The bridge to possible

Successful Migration and Deployment Best Practices for Catalyst 9800 Wireless Networks

Simone Arena, Principal Technical Marketing Engineer, Cisco Wireless

cisco Live! runs on Catalyst Wireless stack!!

YOU are living the Migration!

cisco SPACES

Cisco DNA Center

Cisco Catalyst 9800

Catalyst 9100 Wi-Fi 6 and 6E

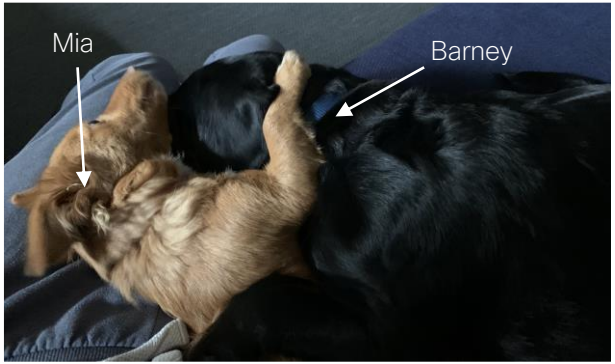
cisco Live!

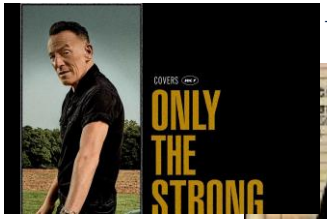
The bridge to possible

Successful Migration and Deployment Best Practices for Catalyst 9800 Wireless Networks

Simone Arena, Principal Technical Marketing Engineer, Cisco Wireless

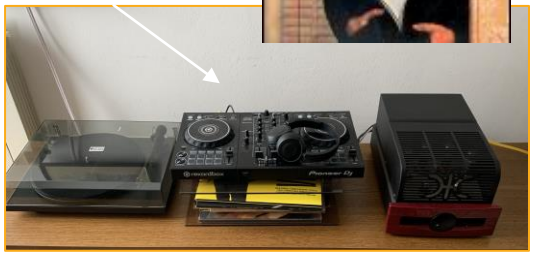
My two Princesses





The Boss, what else??

Tube amplifier



Sagrantino di Montefalco
Caprai 2013

Fiorentina soccer fan

Agenda

- Building a Migration Strategy
- Migration Best Practices
- AireOS configuration migration
- Design with Access Point (AP) tags in mind
- Wi-Fi 6E: what's the impact on migration?
- AireOS and IOS-XE coexistence
- More info…

Cisco Webex App

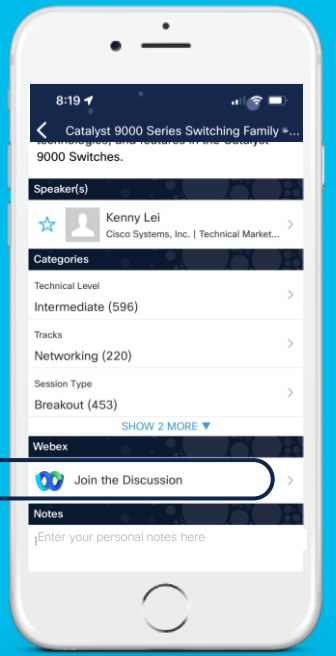
Questions?

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 until February 24, 2023.

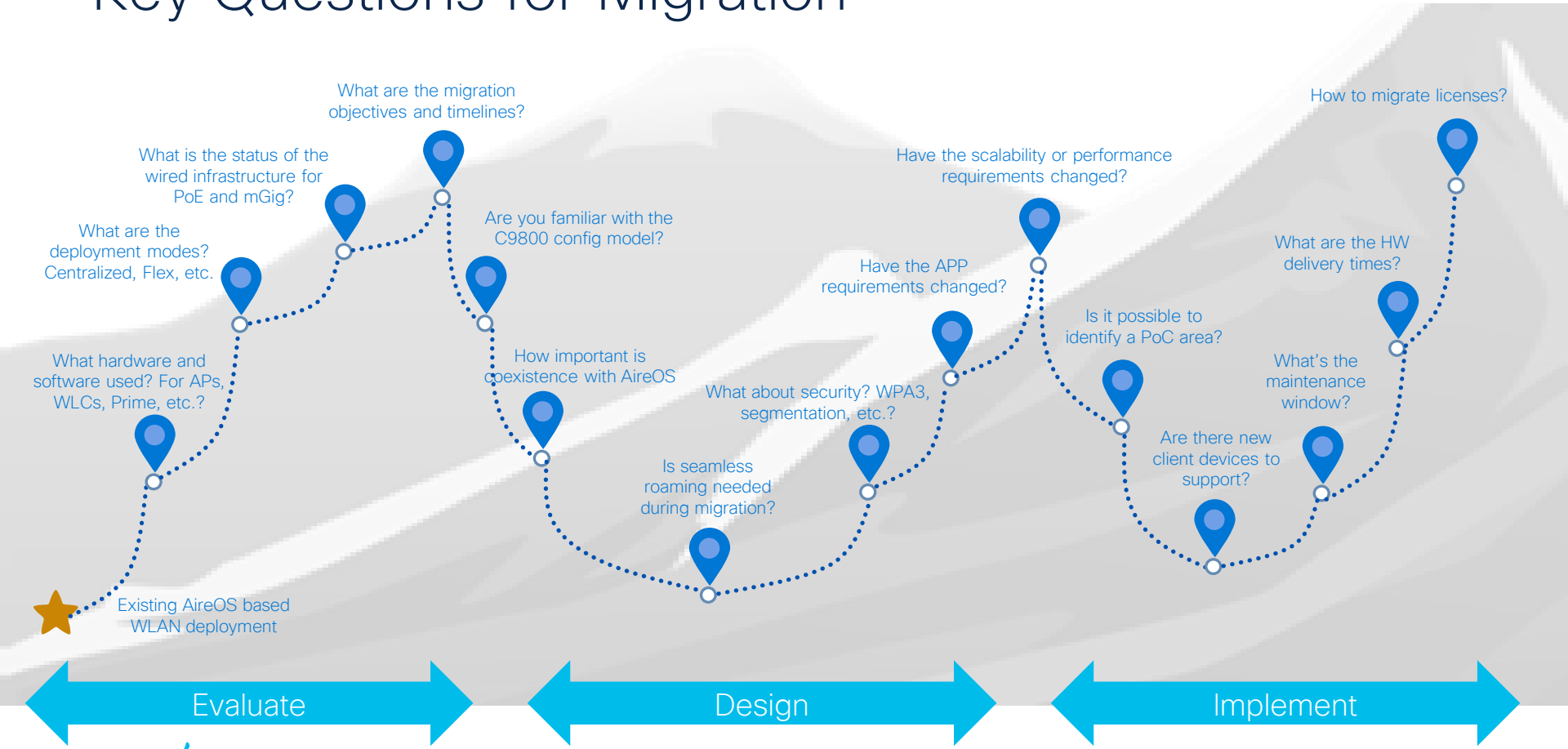


Building a Migration Strategy

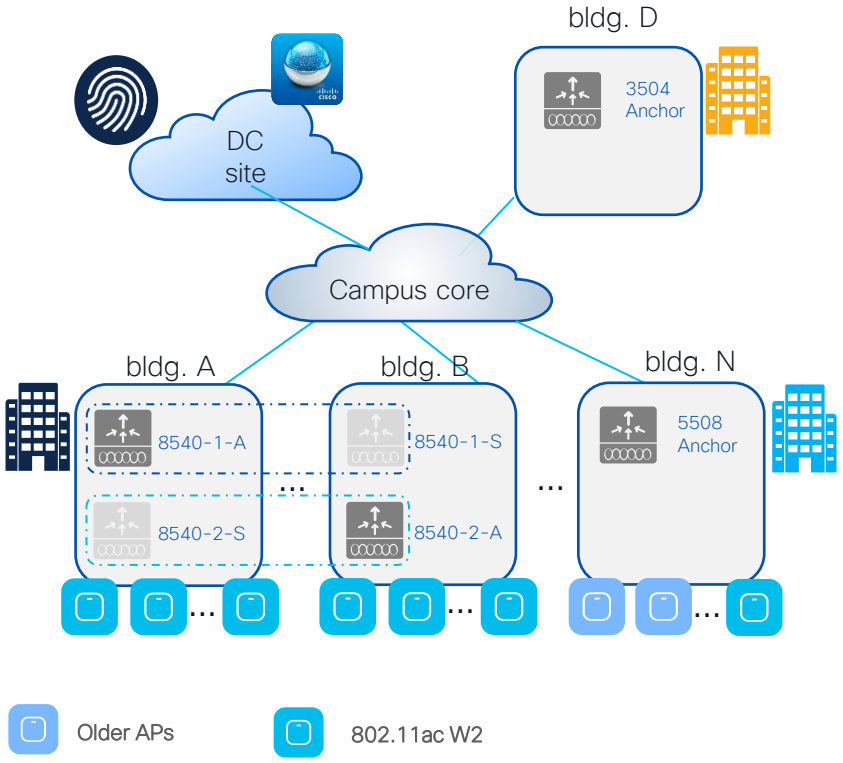
Where shall I start?

....asking questions!

Key Questions for Migration



Customer Migration scenario

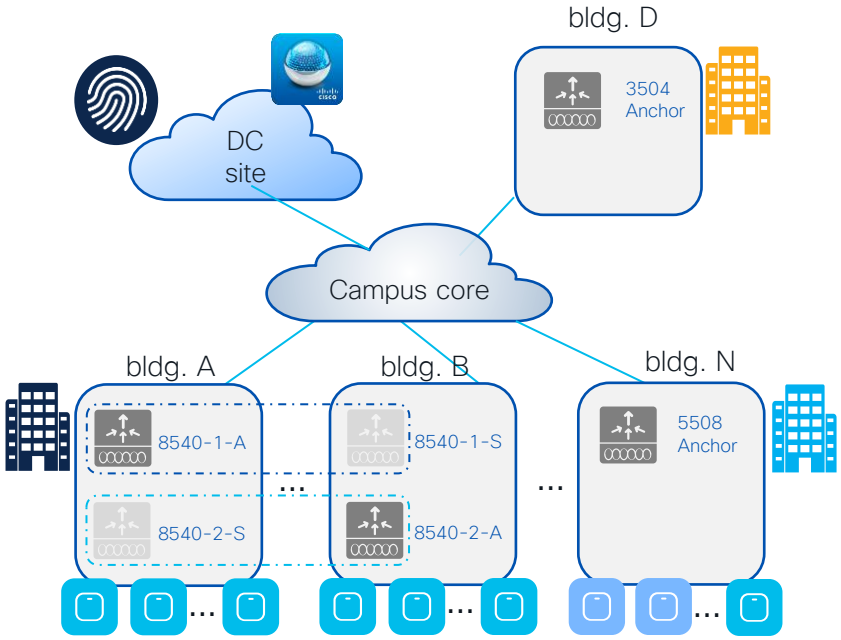


Current deployment:

- University main campus: 100+ buildings, 5k APs, 35k peak of concurrent connected clients. Single roaming domain
- AireOS WLCs: two pairs of 8540 in SSO HA pair running 8.10. Guest Anchor Controllers: 5508 running 8.5 and 3504 running on 8.10
- Mix of 802.11ac Wave 2 (AP 3800, 1815, 1560) and older Access Points (APs 3600 and 3700). Started Wi-Fi 6 journey with Catalyst 9120 and 9130
- Prime for configuration and monitoring. ISE as Radius server and guest portal

WLC = Wireless LAN Controller
HA = High Availability
SSO = Stateful Switch Over

Customer Migration scenario

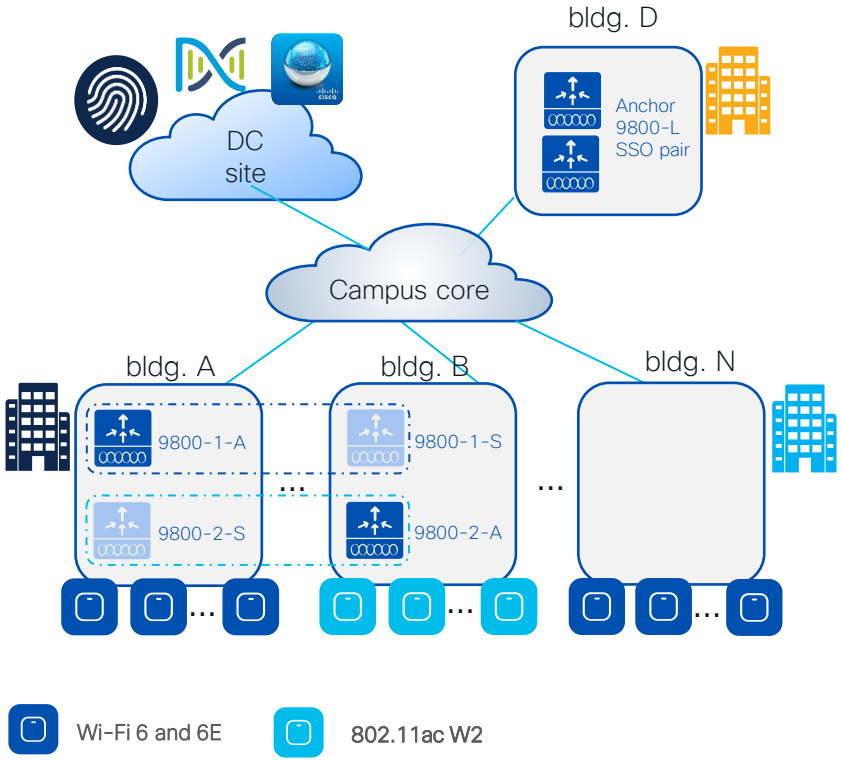


Customer requirements:

- Migrate to the new Catalyst wireless stack with C9800 wireless controllers and Catalyst APs. Leverage new features on Catalyst 9800 like ISSU
- Refresh old WLCs in End of Sale (EoS) and consolidate; provide Guest Anchor redundancy
- Replace 802.11ac Wave1 and older APs. Adopt Wi-Fi 6E, Catalyst 9136 as reference model for Wi-Fi 6E
- Need to pace migration as APs will be replaced in multiple steps. Need coexistence between legacy and new network. Seamless roaming is key
- Introduce DNA Center for visibility and Assurance

ISSU = In-Service Software Upgrade

Customer Migration scenario



Migration considerations:

- Keep same architecture and design for Foreign WLCs
- Consolidate Anchor WLCs in one building and configured in SSO pair
- Older APs replaced with Wi-Fi 6/6E; Wi-Fi 5 are kept. The plan is to eventually migrate all the APs to Wi-Fi 6/6E
- Migration started with code 17.3.x for Catalyst 9800 (C9800), initial lab tests with 17.3.6. Later tests with 17.9.1; finally, customer went in production with 17.9.2
- Keep Prime for now and start deploying Cisco DNA Center for Assurance

Build a Migration Strategy – three phases

Evaluate

- Understand customer requirements
- Evaluate current deployment
- Evaluate possible product gaps
- Evaluate new licensing model
- Get all the required information (topology, device lists, design requirements, configuration)

Migration factors/triggers:

- End of Sales (EoS) announcement for all AireOS controllers*
- EoS announcement of 802.11ac Wave1 APs (x700 series)
- EoS announcement of 802.11ac Wave2 APs (x800 series)
- AP hardware not supported on AireOS (C9124 and Wi-Fi6E)
- New functionalities on C9800 (ISSU, Patching, Programmability, etc.)

Note:

- Software 17.3.x is the last train to support 802.11ac Wave 1 APs (x700 series). Exception: Industrial Wireless 3700 Series AP
- No support for 802.11n or older APs on C9800

(*) Go to https://www.cisco.com/c/en/us/products/wireless/index.html#~resources for latest EoS announcements

EoS/EoL Update – WLC

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

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

EoS/EoL Update – Access Points

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

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

Build a Migration Strategy – three phases

Evaluate

- Understand customer requirements
- Evaluate current deployment
- Evaluate possible product gaps
- Evaluate new licensing model
- Get all the required information (topology, device lists, design requirements, configuration)

Design

- Architecture review
- Migrate the AireOS configuration
- Feature gap verification
- Design with profiles and tags in mind
- Choose the right software release
- Brownfield considerations

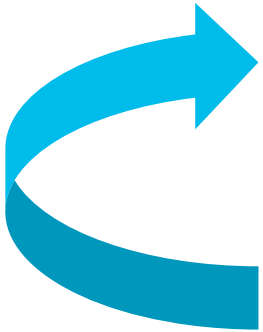
Implement

- Lab validation
- Identify pilot migration areas
- Deploy an area in production
- Start replacing legacy APs
- Post migration checks
- Monitor stability and proceed

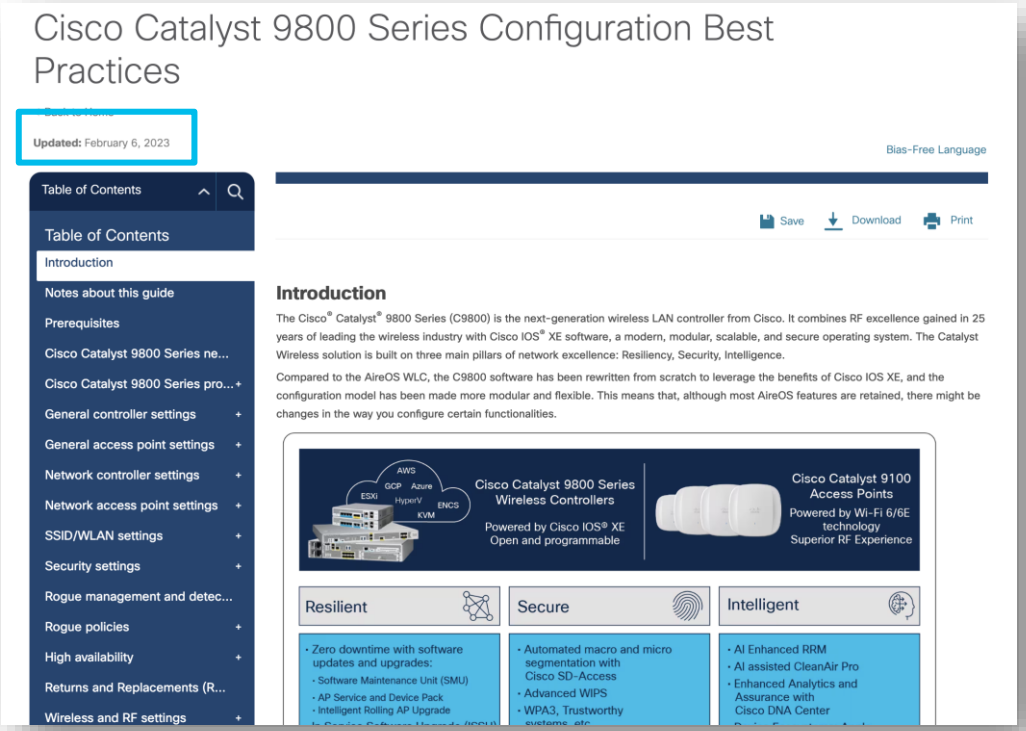
Migration Best Practices

Migration Best Practices

Refer to the latest Best Practice on Cisco Connection On-line (CCO)



Just updated!

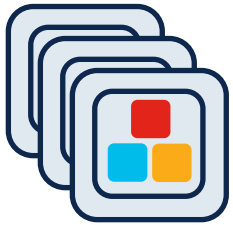


https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html

Migration Best Practices

Deep knowledge of C9800 new configuration model (Profiles & Tags)

Access Points



RF Tag

Policy Pag

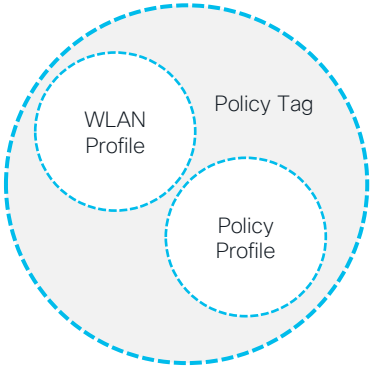
Site Tag

Important to remember:

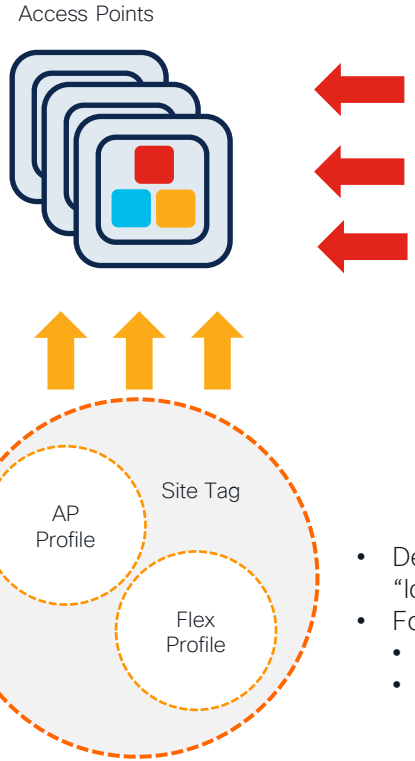
- Profiles (Policy, AP Join and Radio Frequency (RF)) and tags are the new configuration constructs
- Profiles are assigned via tags. Every AP needs to be assigned to the three AP tags (Policy, Site, RF)
- Advantages of the new configuration models:
  - Modular and reusable config constructs
  - Flexible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

Migration Best Practices

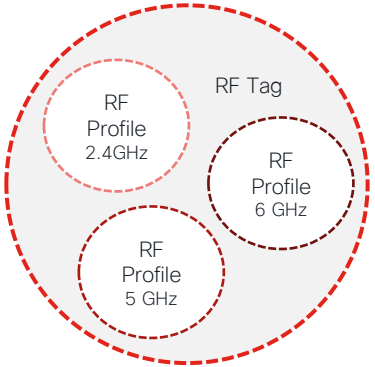
Deep knowledge of C9800 new configuration model (Profiles & Tags)



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

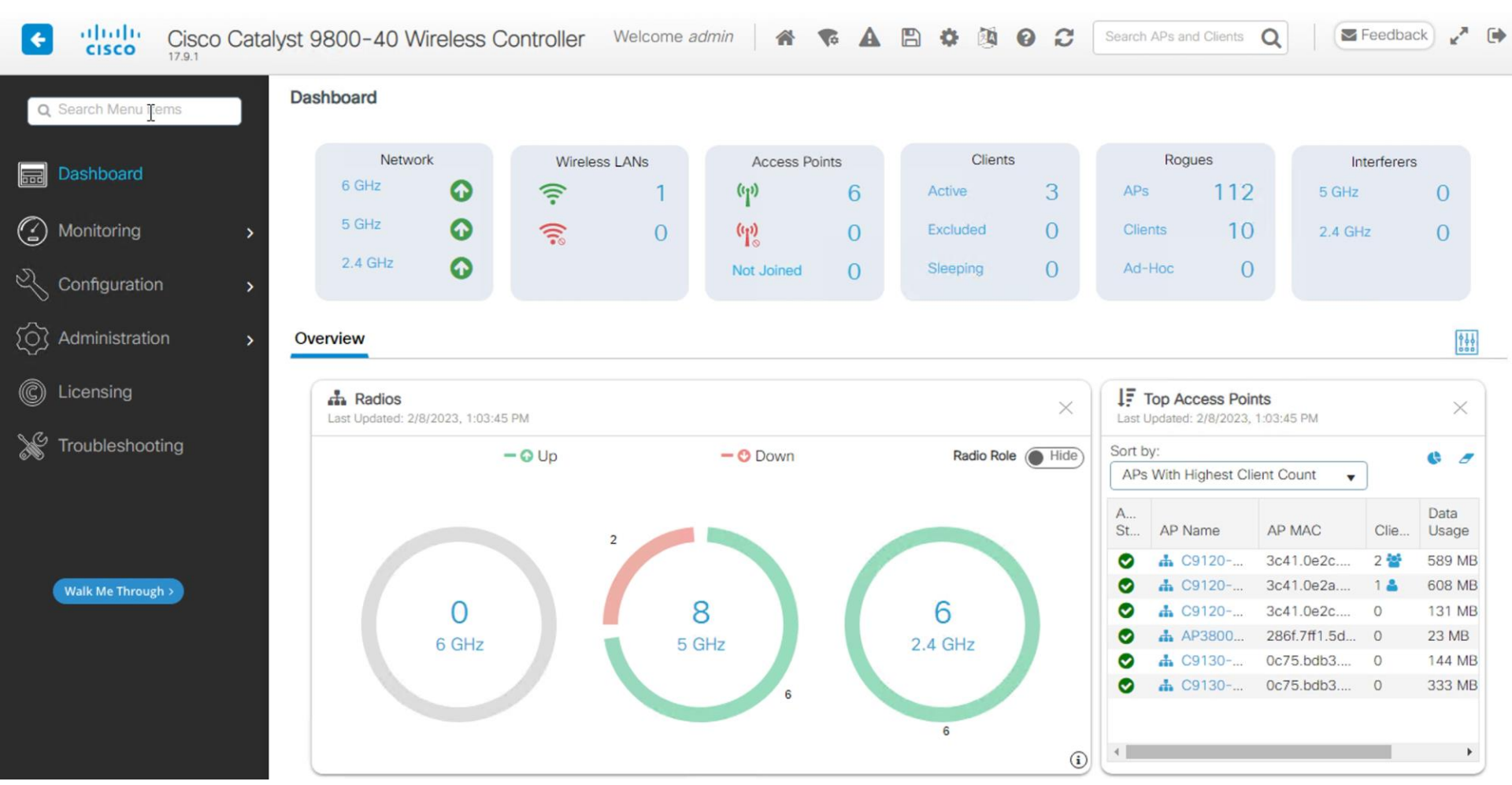


- Defines the APs' properties of the site, central (a.k.a. "local") or remote (a.k.a. "flex") site
- For FlexConnect site:
  - Defines the fast-roaming domain
  - "Equivalent" to Flex Groups in AireOS



