cisco Live!

Let's go

The bridge to possible

High Availability Design with Cisco Catalyst 9800 Wireless Controllers

Business Resiliency with always-on Wireless

Justin Loo, Technical Marketing Engineer

BRKEWN-2846

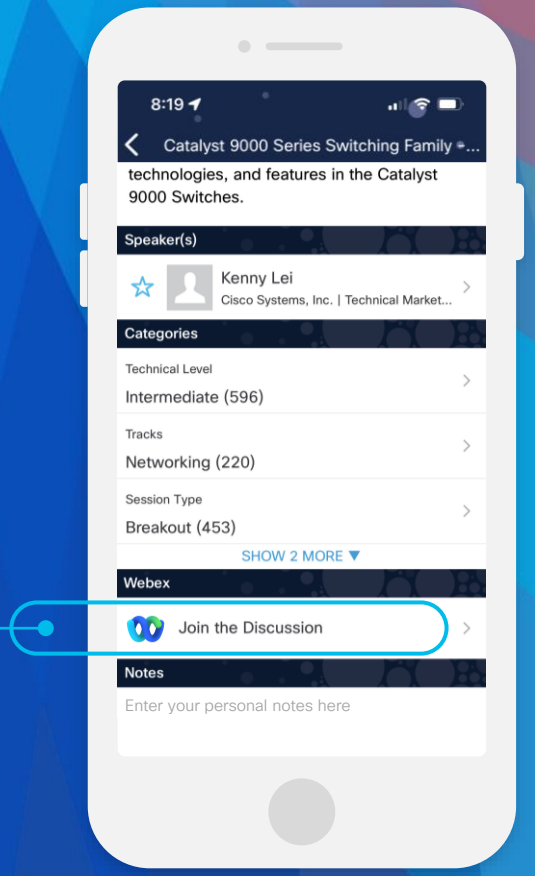
Cisco Webex App

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 June 9, 2023.

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2846

About Me

Fields of Expertise (3 Years at Cisco)

Cisco Catalyst 9800 Wireless LAN Controller, Wireless Assurance and Automation

Personal Life

Born and raised in Southern California, University of California Los Angeles Alum

Hobbies

Triathlon, Trying new foods, Traveling, Watching movies

Why should I care about High Availability?

Agenda

1. **Wireless Controller Redundancy**
   - SSO and N+1 High Availability
   - Gateway Check capability
   - Standby Monitoring
2. **Upstream Switch Redundancy**
   - StackWise Pair and HSRP Topologies
3. **Link Level Redundancy**
   - LAG ON, LACP, PAGP
   - Multi-chassis LAG
4. **Access Point Link Redundancy**
   - Power over Ethernet Redundancy
   - LAG
5. **Controller Software Upgrades**
   - N+1 Site Based Hitless Upgrade
   - In Service Software Upgrade (ISSU)
6. **Software Patching Capabilities**
   - Software Maintenance Updates, AP Service Packs and Device Packs

Agenda

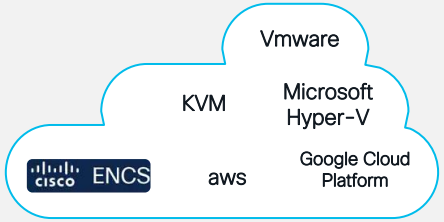
1. Wireless Controller Redundancy
   - SSO and N+1 High Availability
   - Gateway Check capability
   - Standby Monitoring
2. Upstream Switch Redundancy
   - StackWise Pair and HSRP Topologies
3. Link Level Redundancy
   - LAG ON, LACP, PAGP
   - Multi-chassis LAG

Agenda

4. Access Point Link Redundancy
   - Power over Ethernet Redundancy
   - LAG
5. Controller Software Upgrades
   - N+1 Site Based Hitless Upgrade
   - In Service Software Upgrade (ISSU)
6. Software Patching Capabilities
   - Software Maintenance Updates, AP Service Packs and Device Packs

Cisco's Complete Wi-Fi 6E And Wi-Fi 6 Wireless Stack

Enabling next-generation mobility powered by Wi-Fi 6/6E



Cisco Catalyst™ 9800 Series Wireless Controllers

Cisco Catalyst 9100 Access Points

Managed by

Cisco DNA Center

Translate business intent into network policy and capture actionable insights

Digitized by

Cisco Spaces

Digitize people, spaces, and things

Full-stack network intelligence

How long can my network be down?

Catalyst 9800 controller differentiation

	Controller Fault	Controller and AP S/W update	Image Upgrade
Standalone	• 10s of minutes for AP and client recovery	• Zero-downtime with SMU and APSP	• Tens of minutes for AP and client recovery
N+1 HA	• Noticeable Outage to clients and APs	• Zero-downtime with SMU and APSP	• No Outage to APs and Client • Automated Orchestration from Cisco DNA Center
SSO Pair	• Sub-second AP and client recovery	• Zero-downtime with SMU and APSP	• In Service Software Upgrade (ISSU)! • Automated from device and Cisco DNA Center

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 (NEW)

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 Upgrade (All Sites or Site Based) (NEW)
- In Service Software Upgrade (ISSU)

For your reference

Redundancy Feature Comparison

Functionality	AireOS	9800
SSO	Yes	Yes
N+1	Yes	Yes
RMI	Yes	Yes
Dual Active Detection	Yes	Yes
Recovery Mode	Yes	Yes
Default GW Check	Yes	Yes
LACP, PAGP with SSO	No	Yes
SMU for controller patching	No	Yes
APSP for AP Patching	No	Yes
Per-site, per-model AP Patching	No	Yes
AP device pack	No	Yes
ISSU	No	Yes
N+1 Rolling AP Upgrade	Needs Prime, Manual	Yes

For your reference

Resiliency Feature Matrix

	Functionality	EWC on AP	Embedded controller on 9K	9800-L	9800-40	9800-80	9800-CL PVT Cloud	9800-CL Public Cloud
Unplanned Events	SSO	No	Supported	Supported	Supported	Supported	Supported	No
Infrastructure updates	SMU	Supported	Supported	Supported	Supported	Supported	Supported	Supported
	APSP	Supported	Supported	Supported	Supported	Supported	Supported	Supported
	APSP Per-site	No	Supported	Supported	Supported	Supported	Supported	Supported
	APDP	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Image Upgrade	ISSU	No	No	Supported	Supported	Supported	Supported	No
	N+1 Rolling AP Upgrade	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Unplanned events

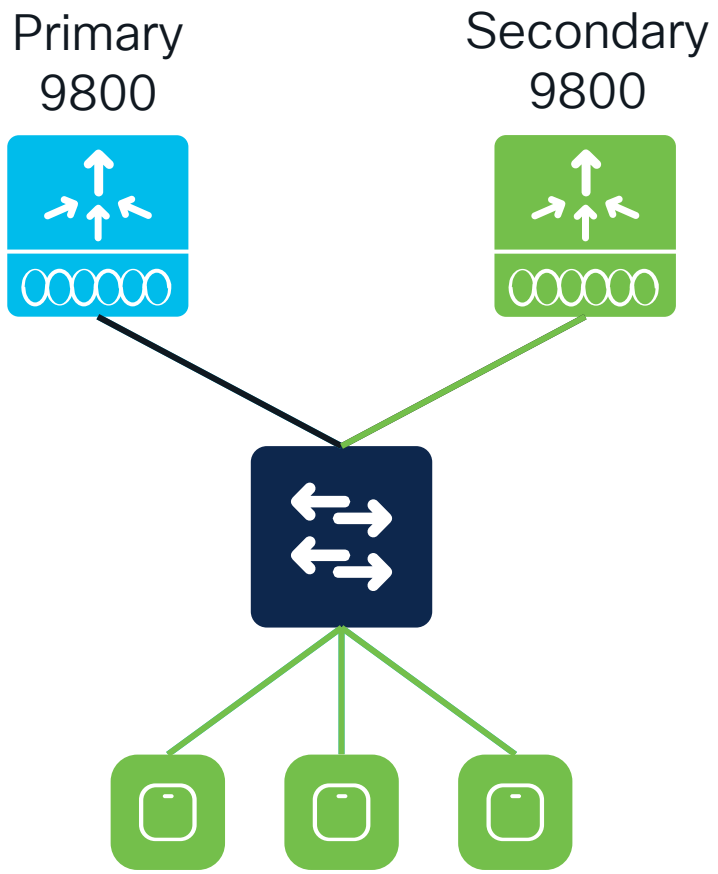
Device and network interruptions

1. Wireless Controller Redundancy

N+1 Redundancy

N+1 Redundancy

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



AP failover takes ~45-60 seconds

N+1 Redundancy Configuration

Can be configured via 2 methods

AP Join Profile

Statically on the APs

Recommended to use ONLY ONE of the methods

Configuration via AP Join Profile

Edit AP Join Profile

General | Client | CAPWAP | AP | Management | Security | ICap | QoS

High Availability | Advanced

CAPWAP Timers

Fast Heartbeat Timeout(sec)*	1
Heartbeat Timeout(sec)*	30
Discovery Timeout(sec)*	10
Primary Discovery Timeout(sec)*	120
Primed Join Timeout(sec)*	0

Retransmit Timers

Count*	5
Interval (sec)*	3

AP Fallback to Primary

Enable ☑

Allows APs to fallback to the Primary WLC upon recovery

Backup Primary Controller

Name	C9800-Secondary
IPv4/IPv6 Address	10.10.120.1

Backup Secondary Controller

Name	C9800-Tertiary
IPv4/IPv6 Address	10.10.210.1

Configuration via AP Join Profile

Edit AP Join Profile

General | Client | CAPWAP | AP | Management | Security | ICap | QoS

High Availability | Advanced

CAPWAP Timers

Fast Heartbeat Timeout(sec)*	1
Heartbeat Timeout(sec)*	30
Discovery Timeout(sec)*	10
Primary Discovery Timeout(sec)*	120
Primed Join Timeout(sec)*	0

Retransmit Timers

Count*	5
Interval (sec)*	3

AP Fallback to Primary

Enable ☑

Backup Primary Controller

Name	C9800-Secondary
IPv4/IPv6 Address	10.10.120.1

Backup Secondary Controller

Name	C9800-Tertiary
IPv4/IPv6 Address	10.10.210.1

Secondary WLC hostname and IP address

Configuration via AP Join Profile

Edit AP Join Profile

General | Client | CAPWAP | AP | Management | Security | ICap | QoS

High Availability | Advanced

CAPWAP Timers

Fast Heartbeat Timeout(sec)*	1
Heartbeat Timeout(sec)*	30
Discovery Timeout(sec)*	10
Primary Discovery Timeout(sec)*	120
Primed Join Timeout(sec)*	0

Retransmit Timers

Count*	5
Interval (sec)*	3

AP Fallback to Primary

Enable ☑

Backup Primary Controller

Name	C9800-Secondary
IPv4/IPv6 Address	10.10.120.1

Backup Secondary Controller

Name	C9800-Tertiary
IPv4/IPv6 Address	10.10.210.1

Tertiary WLC hostname and IP address

Configuration via AP Join Profile

Edit AP Join Profile

General | Client | CAPWAP | AP | Management | Security | ICap | QoS

High Availability | Advanced

Required to be a non-zero config

CAPWAP Timers

Fast Heartbeat Timeout(sec)*	1
Heartbeat Timeout(sec)*	30
Discovery Timeout(sec)*	10
Primary Discovery Timeout(sec)*	120
Primed Join Timeout(sec)*	0

Retransmit Timers

Count*	5
Interval (sec)*	3

AP Fallback to Primary

Enable ☑

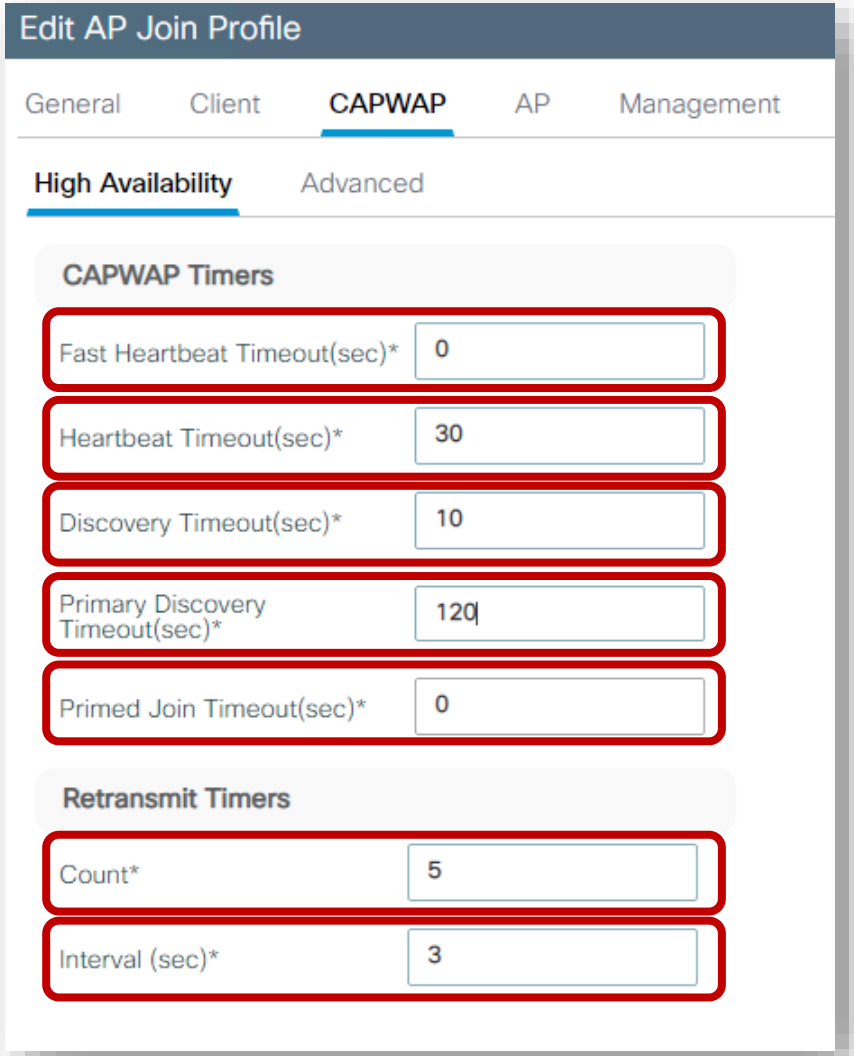
Backup Primary Controller

Name	C9800-Secondary
IPv4/IPv6 Address	10.10.120.1

Backup Secondary Controller

Name	C9800-Tertiary
IPv4/IPv6 Address	10.10.210.1

N+1 Redundancy: Timers



Fast heartbeats are dedicated packets to check the availability of Primary WLC and accelerate the failure detection and hence AP failover > 30-45 sec

- 1-10s (default is 0 = disabled). Dedicated keepalives to detect WLC failure
- 1-30s (default is 30). Regular CAPWAP keepalives
- 1-10s (default is 10). Time AP waits to process received discoveries
- 30-3000s (default is 120). Time AP would check on the Primary
- 120-43200s (default is 0 = disabled). Time AP tries to join only P/S/T

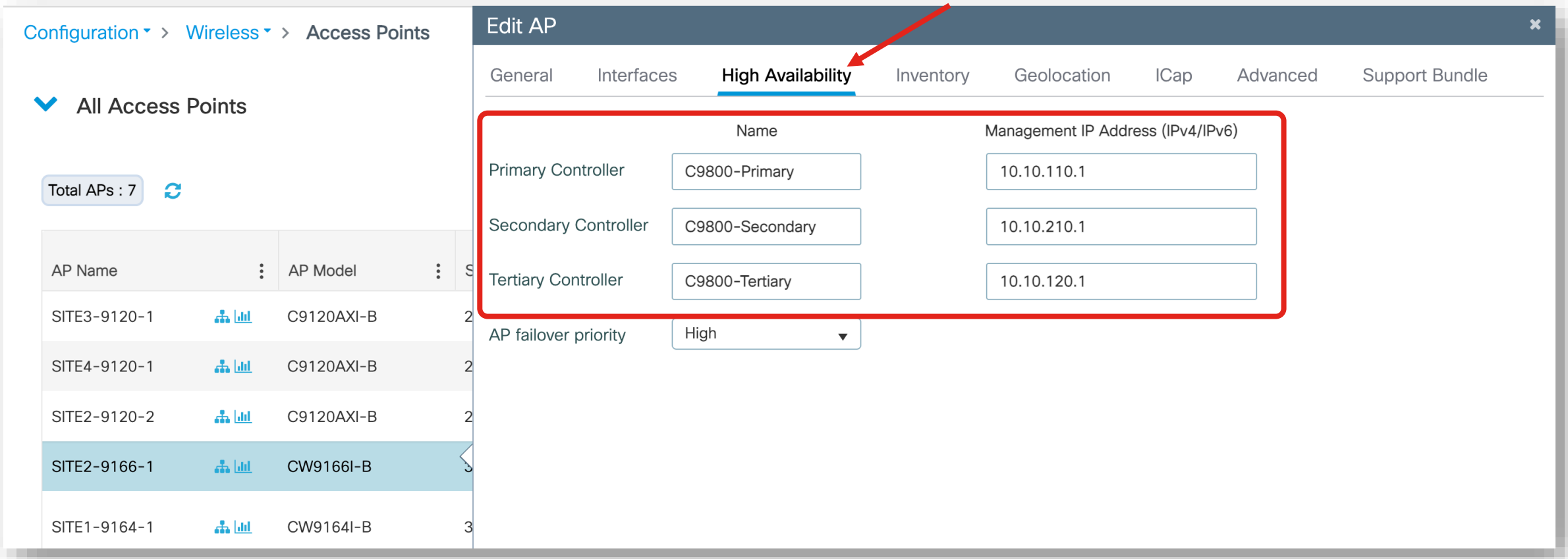
- 3-8 (default is 5)
- 2-5s (default is 3)

Verifying the AP Configuration

```
SITE4-9162-1# show capwap client ha
fastHeartbeatTmr(sec)    1 (enabled)
primaryDiscoverTmr(sec) 120
primaryBackupWlcIp       10.10.120.1
primaryBackupWlcName     C9800-Secondary
secondaryBackupWlcIp     10.10.210.1
secondaryBackupWlcName   C9800-Tertiary
DHCP renew try count     0
Fwd traffic stats get    58
Fast Heartbeat sent      58
Discovery attempt        0
Backup WLC array:
```

Settings can only be verified via the AP CLI

Configuration via the AP



Configuration via the AP

Edit AP Join Profile

General | Client | CAPWAP | AP | Management | Security | ICap | QoS

High Availability | Advanced

CAPWAP Timers

Fast Heartbeat Timeout(sec)*	1
Heartbeat Timeout(sec)*	30
Discovery Timeout(sec)*	10
Primary Discovery Timeout(sec)*	120
Primed Join Timeout(sec)*	0

Retransmit Timers

Count*	5
Interval (sec)*	3

AP Fallback to Primary

Enable ☑

Allows APs to fallback to the Primary WLC upon recovery

Backup Primary Controller

Name	
IPv4/IPv6 Address	

Backup Secondary Controller

Name	
IPv4/IPv6 Address	

Bulk Priming APs in Large Scale Deployments

Pre-IOS XE 17.10.1

- Manually enter Primary, Secondary, and Tertiary for each AP
- Not scalable to enter console of each AP and configure this

IOS XE 17.10.1 or Later

- Create an AP Priming Profile on the C9800 that automatically applies to APs when joining
- Scales to large numbers of APs joining the controller

AP Priming Profile and AP Priming Filter

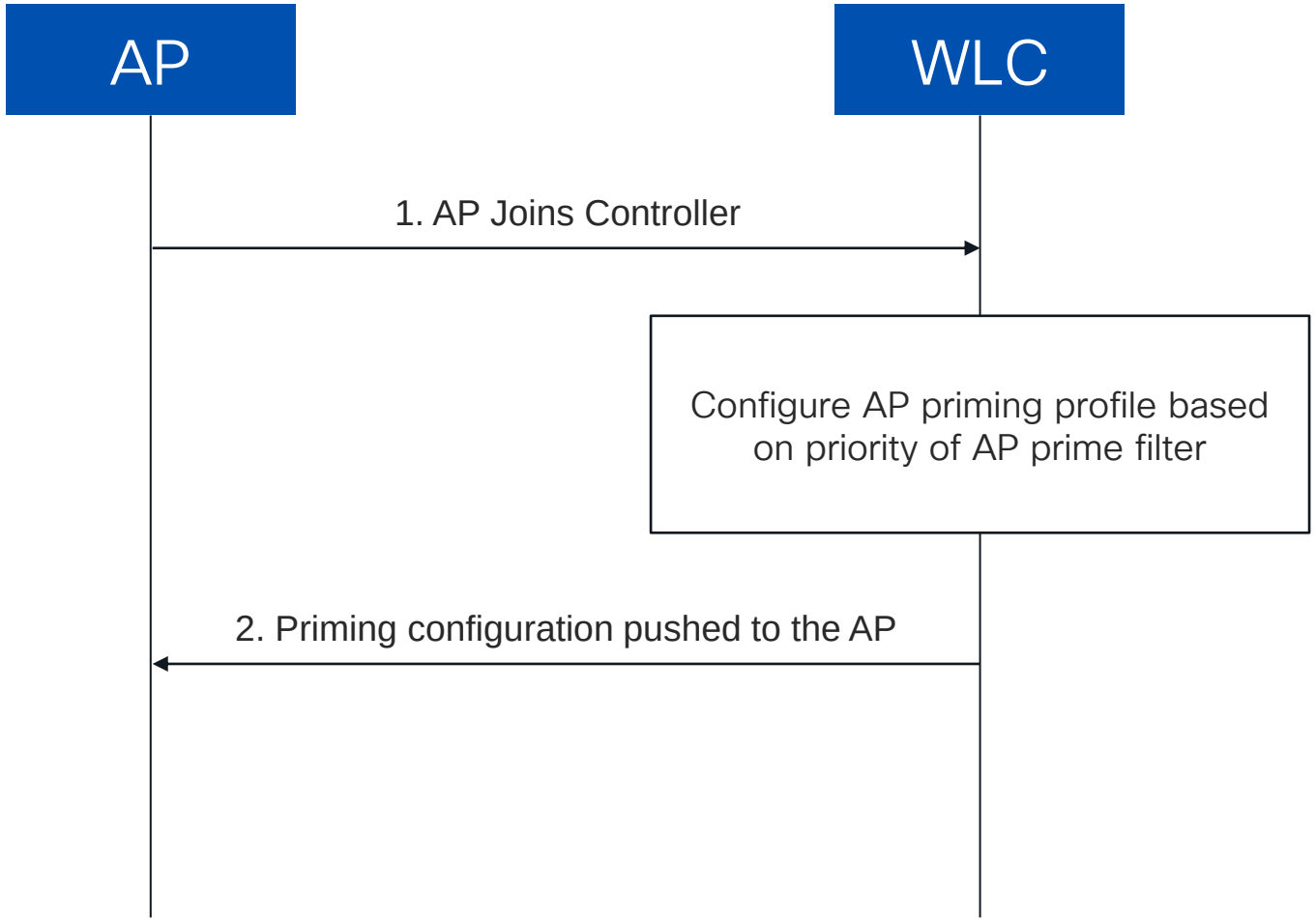
AP Priming Profile

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

AP Priming Filter

- Similar structure as the AP filter for tag mapping
- Uses RegEx string mappings to match APs based on their configured names
- Applies the mapped AP Priming Profile to the matched APs

AP Priming Join Flow



Design Considerations

- Configuration via CLI only
  - No support via WebUI
  - Cisco DNA Center directly writes WLC IP addresses on the AP
- Max of **128** AP Priming Profiles can be configured
- Max of **1024** AP filters can be configured
  - Either for tag mapping or AP priming
  - Reduces number of AP filters available for tagging

Configuring the AP Priming Profile

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

Overrides existing priming configurations
RECOMMENDED – Not enabled by default

Example Priming Profile:

```
wireless profile ap priming ap-priming-profile
 primary C9800-Primary 10.10.110.1
 secondary C9800-Secondary 10.10.210.1
 tertiary C9800-Tertiary 10.10.120.1
 priming-override
```

Configuring the AP Priming Filter

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

Example Priming Filter:

```
ap filter name ap-priming-filter type priming
 ap name-regex SITE
 profile ap-priming-profile
```

Activate AP Filter

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

Example Filter Priority:

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

Statically Assign AP Priming Profile using MAC

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

Example Static Assignment:

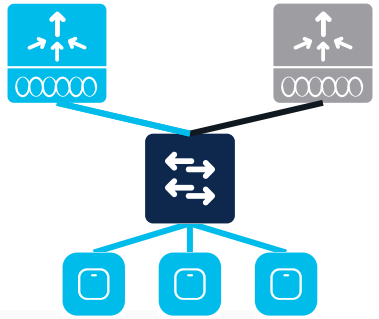
```
ap aaaa.bbbb.cccc
 profile ap-priming-profile
```

Verification
AP Priming Profile

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

```
C9800# show wireless profile ap priming detailed ap-priming-profile
Profile Name                          : ap-priming-profile
Primary Controller Name               : C9800-Primary
Primary Controller IP                 : 10.10.110.3
Secondary Controller Name             : C9800-Secondary
Secondary Controller IP               : 10.10.210.3
Tertiary Controller Name              : C9800-Tertiary
Tertiary Controller IP                : 10.10.120.3
Override                              : Enabled
```

Configure N+1 via Cisco DNA Center
Primary WLC



Cisco DNA Center — Provision / Network Devices / Provision Devices

Network Devices / Provision Devices

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

C9800-40-ACTIVE.justloo-lab.com

Serial Number: TTM22490UL7, TTM22480QSM

Devices: C9800-40-ACTIVE.justloo-lab.com

WLC Role: Active Main WLC / Anchor

Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address
VLAN100	-	100	IP Address

1 Records

Rolling AP Upgrade

Enable — AP Reboot Percentage: 25

Managed AP Location

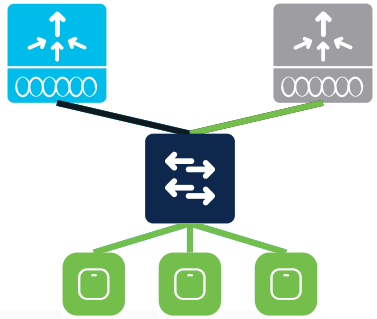
Search Hierarchy

Global (2)
- San Jose
  - Building 14
    - Floor 1

Check the boxes of the locations which the C9800 will be the Primary WLC

Cancel | Save

Configure N+1 via Cisco DNA Center
Secondary WLC



Cisco DNA Center — Provision / Network Devices / Provision Devices

Network Devices / Provision Devices

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

justloo_9800CL.justloo-lab.com

Serial Number: 9THG1Y9Y2CT

Devices: justloo_9800CL.justloo-lab.com

WLC Role: Active Main WLC / Anchor

Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address
VLAN100	-	100	IP Address

1 Records

Rolling AP Upgrade

Enable — AP Reboot Percentage: 25

Managed AP Location

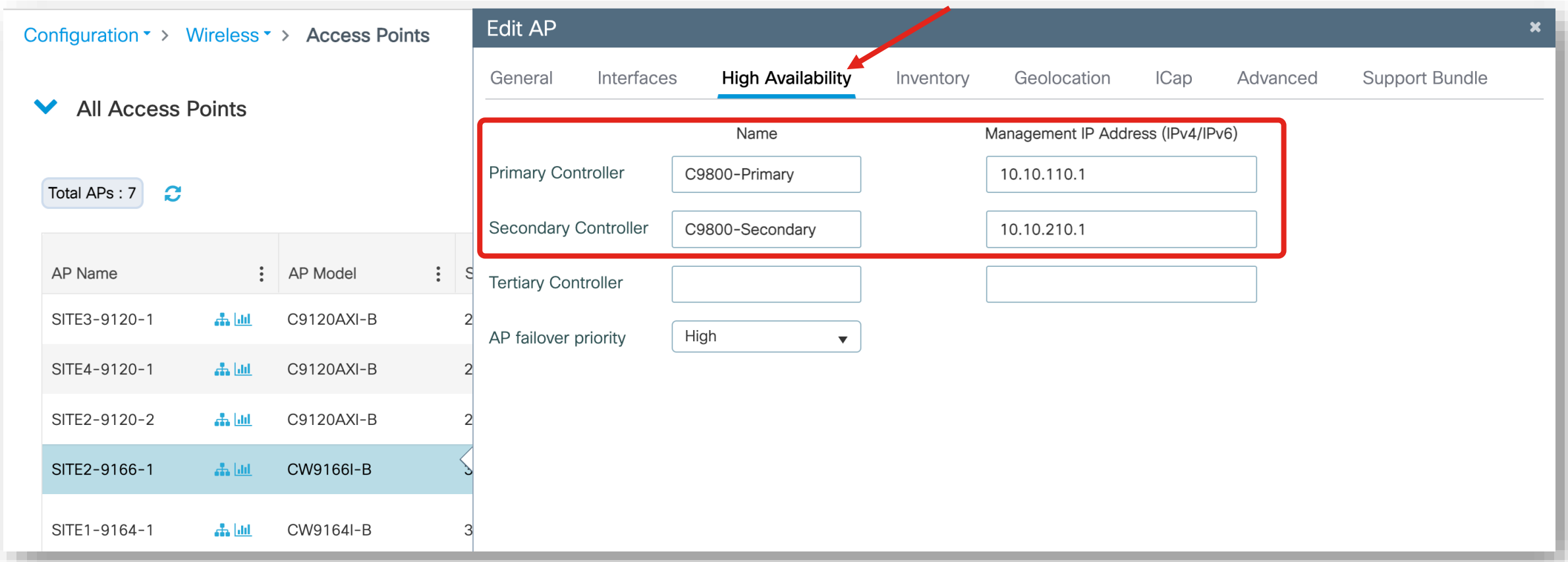
Search Hierarchy

Global (2)
- San Jose
  - Building 14
    - Floor 1

Check the boxes of the locations which the C9800 will be the Secondary WLC

Cancel | Save

Verifying via the C9800 WebUI



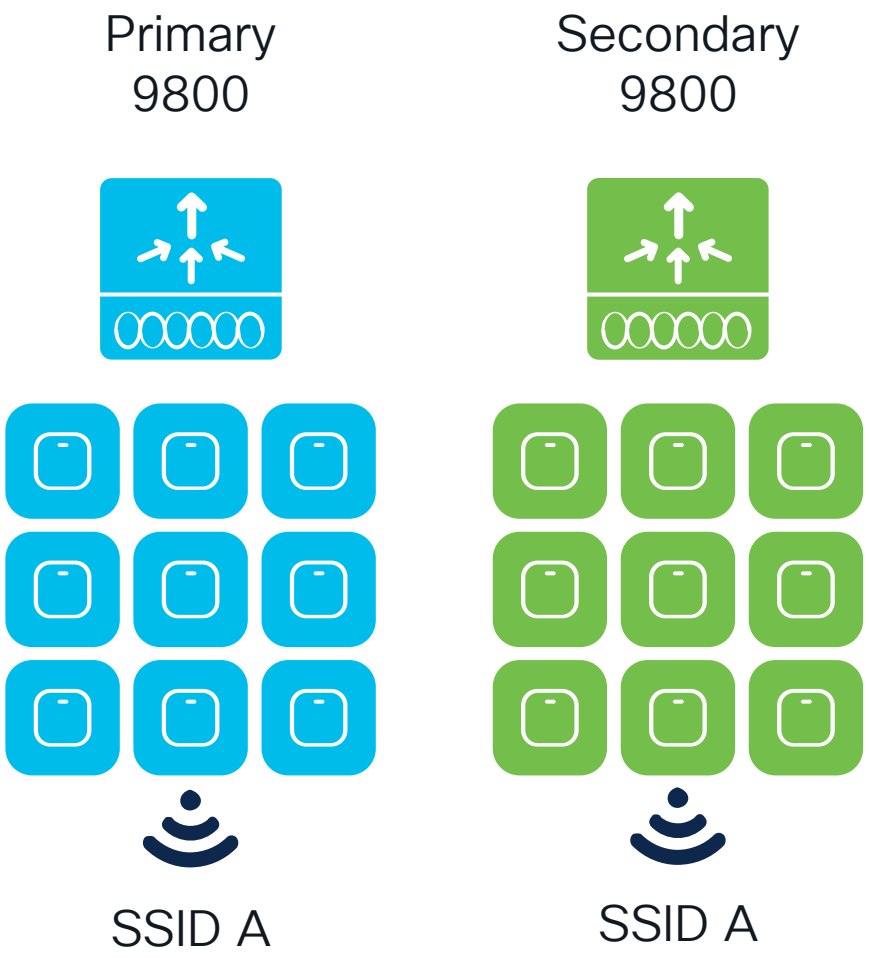
N+1 best practices

Primary and Secondary WLC should run the same software version → No AP Image Download

Configurations should be consistent across the Primary, Secondary, and Tertiary controllers (Use Cisco DNA Center to automate)

- WLANs
- Profiles and Policies
- Mobility Group
- Policy Tag
- Site Tag
- RF Tag
- AP-to-Tag Mappings

N+1 best practices: Saving AP to Tag Mappings



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

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

Pre-17.6.1: Manually write the tags to each AP

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

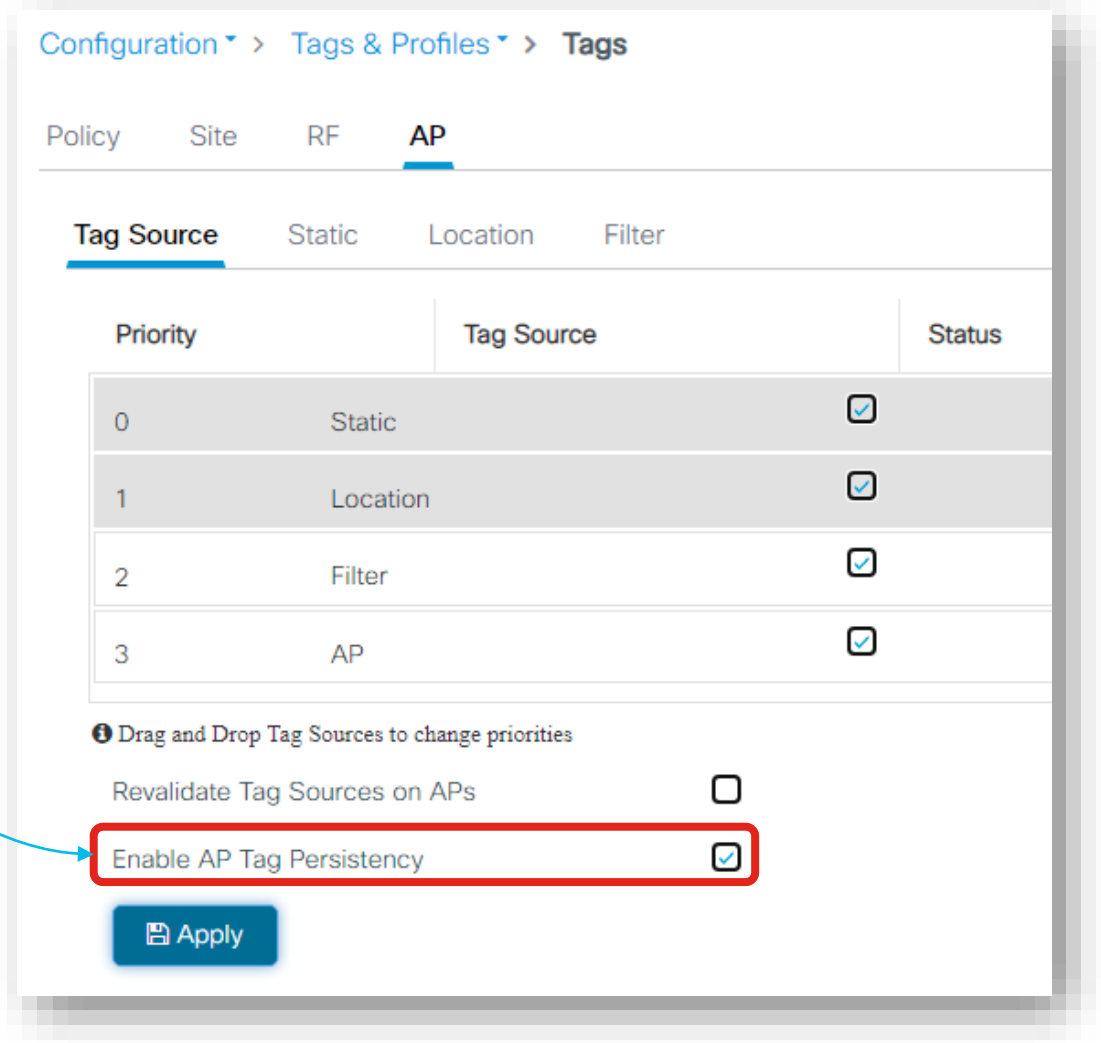
N+1 best practices: AP to Tags assignment

Configuring AP Tag Persistency (SW >17.6)

- 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

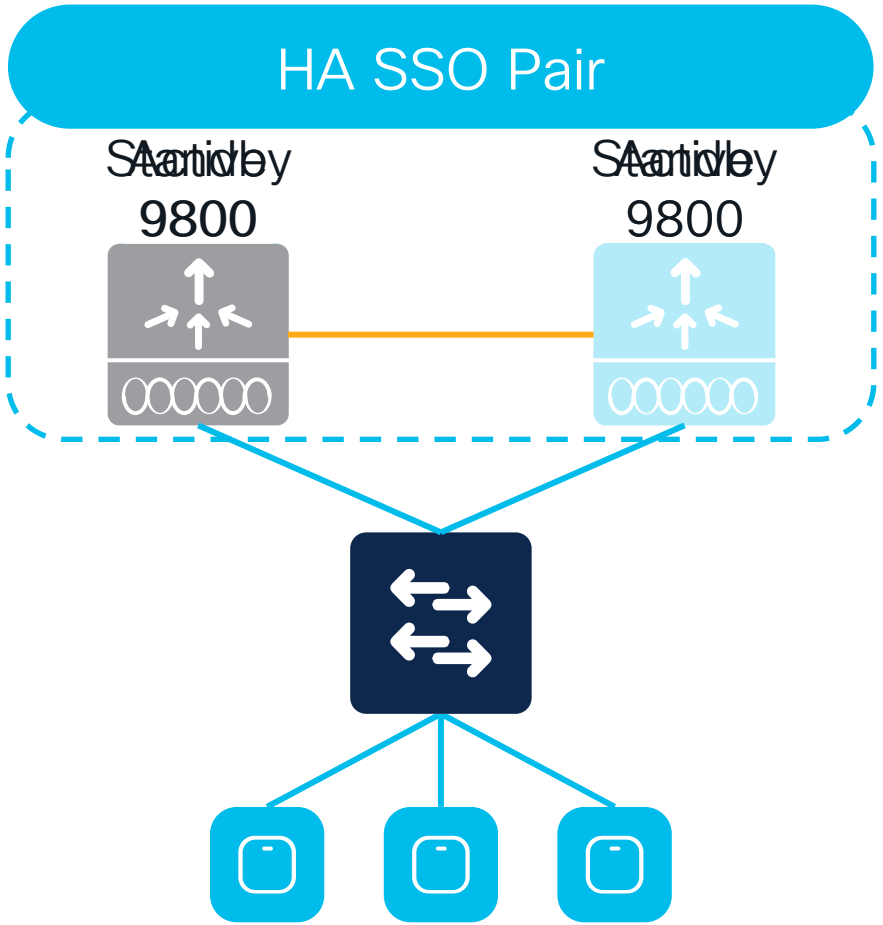
Note: This will enable writing tags to the AP as it joins. For this to be applied to existing APs joined to the C9800, they will need to rejoin the WLC (CAPWAP restart)



High Availability Stateful Switchover (HA SSO)

High Availability Stateful Switchover (HA SSO)

