

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC





Catalyst 9800 Configuration Best Practices

Ric Beeching, Solutions Engineer
BRKEWN-2339

Cisco Webex App

Questions?

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

How

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

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



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

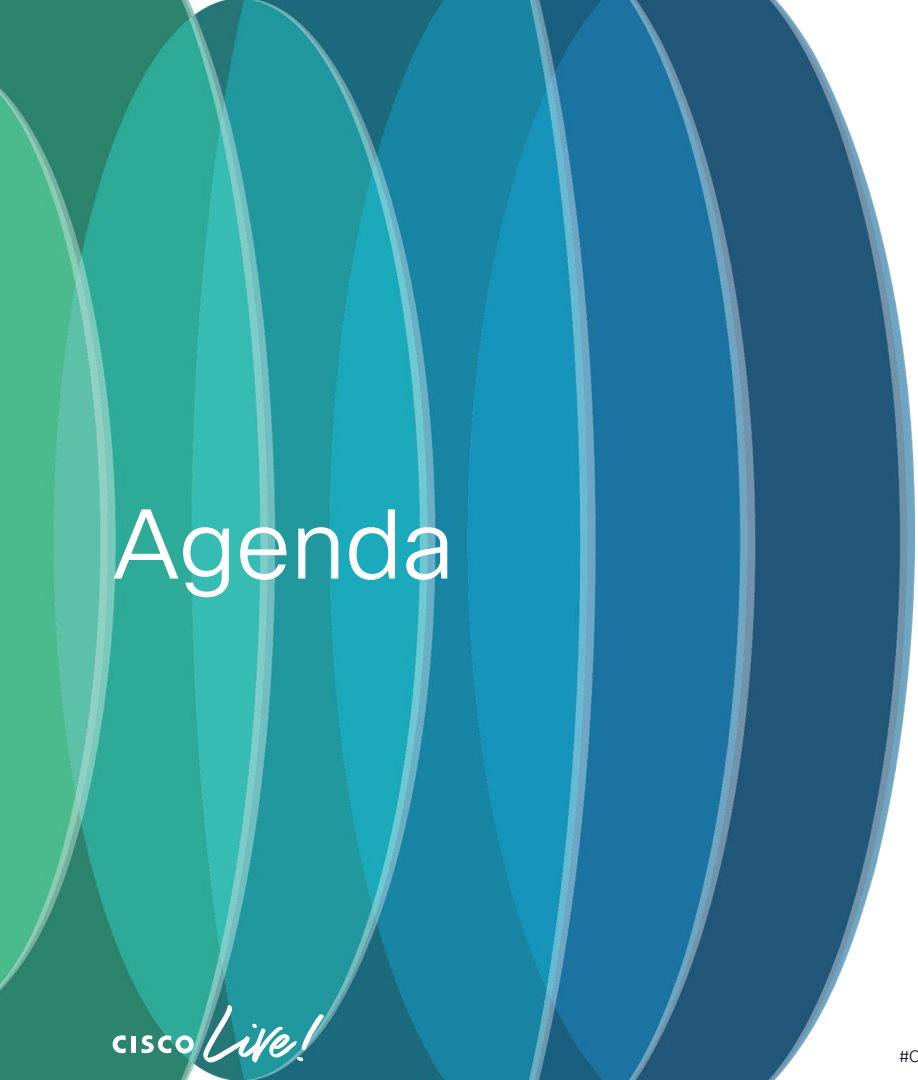




Ric Beeching

Solutions Engineer



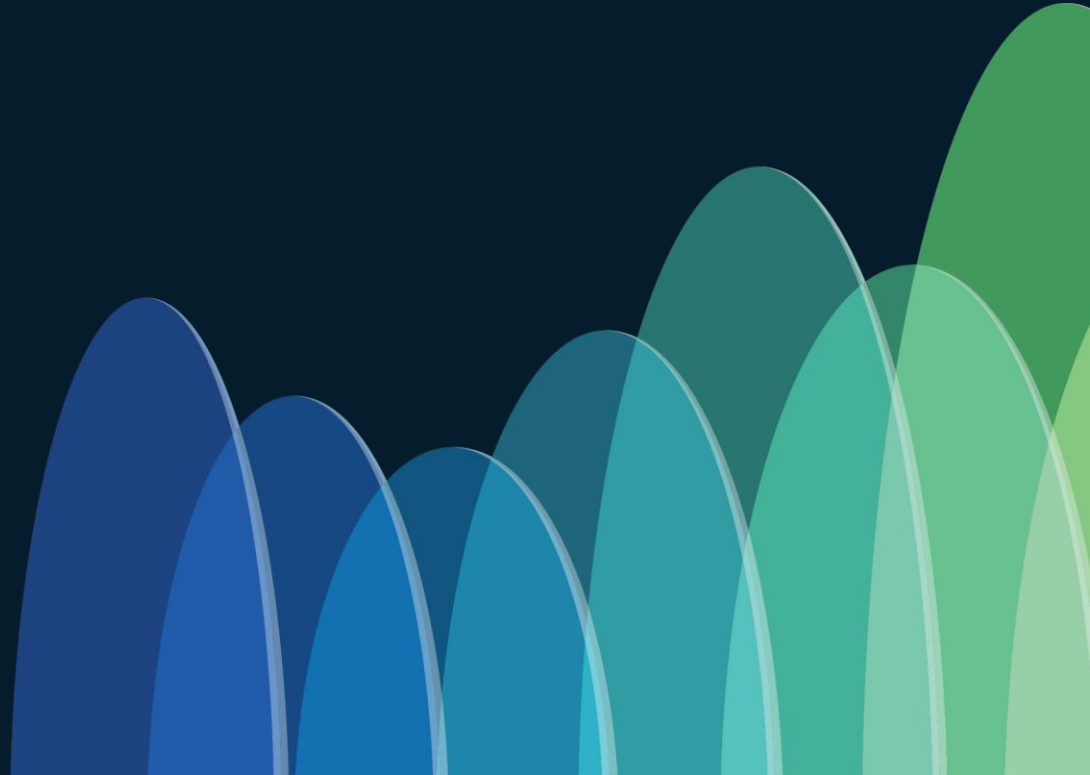


Agenda

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

Day 0

CISCO *Live!*

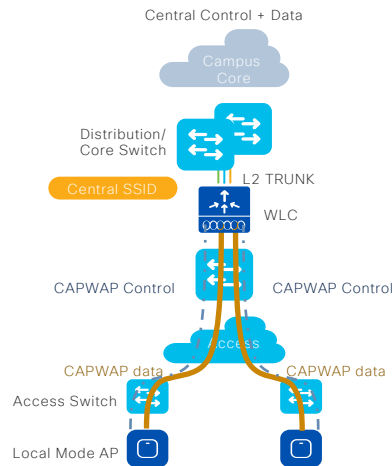


Cisco Catalyst 9800 On-Prem Deployment

Wireless deployment options

On-prem design

Centralised Design

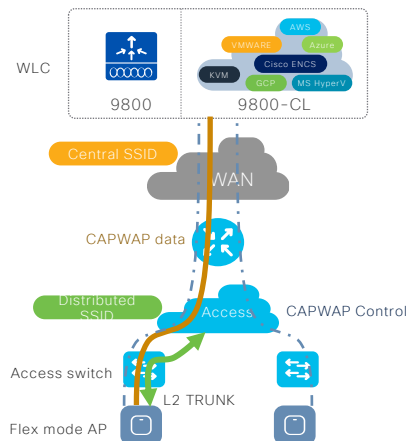


Local mode

- 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

Distributed Design

Central Control | Distributed Data (802.1Q) or centralised

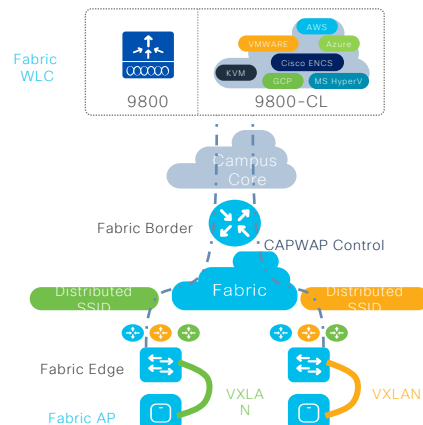


FlexConnect

- 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 centralised via CAPWAP
- Roaming limited to APs in a Flex domain

SDA

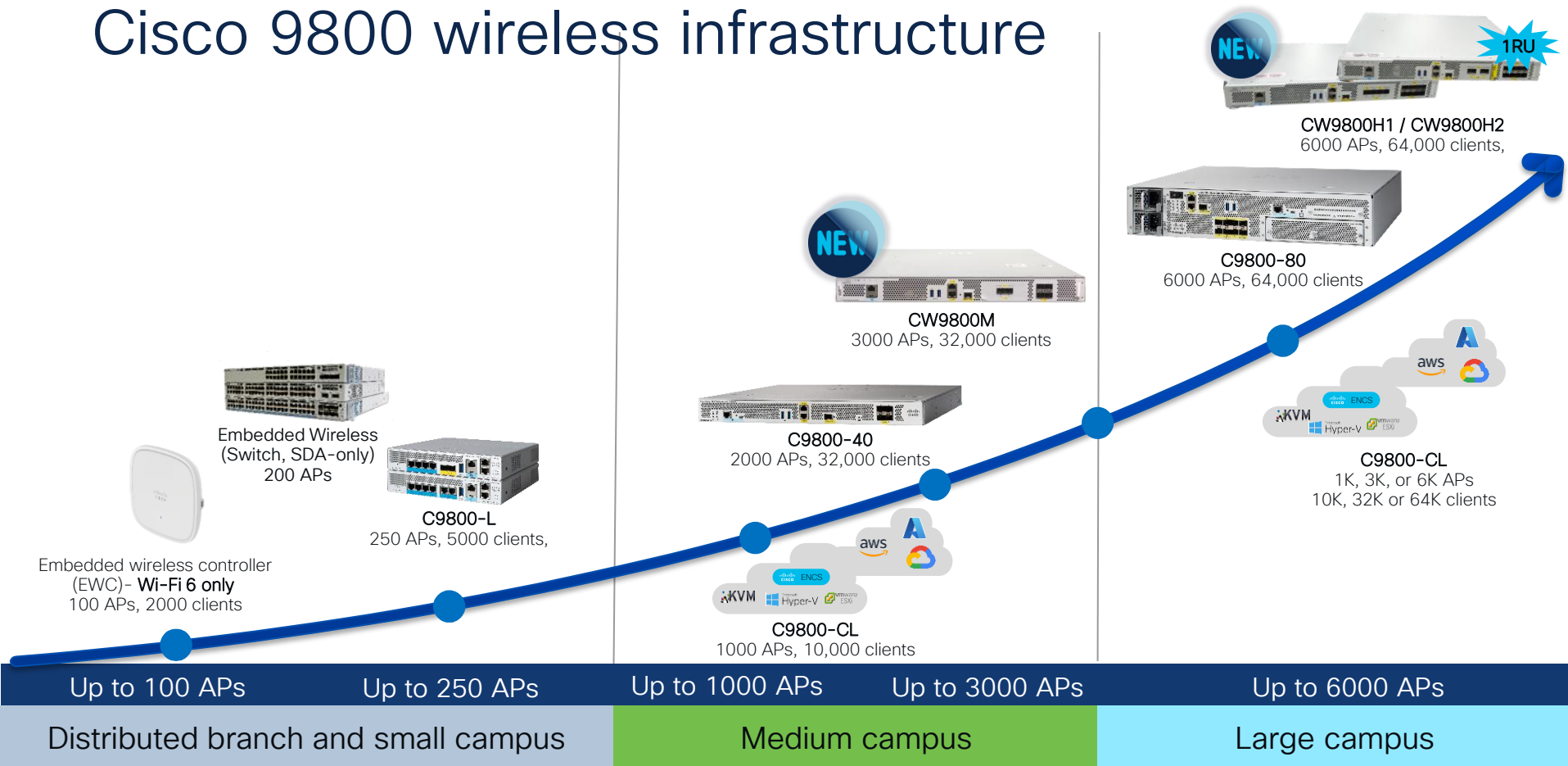
Central Control | Distributed Data (802.1Q)
Cisco Catalyst Center and Cisco ISE



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

Cisco 9800 wireless infrastructure



Cisco Catalyst CW9800H1 & CW9800H2 Wireless Controllers



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

Up to 100 Gbps Backhaul

64,000 Clients

6,000 APs

1RU

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

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

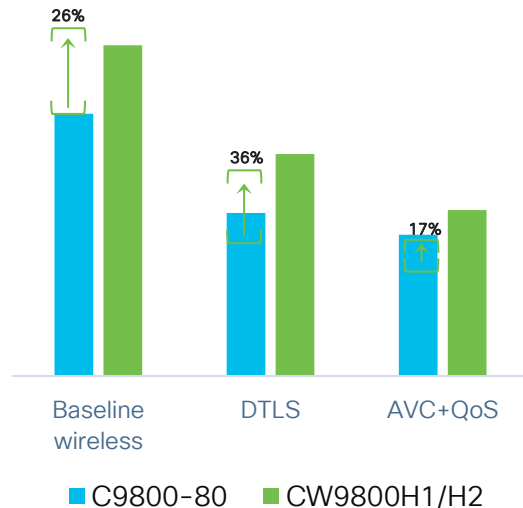
Secure

- 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

Throughput



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

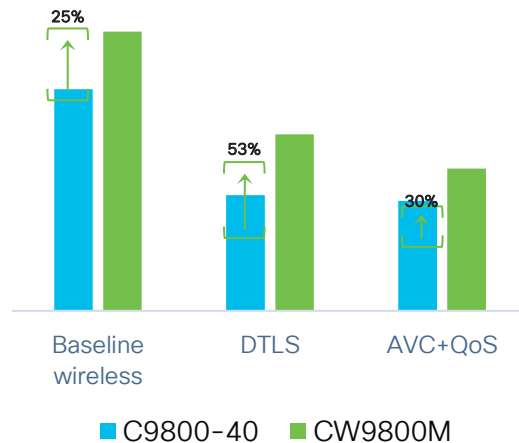
Secure

- 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

Throughput



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



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:

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

no more gold star for 17.6 →



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



Go with 17.15.x:

- If you need support for the new CW9800H and CW9800M WLCs
- [17.15.x](#) Does not support [W1 APs](#)
- [17.15.1](#) released in April 24 and it's the gold star candidate

No gold star release yet →



Controller Settings



Wireless management interface

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

Configuration > Interface > Wireless

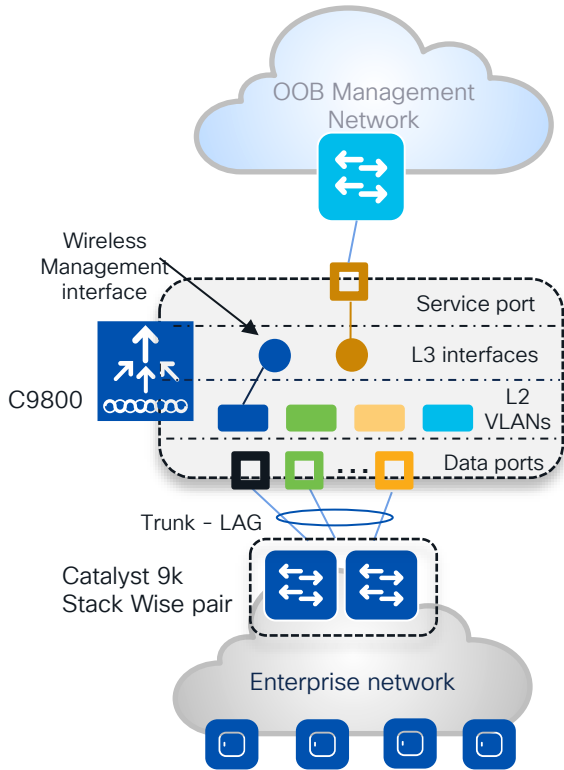
[+ Add](#) [× Delete](#)

	Interface Name	Interface Type	VLAN ID	IP Address	IP Netmask	MAC Address	NAT-IP Address	Configured Trustpoint
☐	Vlan110	Management	110	10.10.110.1	255.255.255.0	001e.e5b3.67ff	0.0.0.0	justloo_9800CL_WLC_TP

10

1 - 1 of 1 items

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:

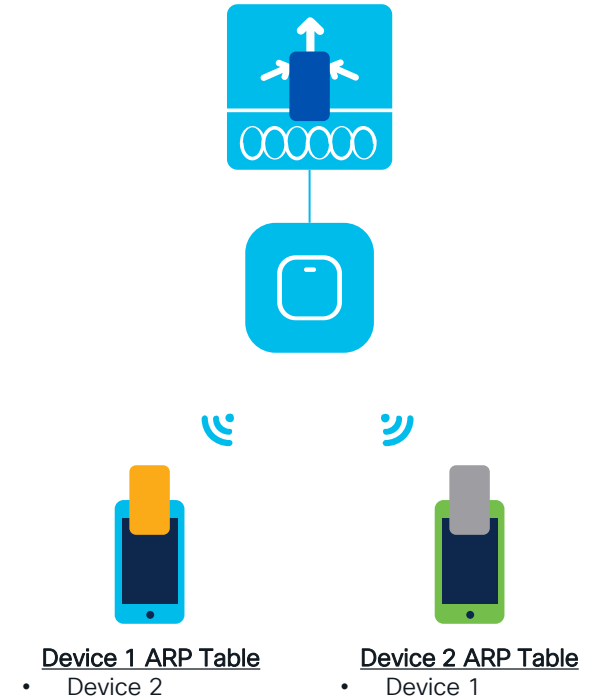
- Switch Virtual Interface (**SVI**) for **wireless management interface** is recommended.
- Do not configure SVIs for client VLANs**, unless really needed (e.g., DHCP relay) – this is different from AireOS where Dynamic interface is required.
- Connect the **uplink ports in a port-channel**, configured 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 behaviour**
 - 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

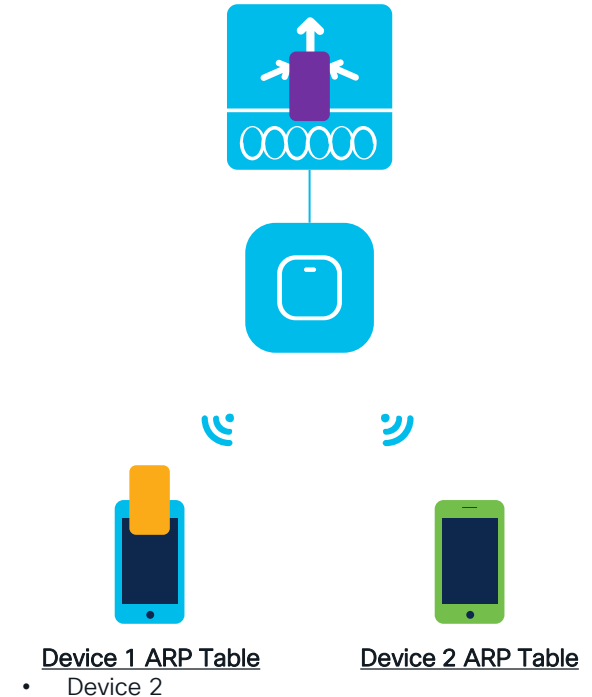
```
C9800# conf t
C9800(config)# wireless profile policy <name>
C9800(config-wireless)# ipv4 arp-proxy
```



Best practice – address resolution protocol (ARP) proxy

- **Default behaviour**
 - 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
```



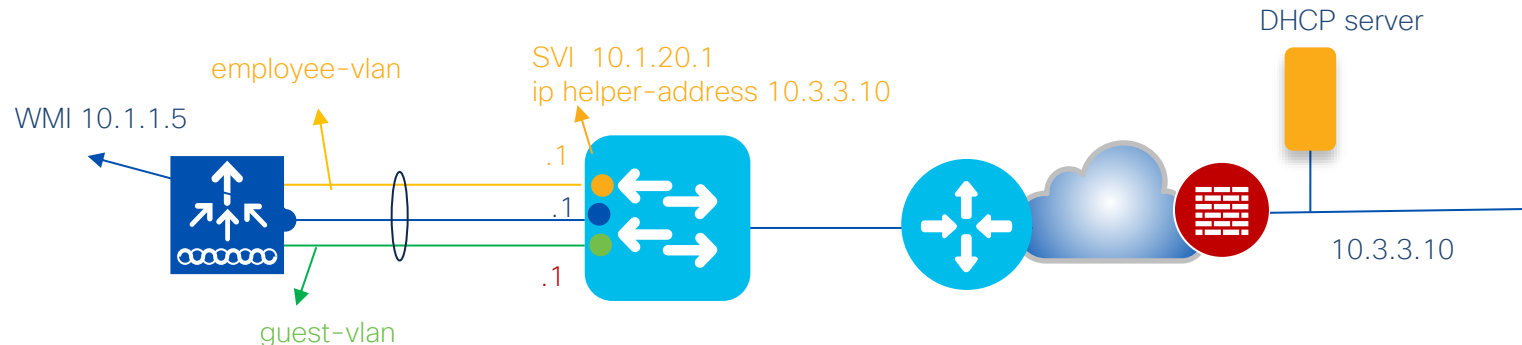
Best practice – DHCP proxy/relay

- **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

Edit SVI: Vlan210

General **Advanced**

IPv4 Outbound ACL None

IPv6 Inbound ACL None

IPv6 Outbound ACL None

DHCP Relay

IPv4 Helper Address xxx.xxx.xxx.xxx +

172.16.3.10 ×

Relay Information Option DISABLED

Subscriber Id

Server Id Override DISABLED

Option Insert DISABLED

Source-Interface Vlan Vlan201

- 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
```

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)

Administration > Management > HTTP/HTTPS/Netconf/VTY

HTTP/HTTPS Access Configuration

1	HTTP Access	☐ DISABLED
2	HTTPS Access	☒ ENABLED
	HTTPS Port	443
	Personal Identity Verification	☐ DISABLED
	Authentication	local

HTTP Trust Point Configuration

	Enable Trust Point	☒ ENABLED
3	Trust Points	Wireless-TME-new

Enable secure web management access

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

Configuration ▾ > Wireless ▾ > Wireless Global

Default Mobility Domain *	<input type="text" value="default"/>
RF Group Name*	<input type="text" value="default"/>
Maximum Login Sessions Per User*	<input type="text" value="0"/>
4 Management Via Wireless	☐
Device Classification	☒