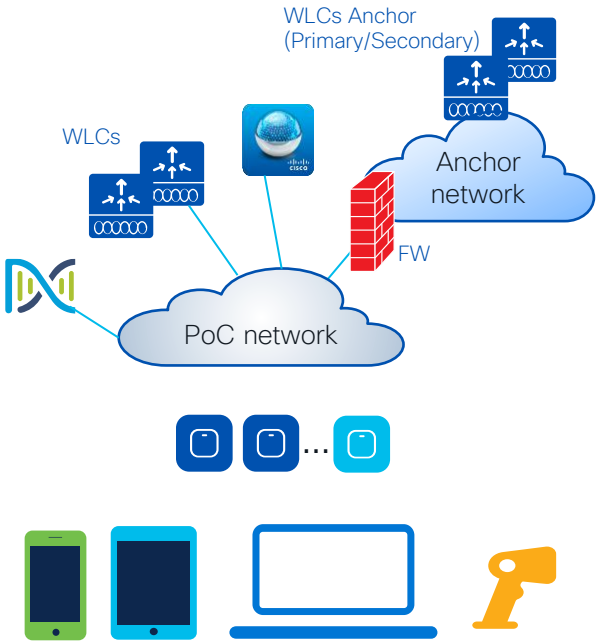
- Defines the Radio Frequency (RF) properties of the group of APs per radio

SSID = Service Set IDentifier



Migration Best Practices

Build a PoC area with same characteristics of the production network



"Same" topology:

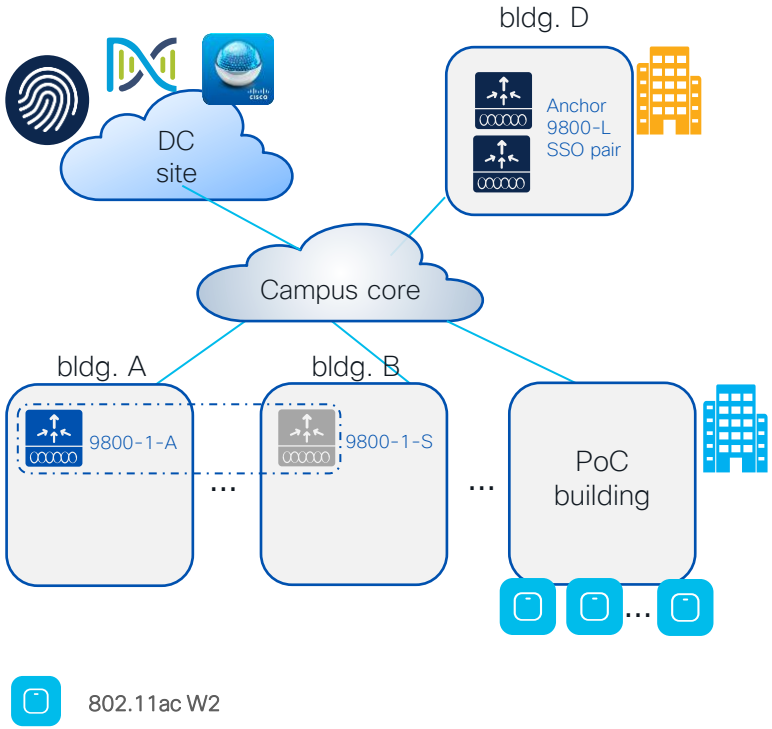
- "Same" = as close as possible to production
- Anchor Controller, High Availability pair, Firewall and other network settings like AAA should be as close as production as possible
- Test the main features customer cares about

"Same" clients:

- Ideally test same clients as in production
- At least Windows, Android and Apple clients
- Test the different authentication types with same version of production AAA and web Portal if present
- Focus on particularly old devices and evaluate if some changes need to be done in the Radio Frequency (RF) default configuration (e.g., old devices might need lower data rates)
- Particularly critical with 6GHz as client drivers are still unstable

PoC = Proof of Concept
AAA = Authorization Authentication Accounting

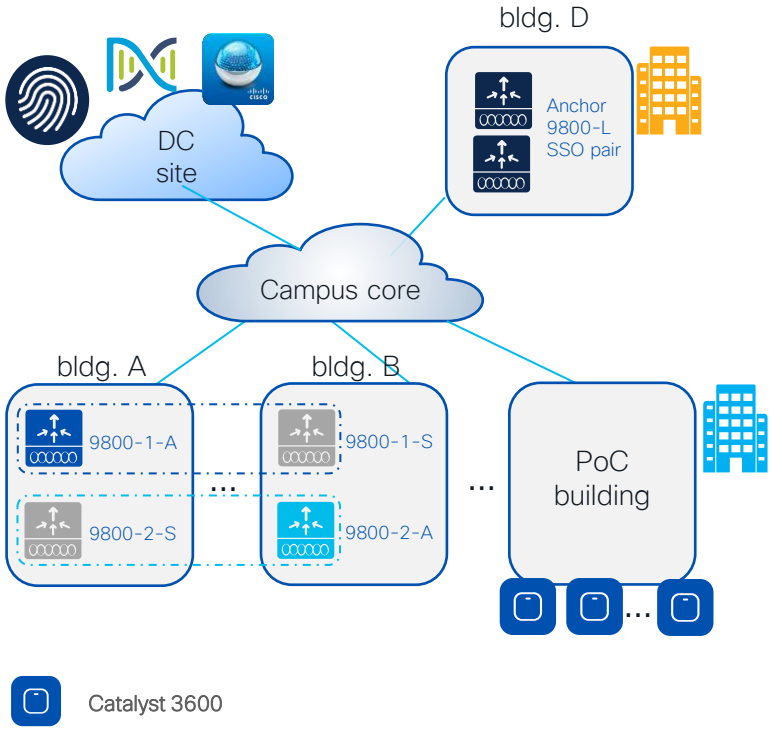
Customer Migration scenario – PoC



PoC steps:

- Installed C9880 HA pair running 17.3.6 serving a small production building
- Initially just #3 AP 3800 to serve some live users. Then added other 27 x 3800 APs
- Used to test the configuration migration and get familiar with C9800

Customer Migration scenario – PoC



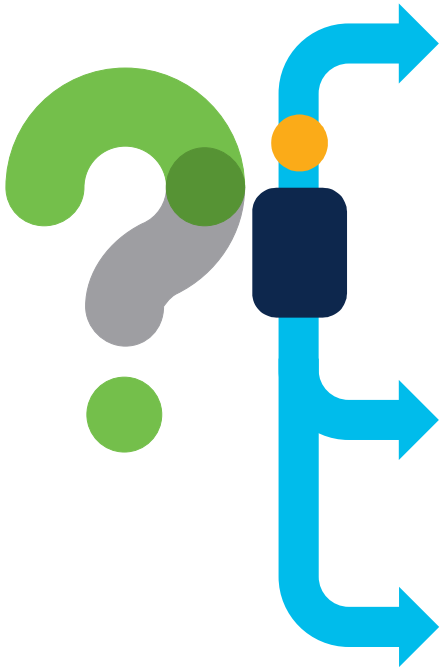
PoC steps:

- Installed C9880 HA pair running 17.3.6 serving a small production building
- Initially just #3 AP 3800 to serve some live users. Then added other 27 x 3800 APs
- Used to test the configuration migration and get familiar with C9800
- Replaced 3800 APs with 30 x Catalyst 9136 APs and #200 live clients at peak
- Installed another C9800 HA pair to test 17.9.2 software with few APs in the lab
- Added 400 APs in production with 17.9.2

Catalyst 9800 Recommended releases

cisco Live!

What is the recommended* release?



Go with latest 17.3.x:

- If you need support for 802.11ac W1 APs (IOS based APs)
- If you want the image with the “star”, with the most soak time in the field
- **Recommended release is for this train is 17.3.6 + APSP2 for COS APs**
- 17.3.6 introduces:
  - Mesh feature and Mesh + Flex feature on Cisco Catalyst 9124AXE and 9124AXI/D outdoor AP
  - Needed for Field Notice FN – 72424: Wi-Fi 6 Access Points Fail to Join the WLAN Controller
  - APSP2 includes important fixes for CSCwd37092, CSCvz99036 and CSCwc78435

Go with latest 17.6.x:

- Stable train for Wi-Fi 6 Catalyst Access Points
- **Cisco recommends 17.6.5 CCO image for all deployments without IOS APs (1700/2700/3700/1572).**
- New software features introduced between 17.3 and this release.
- In 17.6.5 added support for disabling interim accounting under the AP Policy Profile

Go with latest 17.9.x:

- If need support for newest Catalyst Wireless Wi-Fi 6E APs (C9136, CW9166, CW9164, CW9162)
- 17.9.2 is needed for Field Notice FN – 72424: Wi-Fi 6 Access Points Fail to Join the WLAN Controller
- 17.9.2 is the recommended release on this train

(*) Always check TAC recommendations: http://cs.co/recommendediosxe
(**) FN72424 https://www.cisco.com/c/en/us/support/docs/field-notices/724/fn72424.html

Cisco Recommended Software Matrix*

IOS-XE	AP	IRCM with Gen 1 AireOS	IRCM with Gen 2 AireOS	DNA-C	Prime	CMX	ISE
17.3.6	802.11ax 802.11ac W1 and W2	8.5.182.104	8.10.183	Matrix	3.10.1 3.9.1 3.8.1	10.6.2 10.5.1	3.1 3.0 2.7
17.6.4	802.11ax 802.11ac W2	8.5.182.104	8.10.183	Matrix	3.10.1 3.10.2	10.6.2 10.6 10.5.1	3.1 3.0 2.7
17.9.1	802.11ax (Wi-Fi 6/6E) 802.11ac W2	8.5.182.104	8.10.183	Matrix	3.10.2	10.6.3	3.1 3.0 2.7

(*) Please bookmark and check these links for the latest info:
http://cs.co/compatibilitymatrix
http://cs.co/recommendediosxe

AireOS configuration Migration

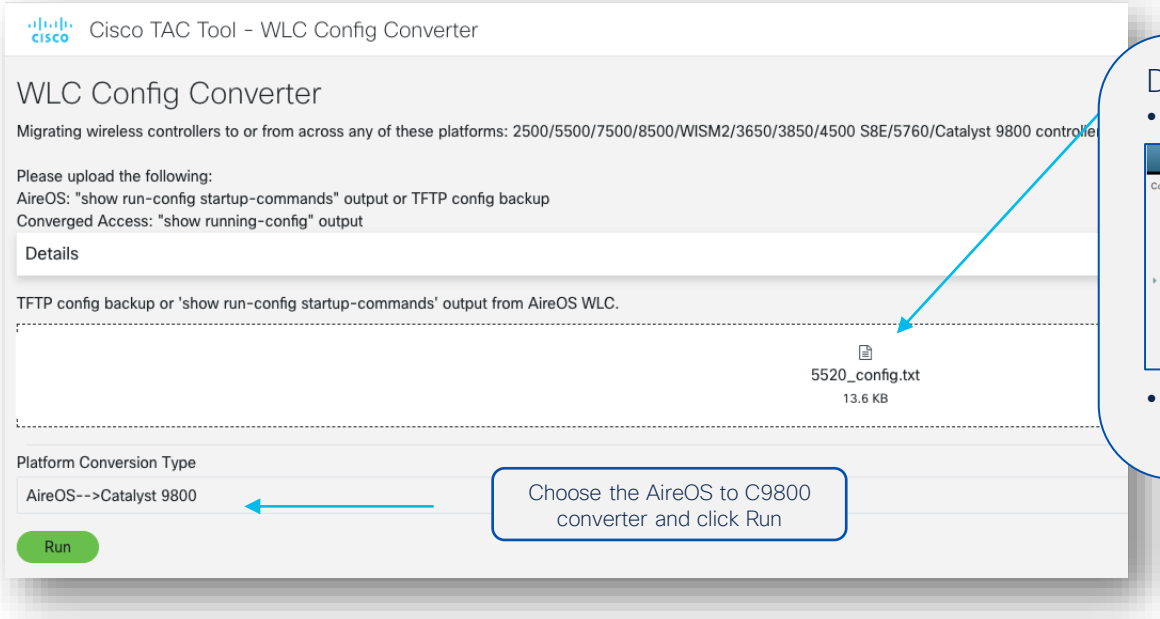
How? Configuration Migration tool

Need to address three key questions:

- Is a specific AireOS feature supported in Catalyst 9800
- How is the AireOS configuration translated into IOS XE
- Does it make sense to keep certain settings done in AireOS

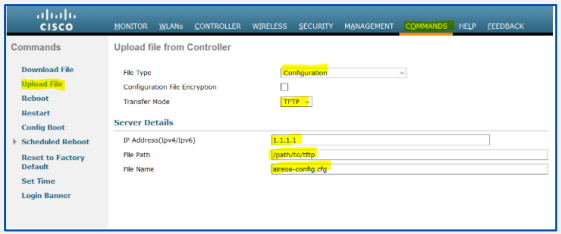
Configuration Migration Tool

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



Drop the AireOS config file:

- Upload it directly from GUI:

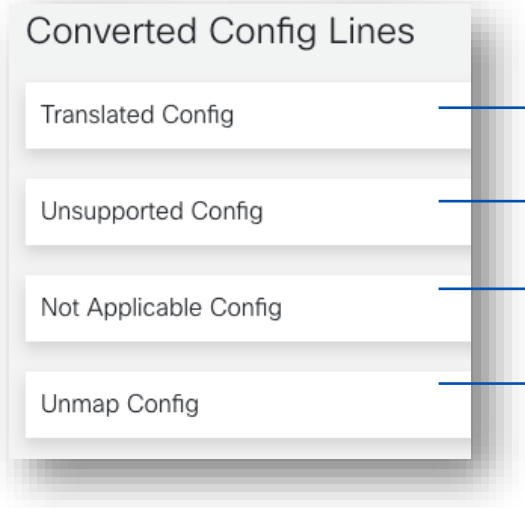


- Or use the “show run-config command” output and put it in a .txt file

CX = Customer eXperience
TAC = Technical Assistance Center

Configuration Migration Tool

Migration Tool output:



Translated (CLI supported in IOS-XE)

Unsupported (CLI not supported in IOS-XE)

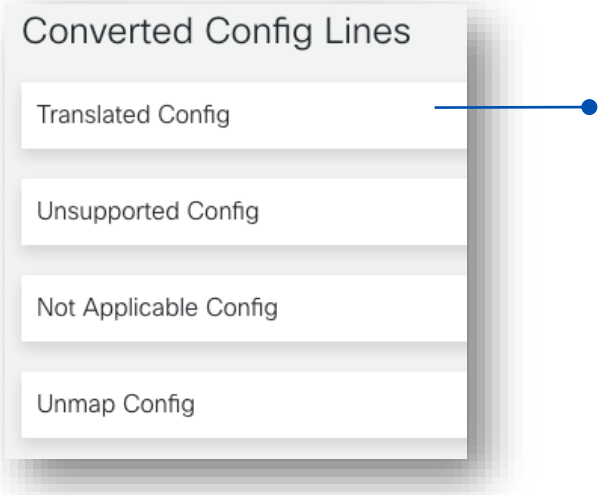
Not Applicable (CLI deprecated/not used commands)

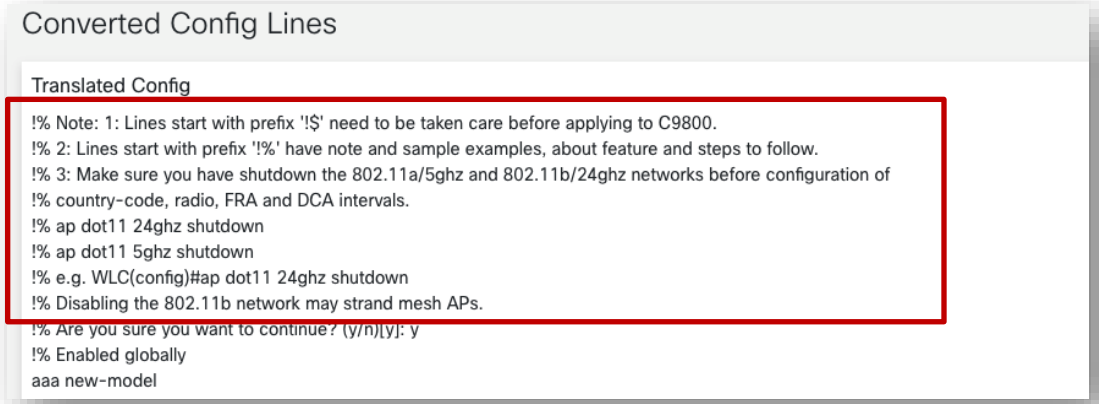
Unmapped (CLI supported but not yet translated)

CLI = Command Line Interface

Configuration Migration Tool

Migration Tool output:



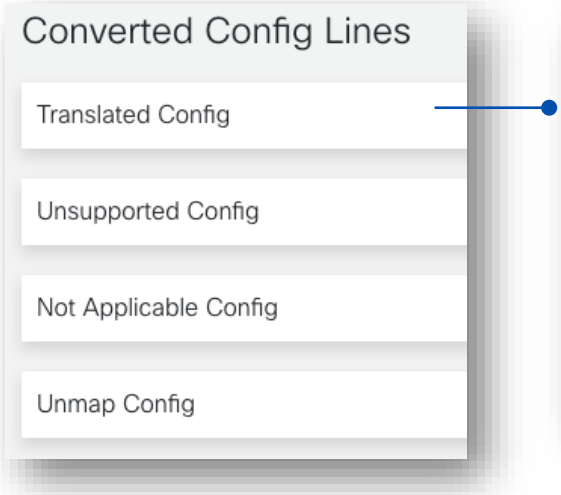


- Clear indications on when user input is required: **"!$"** prefix
- Useful warnings for correctly handing the translated configuration: Layer3 interfaces, ACLs, hostname, etc. > look for **"!%"** prefix

ACL = Access Control List

Configuration Migration Tool

Migration Tool output:

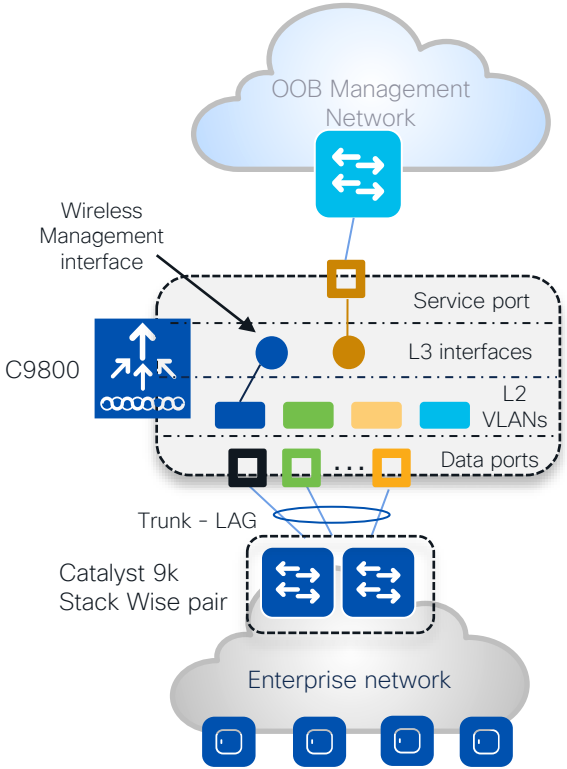



```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Interface Configuration
 !% Please note: Creating L3 interfaces for client VLANs is not needed for C9800 unless some specific functions need to be en
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! config interface create guest 119
! config interface vlan guest 119
! config interface address dynamic-interface guest 172.17.16.1 255.255.240.0 172.17.31.254
! config interface dhcp dynamic-interface guest primary 10.16.161.15 secondary 10.16.160.15
interface vlan 119
    description "guest"
    ip address 172.17.16.1 255.255.240.0
    !% ip helper-address 10.16.161.15,  dhcp proxy disabled, will not be configured
    !% ip helper-address 10.16.160.15,  dhcp proxy disabled, will not be configured
    no shutdown
!
! config interface vlan management 350
! config interface address management 10.24.194.163 255.255.255.240 10.240.194.174
interface vlan 350
    description "management"
    ip address 10.24.194.163 255.255.255.240
    no shutdown
```

- AireOS CLIs and the correspondent translated IOS-XE commands
- Explanation on why certain decisions were made in translating the AireOS configuration > Example: SVI interfaces

SVI = Switch Virtual Interface

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

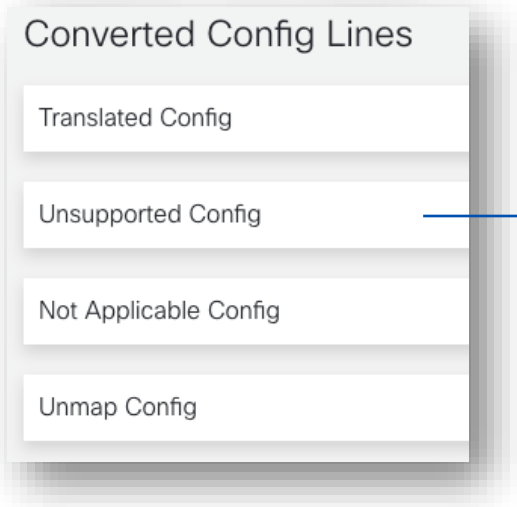
Best practices:

- 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

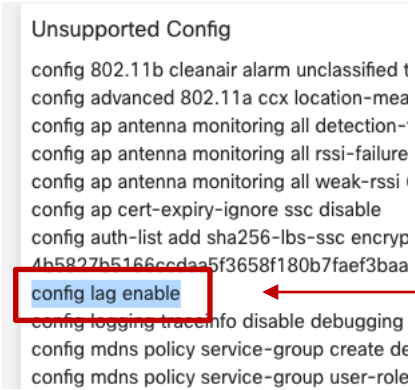
DHCP = Dynamic Host Configuration Protocol
VRF = Virtual Route Forwarding | VLAN = Virtual Local Area Network

Configuration Migration Tool

Migration Tool output:



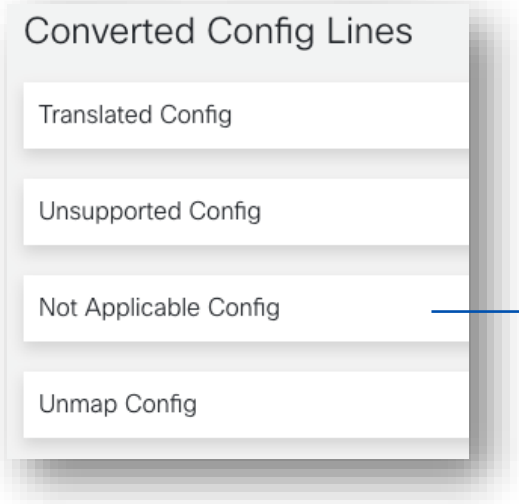
Unsupported (CLI not supported in IOS-XE)



