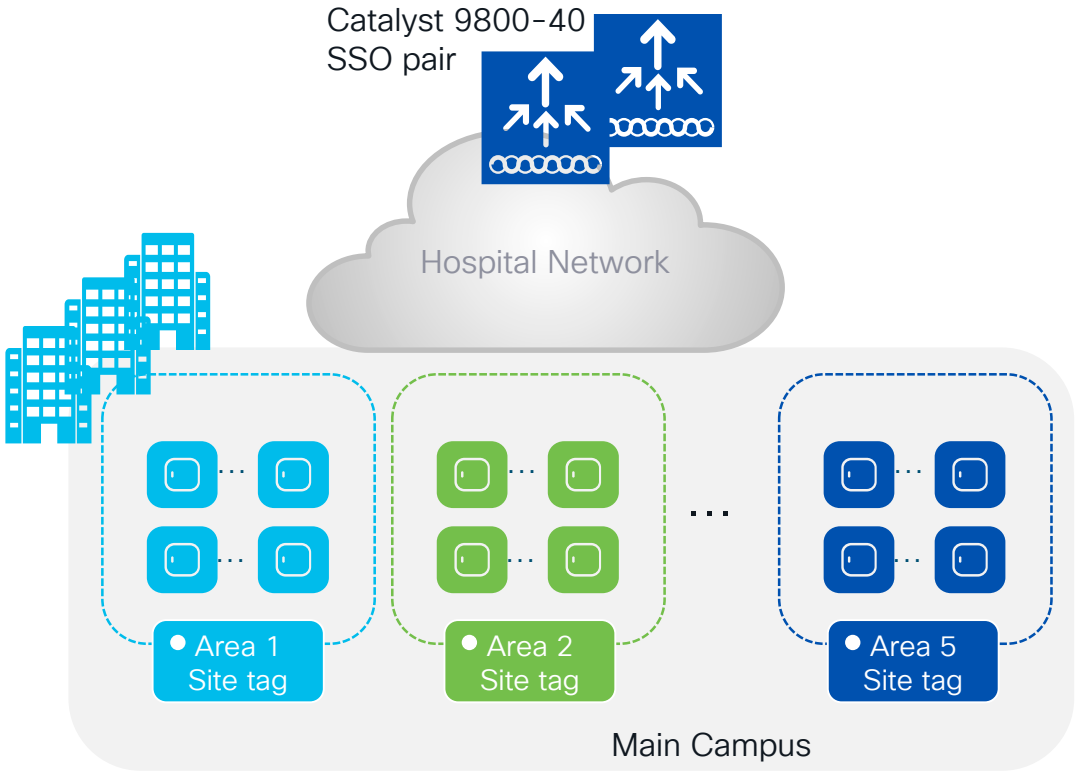
What are the recommendations in this case?

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

Platform	# site tag
C9800-80 / CW9800H1/H2	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 – AP to WNCd distribution



Customer design

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

Recommendations:

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

Wireless Config Analyzer Express (WCAE)

The wireless engineer trowel

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

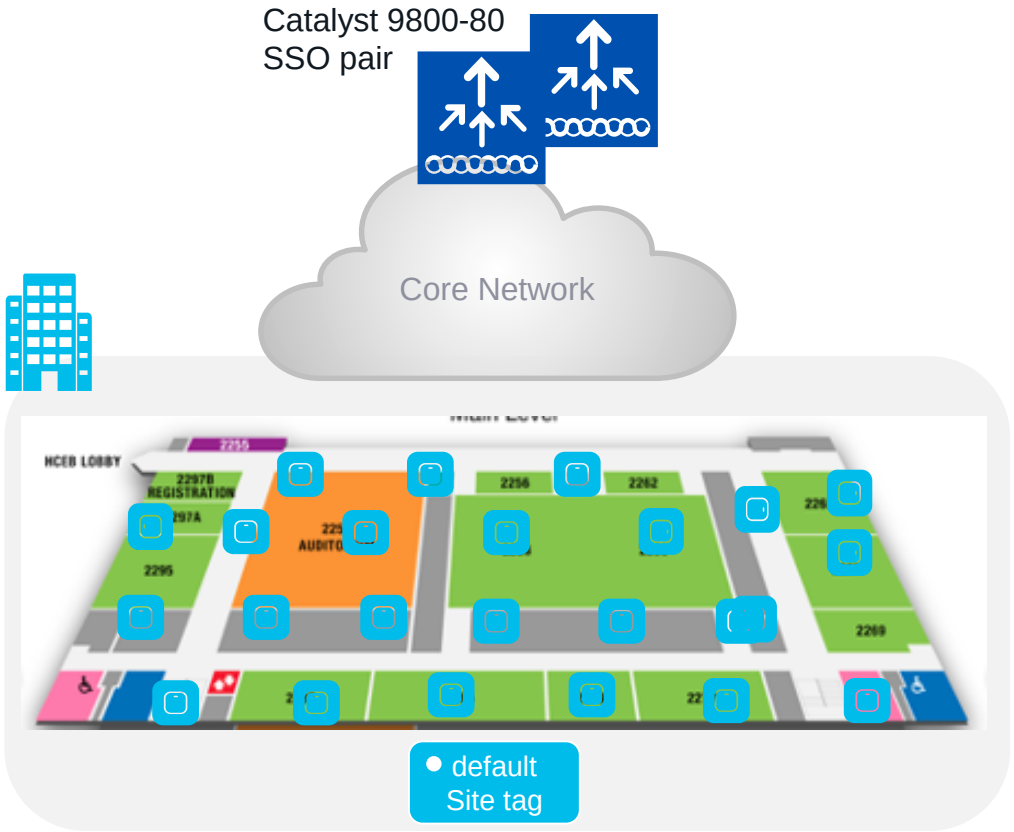
starting 17.9

Back to Content Tab

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

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

Site Tags Design – Special case



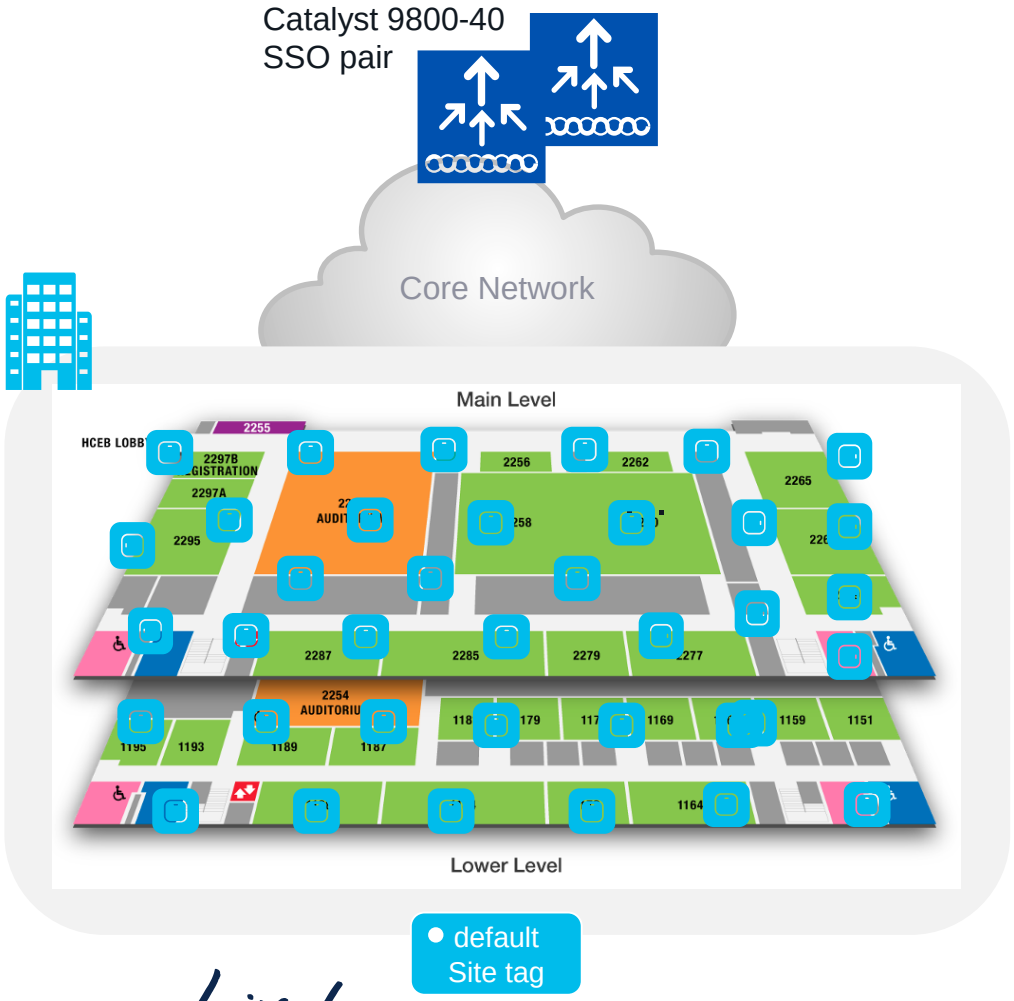
Scenario #2: Large warehouse

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

Can I use the default-site-tag?

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

Site Tags – AP to WNCd distribution



Customer Design

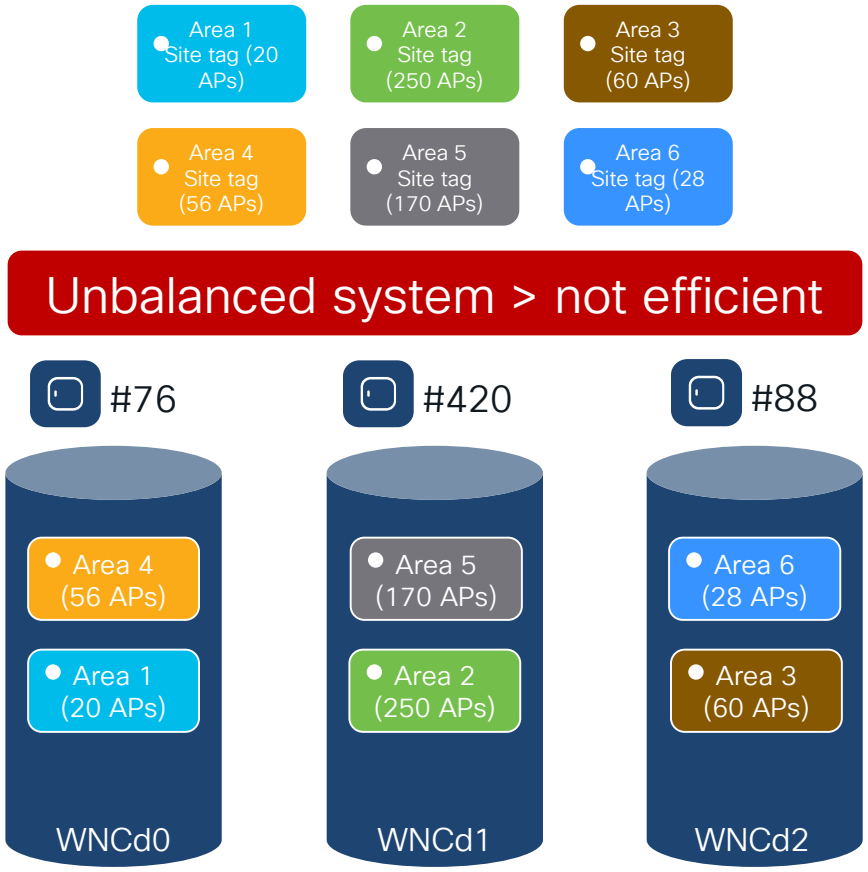
- What if the customer cannot design multiple custom site tags? For example: No AP names, no APs on maps, difficult to identify AP areas, or simply too much operational cost…
- Example: large conference venue with local mode deployment running 17.6 and higher

Is using default-site-tag an option?

- Yes. You can go with default-site tag, as this is local mode deployment and there is no restriction on roaming
- APs are load-balanced across WNCDs in round-robin fashion
- Fast roaming (11r, OKC, etc.) is supported across WNCds
- 802.11k/v is also supported starting 17.6
- This has been tested at scale for IPv4 deployment and we have seen some degradation due to increased inter-WNCd communication, but this is still considered a valid option

OKC = Opportunistic Key Caching

Site Tags – AP to WNCd distribution

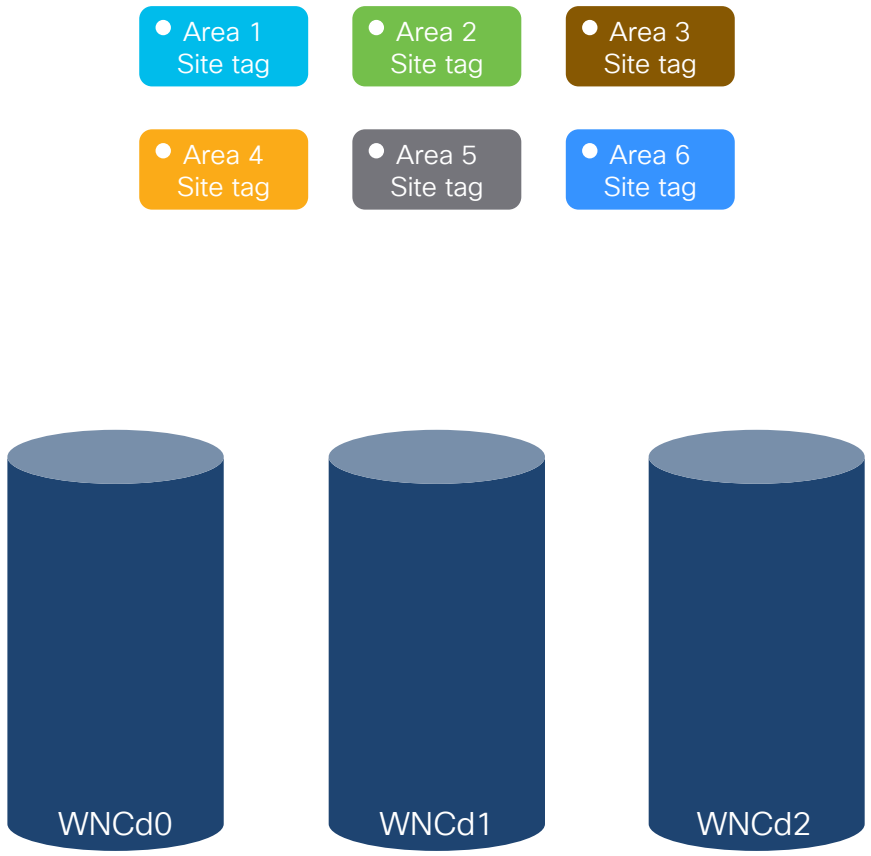


Until 17.9.1, site tags are distributed among WNCds using the least loaded criteria based on the number of site tags. The algorithm doesn't take into considerations the number of APs or clients per site tag

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

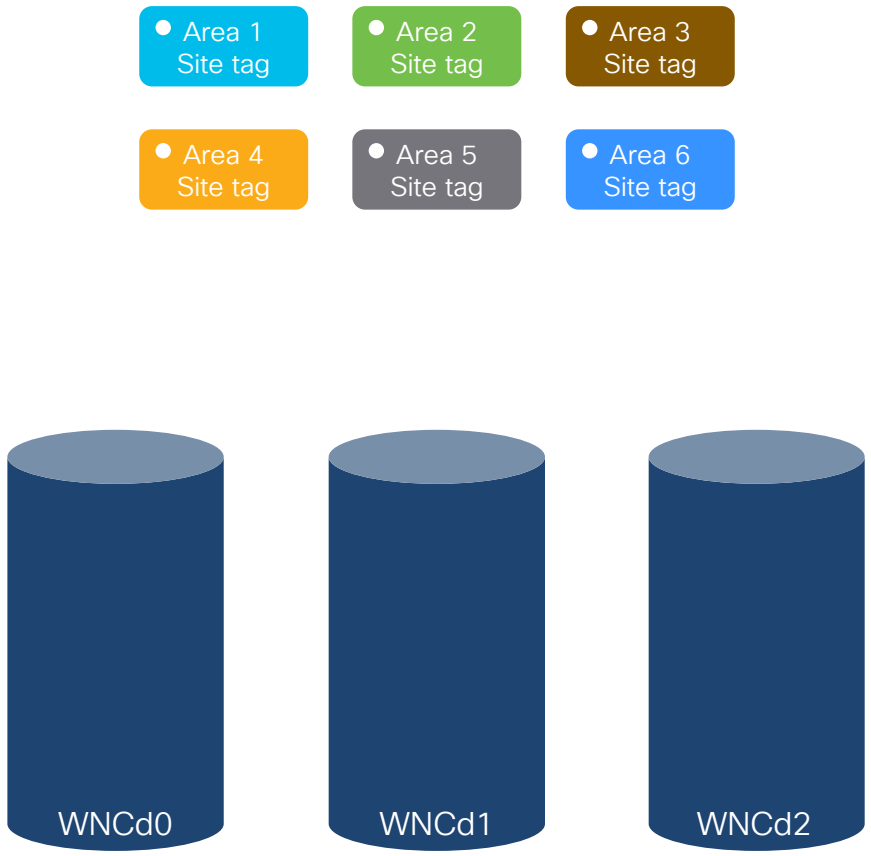


- Starting 17.9.2 and 17.10, the algorithm to distribute APs among WNCds may use the load parameter configured under the site tag:

```
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

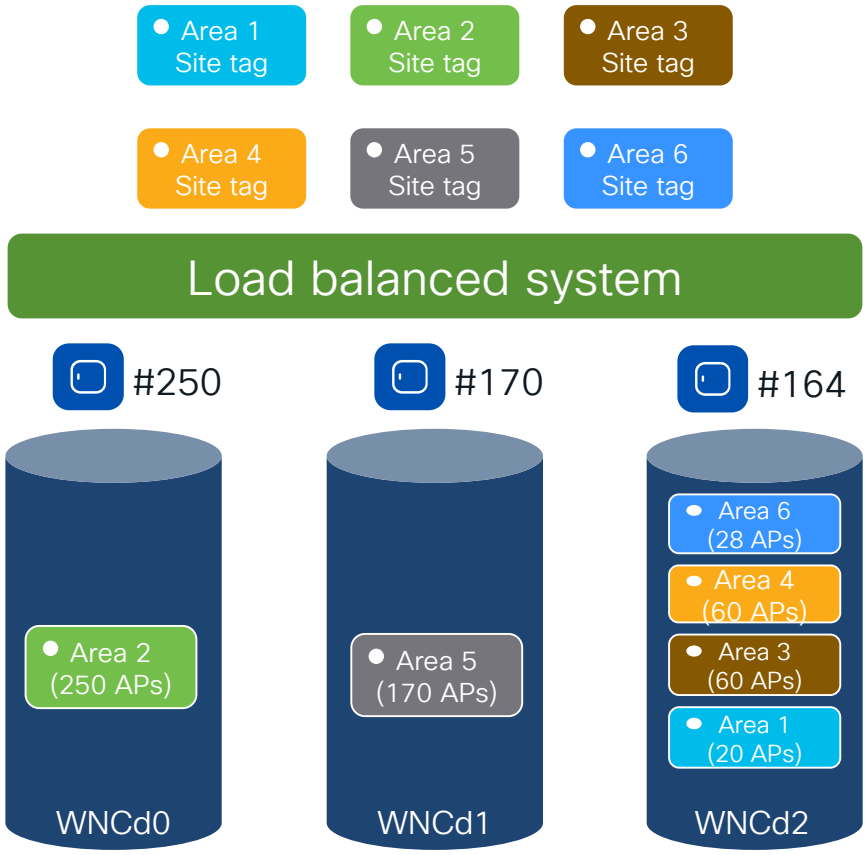
Site Tags – New load balancing Algorithm



How to choose the load?

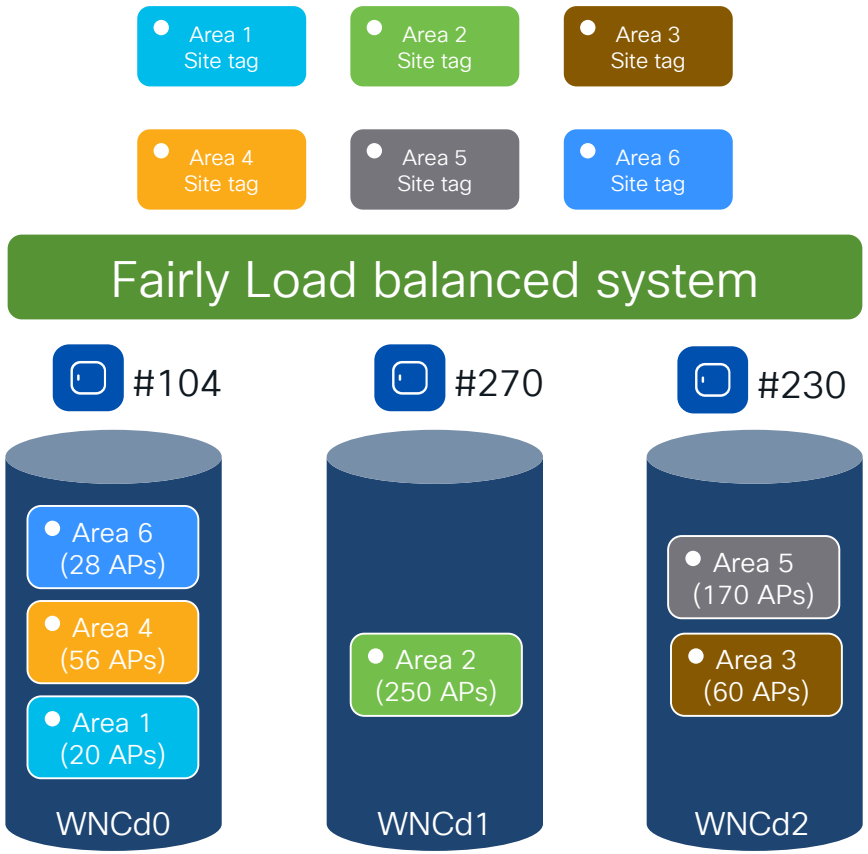
- The default value 0 means no load indication for the site tag. Nothing changes, the algorithm is the same as in 17.9.1 and previous releases
- **Most common option**: Office building with multiple floors/areas. Each floor/area is one site tag. If you estimate similar client/traffic load on each floor/area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

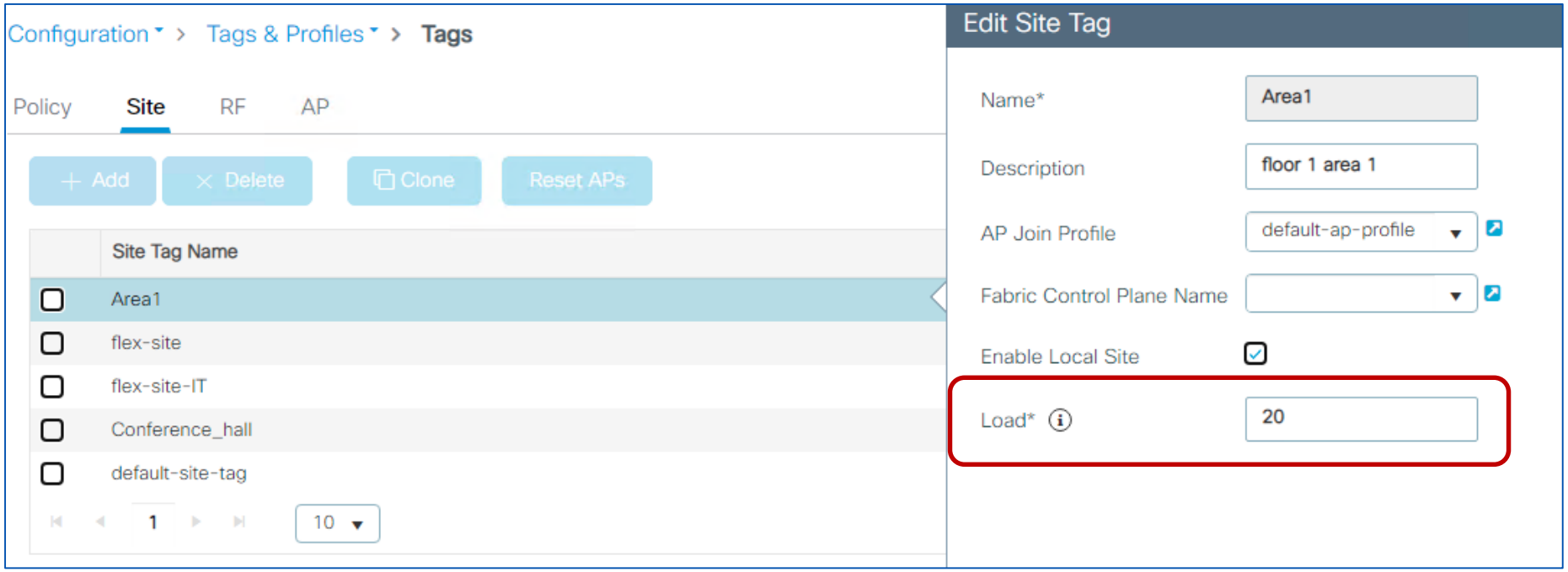
Site Tags – New load balancing Algorithm



- 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.

Verifying the site tag Load- CLI

```
C9800#show wireless loadbalance tag affinity

Tag                          Tag type   No of AP's Joined   Wncd Instance
-------------------------------------------------------------------------
area1                        SITE TAG   20                  0
area3                        SITE TAG   60                  0
area4                        SITE TAG   56                  0
area6                        SITE TAG   28                  0

area2                        SITE TAG   250                 1

area5                        SITE TAG   170                 2
```

#160 APs

#250 APs

#170 APs

Questions on AP <> WNCd load balancing

Q1: I have a C9800-80 and 12 site tags. Given the recommendation to use #8 site tags, shall I redesign?

A1: No site tag redesign should be done unless there is a high CPU utilization issue. If you do have an issue and your deployment is a large venue, with a large roaming domain, then it's recommended to use the same number of site tags as WNCd

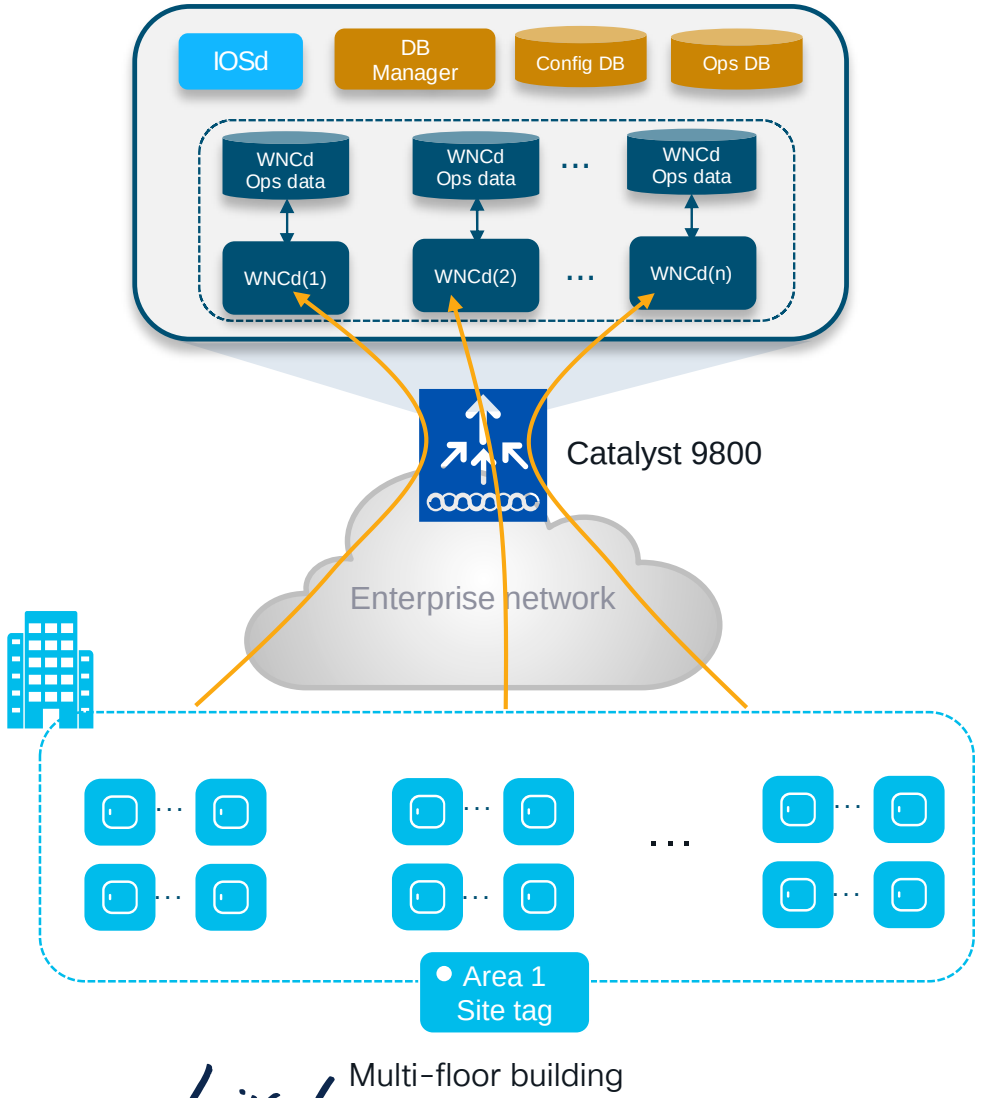
Q2: I have an existing deployment (site tags already configured) and I add new site tags and configure the load parameter only the new ones, what is going to happen?

A2: This is not recommended. If load is configured, it should be configured on all tags, existing and new. Otherwise, the load balance will not be efficient

Q3: I have configured the load and rebooted the WLC; after some time, I want to tweak the load configuration of a few site tags. If I change the load on these tags, what's going to happen?

A3: The load balance will not be the best until you reboot the WLC again. If not rebooted and the APs are disconnected, they will be load balanced based on the least loaded WNCd instance and dependent on the order of AP join

Site Tags – AP to WNCd distribution



What if?

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

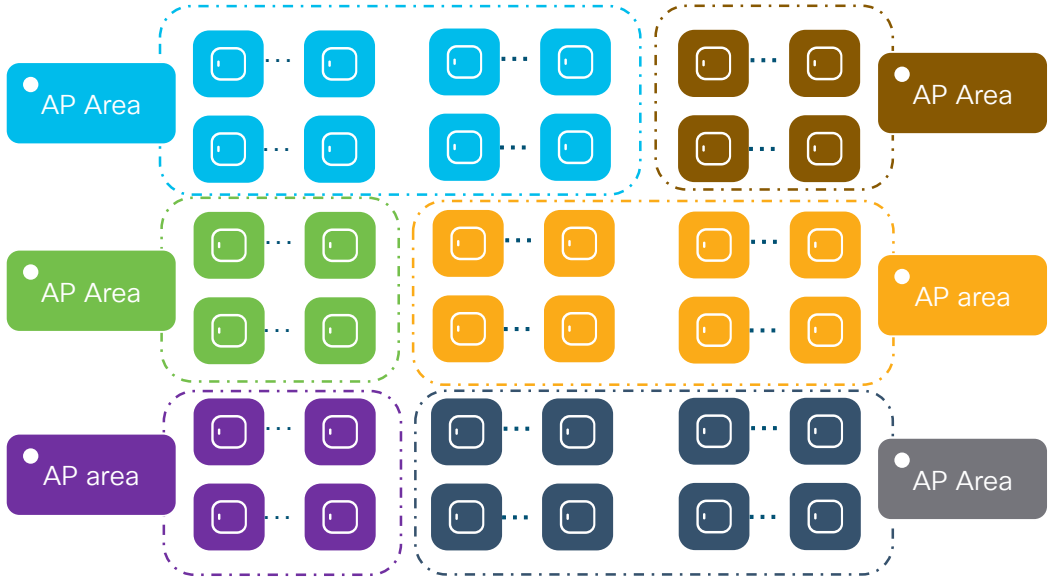
Starting 17.12.1, we have a solution!

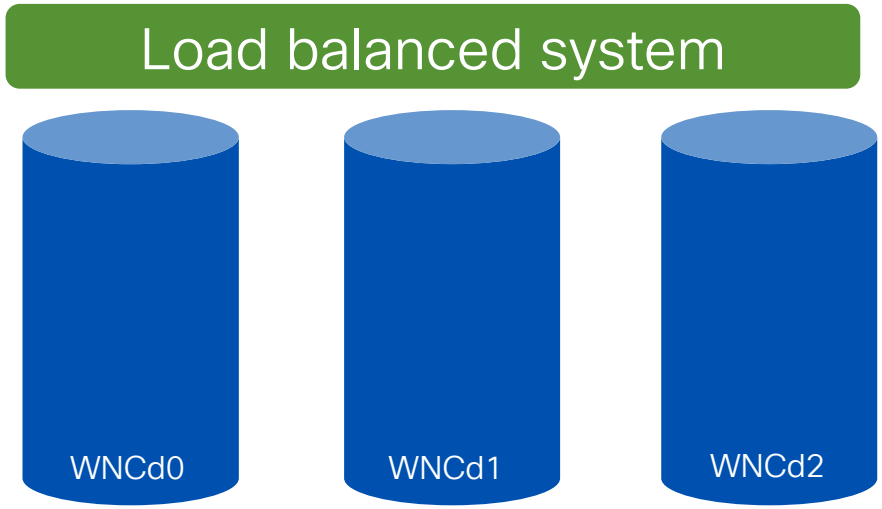
(RRM based) Auto WNCd load balancing

RRM based Auto WNCd load balancing

What is it?

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

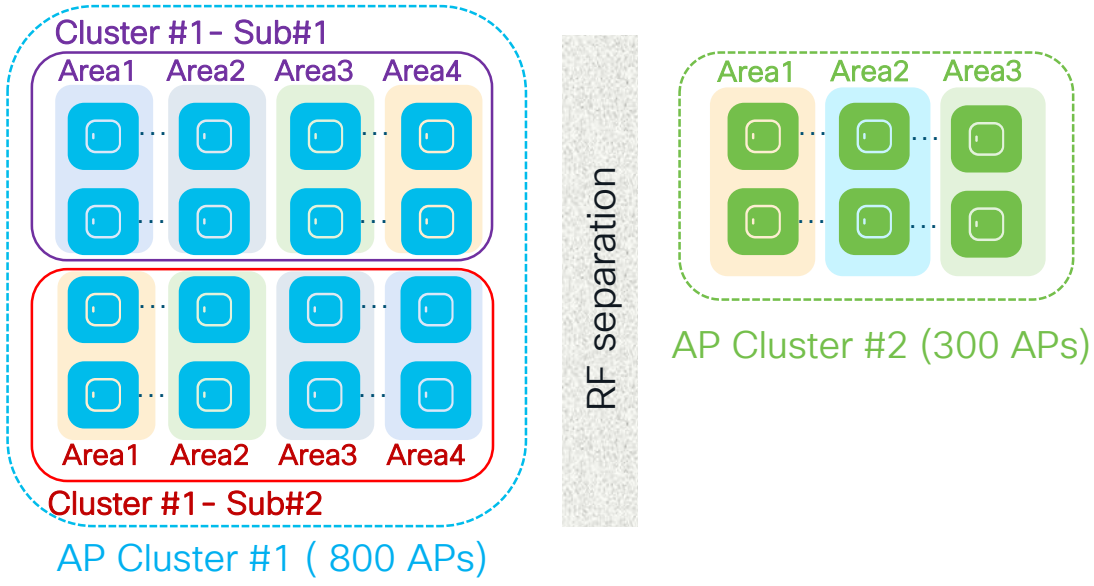




RRM based auto WNCd load balancing

How does the auto load balancing algorithm work?

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



RRM based Load Balancing - Configuration

Before you can run the RF based load balancing algorithm, and to make sure the result is consistent across reloads and on demand iterations, configure the following CLI command,

```
C9800# configure terminal
C9800(config)# wireless load-balance ap method rf
```

On-demand exec CLI to start the algorithm instantly:

```
C9800# ap neighborhood load-balance start
```

On-demand exec CLI to apply the algorithm results instantly. It will re-balance the APs using CAPWAP reset:

```
C9800# ap neighborhood load-balance apply
```

Trigger the Algorithm

Trigger Manually:

```
C9800# ap neighborhood load-balance start
```

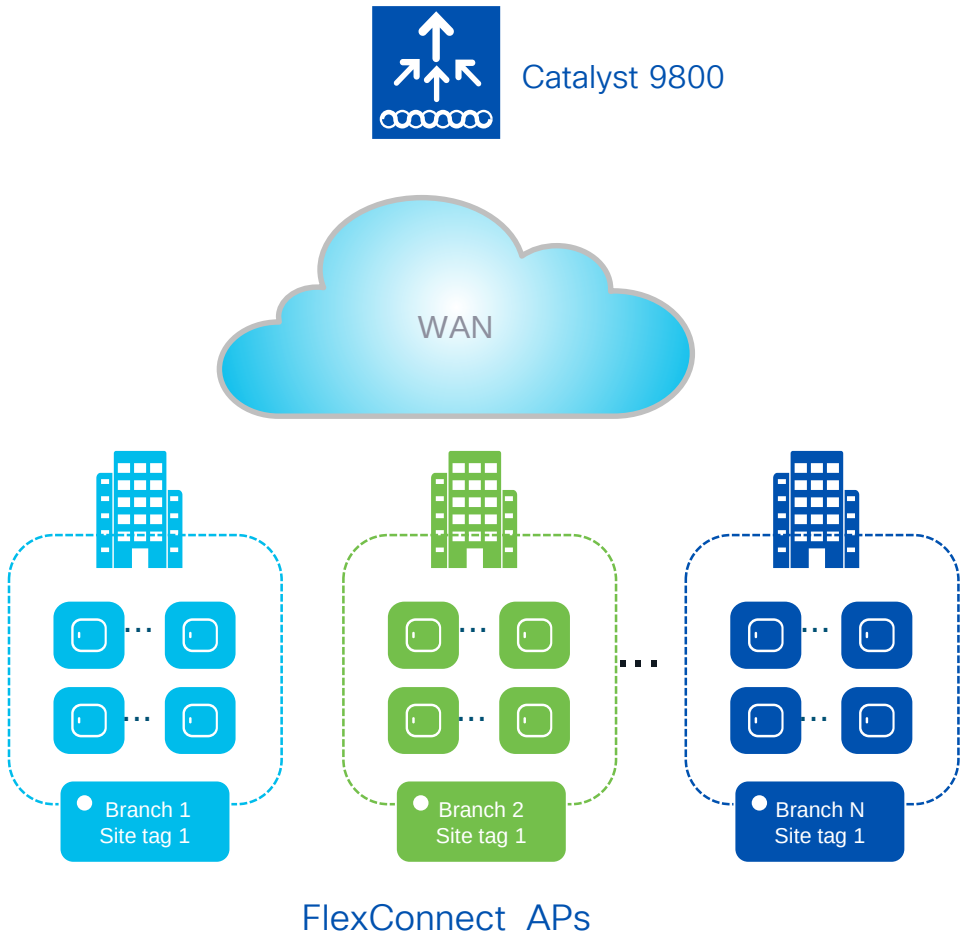
Schedule via Calendar Profile:

```
C9800# conf t
C9800(config)# ap neighborhood calendar-profile <calendar name>
```

Log Message:

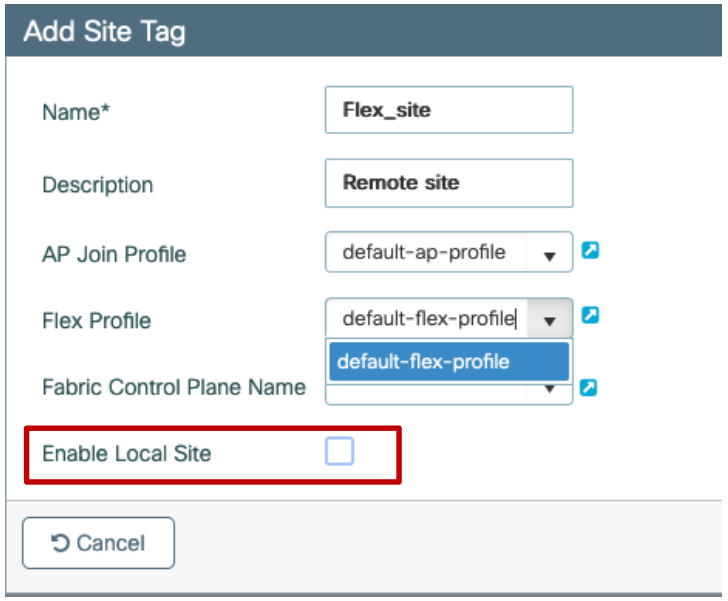
```
March 19 19:38:31.424: %NEIGHBORHOOD_LOG-5-AP_NEIGHBORHOOD_START: Chassis 1 R0/0:
wncmgrd: Starting AP neighborhood clustering formation and distribution across WNCd
instances. Total number of APs collected for calculation: 5.