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
```

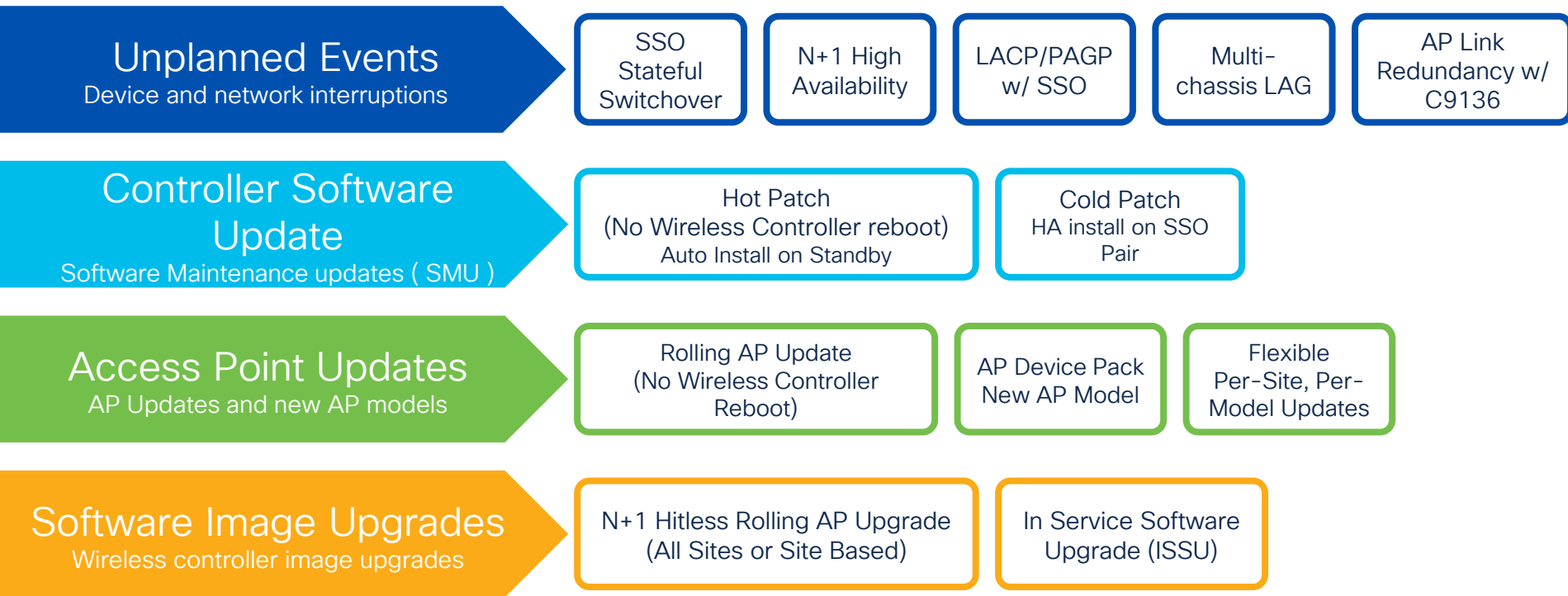
Note: There is no mechanism to decrypt passwords.

High Availability

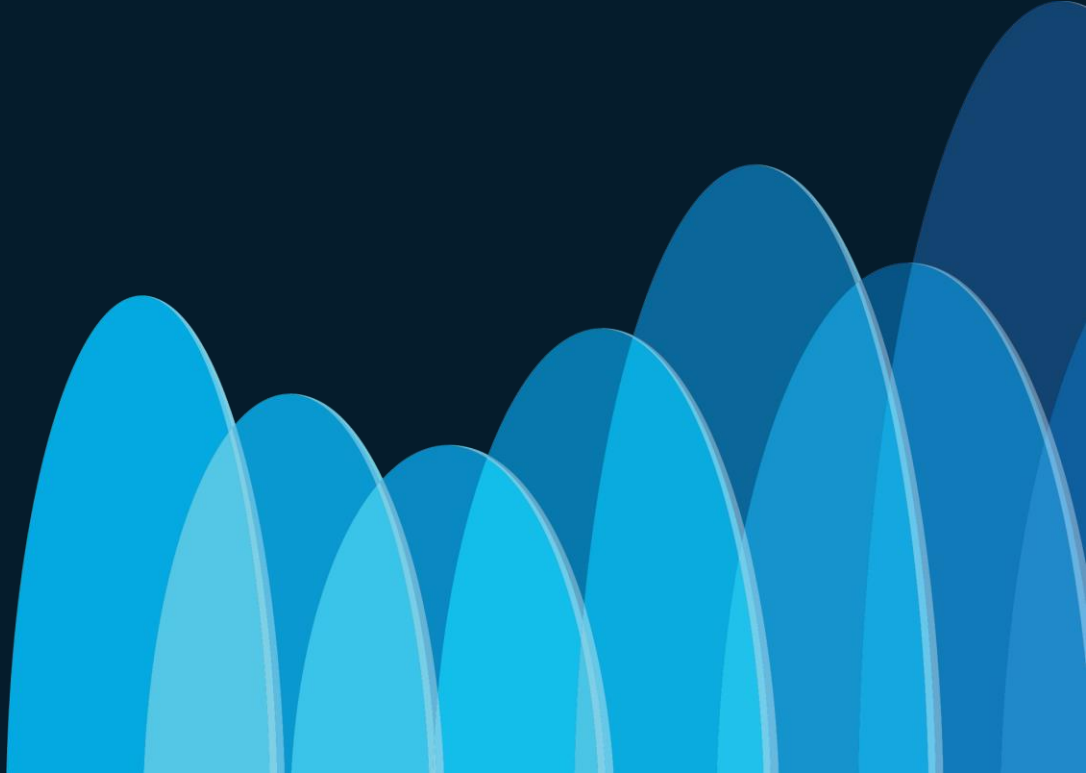


High Availability

Reducing downtime for Upgrades and Unplanned Events

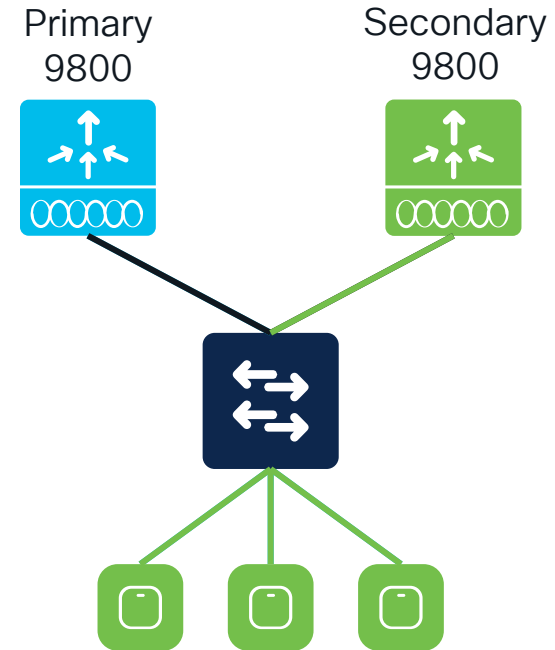


N+1 Redundancy



N+1 redundancy

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



AP failover takes ~45-60 seconds

N+1 best practices



Primary and secondary WLC should run the same software version → No AP image download



Configurations should be consistent across the primary, secondary, and tertiary controllers (Use Cisco Catalyst Center to automate)

WLANs

Profiles and Policies

Mobility Group

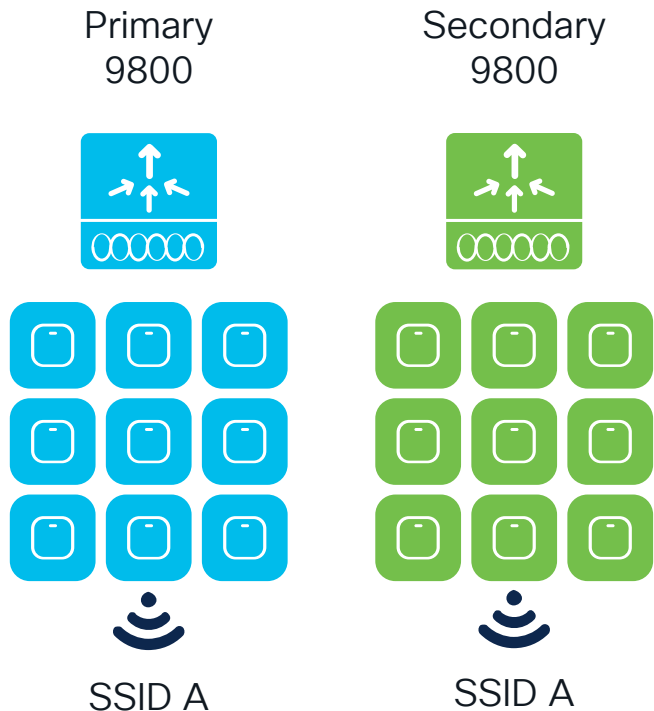
Policy Tag

Site Tag

RF Tag

AP-to-Tag Mappings

N+1 best practices: saving AP to tag mappings



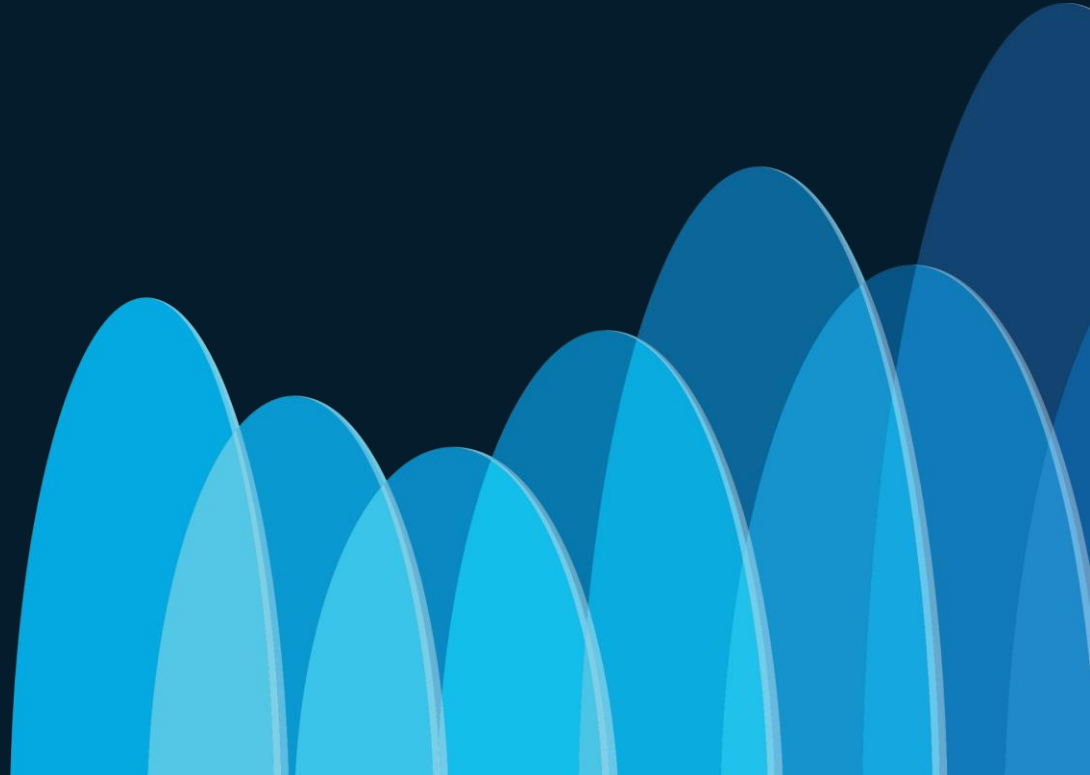
Define tag mappings via static mappings or REGEX based on AP name / location

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

Pre-17.6.1: Manually write the tags to each AP

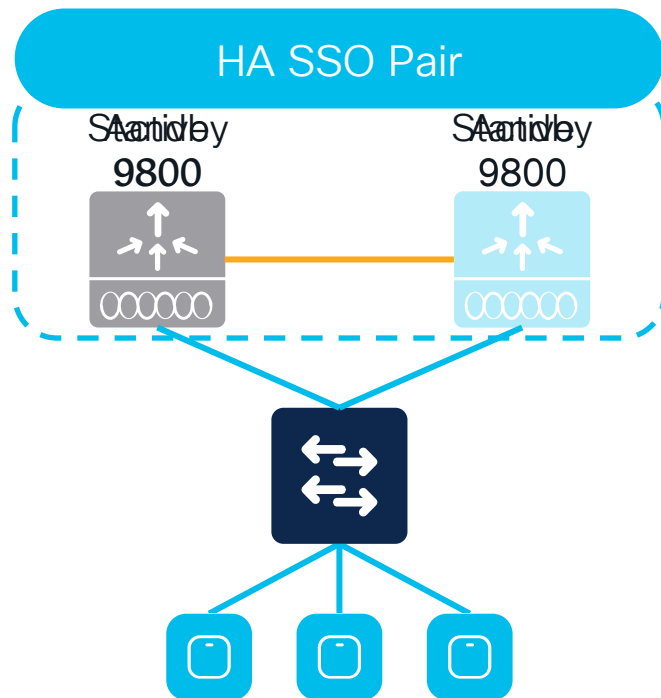
17.6.1 and Later: Automatically write tags to the APs via AP Tag Persistence

High Availability Stateful Switchover (HA SSO)



High availability stateful switchover (HA SSO)

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



AP failover takes order of sub seconds

SSO best practices

Forming SSO pair

Appliance type

- Physical Appliances: Use exact same hardware model
 - C9800-L-C cannot pair with C9800-L-F
- C9800-CL Private Cloud: Pick same scale (large, medium, or small) and throughput (normal or high) template for both VMs

Software

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

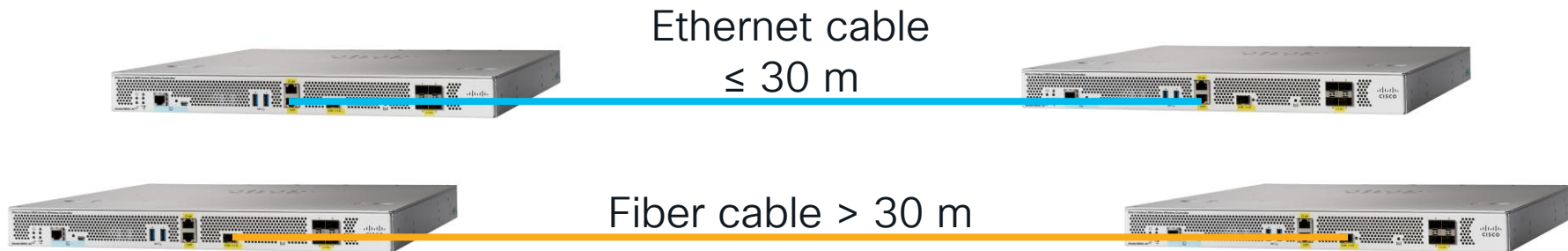
Configurations

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

SSO best practices

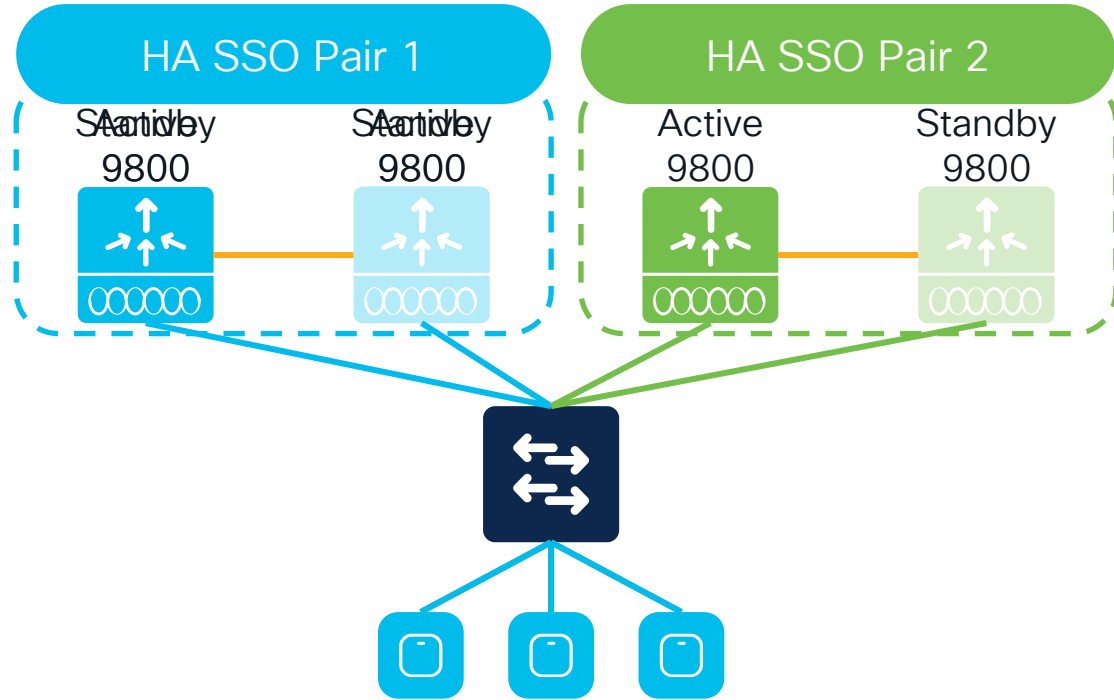
Back-to-back redundancy port connections

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

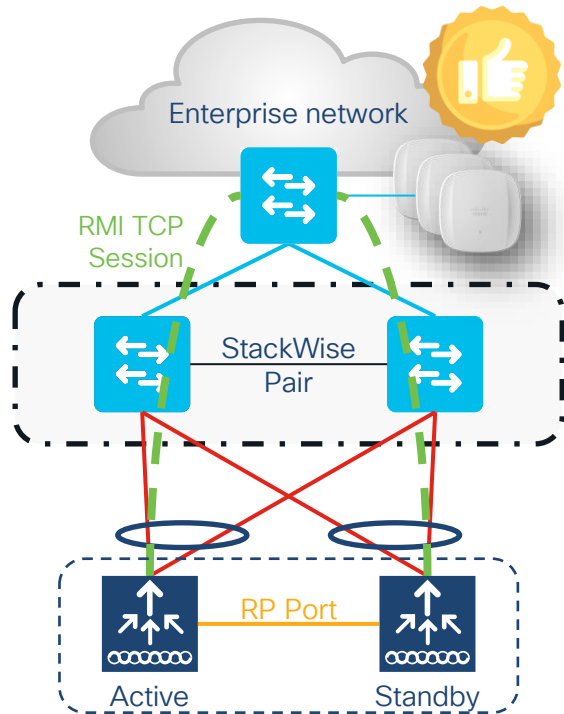


Redundancy with HA SSO and N+1

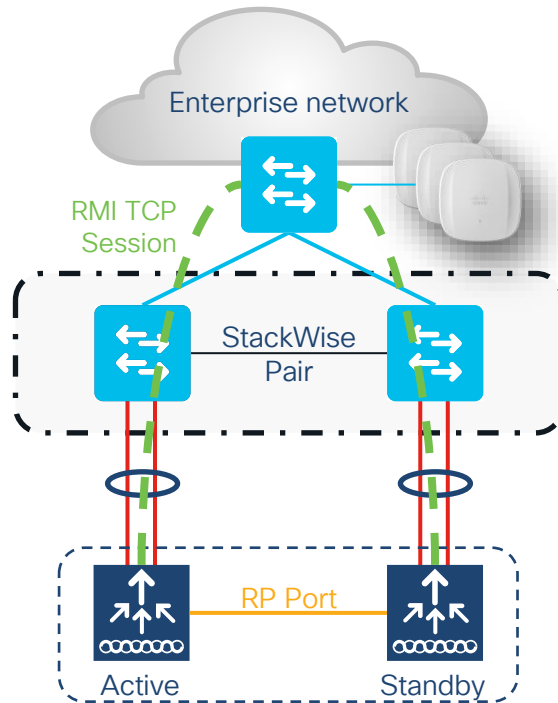
- Highest redundancy model
- Take advantage of sub-second failover
- Redundancy in the event SSO new-active fails before the old-active is recovered
- Hitless upgrades for non-ISSU releases



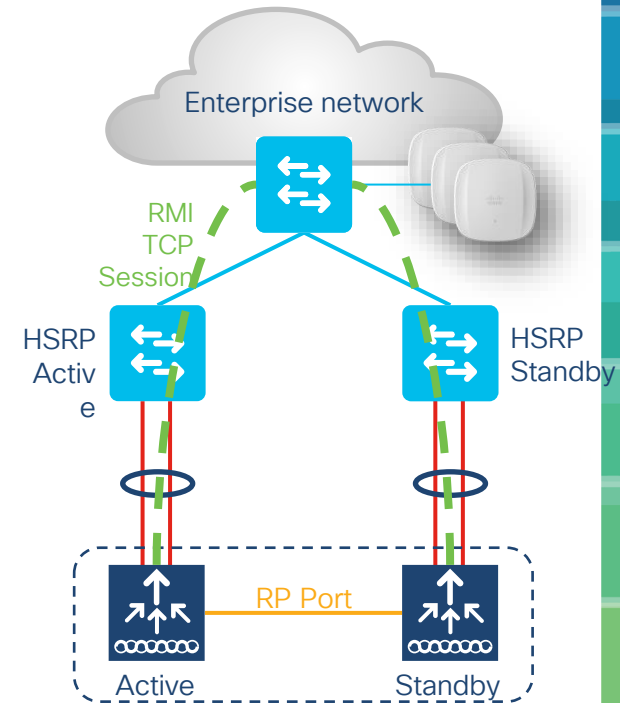
Connecting WLCs to rest of network



StackWise Pair with Split links



StackWise Pair without Split links



HSRP

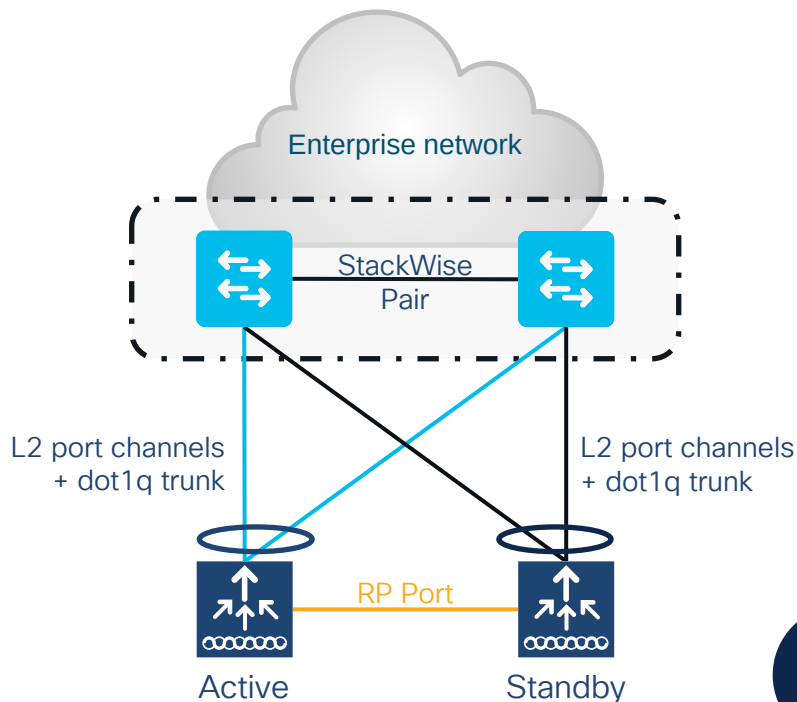
Note: RP can be connected back-to-back or via L2 switches

StackWise pair with split links

SSO HA Pair



Recommended



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

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

Wi-Fi 6E: What's the Impact on Migration?

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



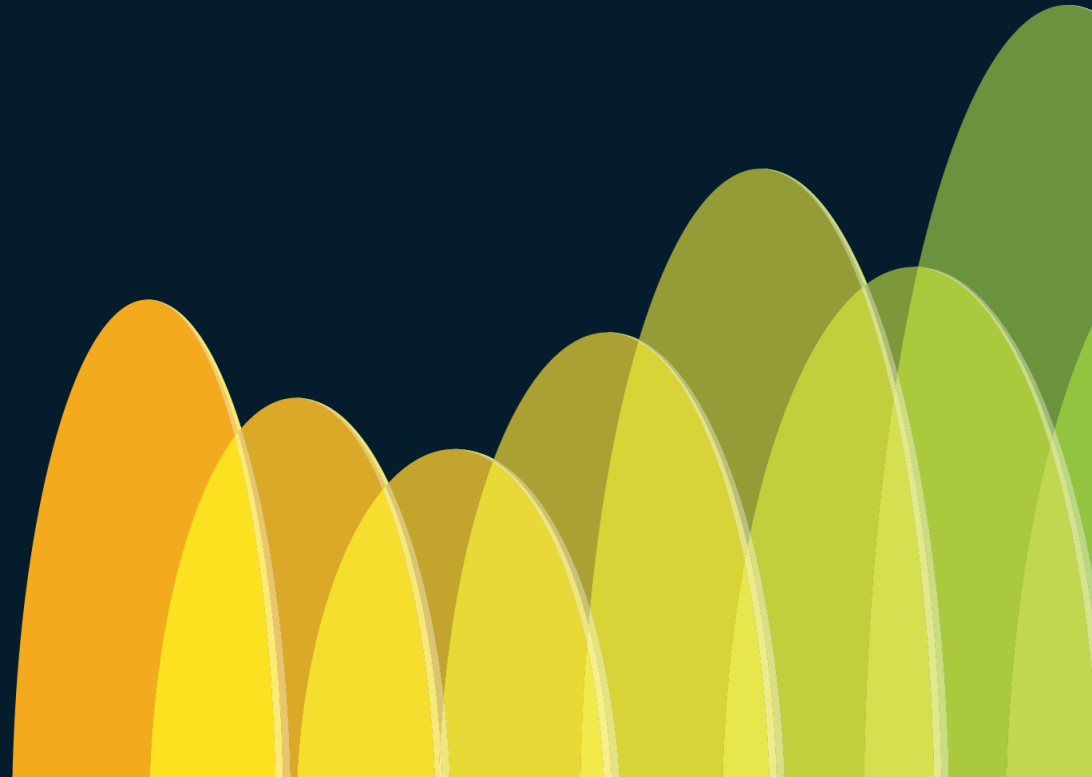
Indoor access points

Outdoor access points

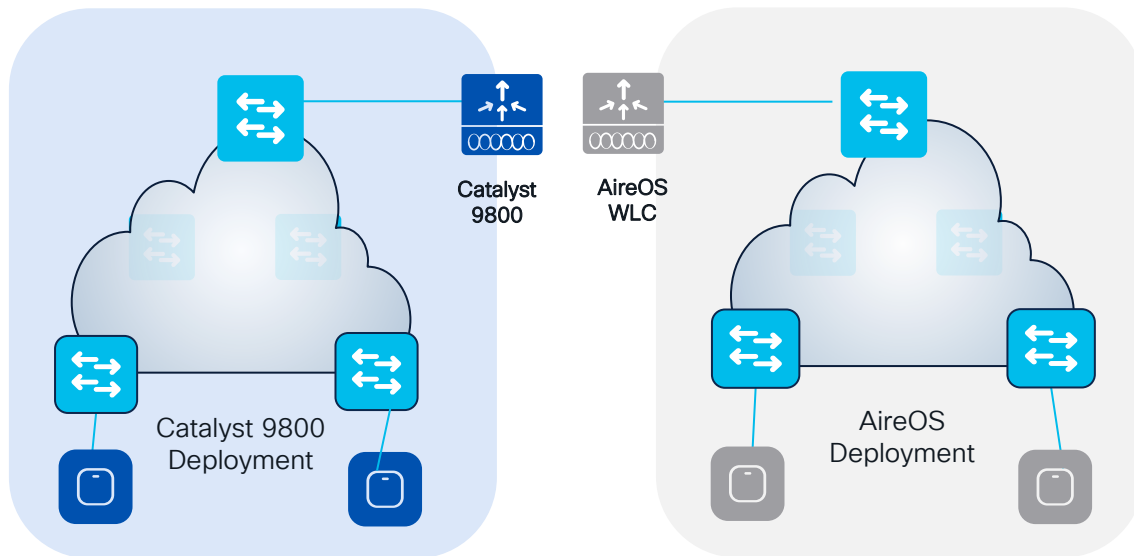
CISCO *Live!*

 Management mode can be changed

What if I Still Have Older Controllers?



AireOS and IOS-XE coexistence



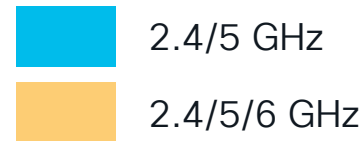
Primary questions:

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

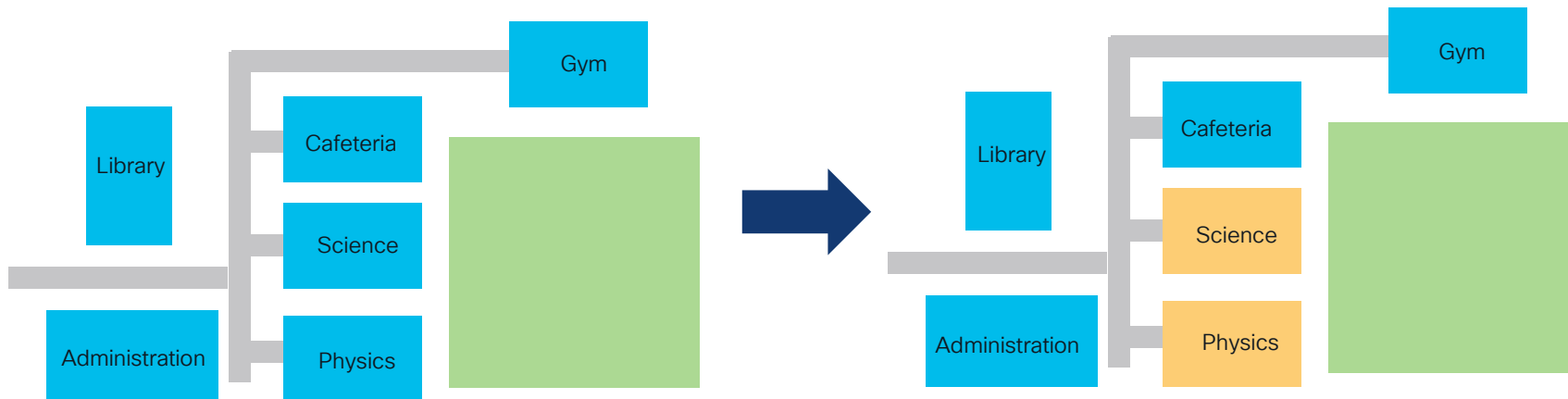
Inter Release Controller Mobility (IRCM) is your friend!

RRM = Radio Resource Management

Customer migration scenario