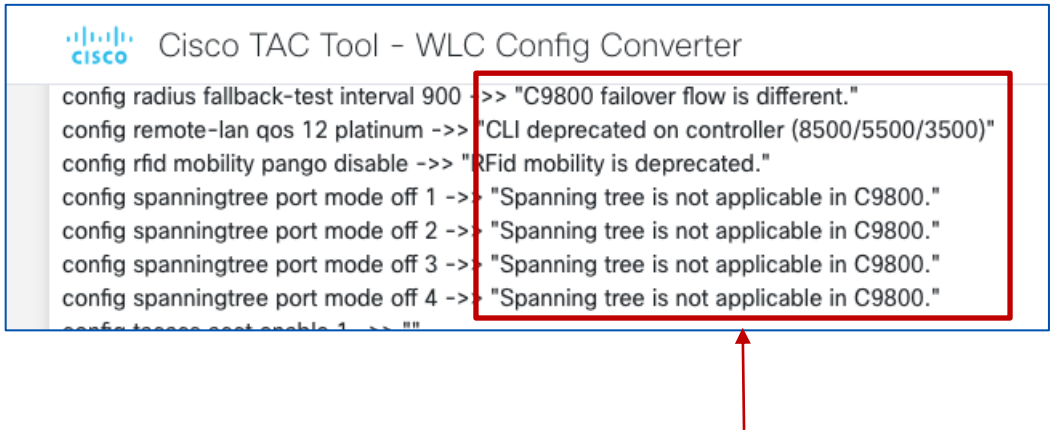
This is a problem with the tool
Should be “not applicable”

Configuration Migration Tool

Migration Tool output:



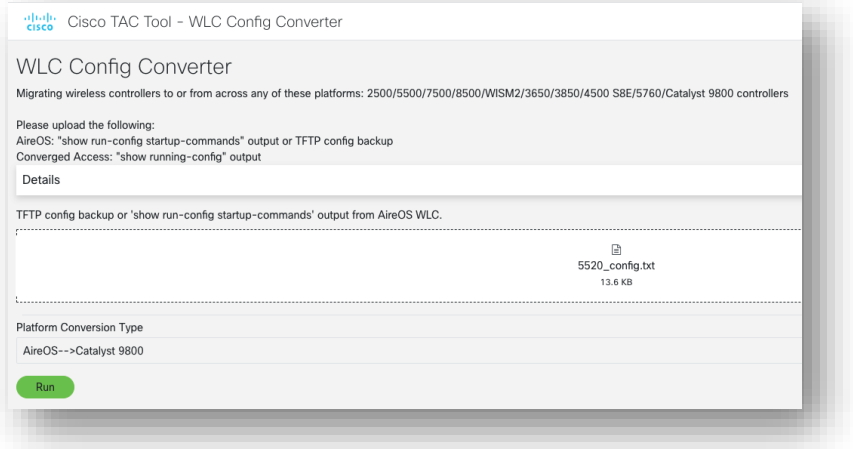
Not Applicable (CLI deprecated/not used commands)



Reason why CLI is not applicable

Configuration Migration – Steps

Step 1 – Upload AireOS in online tool

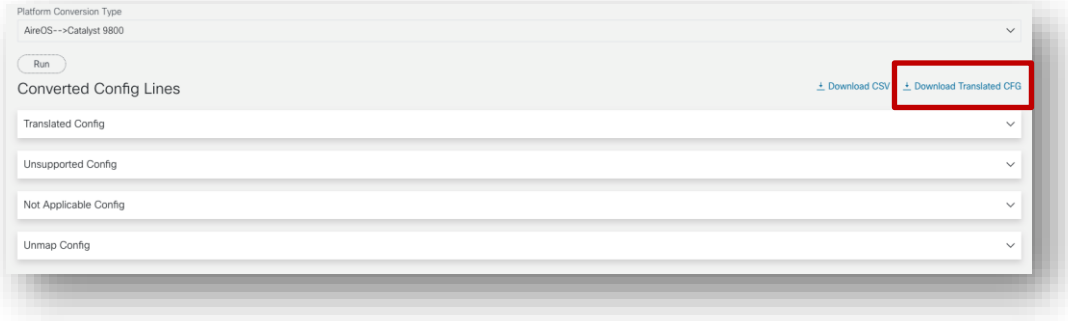


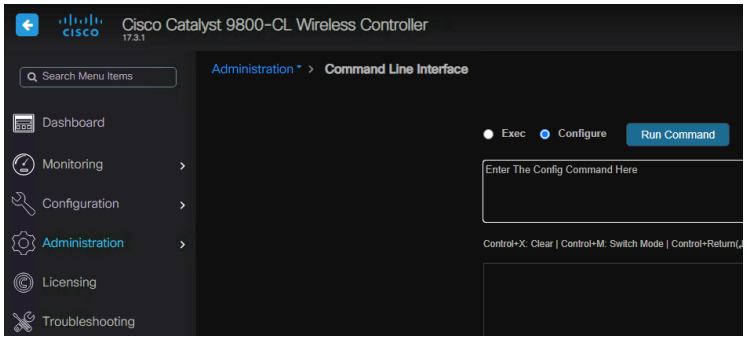
Recommended: The online tool is updated to the latest CCO release and has the latest fixes

The Migration tool integrated in the WebUI is related to a specific IOS-XE release (good to check specific feature support) but might not have latest fixes. Same for the Prime integrated tool

Configuration Migration – Steps

- Step 2 – Analyze the tool output and Download the “Translated config”
- Step 3 – Edit the config file as needed. It’s not recommended to copy directly in bootflash: and use it as running config > need to edit passwords, verify SVIs, ACLs, etc.
- Step 4 – Copy each section of the configuration to C9800’s running-config.
- Recommendation: use CLI to copy & paste. Alternatively, you can use the CLI embedded tool in WebUI once assigned an IP and login credentials
- Note: APs are not automatically assigned to tags, no AP or Flex Group conversion





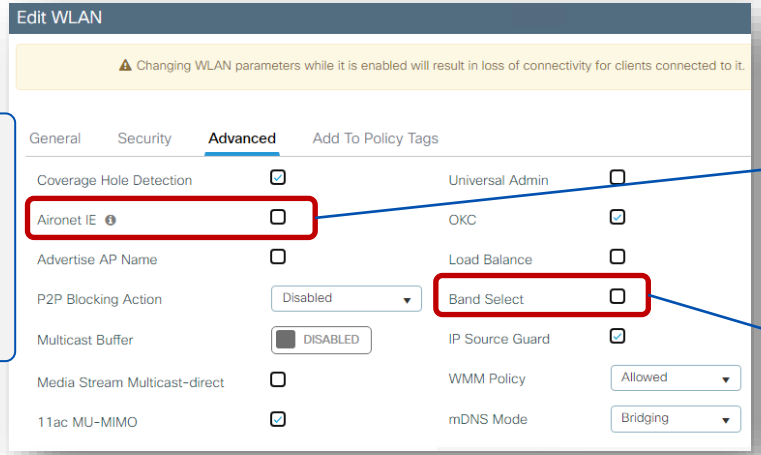
Customer Migration scenario

> Configuration review

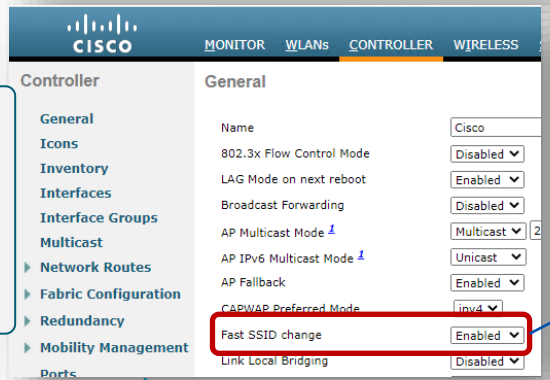
WLAN settings

WLAN settings

C9800-80



8540



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

Q: Do we still need Aironet IE?

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

Q: Do we still need Band Select?

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

Q: What happened to Fast SSID change?

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

Webauth Configuration

Webauth configuration

Problem:

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

Solution:

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

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

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

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

mDNS Configuration

mDNS configuration

Scenario:

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

Recommendation:

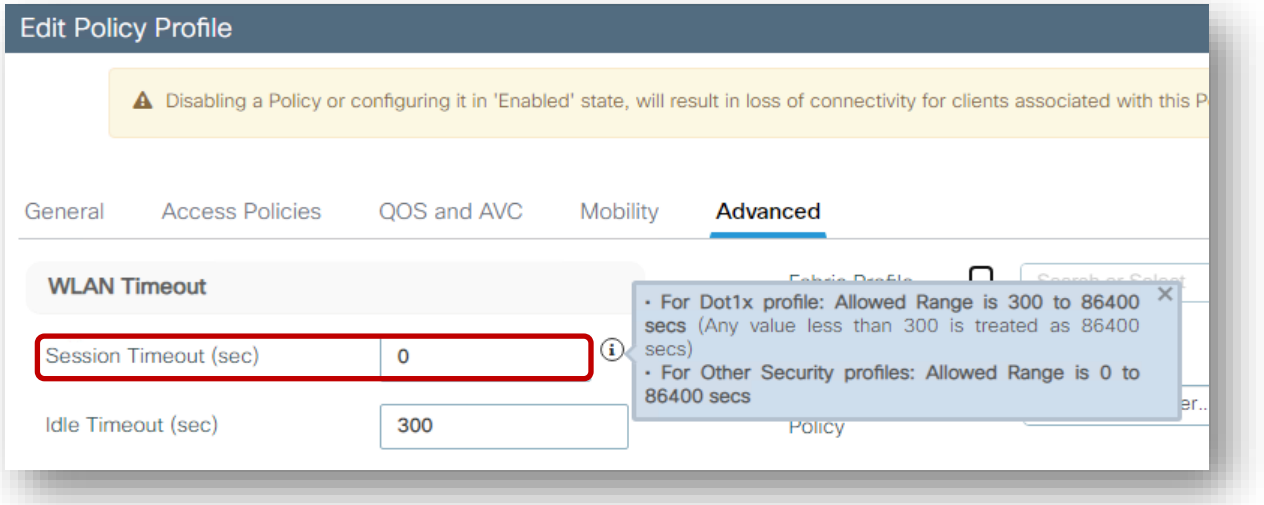
Configure the mDNS policy to use Location Specific Services (LSS) to optimize mDNS responses to clients:

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

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

Policy Profile settings

Policy Profile settings



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

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

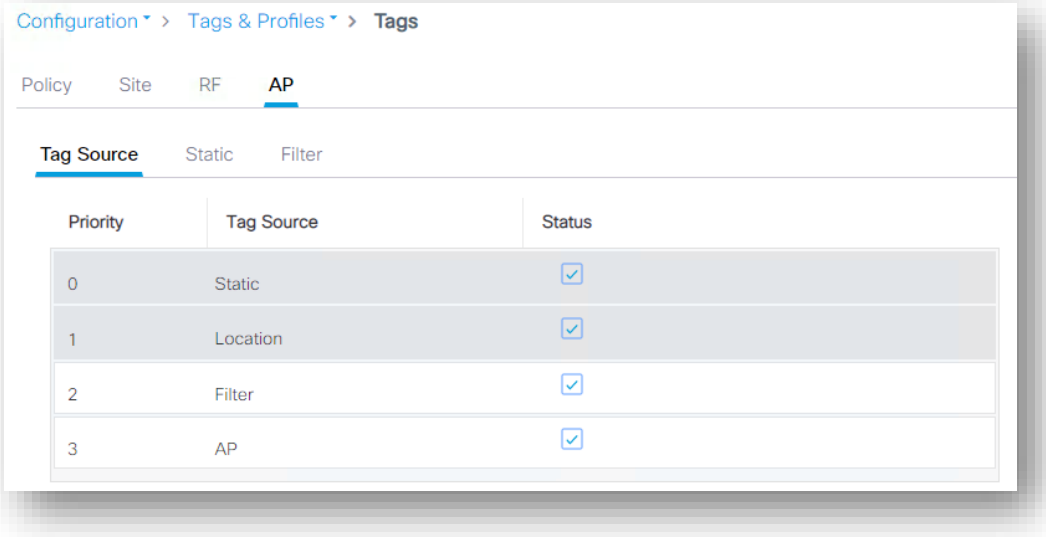
Q: can we use the default policy profile as a "normal" profile

A: Yes, absolutely

APs to Tags mapping

AP to Tags assignment

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

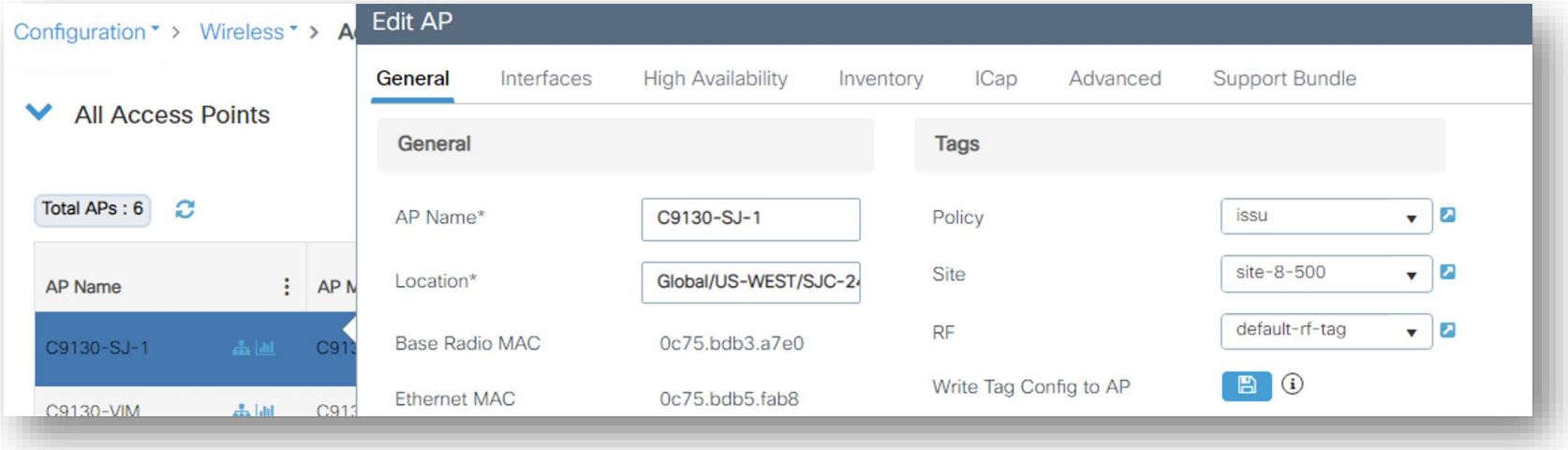


- Static: admin configuration
- Location: Basic Setup flow
- Filter: regular expression
- AP: the tags are saved on AP

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

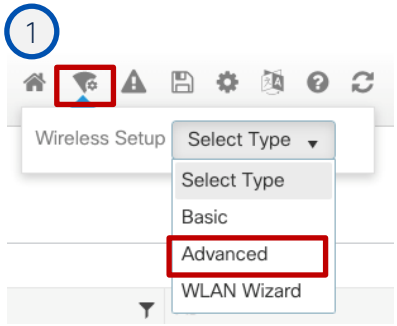
AP to Tags assignment – Source: Static

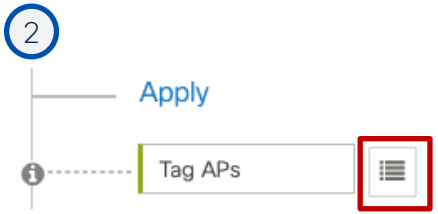
- The static Tag <> AP binding is based on AP's Ethernet MAC and it's a configuration on the Controller: upon joining the C9800, the configuration is applied and AP gets assigned to the selected tags
- Go to Configuration > Wireless > Access Points

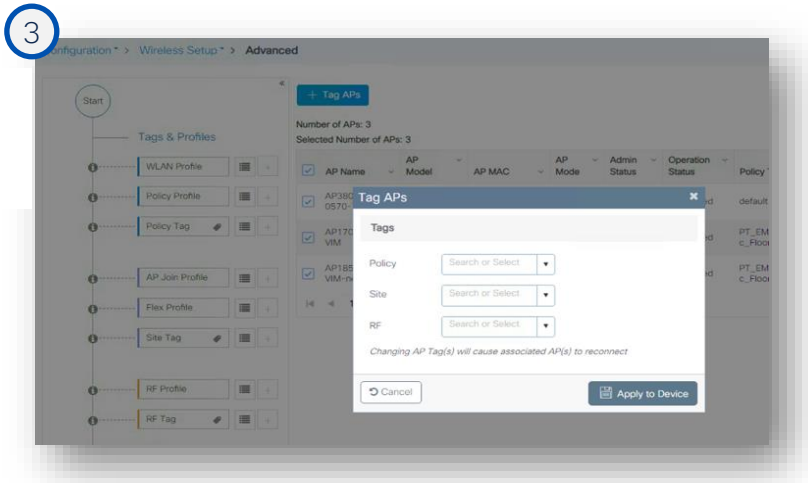


AP to Tags assignment – Source: Static

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

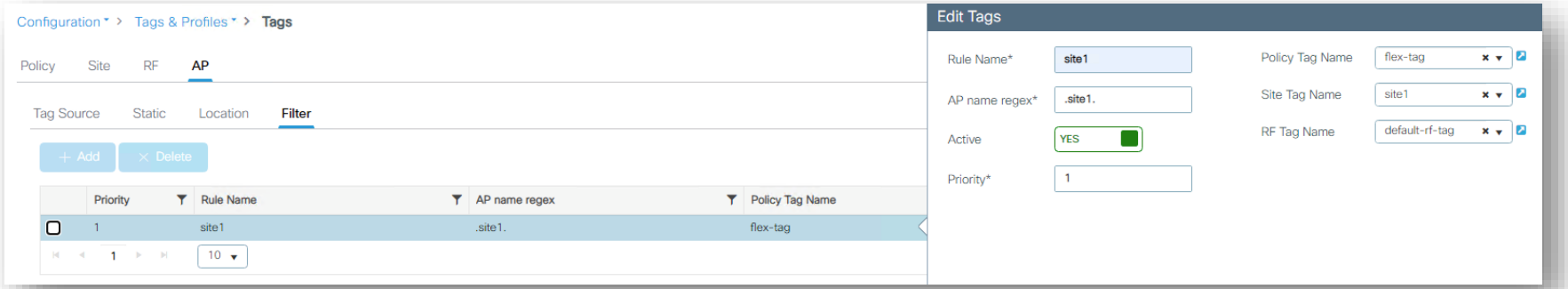






AP to Tags assignment – Source: Filter

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



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

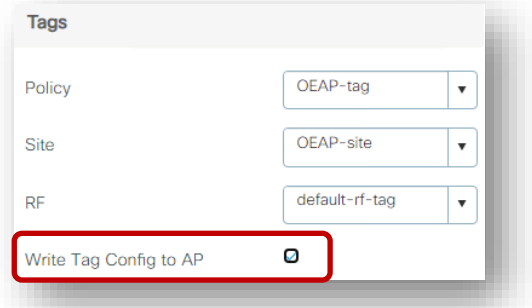
CAPWAP = Control and Provisioning of Wireless Access Points

AP to Tags assignment – Source: AP

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

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

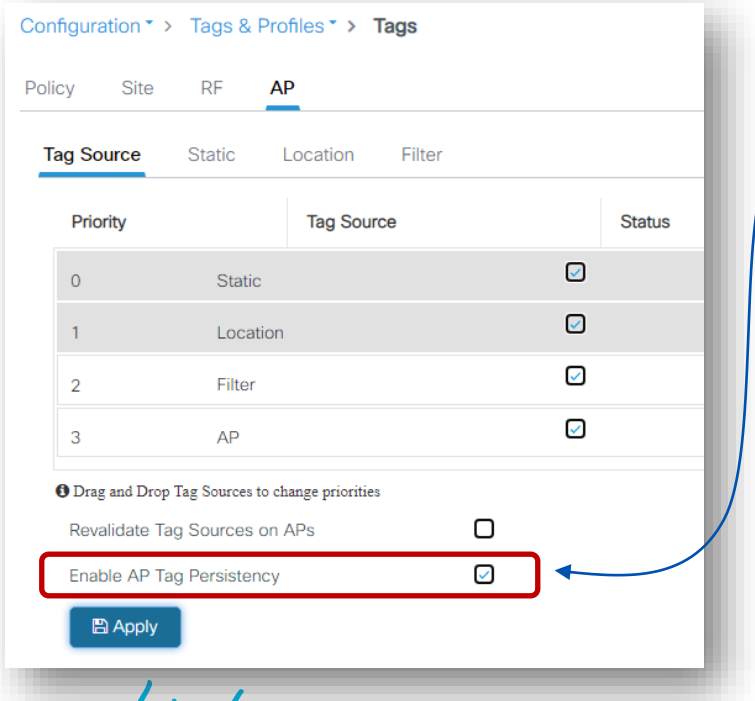
- Using the CLI command could be cumbersome, we have solutions:
  - Event Manager Script (useful for 17.3.x release)
  - Graphical user interface (GUI) settings in 17.4.1 and later
  - Starting 17.6. new feature called AP Tag Persistency



AP to Tags assignment – AP (SW >17.6)

Configuring AP Tag Persistency

Configuration > Tags & Profiles > Tags:



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

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

- 17.6.2 and 17.7 adds support from GUI

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

Verifying AP Tag source

Run the show command below:

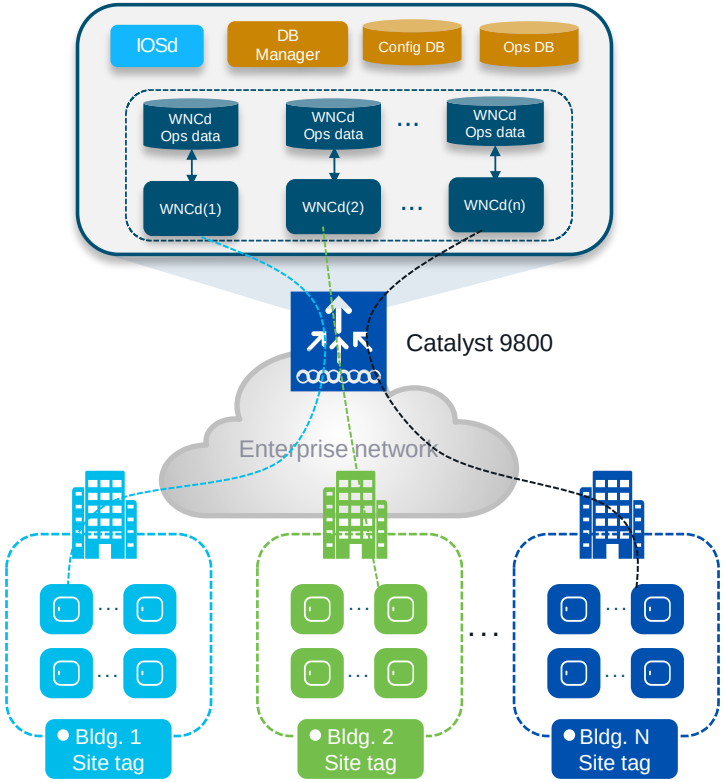
```
C9800#show ap tag summary

Number of APs: 1

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

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

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

Design with AP Tags in mind

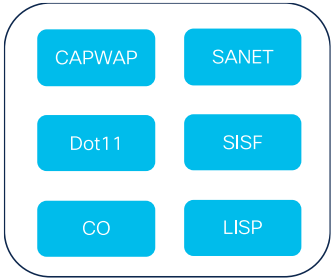
Site Tags – Design considerations

Refresher!



Important facts:

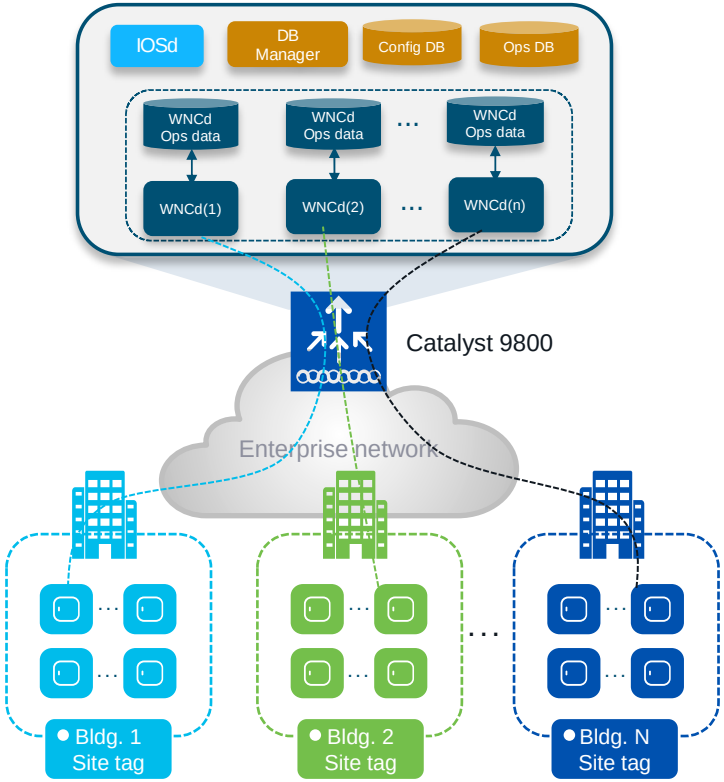
- C9800 has a multi-process software architecture
- AP and client sessions are handled by the Wireless Network Controller processes (WNCd) process within a C9800



WNCd
Wireless Network Controller demon

- CAPWAP : AP discovery
- Dot11 : Client dot11
- SANET/AAA: Client authentication
- SISF : client IP learning
- Client Orchestrator : Client state transitions
- LISP-agent for Fabric deployment

Site Tags – Design considerations



Important facts:

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

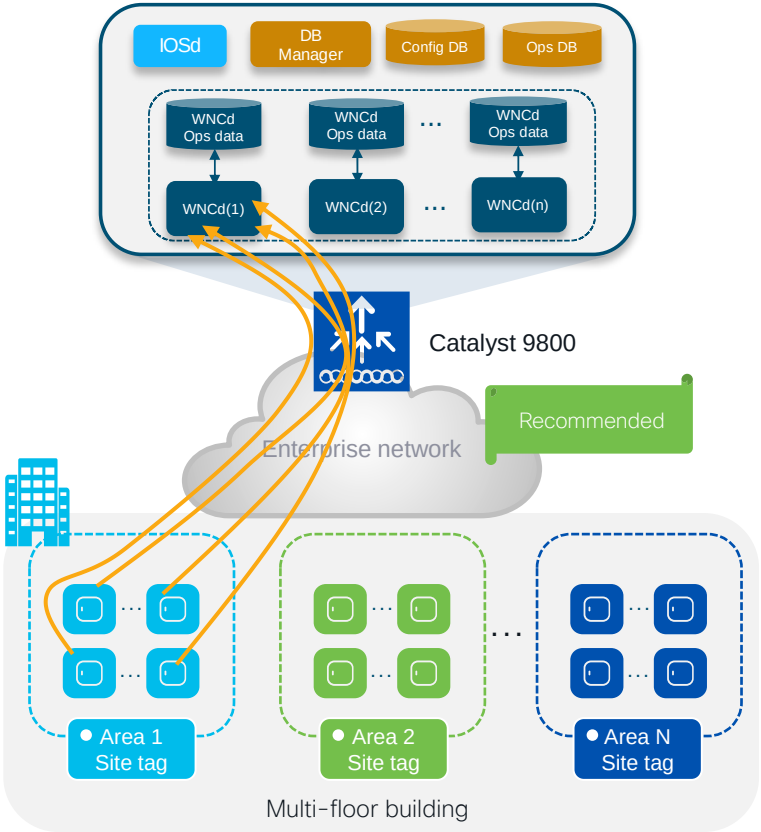
Platform	# of WNCD instances
EWC (on AP or C9k switch)	1
C9800-L	1
C9800-CL (small)	1
C9800-CL (medium)	3
C9800-40	5
C9800-CL (large)	7
C9800-80	8

Following command shows the # of WNCDs processes:

```
C9800#sh processes platform | inc wncd
```

Site Tags – AP to WNCd distribution

Refresher!



How AP distribution across WNCds works:

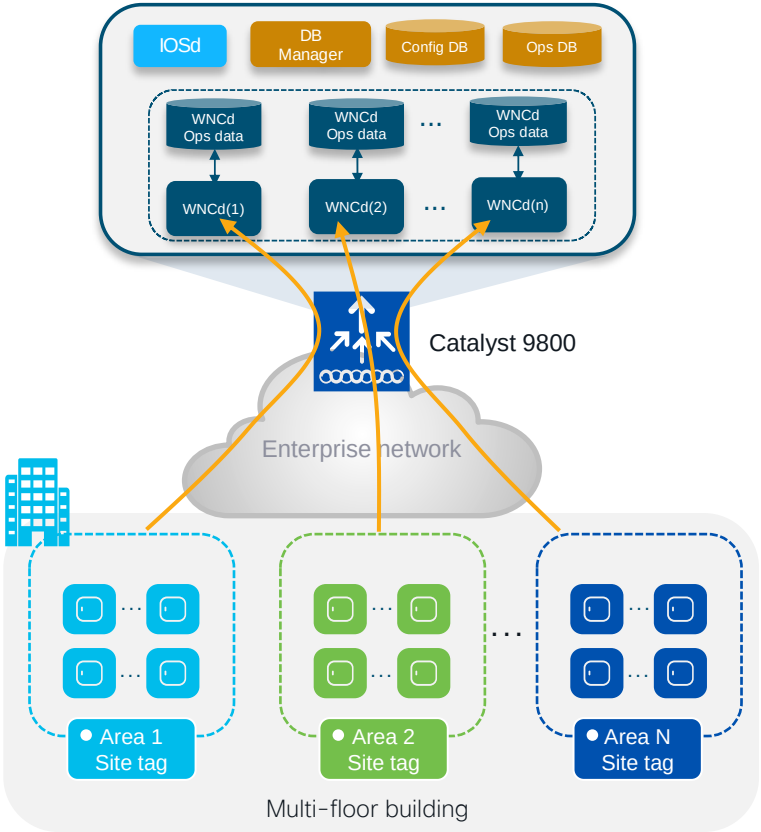
- AP distribution to WNCd processes is based on Site Tag: APs with the same site-tag are managed by the same WNCd
- Except when you using default-site-tag: in this case APs are distributed among WNCds in round robin fashion
- Custom site tags are distributed among WNCds using the least loaded criteria based on the number of site tags (not the # of APs or clients).
- 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
- To show how APs are distributed across WNCds:

```
C9800#sh wireless loadbalance ap affinity wncd
```

IMPORTANT: the site tag doesn't have to coincide with a geographical physical site. The site tag is a logical group of access points

Site Tags – AP to WNCd distribution

Refresher!



Recommendations:

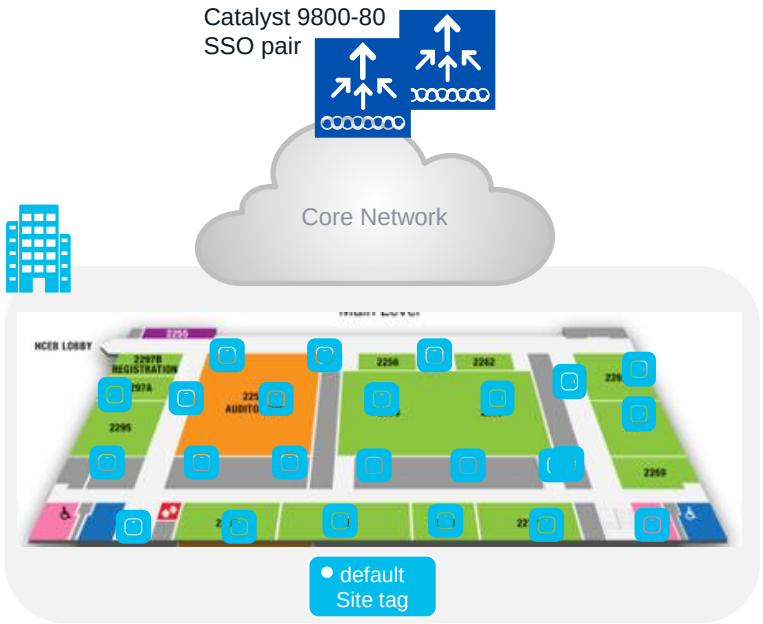
- Use custom site tags
- Whenever possible, have less than 500 APs per site tag
- Do not overwhelm a site-tag and WNCd. Do not exceed the following max number of APs per site tag:

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

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

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,..)

Can I use default-site-tag? Please…



Scenario#1: 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…

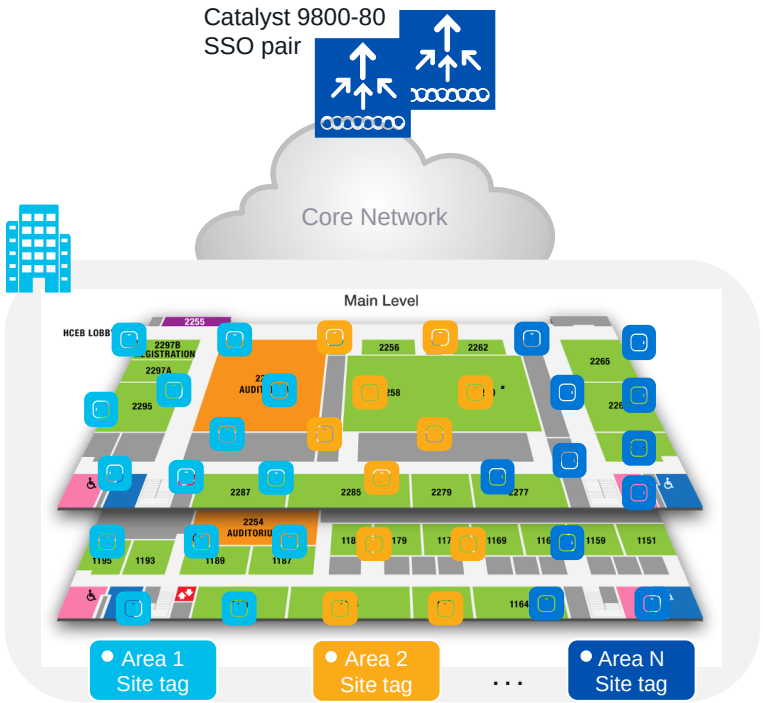
Design Question: Can I use the default-site-tag?

- Default-site-tag: APs will be distributed in round robin across the WNCds, and this may result in inter-WNCd roaming
- Assumption: If the system is not heavely loaded > clients and/or AP scale is 30-40% of the max scale supported on the C9800

Design Answer: it's ok to put all APs in the default-site-tag

- Fast roaming (11r, OKC, etc.) is supported across WNCds
- 802.11k/v is also supported across WNCds starting 17.7
- This recommandation is valid for all authentication types with APs in local mode

Site Tags Design – Large venue deployment



Scenario#2: 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 matching the number of WNCds on that platform:

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

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

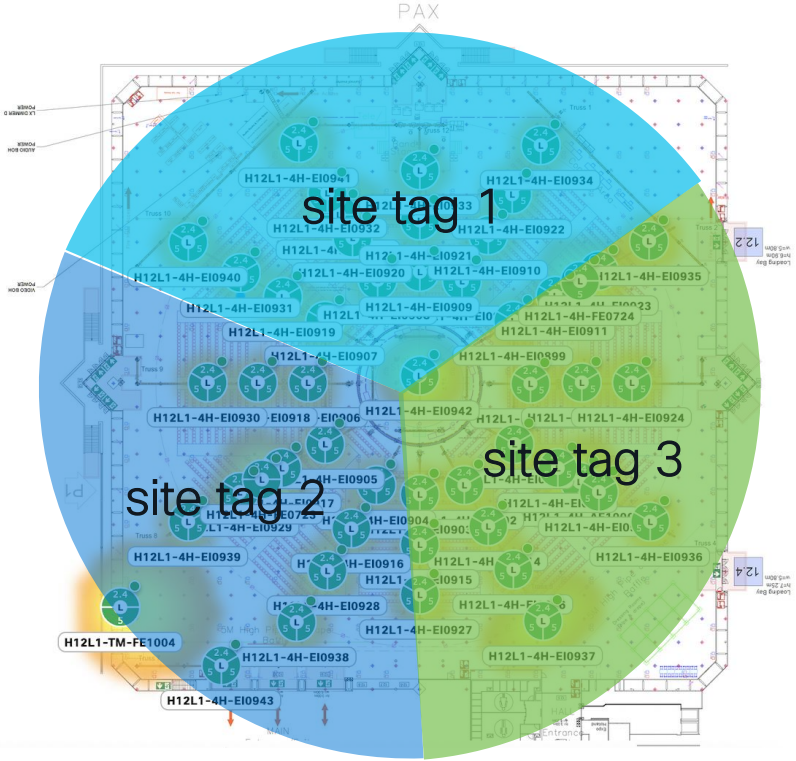
cisco Live! runs on Catalyst Wireless stack!!

- Main even WLC: C9800-80 running 17.9.2
- #506 Catalyst APs, mix of Catalyst 9120 and 9130 with dual-5 GHz
- Peak client count: 13k+ devices
- Designed with #8 site tags
- In this case, the site tag represent eight areas with virtual boundaries

Here is the snapshot of the CPU load on WNCds at peak time!

```
WLC-5#show processes cpu platform sorted | inc Name|---|wncd
   Pid     PPid     5Sec     1Min     5Min  Status          Size  Name
-------------------------------------------------------------------------
 17843   17835      38%      38%      38%  R             692220  wncd_1
 18417   18410      27%      26%      25%  R             670252  wncd_6
 18073   18065      22%      17%      16%  S             644844  wncd_3
 18302   18295      20%      18%      16%  S             597696  wncd_5
 17958   17950      16%      15%      14%  R             590720  wncd_2
 18188   18180      14%      14%      13%  S             616372  wncd_4
 17728   17720      12%      10%       9%  S             611416  wncd_0
 18531   18525       0%      30%      28%  R             660912  wncd_7
```

cisco Live! runs on Catalyst Wireless stack!!



- Keynote WLC: C9800-40 running 17.9.2
- #46 Catalyst 9104
- Peak client count: 4100+
- Designed with #3 site tags

Here is the snapshot of the CPU load on WNCds:

```
WLC-1#show processes cpu platform sorted | inc Name|---|wncd
   Pid    PPid    5Sec    1Min    5Min  Status         Size  Name
-----------------------------------------------------------------
 16226   16218      8%      9%     13%  S            486196  wncd_1
 16111   16103      8%      8%     12%  S            505936  wncd_0
 16341   16333      7%      7%      8%  S            495408  wncd_2
 16570   16563      0%      0%      0%  S            324328  wncd_4
 16456   16448      0%      0%      0%  S            326604  wncd_3
```

Disclaimer for the next set of slides…

If you are able to follow the design guidelines…

If you don’t see any problems of the WNCd CPU load…
(when you should look further?
CPU is > 70% for at least 5 mins)

Then, relax….

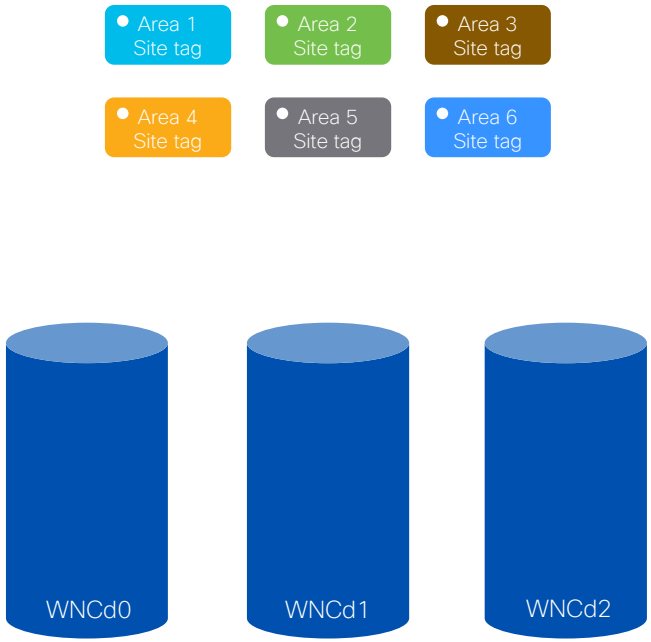
Site Tags – AP to WNCd distribution

Before 17.10 (17.9.3), site tags are distributed among WNCds using the least loaded criteria based on the # of site tags.

Problem: Current algorithm can result in uneven WNCd load, as it doesn't take into considerations the number of APs or clients per site tag and it's dependent the order of AP joining. Also, it might not be possible to follow recommendations and have an even distribution of APs among site tags

- Example: C9800-CL medium (#3 WNCd), six custom site tags with uneven number of APs per tag, 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 following:
  - 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

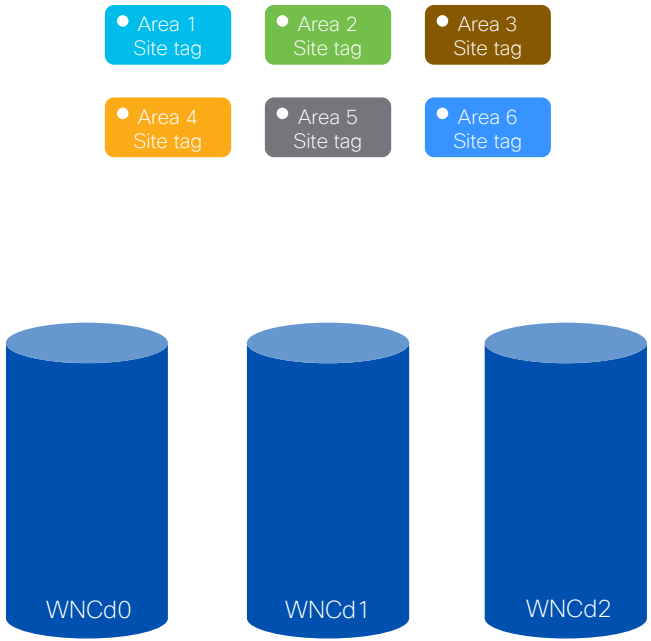


- If you have the number of site tags > the number of WNCd for that C9800 platform, there is now an optimized way to load balance APs across WNCd processes
- Starting 17.9.3 and 17.10, the algorithm to distribute APs among WNCds may use the load parameter configured under the site tag:

```
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 tag (group of APs)
- 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

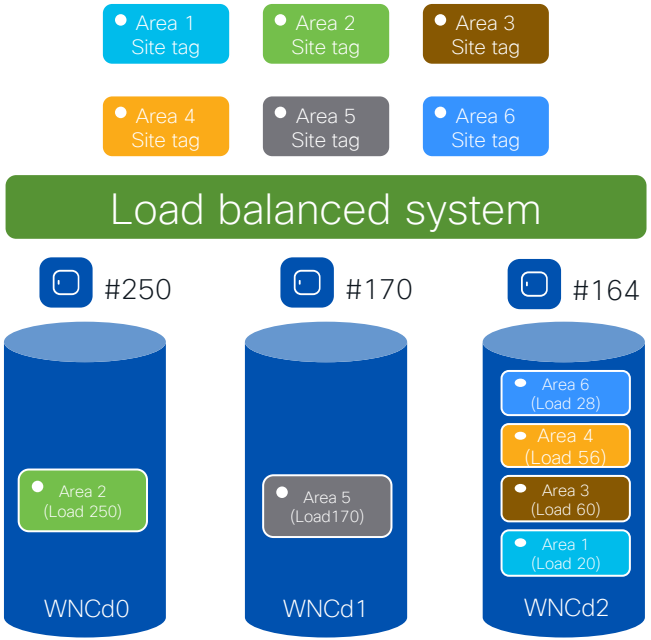
Site Tags – New load balancing Algorithm



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 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

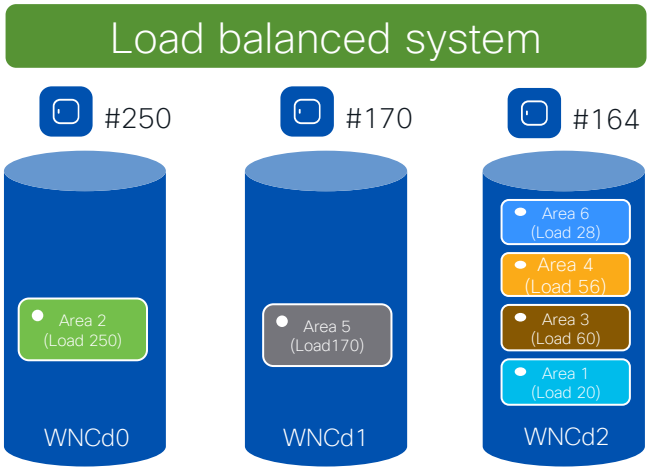
Site Tags – New load balancing Algorithm



Let's see it in action:

- 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 site tag to WNCds mapping would be the following (pre-allocated):
  - WNCd0 > site tags: area2 > **#250** APs
  - WNCd1 > site tags: area5 > **#170** APs
  - WNCd2 > site tags: area1,area3,area4,area6 >**#164** (20+60+56+28) APs
- The result is a load balanced and more efficient system

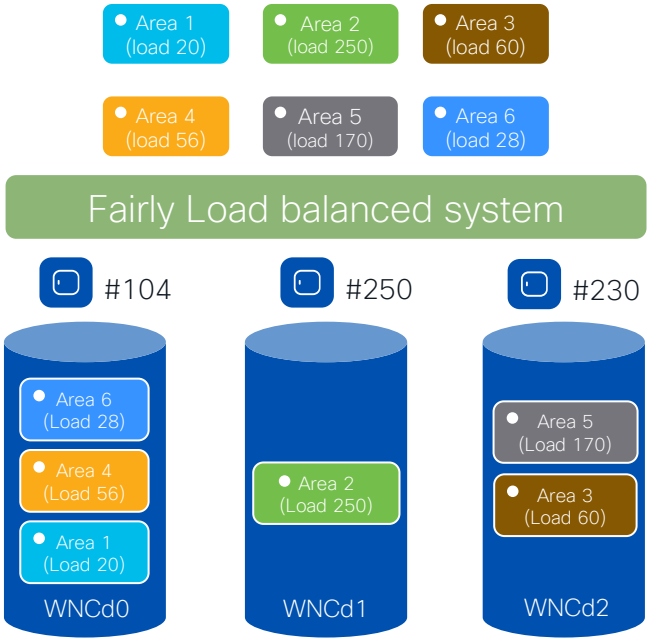
Site Tags – New load balancing Algorithm



Important things to note:

- For the new algorithm to take into consideration the load, and be independent of AP joining order (this example), configure the load parameter under the site tags and reboot the C9800
- For a site tag to be considered for load balancing, it needs to have at least one joined AP. This information is saved and remembered by the system for subsequent runs.
- Since AP join times can vary, the system waits for an hour for APs to come up before persisting the information. The reboot should be triggered after at least one hour of uptime.

Site Tags – New load balancing Algorithm



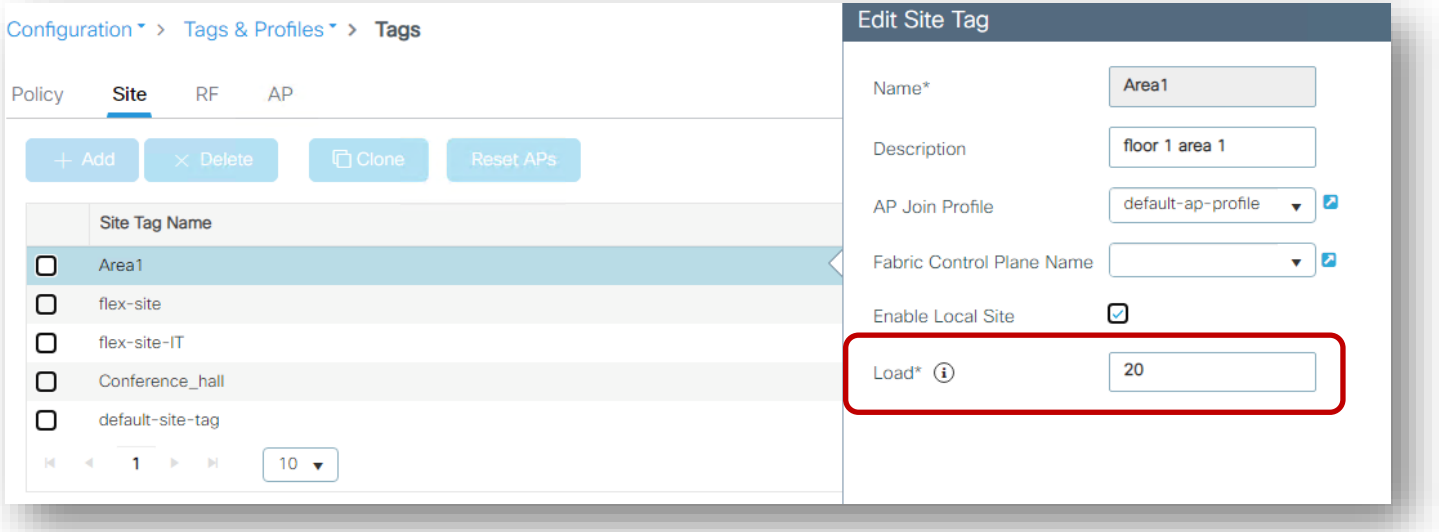
What if you don't reboot?

