cisco Live!

#CiscoLive

The bridge to possible

How to successfully migrate to Catalyst 9800

Catalyst Wireless

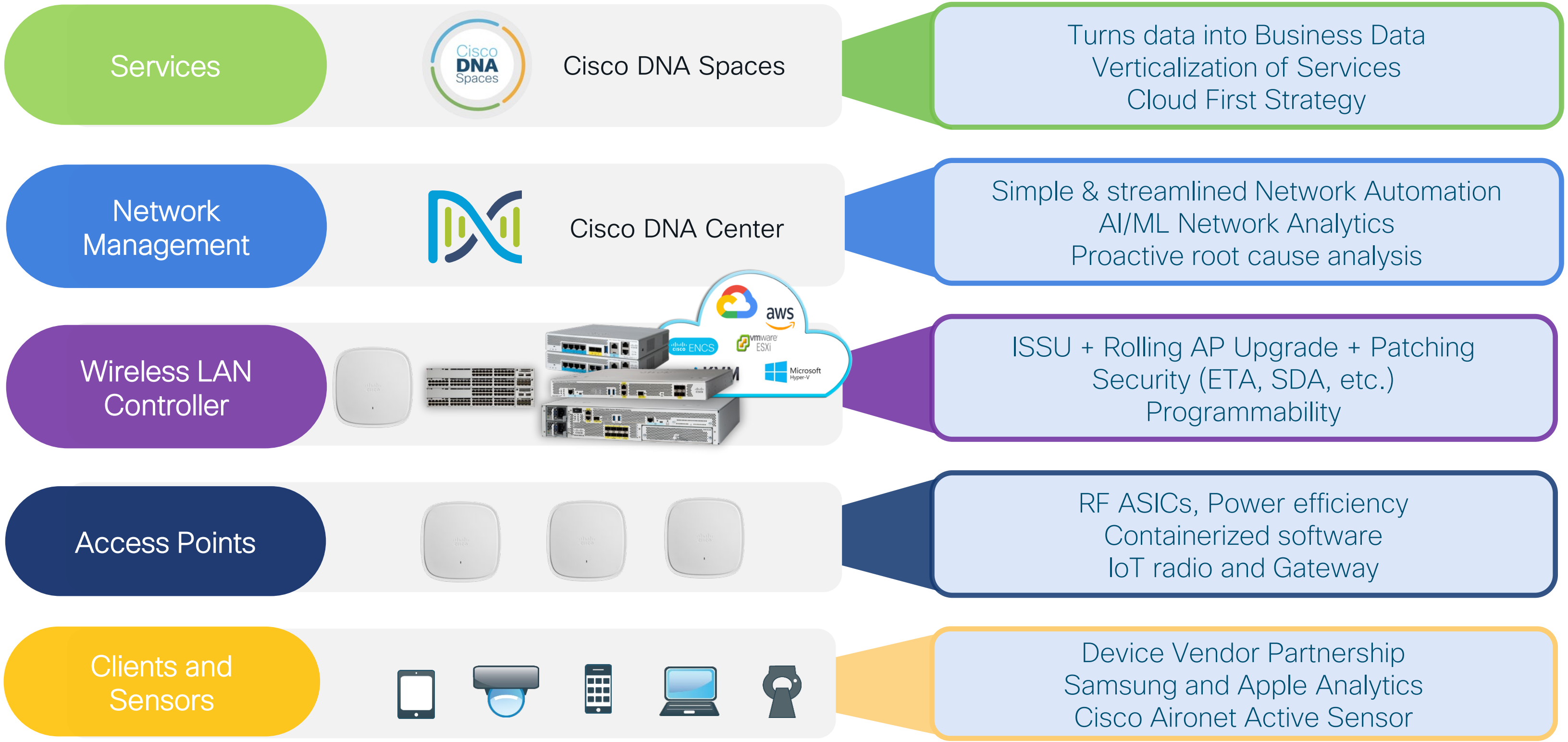
Simone Arena, Principal TME
@siarena71

BRKEWN-2041

Agenda

- Migration plan: A customer use case
- Migration Best Practices
- Design with AP tags in mind
- Lesson Learned
- Recommendations

Catalyst Wireless Innovation at each layer



Services — Cisco DNA Spaces

- Turns data into Business Data
- Verticalization of Services
- Cloud First Strategy

Network Management — Cisco DNA Center

- Simple & streamlined Network Automation
- AI/ML Network Analytics
- Proactive root cause analysis

Wireless LAN Controller

- ISSU + Rolling AP Upgrade + Patching
- Security (ETA, SDA, etc.)
- Programmability

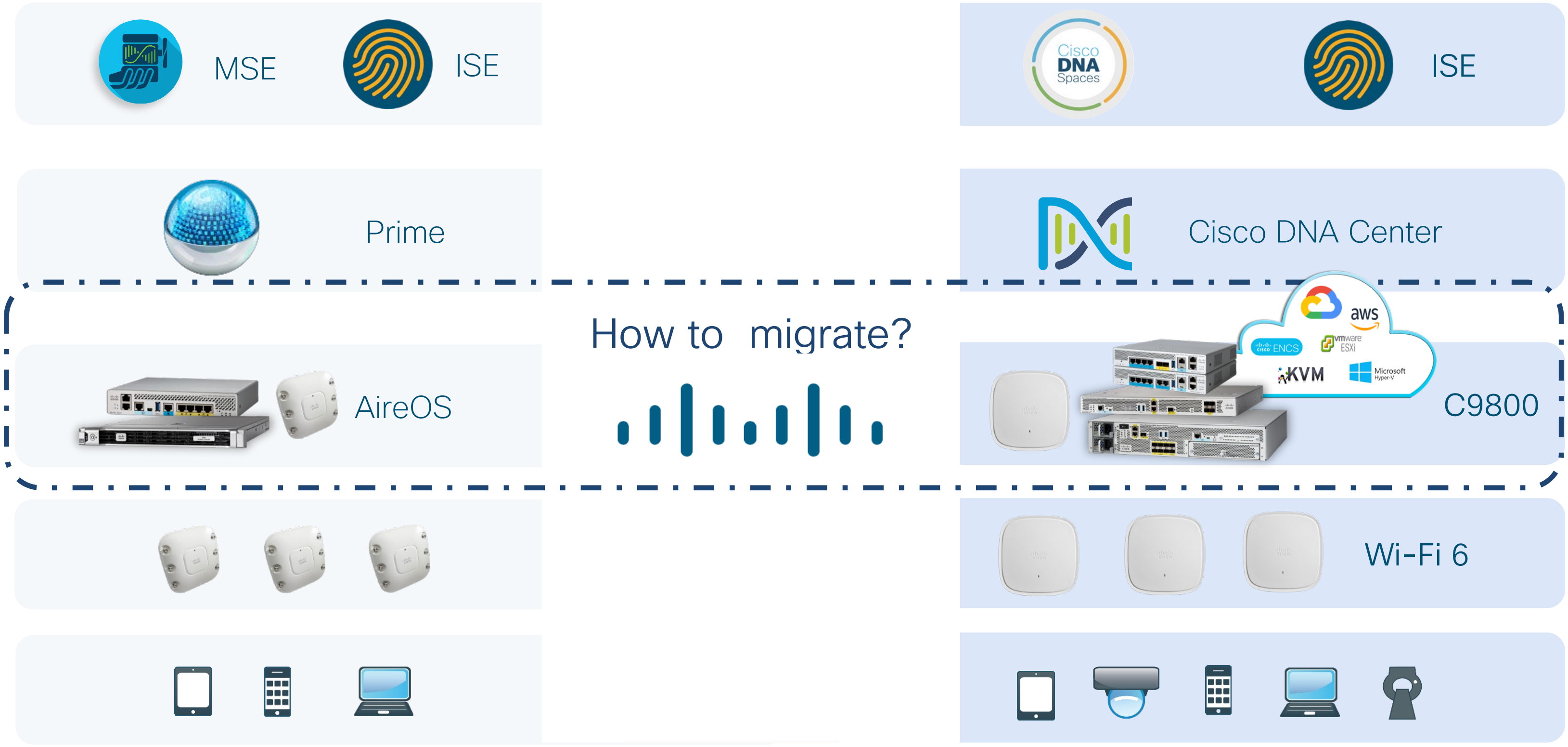
Access Points

- RF ASICs, Power efficiency
- Containerized software
- IoT radio and Gateway

Clients and Sensors

- Device Vendor Partnership
- Samsung and Apple Analytics
- Cisco Aironet Active Sensor

Focus on the “how?”



MSE

ISE

Prime

AireOS

How to migrate?

ISE

Cisco DNA Center

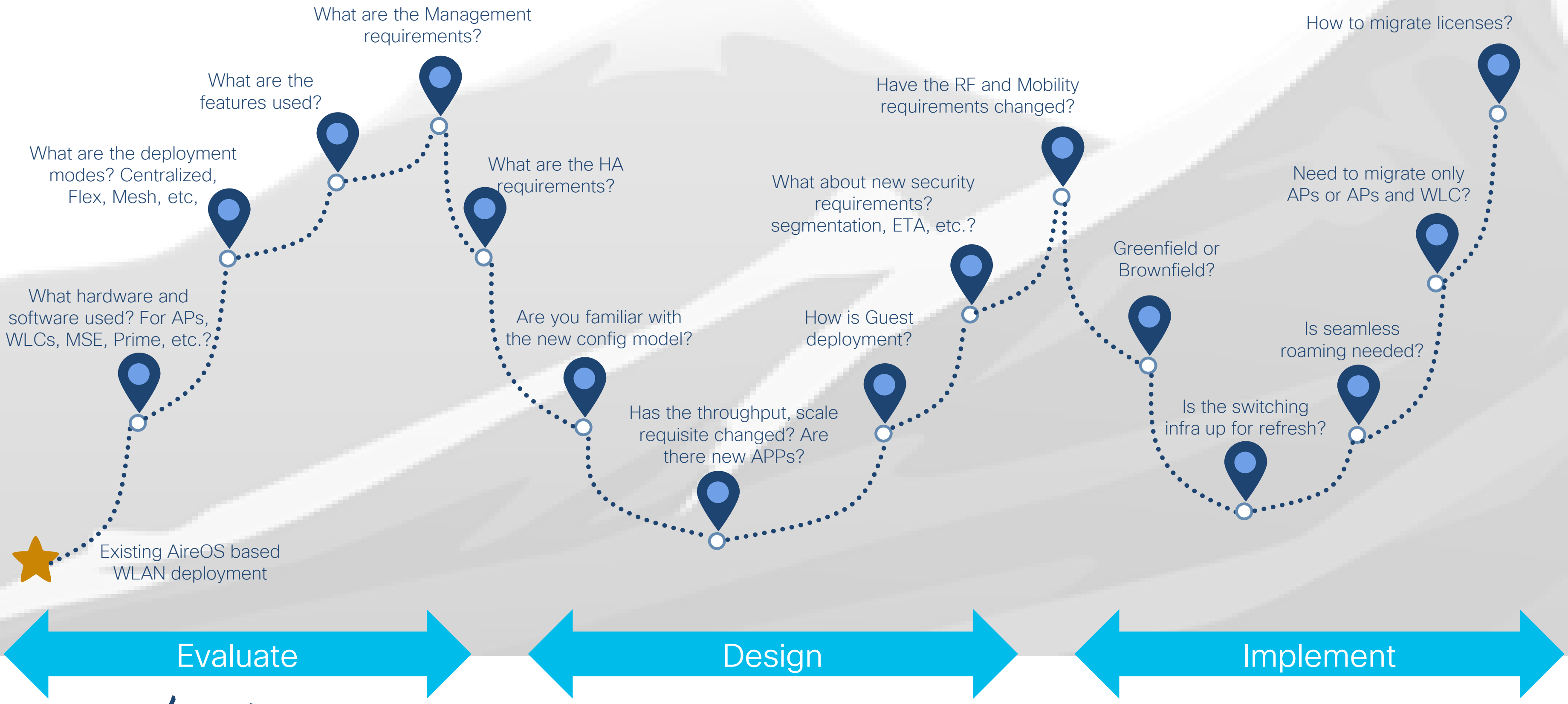
C9800

Wi-Fi 6

Where shall I start?

….asking questions!

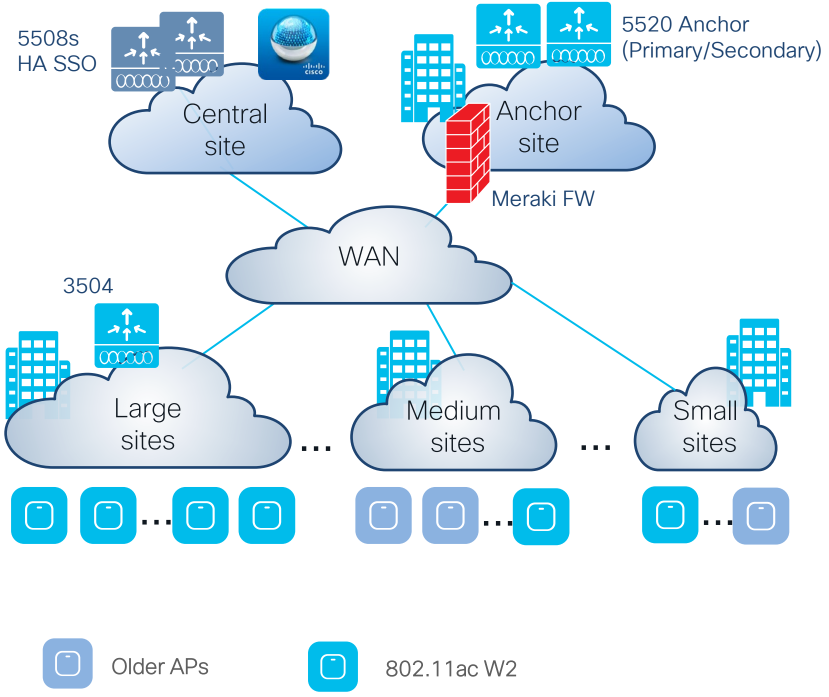
Key Questions for Migration



Existing AireOS based WLAN deployment
What hardware and software used? For APs, WLCs, MSE, Prime, etc.?
What are the deployment modes? Centralized, Flex, Mesh, etc,
What are the features used?
What are the Management requirements?
What are the HA requirements?
Are you familiar with the new config model?
Has the throughput, scale requisite changed? Are there new APPs?
How is Guest deployment?
What about new security requirements? segmentation, ETA, etc.?
Have the RF and Mobility requirements changed?
Greenfield or Brownfield?
Is the switching infra up for refresh?
Is seamless roaming needed?
Need to migrate only APs or APs and WLC?
How to migrate licenses?
Evaluate
Design
Implement

Migration plan: A customer use case

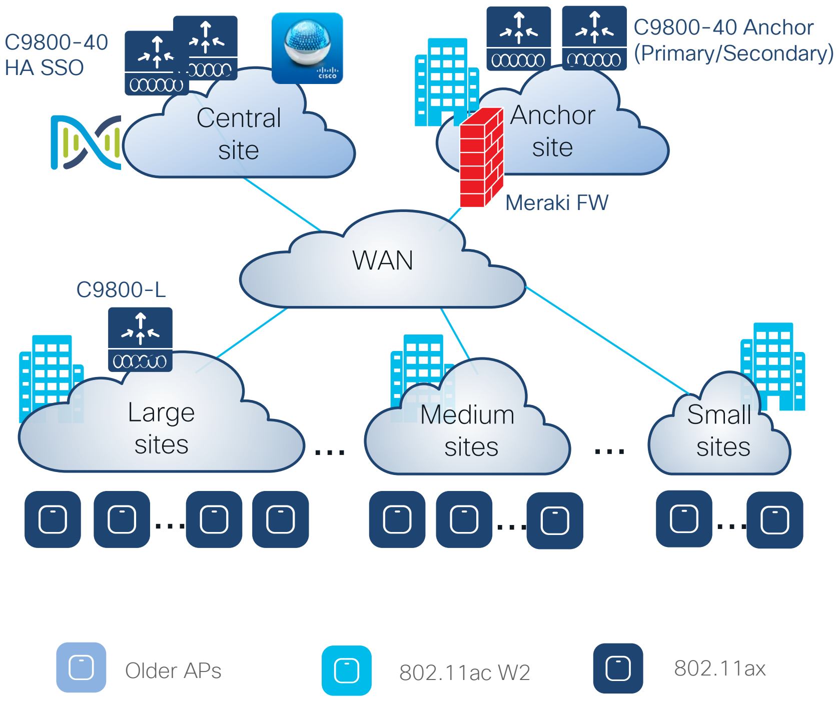
Customer Migration scenario



Current customer deployment:

- Manufacturing customer with about 180 sites
- Larger sites have local controller (3504), smaller sites run in Flex mode with central WLCs in HA SSO mode (5508). AireOS: 8.8 on 3504s an 8.5 on 5508s
- Guest Anchor Controller (Primary and Secondary HA) running on 5508 with 8.5. Meraki firewall at the Anchor site
- Mix of 802.11ac W2 APs, few older APs
- Prime for configuration and monitoring

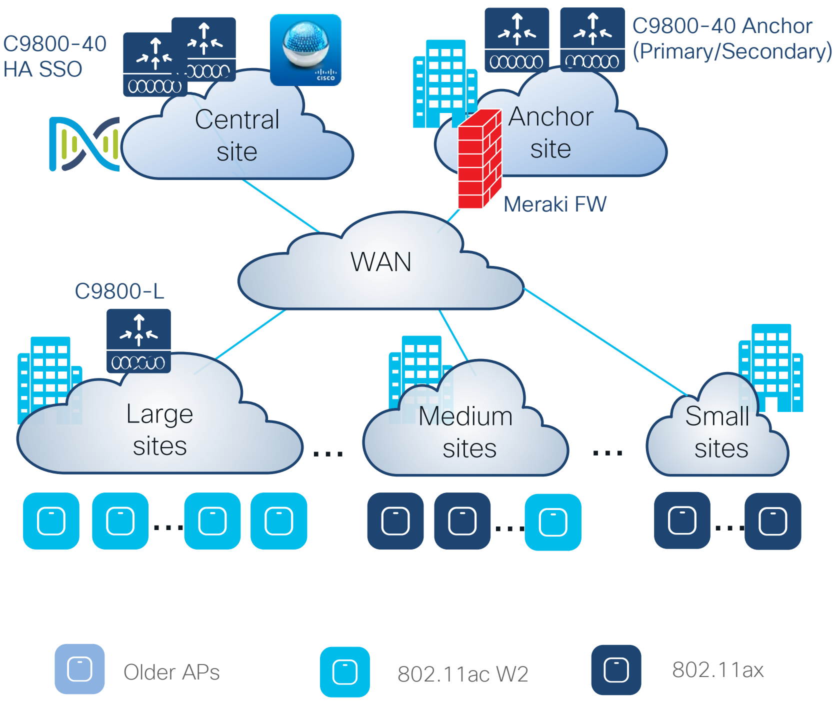
Customer Migration scenario



Customer requirements:

- Migrate to the new Catalyst wireless stack with C9800 wireless controllers and Catalyst APs
- Introduce C9800-L in larger sites and 9800-40 for Central and Anchor sites
- Catalyst 9120 as the reference AP with 9130 introduced in some critical areas where tri-radio is needed
- Introduce DNA Center for assurance with AP1800s sensors at critical sites

Customer Migration scenario



Migration considerations:

- 5508 does not support Catalyst APs so C9800 controllers have been introduced from the start
- Migration started with code 17.2 and then customer went in production with 17.3.2a
- Initially older APs replaced with Wi-Fi 6 APs, Wi-Fi 5 were kept. The plan is to eventually migrate all the APs to Wi-Fi 6
- Is FlexConnect still the best design for smaller sites?

Build a Migration Strategy – three phases

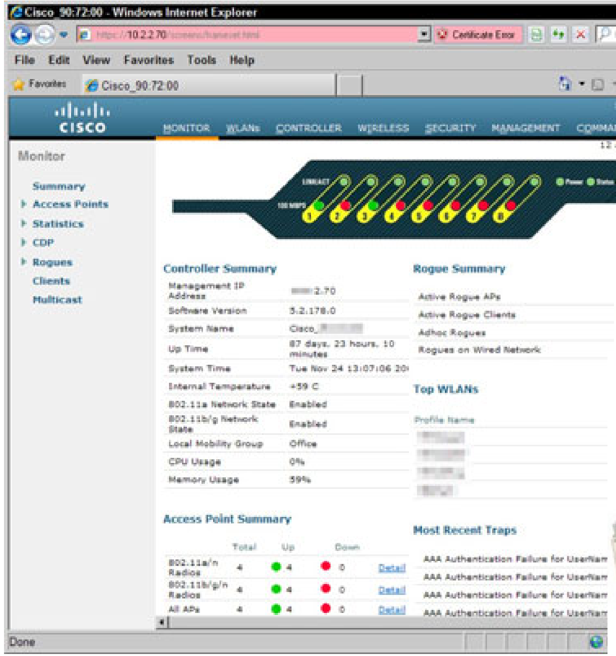
Evaluate

- Build the knowledge of ng stack
- Verify platform support
- Evaluate feature gaps
- Evaluate new licensing model
- Get all the required information (topology, device lists, design requirements, configuration)

Migration factors:

- End of Sales (EoS) announcement for all AireOS controllers
- EoS announcement of 802.11ac Wave1 APs (x700 series)
- 17.3 is the last train to support 802.11ac Wave 1 APs (x700 series)
- No support for 802.11n APs or older on C9800

Thank You, AireOS



Cisco_90:72:00 - Windows Internet Explorer

https://10.2.2.70/screens/frameset.html

Certificate Error

File Edit View Favorites Tools Help

Favorites | Cisco_90:72:00

Page ▾ Safety ▾ Tools ▾

Controller Summary

Management IP Address	[redacted]2.70
Software Version	5.2.178.0
System Name	Cisco_[redacted]
Up Time	87 days, 23 hours, 10 minutes
System Time	Tue Nov 24 13:07:06 20
Internal Temperature	+59 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	Office
CPU Usage	0%
Memory Usage	59%

Rogue Summary

Active Rogue APs

Active Rogue Clients

Adhoc Rogues

Rogues on Wired Network

Top WLANs

Profile Name
[redacted]
[redacted]
[redacted]
[redacted]

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	4	● 4	● 0	Detail
802.11b/g/n Radios	4	● 4	● 0	Detail
All APs	4	● 4	● 0	Detail

Most Recent Traps

AAA Authentication Failure for UserNam

AAA Authentication Failure for UserNam

AAA Authentication Failure for UserNam

AAA Authentication Failure for UserNam

Done

airespace™

The Standard for Wireless LANs

Cisco 4400 Series Wireless LAN Controller
Cisco 4400 Series Wireless LAN Controller
5520 Wireless Controller
Cisco 5500 Series Wireless Controller
Cisco 8500 Series Wireless Controller
CISCO

Build a Migration Strategy – three phases

Evaluate

- Build the knowledge of ng stack
- Verify platform support
- Evaluate feature gaps
- Evaluate new licensing model
- Get all the required information (topology, device lists, design requirements, configuration)

Design

- Architecture and Design review
- Configuration Migration
- Feature gap verification
- Identify pilot migration areas
- Brownfield considerations
- Discuss caveats

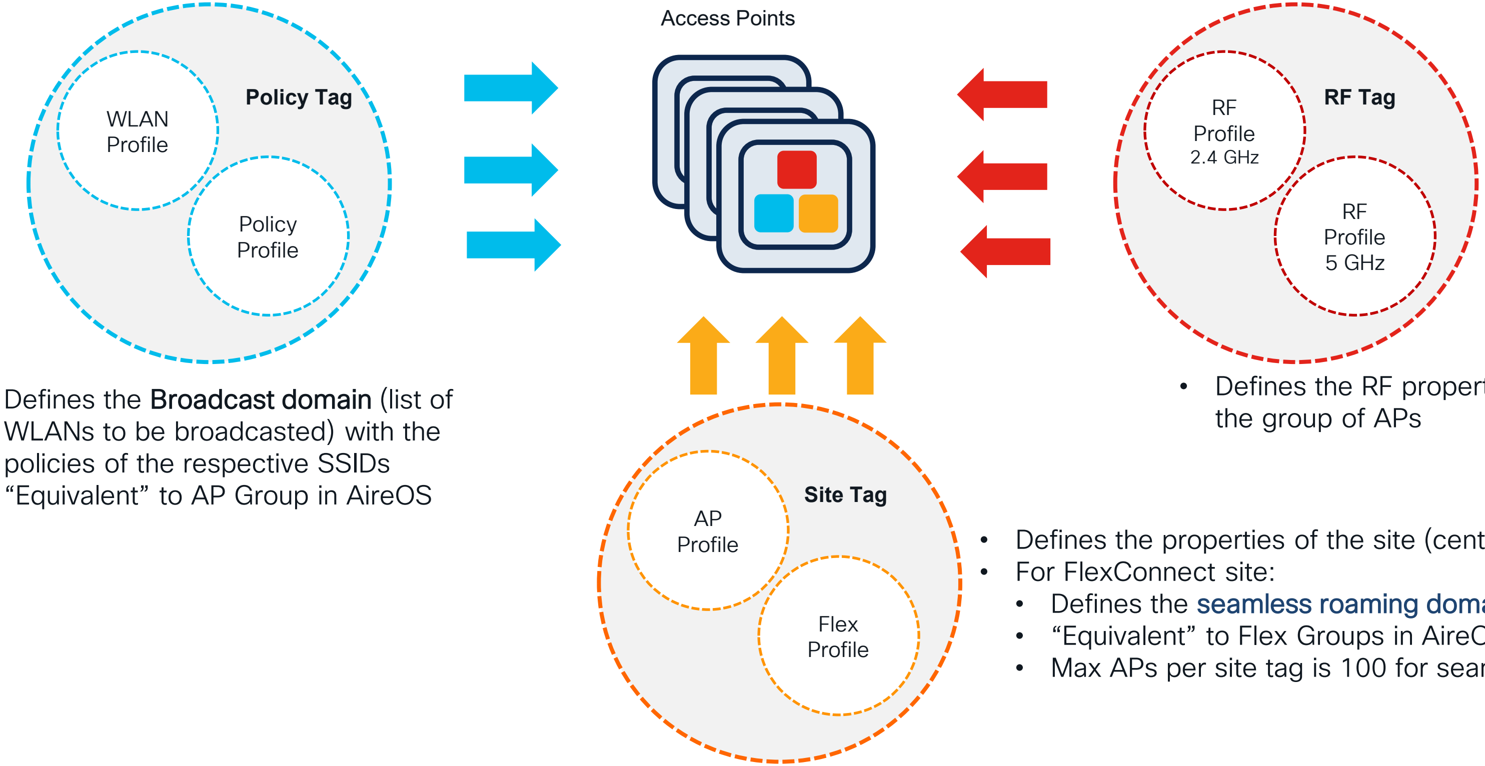
Implement

- Lab validation
- Check the Site Survey
- Deploy a pilot area in production
- Start replacing legacy APs
- Monitor stability and proceed

Migration Best Practices

Migration Best Practices

Knowing configuration model (Profiles & Tags) is a prerequisite to Migration



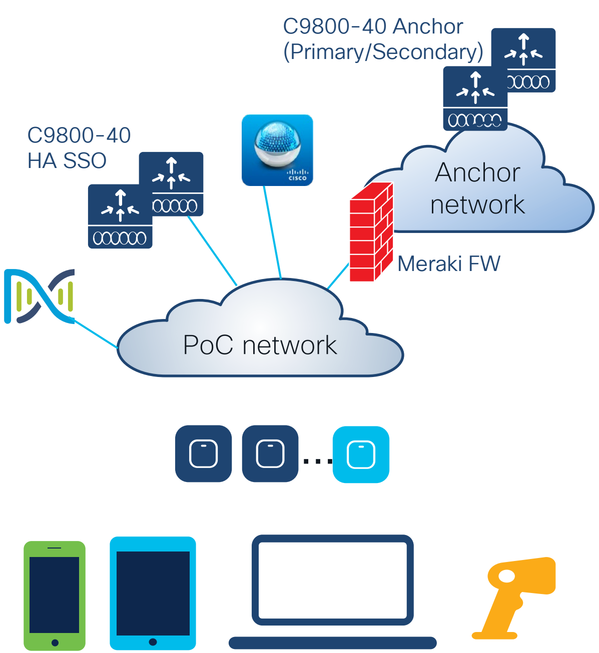
- Defines the **Broadcast domain** (list of WLANs to be broadcasted) with the policies of the respective SSIDs
- “Equivalent” to AP Group in AireOS

- Defines the RF properties of the group of APs

- Defines the properties of the site (central or remote)
- For FlexConnect site:
  - Defines the seamless roaming domain
  - “Equivalent” to Flex Groups in AireOS
  - Max APs per site tag is 100 for seamless roaming

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, HA 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:

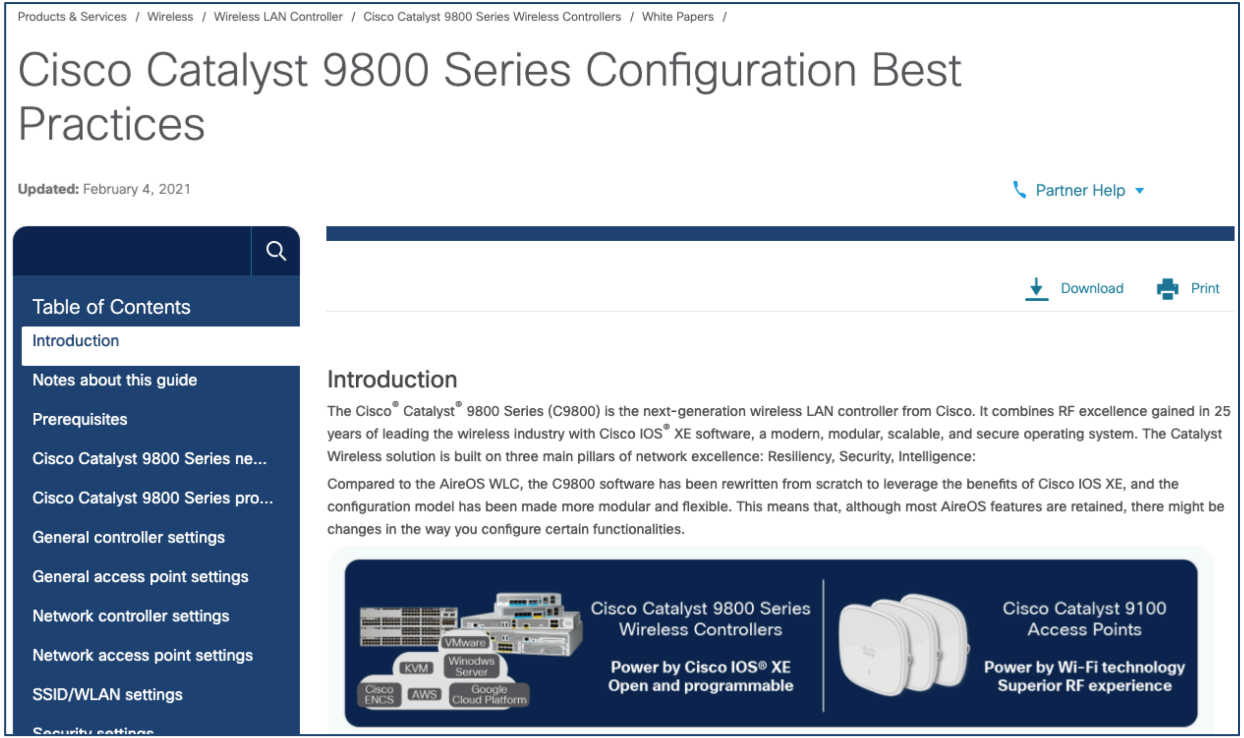
- Ideally test same clients as in production
- At least one Windows, one Android and one Apple client
- Test the different authentication types with same version of production AAA and web Portal if present
- Focus on particularly old devices and evaluate if some changes need to be done in the RF default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

Note: Arrange for Partner/Cisco to remotely access the PoC network to troubleshoot problems during the actual migration

Migration Best Practices

Refer to the latest Best Practice doc on CCO

Good place to start!



Products & Services / Wireless / Wireless LAN Controller / Cisco Catalyst 9800 Series Wireless Controllers / White Papers /

Cisco Catalyst 9800 Series Configuration Best Practices

Updated: February 4, 2021

Table of Contents

Introduction

The Cisco® Catalyst® 9800 Series (C9800) is the next-generation wireless LAN controller from Cisco. It combines RF excellence gained in 25 years of leading the wireless industry with Cisco IOS® XE software, a modern, modular, scalable, and secure operating system. The Catalyst Wireless solution is built on three main pillars of network excellence: Resiliency, Security, Intelligence:

Compared to the AireOS WLC, the C9800 software has been rewritten from scratch to leverage the benefits of Cisco IOS XE, and the configuration model has been made more modular and flexible. This means that, although most AireOS features are retained, there might be changes in the way you configure certain functionalities.

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

Configuration Migration

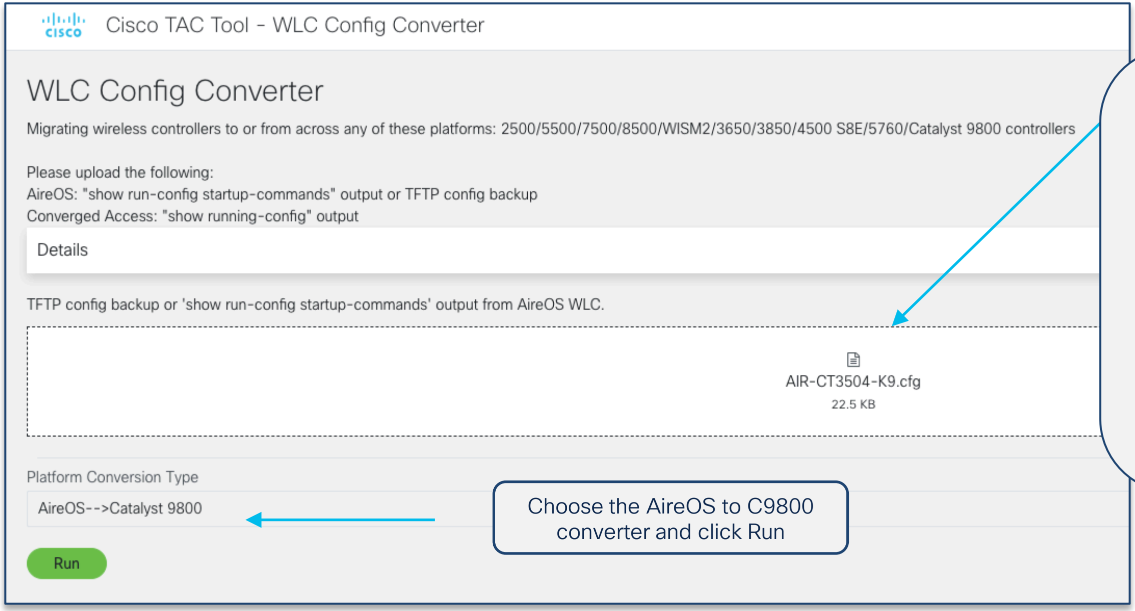
Configuration Migration tool

Need to address two key questions:

- Is this specific AireOS feature supported in Catalyst 9800
- How is this AireOS feature configured in Catalyst 9800

Configuration Migration Tool

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



WLC Config Converter

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

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

Details

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

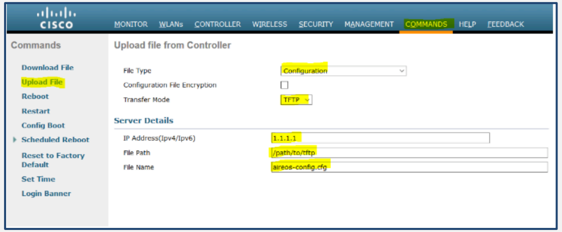
AIR-CT3504-K9.cfg
22.5 KB

Platform Conversion Type
AireOS-->Catalyst 9800

Choose the AireOS to C9800 converter and click Run

Drop the AireOS config file:

- Upload it from directly from GUI:



Upload file from Controller

File Type: Configuration
Configuration File Encryption: □
Transfer Mode: TFTP

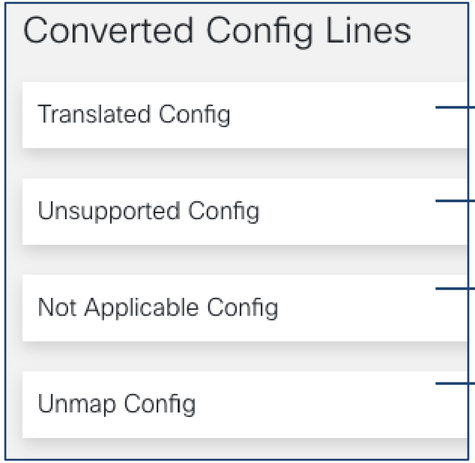
Server Details

IP Address(Ipv4/Ipv6): 1.1.1.1
File Path: /path/to/tftp
File Name: aireos-config.cfg

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

Configuration Migration Tool

Migration Tool output:



Converted Config Lines

Translated Config

Unsupported Config

Not Applicable Config

Unmap Config

Translated (CLI supported in IOS-XE)

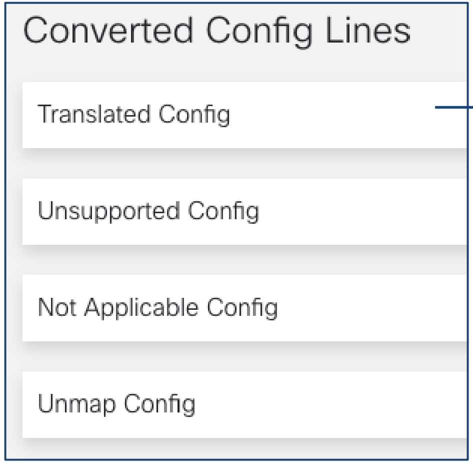
Unsupported (CLI not supported in IOS-XE)

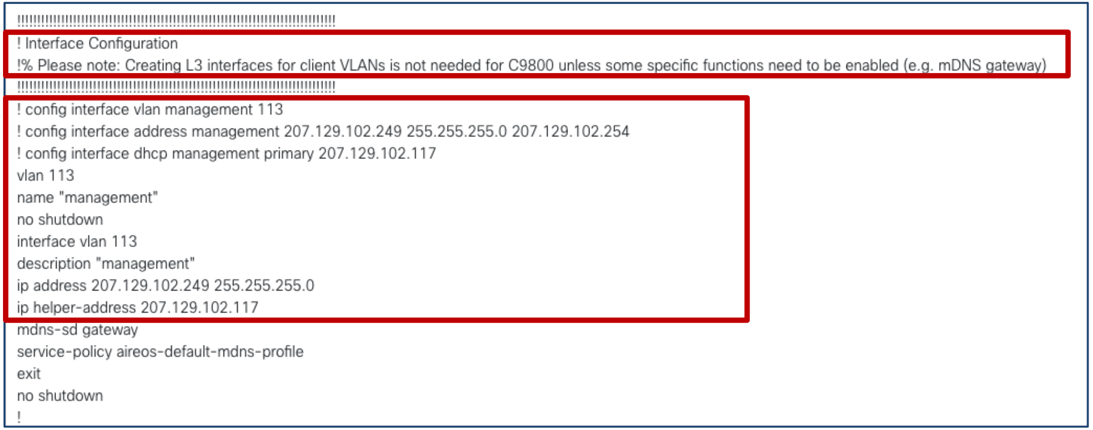
Not Applicable (CLI deprecated/not used commands)

Unmapped (CLI supported but not yet translated)

Configuration Migration Tool

Migration Tool output:



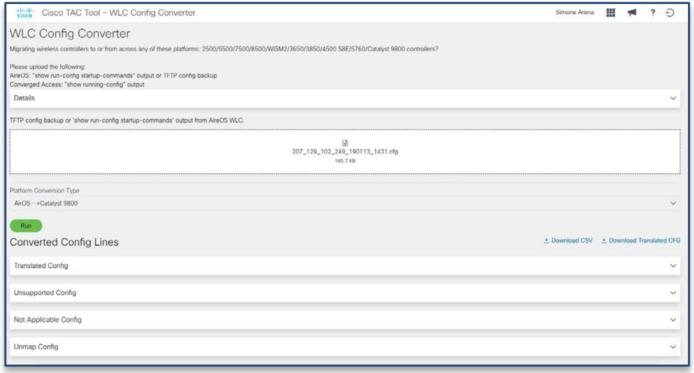


```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Interface Configuration
!% Please note: Creating L3 interfaces for client VLANs is not needed for C9800 unless some specific functions need to be enabled (e.g. mDNS gateway)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! config interface vlan management 113
! config interface address management 207.129.102.249 255.255.255.0 207.129.102.254
! config interface dhcp management primary 207.129.102.117
vlan 113
name "management"
no shutdown
interface vlan 113
description "management"
ip address 207.129.102.249 255.255.255.0
ip helper-address 207.129.102.117
mdns-sd gateway
service-policy aireos-default-mdns-profile
exit
no shutdown
!
```

- AireOS CLIs and the correspondent translated IOS-XE commands
- Added useful warnings for L3 interfaces, ACLs, hostname, parameter maps, etc > look for "!%" symbol
- Added clear indication on when user input is required : "!$" symbol

Configuration Migration – Steps

Step 1 – Upload AireOS in CX tool



WLC Config Converter

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

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

Details

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

207_129_102_249_190113_1431.cfg
185.7 KB

Platform Conversion Type: AirOS-->Catalyst 9800

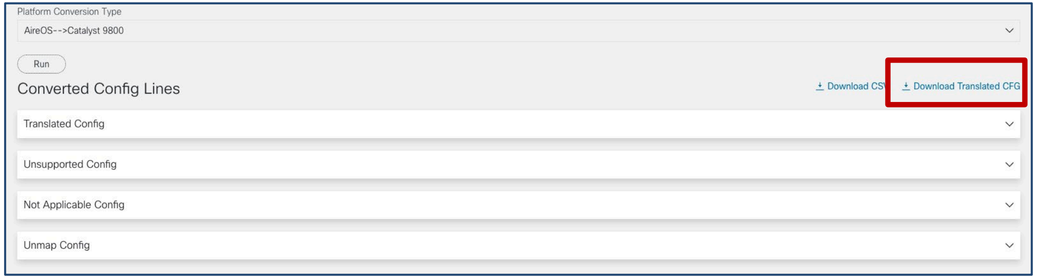
Converted Config Lines

- Translated Config
- Unsupported Config
- Not Applicable Config
- Unmap Config

- **Preferred**: The online tool is always 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

C9800 Configuration Migration – Steps

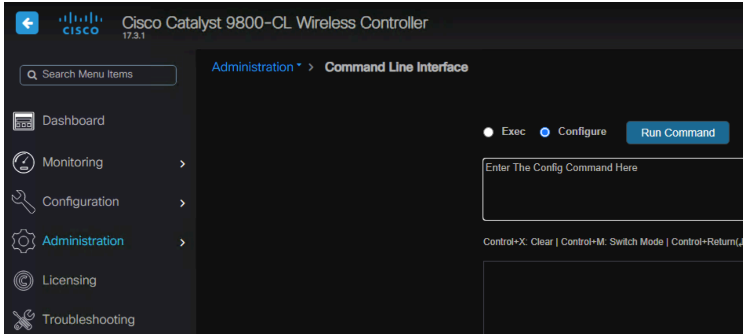
- Step 2 – Analyze the tool output and Download the “Translated config”



Platform Conversion Type: AireOS-->Catalyst 9800

- Step 3 – Edit the config file as needed. This file is NOT meant to be directly copied to the Catalyst 9800 config

- Step 4 – Copy the configuration to C9800’s running-config. Recommendation: use copy & paste to the CLI. Alternatively, you can use the CLI embedded tool in WebUI

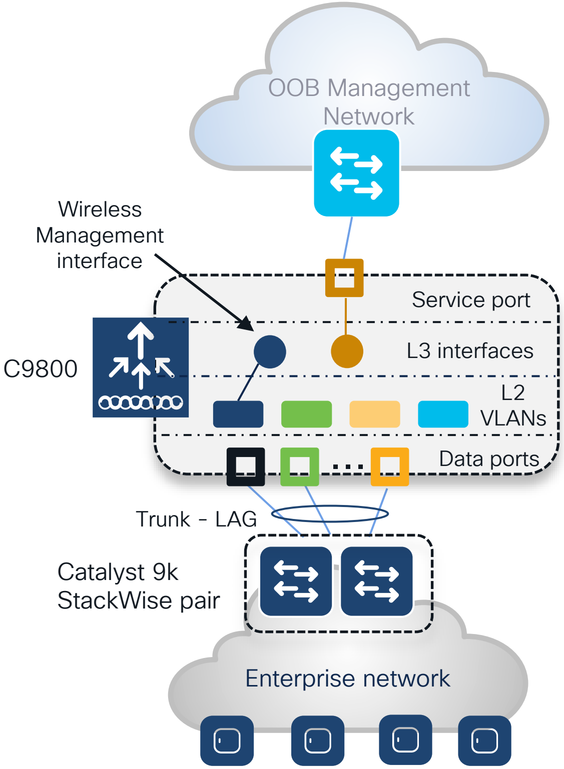


○ Exec ● Configure

Cisco Catalyst 9800-CL Wireless Controller
17.3.1
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Troubleshooting
Administration > Command Line Interface
Run Command
Enter The Config Command Here
Control+X: Clear | Control+M: Switch Mode | Control+Return(

Design with Tags in mind

Design: Port, vlan, SVI and network connectivity



Facts:

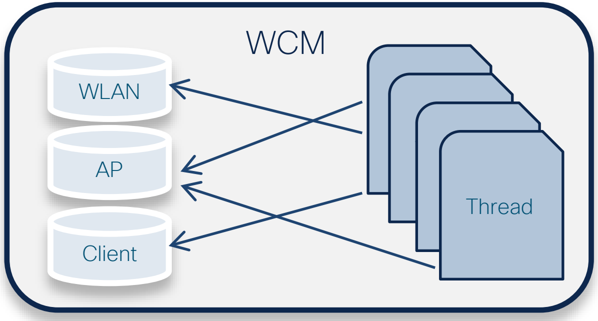
- It's mandatory to have a L3 interface configured as wireless management interface
- CAPWAP traffic is terminated to the wireless management interface. There is only one wireless management interface
- Service port on the appliance belongs to the Management VRF. On the C9800-CL this can be created as a L3 interface but no VRF supported
- For centrally switched traffic, is mandatory to configure a L2 VLAN mapped to the SSID; but the corresponding L3 interface (SVI) is optional, unless you need mDNS feature – this is different from AireOS where Dynamic interface is required.

Design best practices:

- Connect the uplink ports as per AireOS best practice: port-channel configured as trunk to a pair of switches in StackWise virtual domain or similar technologies.
- Switch Virtual Interface (SVI) for wireless management interface is recommended
- C9800-CL in public cloud must use a L3 port and hence has the following feature limitation: no support for sniffer mode AP and Hyperlocation

Cisco Catalyst 9800 – Next Gen Wireless Architecture

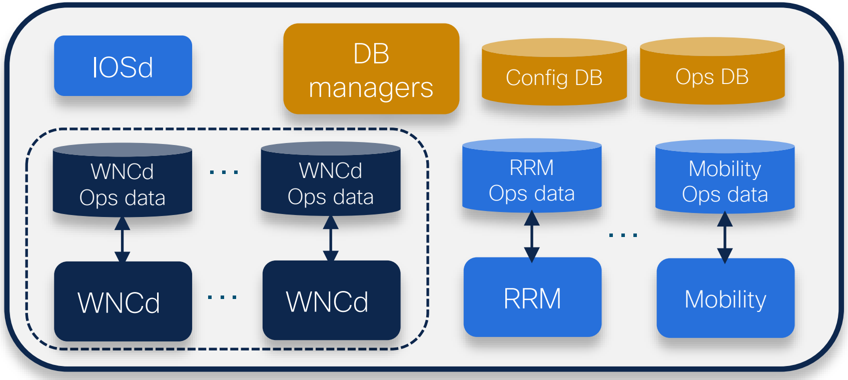
Previous software architecture vs. Catalyst Wireless Controller



High level view

Single process software architecture

- Wireless Controller Manager (WCM)
- 30+ threads
- Data contention cross threads
- Single memory space
- Single fault domain



High level view

Multi-process software architecture

- Processes are single threaded, non-blocking,
- New Wireless Network Controller process (WNCd).
- Multiple WNCd for horizontal scale
- No single fault domain (e.g., memory separation)
- Data model driven & data externalization
- Process patchability & restartability*
- Independent boot*

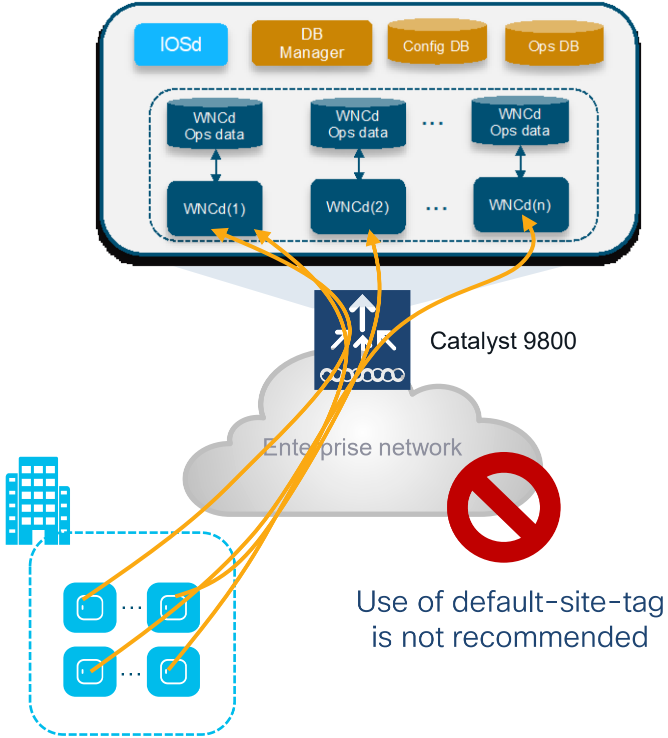
* System capable, roadmap item

How many WNCd in my C9800?

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

Wi-Fi architect should know the implications of having multiple WNCds

Site Tags – AP to WNCd distribution



Use of default-site-tag is not recommended

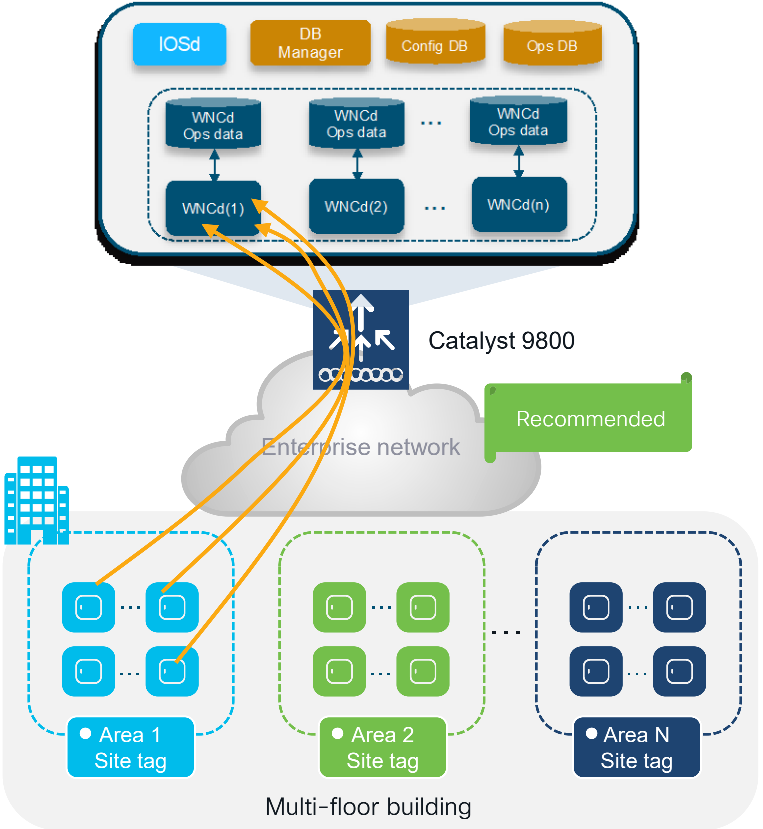
How AP distribution works:

- Load balancing applies to APs only (not directly to clients)
- Today AP distribution is based on Site Tag: APs with the same site-tag are managed by the same WNCd

Let's consider what happens if using the default-site-tag:

- As APs come online and register to the C9800, they are load balanced across WNCd instances in a **round robin** fashion
- Each neighbor AP will be assigned to a different WNCd > lot of inter-process roaming > not optimal design
- 11k/v and Coverage Hole detection (CHD) are managed within a WNCd process. These features **may break if neighbor APs are on different WNCd**
- Important: Full AP scale support and Fast Seamless Roaming (802.11r, CCKM, OKC) always works across site tags in Local mode (for FlexConnect is limited to one site tag)

Site Tags – AP to WNCd distribution



How load balancing works:

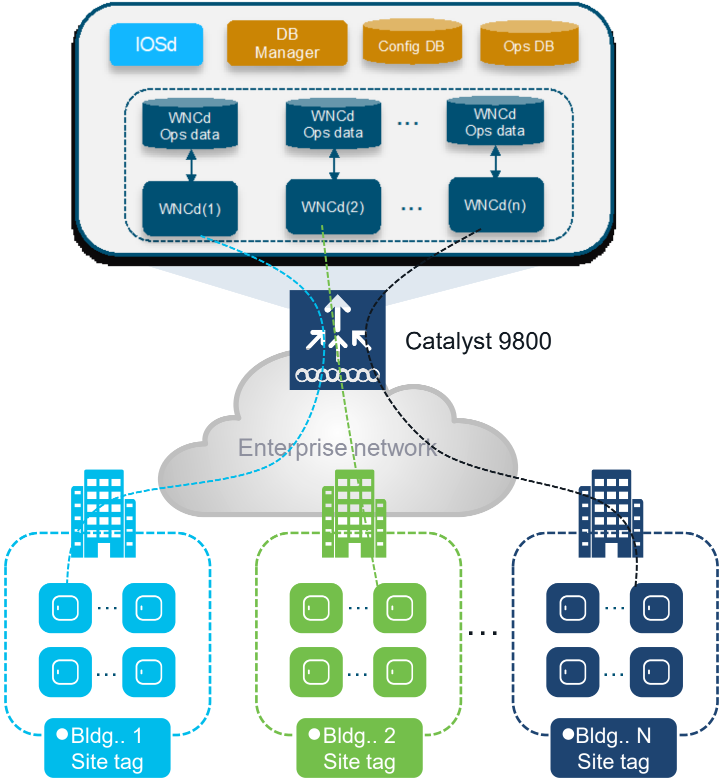
- For best performance, use custom site tag and group APs at a roaming domain level > Site Tag = Roaming Domain
- In this case, neighbor APs will end up joining the same WNCd process and hence optimizing performances
- To show how APs are load-balanced across WNCds:

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

- Syslog which informs the user of a WNCD overload:

```
"Process overload detected, handling %u Access
Points. Ensure that the number of Access Points in a
Site Tag is following recommendation.
```

Site Tags – Design for Campus (local mode)



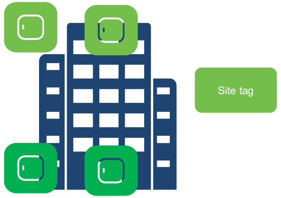
Recommendations:

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

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

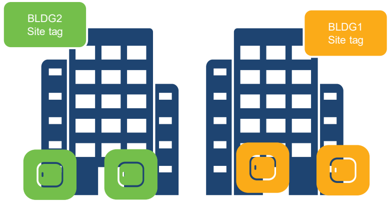
- Example of **Campus with multiple buildings:** if most of the roaming is within a building, a good design choice would be to choose **a site tag per building**

Site Tags – Design for Campus (local mode)



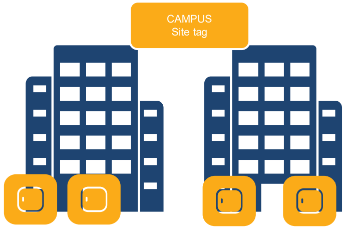
What if my customer has a building with 700 APs and 9800-40?

Recommendation: you can use one site tag, especially if voice (802.11k/v) is a requirement. Or you can split the building in two site tags for upper and lower floors



What if customer has a roaming domain that spans across multiple buildings with more than 1500 APs?

Recommendation: if 9800-40, configure a site tag per building. Roaming anyway works across site tags

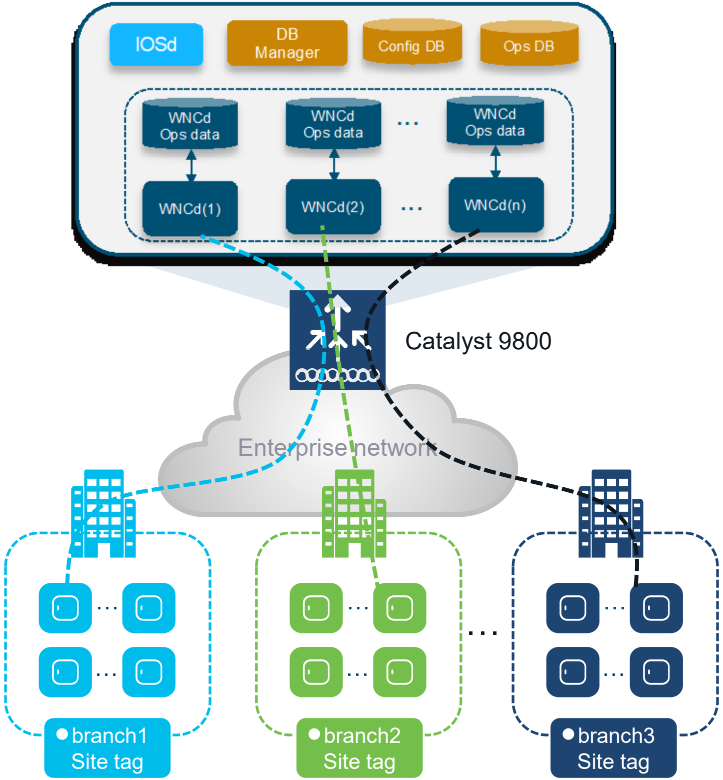


What if customer has multiple buildings with less than 500 APs?

Recommendation: configure just one name site tag and don't use the default site tag

Remember: Fast and seamless roaming is fully supported across site tags

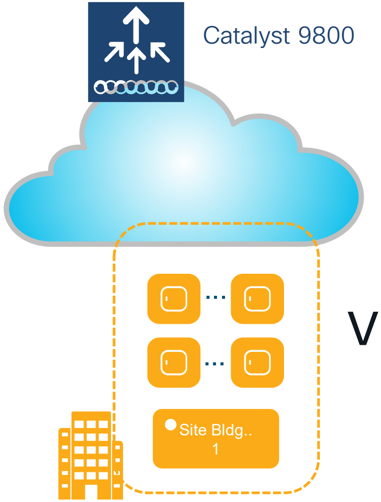
Site Tags – Design for Branch (Flex mode)



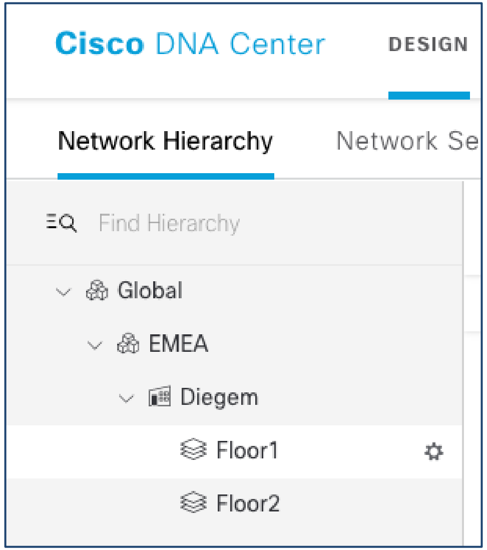
Recommendations:

- For FlexConnect, site tag is a seamless roaming domain
- You should configure at least one site-tag per Flex site
- Don't use the same site tag across multiple Flex sites (this includes the default-site-tag ☺)
- If support for Fast Seamless Roaming (802.11r, CCKM, OKC) is needed, then the max number of APs per site-tag for a Flex site is 100
- If the branch has more than 100 APs, define at least two site-tags and design APs to site-tag assignment so that each site-tag has less 100 APs

Site Tag vs. Site in Cisco DNA Center



vs.



- Site Tag (as any other AP tag) is a C9800 configuration model construct to apply settings to groups of AP
- Cisco DNA Center Site is a design construct that helps creating a network hierarchy to then apply Network Settings and show Assurance data
- Starting 2.1.x release, DNA Center uses named site tags and gives the option to configure custom site tags under the Network Profile
- For local mode APs, DNA Center will use by default a site tag per building. If the site has more than 500 APs, then multiple tags will be generated.
- DNA Center configures a custom site tag for a FlexConnect site with a limit of 100 APs per site tag

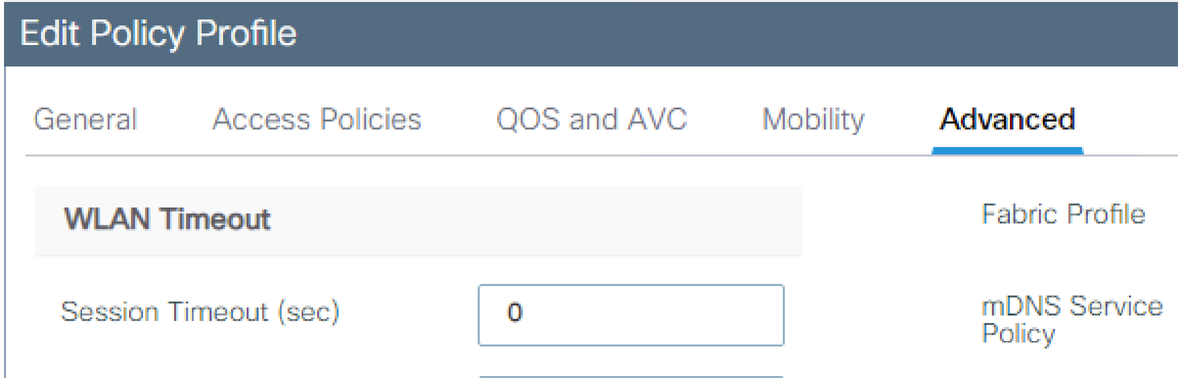
Lesson learnt

Configuration (Day 0, Day 1)

- Make sure box(es) are in install mode. This is the default boot mode and there are no reasons to change it
  - Advantages of install mode vs. bundle: support for High-availability features like ISSU, SMU/ Patching (Hot and Cold), faster boot time, less memory consumption, DNA-C support for upgrade
  - HA SSO pair: make sure both boxes are in the same boot mode
  - How to verify?

```
c9800-1#sh ver | i Installation
Installation mode is INSTALL
```

- Session timeout = 0; in C9800 this makes all client roaming a slow roam (full re-auth!!) – fixed in 17.4.1



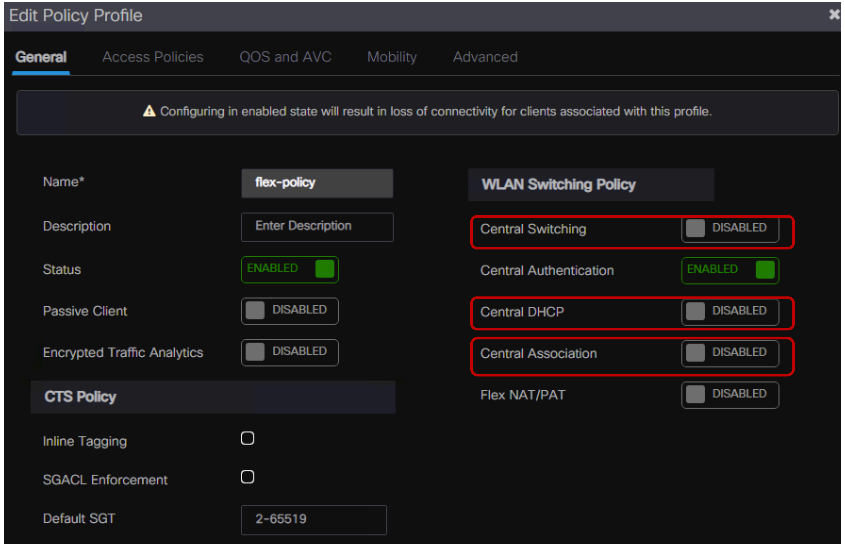
Edit Policy Profile

WLAN Timeout

Session Timeout (sec) 0

FlexConnect: 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**.



Edit Policy Profile

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*: flex-policy

Description: Enter Description

Status: ENABLED

Passive Client: DISABLED

Encrypted Traffic Analytics: DISABLED

CTS Policy

Inline Tagging: □

SGACL Enforcement: □

Default SGT: 2-65519

WLAN Switching Policy

Central Switching: DISABLED

Central Authentication: ENABLED

Central DHCP: DISABLED

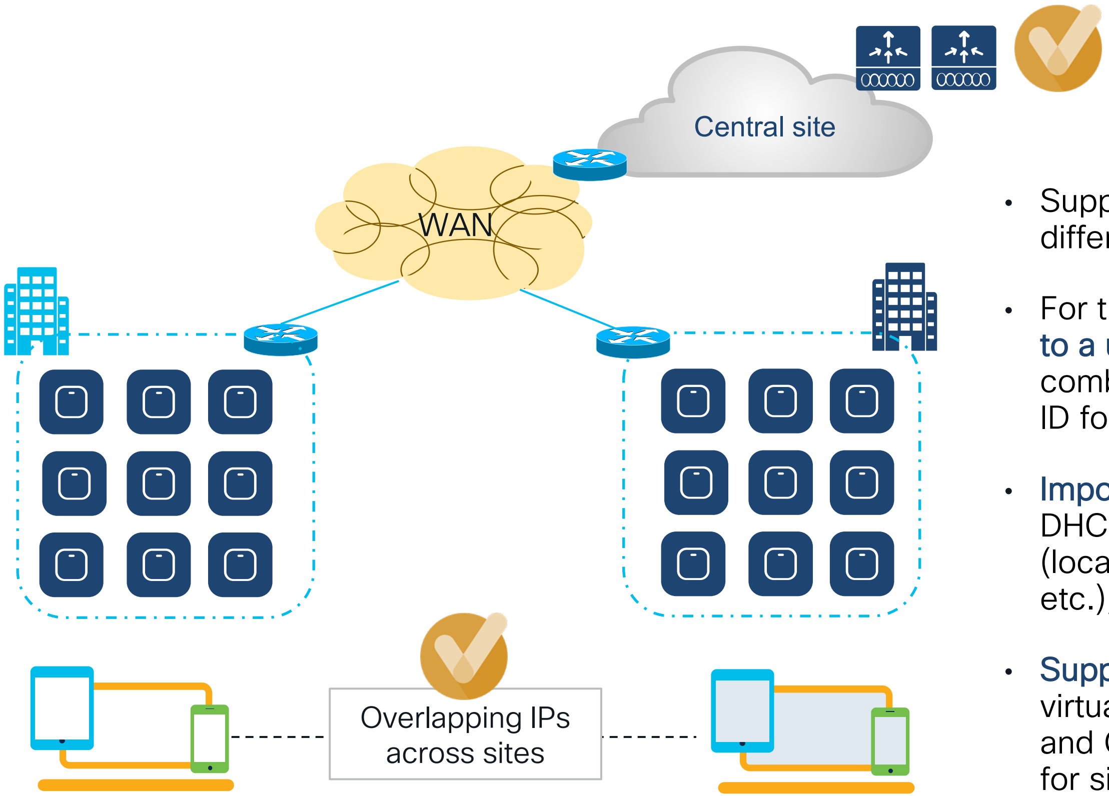
Central Association: DISABLED

Flex NAT/PAT: DISABLED

- If Flex **Local Switching** is configured, then DHCP traffic needs to be local as well. These settings should be automatically configured when toggling Central Switching to Disabled. Today it must be done manually. Fix is planned for upcoming release.

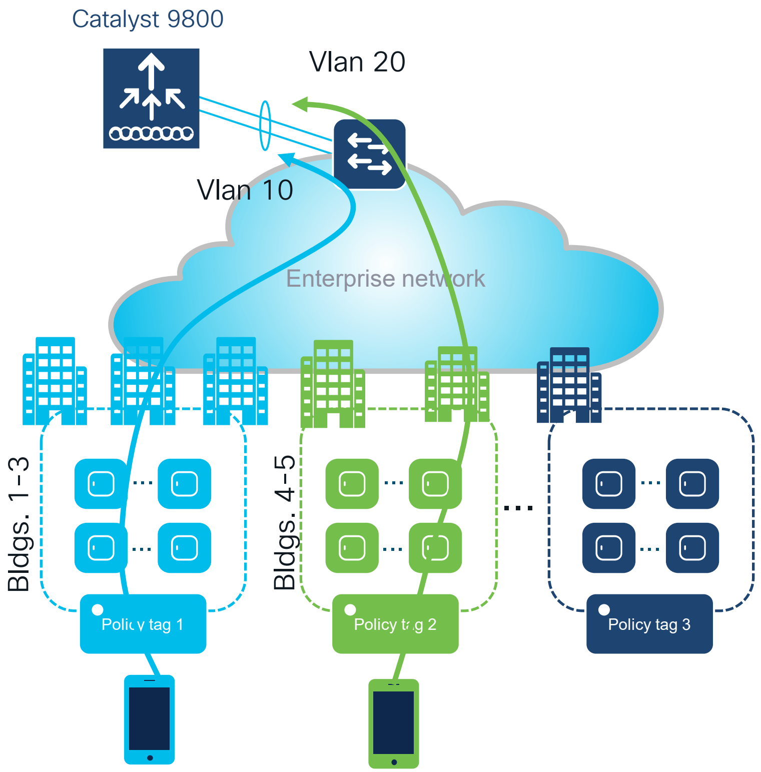
FlexConnect: Overlapping IP across sites

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.

Roaming across different Policy Profiles



- **General rule:** Policy profile defines the client policy associated to a SSID. Seamless roaming between the same SSID associated to different policy profiles is not allowed.

- Before 17.3, if two policy tags are created to associate a different policy profile to same SSID (e.g. different client VLAN), upon roaming, client will need to go through a reauth to re-evaluate the change in policy > client roaming is not seamless

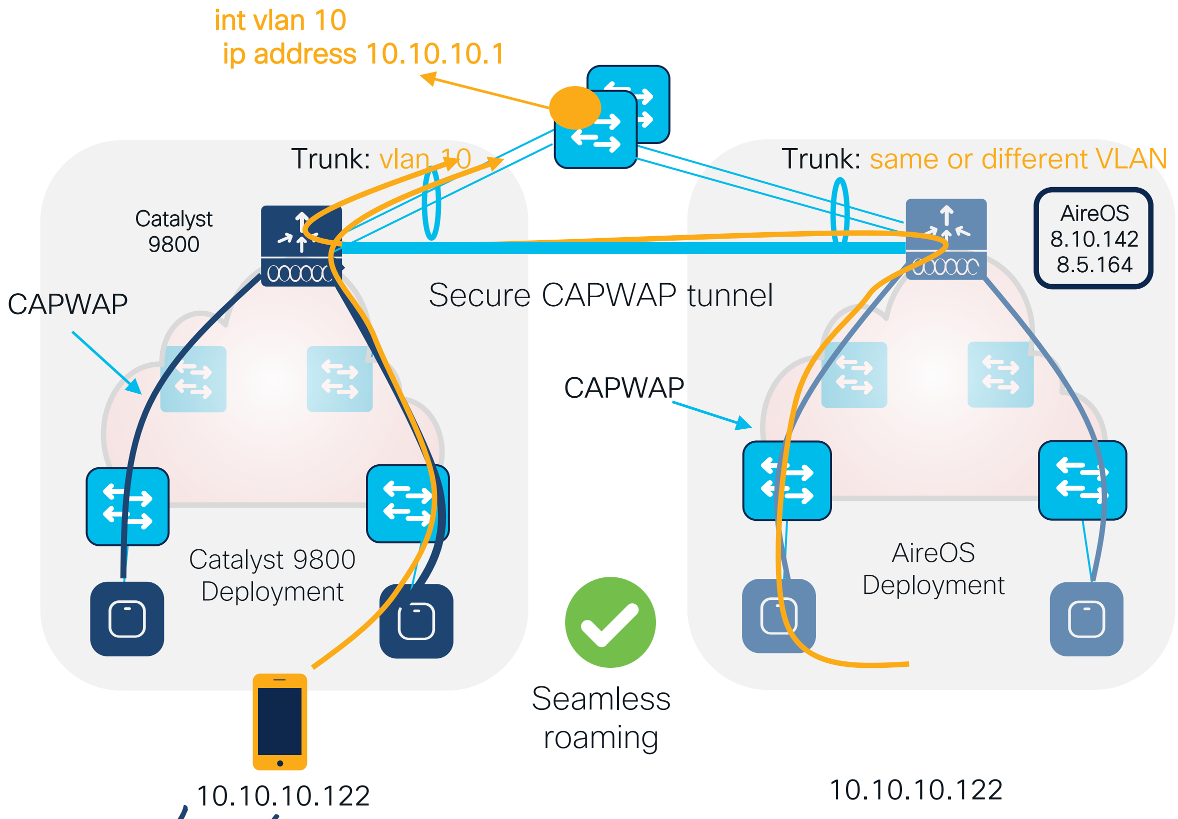
- **Starting from 17.3**, if the policy profiles differ only for certain parameters (VLAN and ACL being the most important), then **seamless roaming is allowed across policy profiles** (and related policy tags)

- To configure the feature, enter the following command in global config mode:

```
c9800(config)#wireless client vlan-persistant
```

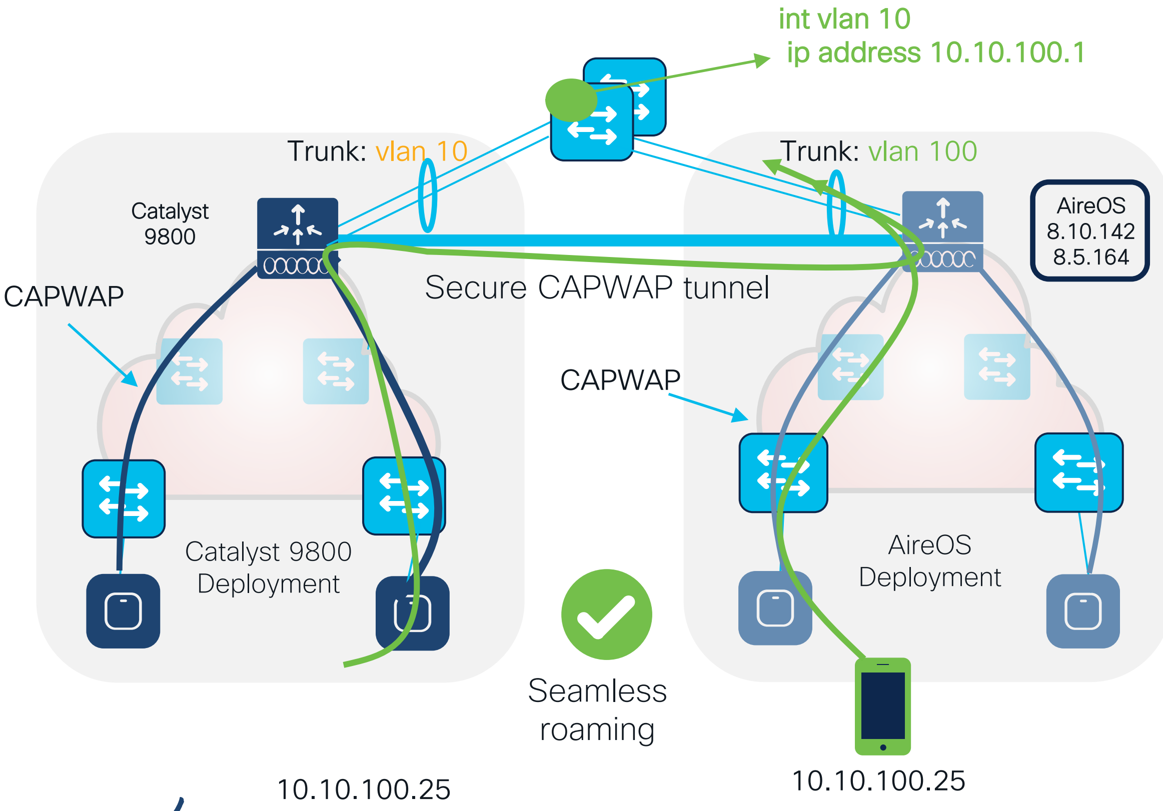
- For a complete list of attributes please go to: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b_wl_17_3_cg/m_client_roaming_policy_profile.html

AireOS / C9800 IRCM - Roaming



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

AireOS / C9800 IRCM - Recommendations



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 / C9800 IRCM - Recommended releases

All known caveats with “same VLAN” IRCM deployment are resolved, and fixes are available. Recommended CCO releases:

- IOS-XE:16.2.5, 17.3.3
- AireOS: 8.5.171 IRCM and 8.10.142

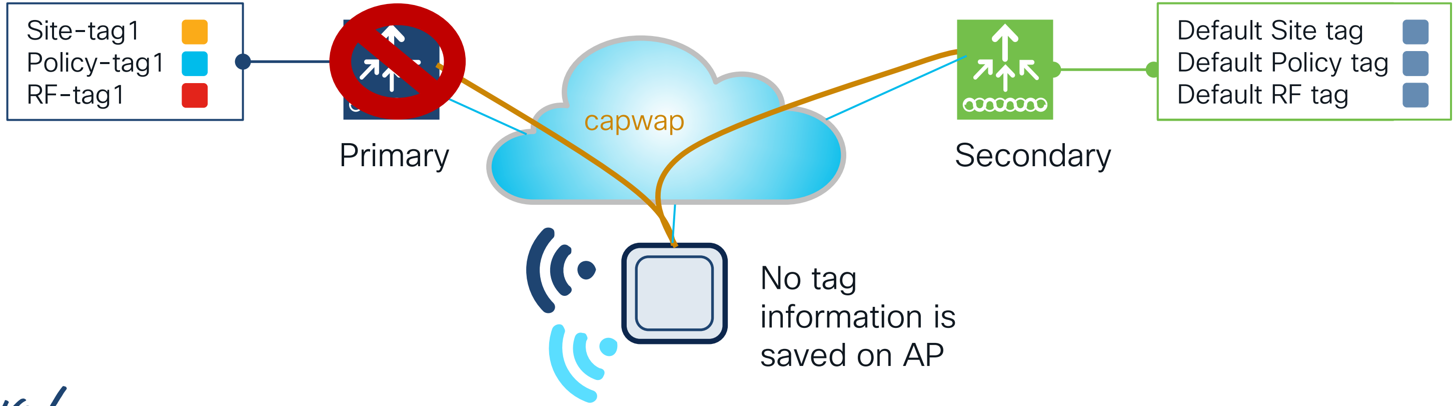
Please check following links for TAC recommended releases and/or wireless release compatibility matrix to have latest recommended versions:

- http://cs.co/compatibilitymatrix
- http://cs.co/recommendediosxe

Moving APs between C9800 controllers

Customer Scenario:

- Customer correctly configured Primary and Secondary with same profiles and tags.
- APs join the Primary and are assigned to the right tags (statically/filter/etc.). AP <> tags mapping is configured on Primary and APs start broadcasting SSIDs
- Primary fails, APs move to Secondary, but since there is no AP <> tags mapping configured on Secondary, APs go to the default tags and no SSID is broadcasted



Site-tag1 🟧
Policy-tag1 🟦
RF-tag1 🟥

Primary

capwap

Secondary

Default Site tag 🟦
Default Policy tag 🟦
Default RF tag 🟦

No tag information is saved on AP

Moving APs between C9800 controllers

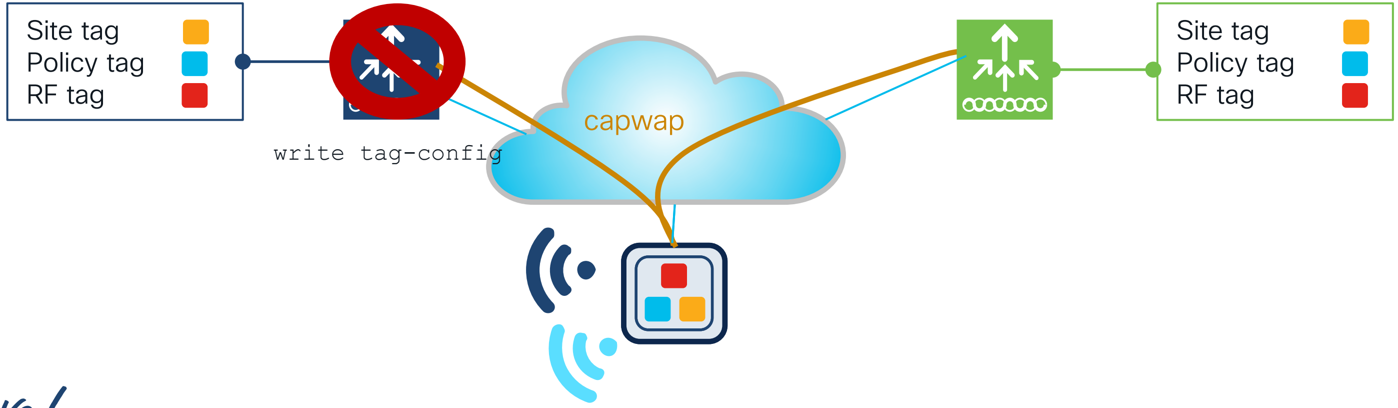
Solution #1

- When assigning APs to tags on Primary, push the tags information to the AP so that the AP can save and remember this information; today you need to use a “per AP” CLI command to do this:

```
c9800-1#ap name <APname> write tag-config
```

<<< exec mode

- When Primary fails and APs move to Secondary, the APs will present the tags and will be mapped correctly as the tags are already configured on the Secondary



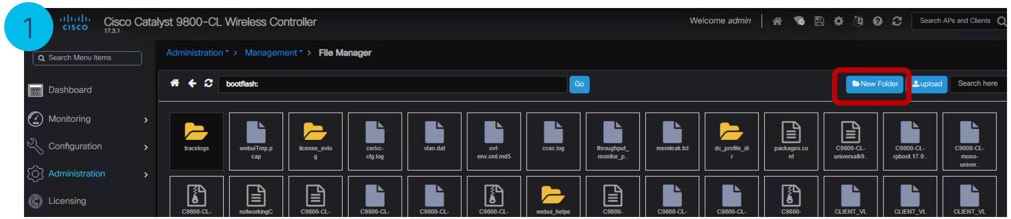
Moving APs between C9800 controllers

Small gift for you! a 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

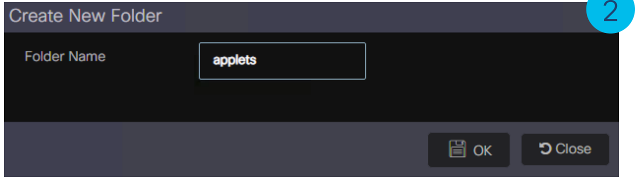
Administration > Management> File Manager: double click on bootflash.

1



Click on New Folder and create folder “applets”

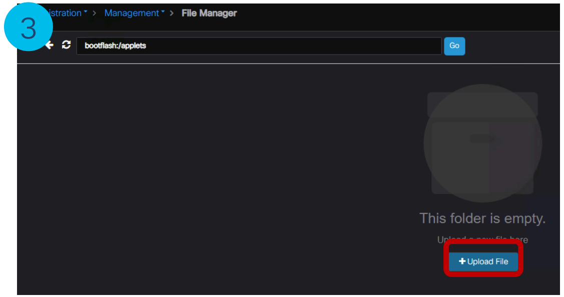
2



Folder Name: applets

Double click on new folder and Click on Upload file

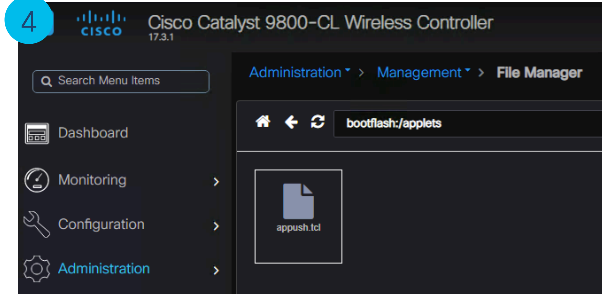
3



bootflash:/applets

Load the “appush.tcl” file

4


Cisco Catalyst 9800-CL Wireless Controller
17.3.1
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Administration > Management > File Manager
appush.tcl

bootflash:/applets

Moving APs between C9800 controllers

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

Primary controller

- Verify on the AP:

Before

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

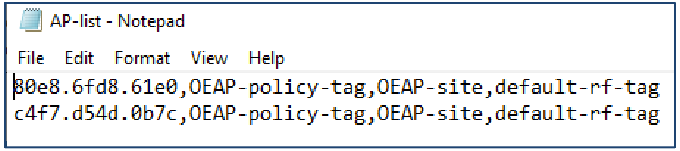
After

```
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
```

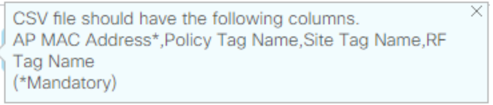
Moving APs between C9800 controllers

Solution #2

- Configure AP <> tag mapping statically on <u>Secondary</u> C9800 by loading a CSV file
- Create the CSV file first. It needs to be in a certain format (AP MAC is the Ethernet MAC):

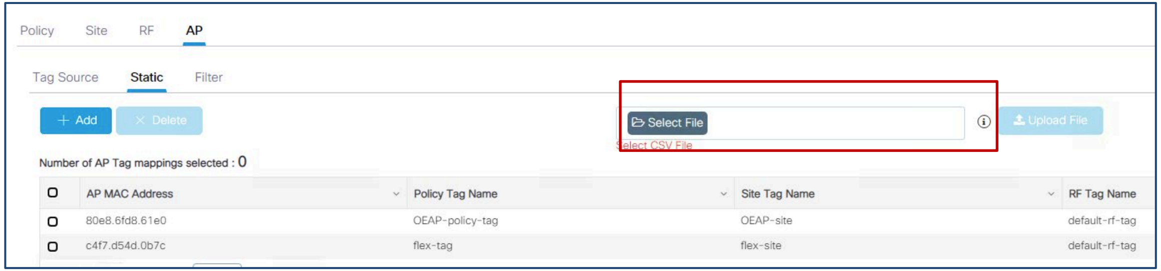


```
80e8.6fd8.61e0,OEAP-policy-tag,OEAP-site,default-rf-tag
c4f7.d54d.0b7c,OEAP-policy-tag,OEAP-site,default-rf-tag
```



CSV file should have the following columns.
AP MAC Address*,Policy Tag Name,Site Tag Name,RF Tag Name
(*Mandatory)

- Load the CSV file in Configuration>Tags & Profiles>Tags :



Number of AP Tag mappings selected : 0

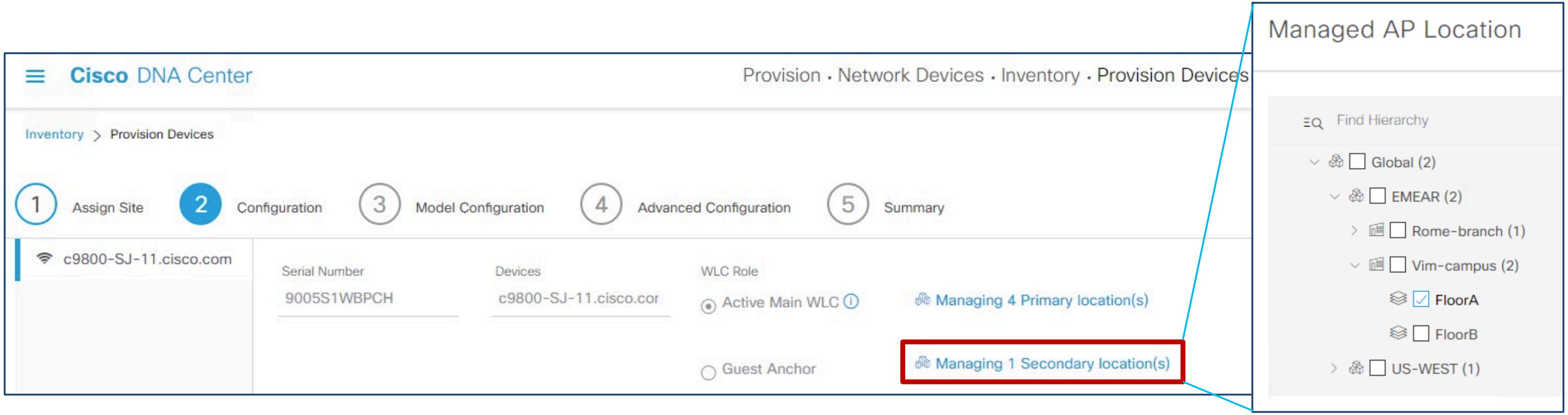
□	AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name
□	80e8.6fd8.61e0	OEAP-policy-tag	OEAP-site	default-rf-tag
□	c4f7.d54d.0b7c	flex-tag	flex-site	default-rf-tag

- When the Primary fails, the Secondary has the mapping > APs will be assigned to the right tags

Moving APs between C9800 controllers

Solution #2 automated with DNA Center

- If using Cisco DNA Center to configure **N+1 deployment**, DNA-C will automatically take care of provisioning the WLC acting as Secondary with the needed AP tags and mapping from Primary
- During Provisioning, assign the desired controller (c9800-SJ in this example), with secondary location/s. This means that the APs in this location will be configured with c9800-SJ as Secondary



Cisco DNA Center

Provision · Network Devices · Inventory · Provision Devices

Inventory > Provision Devices

1 Assign Site — 2 Configuration — 3 Model Configuration — 4 Advanced Configuration — 5 Summary

c9800-SJ-11.cisco.com

Serial Number: 9005S1WBPCH

Devices: c9800-SJ-11.cisco.cor

WLC Role:
- ● Active Main WLC — Managing 4 Primary location(s)
- ○ Guest Anchor — Managing 1 Secondary location(s)

Managed AP Location

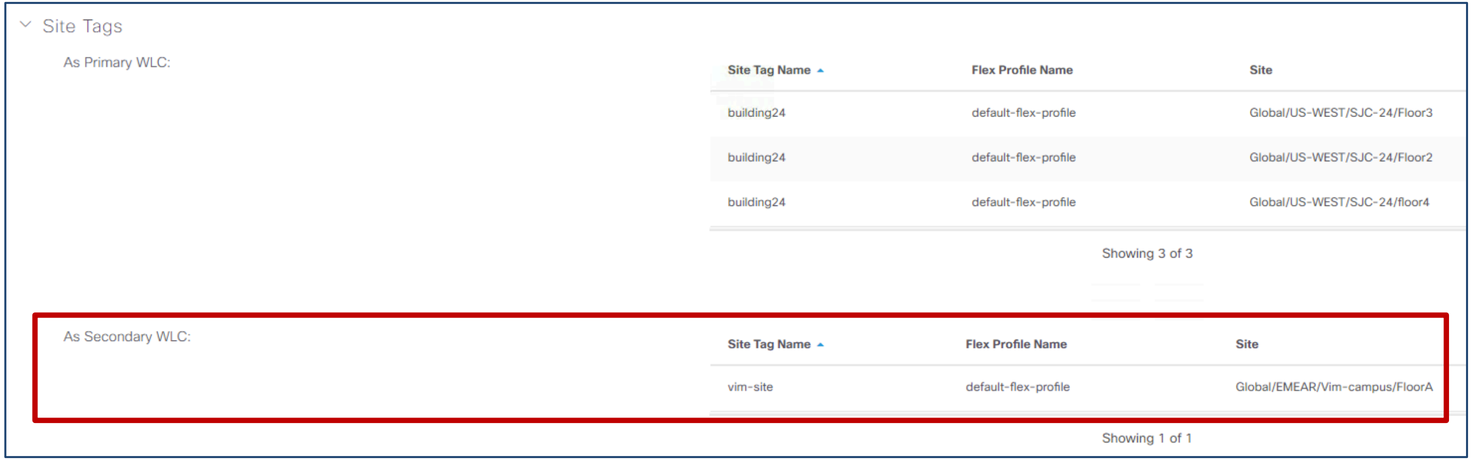
Find Hierarchy

- □ Global (2)
  - □ EMEAR (2)
    - □ Rome-branch (1)
    - □ Vim-campus (2)
      - ☑ FloorA
      - □ FloorB
  - □ US-WEST (1)

Moving APs between C9800 controllers

Solution #2 automated with DNA Center (continue)

- DNA Center will push the tags (and related AP mapping) from the primary WLC to this controller acting as Secondary upon Provisioning. This can be seen in the Summary of the configuration:



Site Tags

As Primary WLC:

Site Tag Name	Flex Profile Name	Site
building24	default-flex-profile	Global/US-WEST/SJC-24/Floor3
building24	default-flex-profile	Global/US-WEST/SJC-24/Floor2
building24	default-flex-profile	Global/US-WEST/SJC-24/floor4

Showing 3 of 3

As Secondary WLC:

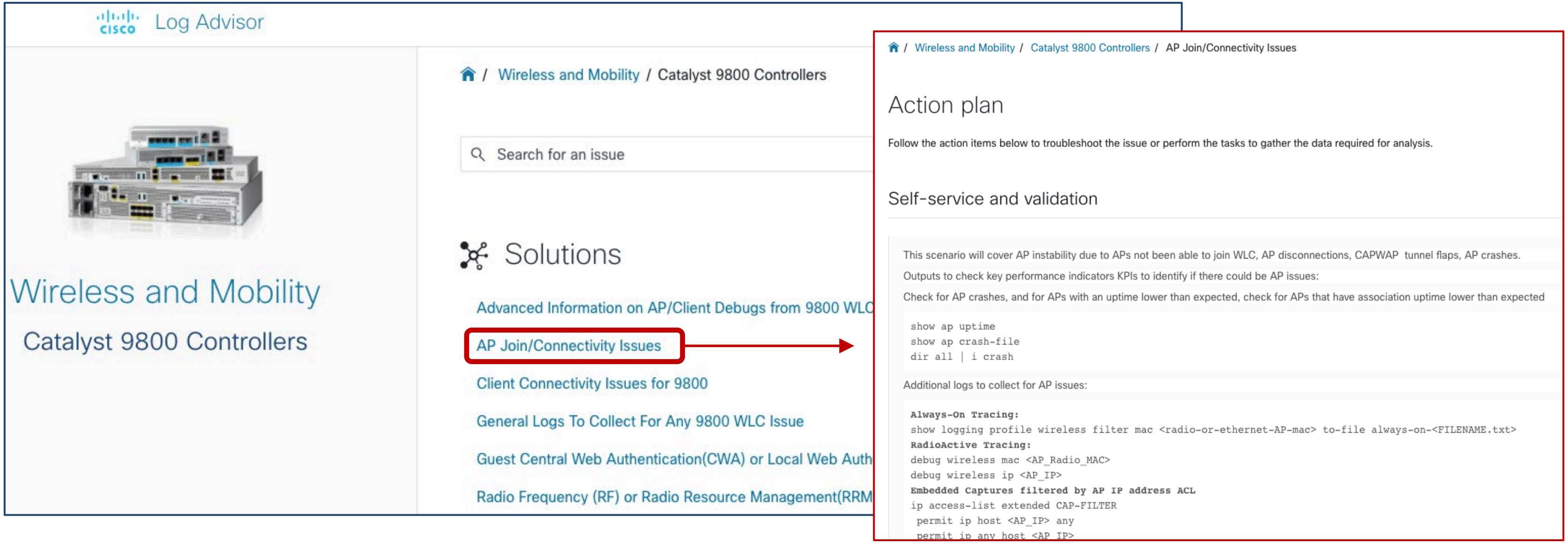
Site Tag Name	Flex Profile Name	Site
vim-site	default-flex-profile	Global/EMEAR/Vim-campus/FloorA

Showing 1 of 1

- When the Primary WLC (for floor A) fails, the Secondary WLC (c9800-SJC) already has the mapping > APs will be assigned to the right tags as they join

DAY2: new Troubleshooting tool

- New useful entry ☺ (besides using WebUI tools, DNA Center Assurance, etc.)
- Log Advisor for Catalyst 9800: https://logadvisor.cisco.com/logadvisor/wireless/9800/


Log Advisor
Wireless and Mobility
Catalyst 9800 Controllers
Wireless and Mobility / Catalyst 9800 Controllers
Search for an issue
Solutions
Advanced Information on AP/Client Debugs from 9800 WLC
AP Join/Connectivity Issues
Client Connectivity Issues for 9800
General Logs To Collect For Any 9800 WLC Issue
Guest Central Web Authentication(CWA) or Local Web Auth
Radio Frequency (RF) or Radio Resource Management(RRM
Wireless and Mobility / Catalyst 9800 Controllers / AP Join/Connectivity Issues

Action plan

Follow the action items below to troubleshoot the issue or perform the tasks to gather the data required for analysis.

Self-service and validation

This scenario will cover AP instability due to APs not been able to join WLC, AP disconnections, CAPWAP tunnel flaps, AP crashes.

Outputs to check key performance indicators KPIs to identify if there could be AP issues:

Check for AP crashes, and for APs with an uptime lower than expected, check for APs that have association uptime lower than expected

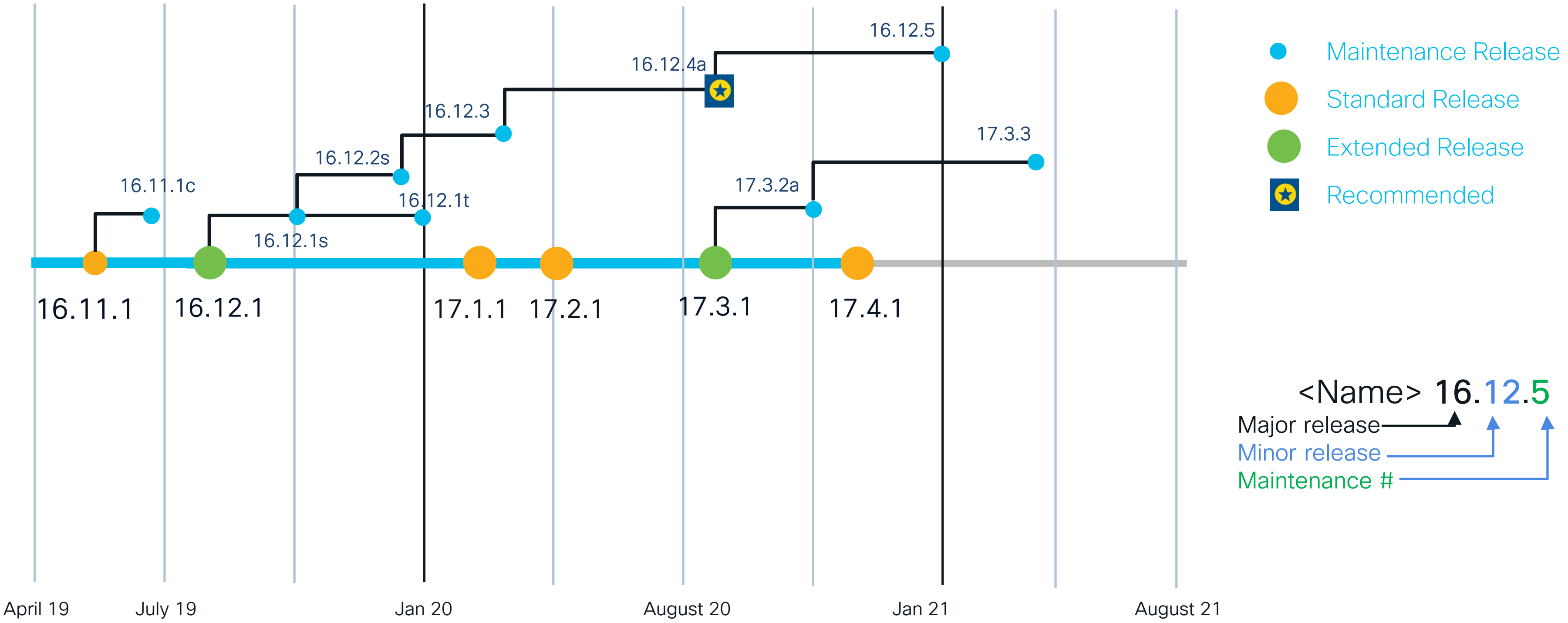
```
show ap uptime
show ap crash-file
dir all | i crash
```

Additional logs to collect for AP issues:

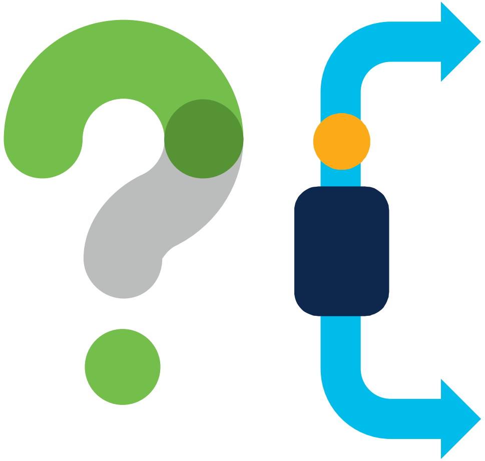
```
Always-On Tracing:
show logging profile wireless filter mac <radio-or-ethernet-AP-mac> to-file always-on-<FILENAME.txt>
RadioActive Tracing:
debug wireless mac <AP_Radio_MAC>
debug wireless ip <AP_IP>
Embedded Captures filtered by AP IP address ACL
ip access-list extended CAP-FILTER
 permit ip host <AP_IP> any
 permit ip any host <AP_IP>
```

Catalyst 9800 Recommended releases

IOS XE Release Schedule



What is the recommended release?



Go with 16.12.x train for:

- Most stable release. 16.12.4a is the “star” release
- Most deployed software in the field
- Hardened IRCM testing done with AireOS 8.5.164
- Customer is not interested in the latest features
- Prime support up to 3.7.1

Go with 17.3.x train for:

- AP hardware support for 9130E, 9105, IW3700, IW6300
- Last release to support 802.11ac W1 APs
- HyperV support for C9800-CL
- Latest features like: HA SSO parity, aWIPS, Wi-Fi6 features (BSS coloring, TWT), C9130 tri-radio support, etc.
- Deployment with Cisco DNA Center 2.1.2 and Prime 3.8.1
- Embedded 9800 in Catalyst switches (SDA)
- 17.3.3 is the recommended “go to release”

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

Cisco Recommended Software Matrix*

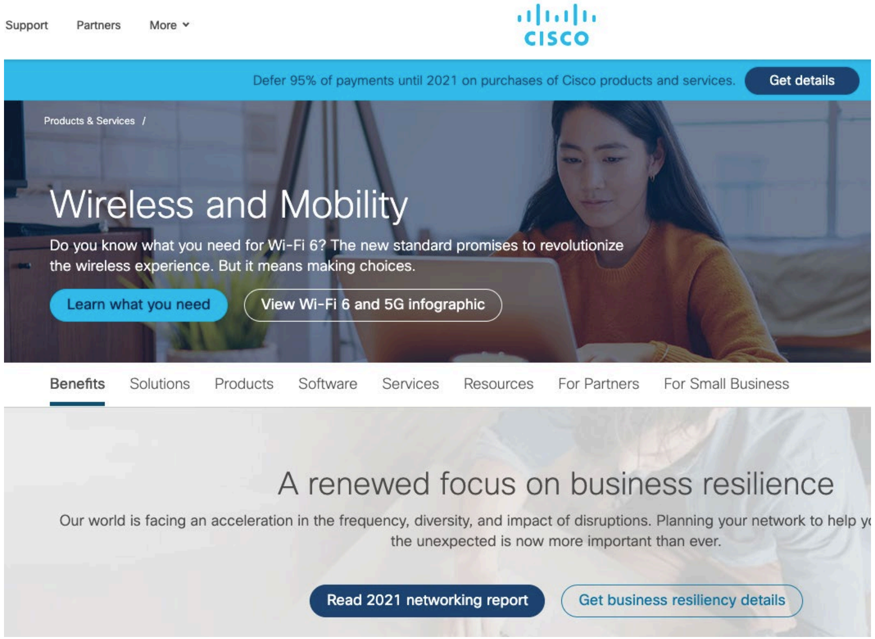
Reference

IOS-XE	AP	IRCM with Gen 1 AireOS	IRCM with Gen 2 AireOS	DNA-C	Prime	CMX	ISE
16.12.4a	802.11ax 802.11ac	8.5.164 (8.5.164.215 ESC for same vlan deployment)	8.10.142	1.3.3.7	3.7.1	10.6.3	2.6 P6 2.4
17.3.3	802.11ax 802.11ac	8.5.164 (8.5.164.215 ESC for same vlan deployment)	8.10.142	2.1.2.x	3.8.1	10.6.3	2.7 2.6 P6 2.4

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

Where can I find more info?

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



Defer 95% of payments until 2021 on purchases of Cisco products and services.

Wireless and Mobility

Do you know what you need for Wi-Fi 6? The new standard promises to revolutionize the wireless experience. But it means making choices.

A renewed focus on business resilience

Our world is facing an acceleration in the frequency, diversity, and impact of disruptions. Planning your network to help y the unexpected is now more important than ever.

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
- Campus CVD:
  https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html

JKU
JOHANNES KEPLER
UNIVERSITÄT LINZ

“For the size of our transition, from our older controllers and access points to the newer product, the migration process went very well, it was smooth. For a product this new and a deployment this large, it was all very quick.”

Stefan Kronawithleitner, Network Administrator – Johannes Kepler University

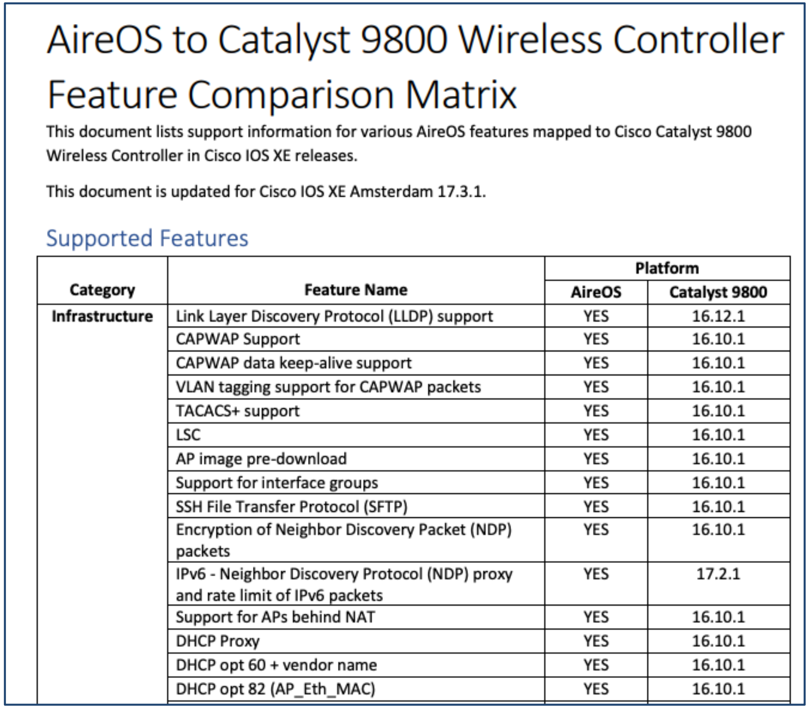
Thank you

cisco Live!

#CiscoLive

Additional material

AireOS feature parity



AireOS to Catalyst 9800 Wireless Controller Feature Comparison Matrix

This document lists support information for various AireOS features mapped to Cisco Catalyst 9800 Wireless Controller in Cisco IOS XE releases.

This document is updated for Cisco IOS XE Amsterdam 17.3.1.

Supported Features

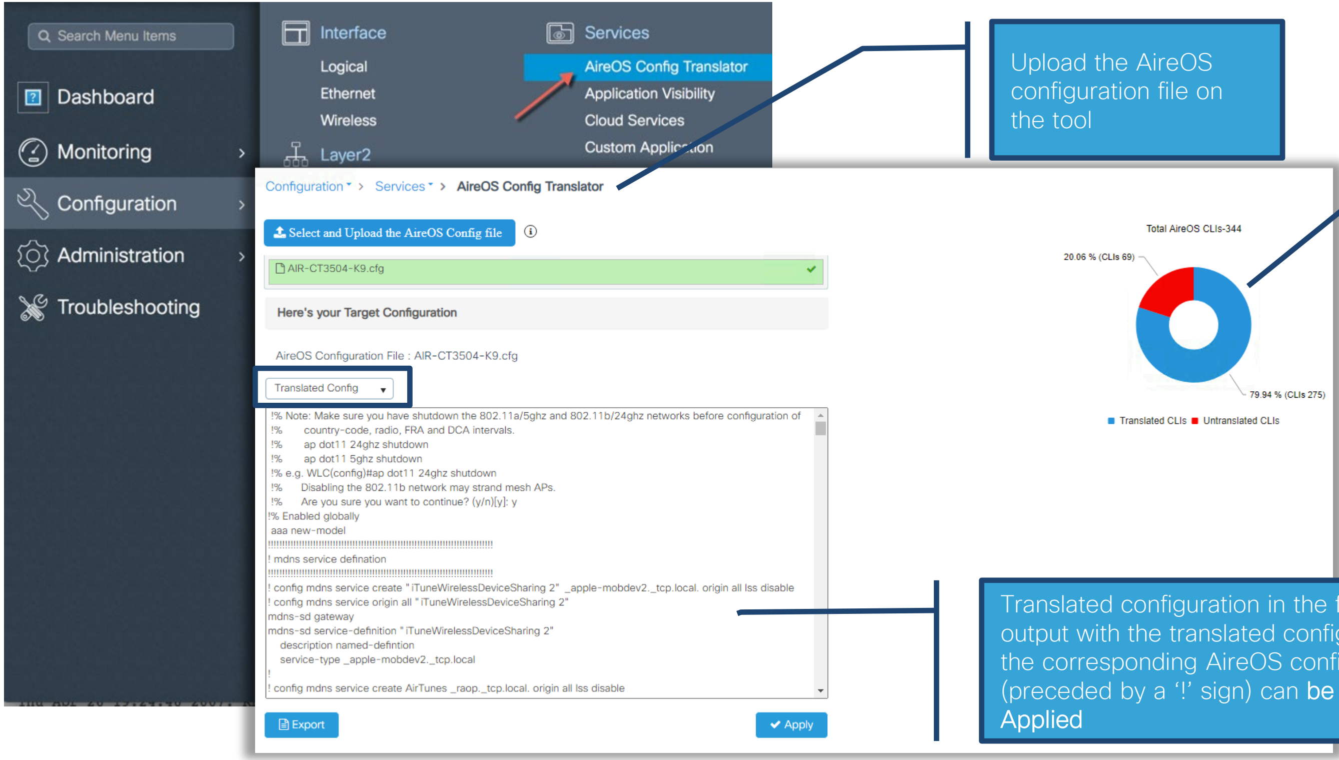
Category	Feature Name	Platform	
		AireOS	Catalyst 9800
Infrastructure	Link Layer Discovery Protocol (LLDP) support	YES	16.12.1
	CAPWAP Support	YES	16.10.1
	CAPWAP data keep-alive support	YES	16.10.1
	VLAN tagging support for CAPWAP packets	YES	16.10.1
	TACACS+ support	YES	16.10.1
	LSC	YES	16.10.1
	AP image pre-download	YES	16.10.1
	Support for interface groups	YES	16.10.1
	SSH File Transfer Protocol (SFTP)	YES	16.10.1
	Encryption of Neighbor Discovery Packet (NDP) packets	YES	16.10.1
	IPv6 - Neighbor Discovery Protocol (NDP) proxy and rate limit of IPv6 packets	YES	17.2.1
	Support for APs behind NAT	YES	16.10.1
	DHCP Proxy	YES	16.10.1
	DHCP opt 60 + vendor name	YES	16.10.1
	DHCP opt 82 (AP_Eth_MAC)	YES	16.10.1

- We are almost there…
- Check the parity list and verify with your Cisco representative
- The online Configuration Migration tool is your friend and is recommended

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/AireOS_Cat_9800_Feature_Comparison_Matrix.pdf

Configuration Migration Tool – GUI embedded

Reference



Here's your Target Configuration

AireOS Configuration File : AIR-CT3504-K9.cfg

```
!% Note: Make sure you have shutdown the 802.11a/5ghz and 802.11b/24ghz networks before configuration of
!%      country-code, radio, FRA and DCA intervals.
!%      ap dot11 24ghz shutdown
!%      ap dot11 5ghz shutdown
!% e.g. WLC(config)#ap dot11 24ghz shutdown
!%     Disabling the 802.11b network may strand mesh APs.
!%     Are you sure you want to continue? (y/n)[y]: y
!% Enabled globally
aaa new-model
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! mdns service defination
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! config mdns service create " iTuneWirelessDeviceSharing 2"  _apple-mobdev2._tcp.local. origin all lss disable
! config mdns service origin all " iTuneWirelessDeviceSharing 2"
mdns-sd gateway
mdns-sd service-definition " iTuneWirelessDeviceSharing 2"
   description named-defintion
   service-type _apple-mobdev2._tcp.local
!
! config mdns service create AirTunes _raop._tcp.local. origin all lss disable
```

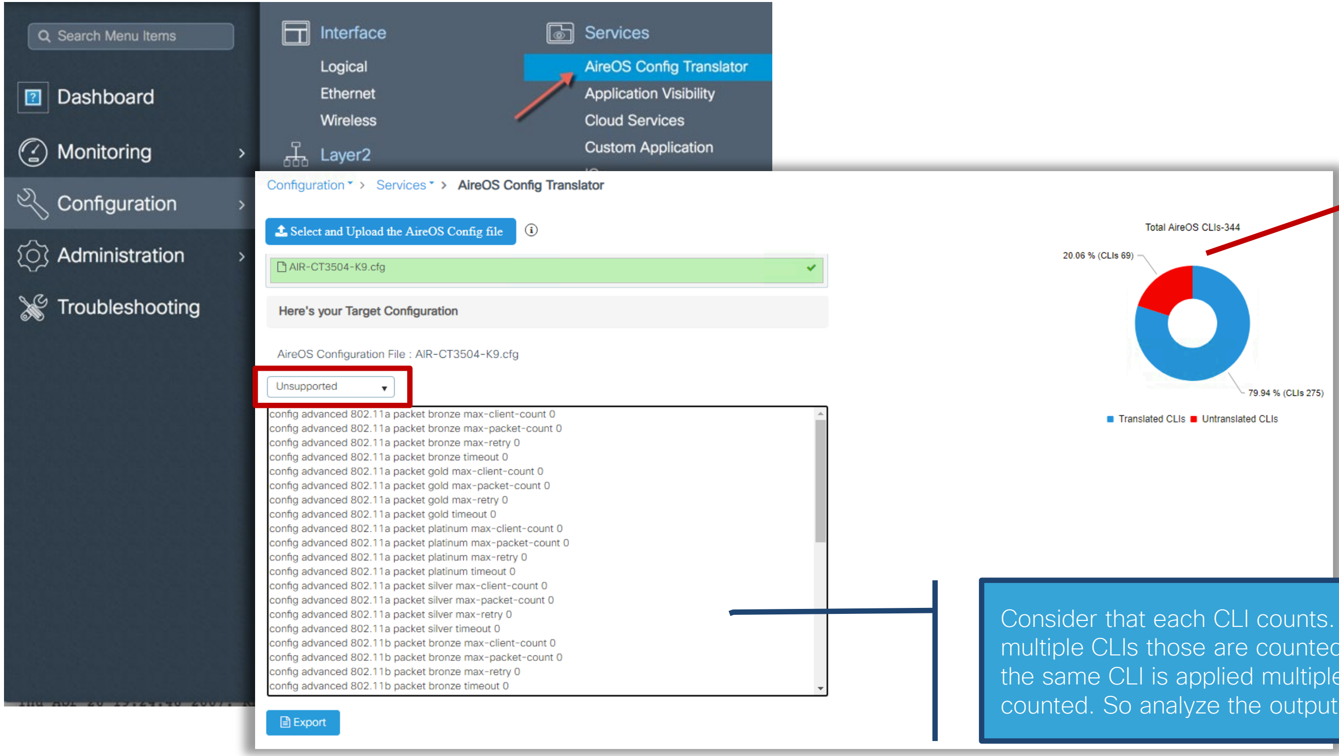
Upload the AireOS configuration file on the tool

The pie chart on the right shows the break-down of translated vs. untranslated configs

Translated configuration in the form of a CLI output with the translated configuration and the corresponding AireOS configuration (preceded by a '!' sign) can **be Exported or Applied**

Configuration Migration Tool – GUI embedded

Reference



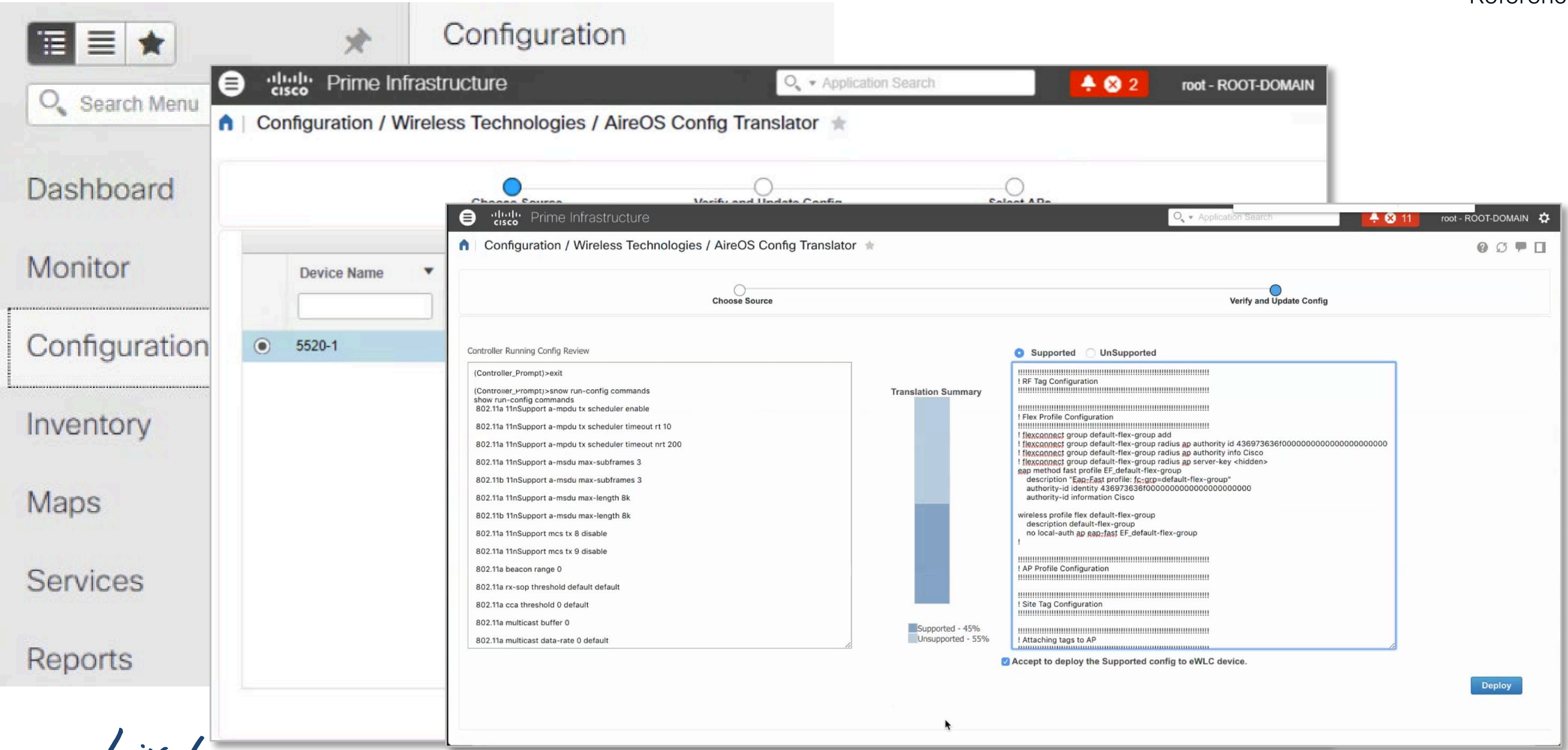
```
config advanced 802.11a packet bronze max-client-count 0
config advanced 802.11a packet bronze max-packet-count 0
config advanced 802.11a packet bronze max-retry 0
config advanced 802.11a packet bronze timeout 0
config advanced 802.11a packet gold max-client-count 0
config advanced 802.11a packet gold max-packet-count 0
config advanced 802.11a packet gold max-retry 0
config advanced 802.11a packet gold timeout 0
config advanced 802.11a packet platinum max-client-count 0
config advanced 802.11a packet platinum max-packet-count 0
config advanced 802.11a packet platinum max-retry 0
config advanced 802.11a packet platinum timeout 0
config advanced 802.11a packet silver max-client-count 0
config advanced 802.11a packet silver max-packet-count 0
config advanced 802.11a packet silver max-retry 0
config advanced 802.11a packet silver timeout 0
config advanced 802.11b packet bronze max-client-count 0
config advanced 802.11b packet bronze max-packet-count 0
config advanced 802.11b packet bronze max-retry 0
config advanced 802.11b packet bronze timeout 0
```

How come 20% is not supported???

Consider that each CLI counts. If a feature has multiple CLIs those are counted each time. If the same CLI is applied multiple times, it's again counted. So analyze the output carefully

Configuration Migration Tool – Prime

Reference



Configuration / Wireless Technologies / AireOS Config Translator

Device Name: ● 5520-1

Choose Source — Verify and Update Config

Controller Running Config Review

```
(Controller_Prompt)>exit

(Controller_Prompt)>snow run-config commands
show run-config commands
 802.11a 11nSupport a-mpdu tx scheduler enable

 802.11a 11nSupport a-mpdu tx scheduler timeout rt 10

 802.11a 11nSupport a-mpdu tx scheduler timeout nrt 200

 802.11a 11nSupport a-msdu max-subframes 3

 802.11b 11nSupport a-msdu max-subframes 3

 802.11a 11nSupport a-msdu max-length 8k

 802.11b 11nSupport a-msdu max-length 8k

 802.11a 11nSupport mcs tx 8 disable

 802.11a 11nSupport mcs tx 9 disable

 802.11a beacon range 0

 802.11a rx-sop threshold default default

 802.11a cca threshold 0 default

 802.11a multicast buffer 0

 802.11a multicast data-rate 0 default
```

Translation Summary

Supported - 45%
Unsupported - 55%

● Supported ○ UnSupported

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! RF Tag Configuration
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Flex Profile Configuration
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! flexconnect group default-flex-group add
! flexconnect group default-flex-group radius ap authority id 436973636f0000000000000000000000
! flexconnect group default-flex-group radius ap authority info Cisco
! flexconnect group default-flex-group radius ap server-key <hidden>
eap method fast profile EF_default-flex-group
   description "Eap-Fast profile: fc-grp=default-flex-group"
   authority-id identity 436973636f0000000000000000000000
   authority-id information Cisco

wireless profile flex default-flex-group
   description default-flex-group
   no local-auth ap eap-fast EF_default-flex-group
!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! AP Profile Configuration
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Site Tag Configuration
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Attaching tags to AP
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

☑ Accept to deploy the Supported config to eWLC device.

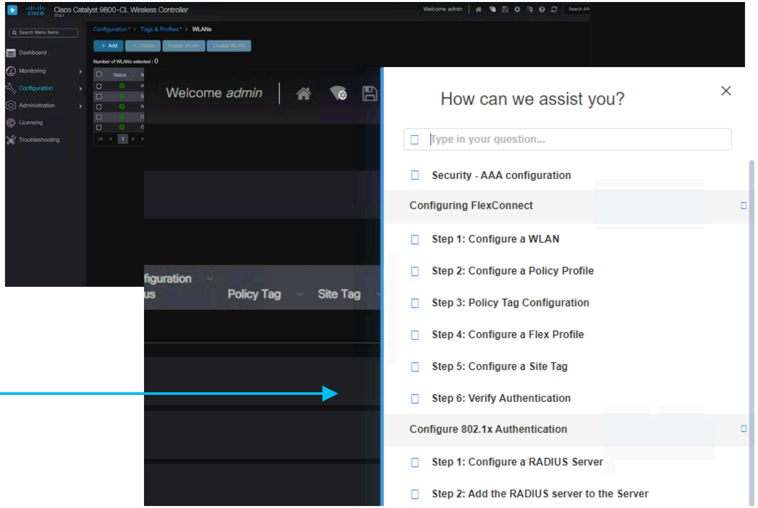
Reference

Config Guide Assistance on WebUI*

- Click the Guide Assistance on any page

- Search and select the desired topic

- Follow the steps by steps instructions



How can we assist you?

Type in your question...

Security - AAA configuration

Configuring FlexConnect

Step 1: Configure a WLAN

Step 2: Configure a Policy Profile

Step 3: Policy Tag Configuration

Step 4: Configure a Flex Profile

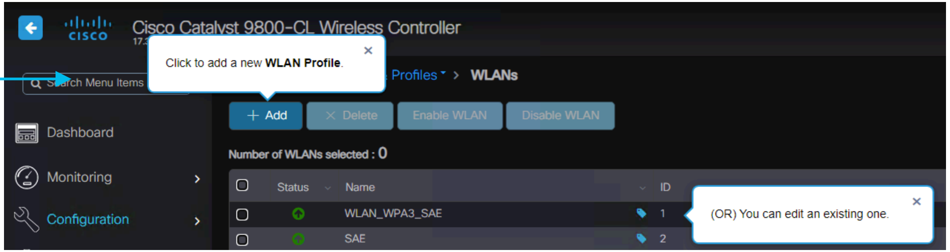
Step 5: Configure a Site Tag

Step 6: Verify Authentication

Configure 802.1x Authentication

Step 1: Configure a RADIUS Server

Step 2: Add the RADIUS server to the Server



Click to add a new WLAN Profile.

Number of WLANs selected : 0

Status	Name	ID
	WLAN_WPA3_SAE	1
	SAE	2

(OR) You can edit an existing one.

(*) Available in 16.12.4a and 17.3.1 and above

Primary/Secondary vs. Backup Primary/Secondary

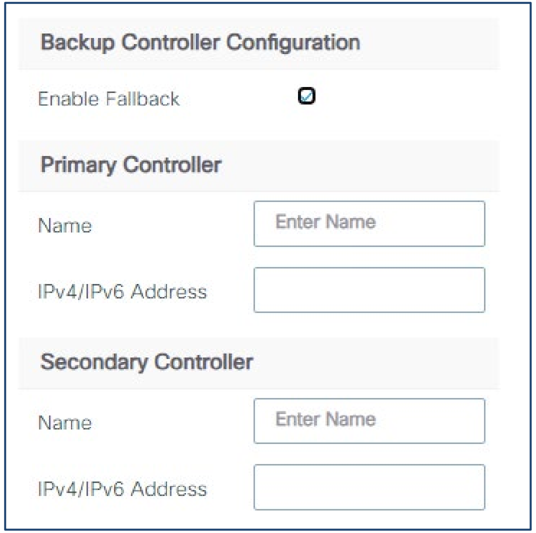
Reference

- It's the same concept as with AireOS:
    - Primary/Secondary/Tertiary: these are configured and saved at AP level. When Primary is set or changed, the AP will do a capwap reset and join the new configured Controller
    - Backup Primary/Backup secondary: these settings are configured at the WLC level. AP will evaluate the backup WLCs only if it loses connection to the currently joined WLC
    - If the AP's current joined controller fails, AP chooses an available controller from the list in this order: primary, secondary, tertiary, primary backup, and secondary backup
    - AP Fallback only applies to Primary and no other backup controller.
- Differently than AireOS, C9800 allows you to configure the Backup WLCs at the AP Join profile level, so for a group of APs. AireOS is only at global level
- Primary/Secondary Controllers are always configured at the AP level

Backup Primary/Secondary configuration

Reference

- Correct naming in the WebUI. Fix available starting 17.4, 17.3.2, 16.12.5)
- AP Fallback to Primary only applies to Primary controller (not Backup primary)
- Before the fix:



Backup Controller Configuration

Enable Fallback ☑

Primary Controller

Name: Enter Name

IPv4/IPv6 Address:

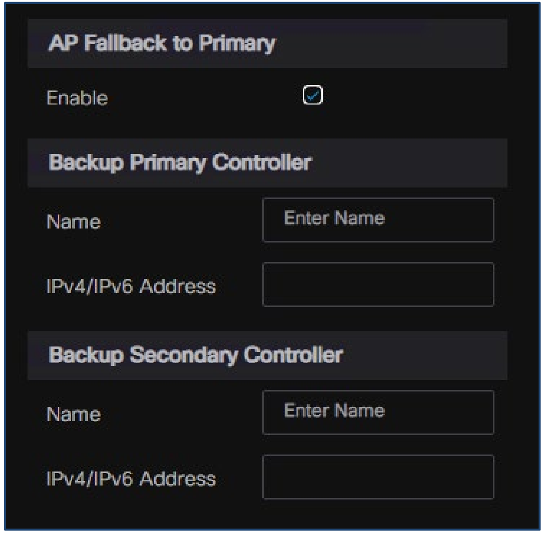
Secondary Controller

Name: Enter Name

IPv4/IPv6 Address:

Changed to...

After the fix:



AP Fallback to Primary

Enable ☑

Backup Primary Controller

Name: Enter Name

IPv4/IPv6 Address:

Backup Secondary Controller

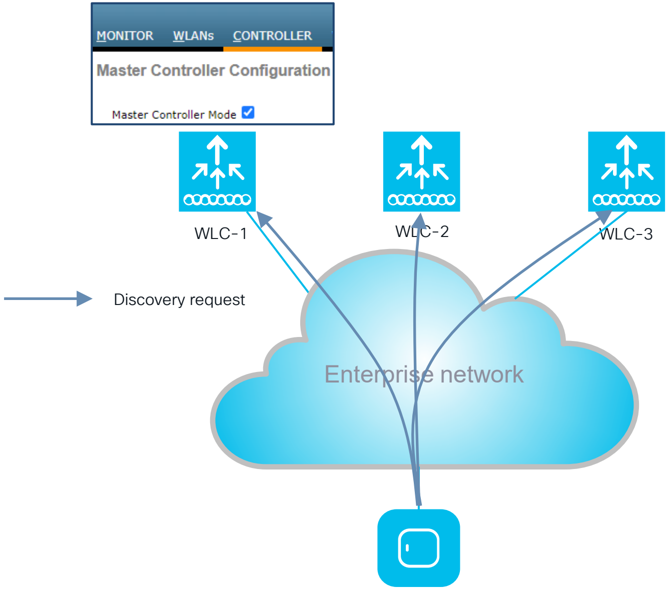
Name: Enter Name

IPv4/IPv6 Address:

Reference

Master Controller in AireOS

The concept of Master Controller in AireOS:

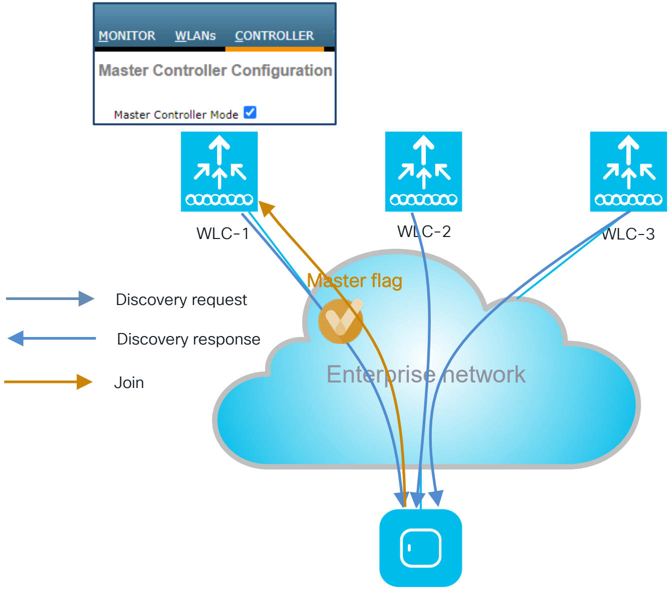


- Master controller is used when you want APs to join a **priming controller** to then set the Primary / Secondary WLC
- If AP learns multiple WLCs at discovery time (via broadcast, Mobility Group, DHCP, DNS, etc.) it will choose the WLC to join based on reported AP load

Master Controller in AireOS

Reference

The concept of Master Controller in AireOS:



Master Controller Configuration

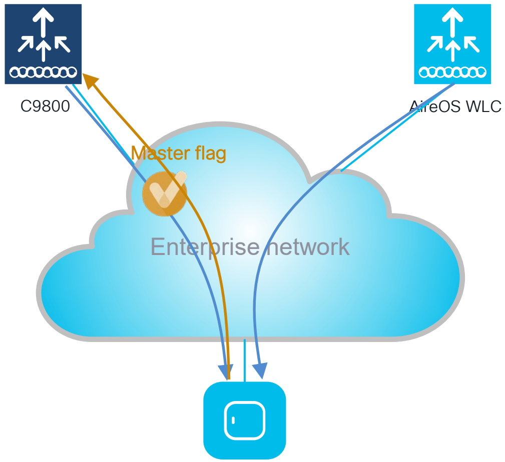
Master Controller Mode ☑

- Master controller is used when you want APs to join a **priming controller** to then set the Primary / Secondary WLC
- If AP learns multiple WLCs at discovery time (via broadcast, Mobility Group, DHCP, DNS, etc.) it will choose the WLC to join based on reported AP load
- **If Master Controller flag is set in the Discovery response, the AP will always join that controller**
- This applies only when AP doesn't have defined Primary / Secondary WLCs

Priming Controller feature in C9800

Reference

- Before 17.3, C9800 had “Master Controller” flag always enabled
- In Migration scenarios, the C9800 would always be chosen…might now be desirable



Solution:

- In 17.3 the flag is always disabled
- Starting 17.4 the flag is configurable:

```
C9800(config)#wireless priming-controller
```

- In C9800 is called Priming Controller

Inter-Release Controller Mobility (IRCM)

Reference

- C9800 utilizes **Secure Mobility** (capwap based) as the mobility protocol > supported only on 5508, 8510, 3504, 5520, 8540 AireOS controllers running 8.5 IRCM/8.8/8.10
- **Typical use cases for IRCM:**
  - Customer cannot replace/move APs in one go; AireOS and C9800 deployment will coexist and seamless roaming is needed
  - Customer has an existing Anchor controller and wants to continue to leverage the investment
  - Customer has older APs and cannot migrate WLC to newer IRCM releases > need an intermediate step in migration, need to deploy a “bridge” controller that can talk secure mobility
- Roaming between AireOS and IOS-XE WLC is **always a L3 roam**
- **Most of the caveats found are related to same client VLAN ID deployments**: SSID is associated to VLANX on 9800 controller and VLANX it’s defined on the AireOS controller (associated or not to the same SSID)
- Issue detected: **one-way audio on voice devices** upon roaming (seen mostly in Healthcare)

Prime and DNAC support

Reference

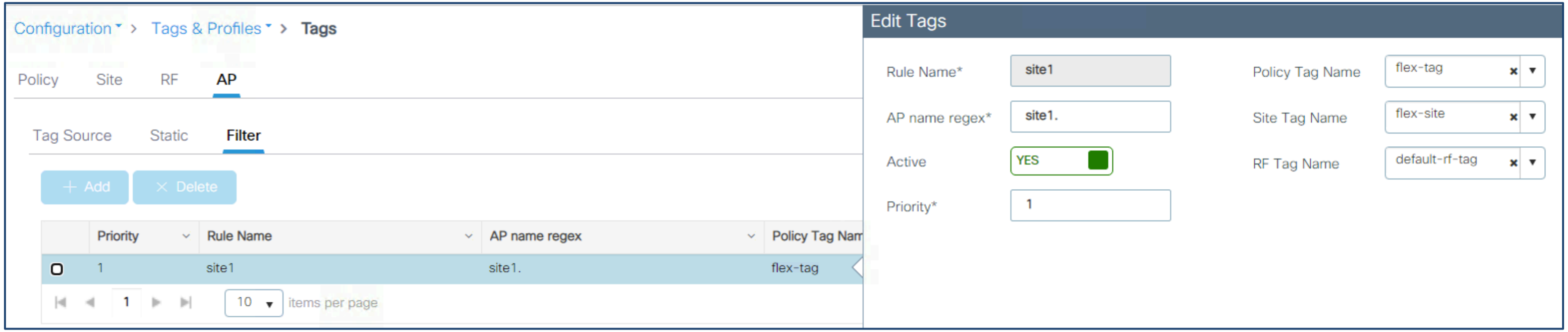
- Check Cisco Wireless Solutions Software Compatibility Matrix > Prime section: https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html
- **IOS-XE 17.3.1** requires an upgrade to **Prime 3.8.1** (3.8 is not supported)
- If DNA Center and Prime coexistence is required with 17.3.1, then DNA Center must be upgraded to 2.1.2 and Prime to 3.8.1
- As of 17.3.1, Telemetry with Prime and Assurance with DNAC is not officially supported out of the SP port
- **Note**: Prime support for older AireOS releases:
  - It is recommended to use Cisco WLC versions 8.5.130.0 and above
  - Rule: for Prime release, validation is targeted for current-2 WLC releases and not all legacy WLC versions.

Moving APs between C9800 controllers

Reference

Solution #3

- This solution works only if you have an AP naming convention
- Under Configuration > Tags & Profiles > Tags go to AP > Filter and, for example, add a regex rule to match all the APs starting with “*site1*” in the AP name and assign them to the desired tags



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

Rule Name*	site1	Policy Tag Name	flex-tag
AP name regex*	site1.	Site Tag Name	flex-site
Active	YES	RF Tag Name	default-rf-tag
Priority*	1		

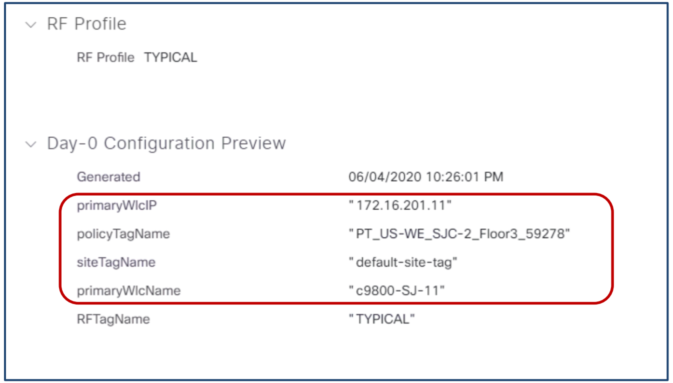
- When APs named “site1<something>” join, they are automatically assigned to specified tags

Reference

Moving APs between C9800 controllers

Solution #4

- Use DNA Center PnP AP onboarding flow to push the tags information to the APs
- After AP is claimed and assigned to a site, this info is pushed via PnP protocol:



RF Profile

RF Profile TYPICAL

Day-0 Configuration Preview

Generated	06/04/2020 10:26:01 PM
primaryWlcIP	"172.16.201.11"
policyTagName	"PT_US-WE_SJC-2_Floor3_59278"
siteTagName	"default-site-tag"
primaryWlcName	"c9800-SJ-11"
RFTagName	"TYPICAL"

In this case tags are automatically saved at the AP

- When Primary fails and APs move to Secondary, in this case DNA Center takes care of configuring the tags and profile on Secondary controller

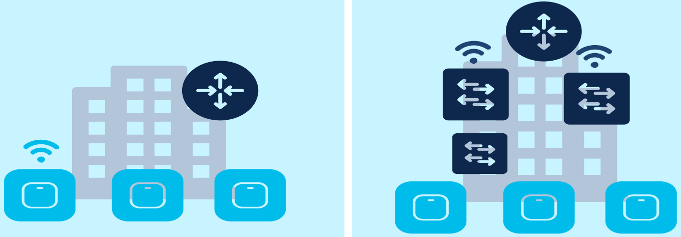
Branch Design options

Branch Design options - Single site

Reference

Local WebUI

Single site



Embedded wireless controller in Catalyst AP (EWC)

Embedded wireless controller in Catalyst switch (non-SDA)

- Manage it via Mobile app (iOS and Android)
- No dependency on Cisco wired infrastructure
- Scales up to 100 APs

- Single Catalyst 9k switch or stack. SSO only with the stack
- Leverages Catalyst switching excellence
- Scale up to 400 APs (#2 separated embedded wireless controller)
- Available from 17.3.1

- Recommended for single standalone site
- Supported on 802.11ac W2 and 11ax APs
- Fire and Forget management model using “on device” Web UI
- EWC on Cat9k (non-SDA):
  - Supported on Catalyst 9300L (50 APs), 9300, 9400, 9500 and 9500H all with 200 APs
  - Under the hood it’s Fabric (LISP and VXLAN), but it’s not SDA because DNAC, ISE not required
  - APs can be connected either directly to cat9k or to a L3 switch
- DNA Licenses:
  - EWC on AP -> not needed anymore (17.3.x)
  - EWC on Cat9k -> DNA advantage for both switch and APs

Branch Design options – Multi site

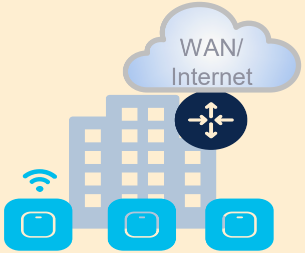
Reference

Cisco DNA Center

Automation

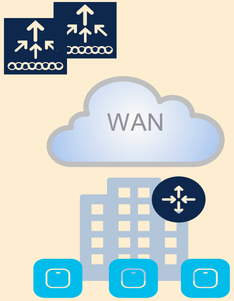
Assurance

Multi site (Enterprise)



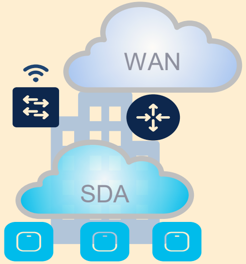
Embedded wireless controller in Catalyst AP (EWC)

- No dependency on Cisco wired infrastructure
- Only on W2 and 11ax APs



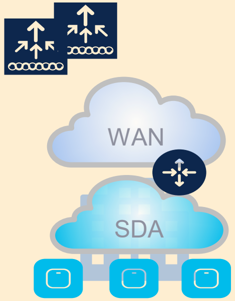
FlexConnect APs with centralized WLC

- Cookie cutter branch config
- Reduced branch footprint
- No dependency on Cisco wired
- Lowest cost solution



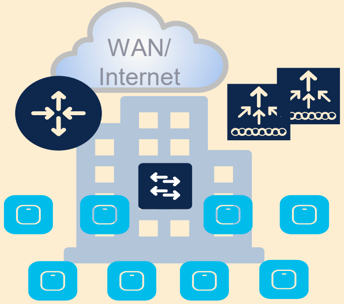
Embedded wireless controller in Catalyst switch (SDA)

- Extending SDA to the branches
- L3 roaming support
- No dependency from WAN
- Scales to 400 APs



FlexConnect APs with centralized WLC over SDA

- Supported starting in DNAC 2.1.2
- Advantages of Flex for wireless
- Allow to migrate wired to SDA first
- Seamless roaming for voice is not supported



Local wireless controller appliance

- Fully featured and full scale
- L3 roaming support
- No dependency on WAN

cisco Live!

#CiscoLive