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

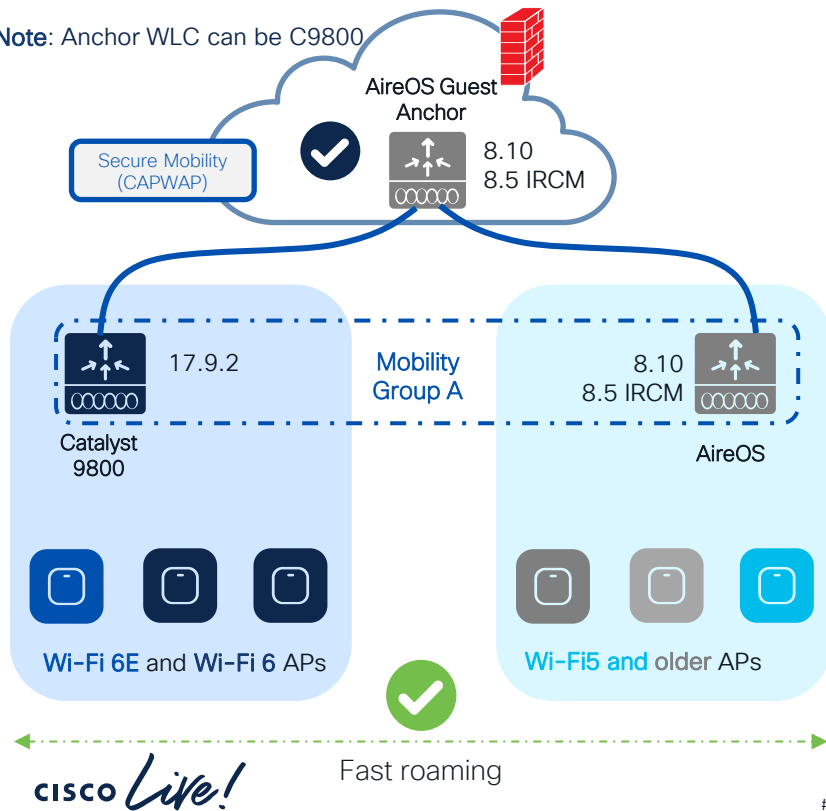


Avoid “Salt & Pepper” deployments. Do not mix APs on different WLCs at the same time.

How do I start adopting 6GHz?

Answer: Inter Release Controller Mobility (IRCM)

Note: Anchor WLC can be C9800

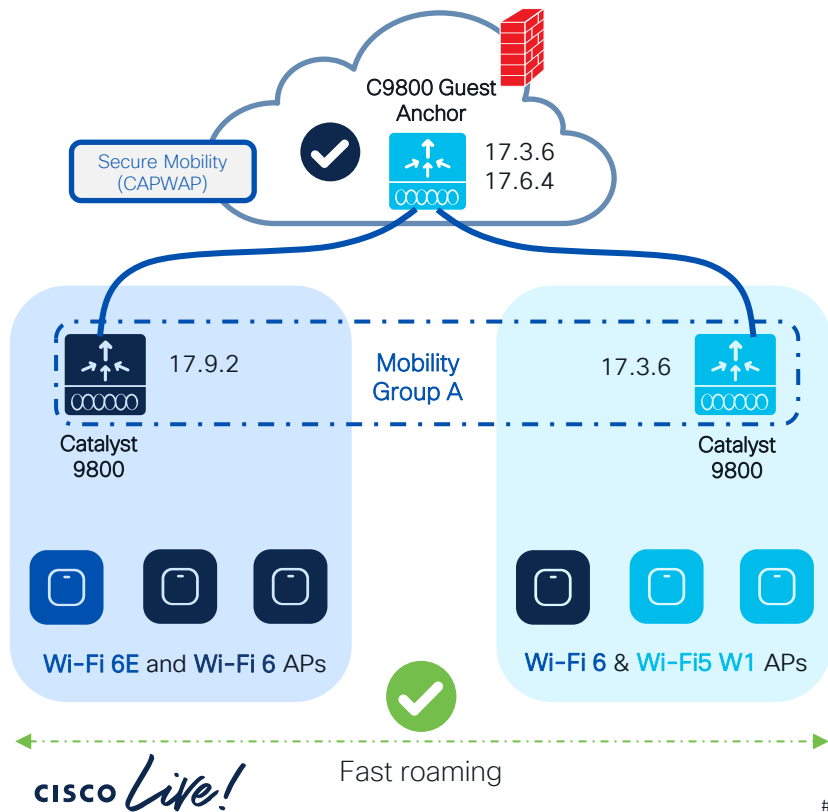


Scenario 1: AireOS WLC supports IRCM

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

How do I start adopting 6GHz?

Answer: Inter Release Controller Mobility (IRCM)



Scenario 2: Catalyst network with W1 APs

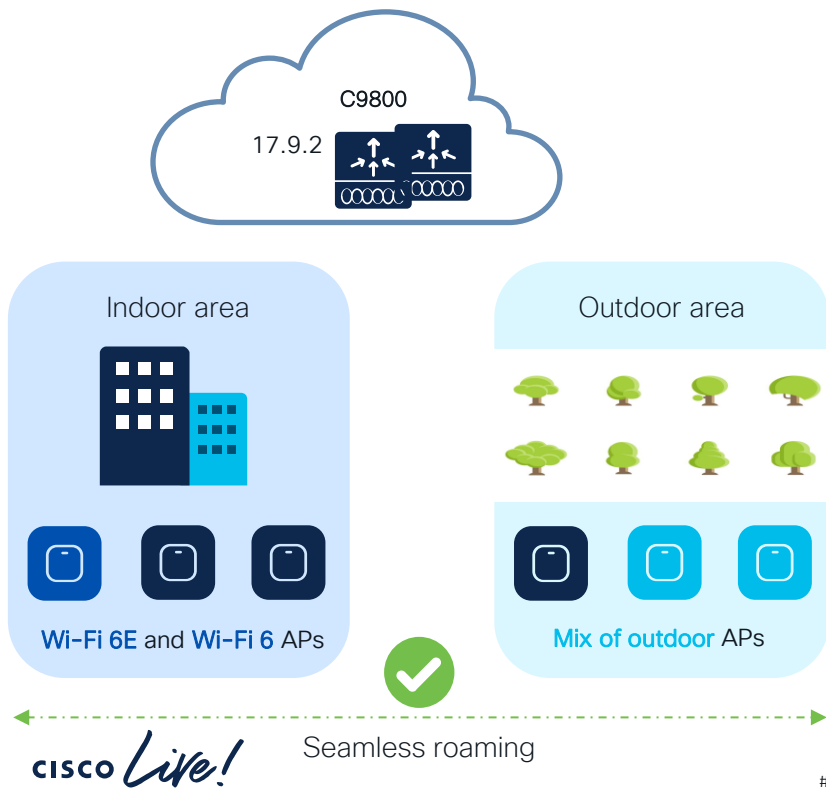
If you have already started your C9800 journey but Wave 1 APs are still present (1700/2700/3700).

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

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

How do I start adopting 6GHz?

What about outdoor areas?

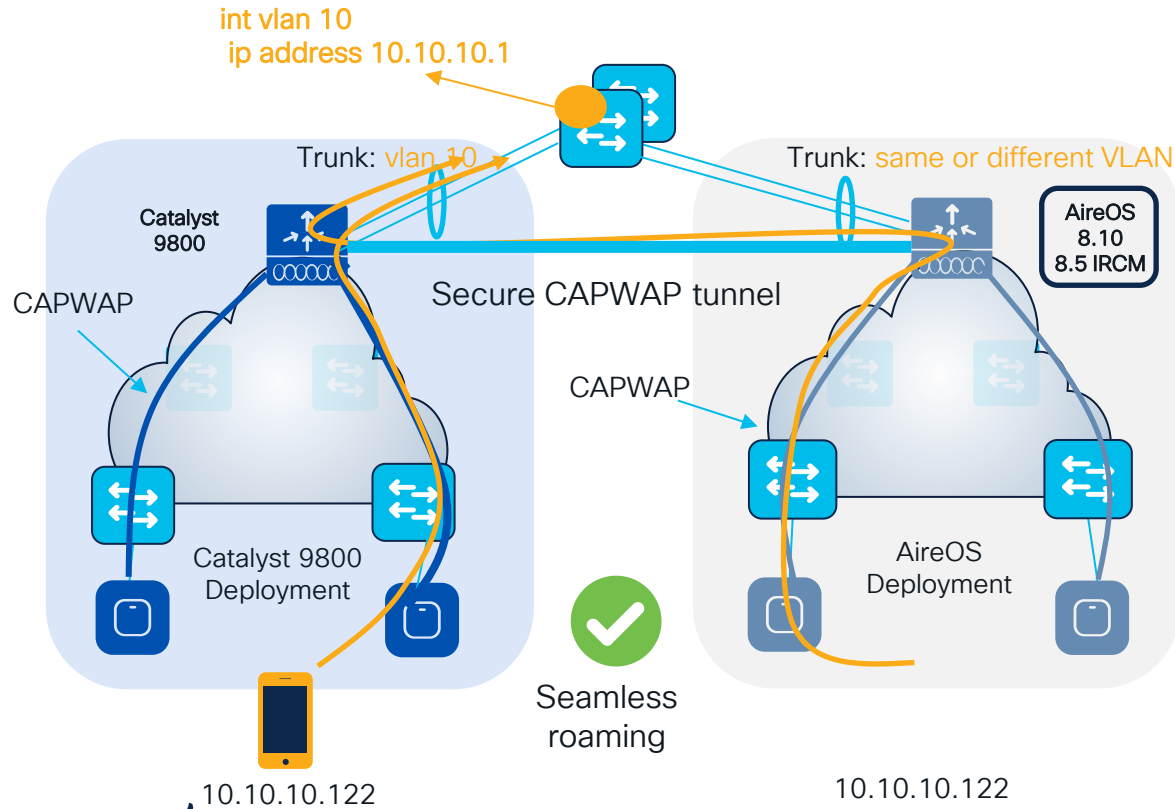


Scenario 3: Mixed indoor and outdoor areas

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

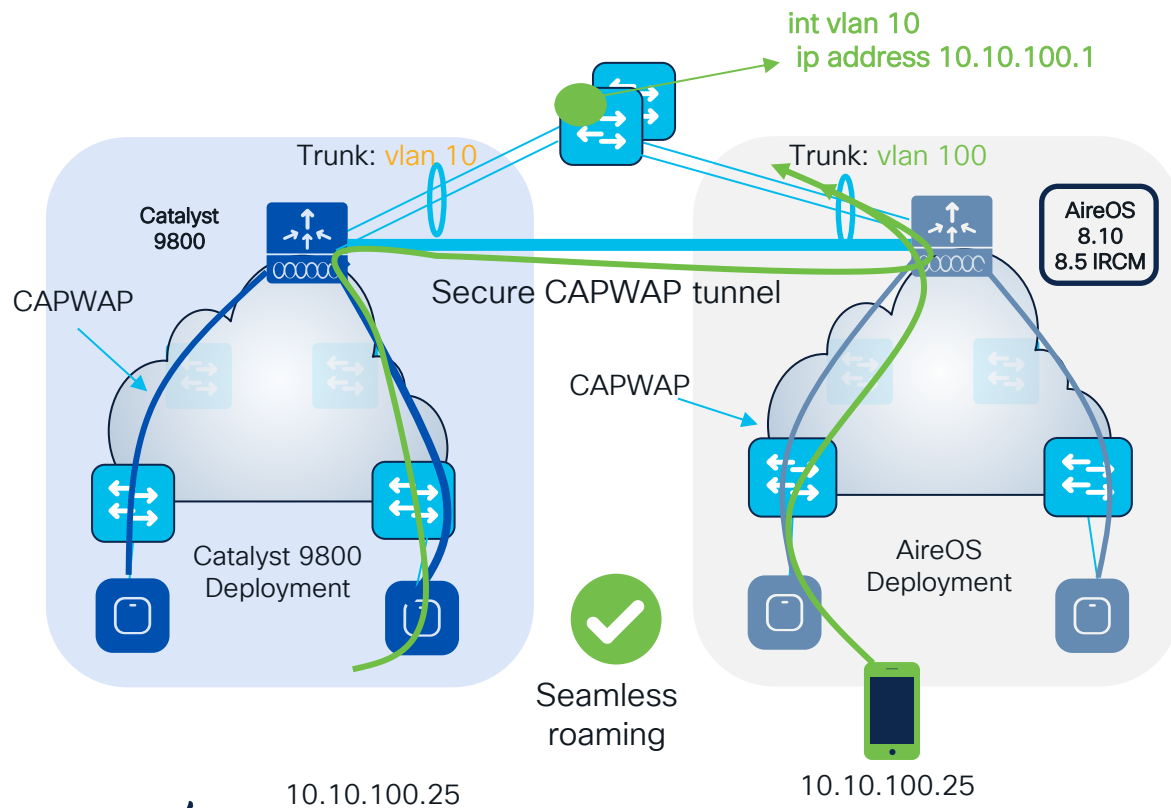
(*) for more details on WLAN Design, please refer to [BRKEWN-2024](#)

AireOS and IOS-XE coexistence – roaming



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

AireOS and IOS-XE coexistence – roaming

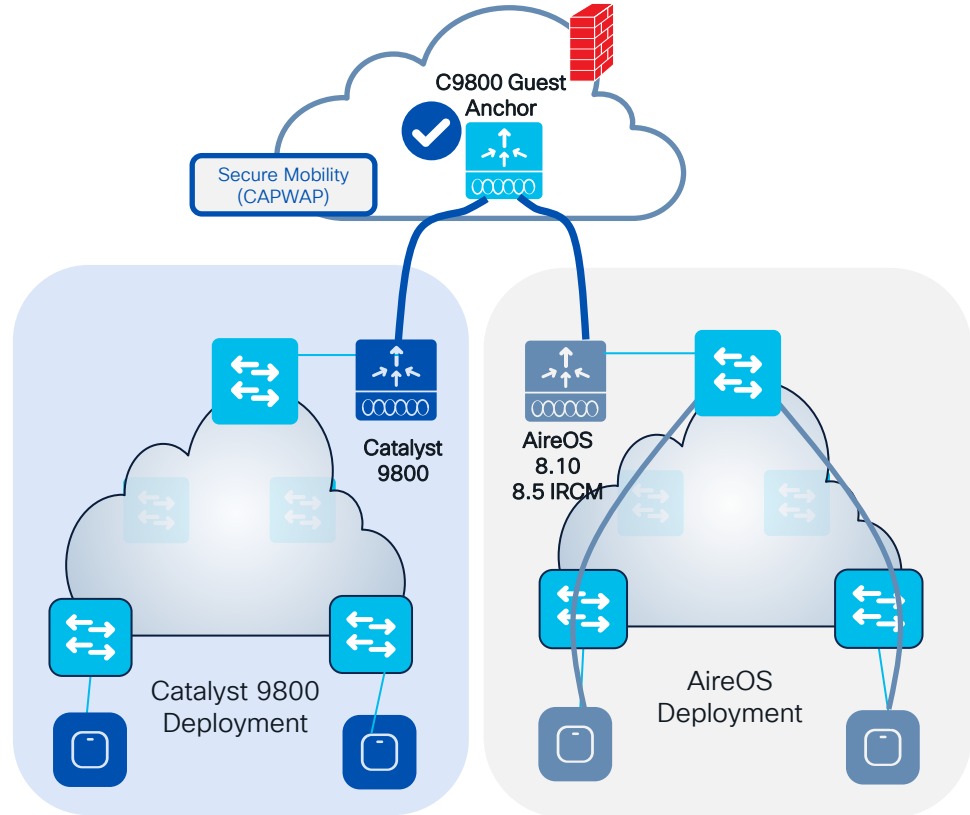


Recommendations:

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

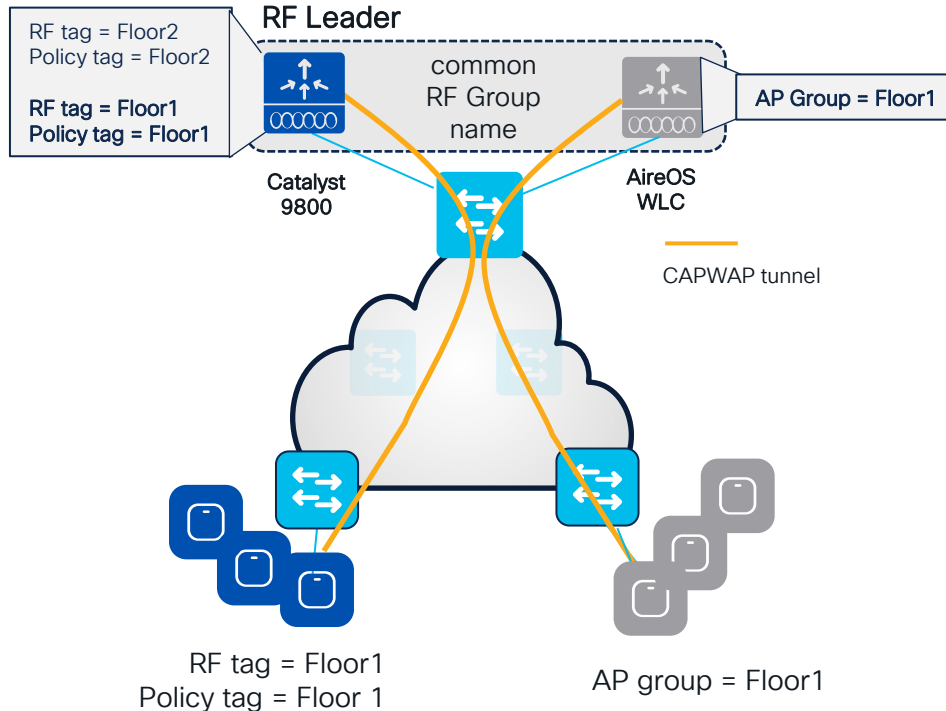
AireOS and IOS XE IRCM – guest anchor

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



AireOS to C9800 migration – common RF Group

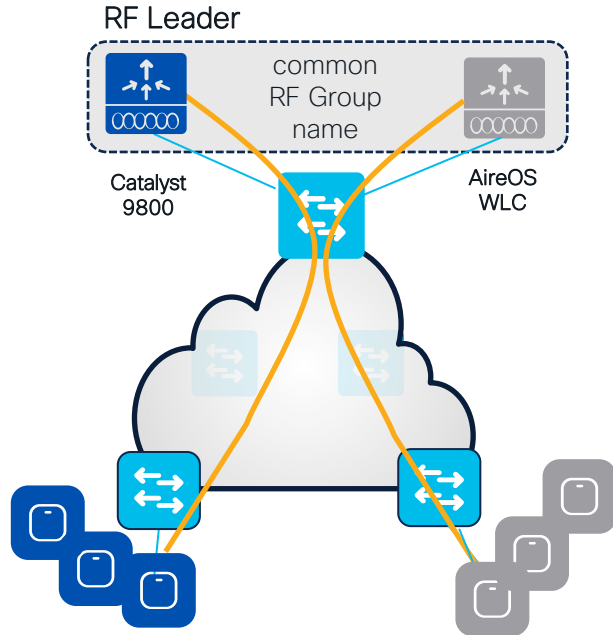
RRM works in a mixed controller environment and we can have one RF master:



- C9800 and AireOS controllers can create one RF domain and share a **common RF plan**
- The **RF group name** on both AireOS and C9800 controllers needs to match
- 8.8 is required on AireOS
 - A RF leader is elected (based on controller capacity) and common channel and power plan will be used for all APs
 - APs will 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:



- RF Leader election happens according to this table

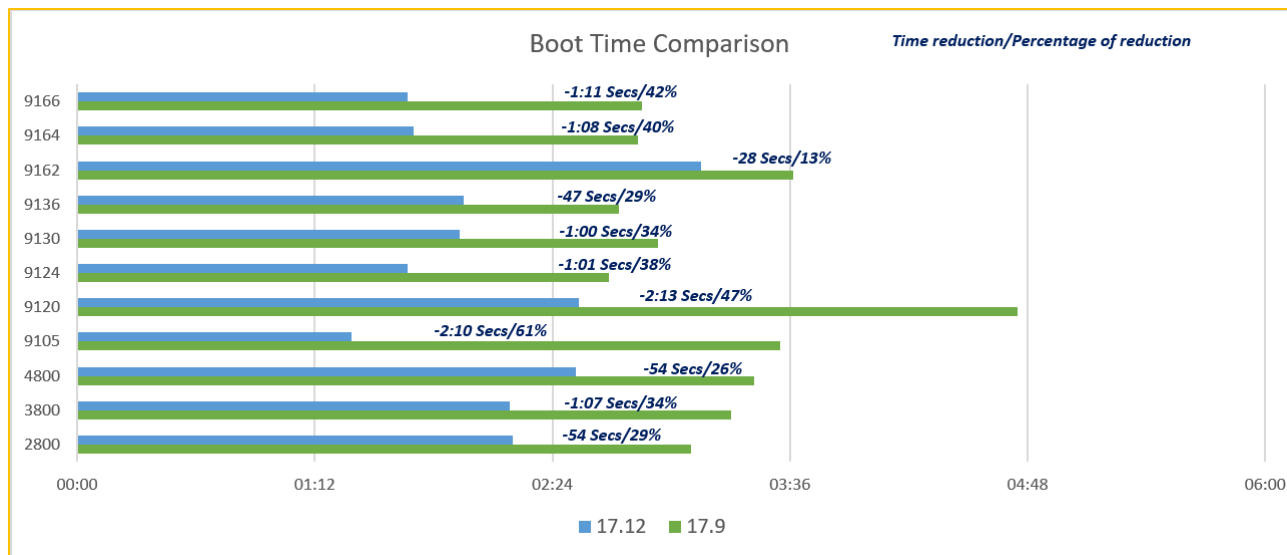
Group Leader order	Maximum AP's	Maximum AP /RF Group
3504	150	500
C9800-L	250	500
5508	500	1000
C9800-CL (Small)	1000	2000
5520	1500	3000
C9800-40	2000	4000
C9800-CL (Medium)	3000	6000
CW9800M	3000	6000
8510/8540	6000	6000
C9800-CL (Large)	6000	12000
C9800-80	6000	12000
CW9800H1/H2	6000	12000

Optimisations



AP boot time optimisation

- AP booting involves initialisation of many modules and the total bootup time is the aggregation of each boot components
- In 17.12.1, we have done some optimisations in these modules' initialisation
- With this optimisation 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 **ssid-neighbor-stats interval** value has been changed from 1 to 180 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.

Set to Factory Default

Clear Configuration on this AP and Reset to Factory Defaults

- ☒ Clear All Config
- ☐ Clear Config except Static IP
- ☐ Clear Personal SSID Config
- ☐ Clear Resolved Tag Config

Clear Config

after AP
reboot



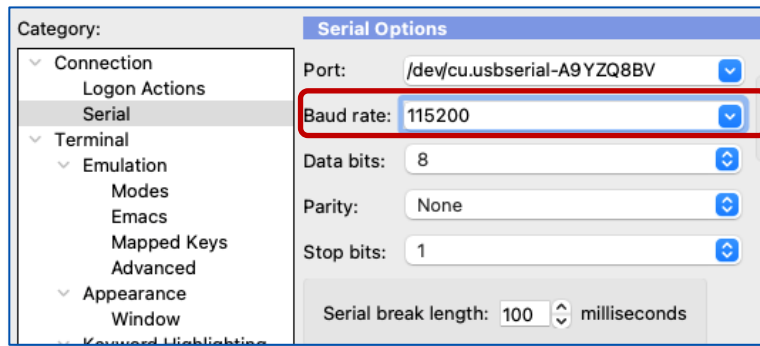
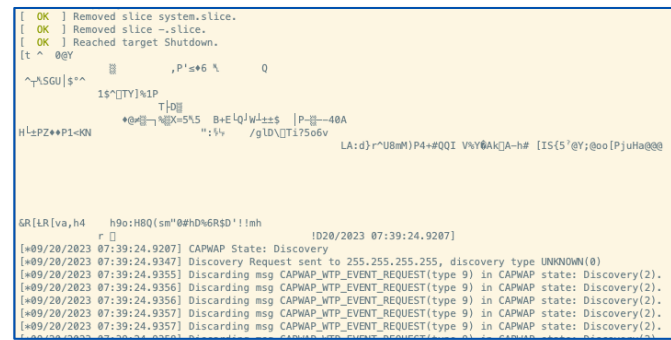
```
[ OK ] Stopped Cisco UBIFS reformat/mount.
      Stopping Cisco UBIFS reformat/mount...
[ OK ] Removed slice system.slice.
[ OK ] Removed slice -.slice.
[ OK ] Reached target Shutdown.
[t ^ 0@Y