- If the C9800 is not rebooted, the load balance algorithm is still improved as it takes into consideration the site load with the configured load parameter, but it's going to be dependent on the order of AP joining
- If APs are de-registered and join again, the resulting AP to WNCds mapping would be the following (given the same order of joining):
  - Area1 : #20 APs > WNCd0
  - Area2 : #250 AP > WNCd1
  - Area3 : #60 AP > WNCd2
  - Area4 : #56 APs > WNCd0 (lowest Load)
  - Area5 : #170 APs > WNCd2 (lowest Load)
  - Area6 : #28 APs > WNCd0 (lowest Load)
- The result is a fairly load balanced and efficient system

Configuring the site tag Load- WebUI

NEW

Configuration > Tags & Profiles > Tags -> Site



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

Verifying the site tag Load- CLI

```
C9800#show wireless loadbalance tag affinity

Tag                          Tag type   No of AP's Joined   Wncd Instance
-------------------------------------------------------------------------

area2                        SITE TAG   250                 0
area5                        SITE TAG   170                 1
area1                        SITE TAG   20                  0
area3                        SITE TAG   60                  0
area4                        SITE TAG   56                  0
area6                        SITE TAG   28                  0
```

#250 APs

#170 APs

#164 APs

Questions on AP <> WNCd load balancing

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

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

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

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

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

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

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

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

Catalyst 9800
Wireless LAN Controller (WLC)

Supported Access Points

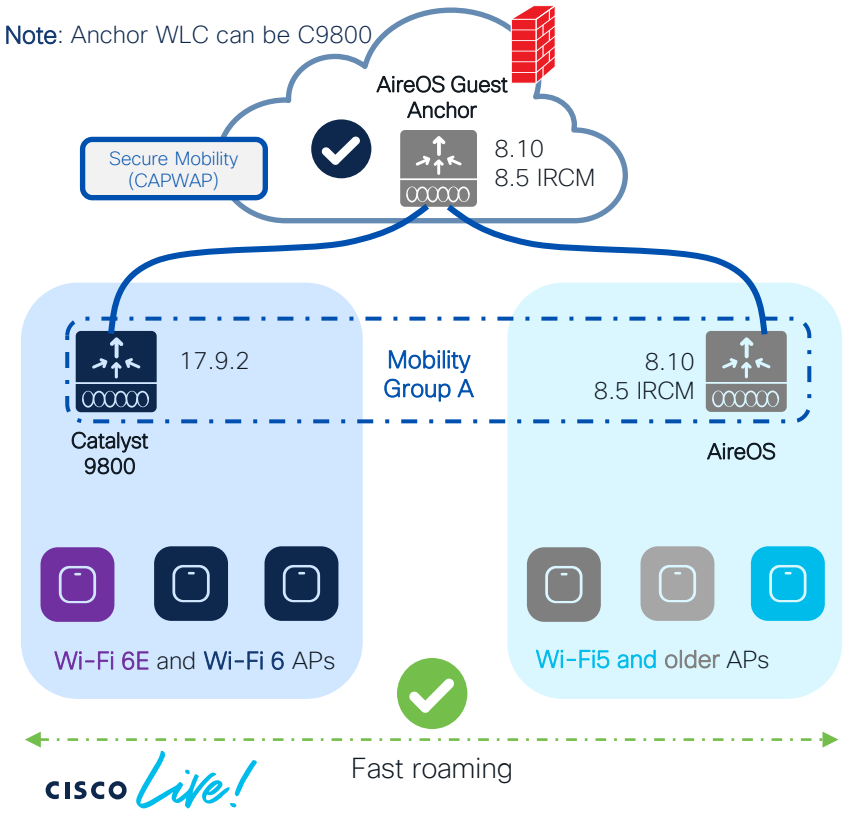
Wi-Fi 6/6E

C9136 | CW9166/64 | CW9162

Wi-Fi 6

9130 | 9124 | 9120 | 9115 | 9105

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



Scenario 1: AireOS WLC supports IRCM

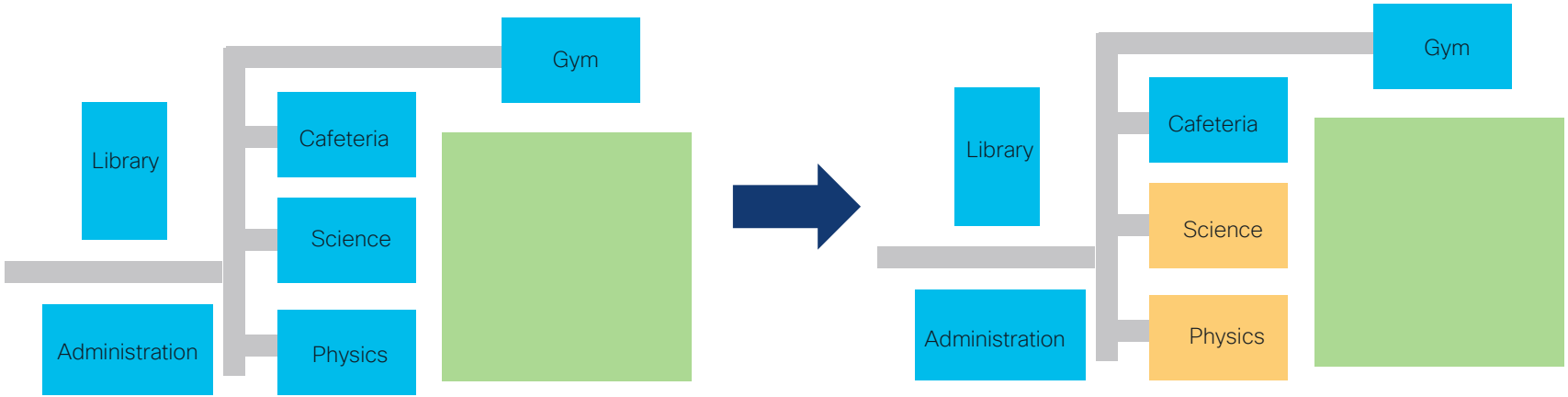
- Introduce new 6/6E AP hadware on the new C9800 and support seamless roaming and Guest Anchor with existing networks
- This method allows the smooth coexistence of both WLCs, with RF areas migrated as needed, without any overnight switchover.
- Things to consider:
  - If the controller is limited to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

Customer Migration Scenario

2.4/5 GHz

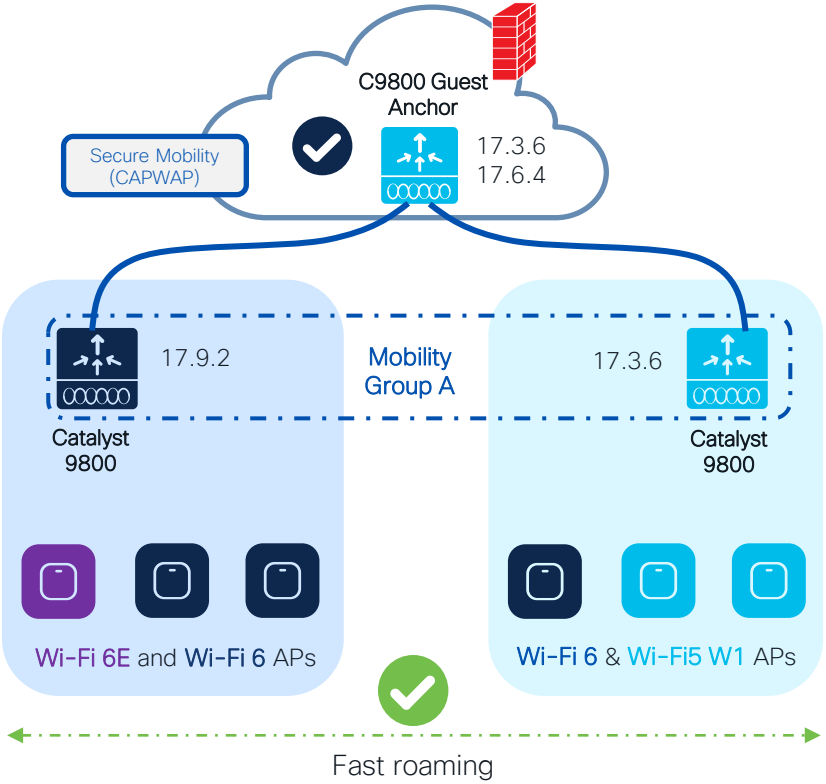
2.4/5/6 GHz

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



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

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



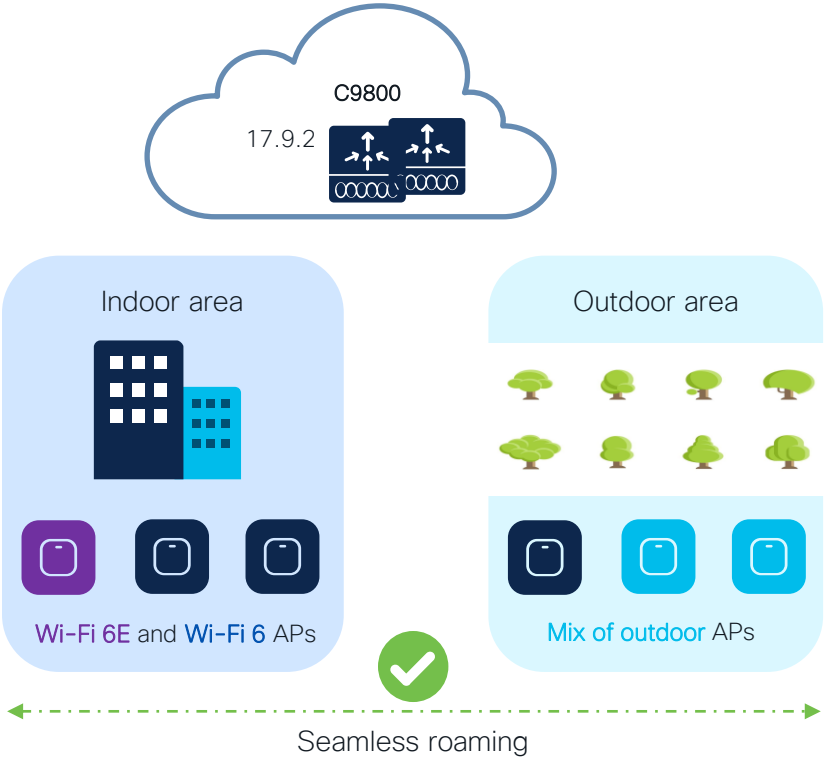
Scenario 2: Catalyst network with W1 APs

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

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

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

How do I start adopting 6GHz?
What about outdoor areas?



Scenario 3: Mixed indoor and outdoor areas

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

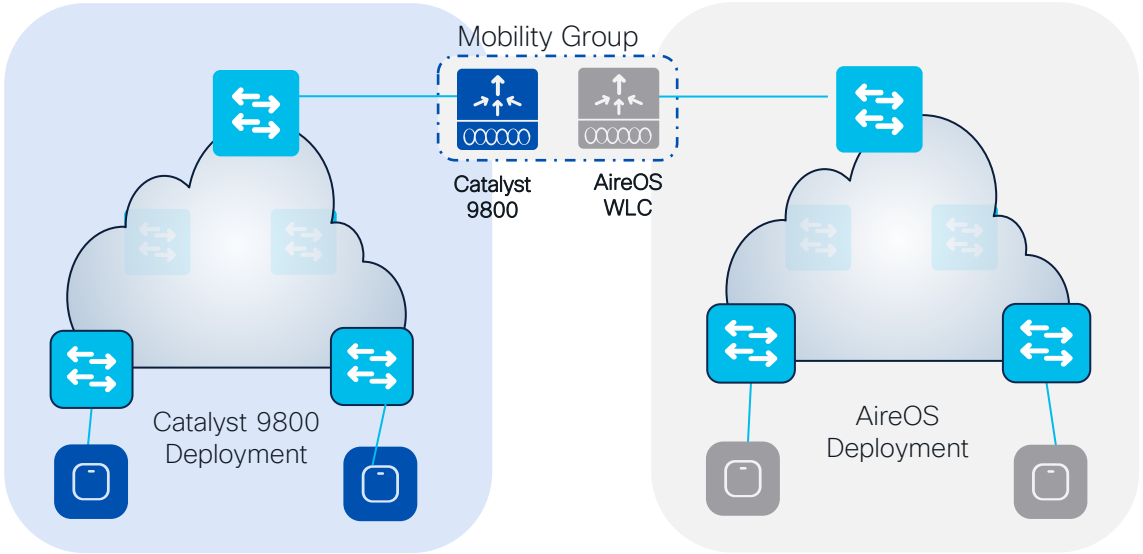
(*) for more details on WLAN Design, please refer to “Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points” - BRKEWN-2024

Design for AireOS and IOS XE coexistence during migration

cisco Live!

AireOS and IOS-XE coexistence

Inter Release Controller Mobility (IRCM) is your friend!

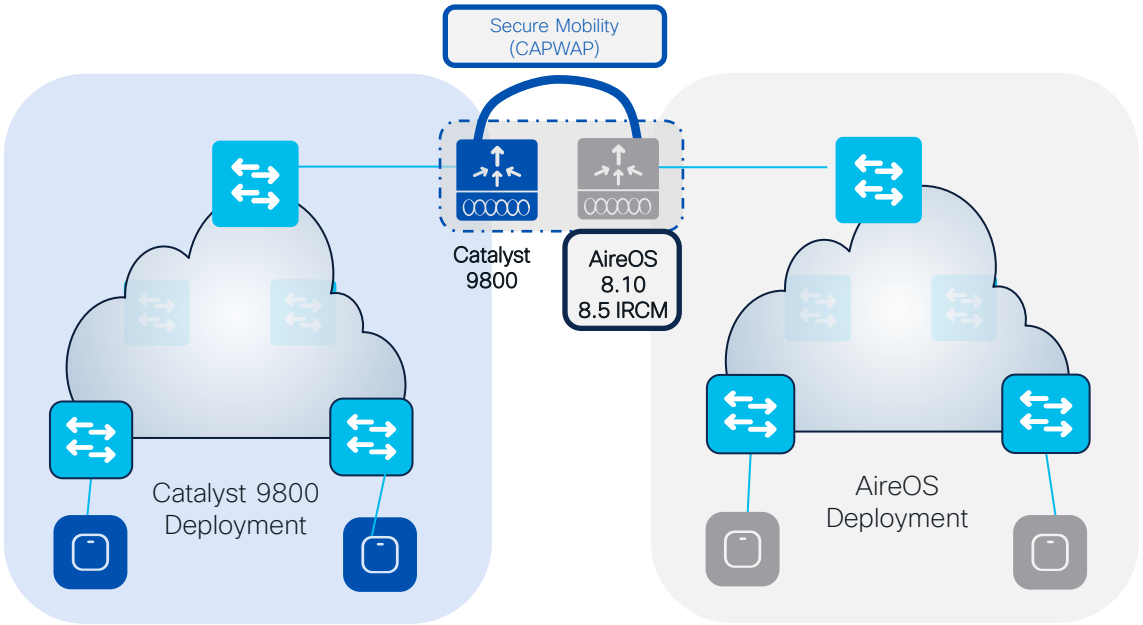


Primary questions:

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

RRM = Radio Resource Management

AireOS and IOS-XE coexistence – Roaming



- Mobility Group provides seamless roaming between WLCs
- IRCM guarantees support for mobility across different platforms and releases
- Mobility Group between AireOS and IOS-XE WLCs is only supported on:
  - 3504, 5520, 8540 (8.10 recommended)
  - 5508, 8510 with 8.5 IRCM (special release)
- This is because C9800 only support CAPWAP based mobility tunnels (Secure Mobility)
- Note: Secure Mobility is NOT supported on AireOS WISM2, 7510, 2500 and virtual WLC (vWLC)

Customer Migration scenario: Mobility Config.

AireOS

Static Mobility Group Members

Local Mobility Group: migration

MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key	Secure Mobility	Data Encryption
00:a6:ca:f0:03:4d	10.58.55.207	migration	0.0.0.0	Up	none	NA	NA
00:1e:49:63:1c:ff	10.58.55.25	migration	0.0.0.0	Control Path Down	471e8376a51b19df77a84	Enabled	Disabled

IOS XE

Mobility Peer Configuration

+ Add | × Delete

MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
00a6.caf0.034d	10.58.55.207	10.58.55.207	migration	0.0.0.0	::	Control And Data Path Down	1385		Enabled

?

Make sure configuration matches on both sides. No need for Data Link Encryption, so disable it:

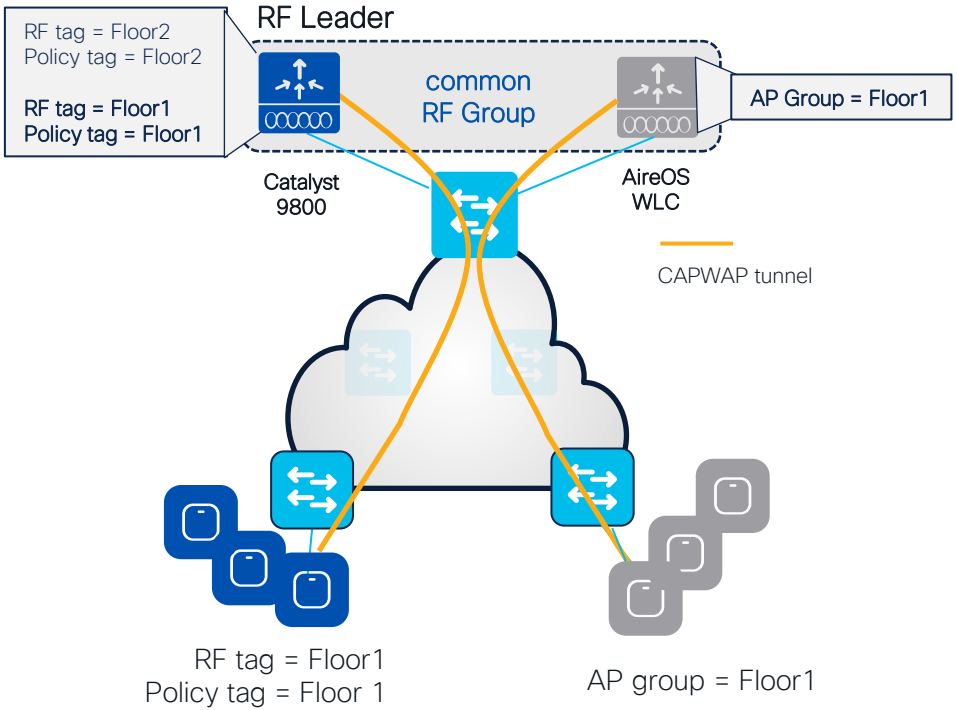
Mobility Peer Configuration

+ Add | × Delete

MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
00a6.caf0.034d	10.58.55.207	10.58.55.207	migration	0.0.0.0	::	Up	1385		Disabled

AireOS and IOS-XE coexistence – RF Grouping

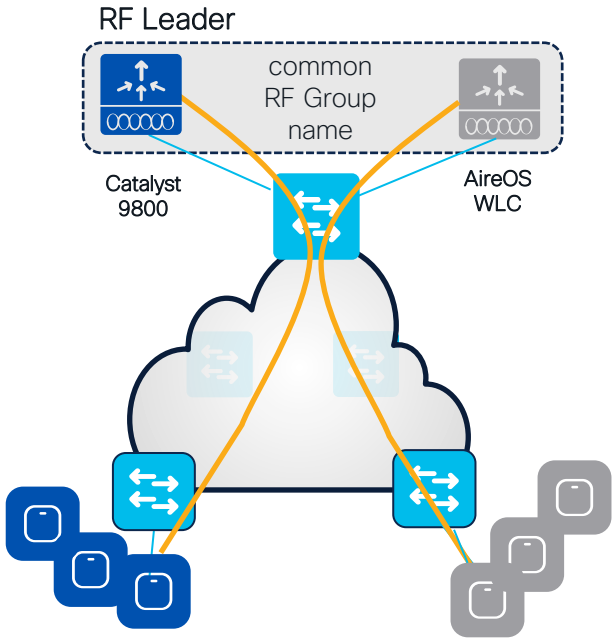
RRM works in a mixed controller environment, and you can have one RF master. It's recommended not to rely on RF leader auto election and select RF Master statically.



- C9800 and AireOS controllers can create one RF domain and share a common RF plan
- The RF group name on both AireOS and C9800 controllers needs to match
- 8.10 is recommended on AireOS
  - A RF leader is elected (based on controller capacity) and common channel and power plan will be used for all APs
  - APs will be not show up as rogue on the other controller
- NOTE: if have custom RF profiles or Flexible Radio Assignment (FRA), then Policy, RF Tags and Profile names need to match the AP Group and RF profile names on AireOS WLC.

AireOS and IOS-XE coexistence – RF Grouping

RRM works in a mixed controller environment, and you can have one RF master. It's recommended not to rely on RF leader auto election and select RF Master statically.



Lower priority

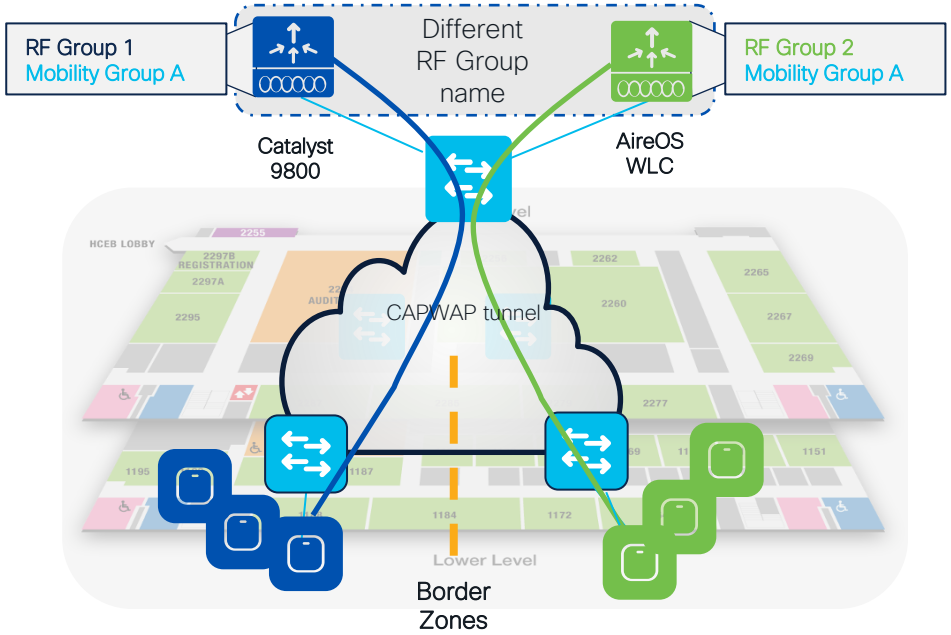
Higher priority

Consider the group leader priority:

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

AireOS and IOS-XE coexistence – RF Grouping

For large scale and high-density deployments, with thousand of APs and heavy roaming, consider placing each WLC in a separate RF group

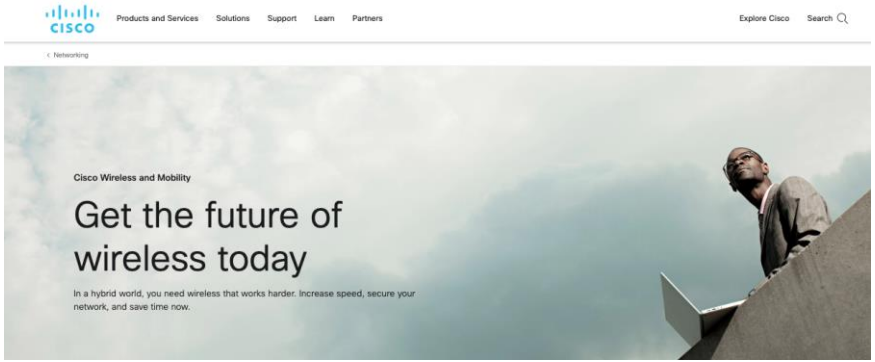


- If it's a very large deployments C9800 and AireOS controllers should be configured with their own respective RF domain
- The RF group name on the AireOS and C9800 controllers will be different
- If seamless roaming is desired at the border zones between the RF domains where:
  - Place the AP is the same mobility group
  - APs will be not show up as rogue on the other controller in this case

More info?