March 19 19:38:31.432: %NEIGHBORHOOD_LOG-5-AP_NEIGHBORHOOD_DONE: Chassis 1 R0/0:
wncmgrd: AP clustering and WNCd assignment algorithm completed. 5 number of AP
neighborhoods formed and ready to be load balanced across WNCd instances.
```

Site Tag for FlexConnect Deployments



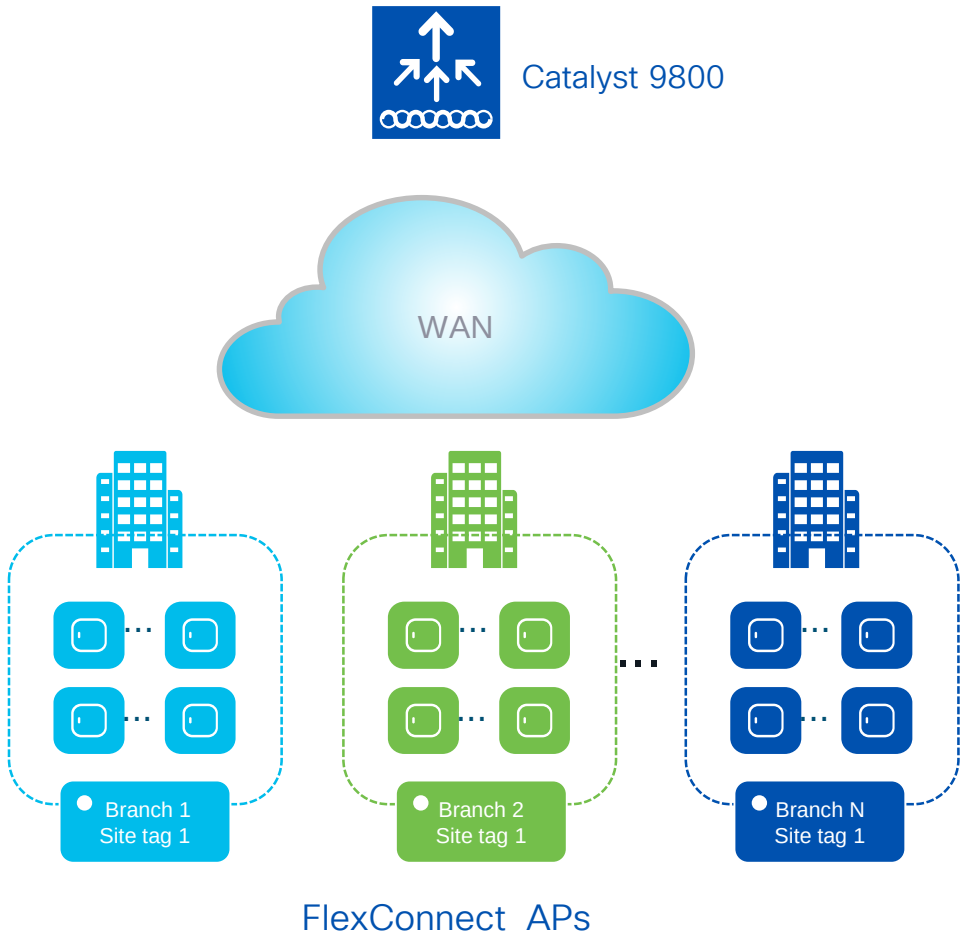
Important facts:

- 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

For your reference

Design- Recommended use of AP Site Tags

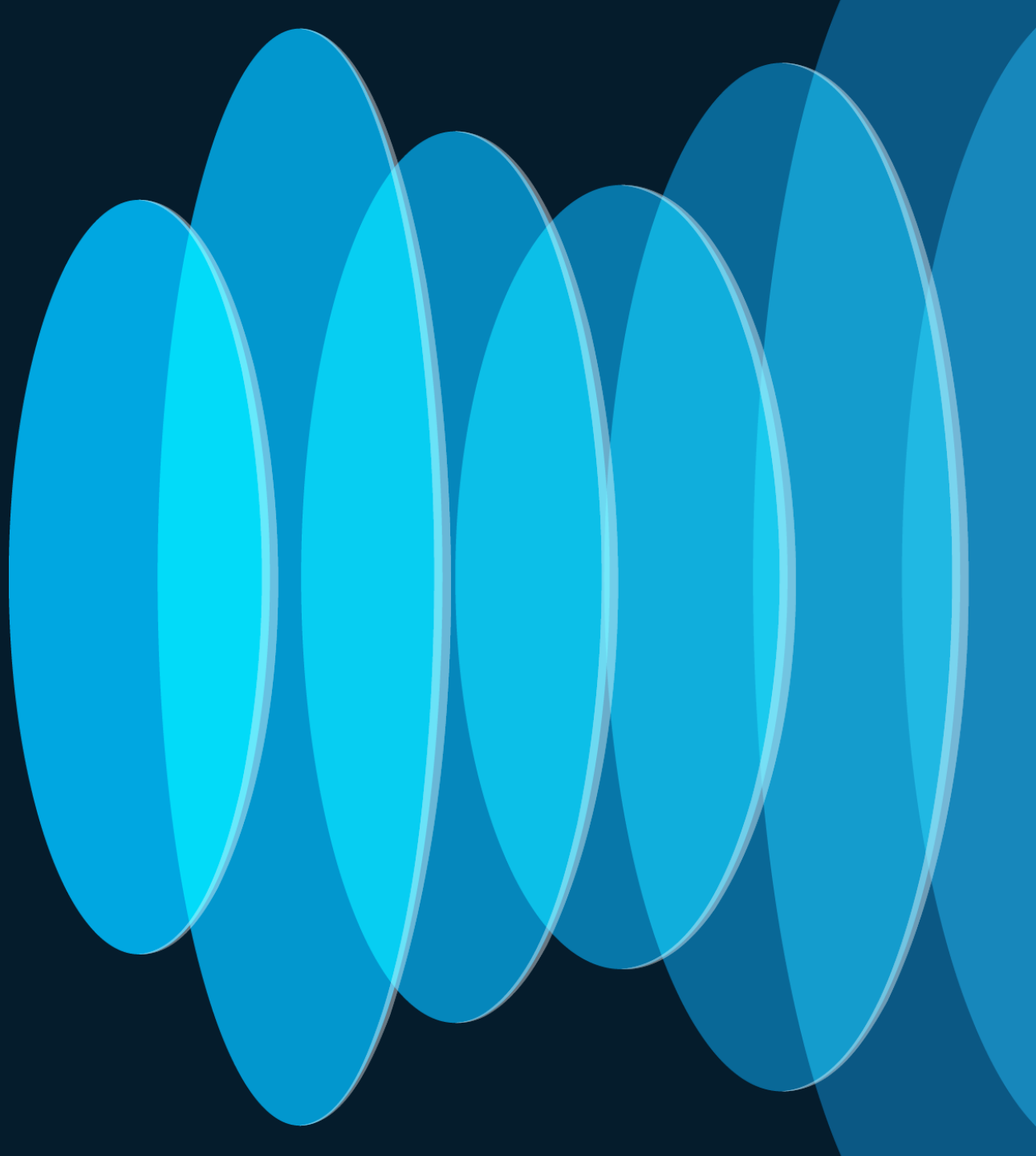
1 For **Local mode APs**, the recommended number is **500 APs per Site Tag**. But it should not exceed the following limit:

Platform	Max APs per site tag
9800-80, 9800-CL (Medium and Large) CW9800H1/H2	1600
9800-40, CW9800M	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 / CW9800H1/H2	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,..)

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

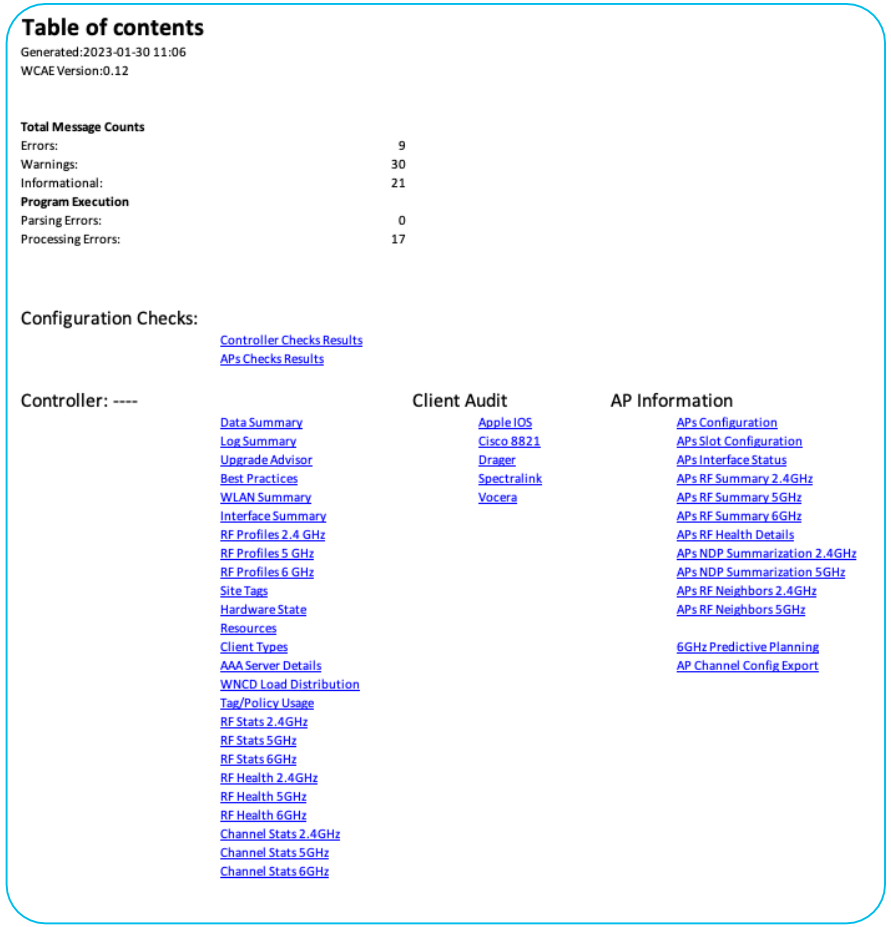


Table of contents

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

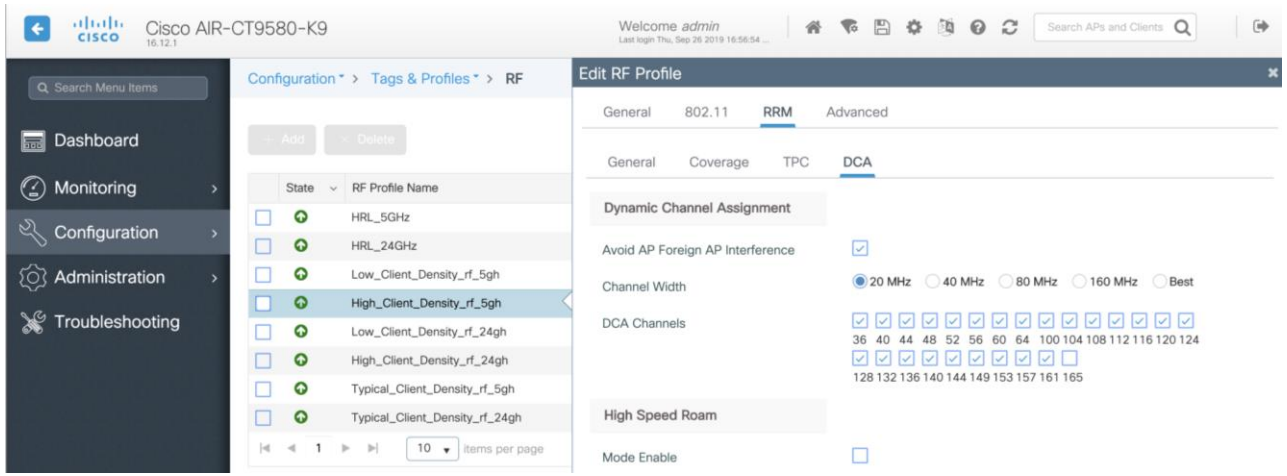
6GHz Predictive Planning
AP Channel Config Export

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) or AutoChannel (Meraki) via RF Profile
- If needed – **eliminate unusable channels** for business-critical areas (DFS, etc)
- Reserve channels for use by other systems



Catalyst Tip: Identifying Potentially Unhealthy Channels

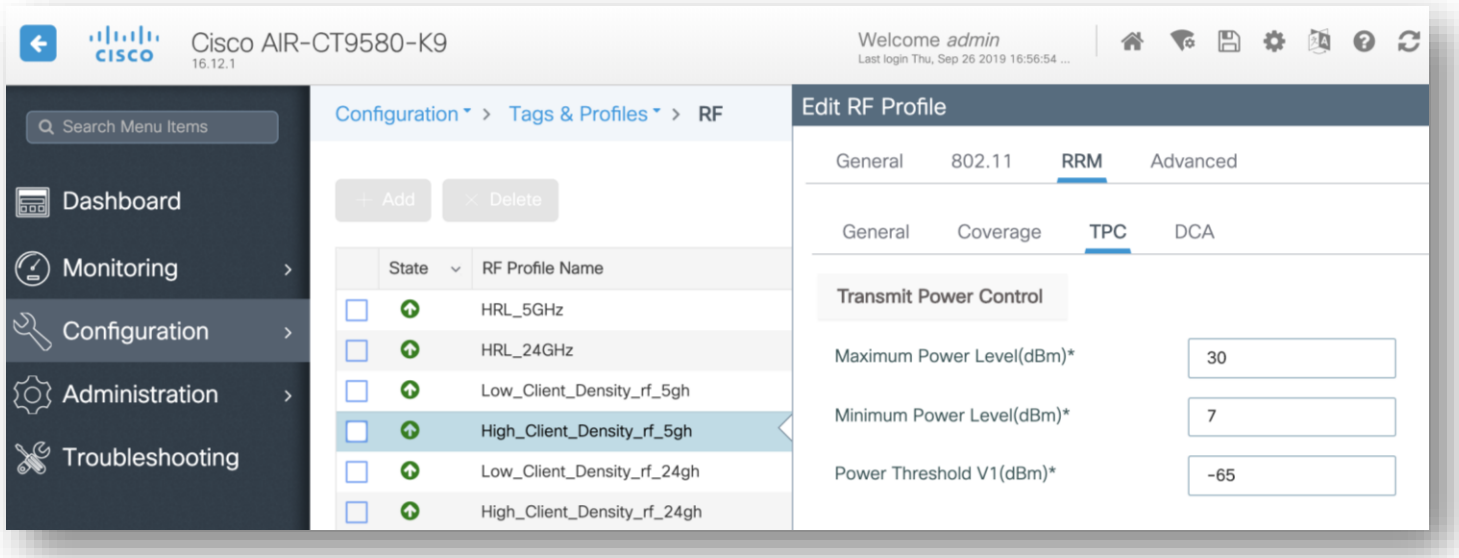
WCAE – 'APs RF Summary' tab – "High Channel Changes" column

C	D	G	H	I	J	K	L	M	N	O	V
Model	Mode	Chann	TX Pow	TX Power dB	Total Clients	RX SOP	CH Util%	CH TX Util%	CH RX Util%	Channel Changes	High Channel Chang
C9130AXI-B	Client Serving	108	3	9	18	medium(-78)	50	3	0	18	Yes
C9130AXI-B	Client Serving	140	2	12	8	medium(-78)	73	50	4	20	Yes
C9130AXI-B	Client Serving	52	2	11	17	medium(-78)	46	5	0	20	Yes
C9130AXI-B	Client Serving	64	2	11	4	medium(-78)	11	0	0	25	Yes
C9130AXI-B	Client Serving	100	3	9	12	medium(-78)	49	2	0	30	Yes
C9130AXI-B	Client Serving	44	5	9	7	medium(-78)	47	8	0	23	Yes
C9130AXI-B	Client Serving	100	3	9	13	medium(-78)	38	7	0	19	Yes
C9130AXI-B	Client Serving	56	2	11	22	medium(-78)	46	17	1	28	Yes
C9130AXI-B	Client Serving	132	3	9	14	medium(-78)	37	8	0	32	Yes
C9130AXI-B	Client Serving	52	2	11	15	medium(-78)	45	1	0	18	Yes
C9130AXI-B	Client Serving	56	2	11	23	medium(-78)	42	7	14	25	Yes
C9130AXI-B	Client Serving	116	3	9	9	medium(-78)	24	3	0	22	Yes
C9130AXE-B	Client Serving	52	2	15	0	medium(-78)	2	0	0	19	Yes
C9130AXE-B	Client Serving	36	2	19	0	medium(-78)	1	0	0	20	Yes
C9130AXE-B	Client Serving	56	2	15	0	medium(-78)	1	0	0	30	Yes
C9130AXE-B	Client Serving	149	2	20	0	medium(-78)	2	0	0	22	Yes
C9130AXE-B	Client Serving	124	2	15	88	medium(-78)	78	19	13	70	Yes
C9130AXE-B	Client Serving	48	2	20	0	medium(-78)	2	0	0	66	Yes
C9130AXE-B	Client Serving	36	2	19	0	medium(-78)	2	0	0	19	Yes
C9130AXE-B	Client Serving	44	2	20	0	medium(-78)	2	0	0	21	Yes
C9130AXE-B	Client Serving	108	2	15	0	medium(-78)	1	0	0	25	Yes
C9130AXE-B	Client Serving	149	2	20	0	medium(-78)	1	0	0	21	Yes

"High Channel Change: Yes" triggered for radios with more than 4 channel changes per day

Balancing Transmit Power with RF Profiles

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



Identifying Possible Power Imbalance

WCAE – 'APs RF Summary' tab – "TX Power dBm" and "Total Clients" columns

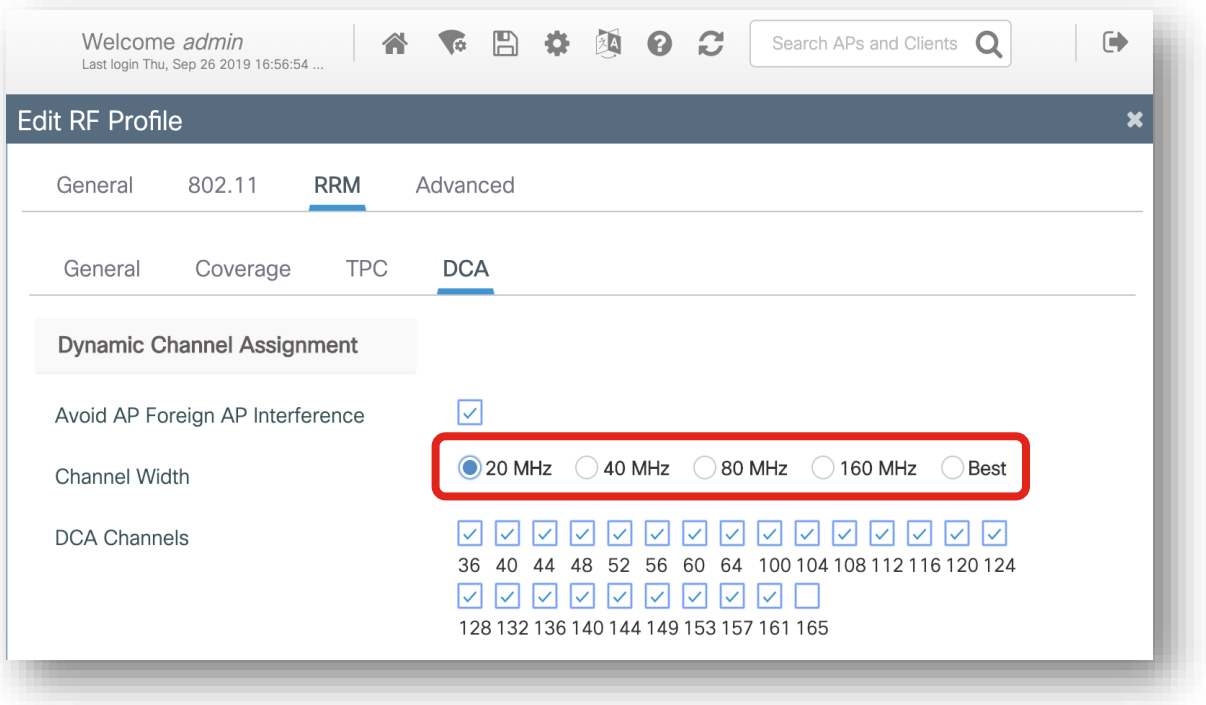
Name	Slot	Band	Channel	TX Power	TX Power dBm	Total Clients
AP1	1	5	100	1	17	21
AP1	2	5	48	1	23	70

6dB power difference = client imbalance

Refer to AP power tables to determine max TX power per UNII band

Use "show controller" on a sample AP for all details

Selecting Channel Width with RF Profiles



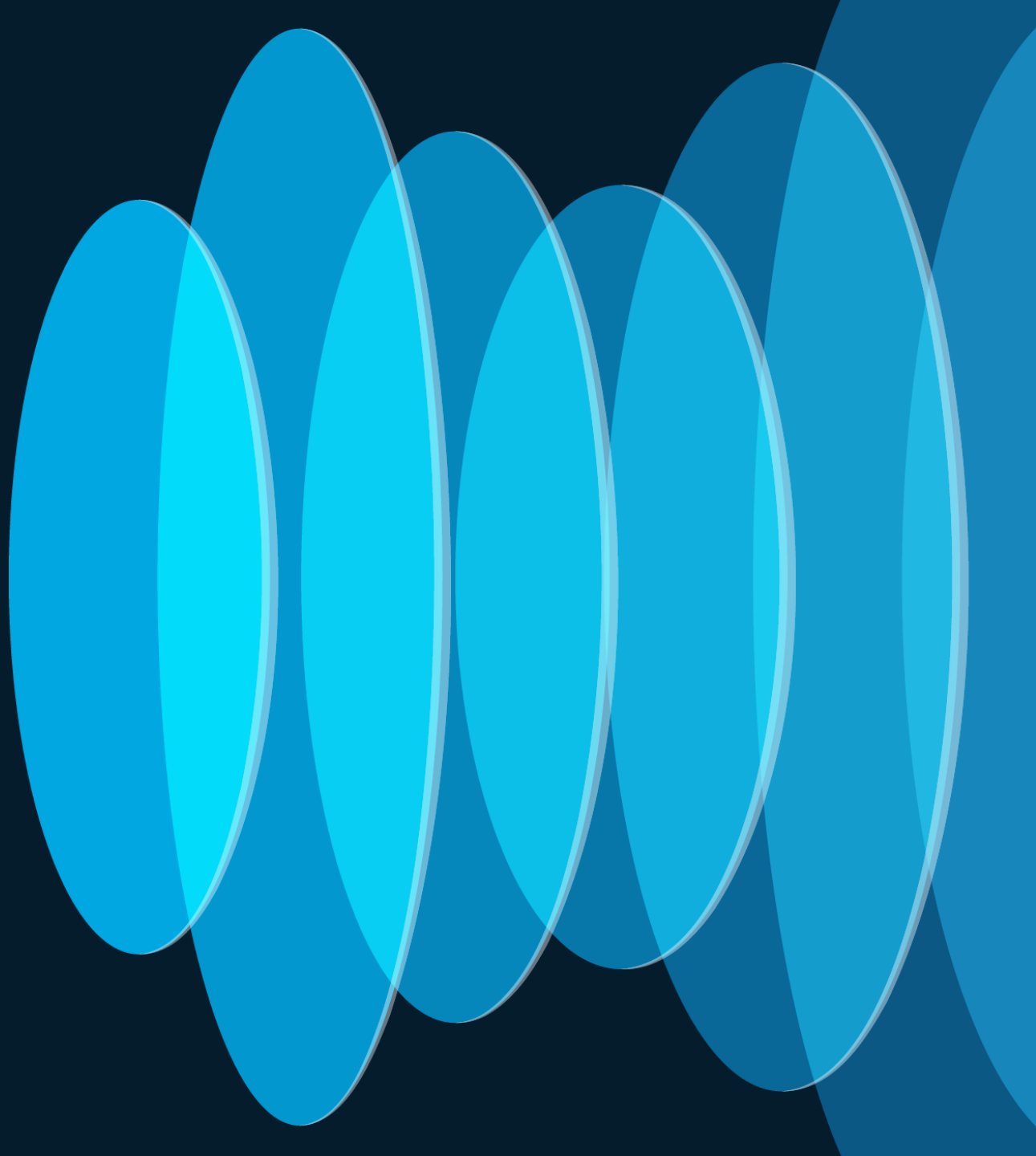
5GHz

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

6GHz

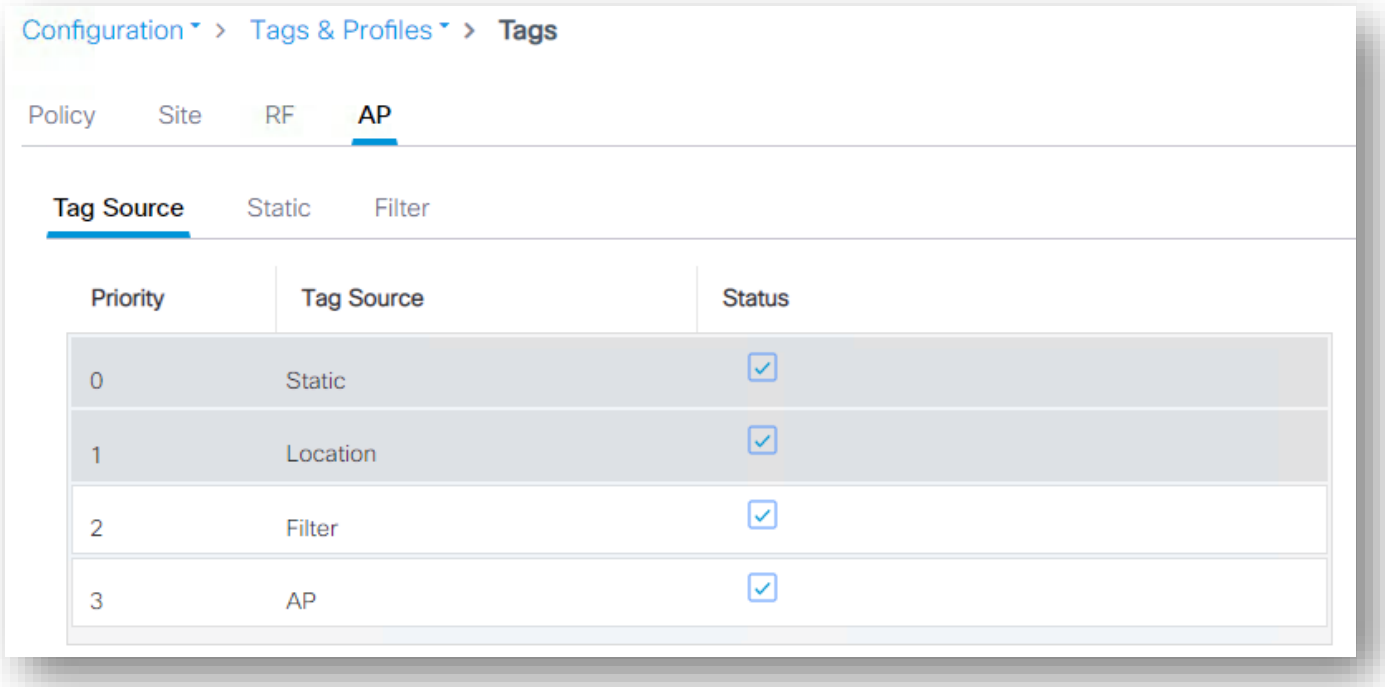
- Heavily dependent on regulatory domain
- Note! Higher channel width results in higher max Tx power for data frames (but not beacons – remember when surveying!)

APs to Tags mapping



AP to Tags assignment

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

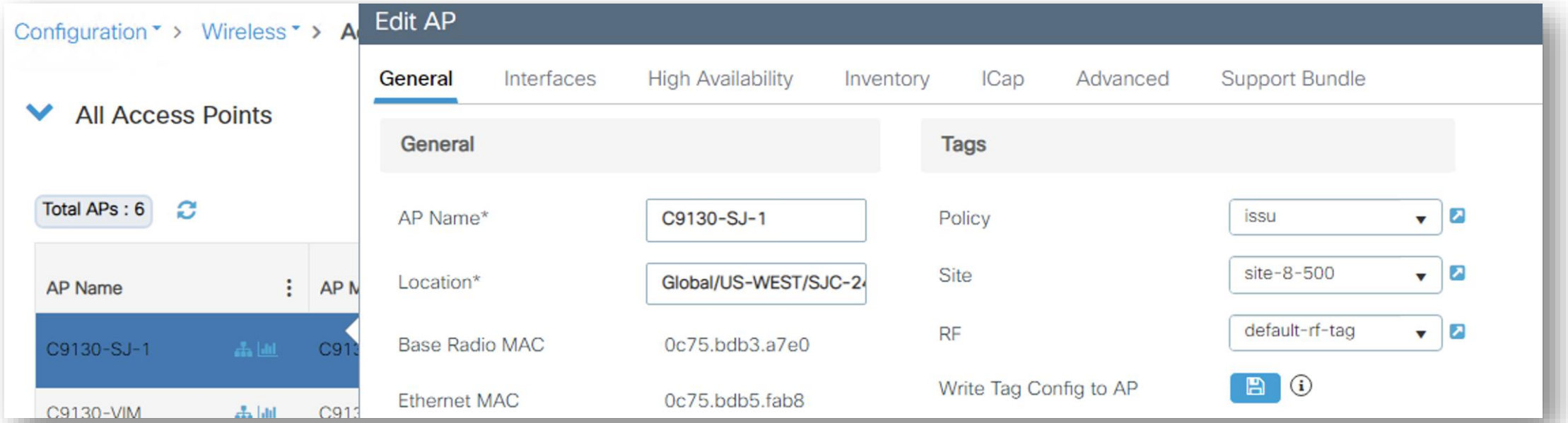


- Static: admin configuration
- Location: Basic Setup flow
- Filter: regular expression
- AP: the tags are saved on AP

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

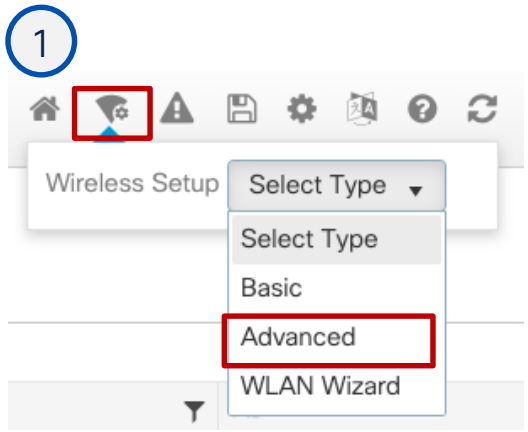
AP to Tags assignment – Source: Static

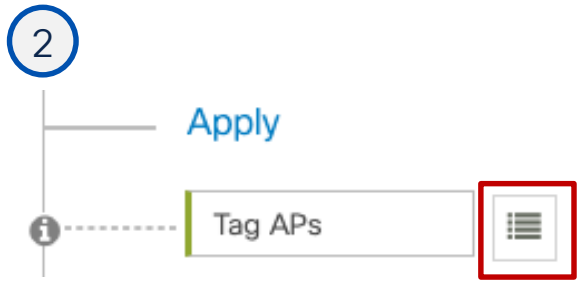
- The **static** Tag <> AP binding is based on AP's Ethernet MAC and it's a configuration on the Controller: upon joining the C9800, the configuration is applied and AP gets assigned to the selected tags
- Go to Configuration > Wireless > Access Points

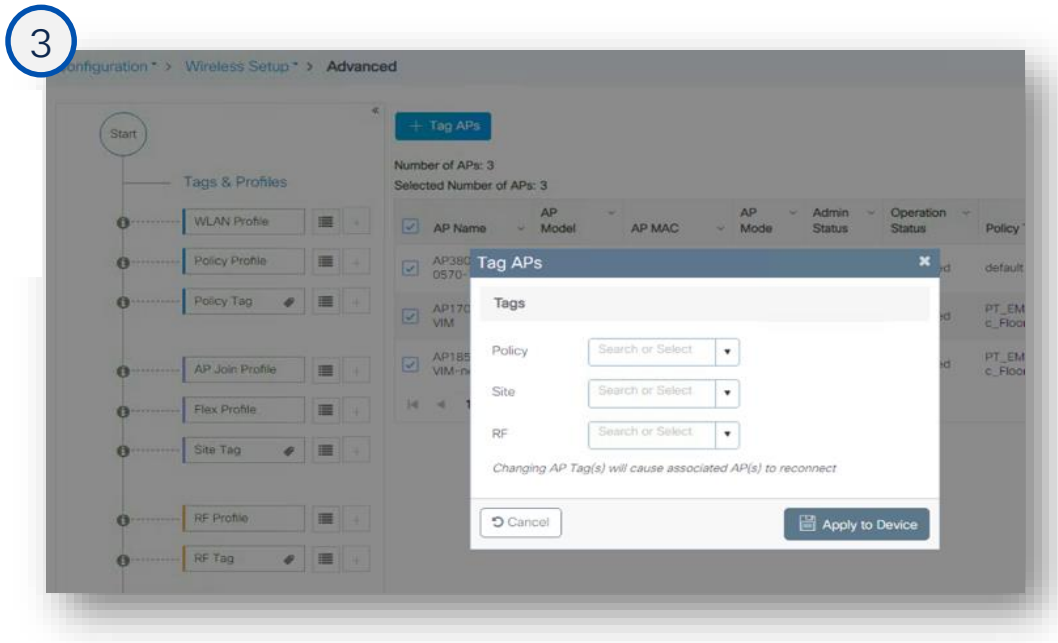


AP to Tags assignment – Source: Static

- 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:

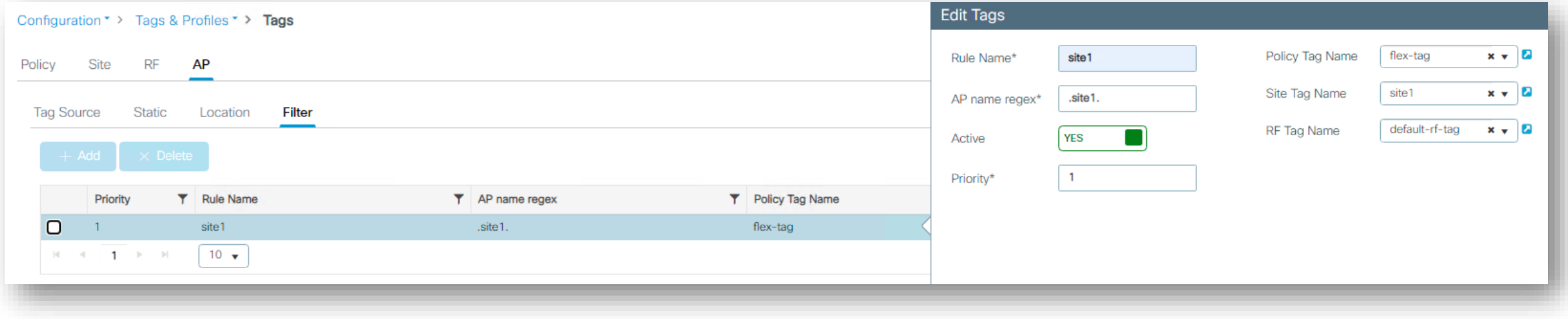






AP to Tags assignment – Source: Filter

- **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



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

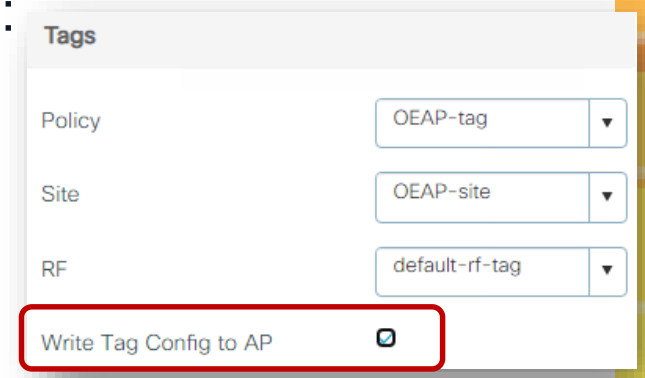
CAPWAP = Control and Provisioning of Wireless Access Points

AP to Tags assignment – Source: AP

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

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

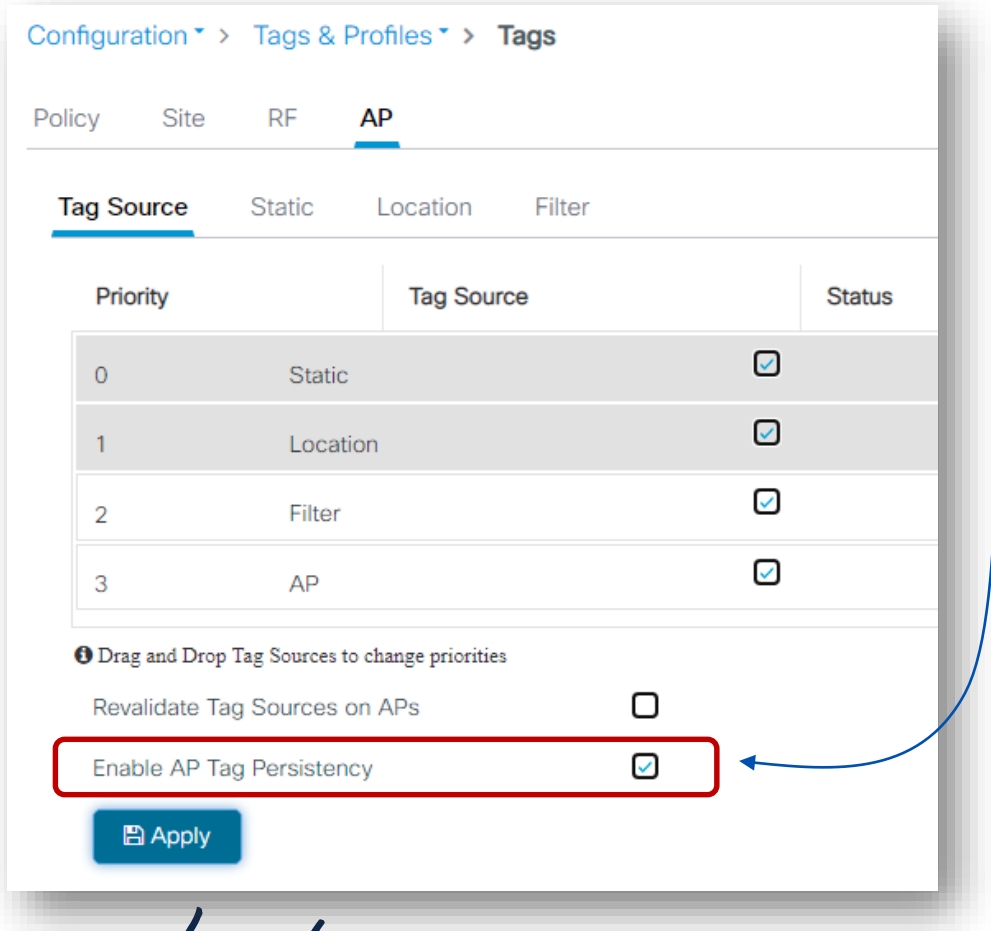
- Using the CLI command could be cumbersome, we have solutions:
  - Event Manager Script (useful for 17.3.x release)
  - Graphical user interface (GUI) settings in 17.4.1 and later
  - Starting 17.6. new feature called AP Tag Persistency



AP to Tags assignment – AP (SW >17.6)

Configuring AP Tag Persistency

Configuration > Tags & Profiles > Tags:



- From 17.6.1 this is supported in CLI in global configuration mode:

```
C9800(config)#ap tag persistency enable
```

- 17.6.2 and 17.7 adds support from GUI

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

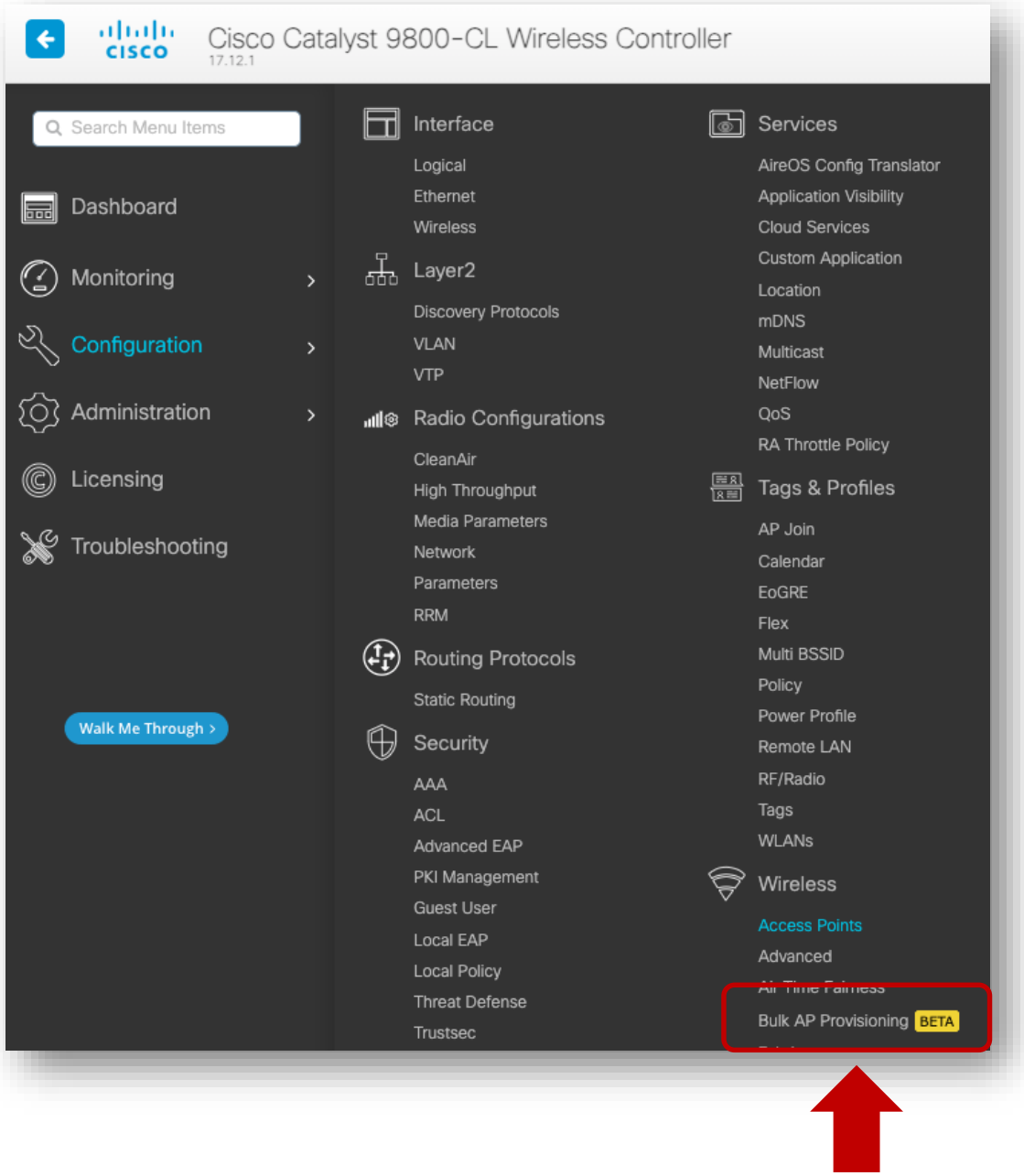
Verifying AP Tag source

Run the show command below:

```
C9800#show ap tag summary

Number of APs: 1

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

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

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

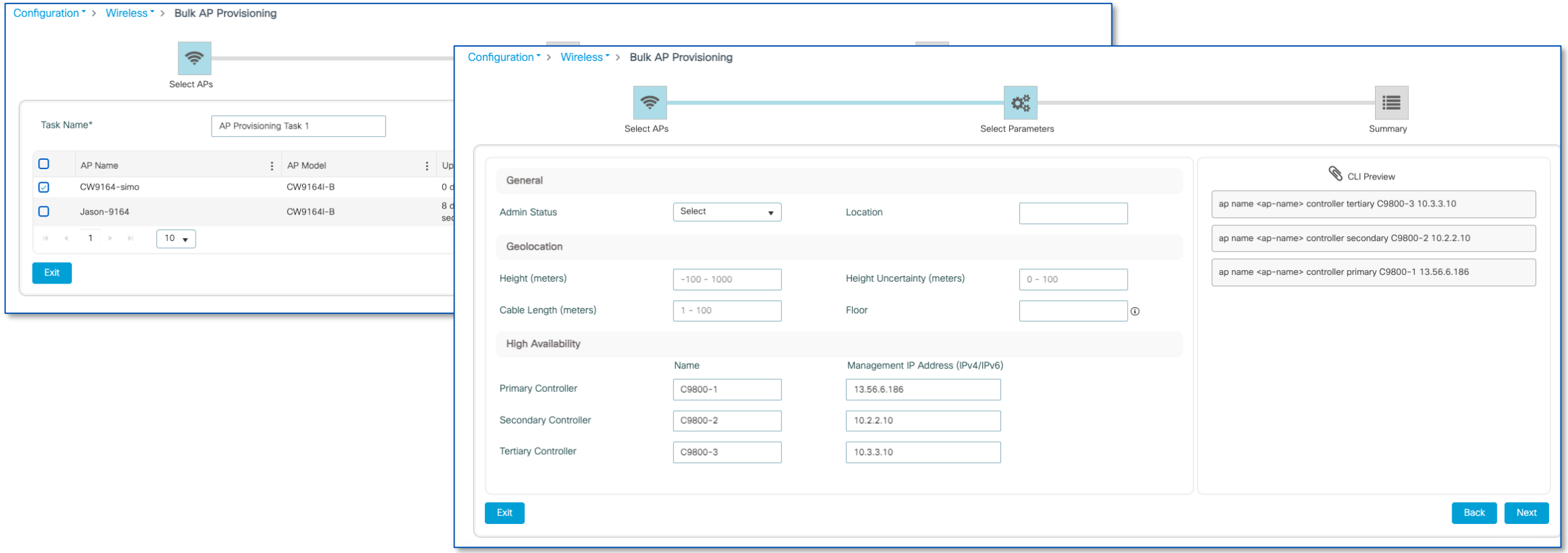
AP Bulk Provisioning



AP Bulk Provisioning

Why would you care?

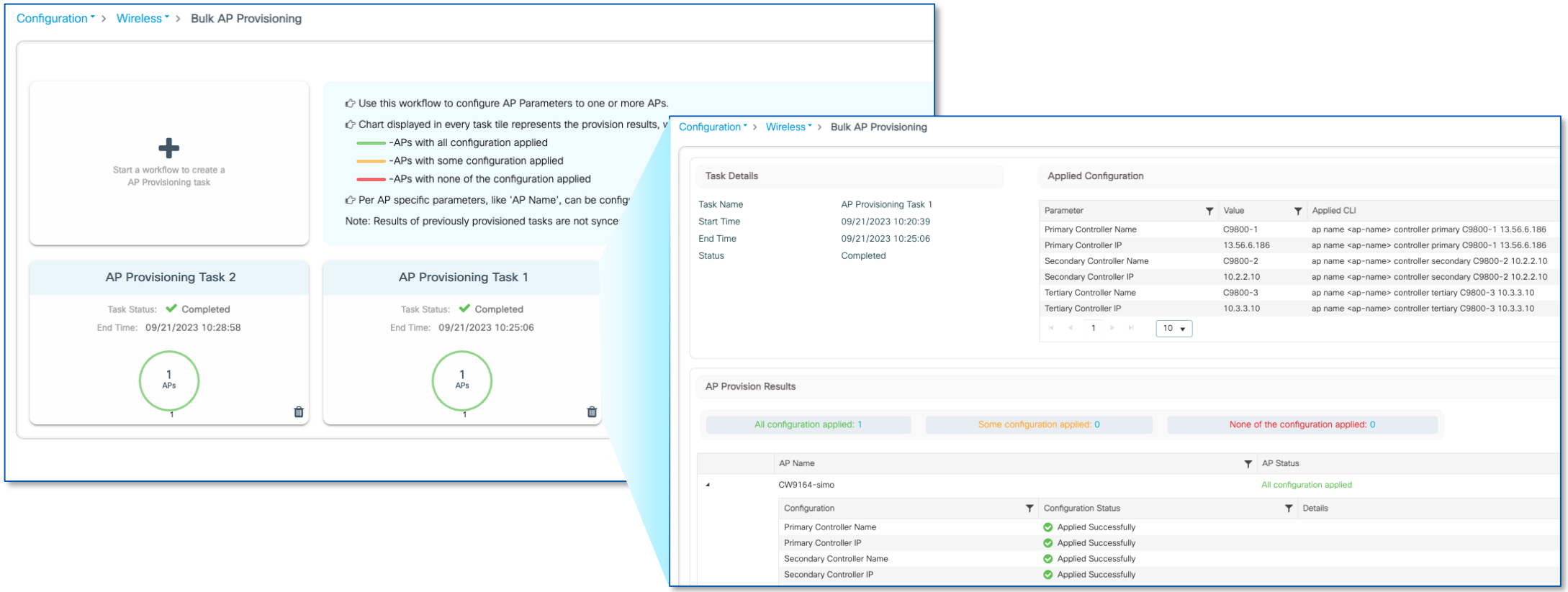
- Change few AP settings…in bulk!
- One of the most requested is changing the Primary (Secondary/Tertiary), to move APs between WLCs



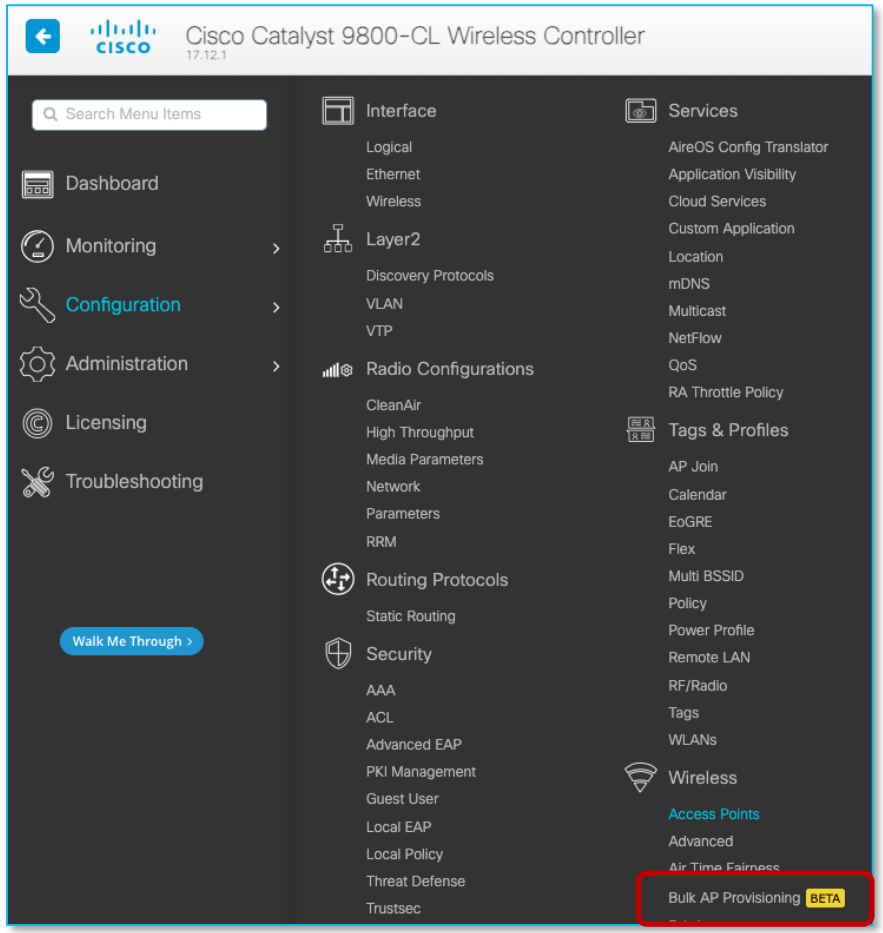
AP Bulk Provisioning

Why would you care?

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

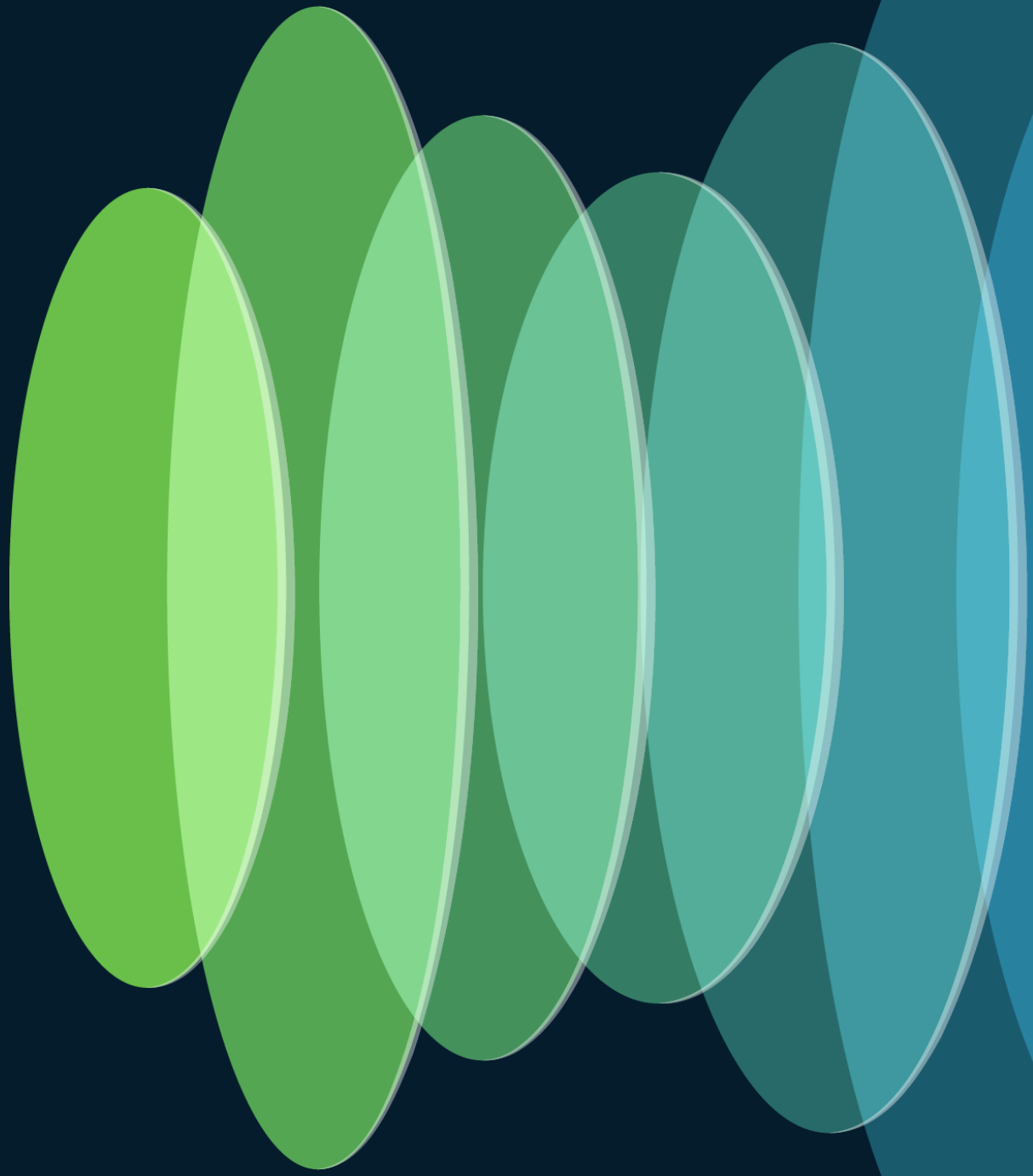


AP Bulk Provisioning – what's next?



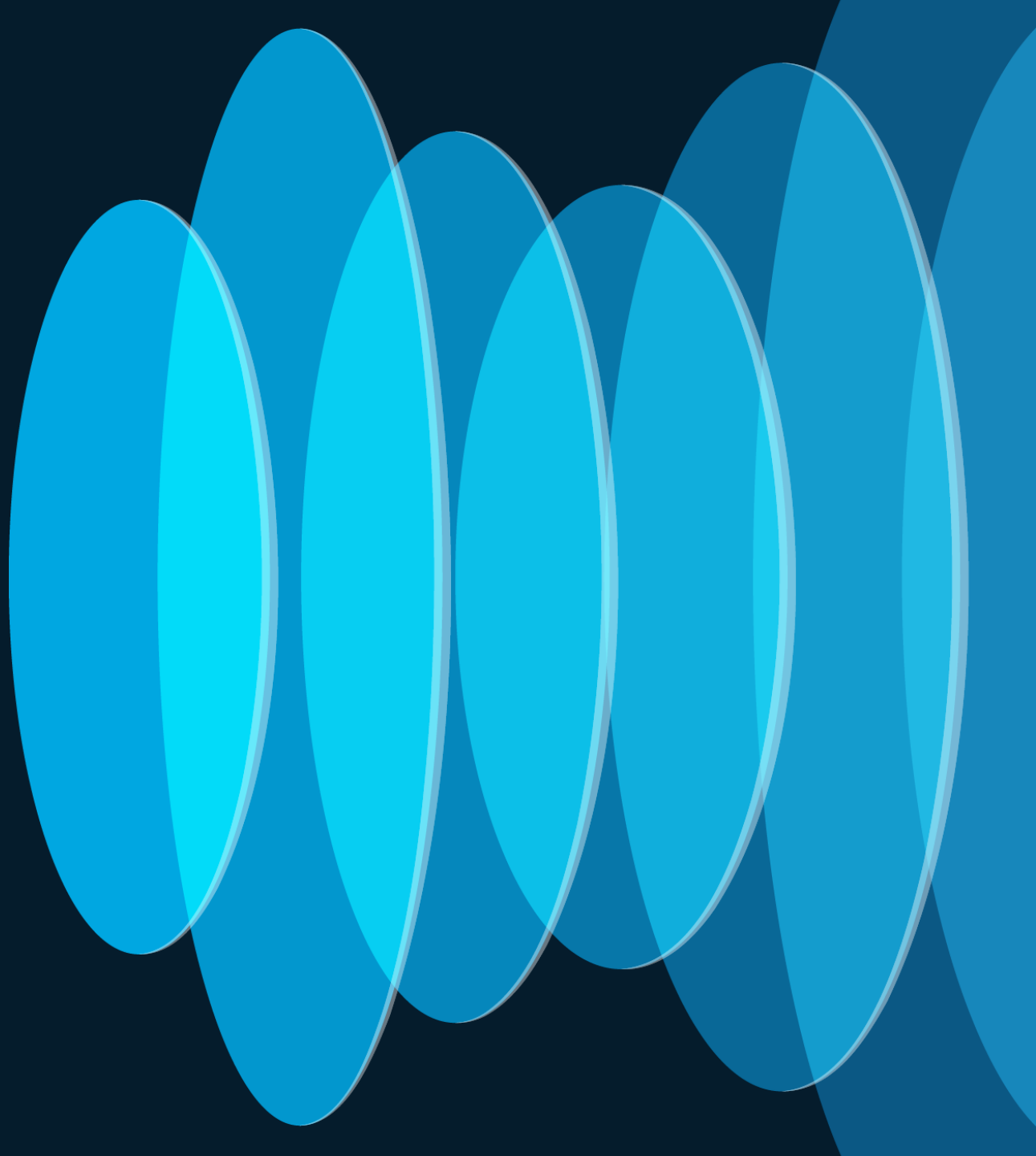
- BETA tag removed in 17.12.2 and 17.13
- Additional filters to select APs (e.g., AP tags) coming in 17.13
- Any other ideas? LET US KNOW!

Day 2



cisco Live!

AI-Enhanced RRM

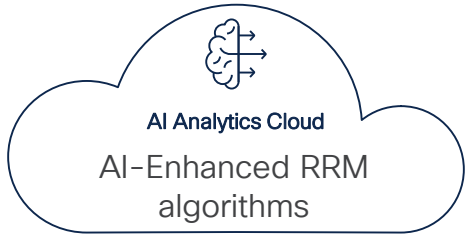


AI-Enhanced RRM key customer benefits

Better RF, better insights, reduced operational costs and time

AI-driven self-optimizing RF

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



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

Performance visibility

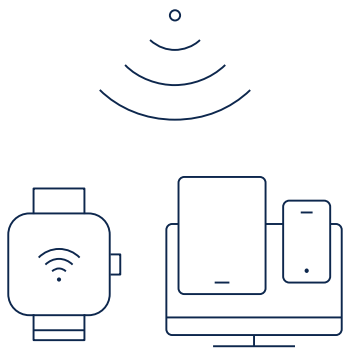
Provides per-building visibility into RF health using Wireless Config Analyzer algorithm.

Actionable insights

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

Complete historical context

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



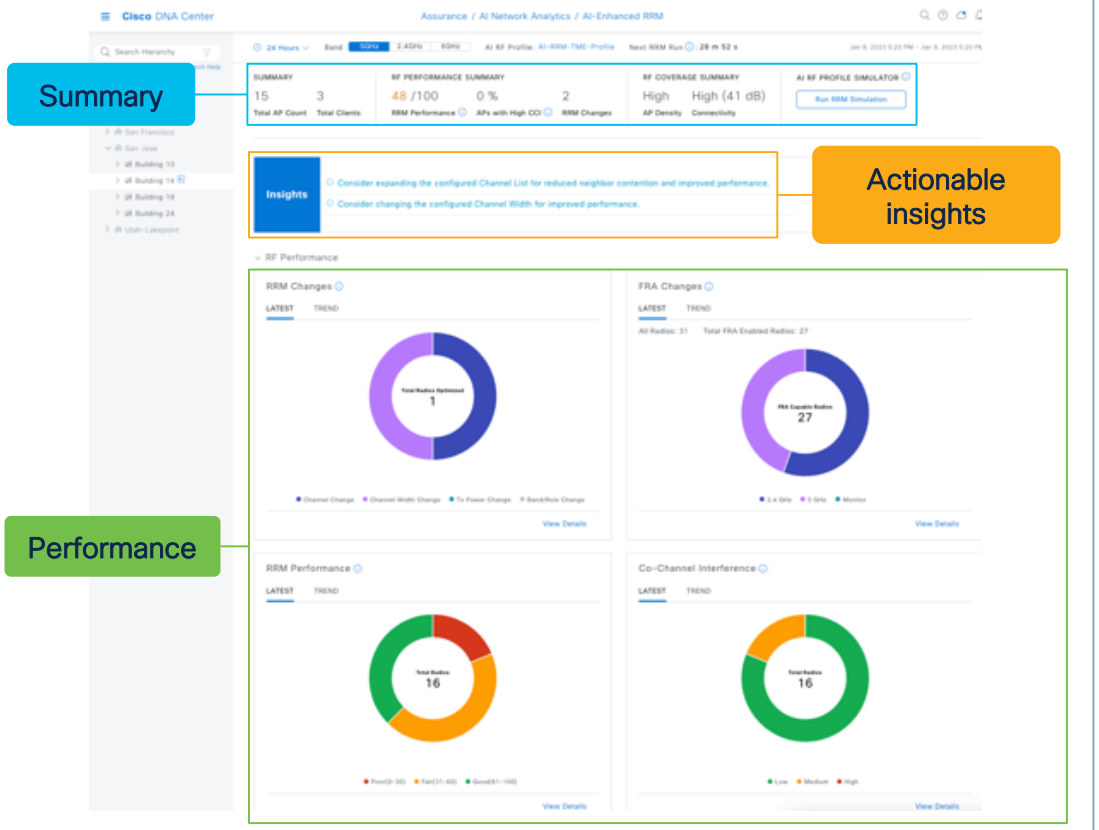
Simplified RRM configuration

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

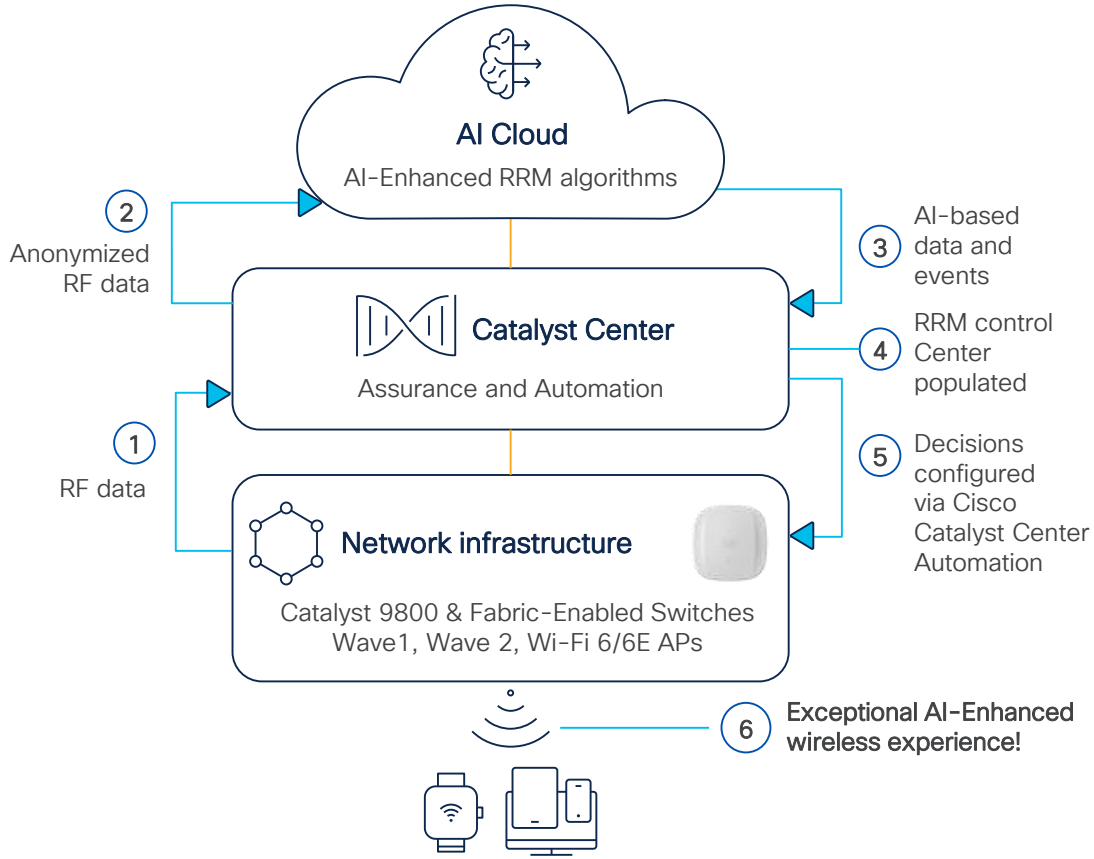
AI-Enhanced RRM is AI that Powers RF Optimization

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

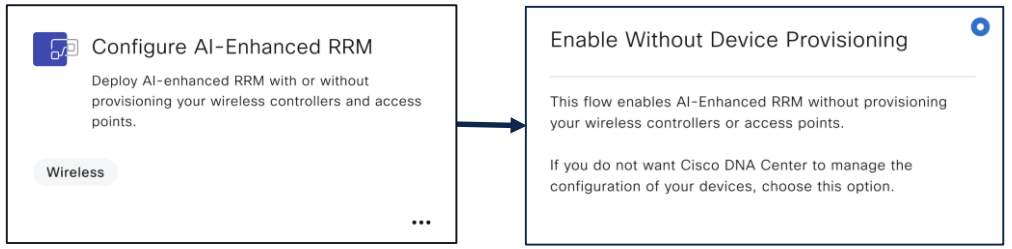
Instantaneous visibility



Proactive optimizations

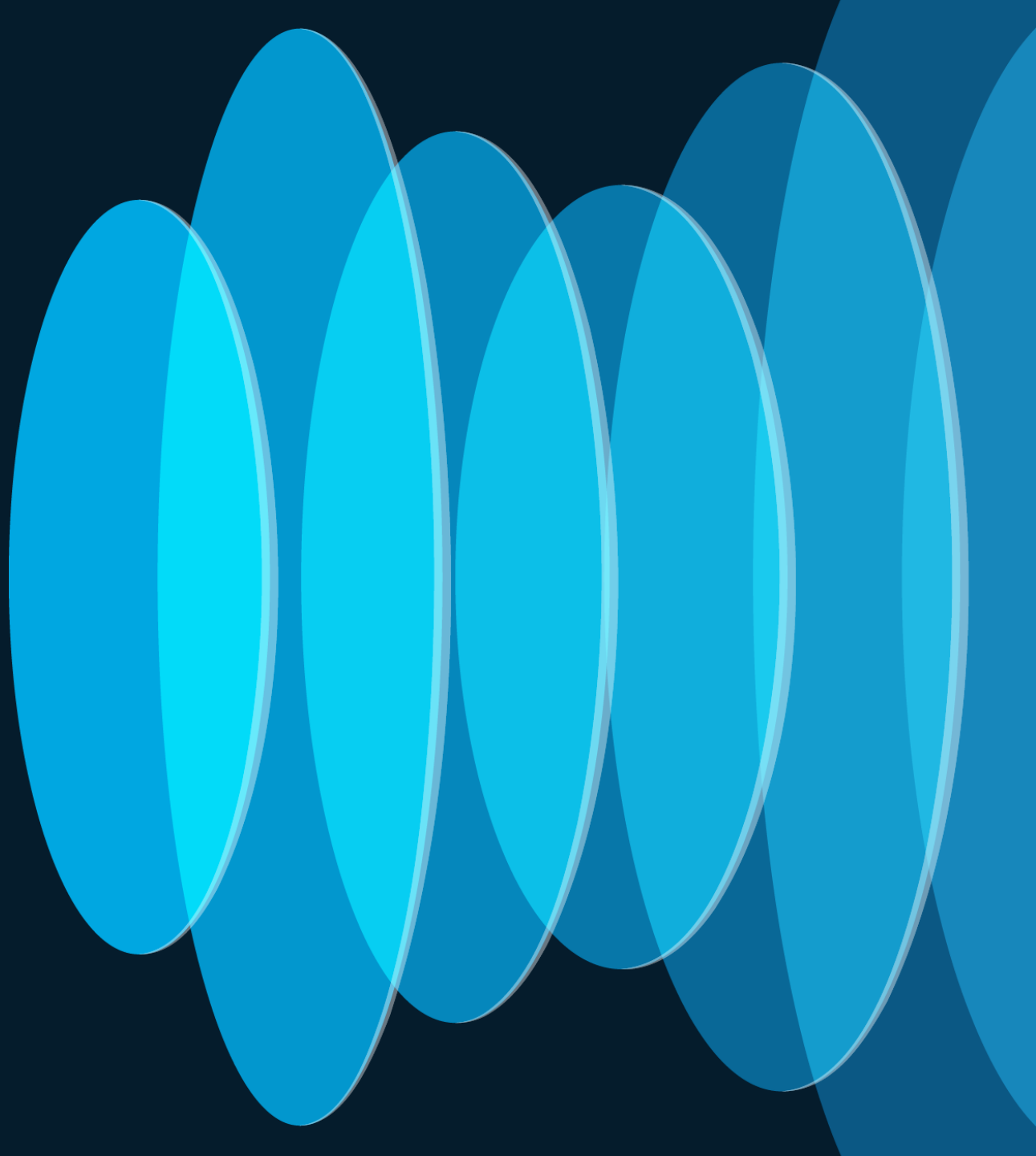


What mitigates these pain points?



New AI-Enhanced RRM Workflow for Assurance Only Customers!

AP Power Optimization

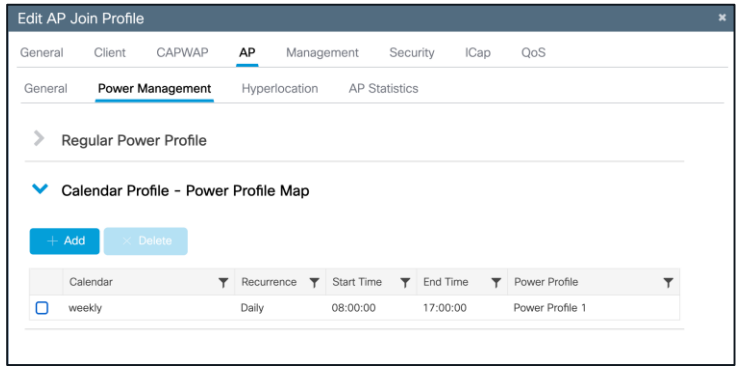


AP Power Optimizations Feature Suite

Save Power, Reallocate Power, and Visibility into Savings

AP Power Save Mode
Lower AP Power Usage

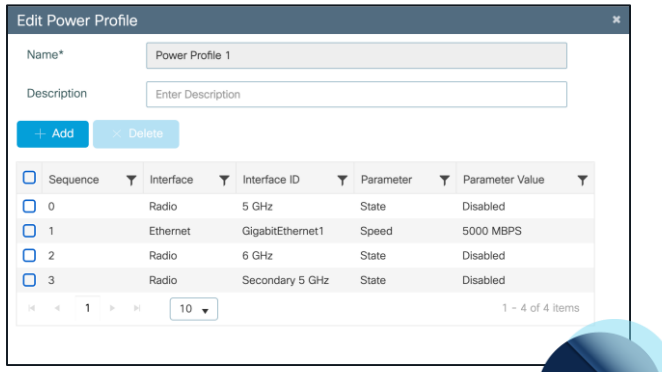
- Create a calendar profile for off-peak hours.
- Create a power profile to lower the power consumption budget during off-peak hours.
- Power Profile: Shut AP Radio or lower spatial Stream, lower port speed, disable USB port.