      ,P'≤+6  L      Q

^T LSGU| $°^
      1$^□TY]%1P
      T|D
      *@#□%X=5 5 B+E LQJW L++$ |P-40A
HL±PZ♦♦
```

AP console baud rate change

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

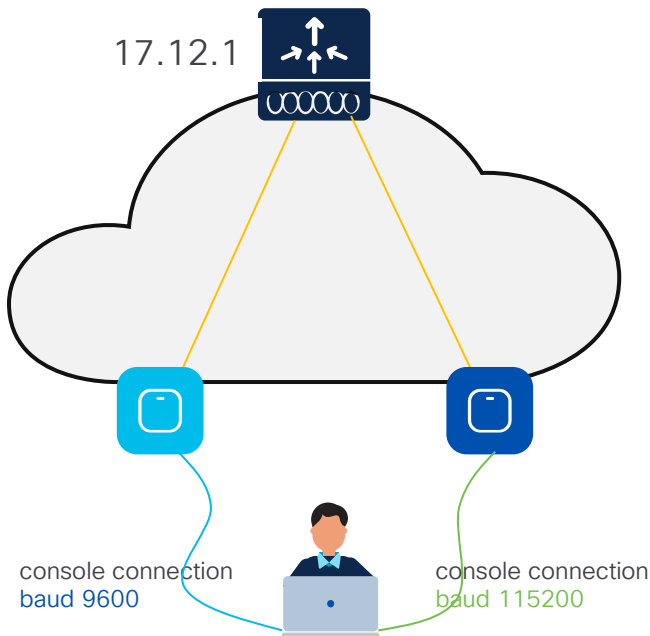
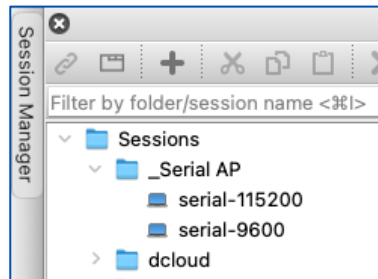


- Why?** To improve boot time; depending on the AP model, you get up to 30s reduction in boot time
- How:** By increasing the baud rate to 115200, the kernel and radio driver/firmware logs are printed faster and hence the AP boots faster (more info in CSCwe88390)

AP console baud rate change

Why would you care?

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



Wireless Product Analytics



Wireless product analytics

Knowing product usage to serve customers better

Product decisions for customer benefit



- SW version, feature and 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)

17.9.4+
17.10+

Auto Enabled

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

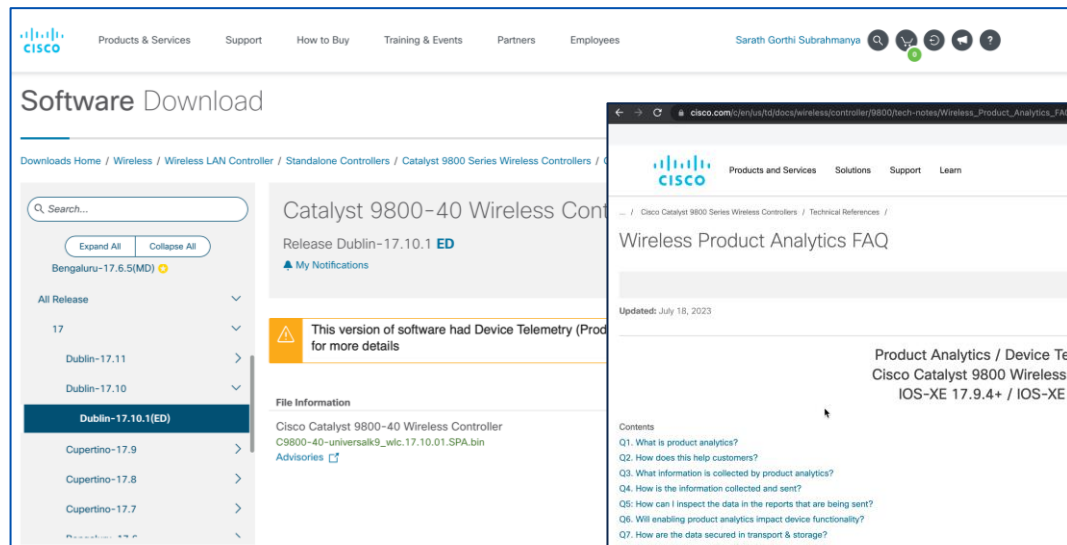
The data collected is non-PII data. CLI is present to view
the report collected/ sent for transparency

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

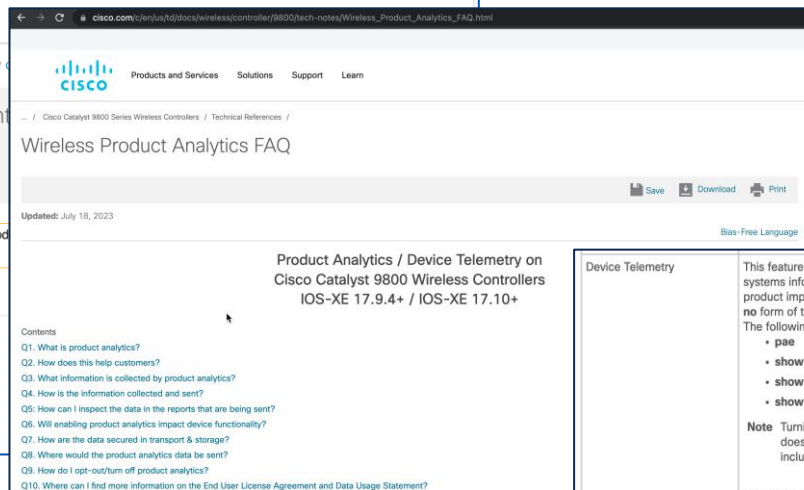
All the data processed is compliant to **GDPR**, Cisco EULA
and Cisco Privacy agreement. More details in FAQ

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

Wireless product analytics – documentation

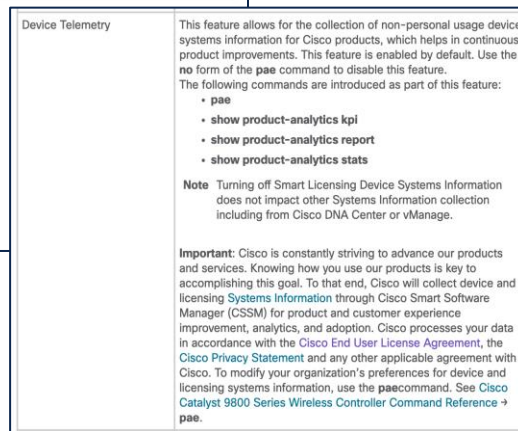


Banner on software download



FAQs

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



Release Notes

cisco Live!

Day 1: C9800 Configurations



Design with Tags in Mind



C9800 configuration model (profiles and tags)

Access Points



RF Tag



Policy Tag

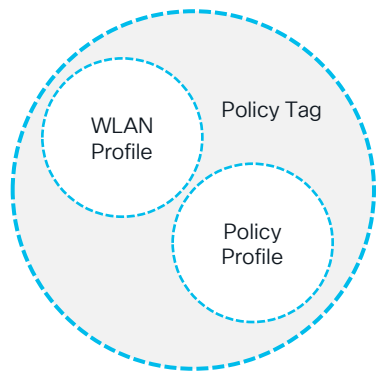


Site Tag

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?)

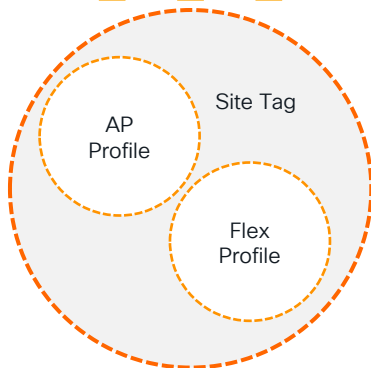
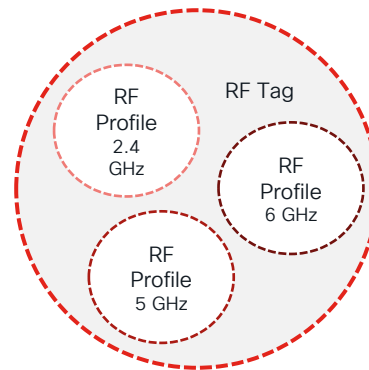
Tag breakdown



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

SSID = Service Set Identifier

Access Points

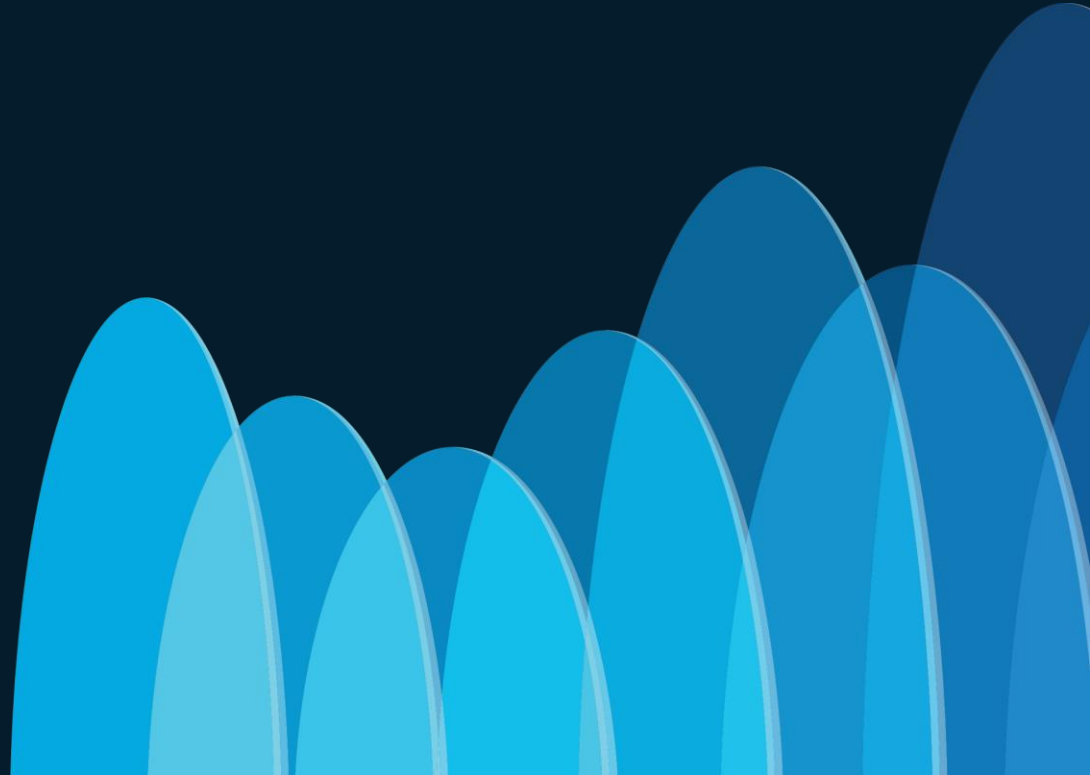


- Defines the **radio frequency (RF) properties** of the group of APs per radio
- Defines the **properties of the site** (central or remote)
- For **FlexConnect site**:
 - Defines the **fast-roaming domain**
 - “Equivalent” to Flex Groups in AireOS

Policy Tag



WLAN Design Updates



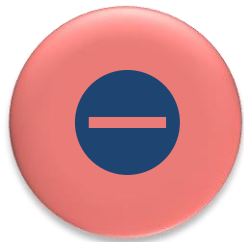
Wi-Fi 6E security (recap)



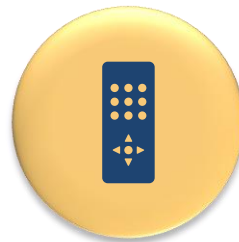
Wi-Fi 6E uplevels security.
WPA3 L2 Security: OWE,
SAE*, 802.1x-SHA256



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



No backward compatibility
with Open and WPA2
Security.

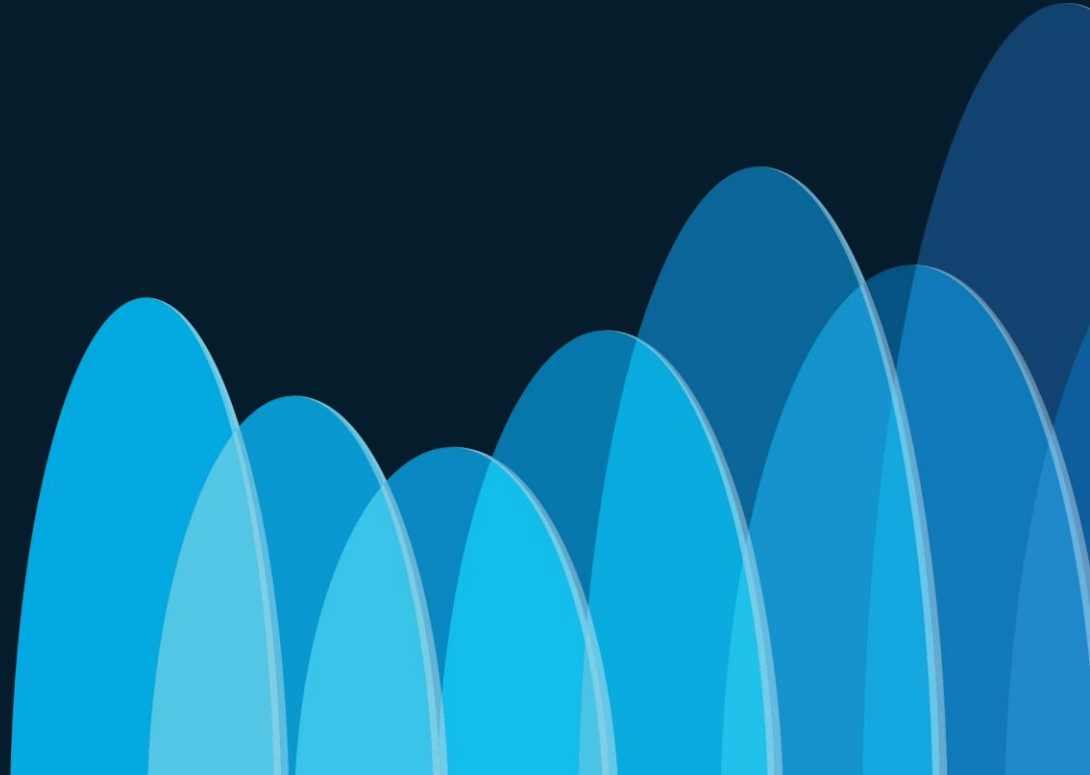


Requires Protected
Management Frame (PMF)
in both AP and Clients.

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

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

WLAN/SSID Design



6GHz WLAN design considerations

What options would you have?

1

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

2

"One SSID" Option: Configure multiple WLANs with same SSID name, different security settings – **Most conservative**

3

"Multiple SSIDs" Option: Redesign your SSIDs, adding specific SSID/WLAN with specific security settings – **Most flexible**

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

WLAN design considerations

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

Existing WLAN serving 2.4 and 5GHz

The screenshot shows the configuration for a WLAN named 'employee'. The 'General' tab is active. The 'Profile Name*' is 'employee', the 'SSID*' is 'employee', and the 'WLAN ID*' is '9'. The 'Status' is 'ENABLED' and 'Broadcast SSID' is also 'ENABLED'. Under the 'Radio Policy' section, the 6 GHz band is 'DISABLED', while the 5 GHz and 2.4 GHz bands are 'ENABLED'. The 2.4 GHz band is configured with the 802.11b/g policy.

New WLAN, same SSID name serving 6GHz

The screenshot shows the configuration for a new WLAN named 'employee-6GHz'. The 'General' tab is active. The 'Profile Name*' is 'employee-6GHz', the 'SSID*' is 'employee', and the 'WLAN ID*' is '10'. The 'Status' is 'ENABLED' and 'Broadcast SSID' is also 'ENABLED'. Under the 'Radio Policy' section, the 6 GHz band is 'ENABLED' (with status 'ENABLED' and a green checkmark), while the 5 GHz and 2.4 GHz bands are 'DISABLED'. The 6 GHz band is configured with WPA2 Disabled, WPA3 Enabled, and Dot11ax Enabled.

AKM = Authentication and Key Management

Going forward ... (IOS-XE 17.12.1)

Single WLAN profile for 2.4/5 and 6 GHz

General Security Advanced Add To Policy Tags

Profile Name* enterprise

SSID* enterprise

WLAN ID* 8

Status ENABLED

Broadcast SSID ENABLED

Radio Policy ①

6 GHz Status ENABLED

5 GHz Status ENABLED

2.4 GHz Status ENABLED

802.11b/g Policy 802.11b/g

- 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

General Security Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy

GTK WPA3 Policy

Randomize Transition Disable

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256

GCMP128 GCMP256

Protected Management Frame

PMF Optional

Association Comeback Timer* 1

Fast Transition

Status Adaptive Ena...

Over the DS

Reassociation Timeout * 20

Auth Key Mgmt

802.1X PSK

CKM SAE

FT + SAE OWE

FT + 802.1X FT + PSK

802.1X-SHA256 PSK-SHA256

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

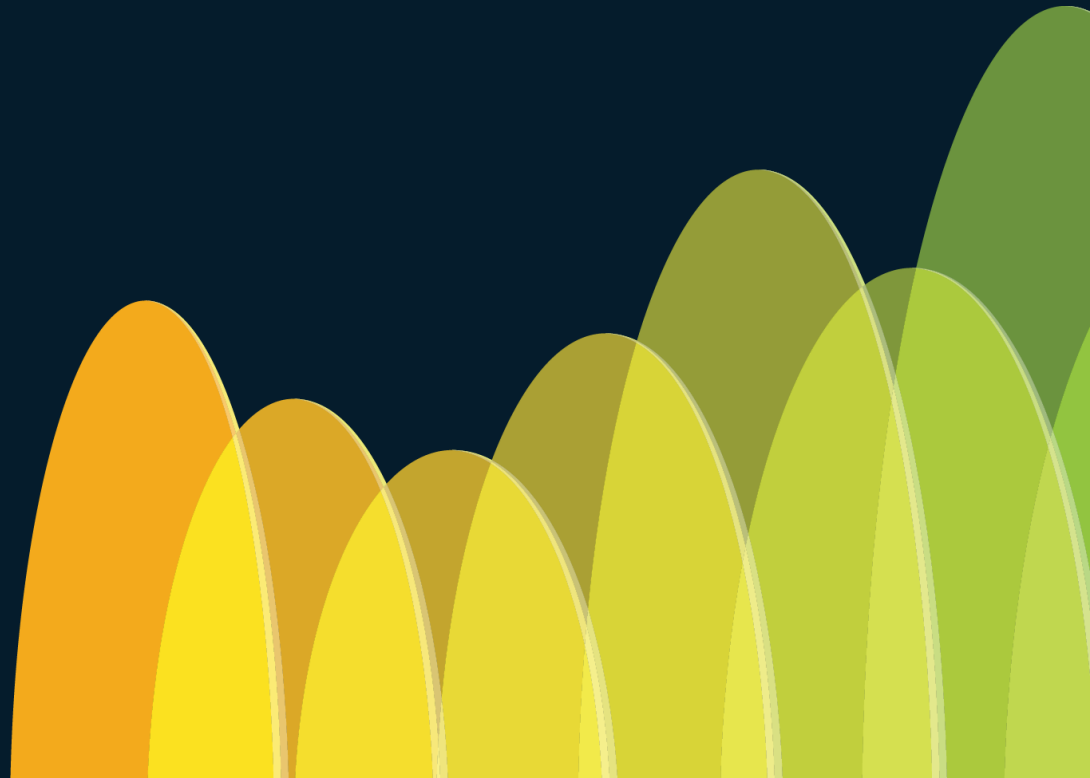
```
802.11 Authentication           : Open System
Wi-Fi Protected Access (WPA/WPA2/WPA3) ← : Enabled
WPA2 (RSN IE)                   : Enabled
AES Cipher                      : Enabled
WPA3 (WPA3 IE)                  : Enabled
    AES Cipher                  : Enabled
Auth Key Management
    802.1x                      : Enabled
```

.....

Security-6GHz

```
WPA3 (WPA3 IE) ← : Enabled
    AES Cipher    : Enabled
Auth Key Management
    Dot1x-SHA256  : Enabled
```

WLAN Settings



WLAN settings

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General Security **Advanced** Add To Policy Tags

Coverage Hole Detection	☒	Universal Admin	☐
Aironet IE	☐	OKC	☒
Advertise AP Name	☐	Load Balance	☐
P2P Blocking Action	Disabled	Band Select	☐
Multicast Buffer	☐	IP Source Guard	☒
Media Stream Multicast-direct	☐	WMM Policy	Allowed
11ac MU-MIMO	☒	mDNS Mode	Bridging

C9800-80

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.

CISCO MONITOR WLANs **CONTROLLER** WIRELESS

Controller General

General

Name	Cisco
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Enabled
Broadcast Forwarding	Disabled
AP Multicast Mode	Multicast
AP IPv6 Multicast Mode	Unicast
AP Fallback	Enabled
CARWAP Preferred Mode	IPv4
Fast SSID change	Enabled
Link Local Bridging	Disabled

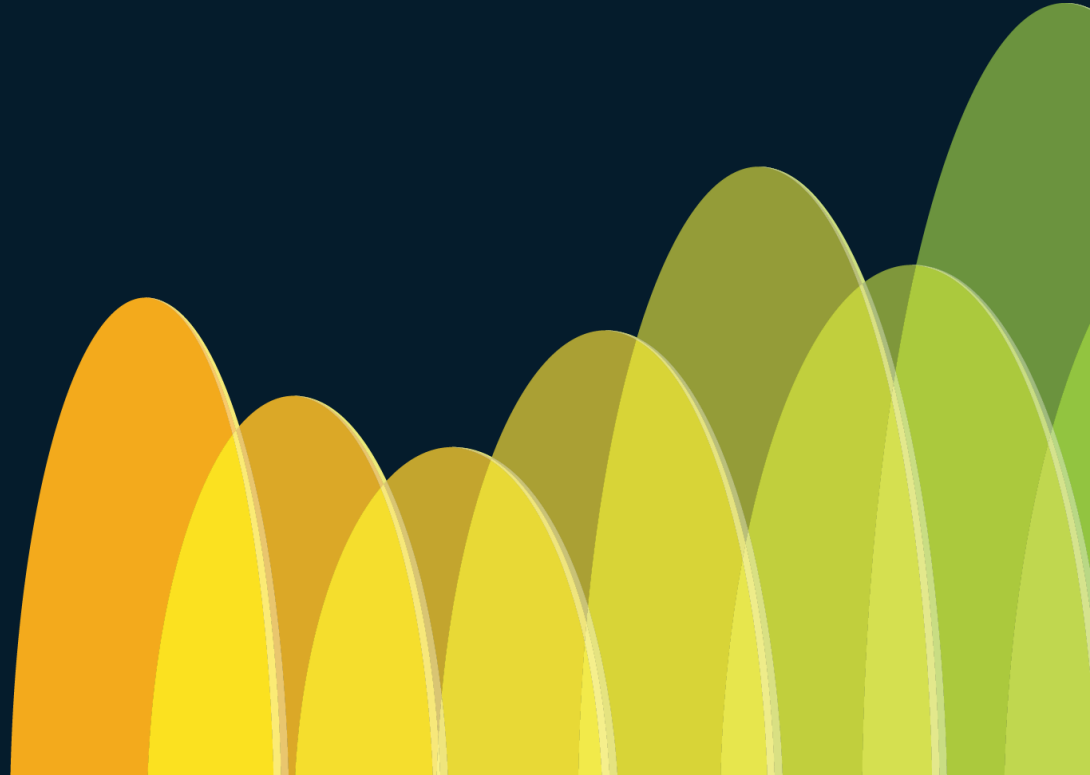
8540

Q: What happened to Fast SSID change?

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

CISCO Live!

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

[illegible]

```
! config interface address virtual 192.0.2.1
```

```
! config interface hostname virtual <name>
```

```
! config custom-web webauth-type external
```

```
! config custom-web ext-webauth-url <url>
```

```
! config custom-web redirecturl <https url>
```

```
!% Note: parameter-map configuration follow interactive-mode
when it get configure first time.
```

!% Please enter prompt option while configuring parameter-map.

!% e.g. : This operation will permanently convert all relevant authentication commands to their CPL control-policy equivalents. As this conversion is irreversible and will disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly advised to back up your current configuration before proceeding.

```
!% Do you wish to continue? [yes]: yes
```

parameter-map type webauth global

```
virtual-ip ipv4 192.0.2.1 virtual-host <name>
```

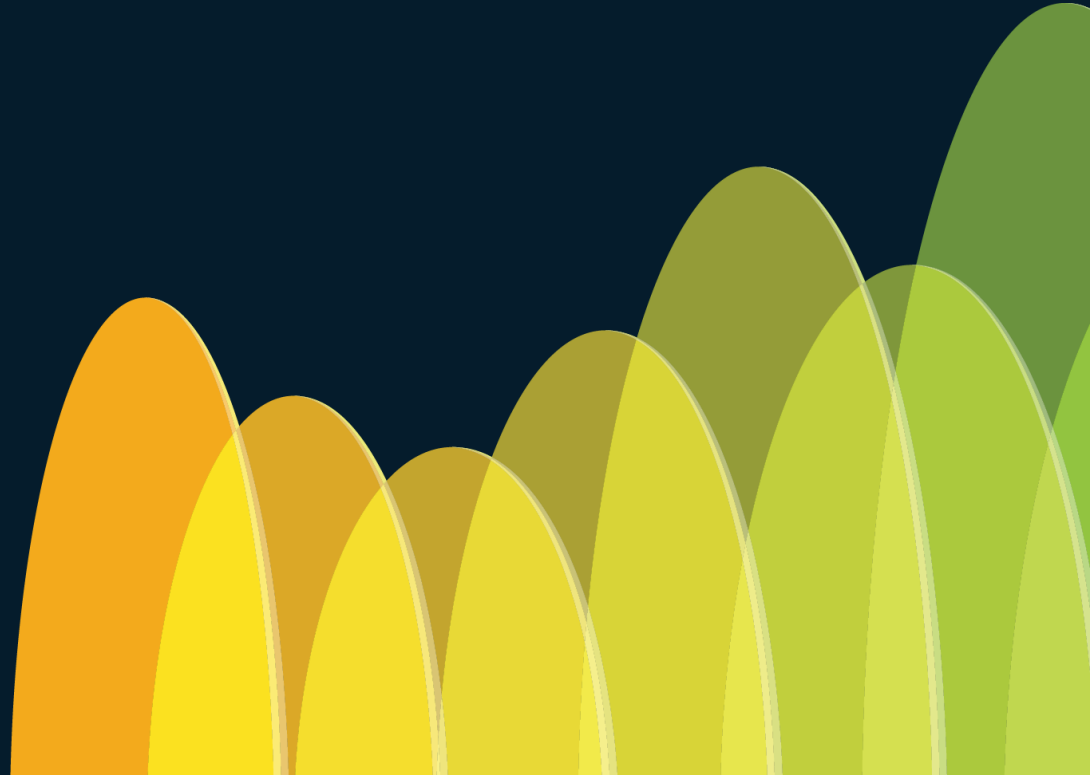
parameter-map type webauth global

```
type webauth
```

```
redirect for-login <http url>
```

redirect on-success <https url>

mDNS Configuration



mDNS configuration

Scenario:

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

Recommendation:

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

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

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

! mdns profile and service mapping

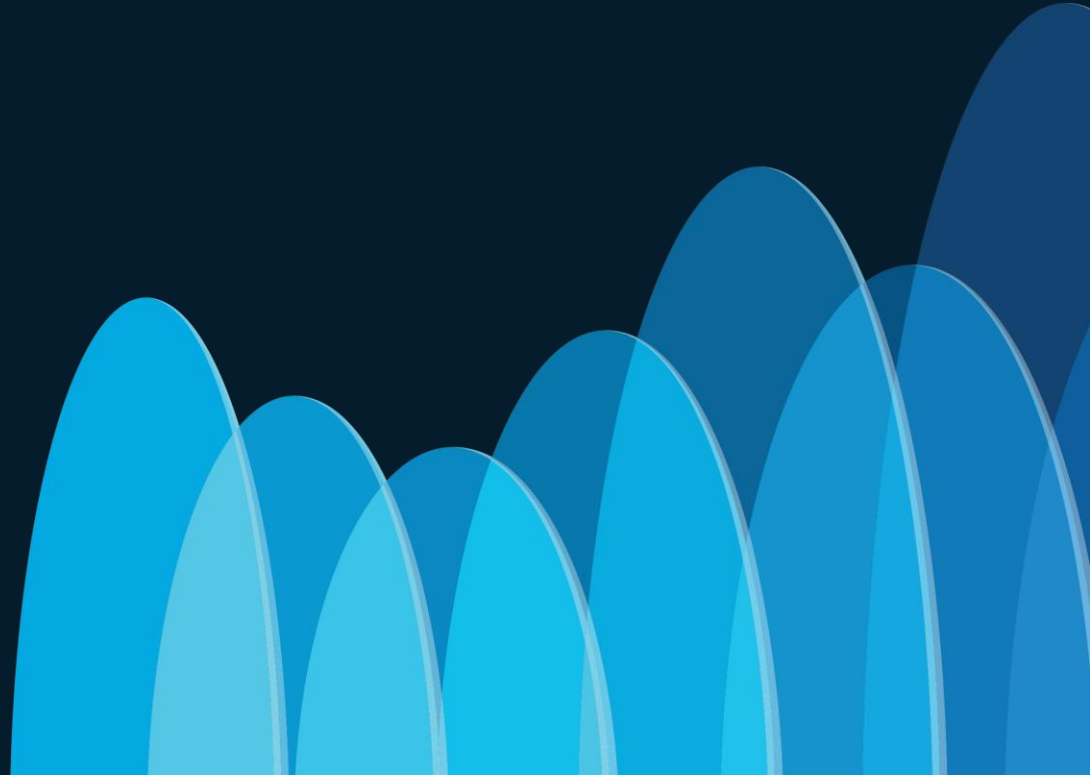
```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

[skip]

```
mdns-sd service-list aireos-default-mdns-profile-out OUT  
match AirTunes  
  
match Printer-IPPS  
  
match Printer-SOCKET  
  
match HP_Photosmart_Printer_2  
  
match HomeSharing  
  
match HP_Photosmart_Printer_1  
  
match Airplay  
  
mdns-sd service-policy aireos-default-mdns-profile  
service-list aireos-default-mdns-profile-in IN  
service-list aireos-default-mdns-profile-out OUT
```

!% "location lss" skipped since it is disabled in any of
"mdns service" mapped under "mdns profile".

Policy Profile Settings



Policy profile settings

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy

General Access Policies QOS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec) 0 ⓘ

Idle Timeout (sec) 300

• For Dot1x profile: Allowed Range is 300 to 86400 secs (Any value less than 300 is treated as 86400 secs)
• For Other Security profiles: Allowed Range is 0 to 86400 secs

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

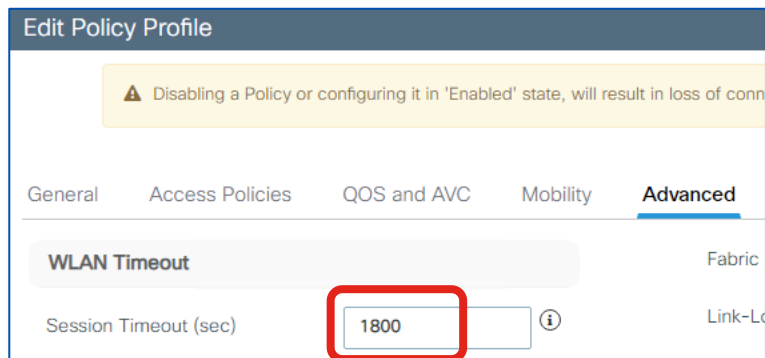
A: Yes, absolutely

Default session timeout to 8 hours

What it is?

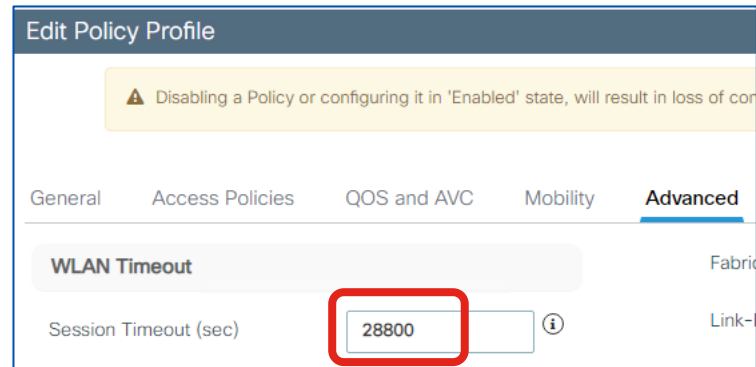
- The default session timeout in policy profile is changed from 30 mins to 8 hours
- Why? Some clients don't like frequent re-auth and re-keying and there have been multiple TAC cases related to this, solved with longer session time out
- This new would help relieve the pressure on AAA servers

Before 17.12 > timeout is 30 mins



The screenshot shows the 'Edit Policy Profile' interface with the 'Advanced' tab selected. A yellow warning banner at the top states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of conn'. Below the tabs, the 'WLAN Timeout' section is visible. The 'Session Timeout (sec)' field is highlighted with a red box and contains the value '1800'. An information icon (i) is located to the right of the input field.

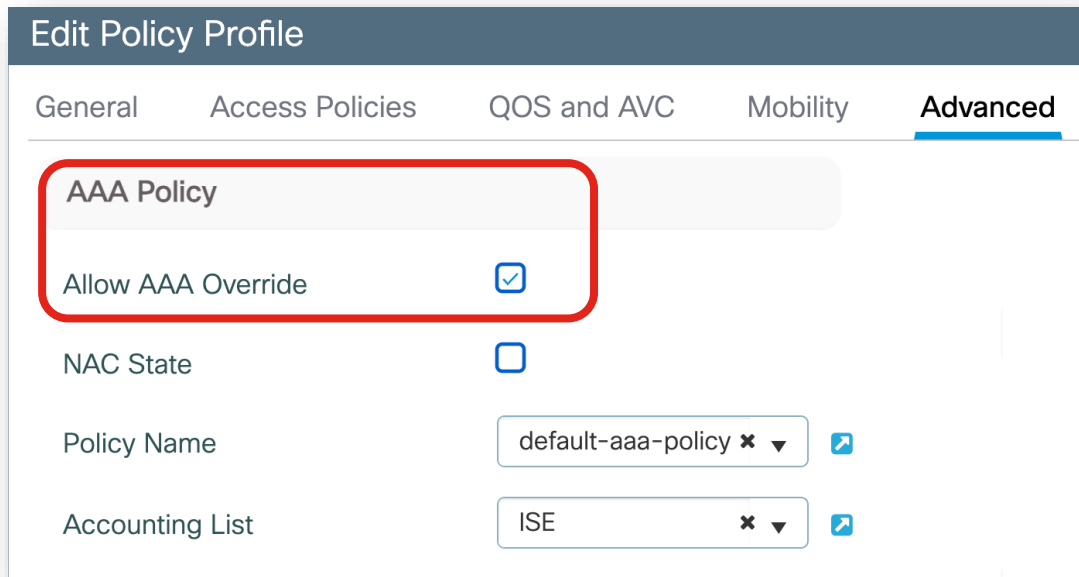
Starting 17.12 > timeout is 8 hours



The screenshot shows the 'Edit Policy Profile' interface with the 'Advanced' tab selected. A yellow warning banner at the top states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of conn'. Below the tabs, the 'WLAN Timeout' section is visible. The 'Session Timeout (sec)' field is highlighted with a red box and contains the value '28800'. An information icon (i) is located to the right of the input field.