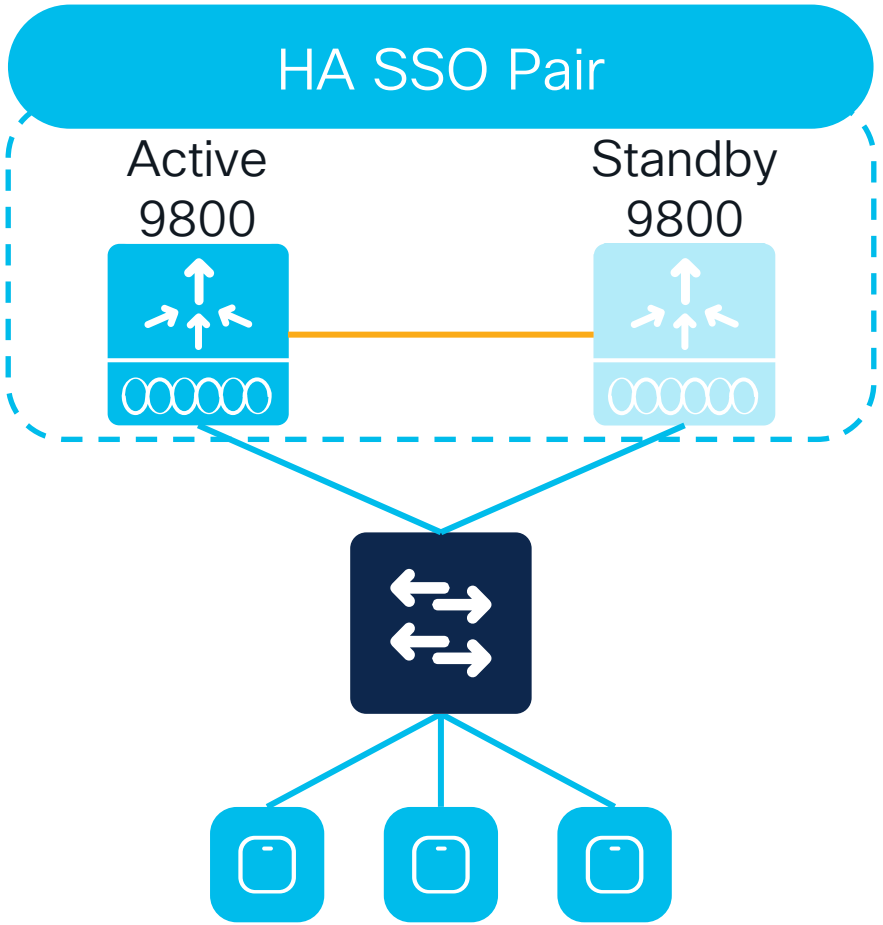
- Pair of 9800 in Active and Hot-Standby appear as a single WLC to the network
- All configuration synced between the pair for seamless, stateful switchover
- Clients and APs do not disconnect



AP failover takes order of sub seconds

High Availability Stateful Switchover (HA SSO)

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

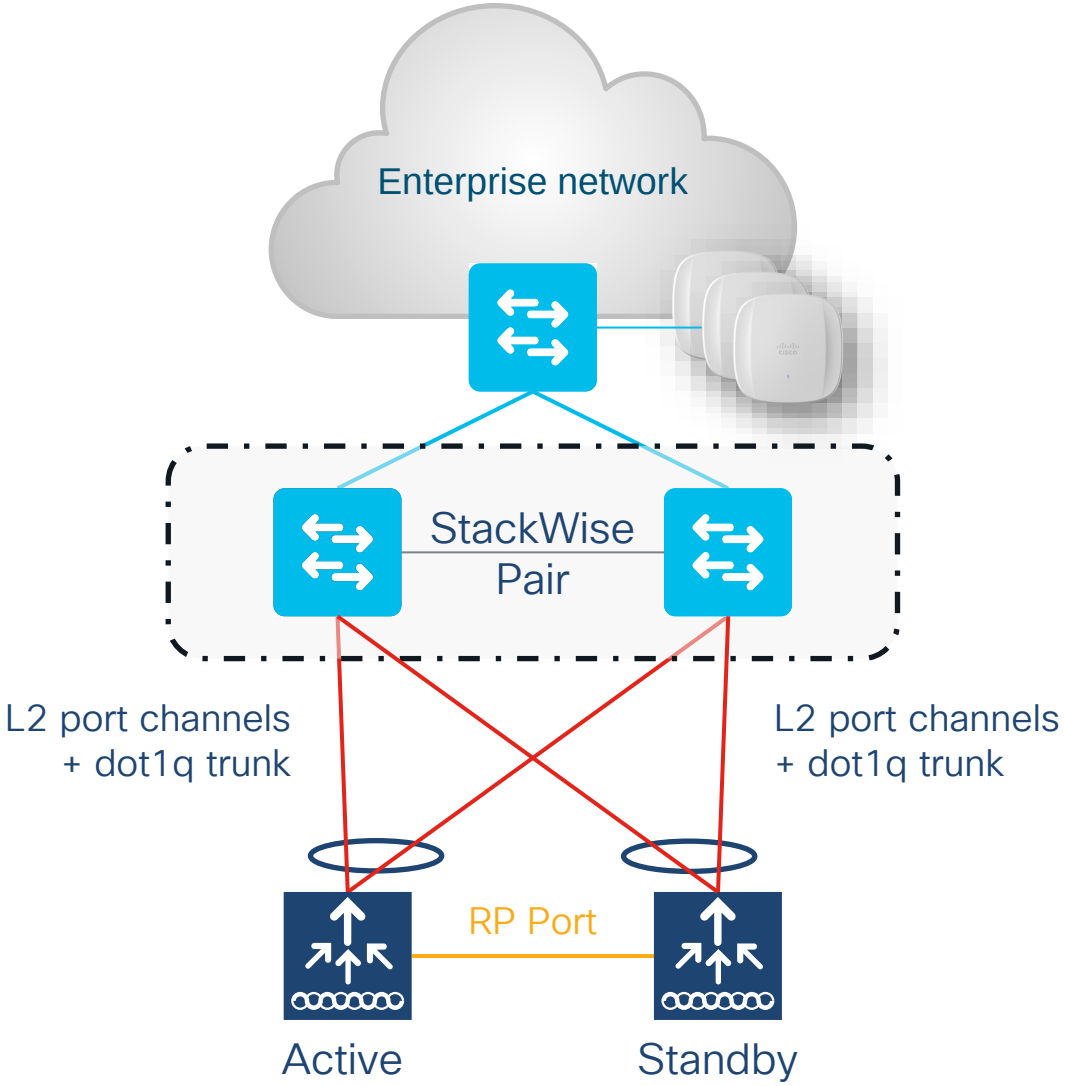


AP failover takes order of sub seconds

HA SSO behavior
Redundancy Port (RP)

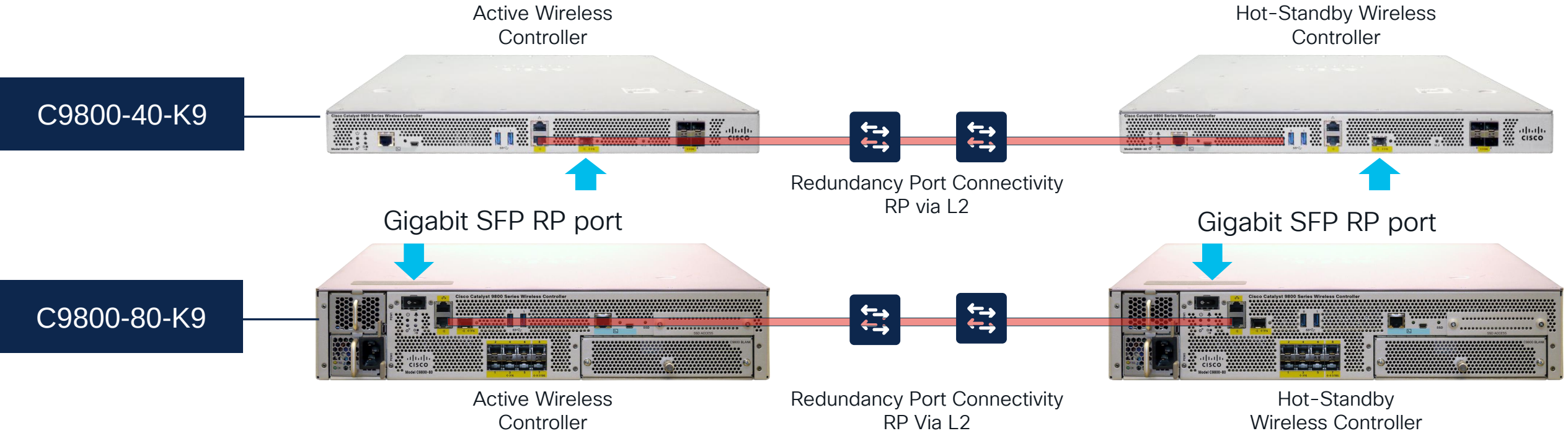
Redundancy Port (RP)

- Syncs configuration and AP/Client databases between Active and Standby
- Monitors status of the chassis
- Possible single point of failure



High Availability (SSO) on C9800-40/80

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



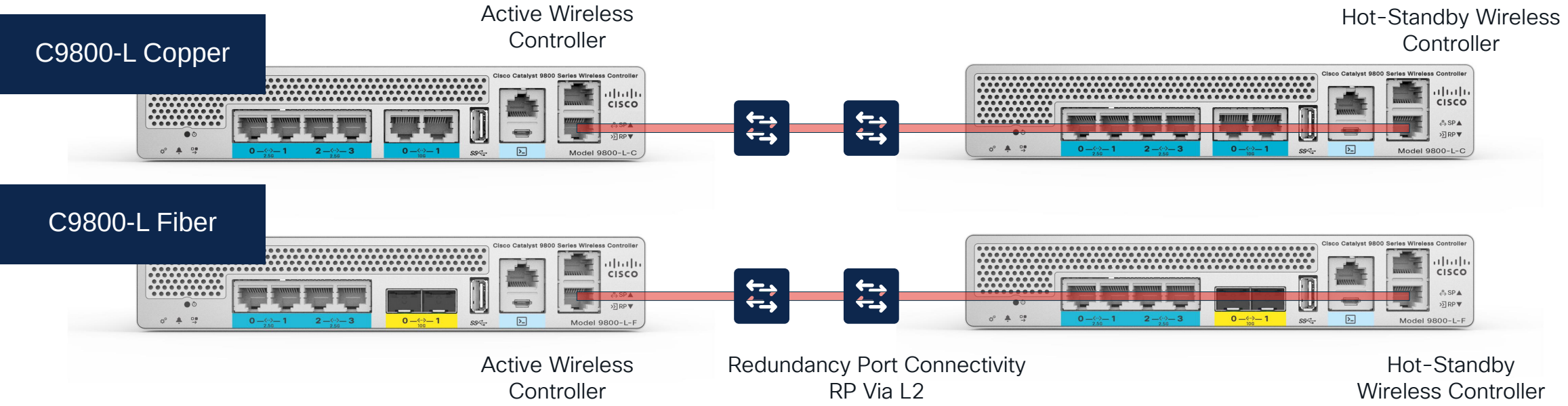
Sub-second failover and zero SSID outage

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

High Availability (Client SSO) on Catalyst 9800-L

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

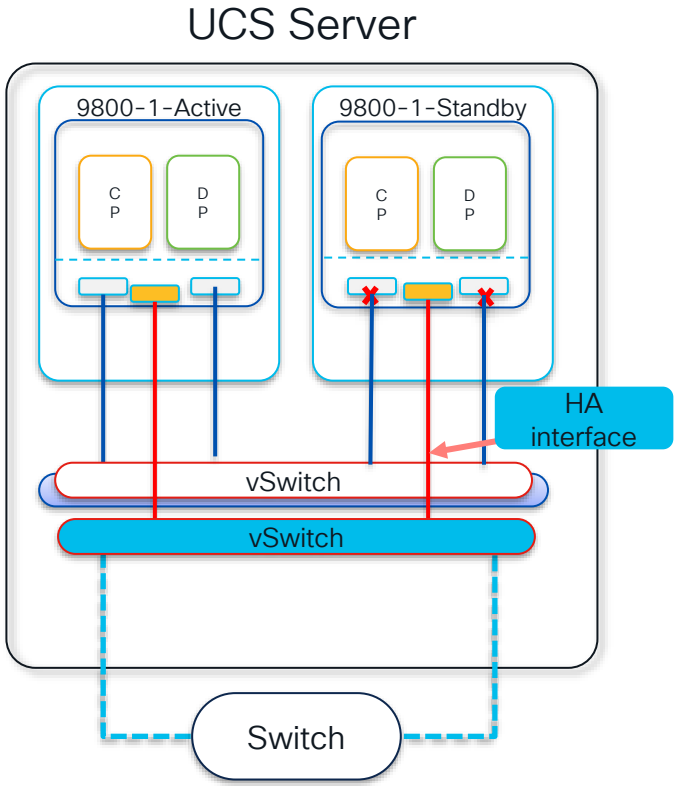
Note: There is no Fiber RP Port on 9800-L.



Sub-second failover and zero SSID outage

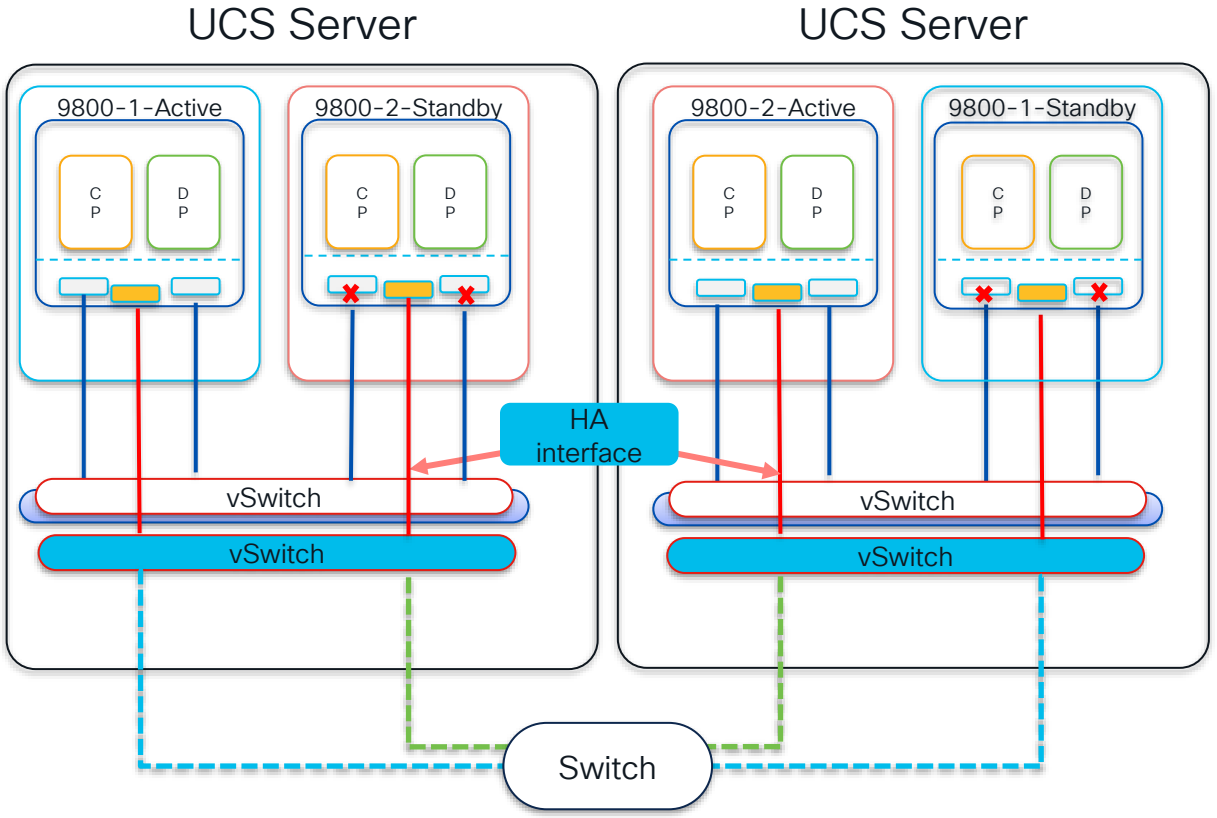
High Availability (SSO) on Catalyst 9800-CL

Intra-Host Redundancy



Redundancy Port Connectivity

Inter-Host Redundancy



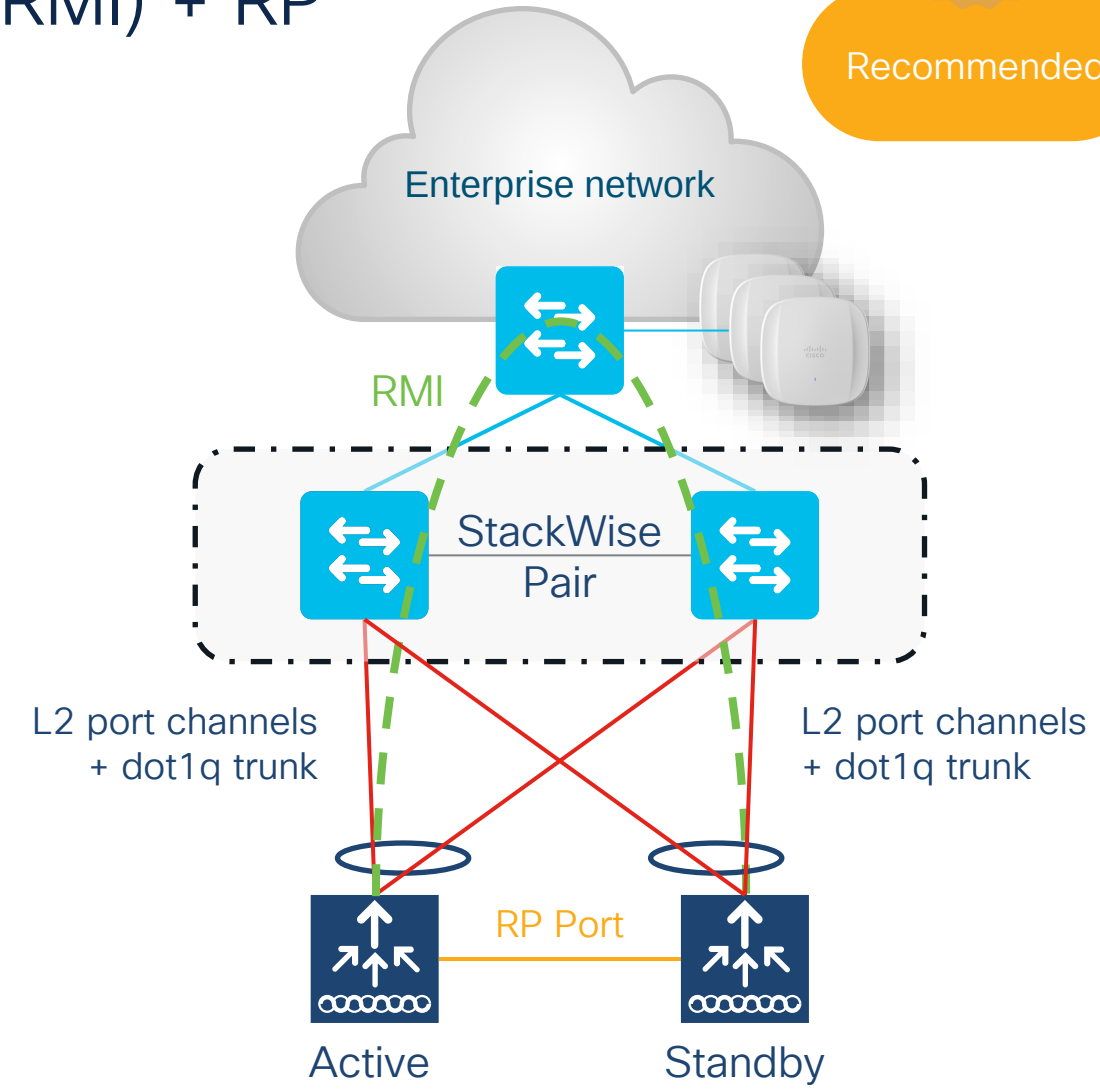
Redundancy Port Connectivity
RP via L2

HA SSO behavior
Redundancy Management Interface (RMI) + RP

Recommended

RMI + RP

- With RP only, there is no way to know if the peer is down or there is a link issue
- RMI is introduced for:
  - Default Gateway check
  - Status of peer through the network
  - Dual Active Detection
- Configure it in same subnet as the Wireless Management Interface (WMI)
- RMI can be used for remote management of the standby (SSH, Programmability)
- IPv6 support introduced in 17.3.2



SSO configuration using RMI+RP option

Recommended

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Licensing
- Troubleshooting

Walk Me Through >

Administration > Device

General

FTP/SFTP/TFTP

Redundancy

Redundancy Configuration	ENABLED
Redundancy Pairing Type	RMI+RP / RP
RMI IP for Chassis 1*	172.16.201.23
RMI IP for Chassis 2*	172.16.201.24
Management Gateway Failover	ENABLED
Gateway Failure Interval (seconds)	8
Local IP	NA
Remote IP	NA
Keep Alive Timer	1
Keep Alive Retries	5
Chassis Renumber	1
Active Chassis Priority*	2

This is the box you want to become **Active**

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

Keepalives: 1-10 ms
Retries: 5-10

Set the chassis # on each box

Set the higher priority (2) on the Active

SSO configuration using RMI+RP option

Recommended

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Licensing
- Troubleshooting

Walk Me Through

Administration > Device

General

FTP/SFTP/TFTP

Redundancy

Redundancy Configuration	ENABLED
Redundancy Pairing Type	RMI+RP / RP
RMI IP for Chassis 1*	172.16.201.23
RMI IP for Chassis 2*	172.16.201.24
Management Gateway Failover	ENABLED
Gateway Failure Interval (seconds)	8
Local IP	NA
Remote IP	NA
Keep Alive Timer	1 x 100 (milliseconds)
Keep Alive Retries	5
Chassis Renumber	2
Active Chassis Priority*	1

This is the box you want to become **Standby**

Same configuration as Active

Set the other chassis # on Standby

Set the lower priority (1) on the Standby

Verifying RMI and derived-RP configuration

Recommended

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Licensing
- Troubleshooting

Walk Me Through >

Administration > Device

- General
- FTP/SFTP/TFTP
- Redundancy

Redundancy Configuration	ENABLED
Redundancy Pairing Type	RMI+RP / RP
RMI IP for Chassis 1*	172.16.201.23
RMI IP for Chassis 2*	172.16.201.24
Management Gateway Failover	ENABLED
Gateway Failure Interval (seconds)	8
Local IP	169.254.201.23
Remote IP	169.254.201.24
Keep Alive Timer	1 x 100 (milliseconds)
Keep Alive Retries	5
Chassis Renumber	1
Active Chassis Priority*	2
Standby Chassis Priority*	1

RP IP address is auto-generated as 169.254.x.x where x.x. is from the RMI IP

View from Active

SSO HA configuration verification

Recommended

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Licensing
- Troubleshooting

Walk Me Through >

Monitoring > General > System

Inventory | Memory Utilization | CPU Utilization | Wireless Interface | Management Summary | Redundancy

General | Active Statistics | Standby Statistics

Refresh

My State	ACTIVE	Redundancy State	sso
Peer State	STANDBY HOT	Manual Swact	enabled
Unit	Primary	Communications	Up
Unit ID	1	Standby Failures	0
Redundant Mode (Operational)	sso	Switchovers System Experienced	0
Redundancy Mode(Configured)	sso		

Chassis Details

Chassis	Role	MAC Address	Priority	H/W Version	Current State	IP Address	RMI IP Address	Mobility MAC Address	Image Version
*1	Active	6c31.0e7b.c600	2	V02	Ready	169.254.201.23	172.16.201.23	6c31.0e7b.c60b	17.9.1
2	Standby	c4b2.39ec.1f80	1	V02	Ready	169.254.201.24	172.16.201.24	0000.0000.0000	17.9.1

1 10

Verifying RMI and derived-RP configuration

```
C9800# show chassis rmi

Chassis/Stack Mac Address : 00a3.8e23.8760 - Local Mac Address

Mac persistency wait time: Indefinite

Local Redundancy Port Type: Twisted Pair

                                          H/W   Current

Chassis#   Role     Mac Address     Priority Version  State                IP                      RMI-IP

-------------------------------------------------------------------------------------------------------------

 1       Standby  00a3.8e23.8760     2       V02      Ready              169.254.199.11           10.10.199.11

*2       Active   00a3.8e23.8900     1       V02      Ready              169.254.199.12           10.10.199.12
```

RP IP address is auto-generated as 169.254.x.x where x.x. is from the RMI IP

Configuring RMI over IPv6

```
[no] redun-management interface <interface name> chassis 1 address
<ipv6-1> chassis 2 address <ipv6-2>
```

- Enables/Disables redundancy
- Requires node reload after configuration is saved.
- The IPv6 address on RMI interface should be configured in the same subnet as the management interface.
- The wireless management IP and the RMI IP will appear as 2 distinct IPs in case of IPv6.

Derived RP IP when RMI over IPv6

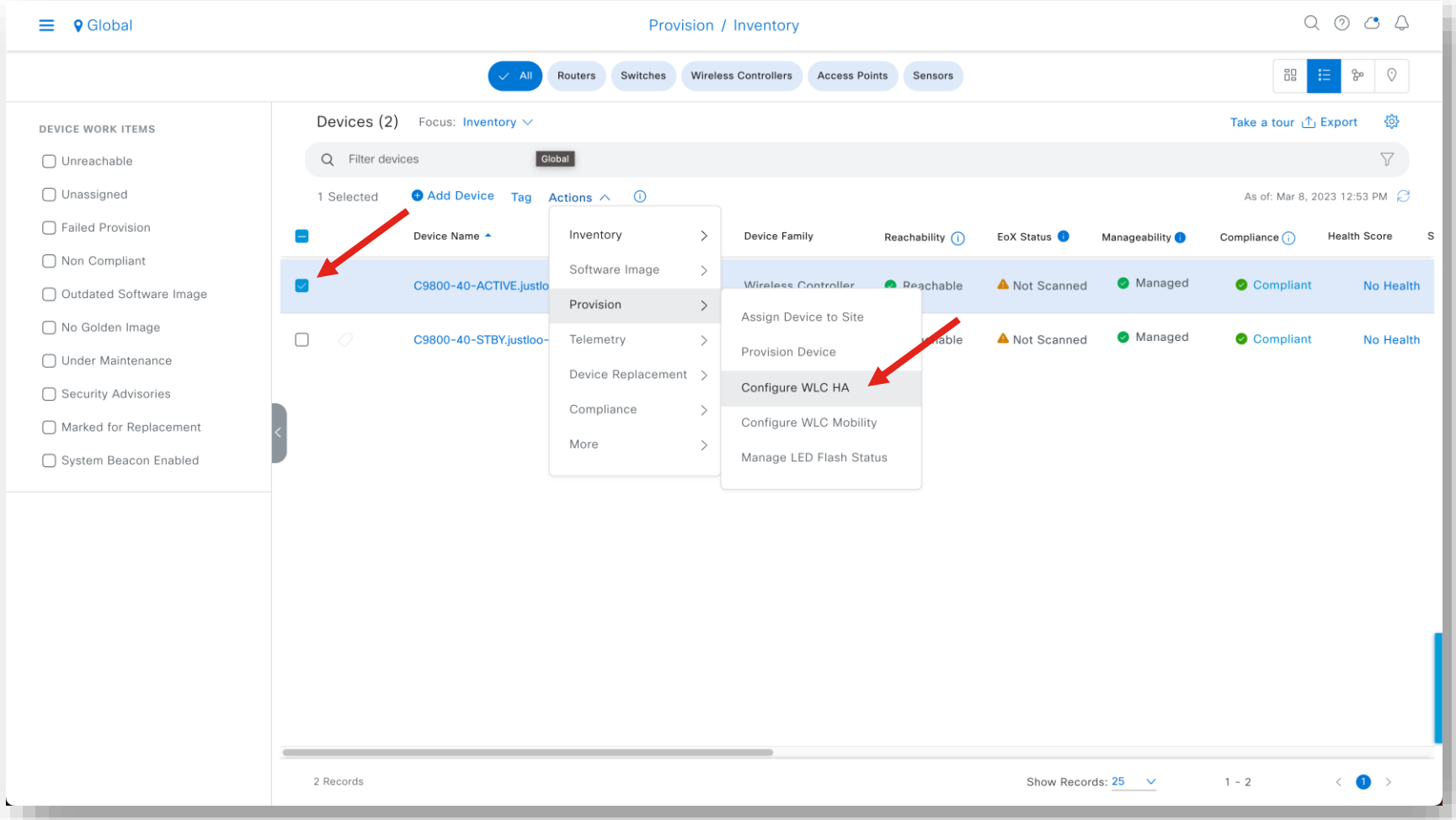
```
C9800# show chassis rmi

Chassis/Stack Mac Address : 00a3.8e23.a540 - Local Mac Address

Mac persistency wait time: Indefinite

Local Redundancy Port Type: Twisted Pair

                                          H/W   Current

Chassis#   Role     Mac Address     Priority Version  State                IP                RMI-IP

-----------------------------------------------------------------------------------------------------

*1       Active   706d.1536.23c0     1       V02      Ready              169.254.254.17     2020:0:0:1::211

 2       Standby  00a3.8e23.a540     1       V02      Ready              169.254.254.18     2020:0:0:1::212
```

Derived RP address will always be IPv4.

Configuring HA SSO via Cisco DNA Center

Select the C9800 that will be the Active Controller

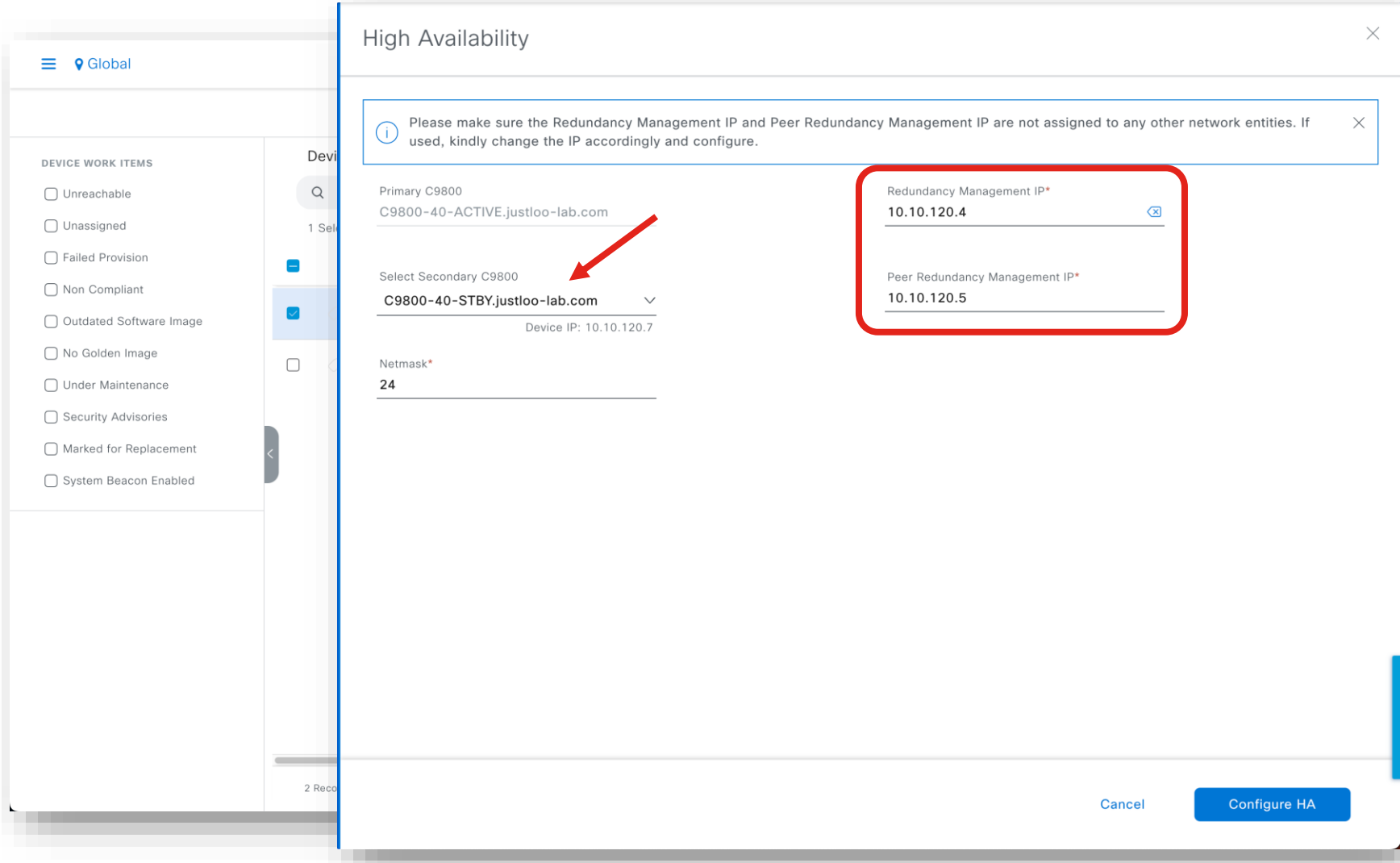
Go to Provision → Configure WLC HA



Configuring HA SSO via Cisco DNA Center

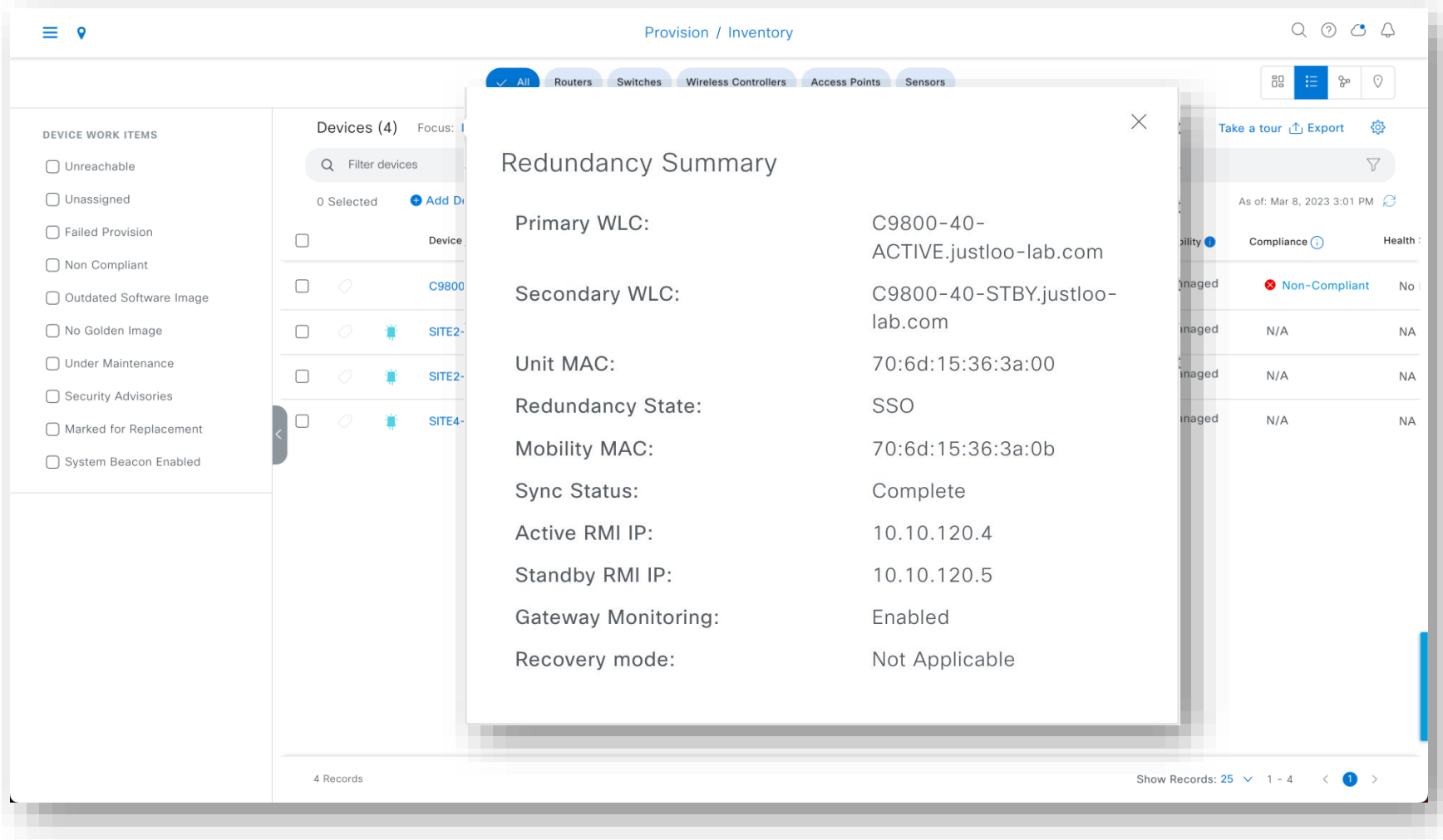
Select the C9800 that will be Hot-Standby Controller

Set the RMI IP for the Active and Standby Controllers



Configuring HA SSO via Cisco DNA Center

Clicking on the HA Icon brings up the Redundancy Summary



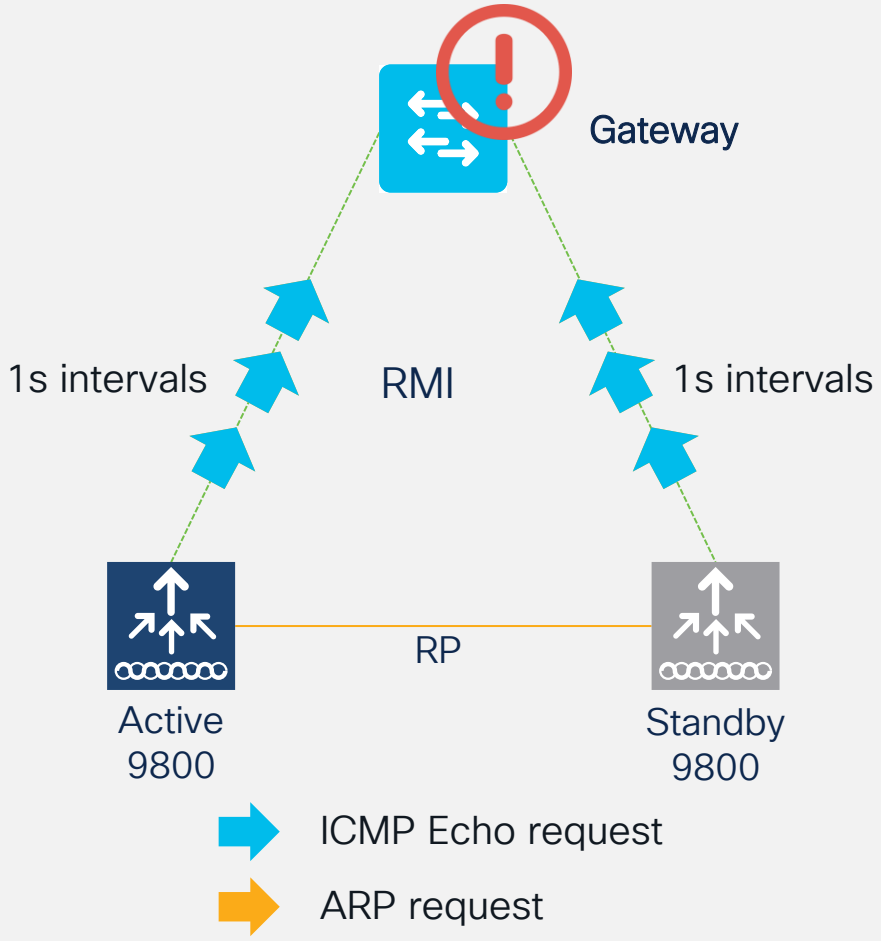
RMI Default Gateway Check

RMI Default Gateway Check

- Periodic ICMP ping to the gateway. every 1 second
- Both the active and the standby controllers use RMI IP as source IP
- 4 ICMP Echo request + 4 ARP request failures (~8 sec) = GW failure

<u>Post 17.4.1:</u>

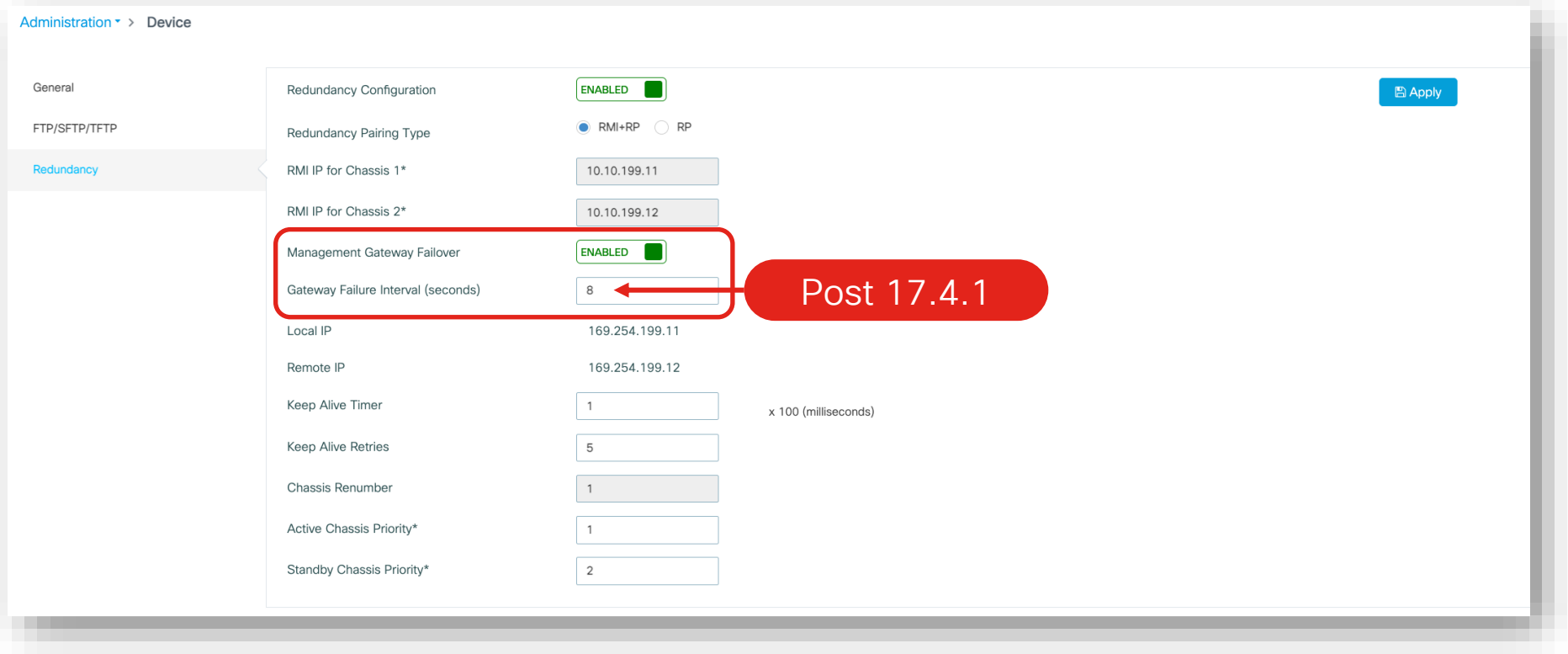
- GW failure interval is configurable – 6 to 20 seconds (Default is 8 sec)
- IPv6 only uses ICMP Echo Requests



Default Gateway Check Configuration

```
C9800(config)# management gateway-failover enable
C9800(config)# management gateway-failover interval <interval value>
```

Post 17.4.1



Verifying Default GW check command

```
C9800# show redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 2
Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso

…

Gateway Monitoring = Enabled
Gateway monitoring interval = 10 secs
```

Selecting the IP for Gateway Check

1. HA infrastructure will choose the static route IP that matches the RMI network.

2. If there are multiple static routes, the route with the broadest network scope is selected.

3. If there are multiple gateways for the same network, broadest mask and least gateway IP is chosen.

4. If the static routes are update, the gateway IP will be reevaluated.

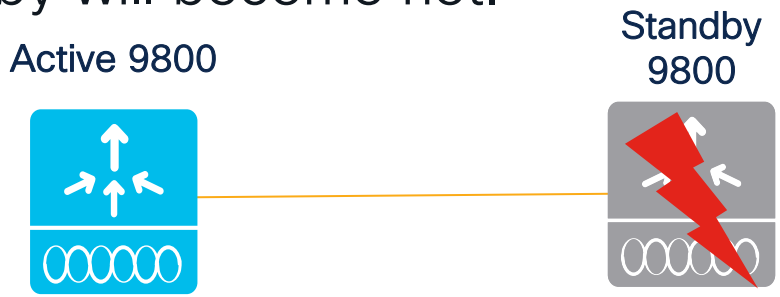
Software and network failover scenarios

Recovery Modes: Active-Recovery and Standby-Recovery

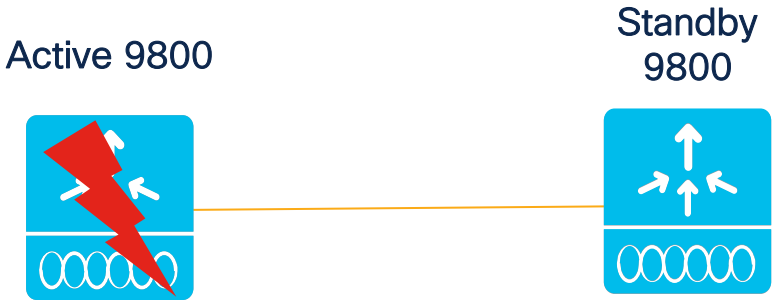
- **Recovery mode** logically means a state where the controller does not have all "resources" available to provide the service. At present, RP, RMI and Gateway are the resources. Ports will be in admin down in recovery mode, so no traffic goes through
- **Standby-Recovery:** If Gateway goes down, standby goes to standby-recovery mode. Standby means, its state is up to date with the active. But since it does not have the other resource (Gateway) it goes to Standby-Recovery. The standby shall not be in a position to take over the active functionality when it is in standby-recovery mode. Standby-Recovery will go back to Standby without a reload, once it detects that the Gateway reachability is restored.
- **Active-Recovery** is when the RP goes down. Active-Recovery does not have its internal state in sync with the Active. Active-Recovery ***must*** reload when RP comes up so that it can come up as Standby (with bulk sync).