IOS-XE 17.8

AP Power Distribution
Control over how power is

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



IOS-XE 17.10

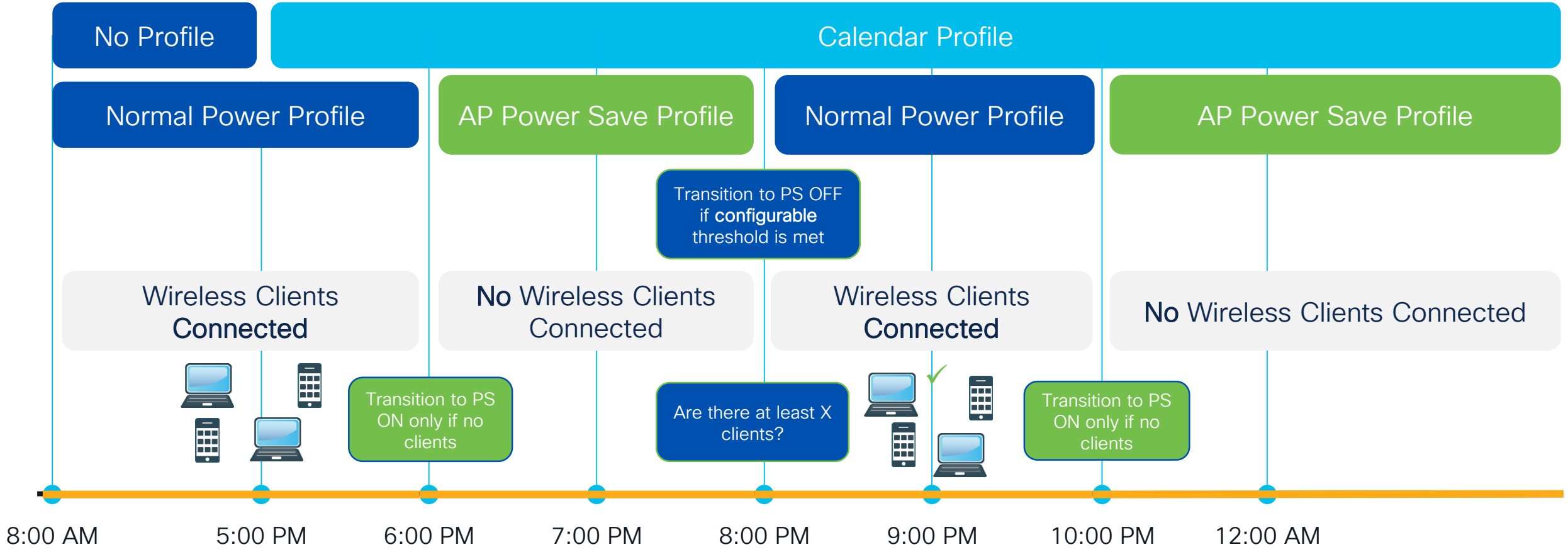
NEW

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

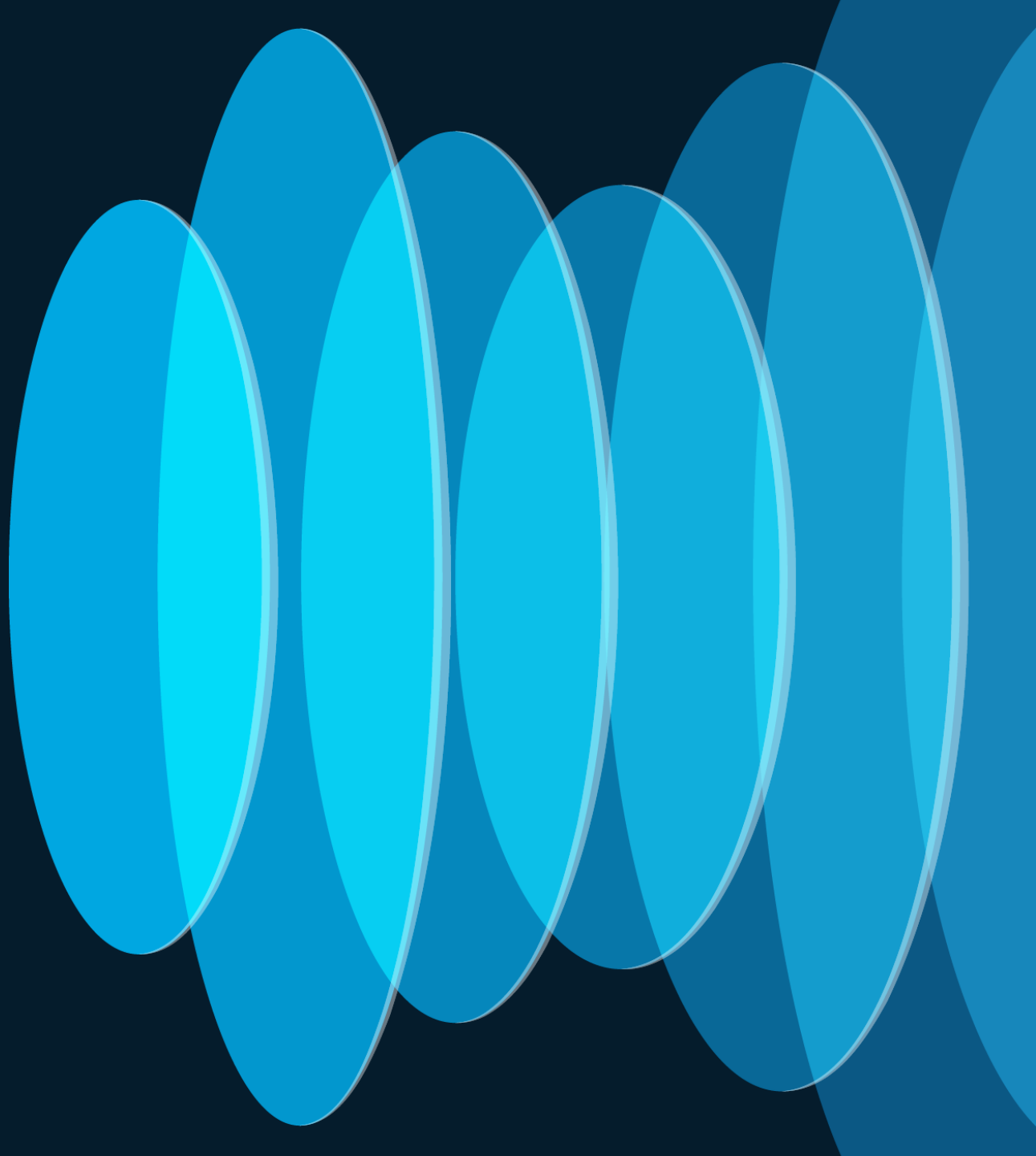
- Cisco Catalyst Center PoE dashboard integration.
- Power Savings, Money Savings, Emissions Reductions.
- Visibility into trends and insights.
- Both site level and AP level view.

Catalyst AP Power Save (PS): Client logic change

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



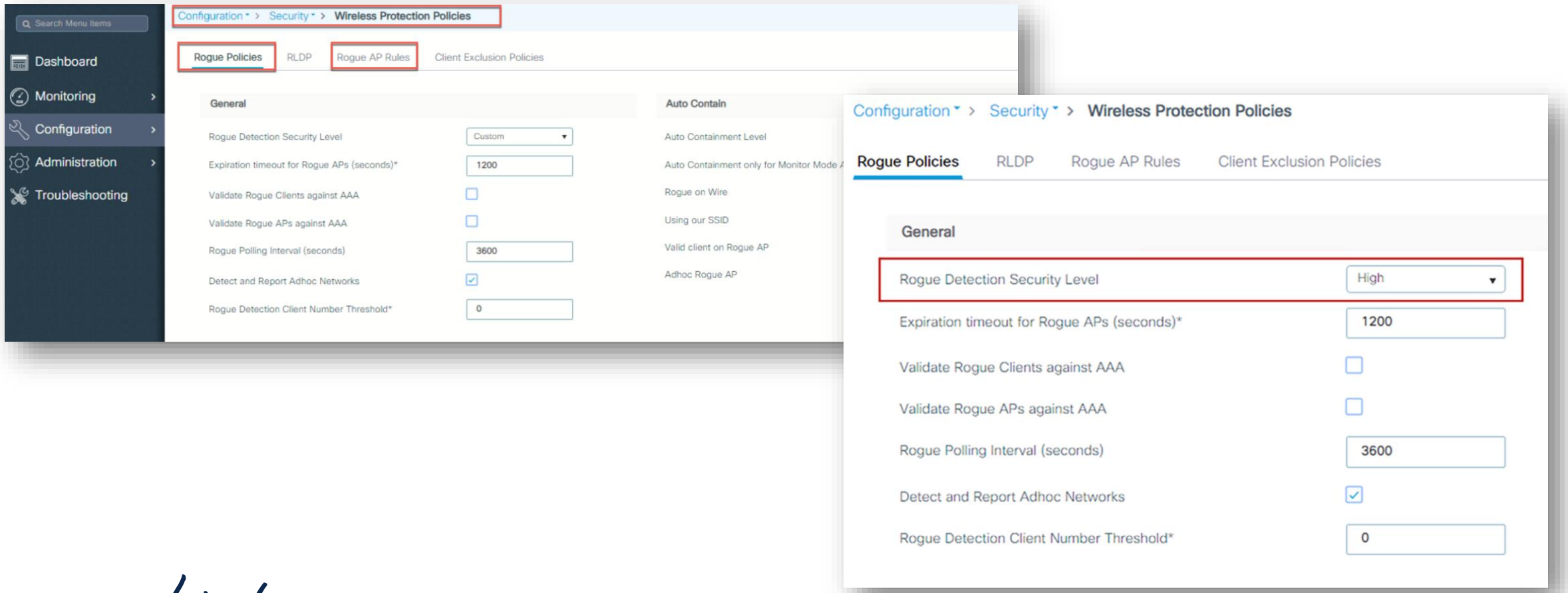
Rogues



Rogue rules on C9800

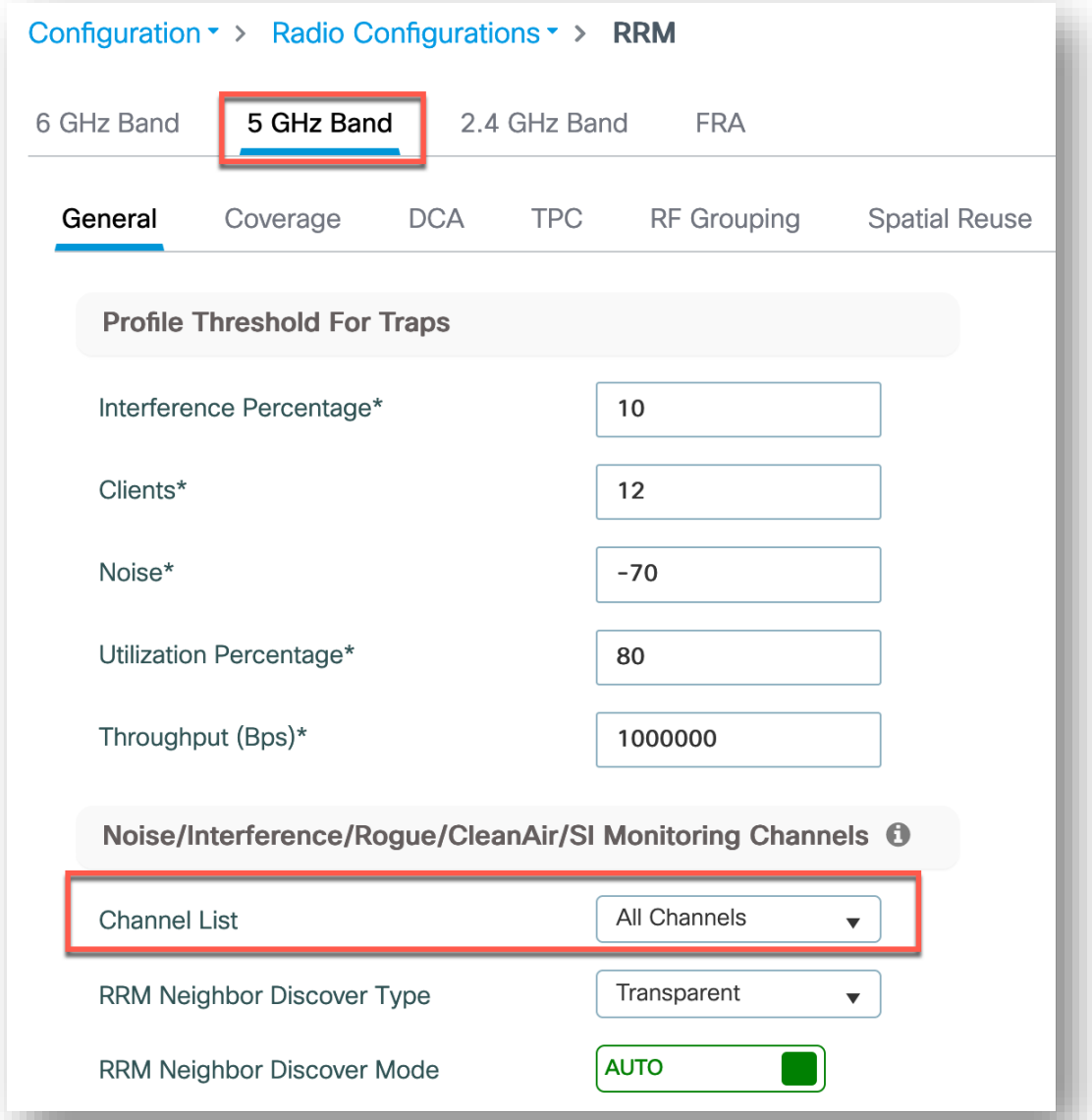
Rogue rules can be configured on C9800 to classify and contain rogues and set thresholds.

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



Rogue Monitoring Channels

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



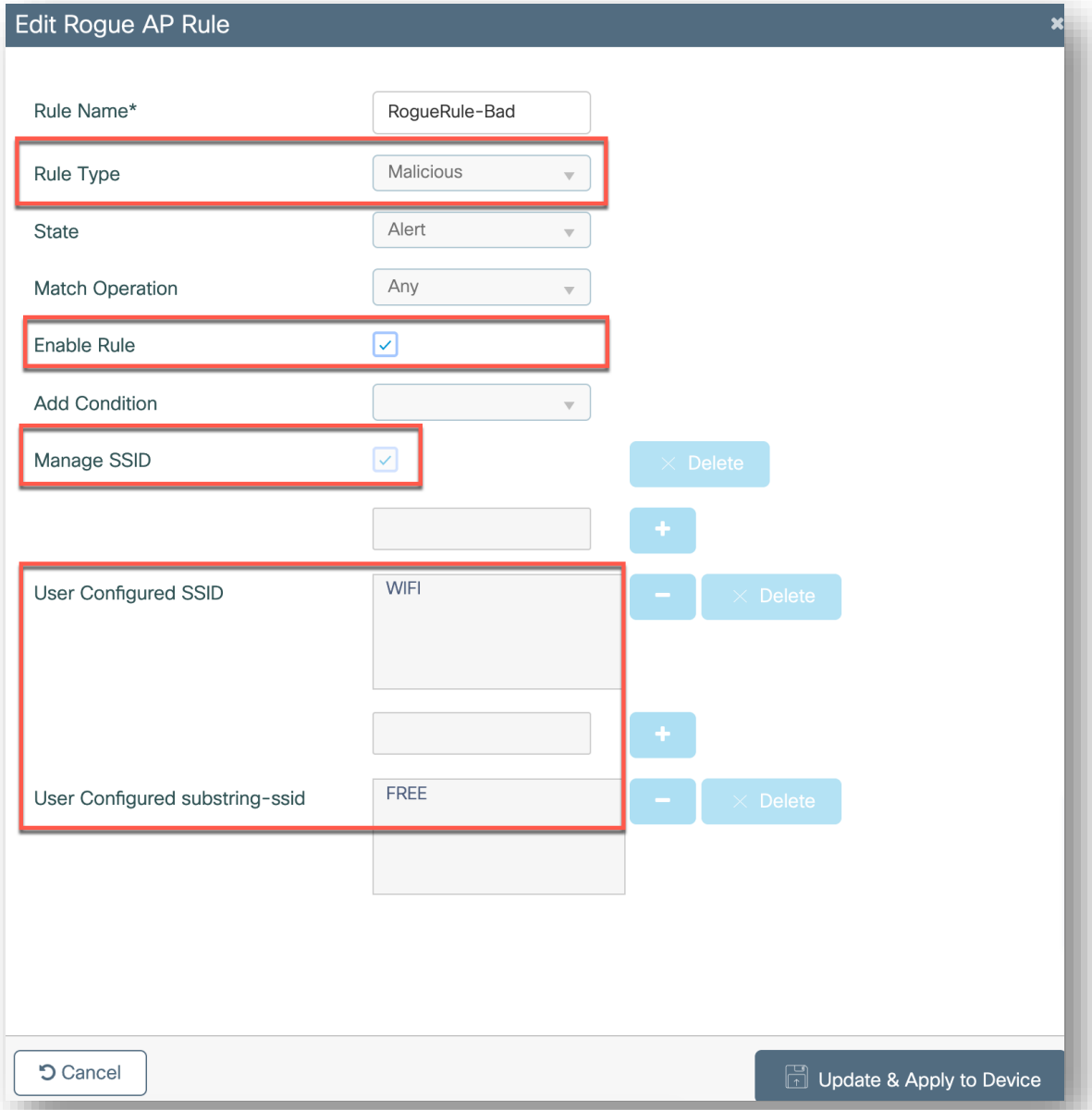
Rogue AP rules

Recommended malicious rogue AP rules

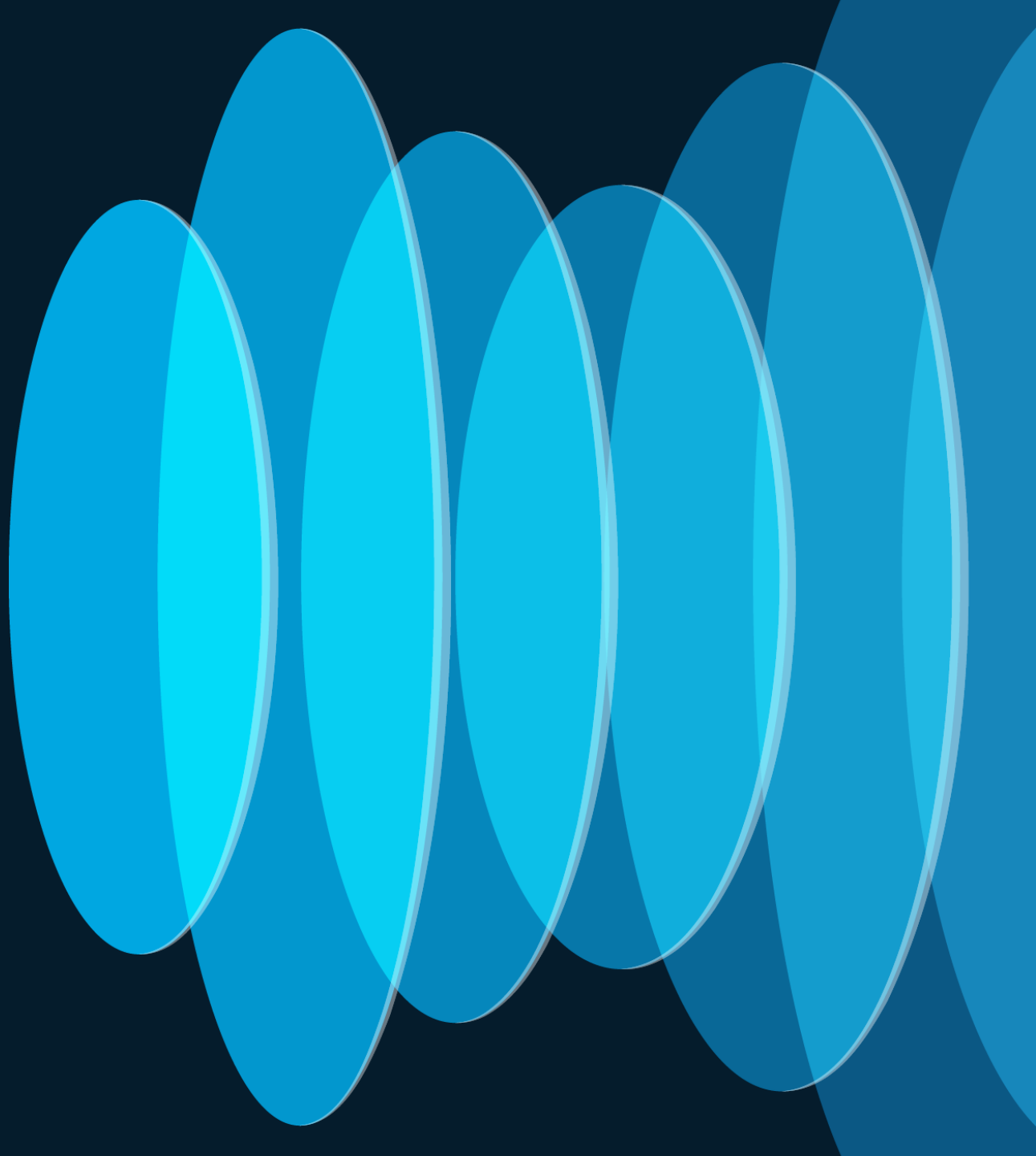
Managed SSIDs: Any rogue APs using managed SSIDs, like your wireless infrastructure, must be marked as malicious.

Minimum RSSI >-70 dBm: For Enterprise deployments

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



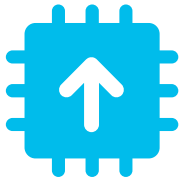
CleanAir Pro™



cisco Live!

Introducing Cisco CleanAir Pro™

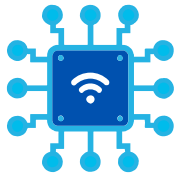
15 years of innovations and excellence carried forward



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™

The Evolution of Cisco Wi-Fi Excellence into 6 GHz

Is Cisco CleanAir **Pro** still CleanAir ?

1. Detect and Classify Non – Wi-Fi interference
   - To Wi-Fi, if it's not Wi-Fi – then its noise
2. Set Severity Metric per Interferer
   - Important to identify which source is causing the most harm
3. Establish Air Quality for all interfaces on the AP
   - Track how much the combined impact is affecting Wi-Fi service in the cell
4. Merge same Type interferers
   - Correlation of duplicate alarms from other neighboring APs of same event

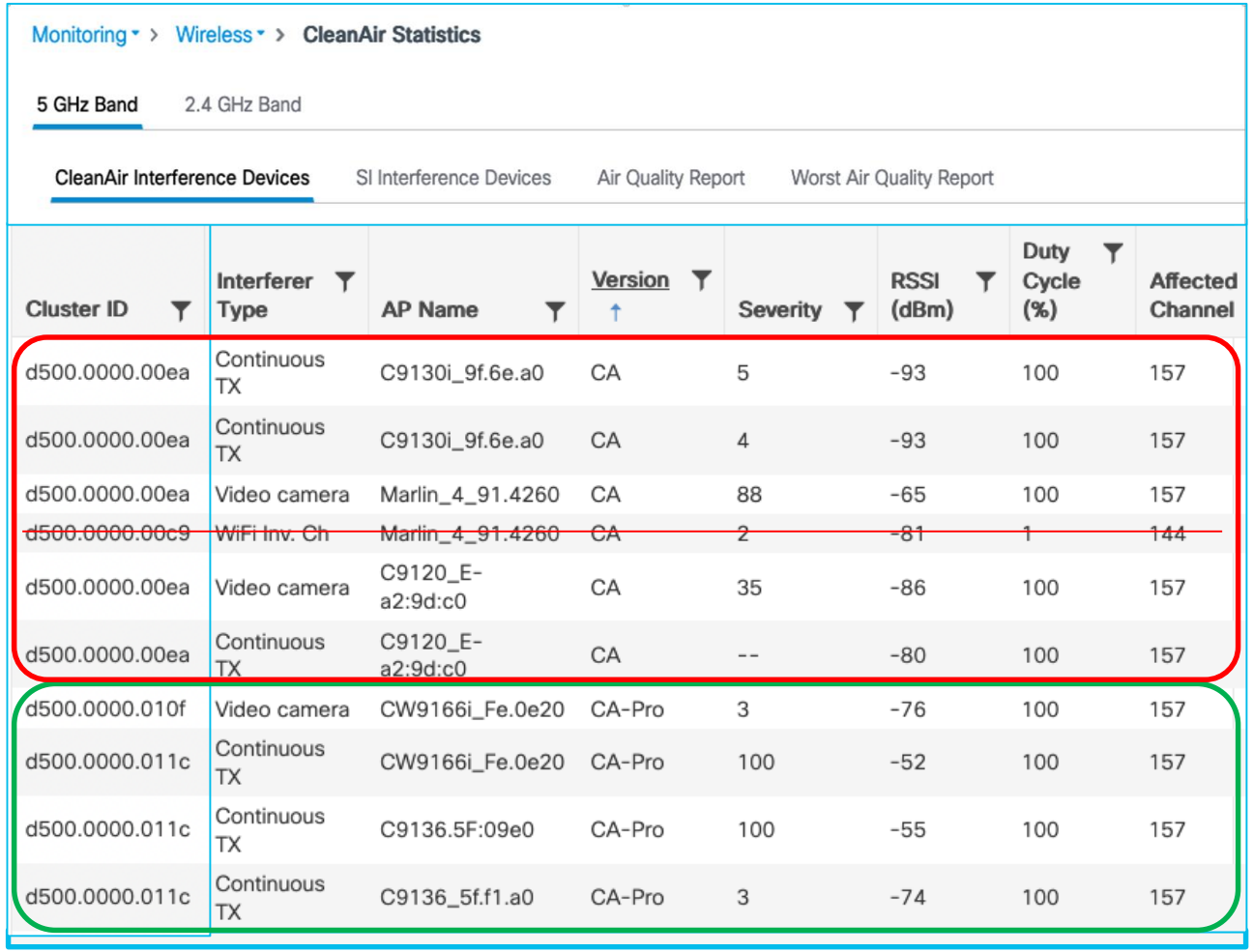
CleanAir	CleanAir Pro
✓	✓
✓	✓
✓	✓
✓	✓

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



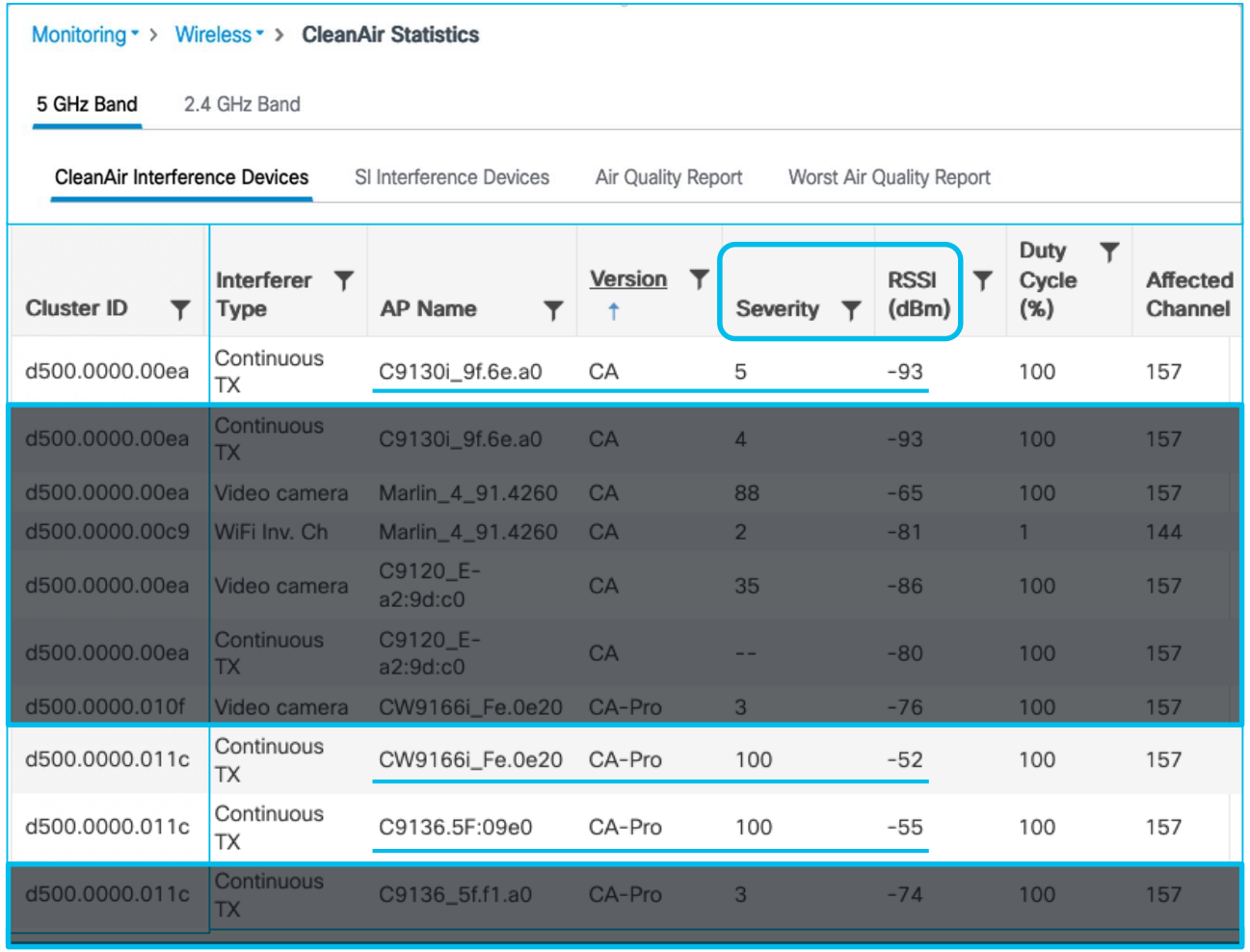
Cluster ID	Interferer Type	AP Name	Version	Severity	RSSI (dBm)	Duty Cycle (%)	Affected Channel
d500.0000.00ea	Continuous TX	C9130i_9f.6e.a0	CA	5	-93	100	157
d500.0000.00ea	Continuous TX	C9130i_9f.6e.a0	CA	4	-93	100	157
d500.0000.00ea	Video camera	Marlin_4_91.4260	CA	88	-65	100	157
d500.0000.00c9	WiFi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

Cisco CleanAir Pro™
Detect/Classify

CleanAir Pro =CA-Pro

5 GHz Video Camera is on Channel 157

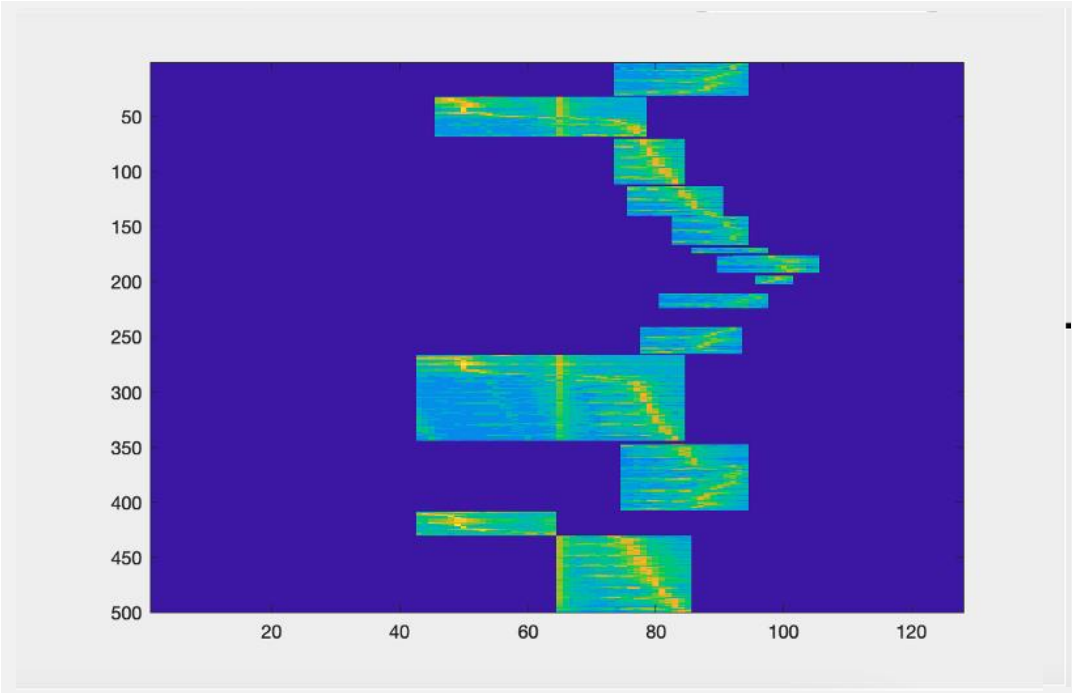
- C9130i_9f.6e.a0 see's 100% DC at -93 dBm and a minor severity of 5 (meh..)
- C9136 and CW9166 see it at - 52 to - 55 dBm with a high severity of 100 (very bad)



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

CleanAir Pro™ Pulse Isolation and Metrics
Cisco Innovation!

- CleanAir **Pro isolates interesting signals from the noise and the Wi-Fi**
- CleanAir Pro the extracts Data from the Isolated Pulses like
  - Pulse Duration
  - Pulse Repetition Interval
  - Pules Width
  - Signal gap statistics
  - Variations in width
  - “Density” statistics
  - Per pulse power statistics



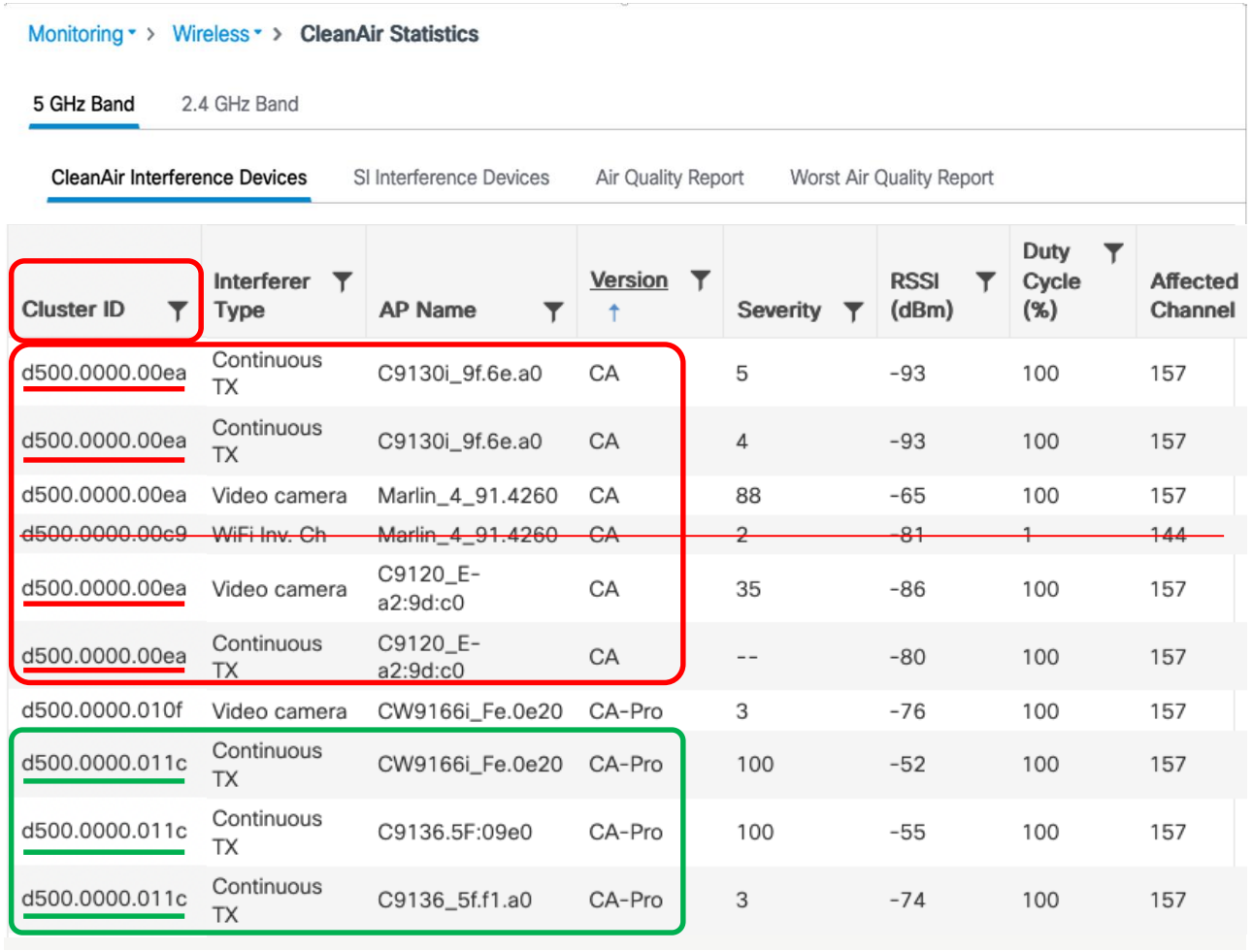
Microwave Oven

CleanAir Pro™ Tracking on AP and WLC

- Up to 64 total interferers Per/AP
- Various conditions add/merge/drop interferers from tracking list
- Merging
  - When an interferer is detected
    - Match with other detections based on Center Frequency and other spectrum measurement points.
    - A narrow CW signal (1 MHz) has a very narrow tolerance
    - A wideband Jammer has very wide tolerance
  - C9800 can merge across connected APs based on same conditions

CleanAir Pro™ – Merging

- Reducing duplicate entries is the Merging Algorithms job
- The Cluster ID, Identifies individual reports from AP's that CleanAir thinks is from the same source
- CA cluster d500.000.00ea across 4 APs
- CA-Pro d500.000.011c across 3 APs detecting



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

CleanAir Pro™ – Merging

- Custer details can be reviewed on the controller CLI, the type of interference, the Custer center (closest AP) and cluster start and last update as well as how many other members are all correct

```
C9800-L_17_9#sh ap dot11 5ghz cleanair device cluster d500.0000.00ea

Cluster-Id                    : d500.0000.00ea
Class-Type                    : Video camera
Cluster-Center-Index          : 2
Cluster-Center-Severity       : 84
Cluster-Center-RSSI           : -66
Affected-Channel-Bitmap       : 4194304
Cluster-Center-Detecting-AP   : 687d.b491.4260
Is-Center-Virtual             : No
Cluster-Init-Time             : 05/06/2022 16:41:23 Eastern
Last-Update-Time              : 05/06/2022 17:15:44 Eastern

Cluster Members :
----------------
409f.6ea1.c003
bda2.9dc1.8098
b491.4261.4105
bda2.9dc1.709f
409f.6ea1.c007
```

```
C9800-L_17_9#sh ap dot11 5ghz cleanair device cluster d500.0000.011c

Cluster-Id                    : d500.0000.011c
Class-Type                    : Continuous TX
Cluster-Center-Index          : 0
Cluster-Center-Severity       : 100
Cluster-Center-RSSI           : -59
Affected-Channel-Bitmap       : 4194304
Cluster-Center-Detecting-AP   : 687d.b45f.09e0
Is-Center-Virtual             : No
Cluster-Init-Time             : 05/06/2022 17:08:32 Eastern
Last-Update-Time              : 05/06/2022 17:14:34 Eastern

Cluster Members :
----------------
b45f.09e1.10a2
20fe.0e21.50ab
b45f.09e1.10ae
```

CleanAir Pro™ In Action

Device Detection Time

- Depends on the Interference device/type 30-90s
- Best observed at the AP command line
  - Narrow Band Interference can be verified quickly with second pass
  - wideband Interference takes more cycles, and channels to quantify
- Dropping an inactive interference source 30-90s