Where can I find more info?

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

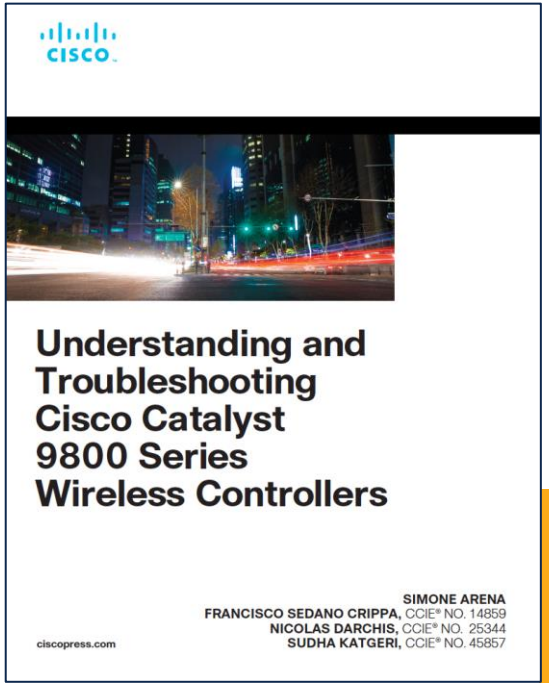


Other links on CCO:

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

Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers 1st Edition

by Simone Arena (Author), Francisco Crippa (Author), Nicolas Darchis (Author), Sudha Katgeri (Author)



Available in any physical or virtual store near you!
Paper or eBook

Visit the Cisco store and use discount code CISCOLIVE during checkout.
Offer valid February 6-10, 2023.

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the " Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

The bridge to possible

Thank you

cisco Live!

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

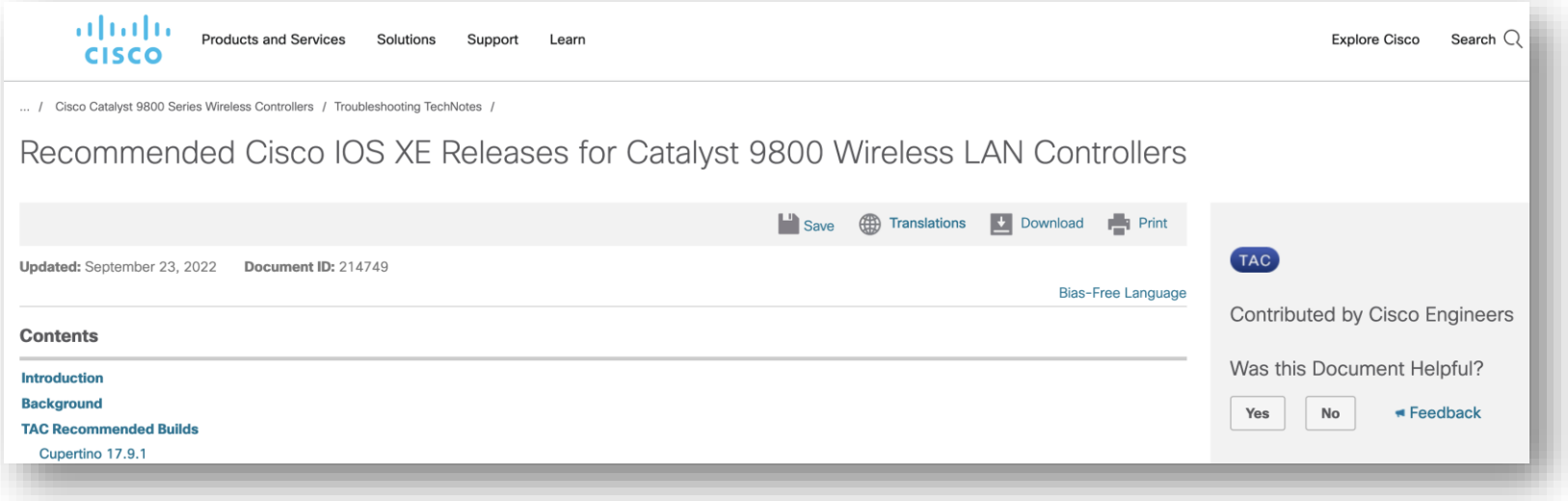
Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

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

Bonus content

TAC recommendations

Read TAC Recommendations carefully!!!
http://cs.co/recommendediosxe



Field Notice: FN - 72424

Some Wi-Fi 6 Access Points Fail to Join the WLAN Controller - Software Upgrade Needed!

- Problem:
  - Wi-Fi 6 access points (APs) manufactured in September 2022 and later with the Version IDs (VIDs) listed in the Products Affected section cannot join Wireless LAN Controllers (WLCs) running software released prior to August 2022.
- Solution:

AireOS

If a Cisco product runs Cisco AireOS 8.10.171.x or earlier, upgrade to Cisco AireOS 8.10.18x.0 or later. **8.10.181.3**

Cisco IOS XE Software

If a Cisco product runs a Cisco IOS XE Software Release listed in the left column of the table, upgrade to the release listed in the right column of the table.

Cisco IOS XE Software Release	Upgrade Release	
17.3.5b or earlier	17.3.6 or later	+ APSP2
17.6.3 or earlier	17.6.4 or later	Aug 2022
17.9.1 or earlier	17.9.2 or later	Nov 2022

Link to FN 72424: https://www.cisco.com/c/en/us/support/docs/field-notices/724/fn72424.html

17.3.6 APSP2 to fix AP COS Fix

Following Fix is committed:

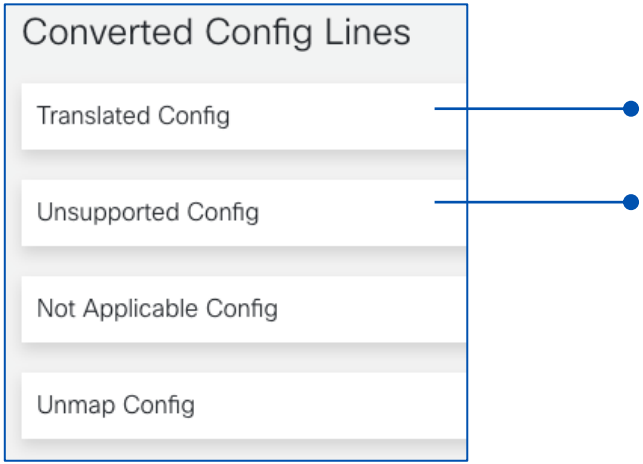
- CSCvz99036: Cisco Access Points VLAN Bypass from Native VLAN Vulnerability
- CSCwd37092: Slow TCP downloads, failing TLS authentications - 2800/3800/4800
- CSCwc78435: 9130 sending incorrect channel list on out of band DFS event causing client connectivity issues

File Information	Release Date	Size
Hitless Recommended APSP SMU, CSCwd40096 17.3.6 APSP2 to fix AP COS Fix C9800-universalk9_wlc.17.03.06.CSCwd40096.SPA.apsp.bin Advisories	31-Oct-2022	364.01 MB

More on the Configuration Migration tool

Configuration Migration Tool

Migration Tool output:



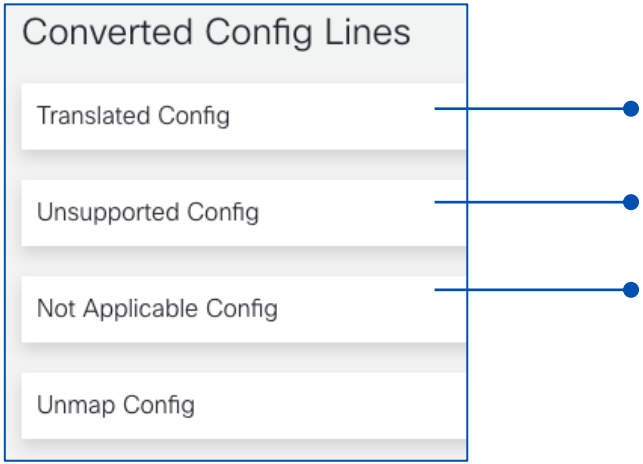
Translated (CLI supported in IOS-XE)

Unsupported (CLI not supported in IOS-XE)

config radius auth ipsec authentication hmac-sha1 3
config radius auth ipsec authentication hmac-sha1 4
config radius auth ipsec authentication hmac-sha1 5
config radius auth ipsec authentication hmac-sha1 6
config radius auth ipsec encryption des 3
config radius auth ipsec encryption des 4
config radius auth ipsec encryption des 5
config radius auth ipsec encryption des 6

Configuration Migration Tool

Migration Tool output:



Translated (CLI supported in IOS-XE)

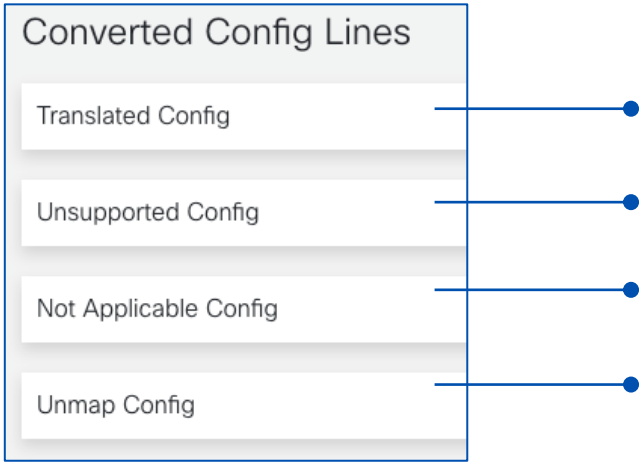
Unsupported (CLI not supported in IOS-XE)

Not Applicable (CLI deprecated/not used commands)

config spanningtree port mode off 1 ->> "SPT is not applicable in C9800."

Configuration Migration Tool

Migration Tool output:



Translated (CLI supported in IOS-XE)

Unsupported (CLI not supported in IOS-XE)

Not Applicable (CLI deprecated/not used commands)

Unmapped (CLI supported but not yet translated)

config custom-web webtitle " Welcome To <Company_Name>"

Pushing tags to APs

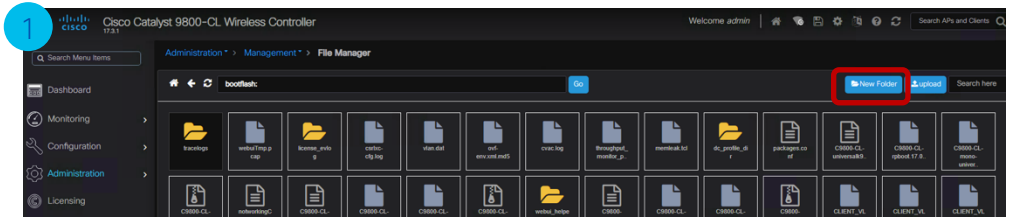
> EEM script (17.3.x)

Pushing tags to the AP (SW < 17.6.1)

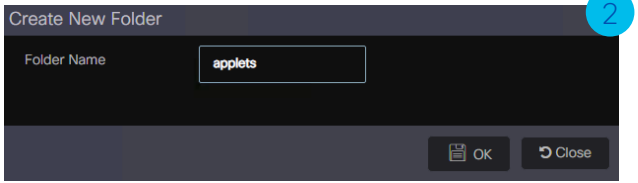
Simple script to do “write tag-config” automatically

- Download the script from here: https://github.com/fsedano/eem_ap_push
- On c9800 create a directory under bootflash and load the script > easily done via WebUI

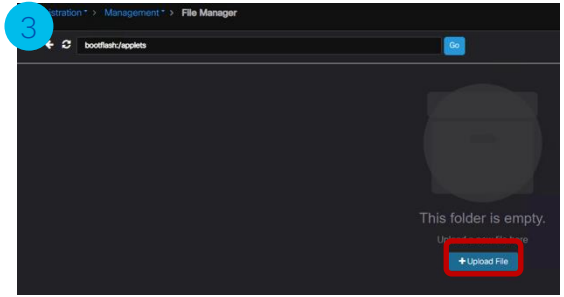
Administration > Management> File Manager: double click on bootflash.



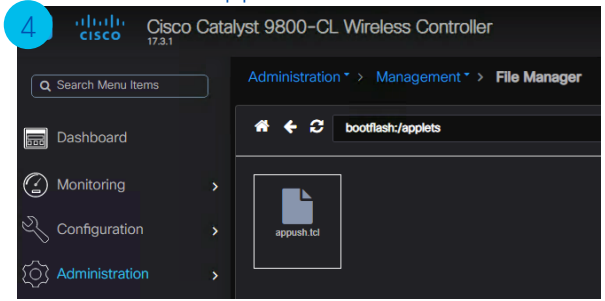
Click on New Folder and create folder “applets”



Double click on new folder and Click on Upload file



Load the “appush.tcl” file



Pushing tags to the AP (SW < 17.6)

- Verify the script is there:

```
C9800#dir bootflash:/applets
Directory of bootflash:/applets/
301922  -rw-             1850   Oct 1 2020 09:46:19 +00:00  appush.tcl
```

- Configure Embedded Event manager (EEM) to use the script:

```
C9800(config)#event manager directory user policy "bootflash:/applets"
C9800(config)#event manager policy appush.tcl
```

- Run the command when you want push the tags to the APs:

```
C9800#event manager run appush.tcl
Send --> ap name AP1 write tag-config
```

Primary controller

- Verify on the AP:

```
AP1# show capwap client config
[..]snip
AP Policy Tag                    : UNKNOWN
AP RF Tag                        : UNKNOWN
AP Site Tag                      : UNKNOWN
AP Tag Source                    : 0
```

Before

```
AP1# show capwap client config
[..]snip
AP Policy Tag                    : flex-tag
AP RF Tag                        : default-rf-tag
AP Site Tag                      : flex-site
AP Tag Source                    : 1
```

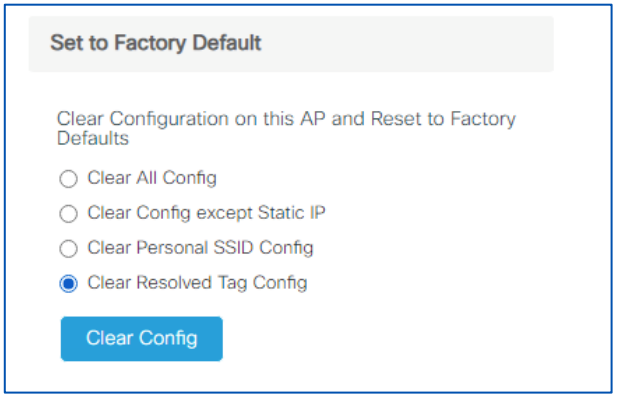
After

Removing AP Tag Persistency

Enter the command **`no ap tag persistency enable`** in the Global Configuration Mode as shown below:

```
9800CL(config)#no ap tag persistency enable
```

Note: this will disable the feature on C9800, it will NOT remove the tags on the APs. For that you can use the following Advanced Tab setting on AP GUI page



The equivalent exec level command:

```
C9800#ap name <name> no write tag-config
```

Or clear the CAPWAP config on the AP

More on Design

Wireless Config Analyzer Express (WCAE)

The wireless engineer trowel

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

starting 17.9

Back to Content Tab

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

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

AP Priming Profile and Filter - Considerations

- Max of **128** AP Priming Profiles can be configured
- Max of **1024** AP filters can be configured
  - Either for AP tag mapping or AP priming
  - Reduces number of AP filters available for tagging
- Pre-requisite: APs need to have a name to use the AP Priming filter

Statically Assign AP Priming Profile using MAC

```
C9800# configure terminal
C9800(config)# ap <MAC Address>
C9800(config-ap-tag)# profile <AP Priming Profile Name>
```

Example Static Assignment:

```
ap aaaa.bbbb.cccc
 profile ap-priming-profile
```

Verification
AP Priming Profile

```
C9800# show ap filters all type priming
Filter Name                    Regex                          Priming Profile
-------------------------------------------------------------------------------------------------
ap-priming-filter              (SITE)*                        ap-priming-profile
```

```
C9800# show wireless profile ap priming summary
Number of AP Priming Profiles: 1
Profile Name
---------------------------------
ap-priming-profile
```

```
C9800# show wireless profile ap priming detailed ap-priming-profile
Profile Name                          : ap-priming-profile
Primary Controller Name               : C9800-2
Primary Controller IP                 : 10.10.110.3
Secondary Controller Name             : C9800-1
Secondary Controller IP               : 10.10.210.3
Tertiary Controller Name              :
Tertiary Controller IP                : 0.0.0.0
Override                              : Enabled
```

Verification

Correct Priming Profile Assigned – Controller Side

Profile Assigned using Filter:

```
C9800# show ap name SITE1-9120-1 config general | sec Priming
Priming Profile                                 : ap-priming-profile
Priming Override                                : Enabled
Priming Source                                  : Filter
Priming Filter name                             : ap-priming-filter
```

Profile Assigned using Static Assignment:

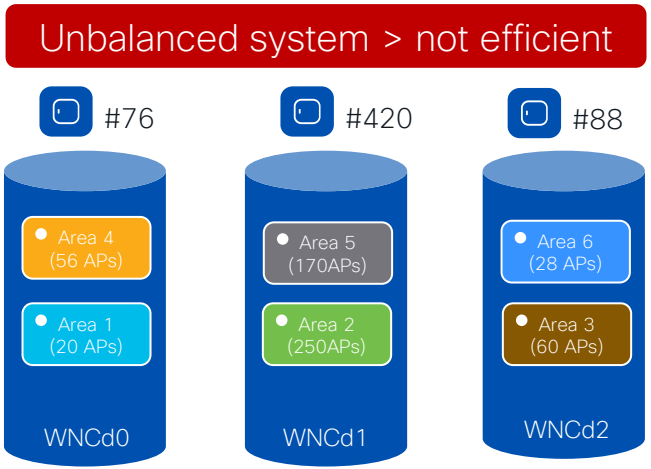
```
C9800# show ap name Static-9120-1 config general | sec Priming
Priming Profile                                 : ap-priming-profile
Priming Override                                : Enabled
Priming Source                                  : MAC
```

Verification

Correct Priming Profile Assigned – AP Side

```
SITE1-9120-1# show capwap client configuration | inc controller

Primary controller name                 : C9800-2
Primary controller IP                   : 10.10.110.3
Secondary controller name               : C9800-1
Secondary controller IP                 : 10.10.210.3
Tertiary controller name                :
```

Site Tags – AP to WNCd distribution



Before 17.10 (and 17.9.3), site tags are distributed among WNCds using the least loaded criteria based on the number of site tags.

Problem: Current algorithm can result in uneven WNCd load, as it doesn't take into considerations the number of APs or clients per site tag and it's dependent the order of AP joining. Also, it might not be possible to have an even distribution of APs among site tags

- Example: C9800-CL medium (#3 WNCd), six custom site tags with uneven number of APs per tag, 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 following:
  - 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 – AP to WNCd distribution

Let's just change the order of APs joining..

- Example: C9800-CL medium (#3 WNCd), six custom site tags with uneven number of APs per tag. Same as before, but with a different join order:
  - Area1 : #20 APs > WNCd0
  - Area3 : #60 AP > WNCd2
  - Area2 : #250 AP > WNCd1
  - Area5 : #170APs > WNCd0 (all WNCd has #1 tag, starting again from WNCd0)
  - Area4 : #56 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, area5 > #190 (20+170) APs
  - WNCd1 > site tags: area3, area4 > #114 (60+56) APs
  - WNCd2 > site tags: area2, area6 > #278 (250+28) APs
- This proves that with software < 17.9.2 (17.10), the distribution of APs across WNCd and hence the result system balance is dependent on the AP joining order

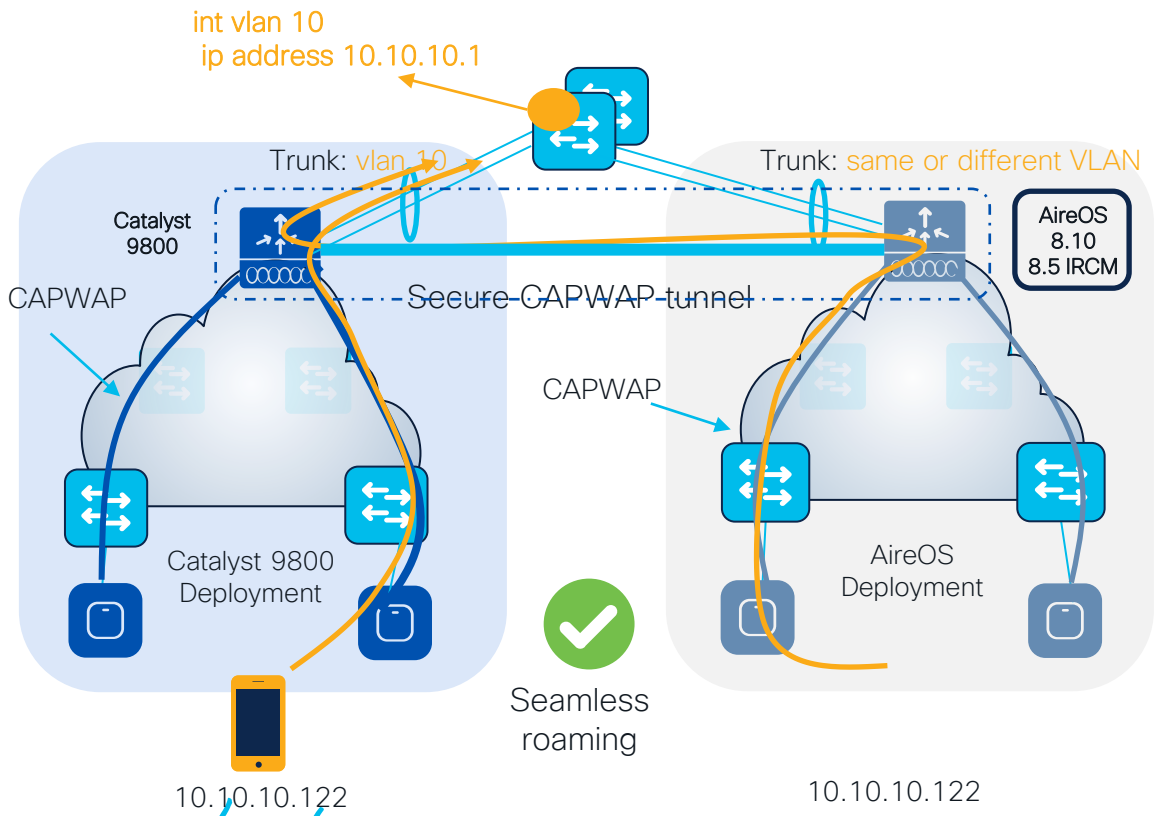
Site Tags – AP to WNCd distribution

Before 17.10 (and 17.9.3), another solution to get to a load balanced system would be to reconfigure the tags to have an even number of APs. Changing tags, will trigger a disruption as the APs will go for a CAPWAP restart.