AAA override

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



Edit Policy Profile

General Access Policies QOS and AVC Mobility **Advanced**

AAA Policy

Allow AAA Override ☒

NAC State ☐

Policy Name default-aaa-policy ✕ ▼ 

Accounting List ISE ✕ ▼ 

EAP timeout

Configuration > Security > Advanced EAP

EAP-Identity-Request Timeout (sec)*

30

EAP-Identity-Request Max Retries*

2

EAP Max-Login Ignore Identity Response

☐ DISABLED

EAP-Request Timeout (sec)*

30

EAP-Request Max Retries*

2

EAPOL-Key Timeout (ms)*

1000

EAPOL-Key Max Retries*

2

EAP-Broadcast Key Interval (sec)*

3600

- 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

Configuration ▾ > Security ▾ > Advanced EAP

EAP-Identity-Request Timeout (sec)*

30

EAP-Identity-Request Max Retries*

2

EAP Max-Login Ignore Identity Response

☐ DISABLED

EAP-Request Timeout (sec)*

30

EAP-Request Max Retries*

2

EAPOL-Key Timeout (ms)*

1000

EAPOL-Key Max Retries*

2

EAP-Broadcast Key Interval (sec)*

3600

- 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

Configuration > Security > Advanced EAP

EAP-Identity-Request Timeout (sec)*

30

EAP-Identity-Request Max Retries*

2

EAP Max-Login Ignore Identity Response

☐ DISABLED

EAP-Request Timeout (sec)*

30

EAP-Request Max Retries*

2

EAPOL-Key Timeout (ms)*

1000

EAPOL-Key Max Retries*

2

EAP-Broadcast Key Interval (sec)*

3600

- 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
- Minimises early expiration of the authentication process

Edit AAA Radius Server

Name*	dnac-radius_10.10.110.8	Support for CoA ⓘ	ENABLED ☒
Server Address*	10.10.110.8	CoA Server Key Type	Clear Text ▼
Set New Key	☐	CoA Server Key ⓘ	*****
Auth Port	1812	Confirm CoA Server Key	*****
Acct Port	1813	Automate Tester	☐
Server Timeout (seconds)	5		
Retry Count	3		

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

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

Global Config

[RADIUS Fallback](#)

Attribute List Name

Device Authentication

AP Policy

Password Policy

AAA Interface

Retransmit Count

Timeout Interval (seconds)

Dead Time (Minutes)

Dead Criteria Time (seconds)

Dead Criteria Tries

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

Edit AAA Radius Server

Support for CoA ⓘ	<div>ENABLED ☒</div>
CoA Server Key Type	<div>Clear Text ▼</div>
CoA Server Key ⓘ	<div>.....</div>
Confirm CoA Server Key	<div>.....</div>
Automate Tester	☒
Username*	<div>tester-account</div>
Ignore Auth Port	☐
Ignore Acct Port	☐
Enable Probe on	☒

TACACS+ management timeout

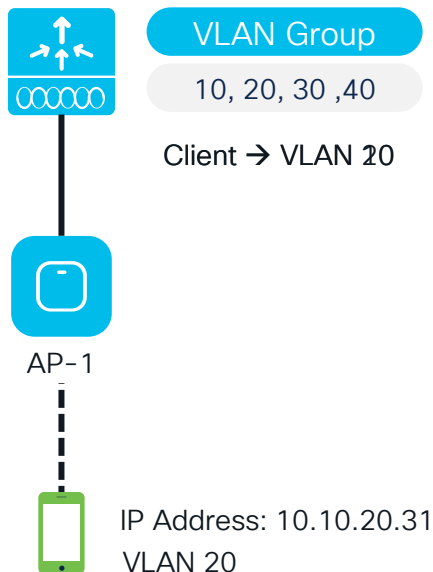
- Increase retransmit timeout if:
 1. Repeated reauthentication requests
 2. Controller falls back to the backup server when primary is still up and reachable
- Recommended value of 1 second

The screenshot shows a configuration window titled "Create AAA Tacacs Server". It contains several input fields for configuring a TACACS+ server. The "Server Timeout (seconds)" field is highlighted with a red rectangle and contains the value "1".

Field	Value
Name*	Tacacs
Server Address*	10.10.110.5
Key Type	Clear Text
Key*	
Confirm Key*	
Port	49
Server Timeout (seconds)	1

Buttons: Cancel, Apply to Device

VLAN group support for DHCP and static IP clients



9800 assigns a VLAN to clients upon joining the network

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

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

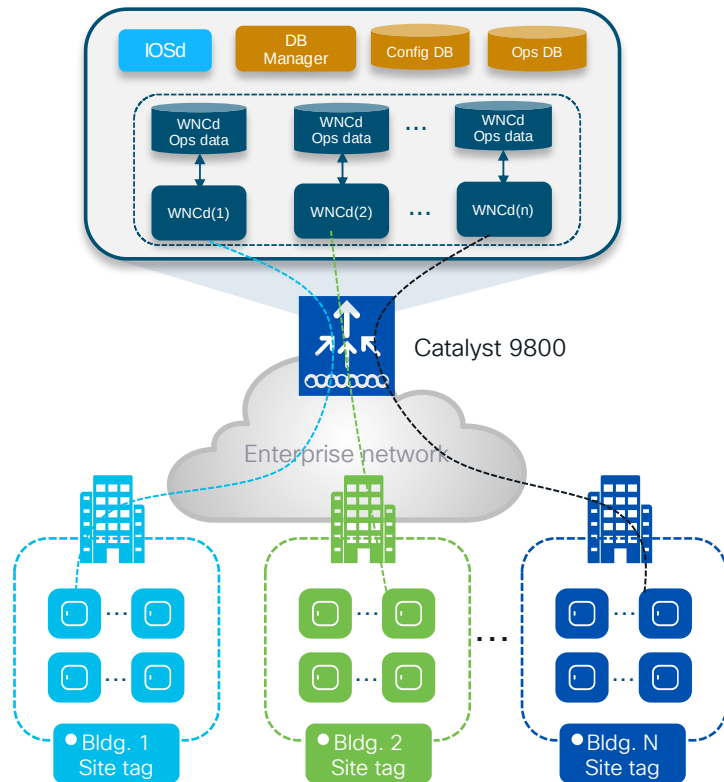
If VLAN does not exist, use Static IP Mobility

Site Tag Design



Site tags – design considerations

Refresher!



Important facts:

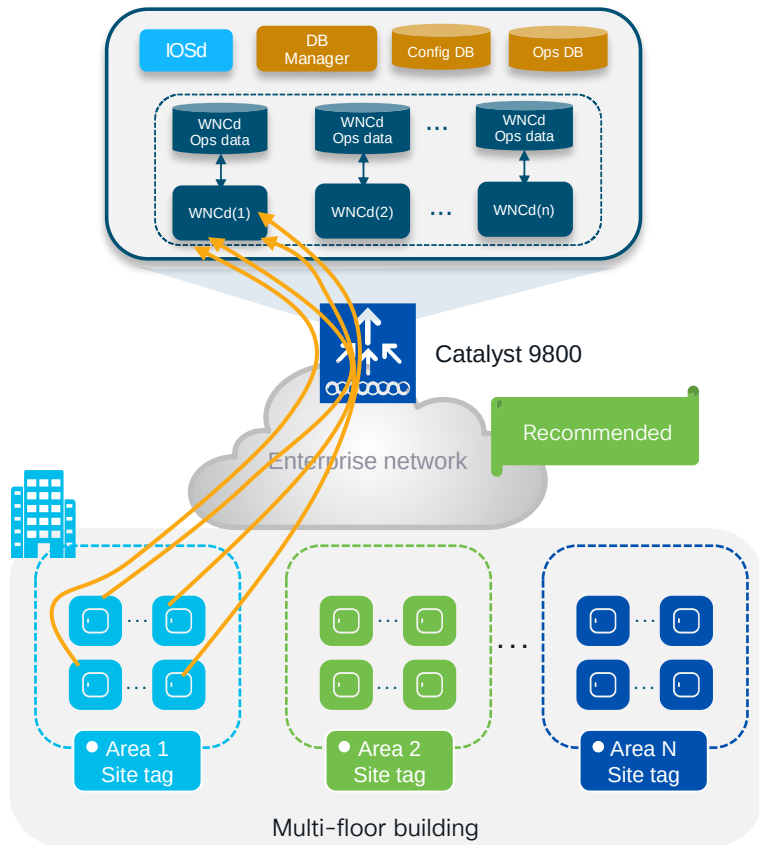
- C9800 has a multi-process software architecture
- APs are distributed across Wireless Network Controller processes (WNCd) within a C9800
- Distributing APs (and clients) across WNCd processes gives better scale and performance
- The number of WNCd varies from platform to platform:

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

Following command shows the # of WNCds processes:
9800#sh processes platform | inc wncd

Site tags – AP to WNCd distribution

Refresher!



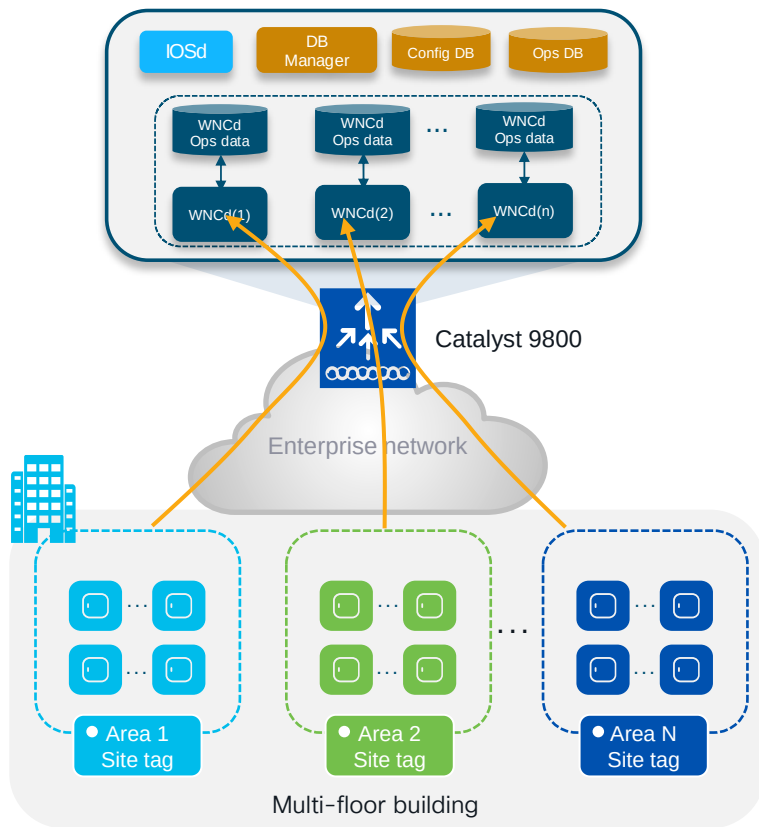
How AP distribution across WNCds works:

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

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

Site tags – AP to WNCd distribution

Refresher!



Recommendations:

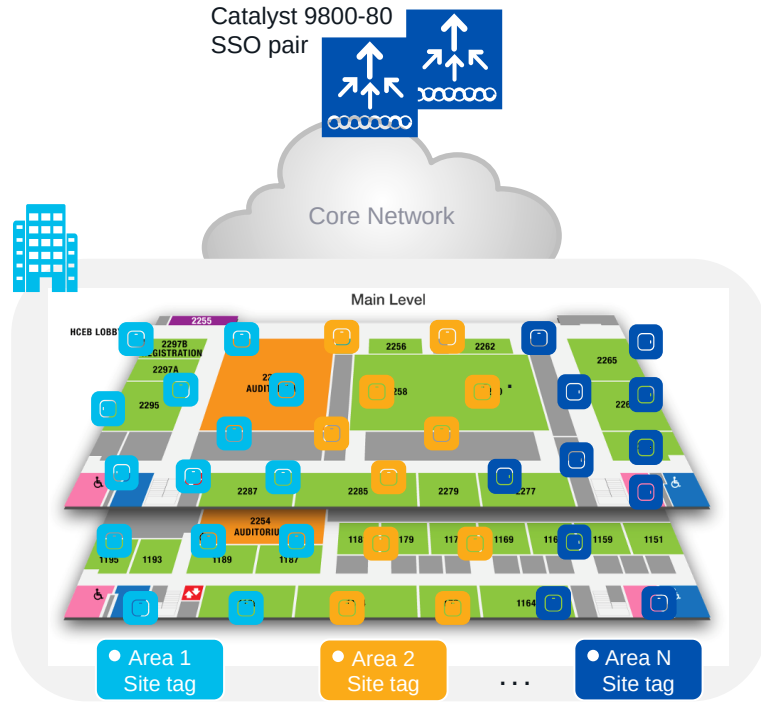
- Use **custom site tags**
- Whenever possible, have **less than 500 APs per site tag**
- **Do not overwhelm a site-tag and WNCd.** Do not exceed the following max number of APs per site tag:

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

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

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

Site tags design – large venue deployment



Scenario#1: Large venue deployment

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

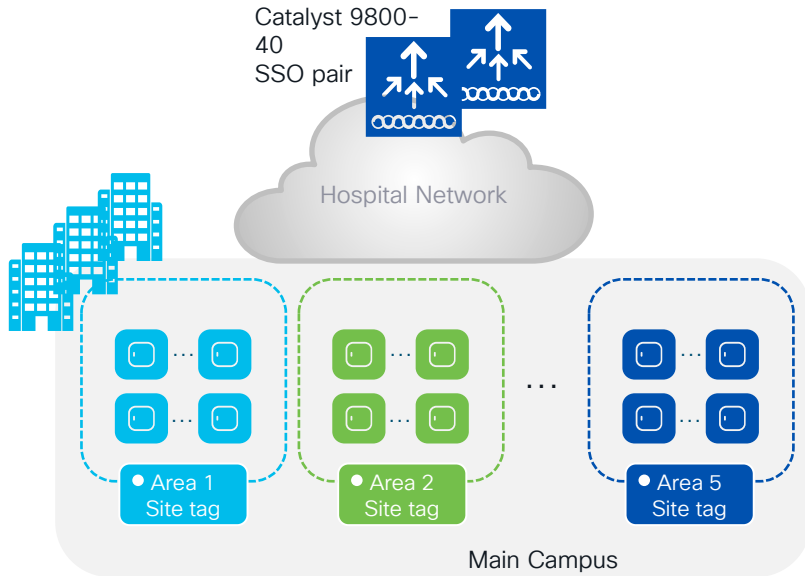
What are the recommendations in this case?

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

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

- This is to minimise 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 Optimised in 17.7 and later.

Wireless Config Analyser Express (WCAE)

The wireless engineer trowel



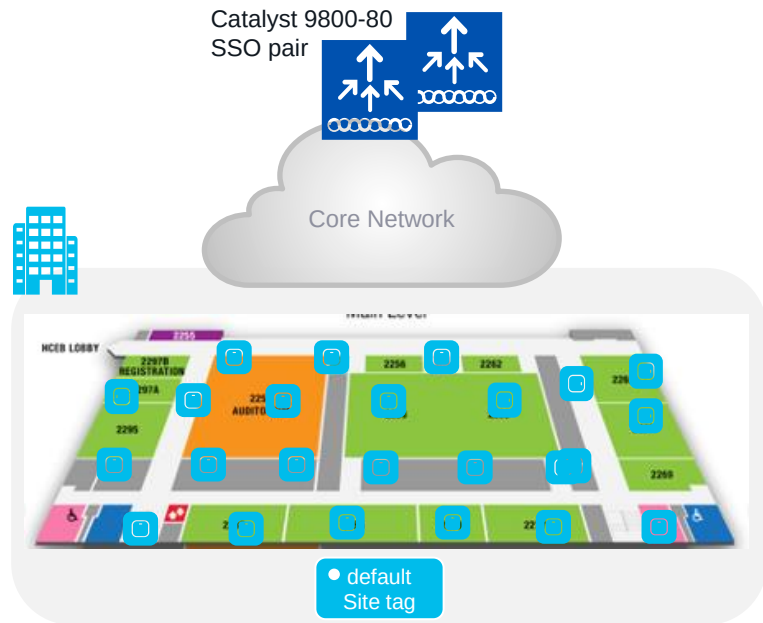
- Do I have a problem with WNCd load balancing?
- WCAE is your friend! Run the WCAE > you get a report like this:

starting 17.9

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



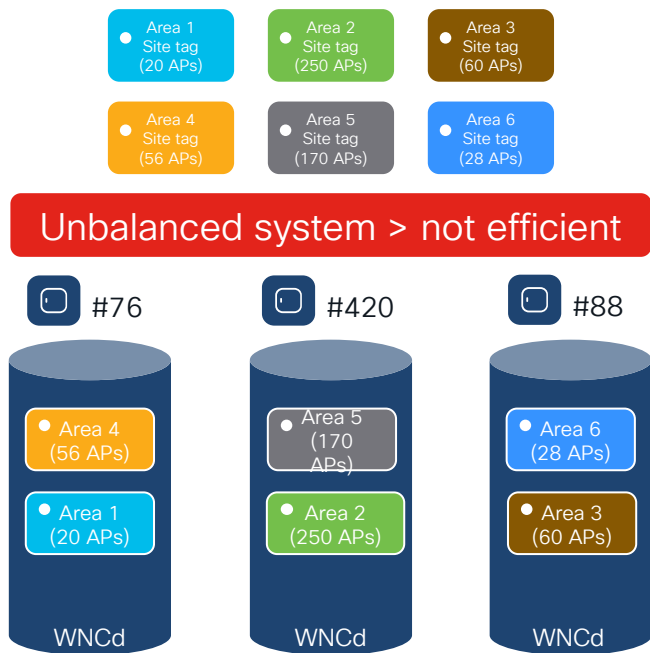
Scenario #2: Large warehouse

- 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 heavily loaded > clients and/or AP scale is **30-40% of the max scale** supported on the C9800
- **Design option:** it's ok to put all APs in the default-site-tag
 - Fast roaming (11r, OKC, etc.) is supported across WNCds
 - 802.11k/v is also supported across WNCds starting 17.7
- This recommendation is valid for all authentication types

Site tags – AP to WNCd distribution

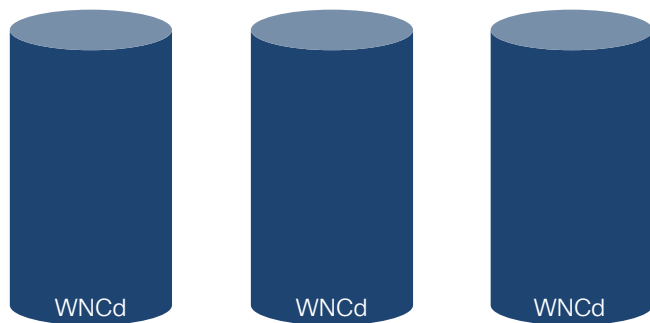


Until 17.9.1, site tags are distributed among WNCds using the **least loaded criteria** based on the **number of site tags**. The algorithm doesn't take into considerations the number of APs or clients per site tag

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

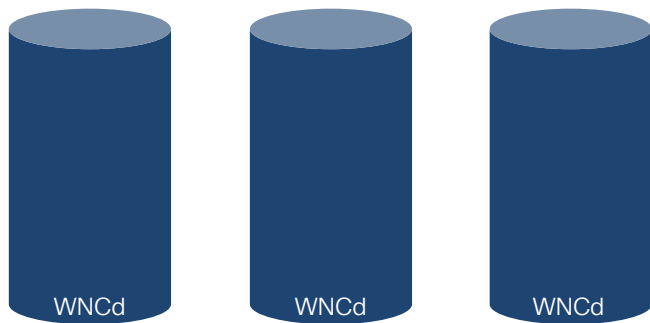
- Example:** C9800-CL medium (#3 WNCd), six custom site tags and APs joining in this order:
 - Area1 : #20 APs > WNCd0
 - Area2 : #250 AP > WNCd1
 - Area3 : #60 AP > WNCd2
 - Area4 : #56 APs > WNCd0 (all WNCd has #1 tag, starting again from WNCd0)
 - Area5 : #170 APs > WNCd1 (as WNCd0 has already #2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

Site tags – new load balancing algorithm



- **Starting 17.9.2 and 17.10**, the algorithm to distribute APs among WNCds may use the **load** parameter configured under the site tag:
 - `C9800(config)#wireless tag site <site-tag-name>`
 - `C9800(config-site-tag)#load <num> (0 to 1000)`
- **Load** is an estimate of the relative WNCd capacity reserved for that site tag. It's about reserving a part of the WNCd for a site
- What contributes to the load of the WNCd: all control plane activities > client joining, authentication, roaming, client probes, but also features like mDNS that require CPU time
- **IMPORTANT:** For load balancing to be efficient it is expected to **configure "load" for all the custom site tags**

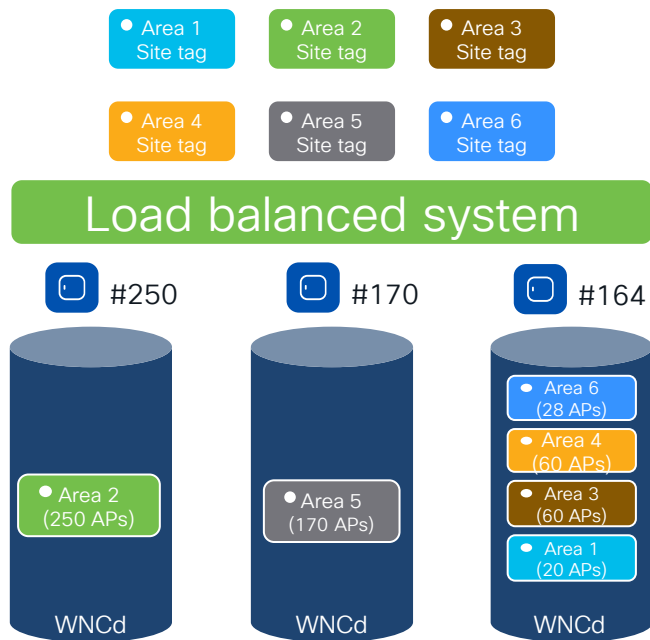
Site tags – new load balancing algorithm



How to choose the load?

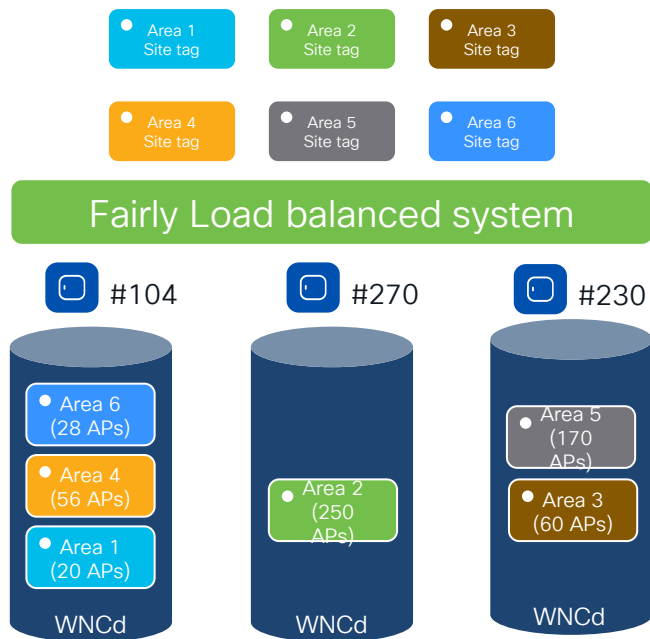
- The default value 0 means no load indication for the site tag. Nothing changes, the algorithm is the same as in 17.9.1 and previous releases
- **Most common option:** Office building with multiple floors/areas. Each floor/area is one site tag. If you estimate similar client/traffic load on each floor/area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

Site tags – new load balancing algorithm



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

Site tags – new load balancing algorithm



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

Configuring the site tag load- WebUI

Configuration > Tags & Profiles > Tags -> Site

The screenshot displays the Cisco WebUI interface for configuring site tags. The breadcrumb path is Configuration > Tags & Profiles > Tags. The 'Site' tab is selected under the 'Policy' section. On the left, a list of site tags includes 'Area1', 'flex-site', 'flex-site-IT', 'Conference_hall', and 'default-site-tag'. The 'Area1' tag is selected. The right pane shows the 'Edit Site Tag' configuration for 'Area1'. Fields include Name* (Area1), Description (floor 1 area 1), AP Join Profile (default-ap-profile), and Fabric Control Plane Name. The 'Enable Local Site' checkbox is checked. The 'Load*' field, which represents the relative load estimate, is highlighted with a red box and set to 20. An information icon is present next to the 'Load*' label.

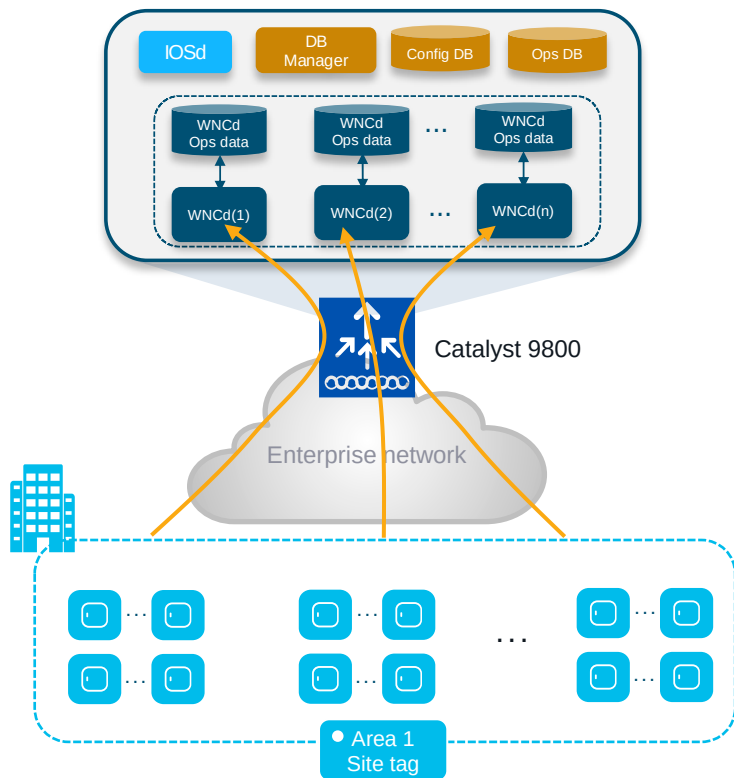
Load* = Estimate of the relative load contributed by this group of APs (site-tag).
AP count can be used as a good approximation.

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	} #160 APs
area3	SITE TAG	60	0	
area4	SITE TAG	56	0	
area6	SITE TAG	28	0	
area2	SITE TAG	250	1	} #250 APs
area5	SITE TAG	170	2	} #170 APs

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

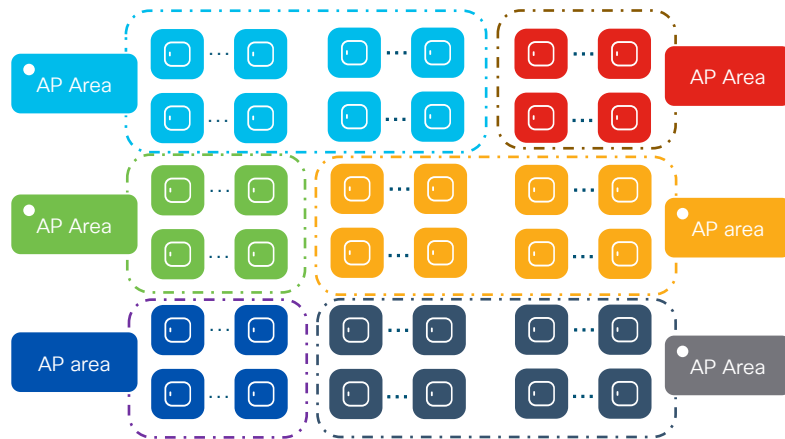
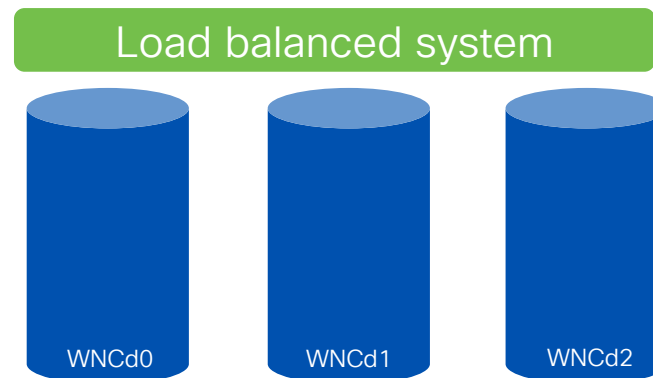
Starting 17.12.1, we have a solution!