Camera ON 32 seconds

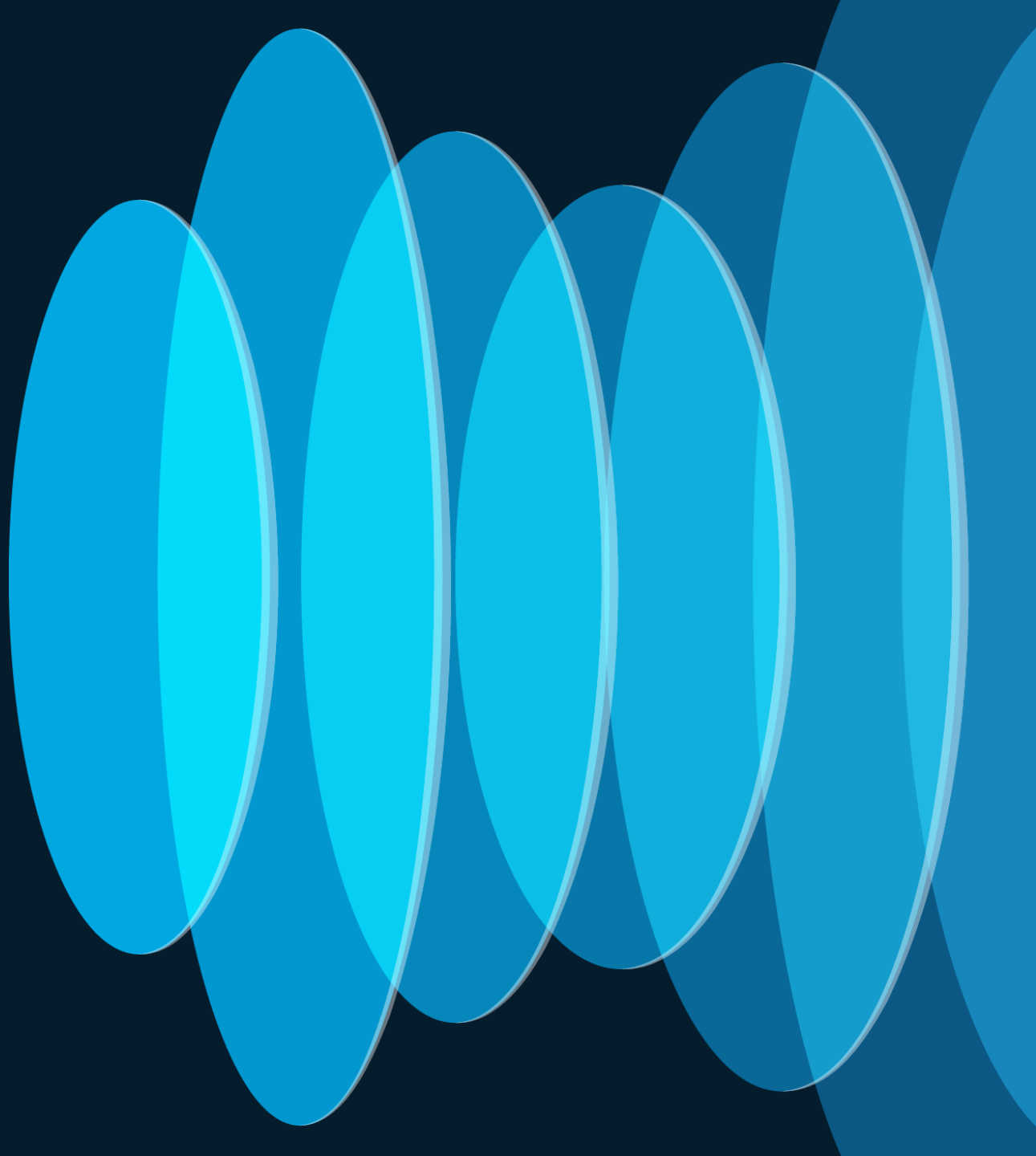
C9136.5F:09e0#sh cleanair interferers
CleanAir: band 2.4GHz number of devices 0:
CleanAir: band 5GHz number of devices 1:
IDR: 2455(4732) Video Camera
ISI=100, -56 dBm, duty=100
c(1)=00400000 sig(4)=00b09e12
on/report/seen 1/1/1 secs ago

Camera OFF –42 seconds

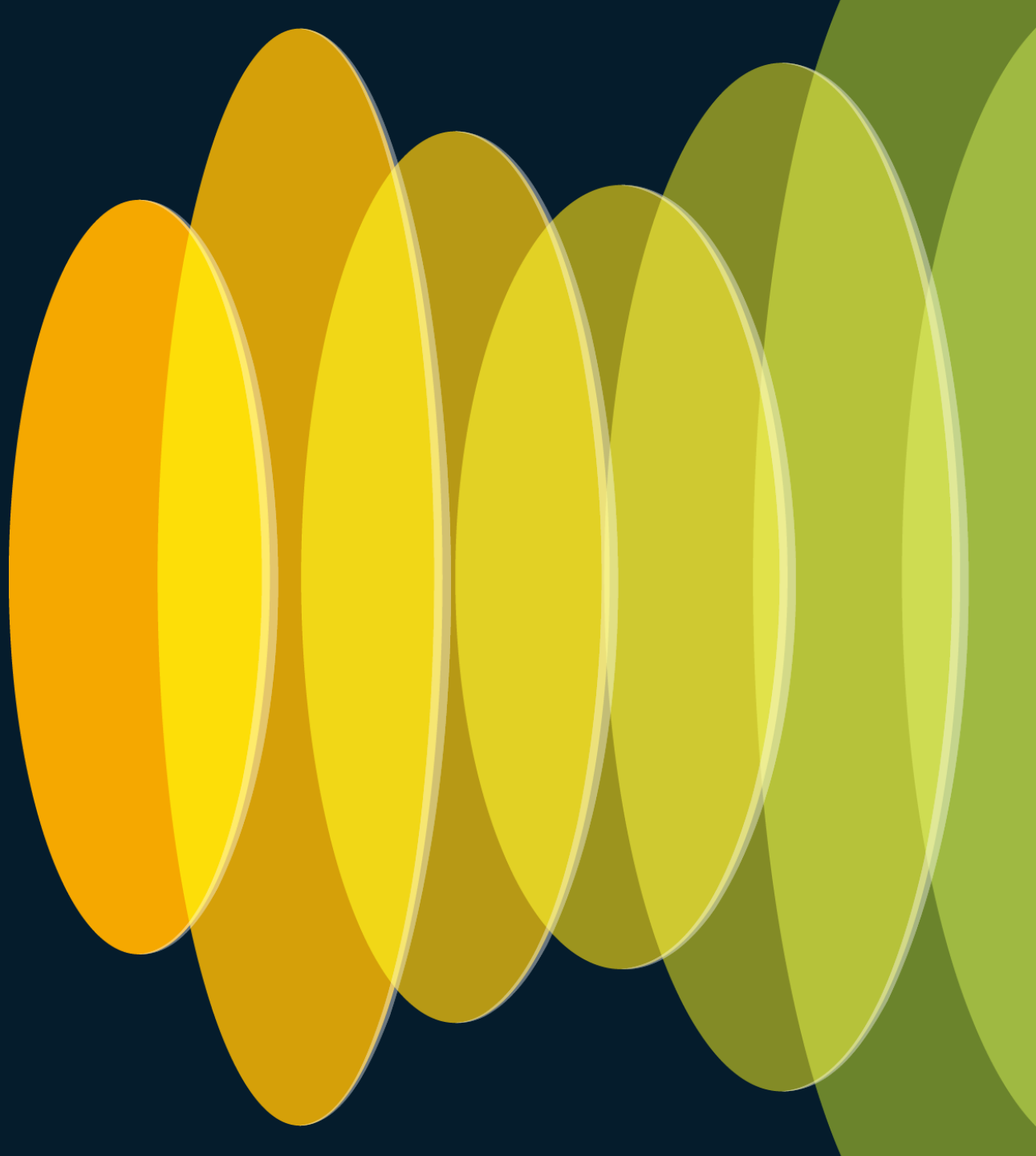
C9136.5F:09e0#sh cleanair interferers
CleanAir: band 2.4GHz number of devices 0:
CleanAir: band 5GHz number of devices 1:

IDR: 2455(4732) Video Camera
ISI=100, -56 dBm, duty=100
c(1)=00400000 sig(4)=00b09e11
on/report/seen 89/34/41 secs ago

Software Updates

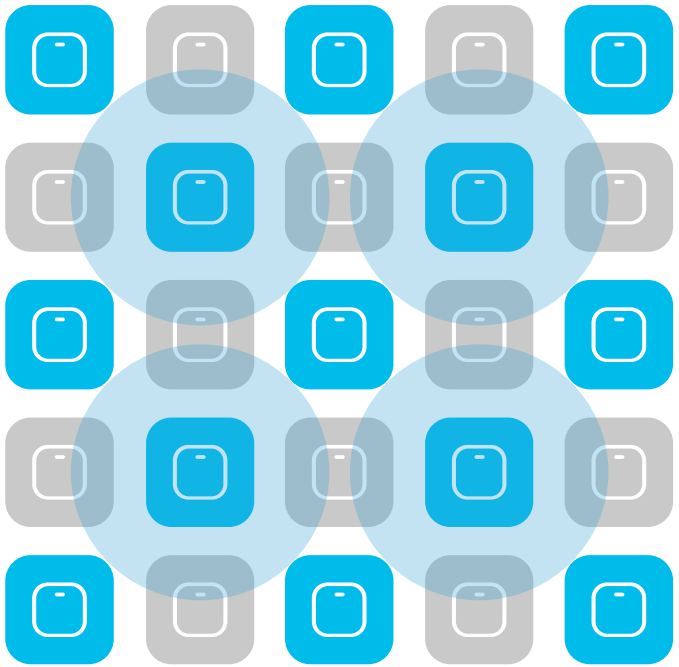


Rolling AP Update/Upgrade Infrastructure



cisco Live!

Rolling AP Upgrade: Neighbor AP marking

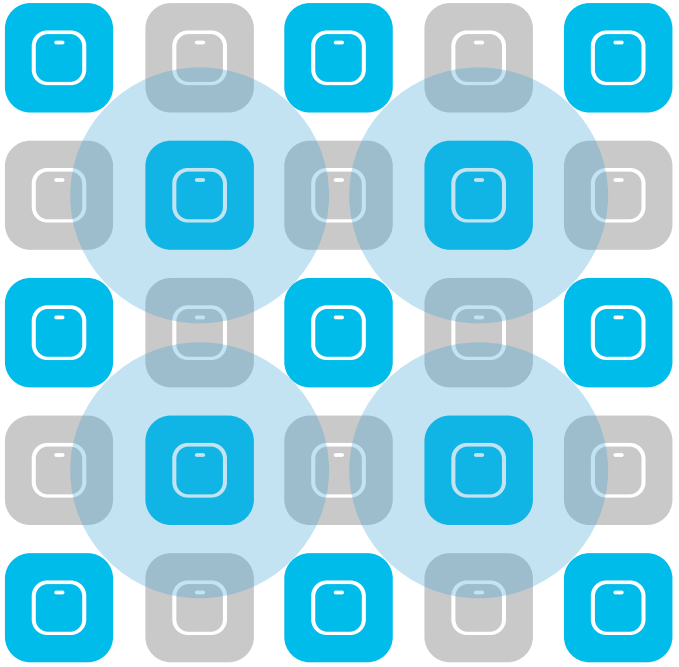


How does it work?

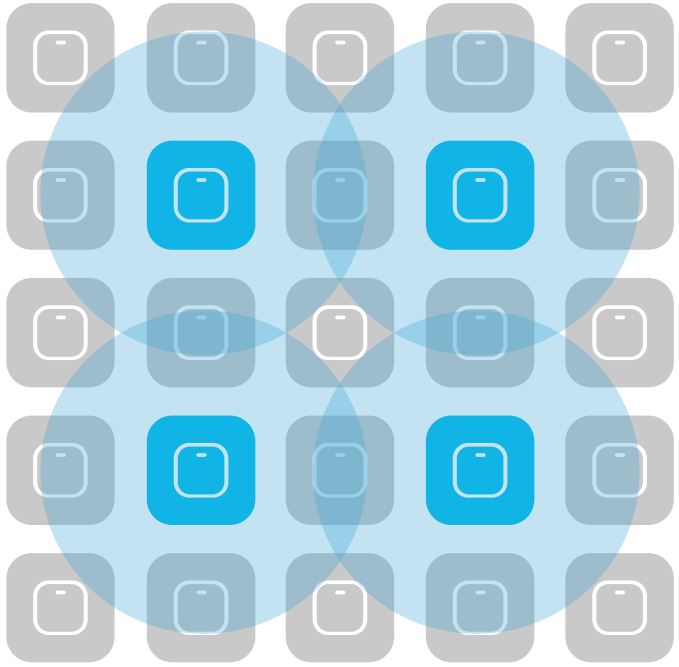
- Group APs into multiple groups and upgrade one group at a time.
- Grouping is done based on RF neighbors
- Admin user can control the impact and determines the number of iterations taken and the Rolling Upgrade time
- Candidate AP selection
  - With **N** = 4: If the AP in blue is selected and 4 of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

Rolling AP Upgrade: Neighbor AP marking

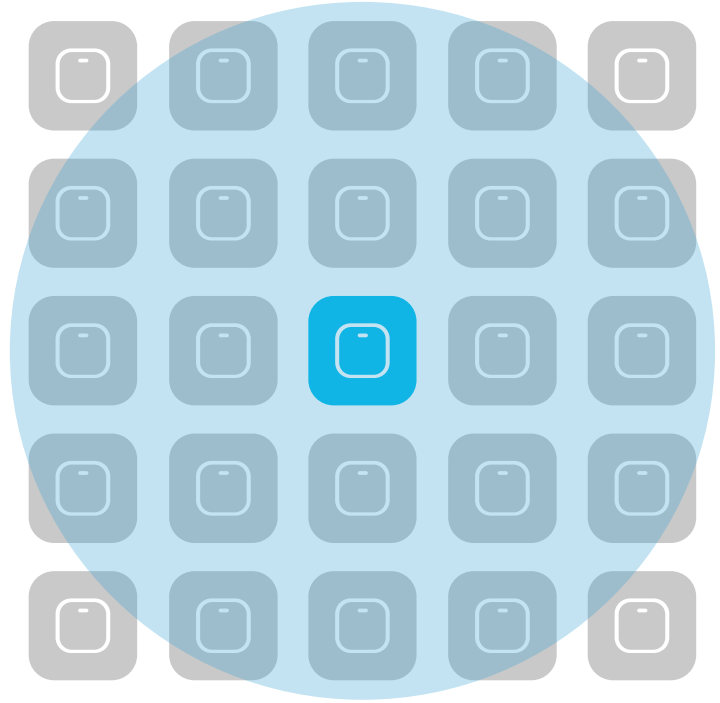
25%



15%



5%



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]

Rolling AP Upgrade: Client steering

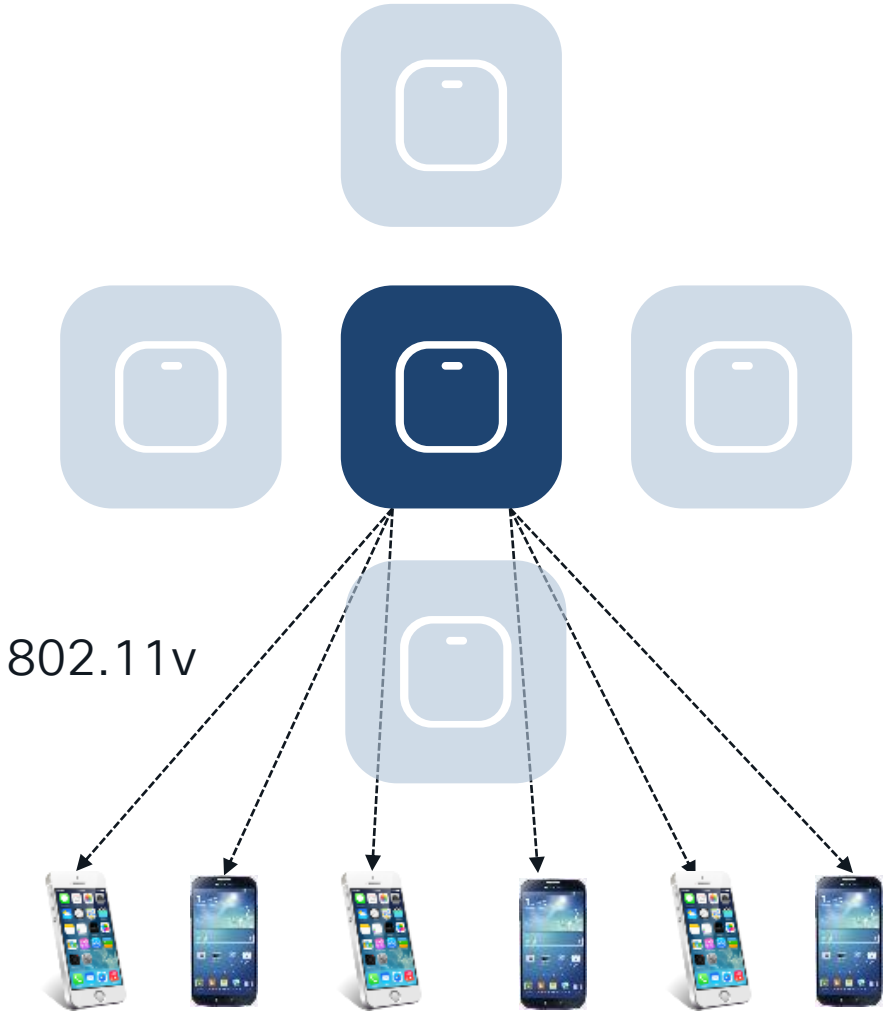
Clients steered from candidate APs to non-candidate APs

802.11v BSS Transition Request → Dissociation Imminent

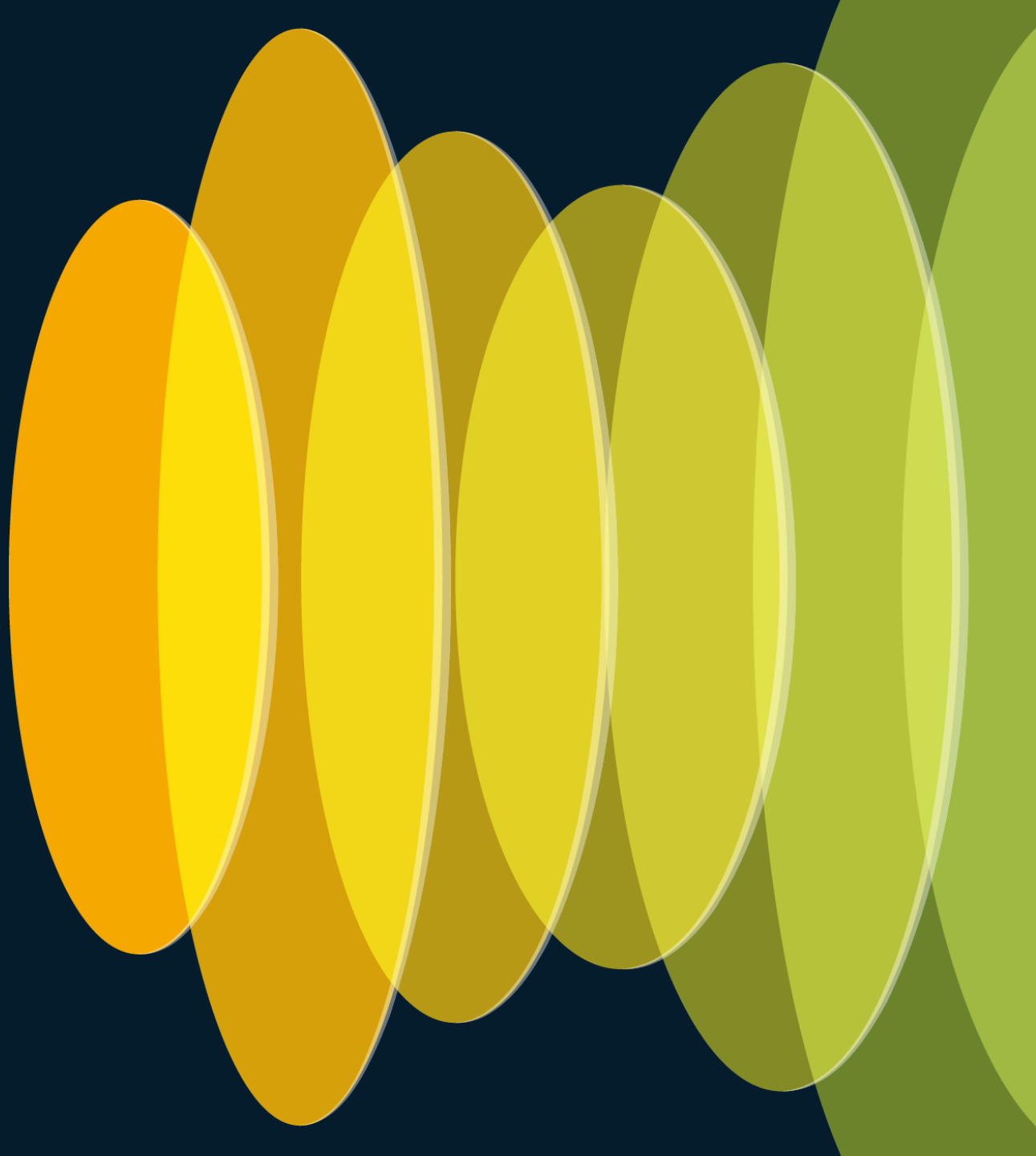
Clients that do not honor this will be de-authenticated before AP reload

NEW

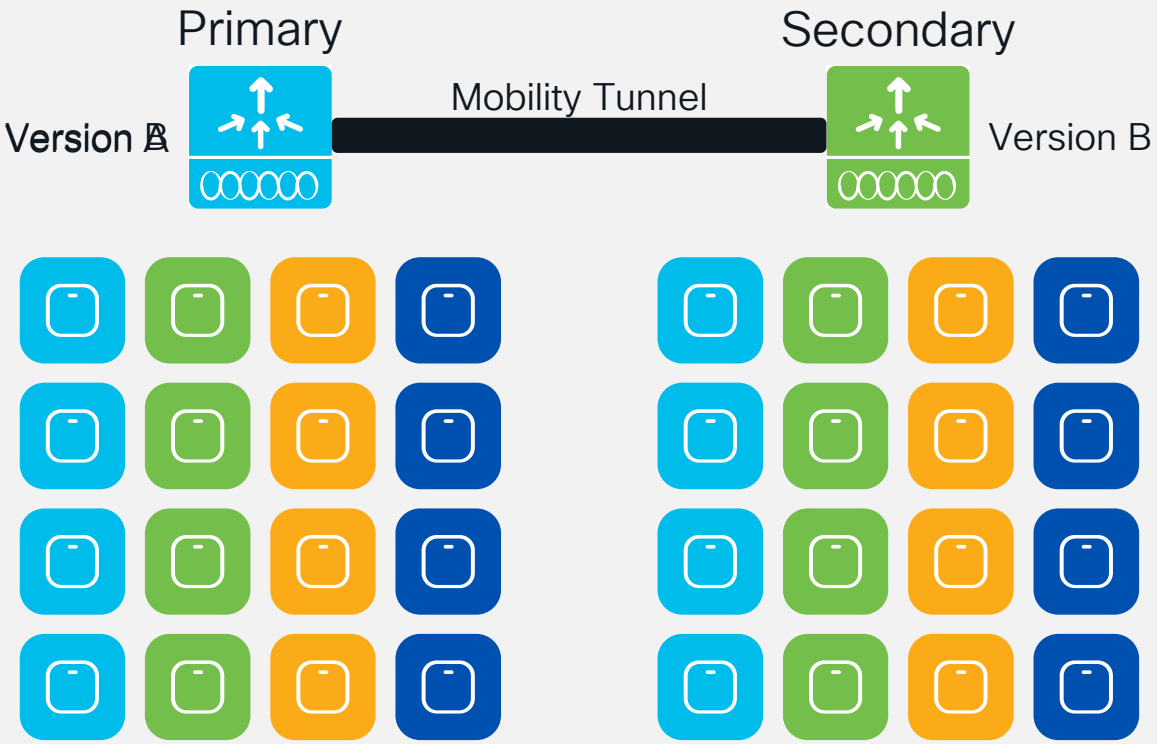
Starting 17.11 AP stops responding to client probes and association (in Flex)