Software Fault Handling

- If the standby controller crashes, it shall reboot and come up as standby. Bulk sync will follow, and the standby will become hot.



- If the active controller crashes, the standby becomes active. The new active shall assume the role of active and try to detect a dual active.



Software failure scenarios

Trigger	RP Link Status	Peer Reachability through RMI	Switchover	Result
Critical Process crash	Up	Reachable	Yes	Switchover happens
Forced switchover	Up	Reachable	Yes	Switchover happens
Critical Process crash	Up	Unreachable	Yes	Switchover happens
Forced switchover	Up	Unreachable	Yes	Switchover happens
Critical Process crash	Down	Reachable	No	No action, one controller will be in recovery mode already.
Forced switchover	Down	Reachable	N/A	No action, one controller will be in recovery mode already.
Critical Process crash	Down	Unreachable	No	Double fault – as mentioned in Network Error handling
Forced switchover	Down	Unreachable	N/A	Double fault – as mentioned in Network Error handling

Network failure scenarios

RP Link	Peer reachability through RMI	Gateway From Active	Gateway from Standby	Switchover	Result
Up	Up	Reachable	Reachable	No	No action
Up	Up	Reachable	Unreachable	No	No Action. Standby is not ready for SSO in this state as it does not have gateway reachability. The standby shall be shown to be in standby-recovery mode. If the RP goes down, standby (in recovery mode) shall become active.
Up	Up	Unreachable	Reachable	Yes	Gateway reachability message is exchanged over the RMI + RP links. Active shall reboot so that standby becomes active.
Up	Up	Unreachable	Unreachable	No	With this, when the active SVI goes down, so will the standby SVI. A switchover is then triggered. If the new active discovers its gateway to be reachable, the system shall stabilise in Active - Standby Recovery. Otherwise, switchovers will happen in a ping-pong fashion.

Network failure scenarios contd.

RP Link	Peer reachability through RMI	Gateway From Active	Gateway from Standby	Switchover	Result
Up	Down	Reachable	Reachable	No	No Action
Up	Down	Reachable	Unreachable	No	Standby is not ready for SSO in this state as it does not have gateway reachability. Standby will go to recovery mode as LMP messages are exchanged over the RP link also.
Up	Down	Unreachable	Reachable	Yes	Gateway reachability message is exchanged over RP link also. Active shall reboot so that standby becomes active.
Up	Down	Unreachable	Unreachable	No	With this, when the active SVI goes down, so will the standby SVI. A switchover is then triggered. If the new active discovers its gateway to be reachable, the system shall stabilise in Active - Standby Recovery. Otherwise, switchovers will happen in a ping-pong fashion.

Network failure scenarios contd.

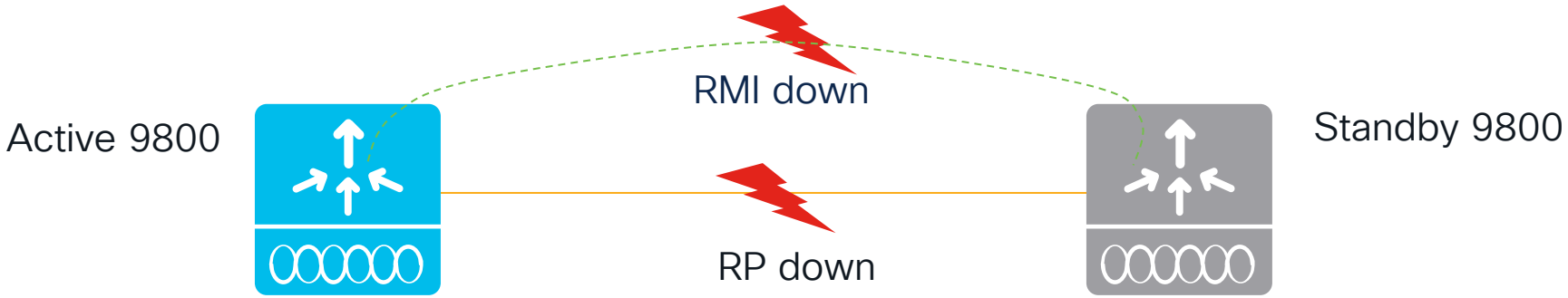
RP Link	Peer reachability through RMI	Gateway From Active	Gateway from Standby	Switchover	Result
Down	Up	Reachable	Reachable	Yes	Standby will become active with (old) active going to active-recovery. Config mode is disabled in active-recovery mode. All interfaces will be ADMIN DOWN with the wireless management interface having RMI IP. The controller in Active Recovery will reload to become standby when the RP link comes UP.
Down	Up	Reachable	Unreachable	Yes	Same as above
Down	Up	Unreachable	Reachable	Yes	Same as above
Down	Up	Unreachable	Unreachable	Yes	Same as above

Network failure scenarios contd.

RP Link	Peer reachability through RMI	Gateway From Active	Gateway from Standby	Switchover	Result
Down	Down	Reachable	Reachable	Yes	Double fault – this may result in a network conflict as there will be 2 active controllers. Standby becomes active. Old active also exists. Role negotiation has to happen once the connectivity is restored and keep the active that came up last
Down	Down	Reachable	Unreachable	Yes	Same as above
Down	Down	Unreachable	Reachable	Yes	Same as Above
Down	Down	Unreachable	Unreachable	Yes	Same as Above

RMI down during bootup

- Note that the RMI is down during boot up. If RP is also down during boot up, it is similar to the case illustrated below.



- The system is in the same state as during a double fault. There is no graceful handling of double faults. The system recovers from this state by checking the timestamps since the controller became active. The controller that has been active for a longer duration shall go to Recovery state.
- Recommendation: Connect RP ports before configuring SSO

Dual Active Detection

Active selection for GW reachability loss handling

Comments	State of Controller 1	State of Controller 2	Active
Scenario: Working condition with no faults	Active	Standby	Active (Controller 1)
Scenario: RP link down with RMI link up	Active	Active in Recovery Mode	Active (Controller 1)
Scenario: RP link and RMI link are down. Each controller does not know about the existence of the other – split brain condition	Active	Active	Both are active
Scenario: System that has auto-recovered from the split brain condition.	Active	Standby	Active (Controller 1)
Scenario: RP link down and hence standby became active. Previous active still exists. The old active will finally go to Recovery State – same as (2) above. The latest active is the active here as in cases where GARP is used to claim the management IP, the IP will belong to the latest active.	Active	Active	Latest Active

HA SSO - Managing Standby WLC

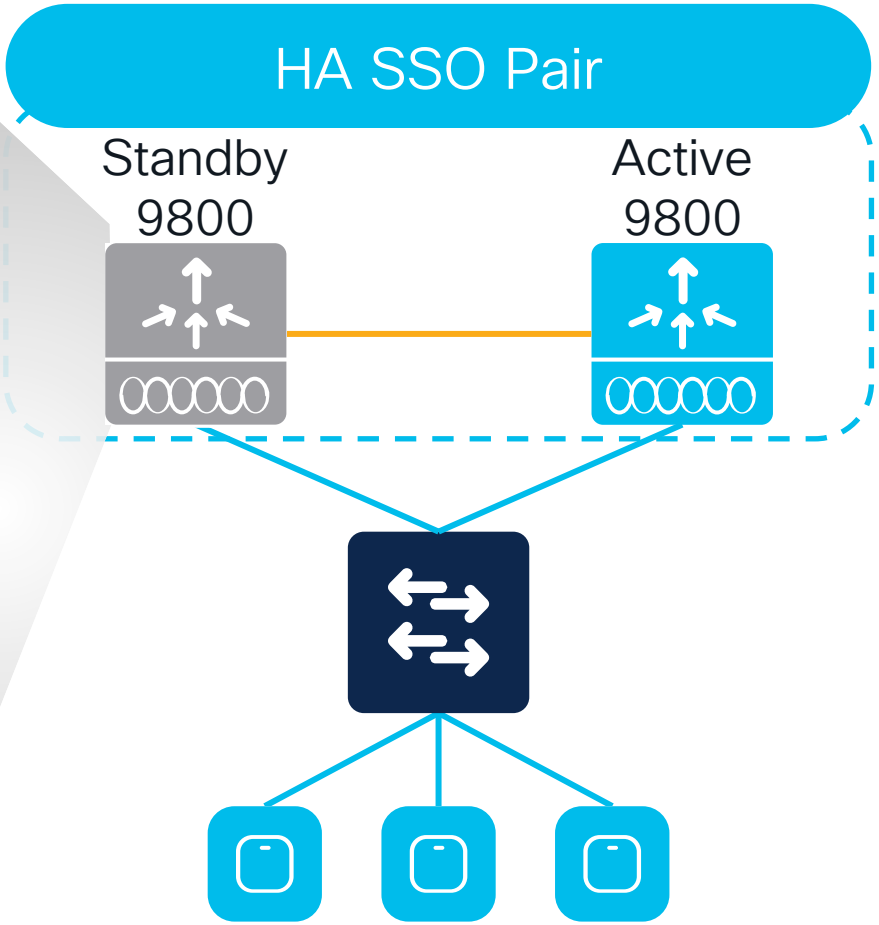
High Availability Stateful Switchover (HA SSO)

Managing Standby WLC directly:

- Use IOS XE CLI show commands, SSH, programmable interfaces (Netconf, RESTCONF, etc.) or SNMP to monitor the status off the Standby
- For SNMP, only OIDs from IF-MIB are officially supported (ifDescr, ifOperStatus)
- To enable console port access, from active configure:

```
redundancy
 mode sso
 main-cpu
  standby console enable
```

- For SNMP and SSH (including Netconf/RESTCONF) use RMI interface
- If external server is configured on active, syslog messages are sent also from the Standby RMI (IOS XE > 17.5)
- SP port is not available on Standby WLC



High Availability Stateful Switchover (HA SSO)

Managing Standby WLC directly:

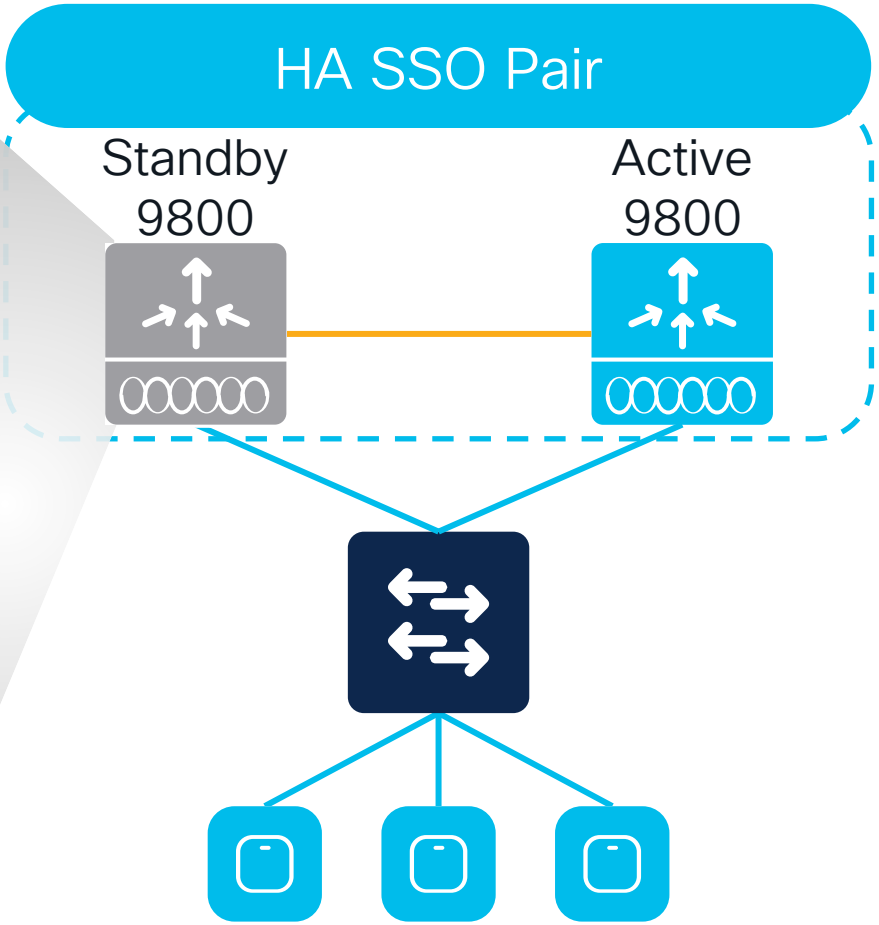
With Netconf/RESTCONF, you can get interfaces, CPU and memory status. Login via SSH on port 830 and get the Yang models supported:

ssh <username>@<RMI's IP> -p 830

An example:

admin@172.16.201.24's password:

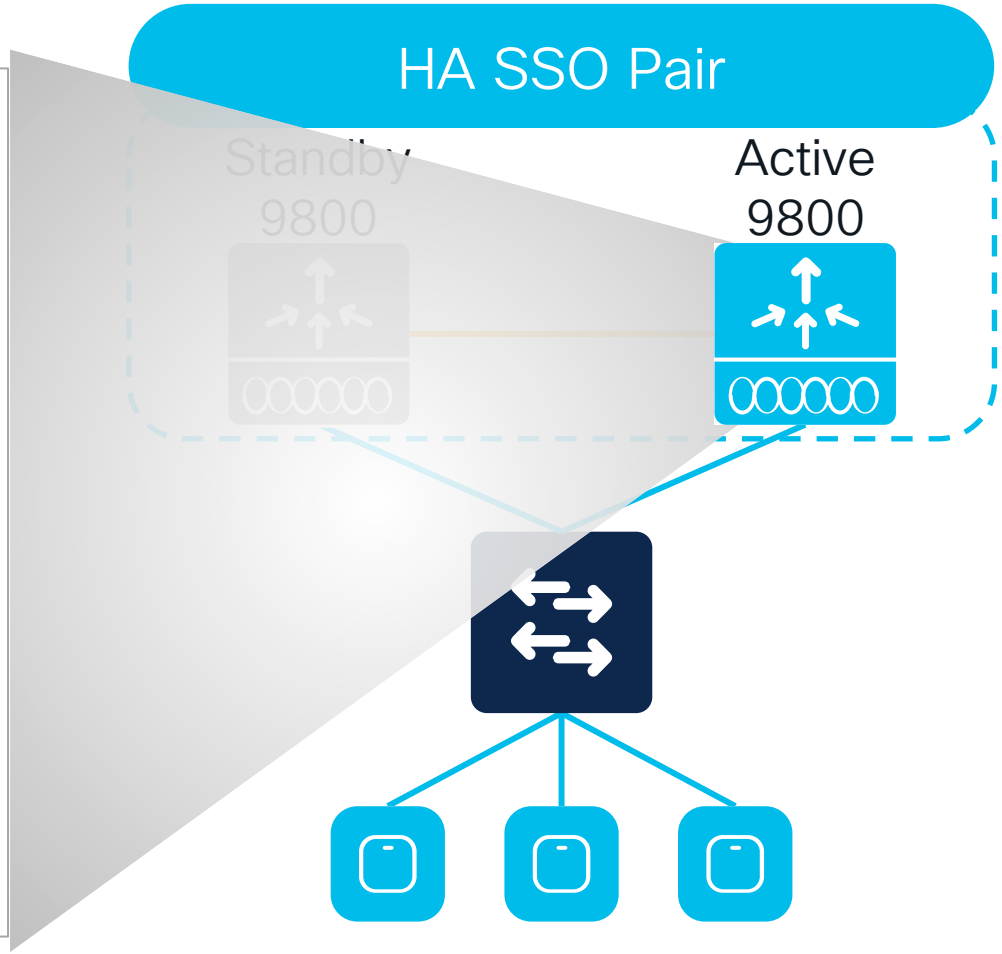
```
<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
[...]
<capability>http://cisco.com/ns/yang/Cisco-IOS-XE-process-cpu-oper?module=Cisco-IOS-XE-process-cpu-oper&amp;revision=2019-05-01</capability>
<capability>http://cisco.com/ns/yang/Cisco-IOS-XE-process-memory-oper?module=Cisco-IOS-XE-process-memory-oper&amp;revision=2019-05-01</capability>
```



High Availability Stateful Switchover (HA SSO)

Managing Standby through Active WLC:

- More SNMP OIDs are available through Active (use CISCO-LWAPP-HA-MIB and CISCO-PROCESS-MIB):
  - IfName, ifAdminStatus, ifOperStatus
  - CPU (e.g., Object name: cpmCPUTotal1min)
  - Memory (e.g., Object Name: cpmCPUMemoryUsed)
  - HA Events (e.g., Object Name: cLHaPeerHotStandbyEvent)
- With Netconf/RESTCONF: info available via model Cisco-IOS-XE-ha-oper-transform.yang
- All redundancy IOS XE CLIs with “chassis standby”, example “sh env chassis standby” or show platform software process slot chassis standby, etc.



HA SSO
Best Practices

SSO best practices
Forming SSO Pair

Appliance Type

- Physical Appliances: Use exact same hardware model
  - C9800-L-C cannot pair with C9800-L-F
- C9800-CL Private Cloud: Pick same scale (Large, Medium, or Small) and throughput (Normal or High) template for both VMs

Software

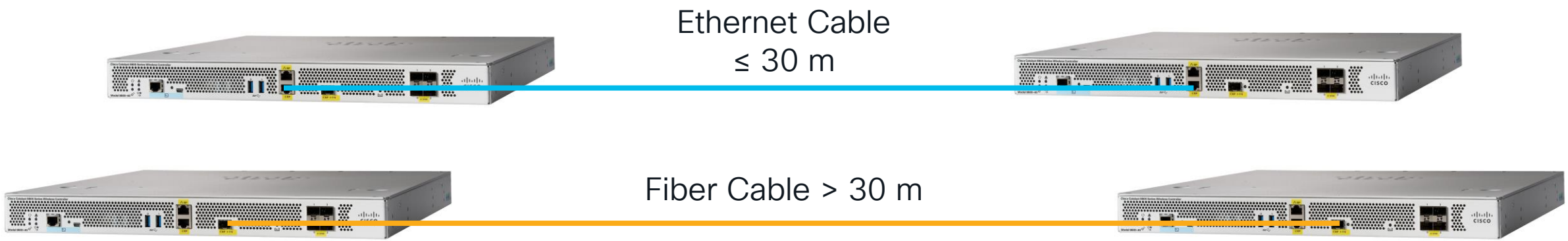
- Both boxes are running the same software and in the same boot mode
- Install mode is recommend

Configurations

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

SSO best practices
Back-to-Back Redundancy Port Connections

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



SSO best practices
C9800-CL Private Cloud with vMotion

vMotion is supported for C9800-CL with caveats

vMotion

- Do not run vMotion on both active and standby simultaneously

Networking

- RP port keepalive timer set to 3 (3 x 100ms) – default is 1
- vSwitch Virtual Guest Tagging (VGT): Initiate traffic from WLC to update ARP table for uplink switch
- SR-IOV does not supported for vMotion and Snapshot

Storage

- Local Storage: RAID 0
- Remote Storage: Less than 10ms latency and 10G link

vMotion: Requirements

- Use recommended tested software releases:
  - ESXi vCenter 6.7
  - C9800-CL software 17.9.2 and above
- Latency (RTT) between the remote storage to the server where C9800-CL is running should be < 10 ms
- C9800-CL VM shouldn't have any ESXi host specific mapping like CD/DVD, serial console port connection, etc.
- VMware guidelines:
  - Host, remote shared storage and networking configuration: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vcenterhost.doc/GUID-D19EA1CB-5222-49F9-A002-4F8692B92D63.html
  - Networking requirements: https://docs.vmware.com/en/VMwarevSphere/6.7/com.vmware.vsphere.vcenterhost.doc/GUID-3B41119A-1276-404B-8BFB-A32409052449.html

vMotion testing results : C9800-CL Standalone

Test	vMotion type	Observations/Comments
1	Compute resource only	Caveat: APs and clients drop seen, which recover after some time, due to Virtual Guest Tagging (802.1q VLAN) issue: https://kb.vmware.com/s/article/2113783 Workaround: Start continuous ping from the controller to any wired network device
2	Storage only	Supported: APs and Clients are stable, single ping drop is seen
3	Compute resource and storage	Caveat: APs and clients drop seen, which recover after some time, due to Virtual Guest Tagging (802.1q VLAN) issue: https://kb.vmware.com/s/article/2113783 Workaround: Start continuous ping from the controller to any wired network device

vMotion testing results: Active C9800-CL

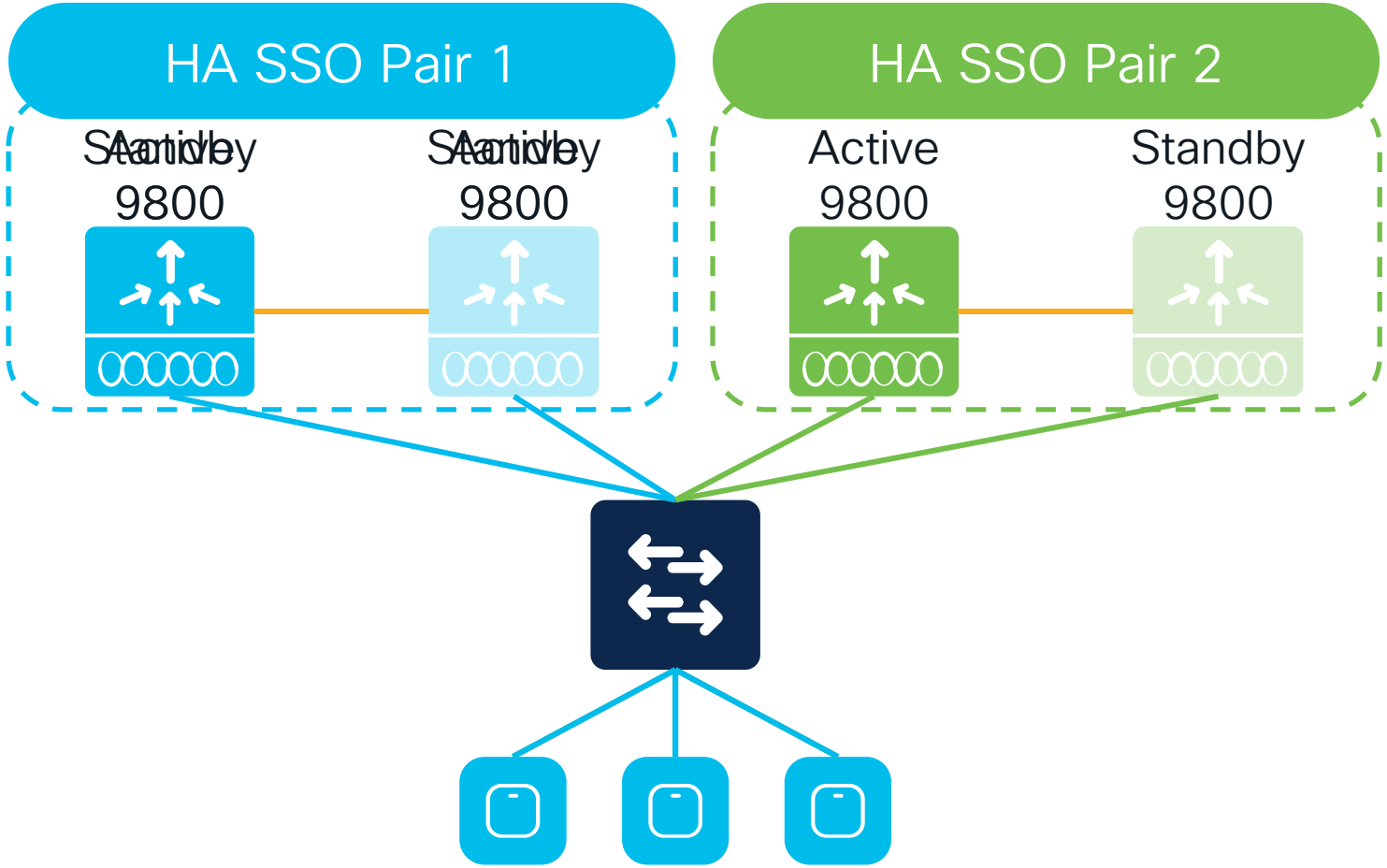
Test	vMotion type	Observations/Comments
1	Compute resource only	Supported: APs and Clients are stable, single ping drop is seen on active, standby also stable
2	Storage only	Supported: APs and Clients are stable, single ping drop is seen on active, stand also stable
3	Compute resource and storage	Supported: APs and Clients are stable, single ping drop is seen on active, stand also stable

- RP keep alive timer is set to 2 or 3 (recommended)
- The Redundancy Management Interface (RMI) is leveraged to check reachability to the gateway, and it generates the traffic that keep the MAC address table on the vswitch updated and the Virtual Guest Tagging problem doesn't happen
- Same results when Standby is moved

Combined HA SSO and N+1

Redundancy with HA SSO and N+1

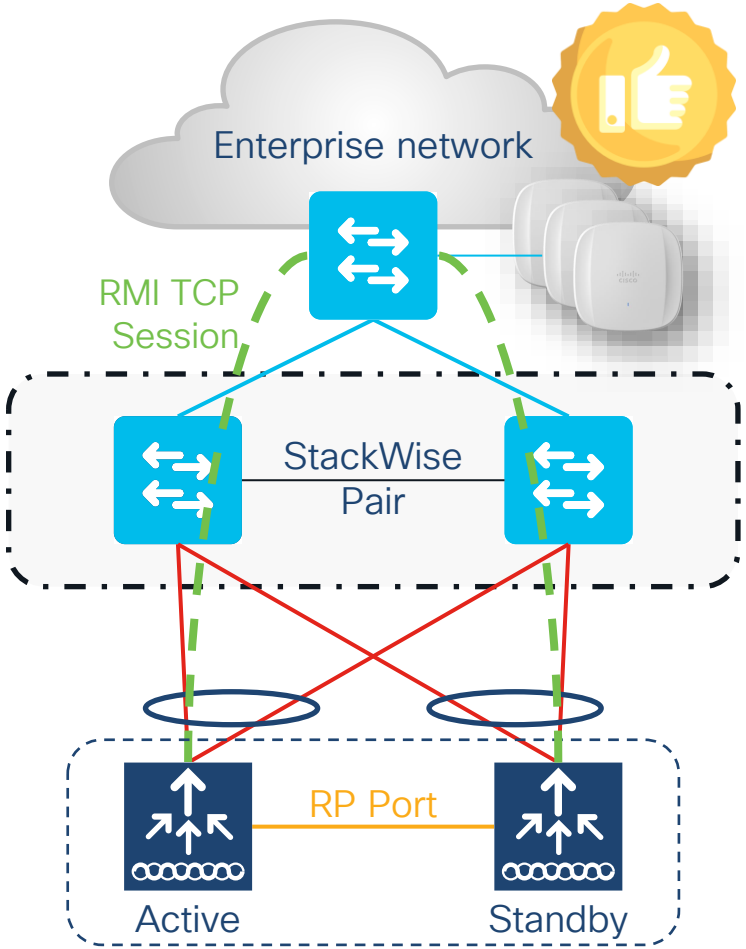
- Highest redundancy model
- Take advantage of sub-second failover
- Redundancy in the event SSO New-Active fails before the Old-Active is recovered
- Hitless upgrades for non-ISSU releases