(RRM based)
Auto WNCd load
balancing

RRM based auto WNCd load balancing

What is it?

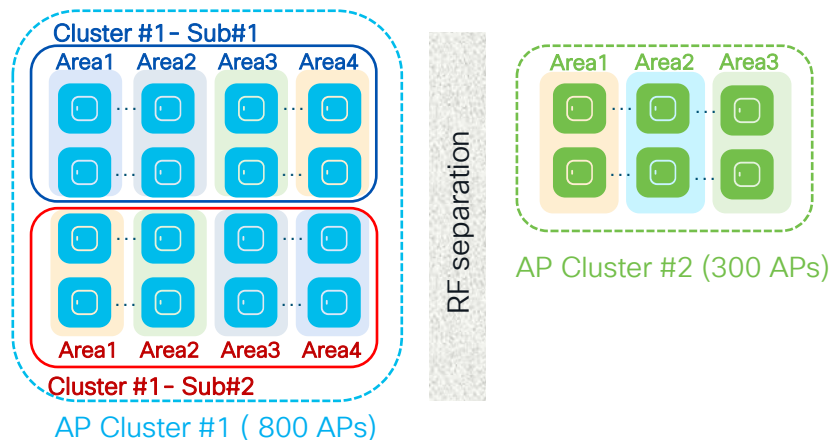
- RRM-based, automatic way of clustering APs and evenly distribute them across WNCds.
- RF based clusters (**AP Areas**) are formed using RSSI info received from RRM AP neighbour reports
- The algorithm can be run on demand or scheduled. It's off by default and it requires the APs deployed and a stable 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 Optimise APs to WNCd load balancing



Trigger the algorithm

Trigger Manually:

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

Schedule via Calendar Profile:

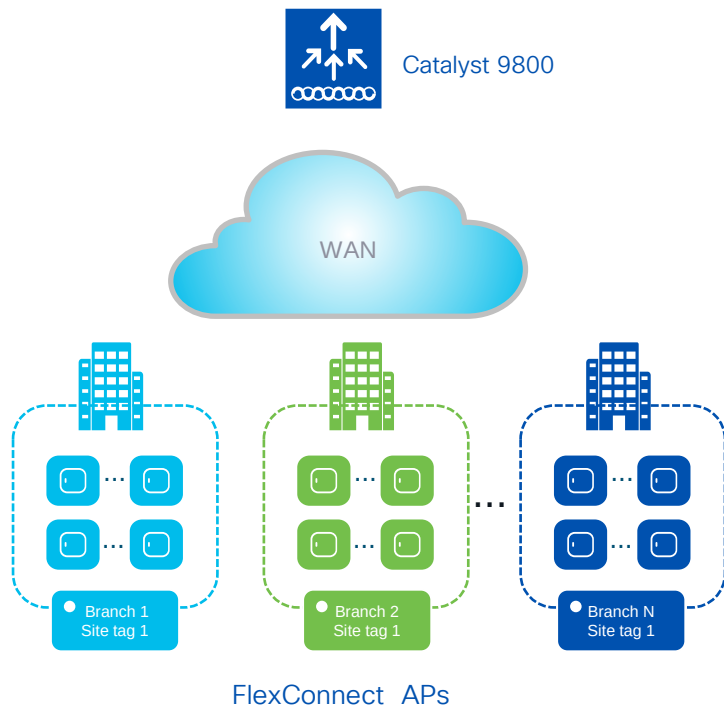
```
C9800# conf t
C9800(config)# ap neighborhood calendar-profile <calendar name>
```

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:

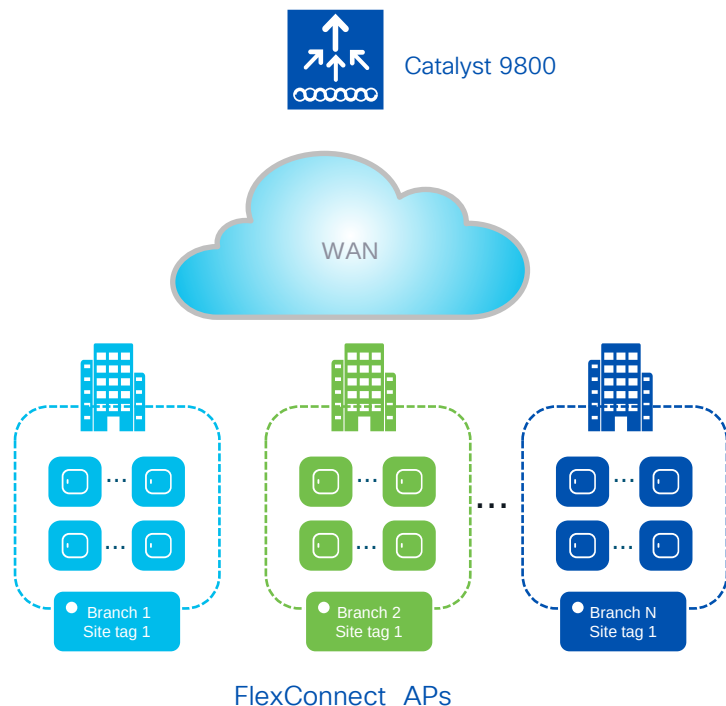
- For a site with FlexConnect APs, configure the site tag to be a non-local site (disable local site)

The 'Add Site Tag' configuration form is shown. It includes the following fields and options:

- Name*: Flex_site
- Description: Remote site
- AP Join Profile: default-ap-profile
- Flex Profile: default-flex-profile
- Fabric Control Plane Name: default-flex-profile
- Enable Local Site: ☐ (highlighted with a red box)
- Buttons: Cancel

- In this case the site tag is equivalent to the FlexConnect Group in AireOS

Site tag for FlexConnect deployments



Important facts:

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

PMK = Pairwise Master Key

Design- recommended use of AP site tags



For your
reference

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

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

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

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

RF Tag



First – a handy (free!) tool: WCAE

- **Wireless Config Analyser Express (WCAE)** is an extremely valuable tool when validating and optimising 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 Optimisation
 - 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](#)
[Draeger](#)
[Spectralink](#)
[Vocera](#)

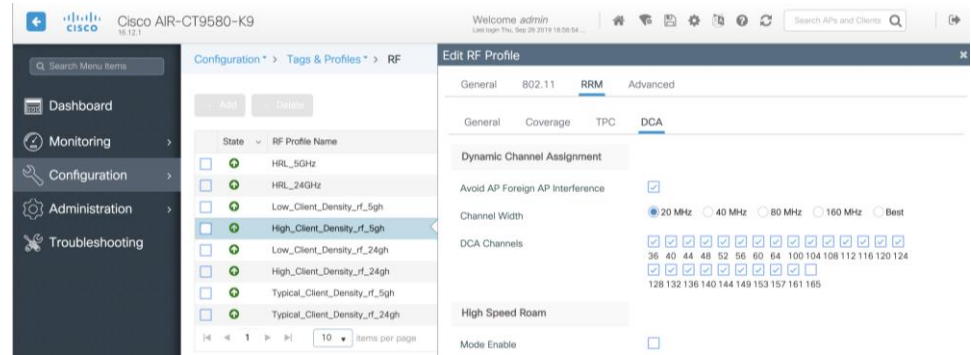
AP Information
[APs Configuration](#)
[APs Slot Configuration](#)
[APs Interface Status](#)
[APs RF Summary 2.4GHz](#)
[APs RF Summary 5GHz](#)
[APs RF Summary 6GHz](#)
[APs RF Health Details](#)
[APs NDP Summarization 2.4GHz](#)
[APs NDP Summarization 5GHz](#)
[APs RF Neighbors 2.4GHz](#)
[APs RF Neighbors 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](#)

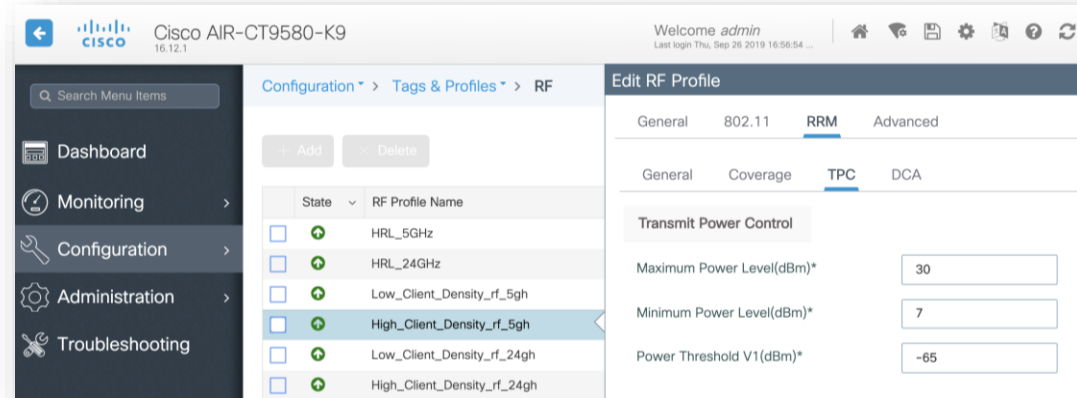
Channel planning with RF profiles

- 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

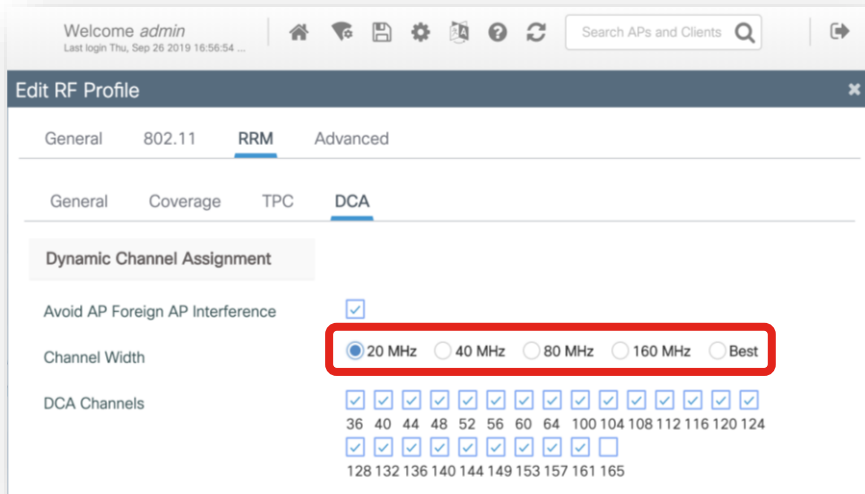


Balancing transmit power with RF profiles

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



Selecting channel width with RF profiles



5GHz

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

6GHz

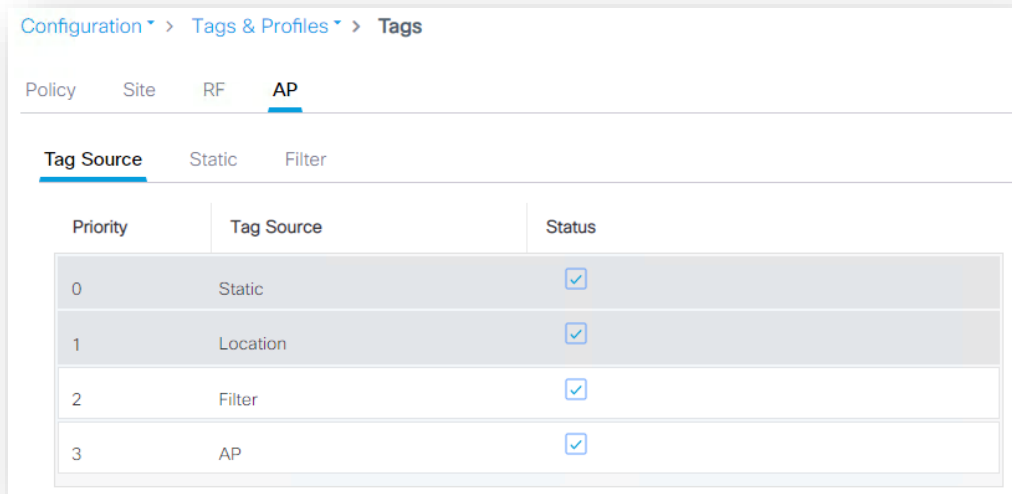
- Heavily dependent on regulatory domain
- Note! Higher channel width results in higher max Tx power for data frames (but not beacons – remember when surveying!)

APs to Tags Mapping



AP to tags assignment

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



Configuration > Tags & Profiles > Tags		
Policy	Site	RF
AP		
Tag Source		
Static	Filter	
Priority	Tag Source	Status
0	Static	☒
1	Location	☒
2	Filter	☒
3	AP	☒

- **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**

Configuration > Wireless > Access Points

▼ All Access Points

Total APs : 6

AP Name	AP Name
C9130-SJ-1	C9130-SJ-1
C9130-VIM	C9130-VIM

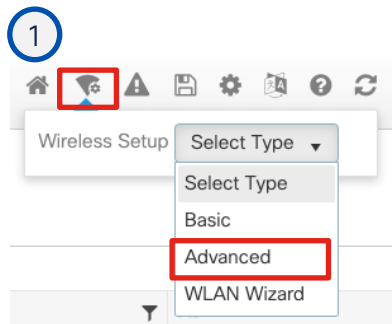
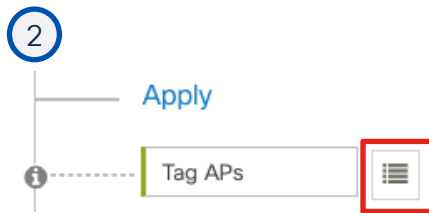
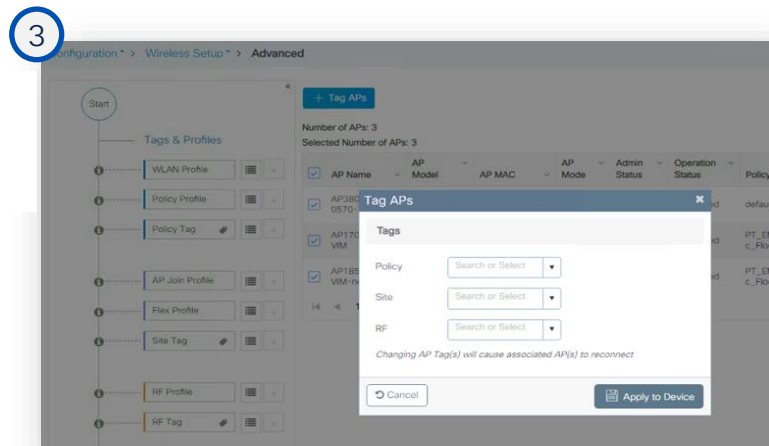
Edit AP

- General
- Interfaces
- High Availability
- Inventory
- ICap
- Advanced
- Support Bundle

General		Tags	
AP Name*	C9130-SJ-1	Policy	issu
Location*	Global/US-WEST/SJC-2	Site	site-8-500
Base Radio MAC	0c75.bdb3.a7e0	RF	default-rf-tag
Ethernet MAC	0c75.bdb5.fab8	Write Tag Config to AP	

AP to tags assignment – source: static

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



AP to tags assignment – source: filter

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

The screenshot displays the Cisco configuration interface for AP tags. On the left, the 'Configuration > Tags & Profiles > Tags' breadcrumb is visible. The 'AP' tab is selected, and the 'Filter' sub-tab is active. Below the 'Tag Source' (Static, Location, Filter) tabs, there are '+ Add' and '× Delete' buttons. A table lists the configured filter rules:

	Priority	Rule Name	AP name regex	Policy Tag Name
☐	1	site1	.site1.	flex-tag

At the bottom of the table, there are navigation controls showing page 1 of 10.

On the right, the 'Edit Tags' dialog is open. It contains the following fields:

- Rule Name*: site1
- AP name regex*: .site1.
- Active: YES (indicated by a green box)
- Priority*: 1
- Policy Tag Name: flex-tag (dropdown menu)
- Site Tag Name: site1 (dropdown menu)
- RF Tag Name: default-rf-tag (dropdown menu)

- 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)

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



Tags

Policy: OEAP-tag

Site: OEAP-site

RF: default-rf-tag

Write Tag Config to AP

AP to tags assignment – AP (SW >17.6)

Configuring AP tag persistency

Configuration > Tags & Profiles > Tags:

The screenshot shows the Cisco GUI for configuring AP tag persistency. The breadcrumb navigation is Configuration > Tags & Profiles > Tags. The 'AP' tab is selected under the 'Tags' section. Below the tabs, there are four sub-tabs: Tag Source, Static, Location, and Filter. The 'Tag Source' sub-tab is active, displaying a table with the following data:

Priority	Tag Source	Status
0	Static	☒
1	Location	☒
2	Filter	☒
3	AP	☒

Below the table, there is a note: 'Drag and Drop Tag Sources to change priorities'. Underneath, there are two checkboxes: 'Revalidate Tag Sources on APs' (unchecked) and 'Enable AP Tag Persistency' (checked). The 'Enable AP Tag Persistency' checkbox is highlighted with a red rectangle. At the bottom, there is an 'Apply' button.

- 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:

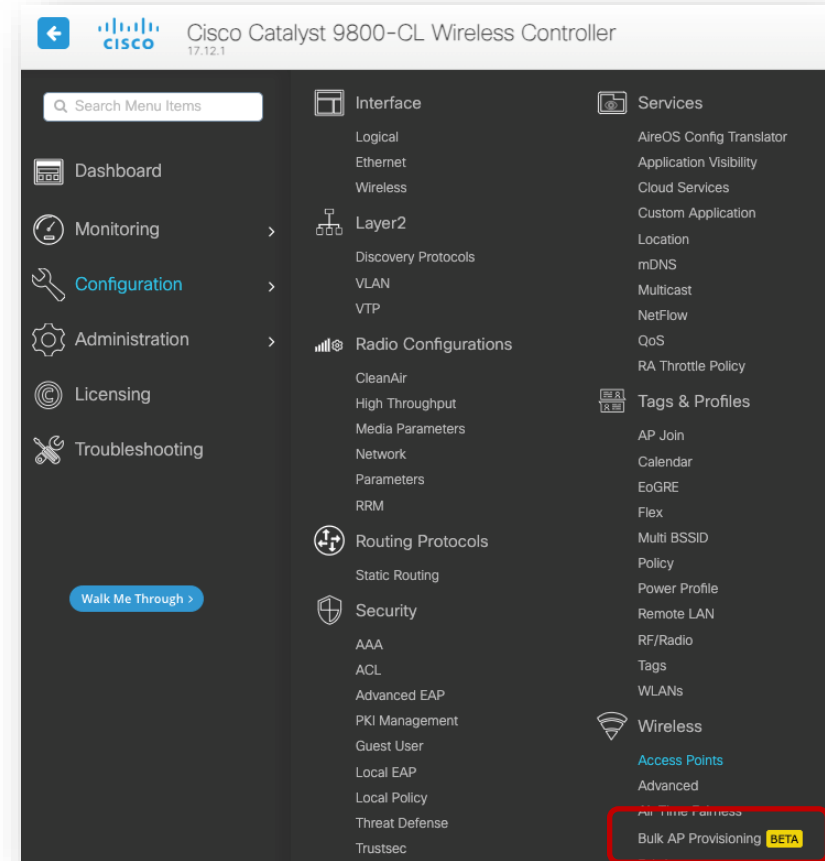
```
C9800#show ap tag summary
```

```
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

Configuration > Wireless > Bulk AP Provisioning

Select APs

Task Name*

☐	AP Name	AP Model	Up
☒	CW9164-simo	CW9164I-B	0 c
☐	Jason-9164	CW9164I-B	8 c

1 10

Exit

Configuration > Wireless > Bulk AP Provisioning

Select APs Select Parameters Summary

General

Admin Status Location

Geolocation

Height (meters) Height Uncertainty (meters)

Cable Length (meters) Floor

High Availability

	Name	Management IP Address (IPv4/IPv6)
Primary Controller	<input type="text" value="C9800-1"/>	<input type="text" value="13.56.6.186"/>
Secondary Controller	<input type="text" value="C9800-2"/>	<input type="text" value="10.2.2.10"/>
Tertiary Controller	<input type="text" value="C9800-3"/>	<input type="text" value="10.3.3.10"/>

Exit

CLI Preview