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

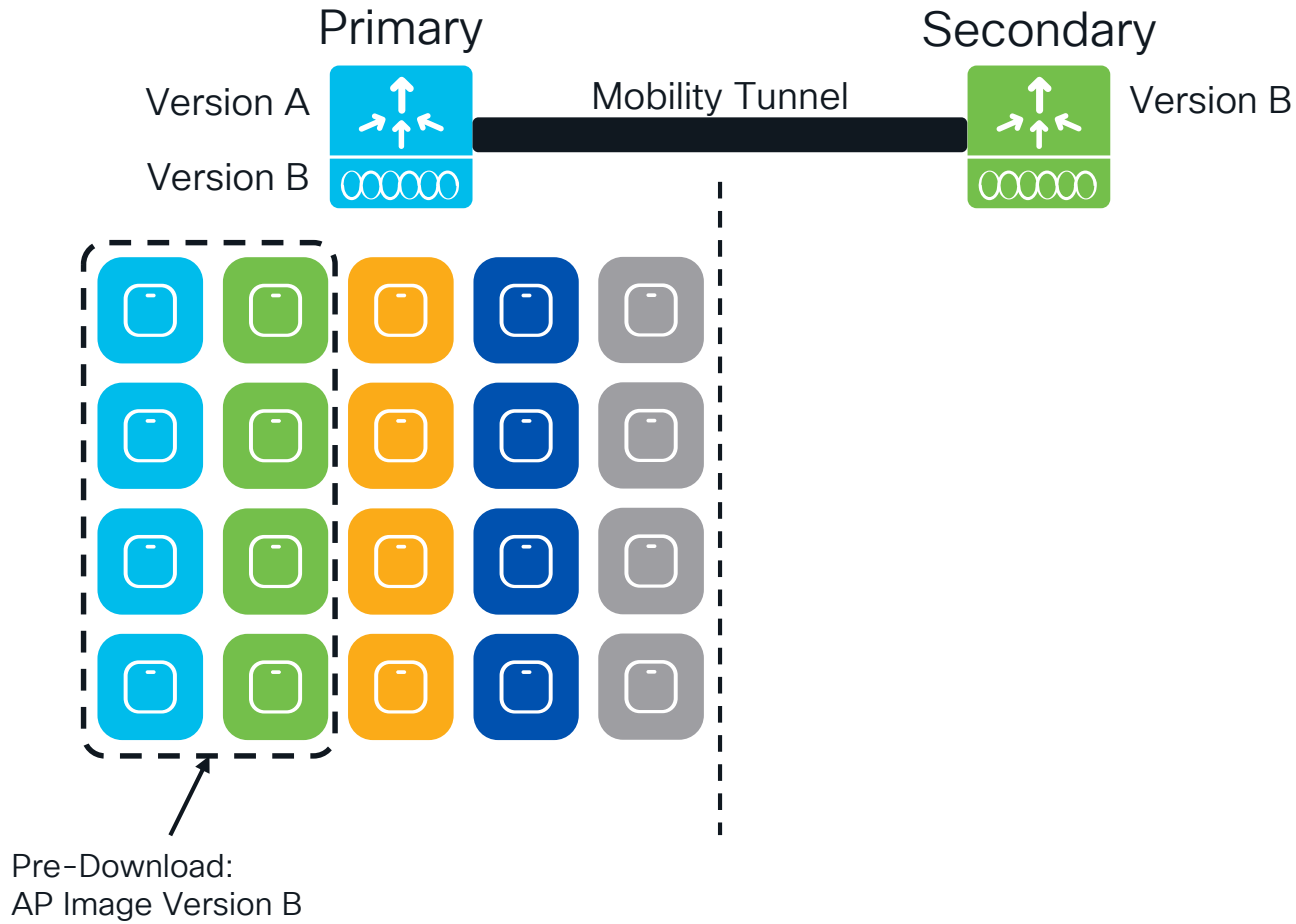
1. Add the new IOS XE image to the controller:
   `install add file <Path to Image>`

```
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`



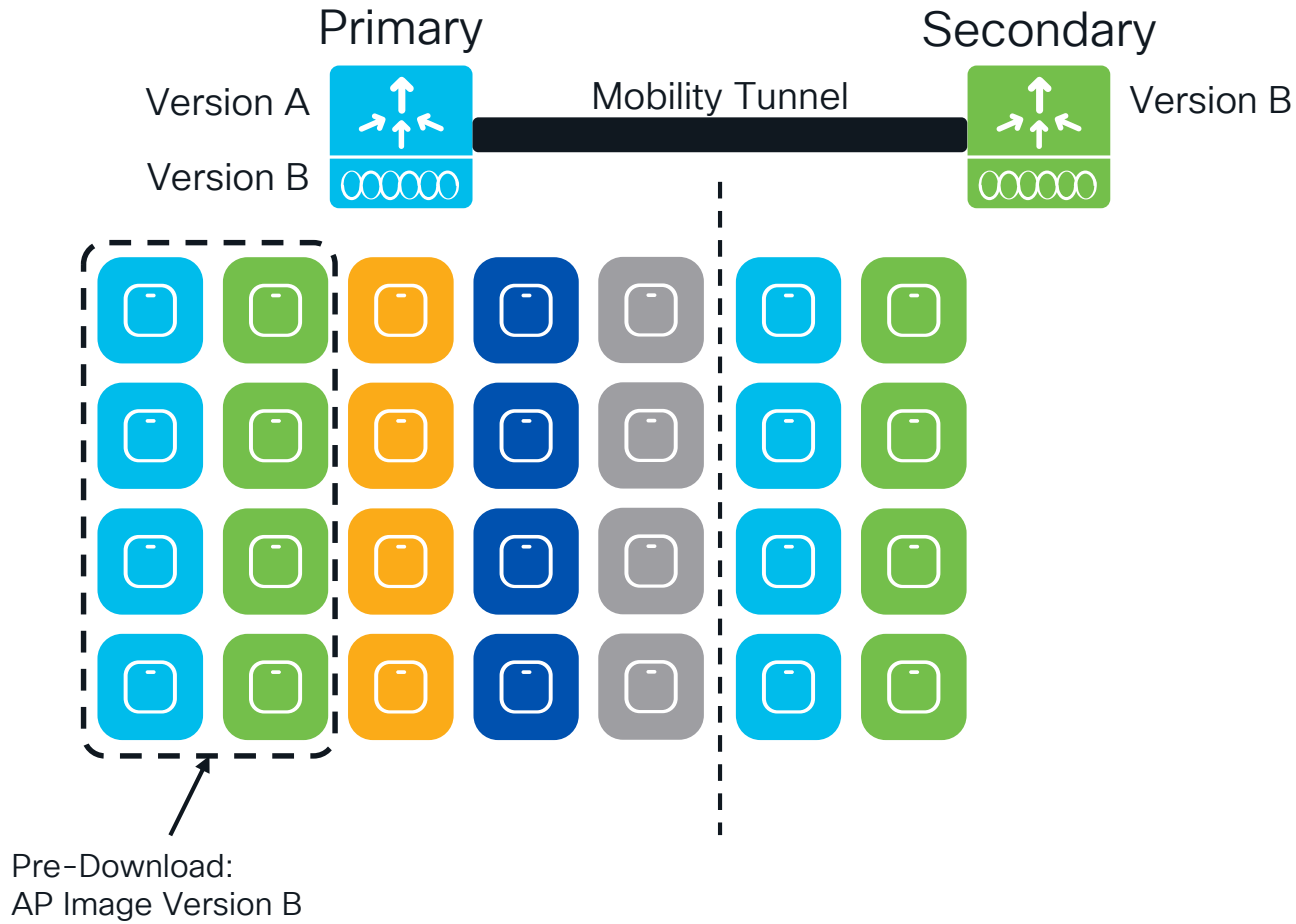
AP upgrade workflow

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.



Site Filter

Site 1

Site 2

Site 3

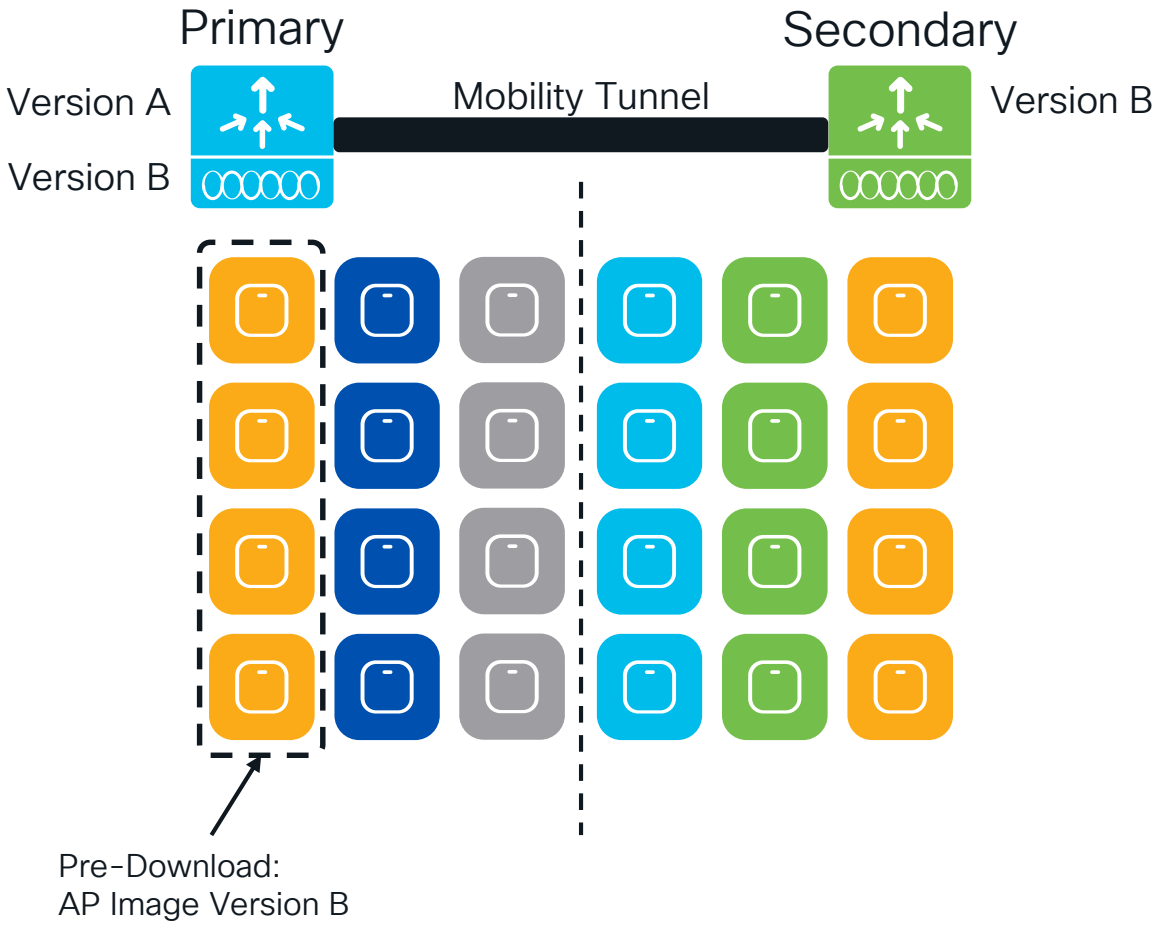
AP upgrade workflow

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.



Site Filter

- Site 1
- Site 2
- Site 3

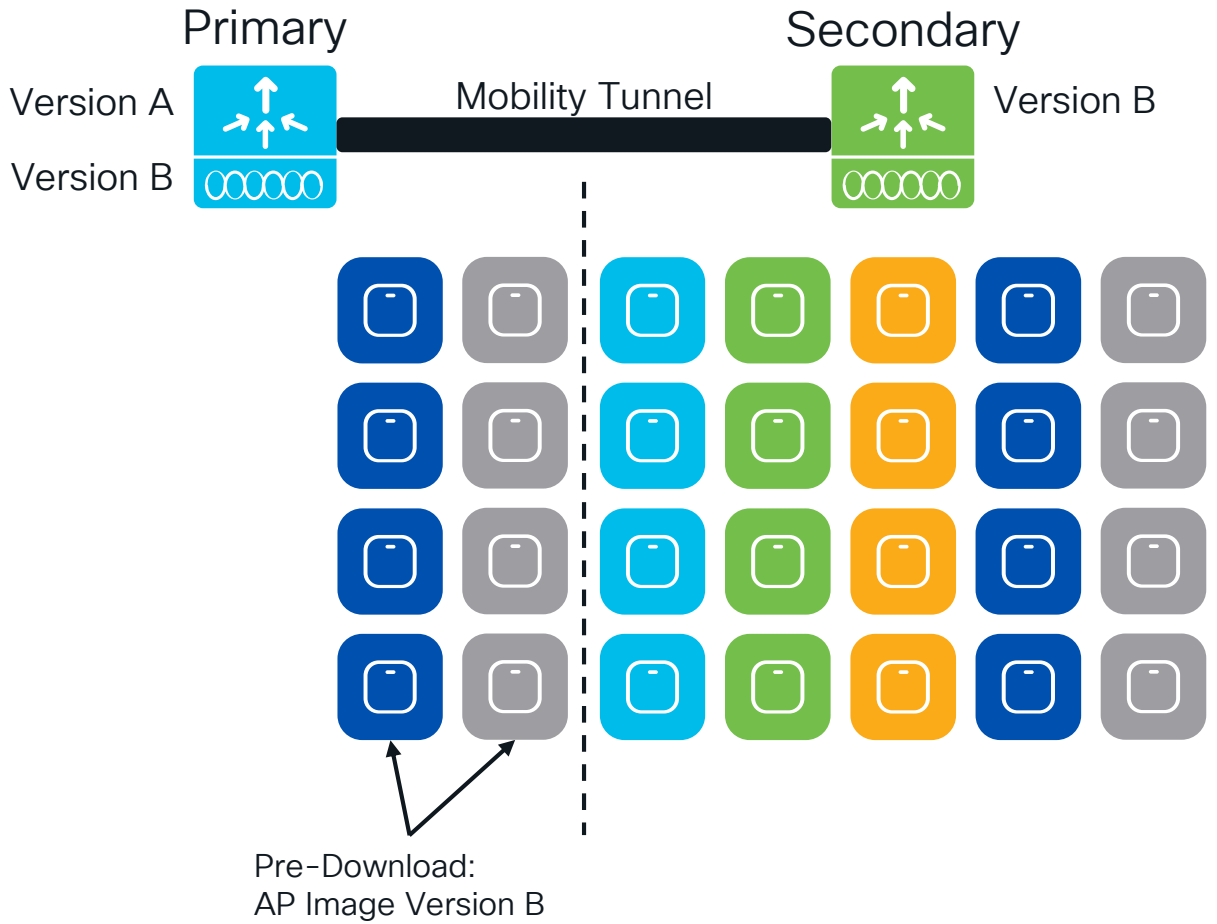
AP upgrade workflow

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

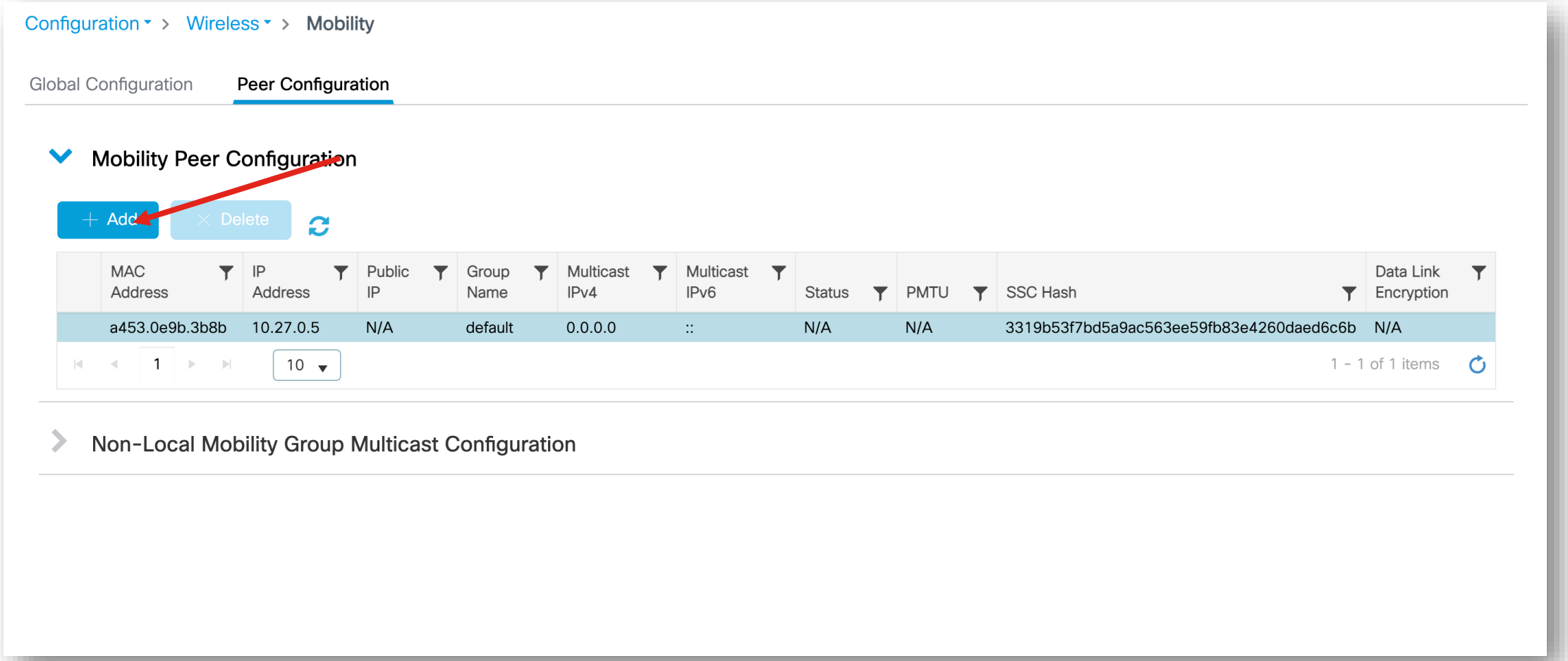
11 APs at the remaining sites will pre-download the image, reload with the new image, and join to the Secondary WLC in rolling fashion.

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

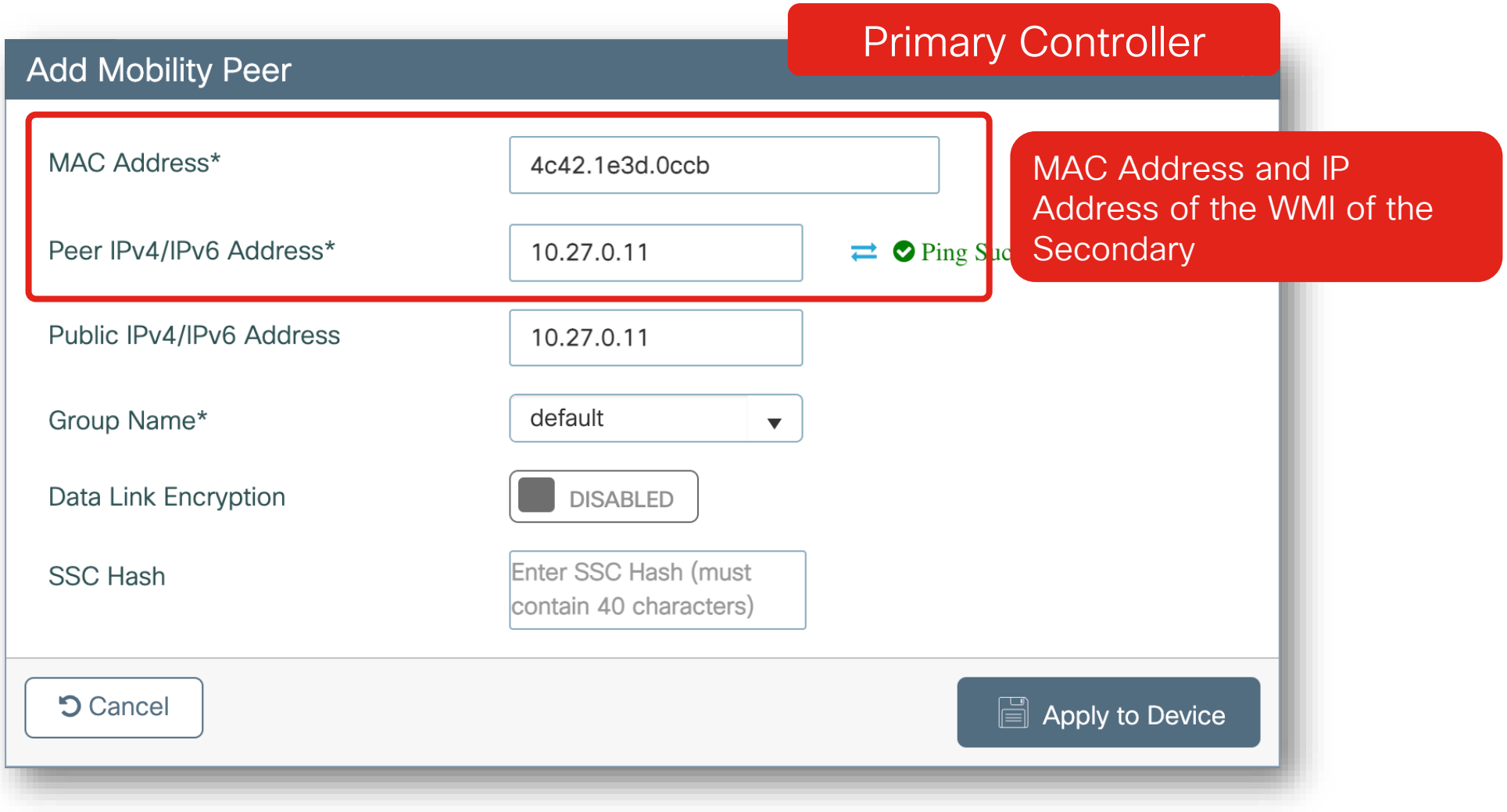
13 Activate the new IOS XE image on the Primary WLC.



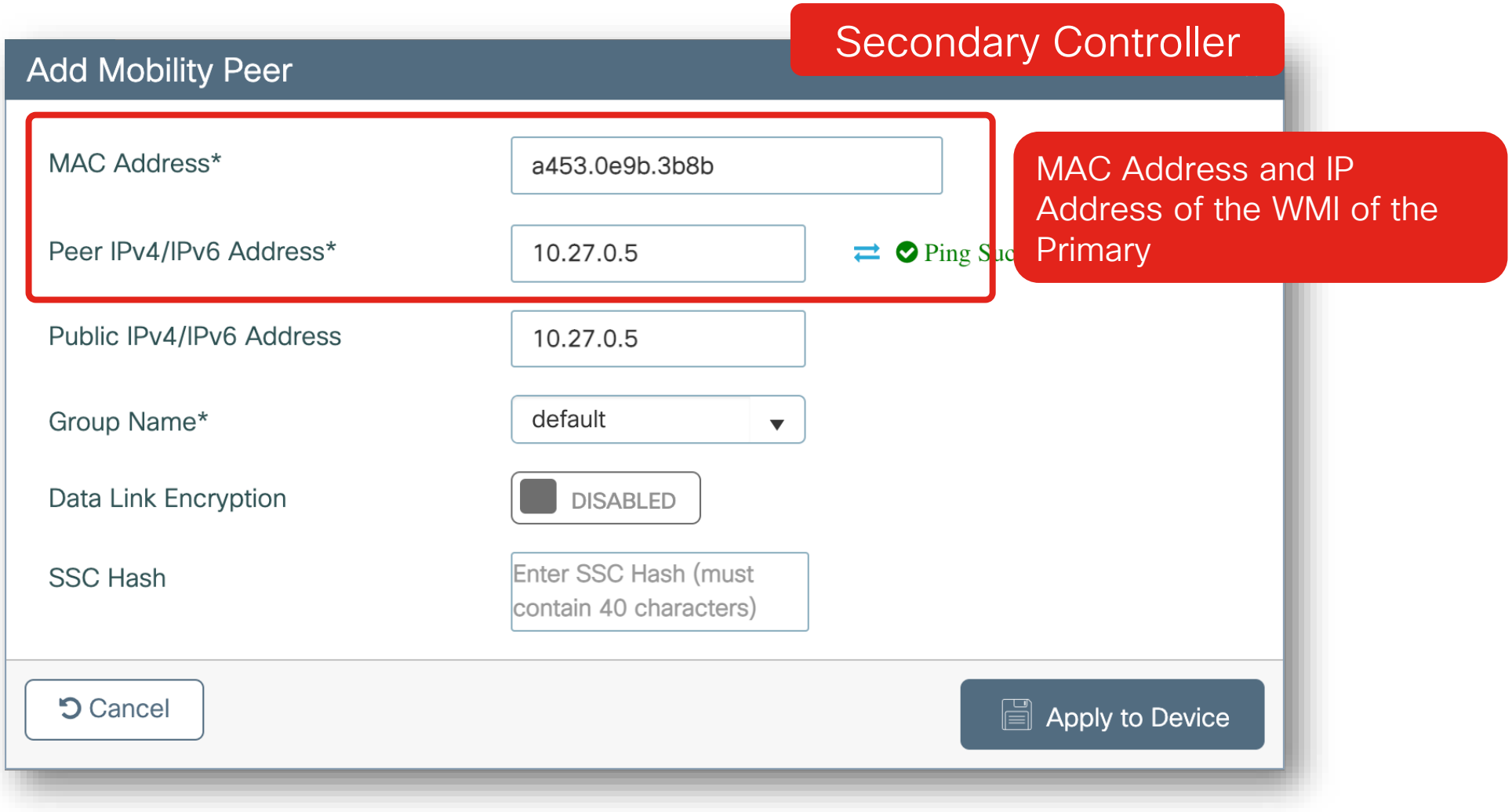
Configuration via WebUI
Mobility Tunnel



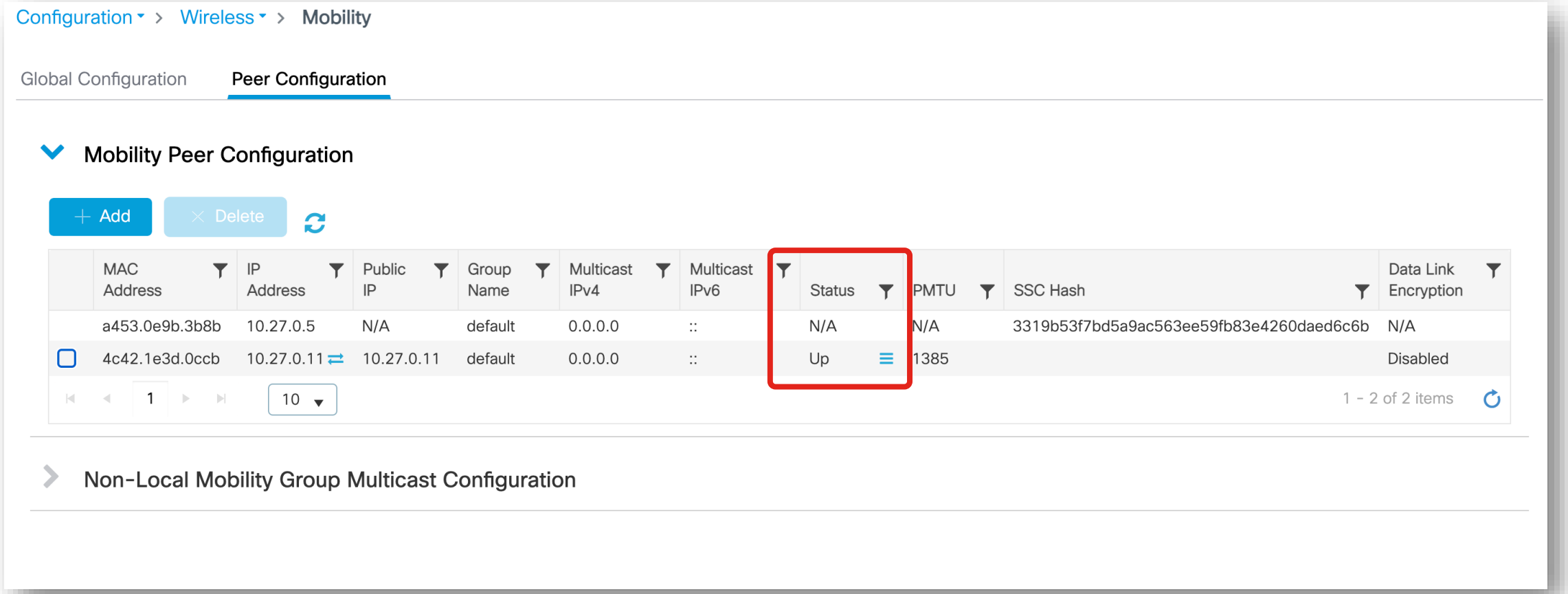
Configuration via WebUI
Mobility Tunnel



Configuration via WebUI
Mobility Tunnel

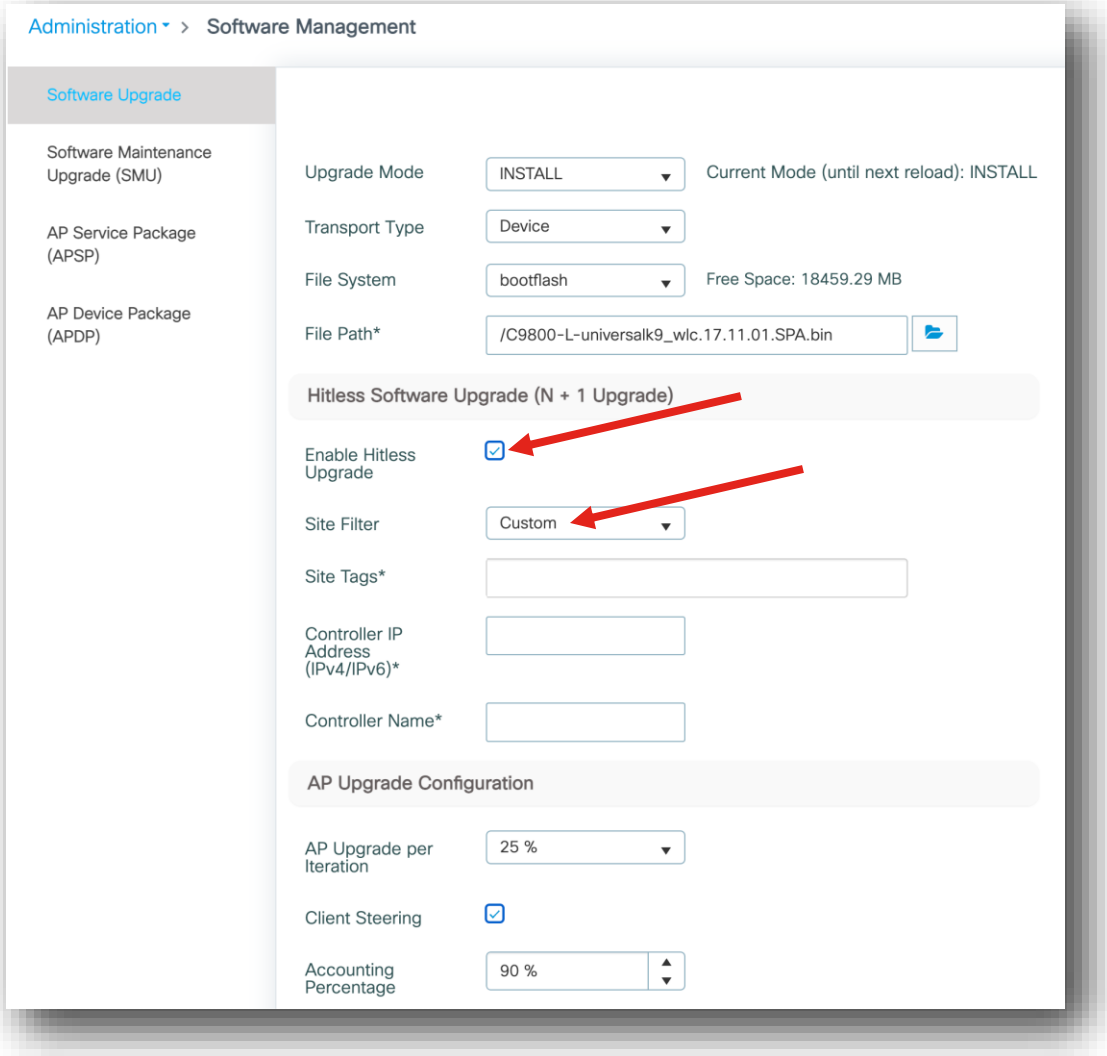


Configuration via WebUI
Mobility Tunnel



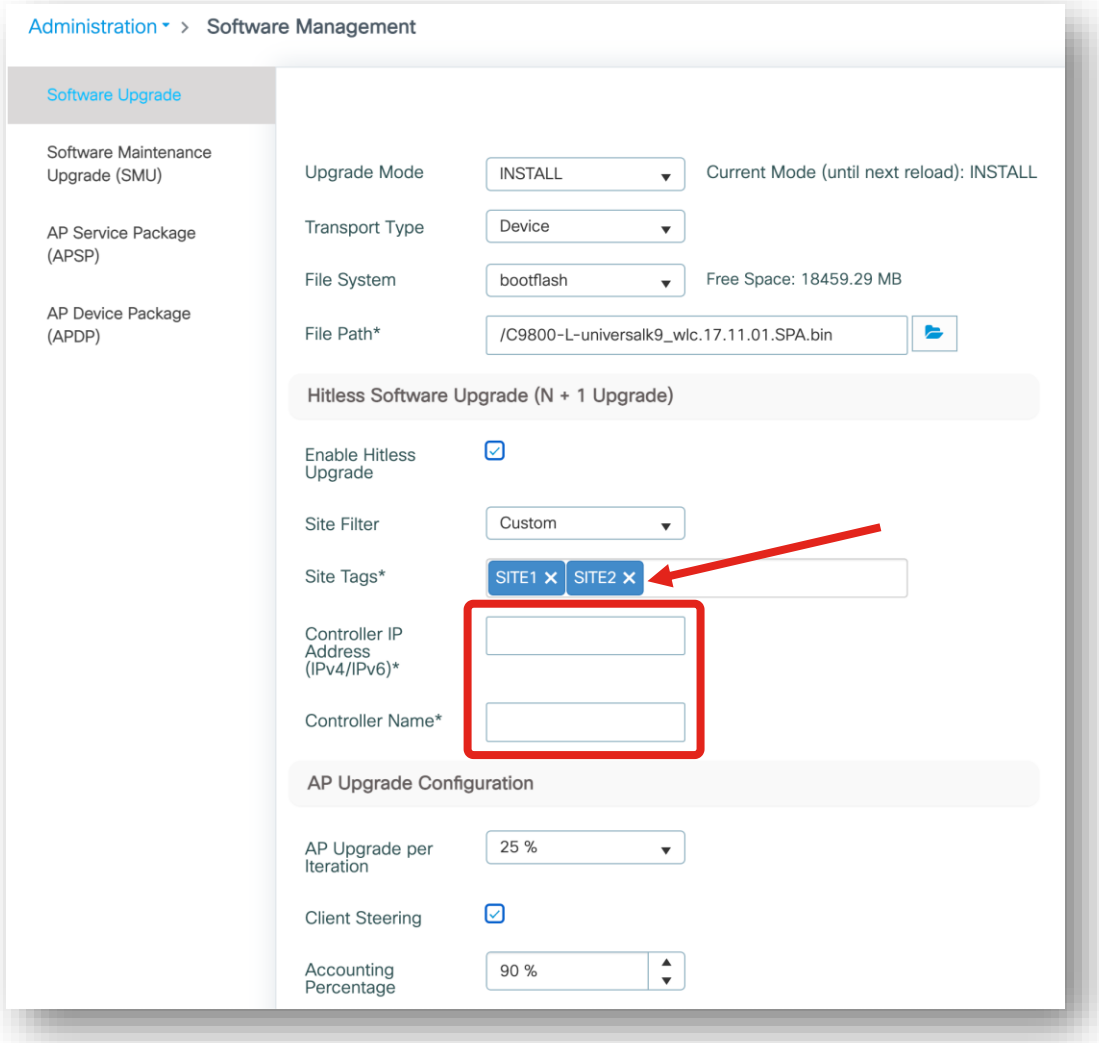
N+1 Site Based Hitless Upgrade with WebUI

1. Check the box for **Enable Hitless Upgrade**
2. Set the Site Filter to **Custom**



N+1 Site Based Hitless Upgrade with WebUI

1. Check the box for **Enable Hitless Upgrade**
2. Set the Site Filter to **Custom**
3. Select the required **Site Tags**
4. Set the Secondary Controller's **IP Address** and **Hostname**



N+1 Site Based Hitless Upgrade with WebUI

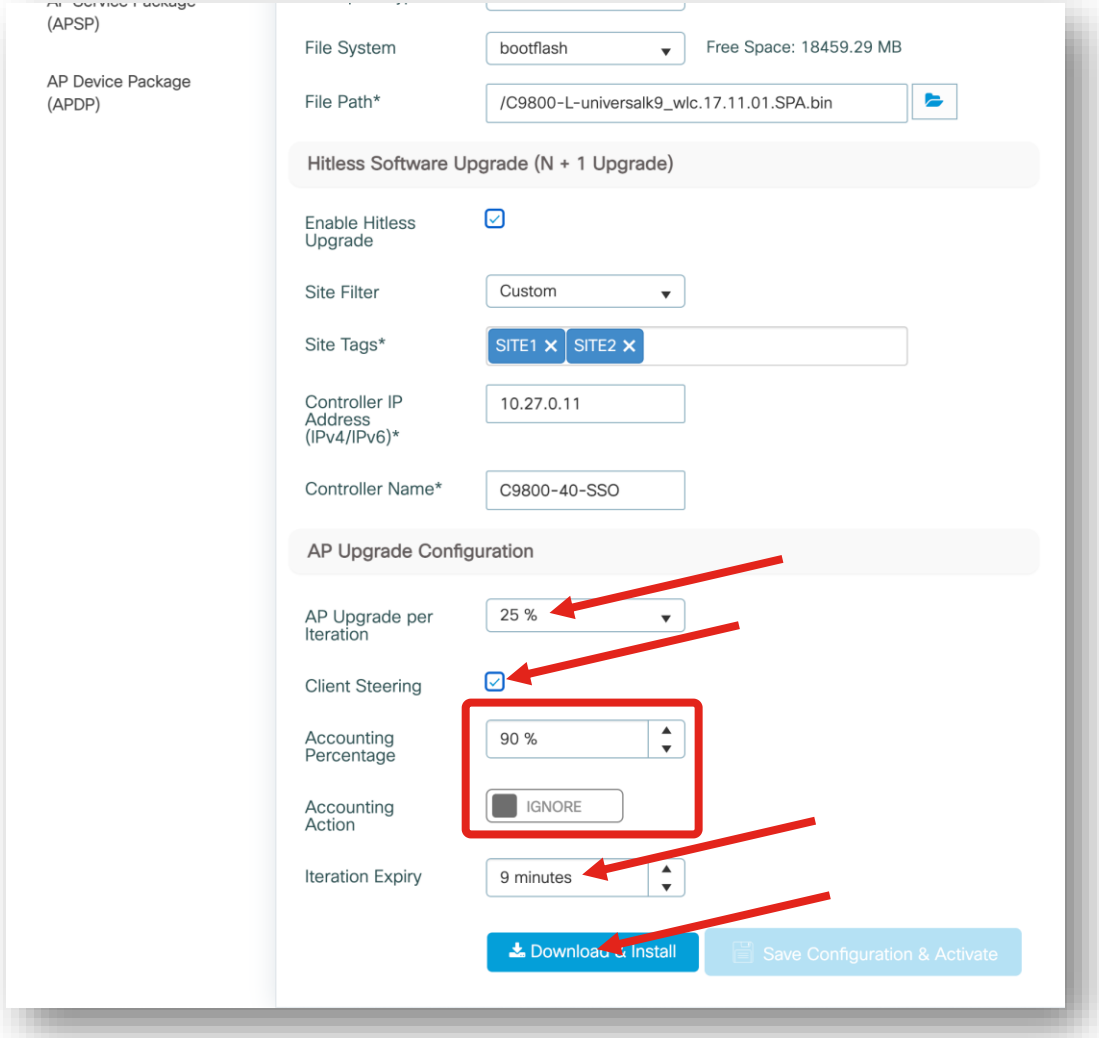
5 Set the required **AP Upgrade per Iteration**

6 Check the box to enable **Client Steering**

7 Choose the required **Accounting Percentage** and **Accounting Action**

8 Set the **Iteration Expiry**

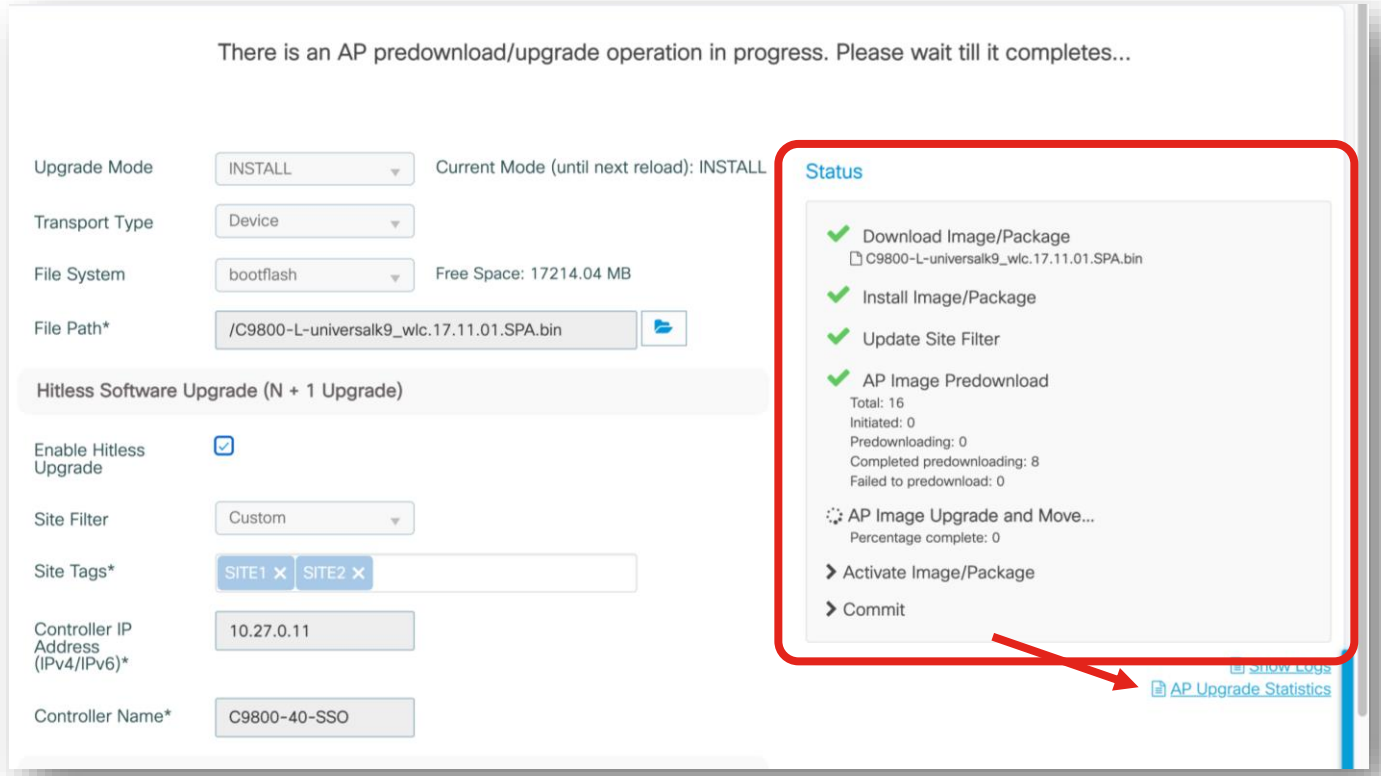
9 Click **Download & Install**



N+1 Site Based Hitless Upgrade with WebUI

10 Monitor the progress of the entire upgrade in the **Status** Window

11 Click **AP Upgrade Statistics** to track each iteration of AP upgrade

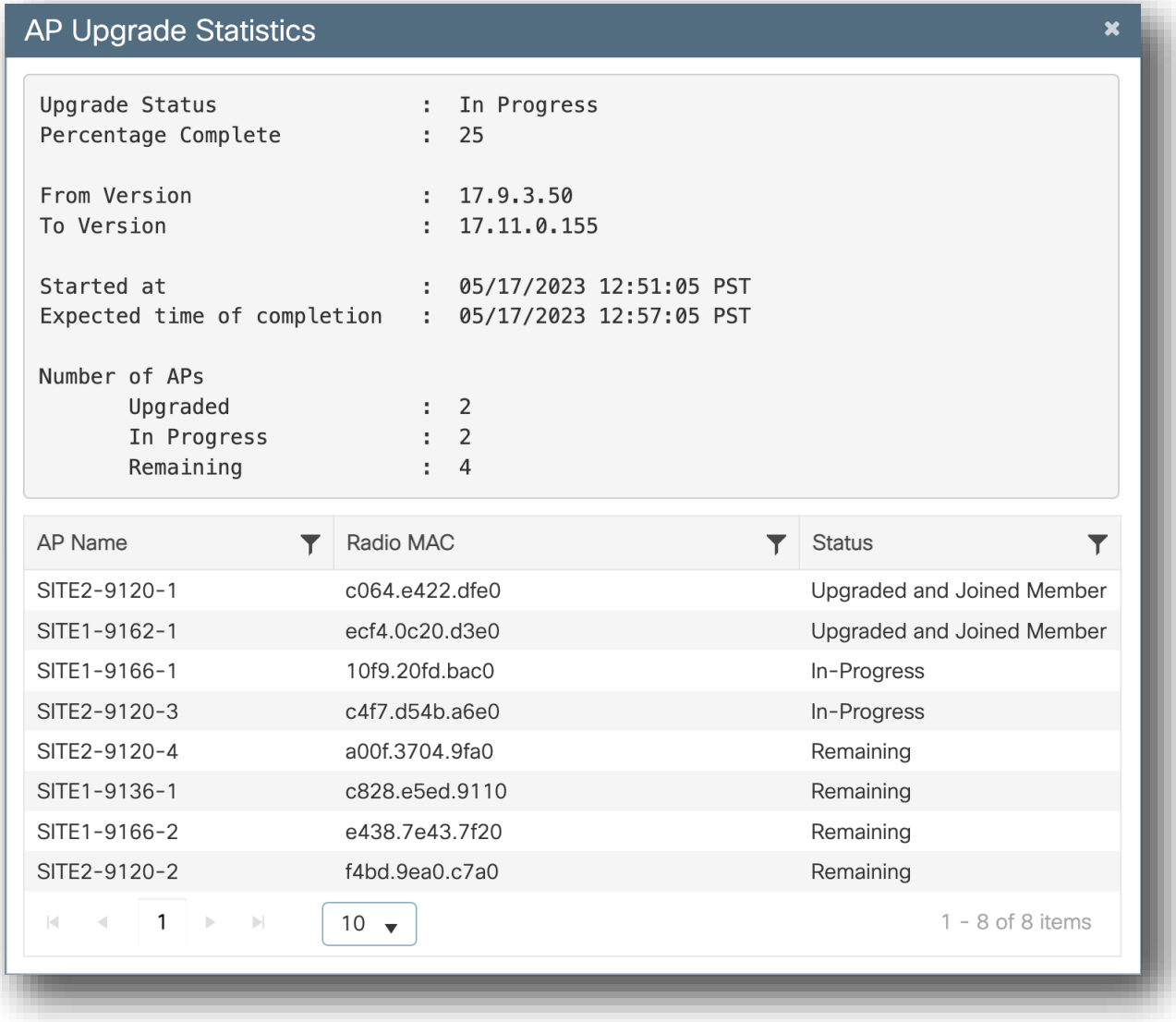


N+1 Site Based Hitless Upgrade with WebUI

10 Monitor the progress of the entire upgrade in the **Status** Window

11 Click **AP Upgrade Statistics** to track each iteration of AP upgrade

12 Wait for the current iteration of APs to finish moving to the secondary controller



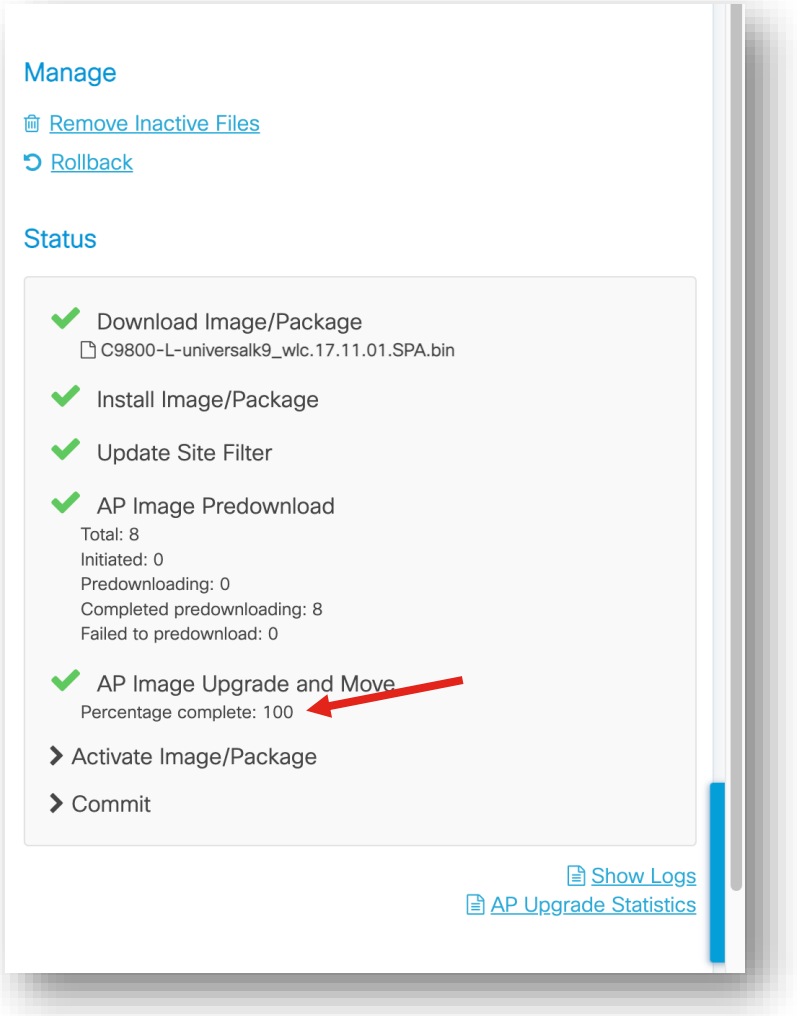
N+1 Site Based Hitless Upgrade with WebUI

10 Monitor the progress of the entire upgrade in the **Status** Window

11 Click **AP Upgrade Statistics** to track each iteration of AP upgrade

12 Wait for the current iteration of APs to finish moving to the secondary controller

13 Once done, add the next Site Tag(s) to the Site Filter and click **Update Site Filter**



N+1 Site Based Hitless Upgrade with WebUI

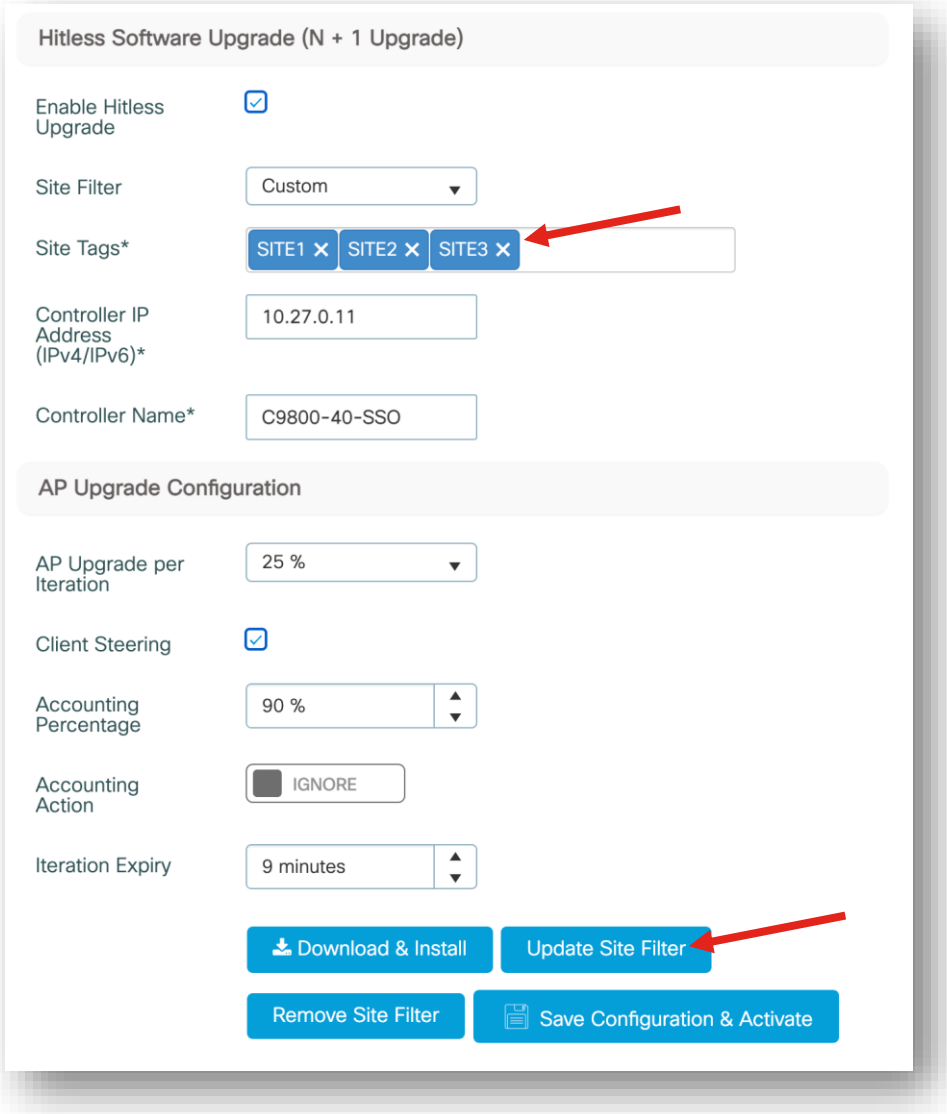
10 Monitor the progress of the entire upgrade in the **Status** Window

11 Click **AP Upgrade Statistics** to track each iteration of AP upgrade

12 Wait for the current iteration of APs to finish moving to the secondary controller

13 Once done, add the next Site Tag(s) to the Site Filter and click **Update Site Filter**

14 Repeat Steps 12 and 13 as needed



N+1 Site Based Hitless Upgrade with WebUI

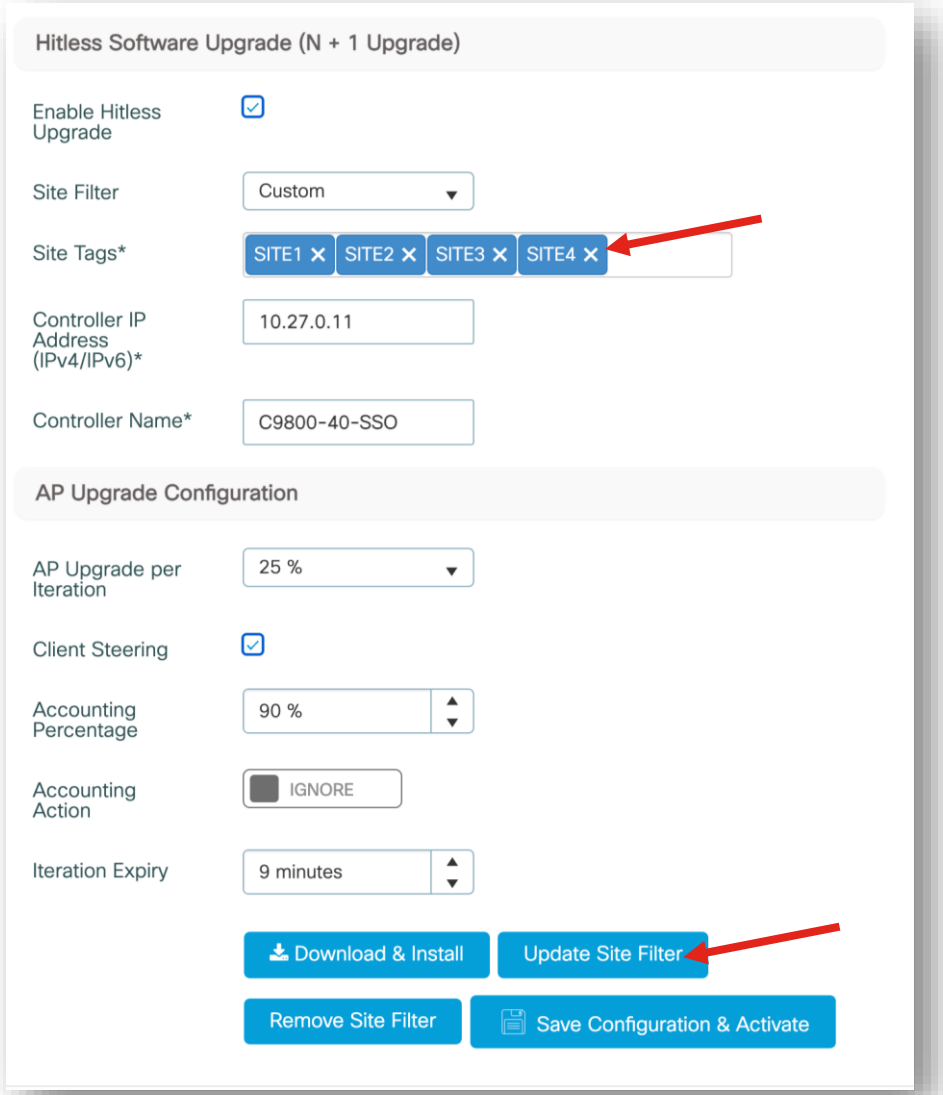
10 Monitor the progress of the entire upgrade in the **Status** Window

11 Click **AP Upgrade Statistics** to track each iteration of AP upgrade

12 Wait for the current iteration of APs to finish moving to the secondary controller

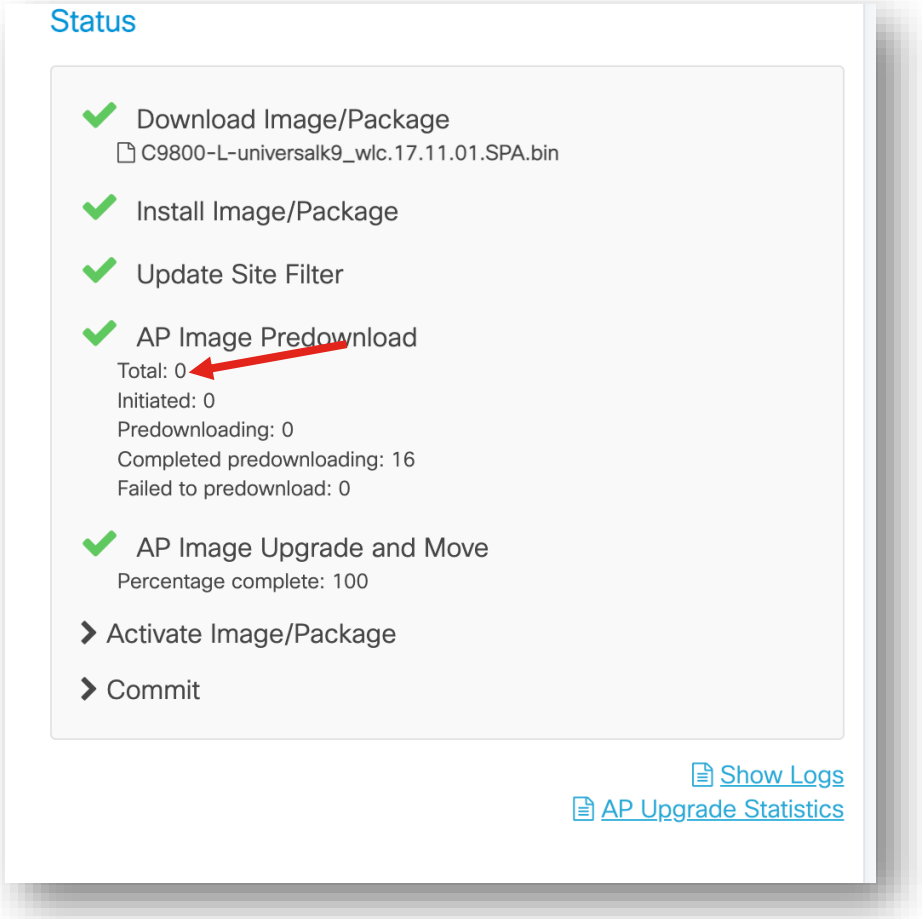
13 Once done, add the next Site Tag(s) to the Site Filter and click **Update Site Filter**

14 Repeat Steps 12 and 13 as needed



N+1 Site Based Hitless Upgrade with WebUI

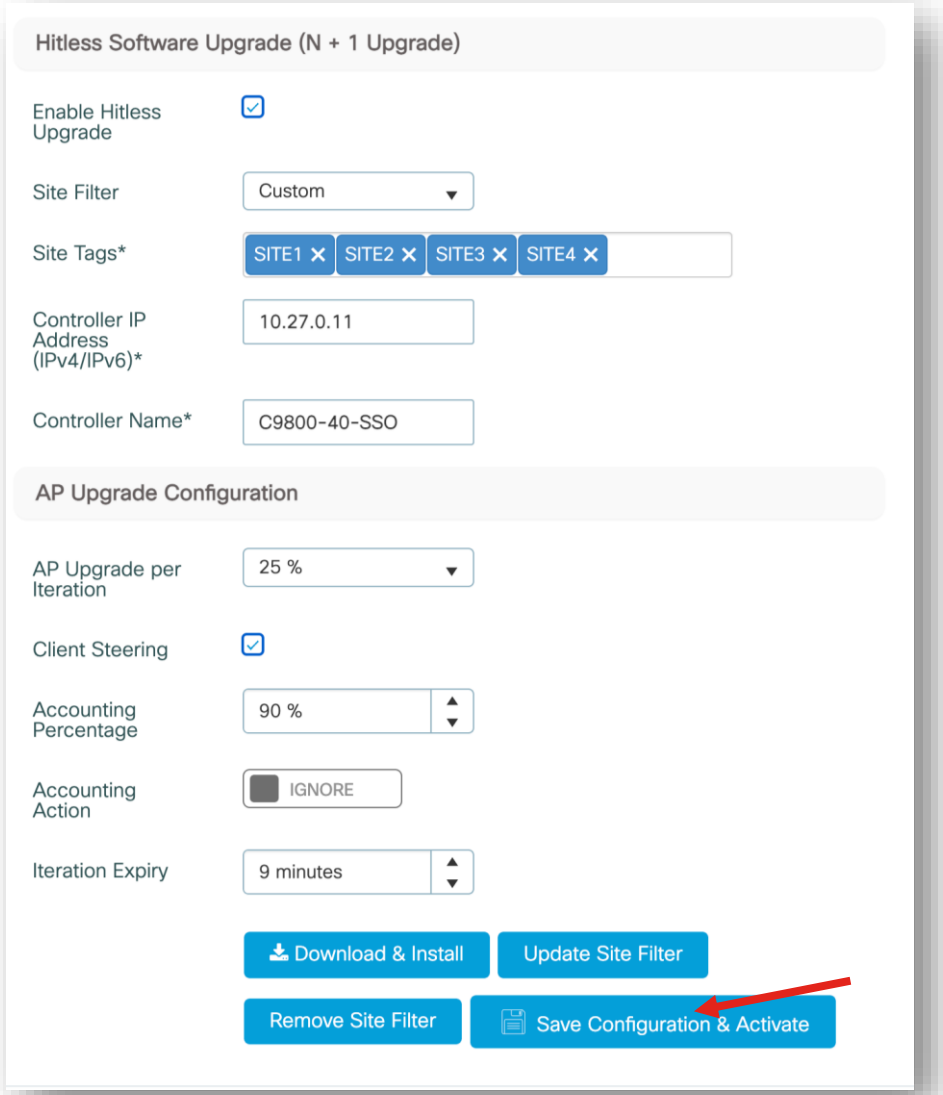
15 All APs are upgraded when the **Total** is 0



N+1 Site Based Hitless Upgrade with WebUI

15 All APs are upgraded when the **Total** is 0

16 Apply the upgrade by clicking **Save Configuration & Activate**



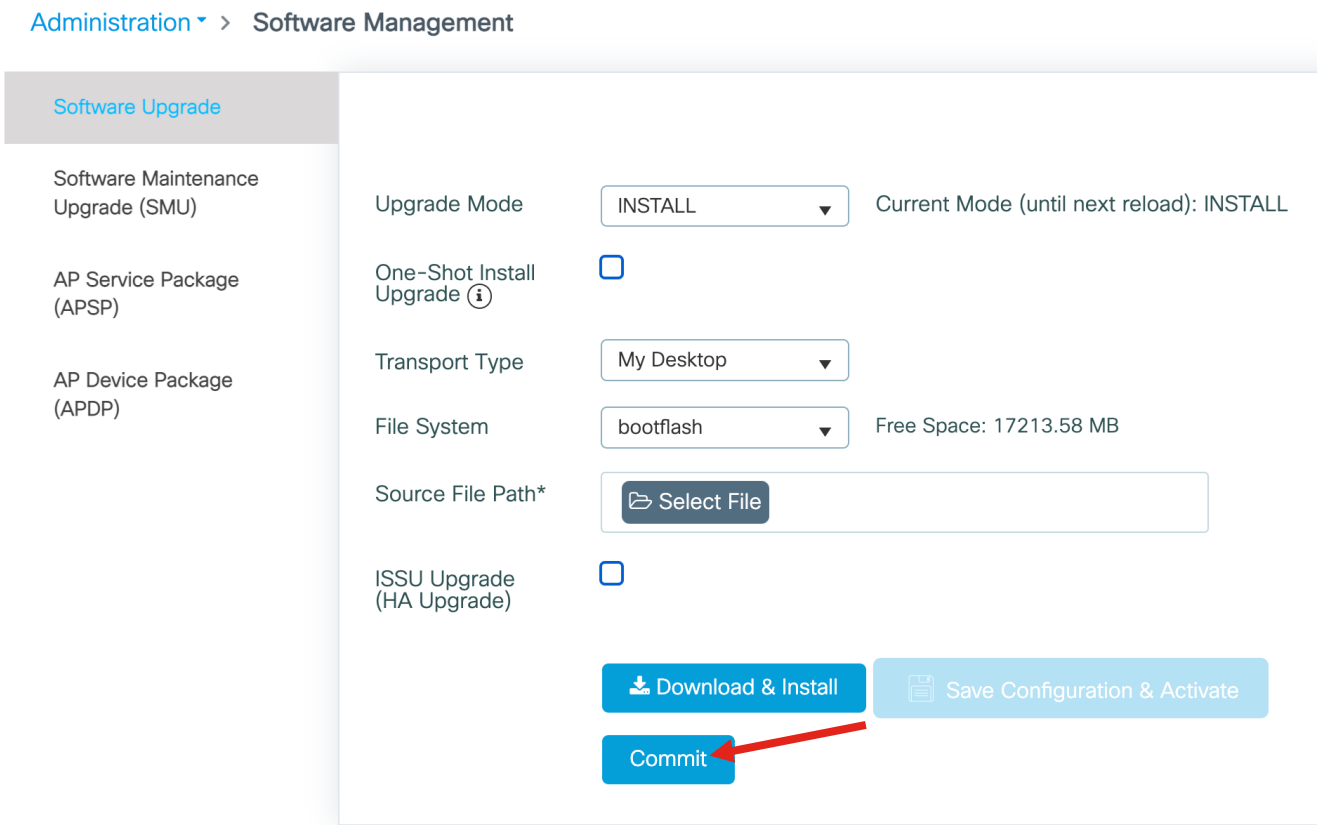
N+1 Site Based Hitless Upgrade with WebUI

15 All APs are upgraded when the **Total** is 0

16 Apply the upgrade by clicking **Save Configuration & Activate**

17 After the controller reloads, commit the upgrade by clicking **Commit**

18 If required, use the CLI to move the APs back to the primary on a site-by-site basis

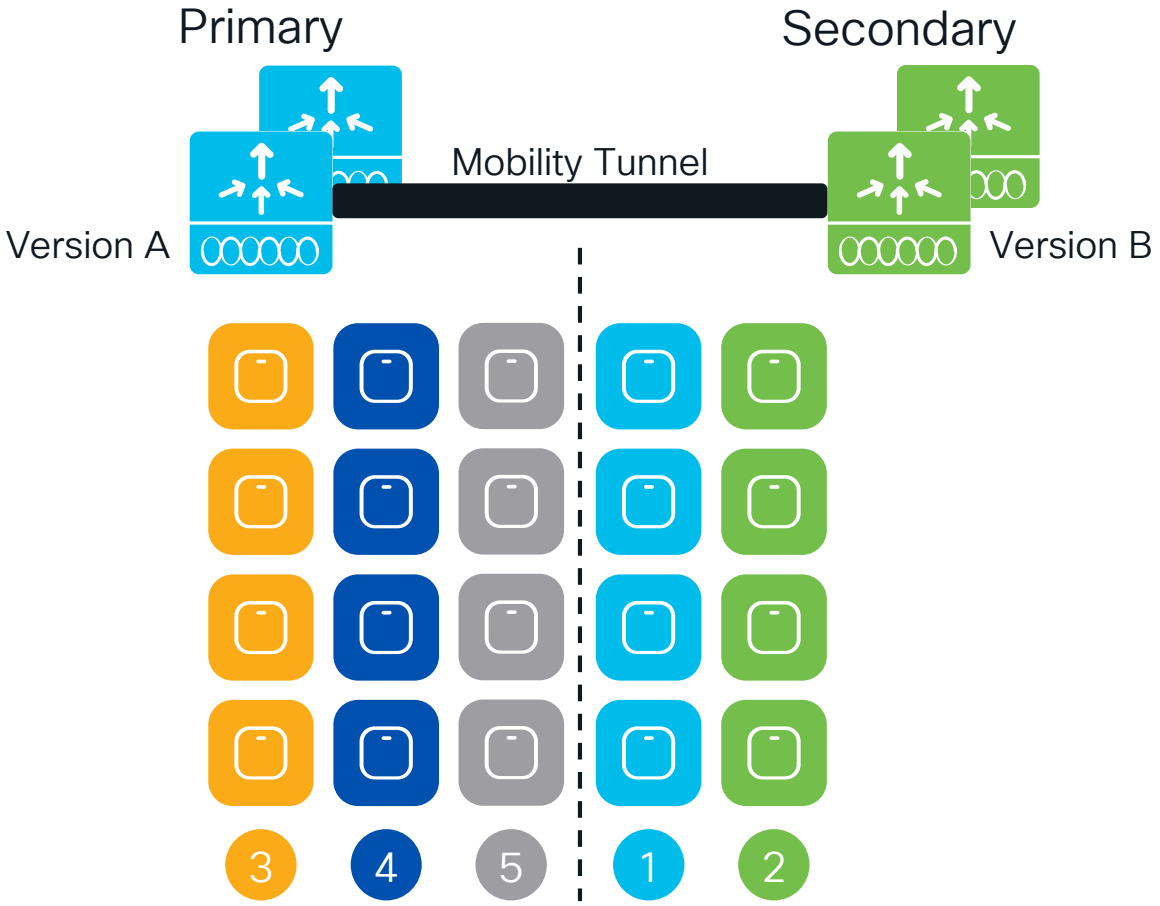


Can I use HA SSO Pair with N+1 Rolling Upgrade?

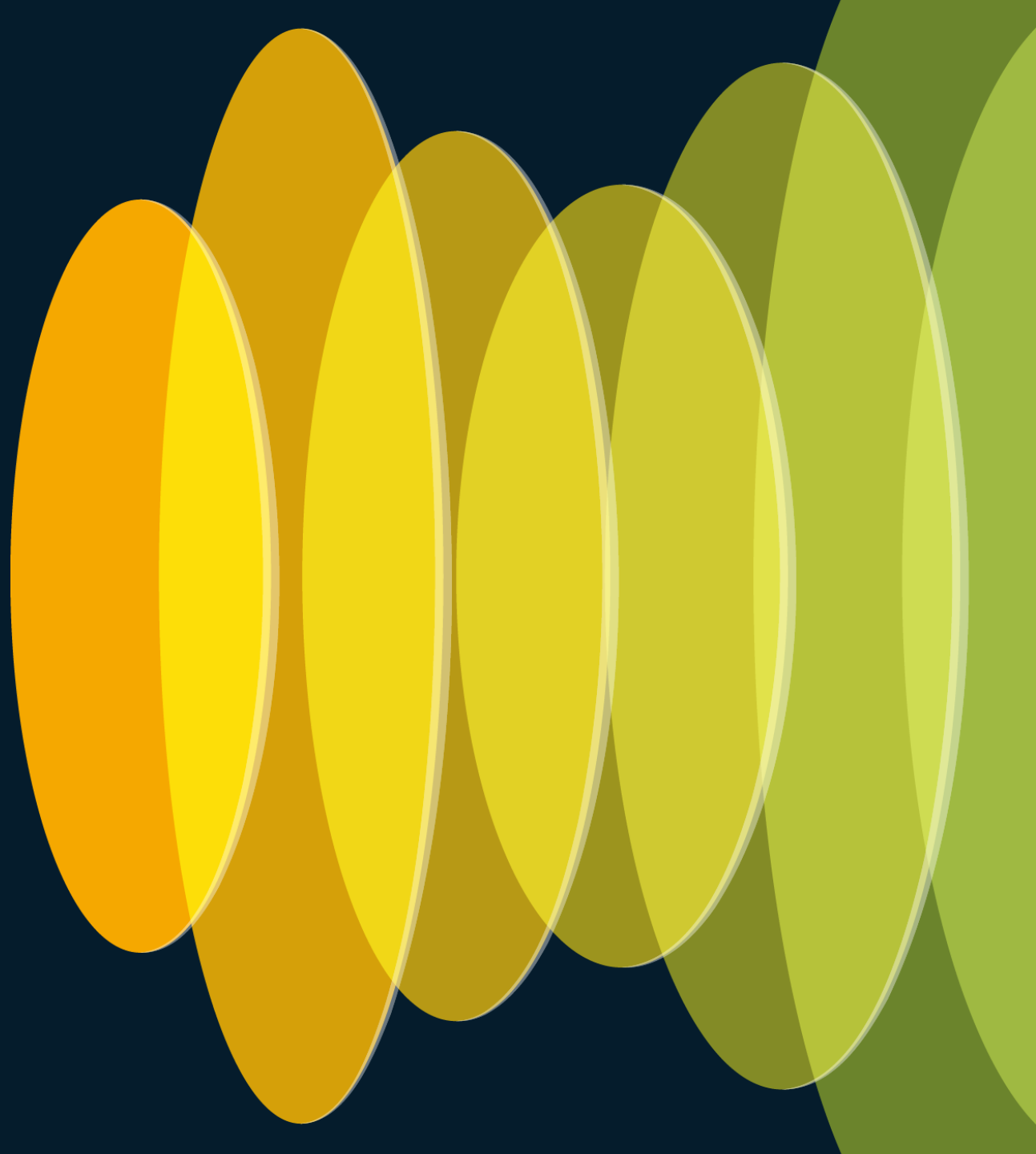
Customers can stay in Secondary HA pair and reduce the upgrade process by half

Add another layer of resiliency if the N+1 chassis fails

Flexibility to upgrade each site while ensuring resiliency



In-Service Software Upgrade (ISSU)



cisco Live!

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

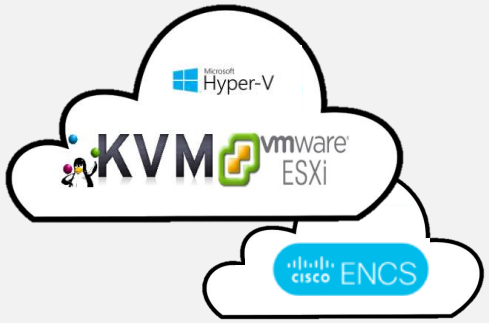
All AP/Client sessions are retained during upgrade process

Pre-requisites:

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

Supported platforms for ISSU

Controllers



Catalyst 9800-CL
Private Cloud

Catalyst 9800-L

Catalyst 9800-40

Catalyst 9800-80

Access Points

Wi-Fi 6 and 6E APs

1815W

1815I, 1815M

1832

1842

1852

2802

3802

1700, 2700, 3700,
1570 Wave 1 APs

1540

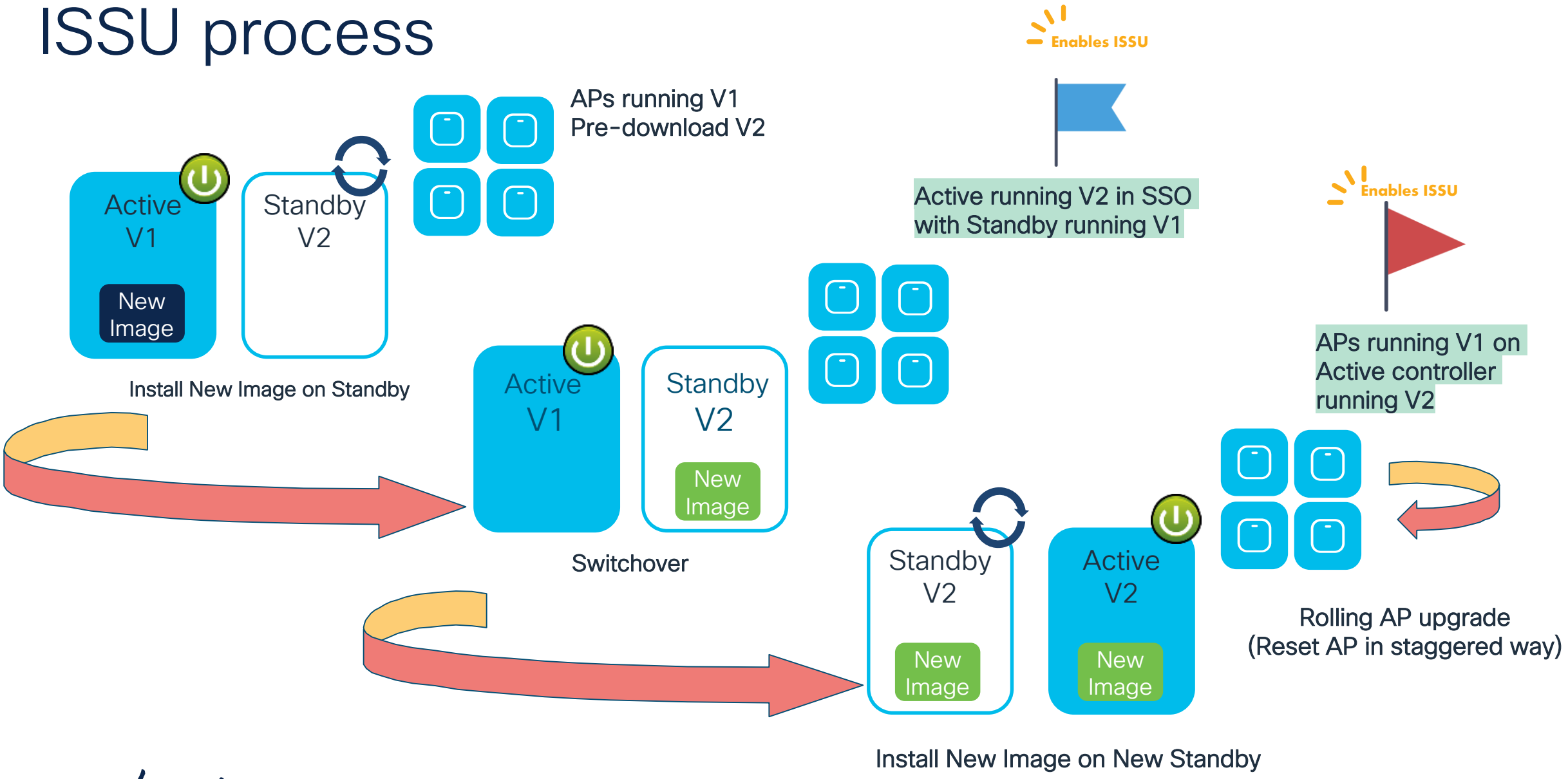
1560

4800

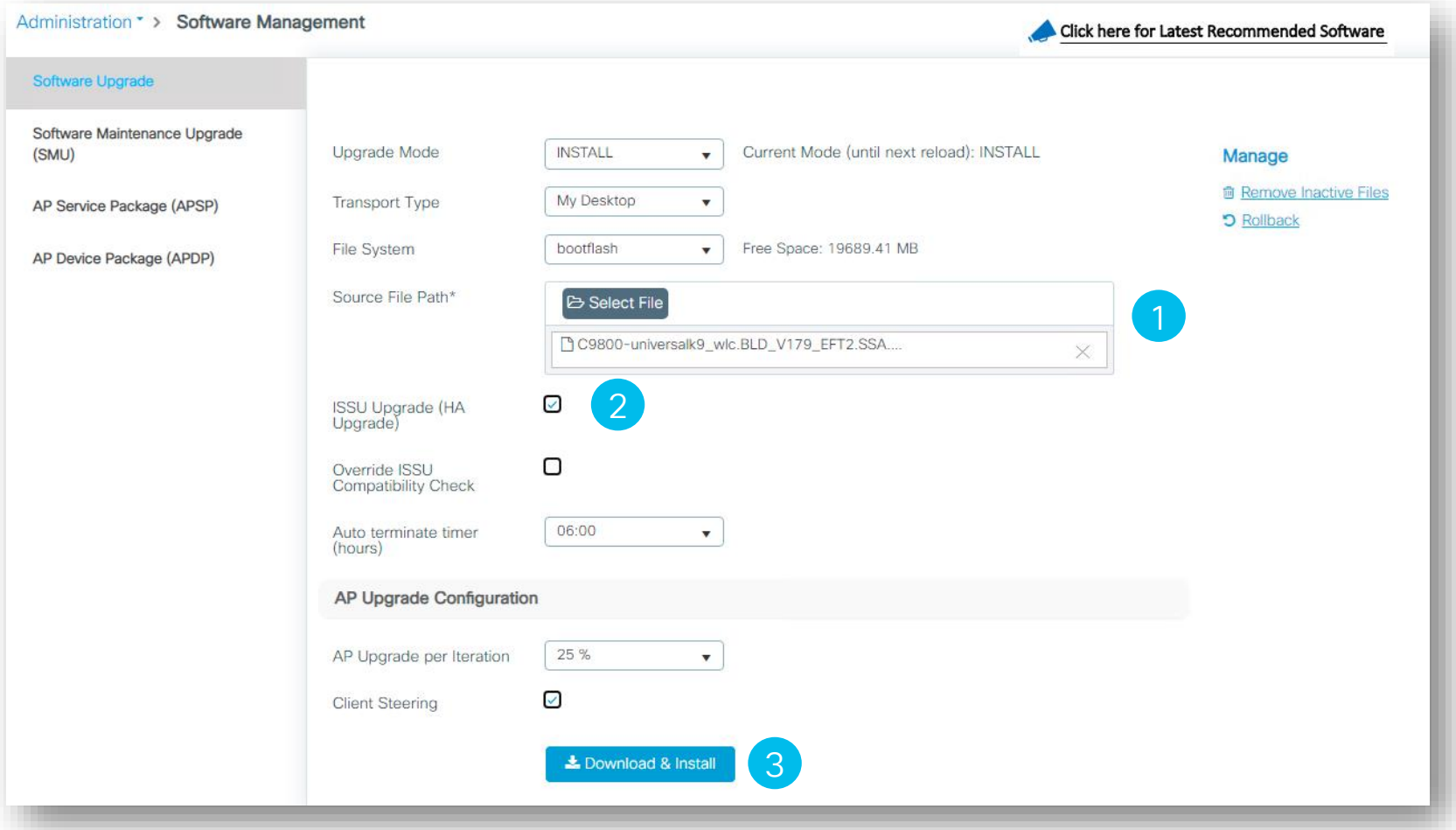
Wave 2 indoor and outdoor APs

Ensure APs are supported by target software version.

ISSU process

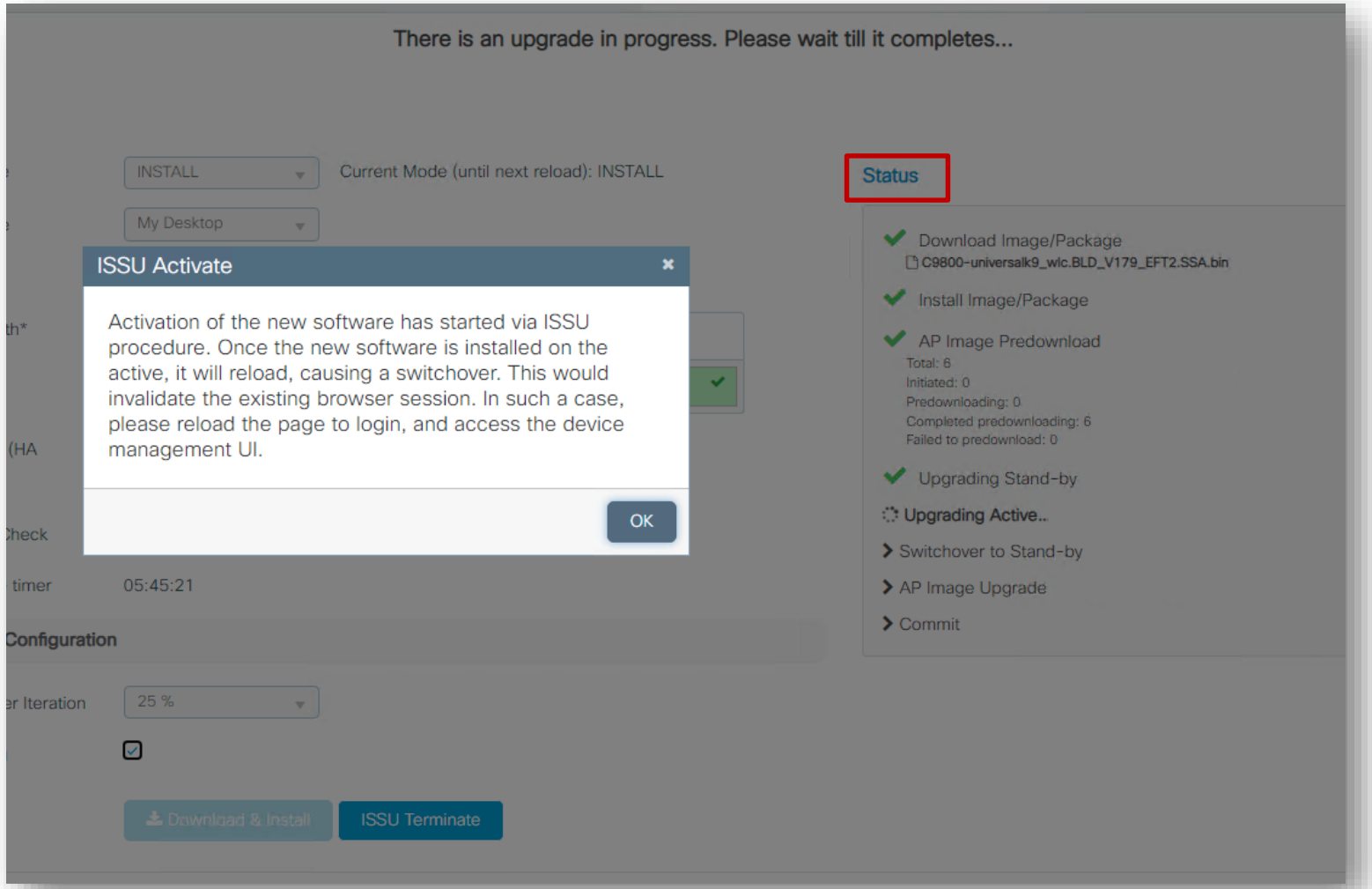


Easy ISSU upgrade with WebUI!



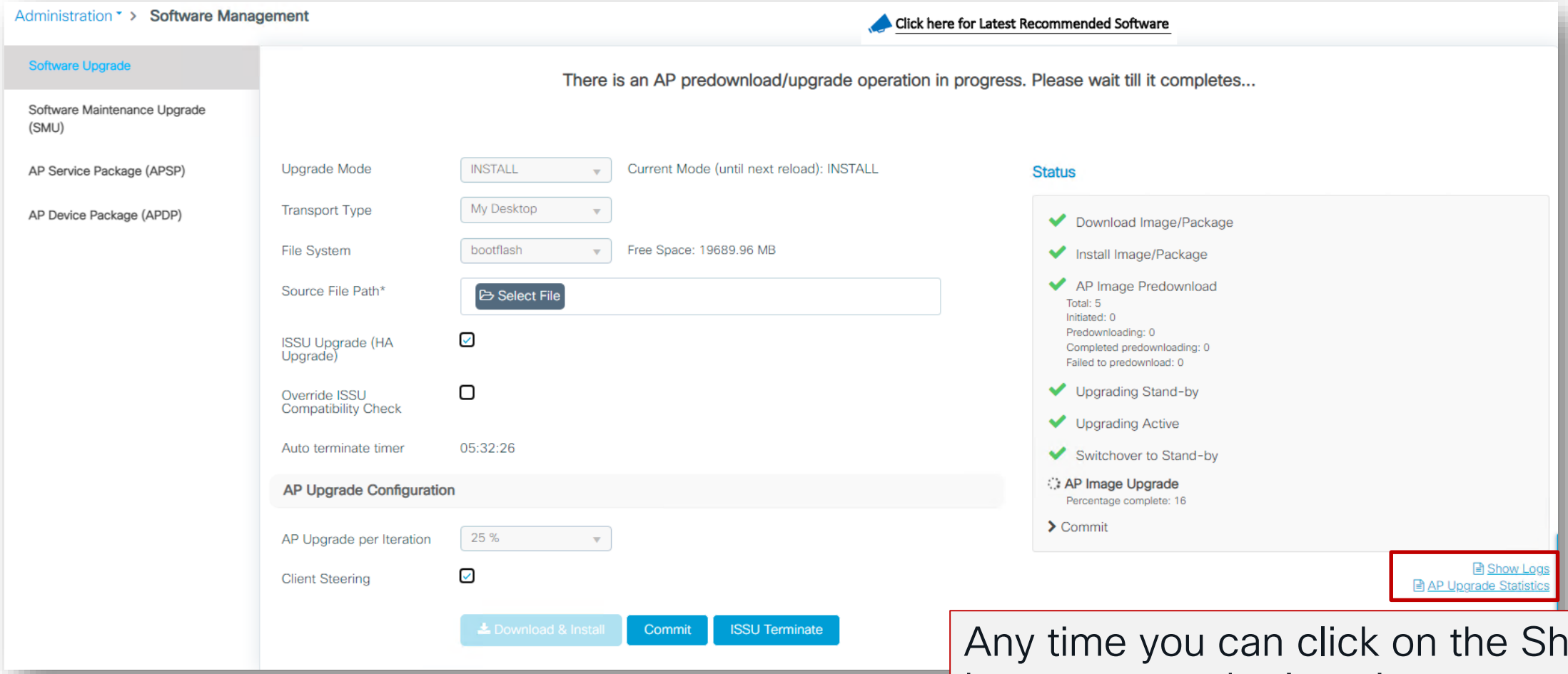
1. Select the image you want to upgrade to
2. Enable ISSU and select % for Rolling AP upgrade
3. Click Download and Install

Easy ISSU upgrade with WebUI!



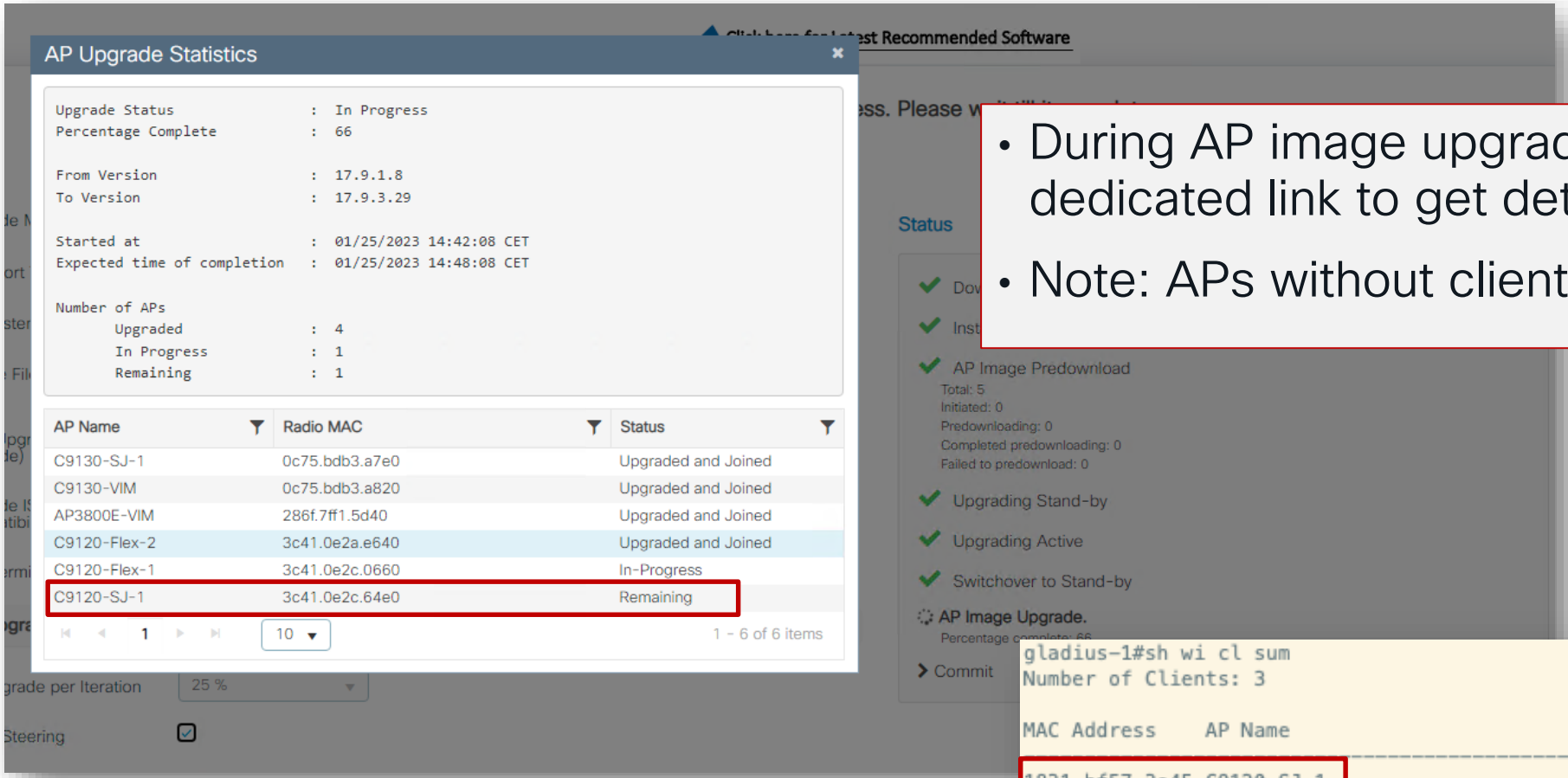
- Monitor the progress of ISSU upgrade via the Status section in GUI
- Any important messages will trigger a popup window

Easy ISSU upgrade with WebUI!



Any time you can click on the Show Logs to see what's going on...

Easy ISSU upgrade with WebUI!



- During AP image upgrade, click on the dedicated link to get detailed information
- Note: APs without clients are upgraded first

```
gladius-1#sh wi cl sum
Number of Clients: 3

MAC Address    AP Name                                  Type ID   State
-------------------------------------------------------------------------
1831.bf57.3e45 C9120-SJ-1                               WLAN 1    Run
4ced.fb3a.d9fe C9120-SJ-1                               WLAN 1    Run
bcec.23c3.6106 C9120-SJ-1                               WLAN 1    Run

Number of Excluded Clients: 0
```

Easy ISSU upgrade with WebUI!

C9120-SJ-1 still not upgraded

`sh ap upgrade`

```
Remaining
---------
Number of APs: 1
AP Name                                  Radio MAC
-----------------------------------------------------
C9120-SJ-1                               3c41.0e2c.64e0
```

- Client steering happens on the AP with clients
- Once all clients are moved the AP is upgraded

Client steering in progress...

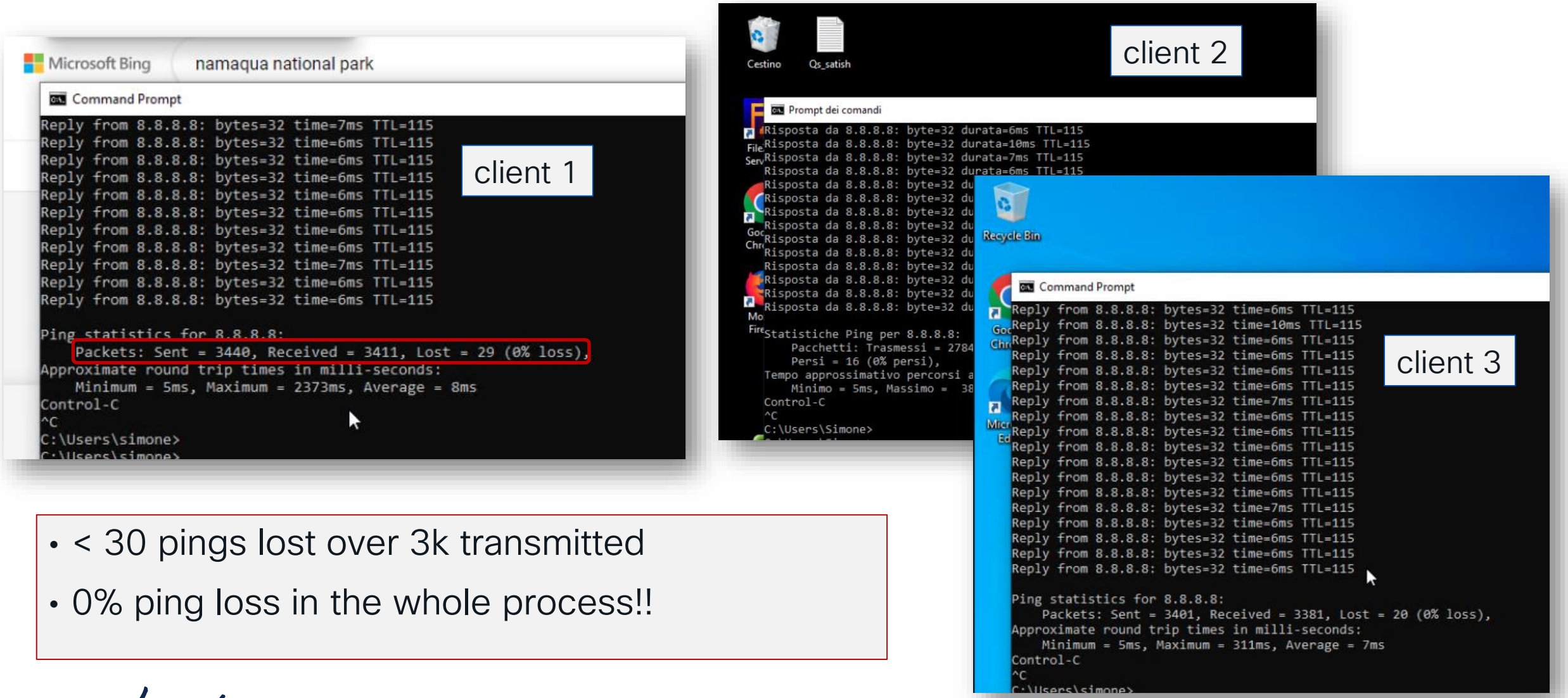
```
gladius-1#sh wi cl summary
Number of Clients: 3

MAC Address    AP Name                                   Type ID   State
-------------------------------------------------------------------------
1831.bf57.3e45 C9120-Flex-2                              WLAN 1    Run
4ced.fb3a.d9fe C9120-SJ-1                                WLAN 1    Run
bcec.23c3.6106 C9120-Flex-2                              WLAN 1    Run
```

```
gladius-1#sh wi cl summary
Number of Clients: 3

MAC Address    AP Name                                   Type ID   State
-------------------------------------------------------------------------
1831.bf57.3e45 C9120-Flex-2                              WLAN 1    Run
4ced.fb3a.d9fe C9120-Flex-2                              WLAN 1    Run
bcec.23c3.6106 C9120-Flex-2                              WLAN 1    Run
```

C9120-SJ-1 upgrade started...

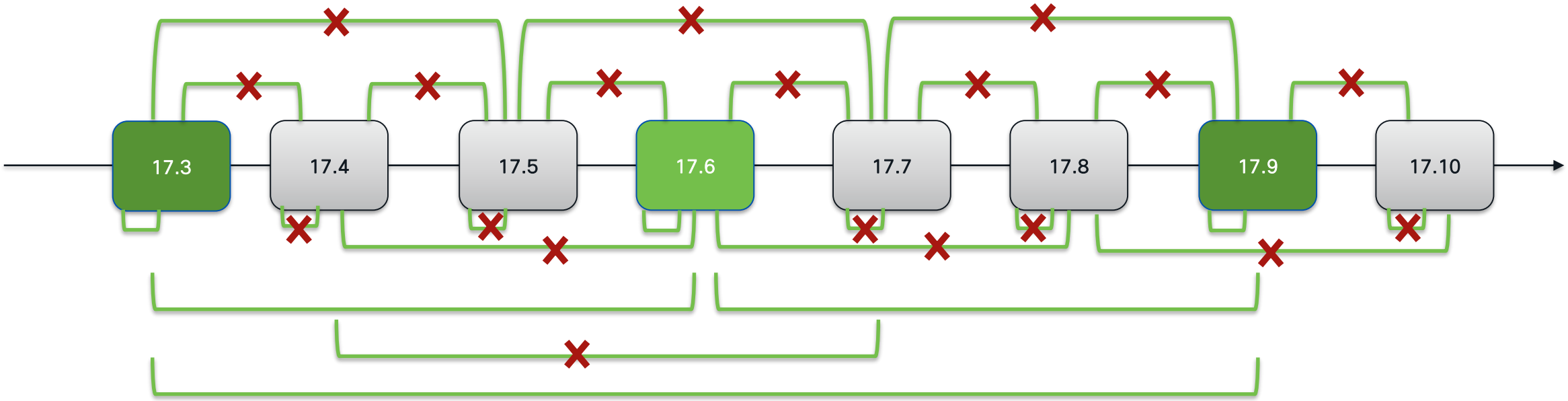
```
In Progress
-----------
Number of APs: 1
AP Name                                  Radio MAC
-----------------------------------------------------
C9120-SJ-1                               3c41.0e2c.64e0

Remaining
---------
Number of APs: 0
AP Name                                  Radio MAC
-----------------------------------------------------
```

Easy ISSU upgrade with WebUI!



- < 30 pings lost over 3k transmitted
- 0% ping loss in the whole process!!

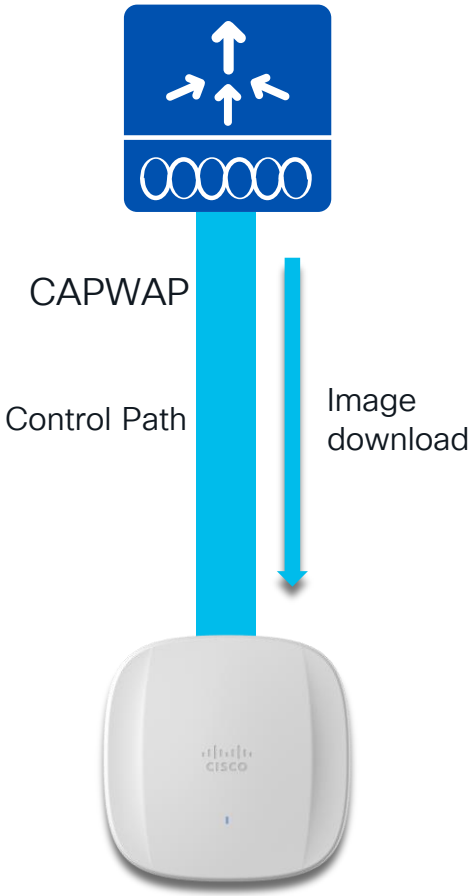
ISSU official support Matrix



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

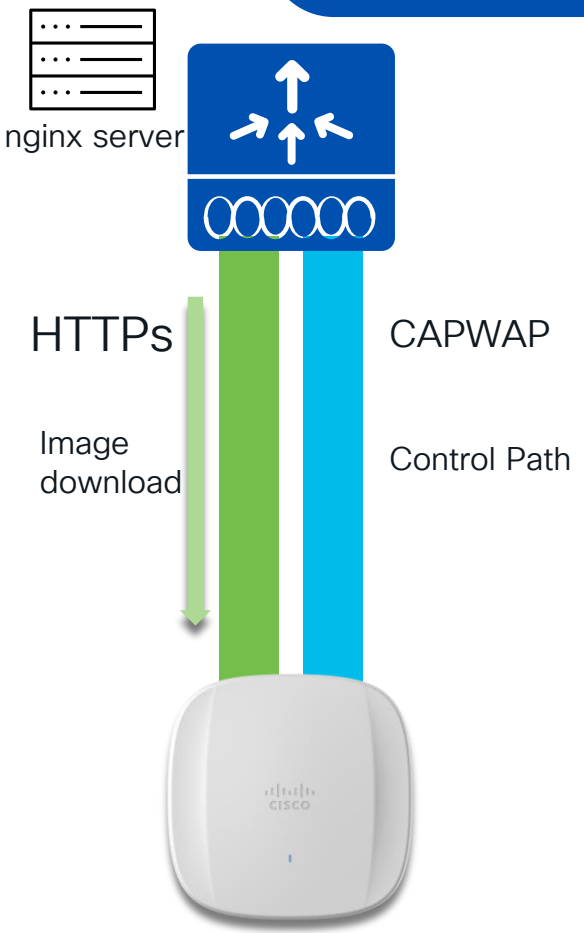
How can I improve AP image download time?

Before IOS XE 17.11.1



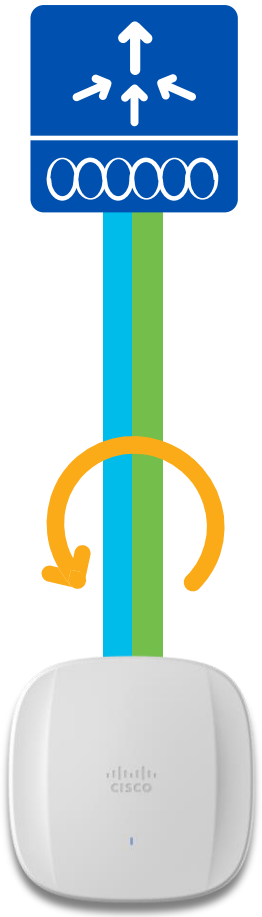
- AP image download happens over CAPWAP Control Path
- Slow by limitation with CAPWAP window size
- Image downloads WNCd process increases CPU work-load

After IOS XE 17.11.1



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

Fallback to CAPWAP if HTTPs Failure



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

Supported Platforms

- All Physical and Virtual Appliances
  - C9800-80, C9800-40, C9800-L, C9800-CL Private and Public Cloud
- Not Supported on:
  - Embedded Wireless Controller on AP

CLI Configuration

- Enable AP image download through HTTPs

```
C9800# conf t
C9800(config)# ap upgrade method https
```

- Customize the HTTPs port number (default is 8443)

```
C9800(config)# ap file-transfer https port <port_number>
```

CLI Verifications

- Verify AP image download method enabled/disabled

```
C9800# show ap upgrade method

 AP upgrade method HTTPS : Disabled
```

- Show command to verify AP file transfer port

```
C9800# show ap file-transfer https summary

  Configured port                 : 8443
  Operational port                : 8443
```

CLI Verifications

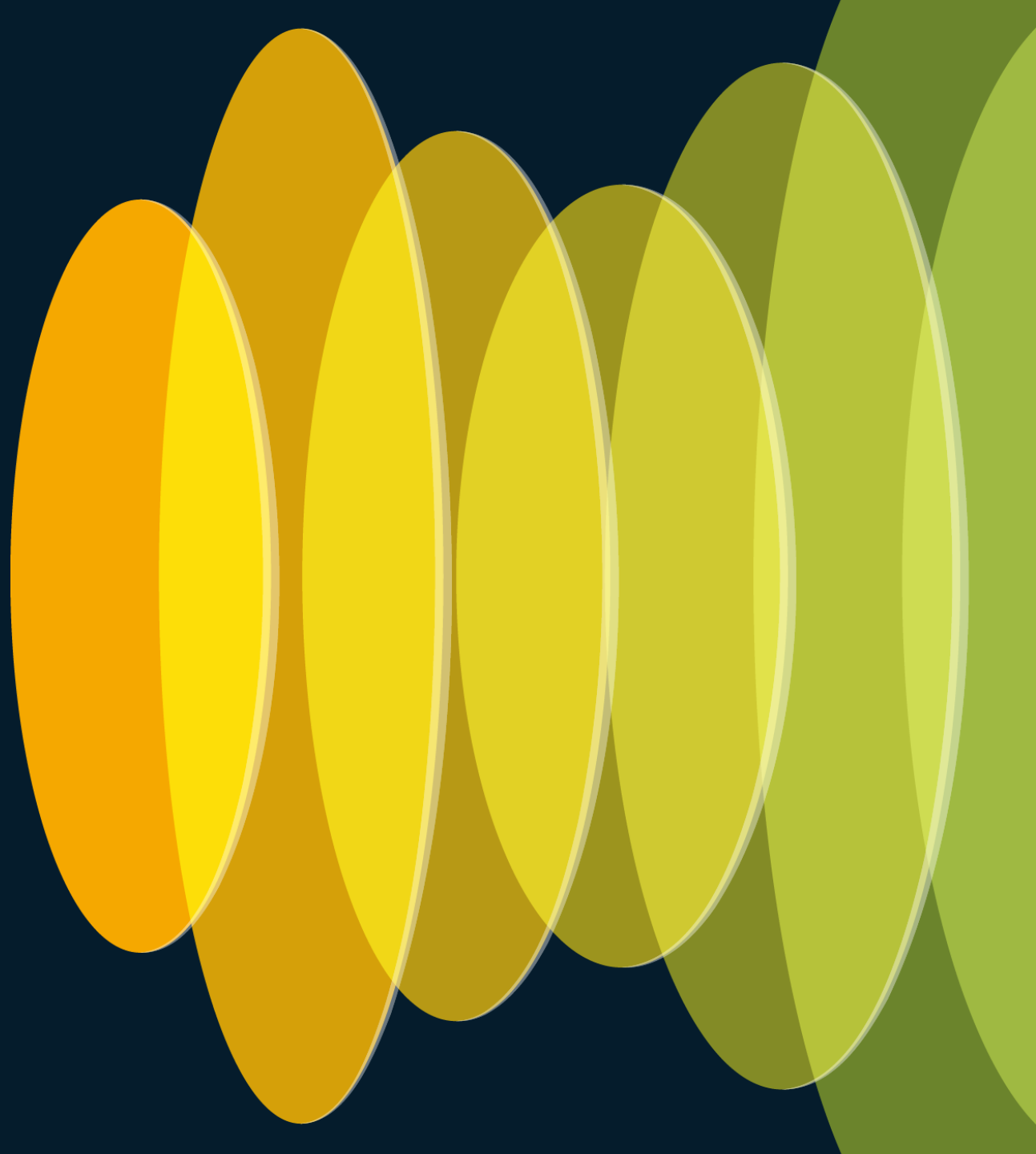
- Verification of ap image download over https support

```
C9800# show ap name AP2800 config general | sec Upgrade

  AP Upgrade Out-Of-Band Capability               : Enabled
```

- Verification of ap image download history

```
C9800# show wireless stats ap image-download

AP image download info for last attempt
AP Name                 Count  ImageSize   StartTime          EndTime            Diff(secs)  Predownload  Aborted              Method
-------------------------------------------------------------------------------------------------------------------------------------
AP_3800_1                1      60856320    11/14/22 12:31:21  11/14/22 12:32:21  59          No           No                   HTTPS
AP2800                   1      60856320    11/14/22 12:27:43  11/14/22 12:28:39  56          No           No                   HTTPS
```

Wireless Controller SMU (Software Maintenance Update)



cisco Live!

Controller SMU

Standalone vs Redundant Wireless Controller

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

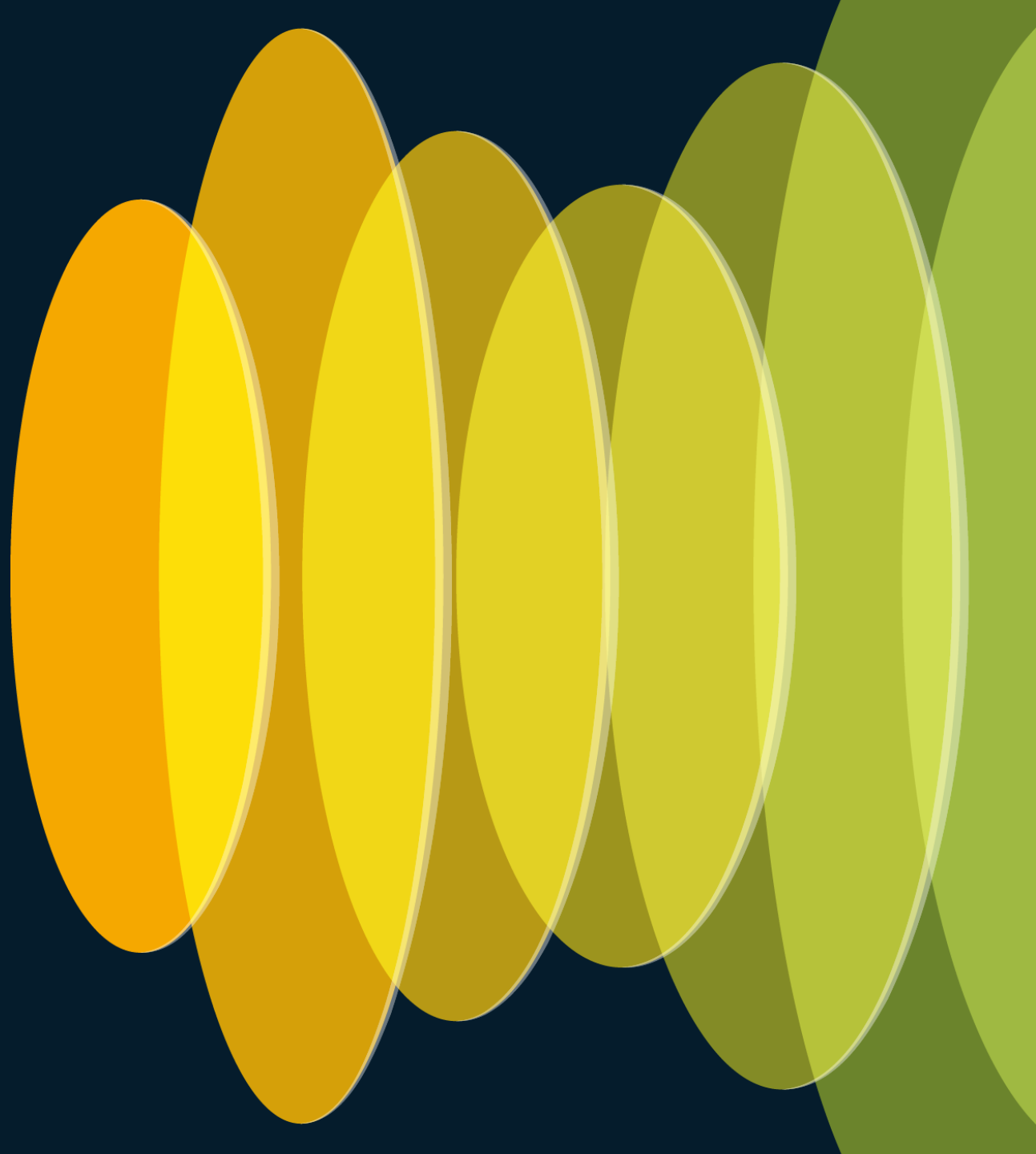
SMU ISSU Install via CLI

```
C9800# install add file flash:C9800-L-universalk9_wlc.17.03.05a.CSCwb45089.SPA.smu.bin
install_add: START Tue Jan 10 15:01:47 PST 2023
install_add: Adding SMU
install_add: Checking whether new add is allowed ....
```

```
C9800# install activate file flash:C9800-L-universalk9_wlc.17.03.05a.CSCwb45089.SPA.smu.bin issu
install_activate: START Tue Jan 10 15:03:37 PST 2023
install_activate: Activating ISSU
```

```
C9800# install commit
install_commit: START Tue Jan 10 15:24:23 PST 2023
install_commit: Committing SMU
```

Per-site & Per-AP Model AP Service Pack



cisco Live!

APSP workflow

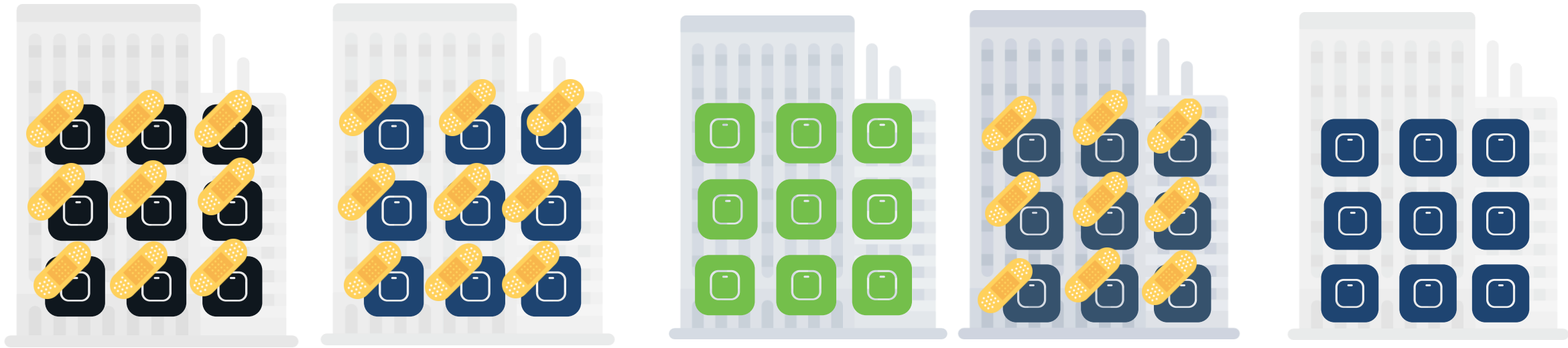
Applying APSP for 9115/9120 APs on per-site and per-model basis

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

Apply on Site A in rolling AP fashion

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

Not applicable for building with 9130AX



9120AX APs 9115AX APs

SiteA

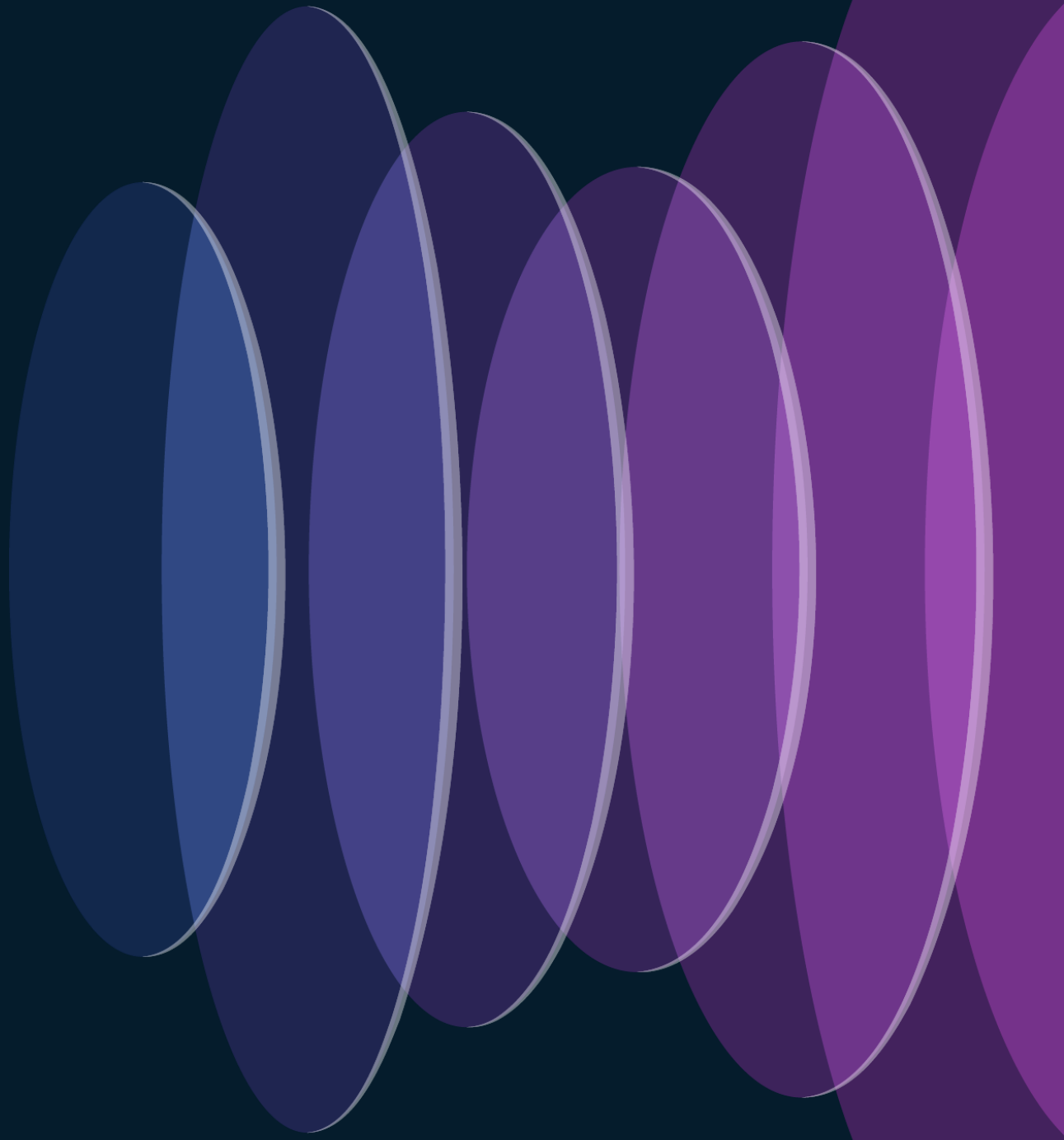
9130AX APs 9120AX APs

SiteB

9115AX APs

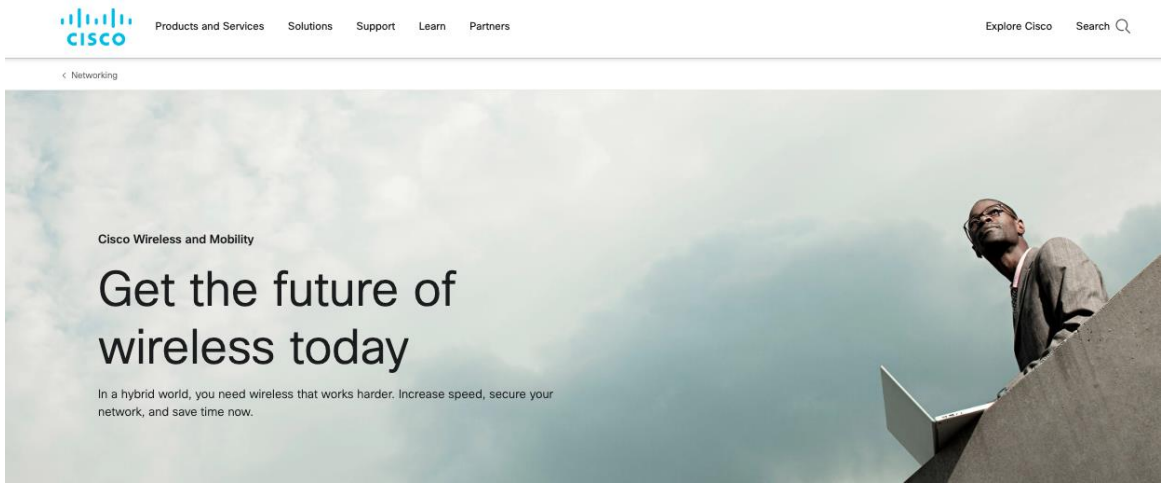
SiteC

More info?



Where can I find more info?

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



Other links on CCO:

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

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 2025.

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

Networking

Secure Wireless Design

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

START

Monday, June 3 | 8:30 a.m.
BRKEWN-2054
Designing the Right Enterprise Wireless Architecture for Challenging Environments (On-Premises, Cloud, and Hybrid)

Monday, June 3 | 10:30 a.m.
BRKEWN-2035
Design your Enterprise Wireless Network with Cisco Meraki

Monday, June 3 | 11:00 a.m.
BRKENS-2834
IPv6-Enabled Wireless (Wi-Fi) Access: Design and Deployment Strategies

Tuesday, June 4 | 10:30 a.m.
BRKEWN-3004
Understanding Wireless Security and the Implications for Secure Wireless Network Design

Wednesday, June 5 | 10:30 a.m.
BRKEWN-2926
Tune Your Cisco Wi-Fi Designs for the Most Demanding Clients and Applications, Boosted with Applied AI

Thursday, June 6 | 9:30 a.m.
BRKEWN-2658
Implement and Troubleshoot Cisco Spaces to Deliver Next-Generation Location-Based Solutions

FINISH

Thursday, June 6 | 1:00 p.m.
BRKEWN-2037
OpenRoaming Under the Hood

Networking

Wi-Fi 6/6E

Learn from experts on wireless topics such as WiFi6 and WiFi6E standards enhancements. You will understand what you need to know about designing for 6GHz, migrating from AireOS to Catalyst 9800 or to Cloud management with Meraki, and what you need to know about 5G and WiFi6E coexistence.

START

Monday, June 3 | 1:00 p.m.
BRKEWN-2087
High-Density Wi-Fi Design, Deployment, and Optimization

Monday, June 3 | 3:00 p.m.
BRKEWN-2339
Catalyst 9800 Configuration Best Practices

Tuesday, June 4 | 1:00 p.m.
BRKEWN-2094
Successfully Configuring Catalyst 9800 Wireless Controllers on Your First Shot

Tuesday, June 4 | 2:30 p.m.
BRKEWN-1107
Cut the Cord: Design Principles to Deliver a Wireless-First Enterprise

Tuesday, June 4 | 3:00 p.m.
BRKEWN-2043
Saving Energy and Money with Your Cisco Wireless Network

Tuesday, June 4 | 3:00 p.m.
BRKOPS-2402
Automate the Deployment of a Wireless Network with the Help of Cisco Catalyst Center

Wednesday, June 5 | 10:30 a.m.
BRKEWN-3413
Advanced RF Tuning for Wi-Fi 6E with Catalyst Wireless: Become an Expert While Getting a Little Help from AI

Wednesday, June 5 | 2:30 p.m.
BRKEWN-2024
Wi-Fi 6E Adoption and a Sneak Peek into the Future with Wi-Fi 7

Wednesday, June 5 | 4:00 p.m.
FINISH
BRKEWN-1538
Internet of Things on the Next Generation Cisco Catalyst Wireless Wi-Fi 6E Access Points

Networking

Wireless Automation & Troubleshooting

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

START

Monday, June 3 | 8:00 a.m.
BRKEWN-2014
Meraki AIOps & Assurance – Optimizing Wireless User Experience at Scale!

Monday, June 3 | 9:30 a.m.
BRKEWN-2029
7 Ways to Save your Wireless OpEx using Catalyst Center AIOps

Tuesday, June 4 | 10:30 a.m.
BRKEWN-2039
Let's Troubleshoot Your Wi-Fi Using Cisco Meraki Wireless

Tuesday, June 4 | 1:00 p.m.
BRKEWN-3007
Demystifying the Role of Applied AI in Your Cisco Wireless Deployments

Tuesday, June 4 | 4:00 p.m.
BRKEWN-2097
Monitoring Cisco Catalyst Wireless with the Meraki Dashboard

Wednesday, June 5 | 2:30 p.m.
BRKEWN-1108
Design, Validate and Certify your Wireless Streaming Telemetry Deployment

Thursday, June 6 | 8:30 a.m.
BRKEWN-3628
Troubleshoot Catalyst 9800 Wireless Controllers

Thursday, June 6 | 10:30 a.m.
BRKEWN-3002
Make a Wireless Engineer's Life Easy by Using Automation to Troubleshoot and Analyze Logs

Thursday, June 6 | 1:00 p.m.
FINISH
BRKEWN-2306
Wireless Network Automation and Assurance with Cisco Catalyst Center


The bridge to possible
Thank you
#CiscoLive

EoS/EoL Update – WLC

Product	End of Sale	EoSW Maintenance	EoVSS	LDOS
Gen 1 AireOS				
2504	18-Apr-2018	18-Apr-2019	18-Apr-2021	30-Apr-2023
5508	4-May-2018	1-Aug-2019	31-Jul-2021	31-Jul-2023
8510	4-Jul-2018	3-Sep-2019	2-Sep-2021	30-Sep-2023
Gen 2 AireOS				
3504	31-Jan-2021	31-Jan-2023	30-Jan-2025	30-Jan-2027
5520	10-Dec-2021	31-Jan-2023	30-Jan-2025	30-Jan-2027
8540	31-Jan-2022	31-Jan-2023	30-Jan-2025	30-Jan-2027
IOS-XE				
9800-L	No plans			
9800-40	No plans			
9800-80	No plans			

EoL = End of Life
EoSW = End of Software Maintenance

EoVSS = End of Vulnerability Software Support
LDoS= Last Day of Support

EoS/EoL Update – Access Points

Product	End of Sale	EoSW Maintenance	EoVSS	LDoS
Wave 1 APs				
1700/2700/3700	30-Apr-2019	29-Apr-2020	30-Apr-2024	
1570	13-Nov-2020	13-Nov-2021	30-Nov-2025	
Wave 2 APs				
1830/1840/1850 and 1540	1-May-2022	1-May-2023	30-Apr-2027	
2800/3800/4800	31-Oct-2022	1-May-2024	31-Oct-2027	
1560	31-Jan-2023	1-May-2024	31-Jan-2028	
Wi-Fi 6 APs				
9117	30-Apr-2021	30-Apr-2022	30-Apr-2026	
9105/9115/9120/9130	No plans			
9124	No plans			

EoL = End of Life
EoSW = End of Software Maintenance
EoVSS = End of Vulnerability Software Support
LDoS= Last Day of Support