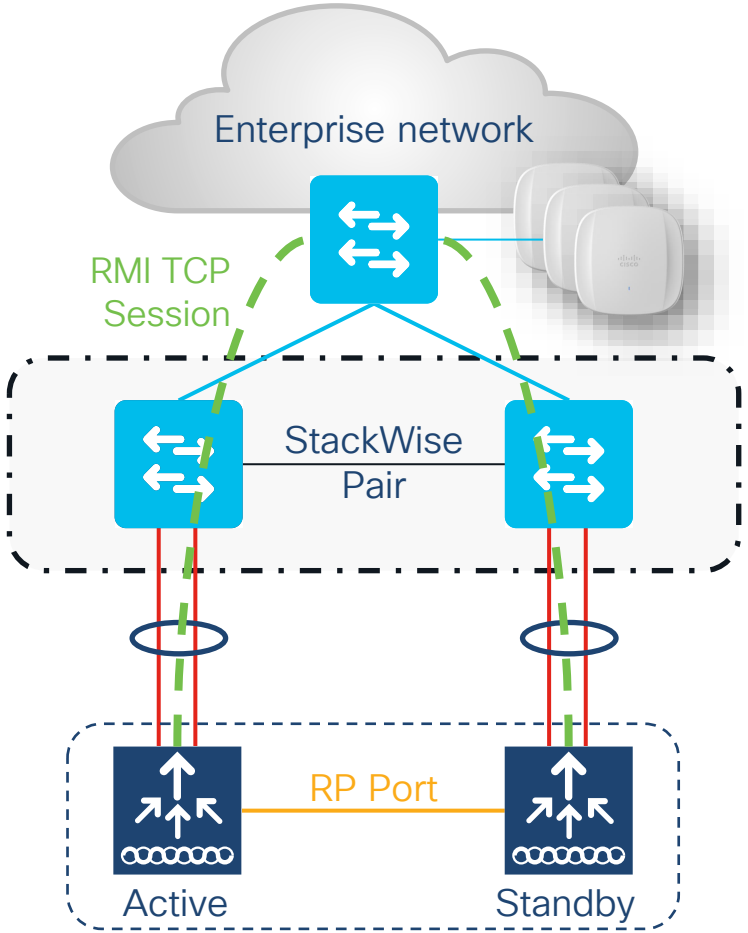
2. Upstream Switch Redundancy

Supported SSO topologies

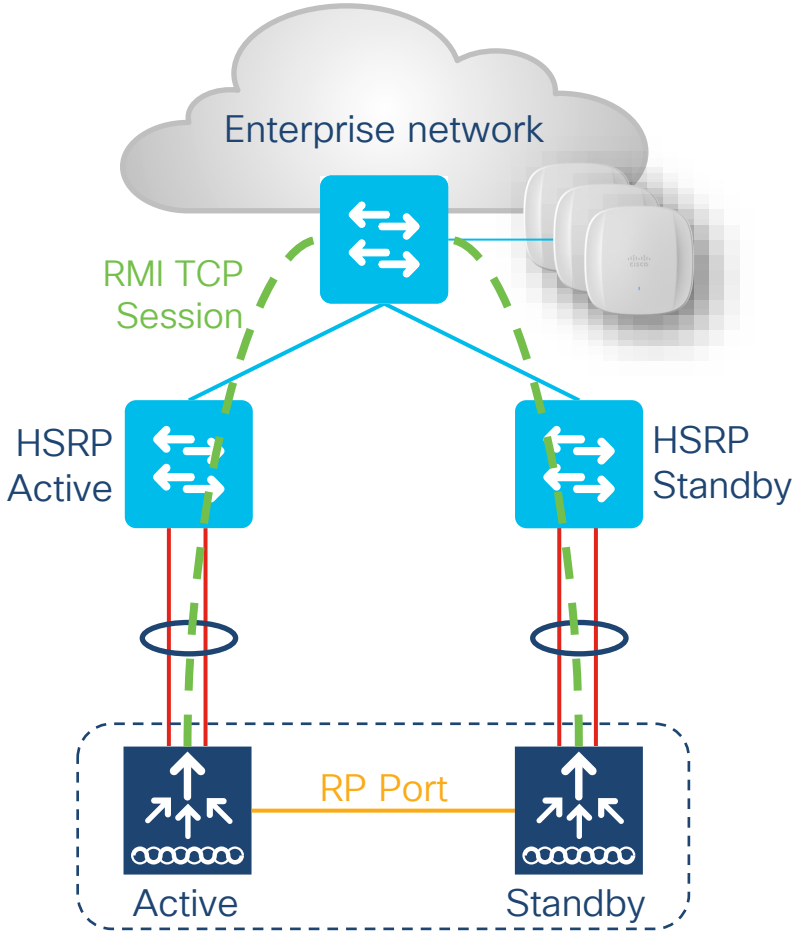
Supported topologies



StackWise Pair with Split links



StackWise Pair without Split links

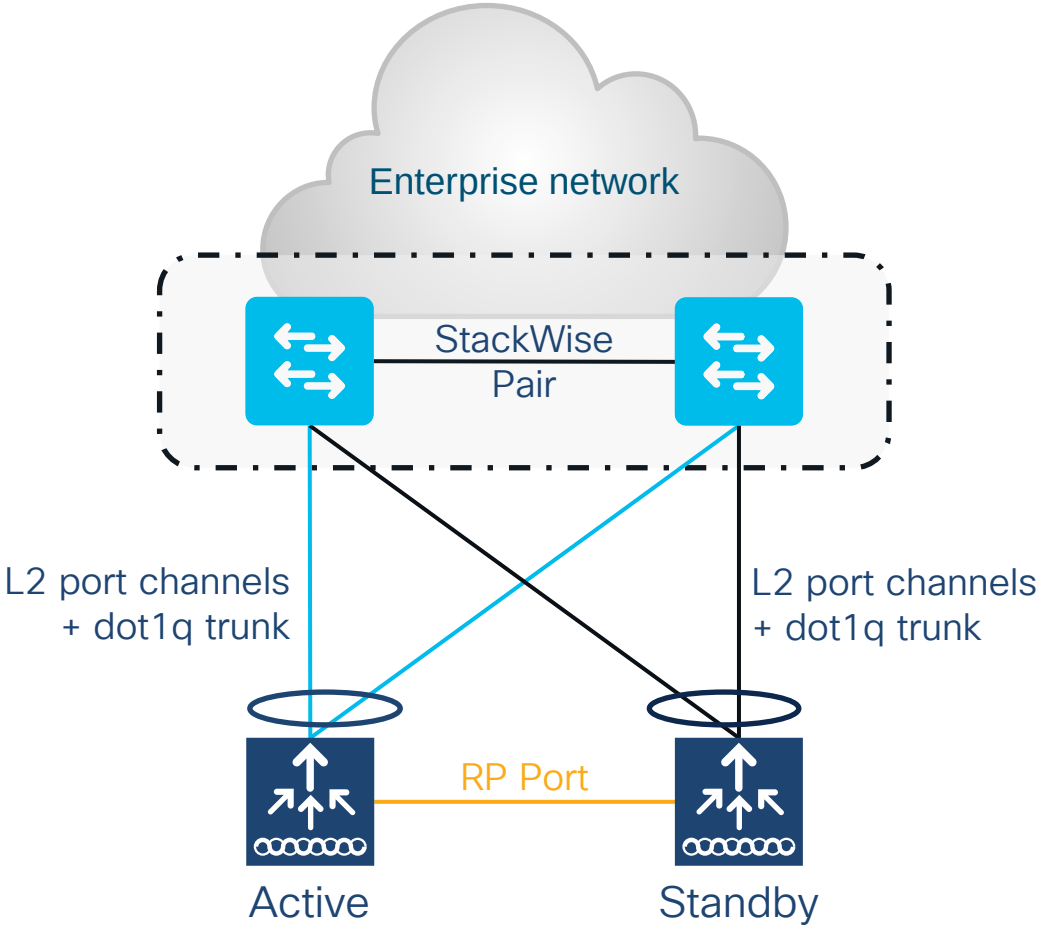


HSRP

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

StackWise Pair with split links
SSO HA Pair

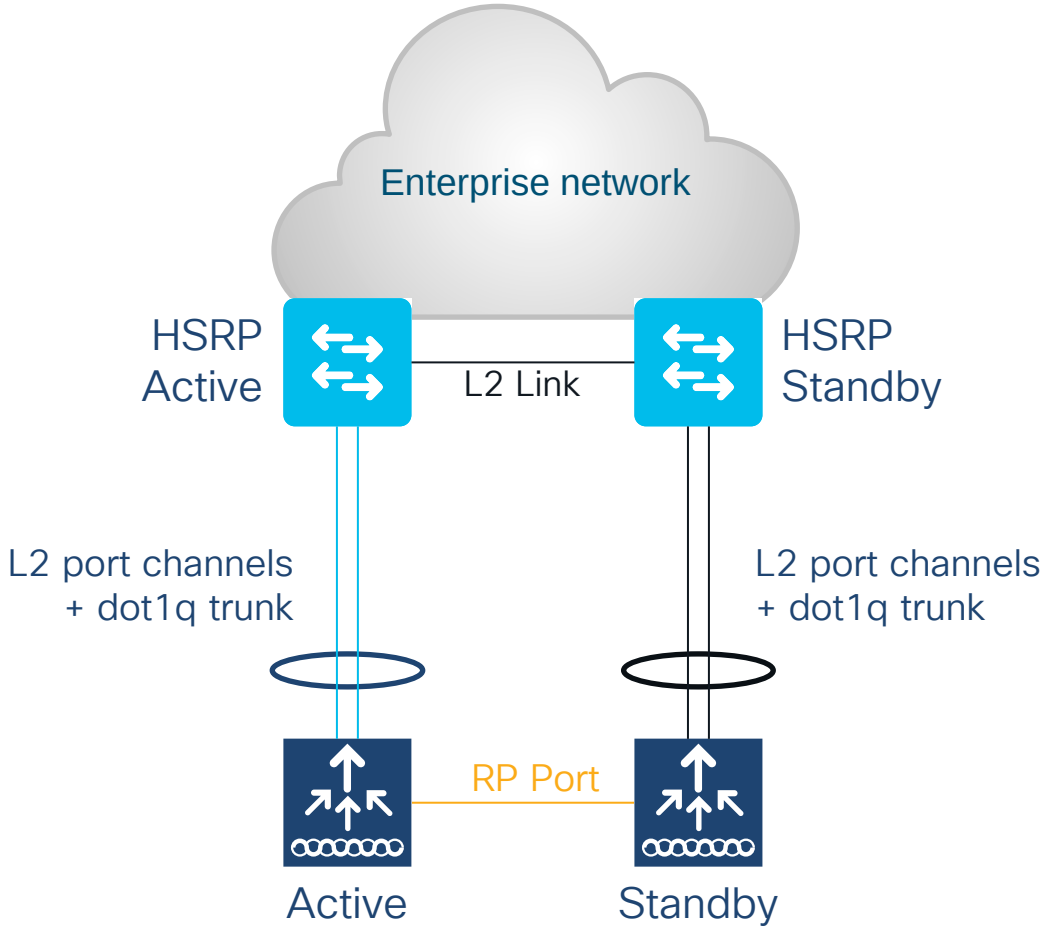
Recommended



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

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

Dual Distribution Switches with HSRP
SSO HA Pair



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

3. Link Level Redundancy

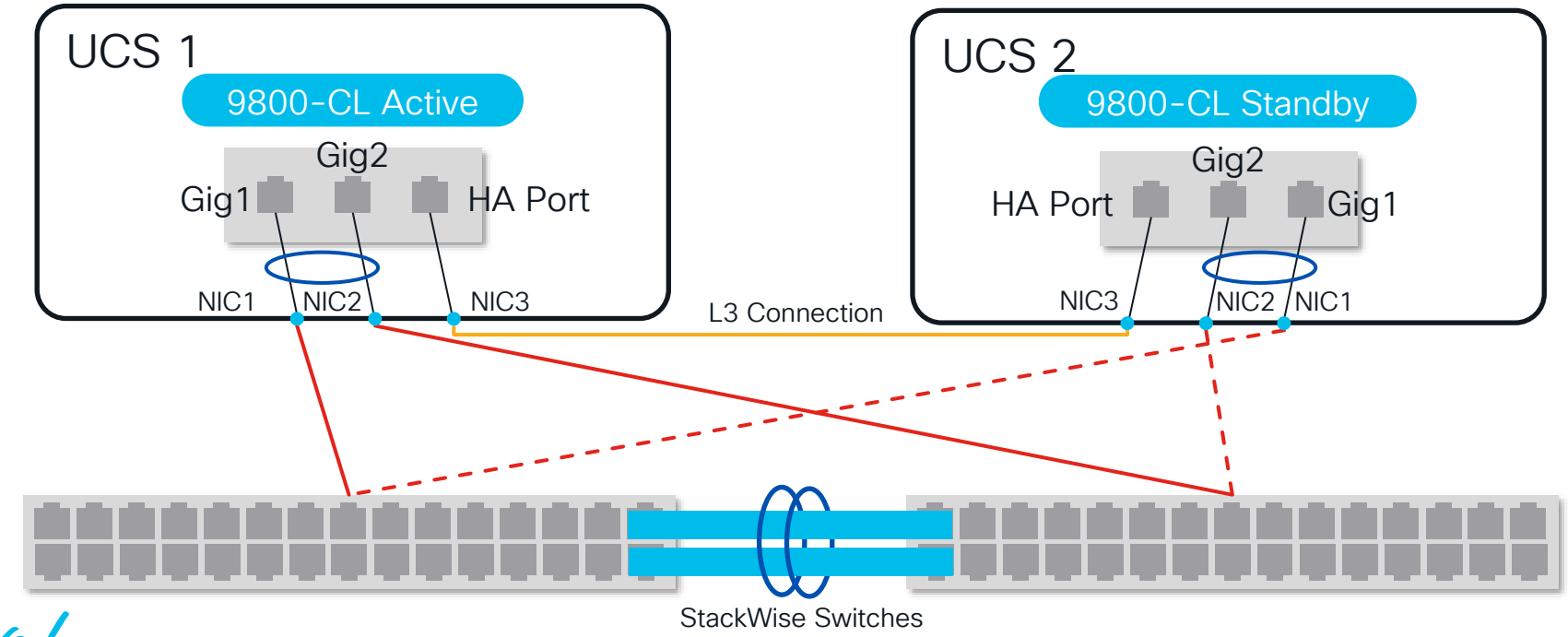
LAG support with LACP and PAGP

LACP, PAGP support in SSO Pair

Platforms supported

- Cisco Catalyst 9800-L, 9800-40, 9800-80 (including module ports)

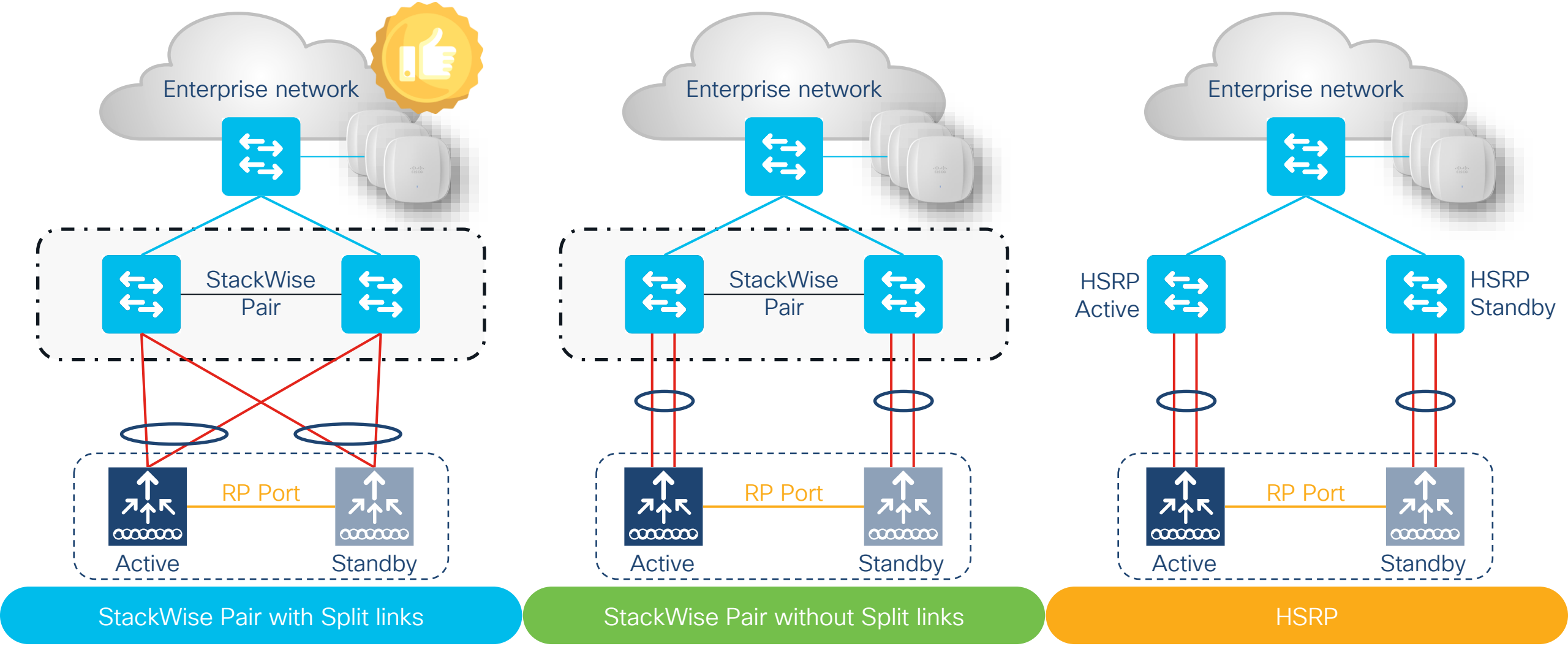
- Cisco Catalyst 9800-CL Private Cloud (Release 17.5.1 and later) - SR-IOV only



LAGP, PAGP support in SSO Pair

- LACP protocol (IEEE 802.3ad) aggregates physical Ethernet interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two devices.
- LAGP, PAGP support is needed on SSO pair in order to have:
  - 1: Ability to detect and monitor the link/connectivity failures on STANDBY.
  - 2: Seamless transfer of client data traffic upon switchover (SSO)

Supported LACP, PAGP topologies



Not supported for LACP, PAGP topologies

- Auto-LAG is not supported.
- C9800-CL (w/o SR-IOV) and EWC on AP is not supported.
- L3 port-channel is not supported.
- SSO pair connected to a single switch is not recommended.

Configuring the Port Channel on C9800 HA SSO
Example

```
C9800# configure terminal
C9800(config)# interface TenGigabitEthernet0/0/0
C9800(config-if)# switchport mode trunk
C9800(config-if)# channel-group 1 mode active

C9800(config)# interface TenGigabitEthernet0/0/1
C9800(config-if)# switchport mode trunk
C9800(config-if)# channel-group 1 mode active

C9800(config)# interface Port-channel 1
C9800(config-if)# switchport mode trunk
```

Configurations on active and standby are synced and will be identical

Configuring the Port Channel on Upstream Switch
Example

```
Switch# configure terminal
Switch(config)# interface range TenGigabitEthernet 1/0/37-38
Switch(config-if)# switchport mode trunk
Switch(config-if)# channel-group 11 mode Active

Switch(config)# interface Port-channel 11
Switch(config-if)# switchport mode trunk

Switch(config)# interface range TenGigabitEthernet 1/0/39-40
Switch(config-if)# switchport mode trunk
Switch(config-if)# channel-group 12 mode Active

Switch(config)# interface Port-channel 12
Switch(config-if)# switchport mode trunk
```

Connection to Active

Connection to Standby

Connections to the Active and Standby Chassis must be kept on separate Port Channels (stack or not)

Multi-chassis LAG Support

Why Multi-chassis LAG?

- Multi-chassis LAG gives the capability to connect multiple uplinks from controller to separate uplink switches.
- **Flexibility in connecting** controller(s) to switch infrastructure.
- **VLAN-based traffic splitting** when connected to a multi-switch topology, for e.g., to isolate Guest traffic on completely different switch/network from Enterprise traffic.
- Multi-chassis LAG is supported with LAG mode ON and dynamic LAG (LACP and PAGP)

Supported platforms

- Catalyst 9800-L, 9800-40 and 9800-80 Wireless Controllers.
- Multi-chassis LAG between ports of similar capabilities (for example, 2.5G and 2.5G or 10G and 10G. 2.5G and a 10G port in a port-channel group are not supported).
- Minimum of two ports in one LAG.

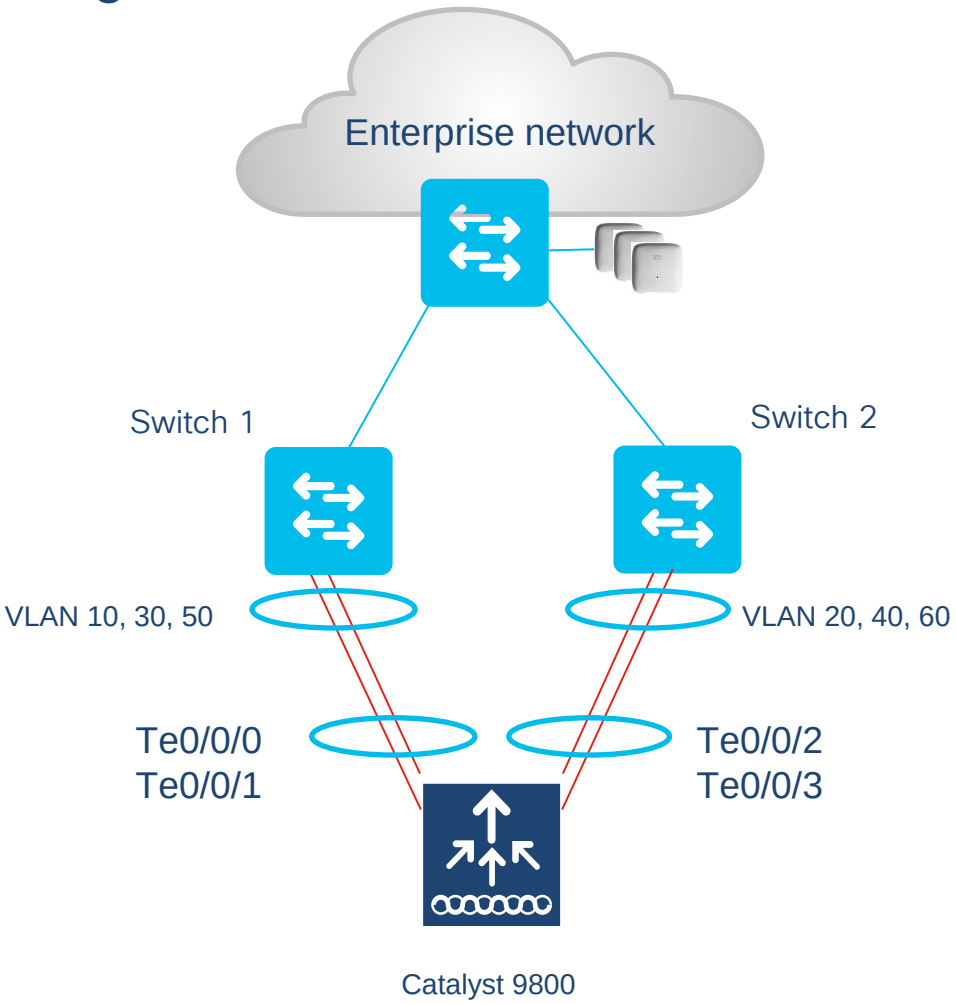
Catalyst 9800-L

Catalyst 9800-40

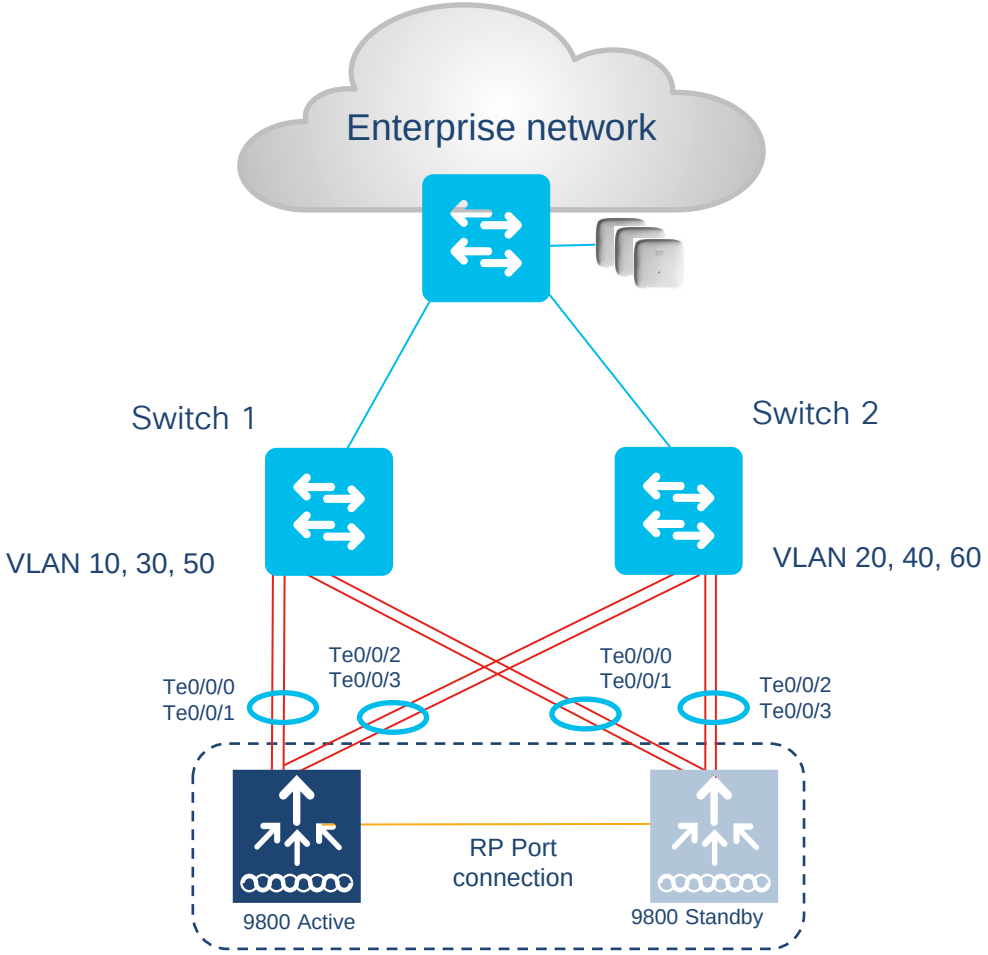
Catalyst 9800-80

Supported topologies

Single controller w/ Multi-chassis LAG

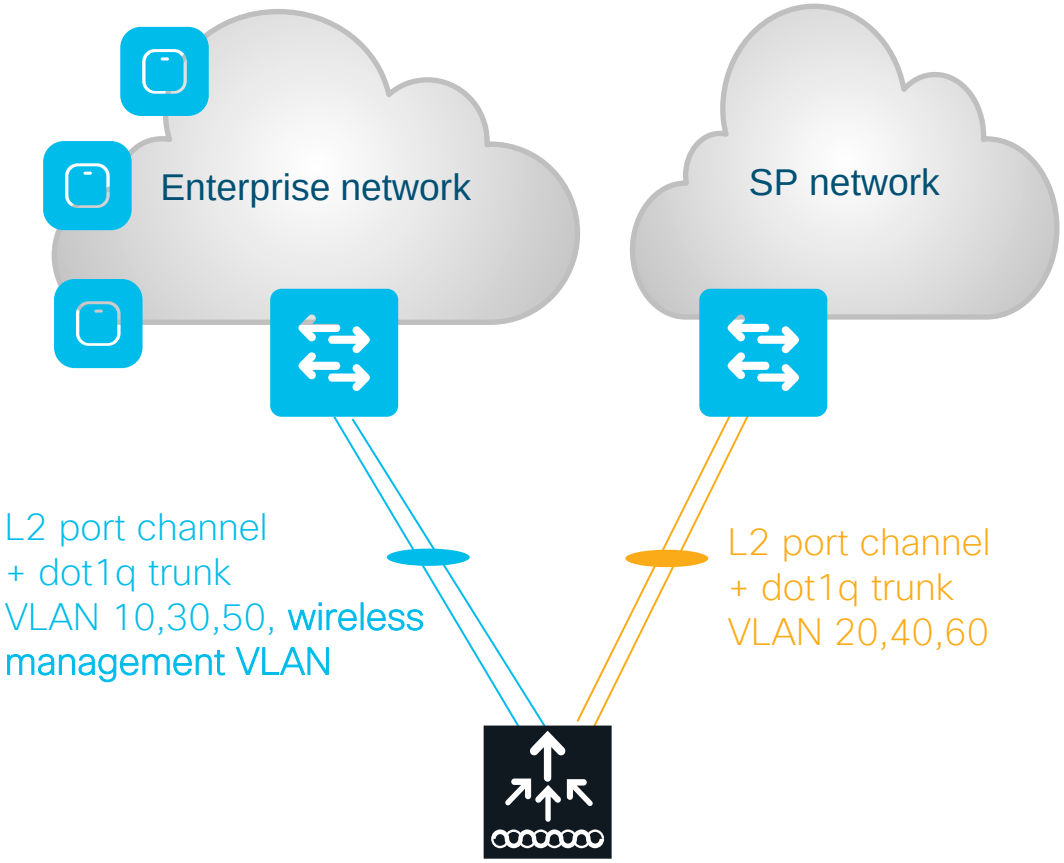


SSO Pair w/ Multi-chassis LAG



Note: You can connect LAG to a single switch, However different VLANs must be connected to different LAGs

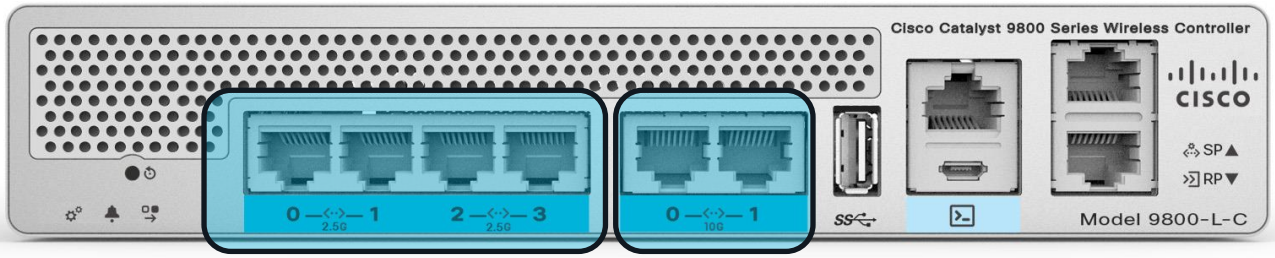
Multi-chassis LAG with separated VLANs



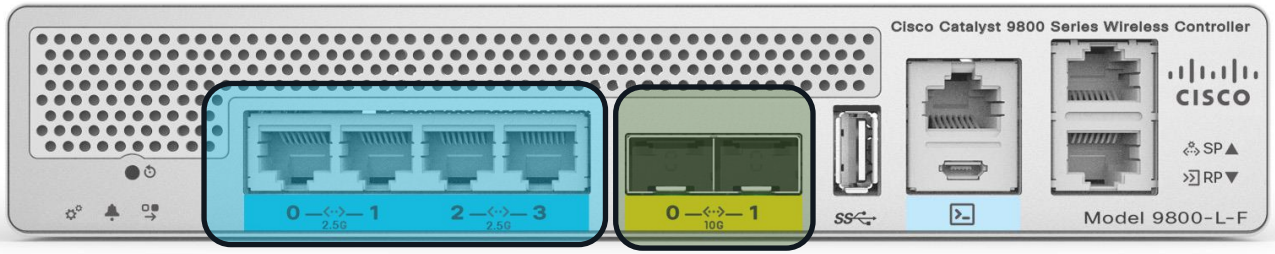
- Use case: map SSIDs to different separated wired network (e.g. Guest traffic to a separated switch/network)
- Dual uplink (port-channel or single link), each with different VLANs.
- Each LAG must be connected to a single switch.
- Different VLANs must be assigned to different LAGs.
- Note: user configuration responsibility not to create a loop

Supported LAG grouping on 9800-L

- Best practice is to have **ports of same type and speed in the port channel**



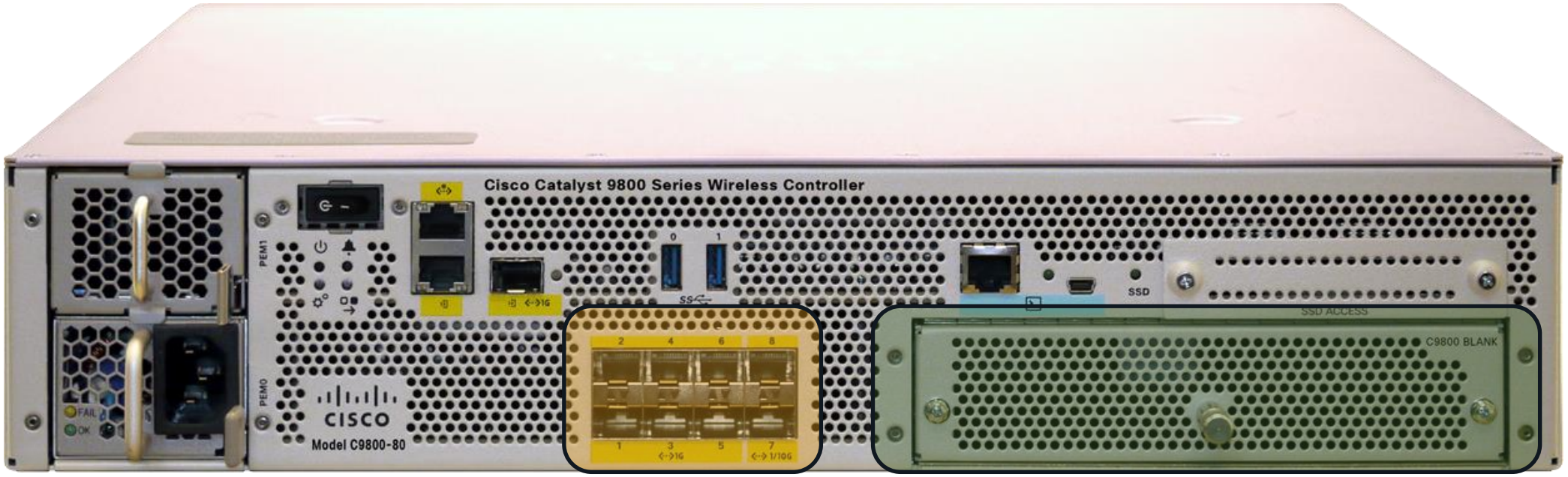
9800-L-C with 2.5G/1G and 10G/mGig ports in different port channels



9800-L-F with 2.5G/1G and 10G/1G Fiber ports in different port channels

Supported LAG grouping on 9800-80

- Best practice is to have <u>ports of same slot in the port channel</u>



For your reference

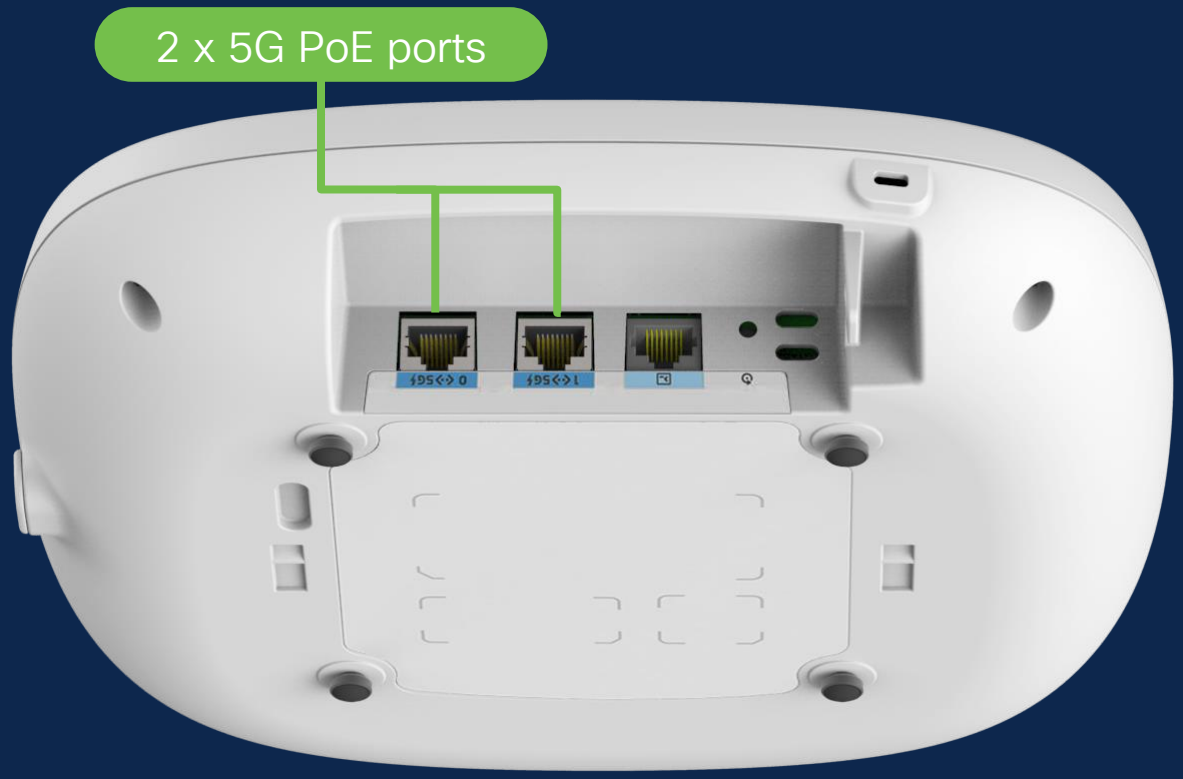
SSO feature matrix

Functionality	Release	Embedded controller on 9K	9800-L	9800-40	9800-80	9800-CL PVT Cloud
RMI interface with config CLI (IPv4)	17.1	Supported	Supported	Supported	Supported	Supported
Dual Active Detection	17.1	Supported	Supported	Supported	Supported	Supported
Recovery Mode	17.1	Supported	Supported	Supported	Supported	Supported
Default GW Check	17.1	Supported	Supported	Supported	Supported	Supported
LACP, PAGP support with SSO	17.1	Supported	Supported	Supported	Supported	Supported for SR-IOV
GW check IP from Static routes	17.2	Supported	Supported	Supported	Supported	Supported
Multi LAG (standalone & SSO)	17.2	Supported	Supported	Supported	Supported	No, use LAG at Hypervisor
Standby Monitoring on RMI	17.3	Supported	Supported	Supported	Supported	Supported

Note: SSO is not supported on EWC and 9800-CL Public Cloud

4. Access Point Redundancy

Redundancy with the Cisco Catalyst 9136 Access Point



Dual PoE ports for hitless PoE:
No reboot required if a port loses power

Uplink ports support:
802.3 link aggregation for increased throughput resiliency

PoE Redundancy with Catalyst 9136

Note: Ensure both switches provide the same power level and have connectivity to the WLC.

*Can also be done with a single switch

Quick demo!

Primary Switch

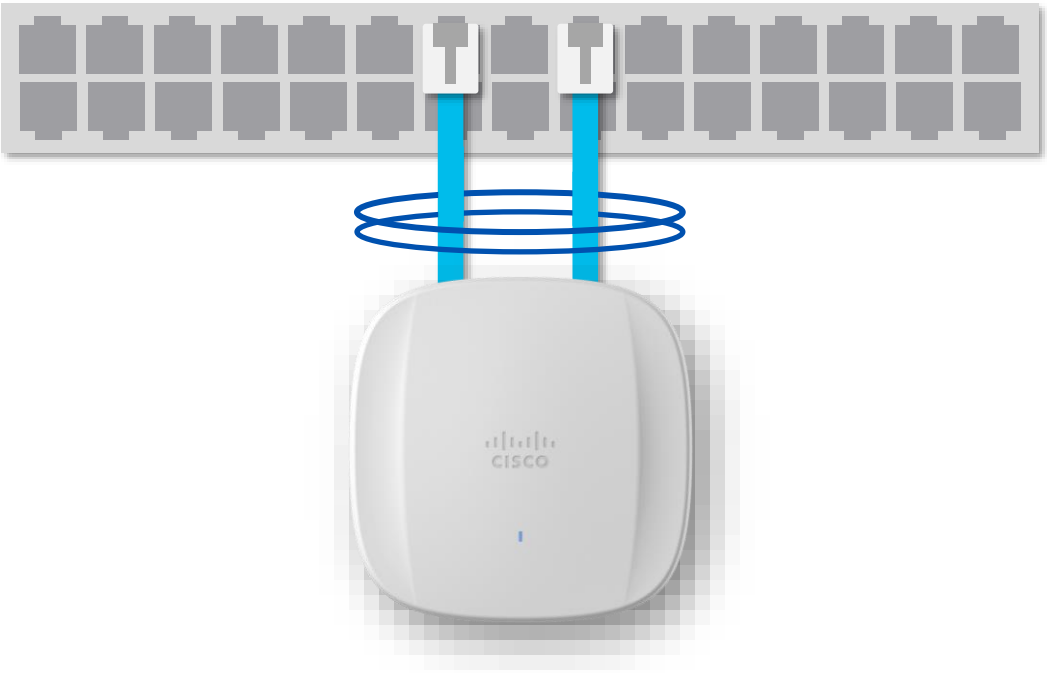
```
TME-Demo-Access-3850 con0 is now available


Press RETURN to get started.


User Access Verification

Username: netadmin
Password:

TME-Demo-Access-3850>en
TME-Demo-Access-3850#
```

Secondary Switch

```
TME-Demo-Core con0 is now available


Press RETURN to get started.


TME-Demo-Core>en
TME-Demo-Core#
```

```
justloo@JUSTLOO-M-HXL2 ~ %
```

LAG on the Catalyst 9136



Overview

- Allows for uplink redundancy to the upstream switch
- Combined throughput of up to 5Gbps
- Supports LAG, LACP, and PAGP

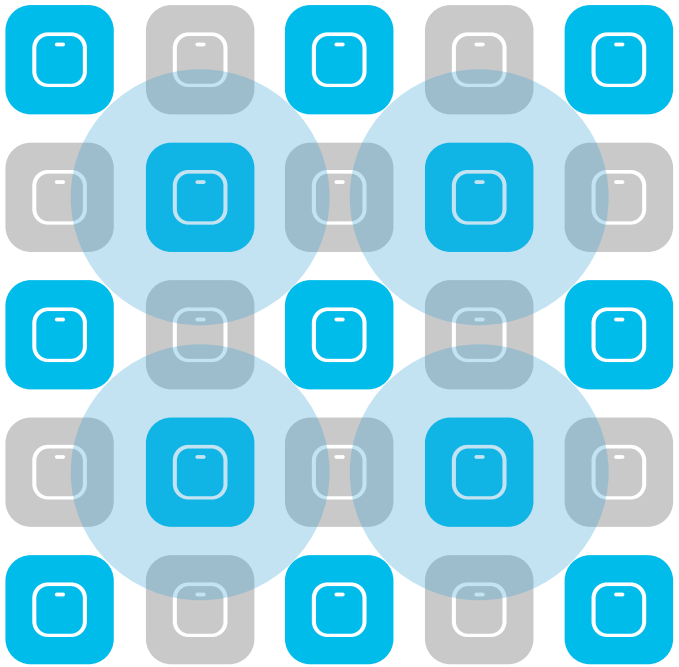
Note: LAG can be configured only between two ports of the same speed.

Infrastructure updates

5. Controller Software Upgrade

Rolling AP Update/Upgrade Infrastructure

Rolling AP Upgrade: Neighbor AP marking

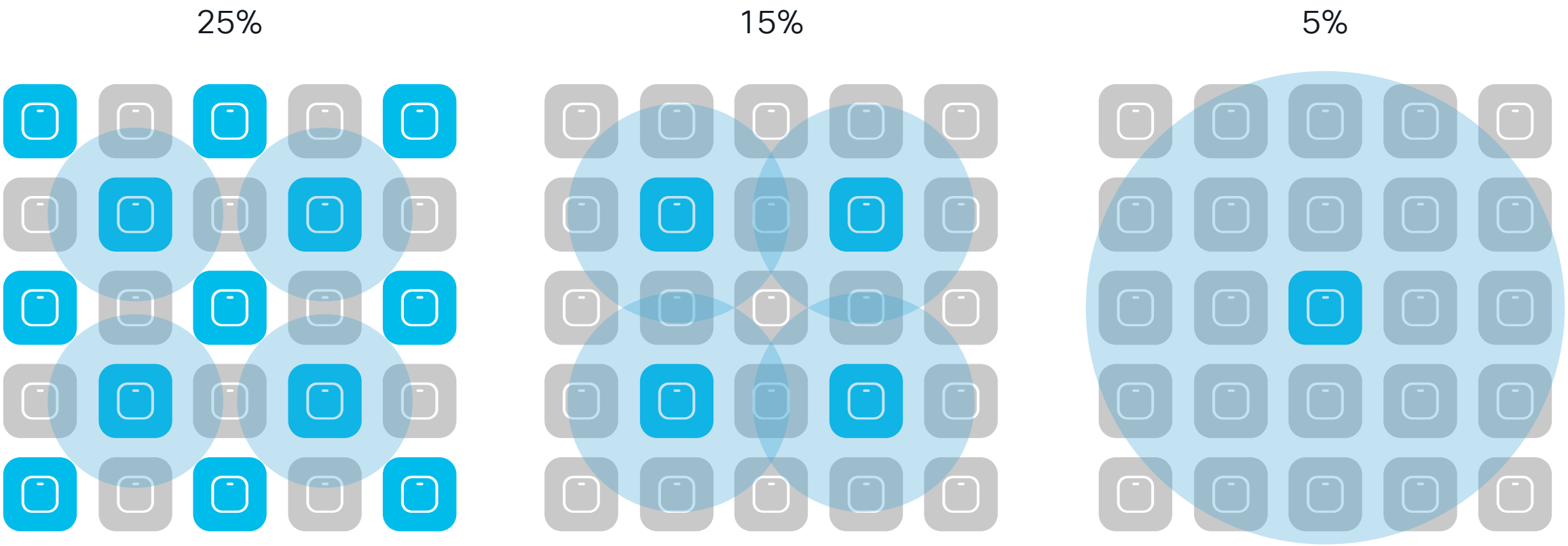


How does it work?

