

The background features a vibrant, abstract design with a color gradient from dark blue on the left to bright yellow and white on the right. The design consists of overlapping, wavy horizontal bands and a radial pattern of lines emanating from a bright white point on the right side, creating a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLiveAPJC



“Reconciliation”- Dustin Koa Art

Cisco Webex App

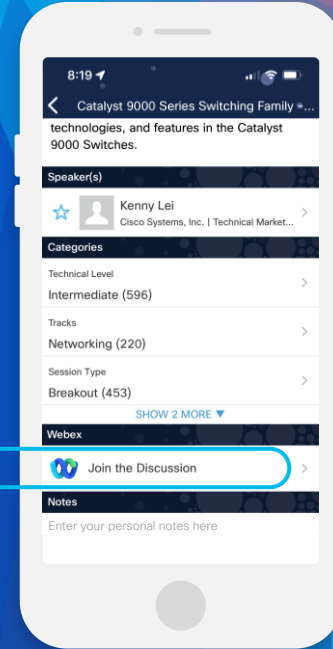
Questions?

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

How

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

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2338>



The bridge to possible

Cisco Catalyst Wireless— How to Successfully Migrate to Catalyst 9800

Sujit Ghosh
TME, Cisco Wireless
BRKEWN-2338

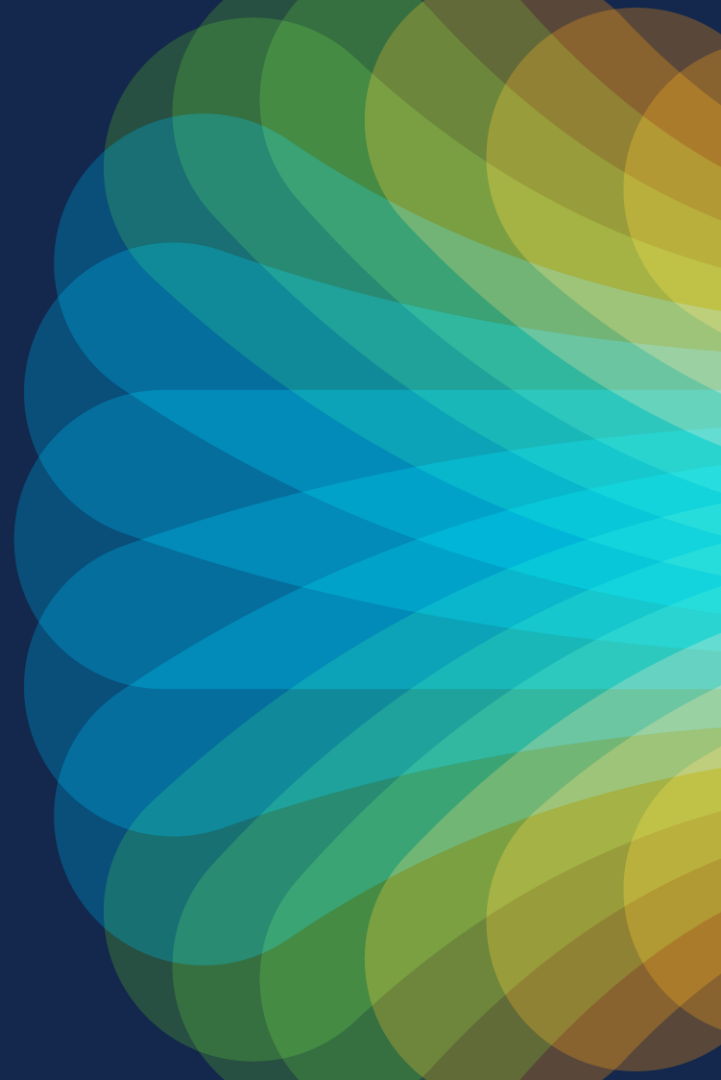
CISCO *Live!*

#CiscoLiveAPJC

Agenda

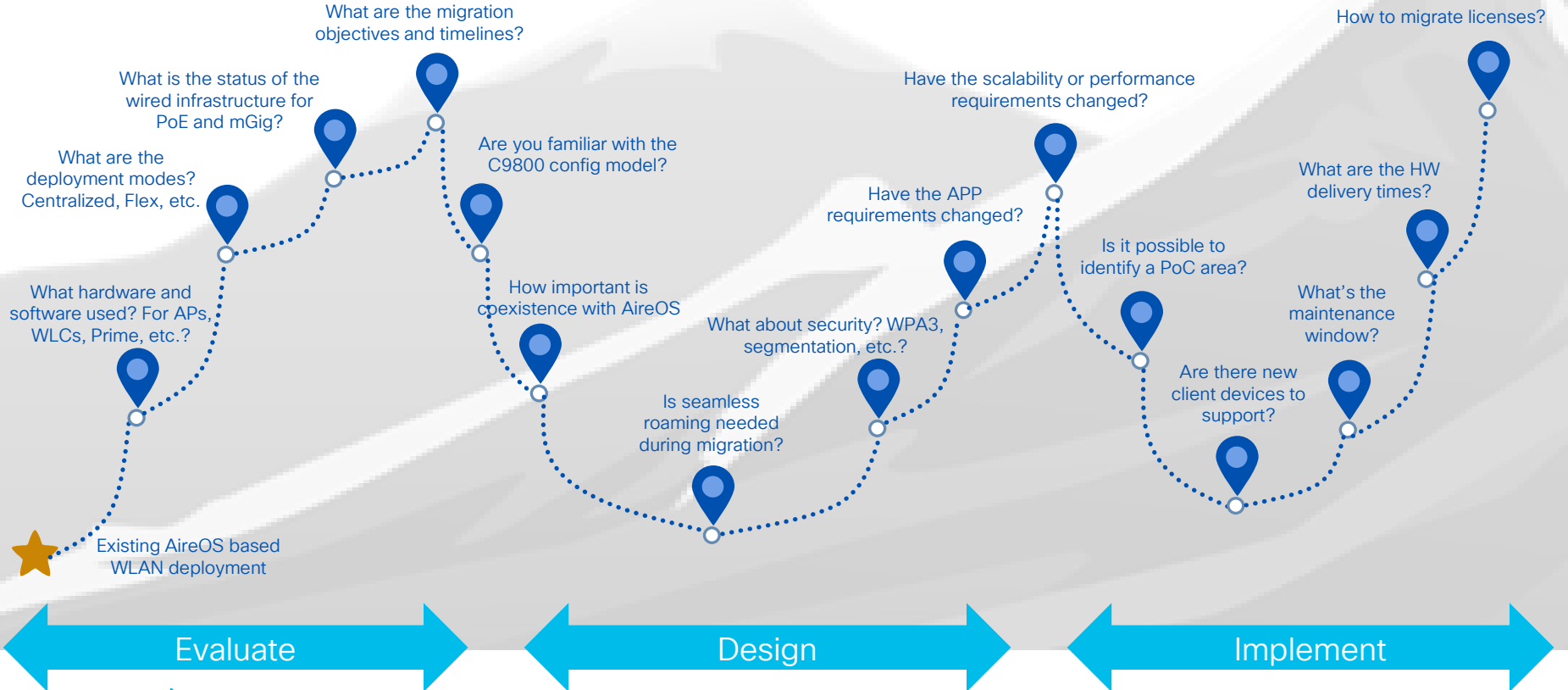
- Building a Migration Strategy
- Migration Best Practices
- AireOS configuration migration
- Design with Access Point (AP) tags in mind
- Wi-Fi 6E: what's the impact on migration?
- AireOS and IOS-XE coexistence
- Monitoring and Troubleshooting

Building a Migration Strategy

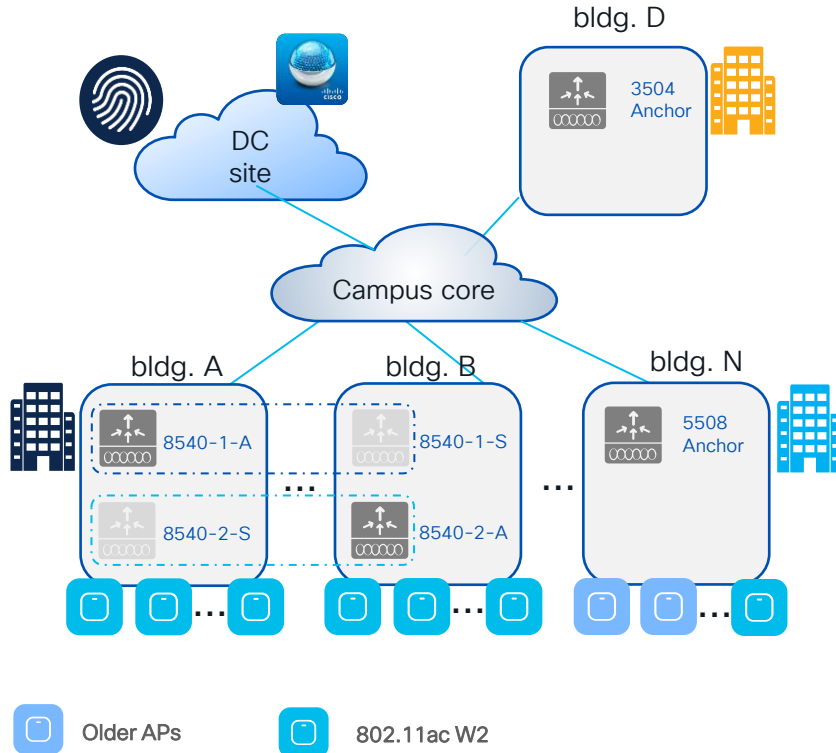


Where shall I start?
....asking questions!

Key Questions for Migration



Customer Migration scenario

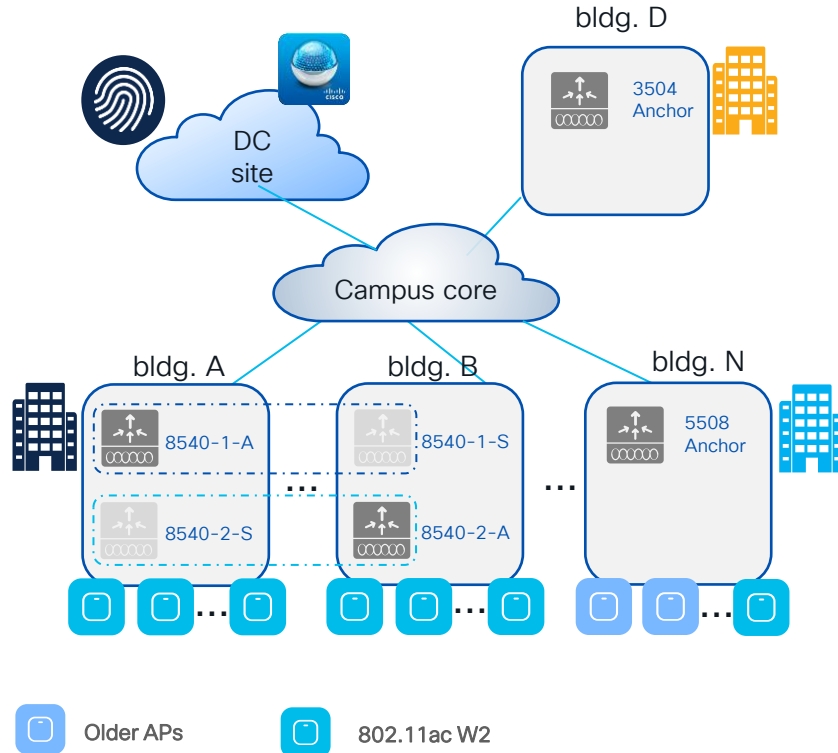


Current deployment:

- 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

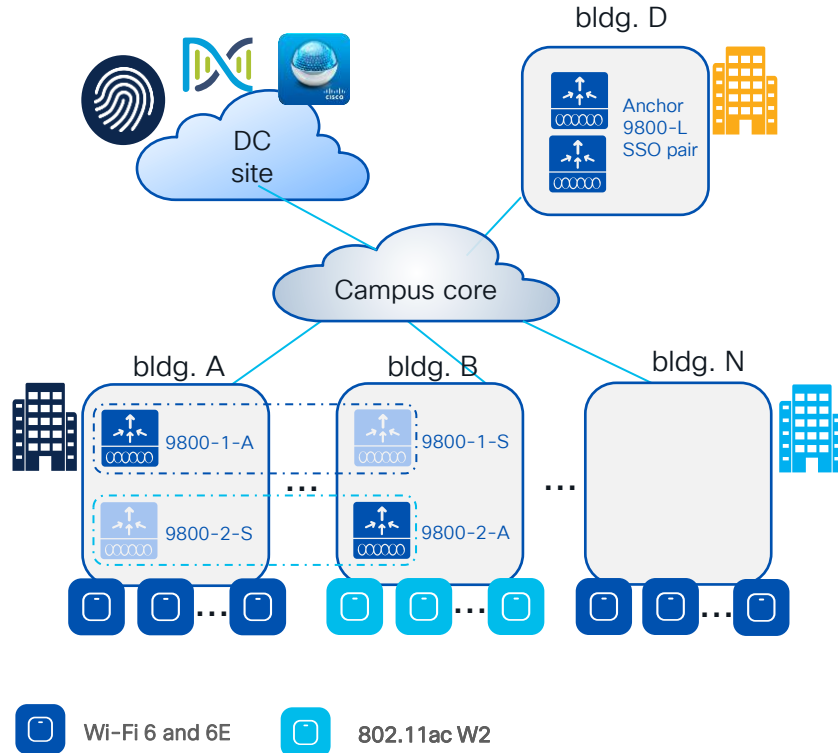


Customer requirements:

- 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 Catalyst 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 Catalyst 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 17.9.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

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

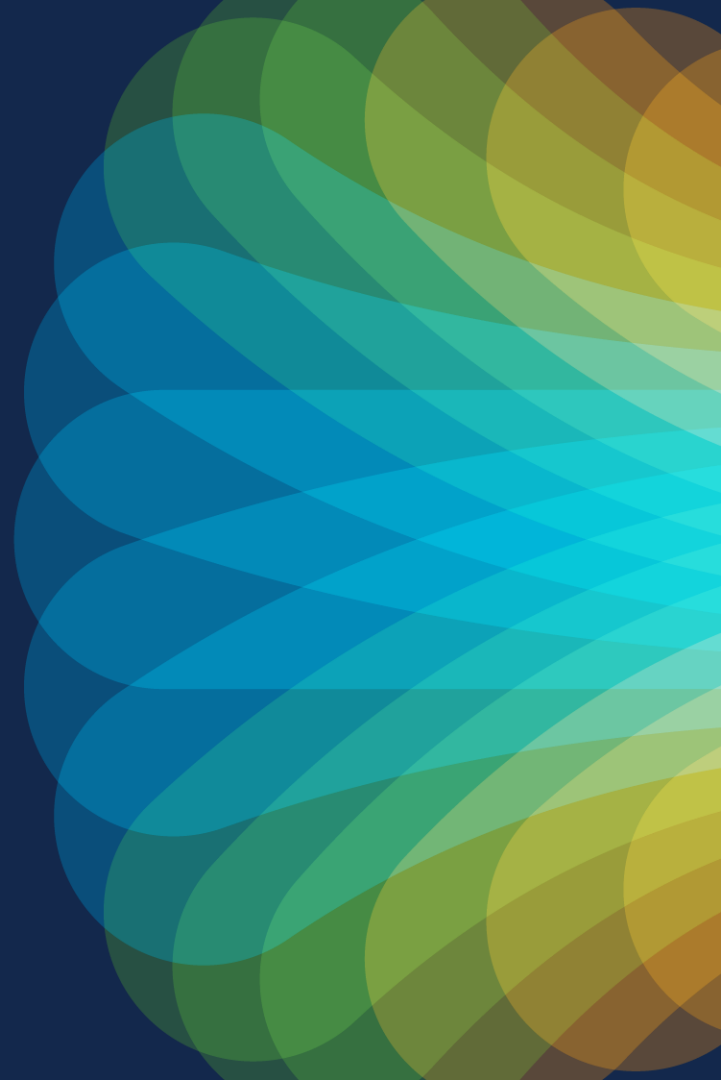
- Architecture review
- Migrate the AireOS configuration
- Feature gap verification
- Design with profiles and tags in mind
- Choose the right software release
- Brownfield considerations



Implement

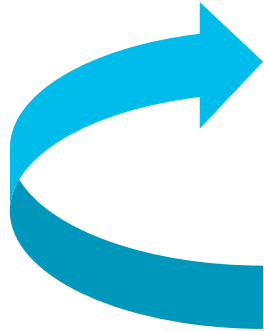
- Lab validation
- Identify pilot migration areas
- Deploy an area in production
- Start replacing legacy APs
- Post migration checks
- Monitor stability and proceed

Migration Best Practices



Migration Best Practices

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



Good place
to start!



Cisco Catalyst 9800 Series Configuration Best Practices

Updated: February 6, 2023

Bias-Free Language

Table of Contents

- Table of Contents
- Introduction
- Notes about this guide
- Prerequisites
- Cisco Catalyst 9800 Series ne...
- Cisco Catalyst 9800 Series pro...
- General controller settings
- General access point settings
- Network controller settings
- Network access point settings
- SSID/WLAN settings
- Security settings
- Rogue management and detec...
- Rogue policies
- High availability
- Returns and Replacements (R...
- Wireless and RF settings

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.

Cisco Catalyst 9800 Series Wireless Controllers

Powered by Cisco IOS® XE

Open and programmable

Cisco Catalyst 9100 Access Points

Powered by Wi-Fi 6/6E technology

Superior RF Experience

Resilient

- Zero downtime with software updates and upgrades:
 - Software Maintenance Unit (SMU)
 - AP Service and Device Pack
 - Intelligent Rolling AP Upgrade
- Cisco Software Upgrade (CSU)

Secure

- Automated macro and micro segmentation with Cisco SD-Access
- Advanced WIPS
- WPA3, Trustworthy systems, etc.

Intelligent

- AI Enhanced RRM
- AI assisted CleanAir Pro
- Enhanced Analytics and Assurance with Cisco DNA Center

<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 Tag



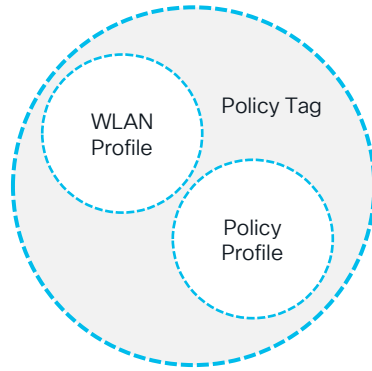
Site Tag

Important to remember:

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

Migration Best Practices

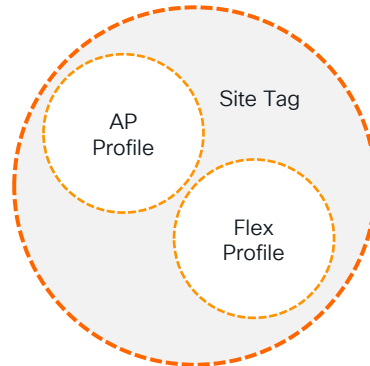
Deep knowledge of C9800 new configuration model (Profiles & Tags)



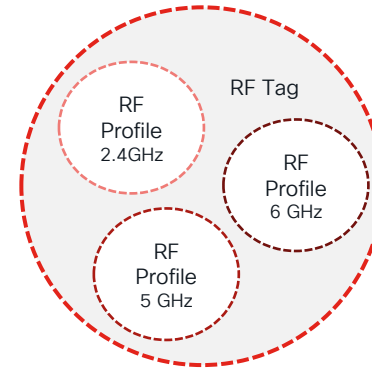
- Defines the **Broadcast domain** (list of WLANs to be broadcasted) with the policies of the respective SSIDs
- “Equivalent” to AP Group in AireOS

SSID = Service Set Identifier

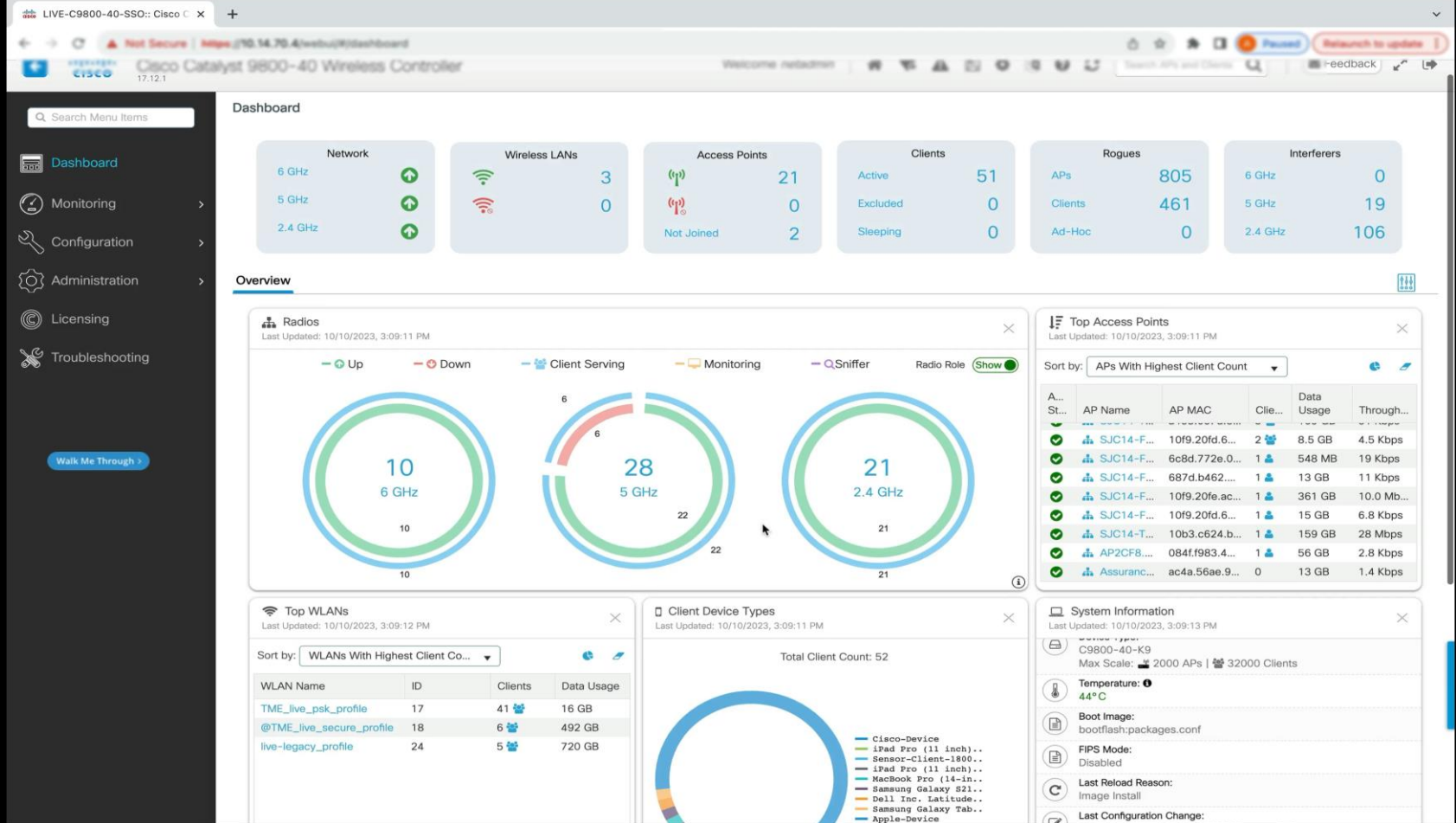
Access Points



- 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

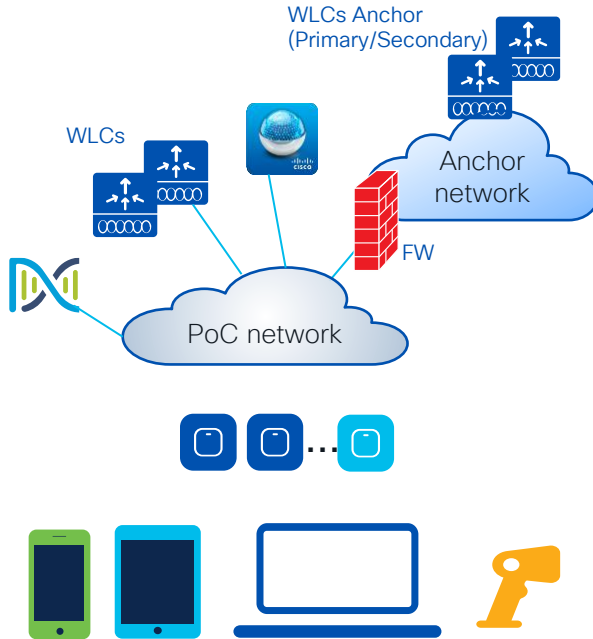


- Defines the **Radio Frequency (RF) properties** of the group of APs per radio



Migration Best Practices

- Build a PoC area with same characteristics of the production network



“Same” topology:

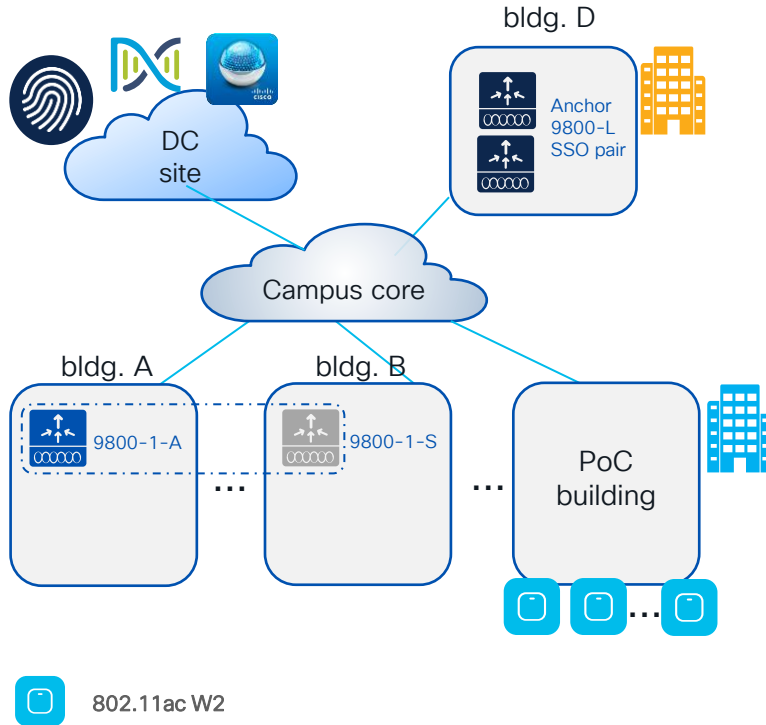
- “Same” = as close as possible to production
- Anchor Controller, High Availability pair, Firewall and other network settings like AAA should be as close as production as possible
- Test the main features customer cares about

“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

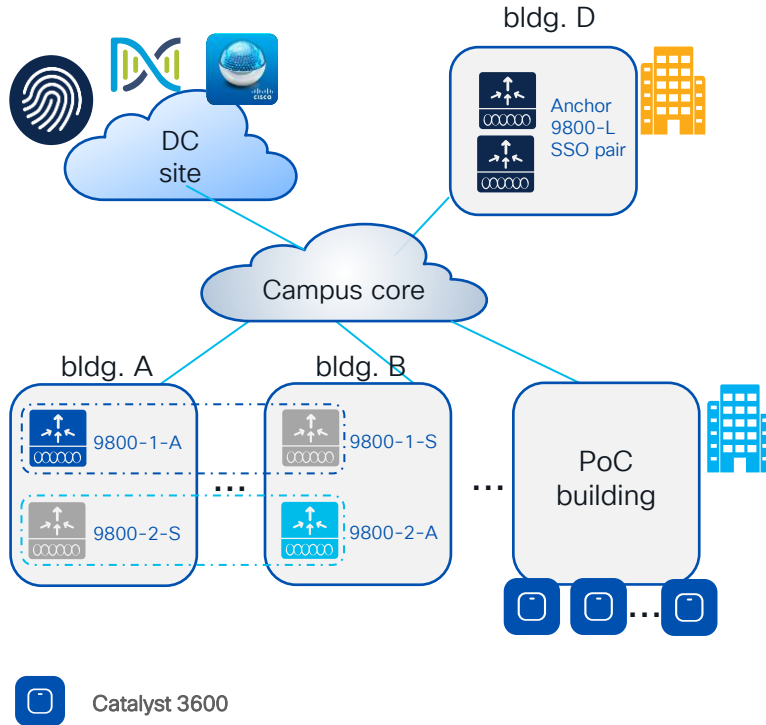
Customer Migration scenario – PoC



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

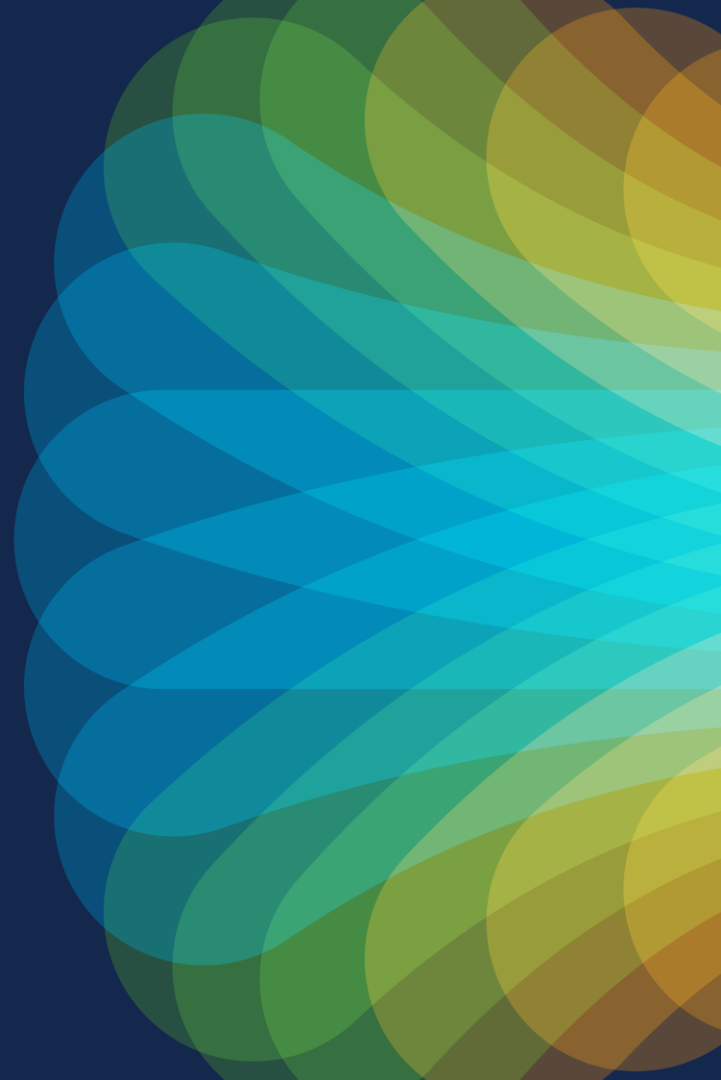
Customer Migration scenario – PoC



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 17.9.4 software with few APs in the lab
- Added 400 APs in production with 17.9.4

Catalyst 9800 Recommended Releases



What is the recommended release?

no more “gold star”

Go with 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
- 17.3.8 has been released in September, recommended release for this train



Go with 17.6.x:

- If you want the most stable train for Wi-Fi 6 Catalyst Access Points without support for W1 APs (1700/2700/3700/1572)
- 17.6.6 has



Go with 17.9.x:

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



Go with 17.12.x:

- Only if you need support for 9166D and IW9167I, new countries supporting 6GHz, FIPS 140-3 compliance, and the new features in this release (VRF, Mesh on SDA, RF based load balance, etc.)
- 17.12.x supports **802.11ac W1 APs** to ease the migration to C9800 & Wi-Fi 6E
- 17.12.2 will be out at the end of October

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



Reference

Cisco Recommended Software Matrix*

IOS-XE	AP	IRCM with Gen 1 AireOS	IRCM with Gen 2 AireOS	DNA-C	Prime	CMX	ISE
17.3.7	802.11ax 802.11ac W1 and W2	8.5.182.104	8.10.185	Matrix	3.10.1	10.6.2	3.1 3.0 2.7
17.6.5	802.11ax 802.11ac W2	8.5.182.104	8.10.185	Matrix	3.10.1	10.6.2	3.1 3.0 2.7
17.9.3	802.11ax (Wi-Fi 6/6E) 802.11ac W1 and W2	8.5.182.104	8.10.185	Matrix	3.10.4	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>

DNAC Matrix <https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html>

Catalyst Wireless C9800

Platforms

- ❑ Country code on AP parity with MR

- ❑ Zero Wait DFS - C9136

❑ **CleanAir Pro Enhancements**

- ❑ Background scanning for mesh in 9124

- ❑ Ultra Low 9800-CL (2 cores & 4GB RAM#) – EFT
- ❑ AP9166D1 support

- ❑ 9124 indoor usage in ETSI
- ❑ 9124 AP Power distribution support with 30W

Innovations

- ❑ **Efficient AP image download through TCP**

- ❑ **Jumbo Frame Support for AAA**

- ❑ Policy retention post Dot1x/MAB for Consent

- ❑ **Walk me integration for additional use cases (DCR) , known issues**

- ❑ WGB Support in SDA
- ❑ Mesh Support in SDA
- ❑ Layer 3 Access (VRF support#)
- ❑ PMF Rogue Containment

❑ **Automated Frequency Coordination (AFC) on 6GHz**

❑ **Auto AP Location**

- ❑ ED-RRM with CleanAir Pro
- ❑ Layer 3 Access (OSPF support#)

- ❑ **RF Based Automatic AP load balancing**

- ❑ **WPA2 and WPA3 transition for 6GHz adoption**

- ❑ DHCP Option 82 support from AP in Flex & Guest Foreign/Anchor scenario

- ❑ WGB concurrent radio support on 9130/9124

Simplification

IOS-XE 17.11.1
Mar 22

IOS-XE 17.12.1
July 23

IOS-XE 17.13.1*
Nov 23

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/>

Cisco TAC Tool - 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 controller

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.

5520_config.txt
13.6 KB

Platform Conversion Type
AireOS-->Catalyst 9800

Run

Choose the AireOS to C9800 converter and click Run

Drop the AireOS config file:

- Upload it directly from GUI:

Cisco TAC Tool - WLC Config Converter

Commands

Upload file from Controller

File Type: Configuration

Configuration File Encryption: ☐

Transfer Mode: TFTP

Server Details

IP Address (IPv4/IPv6): 1.1.1.1

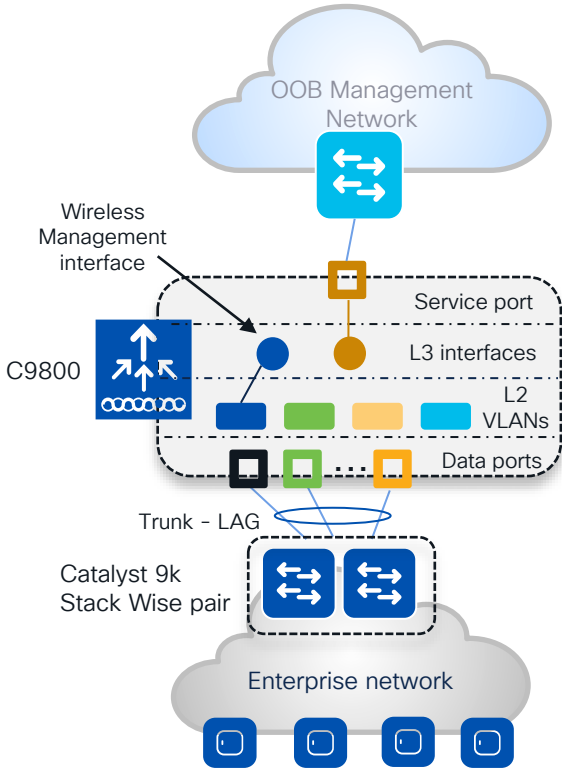
File Path: /path/to/5520_config.txt

File Name: 5520_config.txt

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

CX = Customer eXperience
TAC = Technical Assistance Center

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

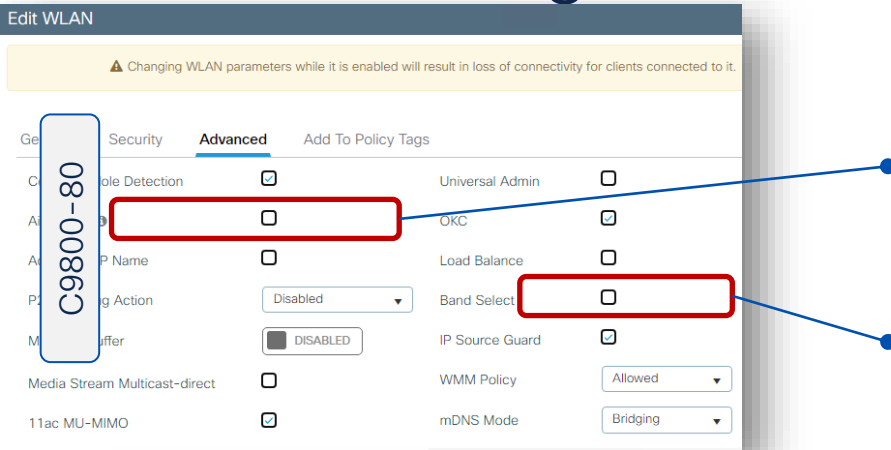
DHCP = Dynamic Host Configuration Protocol
VRF = Virtual Route Forwarding | VLAN = Virtual Local Area Network

Customer Migration scenario

> Configuration review

WLAN settings

WLAN settings



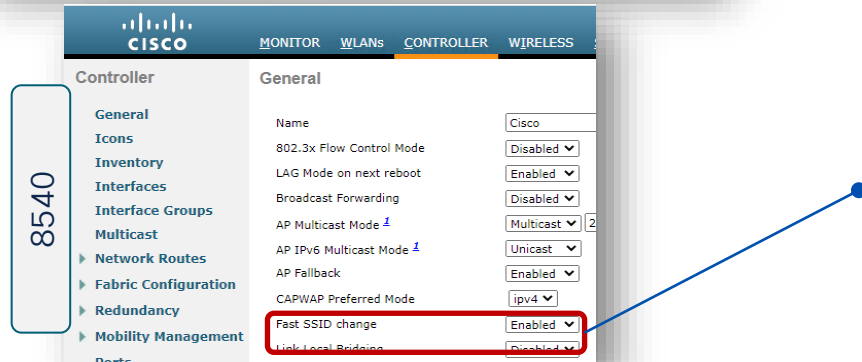
We used to have these commands in AireOS, shall we keep them in IOS XE WLC?

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
```

redirect on-success <https url>

mDNS Configuration

Scenario:

Recommendation:

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

CISCO *Live!*

Policy Profile settings

Policy Profile settings

Edit Policy Profile

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

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

WLAN Timeout

Session Timeout (sec) 0 ⓘ

Idle Timeout (sec) 300

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

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

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

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

A: Yes, absolutely

Default session timeout to 8 hours

What it is?

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

Before 17.12 > timeout is 30 mins

The screenshot shows the 'Edit Policy Profile' configuration page. At the top, there is a warning message: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of conn'. Below this, there are tabs for 'General', 'Access Policies', 'QOS and AVC', 'Mobility', and 'Advanced'. The 'Advanced' tab is selected. Under the 'WLAN Timeout' section, the 'Session Timeout (sec)' is set to 1800, which is highlighted with a red box. There is also an information icon (i) next to the input field.

Starting 17.12 > timeout is 8 hours

The screenshot shows the 'Edit Policy Profile' configuration page, similar to the previous one. The 'Advanced' tab is selected. Under the 'WLAN Timeout' section, the 'Session Timeout (sec)' is now set to 28800, which is highlighted with a red box. An information icon (i) is also present next to the input field.

High Availability

High Availability Evolution

Flexible Redundancy Support

- N+1 Redundancy
- HA SSO

AP Update Innovations

- Rolling AP Upgrade
- N+1 Hitless Rolling AP Upgrade

Patching (SMU)

- Hot Patch / Cold Patch
- AP Service Packs (APSP)
- AP Device pack
- Flexible Per-Site ,Per-Model Updates

Cisco IOS XE 16.1x
CY 2018-19

ISSU

(In-Service Software Upgrade)

Eliminate the network downtime during WLC software upgrade in a HA SSO Pair

HA SSO Improvements

- RMI IPv4, RMI IPv6
- Dual Active Detection
- GW Check
- Standby Monitoring
- Radius Login on Standby

Cisco IOS XE 17.3
CY 2020

Standby Monitoring

- Standby Monitoring through Active
- Direct Standby Monitoring

Network Error Handling for RMI

Cisco IOS XE 17.5
CY 2021

HA Programmability Support

- Yang/Net Conf support for ISSU Install Operations
- Yang/Net Conf support for APSP/APDP

Cisco IOS XE 17.7
CY 2021

N+1 Upgrade Improvements

- Site based N+1 Upgrade
- Yang/RPC support for N+1 Hitless Upgrade and Rolling AP Upgrade

Standby Enhancements

- LLDP Support on Standby
- RADIUS/TACACS support on Standby

Cisco IOS XE 17.9
CY 2022

High Availability

Reducing downtime for Upgrades and Unplanned Events

Unplanned Events

Device and network interruptions

SSO
Stateful
Switchover

N+1 High
Availability

LACP/PAGP
w/ SSO

Multi-
chassis LAG

AP Link
Redundancy w/
C9136

Controller Software Update

Software Maintenance updates (SMU)

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

Cold Patch
HA install on SSO
Pair

Access Point Updates

AP Updates and new AP models

Rolling AP Update
(No Wireless Controller
Reboot)

AP Device Pack
New AP Model

Flexible
Per-Site, Per-
Model Updates

Software Image Upgrades

Wireless controller image upgrades

N+1 Hitless Rolling AP Upg
(All Sites or **Site Based**)



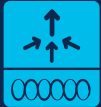
In Service Software
Upgrade (ISSU)

How long can my network be down?

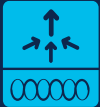
Controller Fault



Standalone



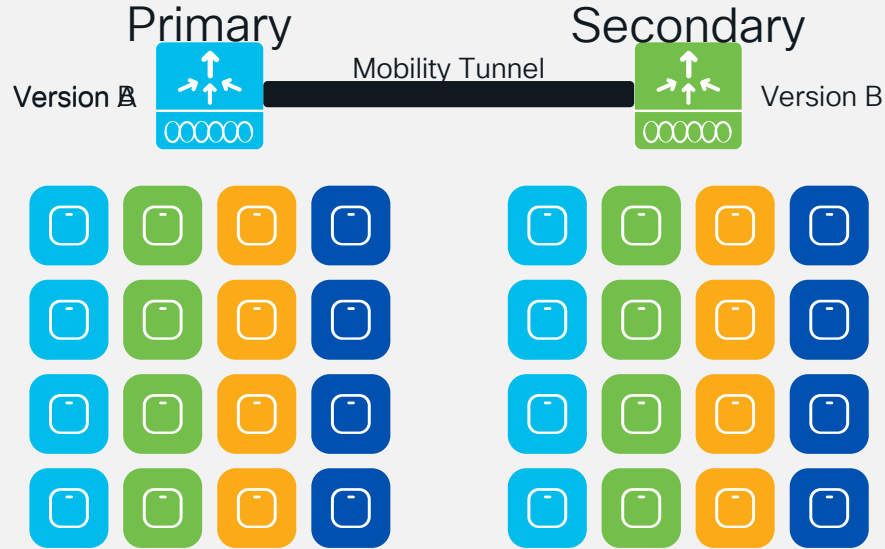
N+1 HA



SSO Pair



N+1 Site Based Hitless Upgrade – 17.9.1



- Use new Site Filters for per-site image upgrades of APs in N+1 scenarios
- Like the previous N+1 Hitless Upgrades, APs will pre-download the images
- During site upgrades, APs will upgrade to new image in rolling fashion
- After the primary controller is upgraded, APs can move back in similar fashion

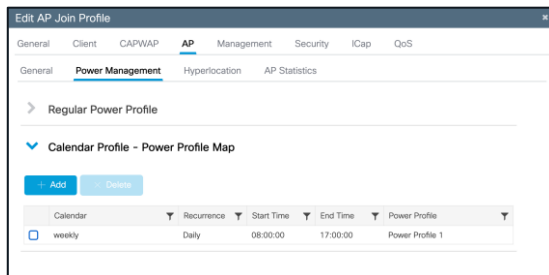
AP Power Optimization

AP Power Optimizations Feature Suite

Save Power, Reallocate Power, and Visibility into Savings

AP Power Save Mode Lower AP Power Usage

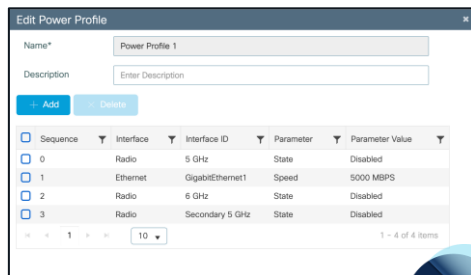
- Create a calendar profile for off-peak hours.
- Create a power profile to lower the power consumption budget during off-peak hours.
- Power Profile: Shut AP Radio or lower spatial Stream, lower port speed, disable USB port.



IOS-XE 17.8

AP Power Distribution Control over how power is

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

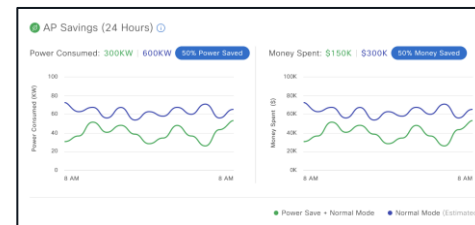


IOS-XE 17.10



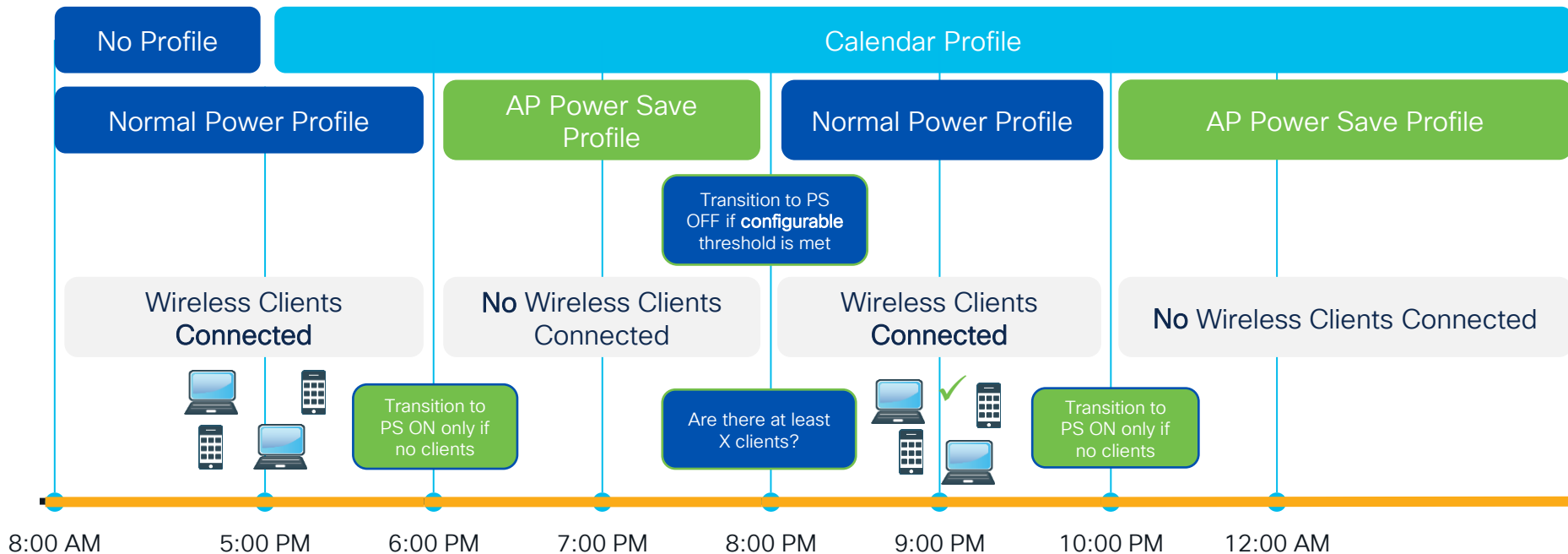
AP Power Savings Insight Power, Money, and Emissions Savings on Cisco Catalyst Center

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



Catalyst AP Power Save (PS): Client logic change

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



AP Console baud rate change

AP Console baud rate change

- In 17.12.1 release notes:

- WPA2 should be disabled while WPA3, PMF and dot11ax are enabled to broadcast WLAN exclusively on 6-GHz band. WPA2 ca
- The inner MAC filtering feature of Embedded Packet Capture (EPC), captures CAPWAP data fragments and CAPWAP control no
- When wireless interface is not available, the RMI +RP configuration on the Web UI is disabled.
- From this release, the **ssid-neighbor-stats interval** value has been changed from 1 to 180 seconds to 30 to 600 seconds. The
- From this release, the default console baud rate of the 802.11AX APs is changed from 9600 bps to 115200 bps.

- True for new AP joining a 17.12.1 C9800, or existing APs after clearing the AP config:

Set to Factory Default

Clear Configuration on this AP and Reset to Factory Defaults

☒ Clear All Config

☐ Clear Config except Static IP

☐ Clear Personal SSID Config

☐ Clear Resolved Tag Config

Clear Config

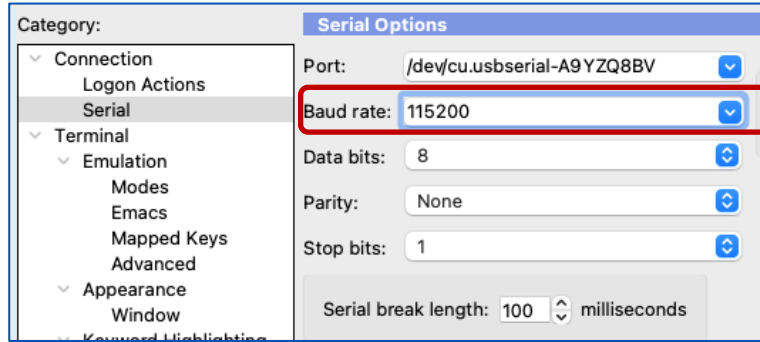
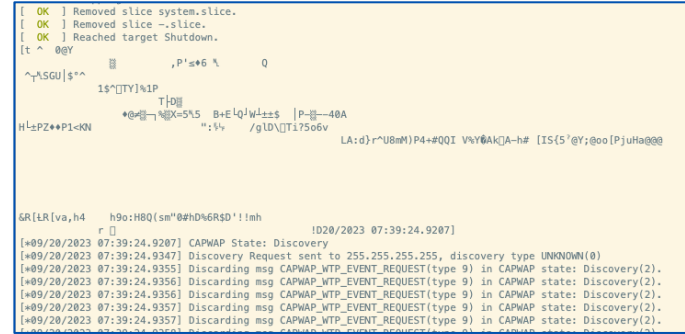
after AP
reboot



```
[ OK ] Stopped Cisco UBIFS reformat/mount.
Stopping Cisco UBIFS reformat/mount...
[ OK ] Removed slice system.slice.
[ OK ] Removed slice -.slice.
[ OK ] Reached target Shutdown.
[t ^ 0@Y
^T LSGU | $ ^ ^
1$ ^ [TY] %1P
T | D
* @ = [ ] % X = 5 5 B + E L Q J W L + + $ | P - - - 40A
H L + P Z + +
```

AP Console baud rate change

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

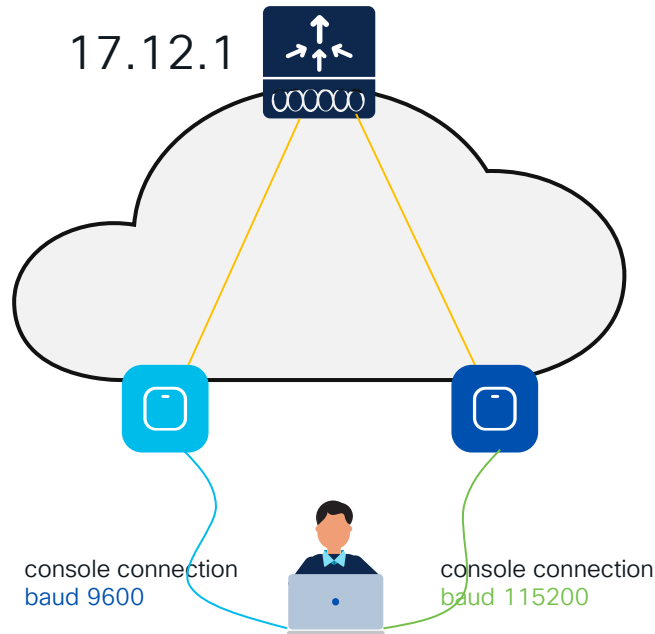
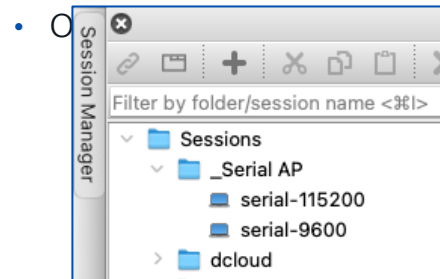


- Why?** To improve boot time; depending on the AP model, you get up to 30s reduction in boot time
- How:** By increasing the baud rate to 115200, the kernel and radio driver/firmware logs are printed faster and hence the AP boots faster (more info in CSCwe88390)

AP Console baud rate change

Why would you care?

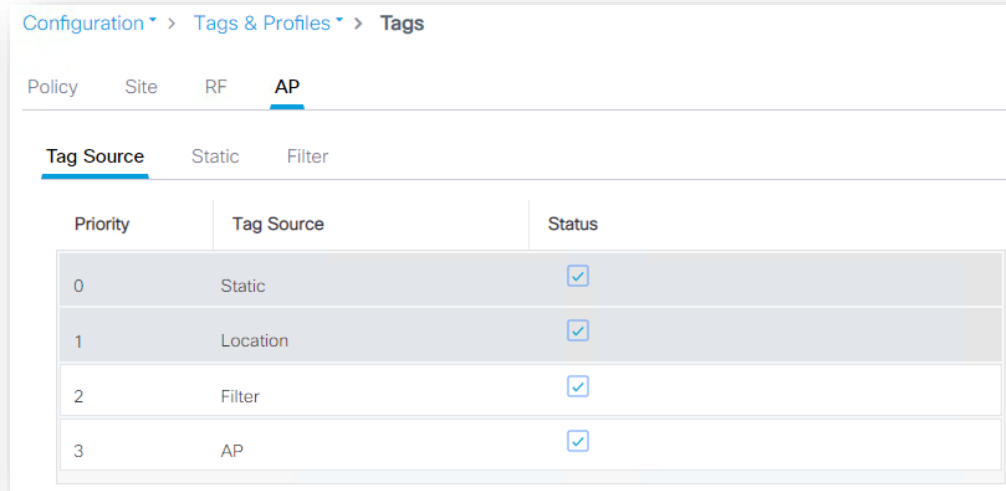
- Customer is on 17.9.4, admin is connected to AP via console with baud rate of 9600. All good
- C9800 is upgraded to 17.12.1. Existing AP still reachable with same console connection. All good
- New AP is added to the network > baud rate on new AP is automatically set to 115200
- Admin needs separate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



APs to Tags mapping

AP to Tags assignment

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



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

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

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

Design with AP Tags in mind

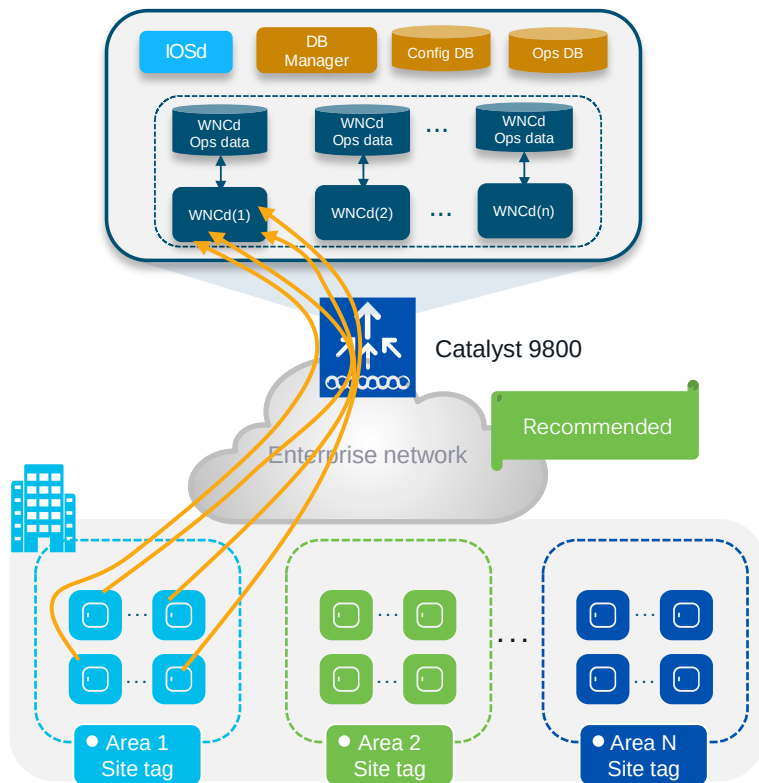
C9800 Architecture

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:
- Better load balance is required to scale

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

Site Tags – AP to WNCd distribution



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 Based Load Balancing

To address the challenges faced in previous design, co-located APs are processed in the same WNCd process. To achieve this,

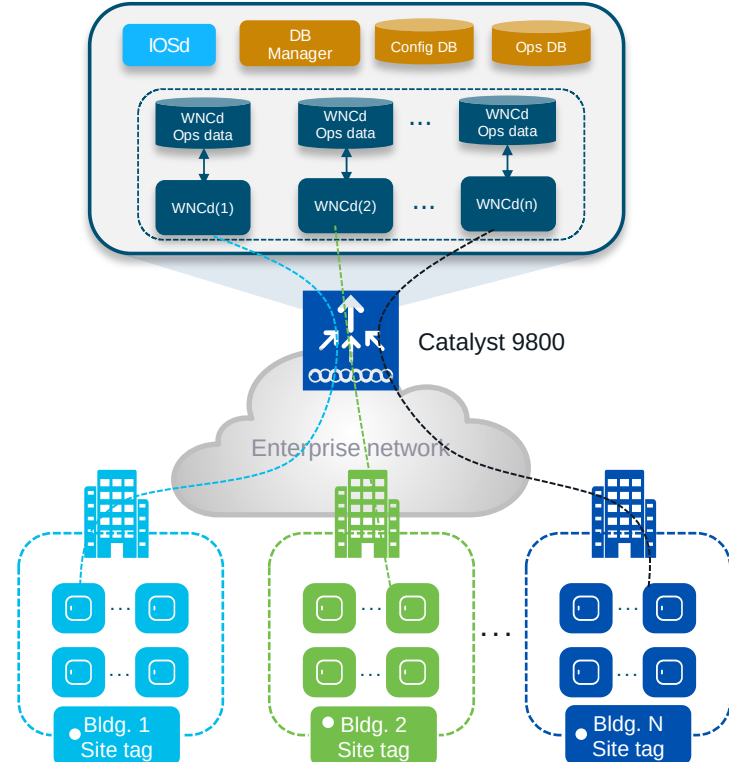
Method: Site Based Load Balancing

AP distribution to WNCd processes is based on Site Tag. APs with the same site-tag are managed by the same WNCd.

Deployment Recommendation: Ideal in deployments where there are **less than 500 APs per site tag** and locations where logically grouping of roaming domain can be defined.

Challenges in this method: Load balancing of APs across WNCds in this implementation resulting in a skew distribution. Site size is not taken into consideration while the site to WNCd mapping is performed.

! Note: No specific configurations required! This is enabled by default.



Load Based Load Balancing

To address the challenges faced in previous design, site load is also considered along with co-location. To achieve this,

Method: Site-load based Load Balancing

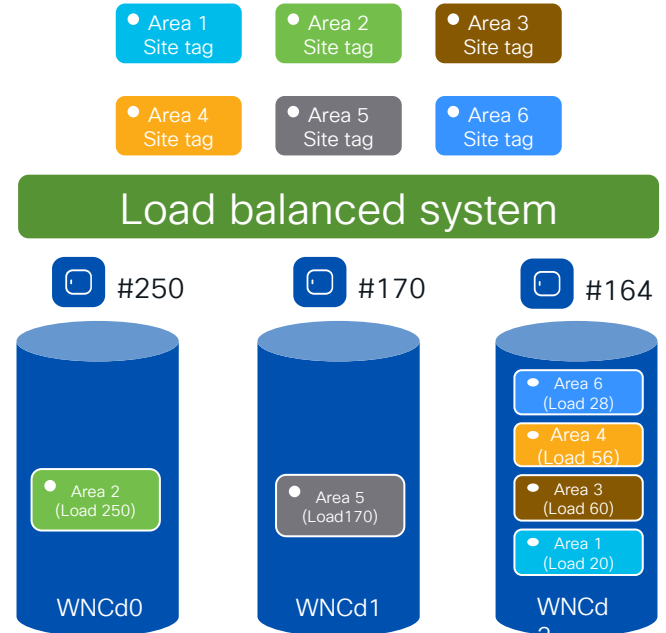
Site tags are distributed among WNCds using the **least loaded criteria** based on the # of site tags.

Deployment Recommendation: Deployments where the site load is known and where the customer needs Weighted option, to configure load based on user activity.

Challenges in this method: May not be an ideal design in deployments where there are no Custom Site Tags configured.

```
C9800# configure terminal
C9800(config)# wireless tag site <Site Tag Name>
C9800(config)# load <Load Number>
```

Load Configured: site-tag load = 20; site-tag load = 250; site-tag load = 60; site-tag load = 56; site-tag load = 170; site-tag load = 28;



RRM based Load Balancing

To address the challenges faced in previous designs, RF based load balancing is preferred. To achieve this,

Method: RRM – AP Neighbor based Load Balancing.

In RRM based, we have a method to automatically cluster the APs and evenly distribute them across WNCds. RRM neighbor report-based co-located AP grouping and load-balancing across WNCd instances will help in solving the site-tag based & load-based AP load-balancing issues.

Deployment Recommendations: Large Venues, One big RF domain & where no custom site tag is configured

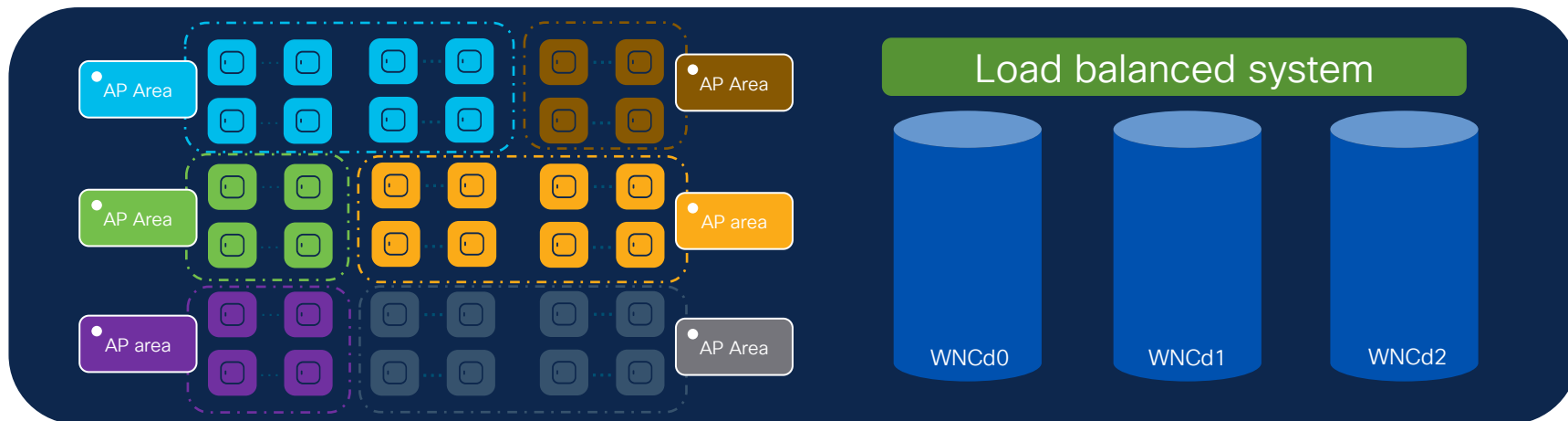
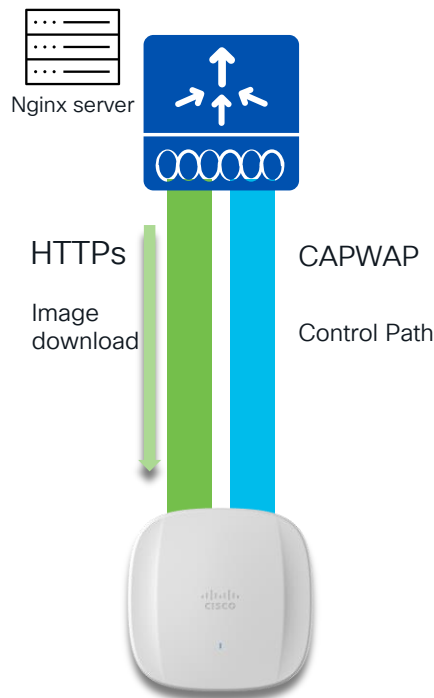
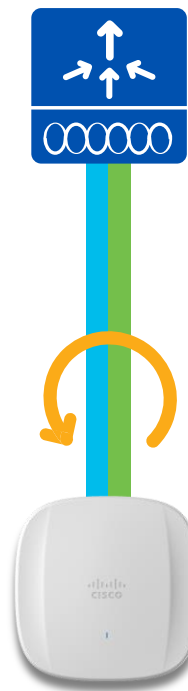


Image Upgrade- TCP

AP image download through TCP



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



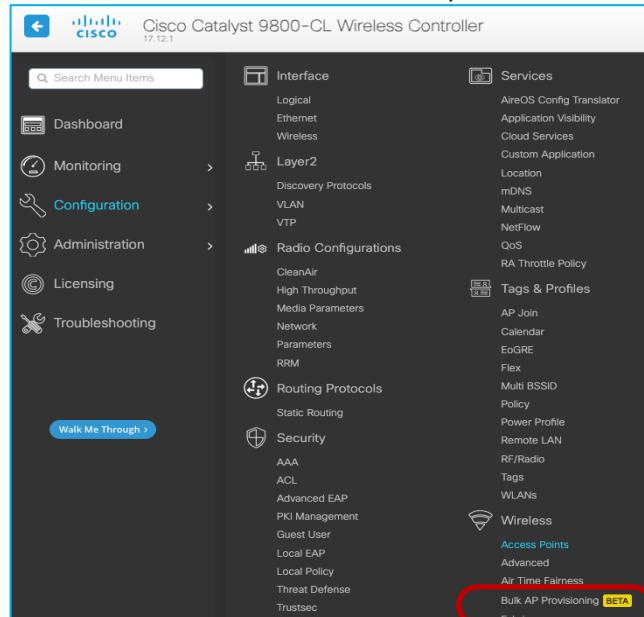
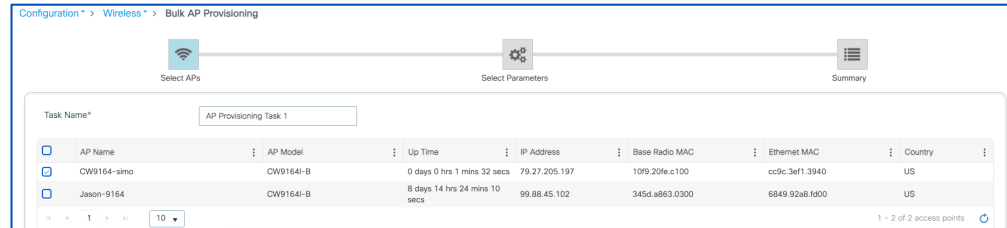
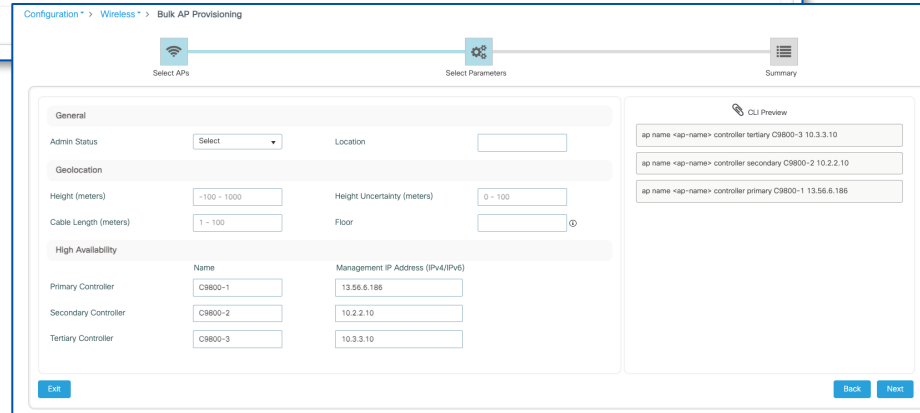
If any **failure** happens in image download over HTTP, it will **fall back to CAPWAP** method to keep the upgrade functionality.

AP Bulk Provisioning

AP Bulk Provisioning

Why would you care?

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



AP Bulk Provisioning

Why would you care?

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

The image displays two screenshots of the Cisco Bulk AP Provisioning interface, showing the 'Configuration' > 'Wireless' > 'Bulk AP Provisioning' path.

Left Screenshot (Select APs):

- Task Name*: AP Provisioning Task 1
- Table of APs:

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

- Page 1 of 1, 10 items.
- Exit button.

Right Screenshot (Select Parameters):

- General section:
 - Admin Status: Select
 - Location: []
- Geolocation section:
 - Height (meters): -100 - 1000
 - Height Uncertainty (meters): 0 - 100
 - Cable Length (meters): 1 - 100
 - Floor: []
- High Availability section:
 - Name: C9800-1
 - Management IP Address (IPv4/IPv6): 13.56.6.186
- Controller Selection:
 - Primary Controller: C9800-1
 - Secondary Controller: C9800-2
 - Tertiary Controller: C9800-3
- CLI Preview (Right Panel):
 - ap name <ap-name> controller tertiary C9800-3 10.3.3.10
 - ap name <ap-name> controller secondary C9800-2 10.2.2.10
 - ap name <ap-name> controller primary C9800-1 13.56.6.186
- Exit, Back, Next buttons.

AP Bulk Provisioning

Why would you care?

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

Configuration > Wireless > Bulk AP Provisioning

Start a workflow to create a AP Provisioning task

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

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

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

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

Note: Results of previously provisioned tasks are not sync

AP Provisioning Task 2

Task Status: ✔ Completed

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

1 APs

AP Provisioning Task 1

Task Status: ✔ Completed

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

1 APs

Configuration > Wireless > Bulk AP Provisioning

Task Details

Task Name	AP Provisioning Task 1
Start Time	09/21/2023 10:20:39
End Time	09/21/2023 10:25:06
Status	Completed

Applied Configuration

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

AP Provision Results

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

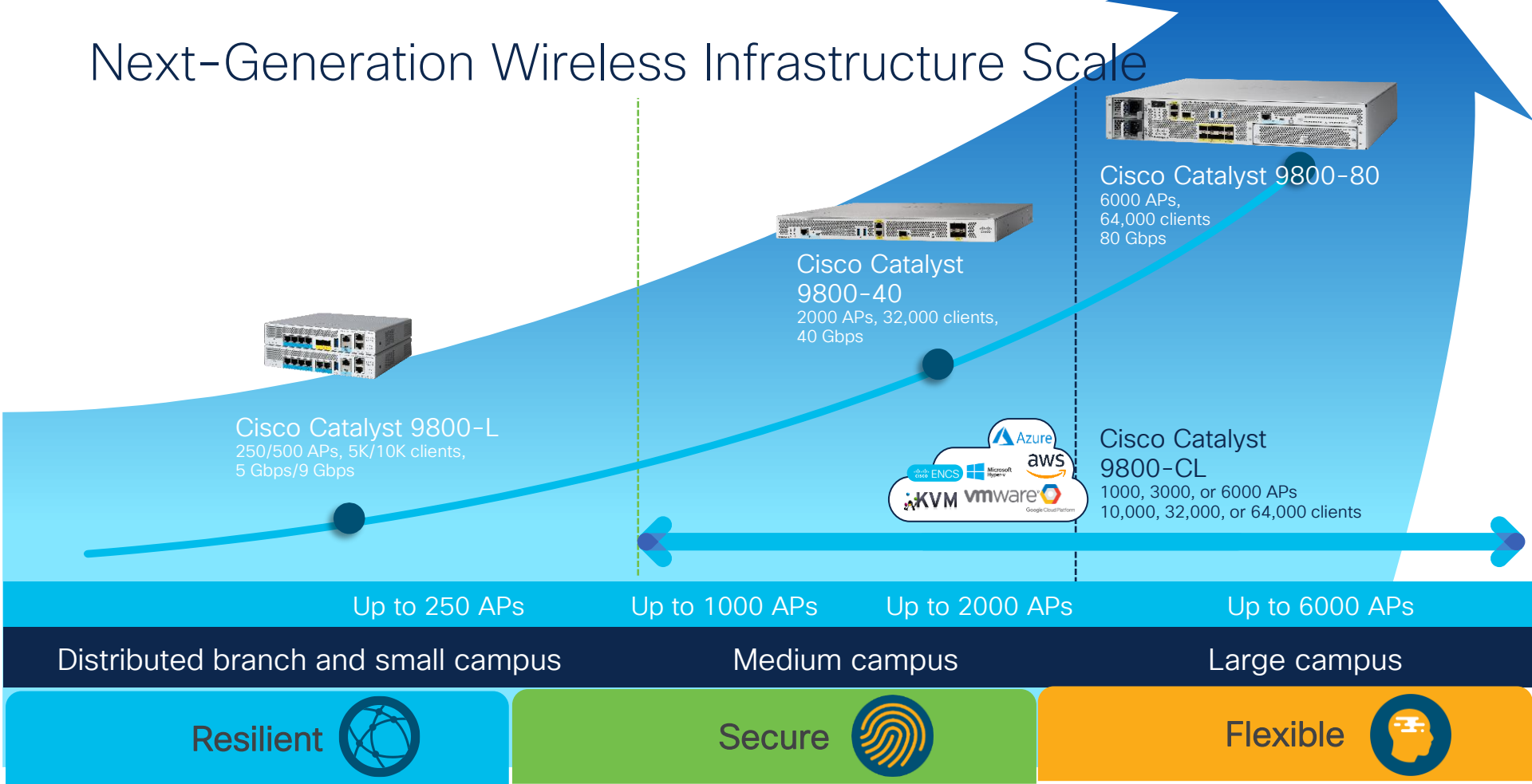
AP Name	AP Status
CW9164-simo	All configuration applied

Configuration

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

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

Next-Generation Wireless Infrastructure Scale



C9800-CL Private Cloud Ultra Low Template

EFT

What is supported?

FlexConnect, Local Switching only

Full feature parity with other deployment templates unless otherwise stated

Supported Hypervisors*

VMWare ESXi

KVM

NFVIS

Microsoft Hyper-V

Max APs Supported

100

Max Clients Supported

1000

vCPUs

2

Memory

4 GB

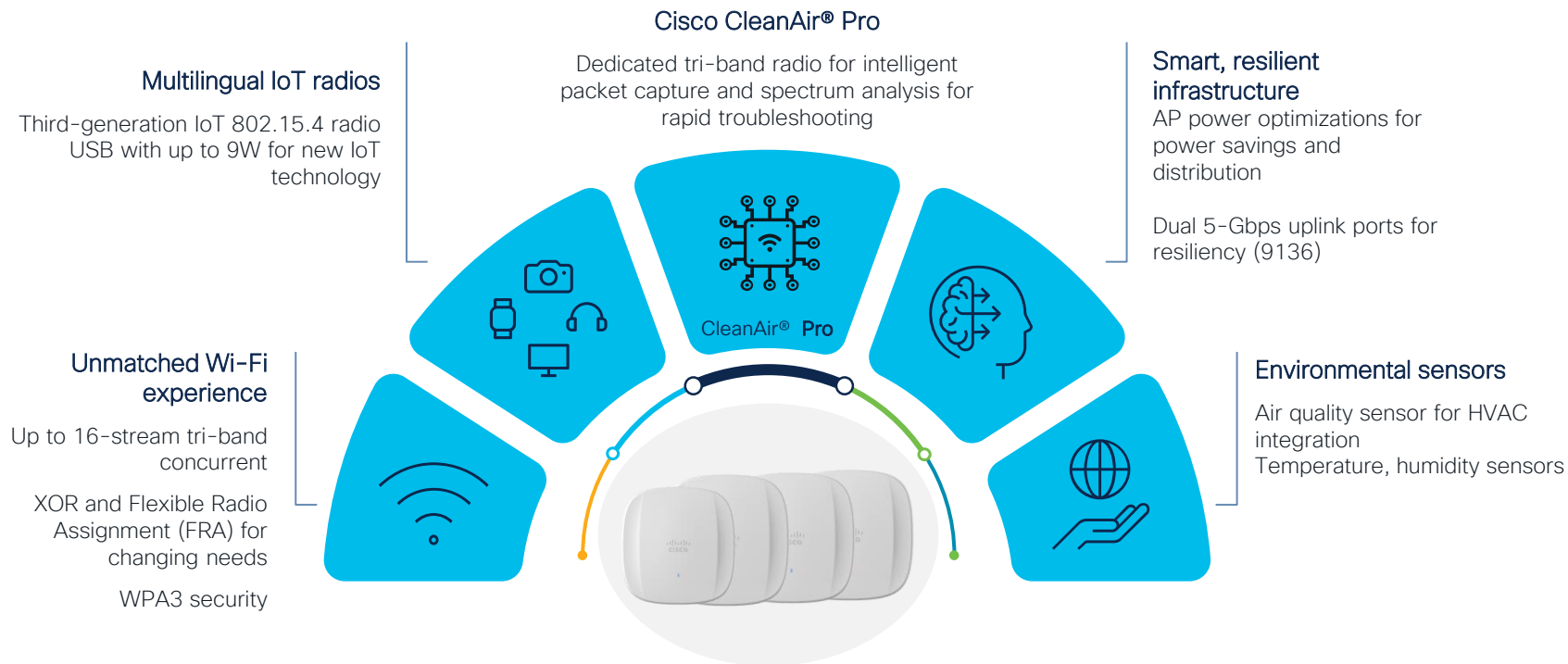
Storage

16 GB

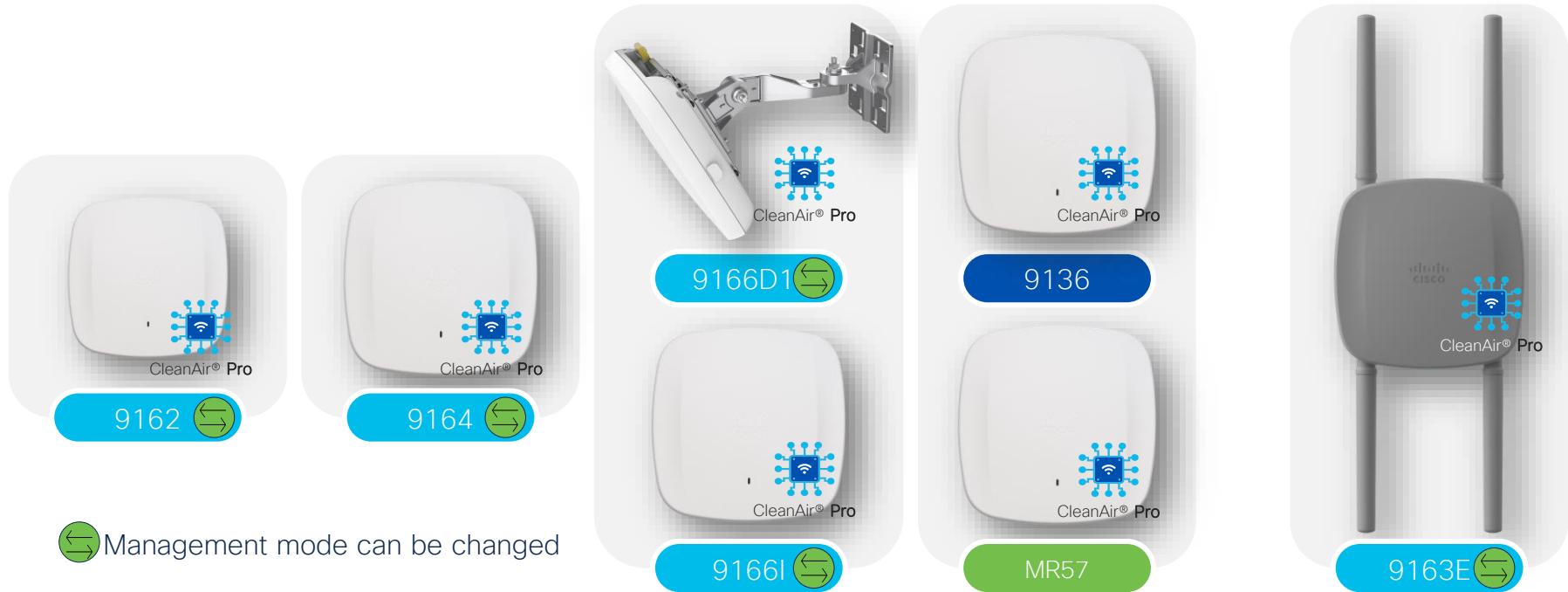
(*) Public Cloud support on roadmap

Catalyst 6E Access Points

Enabling New Experiences



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



 Management mode can be changed

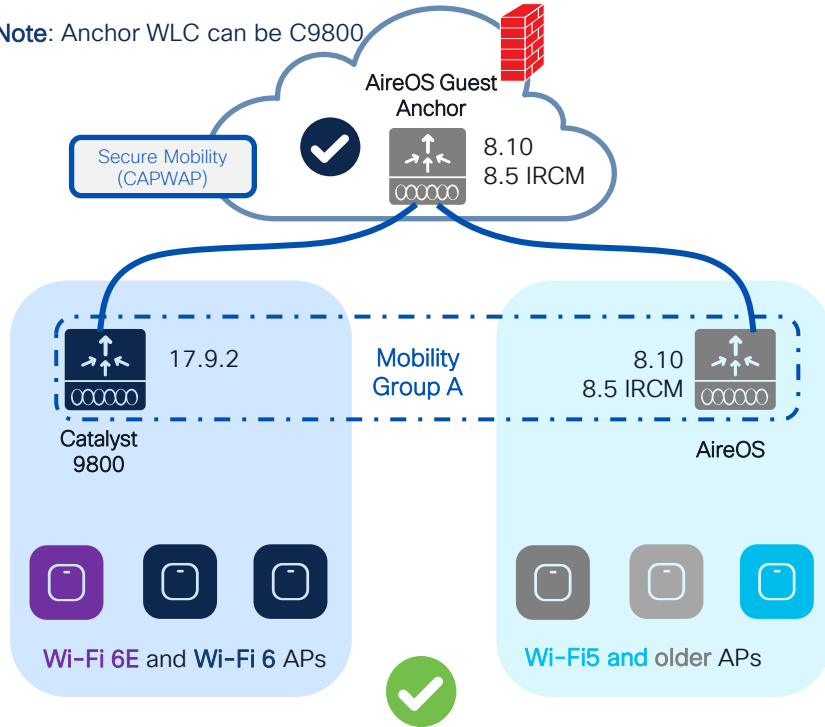
Indoor Access Points

Outdoor Access Points

How do I start adopting 6GHz?

Answer: Inter Release Controller Mobility (IRCM)

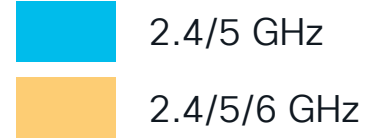
Note: Anchor WLC can be C9800



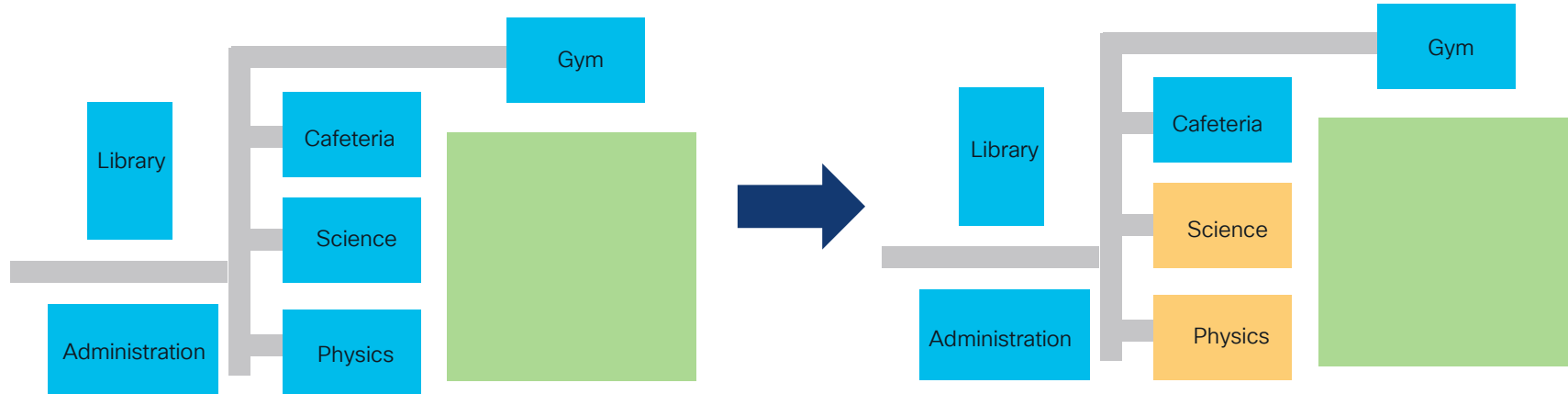
Scenario 1: AireOS WLC supports IRCM

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

Customer Migration Scenario



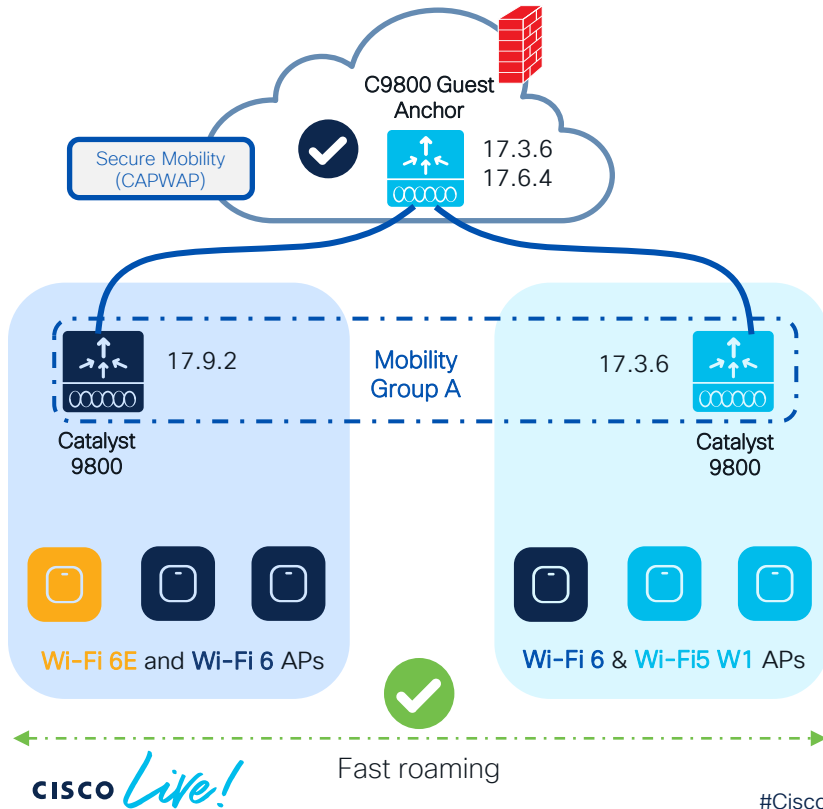
- Move “per RF blocks”
- Move a building or complete floor into the new hardware and software



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

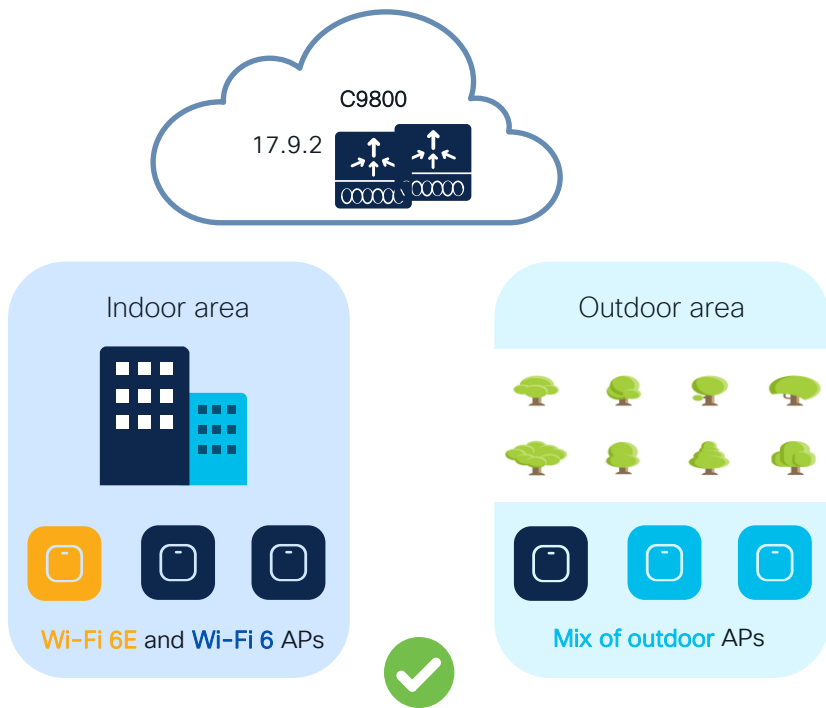
If you have already started your C9800 journey but Wave 1 APs are still present (1700/2700/3700).

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

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

How do I start adopting 6GHz?

What about outdoor areas?

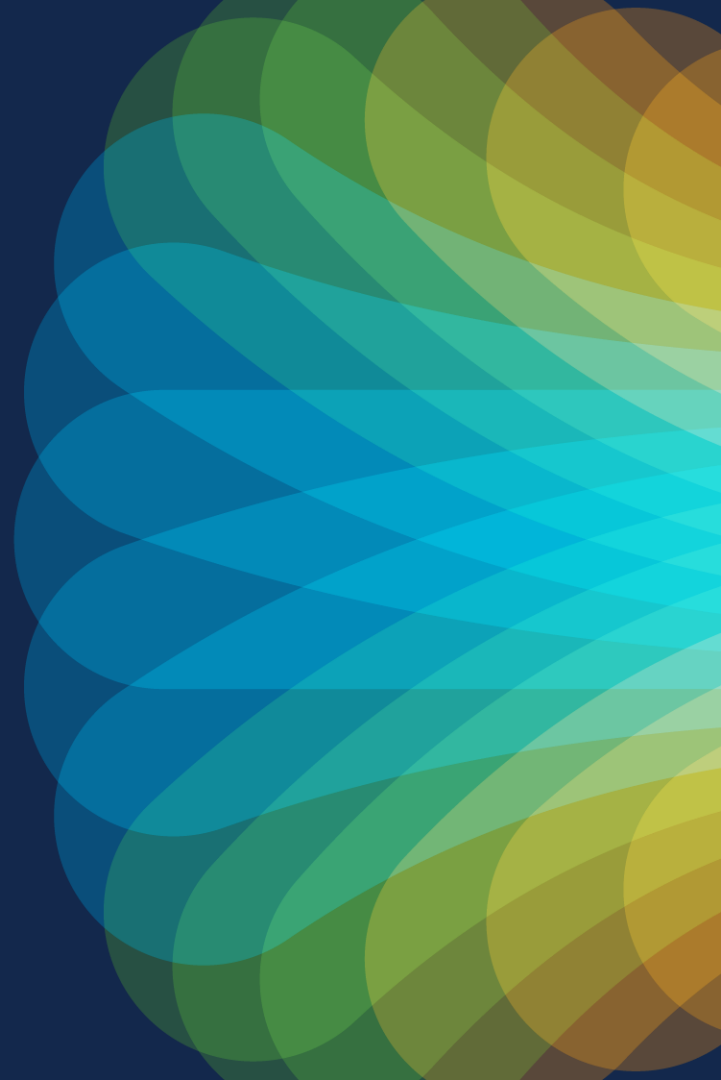


Scenario 3: Mixed indoor and outdoor areas

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

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

Security



WLAN/SSID Design for 6GHz

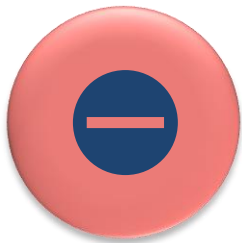
Wi-Fi 6E Security (Recap)



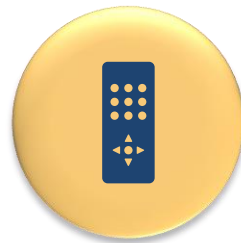
Wi-Fi 6E uplevels security.
WPA3 L2 Security: OWE,
SAE*, 802.1x-SHA256



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



No backward compatibility
with Open and WPA2
Security.



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

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

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

Use Cases



17.12 adds support for Transition Mode 1 profile to rule them all!

- 3 Band SSID
- All WPA3
- Control of devices

BOH/Office



- Separate 2.4+5 and 6GHz
- WPA 2 legacy
- WPA 3 6GHz
- Same SSID

General Use



- Separate 2.4+5 and 6GHz
- WPA 2 legacy
- WPA 3 6GHz
- Different 6GHz SSID

Special Case



- Separate 2.4+5 and 6GHz
- WPA 2 transition legacy
- WPA 3 6GHz
- Same 6GHz SSID

Not recommended



- BOH/Office
 - If you can control the devices.
 - Cisco has this deployed in certain offices
 - Fast roaming works across bands
- General use
 - Accommodates legacy clients
 - Not fast roaming between bands
 - Some clients may “bounce” causing disruption to client and network loading.
 - Typically recommended for Eduroam
- Special Case
 - Like General Use
 - Can help reduce the bounce in general use
 - RNR is still effective⁷⁸
 - Clients will often stay at 5GHz
- Not recommended
 - It works
 - Client may think they are on WPA3 when on WPA2

Single WLAN Profile for 2.4/5 and 6 GHz

Auth Key Mgmt	
802.1X	☒
CCKM ⚠	☐
FT + SAE	☐
FT + PSK	☐
PSK-SHA256	☐
PSK	☐
SAE	☐
FT + 802.1X	☐
802.1X-SHA256	☒

- ✓ L2 Security would be WPA2+ WPA3.
- ✓ AKM should be set to **802.1x-SHA256** and **802.1x (SHA1)** for Enterprise; **SAE** and **PSK** for Personal.
- ✓ PMF as **Optional**
- ✓ For **FT**, enable appropriate AKMs
- ✓ How to configure the client side?
 - For clients that don't support 6 GHz, configure a **WPA2 profile** or **WPA3 Enterprise with PMF as Optional** depending on the client support.
 - For clients that support 6 GHz, configure **WPA3 Enterprise**. They will use these settings to connect to both 2.4/5 GHz and 6GHz

How does a SSID look like?

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

```
C9800#show wlan name Blizzard
```

Security-2.4GHz/5GHz

```

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

```

.....

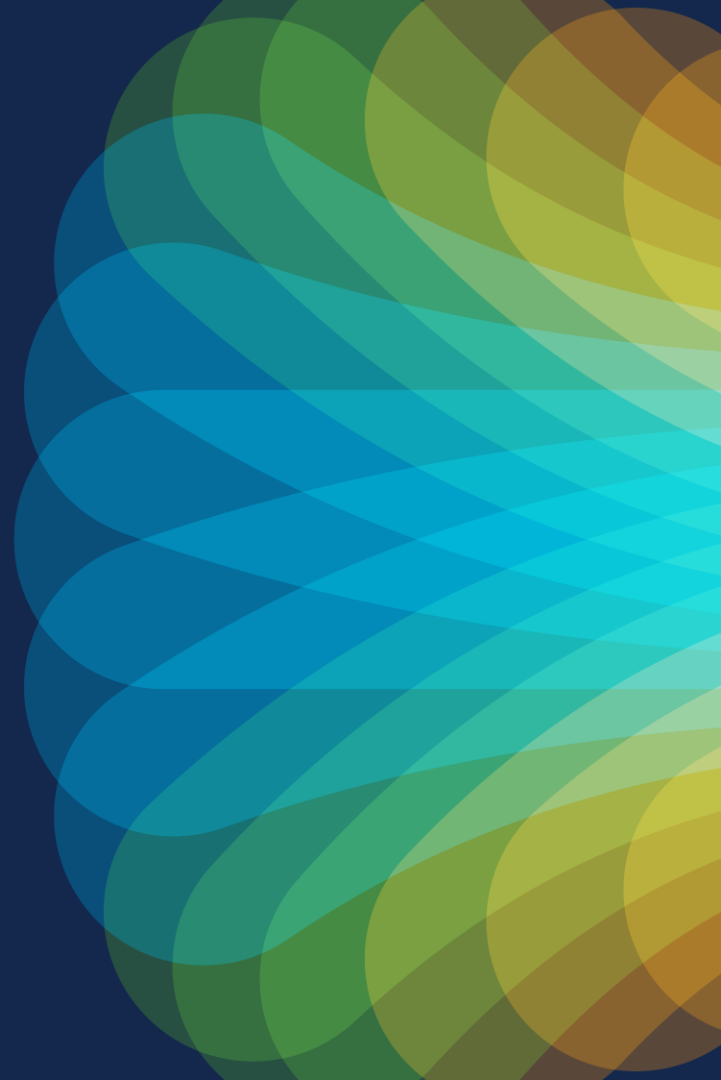
Security-6GHz

```

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

```

PMF Containment



PMF Containment... WHY?

6GHz Design

- ❑ With newer 6GHz band and WPA3 AKMs, PMF is mandatory
- ❑ With PMF, deauthentication frames must be encrypted with MIC once 4-way handshake is completed
- ❑ **Additional security provided by PMF motivates threat actors to use PMF WLANs compared to open non-PMF WLANs**

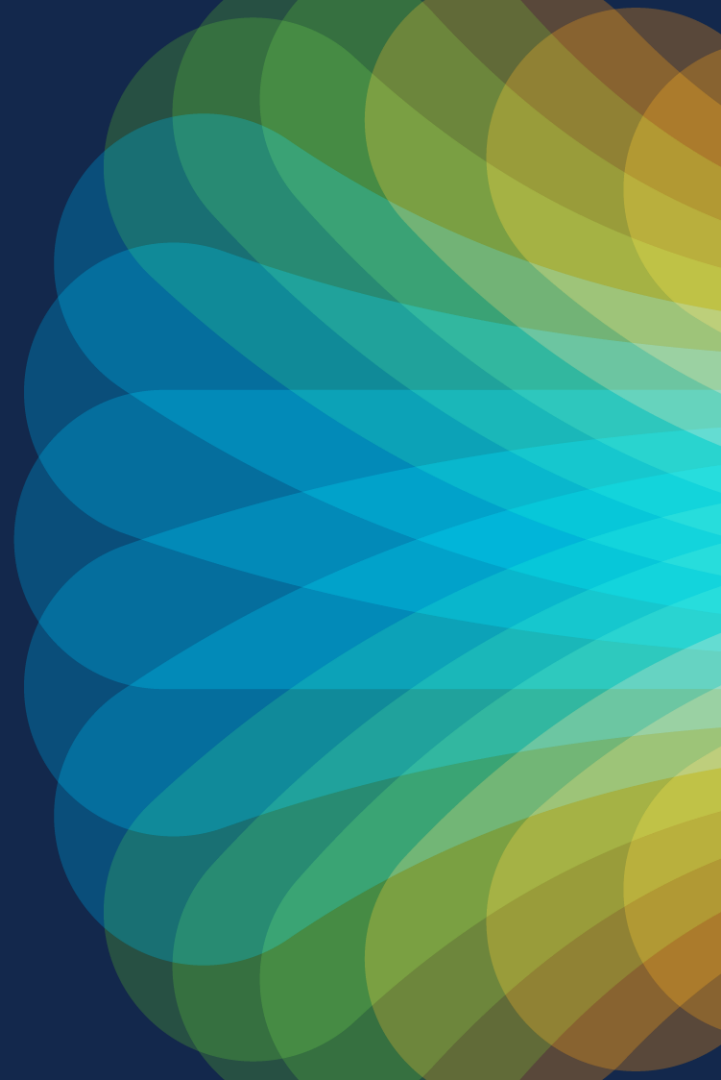
Solution

- ❑ Provide support to **STOP** threat actors from abusing PMF feature
- ❑ Faster Rogue detection is enabled
- ❑ **CONTAIN** clients from joining rogue PMF WLANs

PMF Containment only supports on serving channel
with AP in Local Mode

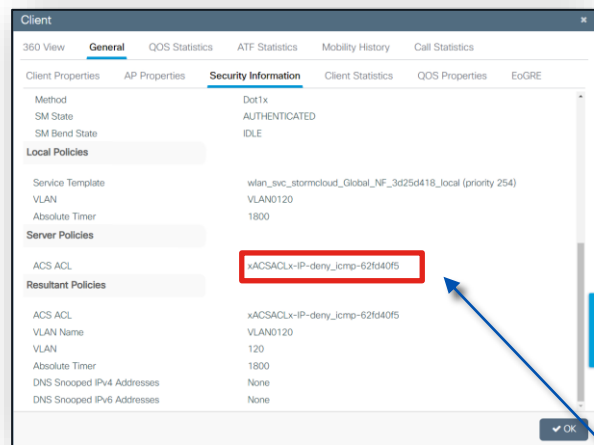
Supported AP Platforms: 9130, 9136, 916x (9166, 9164,
9162 or later)

C9800 dACL



C9800 Download ACL

dACLs are downloaded on the WLC and applied when client connects



dACLs



Supported on Centrally switched SSIDs

Not Supported on EWC Platforms

C9800-CL/C9800-L/C9800-40



128 ACLs
128 ACEs

C9800-80



256 ACLs
256 ACEs

VRF support and Overlapping IP Address

L3 Access in Wireless

Network Simplification & Security

1 Segmentation For Security

- Macro Segmentation with VRF Support
- Support for Overlapping IP
- Flexible routing to services

Managed Service Providers :

- Airports
- Multi-dwelling units

2 Optimized Network Design

- Less constraints on AGGR switch (ARP, MAC tables)
- Better load balancing and high availability with ECMP
- L3 routing based faster network reconvergence

3 Cloud Integration

- Enabling centralized data switching in L3 only networks
- Public cloud integration :
 - AWS
 - GCP
 - Azure

VRF support & L3 Access – 17.12.1

Splitting the control plane and data plane into multiple segregated instances with in single C9800

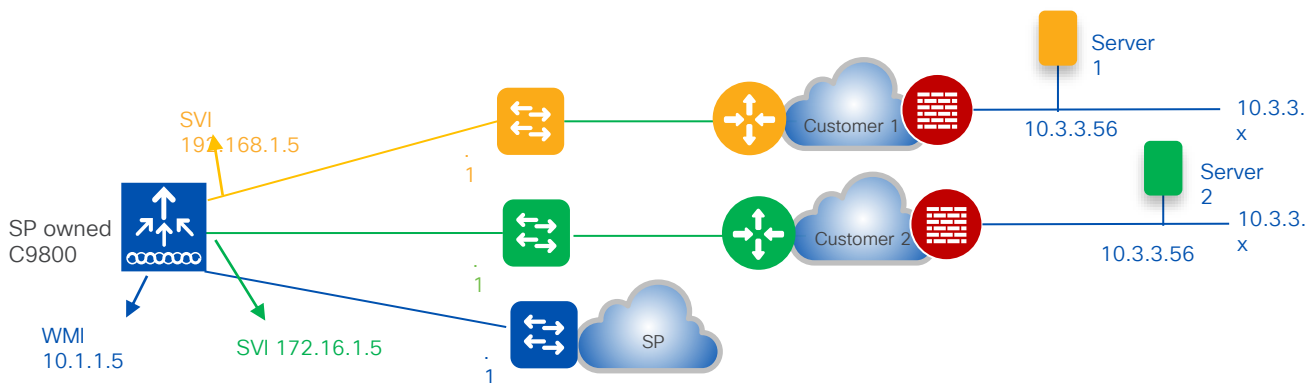


(*) IP overlapping in Flex Local switching is supported from 17.4.1 with different site tags

C9800 L3 Access: Flexible Routing to Services

Use case:

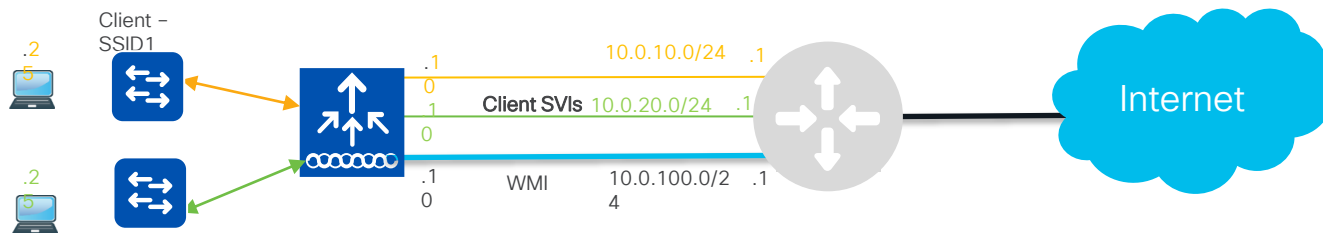
- SP owned C9800. Different customer networks (no routing between these networks)
- Overlapping IP on customer Services' side
- Example: AAA traffic from customer 1 to go to server 1 out of SVI 1, from customer 2 to go to server 2 out of SVI2. Could be same for DHCP



C9800 L3 Access: Macro Segmentation

Use case:

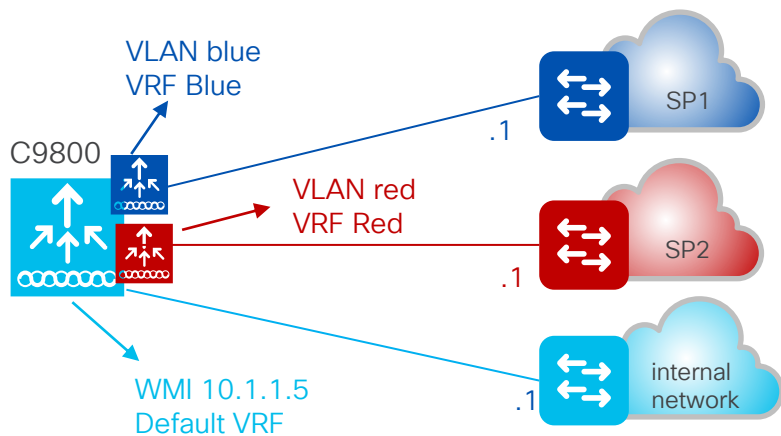
- Customer configures SVI on client VLANs (not for routing but for DHCP relay with option 82)
- The interface SVI is completely opened, no security to block traffic
- Preventing clients from “jumping” between VLANs



C9800 L3 Access: Client Overlapping IPs

IP-overlapping use case:

- Multi-dwelling facility (e.g., airport). C9800-based network is part of the infrastructure service
- Each customer/tenant gets an SSID, and traffic is offloaded to a different SP
- No control on SP network and IP assignment > need support for client overlapping IP address



Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 3 Clients

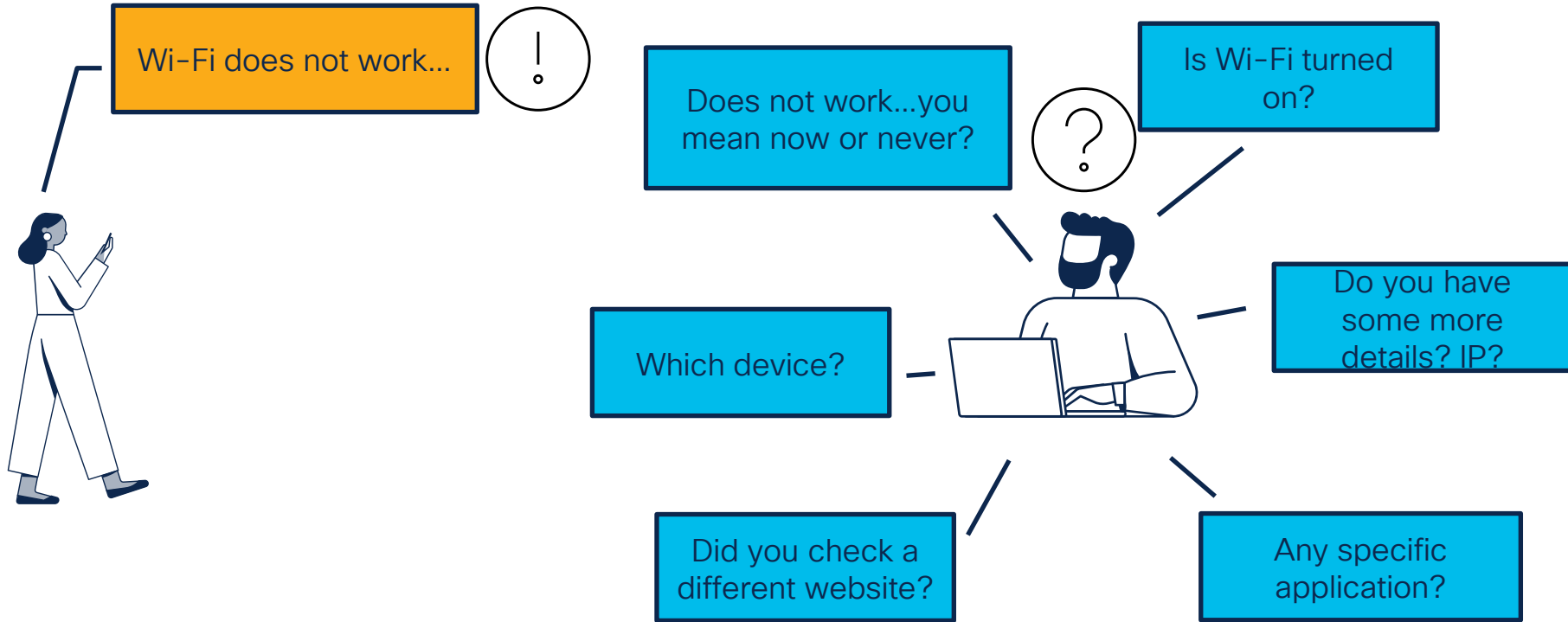
☐	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID
☐	1831.bf57.3e45	172.16.33.254	N/A	C9120-VIM-1	1	VRF-red	3
☐	4ced.fb3a.d9fe	172.16.33.254	fe80::38fb:1ae8:48d3:1e96	C9120-SJ-1	1	VRF-blue	2

- With VRF support, this would result in IP theft
- Pure bridging on C9800, no need for client SVI

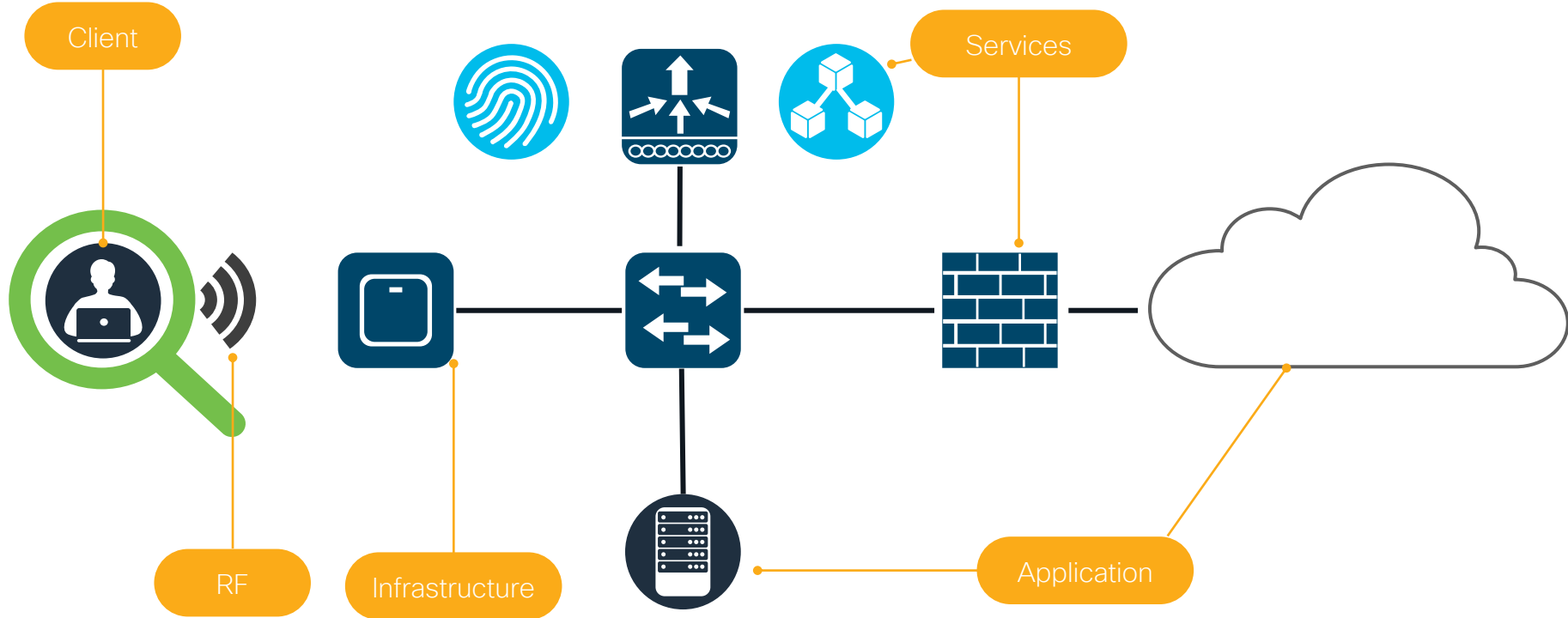


Monitoring and Troubleshooting

The typical user ticket if a Wi-Fi device is involved...



Context and Visibility required to make Wi-Fi great...



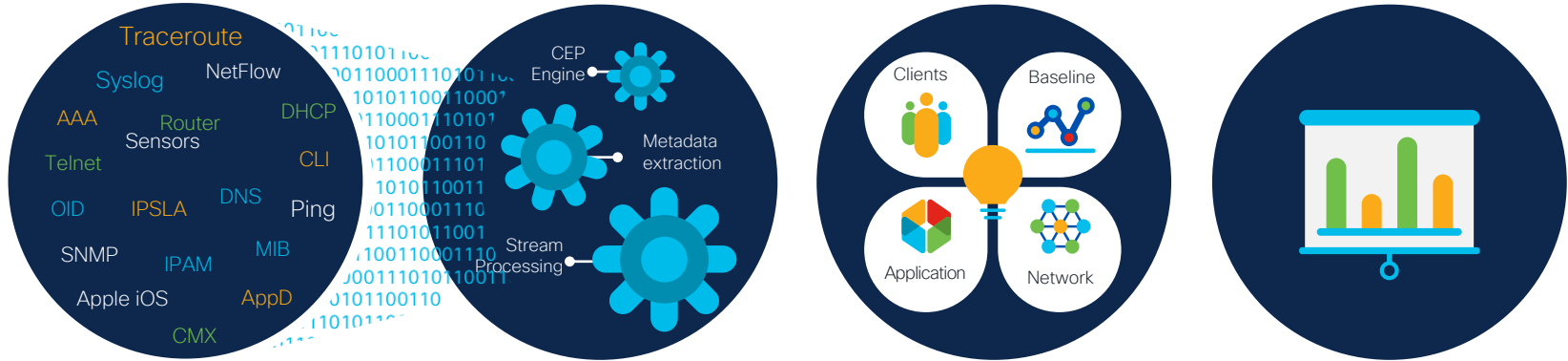
AIOps Turns Raw Data to Insights

Raw Network
Telemetry

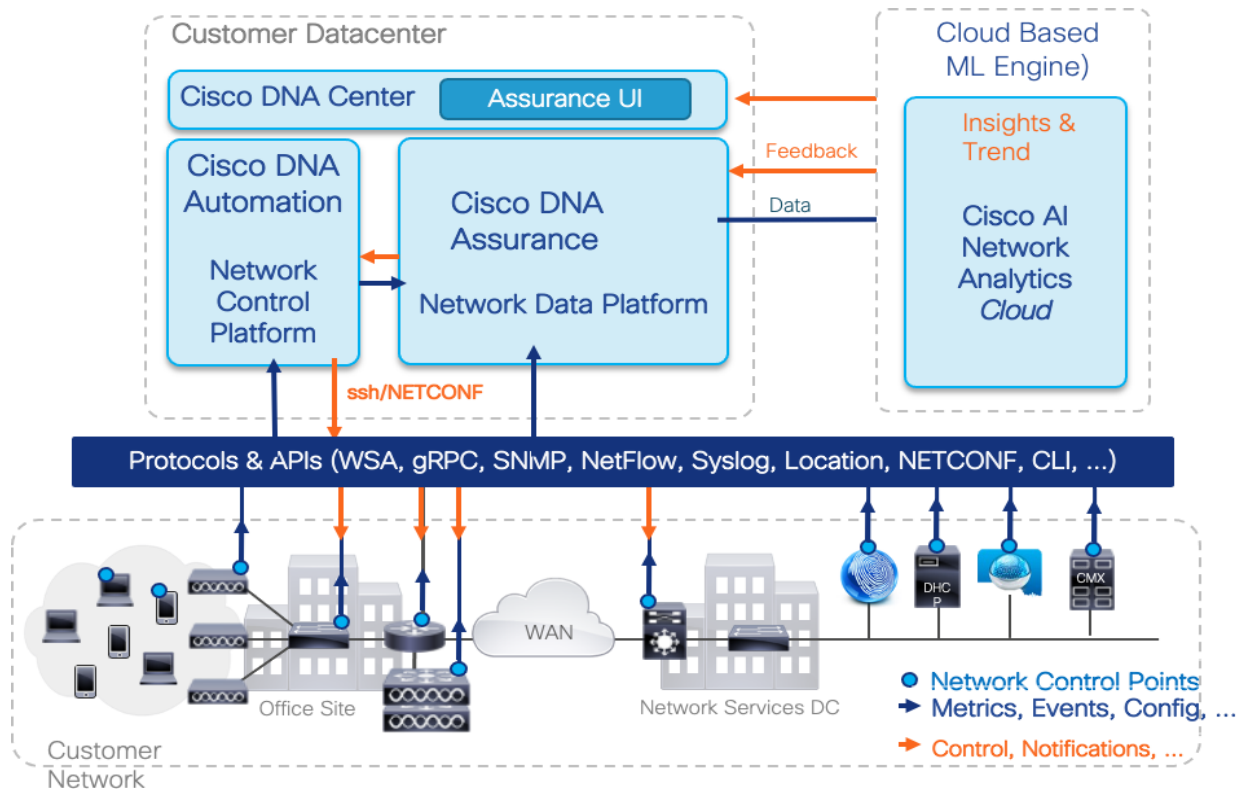
Data
Processing

Health Scores
and Insights

Monitor and
Troubleshoot



Cisco Catalyst Center (formerly Cisco DNA Center) AIOps Architecture



Serviceability

Contents of the debug bundle

RA Traces

- This collects and captures both RA traces(debug level) and internal RA for the configured clients

Client detail

- Show tech wireless client MAC of two instances, one before RA trace is enabled and once after RA trace is stopped are captured

Packet Capture

- Packet captures at the WLC control plane is collected for the clients

AP Archive

- Debugs pertaining to chosen clients collected at the APs at site level

Ease of debugging

Traces available at AP level

Objective:

For any client issue, we should be able to provide a simple way to fetch the important debug data at the time of event in a single command from all involved entities which can facilitate in triaging and troubleshooting the issue quickly

Solution: Client Debug Bundle (At AP Level)

- I. Pre-17.12.1, the Client Debug Bundle was available from WLC which allows the users to enable the RA traces/EPC and AP Archive from the WLC for the max of 5 Clients
- II. Now, starting from 17.12.1, we have option to enable the debugs directly in the AP for individual Client, multiple Clients or All the Clients associated to the AP
- III. In this version, 4 types of debug log levels are available (critical, debug, error and verbose)

Commands to trigger the debug bundle

1

Start the debug bundle

Choose the clients

```
AP# debug client-bundle start <level> <MAC Addr or all>
```

2

Trigger the test

RUN THE REQUIRED TEST

3

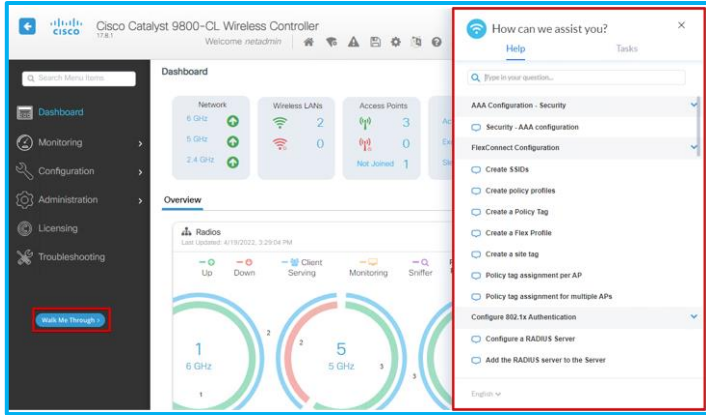
Stop the debug bundle

Choose the clients

```
AP# debug client-bundle stop <MAC Addr or all>
```

Levels Supported: Critical/Error/Debug/Verbose

WalkMe Assistance



Chrome

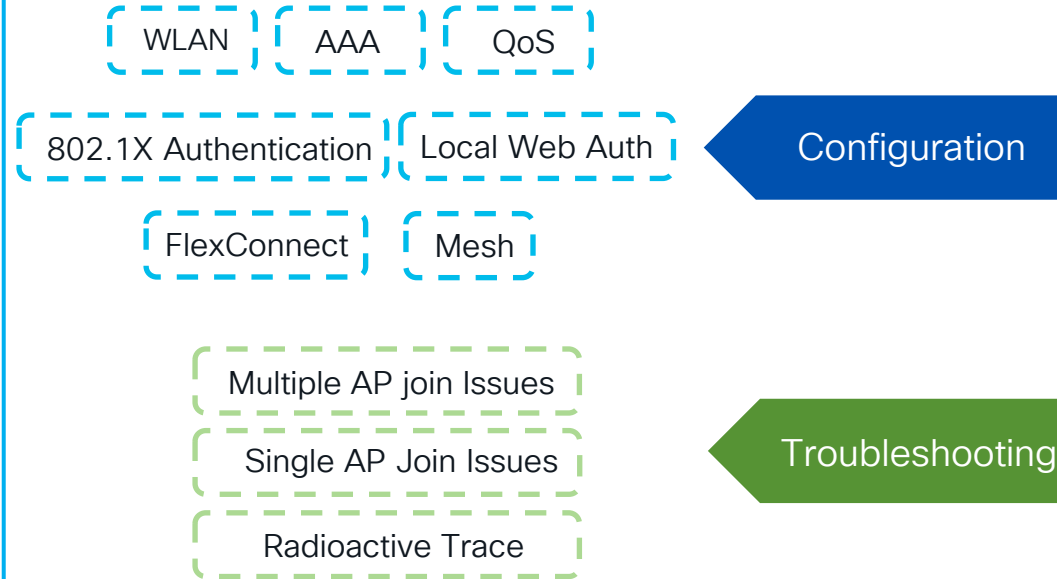
Firefox

Safari

Integrated in Client Browser

Enable/Disable on the Controller GUI

WalkMe extension is needed for Firefox and Safari



Wireless Network Automation

Wireless Automation Update 2.3.7.x

AIOps

Event Analytics

RAS (Reliability, Accessibility and Scalability) Quality Improvements

Additional RF Insights in ICAP

MacBook Analytics

Log collection MRE in Client & AP 360

Issue and AP-360 chart improvements

Support for 3k+ NBAR cloud applications

Design (2.3.7 P2)

AI-Enhanced RRM for Assurance only users

Per Device Configuration (EFT)

NetOps

Rogue PMF Containment & improved detection

Country Code changes on 17.12

Mesh support with SDA

AP pre-image download progress visibility

ISE Sync Status visibility

SSID & profile Config completion

Reuse policy tags across sites

AP join profile Rogue Parameters

Platform

Support of **CW9166D1 APs**

Ultra low end 9800-CL Support

Catalyst Center Virtual Appliance on ESXi

Flexible reporting - add PoE and operator-based filtering support

Per Device Configuration

Simplification of Wireless Automation for Catalyst Center



Several Prime Wireless customers are not on Catalyst Center

*With Prime EOS announcement, Catalyst Center wireless automation must provide a **robust brownfield WLC config learn method** and improve overall quality and **extent of wireless configurations** supported*



Active Catalyst Center Wireless customers are not using Wireless Automation

*Existing wireless customers should get more **value from Catalyst Center**; configuration and automation flows need to be simplified and improved*

Top Priorities



Feature Parity
between Device
and Catalyst Center

Robust WLC
config learn
method

*Automation designs
are aligned across
Wired and Wireless*

More **visibility** and
easy **scalability** for
configuration
Automation

*Improve network
automation design*

*Increase
Automation feature
velocity & agility to
simplify integration
of **ongoing WLC**
config changes on
Catalyst Center UI
(release after
release)*

These **overall priorities** are intended to guide Cisco Wireless and Catalyst Center on our phased journey to improve Campus Wireless Automation overall

Wireless Automation Improvements to be done in Phases

With Phase 1 / MVP, this will serve as an alternate and simplified way to do **wireless automation**; present wireless automation workflows are not going away

Phase 1*

Per Device Configuration

- **MVP** will focus on achieving **full wireless configuration** functionality (C9800 WebUI & Prime UI parity) for customers to onboard and manage WLCs at a **per device level**
- Primary focus will be on **onboarding brownfield WLCs** and managing Day 0 – Day N configs through Catalyst Center at a per WLC level
- Design is intended to increase **Automation feature velocity**, in order to simplify integration of forward looking WLC config changes also on Catalyst Center UI (release after release)
- Solution will deliver a **unified UX experience** across switching & wireless on Catalyst Center and is intended to simplify overall wireless automation



Phase 2* & Beyond

- **Phase 2** will focus on bringing wireless automation configurability for multiple WLCs, across multiple wireless networks, all at once
- Configuration of wireless automation through **Catalyst Center at scale** is a primary use case that needs to be solved
- Planning for alignment across Catalyst Center Wired, Wireless and Meraki

Per Device Config Demo



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Software Image Management

Challenge

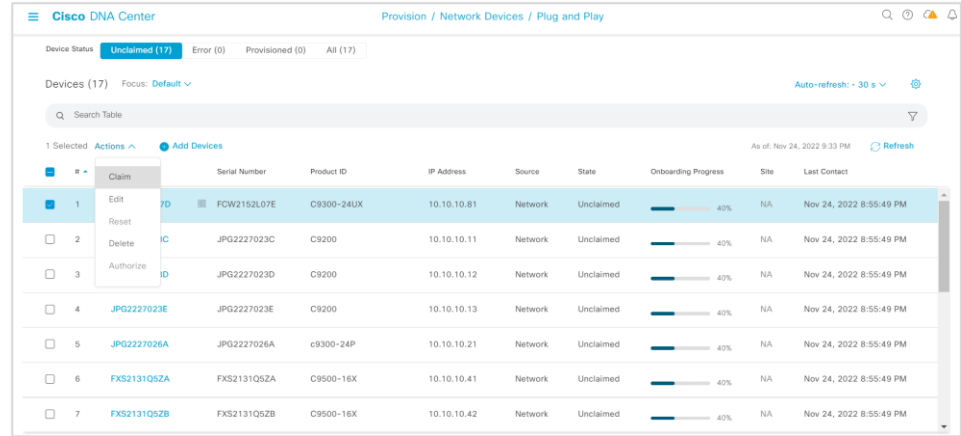
Network administrators want manage software upgrades and controls the consistency of image versions and configurations across the network.

Use Case

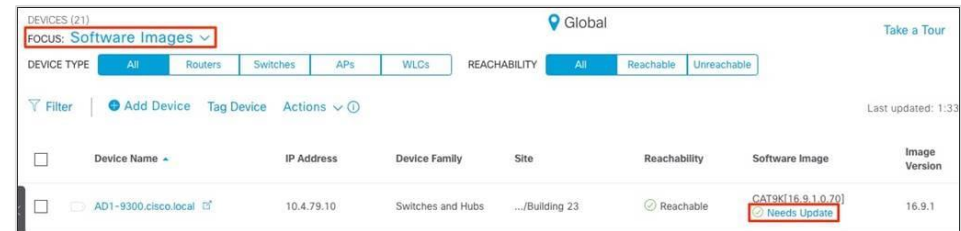
Using Software image management, admin upgrades any device that's not on a recommended image version

Details

- Golden Image based workflows drive software consistency
- Pre/Post check ensures that software updates do not have adverse effects on the network
- Patching provides small updates to react quickly to security fixes



#	Serial Number	Product ID	IP Address	Source	State	Onboarding Progress	Site	Last Contact
1	FCW2152L07E	C9300-24UX	10.10.10.81	Network	Unclaimed	40%	NA	Nov 24, 2022 8:55:49 PM
2	JPG2227023C	C9200	10.10.10.11	Network	Unclaimed	40%	NA	Nov 24, 2022 8:55:49 PM
3	JPG2227023D	C9200	10.10.10.12	Network	Unclaimed	40%	NA	Nov 24, 2022 8:55:49 PM
4	JPG2227023E	C9200	10.10.10.13	Network	Unclaimed	40%	NA	Nov 24, 2022 8:55:49 PM
5	JPG2227026A	c9300-24P	10.10.10.21	Network	Unclaimed	40%	NA	Nov 24, 2022 8:55:49 PM
6	FXS2131Q5ZA	C9500-16X	10.10.10.41	Network	Unclaimed	40%	NA	Nov 24, 2022 8:55:49 PM
7	FXS2131Q5ZB	C9500-16X	10.10.10.42	Network	Unclaimed	40%	NA	Nov 24, 2022 8:55:49 PM



Device Name	IP Address	Device Family	Site	Reachability	Software Image	Image Version
AD1-9300.cisco.local	10.4.79.10	Switches and Hubs	.../Building 23	Reachable	CAT9K16.9.1.0.70	16.9.1

Wi-Fi 6/6E Readiness

Challenge

Network administrators want to know if their network needs an upgrade to new wireless technology

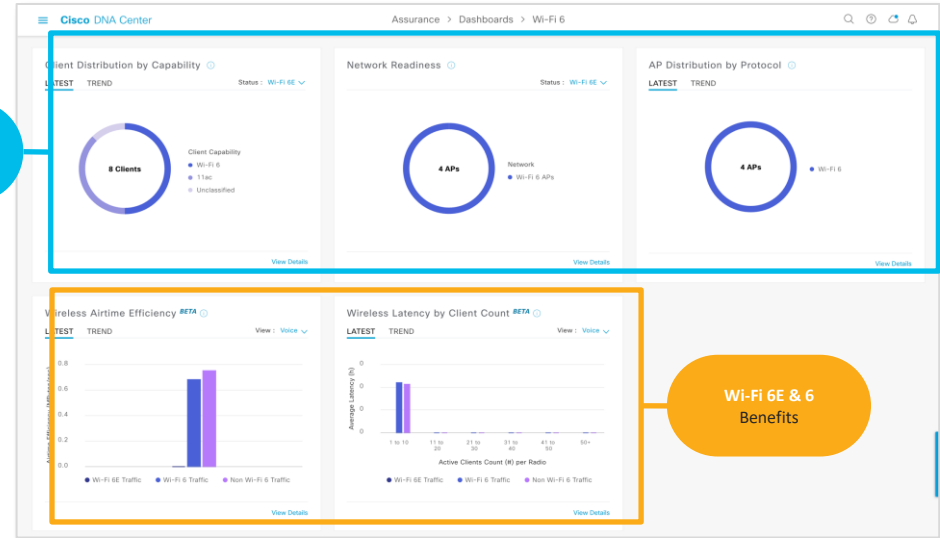
Use Case

Wi-Fi 6/6E dashboard provides insights into what infra level upgrade is needed to enable the new wireless technology in the network.

Details

- Wi-Fi 6/6E readiness by showing number of newer Wi-Fi 6/6E clients in the network
- In a mix environment, visualize the benefits of Wi-Fi 6E over Wi-Fi 5 or older

Wi-Fi 6E & 6
Readiness



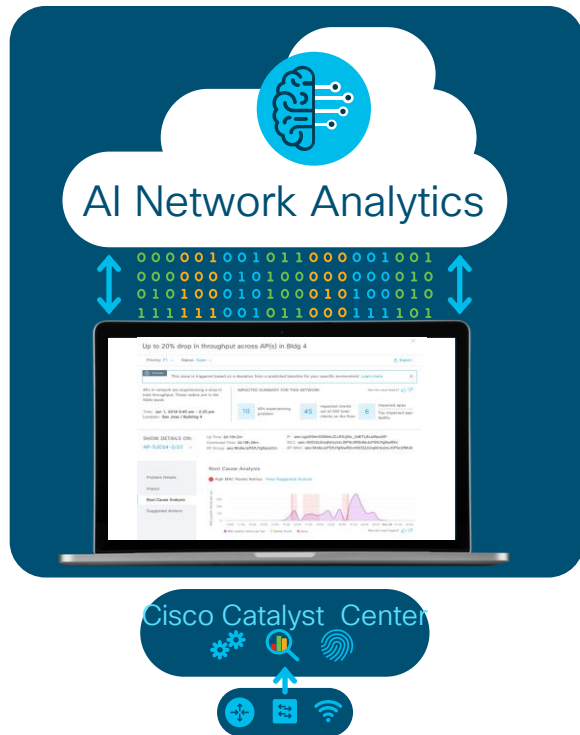
Wi-Fi 6E & 6
Benefits

Optimization using AI/ML



Cisco AI Network Analytics

Machine learning makes Cisco Catalyst Center Assurance smarter



Visibility: Personalized baselining

Intelligently define personalized "network normal" using unified global telemetry collected

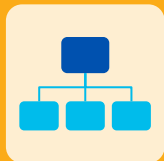
NEW



Insight: Intelligent data analysis

Increase signal to noise, reduce false positives, and accurately identify trends and root causes.

NEW



Action: Accelerated remediation

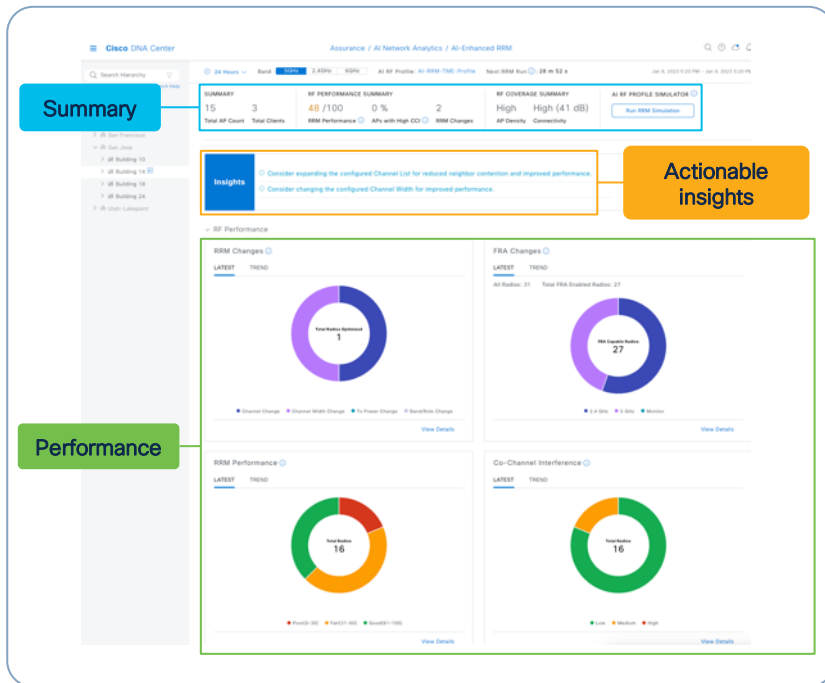
Create automated resolution options for IT to act on based on machine reasoning algorithms.

NEW

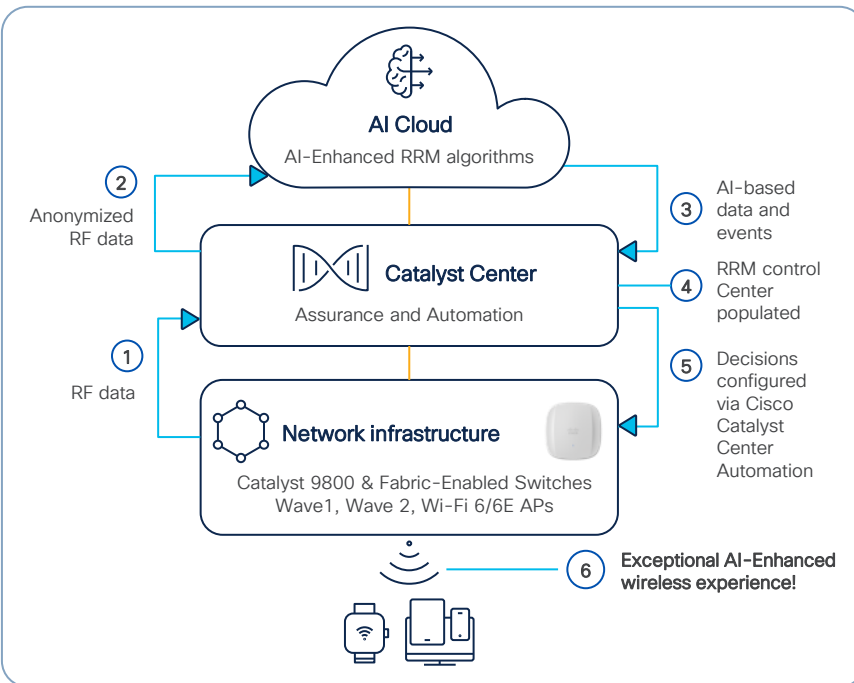
AI-Enhanced RRM is AI that Powers RF Optimization

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

Instantaneous visibility



Proactive optimizations



AI-Enhanced RRM key customer benefits

Better RF, better insights, reduced operational costs and time

AI-driven self-optimizing RF

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



Measured Improvements in RF KPIs!

- CCI Reduction: Up to 40%
- SNR Downlink Gain: Up to 7 dB
- RRM Changes Reduction: Up to 75% at busy hours

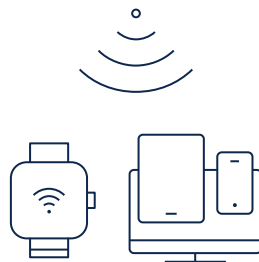
Performance visibility

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



Complete historical context

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



Actionable insights

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

Simplified RRM configuration

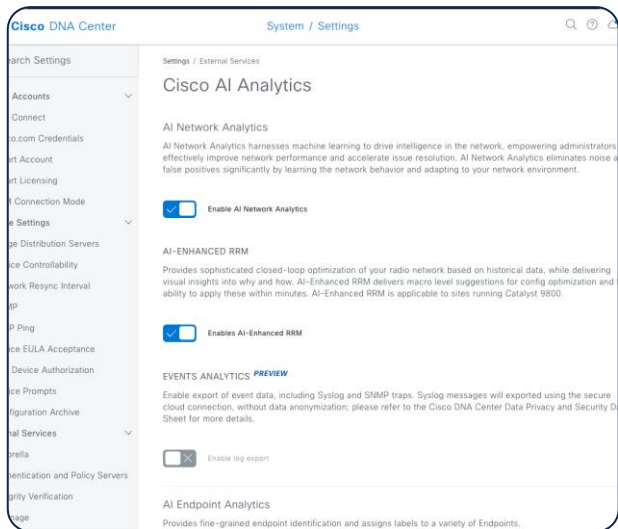
Complicated traditional RRM configurations are simplified, with policy toggles and thresholds.

Enabling AI-Enhanced RRM for Provisioning-Enabled Deployments

Traditionally, this solutions requires customers to manage their Catalyst 9800 configurations through Catalyst Center's Network Settings

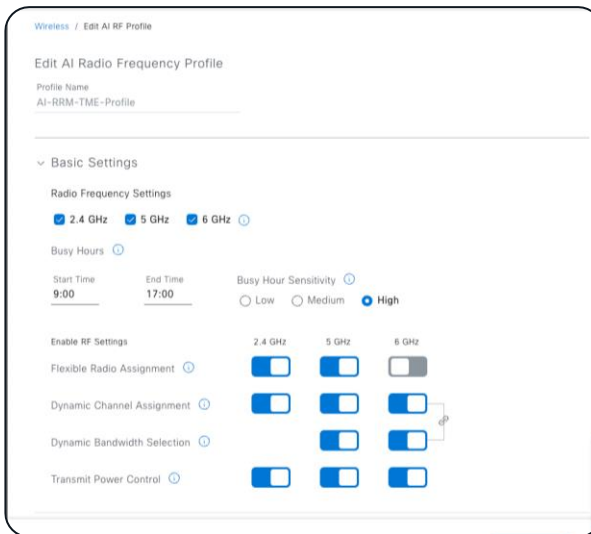
1

Give AI-Enhanced RRM
Cloud Access in Settings.



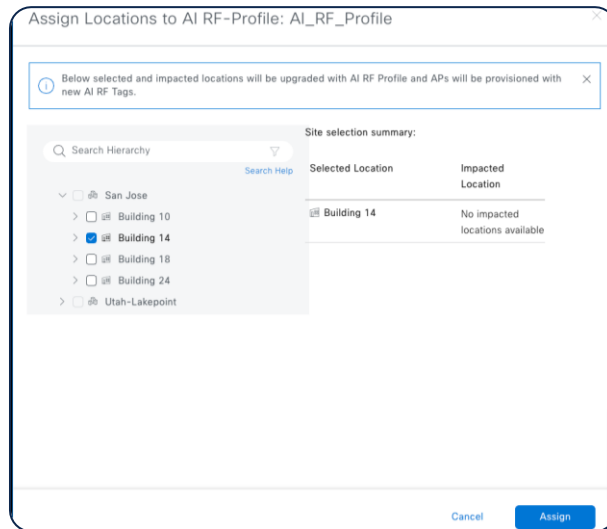
2

Create an AI RF Profile.



3

Assign AI RF Profile to a building,
and **provision** your C9800 & APs.





Design >

Policy >

Provision >

Assurance >

Workflows >

Tools >

Platform >

Explore

Requirements have not been met. [Learn more.](#)

Value from your Cisco DNA Center with the adoption journey map.

Feature adoption with simplicity and time to value, as you guide your organization on its digital transformation center.



100%

Wireless Clients

--%

Wired Clients

[View Details](#)

Critical Issues

Last 24 Hours

1

P1

23

P2

[View Details](#)

Trends and Insights

Last 30 Days

0

AP Performance
Advisories

0

Trend Deviations

[View Details](#)

Software and Hardware Support Matrix

for AI-Enhanced RRM's Workflow for Assurance-Only Deployments

Cisco IOS XE WLC Software	Cisco Catalyst Center Software and Licensing
17.9.3 or newer (17.12.1 recommended)	2.3.7.4 (Patch 2) with DNA Advantage License
Cisco Access Point Hardware	
Wave 1, Wave 2, Catalyst Wi-Fi 6 and 6E Access Points	
Cisco IOS XE WLC Hardware	
C9800-CL	
C9800-L	
C9800-40	
C9800-80	

Wireless Product Analytics

Wireless Product Analytics

Knowing usage to serve customers better

Product Decisions for Customer benefit



- SW version, feature & scale usage
- New APs on better software release for ease of use
- Continued product and feature improvements

Better Product Experiences for Customers



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

Wireless Product Analytics (FAQs)



- Release Notes (Existing)
- Product Analytics FAQ (New)



Product Analytics is present on 17.9 train and 17.12 train but turned off.

Plan to turn on in future



The data collected is non-PII data .

CLI's present to view the report collected/ sent for transparency



Plan is to send first Product Analytics 7 days after upgrades



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



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

Customer can turn on using command “pae” in 17.9.4 and 17.12.1

Cloud Monitoring for C9800

Cloud Monitoring for Catalyst Wireless

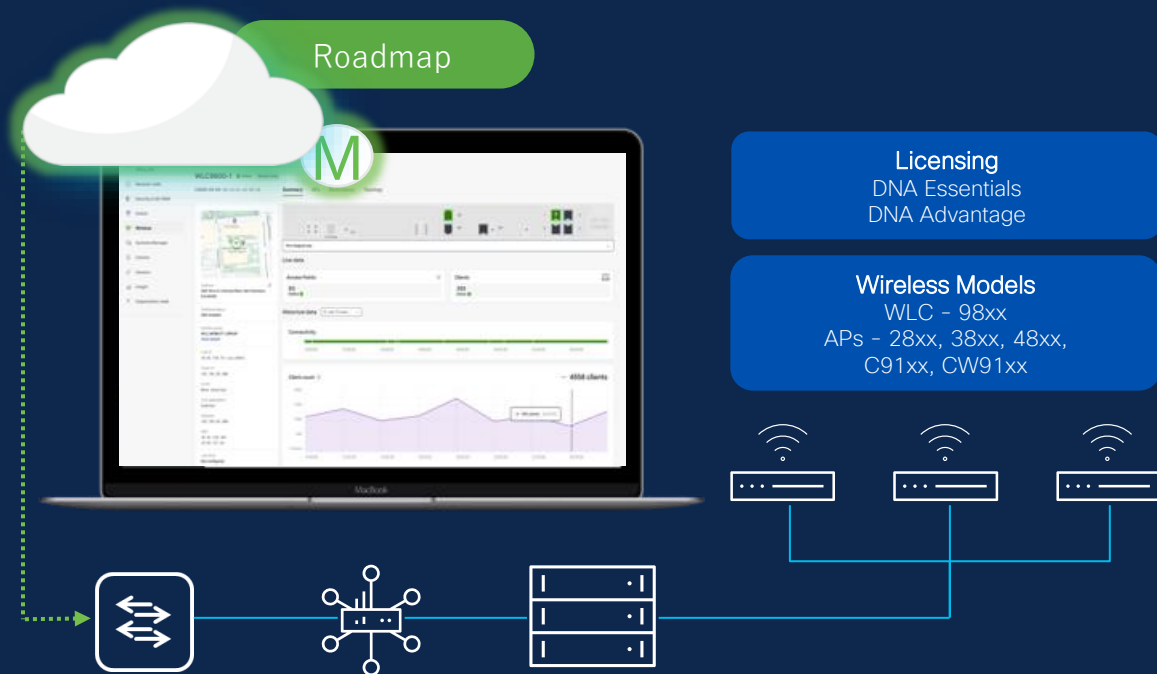
On-premise functionality in the cloud | Deployed & monitored by you



Unified view of Cisco
Wireless Infrastructure

Device Health and
Troubleshooting

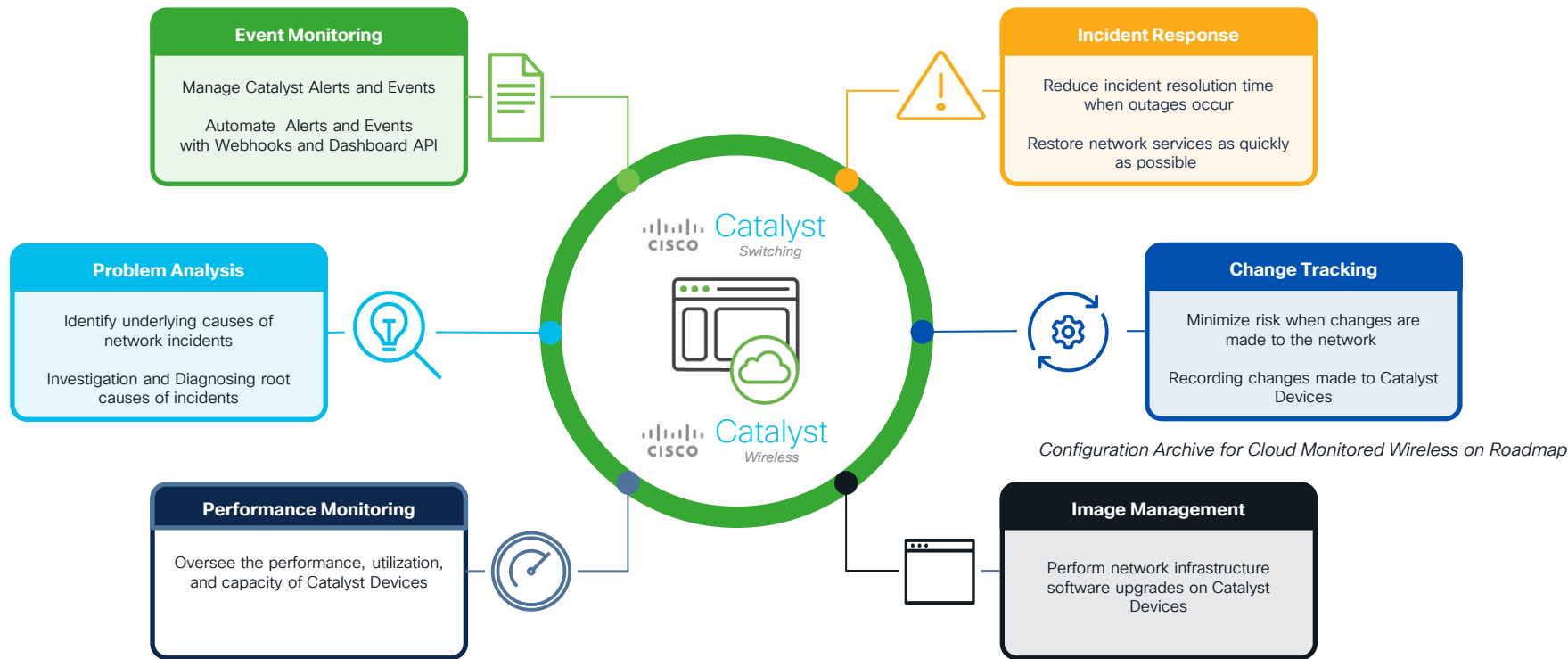
Network Client and
Traffic Information



Licensing
DNA Essentials
DNA Advantage

Wireless Models
WLC - 98xx
APs - 28xx, 38xx, 48xx,
C91xx, CW91xx

Simplify Catalyst Network Operations



Configuration Archive for Cloud Monitored Wireless on Roadmap

Image management for Cloud Monitored Wireless on Roadmap

Capabilities at Launch

Centralized view of entire network

Visibility into Meraki devices and Cisco Catalyst Networks from one Dashboard

Onboard Controllers and Access Points with Single Command

Automatic Access Point Registration and Network Assignment

Per Controller Access Point Mapping Rules: How do you want access points placed into Dashboard Networks

Onboarding

Live Status: See Live Access Points and Client Counts on your Controller

HA SSO Health: See the status of your standby unit and overall system health

Performance Health: Track historical CPU and Memory Utilization, Client Load, and Ports and Interfaces status and traffic statistics

Wireless Controller Operations

Remote monitoring

Identifying and Troubleshoot issues, even from thousands of miles away

Live View of Associated Clients and Radio Channel Utilization

Monitor Live RF Settings including Current Channel and Power Settings

Visualize your access point placements with Maps & floor plans

Access Point Operations

Client Layer 7 Visibility: Enable NetFlow to view detailed client application usage

Client Connection Health: See the health of wireless connections across the entire network

Client Performance Health: View Latency, Packet loss and SNR of the client devices

Client and Application Operations

Access Points

Wi-Fi 6E

C9136
CW9166I/D1
CW9164
CW9163
CW9162

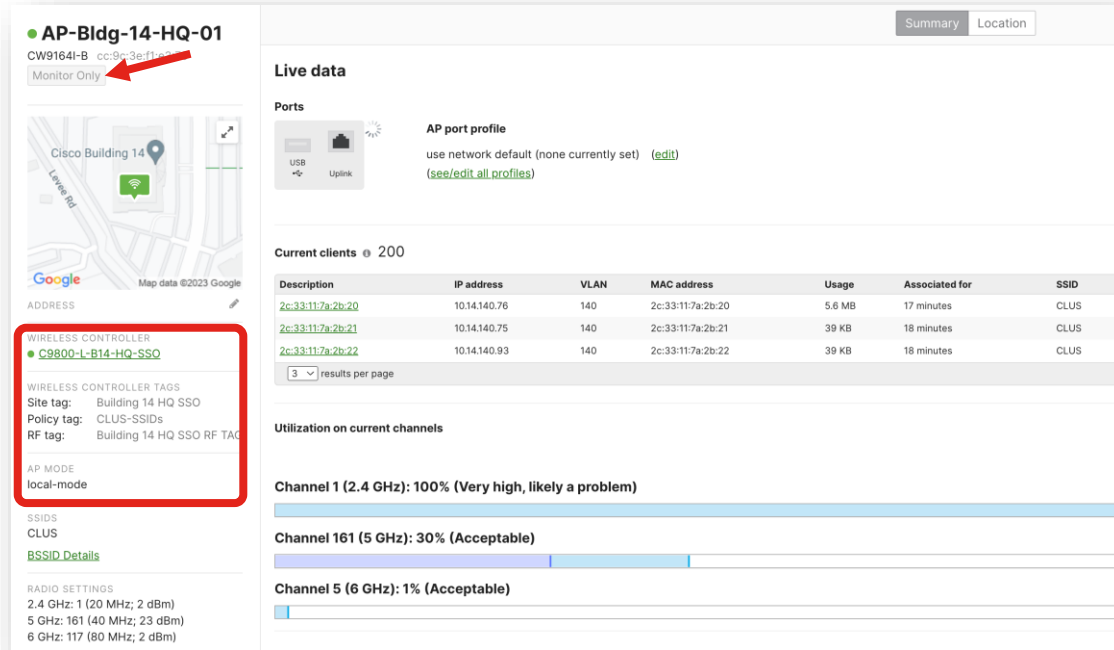
Wi-Fi 6

C9130
C9124
C9120
C9117
C9115
C9105

Wave 2

AP4800
AP3800
AP2800

IOS-XE 17.12.3 / 17.15.1



AP-Bldg-14-HQ-01
CW9164I-B cc:9c3ef1a3
[Monitor Only](#)

Live data

Ports

AP port profile
use network default (none currently set) [\(edit\)](#)
[\(see/edit all profiles\)](#)

Current clients 200

Description	IP address	VLAN	MAC address	Usage	Associated for	SSID
2c:33:11:7a:2b:20	10.14.140.76	140	2c:33:11:7a:2b:20	5.6 MB	17 minutes	CLUS
2c:33:11:7a:2b:21	10.14.140.75	140	2c:33:11:7a:2b:21	39 KB	18 minutes	CLUS
2c:33:11:7a:2b:22	10.14.140.93	140	2c:33:11:7a:2b:22	39 KB	18 minutes	CLUS

3 results per page

Utilization on current channels

Channel 1 (2.4 GHz): 100% (Very high, likely a problem)

Channel 161 (5 GHz): 30% (Acceptable)

Channel 5 (6 GHz): 1% (Acceptable)



Cisco Catalyst Full Stack Solution

Automate



Control



DNA Center
(appliance or VM)



vManage
(SDWAN/SASE)



Analyze



Cisco Spaces



ThousandEyes



vAnalytics

App Hosting
Platform APIs



Secure



ISE



ETA + Cisco Secure Analytics



Umbrella



Connect

Catalyst Switching



Catalyst Wireless



Catalyst Routing



- IOS-XE
- UPOE
- Custom ASICs
- Container App Hosting

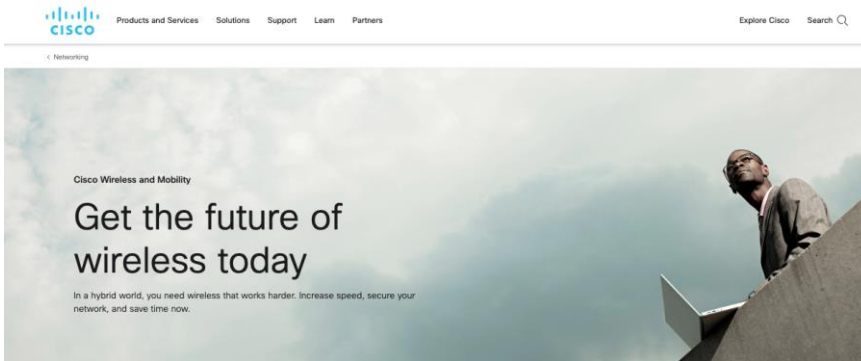
Catalyst 9000 and 8000 series : Switching | Wireless | Routing
Powered by best-in-class integrated networking hardware and software

More info?

Where can I find more info?

Wireless and Mobility page on CCO:

<https://www.cisco.com/c/en/us/products/wireless/index.html>



Other links on CCO:

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

Cisco Networking Bot

Cisco Networking Bot



Switching

The Cisco Catalyst family of campus LAN switches, including the Catalyst 9000 Series, delivers a connected environment that's always-on, always-secure, and intuitive to manage.



Wireless

Cisco Wireless LAN Controllers and Access Points, including the Catalyst 9800 Series and Catalyst 9100 APs, create a best-in-class wireless experience for your evolving and growing organization.



Cisco DNA Center

A powerful network controller and management dashboard and also includes Software-Defined Access that delivers policy-based network automation from the edge to the cloud.



Routing

Cisco Routers, including small business, branch, edge, enterprise, and virtual routers, seamlessly and securely connect applications across your cloud, data center, and edge locations.



Software-Defined WAN

A SASE-enabled architecture that connects any user to any application with integrated capabilities for multicloud, security, unified communications, and application optimization.



Identity Services Engine

Cisco Identity Services Engine (ISE) enables a dynamic and automated approach to policy enforcement that simplifies the delivery of highly secure network access control.



Industrial Internet of Things

Industrial IoT is an ecosystem of devices, sensors, applications, and associated networking equipment that work together to collect, monitor, and analyze data from industrial operations, increases visibility and enhances troubleshooting and maintenance capabilities. It can also increase efficiencies, reduce costs, and improve safety and security.



Solution Engineering

Solutions Engineering org is responsible for validating and delivering high quality outcome-based solutions and providing delightful adoption experience for Enterprise Customers.

cnb.cisco.com

Release Information

- ❖ Release recommendation for all Enterprise products/solutions.
- ❖ Release Cadence / Timing for IOS-XE releases
- ❖ SMU details

EoL/EoS

- ❖ EoL/EoS for Software releases
- ❖ EoL/EoS for Hardware products

Migration/Onboarding Help

- ❖ AireOS to C9800 Migration
- ❖ DNA Center Onboarding
- ❖ Prime Infrastructure to DNA Center Migration
- ❖ Wireless UDN Deployment
- ❖ CMX to DNA Spaces Migration

Product Adoption

- ❖ Configuration Guides
- ❖ Troubleshooting Guides
- ❖ Software Upgrades (Cat9k, ISE, DNAC, Wireless, Routing)
- ❖ Tools Repository

Hardware-Software Matrix

- ❖ Hardware Matrix
- ❖ Software Feature Navigator
- ❖ Compatibility Matrix across all Enterprise products/solutions

Security Advisories (PSIRTs)

- ❖ Search by CVE ID /Advisory ID
- ❖ Search by Bug ID
- ❖ Search by IOS/IOS-XE release
- ❖ Search by Product

CISCO *Live!*

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are overlapping, wavy bands of color in shades of orange, red, and yellow. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC

Configuration Migration Tool

Configuration Migration Tool

Migration Tool output:

Converted Config Lines

Translated Config

Translated (CLI supported in IOS-XE)

Unsupported Config

Unsupported (CLI not supported in IOS-XE)

Not Applicable Config

Not Applicable (CLI deprecated/not used commands)

Unmap Config

Unmapped (CLI supported but not yet translated)

CLI = Command Line Interface

Configuration Migration Tool

Migration Tool output:

Converted Config Lines

Translated Config

Unsupported Config

Not Applicable Config

Unmap Config

Converted Config Lines

Translated Config

```
!% Note: 1: Lines start with prefix '!' need to be taken care before applying to C9800.  
!% 2: Lines start with prefix '!' have note and sample examples, about feature and steps to follow.  
!% 3: 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
```

- 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:

Converted Config Lines

Translated Config

Unsupported Config

Not Applicable Config

Unmap Config

```

!! 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

Configuration Migration Tool

Migration Tool output:

Converted Config Lines

Translated Config

Unsupported Config

Not Applicable Config

Unmap Config

Unsupported (CLI not supported in IOS-XE)

Unsupported Config

```
config 802.11b cleanair alarm unclassified t
config advanced 802.11a ccx location-mea
config ap antenna monitoring all detection-
config ap antenna monitoring all rssi-failure
config ap antenna monitoring all weak-rssi
config ap cert-expiry-ignore ssc disable
config auth-list add sha256-lbs-ssc encryp
4b5827b5166cedaa5f3658f180b7faef3baa
config lag enable
config logging traceinfo disable debugging
config mdns policy service-group create de
config mdns policy service-group user-role
```

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

Configuration Migration Tool

Migration Tool output:

Converted Config Lines

Translated Config

Unsupported Config

Not Applicable Config

Unmap Config

Not Applicable (CLI deprecated/not used commands)



Cisco TAC Tool - WLC Config Converter

```
config radius fallback-test interval 900 -> "C9800 failover flow is different."
config remote-lan qos 12 platinum -> "CLI deprecated on controller (8500/5500/3500)"
config rfid mobility pango disable -> "RFid mobility is deprecated."
config spanningtree port mode off 1 -> "Spanning tree is not applicable in C9800."
config spanningtree port mode off 2 -> "Spanning tree is not applicable in C9800."
config spanningtree port mode off 3 -> "Spanning tree is not applicable in C9800."
config spanningtree port mode off 4 -> "Spanning tree is not applicable in C9800."
config spanningtree port mode off 5 -> "Spanning tree is not applicable in C9800."
```

Reason why CLI is not applicable

Configuration Migration – Steps

Step 1 – Upload AireOS in online tool



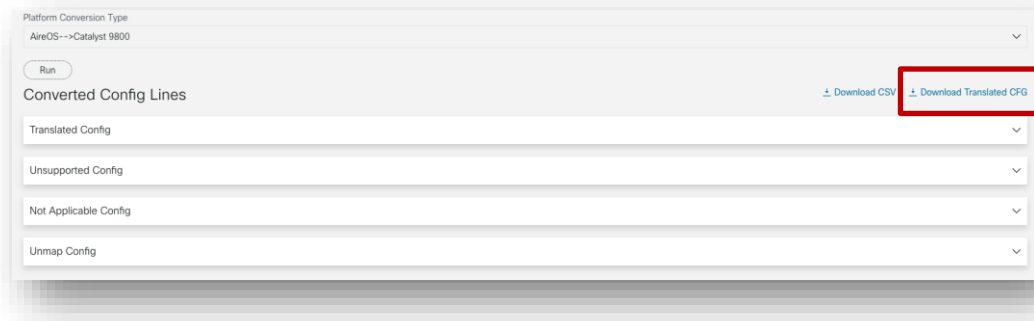
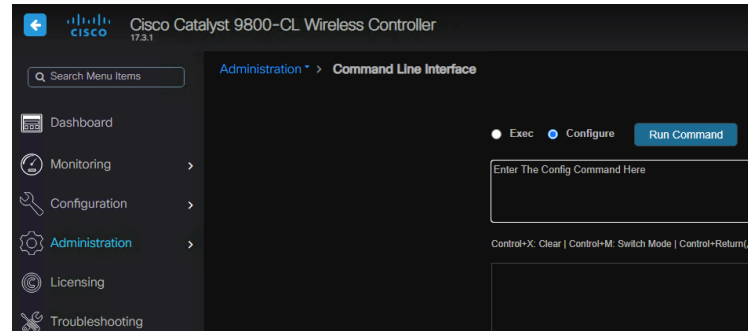
The screenshot shows the 'Cisco TAC Tool - WLC Config Converter' web interface. It includes a title bar with the Cisco logo and the tool name. Below is a section titled 'WLC Config Converter' with a description: 'Migrating wireless controllers to or from across any of these platforms: 2500/5500/7500/8500/WISM2/3650/3850/4500 S8E/5760/Catalyst 9800 controllers'. It lists instructions: 'Please upload the following: AireOS: "show run-config startup-commands" output or TFTP config backup; Converged Access: "show running-config" output'. A 'Details' tab is active, showing a text area for the configuration. A file named '5520_config.txt' (13.6 KB) is shown as uploaded. At the bottom, there is a 'Platform Conversion Type' dropdown set to 'AireOS-->Catalyst 9800' and a green 'Run' button.

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



AP Tags

AP to Tags assignment – Source: Static

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

Configuration > Wireless > Access Points

▼ All Access Points

Total APs : 6

AP Name	AP Model
C9130-SJ-1	C9130-K9
C9130-VIM	C9130-K9

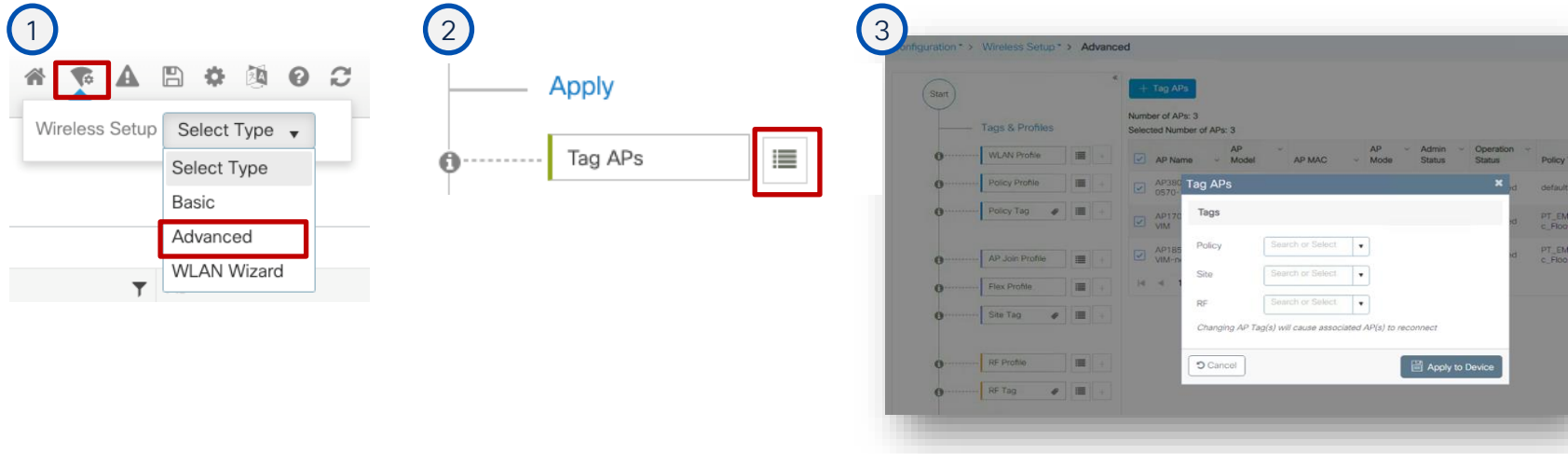
Edit AP

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

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

AP to Tags assignment – Source: Static

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



AP to Tags assignment – Source: Filter

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

Configuration > Tags & Profiles > Tags

Policy Site RF **AP**

Tag Source Static Location **Filter**

+ Add - Delete

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

1 10

Edit Tags

Rule Name* site1

AP name regex* .site1.

Active YES

Priority* 1

Policy Tag Name flex-tag

Site Tag Name site1

RF Tag Name default-rf-tag

- 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)

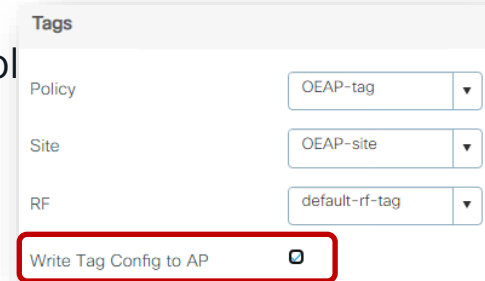
CAPWAP = Control and Provisioning of Wireless Access Points

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 sol
 - 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:

Configuration > Tags & Profiles > Tags

Policy Site RF **AP**

Tag Source Static Location Filter

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

ⓘ Drag and Drop Tag Sources to change priorities

Revalidate Tag Sources on APs ☐

Enable AP Tag Persistency ☒

Apply

- 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.



Reference

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



Reference

EoS/EoL Update – Access Points

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

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