```
ap name <ap-name> controller tertiary C9800-3 10.3.3.10
ap name <ap-name> controller secondary C9800-2 10.2.2.10
ap name <ap-name> controller primary C9800-1 13.56.6.186
```

Back Next

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

Configuration > Wireless > Bulk AP Provisioning

Start a workflow to create a AP Provisioning task

Use this workflow to configure AP Parameters to one or more APs.

Chart displayed in every task tile represents the provision results, v

- APs with all configuration applied
- APs with some configuration applied
- APs with none of the configuration applied

Per AP specific parameters, like 'AP Name', can be config

Note: Results of previously provisioned tasks are not sync

AP Provisioning Task 2

Task Status: ✔ Completed

End Time: 09/21/2023 10:28:58

1 APs

AP Provisioning Task 1

Task Status: ✔ Completed

End Time: 09/21/2023 10:25:06

1 APs

Configuration > Wireless > Bulk AP Provisioning

Task Details

Parameter	Value	Applied CLI
Primary Controller Name	C9800-1	ap name <ap-name> controller primary C9800-1 13.56.6.186
Primary Controller IP	13.56.6.186	ap name <ap-name> controller primary C9800-1 13.56.6.186
Secondary Controller Name	C9800-2	ap name <ap-name> controller secondary C9800-2 10.2.2.10
Secondary Controller IP	10.2.2.10	ap name <ap-name> controller secondary C9800-2 10.2.2.10
Tertiary Controller Name	C9800-3	ap name <ap-name> controller tertiary C9800-3 10.3.3.10
Tertiary Controller IP	10.3.3.10	ap name <ap-name> controller tertiary C9800-3 10.3.3.10

AP Provision Results

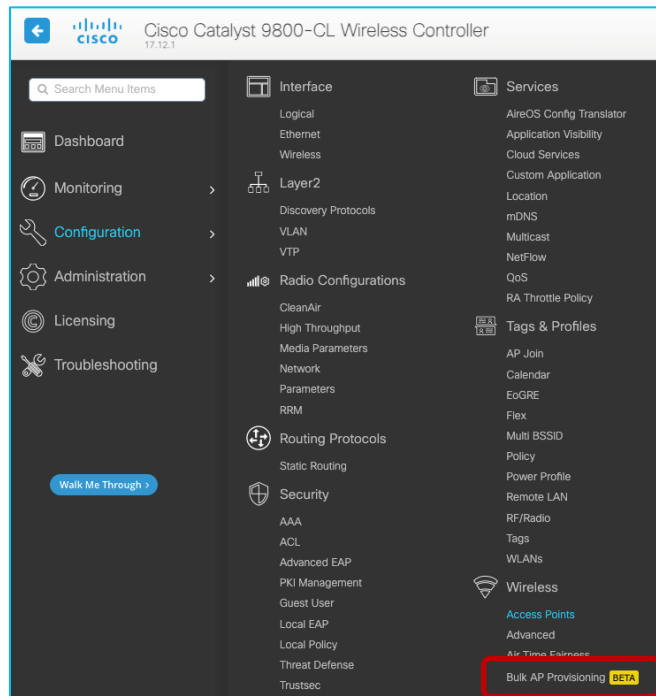
All configuration applied: 1 Some configuration applied: 0 None of the configuration applied: 0

AP Name	AP Status
CW9164-simo	All configuration applied

Configuration

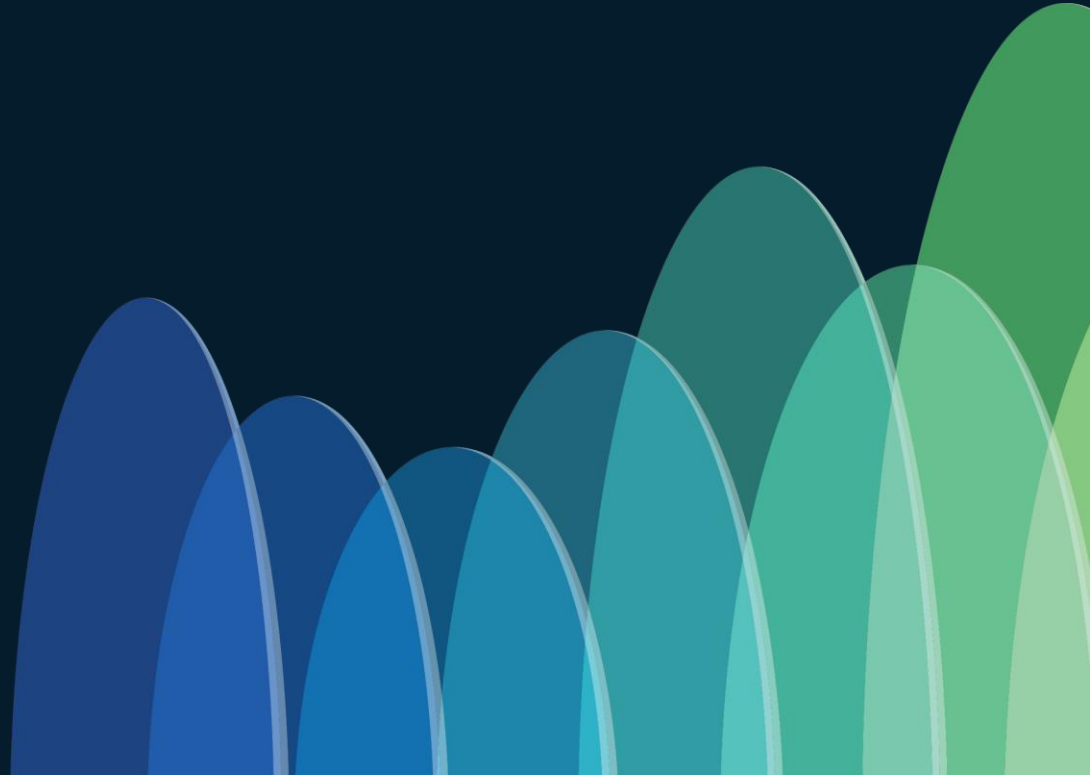
Configuration	Configuration Status	Details
Primary Controller Name	✔ Applied Successfully	
Primary Controller IP	✔ Applied Successfully	
Secondary Controller Name	✔ Applied Successfully	
Secondary Controller IP	✔ Applied Successfully	

AP bulk provisioning – what's next?



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

Day 2



AI-Enhanced RRM



AI-enhanced RRM key customer benefits

Better RF, better insights, reduced operational costs and time

AI-driven self-optimising RF

Leverages machine learning to find patterns and Optimise 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

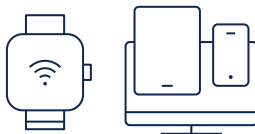
Performance visibility

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



Complete historical context

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



Actionable insights

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

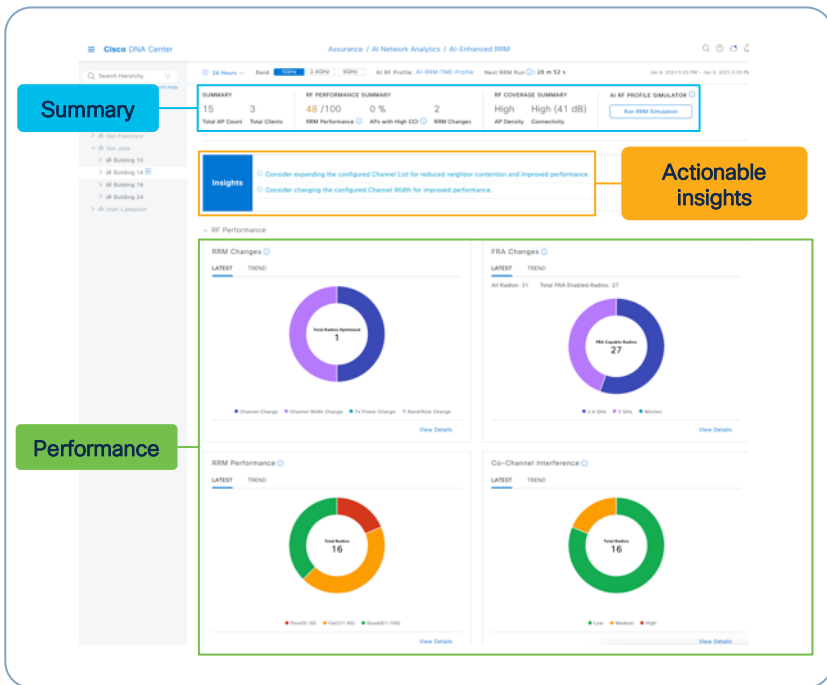
Simplified RRM configuration

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

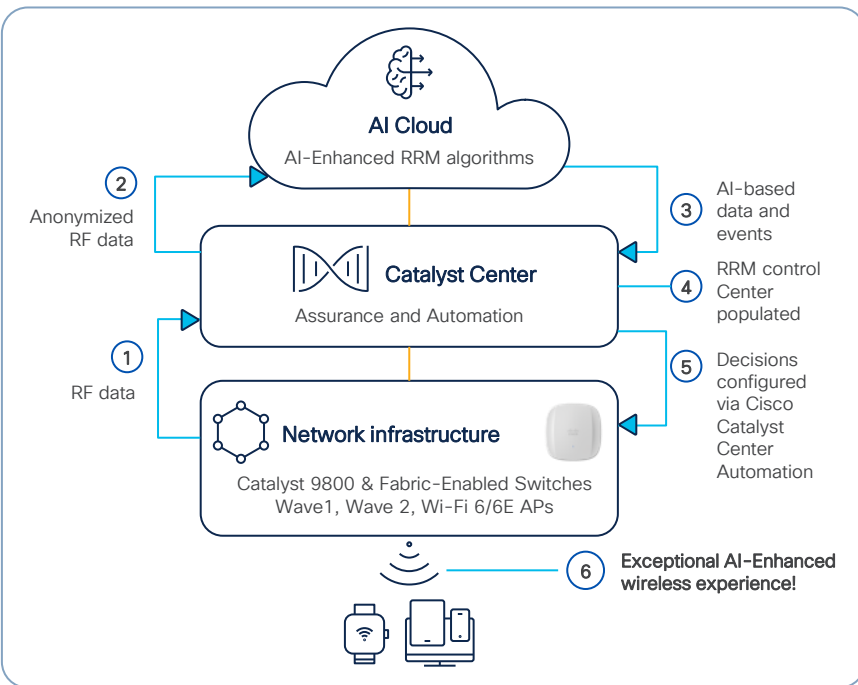
AI-enhanced RRM is AI that powers RF optimisation

Provides users with better Wi-Fi and admins with a better RF management experience!

Instantaneous visibility

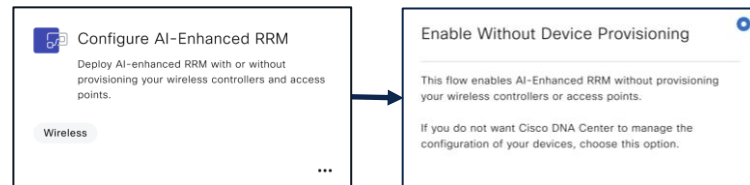


Proactive optimisations





What mitigates
these pain points?



New AI-enhanced RRM Workflow
for Assurance Only Customers!

AP Power Optimisation

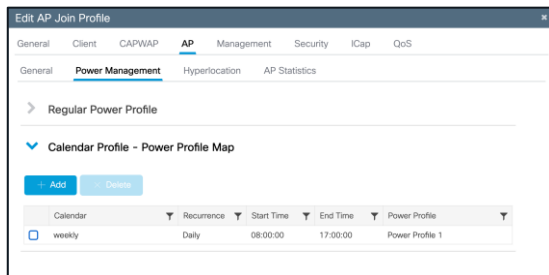


AP Power Optimisations Feature Suite

Save Power, Reallocate Power, and Visibility into Savings

AP Power Save Mode Lower AP Power Usage

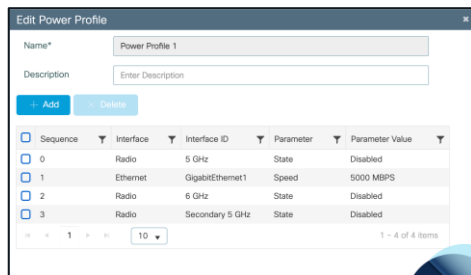
- Create a calendar profile for off-peak hours.
- Create a power profile to lower the power consumption budget during off-peak hours.
- Power profile: shut AP radio or lower spatial stream, lower port speed, disable USB port.



IOS-XE 17.8

AP Power Distribution Control over how power is

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



IOS-XE 17.10



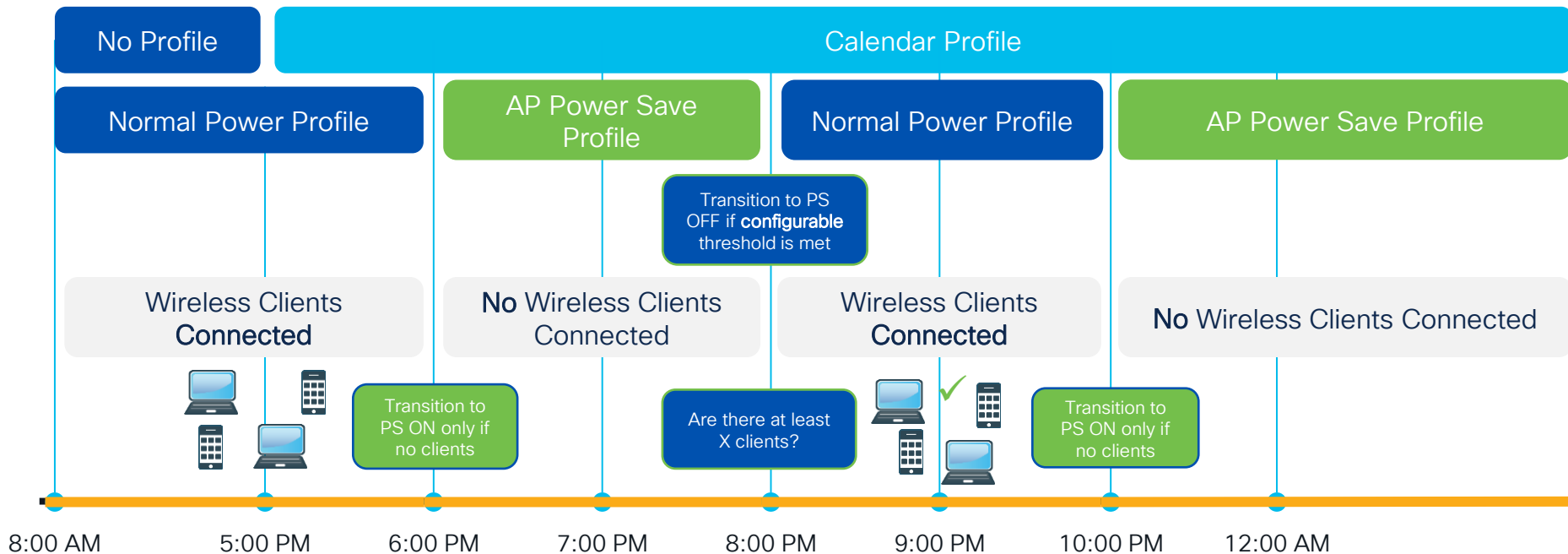
AP Power Savings Insight Power, Money, and Emissions Savings on Cisco Catalyst Center

- 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**

The image displays two screenshots of the Cisco C9800 configuration interface, specifically the 'Wireless Protection Policies' section under 'Security'.

Left Screenshot: Shows the full configuration page. The 'Rogue Policies' tab is selected. The 'Rogue Detection Security Level' is set to 'Custom'. The 'Expiration timeout for Rogue APs (seconds)*' is 1200. 'Validate Rogue Clients against AAA' and 'Validate Rogue APs against AAA' are unchecked. 'Rogue Polling Interval (seconds)' is 3600. 'Detect and Report Adhoc Networks' is checked. 'Rogue Detection Client Number Threshold*' is 0.

Right Screenshot: A zoomed-in view of the 'Rogue Policies' configuration page. The 'Rogue Detection Security Level' dropdown menu is highlighted with a red box, showing the 'High' option selected.

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.

Configuration > Radio Configurations > RRM

6 GHz Band **5 GHz Band** 2.4 GHz Band FRA

General Coverage DCA TPC RF Grouping Spatial Reuse

Profile Threshold For Traps

Interference Percentage*	10
Clients*	12
Noise*	-70
Utilization Percentage*	80
Throughput (Bps)*	1000000

Noise/Interference/Rogue/CleanAir/SI Monitoring Channels ⓘ

Channel List	All Channels ▼
RRM Neighbor Discover Type	Transparent ▼
RRM Neighbor Discover Mode	AUTO ☒

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.

Edit Rogue AP Rule

Rule Name*

Rule Type

State

Match Operation

Enable Rule ☒

Add Condition

Manage SSID ☒

User Configured SSID

User Configured substring-ssid

Buttons:

Buttons:

Buttons:

CleanAir Pro™



Introducing Cisco CleanAir Pro™

15 years of innovations and excellence carried forward



Cisco CleanAir®

RF ASIC-based excellence

Purpose built for 2.4- and 5-GHz wireless



Cisco CleanAir™ Pro

Evolving Wi-Fi excellence into 6 GHz

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

CleanAir Pro™ ML based classification

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



Cisco CleanAir Pro™

Detect/classify

CleanAir Pro =CA-Pro

5 GHz Video Camera is on
Channel 157

- All the CleanAir and CleanAir Pro radios agree – channel 157 is messed up and it is severe.
- Some Disagreement on device type
- All agree on the Duty Cycle

Monitoring > Wireless > CleanAir Statistics

5 GHz Band2.4 GHz Band

CleanAir Interference DevicesSI Interference DevicesAir Quality ReportWorst Air Quality Report

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

Cisco CleanAir Pro™

Detect/classify

CleanAir Pro =CA-Pro

5 GHz Video Camera is on
Channel 157

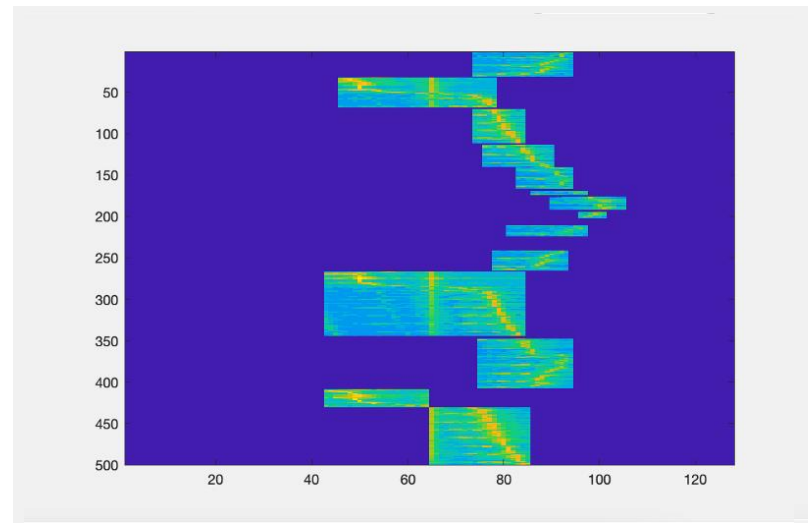
- C9130i_9f.6e.a0 see's 100% DC at -93 dBm and a minor severity of 5 (meh..)
- C9136 and CW9166 see it at -52 to -55 dBm with a high severity of 100 (very bad)

Monitoring > Wireless > CleanAir Statistics							
5 GHz Band		2.4 GHz Band					
CleanAir Interference Devices		SI Interference Devices		Air Quality Report		Worst Air Quality Report	
Cluster ID	Interferer Type	AP Name	Version	Severity	RSSI (dBm)	Duty Cycle (%)	Affected Channel
d500.0000.00ea	Continuous TX	C9130i_9f.6e.a0	CA	5	-93	100	157
d500.0000.00ea	Continuous TX	C9130i_9f.6e.a0	CA	4	-93	100	157
d500.0000.00ea	Video camera	Marlin_4_91.4260	CA	88	-65	100	157
d500.0000.00c9	WiFi Inv. Ch	Marlin_4_91.4260	CA	2	-81	1	144
d500.0000.00ea	Video camera	C9120_E-a2:9d:c0	CA	35	-86	100	157
d500.0000.00ea	Continuous TX	C9120_E-a2:9d:c0	CA	--	-80	100	157
d500.0000.010f	Video camera	CW9166i_Fe.0e20	CA-Pro	3	-76	100	157
d500.0000.011c	Continuous TX	CW9166i_Fe.0e20	CA-Pro	100	-52	100	157
d500.0000.011c	Continuous TX	C9136.5F:09e0	CA-Pro	100	-55	100	157
d500.0000.011c	Continuous TX	C9136_5f.f1.a0	CA-Pro	3	-74	100	157

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

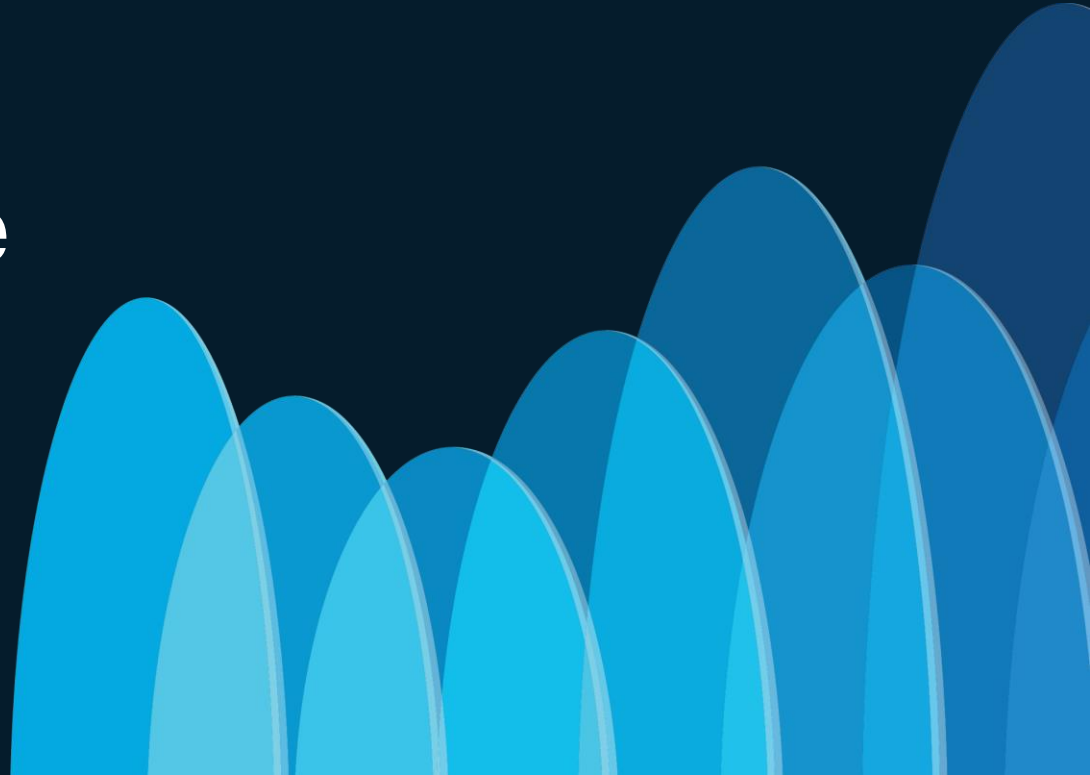


Microwave oven

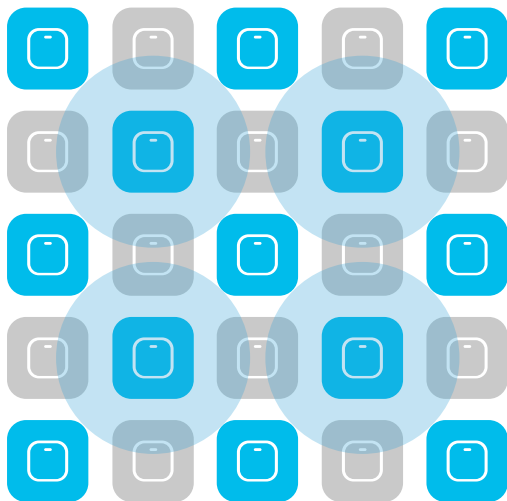
Software Updates



Rolling AP Update/Upgrade Infrastructure



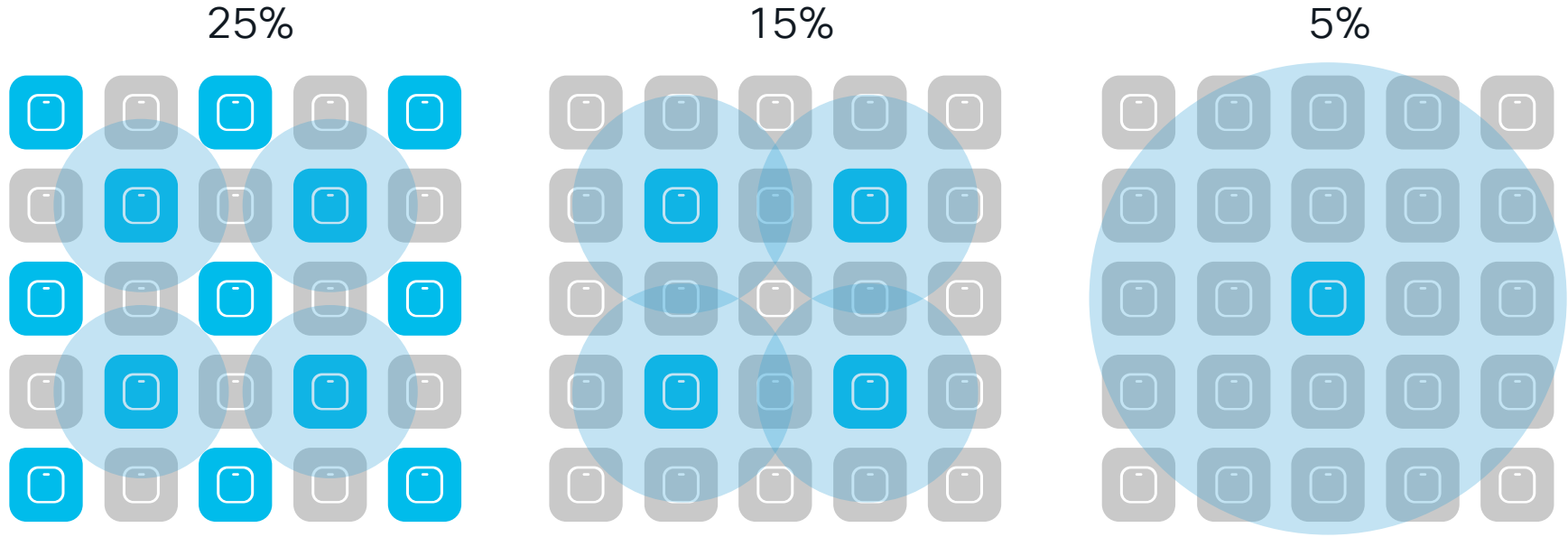
Rolling AP upgrade: neighbour AP marking



How does it work?

- Group APs into multiple groups and upgrade one group at a time.
- Grouping is done based on RF neighbours
- 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 $\sim 5 > \sim 1h$
 - For $P = 15\%$, $N = 12$, expected iterations all ap upgrade $\sim 12 > \sim 2h$
 - For $P = 5\%$, $N = 24$, expected iterations all ap upgrade $\sim 22 > \sim 4h$
- APs reload and re-join (AP image pre-download is used) determines the rolling AP upgrade time

Rolling AP upgrade: neighbour AP marking



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

Rolling AP upgrade: client steering

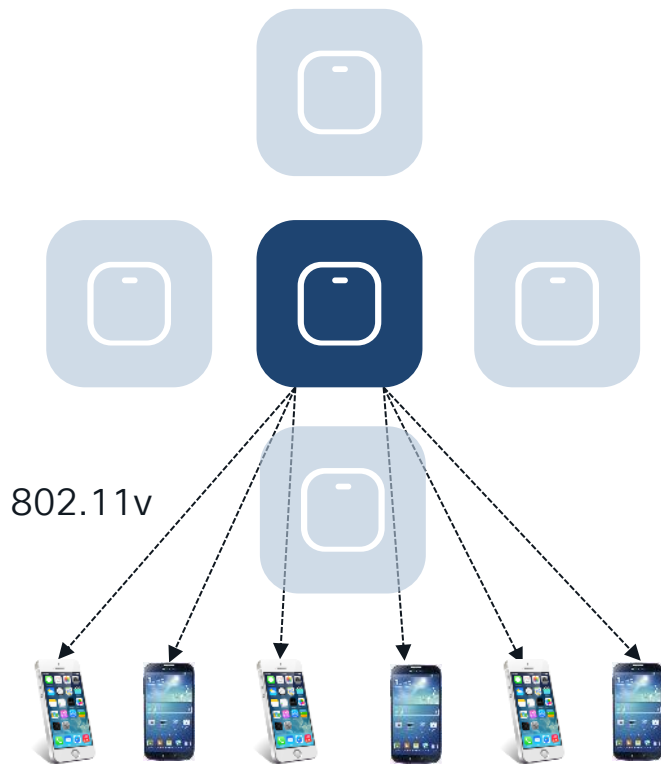
Clients steered from candidate APs to non-candidate APs

802.11v BSS transition request →
dissociation imminent

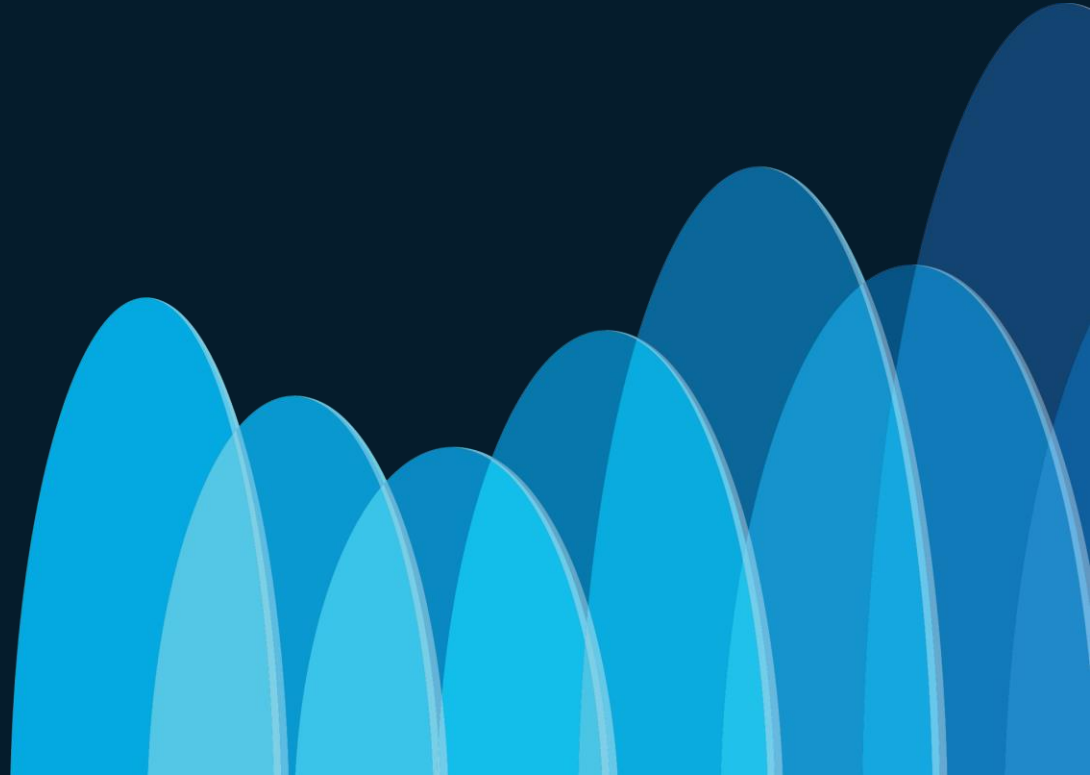
Clients that do not honour this will be de-
authenticated before AP reload

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

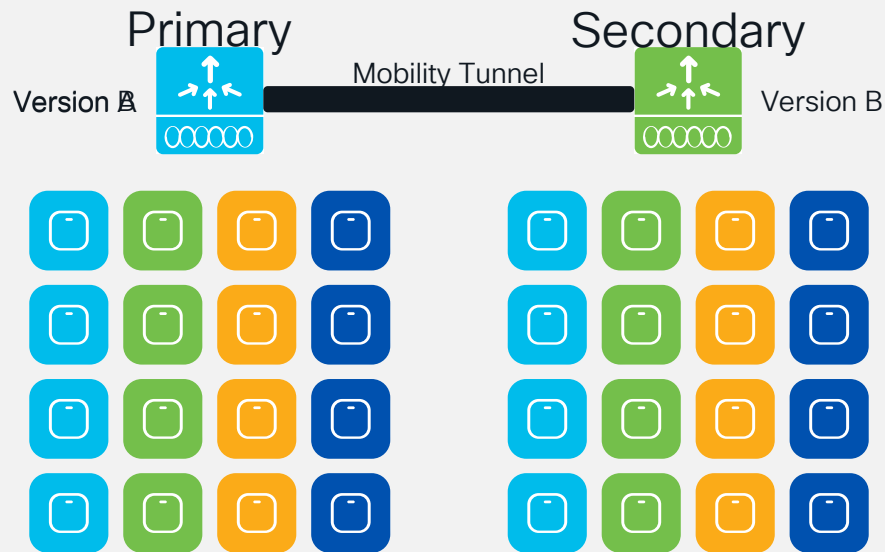
NEW



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

Configuration via WebUI

Mobility tunnel

Configuration > Wireless > Mobility

Global Configuration Peer Configuration

▼ Mobility Peer Configuration

+ Add × Delete ↺

MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
a453.0e9b.3b8b	10.27.0.5	N/A	default	0.0.0.0	::	N/A	N/A	3319b53f7bd5a9ac563ee59fb83e4260daed6c6b	N/A

1 - 1 of 1 items ↺

> Non-Local Mobility Group Multicast Configuration

Configuration via WebUI

Mobility tunnel

Add Mobility Peer

Primary Controller

MAC Address*

4c42.1e3d.0ccb

Peer IPv4/IPv6 Address*

10.27.0.11

↔️ Ping Success

Public IPv4/IPv6 Address

10.27.0.11

Group Name*

default ▼

Data Link Encryption

☐ DISABLED

SSC Hash

Enter SSC Hash (must contain 40 characters)

↶ Cancel

Apply to Device

MAC Address and IP Address of the WMI of the Secondary

Configuration via WebUI

Mobility tunnel

Add Mobility Peer

MAC Address*

a453.0e9b.3b8b

Peer IPv4/IPv6 Address*

10.27.0.5

↔️ Ping Success

Public IPv4/IPv6 Address

10.27.0.5

Group Name*

default ▼

Data Link Encryption

☐ DISABLED

SSC Hash

Enter SSC Hash (must contain 40 characters)

Cancel

Apply to Device

Secondary Controller

MAC Address and IP Address of the WMI of the Primary

Configuration via WebUI

Mobility tunnel

Configuration > Wireless > Mobility

Global Configuration

Peer Configuration

▼ Mobility Peer Configuration

+ Add

× Delete



	MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
	a453.0e9b.3b8b	10.27.0.5	N/A	default	0.0.0.0	::	N/A	N/A	3319b53f7bd5a9ac563ee59fb83e4260daed6c6b	N/A
☒	4c42.1e3d.0ccb	10.27.0.11	10.27.0.11	default	0.0.0.0	::	Up	1385		Disabled

1 - 2 of 2 items

➤ Non-Local Mobility Group Multicast Configuration

N+1 site based hitless upgrade with WebUI

1 Check the box for **Enable Hitless Upgrade**

2 Set the Site Filter to **Custom**

The screenshot shows the 'Software Management' page in the Cisco Catalyst 9800 WebUI. The left sidebar has a 'Software Upgrade' section with links for 'Software Maintenance Upgrade (SMU)', 'AP Service Package (APSP)', and 'AP Device Package (APDP)'. The main content area is titled 'Hitless Software Upgrade (N + 1 Upgrade)' and contains the following configuration options:

- Upgrade Mode:** A dropdown menu set to 'INSTALL'. To its right, it says 'Current Mode (until next reload): INSTALL'.