- Group APs into multiple groups and upgrade one group at a time.
- Grouping is done based on RF neighbors
- Admin user can control the impact and determines the number of iterations taken and the Rolling Upgrade time
- Candidate AP selection
  - With **N** = 4: If the AP in blue is selected and 4 of its best neighbours marked unavailable for selection. The resultant selection will be about **P** = 50% of APs
  - For P = 25%, N = 6, expected iterations all ap upgrade ~ 5 > ~1h
  - For P = 15%, N = 12, expected iterations all ap upgrade ~ 12 > ~2h
  - For P = 5%, N= 24, expected iterations all ap upgrade ~ 22 > ~4h

  - APs reload and re-join (AP image pre-download is used) determines the Rolling AP Upgrade time

Rolling AP Upgrade: Neighbor AP marking



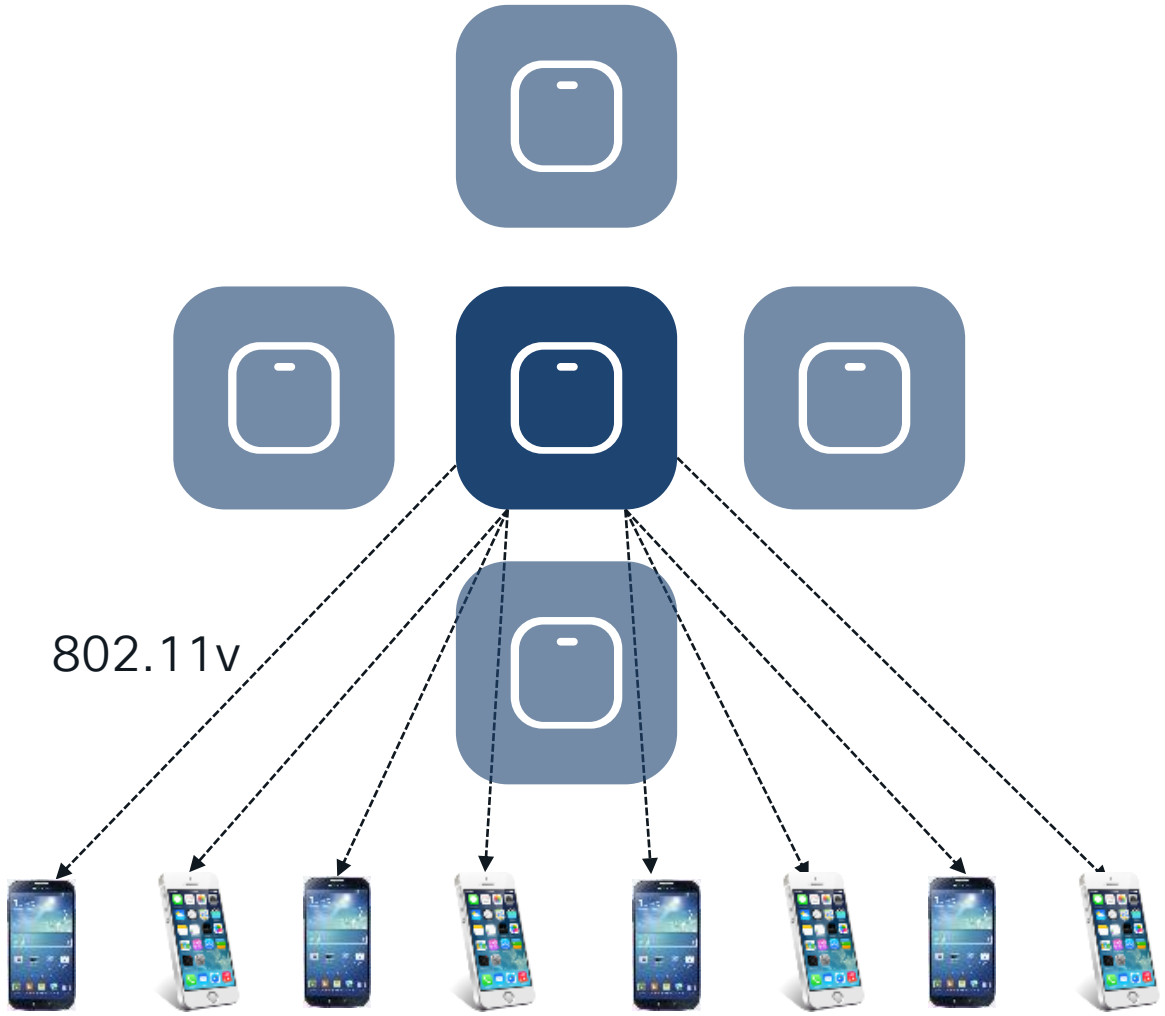
User selects % of APs to upgrade in one go [5, 15, 25]
For 25%, Neighbors marked = 6 [Expected number of iterations ~ 5]
For 15%, Neighbors marked = 12 [Expected number of iterations ~ 12]
For 5%, Neighbors marked = 24 [Expected number of iterations ~ 22]

Client steering

Clients steered from candidate APs to non-candidate APs

802.11v BSS Transition Request → Dissociation Imminent

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



Rolling AP Upgrade: Client steering

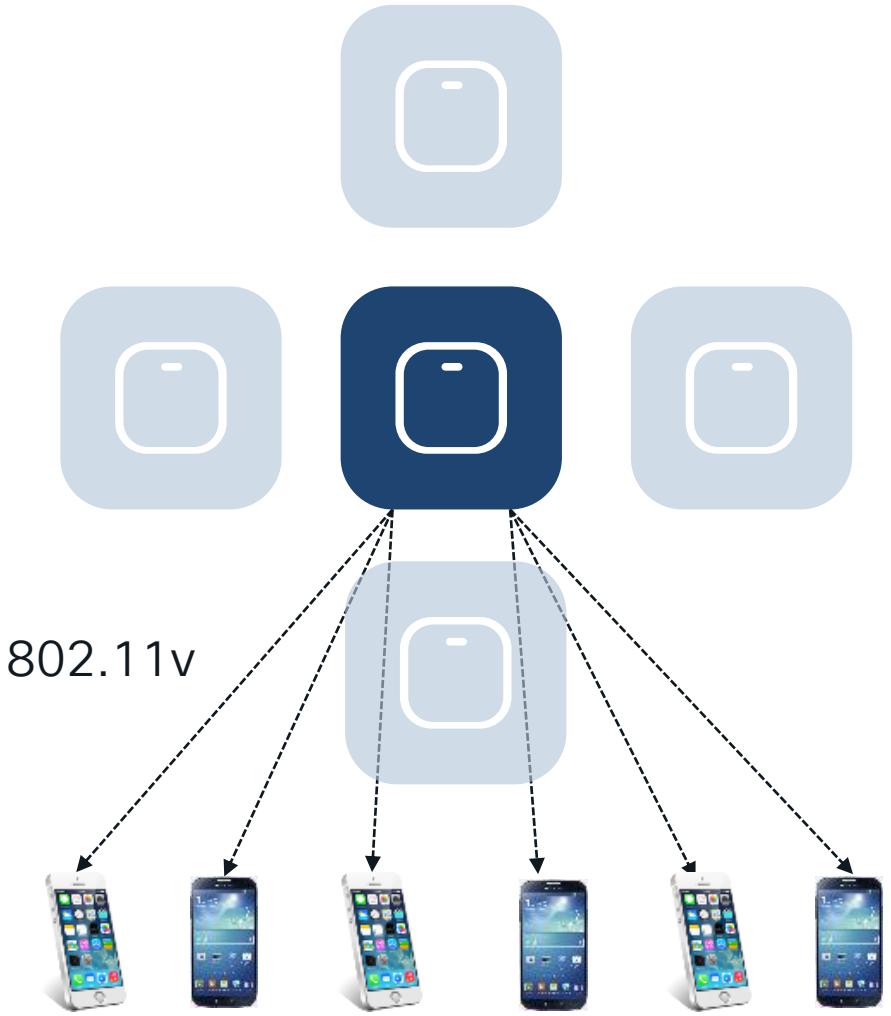
Clients steered from candidate APs to non-candidate APs

802.11v BSS Transition Request → Dissociation Imminent

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

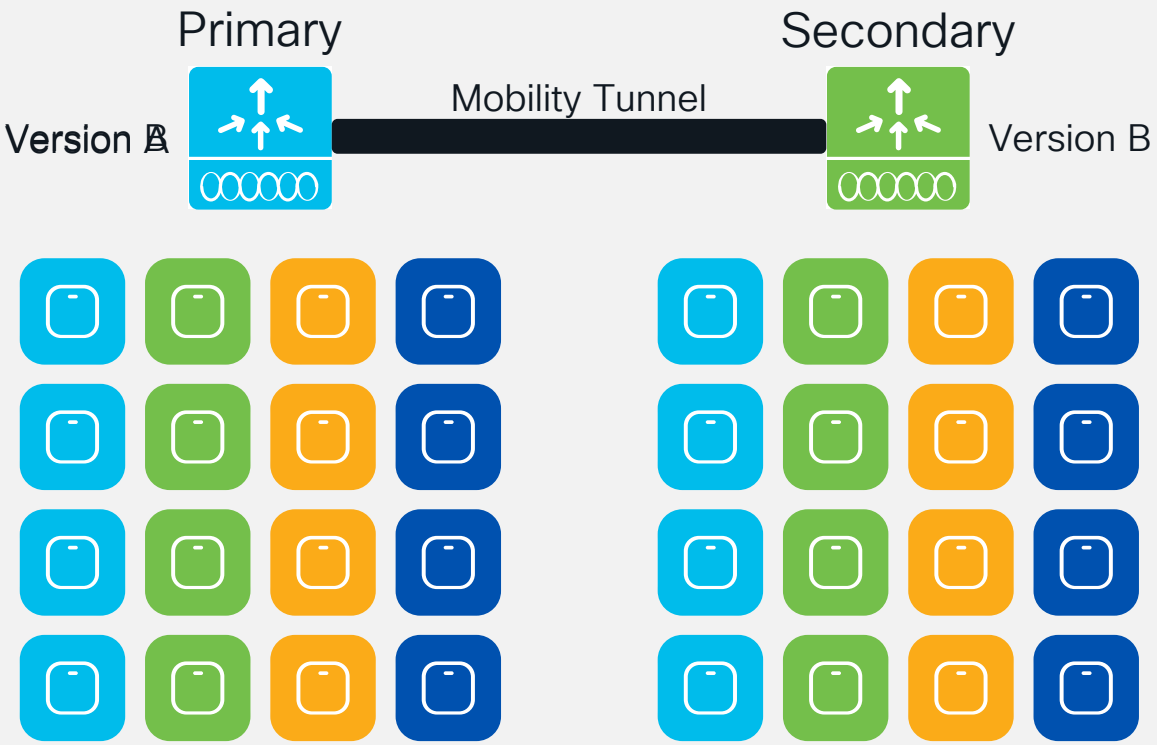
Starting 17.11 AP stops responding to client probes and association (in Flex)

NEW



N+1 Site Based Hitless Upgrade

N+1 Site Based Hitless Upgrade



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

Site Filter

Site 1

Site 2

AP upgrade workflow

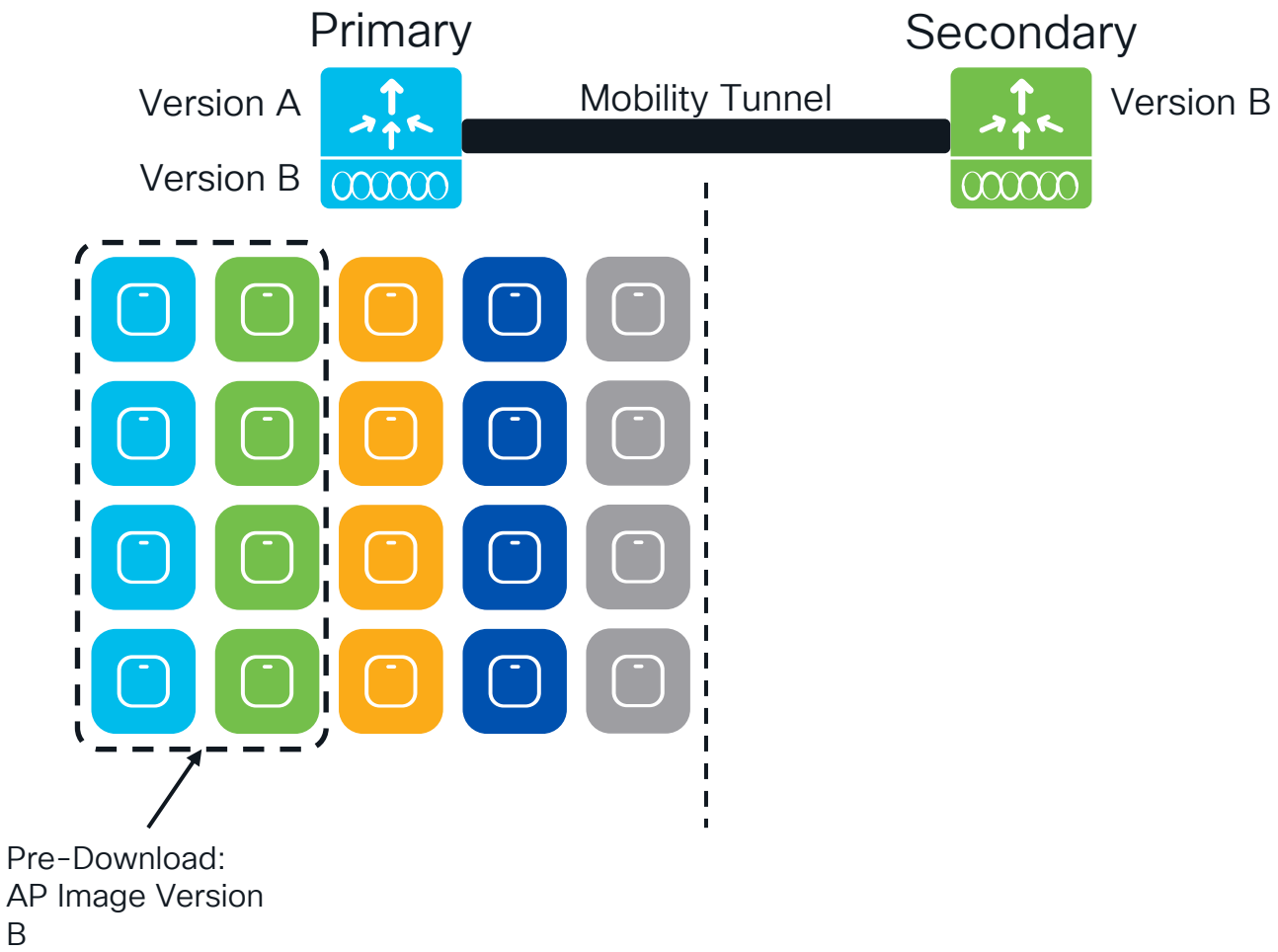
1. Add the new IOS XE image to the controller:
   install add file <Path to Image>

```
install add file bootflash:IOS-VersionB.bin
```

2. Add the sites that will be upgraded first to the site filter:
   ap image site-filter any-image add <Site Tag Name>

```
ap image site-filter any-image add Site1
ap image site-filter any-image add Site2
```

3. Pre-download image to the APs:
   ap image predownload



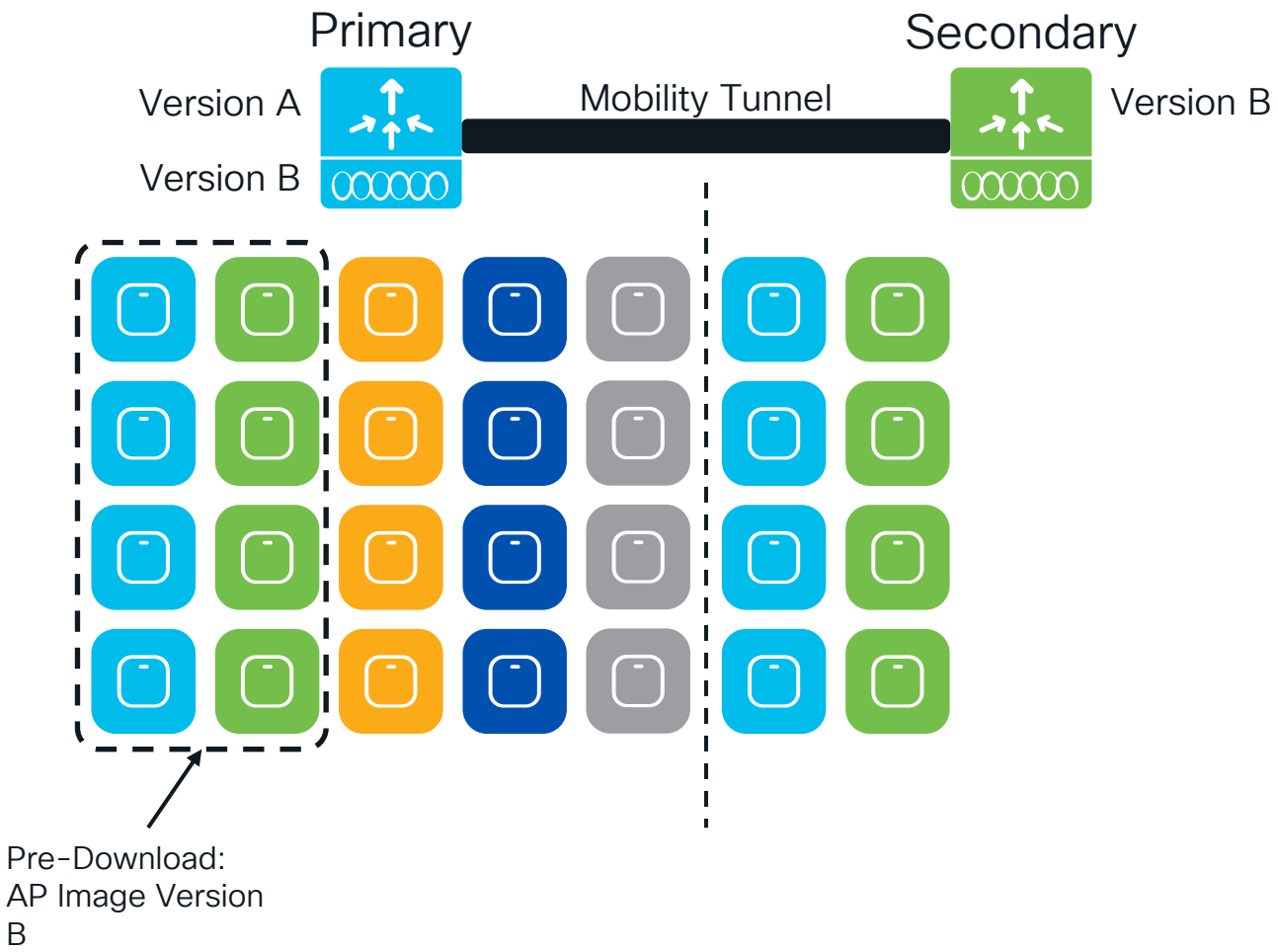
AP upgrade workflow

4 Move APs to the new destination WLC:
ap image upgrade destination <Destination WLC Name> <Destination WLC IP>

```
ap image upgrade destination Secondary-WLC 10.10.110.4
```

5 APs will reload with the new image and join the Secondary WLC on a rolling basis

6 As the APs successfully join the Secondary WLC, the Secondary will update the Primary WLC.



Site Filter

- Site 1
- Site 2
- Site 3

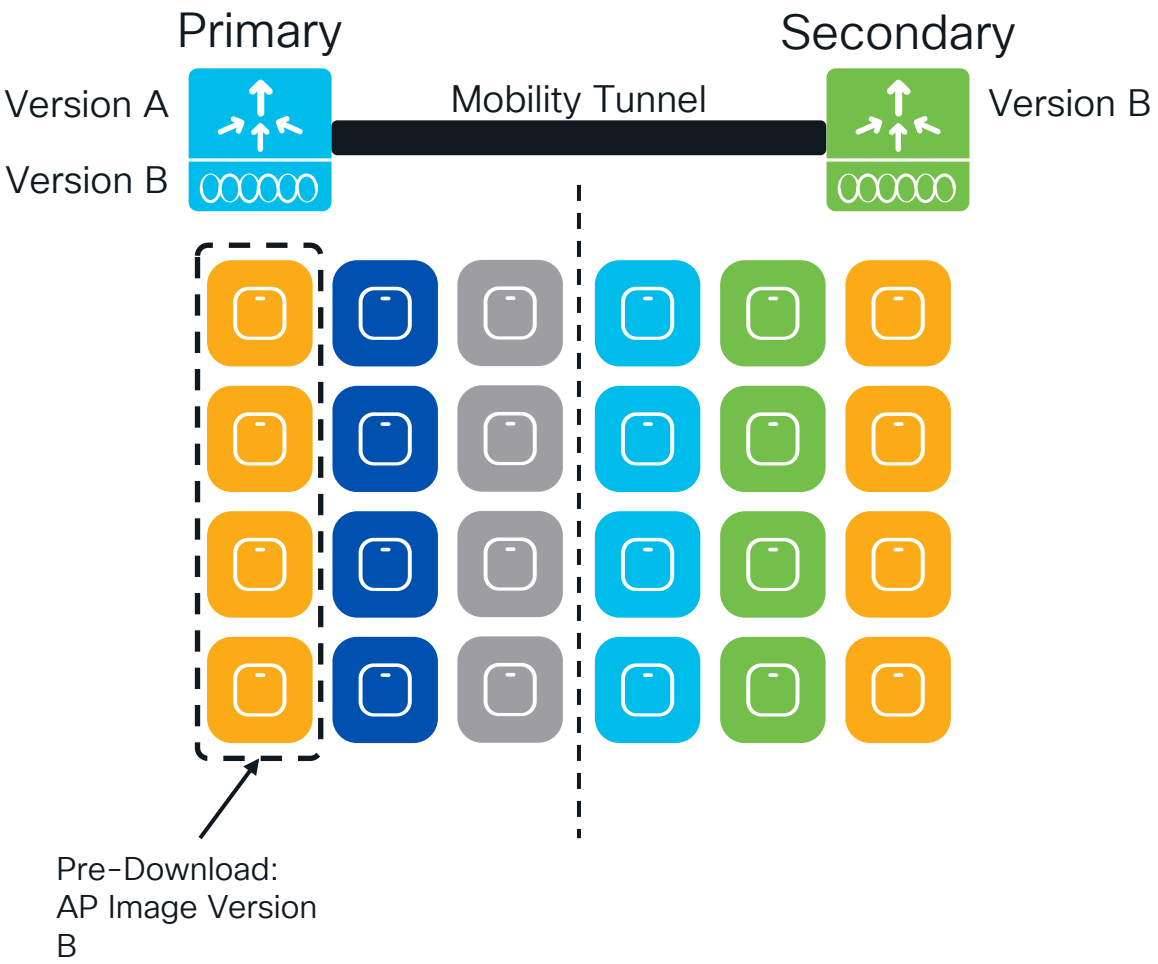
AP upgrade workflow

7. Add further sites to the site filter:
   `ap image site-filter any-image add <Site Tag Name>`

```
ap image site-filter any-image add Site3
```

8. Initiate the AP image pre-download, reload with the new image, and join to the Secondary WLC in rolling fashion:
   `ap image site-filter any-image apply`

9. As the APs successfully join the Secondary WLC, the Secondary will update the Primary WLC.



AP upgrade workflow

Site Filter

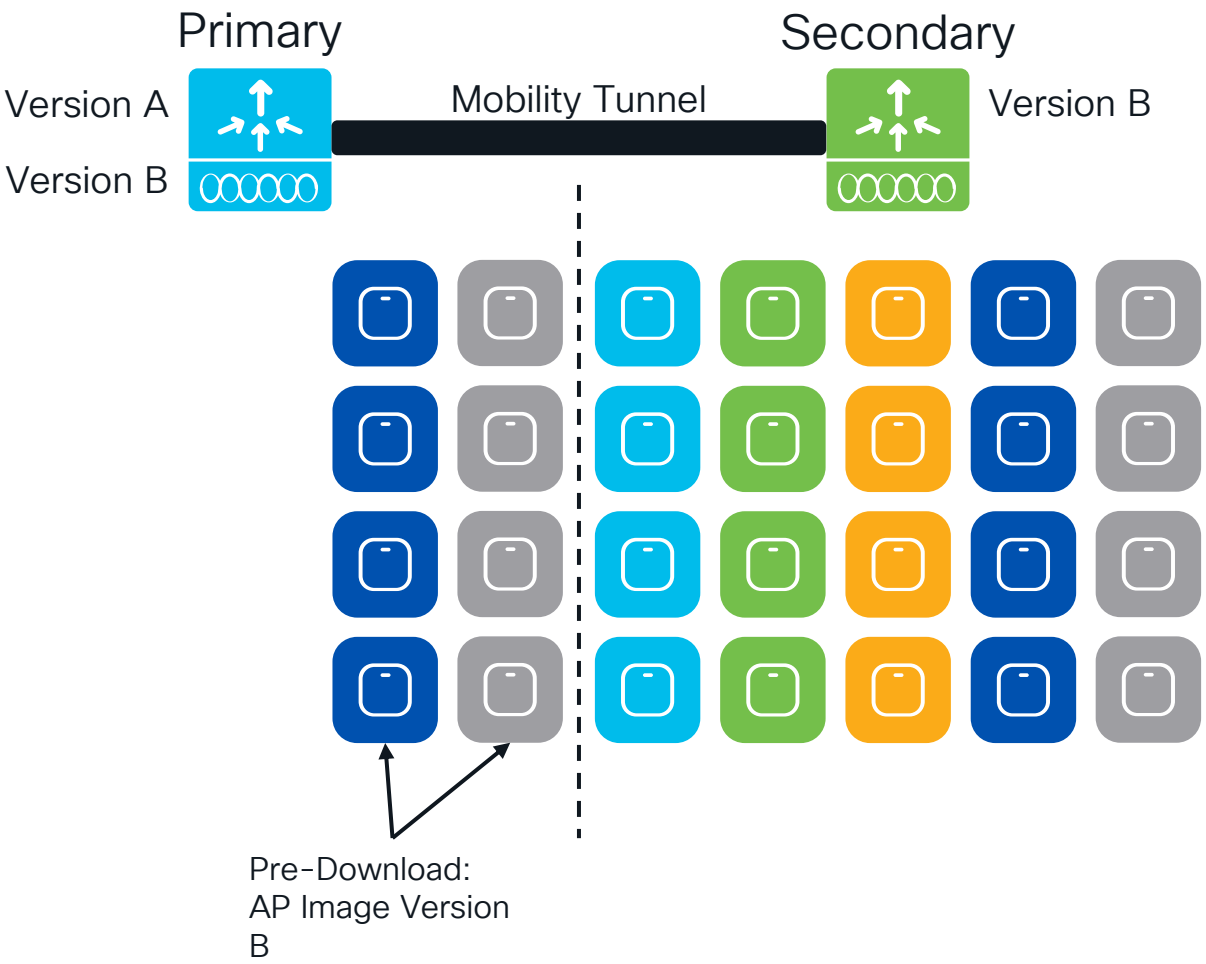
- Site 1
- Site 2
- Site 3

10. Upgrade the rest of the sites by clearing the site filter:
    `ap image site-filter any-image clear`

11. APs at the remaining sites will pre-download the image, reload with the new image, and join to the Secondary WLC in rolling fashion.

12. As the APs successfully join the Secondary WLC, the Secondary will update the Primary WLC.

13. Activate the new IOS XE image on the Primary WLC.



Configuration via WebUI
Mobility Tunnel

Configuration > Wireless > Mobility

Global Configuration | Peer Configuration

Mobility Peer Configuration

+ Add | Delete

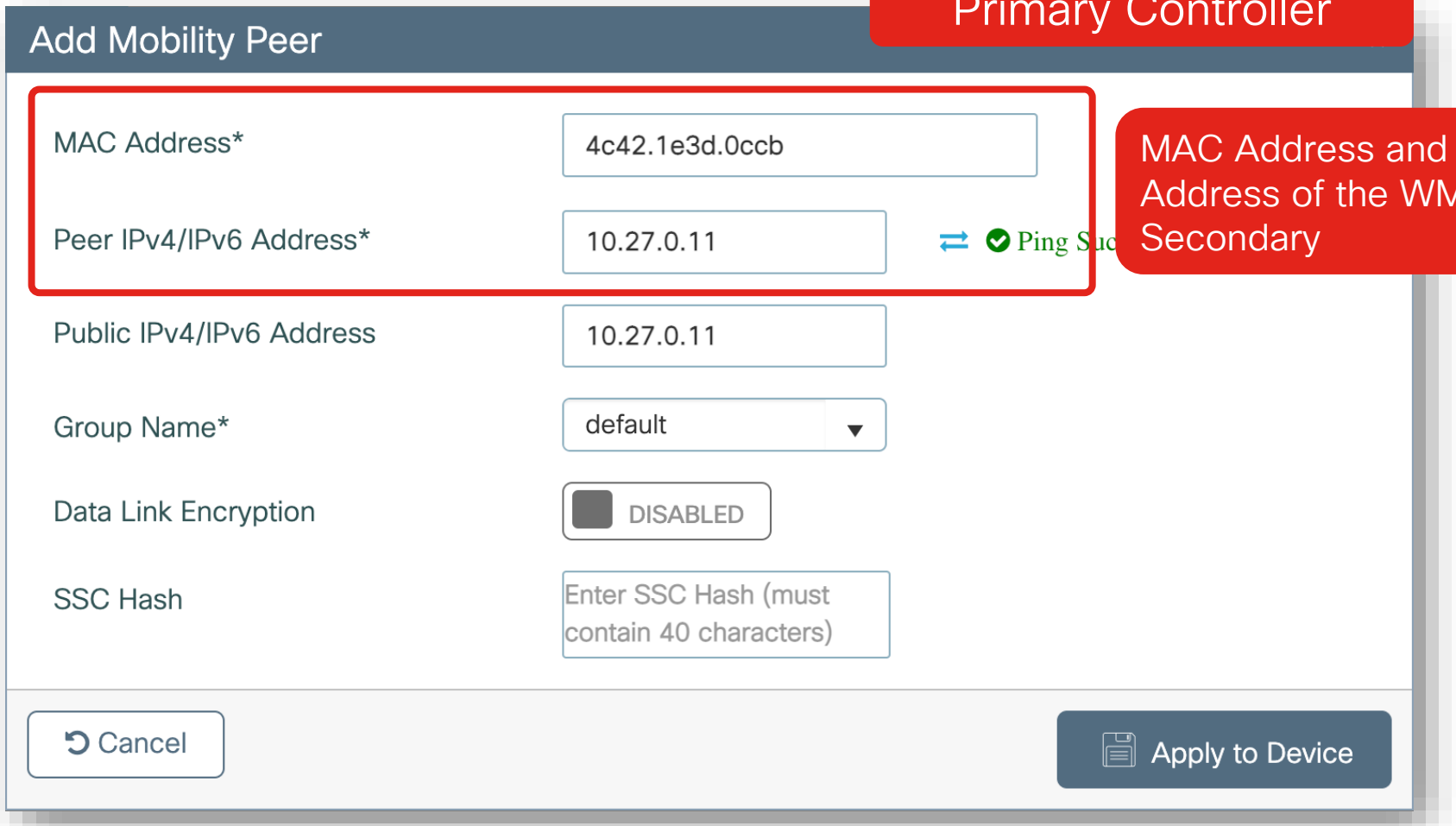
MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
a453.0e9b.3b8b	10.27.0.5	N/A	default	0.0.0.0	::	N/A	N/A	3319b53f7bd5a9ac563ee59fb83e4260daed6c6b	N/A

1 | 10 | 1 - 1 of 1 items

Non-Local Mobility Group Multicast Configuration

Configuration via WebUI
Mobility Tunnel

Primary Controller



MAC Address and IP Address of the WMI of the Secondary

Configuration via WebUI
Mobility Tunnel

Secondary Controller

Add Mobility Peer

MAC Address*	a453.0e9b.3b8b
Peer IPv4/IPv6 Address*	10.27.0.5 Ping Suc
Public IPv4/IPv6 Address	10.27.0.5
Group Name*	default
Data Link Encryption	DISABLED
SSC Hash	Enter SSC Hash (must contain 40 characters)

Cancel

Apply to Device

MAC Address and IP Address of the WMI of the Primary

Configuration via WebUI
Mobility Tunnel

Configuration > Wireless > Mobility

Global Configuration | Peer Configuration

Mobility Peer Configuration

+ Add | Delete

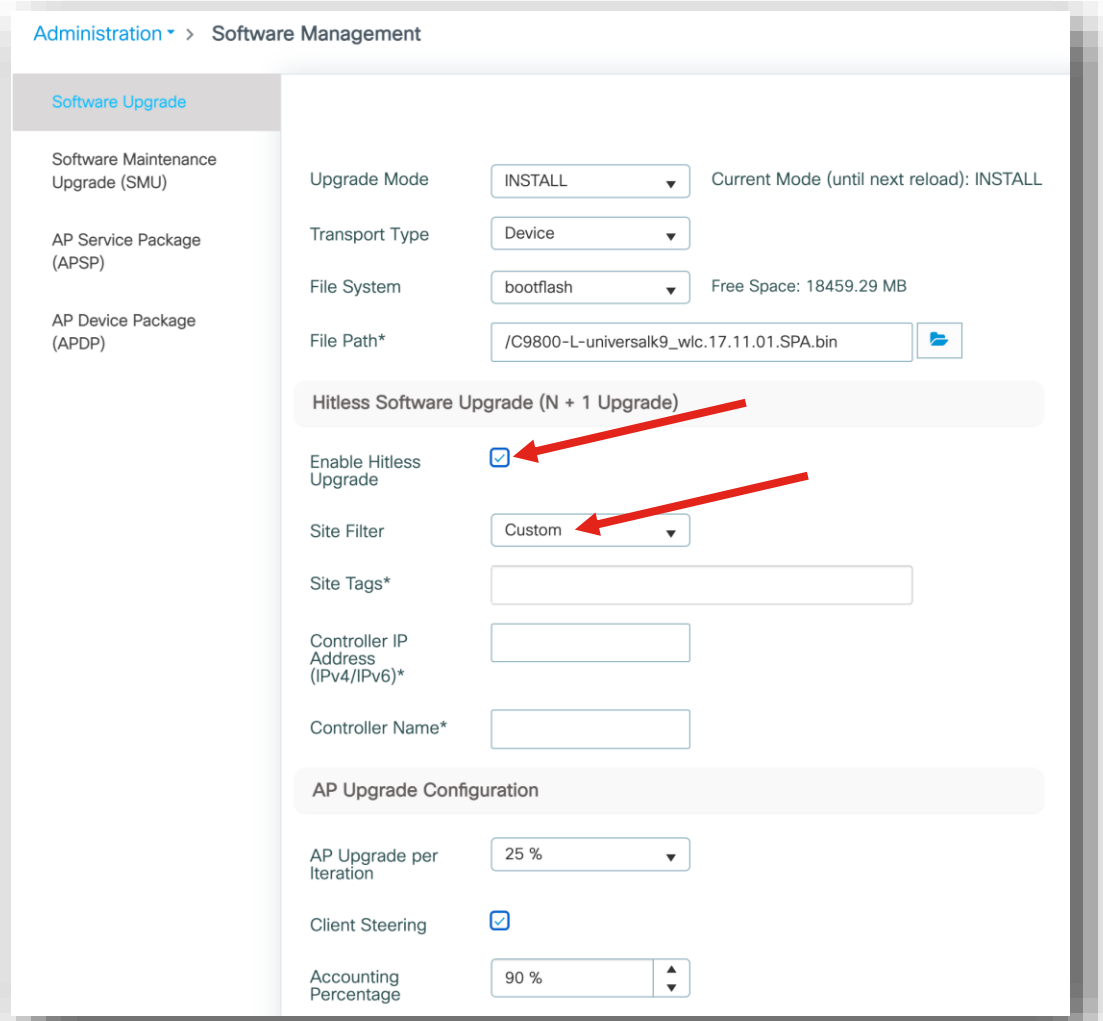
MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
a453.0e9b.3b8b	10.27.0.5	N/A	default	0.0.0.0	::	N/A	N/A	3319b53f7bd5a9ac563ee59fb83e4260daed6c6b	N/A
4c42.1e3d.0ccb	10.27.0.11	10.27.0.11	default	0.0.0.0	::	Up	1385		Disabled

1 | 10 | 1 - 2 of 2 items

Non-Local Mobility Group Multicast Configuration

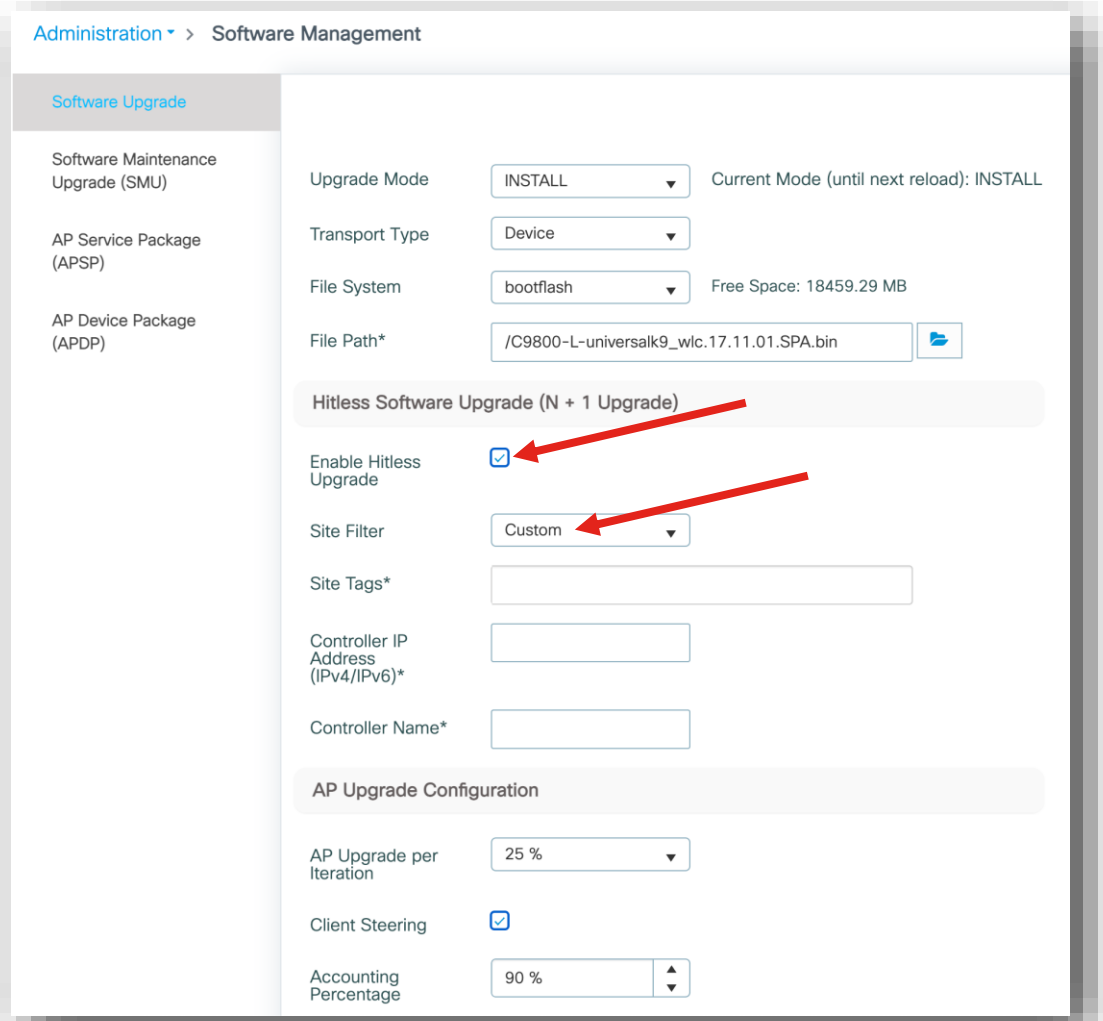
N+1 Site Based Hitless Upgrade with WebUI

1. Check the box for **Enable Hitless Upgrade**
2. Set the Site Filter to **Custom**



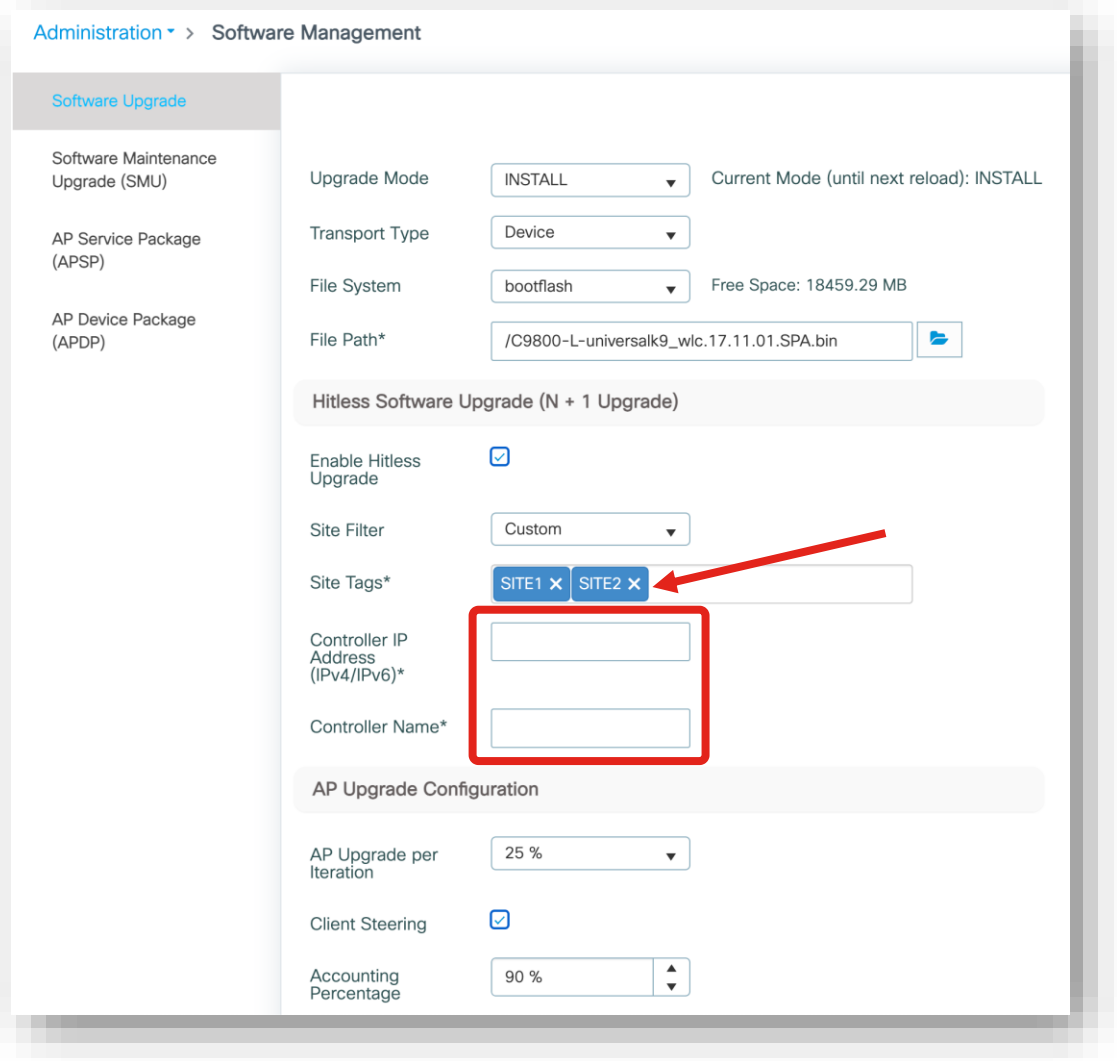
N+1 Site Based Hitless Upgrade with WebUI

1. Check the box for **Enable Hitless Upgrade**
2. Set the Site Filter to **Custom**



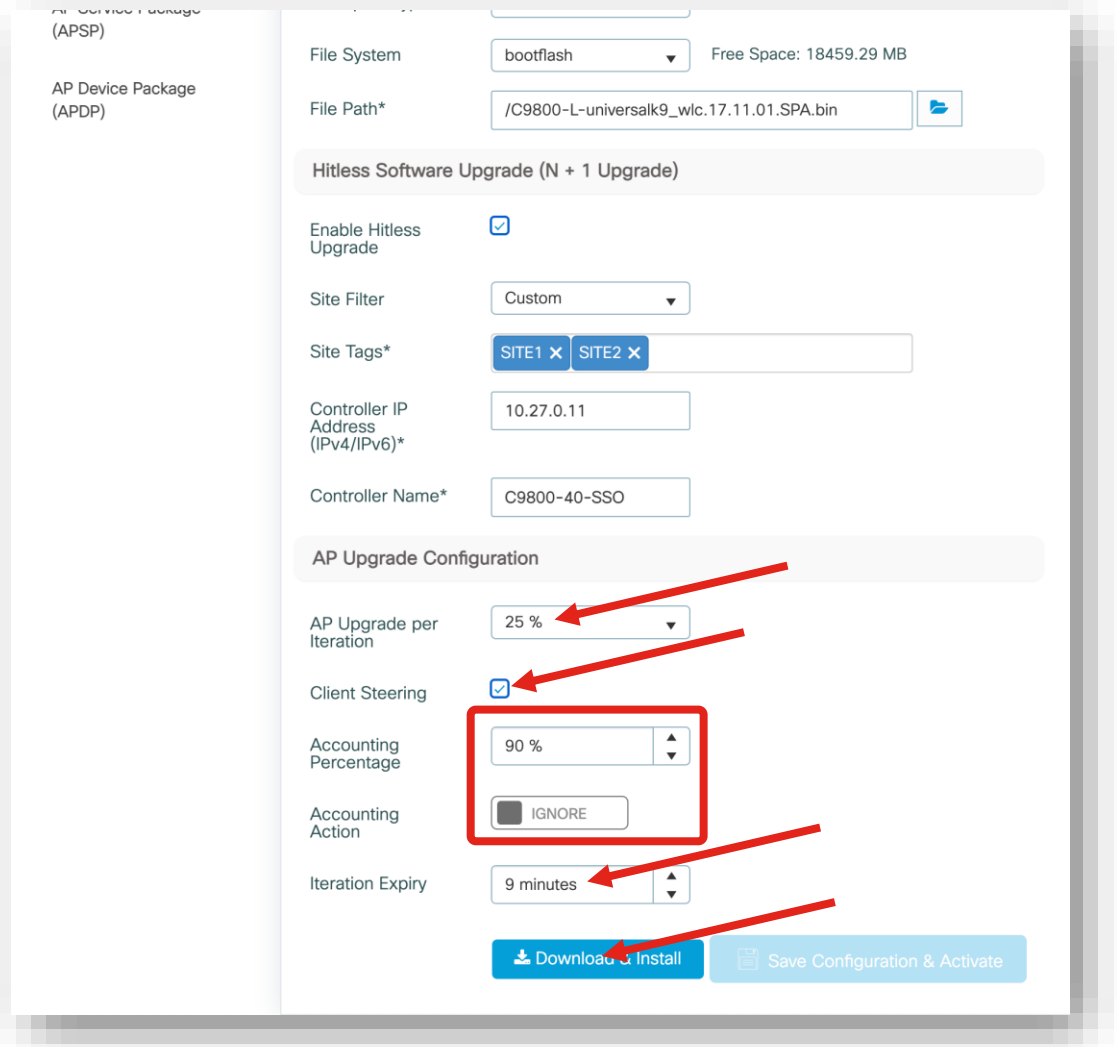
N+1 Site Based Hitless Upgrade with WebUI

1. Check the box for **Enable Hitless Upgrade**
2. Set the Site Filter to **Custom**
3. Select the required **Site Tags**
4. Set the Secondary Controller's **IP Address** and **Hostname**



N+1 Site Based Hitless Upgrade with WebUI

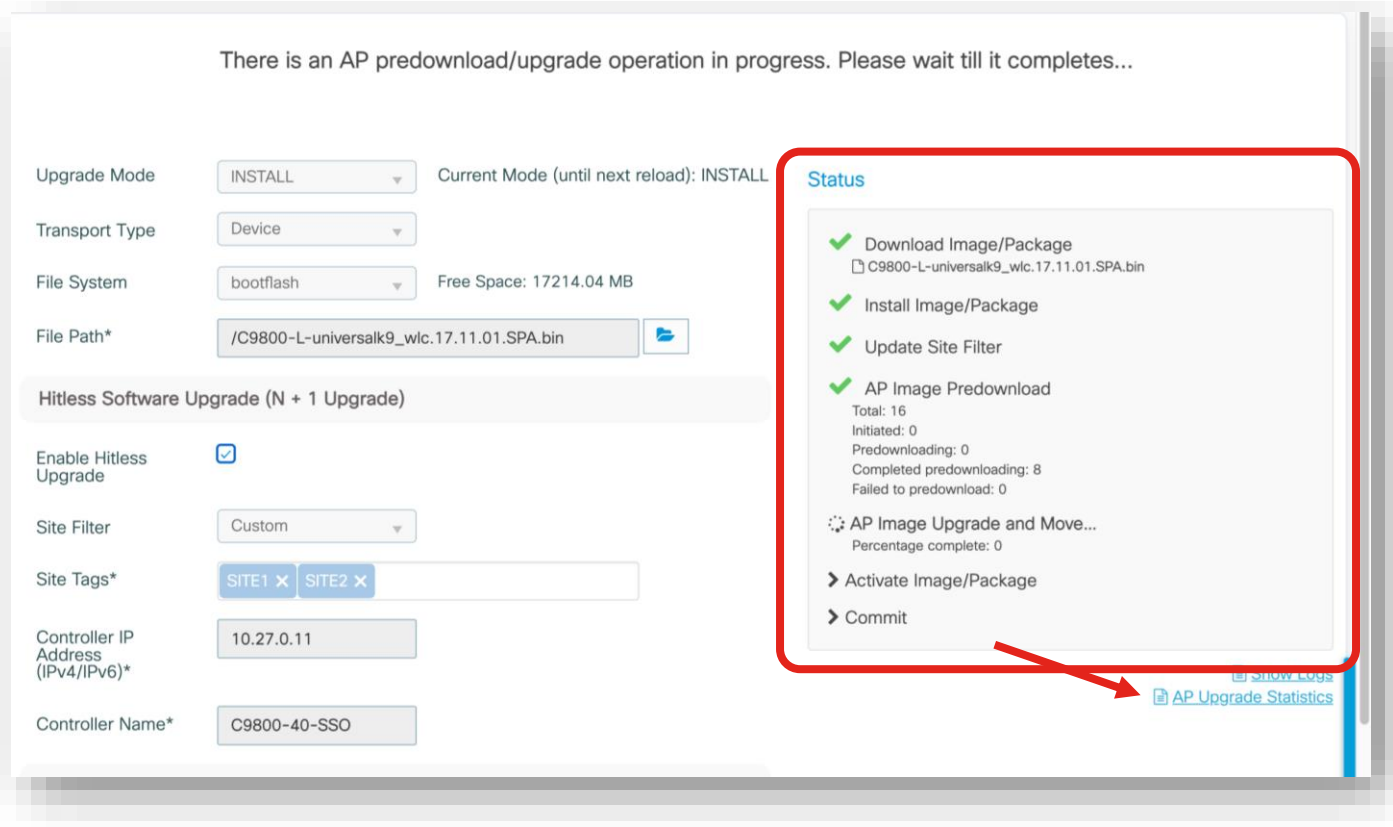
5. Set the required **AP Upgrade per Iteration**
6. Check the box to enable **Client Steering**
7. Choose the required **Accounting Percentage** and **Accounting Action**
8. Set the **Iteration Expiry**
9. Click **Download & Install**



N+1 Site Based Hitless Upgrade with WebUI

10 Monitor the progress of the entire upgrade in the **Status** Window

11 Click **AP Upgrade Statistics** to track each iteration of AP upgrade

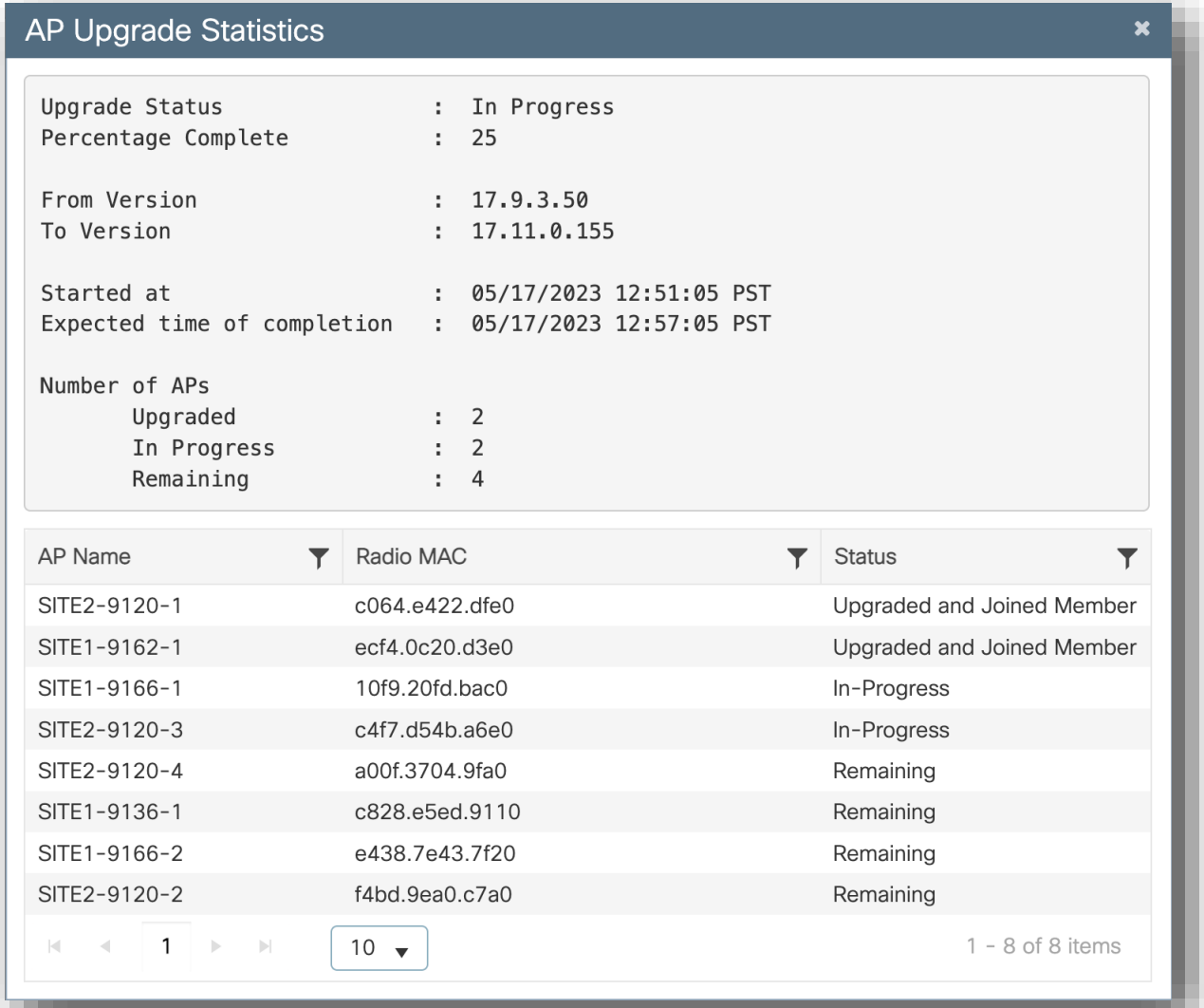


N+1 Site Based Hitless Upgrade with WebUI

10 Monitor the progress of the entire upgrade in the **Status** Window

11 Click **AP Upgrade Statistics** to track each iteration of AP upgrade

12 Wait for the current iteration of APs to finish moving to the secondary controller



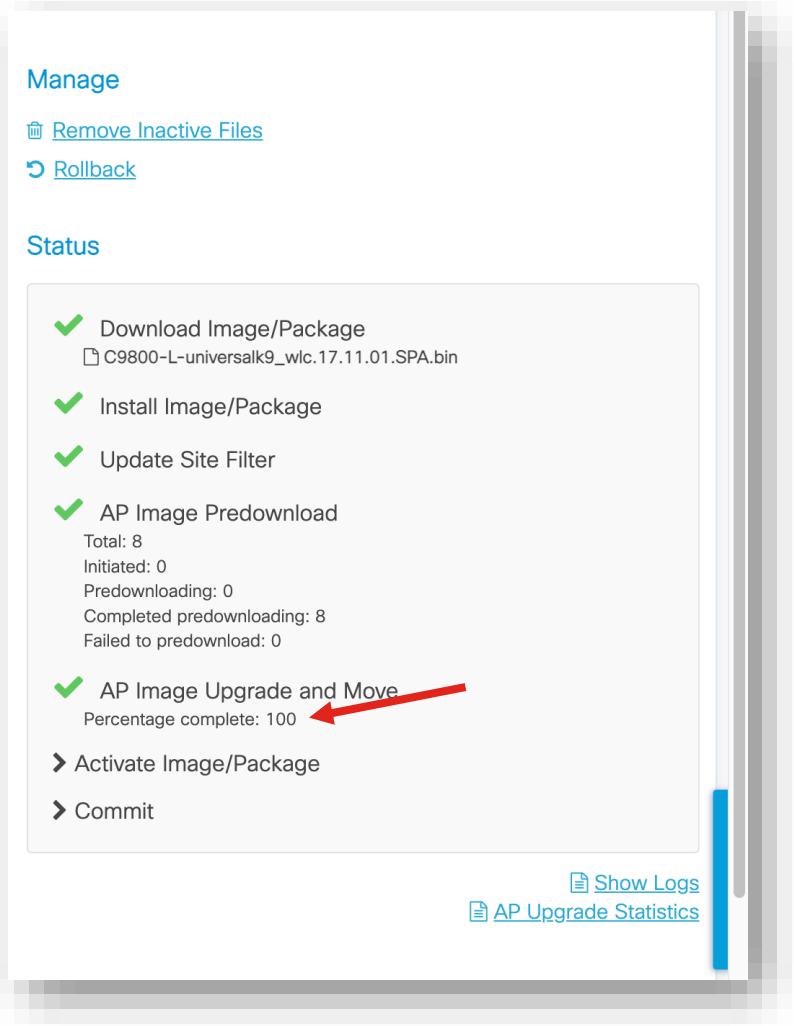
N+1 Site Based Hitless Upgrade with WebUI

10 Monitor the progress of the entire upgrade in the **Status** Window

11 Click **AP Upgrade Statistics** to track each iteration of AP upgrade

12 Wait for the current iteration of APs to finish moving to the secondary controller

13 Once done, add the next Site Tag(s) to the Site Filter and click **Update Site Filter**



N+1 Site Based Hitless Upgrade with WebUI

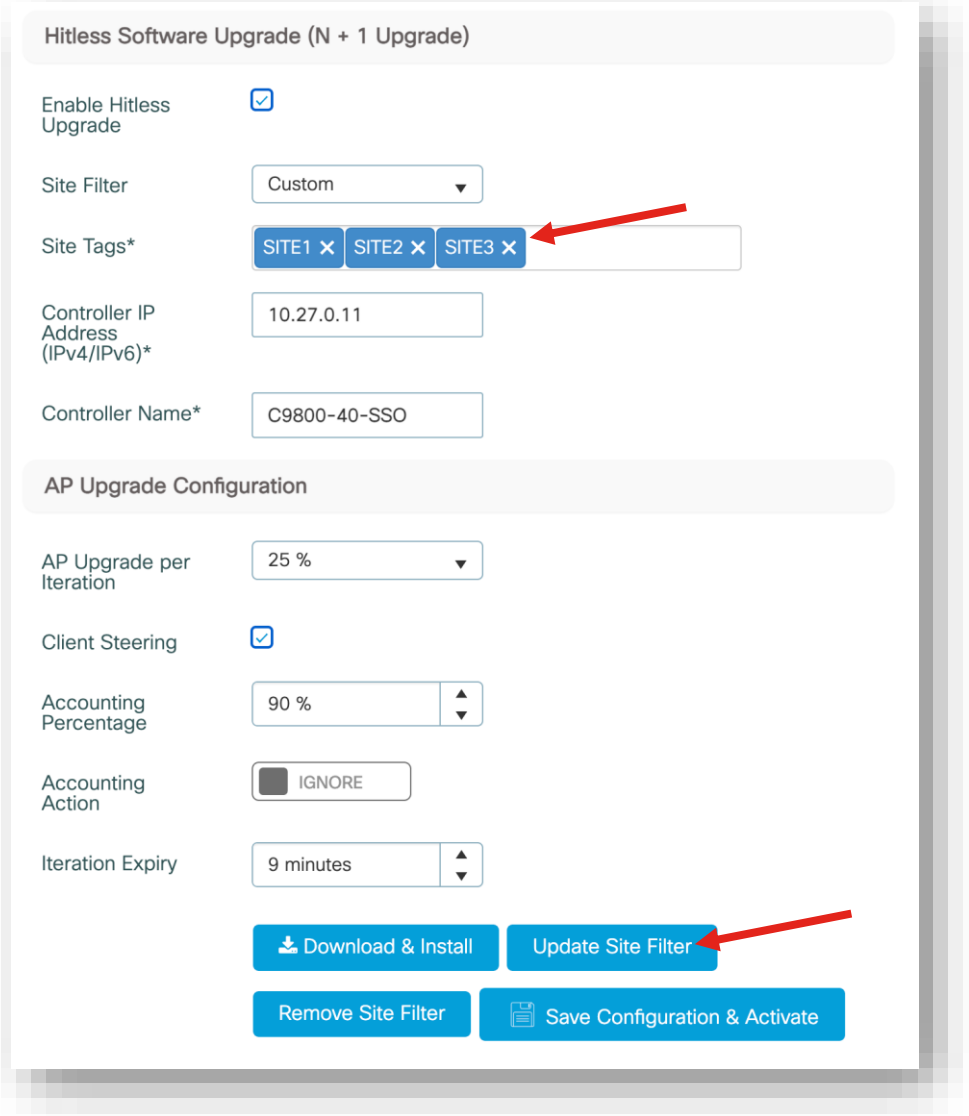
10 Monitor the progress of the entire upgrade in the **Status** Window

11 Click **AP Upgrade Statistics** to track each iteration of AP upgrade

12 Wait for the current iteration of APs to finish moving to the secondary controller

13 Once done, add the next Site Tag(s) to the Site Filter and click **Update Site Filter**

14 Repeat Steps 12 and 13 as needed



N+1 Site Based Hitless Upgrade with WebUI

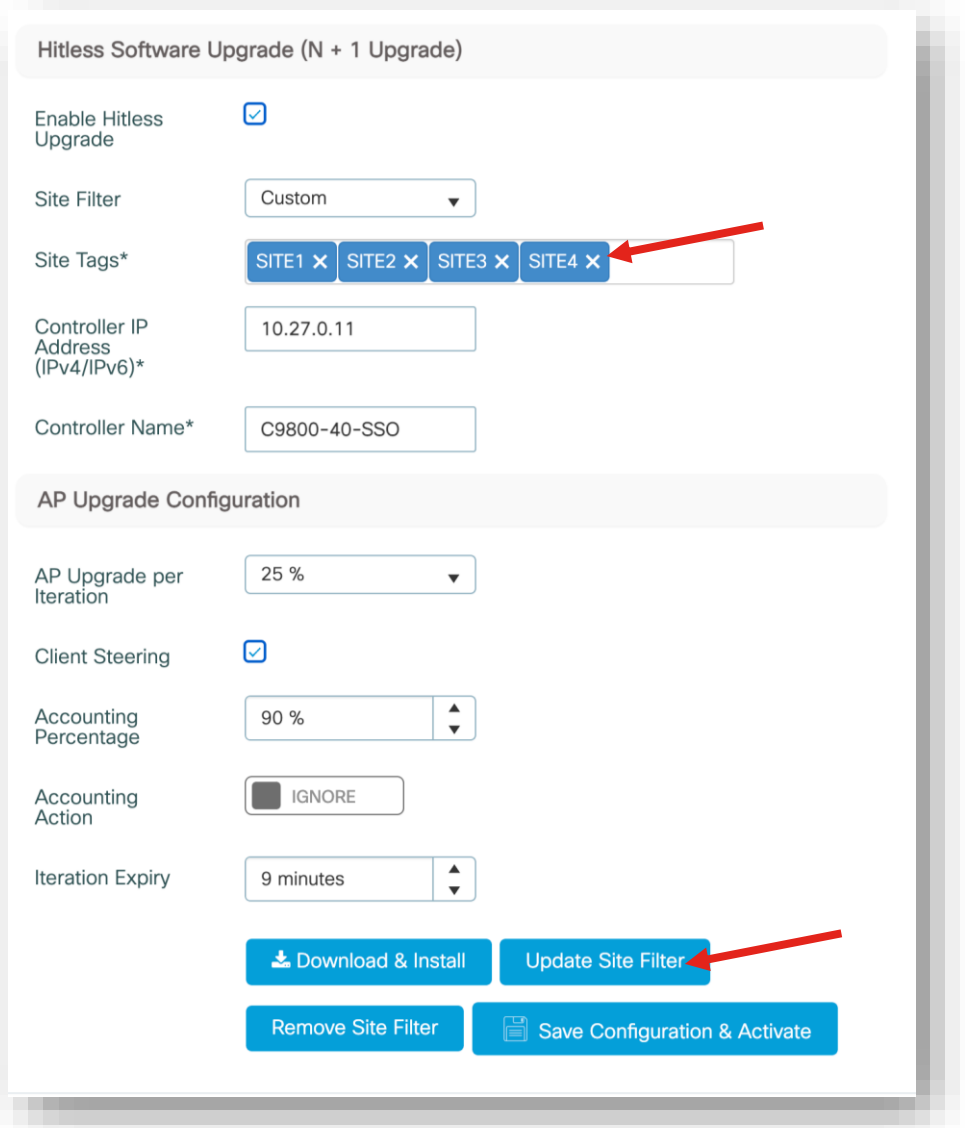
10 Monitor the progress of the entire upgrade in the **Status** Window

11 Click **AP Upgrade Statistics** to track each iteration of AP upgrade

12 Wait for the current iteration of APs to finish moving to the secondary controller

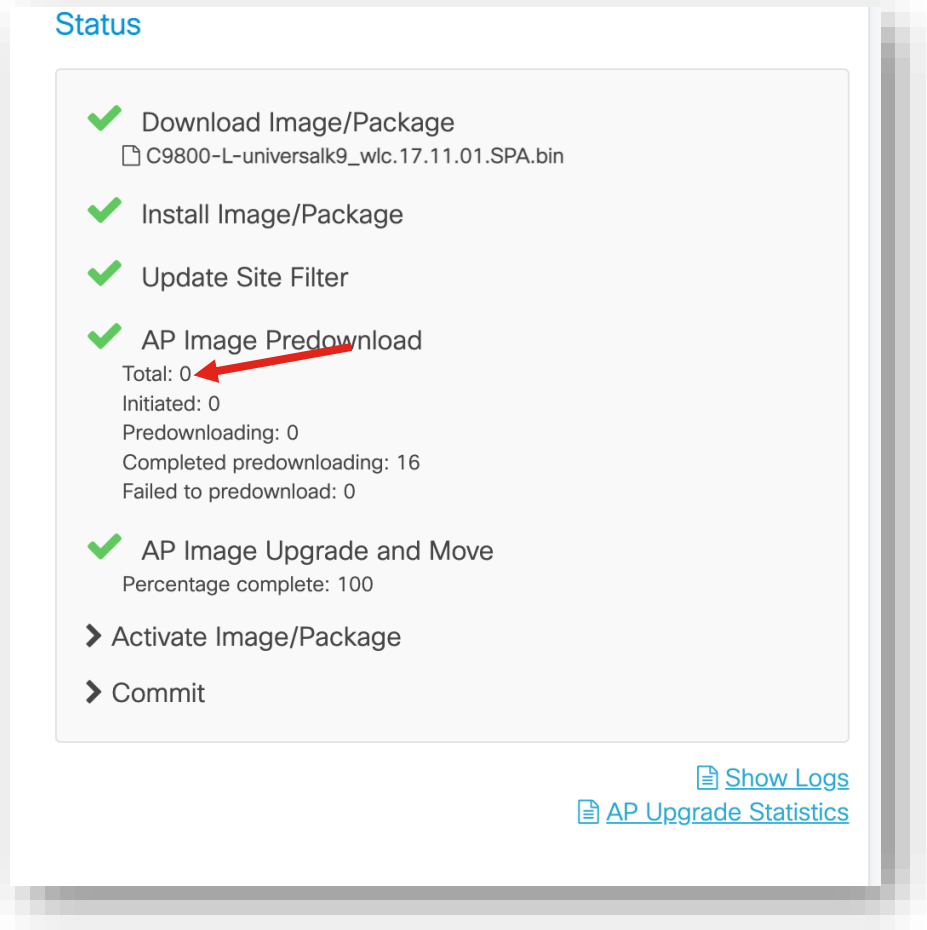
13 Once done, add the next Site Tag(s) to the Site Filter and click **Update Site Filter**

14 Repeat Steps 12 and 13 as needed



N+1 Site Based Hitless Upgrade with WebUI

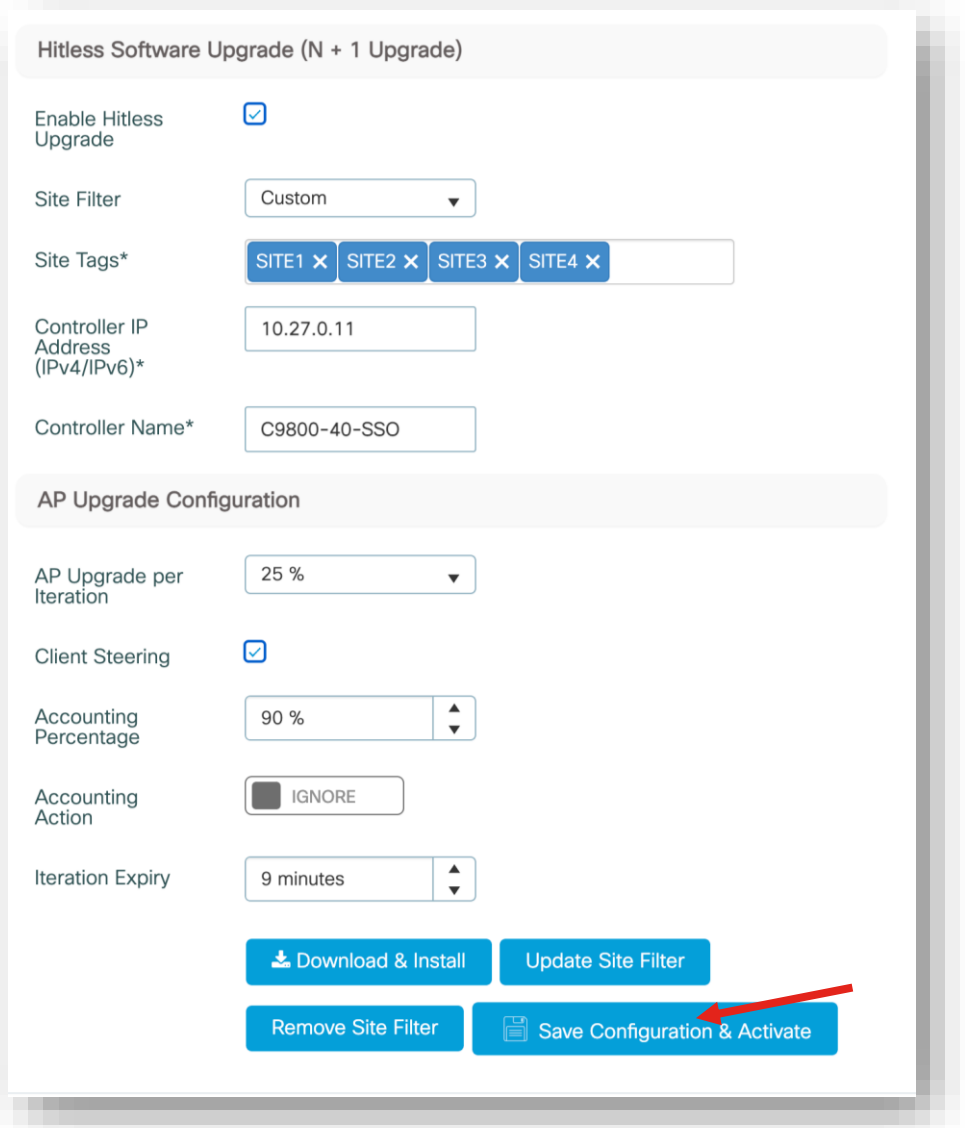
15 All APs are upgraded when the **Total** is 0



N+1 Site Based Hitless Upgrade with WebUI

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

16 Apply the upgrade by clicking **Save Configuration & Activate**



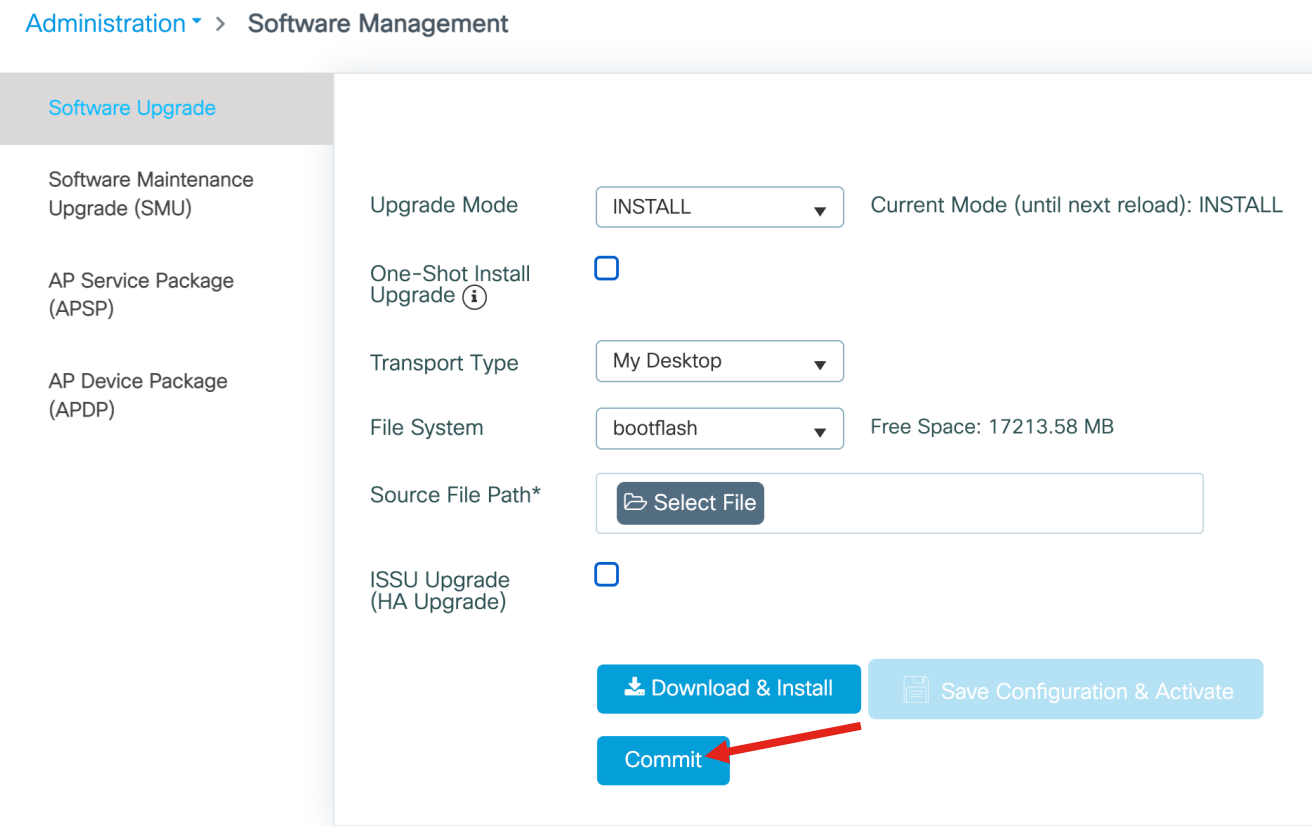
N+1 Site Based Hitless Upgrade with WebUI

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

16 Apply the upgrade by clicking **Save Configuration & Activate**

17 After the controller reloads, commit the upgrade by clicking **Commit**

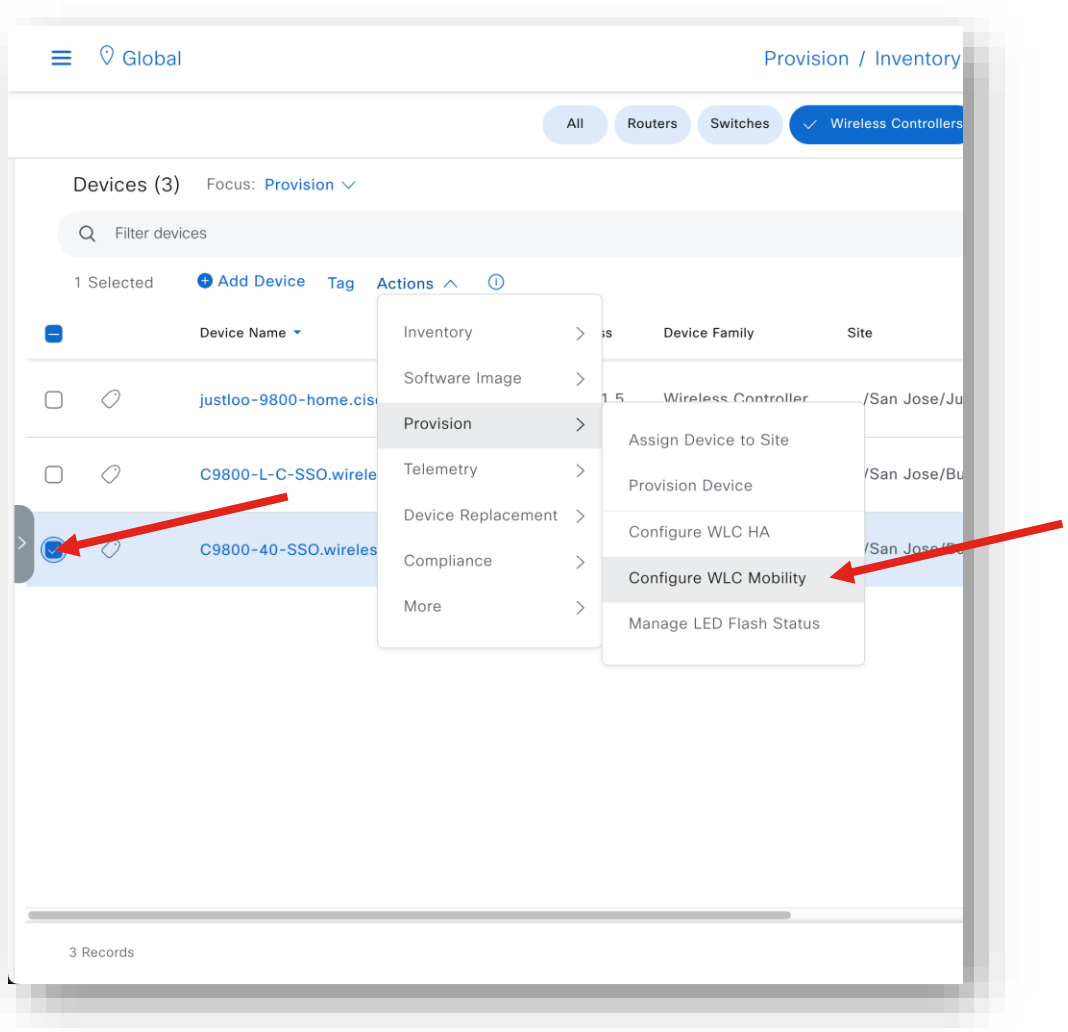
18 If required, use the CLI to move the APs back to the primary on a site-by-site basis



N+1 Hitless Upgrade with Cisco DNA Center

Create Mobility Group

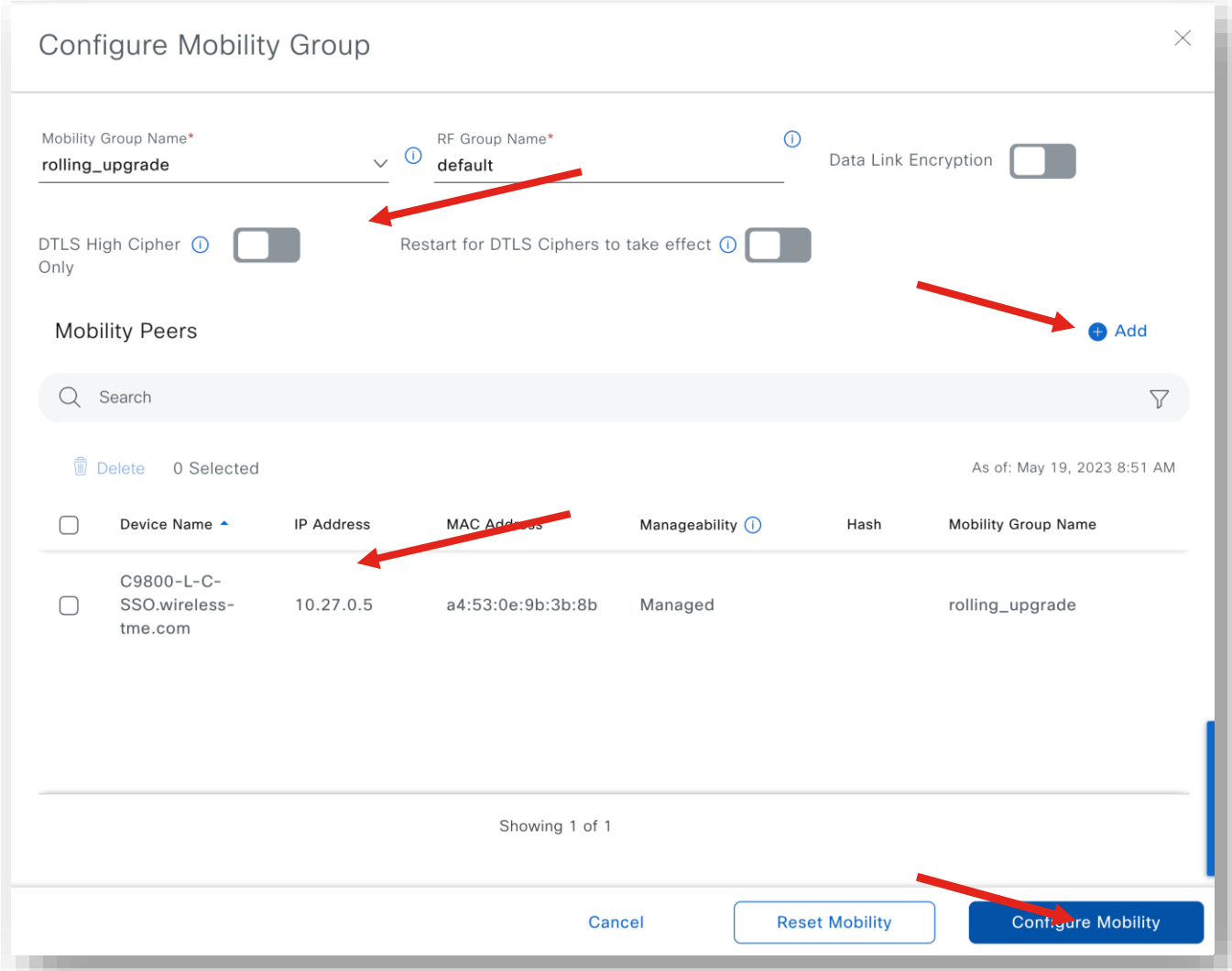
1. Select the Primary Controller
2. Go to **Provision → Configure WLC Mobility**



N+1 Hitless Upgrade with Cisco DNA Center

Create Mobility Group

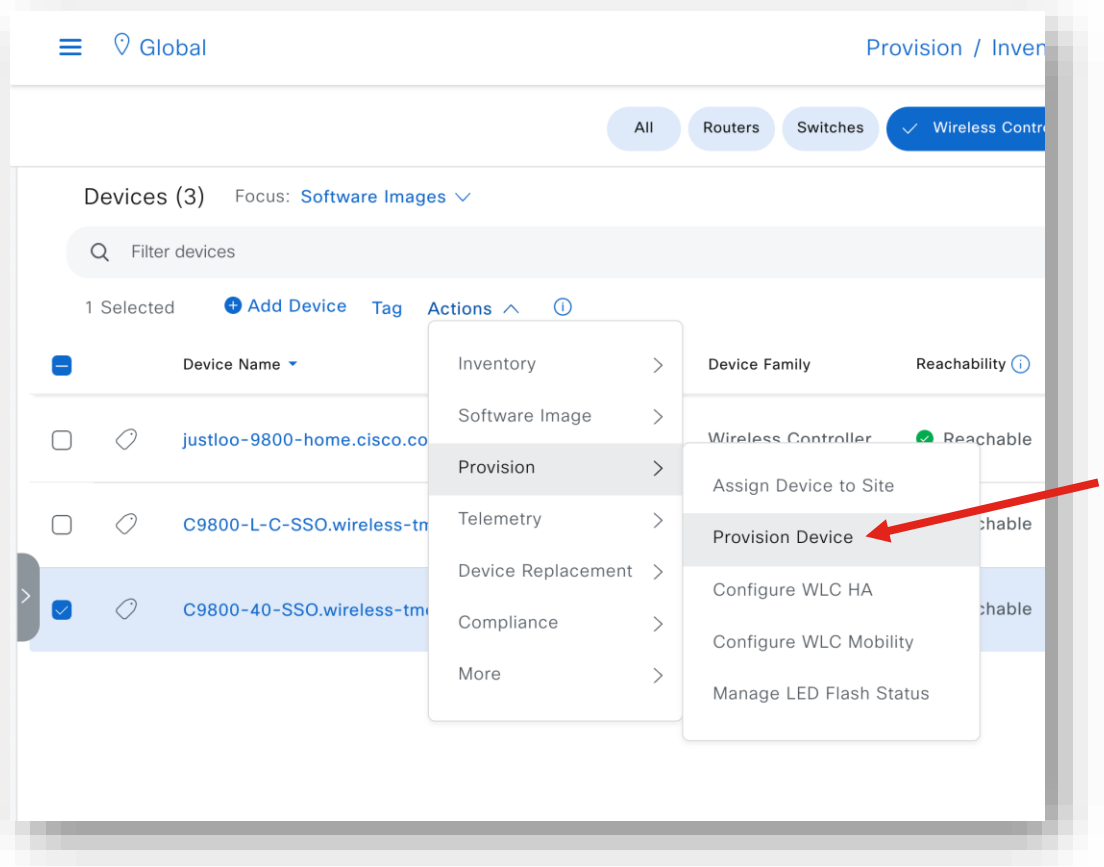
3. Add a new **Mobility Group Name**
4. Click **Add** to add a new Mobility Peer
5. In the Device Details, select the **Secondary WLC** and click **Save**.
6. Click **Configure Mobility**



N+1 Hitless Upgrade with Cisco DNA Center

Enable Rolling AP Upgrade

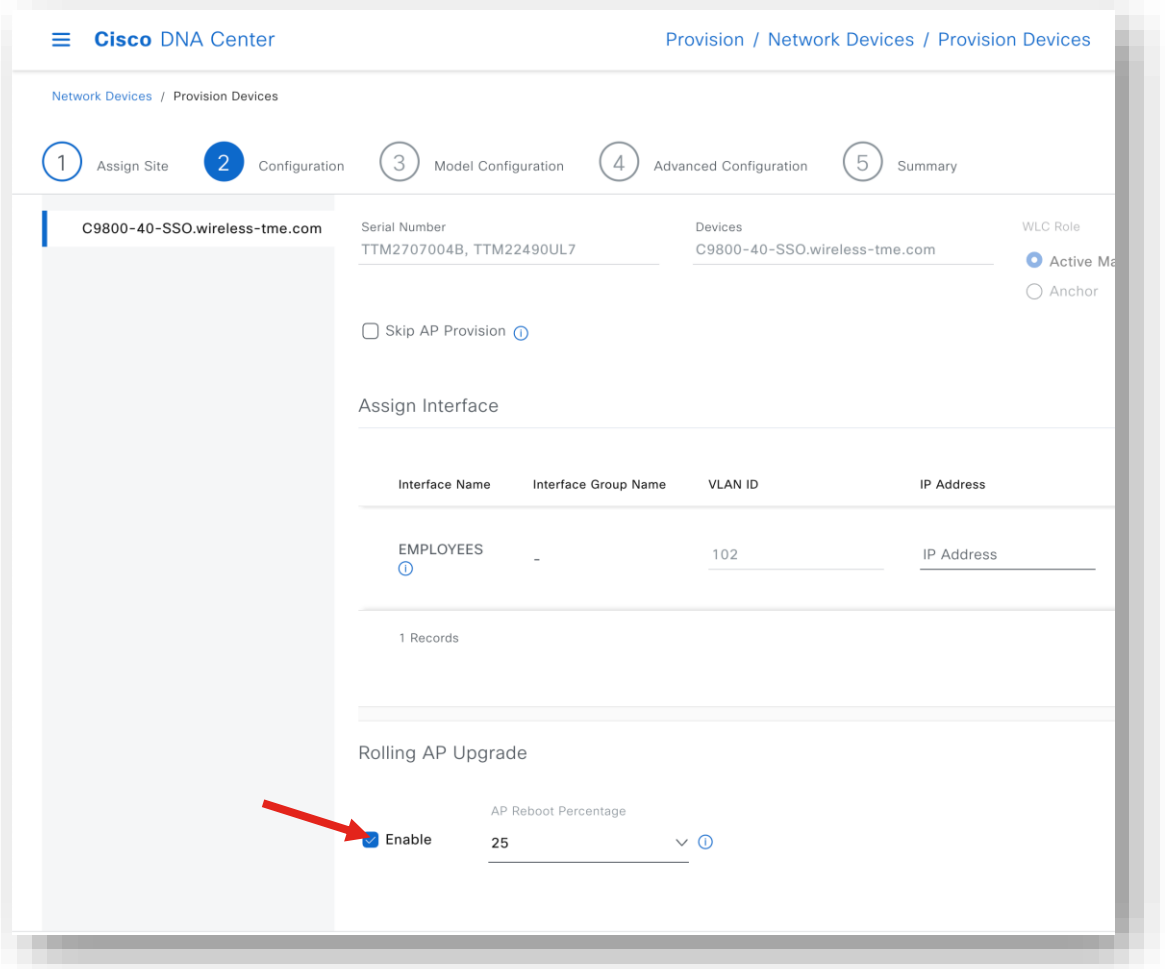
1. Select the Primary WLC and go to **Provision → Provision Device**



N+1 Hitless Upgrade with Cisco DNA Center

Enable Rolling AP Upgrade

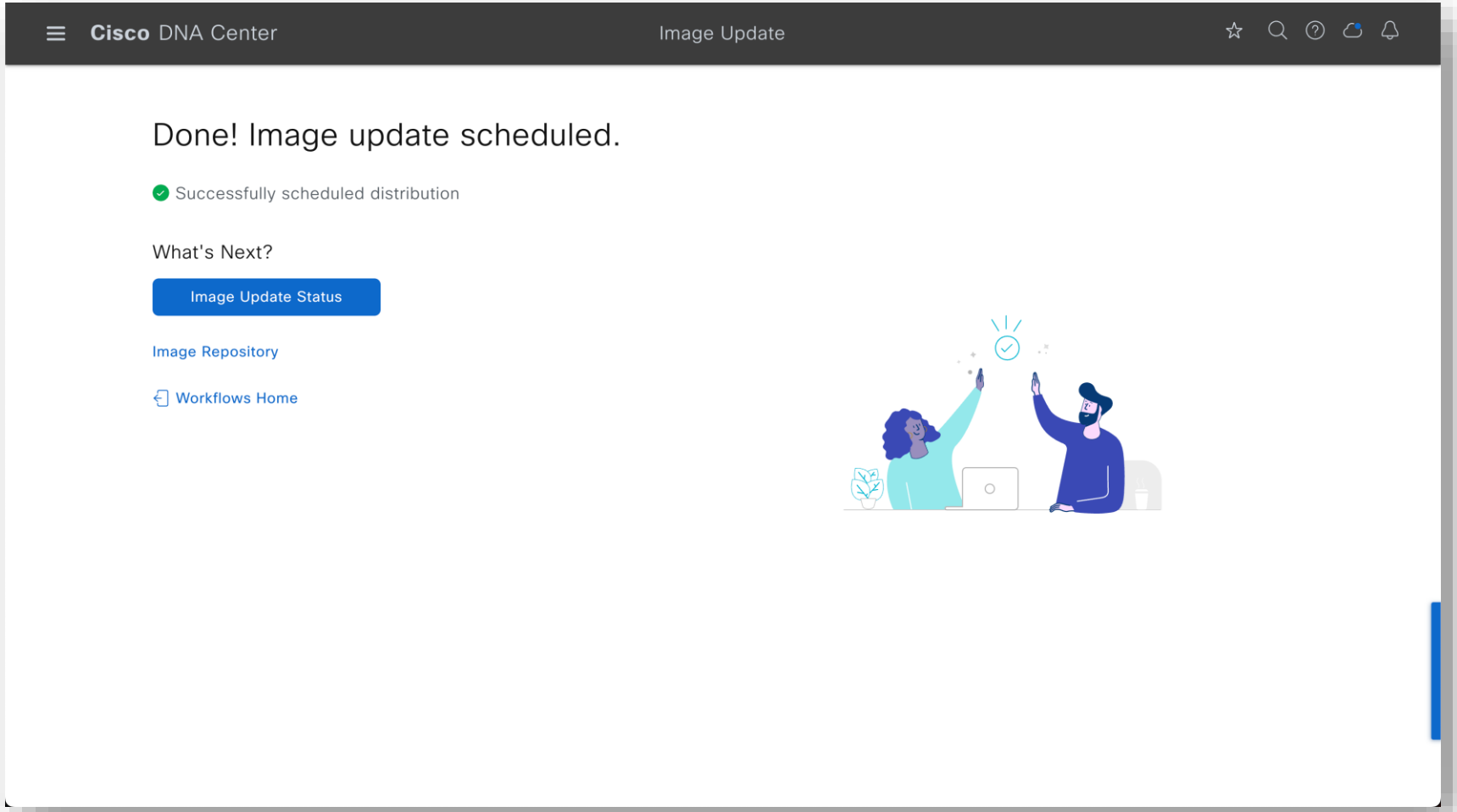
1. Select the Primary WLC and go to **Provision → Provision Device**
2. Check the box for **Enable** choose the **AP Reboot Percentage**
3. Continue the device provisioning as normal



N+1 Hitless Upgrade with Cisco DNA Center

Upgrading the Primary Controller

1. Go through the image upgrade procedure as normal

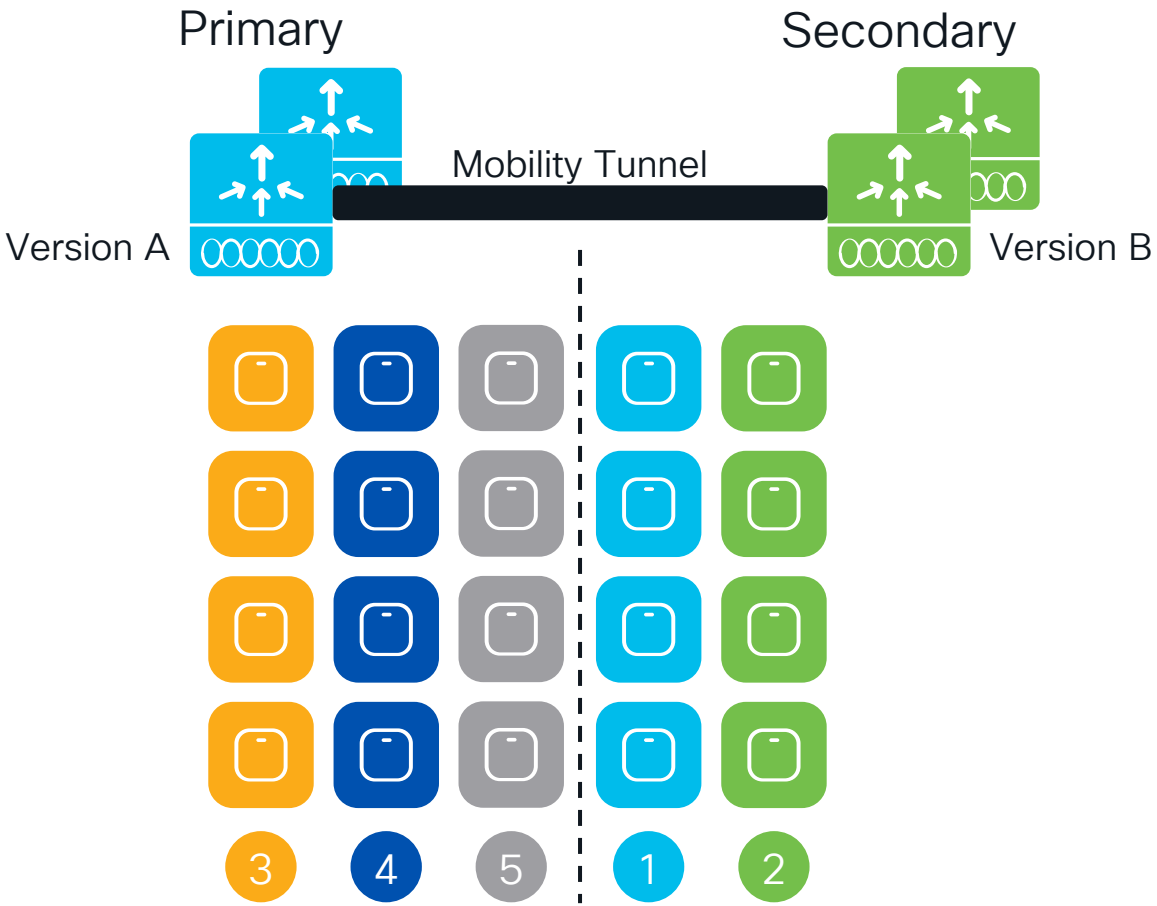


Can I use HA SSO Pair with N+1 Rolling Upgrade?

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

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

Flexibility to upgrade each site while ensuring resiliency



In-Service Software Upgrade (ISSU)

Why ISSU?

Eliminate network downtime during controller upgrade process

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

Automate the process of upgrade without manual intervention

What is ISSU ?

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

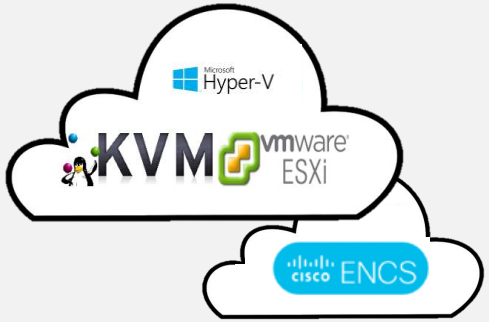
All AP/Client sessions are retained during upgrade process

Pre-requisites:

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

Supported platforms for ISSU

Controllers



Catalyst 9800-CL
Private Cloud

Catalyst 9800-L

Catalyst 9800-40

Catalyst 9800-80

Access Points

Wi-Fi 6 and 6E APs

1815W

1815I, 1815M

1832

1842

1852

2802

3802

1700, 2700, 3700,
1570 Wave 1 APs

1540

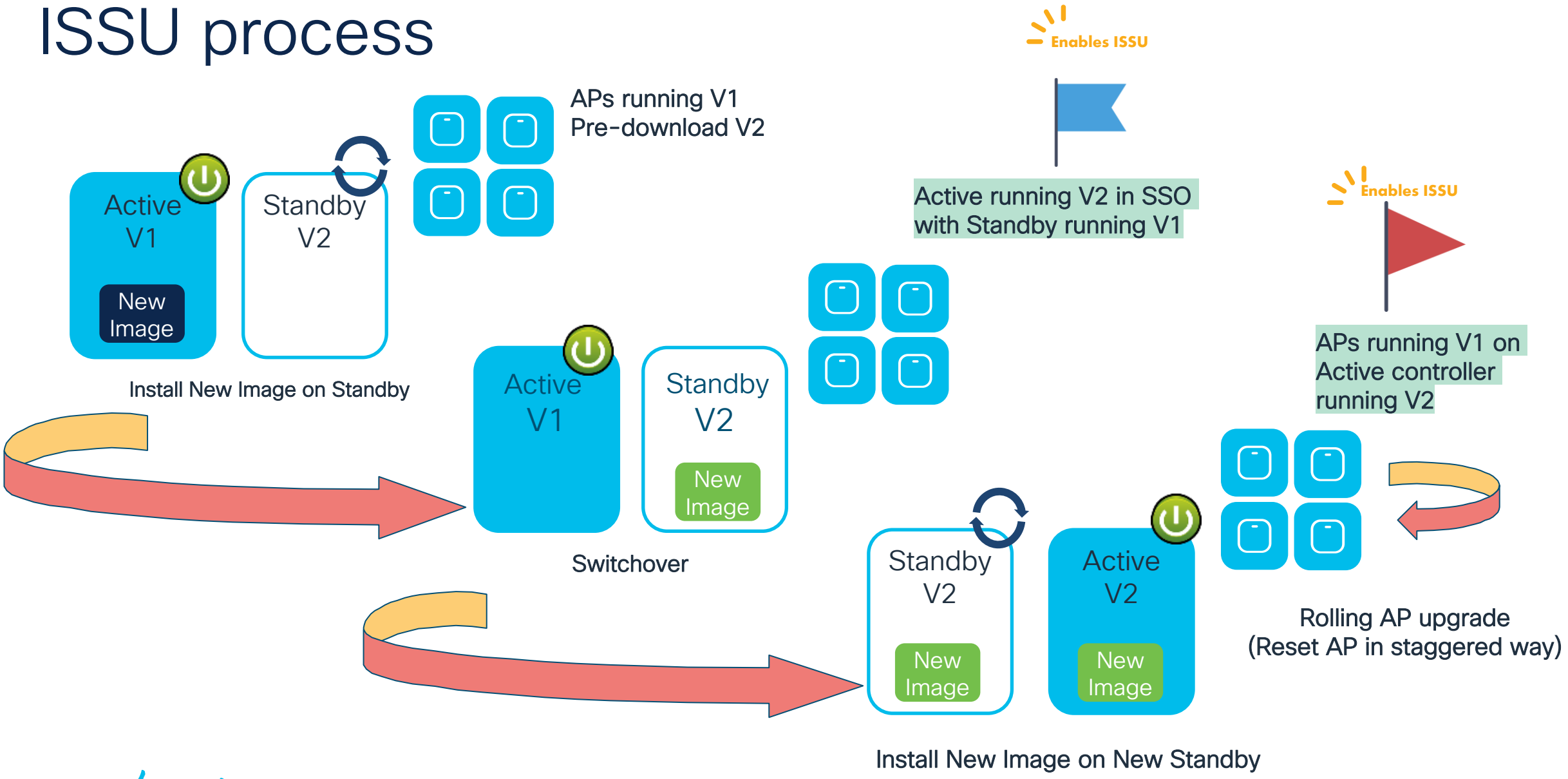
1560

4800

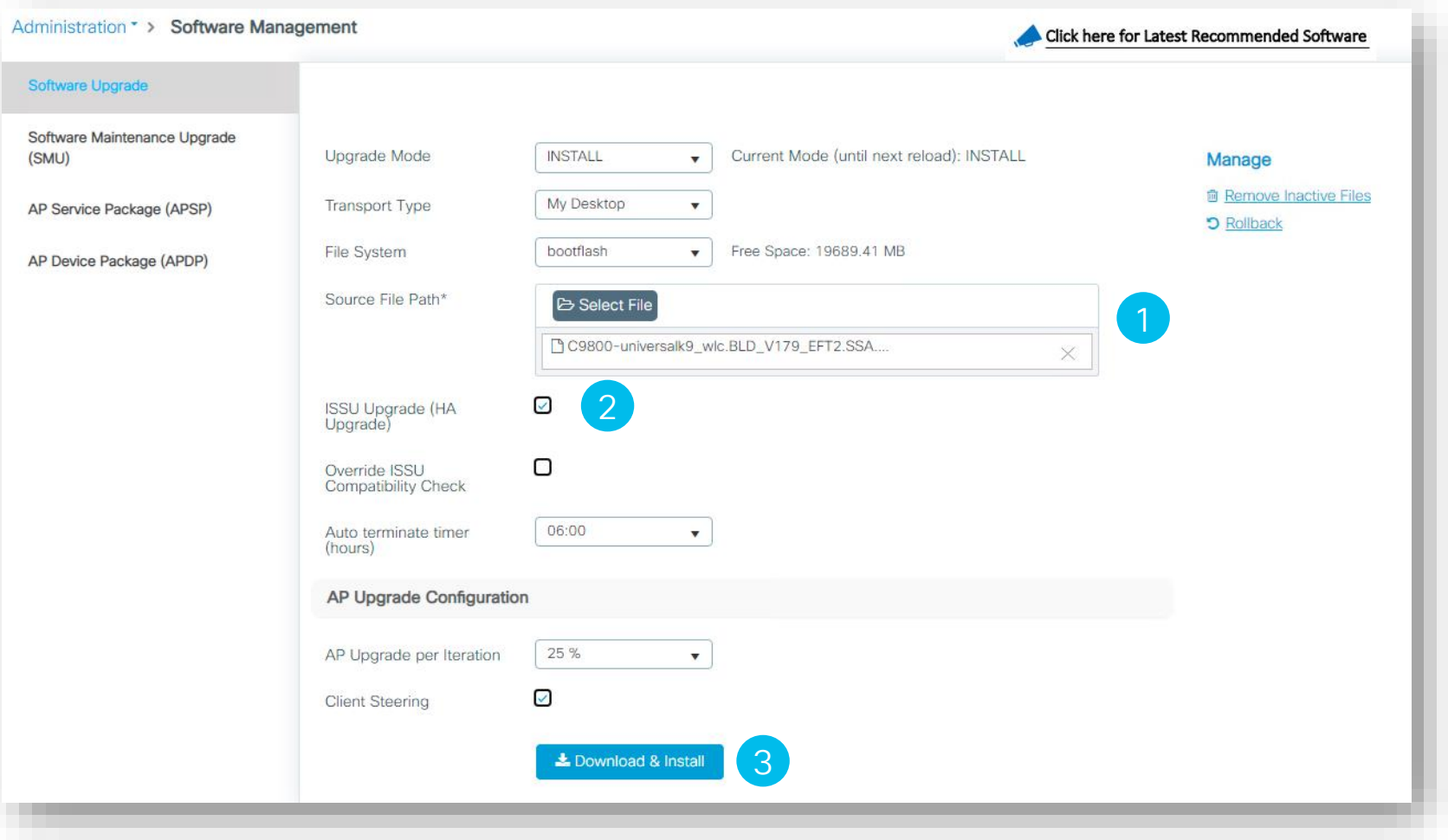
Wave 2 indoor and outdoor APs

Ensure APs are supported by target software version.

ISSU process

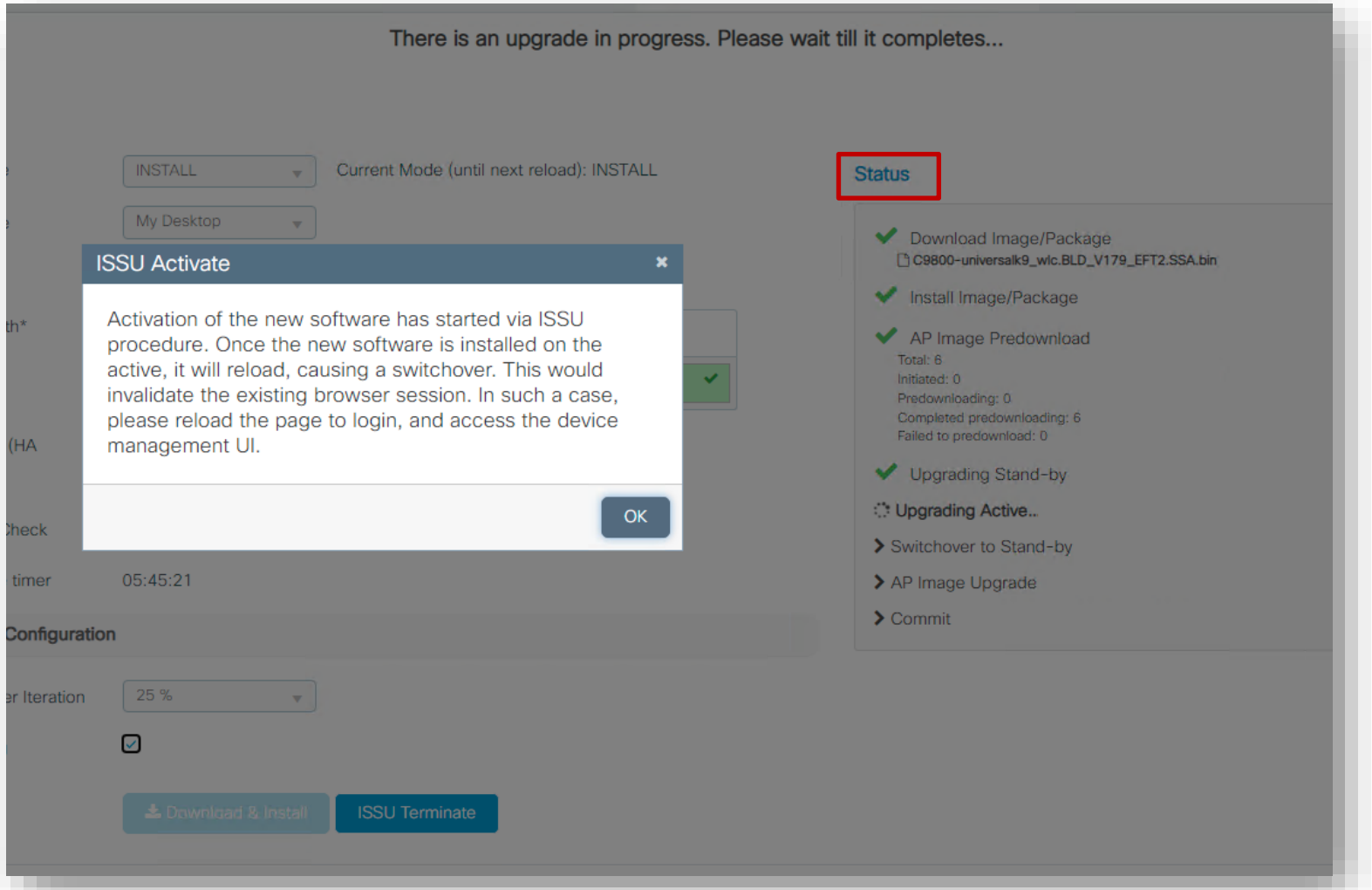


Easy ISSU upgrade with WebUI!



1. Select the image you want to upgrade to
2. Enable ISSU and select % for Rolling AP upgrade
3. Click Download and Install

Easy ISSU upgrade with WebUI!



- Monitor the progress of ISSU upgrade via the Status section in GUI
- Any important messages will trigger a popup window

Easy ISSU upgrade with WebUI!

Administration > Software Management

Click here for Latest Recommended Software

- Software Upgrade
- Software Maintenance Upgrade (SMU)
- AP Service Package (APSP)
- AP Device Package (APDP)

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

Upgrade Mode	INSTALL	Current Mode (until next reload): INSTALL
Transport Type	My Desktop	
File System	bootflash	Free Space: 19689.96 MB
Source File Path*	Select File	
ISSU Upgrade (HA Upgrade)	☑	
Override ISSU Compatibility Check	☐	
Auto terminate timer	05:32:26	

AP Upgrade Configuration

AP Upgrade per Iteration	25 %
Client Steering	☑

Download & Install | Commit | ISSU Terminate

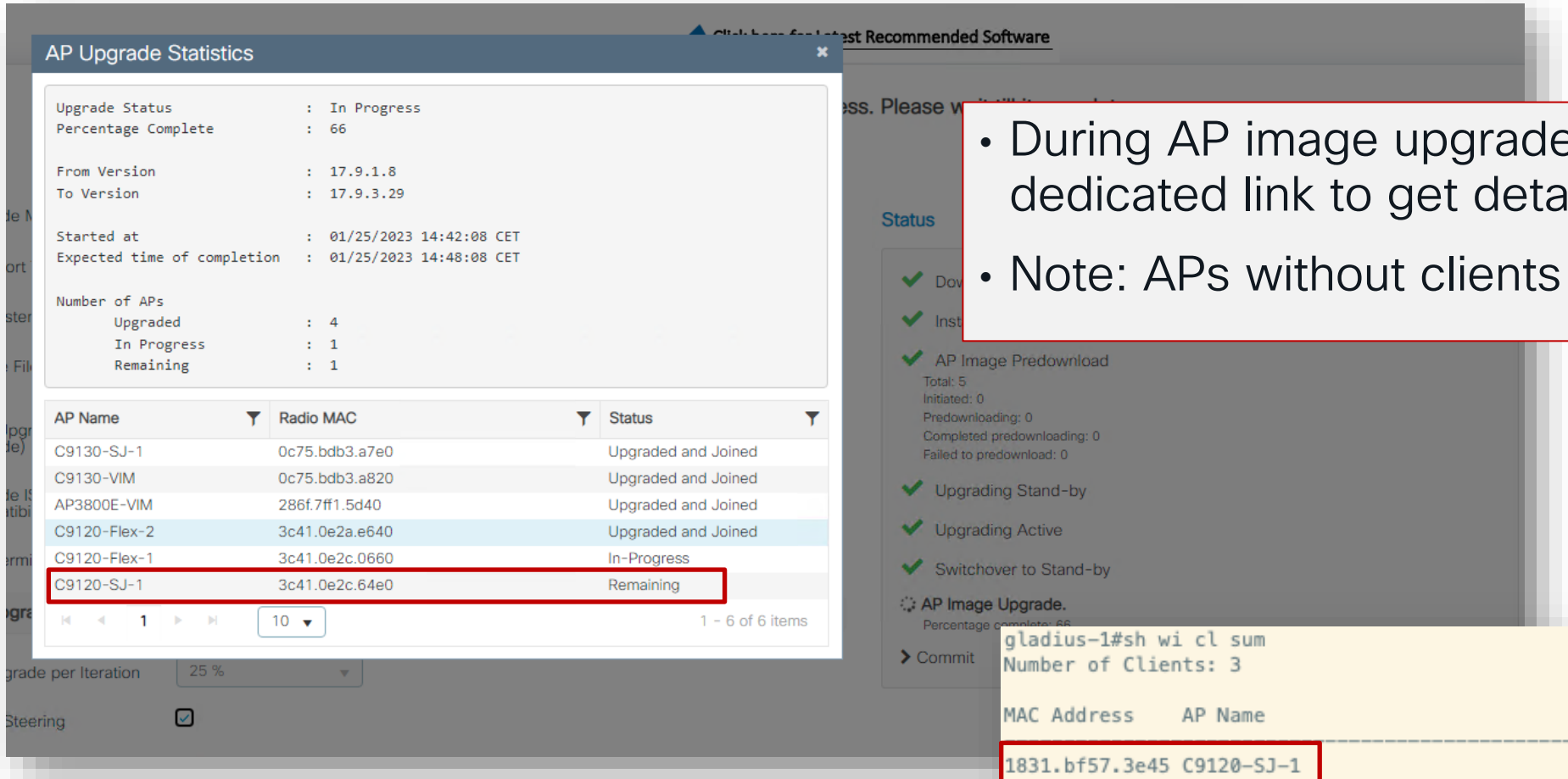
Status

- ✔ Download Image/Package
- ✔ Install Image/Package
- ✔ AP Image Predownload
  Total: 5
  Initiated: 0
  Predownloading: 0
  Completed predownloading: 0
  Failed to predownload: 0
- ✔ Upgrading Stand-by
- ✔ Upgrading Active
- ✔ Switchover to Stand-by
- AP Image Upgrade
  Percentage complete: 16
- Commit

Show Logs
AP Upgrade Statistics

Any time you can click on the Show Logs to see what's going on...

Easy ISSU upgrade with WebUI!



- During AP image upgrade, click on the dedicated link to get detailed information
- Note: APs without clients are upgraded first

```
gladius-1#sh wi cl sum
Number of Clients: 3

MAC Address    AP Name                                    Type ID   State
-------------------------------------------------------------------------
1831.bf57.3e45 C9120-SJ-1                                 WLAN 1    Run
4ced.fb3a.d9fe C9120-SJ-1                                 WLAN 1    Run
bcec.23c3.6106 C9120-SJ-1                                 WLAN 1    Run

Number of Excluded Clients: 0
```

Easy ISSU upgrade with WebUI!

C9120-SJ-1 still not upgraded

```
sh ap upgrade
```

```
Remaining
---------
Number of APs: 1
AP Name                          Radio MAC
-----------------------------------------------
C9120-SJ-1                       3c41.0e2c.64e0
```

- Client steering happens on the AP with clients
- Once all clients are moved the AP is upgraded

Client steering in progress...

```
gladius-1#sh wi cl summary
Number of Clients: 3

MAC Address    AP Name                                    Type ID   State
-----------------------------------------------------------------------------
1831.bf57.3e45 C9120-Flex-2                               WLAN 1    Run
4ced.fb3a.d9fe C9120-SJ-1                                 WLAN 1    Run
bcec.23c3.6106 C9120-Flex-2                               WLAN 1    Run
```

```
gladius-1#sh wi cl summary
Number of Clients: 3

MAC Address    AP Name                                    Type ID   State
-----------------------------------------------------------------------------
1831.bf57.3e45 C9120-Flex-2                               WLAN 1    Run
4ced.fb3a.d9fe C9120-Flex-2                               WLAN 1    Run
bcec.23c3.6106 C9120-Flex-2                               WLAN 1    Run
```

C9120-SJ-1 upgrade started...

```
In Progress
-----------
Number of APs: 1
AP Name                          Radio MAC
-----------------------------------------------
C9120-SJ-1                       3c41.0e2c.64e0

Remaining
---------
Number of APs: 0
AP Name                          Radio MAC
-----------------------------------------------
```

Easy ISSU upgrade with WebUI!

Microsoft Bing namaqua national park

Command Prompt

client 1

```
Reply from 8.8.8.8: bytes=32 time=7ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=7ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115

Ping statistics for 8.8.8.8:
    Packets: Sent = 3440, Received = 3411, Lost = 29 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 2373ms, Average = 8ms
Control-C
^C
C:\Users\simone>
C:\Users\simone>
```

client 2

Prompt dei comandi

```
Risposta da 8.8.8.8: byte=32 durata=6ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=10ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=7ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=6ms TTL=115
Risposta da 8.8.8.8: byte=32 du
Risposta da 8.8.8.8: byte=32 du
Risposta da 8.8.8.8: byte=32 du
Risposta da 8.8.8.8: byte=32 du
Risposta da 8.8.8.8: byte=32 du
Risposta da 8.8.8.8: byte=32 du
Risposta da 8.8.8.8: byte=32 du
Risposta da 8.8.8.8: byte=32 du
Risposta da 8.8.8.8: byte=32 du
Risposta da 8.8.8.8: byte=32 du

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 2784
    Persi = 16 (0% persi),
Tempo approssimativo percorsi a
    Minimo = 5ms, Massimo =  38
Control-C
^C
C:\Users\Simone>
```

client 3

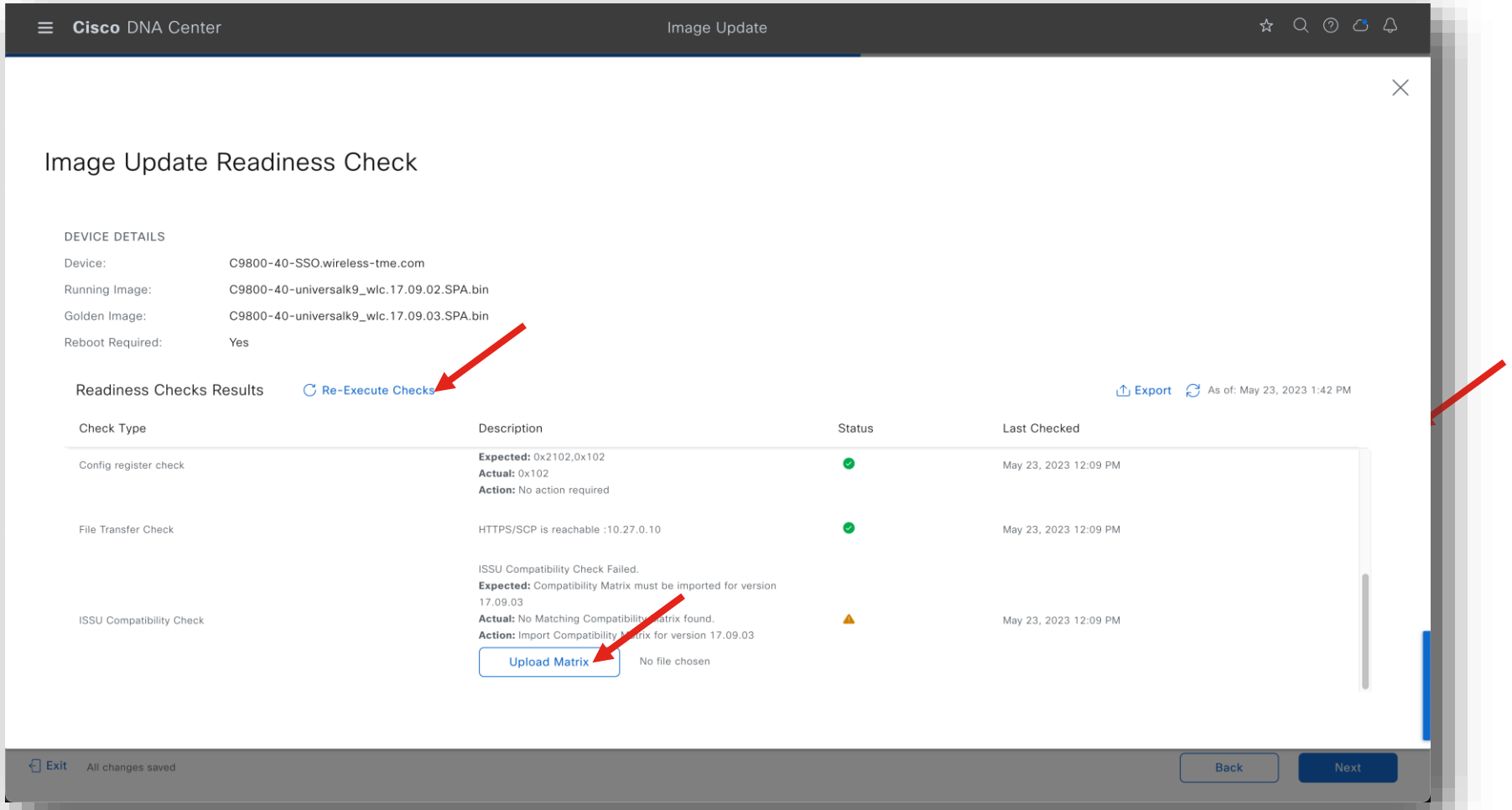
Command Prompt

```
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=10ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=7ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=7ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115
Reply from 8.8.8.8: bytes=32 time=6ms TTL=115

Ping statistics for 8.8.8.8:
    Packets: Sent = 3401, Received = 3381, Lost = 20 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 311ms, Average = 7ms
Control-C
^C
C:\Users\simone>
```

- < 30 pings lost over 3k transmitted
- 0% ping loss in the whole process!!

Upgrading HA SSO Pair using ISSU and Cisco DNA Center

1. Upload the ISSU Compatibility Matrix, if not uploaded already
2. Re-Execute the Readiness Check



Upgrading HA SSO Pair using ISSU and Cisco DNA Center

3 Enable ISSU Update for the Controller

4 Go through the image upgrade procedure as normal

Cisco DNA Center | Image Update

Device Activation Order

You can use filters to sort devices and order their activation in parallel or sequentially. After devices are sorted, you can reorder them sequentially.

Device in Parallel(1) Edit Order

Parallel Sequential

Filter Devices

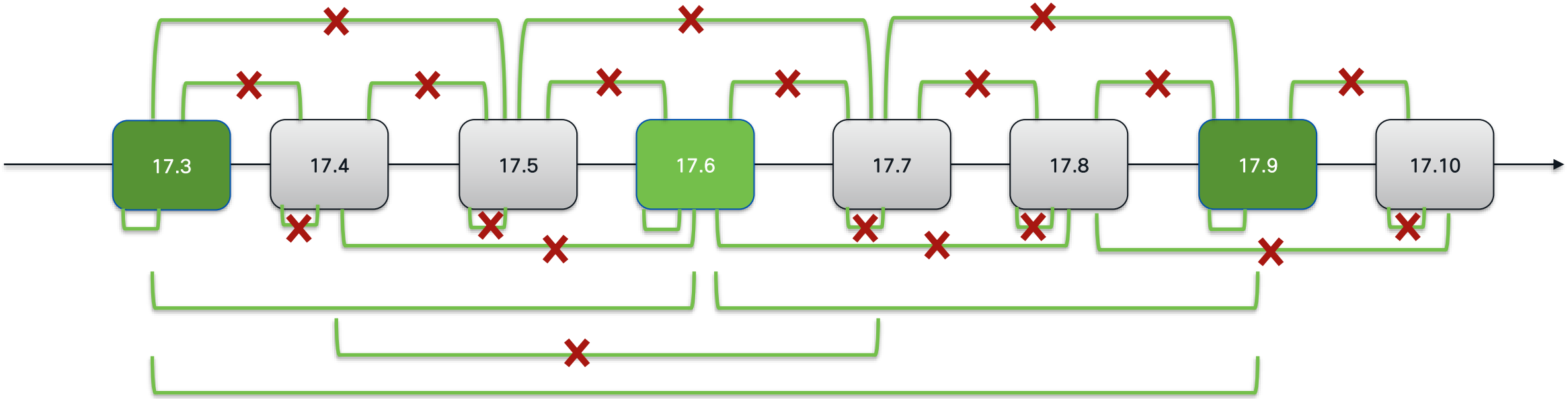
1 Selected Move to Sequential Update Order ISSU

Device Name	IP Address	Site	Device Series	Device Role	Current Image	Update Image	Comment
C9800-40-SSO.wireless-tme.com	10.27.0.11	Global/San Jose/Buildi...	Cisco Catalyst 9800 S...	Access	C9800-40-universalk9_...	C9800-40-universalk9_... ISSU	ISSU Validation Successful Update Readiness Report

1 Records Show Records: 25 1 - 1

Exit All changes saved Back Next

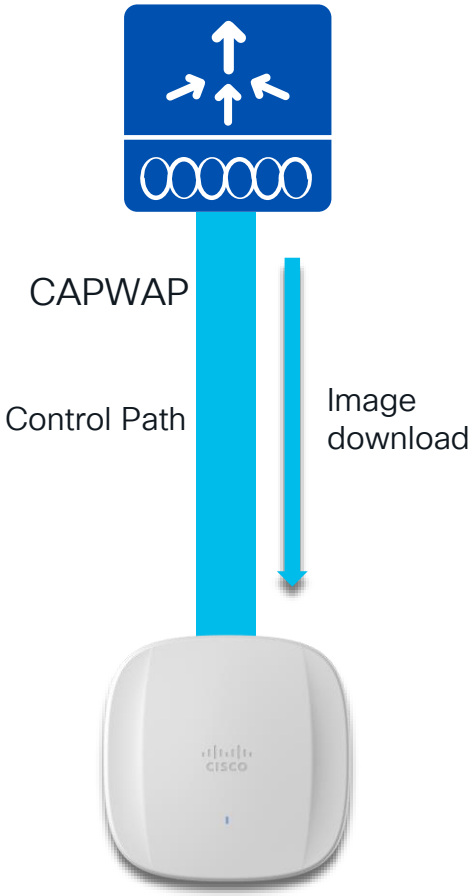
ISSU official support Matrix



Supported	Not Supported
• N +2 - Within EM release (17.9.1 <> 17.9.3) • N +2 - Across EM release (17.3.X <> 17.9.X) *EM = Extended Maintenance release* *SM = Standard Maintenance release*	• Within EM release beyond +2 release • Across EM release beyond +2 release • Across software release trains (e.g., 17.12 to 18.1) • Within SM release (17.1.1 <> 17.1.2) • Across SM release • EM <> SM release • Downgrade from any release to any release • No support on Engineering Special (ES) releases

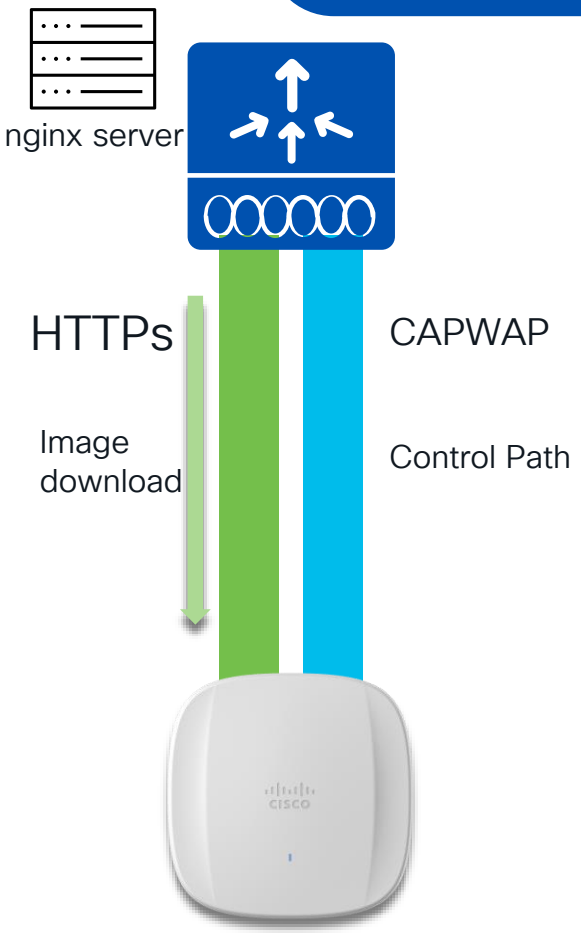
How can I improve AP image download time?

Before IOS XE 17.11.1



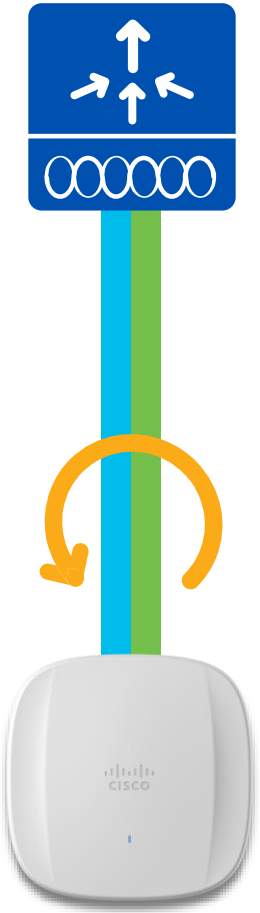
- AP image download happens over CAPWAP Control Path
- Slow by limitation with CAPWAP window size
- Image downloads WNCd process increases CPU work-load

After IOS XE 17.11.1



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

Fallback to CAPWAP if HTTPs Failure



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

Supported Platforms

- All Physical and Virtual Appliances
  - C9800-80, C9800-40, C9800-L, C9800-CL Private and Public Cloud
- Not Supported on:
  - Embedded Wireless Controller on AP

CLI Configuration

- Enable AP image download through HTTPs

```
C9800# conf t
C9800(config)# ap upgrade method https
```

- Customize the HTTPs port number (default is 8443)

```
C9800(config)# ap file-transfer https port <port_number>
```

CLI Verifications

- Verify AP image download method enabled/disabled

```
C9800# show ap upgrade method

 AP upgrade method HTTPS : Disabled
```

- Show command to verify AP file transfer port

```
C9800# show ap file-transfer https summary

  Configured port                    : 8443
  Operational port                   : 8443
```

CLI Verifications

- Verification of ap image download over https support

```
C9800# show ap name AP2800 config general | sec Upgrade


  AP Upgrade Out-Of-Band Capability                : Enabled
```

- Verification of ap image download history

```
C9800# show wireless stats ap image-download



AP image download info for last attempt
AP Name                  Count  ImageSize   StartTime          EndTime            Diff(secs)  Predownload  Aborted              Method
-----------------------------------------------------------------------------------------------------------------------------------------
AP_3800_1                 1      60856320    11/14/22 12:31:21  11/14/22 12:32:21  59          No           No                   HTTPS
AP2800                    1      60856320    11/14/22 12:27:43  11/14/22 12:28:39  56          No           No                   HTTPS
```

6. Software Patching Capability

^SMU on MD Release only

Controller and AP software upgrades

Controller Updates

Controller update or bug fixes

SMU^

PSIRTs, Fixes on APs

AP updates or bug fixes

AP Service Pack

New AP Model Support

Hot-patchable support for Device Pack

AP Device Pack

Contain impact within release
Fixes for defects and security issues without need to requalify a new release

Faster resolution to critical issues
Provide fixes to critical issues found in network devices that are time-sensitive

Wireless Controller SMU (Software Maintenance Update)

Wireless Controller SMU

Wireless Controller SMU installation Options

- Software Maintenance Update (SMU) is the ability to apply patch fixes on a software release in the customer network
- Current mechanism relies on Engineering Specials
  - Entire image is rebuilt and delivered to customer

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

Hot-Patching

Inline replace of functions without restarting the process

On SSO Systems, patch will be applied on both active and standby without any reload

Cold Patch
Wireless Controller Reboot

Cold Patching

Install of a SMU will require a system reload

On SSO systems, SMU updates can be installed on the HA Pair with zero downtime

Controller SMU

Standalone vs Redundant Wireless Controller

	Hot Patch (No Wireless Controller reboot) Auto Install on Standby	Cold Patch Wireless Controller Reboot
Standalone box	No reload of Controller. AP & Client session won't be affected.	Reload controller. AP & Client sessions would be affected.
Redundant box	SMU activation applies patch on Active & Standby. There is no controller reload and there is no impact to AP and Client sessions.	Follows ISSU path and both Standby & Active controller reloaded but there is no impact to AP and Client session. CLI required for ISSU

Wireless Controller SMU

Standalone vs Redundant Wireless Controller

- Software Maintenance Update (SMU) is the ability to apply patch fixes on a software release in the customer network
- Current mechanism relies on Engineering Special: Entire image is rebuilt and delivered to customer

	Hot Patch (No Wireless Controller reboot) Auto Install on Standby	Cold Patch Wireless Controller Reboot
Standalone box	No reload of Controller. AP & Client session won't be affected.	Reload controller. AP & Client sessions would be affected.
Redundant box	SMU activation applies patch on Active & Standby. There is no controller reload and there is no impact to AP and Client sessions.	Follows ISSU path and both Standby & Active controller reloaded but there is no impact to AP and Client session.

SMU Install via WebUI

Administration > Software Management

Click here for Latest Recommended Software

- Software Upgrade
- Software Maintenance Upgrade (SMU)
- AP Service Package (APSP)
- AP Device Package (APDP)

+ Add Rollback

	Type	State	Filename
○	SMU	Activated and Committed	bootflash:C9800-L-universalk9_wlc.17.03.05a.CSCwb45089.SPA.smu.bin

1 | 10 items per page | 1 - 1 of 1 items

Auto terminate timer: inactive

```
INSTALL COMMIT OPERATION:

Initiating INSTALL_COMMIT operation
install_commit: START Tue Jan 10 14:10:16 PST 2023
install_commit: Committing SMU
Executing pre scripts....
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
  [1] SMU_COMMIT package(s) on chassis 1/R0
  [1] Finished SMU_COMMIT on chassis 1/R0
  [2] SMU_COMMIT package(s) on chassis 2/R0
  [2] Finished SMU_COMMIT on chassis 2/R0
Checking status of SMU_COMMIT on [1/R0 2/R0]
SMU_COMMIT: Passed on [1/R0 2/R0]
Finished SMU Commit operation

SUCCESS: install_commit /bootflash/C9800-L-universalk
9_wlc.17.03.05a.CSCwb45089.SPA.smu.bin Tue Jan 10 14:
10:26 PST 2023
```

SMU ISSU Install via CLI

```
C9800# install add file flash:C9800-L-universalk9_wlc.17.03.05a.CSCwb45089.SPA.smu.bin
install_add: START Tue Jan 10 15:01:47 PST 2023
install_add: Adding SMU
install_add: Checking whether new add is allowed ....
```

```
C9800# install activate file flash:C9800-L-universalk9_wlc.17.03.05a.CSCwb45089.SPA.smu.bin issu
install_activate: START Tue Jan 10 15:03:37 PST 2023
install_activate: Activating ISSU
```

```
C9800# install commit
install_commit: START Tue Jan 10 15:24:23 PST 2023
install_commit: Committing SMU
```

Per-site & Per-AP Model AP Service Pack

Per-site / Per-model AP Service Pack

Supported on all platforms and all deployment scenarios (Flex, Local and Fabric)

Per-model APSP works in conjunction with site-specific rollout

Pre-downloaded to and activated on the affected AP models only

AP Service Packs

Per-AP model Service Pack

APSP can have a subset of APs that are affected by the update

Update on Subset APs

Fix applied on a subset of APs in the deployment using a site-filter

Controlled Propagation

Enables user to control the propagation of APSP in the network

APSP workflow

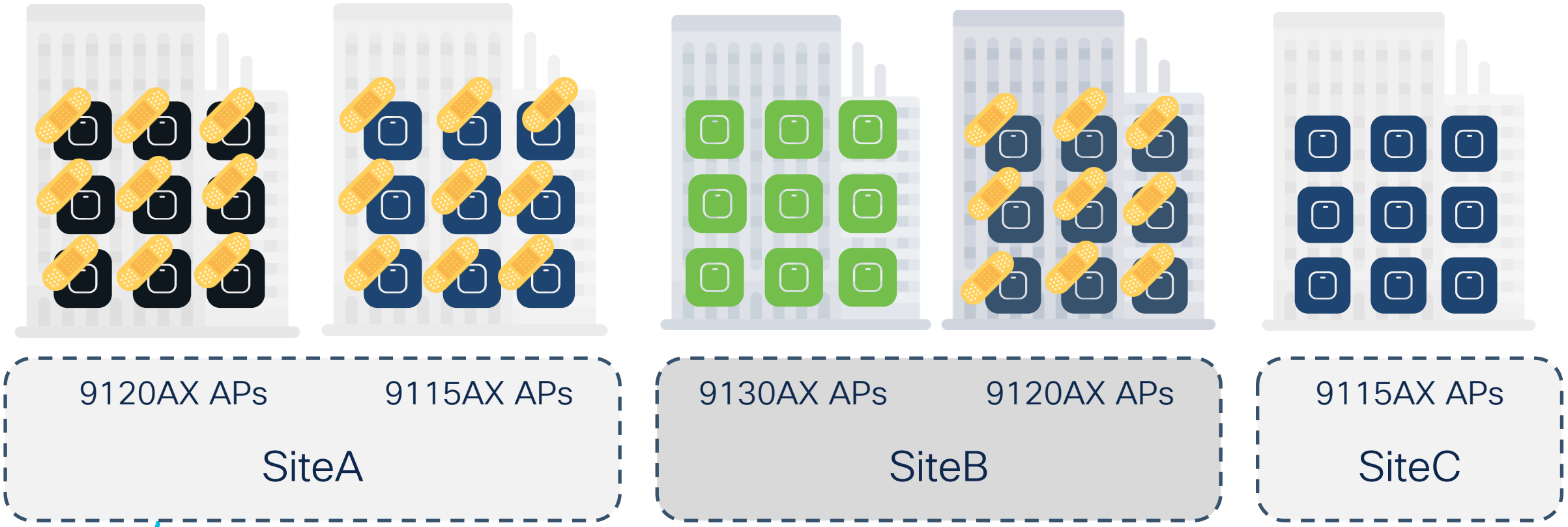
Applying APSP for 9115/9120 APs on per-site and per-model basis

ap image site-filter file APSP1 add SiteA
Install prepare activate
Install activate
Install commit

Apply on Site A in rolling AP fashion

ap image site-filter file APSP1 add Site B
ap image file APSP1 site-filter apply

Not applicable for building with 9130AX



AP Device Pack (APDP)

AP Device Pack

Traditionally …

New AP hardware models need new WLC software

Wait for CCO version and re-qualify new release

Plan for Upgrading entire network

With AP Device Packs

Contain Impact within release

Deploy new hardware without need to requalify a new controller release

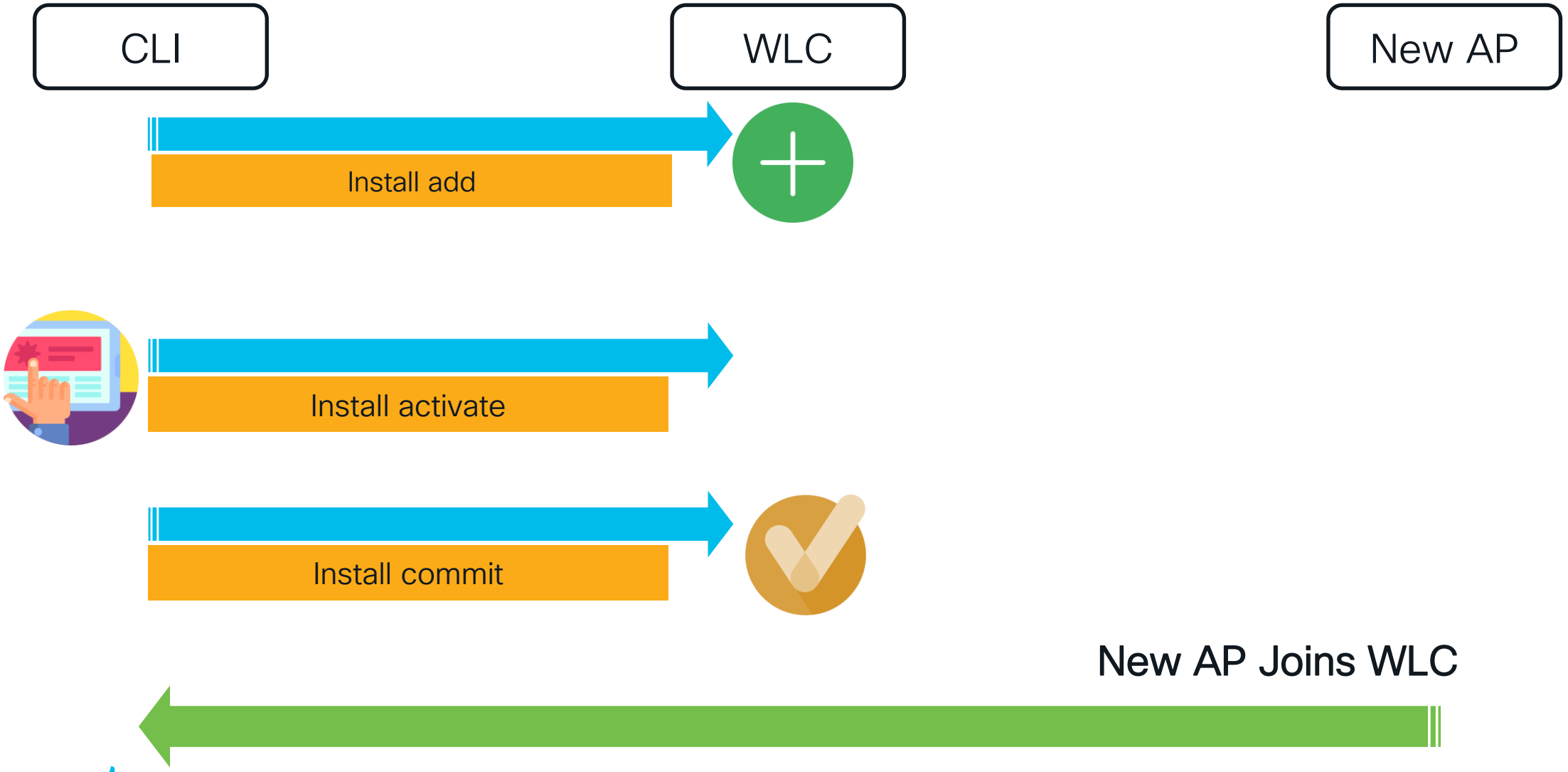
Reduce Lifecycle delays

Faster deployment of latest AP hardware and technology

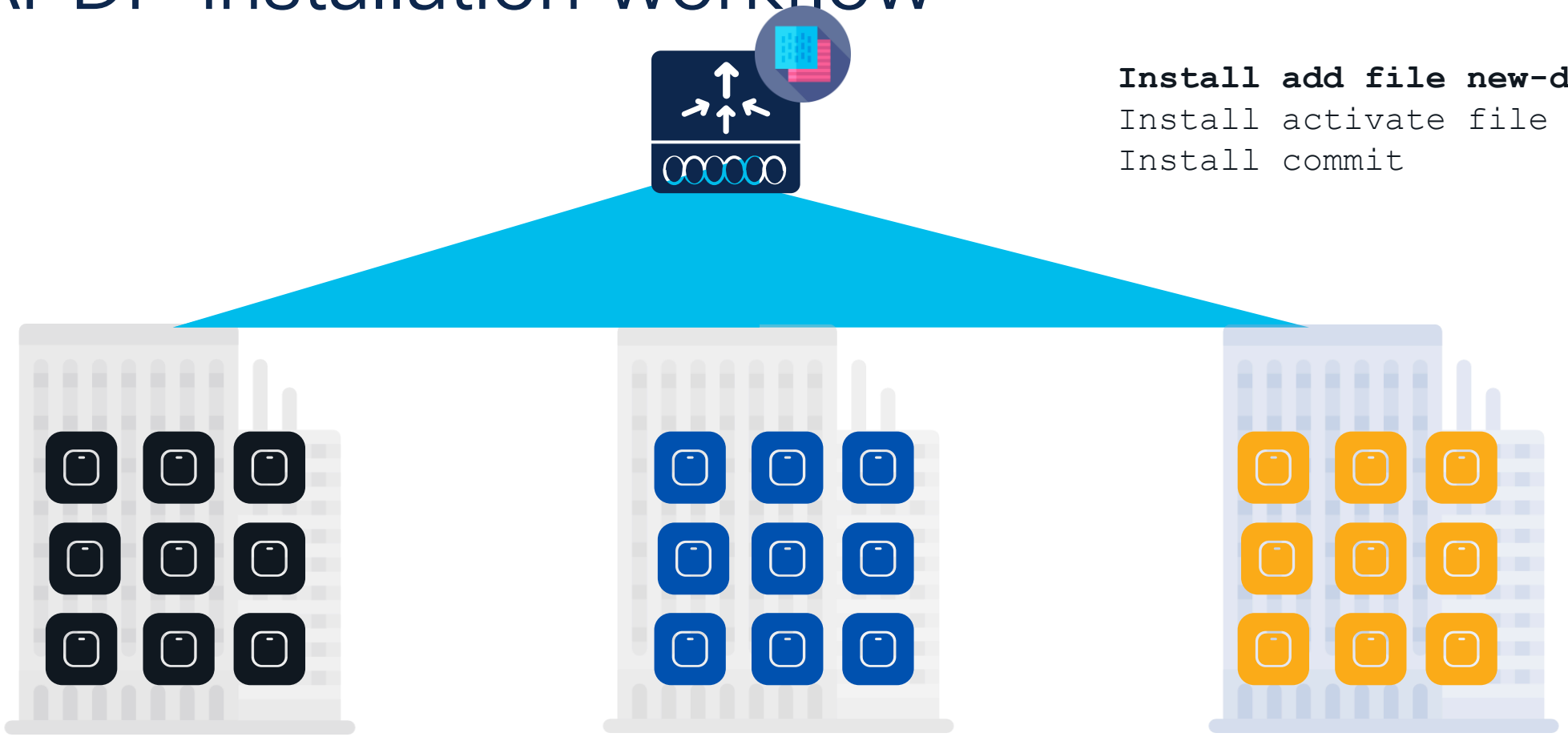
Zero Network Downtime

Applied as HOT patch on the controller with no service impact for APs and Clients

APDP installation workflow



APDP installation workflow

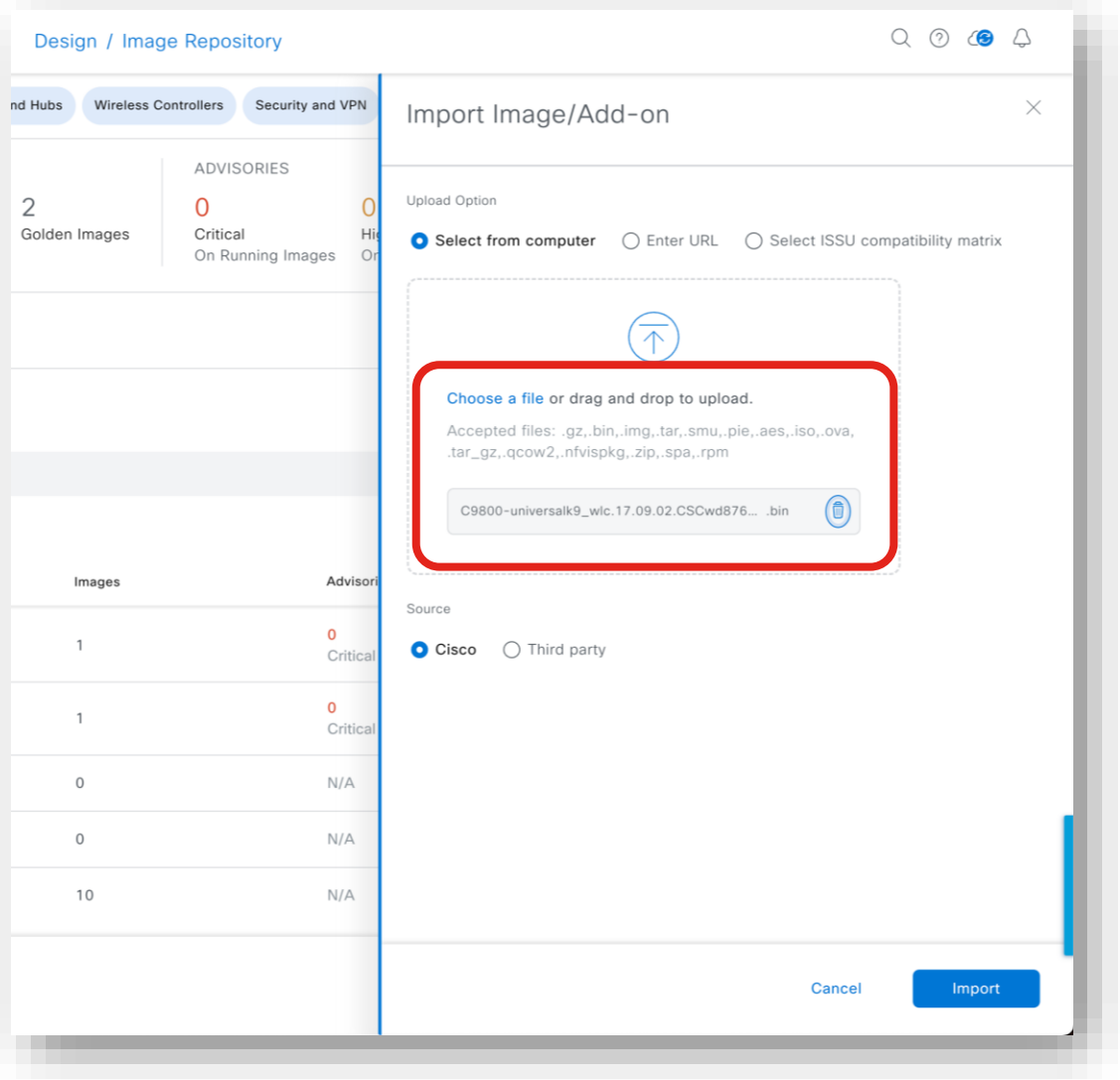



```
Install add file new-dp.bin
Install activate file new-dp.bin
Install commit
```

Note: Fixes for the AP installed via APDP will be via AP Service packs like a baseline supported AP.

Installing SMU, APDP, APSP with Cisco DNA Center

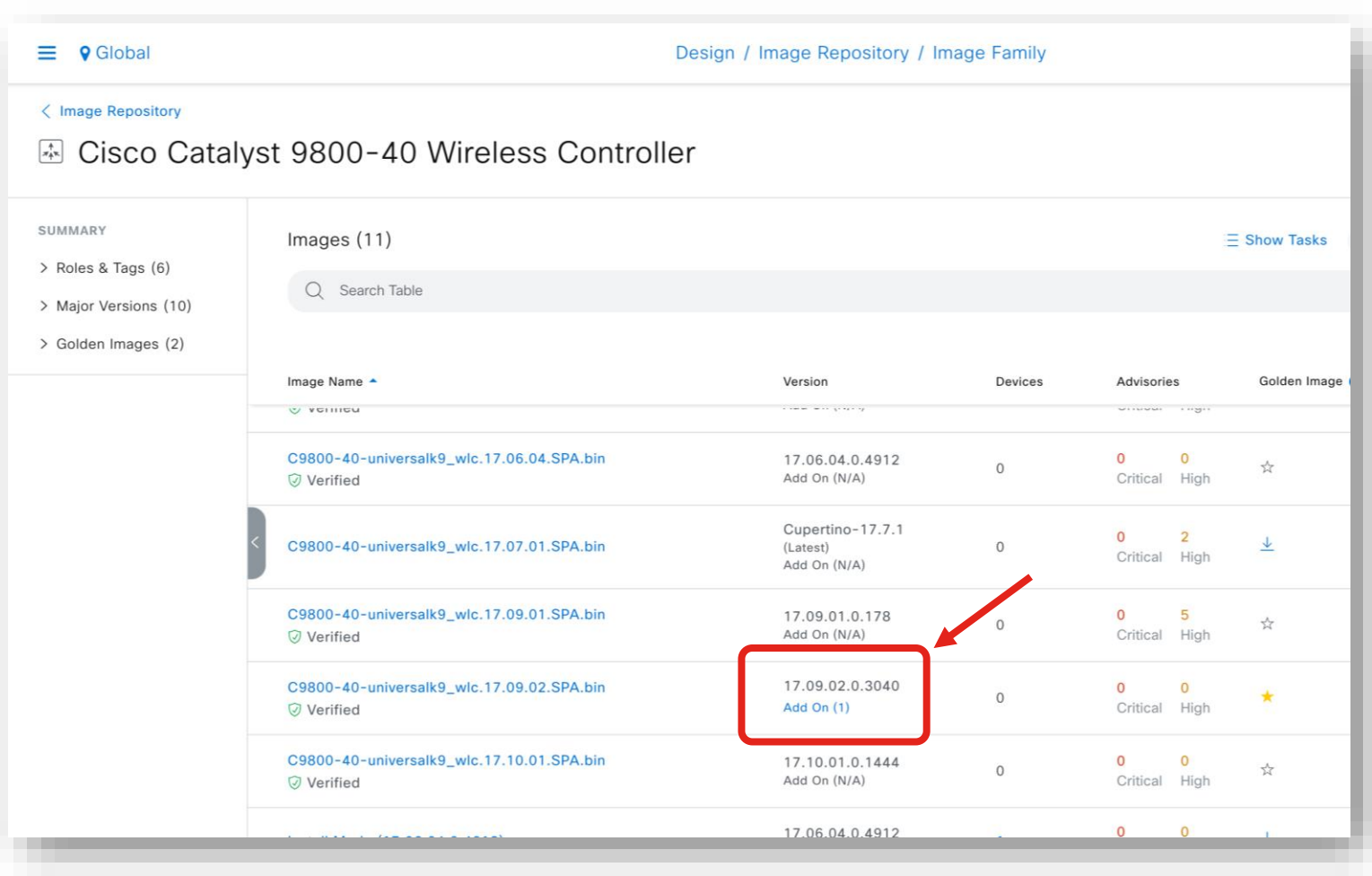
1 Import/Download SMU/APDP/APSP into inventory



Installing SMU, APDP, APSP with Cisco DNA Center

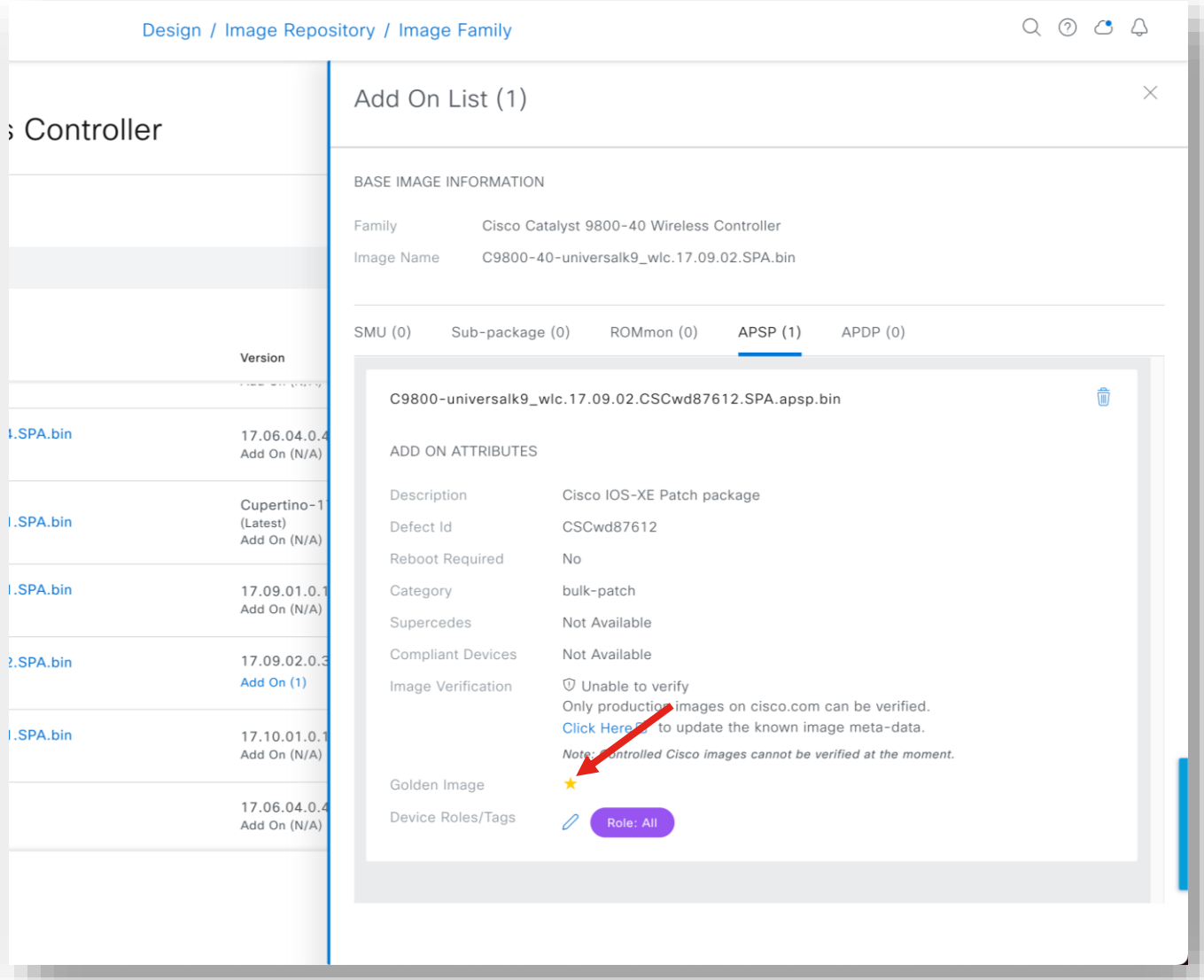
1. Import/Download SMU/APDP/APSP into inventory

2. Click Add On for the required software version



Installing SMU, APDP, APSP with Cisco DNA Center

1. Import/Download SMU/APDP/APSP into inventory
2. Click Add On for the required software version
3. Mark it as Golden, additionally to Golden Image
4. Go through the image upgrade procedure



Achieving the zero downtime win!




Unplanned Events

- ✓ Stateful switchover with an active standby
- ✓ N+1 redundancy for always-on network, services, and clients
- ✓ LAG on WLC and APs

Infrastructure Updates

- ✓ Patching capability with SMU and APSP for wireless controllers and APs
- ✓ APDP and flexible per-site updates contain impact area

Image Upgrades

- ✓ ISSU for Seamless Upgrades
- ✓ N+1 rolling AP upgrades help ensure seamless client connectivity

References

- Cisco Catalyst 9800 Wireless Controller High Availability SSO Deployment Guide: https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-5/deployment-guide/c9800-ha-sso-deployment-guide-rel-17-5.pdf

- Cisco Catalyst 9800 Wireless Controller N+1 High Availability Deployment Guide: https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-4/deployment-guide/c9800-n-plus-1-high-availability-wp.pdf

- High Availability Using Patching and Rolling AP Upgrade on Cisco Catalyst 9800 Series Wireless Controllers: https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-8/Cisco_Catalyst_9800_Series_Wireless_Controllers_Patching.pdf

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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

Thank you

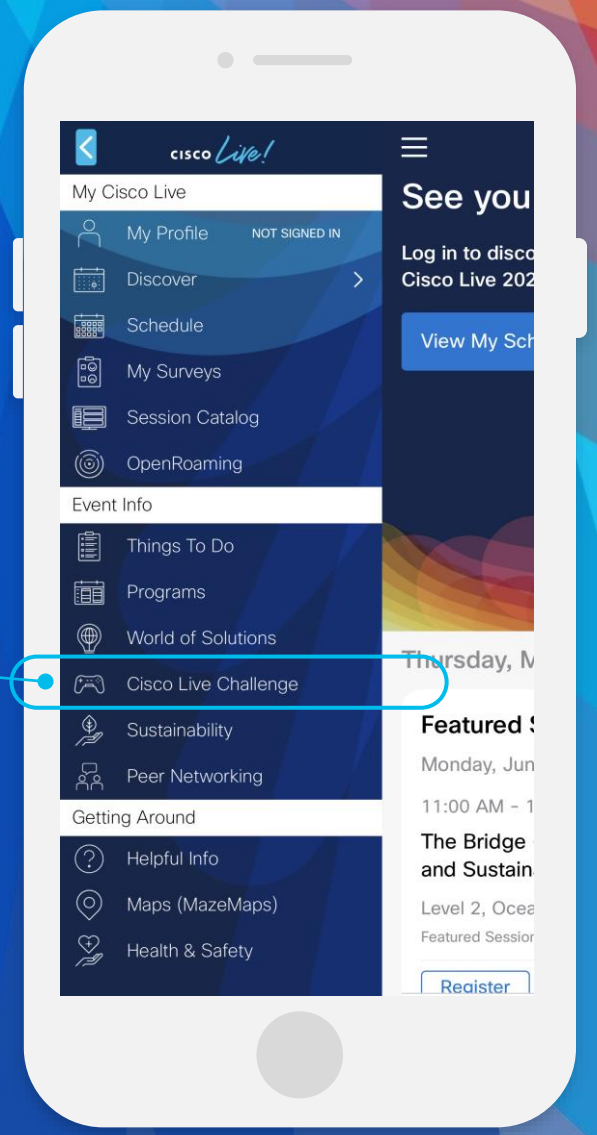
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

Let's go