- Example: C9800-CL medium (#3 WNCd), six custom site tags with ~ even number of APs per tags and APs joining in this order:
  - Area1 : #90 APs > WNCd0
  - Area2 : #95 AP > WNCd1
  - Area3 : #92 AP > WNCd2
  - Area4 : #88 APs > WNCd0 (all WNCd has #1 tag, starting again from WNCd0)
  - Area5 : #105 APs > WNCd1 (as WNCd0 has already #2 tags)
  - Area6 : #114 Ps > 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 > #178 (90+88) APs
  - WNCd1 > site tags: area2, area5 > #200 (95+105) APs
  - WNCd2 > site tags: area3, area6 > #206 (92+114) APs
- System turns out to be balanced

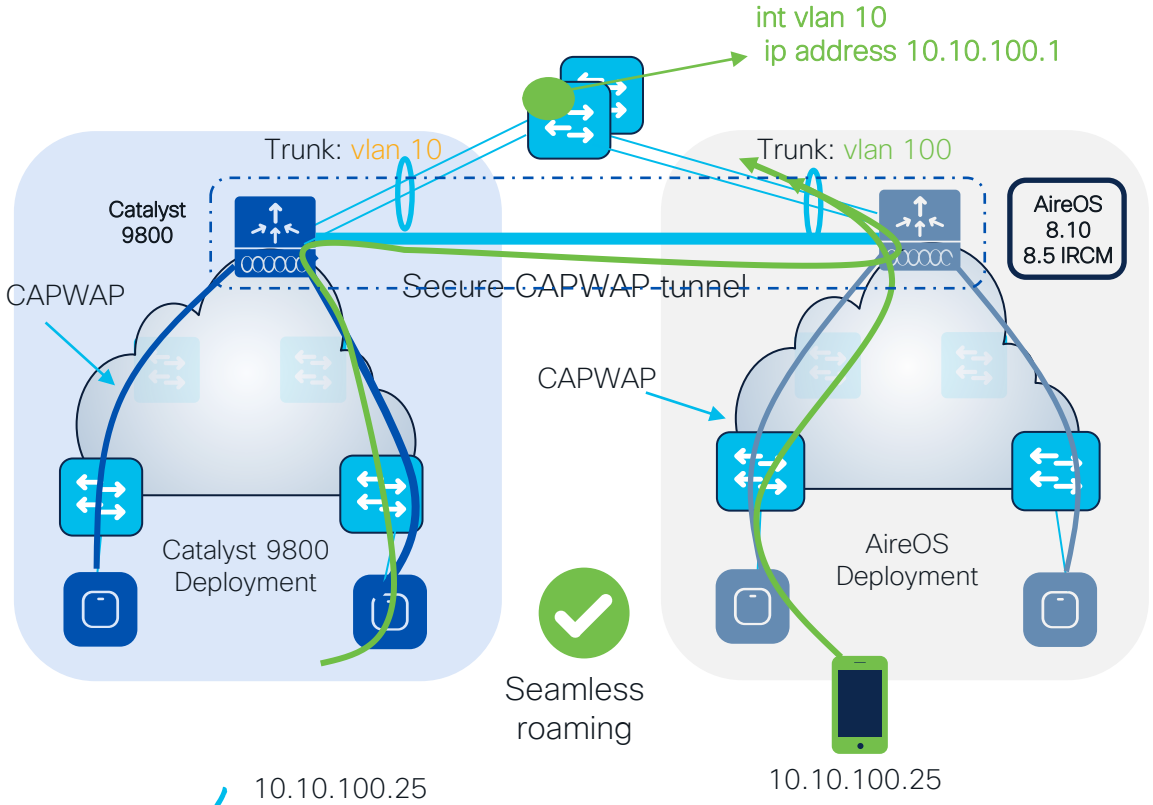
More on Migration scenarios

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 presence 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

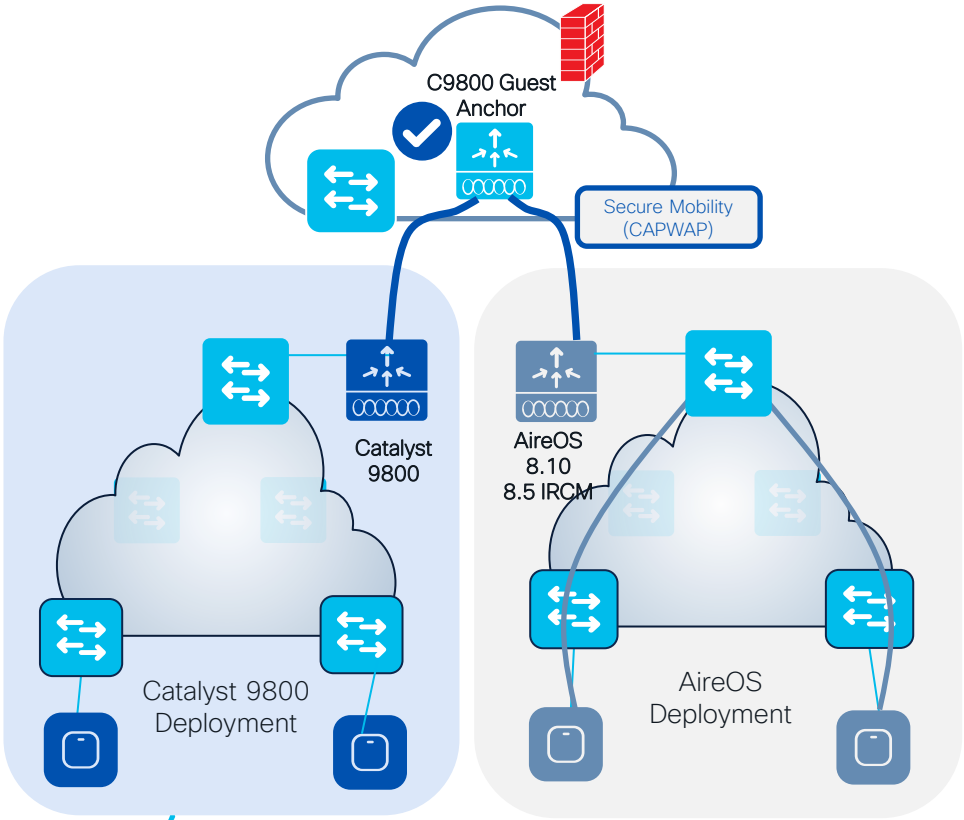
AireOS and IOS-XE coexistence – Roaming



Recommendations:

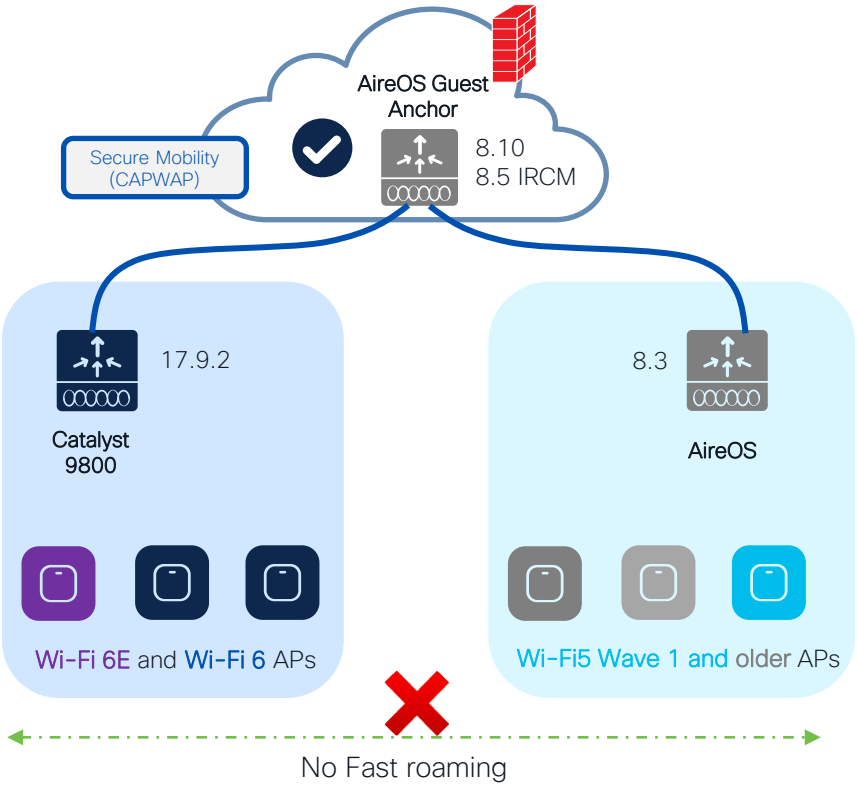
- In the Design Migration phase, whenever possible, use different VLAN IDs and use different subnets
- Consequence: clients will get a different IP whether it joins first 9800 or AireOS; seamless roaming is anyway guaranteed
- When this might not be possible:
  - Customer is not willing to change the 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 coexistence – Guest Anchor



- Same IRCM code recommendations apply for Foreign – Anchor
- List of parameters that must match between Foreign and Anchor:
  - WLAN and Policy profiles names
  - WLAN profile > security settings
  - Policy profile > DHCP need to match
  - WebAuth parameter-map name and type
- Note: When anchoring to and from AireOS, use the IRCM image and match WLAN profile name, security and DHCP settings

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



Scenario 4: AireOS WLC not supporting IRCM

- Not possible to establish IRCM between AireOS controller and new 9800 handling Wi-Fi6E APs
- Limited options available > Forces more aggressive migration process.
- Migration considerations:
  - Keep the two networks separated ; migrate physical RF areas as new APs are added.
  - Fast and seamless roaming is not possible.
  - Avoid migrations “per floor” as in most building types, it is normal to see clients roaming between APs on different floor.
  - Temporarily, replace the legacy controller with one that supports IRCM.

Access Points – Migration Options

Model/Series	Last AireOS support	IOS-XE Support	Wi-Fi 6 AP Equivalent	Wi-Fi 6E AP Equivalent	Migration Notes
700/700W Series	8.10	Not supported	9105	9162	Migration through IRCM
1040	8.3	Not supported	9115	9164	AP needs to be replaced
1260	8.3	Not supported	9115	9164	AP needs to be replaced
1600	8.5	Not supported	9115	9164	Either 8.5 IRCM, or Hardware replaced
1700	8.10	17.3	9115	9164	Migration through IRCM
2700	8.10	17.3	9120	9166	Migration through IRCM
3700	8.10	17.3	9120	9166	Migration through IRCM
1810	8.10	Up to 17.3	9105	9162	Hardware replaced or IRCM between IOS-XE versions
1815/1830/1840/1850	8.10	Supported	9105	9162	Directly supported
2800/3800/4800	8.10	Supported	9120/9130	9164/9166	Directly supported
1540	8.10	Supported	9124	NA	Directly supported
1550	8.5	Not supported	NA	NA	Migration through IRCM
1560	8.10	Supported	9124	NA	Directly supported
1570	8.10	Up to 17.3	9124	NA	Migration through IRCM

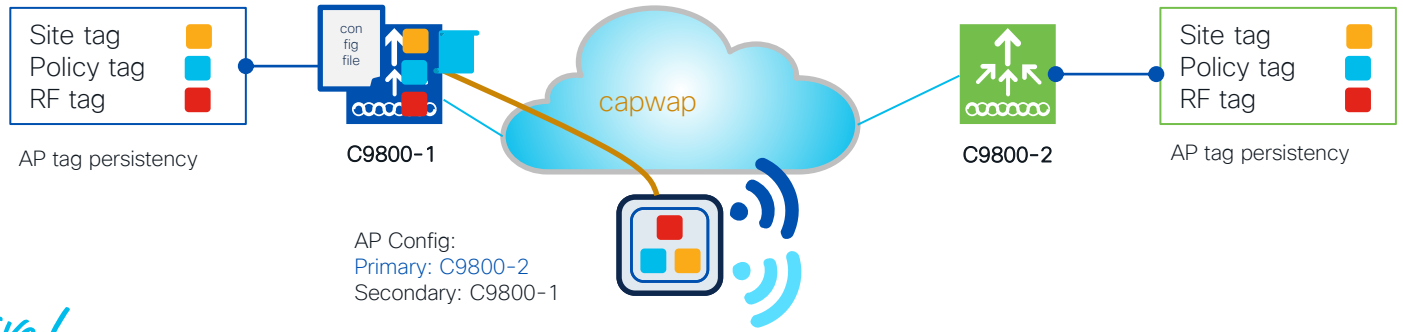
Complete List : Cisco Wireless Solutions Software Compatibility Matrix: https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

Customer Migration scenario: Moving APs between WLCs @scale

Moving APs between WLCs @scale

How to move APs between WLCs @ scale? Best way is to change the Primary WLC for all the APs you want to move > Priming the APs with the new WLC's IP

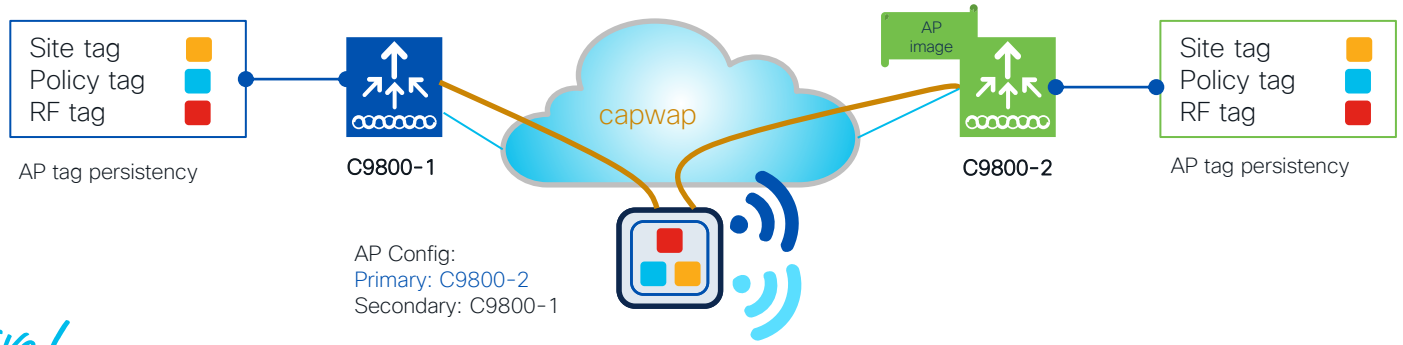
1. Match the C9800-1 configuration using a different set of IP for Management interface
2. Configure C9800-2 with same AP tags and enable tag persistency on both WLCs
3. On C9800-1 change the primary WLC on APs to point to C9800-2. This can be done easily with DNA Center Configure AP workflow or with the new Priming Profile in 17.10. For release before 17.10, see the Event Manager script in bonus slides



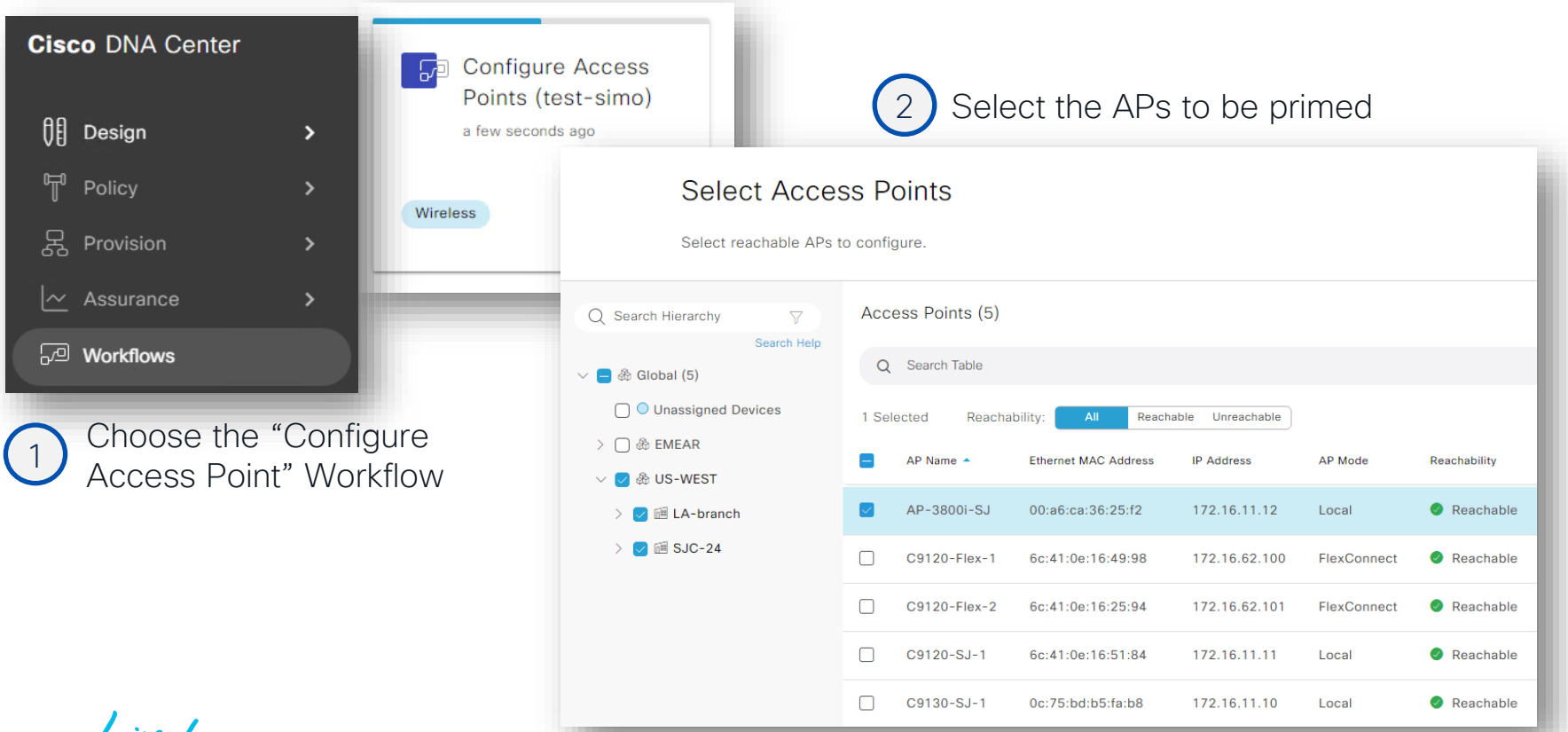
Moving APs between WLCs @scale

How to move APs between WLCs @ scale? Best way is to change the Primary WLC for all the APs you want to move > Priming the APs with the new WLC's IP

1. Match the C9800-1 configuration using a different set of IP for Management interface
2. Configure C9800-2 with same AP tags and enable tag persistency on both WLCs
3. On C9800-1 change the primary WLC on APs to point to C9800-2. This can be done easily with DNA Center Configure AP workflow or with the new Priming Profile in 17.10. If no Cisco DNA Center, for release before 17.10, see the Event Manager script in bonus slides
4. APs will move C9800-2. In this case, AP will download the new code, reboot and join again



DNA Center: Configure AP workflow

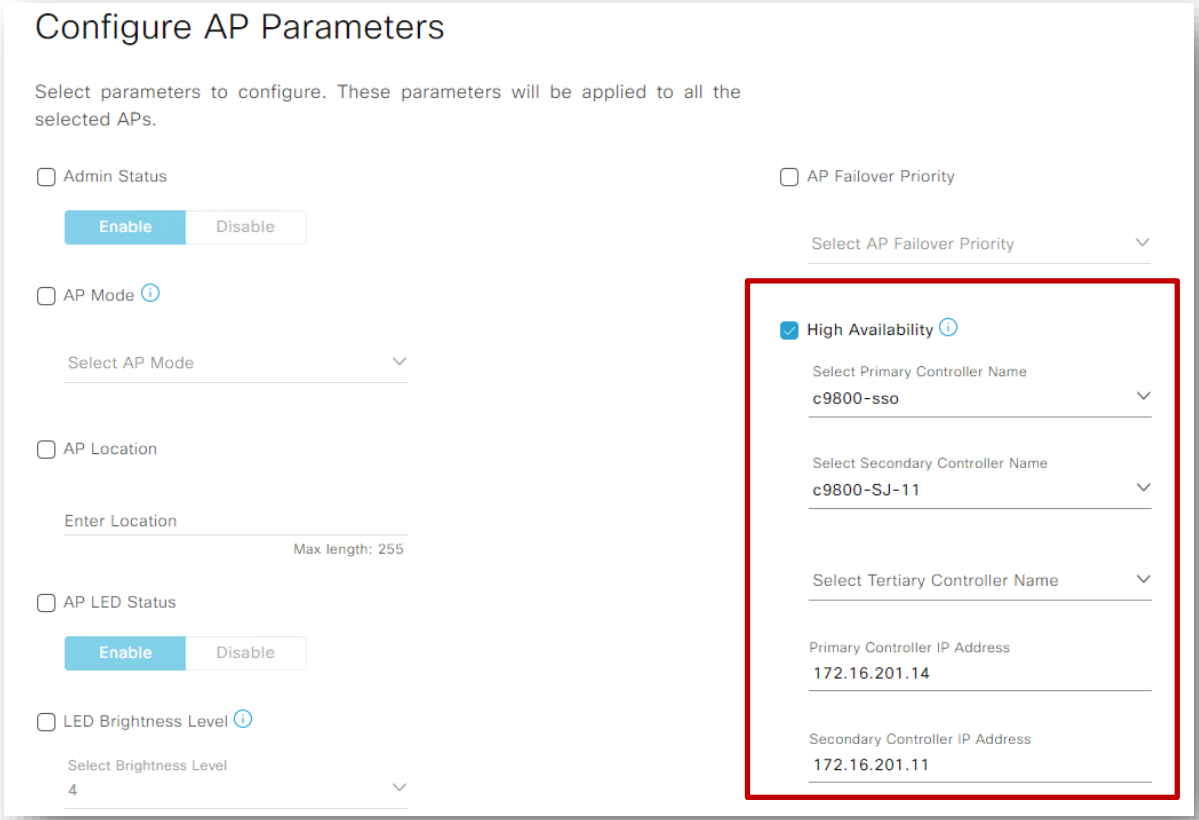


1 Choose the “Configure Access Point” Workflow

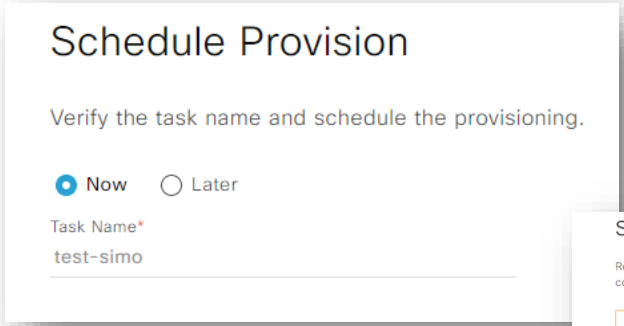
2 Select the APs to be primed

DNA Center: Configure AP workflow

3 Configure Primary and optionally Secondary WLC

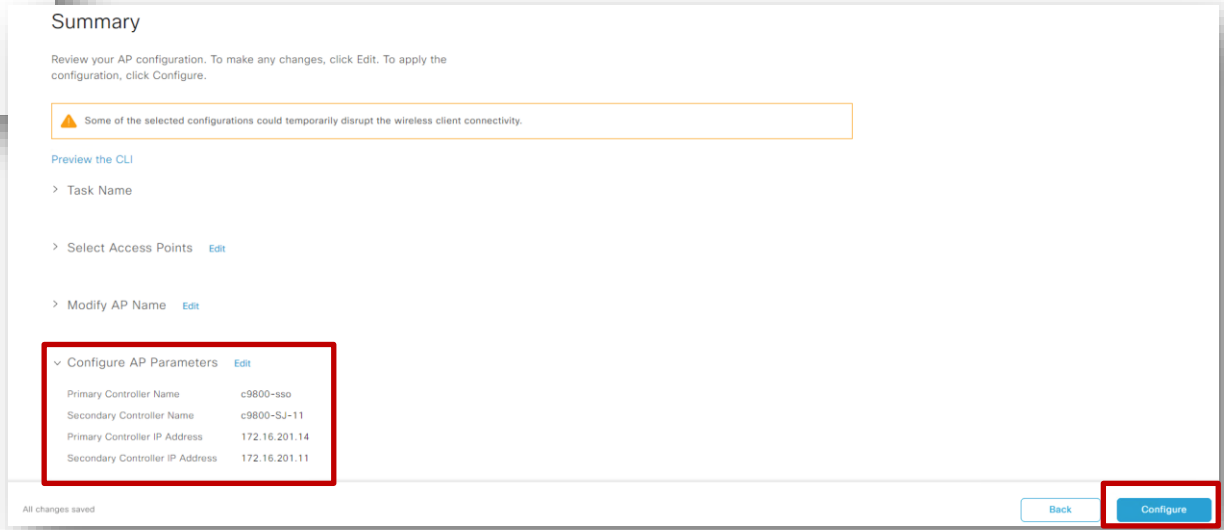


DNA Center: Configure AP workflow



4 Schedule the changes

5 Review and apply the configuration



AP Priming Profile and AP Priming Filter

AP Priming Profile

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

AP Priming Filter

- Similar structure as the filter for AP tag mapping
- Uses RegEx string to match APs based on their names > need APs to be named!
- Applies the mapped AP Priming Profile to the matched APs