- Transport Type:** A dropdown menu set to 'Device'.
- File System:** A dropdown menu set to 'bootflash'. To its right, it says 'Free Space: 18459.29 MB'.
- File Path*:** A text input field containing '/C9800-L-universalk9_wlc.17.11.01.SPA.bin'.
- Enable Hitless Upgrade:** A checkbox that is checked. A red arrow points to this checkbox from the text '1 Check the box for Enable Hitless Upgrade'.
- Site Filter:** A dropdown menu set to 'Custom'. A red arrow points to this dropdown from the text '2 Set the Site Filter to Custom'.
- Site Tags*:** An empty text input field.
- Controller IP Address ((IPv4/IPv6)*):** An empty text input field.
- Controller Name*:** An empty text input field.
- AP Upgrade Configuration:** A section containing:
 - AP Upgrade per Iteration:** A dropdown menu set to '25 %'.
 - Client Steering:** A checkbox that is checked.
 - Accounting Percentage:** A dropdown menu set to '90 %'.

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**

Administration > Software Management

Software Upgrade

Software Maintenance Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

Upgrade Mode: INSTALL (Current Mode (until next reload): INSTALL)

Transport Type: Device

File System: bootflash (Free Space: 18459.29 MB)

File Path*: /C9800-L-universalk9_wlc.17.11.01.SPA.bin

Hitless Software Upgrade (N + 1 Upgrade)

Enable Hitless Upgrade: ☒

Site Filter: Custom

Site Tags*: SITE1 x SITE2 x

Controller IP Address (IPv4/IPv6)*

Controller Name*

AP Upgrade Configuration

AP Upgrade per Iteration: 25 %

Client Steering: ☒

Accounting Percentage: 90 %

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**

The screenshot displays the 'Hitless Software Upgrade (N + 1 Upgrade)' configuration page in the Catalyst 9800 WebUI. The page includes the following fields and settings:

- File System:** bootflash (Free Space: 18459.29 MB)
- File Path*:** /C9800-L-universalk9_wlc.17.11.01.SPA.bin
- Hitless Software Upgrade (N + 1 Upgrade):**
 - Enable Hitless Upgrade:** ☒
 - Site Filter:** Custom
 - Site Tags*:** SITE1 x, SITE2 x
 - Controller IP Address ((IPv4/IPv6)*):** 10.27.0.11
 - Controller Name*:** C9800-40-SSO
- AP Upgrade Configuration:**
 - AP Upgrade per Iteration:** 25 % (indicated by a red arrow)
 - Client Steering:** ☒ (indicated by a red arrow)
 - Accounting Percentage:** 90 % (indicated by a red box)
 - Accounting Action:** IGNORE (indicated by a red box)
 - Iteration Expiry:** 9 minutes (indicated by a red arrow)
- Buttons:** Download & Install (indicated by a red arrow), Save Configuration & Activate

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

There is an AP predownload/upgrade operation in progress. Please wait till it completes...

Upgrade Mode: Current Mode (until next reload): INSTALL

Transport Type:

File System: Free Space: 17214.04 MB

File Path*: 

Hitless Software Upgrade (N + 1 Upgrade)

Enable Hitless Upgrade: ☒

Site Filter:

Site Tags*:

Controller IP Address (IPv4/IPv6)*:

Controller Name*:

Status

- ✓ Download Image/Package
C9800-L-universalk9_wlc.17.11.01.SPA.bin
- ✓ Install Image/Package
- ✓ Update Site Filter
- ✓ AP Image Predownload
Total: 16
Initiated: 0
Predownloading: 0
Completed predownloading: 8
Failed to predownload: 0
- ⚙ AP Image Upgrade and Move...
Percentage complete: 0
- Activate Image/Package
- Commit

[AP Upgrade Statistics](#)

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

AP Upgrade Statistics		
Upgrade Status	:	In Progress
Percentage Complete	:	25
From Version	:	17.9.3.50
To Version	:	17.11.0.155
Started at	:	05/17/2023 12:51:05 PST
Expected time of completion	:	05/17/2023 12:57:05 PST
Number of APs		
Upgraded	:	2
In Progress	:	2
Remaining	:	4

AP Name	Radio MAC	Status
SITE2-9120-1	c064.e422.dfe0	Upgraded and Joined Member
SITE1-9162-1	ecf4.0c20.d3e0	Upgraded and Joined Member
SITE1-9166-1	10f9.20fd.bac0	In-Progress
SITE2-9120-3	c4f7.d54b.a6e0	In-Progress
SITE2-9120-4	a00f.3704.9fa0	Remaining
SITE1-9136-1	c828.e5ed.9110	Remaining
SITE1-9166-2	e438.7e43.7f20	Remaining
SITE2-9120-2	f4bd.9ea0.c7a0	Remaining

10 1 - 8 of 8 items

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**

Manage

[Remove Inactive Files](#)

[Rollback](#)

Status

✓ Download Image/Package
C9800-L-universalk9_wlc.17.11.01.SPA.bin

✓ Install Image/Package

✓ Update Site Filter

✓ AP Image Predownload

Total: 8
Initiated: 0
Predownloading: 0
Completed predownloading: 8
Failed to predownload: 0

✓ AP Image Upgrade and Move
Percentage complete: 100

➤ Activate Image/Package

➤ Commit

[Show Logs](#)

[AP Upgrade Statistics](#)

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

Hitless Software Upgrade (N + 1 Upgrade)

Enable Hitless Upgrade ☒

Site Filter Custom

Site Tags* SITE1 X SITE2 X SITE3 X

Controller IP Address (IPv4/IPv6)* 10.27.0.11

Controller Name* C9800-40-SSO

AP Upgrade Configuration

AP Upgrade per Iteration 25 %

Client Steering ☒

Accounting Percentage 90 %

Accounting Action IGNORE

Iteration Expiry 9 minutes

Download & Install Update Site Filter Remove Site Filter Save Configuration & Activate

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

Hitless Software Upgrade (N + 1 Upgrade)

Enable Hitless Upgrade ☒

Site Filter Custom

Site Tags* SITE1 X SITE2 X SITE3 X SITE4 X

Controller IP Address (IPv4/IPv6)* 10.27.0.11

Controller Name* C9800-40-SSO

AP Upgrade Configuration

AP Upgrade per Iteration 25 %

Client Steering ☒

Accounting Percentage 90 %

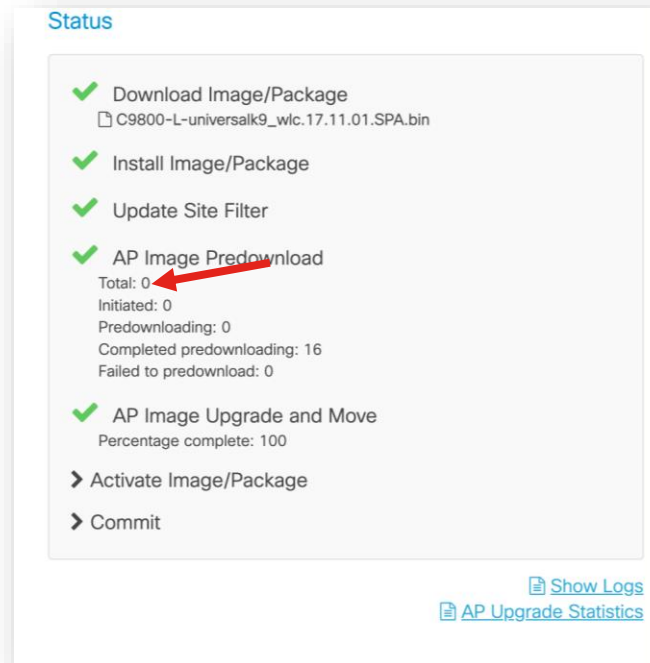
Accounting Action IGNORE

Iteration Expiry 9 minutes

Download & Install Update Site Filter Remove Site Filter Save Configuration & Activate

N+1 site based hitless upgrade with WebUI

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



Status

- ✓ Download Image/Package
C9800-L-universalk9_wlc.17.11.01.SPA.bin
- ✓ Install Image/Package
- ✓ Update Site Filter
- ✓ AP Image Predownload
Total: 0
Initiated: 0
Predownloading: 0
Completed predownload: 16
Failed to predownload: 0
- ✓ AP Image Upgrade and Move
Percentage complete: 100
- Activate Image/Package
- Commit

[Show Logs](#)
[AP Upgrade Statistics](#)

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

Hitless Software Upgrade (N + 1 Upgrade)

Enable Hitless Upgrade ☒

Site Filter

Site Tags* SITE1 x SITE2 x SITE3 x SITE4 x

Controller IP Address (IPv4/IPv6)*

Controller Name*

AP Upgrade Configuration

AP Upgrade per Iteration

Client Steering ☒

Accounting Percentage

Accounting Action

Iteration Expiry

[Download & Install](#) [Update Site Filter](#)

[Remove Site Filter](#) [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

Administration > Software Management

Software Upgrade

Software Maintenance Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

Upgrade Mode

Current Mode (until next reload): INSTALL

One-Shot Install Upgrade

☐

Transport Type

File System

Free Space: 17213.58 MB

Source File Path*

Select File

ISSU Upgrade (HA Upgrade)

☐

Download & Install

Save Configuration & Activate

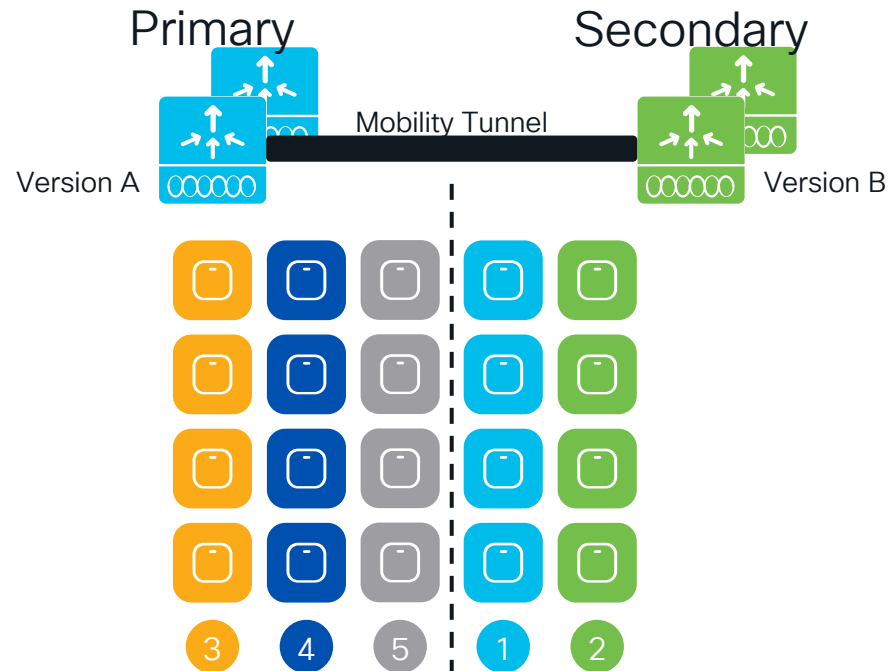
Commit

Can I use HA SSO pair with N+1 rolling upgrade?

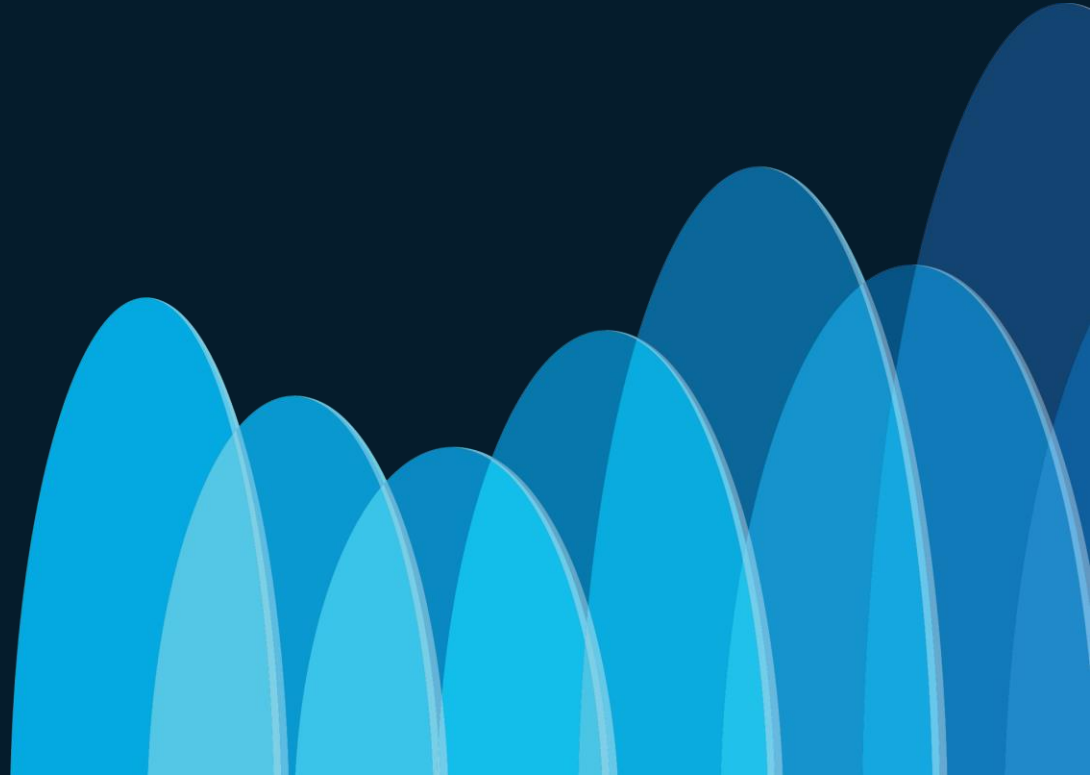
Customers can stay in secondary HA pair and reduce the upgrade process by half

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

Flexibility to upgrade each site while ensuring resiliency



In-Service Software Upgrade (ISSU)



Why ISSU?

Eliminate network downtime during controller upgrade process



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



Automate the process of upgrade without manual intervention



What is ISSU ?



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



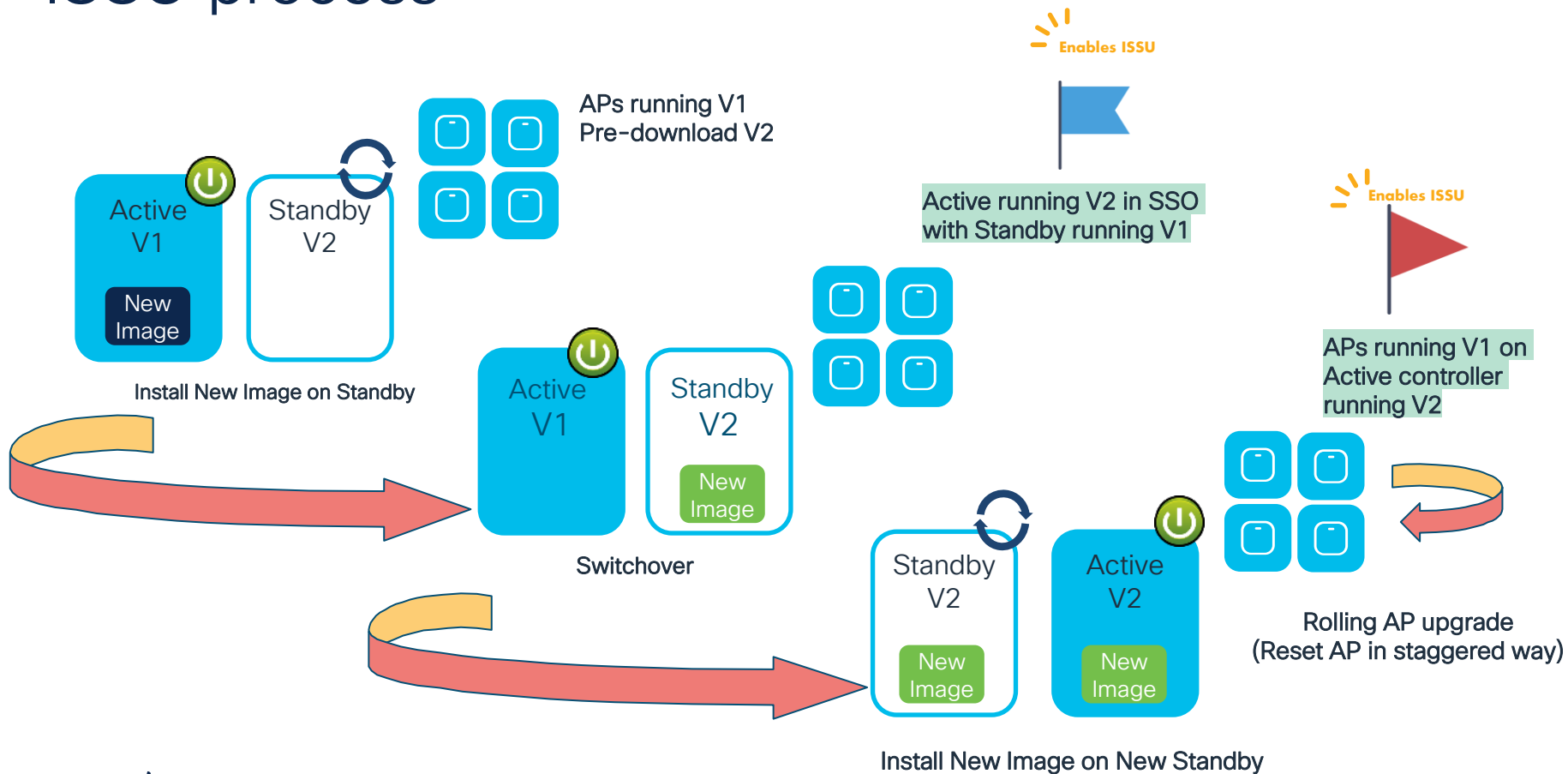
All AP/Client sessions are retained during upgrade process



Pre-requisites:

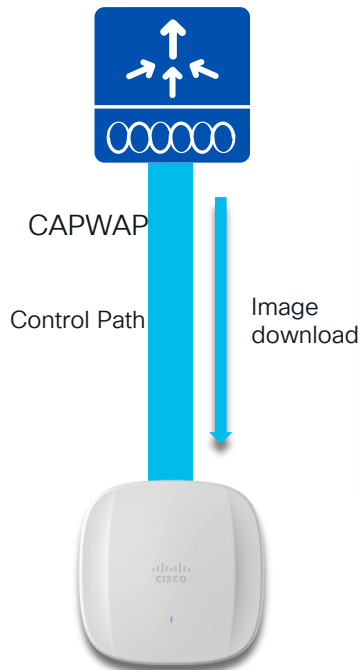
- ✓ Base image is ISSU capable
- ✓ SSO pair in Active-Hot Standby
- ✓ Controllers in INSTALL mode

ISSU process



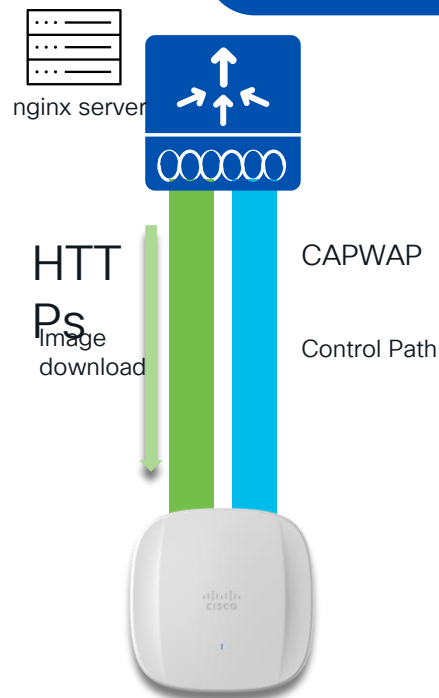
How can I improve AP image download time?

Before IOS XE 17.11.1



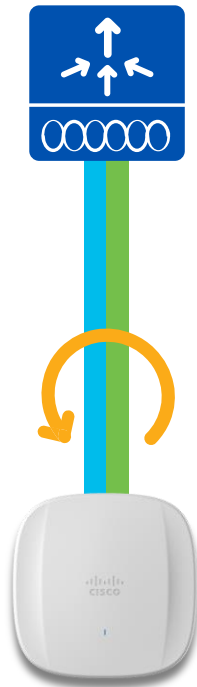
- AP image download happens over CAPWAP Control Path
- Slow by limitation with CAPWAP window size
- Image downloads WNCd process increases CPU work-load

After IOS XE 17.11.1



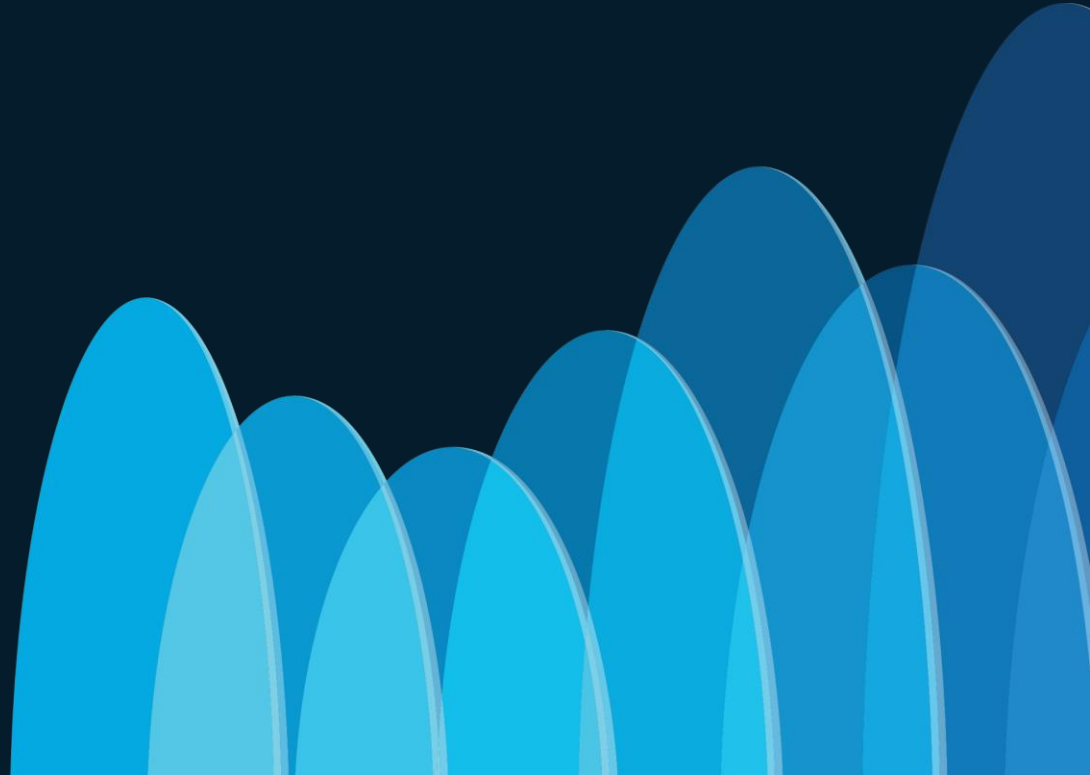
- AP image download happens over HTTPs
- Fast download speed
- Reduce CPU load and frees up CAPWAP

Fallback to CAPWAP if HTTPs failure



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

Wireless Controller SMU (Software Maintenance Update)



Controller SMU

Standalone vs redundant wireless controller

Hot Patch
(No Wireless Controller reboot)
Auto Install on Standby

Cold Patch
Wireless Controller Reboot

Standalone
box



No reload of Controller. AP and client session won't be affected.



Reload controller. AP and client sessions would be affected.

Redundant
box



SMU activation applies patch on active and standby. There is no controller reload and there is no impact to AP and client sessions.



Follows ISSU path and both standby and active controller reloaded but there is no impact to AP and client session.

CLI required for ISSU

Per-site & Per- AP Model AP Service Pack

APSP workflow

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

ap image site-filter file APSP1 add SiteA

Install prepare activate

Install activate

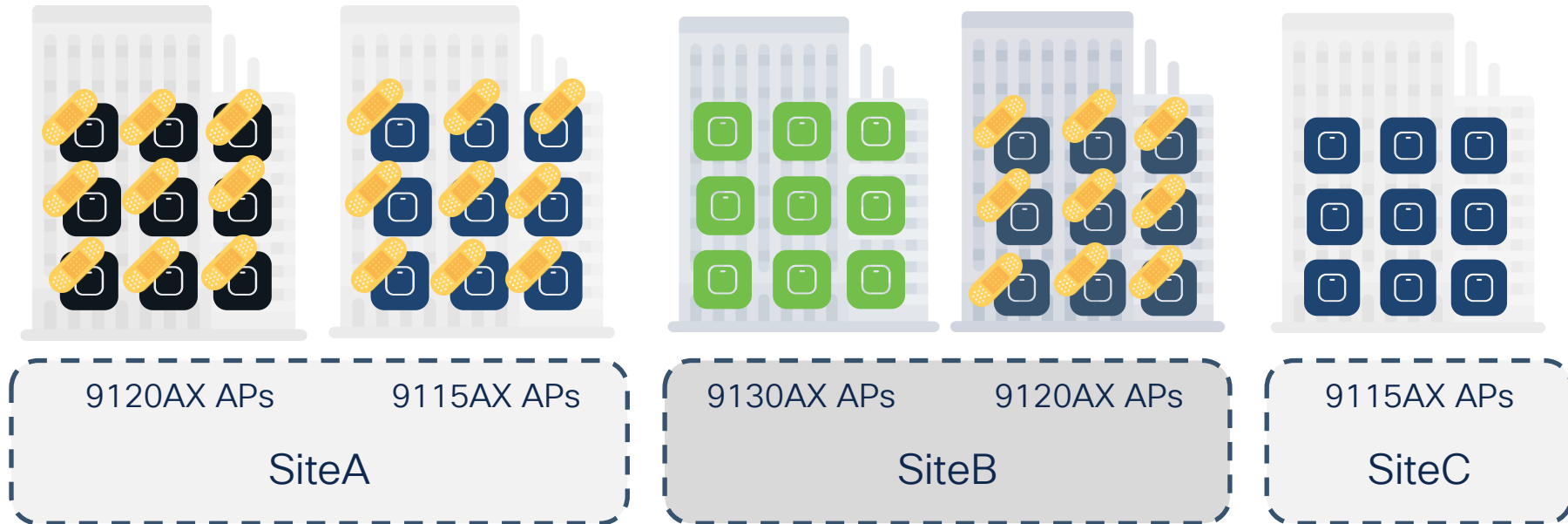
Install commit

ap image site-filter file APSP1 add Site B

ap image file APSP1 site-filter apply

Not applicable for building with 9130AX

Apply on Site A in rolling AP fashion



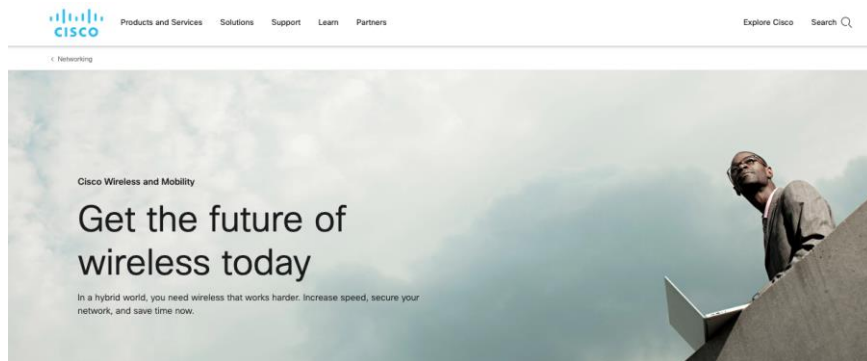
More info?



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-aios ircm_dg.html

Networking

Wi-Fi 6/6E

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

BRKEWN-1538

Internet of Things on the Next Generation Cisco Catalyst Wireless Wi-Fi 6E Access Points

FINISH

Networking

Wireless Automation & Troubleshooting

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



START

Monday, 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

FINISH

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.

BRKEWN-2306

Wireless Network Automation and
Assurance with Cisco Catalyst
Center

EoS/EoL update - WLC



Reference

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



Reference

Product	End of Sale	EoS 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
EoS = End of Software Maintenance
EoVSS = End of Vulnerability Software Support
LDoS = Last Day of Support

Keynote Deep Dives

Wednesday
10:30am – 11:30am



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

Level 1
Room 106



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

Level 2
Room 204



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

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



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



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



Continue your education



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

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

FINISH

Thursday, June 6 | 9:30 a.m.

BRKEWN-2658

Implement and Troubleshoot Cisco Spaces to Deliver Next-Generation Location-Based Solutions

Thursday, June 6 | 1:00 p.m.

BRKEWN-2037

OpenRoaming Under the Hood



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC