

Migrando sua infraestrutura para Catalyst 9800



Flavio Correa, Technical Solutions Architect, CCIE #38913

Felipe Amorim, Solutions Architect, CCIE #52925

Join at
Slido.com
#573 021



Quantos anos de experiência você tem com Wi-Fi Cisco?

Agenda

- Conhecendo melhor o Catalyst 9800
- Planejando a migração
- Entendendo o IOS-XE Configuration Model
- Considerações de design
- Melhores práticas



Agenda

Catalyst 9800, Under the Hood

Planning for Your Migration

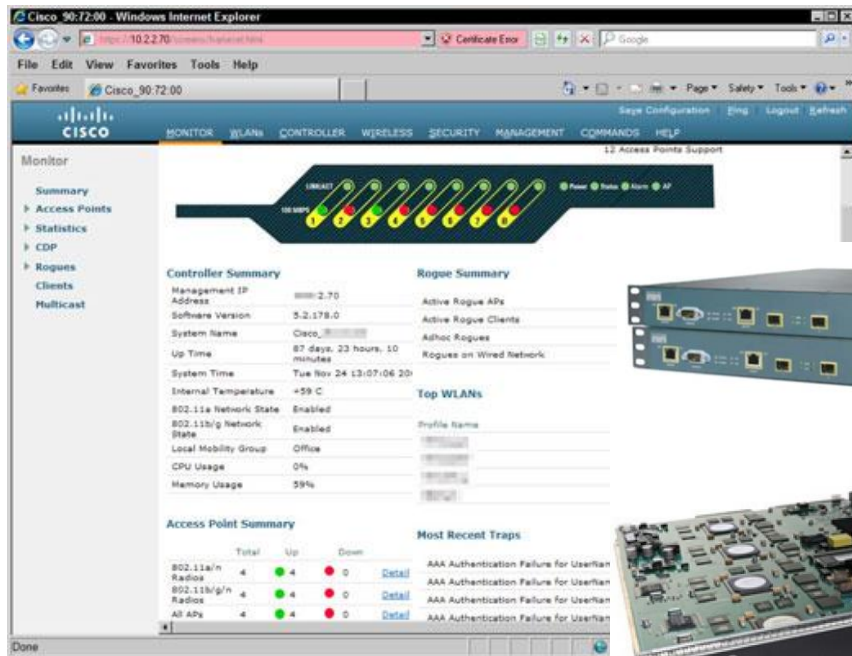
Understanding IOS-XE Configuration Model

Design Considerations

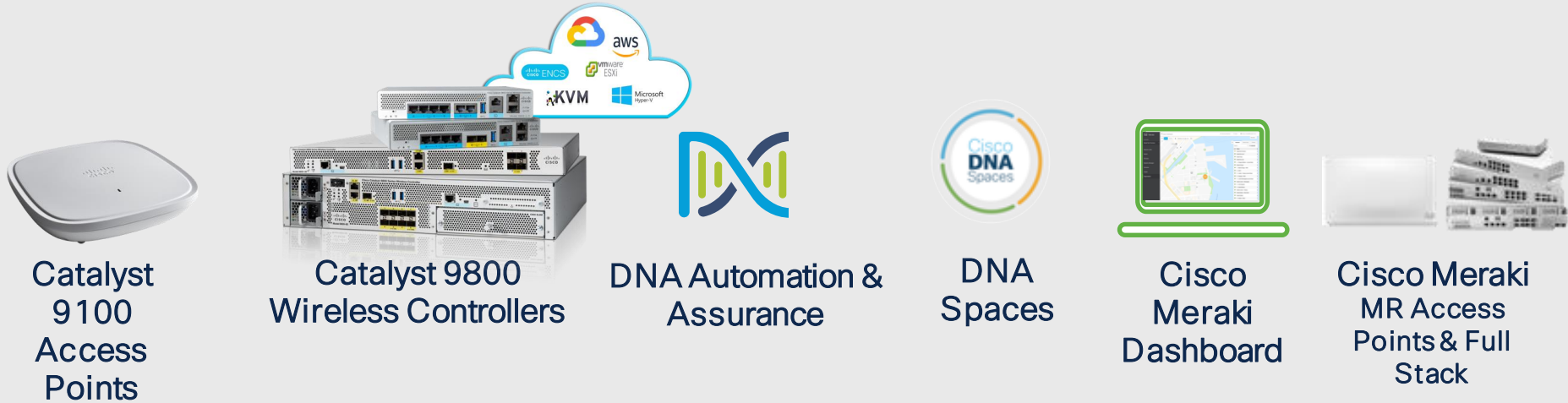
Best Practices

Additional Learning Opportunities

Thank You, AireOS

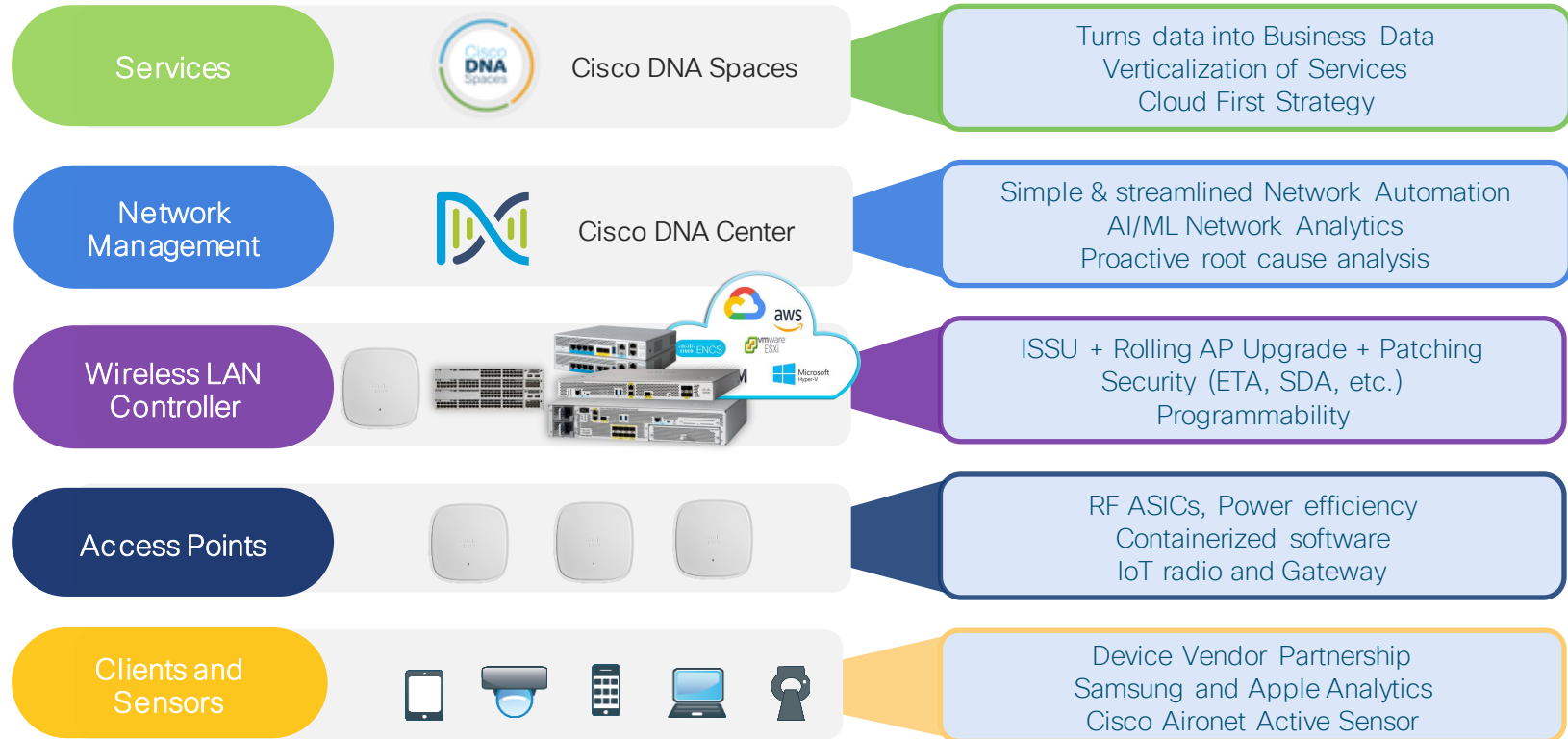


Next-Generation Cisco Wireless Stack



Resilient, Secure, Intelligent
with Innovations in Performance, Security and Analytics

Catalyst Wireless Innovation at each layer



Cisco Catalyst 9800 – Next Gen Wireless Controller



Cisco Catalyst 9800 Series Wireless Controllers

*Powered by Cisco IOS® XE
Open and programmable*

Resilient



- Zero downtime with software updates and upgrades
 - WLC SMU
 - AP Service and Device Pack
 - Intelligent Rolling AP Upgrade
- In Service Software upgrade (ISSU)
- RF based Rolling AP upgrades

Secure



- Automated macro and micro segmentation with SD-Access
- Detect encrypted threats with Encrypted Traffic Analytics (ETA)
- WPA3, Trustworthy systems, etc.

Intelligent



- Programmable network processor and IOx infra support
- Deploy in infrastructure of choice and cloud of choice
- Enhanced analytics with Cisco DNA Center
- Device Ecosystems: Apple and Samsung analytics, Apple Fastlane+

Leadership in Wireless networking

Extending Cisco's
intent-based network

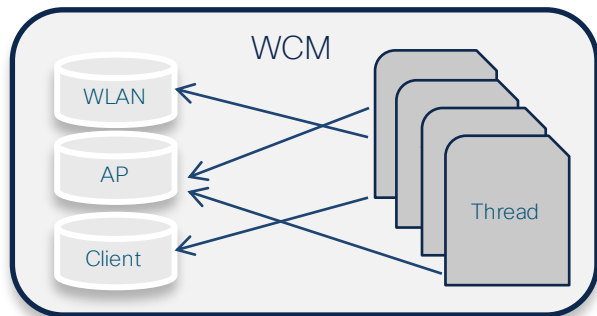
Innovation Beyond
the Standard

Cisco Catalyst 9800 Software

Previous software architecture

vs.

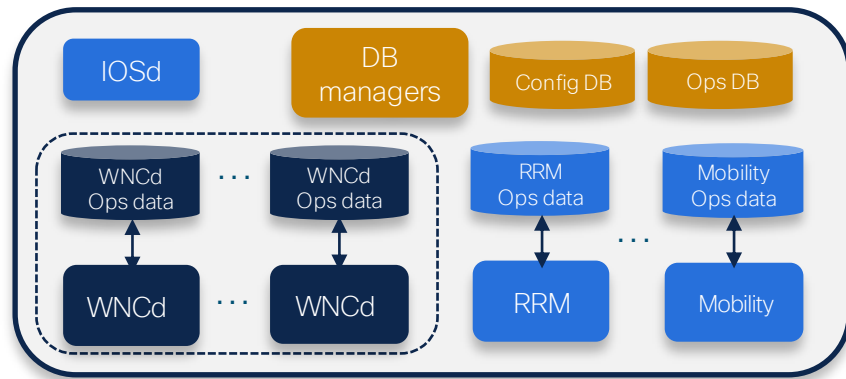
Catalyst Wireless Controller



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

Join at
Slido.com
#573 021



Qual plataforma de WLC você utiliza atualmente na maior parte da sua rede?

The background is a dark blue field filled with numerous small, semi-transparent squares and dots. These elements are scattered across the frame, with a higher concentration of larger squares in the upper left and lower right corners. The colors of these elements include various shades of blue, teal, green, yellow, orange, and red, creating a vibrant, pixelated effect.

Kicking off Your Migration

Focus on the “how?”



MSE



ISE



Prime



AireOS

How to migrate?



ISE



Cisco DNA Center



C9800



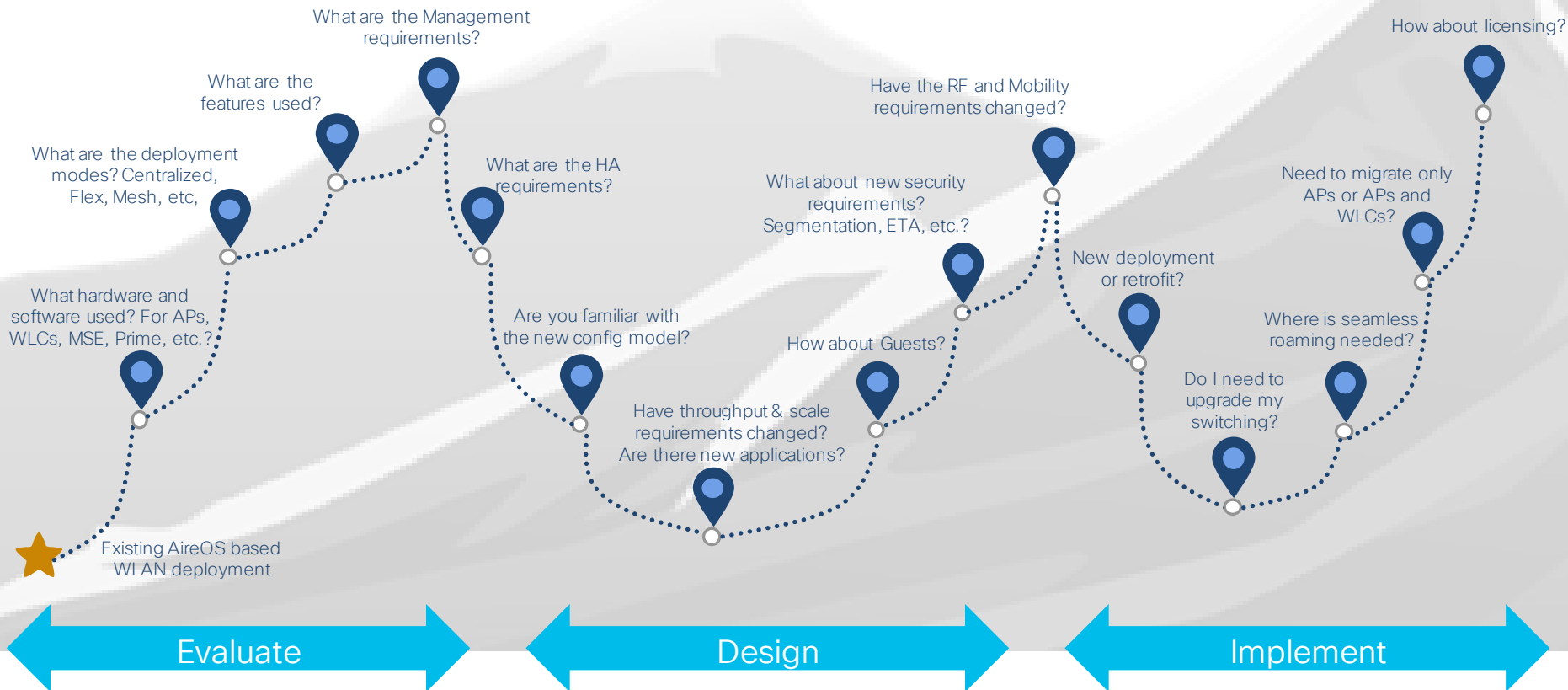
Wi-Fi 6



The background is a solid black field. It is populated with a large number of small, light blue squares and dots. These elements are scattered across the frame, with a higher density in the upper-left and lower-right quadrants, creating a sense of depth and movement, similar to a digital particle simulation or a star field.

Where to start?
Begin asking questions

Key Questions for Migration





Let the Planning Begin!

Catalyst 9800 Controller Transition from Aironet WLCs

Up to 100 APs
SMB, Small Campus and branch



Mobility Express



2504
Wireless Controller



Embedded Wireless in Catalyst APs

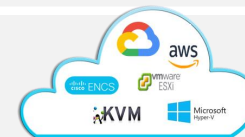
100-150 APs
Distributed Branch, Small Campus



3504
Wireless Controller



C9800-L



C9800-CL
C9800 for cloud

150 to 1500 APs
Medium Campus



5508, 5520
Wireless Controller



C9800-40



C9800-CL
C9800 for cloud

1500 to 6000 APs
Large Campus



7510, 8510, 8540
Wireless Controller



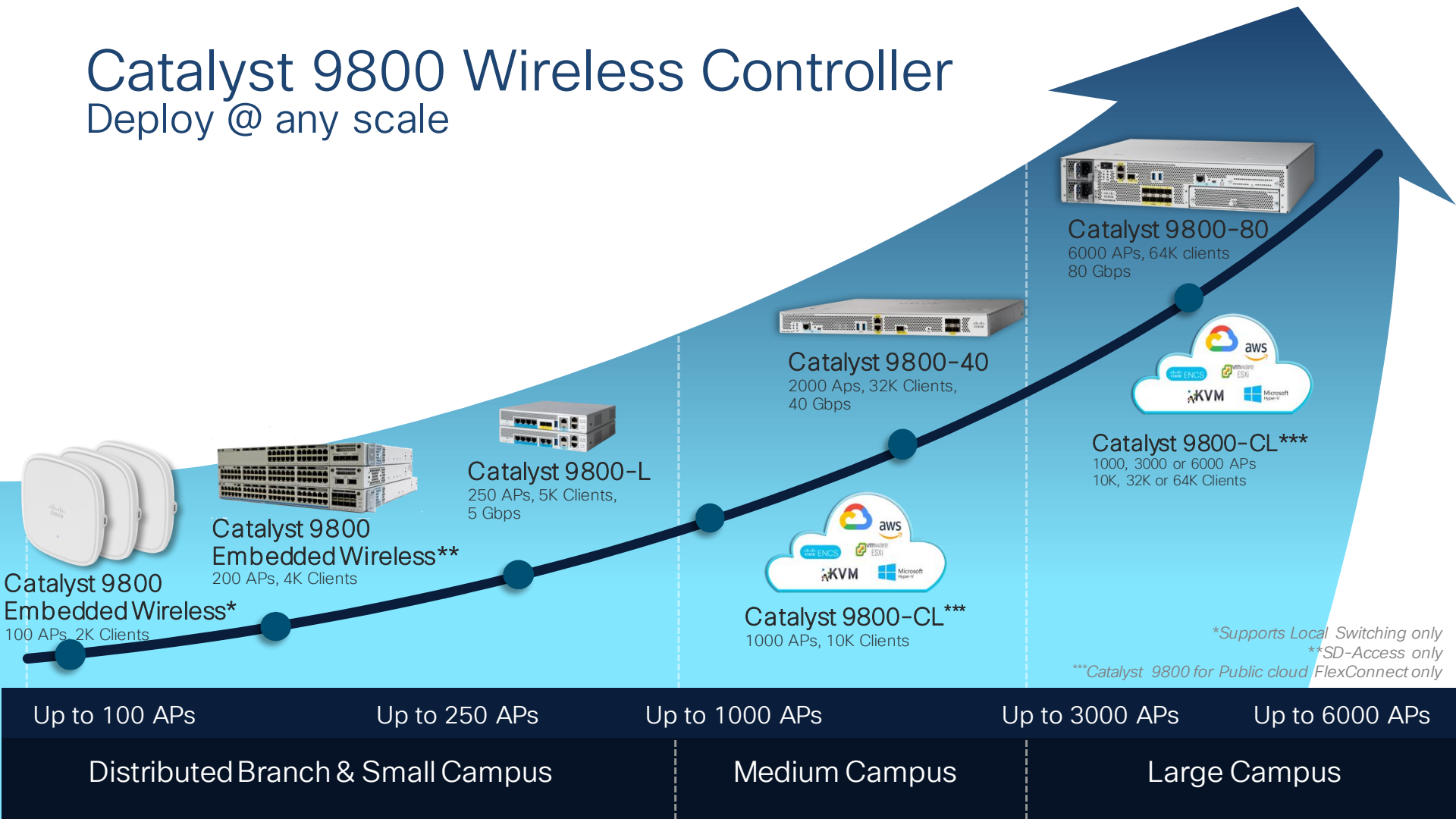
C9800-80



C9800-CL
C9800 for cloud

Catalyst 9800 Wireless Controller

Deploy @ any scale



Join at
Slido.com
#573 021



Qual a sua principal dificuldade no processo de migração?



Catalyst 9800 Configuration Migration Tool

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/>

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 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

Run

Drop the AireOS config file:

- Upload it from 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

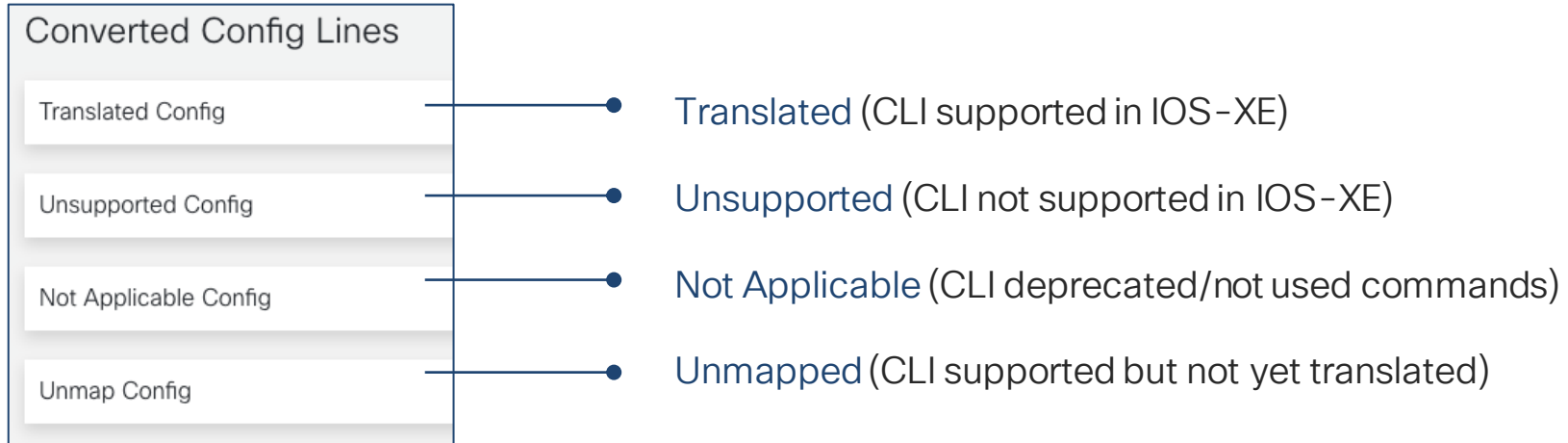
File Path: /panchurthy

File Name: aere-config.cfg

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

Configuration Migration Tool

Migration Tool output:





Getting Started

(HA, Mobility Groups and Config Model)

The background is a dark blue field filled with numerous small squares and dots. The colors of these shapes are primarily orange, yellow, and light blue. They are scattered across the frame, with a higher concentration in the upper left and lower right corners, creating a sense of depth and movement.

High Availability

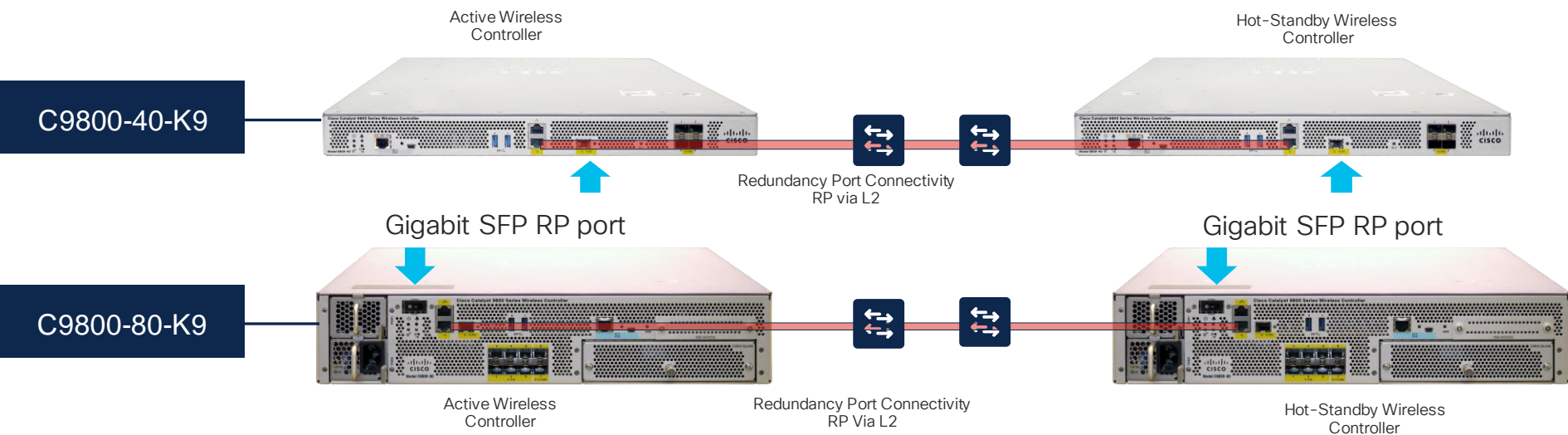
High Availability

Reducing downtime for Upgrades and Unplanned Events



High Availability (SSO)

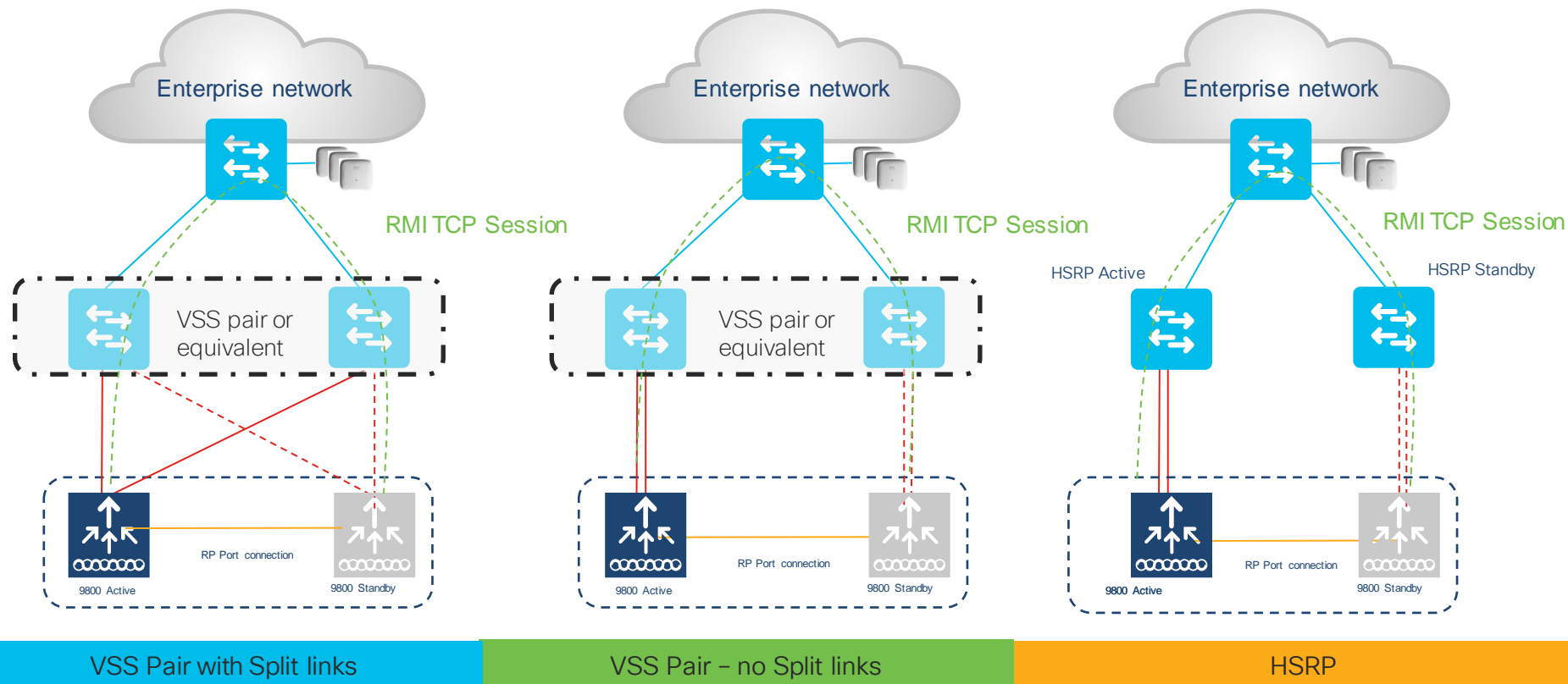
A direct physical connection between Active and Standby Redundant Ports or Layer 2 connectivity is required to provide stateful redundancy within or across datacenters



Sub-second failover and zero SSID outage

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

Supported HA SSO Topologies (17.1.x and above)



Note: RP can be connected back-to-back or via L2 switch in a dedicated VLAN

SSO Configuration Using RMI+RP option



Recommended

Administration > Device

General

FTP/SFTP/TFTP

Redundancy

Redundancy Configuration **ENABLED**

Redundancy Pairing Type ☒ RMI+RP ☐ RP

RMI IP for Chassis 1* 172.20.226.148

RMI IP for Chassis 2* 172.20.226.149

Management Gateway Fallover **ENABLED**

Local IP N/A

Remote IP N/A

Active Chassis Priority* 1

Apply

RMI IP for chassis 1 and 2 (same IPs configured on both controllers)

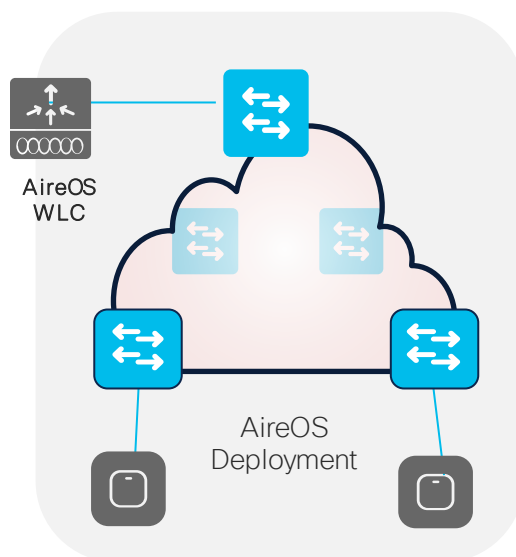
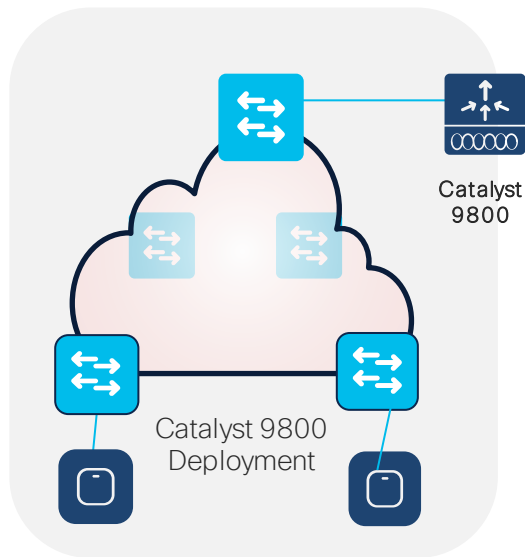
RP IP configuration for chassis 1 and 2 auto-generated as 169.254.x.x where x.x. is from the RMI IP

Note: RMI can be in the **same VLAN** as the wireless management (recommended) or in a different VLAN. The netmask for RMI is picked up from the netmask configured on the VLAN

The background is a dark blue field filled with a dense distribution of small squares and dots. The colors of these elements are primarily orange and light blue. There is a subtle diagonal gradient, with more orange elements appearing towards the top-left and bottom-right corners, and more light blue elements appearing towards the center and top-right. The overall effect is a textured, pixelated aesthetic.

Mobility Config

How to migrate from Cisco AireOS Controllers to Catalyst 9800?

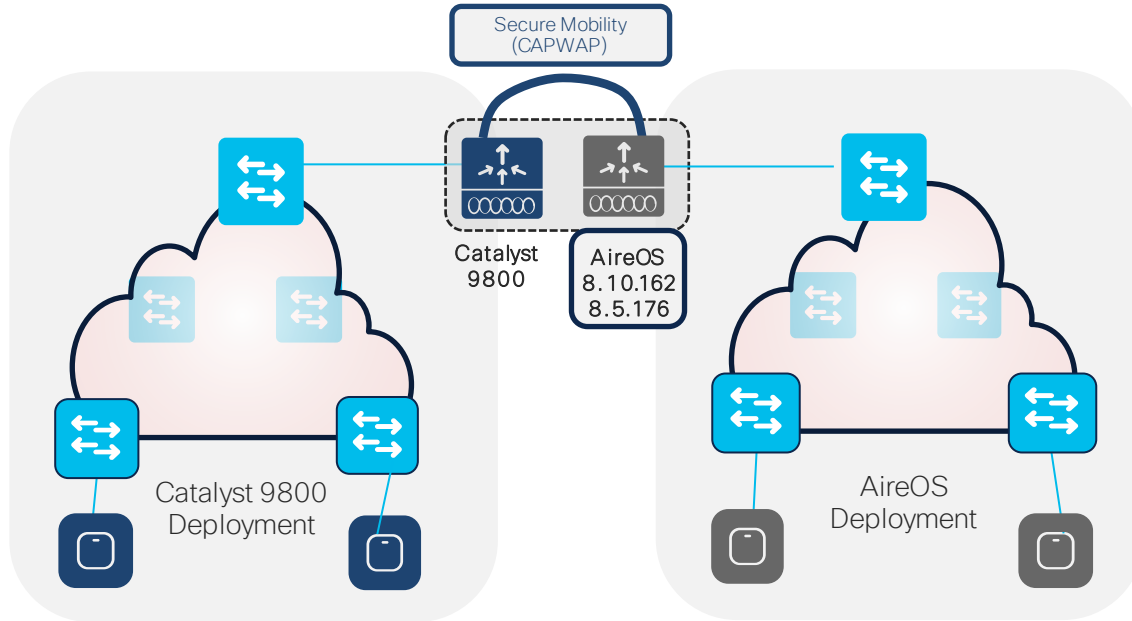


Primary questions:

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

*Radio Resource Management

AireOS to C9800 migration - Roaming

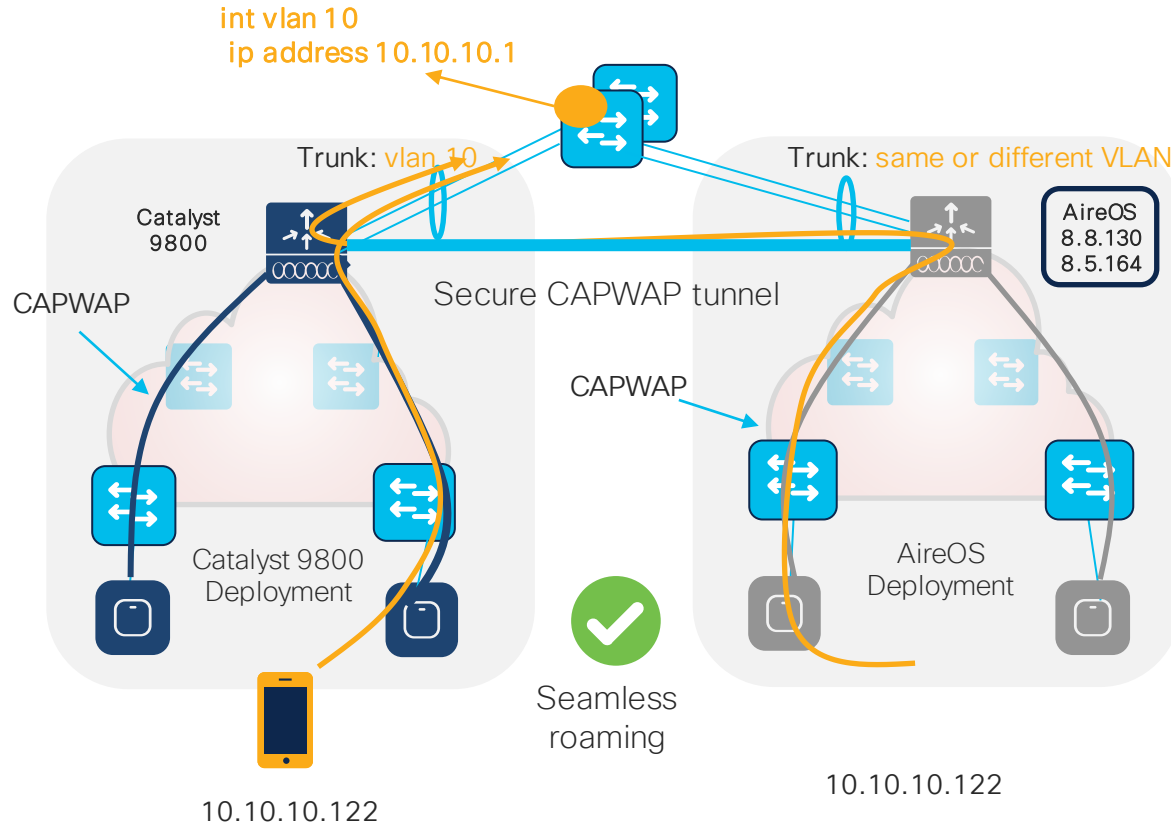


- Mobility Group provides seamless roaming between wireless controllers
- Mobility Group between AireOS and IOS-XE WLCs is only supported on:
 - 3504, 5520, 8540 with 8.10.162 and higher
 - 5508, 8510 with 8.5.176 IRCM and higher
- This is because C9800 only support CAPWAP based mobility tunnels (Secure Mobility)
- **Note: Secure Mobility is NOT supported on WISM2, 7510, 2500**

Inter-Release Controller Mobility (IRCM)

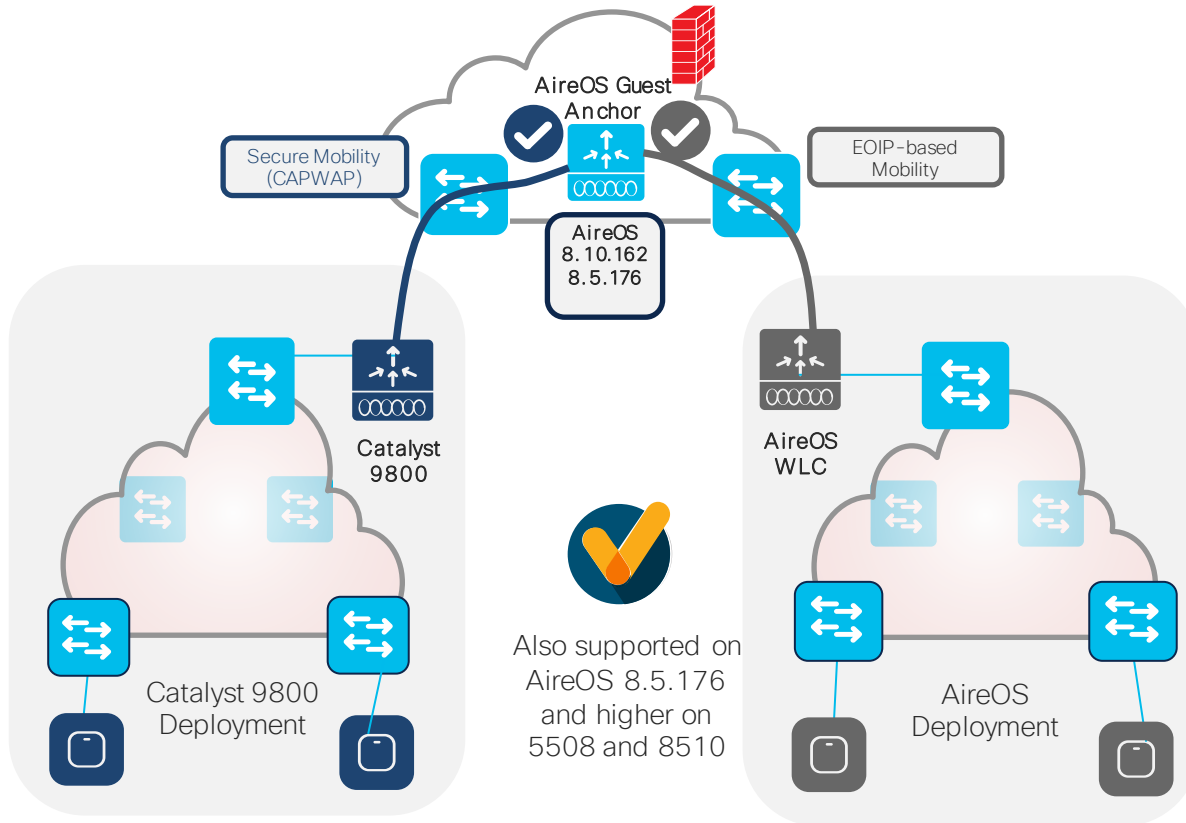
- C9800 utilizes **Secure Mobility** (capwap based) as the mobility protocol > supported only on 5508, 8510, 3504, 5520, 8540 AireOS controllers running 8.5 IRCM/8.8/8.10
- **Typical use cases for IRCM:**
 - You cannot replace/move APs in one go; AireOS and C9800 deployment will coexist and seamless roaming is needed
 - You have an existing Anchor controller and wants to continue to leverage the investment
- Roaming between AireOS and IOS-XE WLC is **always a L3 roam**

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 - Guest



- IRCM is needed to build a mobility tunnel between AireOS and IOS-XE WLCs
- AireOS anchor running IRCM release (8.10 or 8.5) can talk both tunneling protocols (CAPWAP to c9800 and EoIP to AireOS).
- It can provide Guest Anchor functionalities for both the new C9800 based deployments and the legacy AireOS based network
- Note: no need to have anchor and Foreign controllers in the same Mobility Group

Cisco Recommended Releases

9800 IOS-XE	AP	IRCM with Gen 1 AireOS : 5508/8510	IRCM with Gen 2 AireOS 5520/8540/3504
16.12.5 (EoS)	802.11ax 802.11ac	8.5.176.2	8.10.162
17.3.4 ES	802.11ax 802.11ac	8.5.176.2	8.10.162

Please check the

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html>

<https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/200046-tac-recommended-airios.html>

The background is a dark blue field filled with numerous small squares and dots. The colors of these elements are primarily orange, yellow, and light blue. They are scattered across the frame, with a higher concentration of larger orange squares in the upper left and a denser cluster of smaller orange and blue dots in the lower right, creating a sense of movement or a trail.

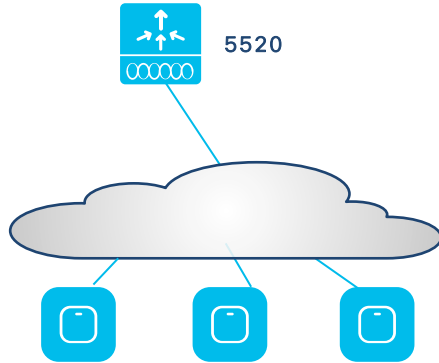
C9800 Migration Scenario

Catalyst 9800 migration

Customer Scenarios

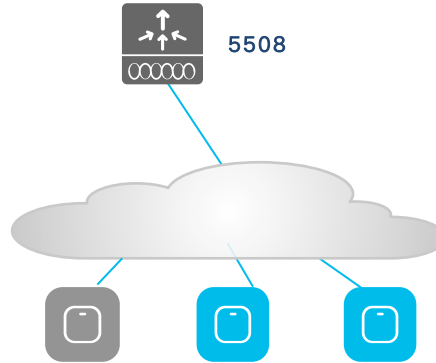
C9800 migration: common customer scenarios

Scenario A



Mix of 802.11ac APs

Scenario B

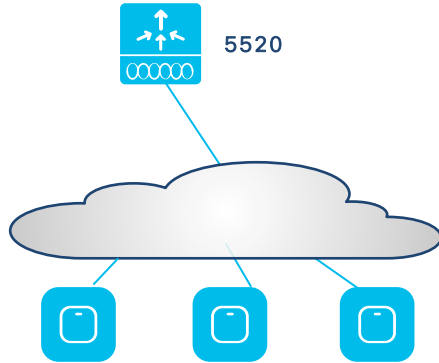


Mix of 802.11n and 802.11ac APs

Goal: migrate to Catalyst 9800 controller and Catalyst APs

C9800 migration: scenario A

Scenario A

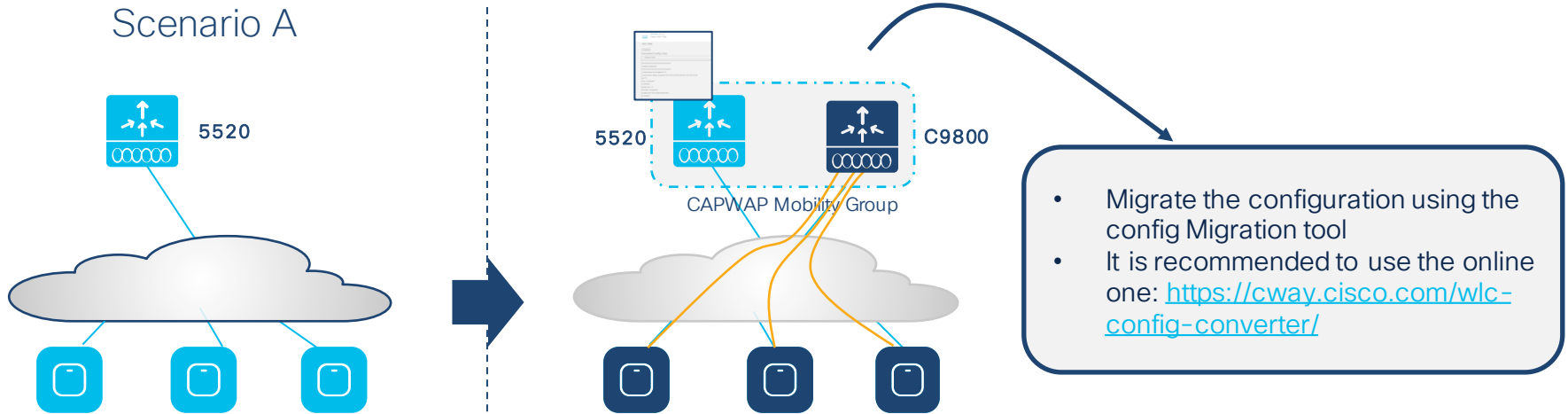


Mix of 802.11ac APs

- Best case scenario
- User can choose to start migrating APs first or add the C9800 first
- 11ax APs can be added to 5520 controller
- Customer need to migrate licenses

C9800 migration: scenario A

Scenario A

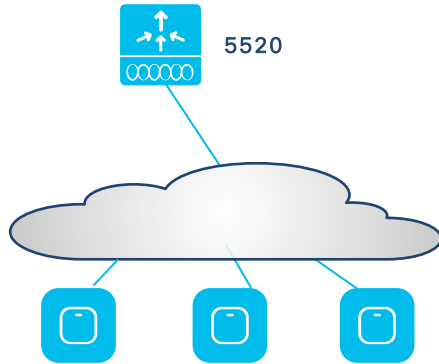


- Best case scenario
- User can choose to start migrating APs first or add the C9800 first
- 11ax APs can be added to 5520 controller
- Customer need to migrate licenses

- Upgrade 5520 to recommended 8.10
- Purchase new 11ax APs first
- 1:1 AP replacement if coverage is correct and same client requirements
- Don't "Salt & Pepper" old with new AP model – migrate per "area"
- Add 9800 in the same Mobility Group and Migrate the AireOS config
- Move the APs and Decommission 5520

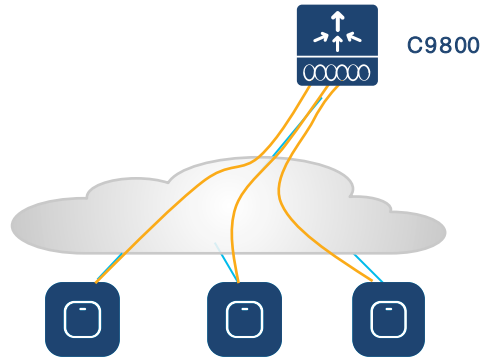
C9800 migration: scenario A

Scenario A



Mix of **802.11ac** APs

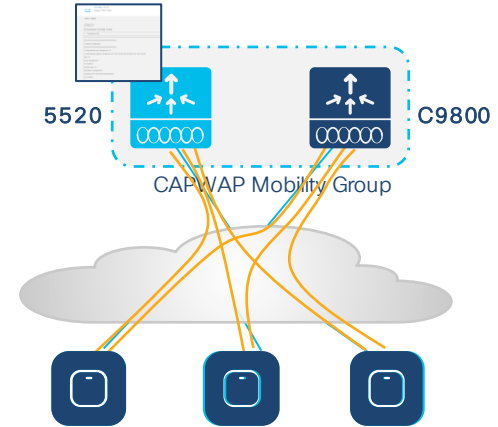
- Best case scenario
- User can choose to start migrating APs first or add the C9800 first
- 11ax APs can be added to 5520 controller
- Customer need to migrate licenses



Migrate first to new **802.11ax** APs

- Upgrade 5520 to recommended 8.10
- Purchase new 11ax APs first
- 1:1 AP replacement if coverage is correct and same client requirements
- Don't "Salt & Pepper" old with new AP model – migrate per "area"
- Add 9800 in the same Mobility Group and Migrate the AireOS config
- Move the APs and Decommission 5520

OR

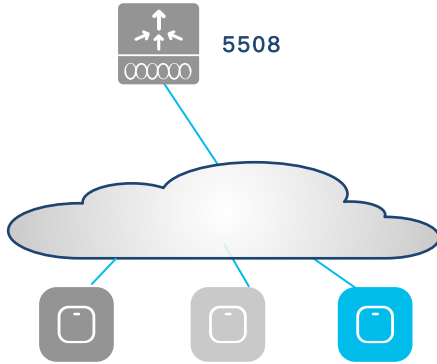


Add **C9800** controller

- Add C9800 first and migrate configuration
- Create CAPWAP Mobility Group
- Move APs to C9800
- Move APs per roaming domain area
- Seamless roaming during migration
- Decommission 5520
- Purchase and install the new 11ax APs (use the AP Refresh workflow)

C9800 migration: scenario B

Scenario B

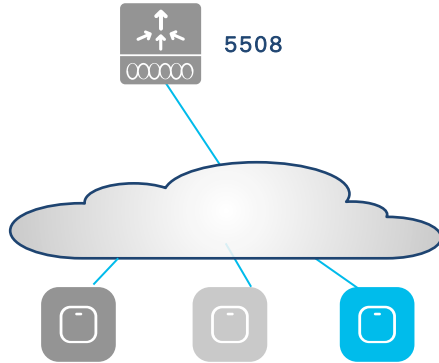


Mix of 802.11n and 802.11ac APs

- 5508 do not support 11ax APs
- User need to add the C9800 first
- 802.11n APs are not supported with C9800 and will need to be replaced

C9800 migration: scenario B

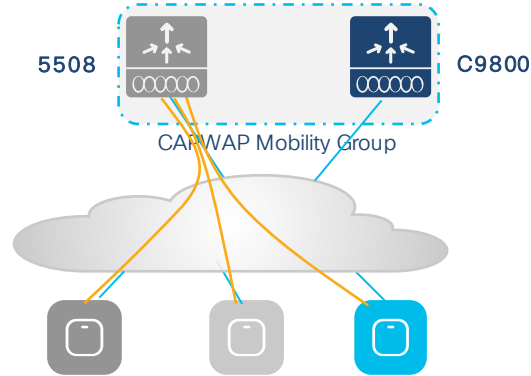
Scenario B



Mix of 802.11n and 802.11ac APs

- 5508 do not support 11ax APs
- User need to add the C9800 first
- 802.11n APs are not supported with C9800 and will need to be replaced

First step

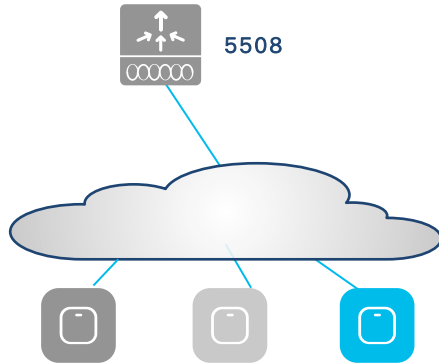


Add new **C9800** first

- Upgrade 5508 to 8.5.164 image
- Add C9800 and migrate configuration
- Create CAPWAP Mobility Group
- Seamless mobility during migration

C9800 migration: scenario B

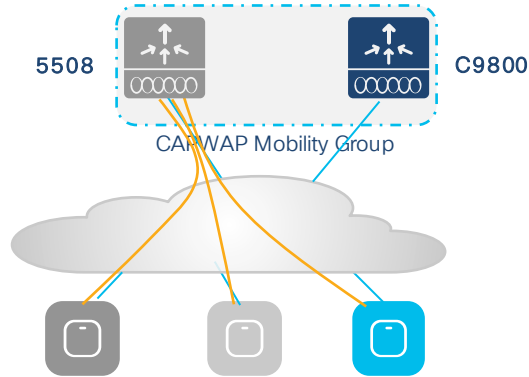
Scenario B



Mix of 802.11n and 802.11ac APs

- 5508 do not support 11ax APs
- User need to add the C9800 first
- 802.11n APs are not supported with C9800 and will need to be replaced

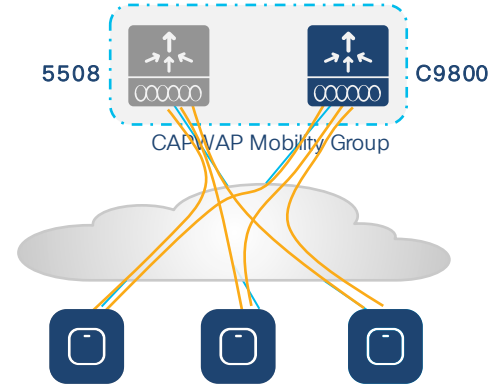
First step



Add new **C9800** first

- Upgrade 5508 to 8.5.164 image
- Add C9800 and migrate configuration
- Create CAPWAP Mobility Group
- Seamless mobility during migration

Second step



Migrate to new **802.11ax** APs

- Replace 802.11n APs with 11ax APs
1:1 AP replacement if coverage is correct
Don't "Salt & Pepper" old with new AP model
Connect new 802.11ax APs to 9800
- Move 11ac APs to 9800
- Move APs per roaming domain area
- Decommission 5508
- Replace 11ac APs with new 11ax APs

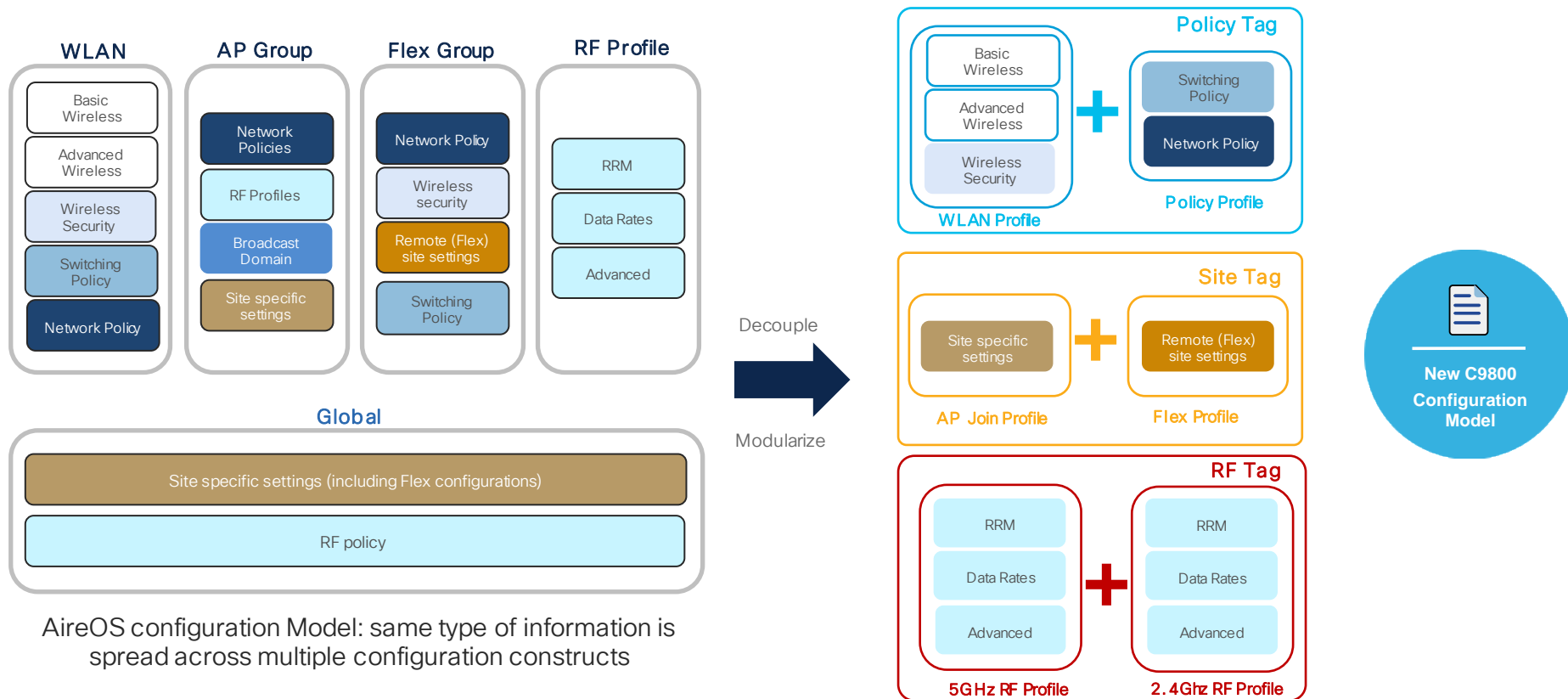


C9800 Config Model

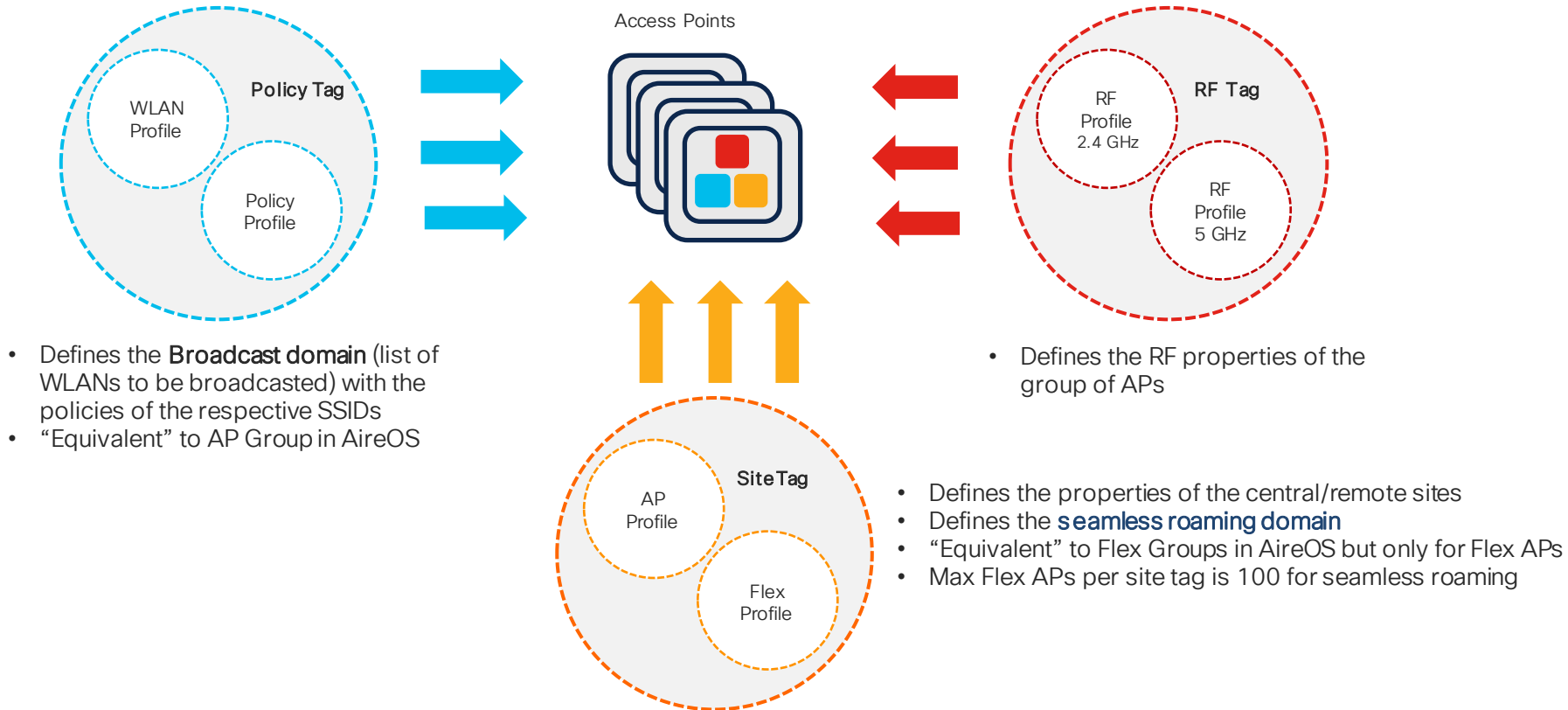
Profiles & Tags

Catalyst 9800 vs. AireOS Configuration Model

Modularized model with logical decoupling of configuration entities






Catalyst 9800 Config Model



Catalyst 9800 Config Model - Benefits

Access Points



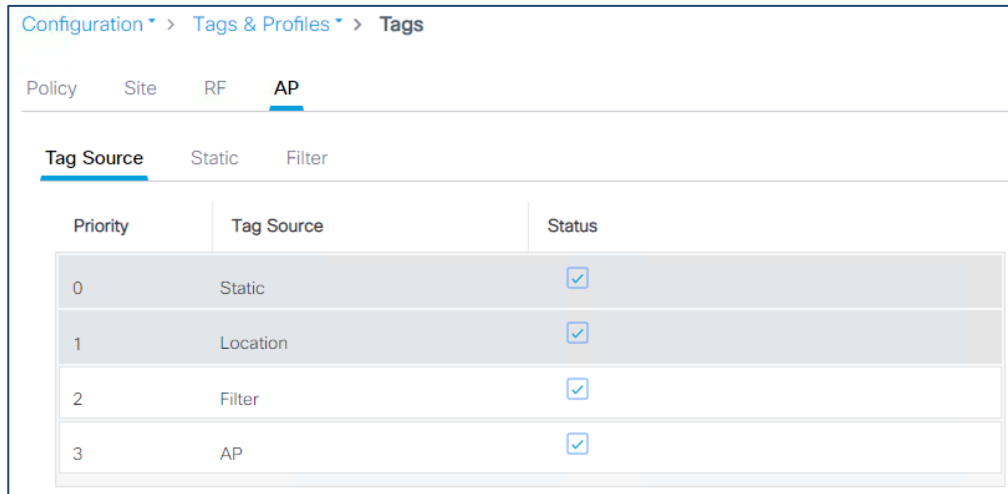
-  RF Tag
-  Policy Tag
-  Site Tag

Profiles and Tags benefits:

- Modular and reusable config constructs
- Flexible in assigning configuration just a group of APs
- Easy to manage site specific configuration across geo-distributed locations
- No reboot needed when applying config changes via tags (remember AP groups?)

AP to Tags binding

- Without previous 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 can have multiple tag sources:



Configuration > Tags & Profiles > Tags		
Policy	Site	RF
AP		
Tag Source	Static	Filter
Priority	Tag Source	Status
0	Static	<input checked="" type="checkbox"/>
1	Location	<input checked="" type="checkbox"/>
2	Filter	<input checked="" type="checkbox"/>
3	AP	<input checked="" type="checkbox"/>

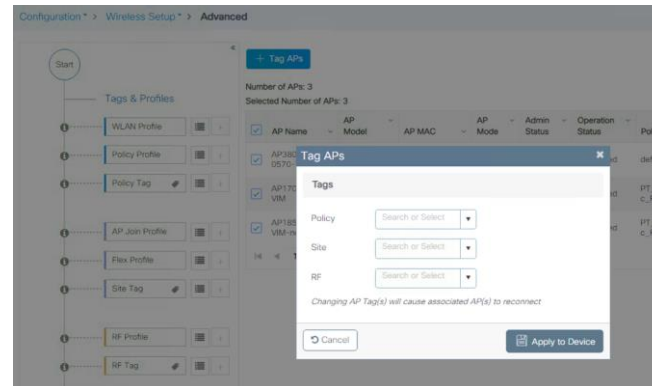
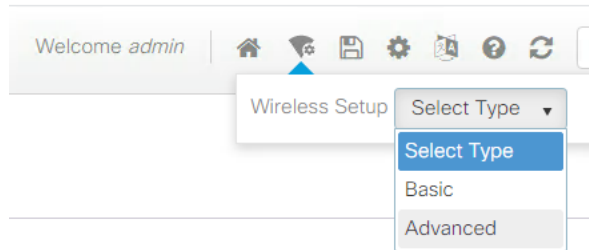
- Static: user configuration
- Location*: Basic Setup flow
- Filter: regular expression
- AP: the tag is saved on AP

These are in order of priority

(*) Location here is not the AP Location but a config construct internal to C9800

AP to Tags binding

- The **static** Tag <> AP binding is based on AP's MAC and it's a configuration on the Controller: upon joining the C9800, the configuration gets applied and AP gets assigned to the selected tags
- Note: when the AP joins another controller that doesn't have the static mapping configured, it will get assigned to the default tags
- To statically assign Tags to multiple APs, you can use the Advanced Wireless Setup



AP to Tags binding – GUI /CLI verification

- Available in 16.12.2s and later
- Configuration > Wireless > Access Points

Configuration > Administration > ap_configuration_viewer

AP Name	AP Model	common_slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Policy Tag	Site Tag	RF Tag	Tag Source	Location	Country
LABap_2802	AIR-CT5502-K9	2	✓	192.168.68.195	0027.e38f.33a0	Flex	Registered	default-policy-tag	default-site-tag	default-rf-tag	Default	default location	BE

LABap_2802

- wlans_and_policies (default-policy-tag)
 - WLAN : ACLtest
Policy : leap
VLAN ID : 1468
Security : Open
 - WLAN : ndarchis_leap
Policy : leap
VLAN ID : 1468
Security : WPA2
- site_properties (default-site-tag)
 - AP Join : default-ap-profile
LED State :
 - Rogue Detection :
 - Flex Profile ...
Native VLAN ID : 1
- rf_properties (default-rf-tag)
 - 5 GHz Band : Global Config
 - 2.4 GHz Band : Global Config

```
C9800-US-WEST#sh ap tag summary
Number of APs: 1
```

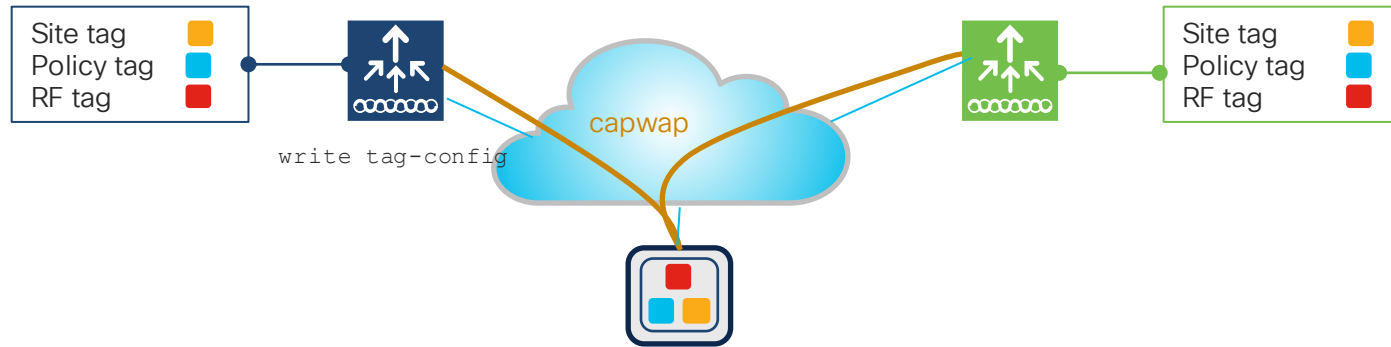
AP Name	AP Mac	Site Tag Name	Policy Tag Name	RF Tag Name	Misconfigured	Tag Source
AP0081.C4F4.2972	0081.c4f4.2972	NH	NH Policy Tag	default-rf-tag	No	Static

AP to Tags binding

- In earlier releases, to push the Tags information to the AP so that the AP can save and remember this information, you need to use a CLI command in exec mode:

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

- The AP will retain its tags assignments when moved between two controllers if the tags are saved to the AP (with the write tag-config command) and the tags are defined on both controllers. If not defined, the AP is assigned default tags



- From Cisco IOS XE Bengaluru 17.6.1 onwards, AP tag persistency is enabled globally on the controller. When APs join a controller with tag persistency enabled, the mapped tags are saved on the APs without having to write the tag configurations on each AP, individually.

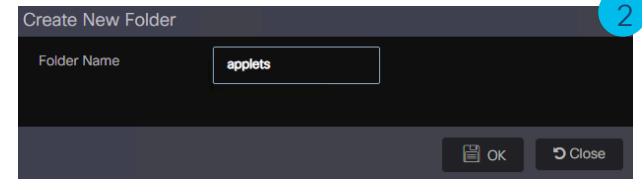
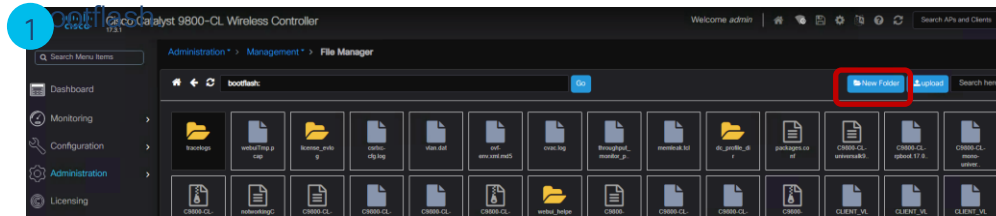
Moving Aps between C9800 Controllers

Solution 1 : Install 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

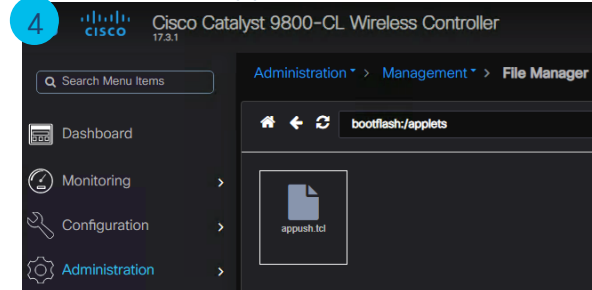
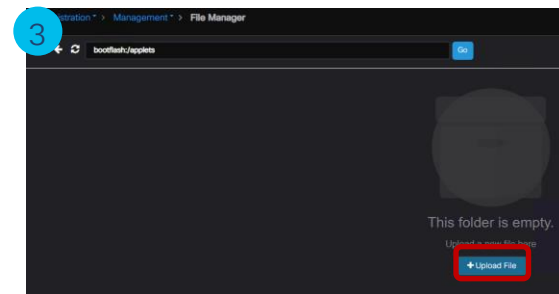
Administration > Management > File Manager: double click on

Click on New Folder and create folder “applets”



Double click on new folder and Click on Upload file

Load the “appush.tcl” file



Moving APs between C9800 controllers

- Verify the script is there:

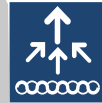
```
C9800#dir bootflash:/applets
Directory of bootflash:/applets/
301922  -rw-                1850   Oct 1 2020 09:46:19 +00:00  appush.tcl
```

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

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

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

Before



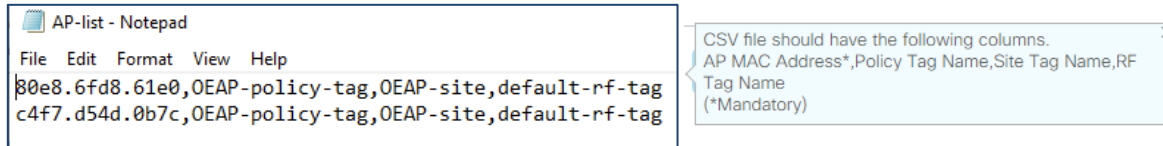
```
AP1# show capwap client config
[..]snip
AP Policy Tag           : flex-tag
AP RF Tag               : default-rf-tag
AP Site Tag             : flex-site
AP Tag Source           : 1
```

After

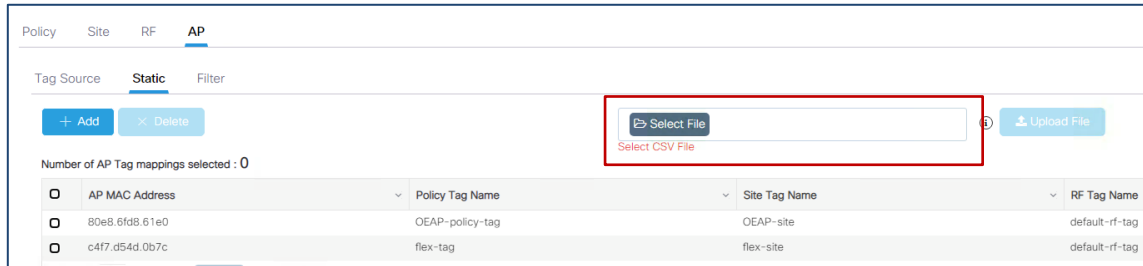
Moving APs between C9800 controllers

Solution #2

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



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



- When the Primary fails, the Secondary already 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	Devices	WLC Role
9005S1WBPCH	c9800-SJ-11.cisco.cor	<input checked="" type="radio"/> Active Main WLC ① <input type="radio"/> Guest Anchor

Managing 4 Primary location(s)

Managing 1 Secondary location(s)

Managed AP Location

Find Hierarchy

- Global (2)
- EMEAR (2)
 - Rome-branch (1)
 - Vm-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

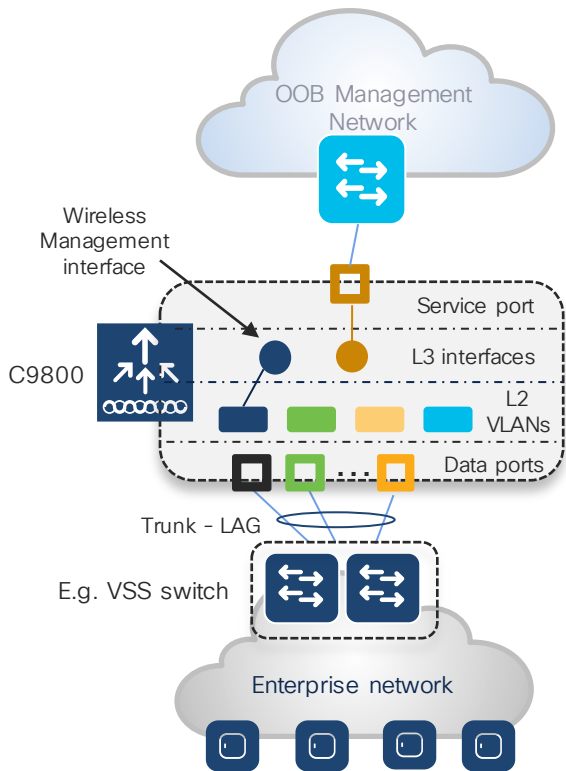
Showing 1 of 1

- 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



Catalyst 9800 Design Considerations

Network Connectivity (SVIs, VLANs, etc)



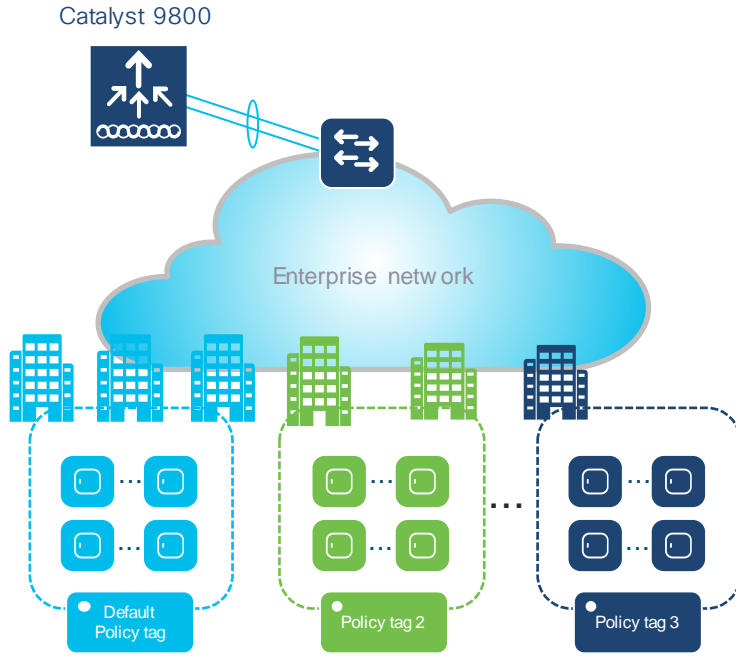
Facts:

- It's mandatory to have a **L3 interface** configured as **wireless management interface**
- AP CAPWAP traffic is terminated to the wireless management interface. There is only one **wireless management interface**
- 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.
- 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

Design best practices:

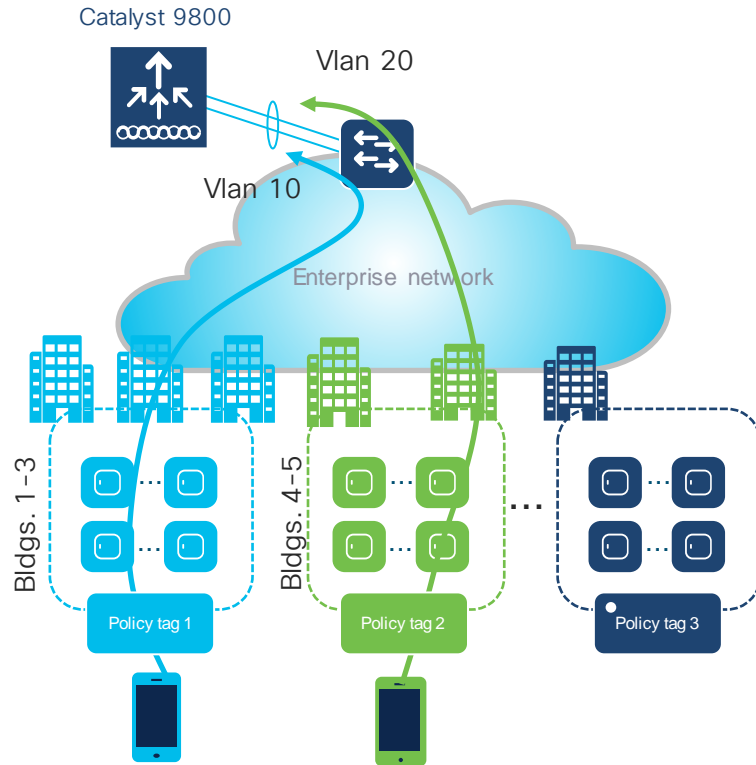
- **Uplink ports** follow AireOS best practices: port-channel configured as trunk to a pair of VSS/VSL pair of switches or to a multi-switch stack.
- **C9800-CL in Public Cloud** must use a L3 port. Sniffer Mode and Hyperlocation not supported.
- **C9800 Appliances and C9800-CL in Private Cloud** use an L3 SVI for Wireless Management Interface, otherwise above limits will apply.

Policy Tags – Default Policy Tag



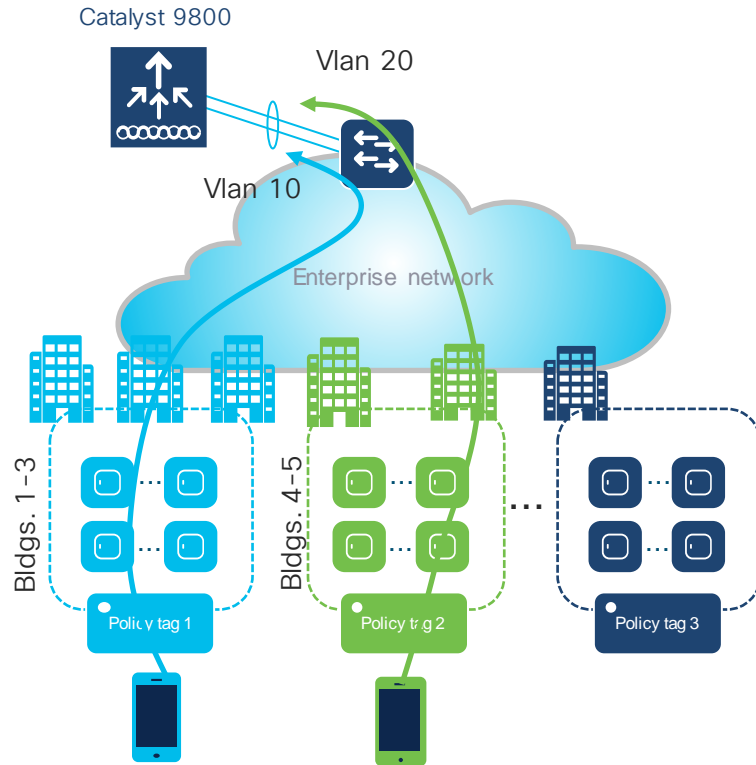
- **Policy Tag** defines which SSID is broadcasted by the AP or group of APs and the associated policy (VLAN, QoS, AVC, etc). In this, it's equivalent to the AP Group in AireOS
- Like any other tags, policy tag has a default-policy-tag that gets assigned by default when the AP first join the C9800
- In release **16.12.1s and below** all the WLANs defined with ID < 16 are automatically mapped to the default-policy-profile, added to the default-policy-tag and hence broadcasted automatically (same as the default AP Group)
- Starting release **16.12.2s and above**, the behavior changes: user must explicitly map any WLAN (no matter the WLAN ID) to the default-policy-profile via the default policy tag for the SSID to be broadcasted. In other words, no SSID will be broadcasted by default
- If you are upgrading from 16.12.1s (or prior) to 16.12.2s and above, you have to make this change

Policy Tags – Roaming across Policy Profiles



- **Policy Tags** can be used to assign different policies to the same SSID in different locations or group of APs.
- Use Case: IT wants to assign a different VLAN to the campus wide SSID according to client joining location. For example: if client joins from bldg. 1-3 assign it to VLAN 10, if it joins from bldg. 4-5, assign VLAN 20 and so on...
- This can be easily achieved by using a different policy tag per group of APs in those buildings and *mapping the same SSID to a different policy profile (where the different VLAN is defined)*.
- **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.

Policy Tags – Roaming across Policy Profiles

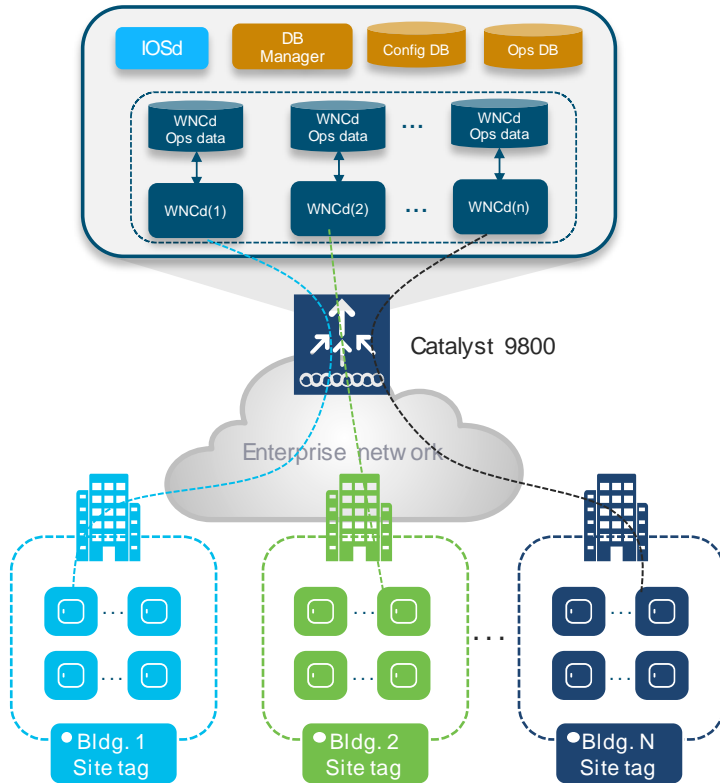


- Before 17.3, if two policy tags are created to associate a different policy profile to same SSID (e.g. different client VLAN), upon roaming, client will need to go through a reauth to re-evaluate the change in policy > client roaming is not seamless
- **Starting from 17.3**, if the policy profiles 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-persistent`
- Even if the command only mentions “VLAN”, in reality there are many other parameters that can differ between the two policy profiles and still result in a seamless roam.

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

Site Tags – Design Considerations



Important facts:

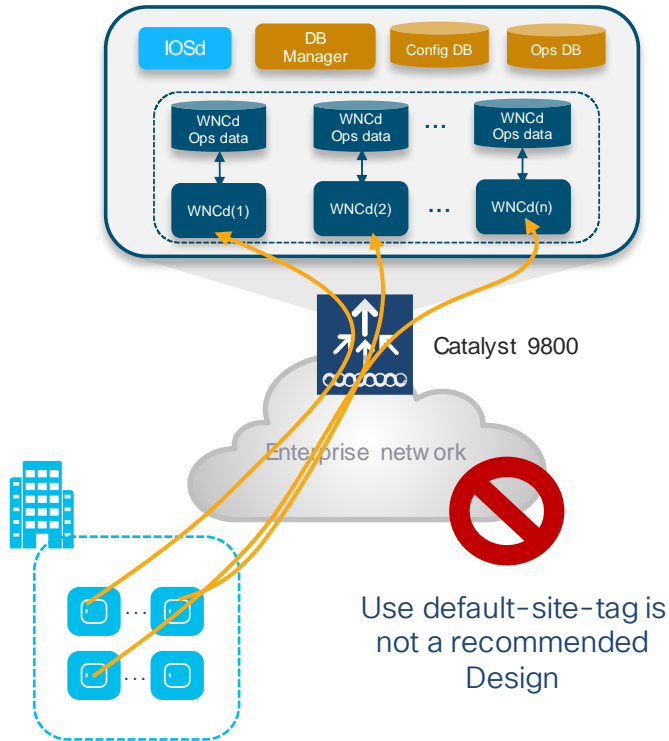
- C9800 has a multi-process software architecture
- APs are distributed across Wireless Network Controller processes (WNCd) within a C9800
- Load balancing of APs (and clients) across WNCd gives better scale and performance
- The number of WNCds varies:

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

Following command shows the # of WNCds processes:

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

Site Tags – AP to WNCd Distribution



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

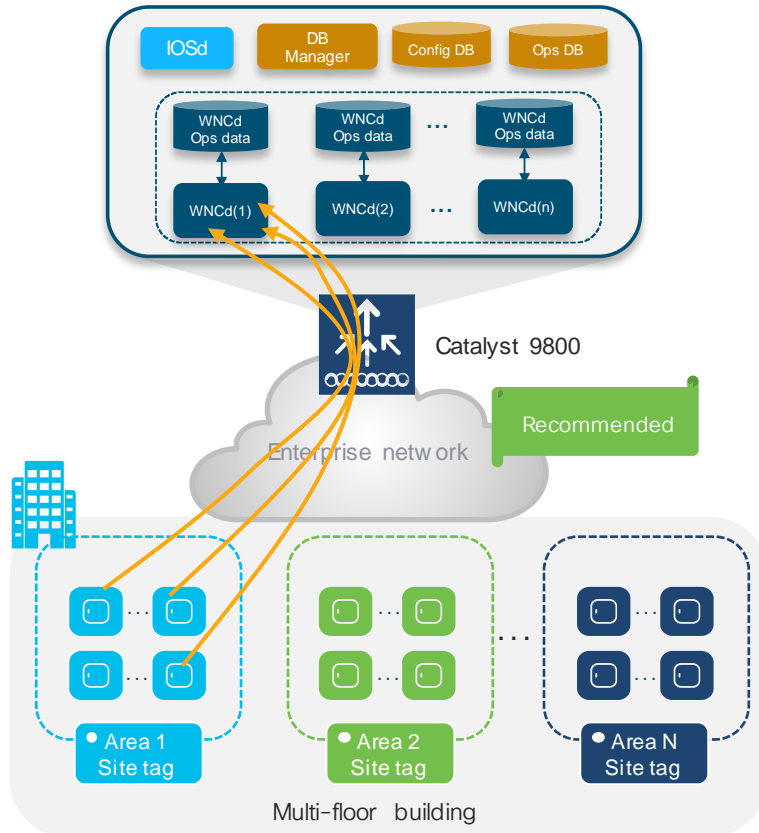
One exception is what happens if using the **default-site-tag**:

- 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**
 - 11k – Assisted Roaming – Channel Neighbor List
 - 11v – BSS transition / Disassociation control

Note: 17.6 MR and 17.7 will support 11k/v across WNCds

- **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)

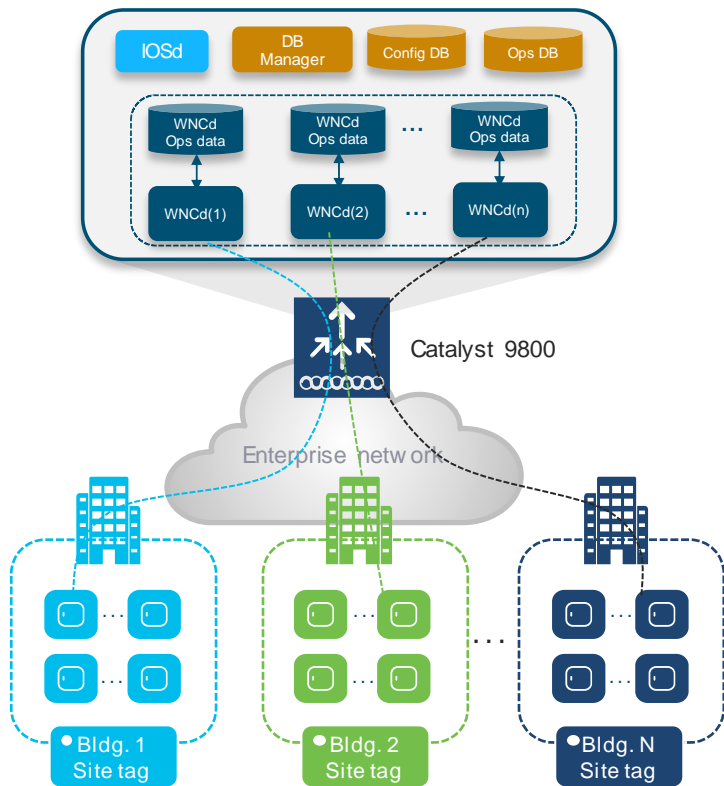
Site Tags – AP to WNCd Distribution



How AP distribution 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)



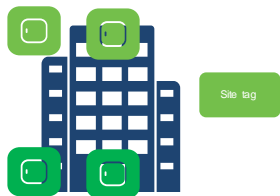
Recommendations:

- You don't want to assign all the APs to the same site tag (WNCd) as this will not be very efficient
- 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** (this is the DNA Center criteria)

Site Tags – Design for Campus (local mode)



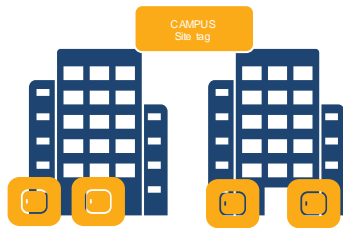
What if my customer has a building with 700 APs and 9800-40?

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

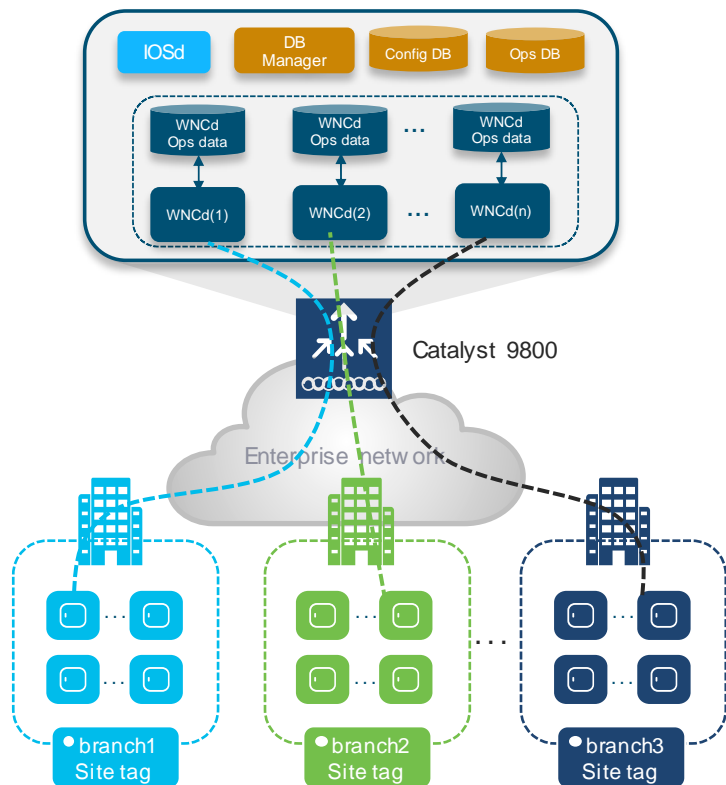


What if customer has multiple buildings with less than 500 APs?

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

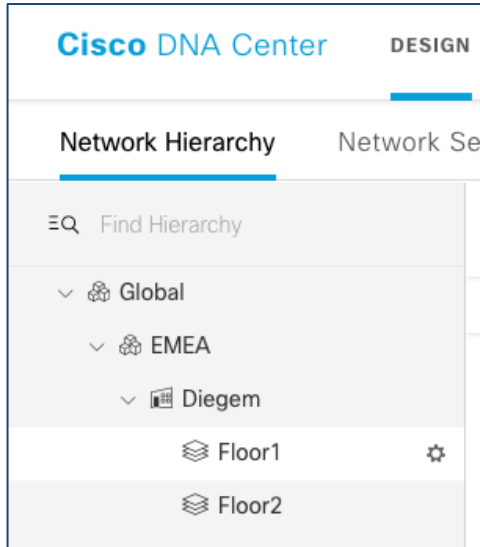
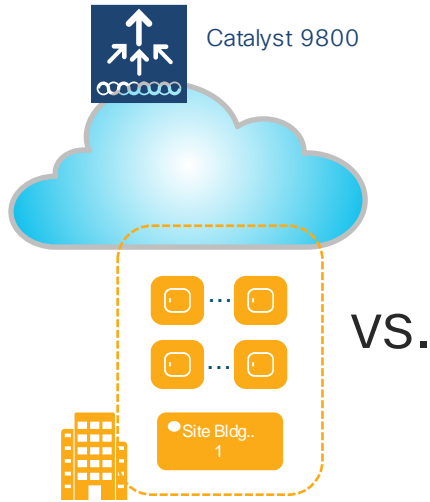
Site Tags – Design for Branch (Flex mode)



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



- **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



Catalyst 9800 Best Practices

Migration Best Practices

- **Understand** the IOS-XE Configuration Model (Profiles & Tags)
- **Build a Test area** with same characteristics of the production network
 - Same topology: Anchor Controller, HA config, Firewall and other network settings like AAA
 - Ideally test same client types but at least one Windows, one Android and one Apple client
 - Test the different authentication types with same version of production AAA and Portals
 - Tip: No hardware? C9800-CL can be downloaded from Cisco.com
- **Assess** the client devices and evaluate if some changes need to be done in the RF default configuration (e.g. old devices might need lower data rates)

Best Practices Guide on Cisco.com

<http://cs.co/c9800-BP>

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

Cisco Catalyst 9800 Series Configuration Best Practices

Updated: May 7, 2020

Contact Cisco

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...

Share

Download

Print

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:



Cisco Catalyst 9800 Series Wireless Controllers

Power by Cisco IOS® XE
Open and programmable



Cisco Catalyst 9100 Access Points

Power by Wi-Fi technology
Superior RF experience

Resilient



ISSU

Secure



User Define Network

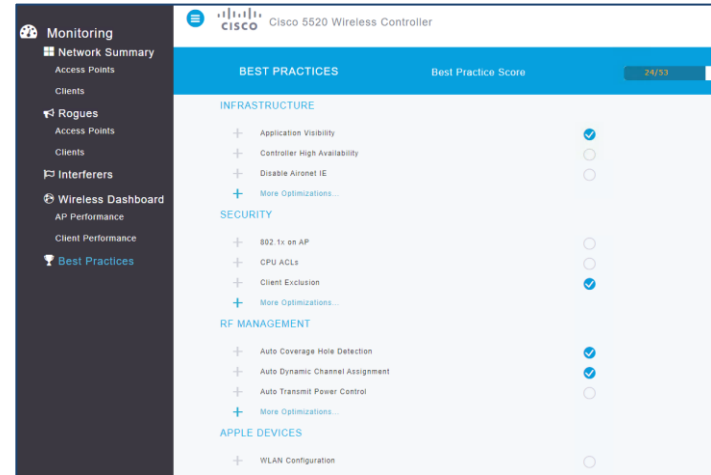
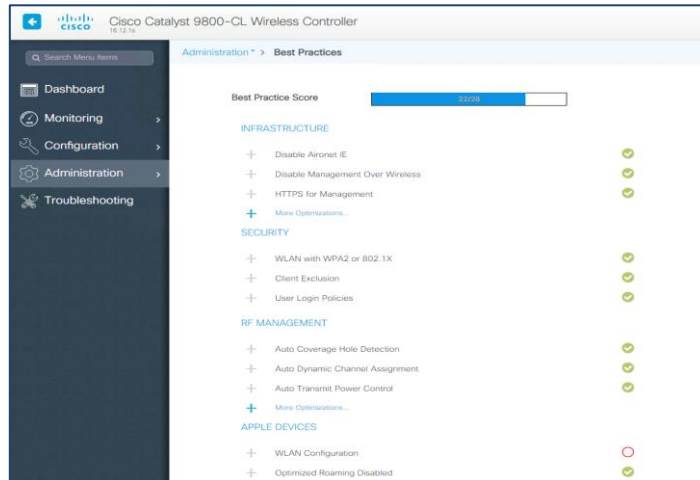
Intelligent



11ax Analytics
Samsung Analytics

Best Practices - Dashboard

C9800 (in 16.12.1s and later) introduces the same Best Practice dashboard



There are some differences that you should be aware of...

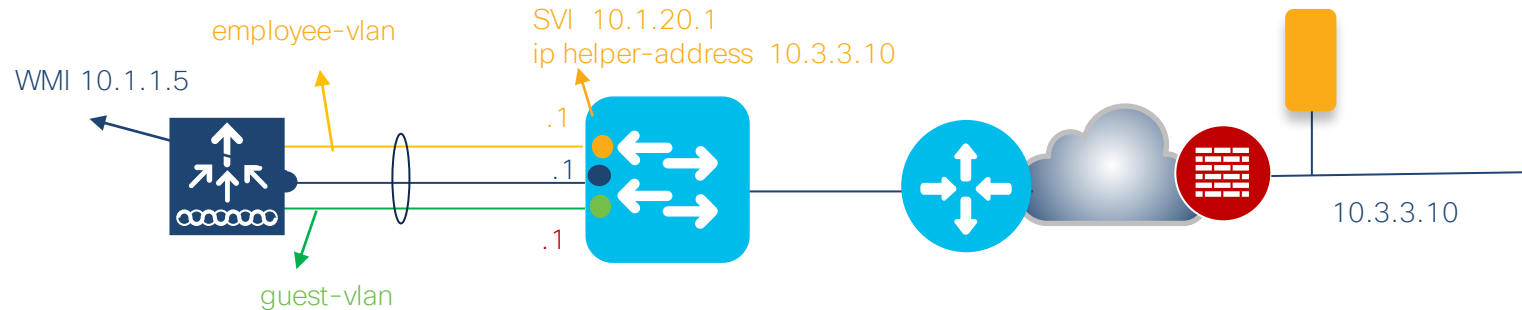
Best Practice – DHCP proxy/relay

- **DHCP Proxy mode:**

- In AireOS, enabling DHCP Proxy for wireless clients is a best practice
- In C9800 DHCP proxy is not needed as IOS-XE has embedded security features like DHCP snooping, ARP inspection, etc. that don't require a L3 interface. There is no equivalent config in 9800.

- **DHCP relay or bridging mode?**

- DHCP bridging is the **recommended mode** and should be used if DHCP relay can be configured on the upstream switch or if the DHCP server is on the client VLAN



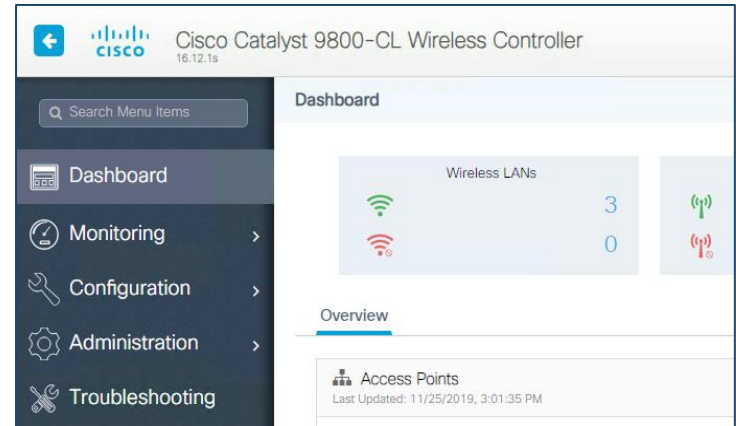
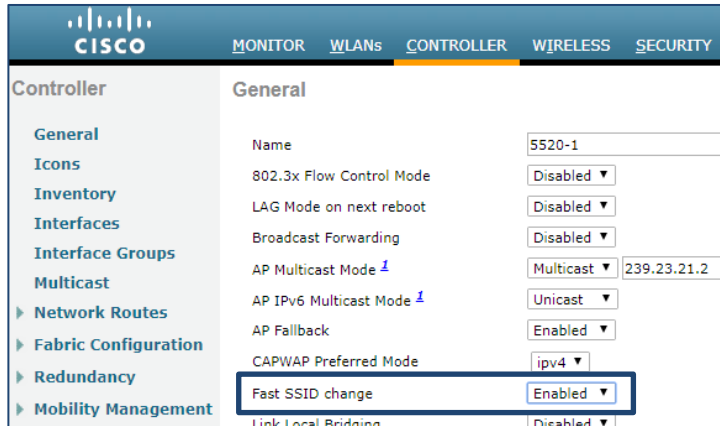
Best Practice – DHCP Proxy

- **DHCP Proxy mode:**
 - In AireOS, enabling DHCP Proxy for wireless clients is a best practice
 - In C9800 DHCP proxy is not needed as IOS-XE has embedded security features like DHCP snooping, ARP inspection, etc. that don't require a L3 interface
- **DHCP Proxy or Bridging mode?**
 - DHCP Bridging is the **recommended mode** and should be used if DHCP relay can be configured on the upstream switch or if the DHCP server is on the client VLAN
 - DHCP Proxy on C9800 should be configured if you would like to add option 82
 - On box DHCP Proxy can be configured on the client interface VLAN (SVI) or per WLAN basis
 - SVI must be configured with an IP address
 - The outgoing interface for DHCP traffic will be determined by routing table lookup for DHCP server's IP
 - DHCP Proxy Mode: the real IP of the DHCP server is hidden from the client but the IP of the controller is exposed, so you may want to consider any security implications

Best Practice – What's Different?

Fast SSID Change

- In AireOS, Fast SSID change is a best practice to allow clients to roam faster between different SSIDs



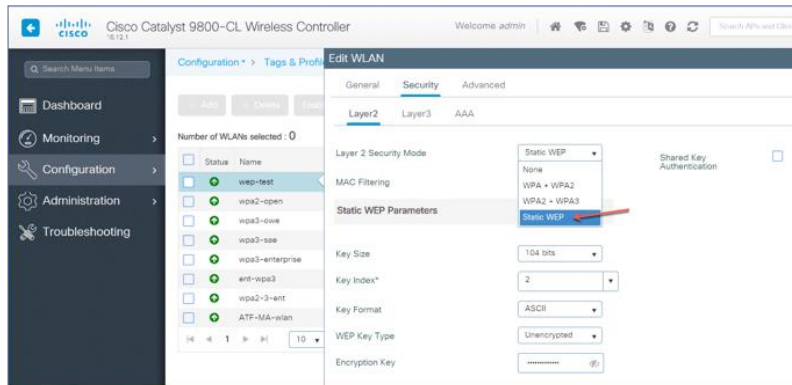
In C9800 there **no setting called Fast SSID** change and is not required as **C9800** allows this behavior by default

Best Practice – TKIP and WEP support

- TKIP and WEP are deprecated by WFA. However...
- TKIP configuration is available in CLI only (same as in AireOS) and supported on all APs

```
c9800-SJ-11(config)#wlan psk-psk 17 sj-psk  
c9800-SJ-11(config-wlan)#security wpa wpa1 ciphers tkip
```

- WEP configuration is also available on C9800 and is supported with Wave-1 APs only (x700 series and 1570). Wave-2 APs or new Catalyst APs will not broadcast SSID configured with WEP.



Best Practice – Configurations

Make sure box(es) are in **install mode**. This is the default mode and there are no reasons to change it. In HA pair both boxes need to have the same mode

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

WLAN Session timeout = Zero (0)

Different behavior from AireOS; in C9800 this makes all client roaming going through a full reauth! This is fixed in 17.4, where we have the same behavior as AireOS and the max timeout will be used.



Key Takeaways

Key Takeaways

Use the Migration Tool and review the conversion output

Understand the IOS-XE Configuration Model

Review your requirements for AireOS and IOS-XE co-existence

Utilize deployment Best Practices



Learn More



[Migration to the New Catalyst Wireless Stack, a practical guide!](#)



[Campus LAN and WLAN Solution Design CVD](#)

[C9800 Release Notes](#)

[C9800 Configuration Guides](#)

[C9800 Technical References](#)

[C9800 Command References](#)

[C9800 Configuration Examples and Tech Notes](#)

[C9800 Deployment Best Practices](#)

[C9800 WLC Configuration Model](#)

[WLC Configuration Converter](#)

[WLC Compatibility Matrix](#)

[AireOS to IOS-XE Command Mapping](#)

[AireOS to C9800 Wireless Controller Feature Comparison Matrix](#)

[Cisco Learning Partners](#)



[Cisco WLAN YouTube Channel](#)





Quint@s Quinze

Dúvidas?



Quint@s Quinze

Muito Obrigado!