Configuring the AP Priming Profile

```
C9800# configure terminal
C9800(config)# wireless profile ap priming <Priming Profile Name>
C9800(config-priming)# primary <Primary WLC Name> <Primary WLC IP Address>
C9800(config-priming)# secondary <Secondary WLC Name> <Secondary WLC IP Address>
C9800(config-priming)# tertiary <Tertiary WLC Name> <Tertiary WLC IP Address>
C9800(config-priming)# priming-override
```

Overrides existing priming configurations; NEEDED for already configured APs – Not enabled by default

Example of AP Priming Profile:

```
wireless profile ap priming ap-priming-profile
 primary C9800-2 10.10.110.3
 secondary C9800-1 10.10.210.3
 priming-override
```

Configuring the AP Priming Filter

```
C9800# configure terminal
C9800(config)# ap filter name <Filter Name> type priming
C9800(config-ap-pr-filter)# ap name-regex <RegEx String to Match>
C9800(config-ap-pr-filter)# profile <AP Priming Profile Name>
```

Example Priming Filter:

```
ap filter name ap-priming-filter type priming
 ap name-regex (SITE)*
 profile ap-priming-profile
```

Activate AP Filter

```
C9800# configure terminal
C9800(config)# ap filter priority <Priority Number> filter-name <Filter Name>
```

Example Filter Priority:

```
ap filter priority 1 filter-name ap-priming-filter
```

Setting Primary/Secondary/Tertiary (EEM script)

Moving APs between C9800 controllers
Event Manager script

- (Optional) Configure a first EEM script to just get the number of APs and print the configuration to be pushed. Just copy and paste the below lines in configuration mode:

```
event manager applet CHECK_APS
 event none
 action 101 cli command "en"
 action 102 cli command "term len 0"
 action 104 cli command "sh ap summary | ex AP Name|Number of APs:|----------------------------"
 action 106 foreach line "$_cli_result" "\n"
 action 107  regexp "^([^ ]+).*\r$" "$line" _match _AP_NAME
 action 108  if $_regexp_result eq "1"
 action 113   puts "ap name $_AP_NAME controller primary WLC1  IP1"
 action 114   puts "ap name $_AP_NAME controller secondary WLC2  IP2"
 action 115   puts "ap name $_AP_NAME controller tertiary WLC3 IP3"
 action 116  end
 action 117 end
```

- Run the script with the following command:

```
C9800#event manager run CHECK_APS
```

Moving APs between C9800 controllers
Event Manager script

- Configure the actual EEM script to push the Primary/Secondary and eventually Tertiary configuration to the APs. This applies to all the APs you have on the controller:

```
event manager applet PRIMARY_SECONDARY_TERTIARY
 event none maxrun 600
 action 101 cli command "en"
 action 102 cli command "term len 0"
 action 104 cli command "sh ap summary | ex AP Name|Number of APs:|----------------------------"
 action 106 foreach line "$_cli_result" "\n"
 action 107  regexp "^([^ ]+).*\r$" "$line" _match _AP_NAME
 action 108  if $_regexp_result eq "1"
 action 110   cli command "ap name $_AP_NAME no controller primary WLC1"
 action 111   cli command "ap name $_AP_NAME no controller secondary WLC2"
 action 112   cli command "ap name $_AP_NAME no controller tertiary WLC3"
 action 123   cli command "ap name $_AP_NAME controller primary C9800-OEAP 2.228.173.185"
 action 124   cli command "ap name $_AP_NAME controller secondary Gladius1 192.168.25.41"
 action 125   cli command "ap name $_AP_NAME controller tertiary Gladius2 192.168.25.42"
 action 135  end
 action 136 end
 action 141 cli command "sh ap config general | i Cisco Controller"
 action 142 puts "Final Configuration:"
 action 143 puts "($_cli_result)”

!! In case of fallback disabled or you want to move APs immediately, add this line
 action 126 cli command "ap name $_AP_NAME reset capwap"
```

Moving APs between C9800 controllers
Event Manager script – verification

- AP is not configured with Primary/Secondary/Tertiary

```
C9800#sh ap name AP-1815 config general | b Primary Cisco Controller Name
Primary Cisco Controller Name                    : Not Configured
Primary Cisco Controller IP Address              : 0.0.0.0
Secondary Cisco Controller Name                  : Not Configured
Secondary Cisco Controller IP Address            : 0.0.0.0
Tertiary Cisco Controller Name                   : Not Configured
Tertiary Cisco Controller IP Address             : 0.0.0.0
Administrative State                             : Enabled
```

- Let's verify if settings are correct first (only one AP is on the WLC):

```
C9800#event manager run CHECK_APS
ap name AP-1815 controller primary C9800-1 10.1.1.1
ap name AP-1815 controller secondary C9800-2 1 10.2.2.2
ap name AP-1815 controller tertiary C9800-3 10.3.3.3
```

Moving APs between C9800 controllers
Event Manager script - verification

- Push the configuration to the APs

```
C9800#event manager run PRIMARY_SECONDARY_TERTIARY
Final Configuration:
Primary Cisco Controller Name                    : C9800-1
Primary Cisco Controller IP Address              : 10.1.1.1
Secondary Cisco Controller Name                  : C9800-2
Secondary Cisco Controller IP Address            : 10.2.2.2
Tertiary Cisco Controller Name                   : C9800-3
Tertiary Cisco Controller IP Address             : 10.3.3.3
```

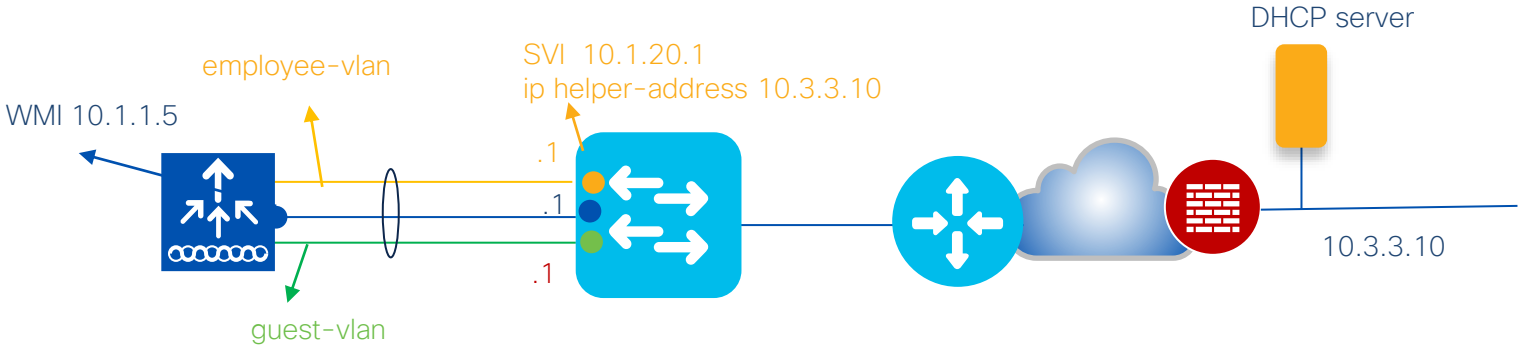
- Let's verify if settings have been applied

```
C9800#sh ap name AP-1815 config general | b Primary Cisco Controller Name
Primary Cisco Controller Name                    : C9800-1
Primary Cisco Controller IP Address              : 10.1.1.1
Secondary Cisco Controller Name                  : C9800-2
Secondary Cisco Controller IP Address            : 10.2.2.2
Tertiary Cisco Controller Name                   : C9800-3
Tertiary Cisco Controller IP Address             : 10.3.3.3
Administrative State                             : Enabled
```

IP DHCP relay on C9800

Understanding DHCP proxy/relay

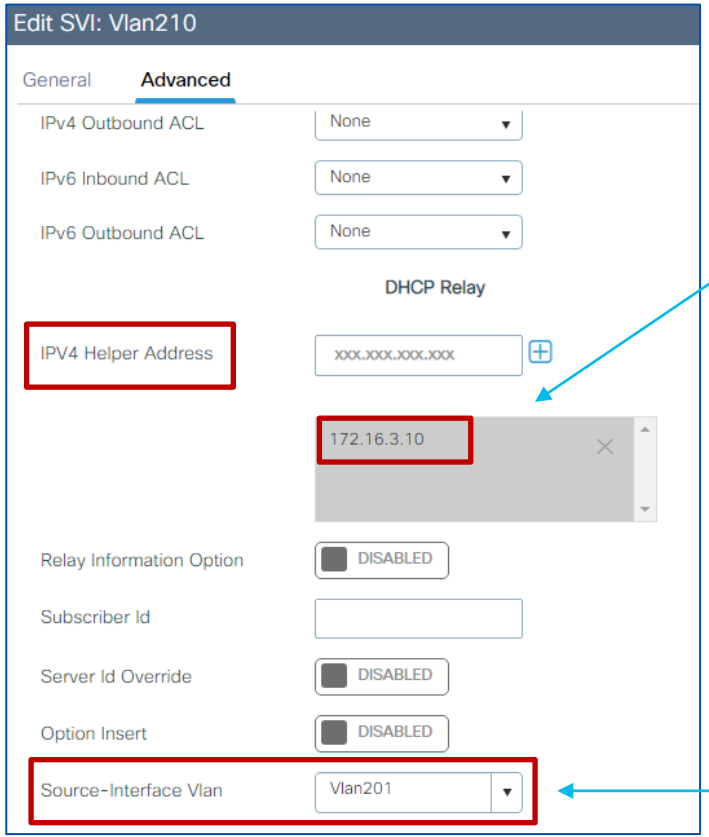
- DHCP Proxy mode:
  - In AireOS, enabling DHCP Proxy for wireless clients is a best practice
  - In C9800 DHCP proxy is not needed as IOS-XE has embedded security features like DHCP snooping, ARP inspection, etc. that don't require a L3 interface
- DHCP relay or DHCP bridging mode?
  - DHCP bridging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



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

C9800 as DHCP relay for client VLAN



- Create an SVI for the client VLAN (e.g. “Vlan210” in this case)
- Add the DHCP Server IP > this configures “ip helper” 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 may result in asymmetric traffic and in Reverse Path Forwarding (RPF) failures on the first hop switch/firewall
- To avoid this, the first step is to configure a specific interface as source for DHCP packets > in this case we want DHCP traffic to be sourced from WMI (e.g., Vlan 201 > IP 172.16.201.11):

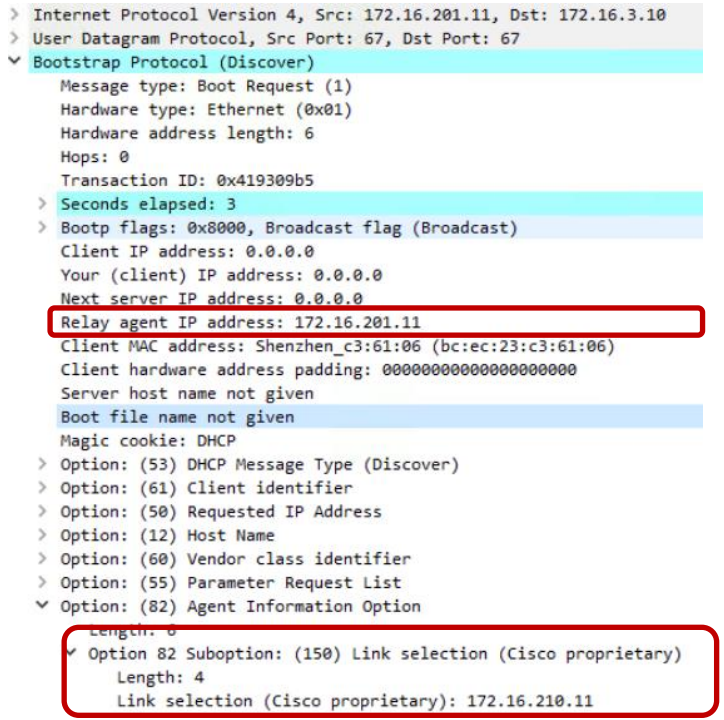
```
interface Vlan210
 description Employee-SVI
 ip address 172.16.210.21 255.255.255.0
 ip helper-address 172.16.3.10
 ip dhcp relay source-interface vlan 201
```

C9800 as DHCP relay for client VLAN

- In this case the source of the DHCP packets and the GIADDR are set to the interface specified in the DHCP relay command (172.16.201.11 in this case)

How does the DHCP server know how to assign the IP from the right client pool?

- When the “ip dhcp relay source-interface” command is used, C9800 automatically adds the client subnet information in a proprietary sub option 150 of option 82 (called “link selection”), as you can see from the capture
- You need to configure your DHCP server to assign IP addresses based on the link selection information, as this indicates the right client pool…

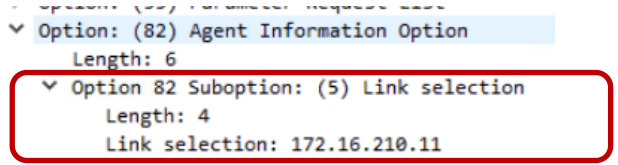


C9800 as DHCP relay for client VLAN

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

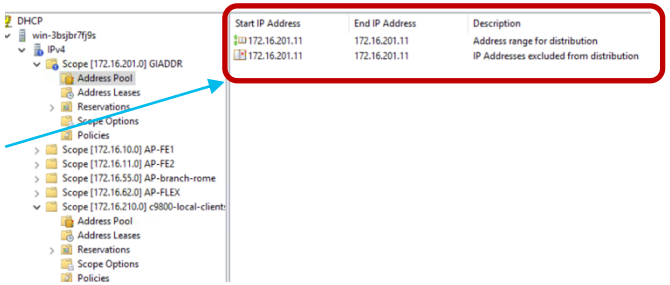
```
ip dhcp compatibility suboption link-selection standard
```

As you can see the option for link selection has changed



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

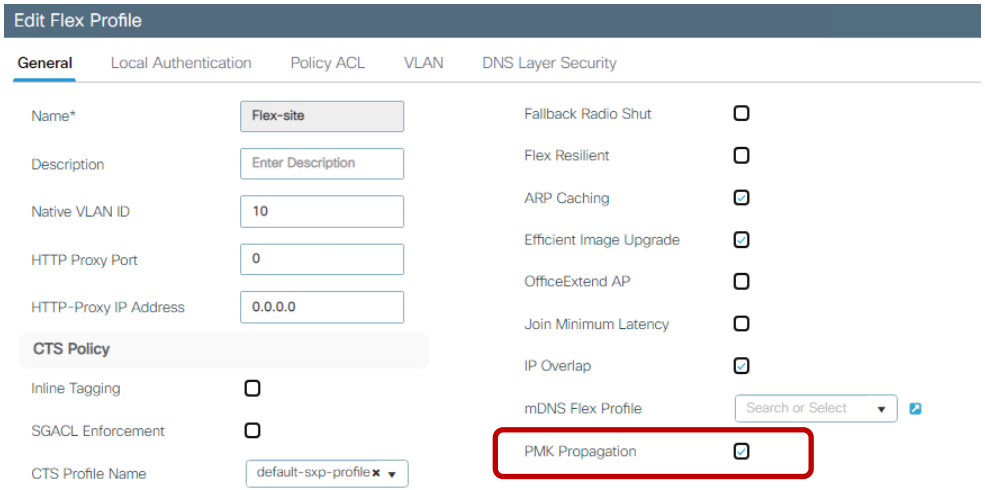
- You have to create a dummy scope to “authorize” the IP of the relay agent. In our example, it’s the IP of the VLAN 201, the WMI (172.16.201.11). You have to add the IP to the scope and then exclude it from the distribution



FlexConnect

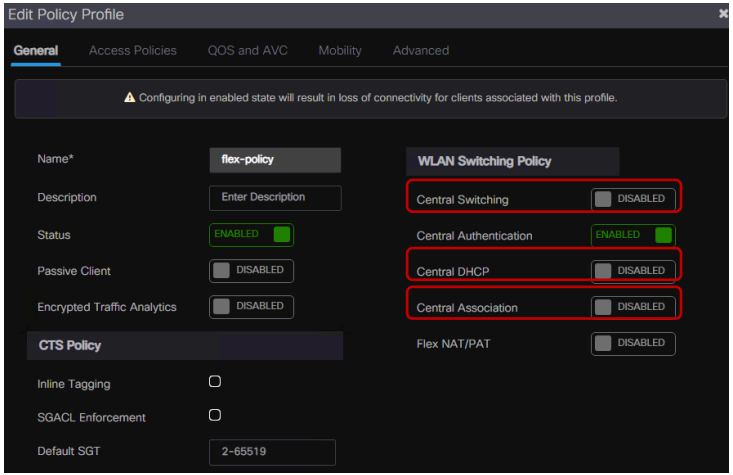
Site Tag for FlexConnect Deployments

- Starting 17.8, the limit is extended to 300 APs and 3000 clients
- This is achieved by using a local Pairwise Master Key (PMK) distribution. This needs to be enabled at a Flex Profile level

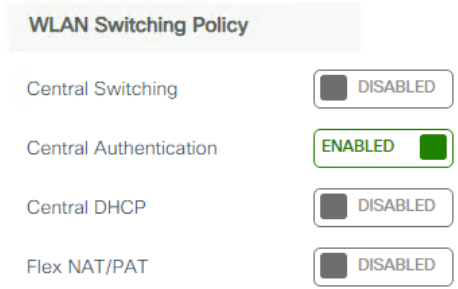


Important > Flex Policy Profile configuration

- In a FlexConnect deployment, the client (802.11) association is handled at the AP. This needs to be reflected in the Policy Profile configuration > Central Association needs to be disabled.



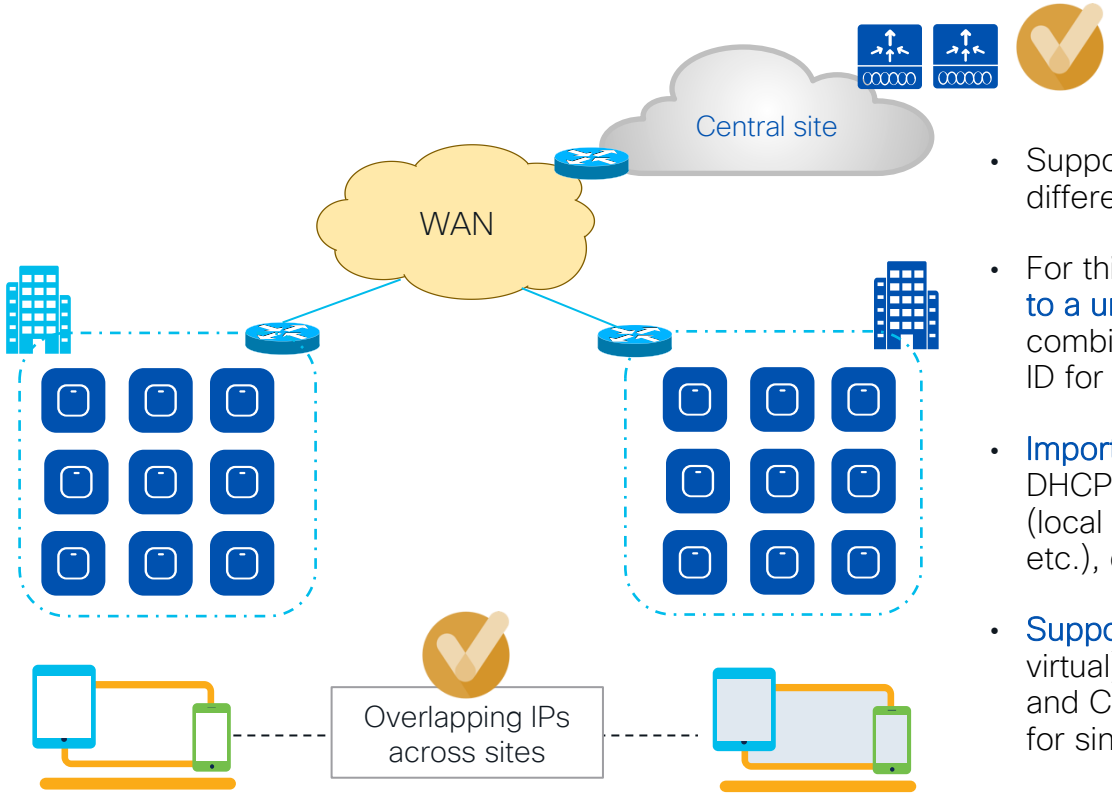
From 17.5 Central association is removed!



- If Flex Local Switching is configured, then DHCP traffic needs to be local as well

FlexConnect: Overlapping IP across sites

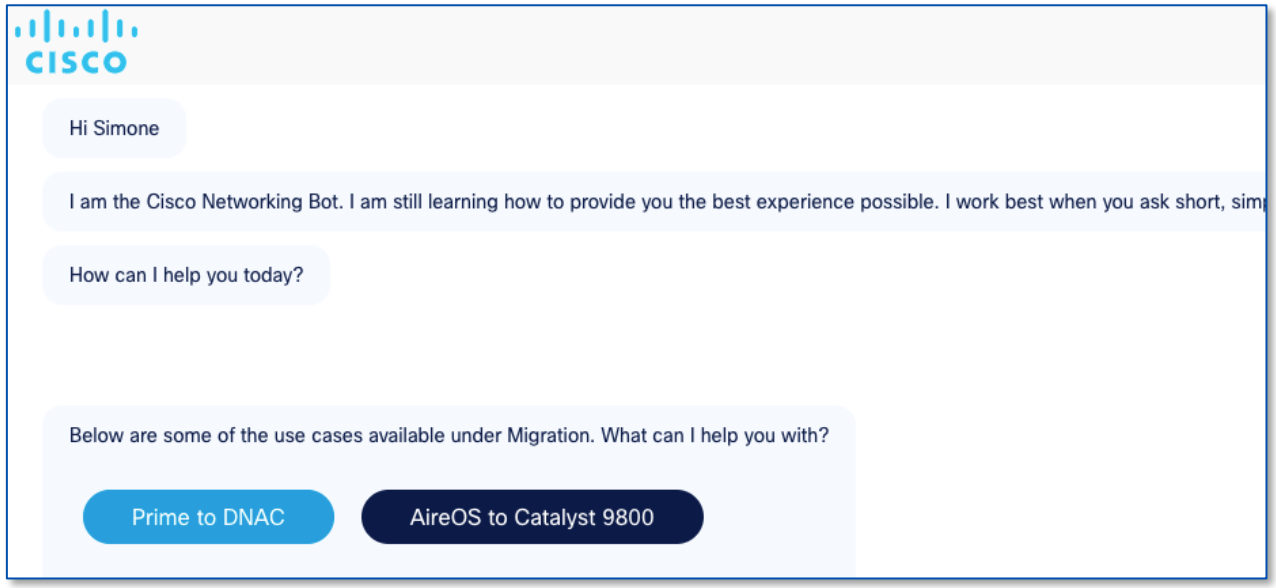
Solution supported starting 17.3.3



- Support for client overlapping IP addresses in different sites is introduced in 17.3.3
- For this to work, every site needs to be assigned to a unique site-tag > C9800 uses the combination of site-tag + IP address as a unique ID for the client (called zone-id)
- Important: this is only available for Flex local DHCP/ local switching; for all other deployments (local mode, central switching, central DHCP, etc.), overlapping IPs are still not supported
- Supported on all C9800 appliances (physical and virtual). Not supported on EWC on Catalyst AP and Catalyst 9k switch because these are meant for single site deployments

NEW self-guided migration tool

- Use the Cisco Networking bot: https://cnb.cisco.com/web > type “migration” as the question > choose AireOS to C9800 for a self-guided migration. Need CCO account



Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the " Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

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

The bridge to possible

Thank you

cisco Live!


CISCO Live!
ALL IN