cisco Live!

Let's go

The bridge to possible

High Availability Design with Cisco Catalyst 9800 Wireless Controller

Robert Moretti
Technical Solutions Specialist
BRKEWN-2846

cisco Live!

"Reconciliation"- Dustin Koa Art

Cisco Webex App

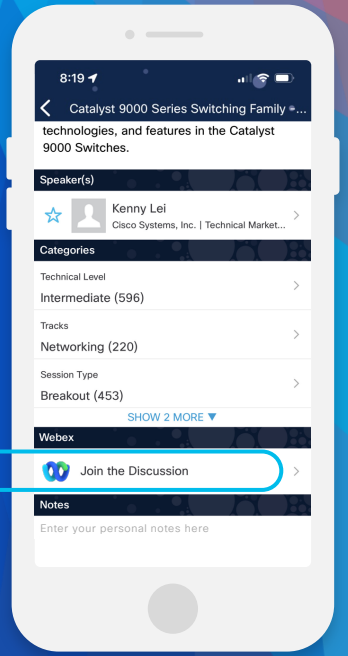
Questions?

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

How

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

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

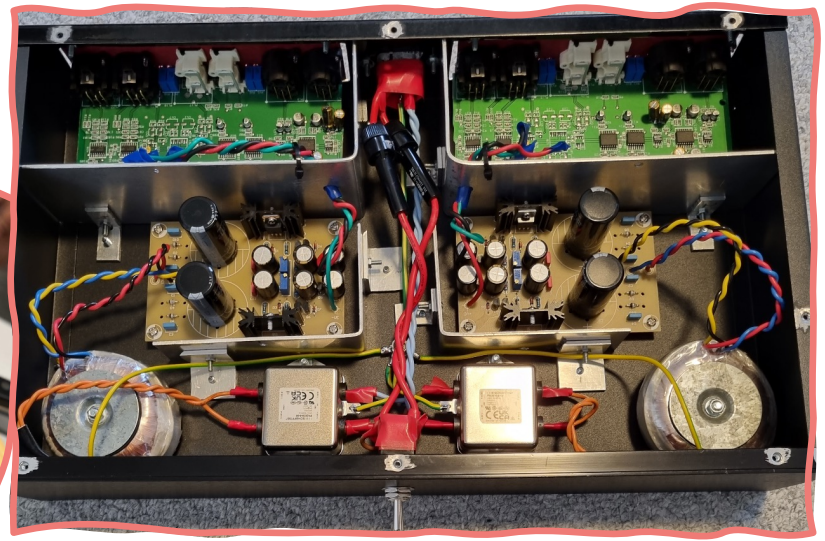


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2846

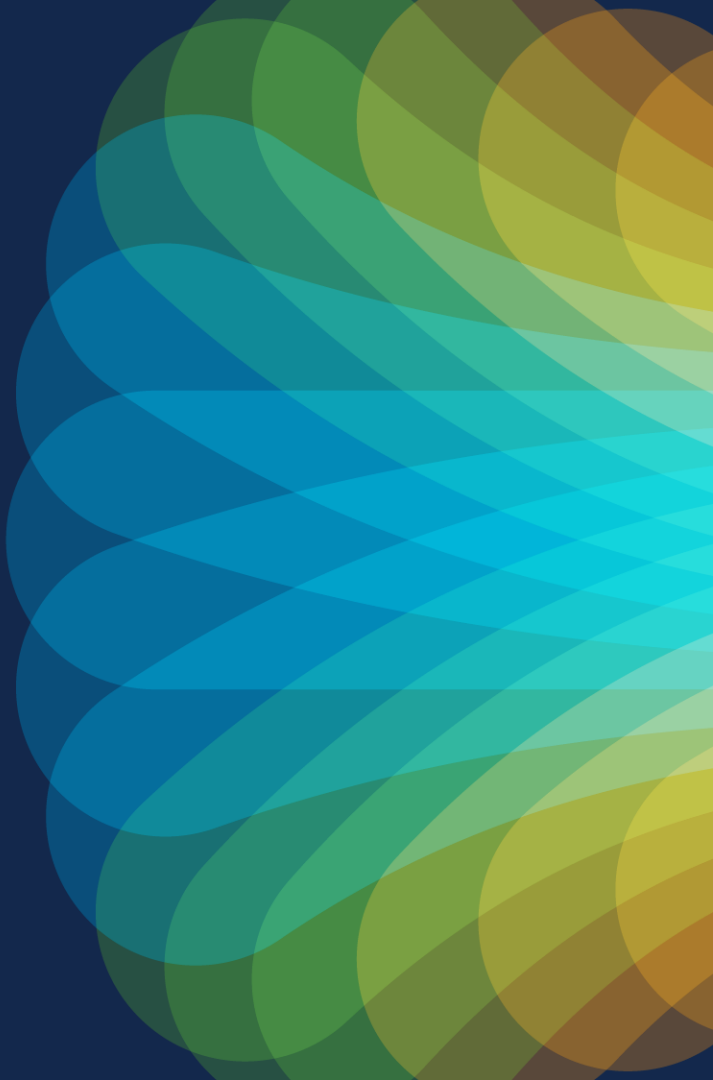
Agenda

1. Importance of wireless High Availability
2. N+1 Wireless Controller Redundancy
3. SSO Wireless Controller Redundancy
4. Upstream Switch & Link Level Redundancy
5. Software Upgrades; ISSU & N+1 Hitless
6. Software Patching Capabilities

..But First Let me Introduce Myself



Importance of wireless High Availability



The New Normal: Zero Downtime




Unplanned events

- Power outage
- Network or controller failure
- WAN Down

Image Upgrades

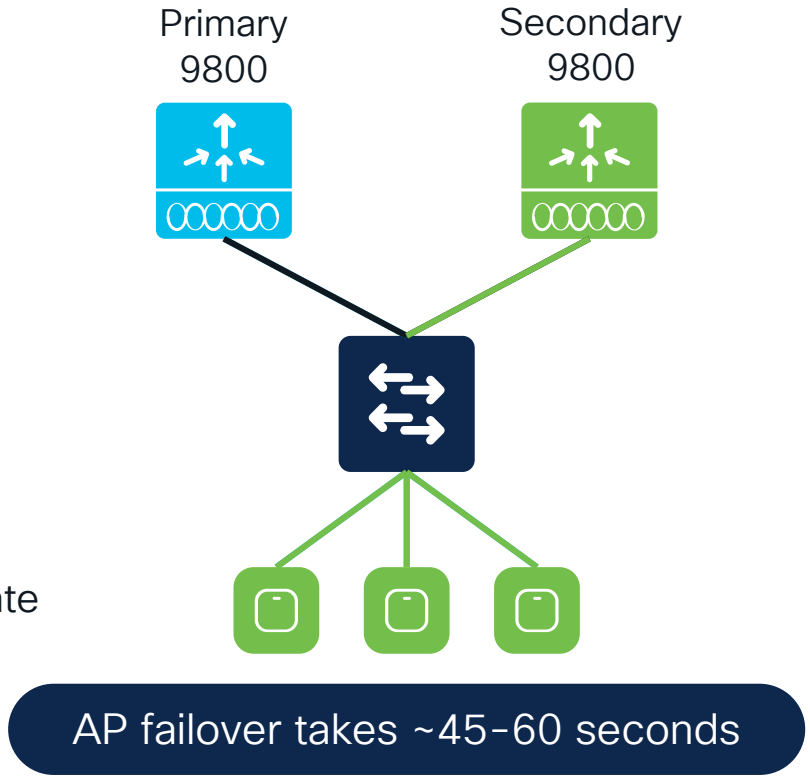
- Image Upgrade
- Network Upgrade

- Software Updates
- Hot/Cold Patching
- PSIRT Fix

N+1 Wireless Controller Redundancy

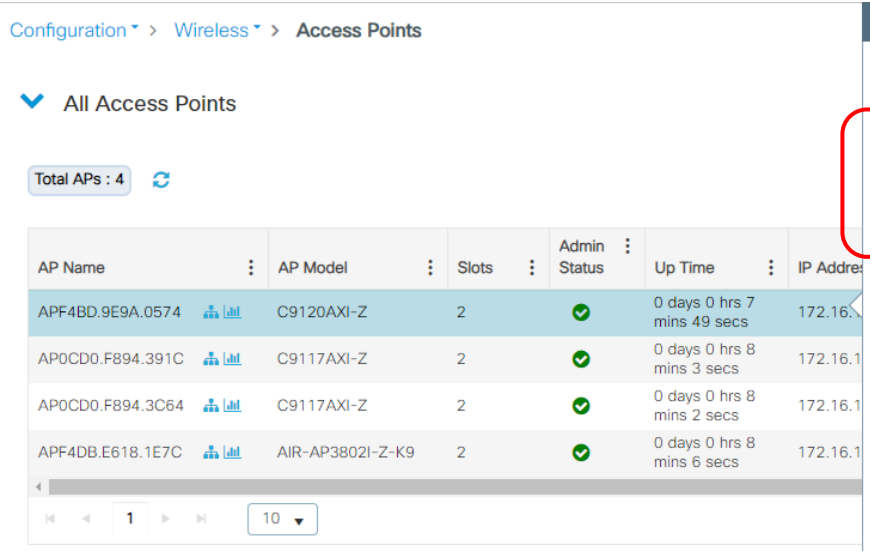
N+1 Redundancy

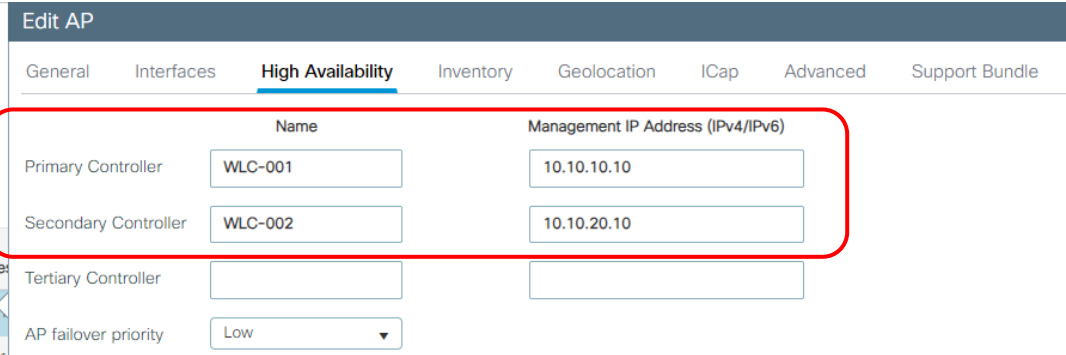
- Single 9800 serves as backup for N number of controllers
- Backup controller can be different model and software version
- Can be configured to automatically fallback to primary
- APs will need to rejoin, and clients re-authenticate
- Secondary WLC can be on a different subnet



N+1 Redundancy

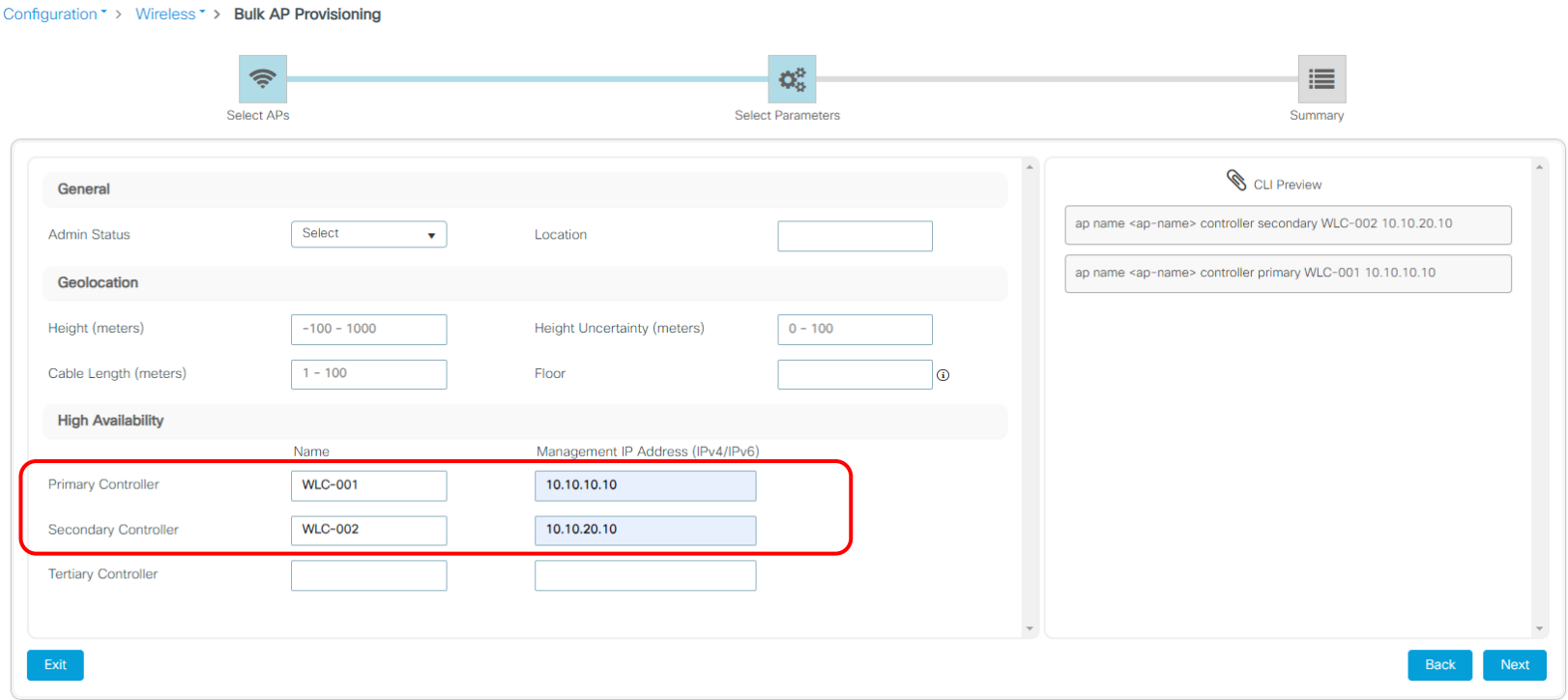
Configuration





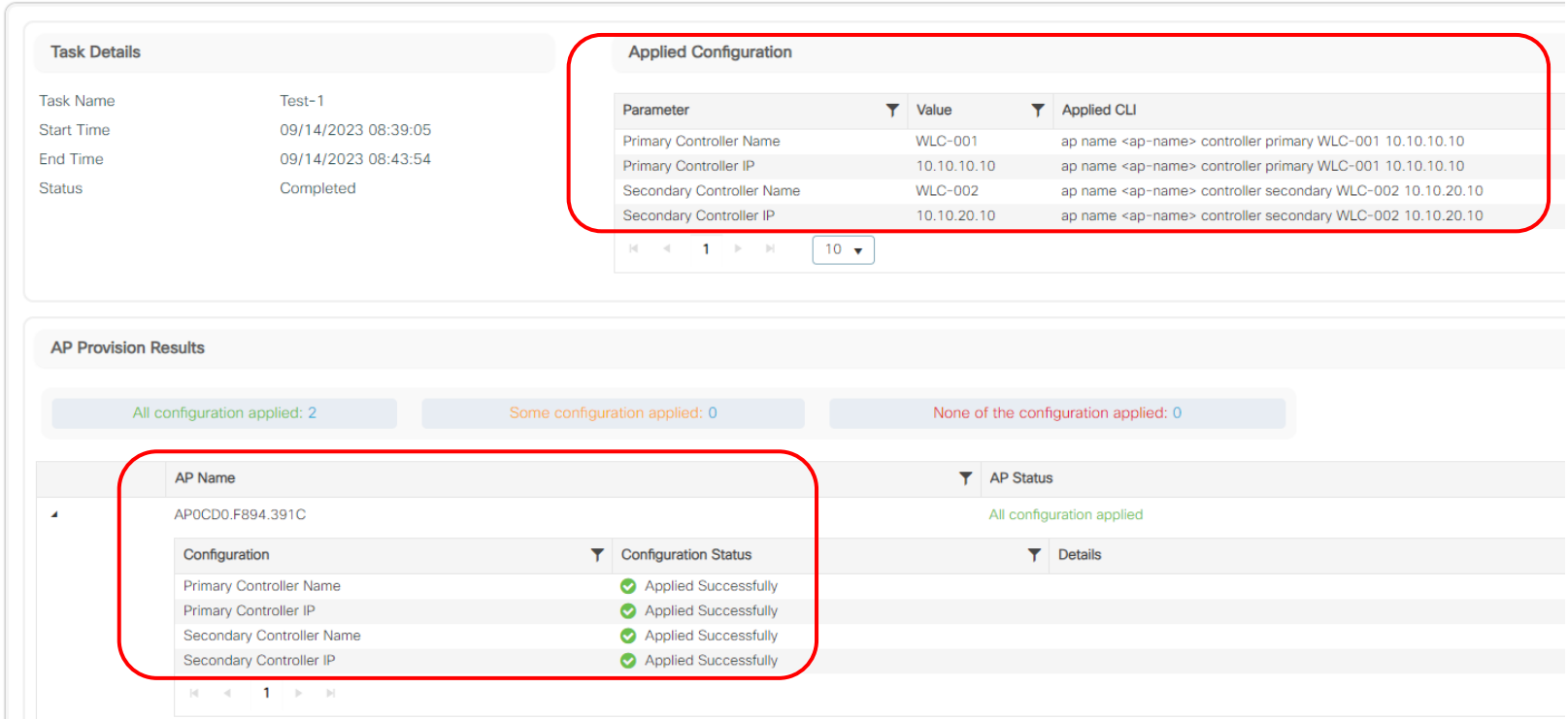
N+1 Redundancy

Bulk AP Provisioning



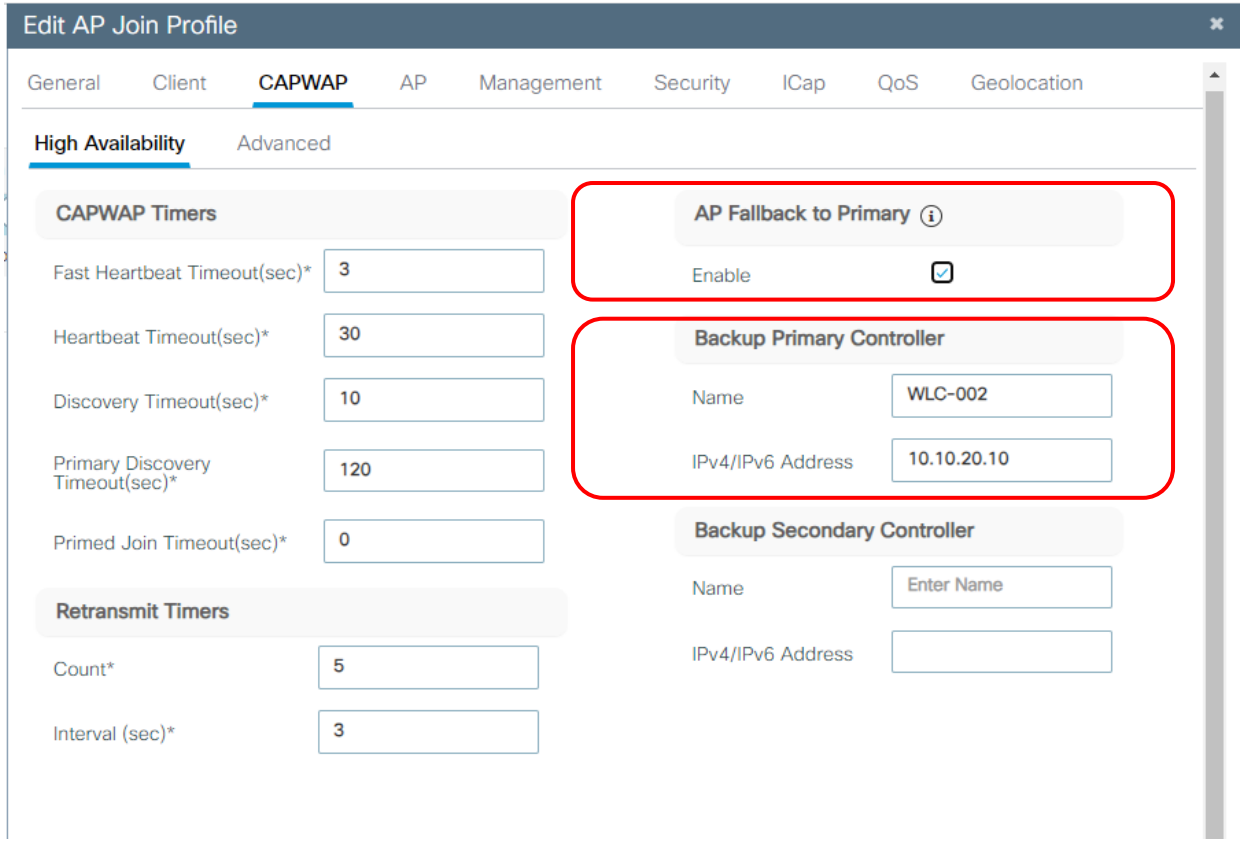
N+1 Redundancy

Bulk AP Provisioning



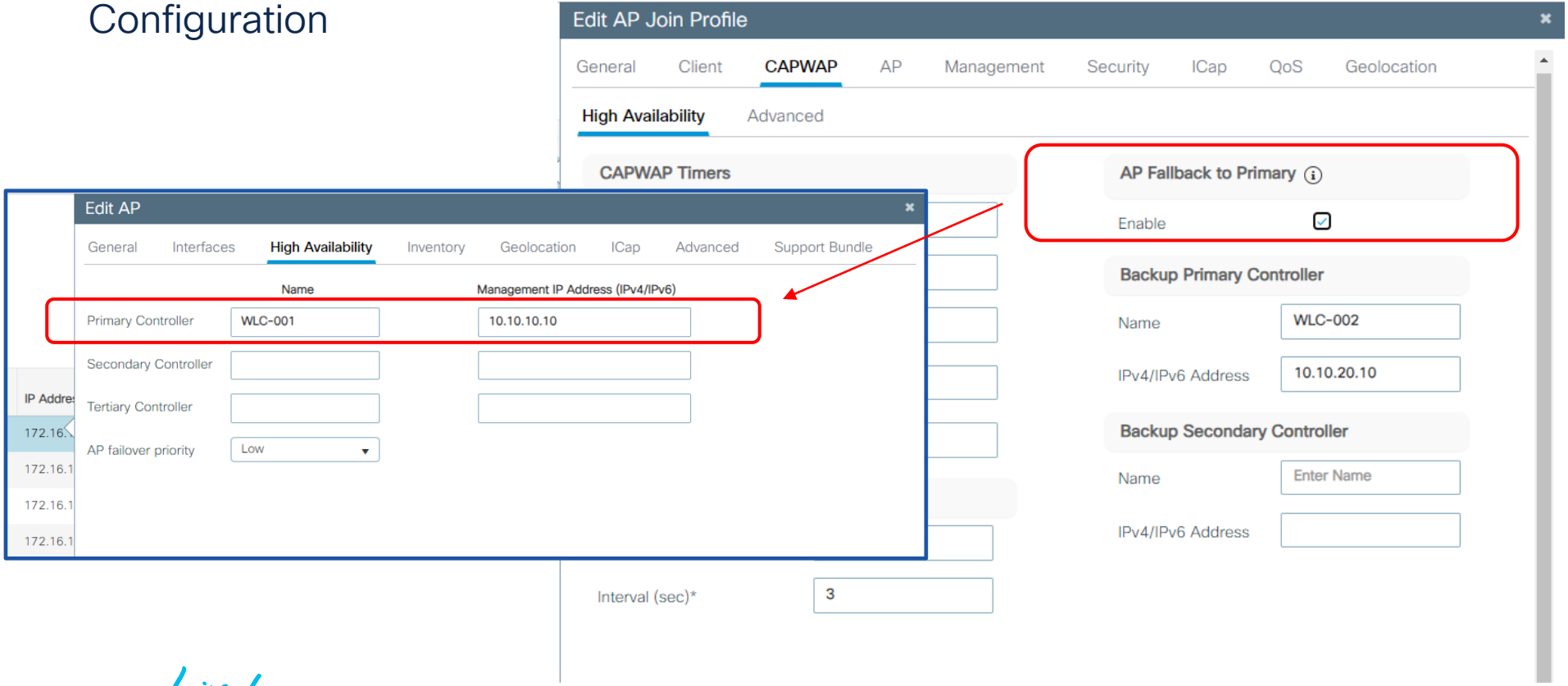
N+1 Redundancy

Configuration



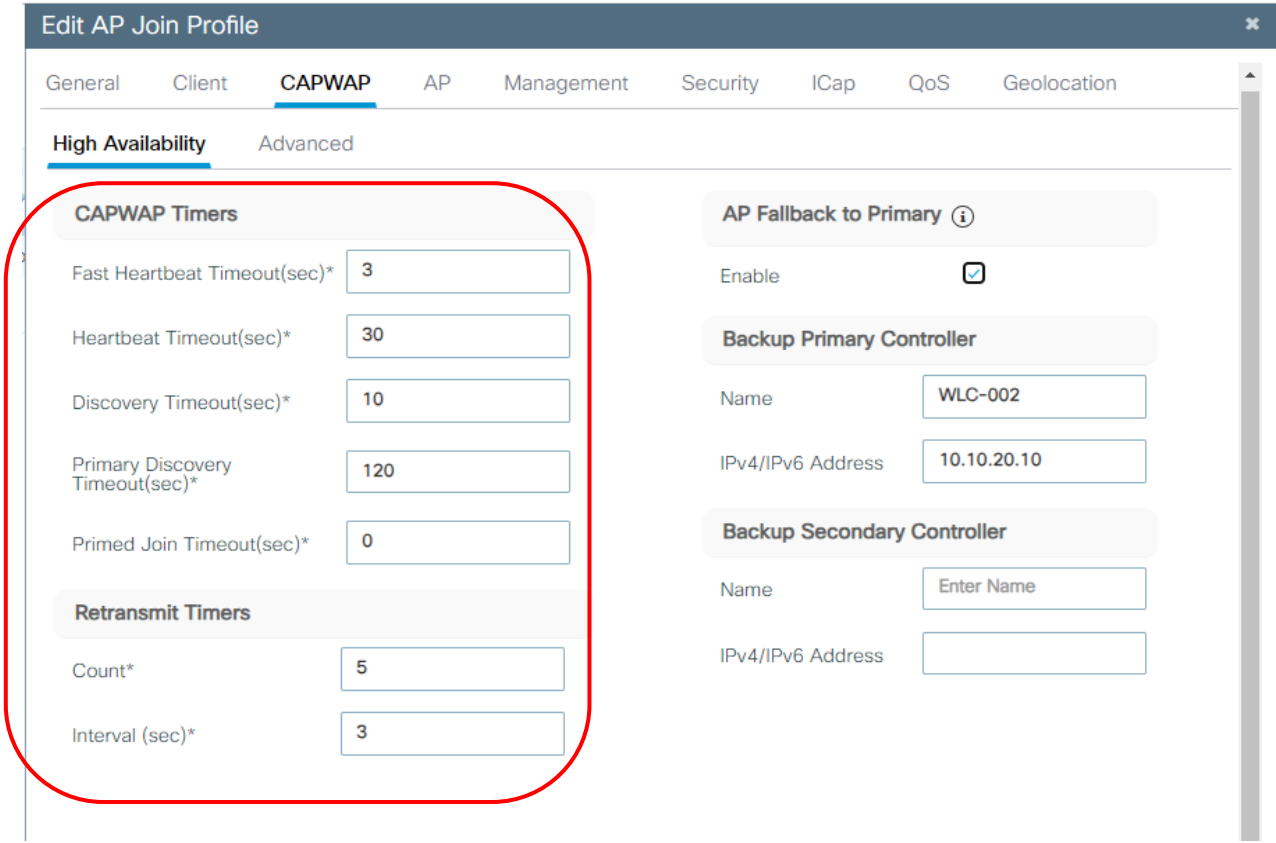
N+1 Redundancy

Configuration



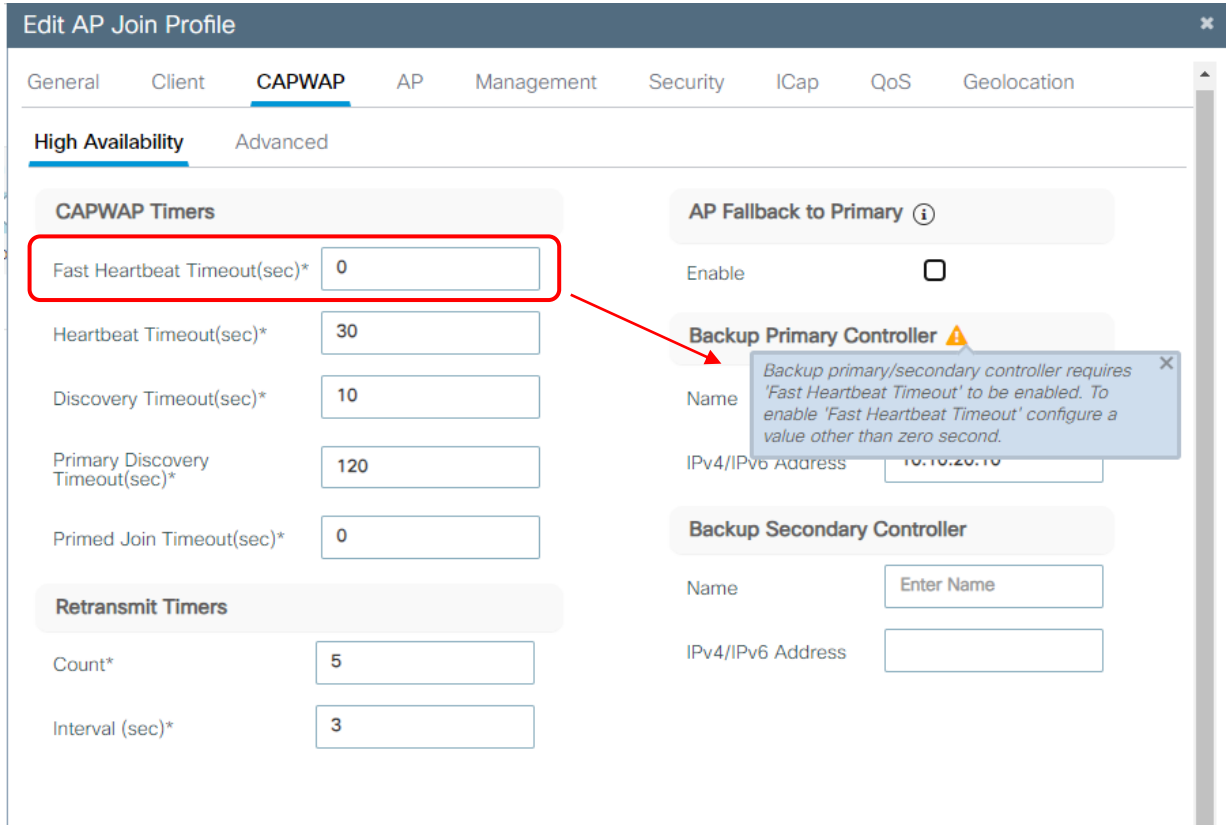
N+1 Redundancy

Configuration

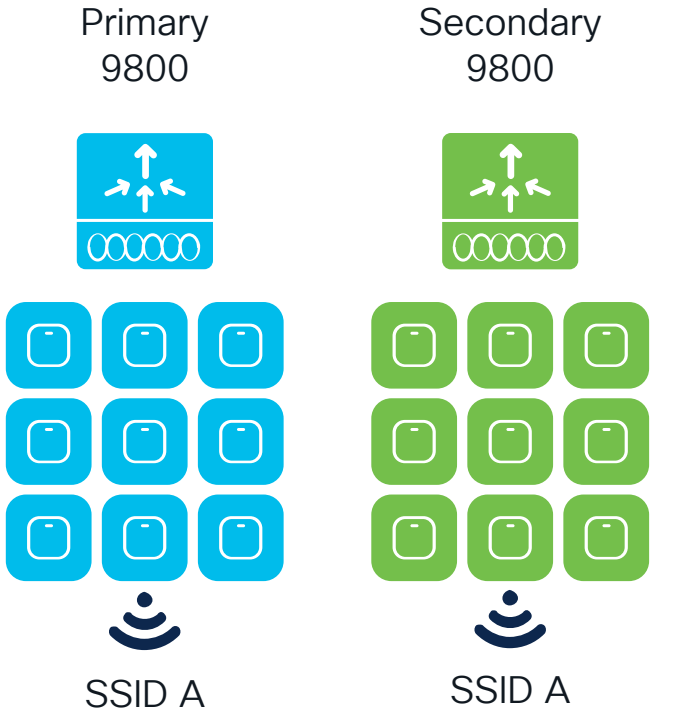


N+1 Redundancy

Configuration



AP to Tag Mappings

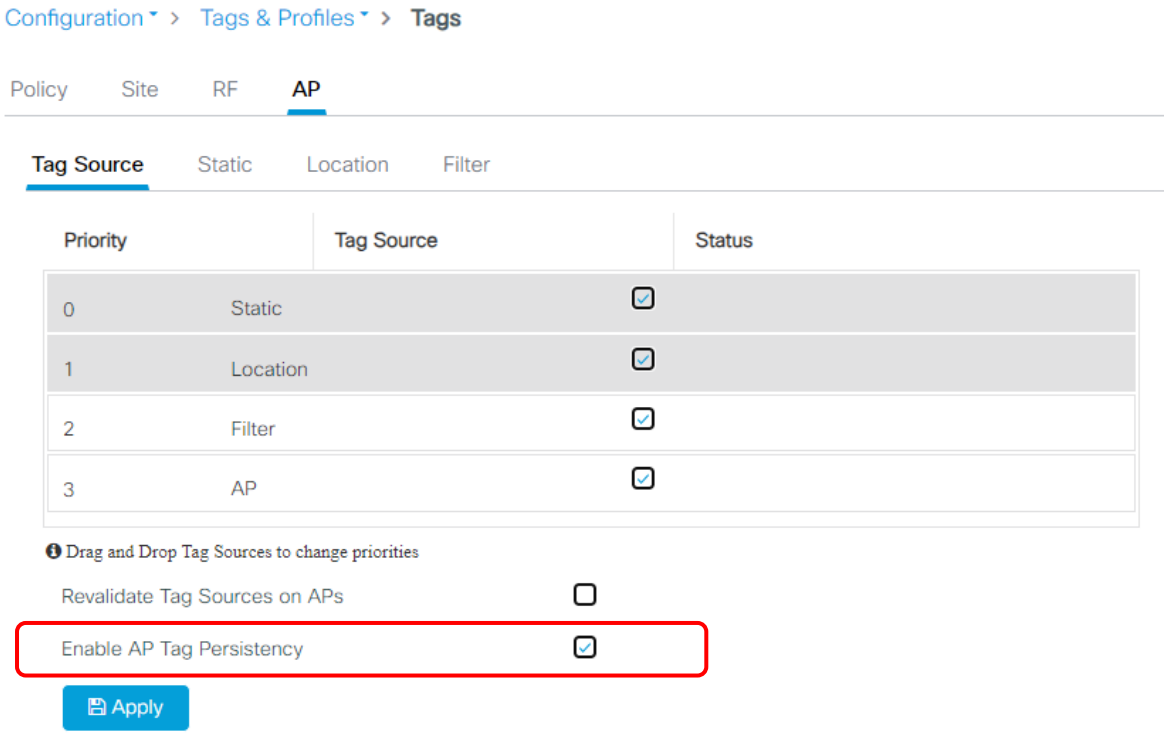


Define tag mappings via static mappings

Save tag mappings on the AP
(& define tags on secondary controller)

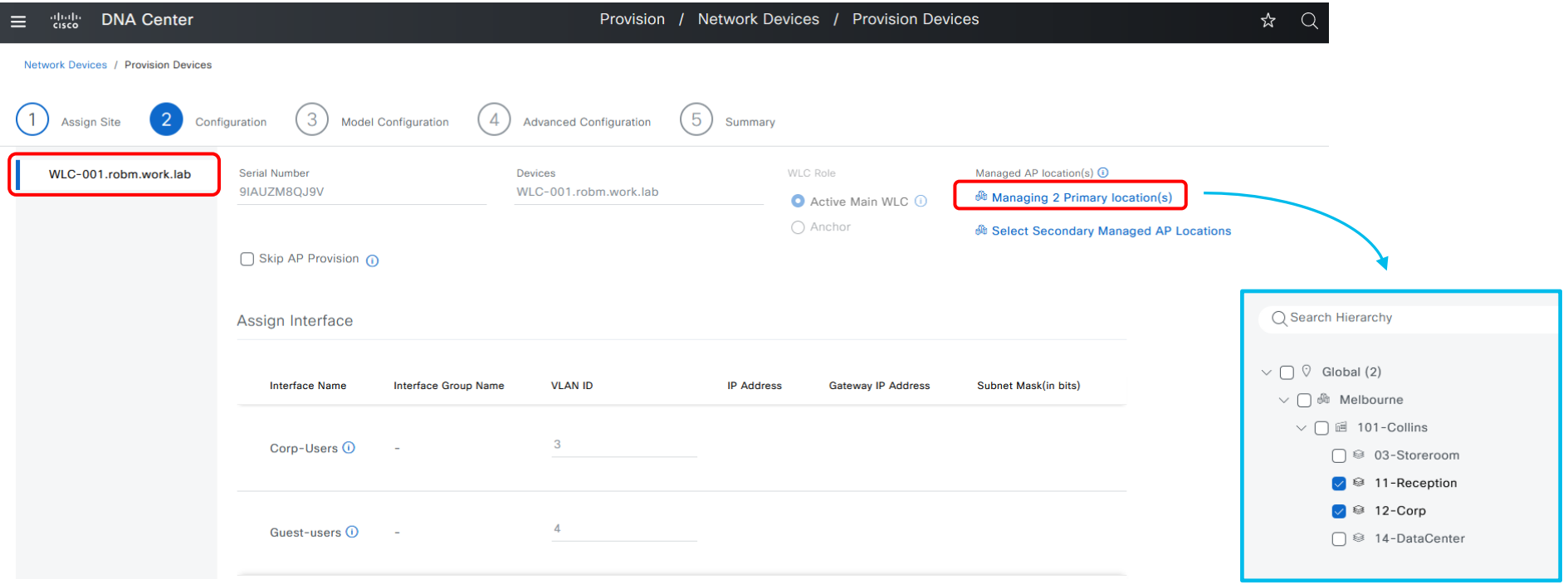
AP to Tag Mappings

Configuration



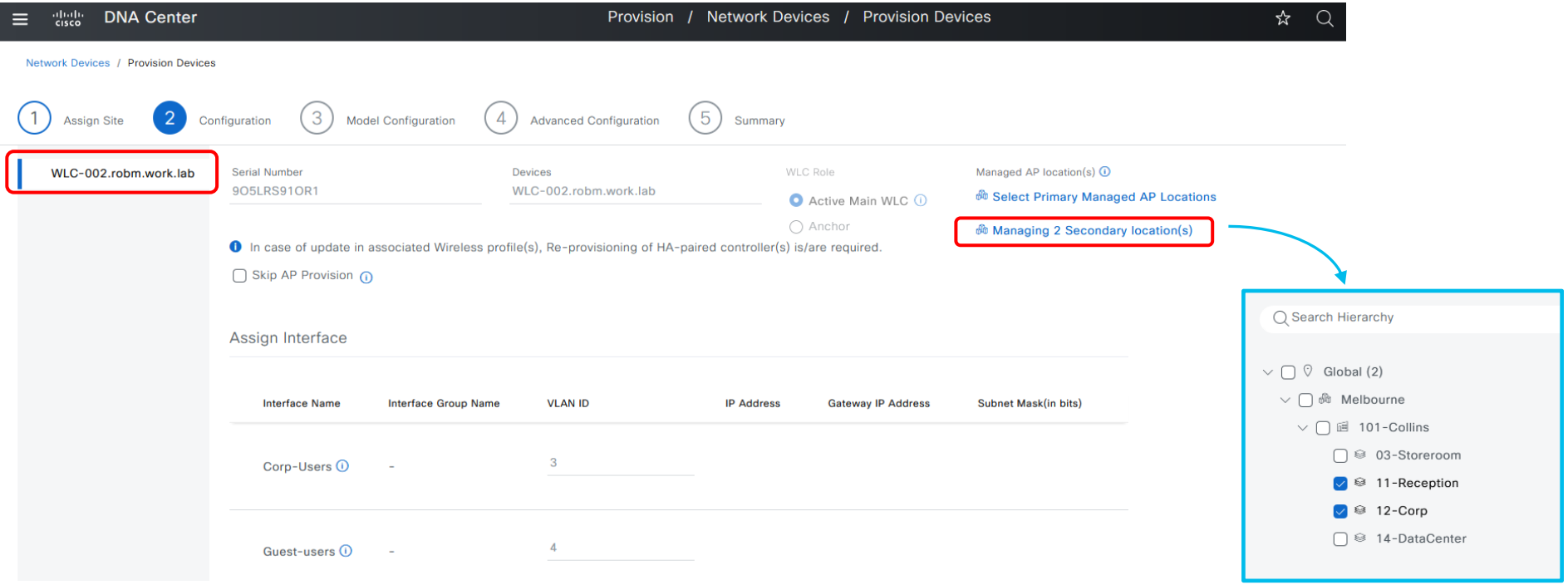
N+1 Redundancy

Using Catalyst Center; Primary WLC



N+1 Redundancy

Using Catalyst Center; Secondary WLC



N+1 Redundancy

Best Practices

Primary and Secondary WLC should run the same software version

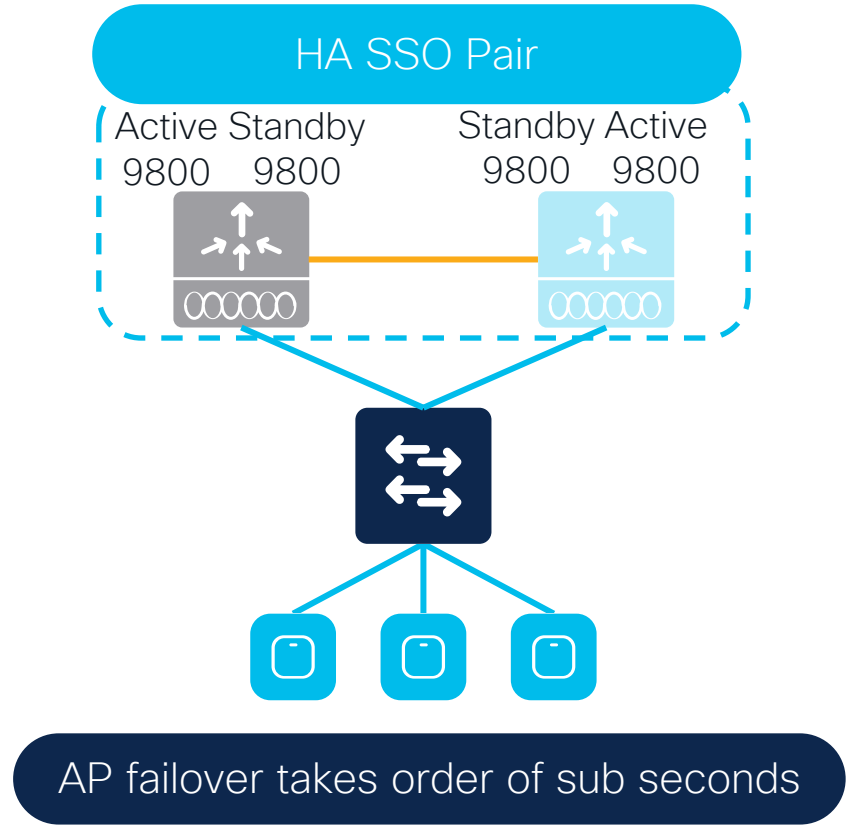
Configurations should be consistent across the Primary, Secondary, and controllers (use Catalyst Center to automate)

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

SSO Wireless Controller Redundancy

Stateful Switchover (SSO)

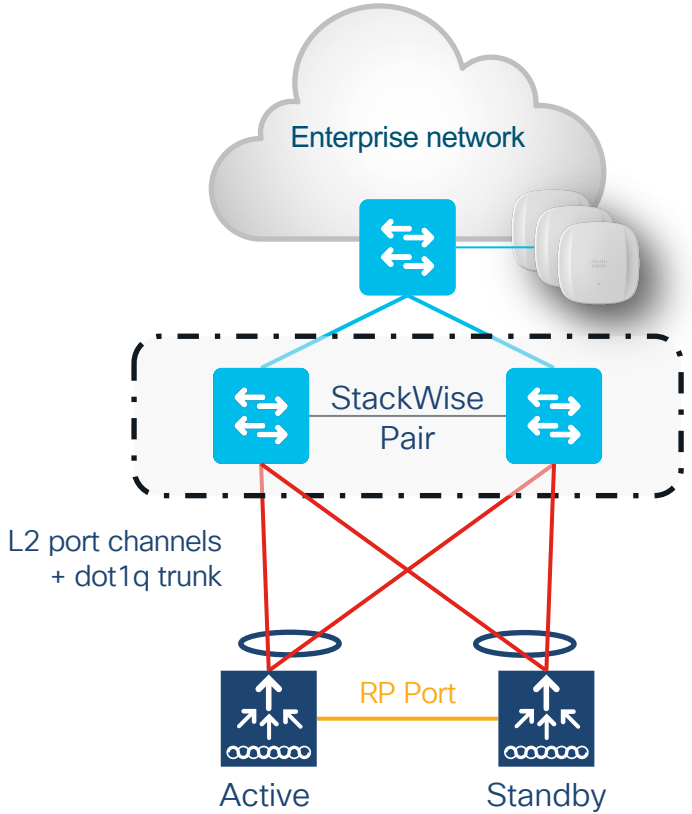
- Pair of 9800 in Active & Hot-Standby appear as a single WLC to the network
- All configuration synced between the pair for seamless, stateful switchover
- Clients and APs do not disconnect



Stateful Switchover (SSO)

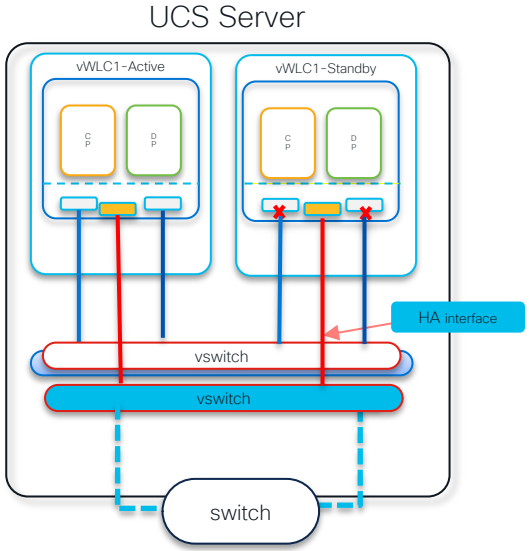
Redundancy Port (RP)

- Syncs configuration and AP/Client databases between Active and Standby
- Monitors status of the chassis
- Layer 2 adjacent

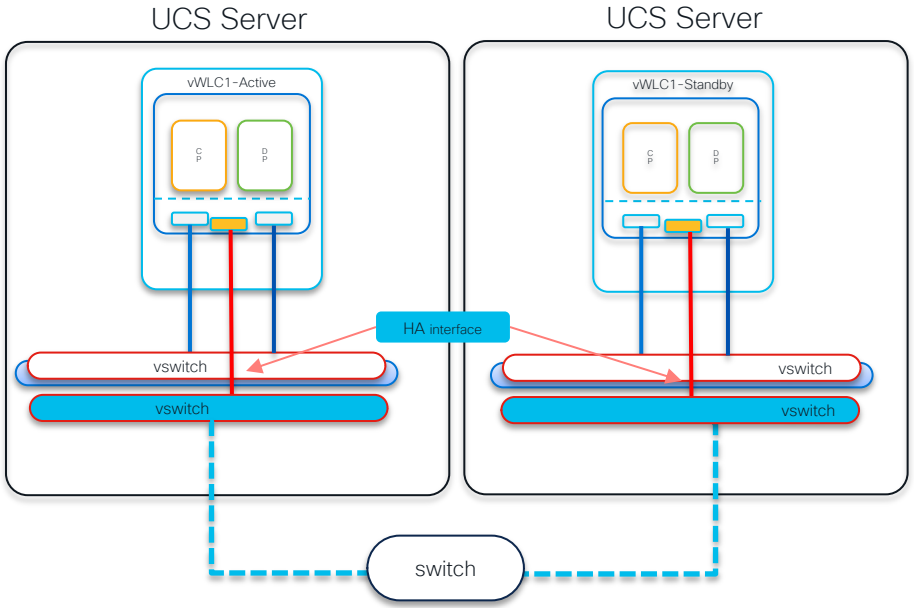


Stateful Switchover (SSO)

Redundancy Port on 9800-CL Virtual (on-prem)



Intra-Host Redundancy



Inter-Host Redundancy

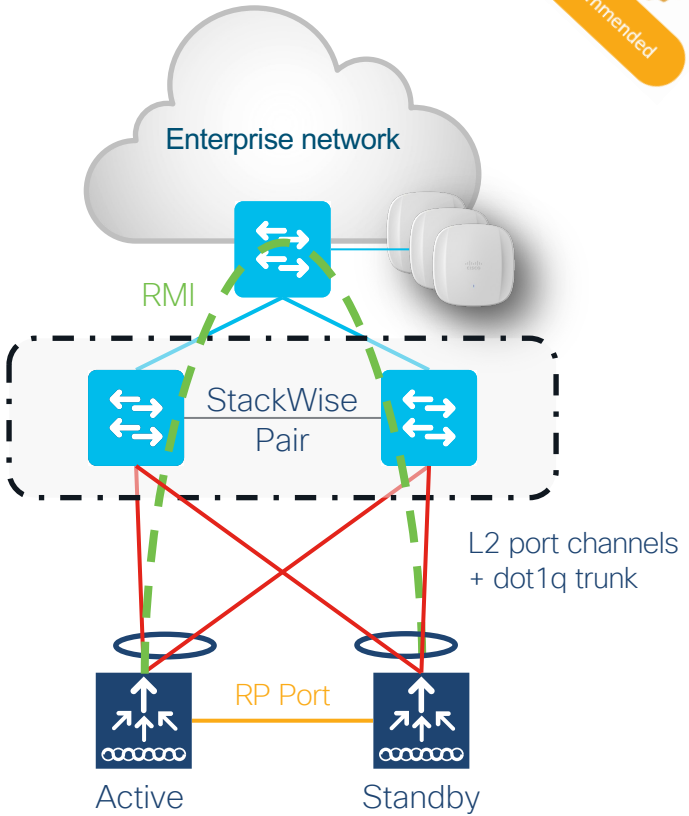
Stateful Switchover (SSO)

Redundancy Management Interface (RMI)

Recommended

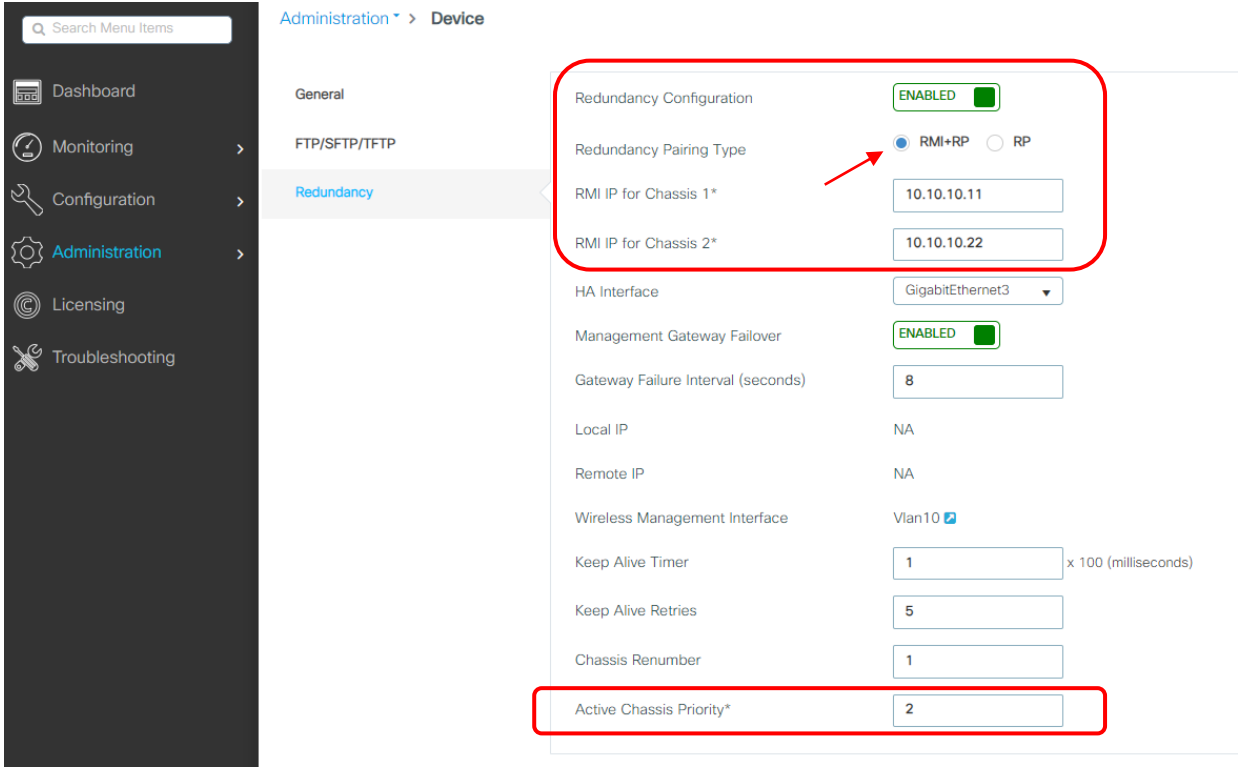
RMI + RP

- RMI is virtual interface used for:
  - Dual Active Detection
  - Monitor status of Active/Standby
- Default Gateway Check with RMI
- RP is recommended to have back-to-back connection
- RMI utilizes same underlay as wireless traffic



Stateful Switchover (SSO)

Configuring SSO



Stateful Switchover (SSO)

Verifying the State of SSO; *"show redundancy states"*

Chassis-1

```
WLC-001-SSO#sh redundancy states
     my state = 13 -ACTIVE
    peer state = 8  -STANDBY HOT
          Mode = Duplex
          Unit = Primary
       Unit ID = 1

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 128
 client_notification_TMR = 30000 milliseconds
          RF debug mask = 0x0
Gateway Monitoring = Enabled
Gateway monitoring interval  = 8 secs

WLC-001-SSO#
```

Chassis-2

```
WLC-001-SSO-stby#sh redundancy states
     my state = 8  -STANDBY HOT
    peer state = 13 -ACTIVE
          Mode = Duplex
          Unit = Primary
       Unit ID = 2

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
    Manual Swact = cannot be initiated from this the standby unit
 Communications = Up

   client count = 128
 client_notification_TMR = 30000 milliseconds
          RF debug mask = 0x0
Gateway Monitoring = Enabled
Gateway monitoring interval  = 8 secs

WLC-001-SSO-stby#
```

Stateful Switchover (SSO)

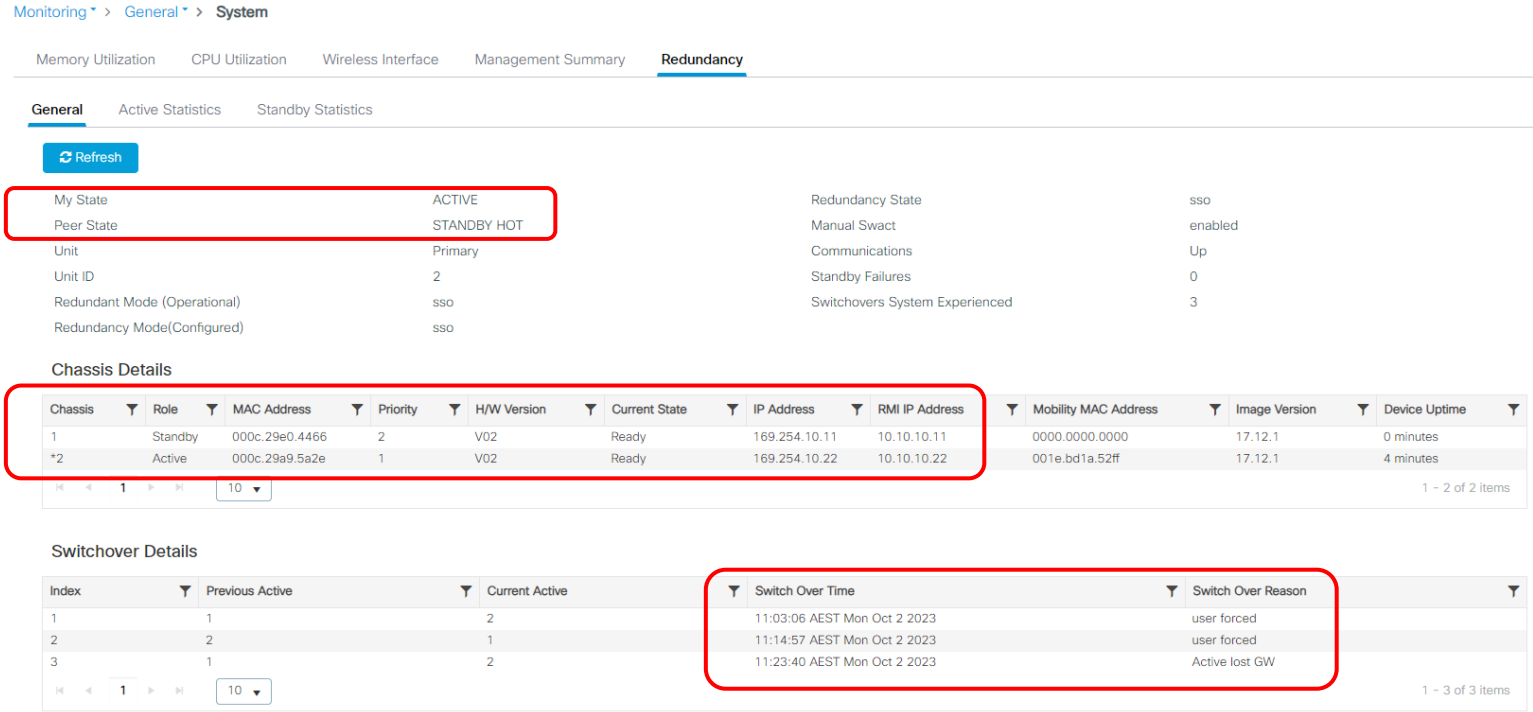
Verifying the State of SSO; *"show redundancy states"*

Chassis-1

```
WLC-001-SSO#sh redundancy states
       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 1

Redundancy Mode (Operational) = Non-redundant
Redundancy Mode (Configured)  = sso
Redundancy State              = Non Redundant
     Maintenance Mode = Disabled
    Manual Swact = disabled (system is simplex (no peer unit))
 Communications = Down      Reason: Simplex mode

   client count = 128
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
Gateway Monitoring = Enabled
Gateway monitoring interval  = 8 secs

WLC-001-SSO#
```

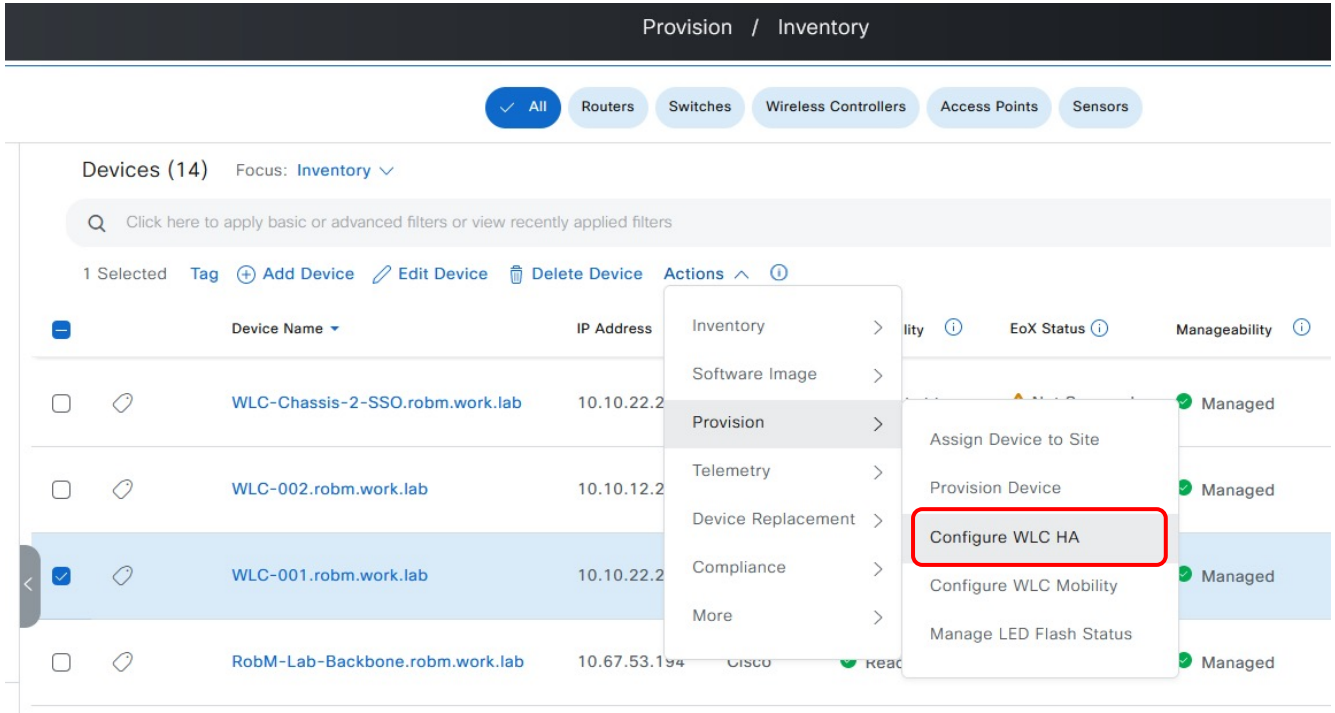
Stateful Switchover (SSO)

Verifying the State of SSO; from the GUI



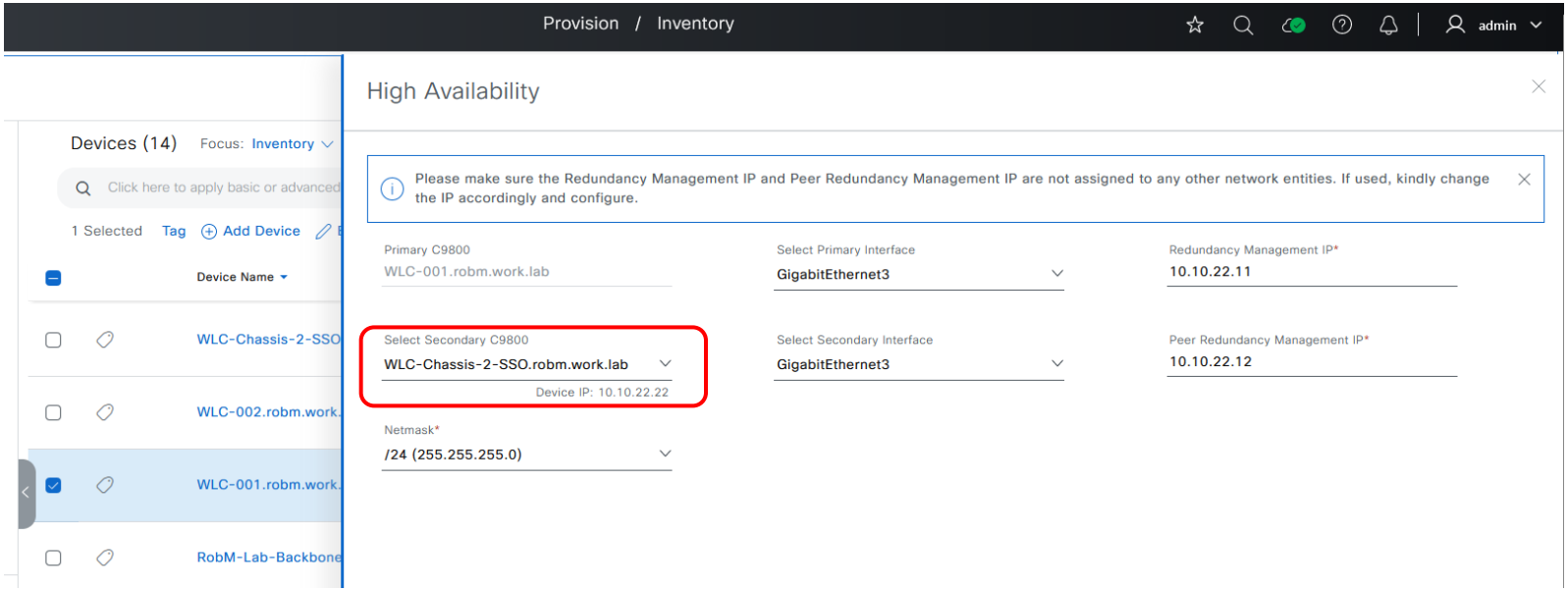
Stateful Switchover (SSO)

Using Catalyst Center



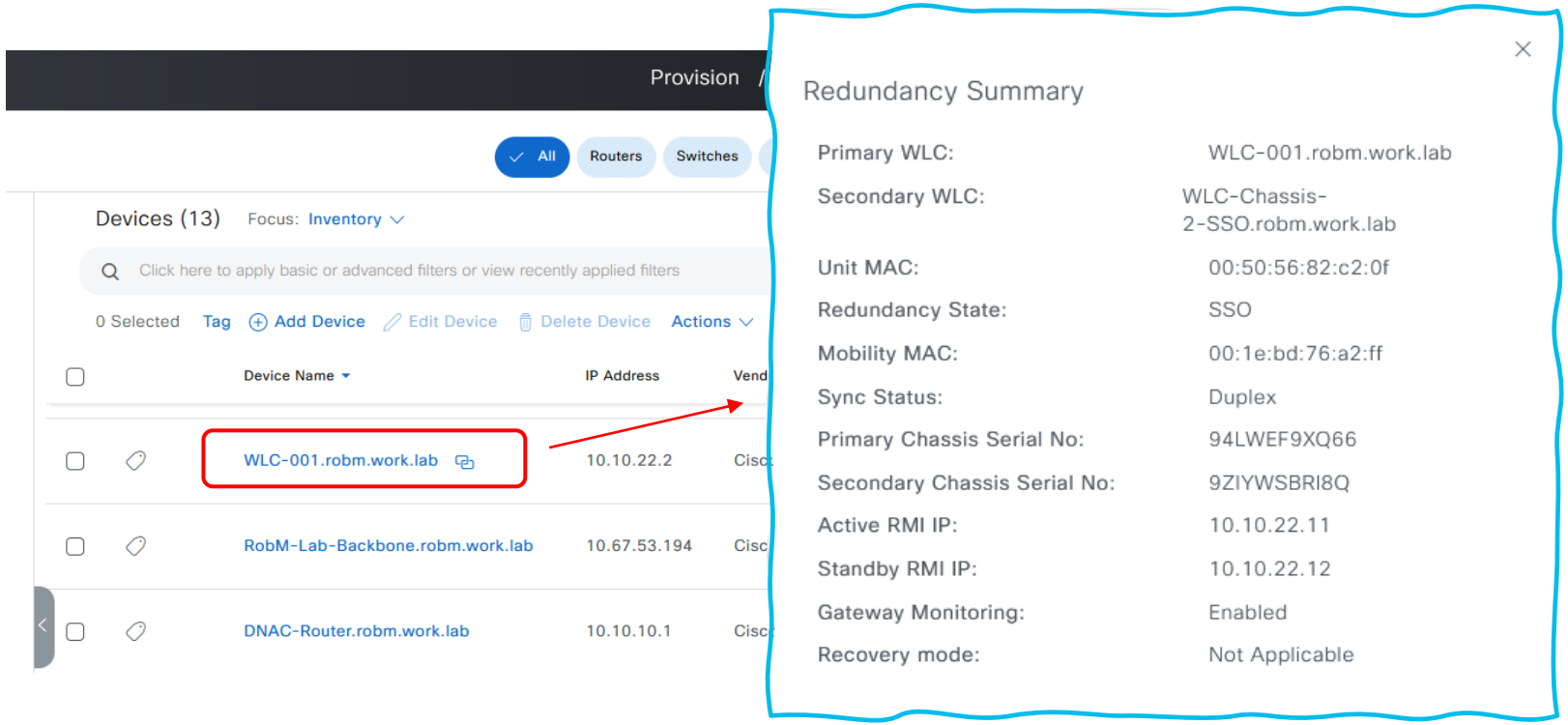
Stateful Switchover (SSO)

Using Catalyst Center



Stateful Switchover (SSO)

Using Catalyst Center



Stateful Switchover (SSO)

Best Practices

Appliance Type

- Physical Appliances: Use exact same hardware model
  Eg, C9800-L-C cannot pair with C9800-L-F
- C9800-CL Private Cloud: Pick same template for both VMs

Software

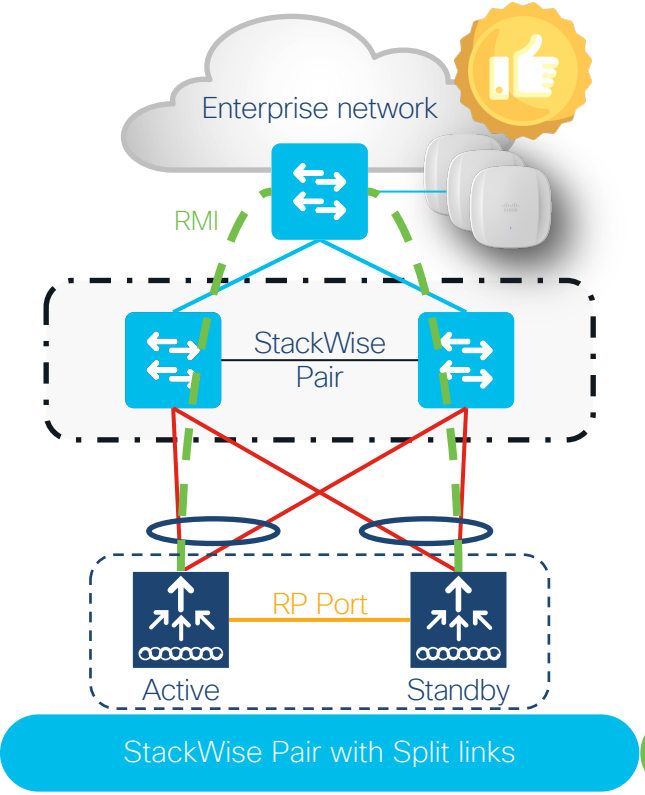
- Both boxes are running the same software and in the same boot mode
- Install mode is recommend

Configurations

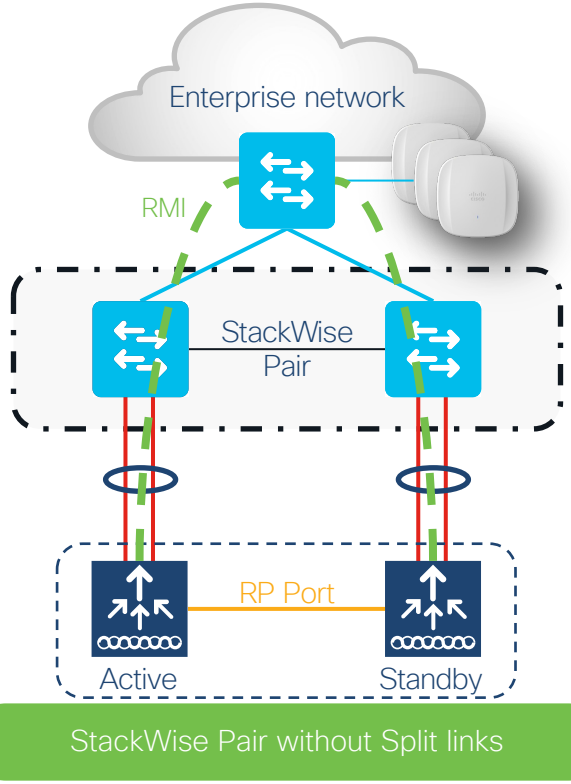
- Set keep-alive retries to 5
- Set the higher priority (2) on the chassis that should be active
- Renumber chassis prior to configuring

Upstream Switch & Link Level Redundancy

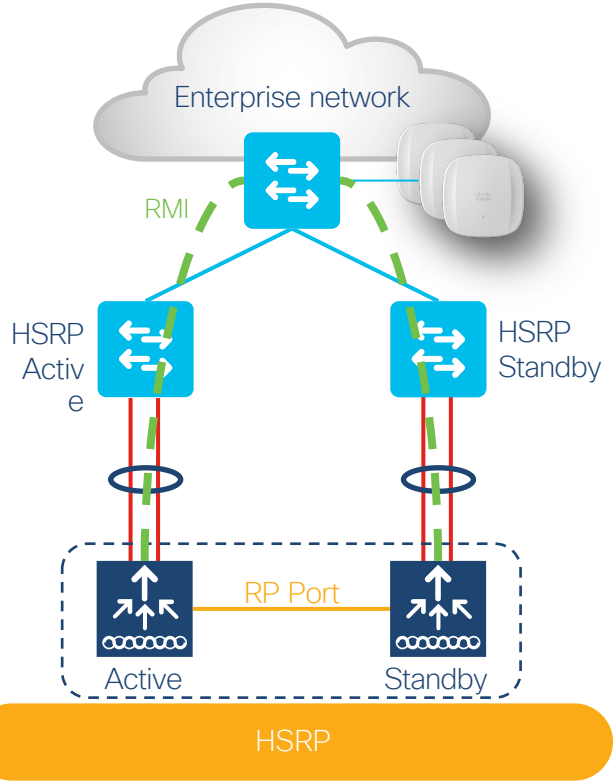
Supported Topologies



StackWise Pair with Split links



StackWise Pair without Split links

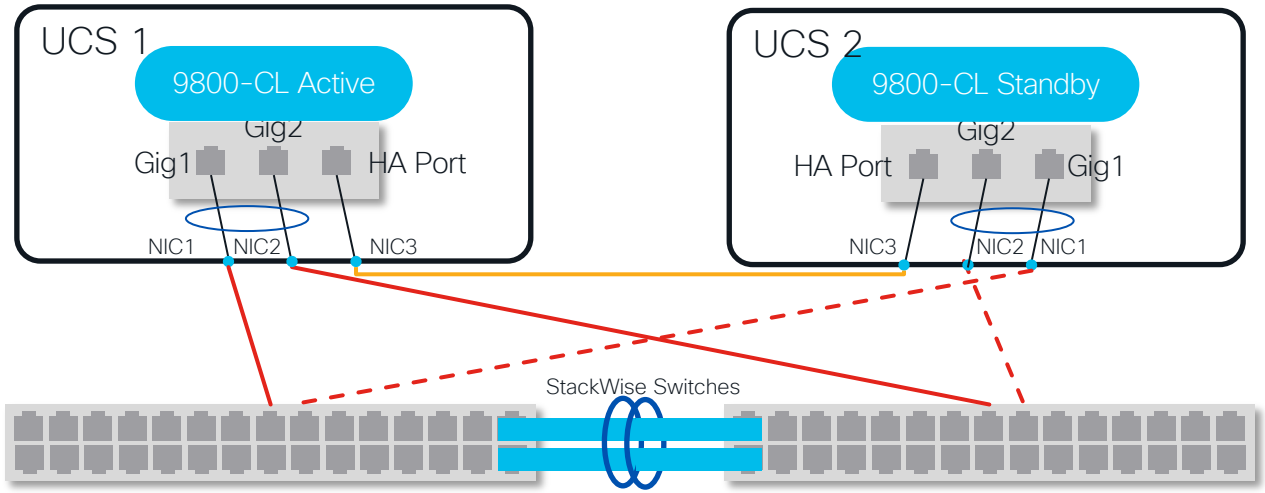


HSRP

9800-CL Port Channel

Link Level Connections

- 9800-CL Private Cloud (17.5.1 and later) – SR-IOV only



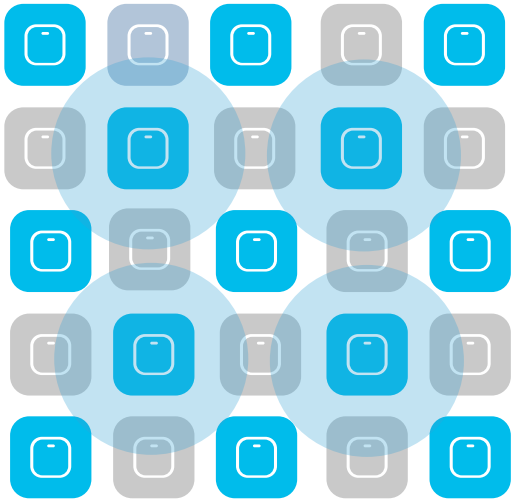
Software Upgrades; ISSU & N+1 Hitless

Rolling AP Upgrades

Rolling AP Upgrad

Neighbor Marking

25%



Rolling AP Upgrades

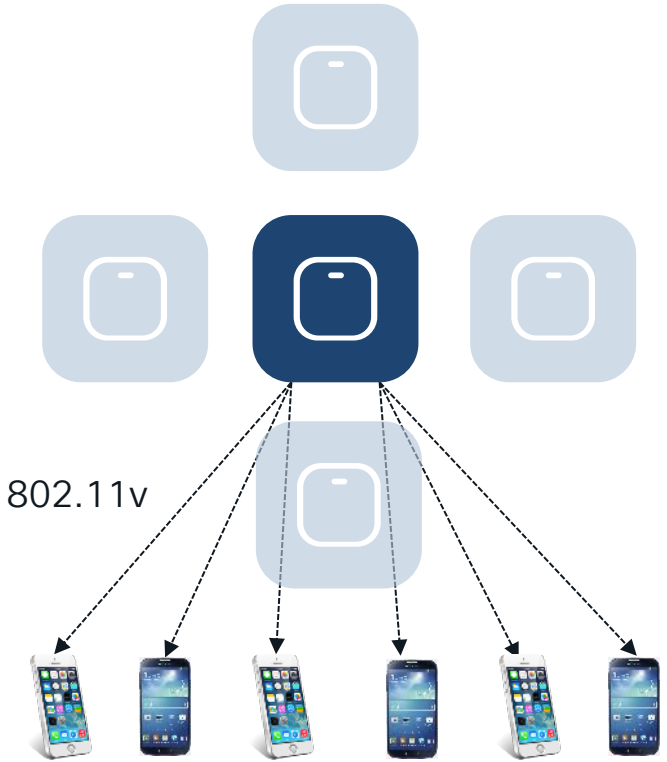
Client Steering

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)



In Service Software Upgrades (ISSU)

In Service Software Upgrades (ISSU)

What is 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

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

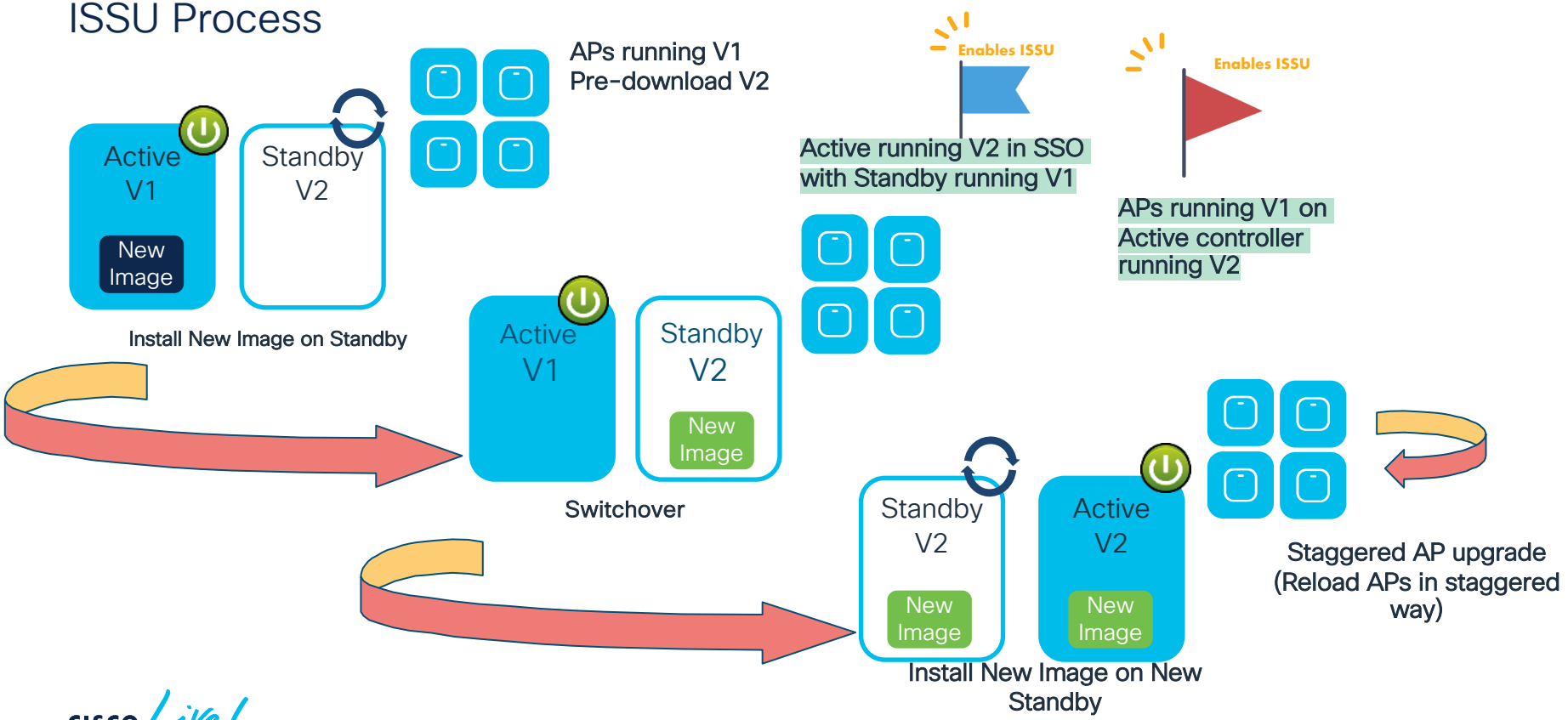
All AP/Client sessions are retained during upgrade process

Pre-requisites:

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

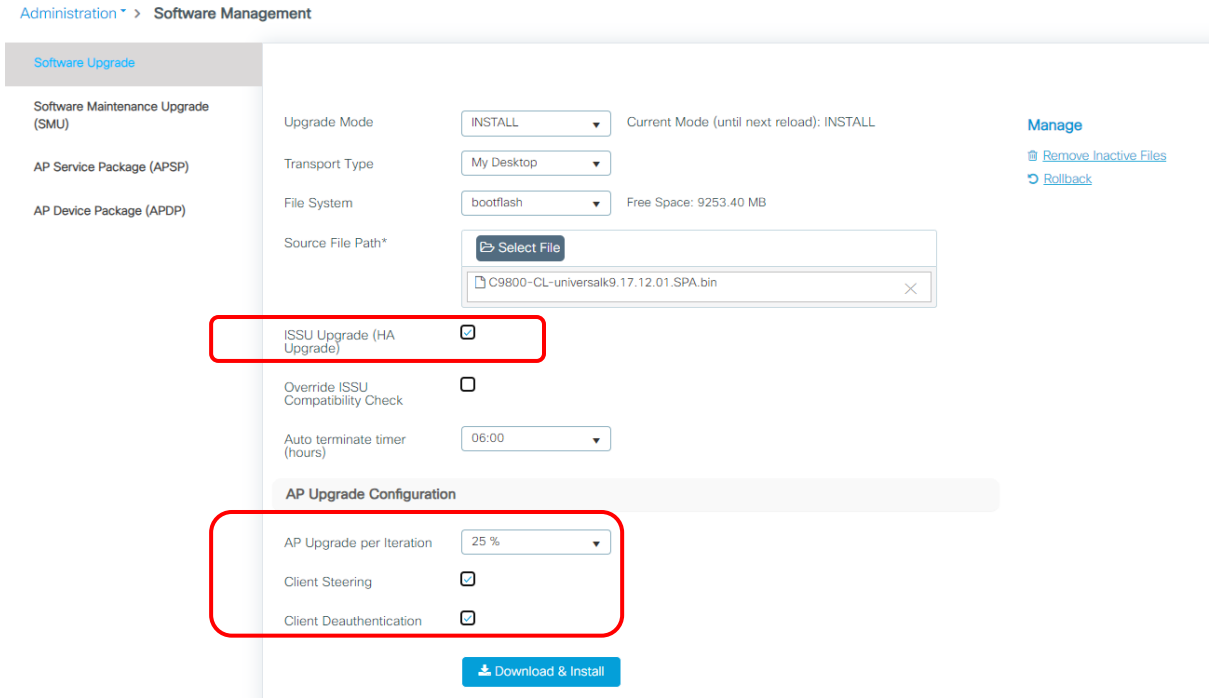
In Service Software Upgrades (ISSU)

ISSU Process



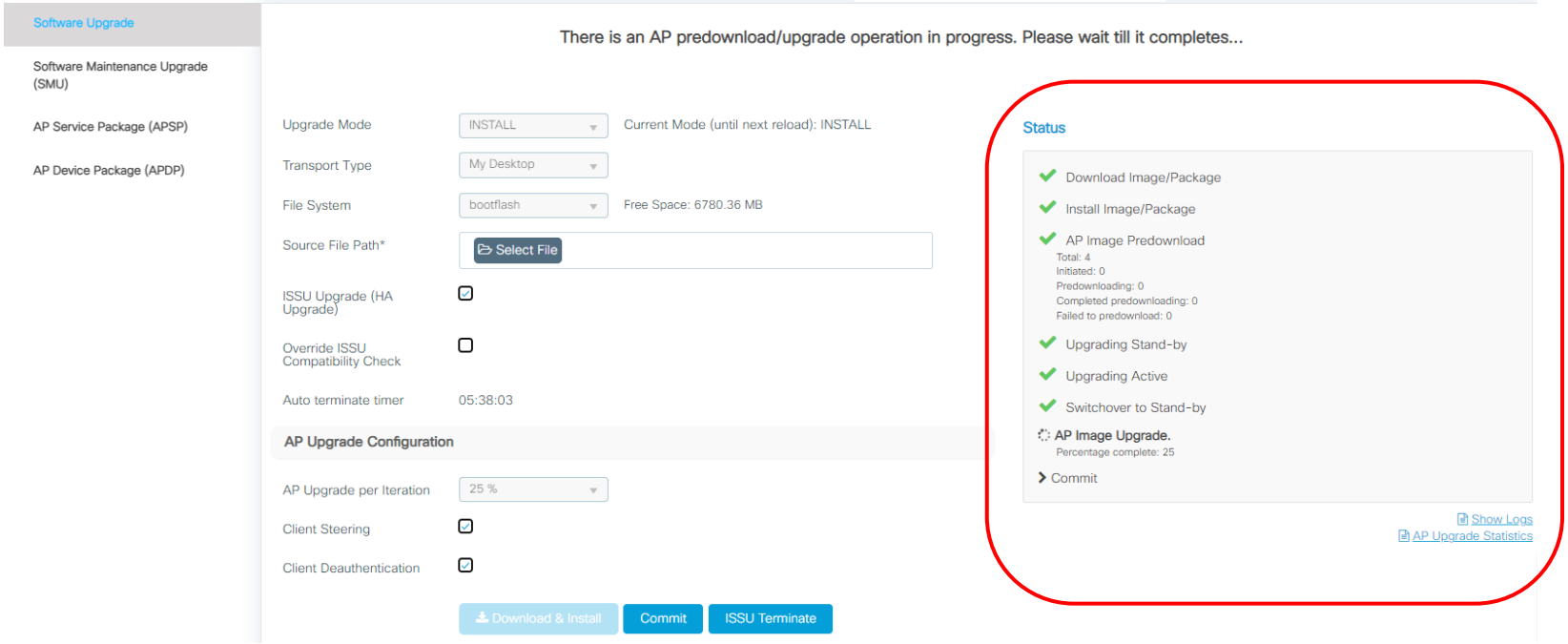
In Service Software Upgrades (ISSU)

ISSU Configuration



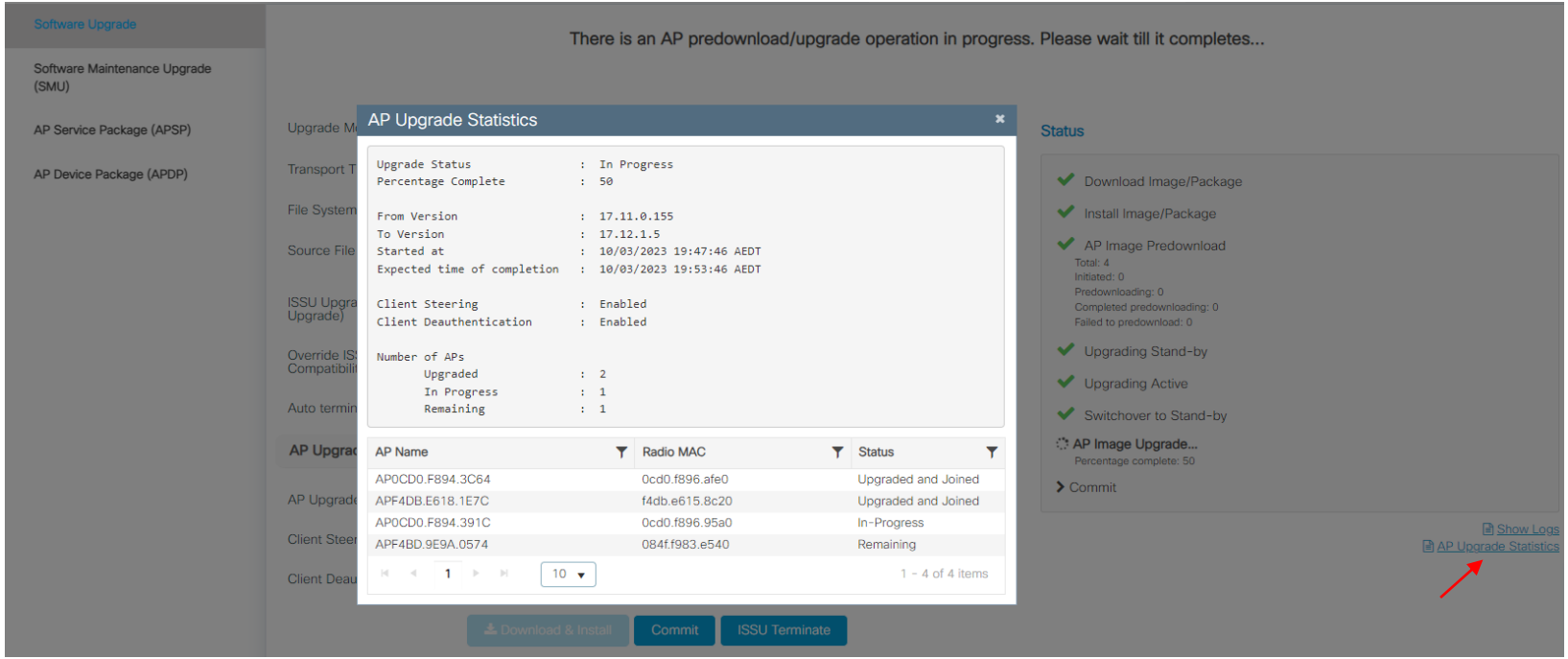
In Service Software Upgrades (ISSU)

ISSU; Monitoring the Process



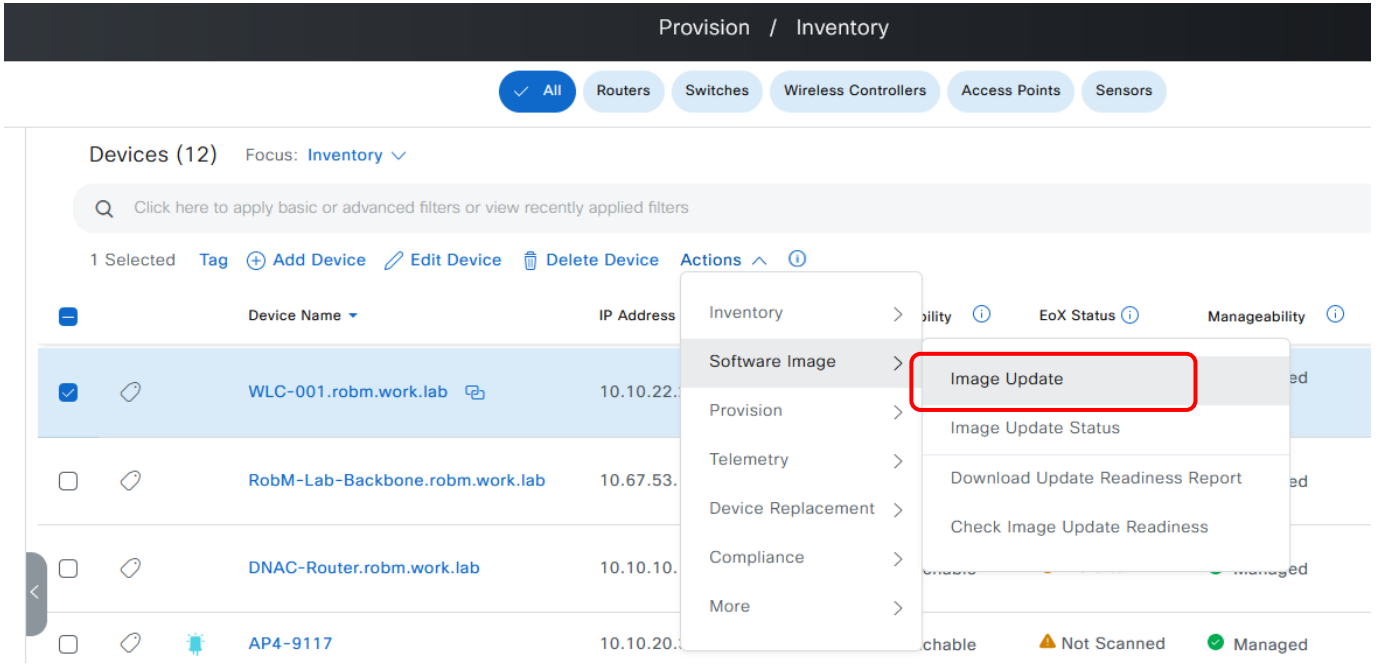
In Service Software Upgrades (ISSU)

ISSU; Monitoring the Process



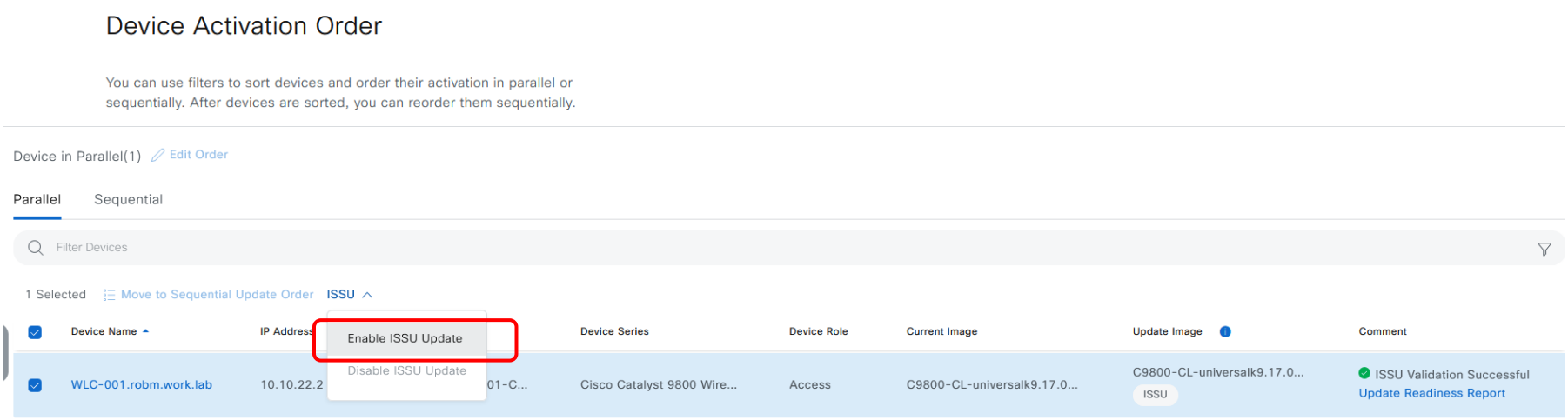
In Service Software Upgrades (ISSU)

Using Catalyst Center



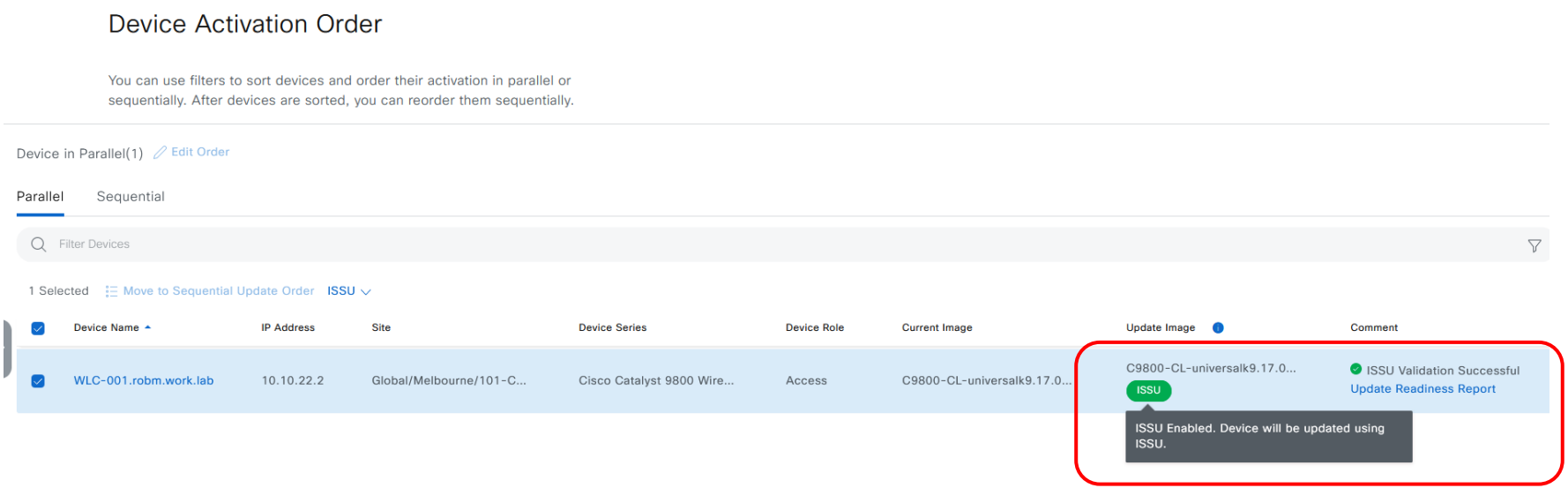
In Service Software Upgrades (ISSU)

Using Catalyst Center



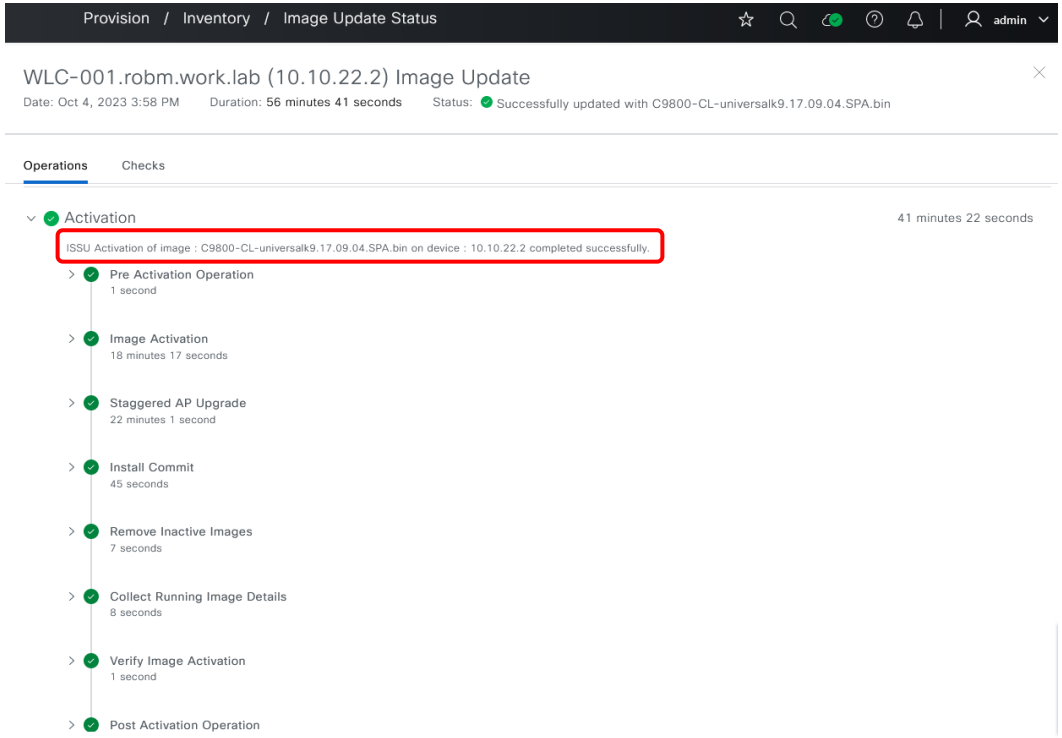
In Service Software Upgrades (ISSU)

Using Catalyst Center



In Service Software Upgrades (ISSU)

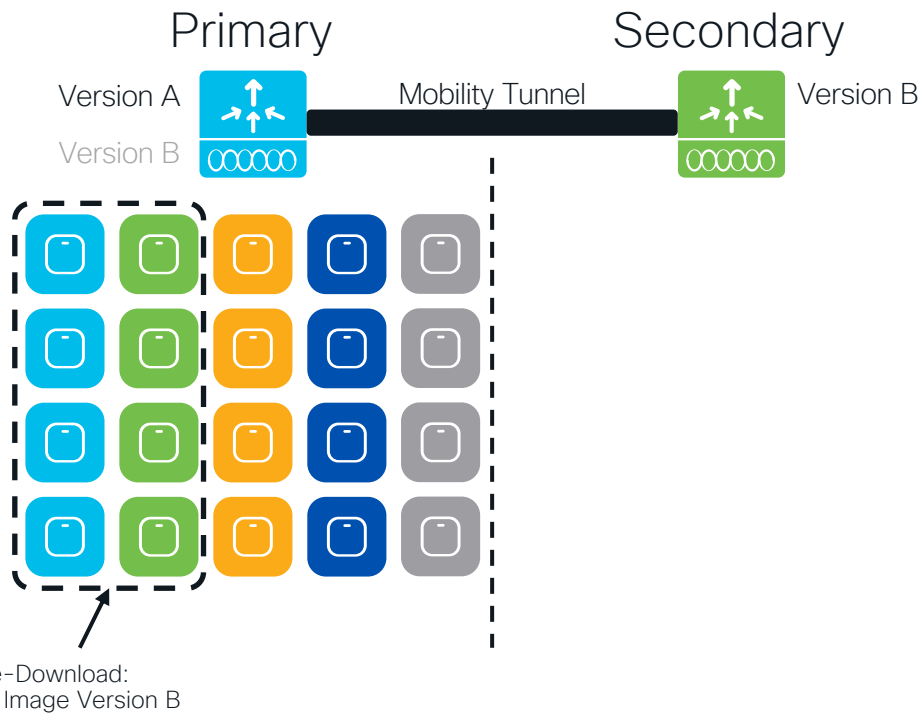
Using Catalyst Center



N+1 Site Based Hitless Upgrades

N+1 Site Based Hitless Upgrade

1. Load the new IOS XE image to the Primary controller
2. Add the Sites that will be upgraded first
3. Pre-download image to the APs:

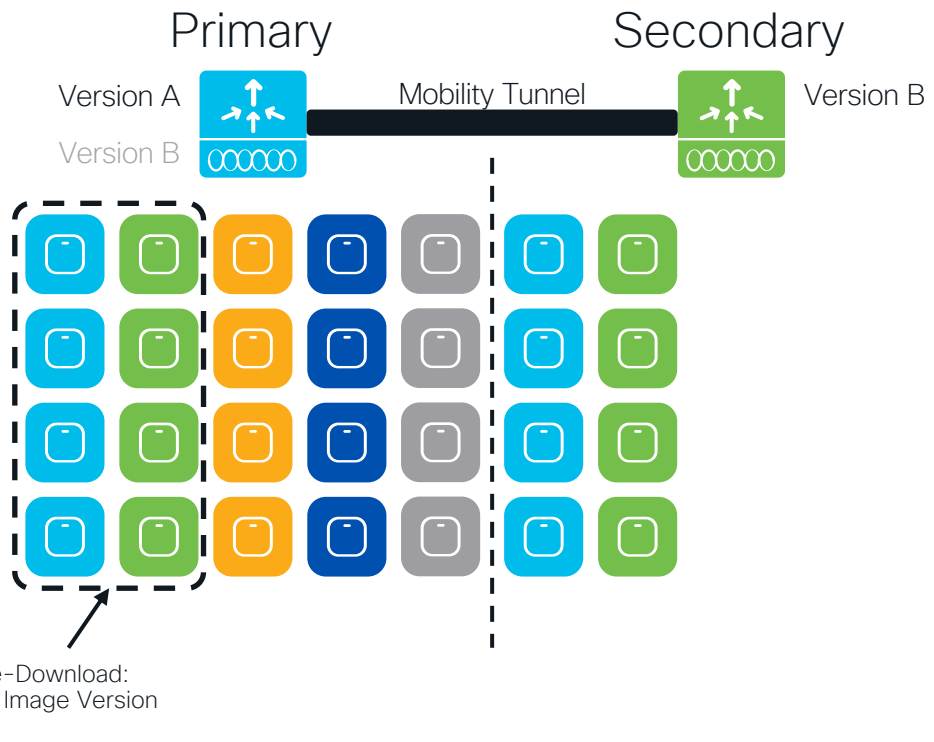


N+1 Site Based Hitless Upgrade

4 Candidate AP and neighbor marking selection begins

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.

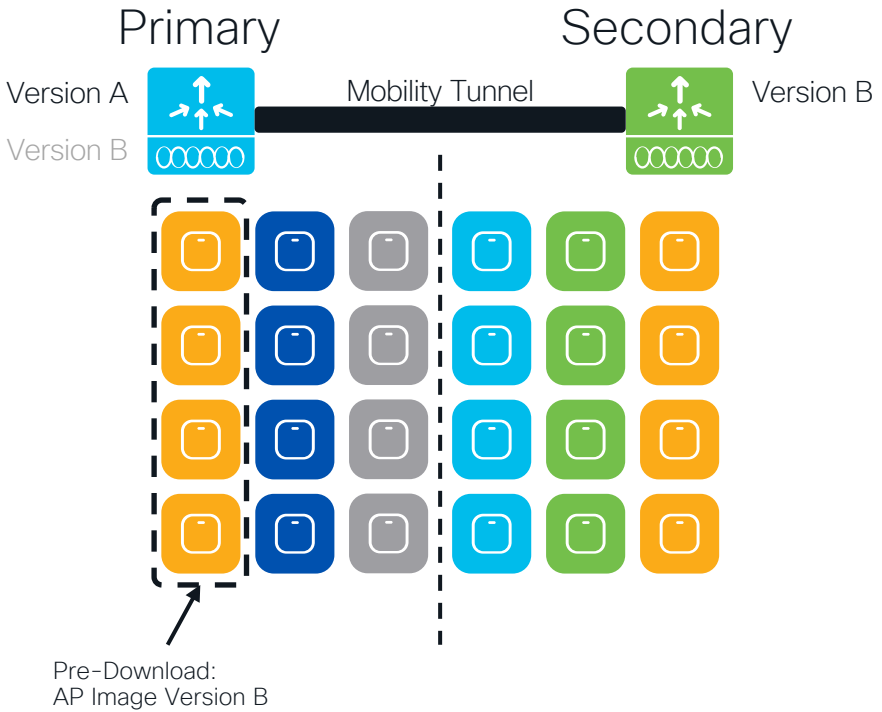


N+1 Site Based Hitless Upgrade

7 Add further sites to the site filter:

8 Initiate the AP image pre-download, reload with the new image, and join to the Secondary WLC in rolling fashion

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



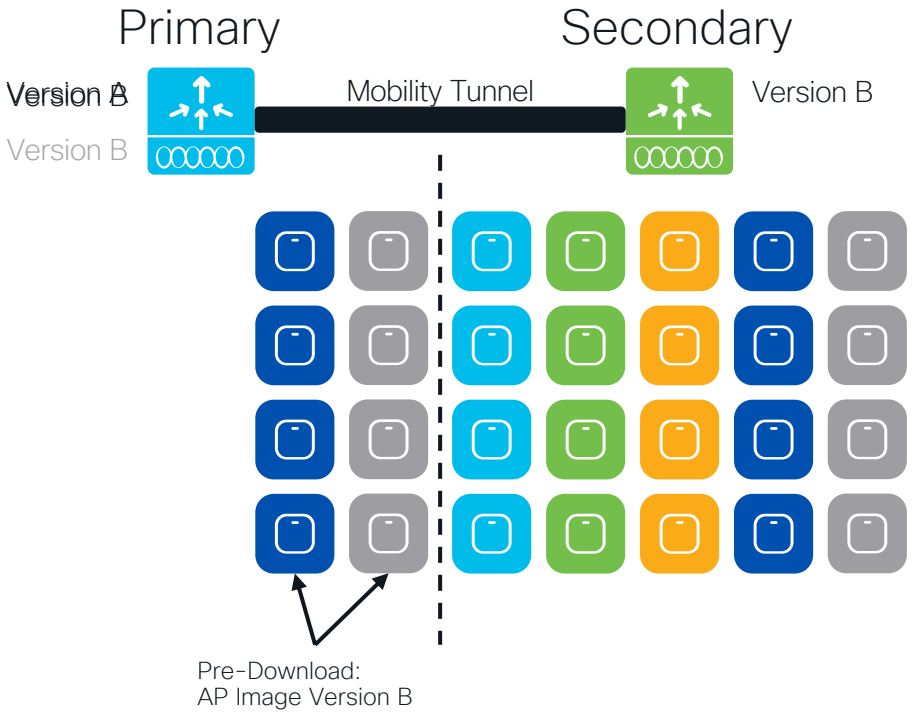
N+1 Site Based Hitless Upgrade

10 Upgrade the rest of the sites by clearing the site filter

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.

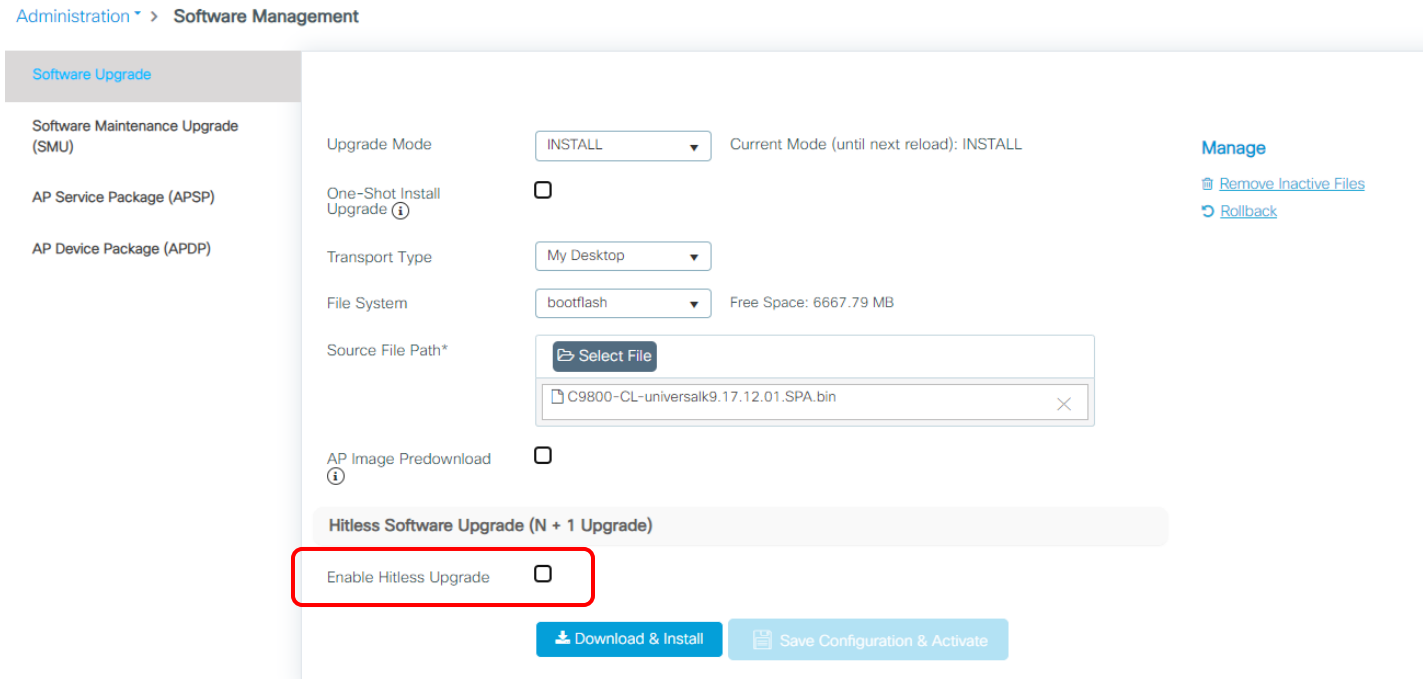
12 As the APs successfully join the Secondary WLC, the Secondary will update the Primary WLC.

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



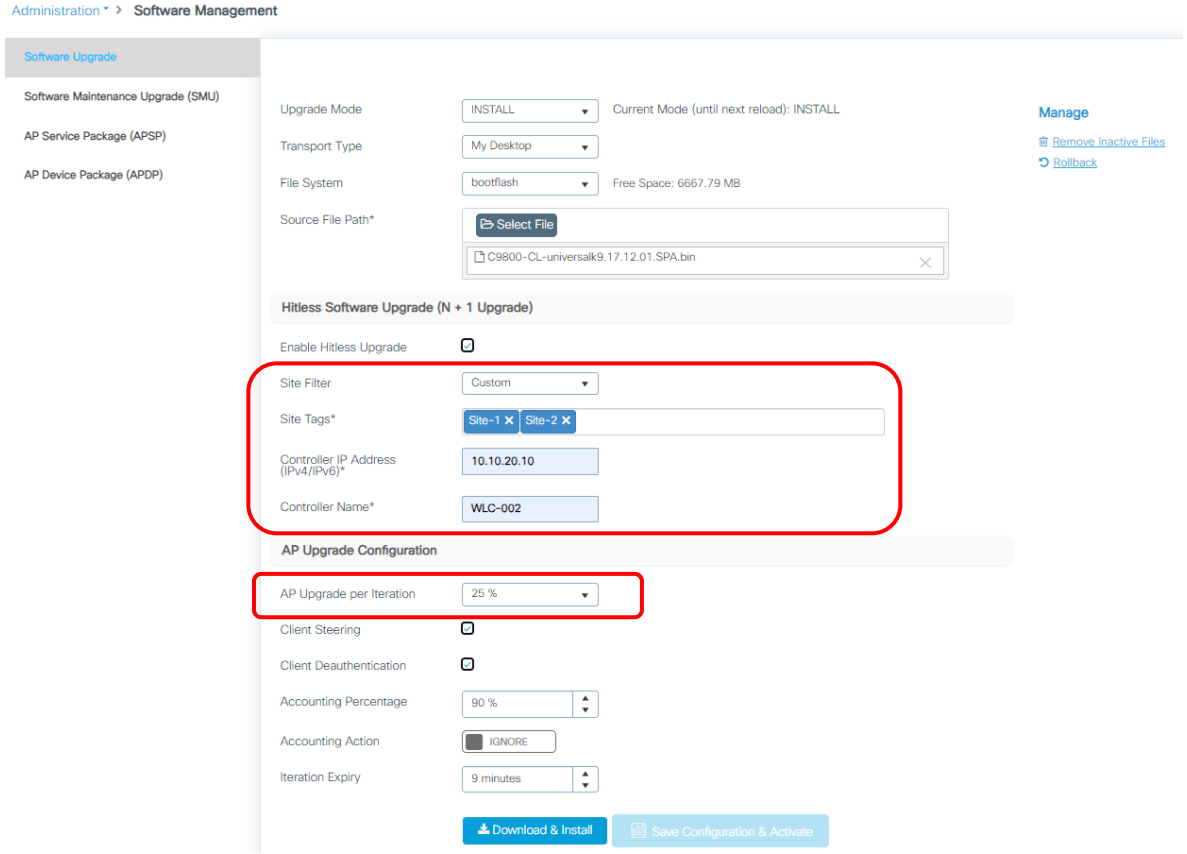
N+1 Site Based Hitless Upgrade

Configuration



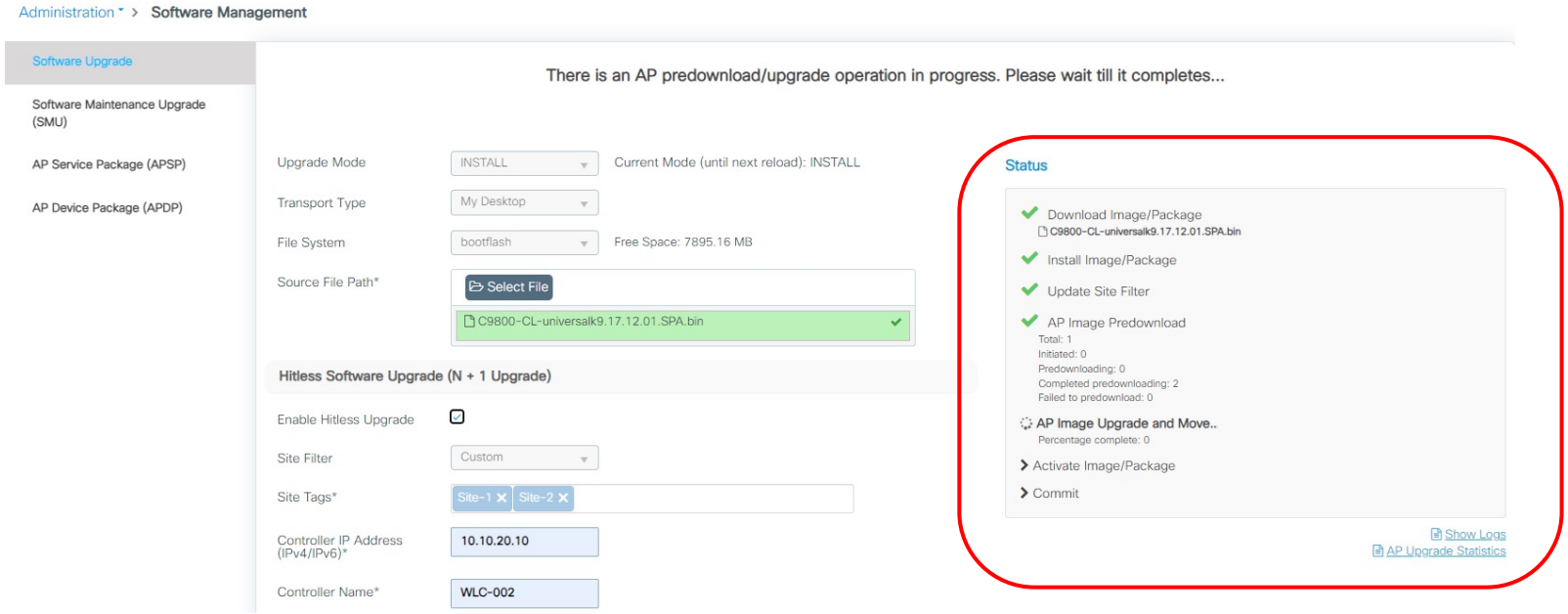
N+1 Site Based Hitless Upgrade

Configuration



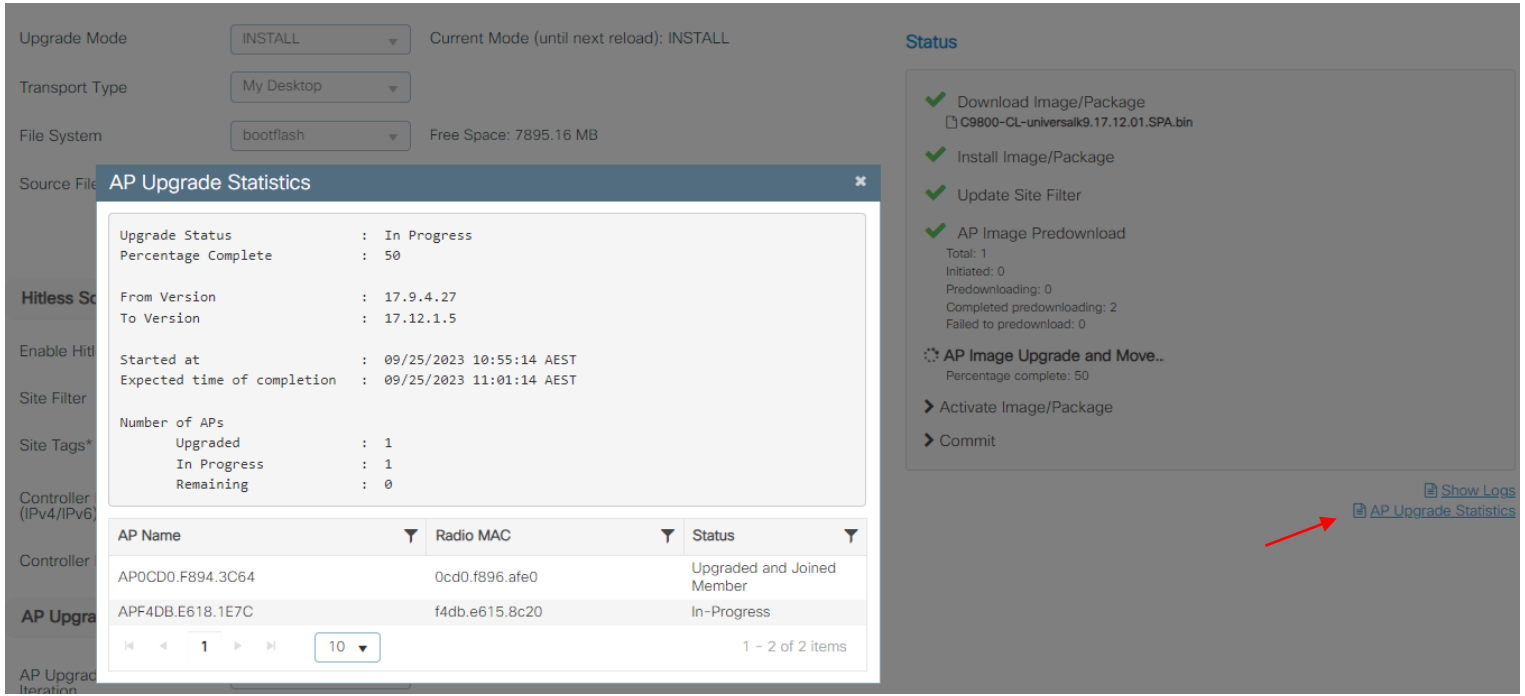
N+1 Site Based Hitless Upgrade

Verification



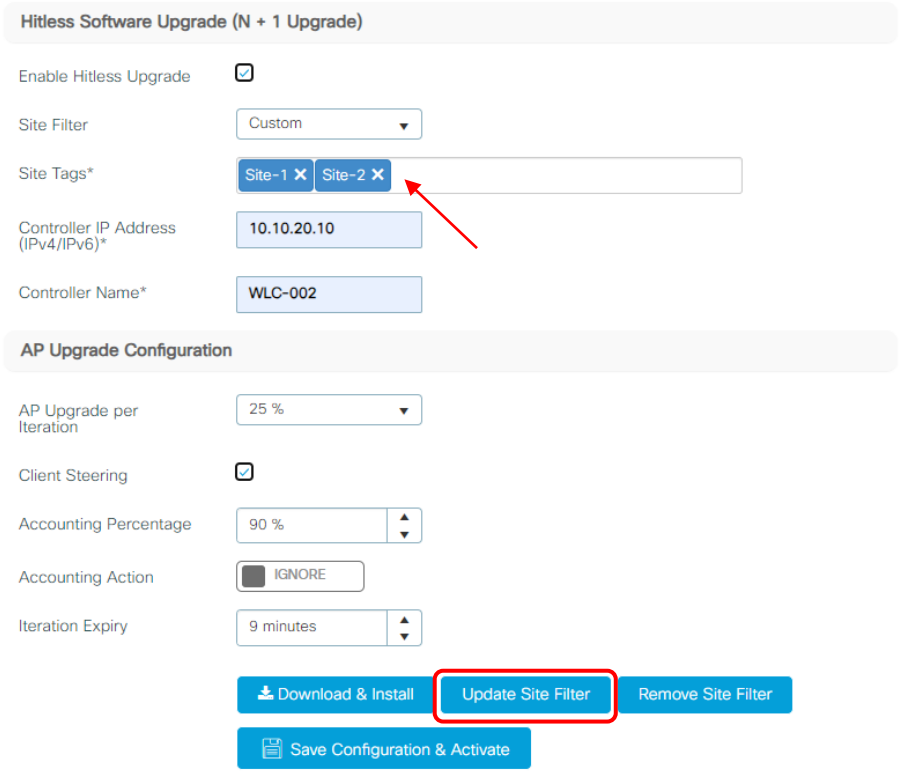
N+1 Site Based Hitless Upgrade

Verification



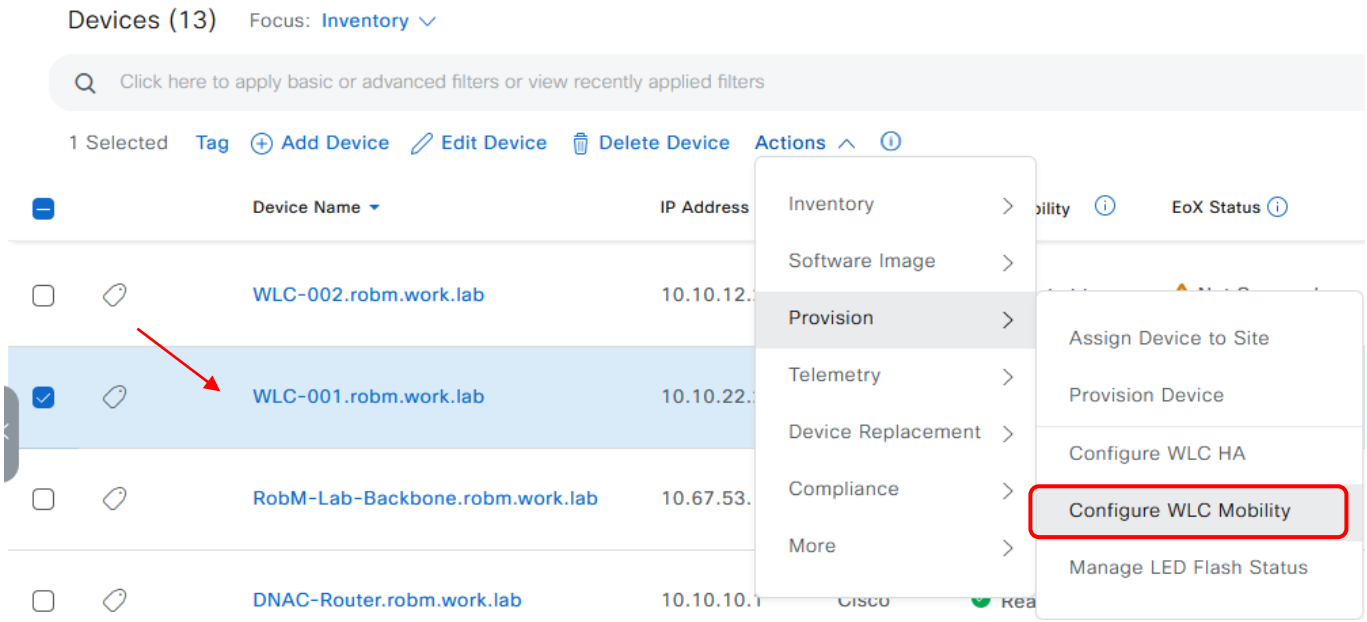
N+1 Site Based Hitless Upgrade

Verification



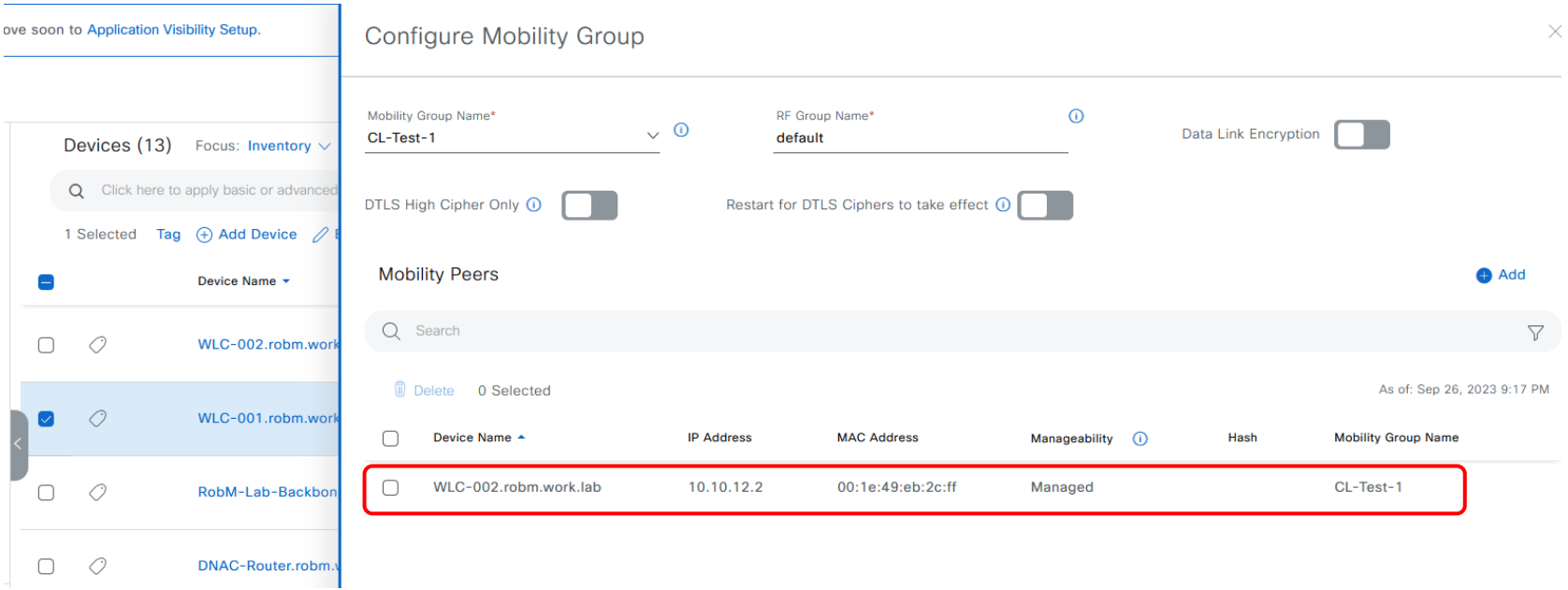
N+1 Hitless Upgrade

Using Catalyst Center



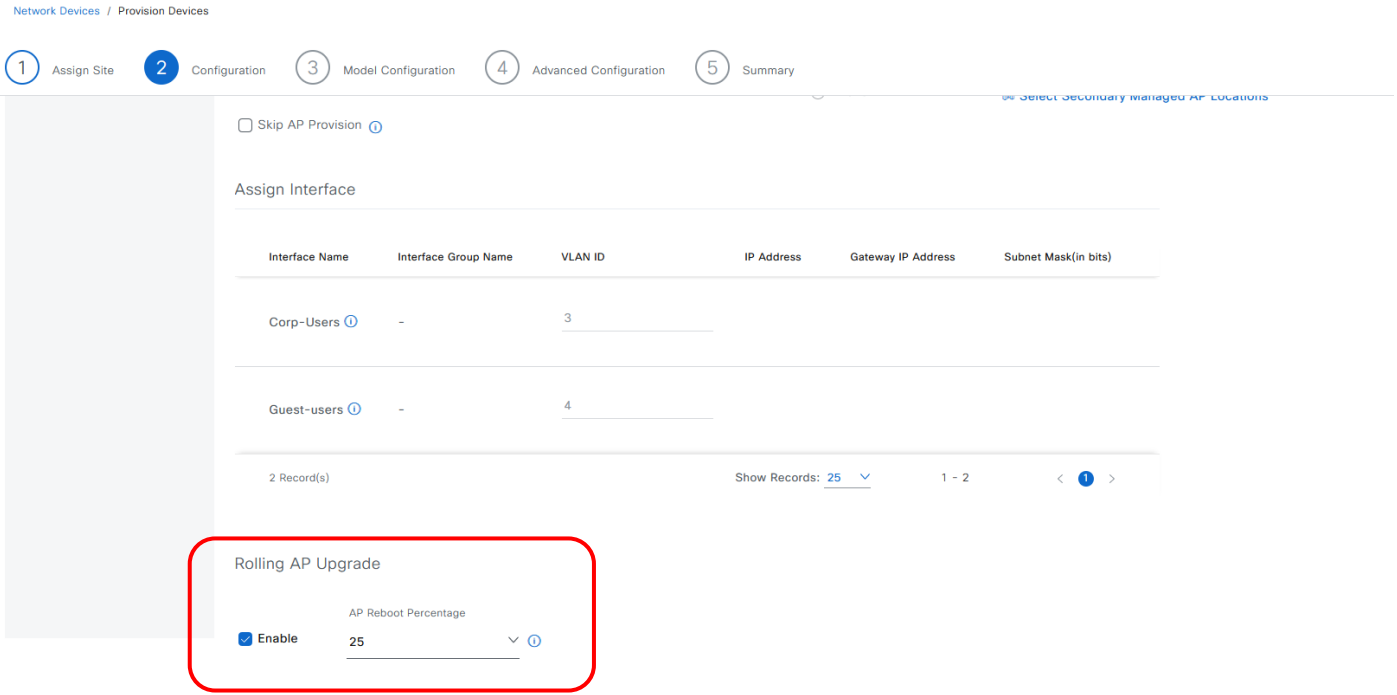
N+1 Hitless Upgrade

Using Catalyst Center



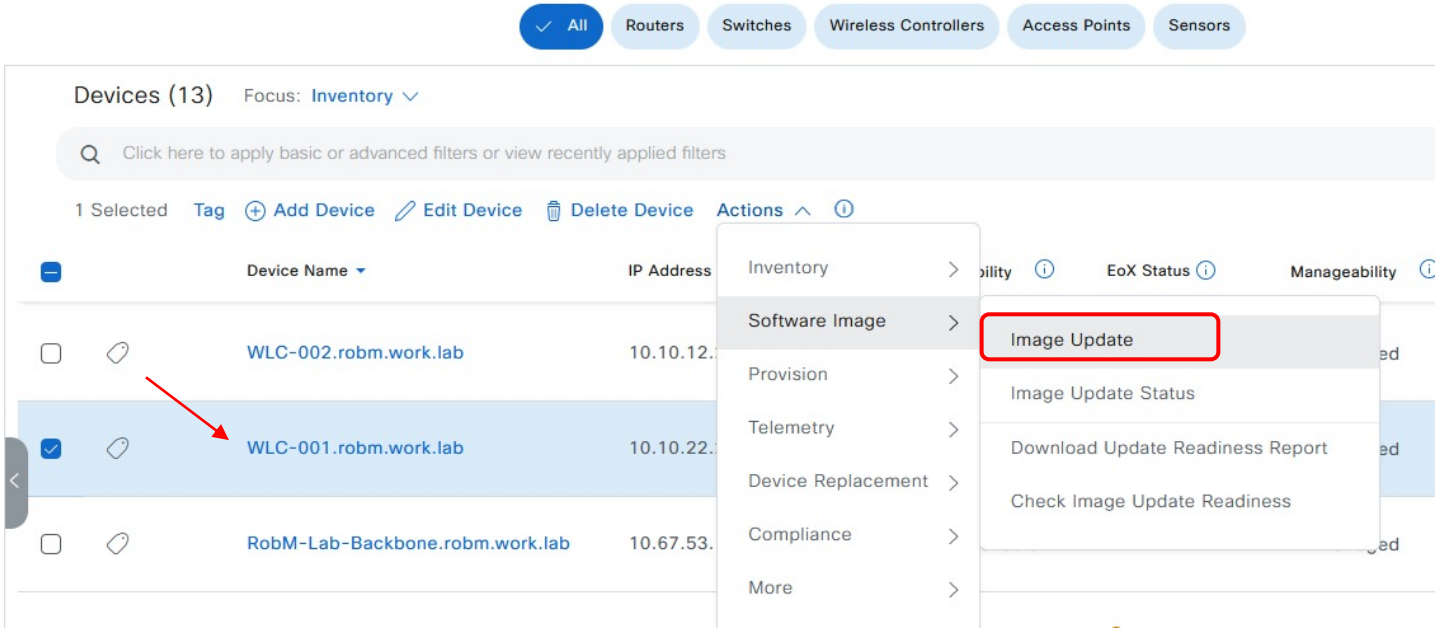
N+1 Hitless Upgrade

Using Catalyst Center



N+1 Hitless Upgrade

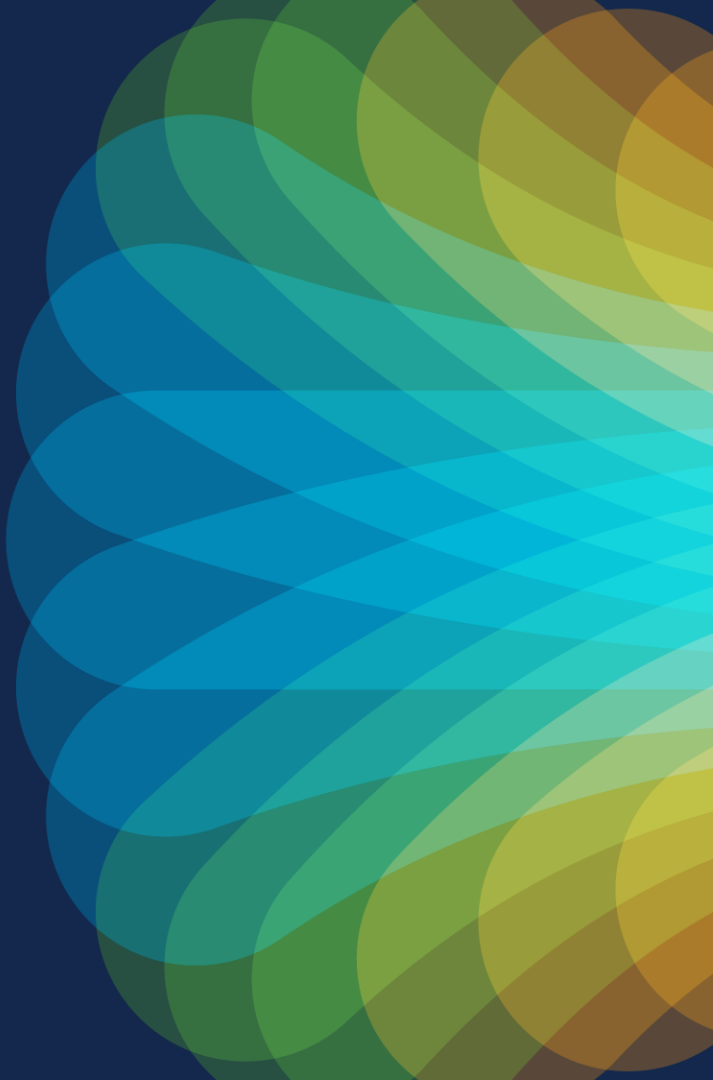
Using Catalyst Center



N+1 Hitless Upgrade

Using Catalyst Center

Software Patching Capabilities



^SMU on MD Release only

Software Patching Capabilities

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

Software Maintenance Update (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

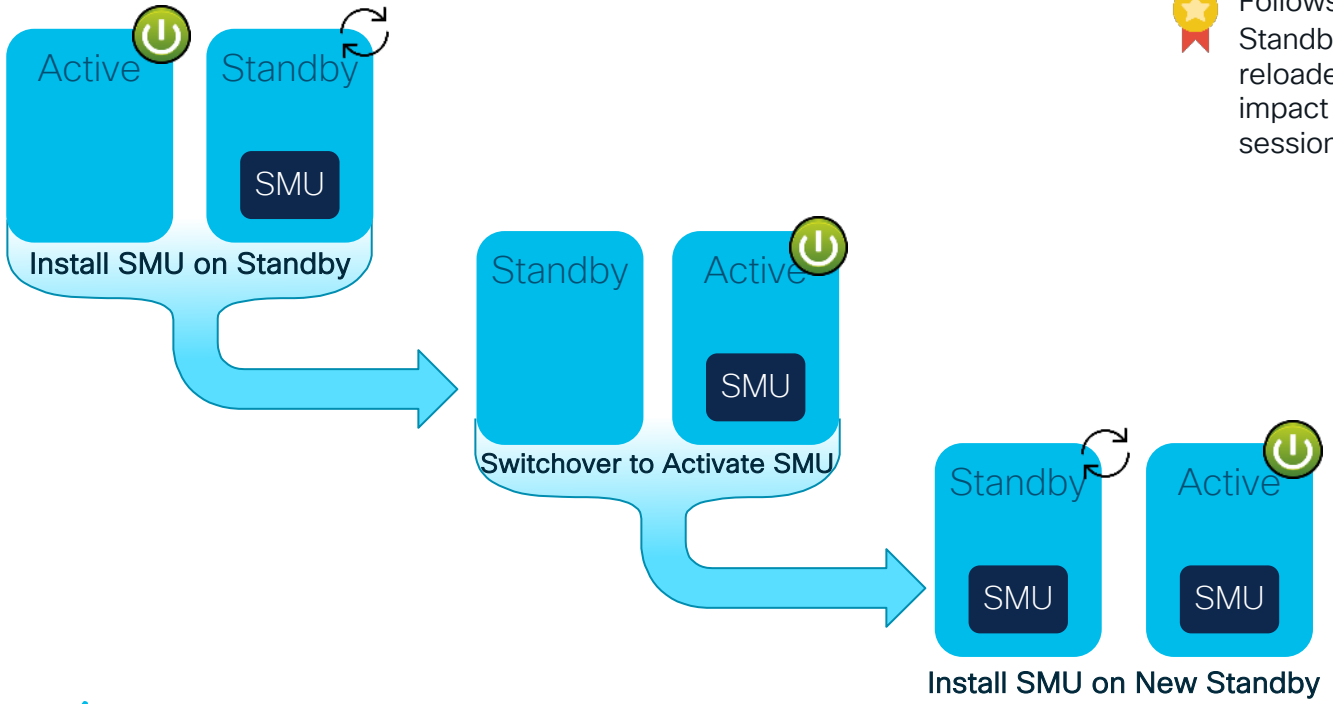
Software Maintenance Update (SMU)

Standalone vs Redundant Wireless Controller

	Hot Patch (No Wireless Controller reboot) Auto Install on Standby	Cold Patch Wireless Controller Reboot
Standalone Wireless Controller	No reload of Controller. AP & Client session won't be affected.	Reload controller. AP & Client sessions would be affected.
SSO Pair	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.

Software Maintenance Update (SMU)

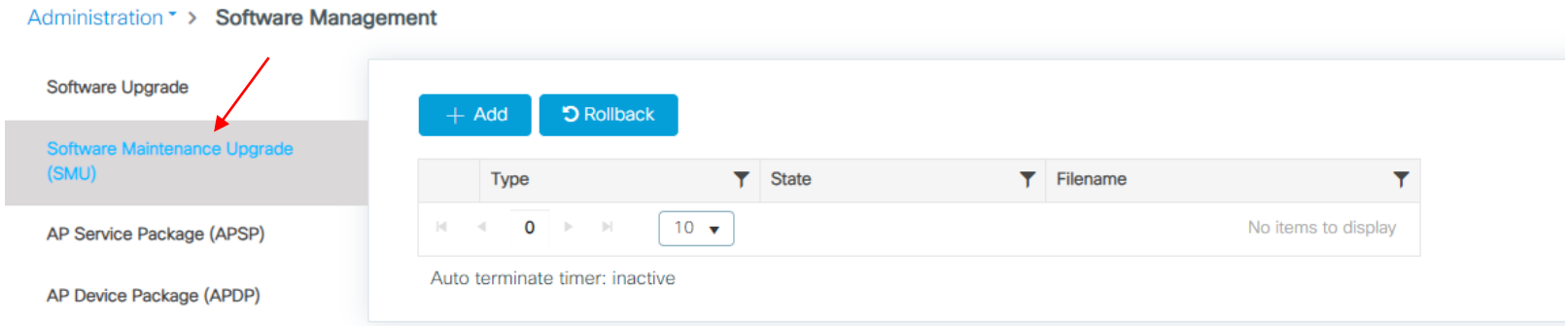
Cold Patch SMU on SSO Pair



Follows ISSU path and both Standby & Active controller reloaded but there is no impact to AP and Client session.

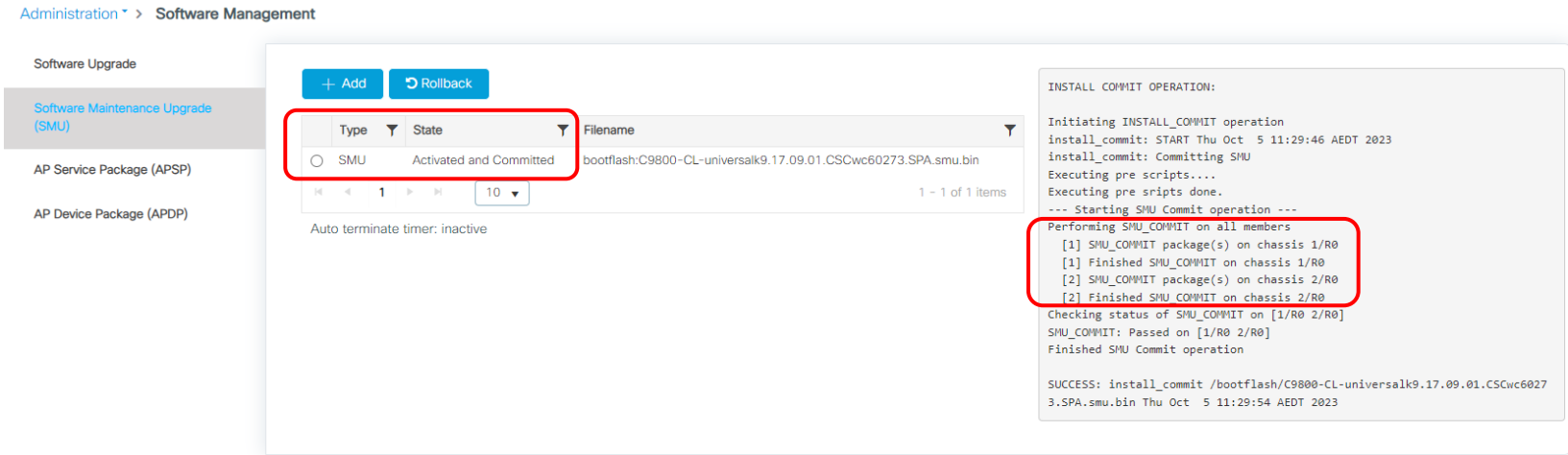
Software Maintenance Update (SMU)

Configuration



Software Maintenance Update (SMU)

SSO



AP Service Pack (APSP)

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

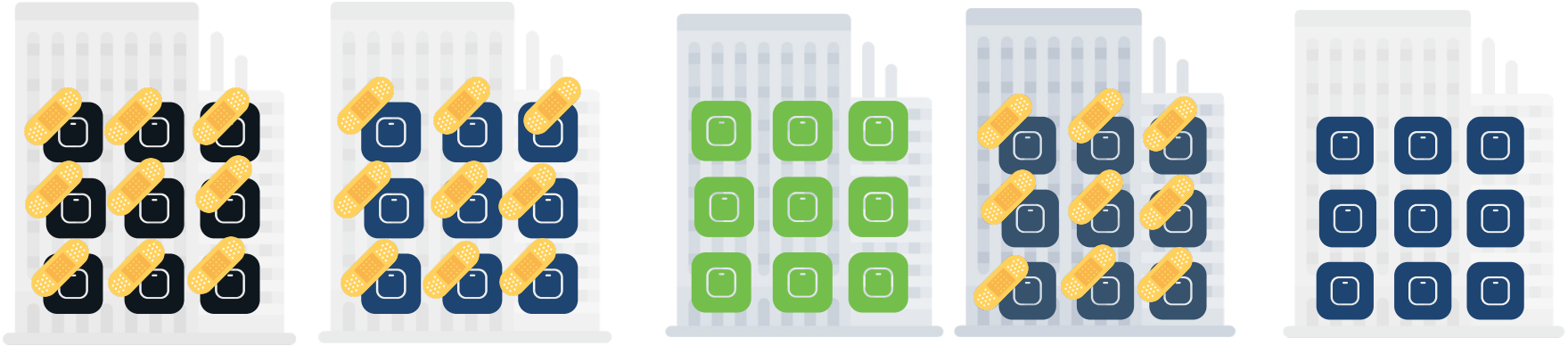
Enables user to control the propagation of APSP in the network

AP Service Pack (APSP)

Per-Site / Per-Model Workflow

Apply on Site A in rolling AP fashion

Not applicable for building with 9130AX



9120AX APs 9115AX APs

SiteA

9130AX APs 9120AX APs

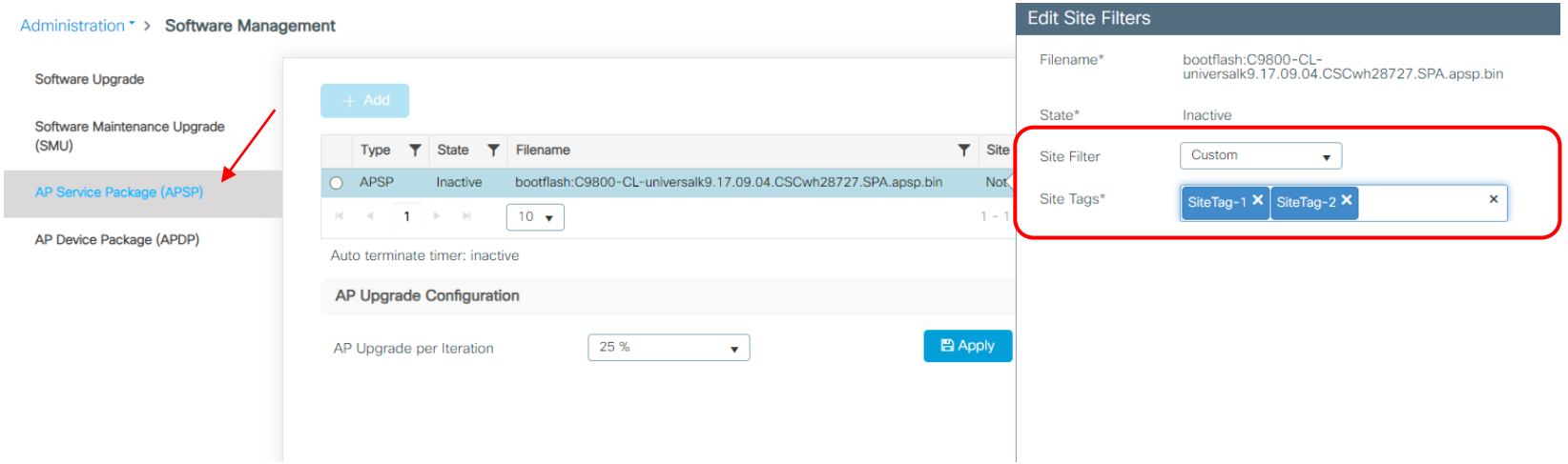
SiteB

9115AX APs

SiteC

AP Service Pack (APSP)

Configuration



AP Service Pack (APSP)

Verification

AP Upgrade Statistics

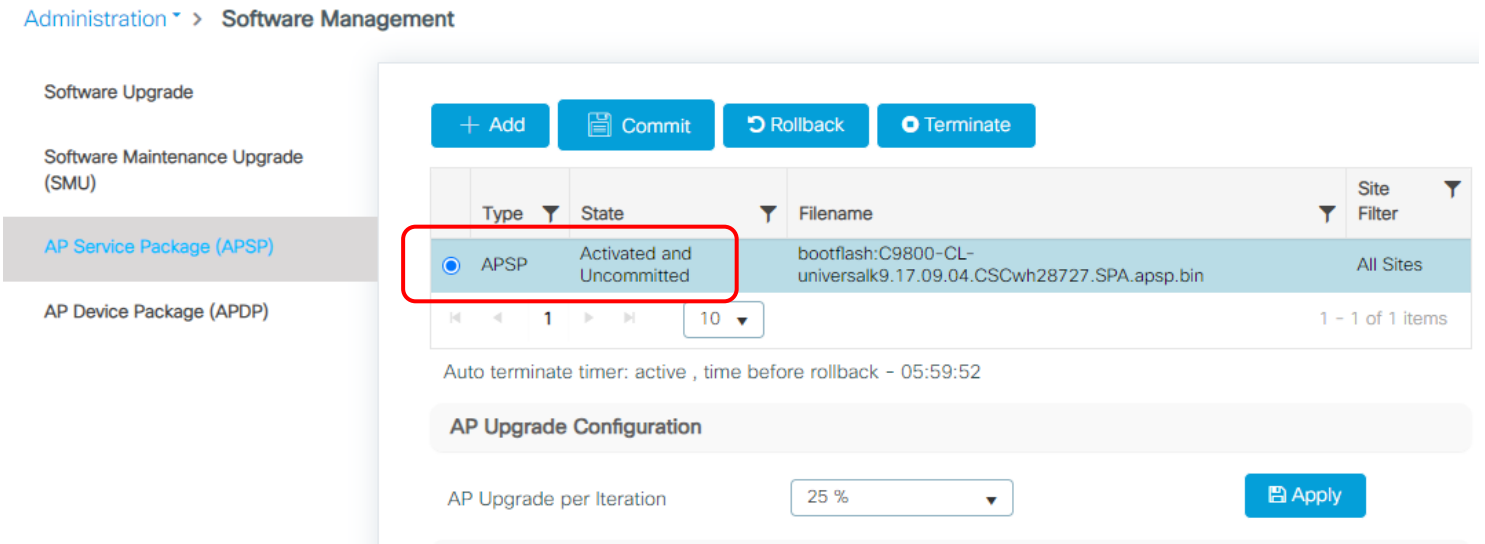
```
Upgrade Status                  :  Complete
Percentage Complete             :  100

From Version                    :  17.9.4.27
To Version                      :  17.9.4.201

Started at                      :  10/05/2023 16:50:22 AEDT
Ended at                        :  10/05/2023 16:50:22 AEDT

Number of APs
       Upgraded                 :  4
       In Progress              :  0
       Remaining                :  0
```

AP Name	Radio MAC	Status
APF4BD.9E9A.0574	084f.f983.e540	Upgraded and Not Impacted
AP0CD0.F894.391C	0cd0.f896.95a0	Upgraded and Not Impacted
AP0CD0.F894.3C64	0cd0.f896.afe0	Upgraded and Not Impacted
APF4DB.E618.1E7C	f4db.e615.8c20	Upgraded and Not Impacted

1 10 1 - 4 of 4 items

AP Service Pack (APSP)

Verification



AP Device Pack (APDP)

Traditionally ...

New AP hardware models need new WLC software

Wait for CCO version and re-qualify new release

Plan for Upgrading entire network

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

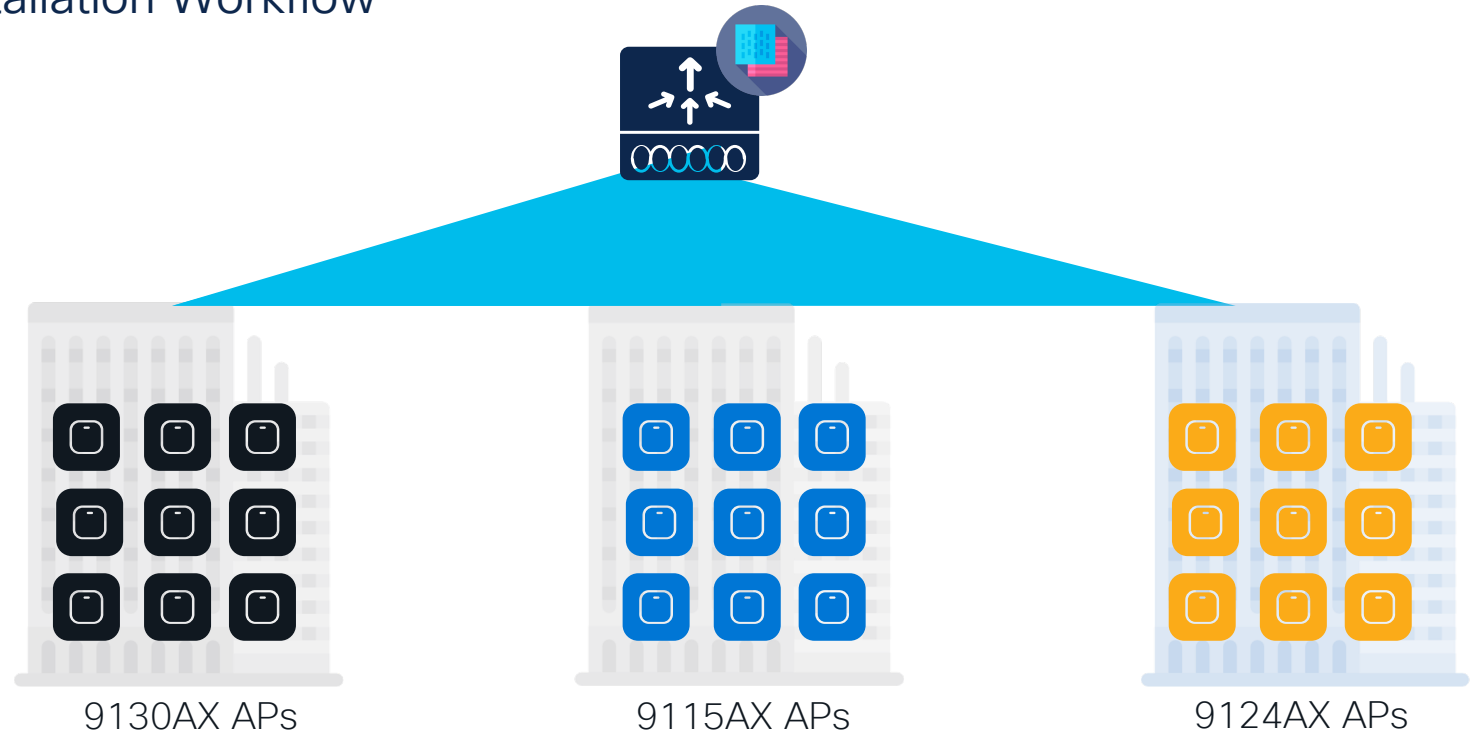
Zero Network Downtime

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

With AP Device Packs

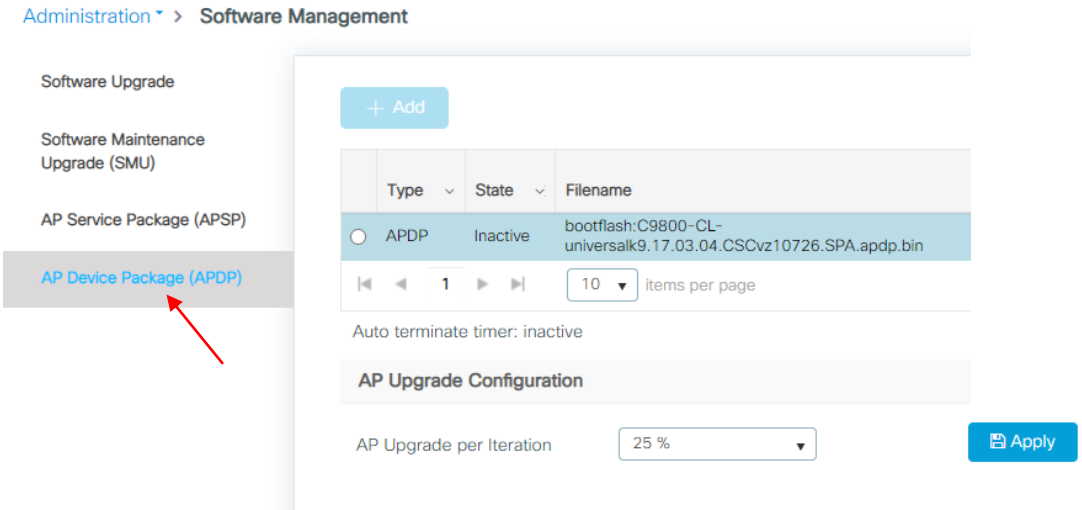
AP Device Pack (APDP)

Installation Workflow



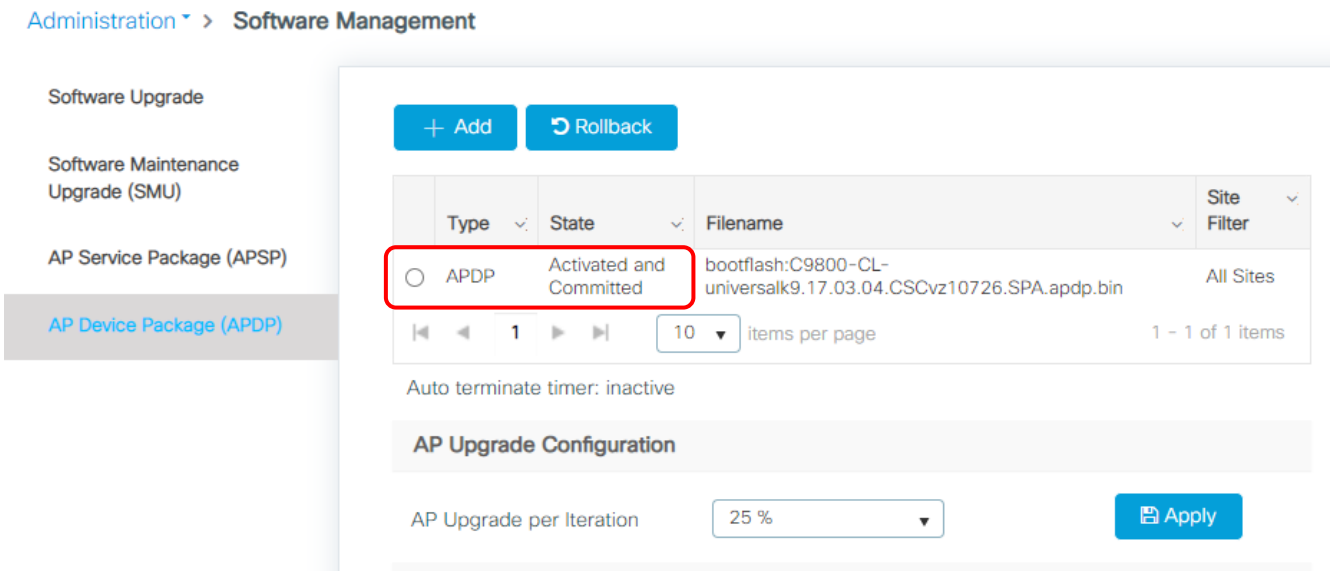
AP Device Pack (APDP)

Configuration



AP Device Pack (APDP)

Verification

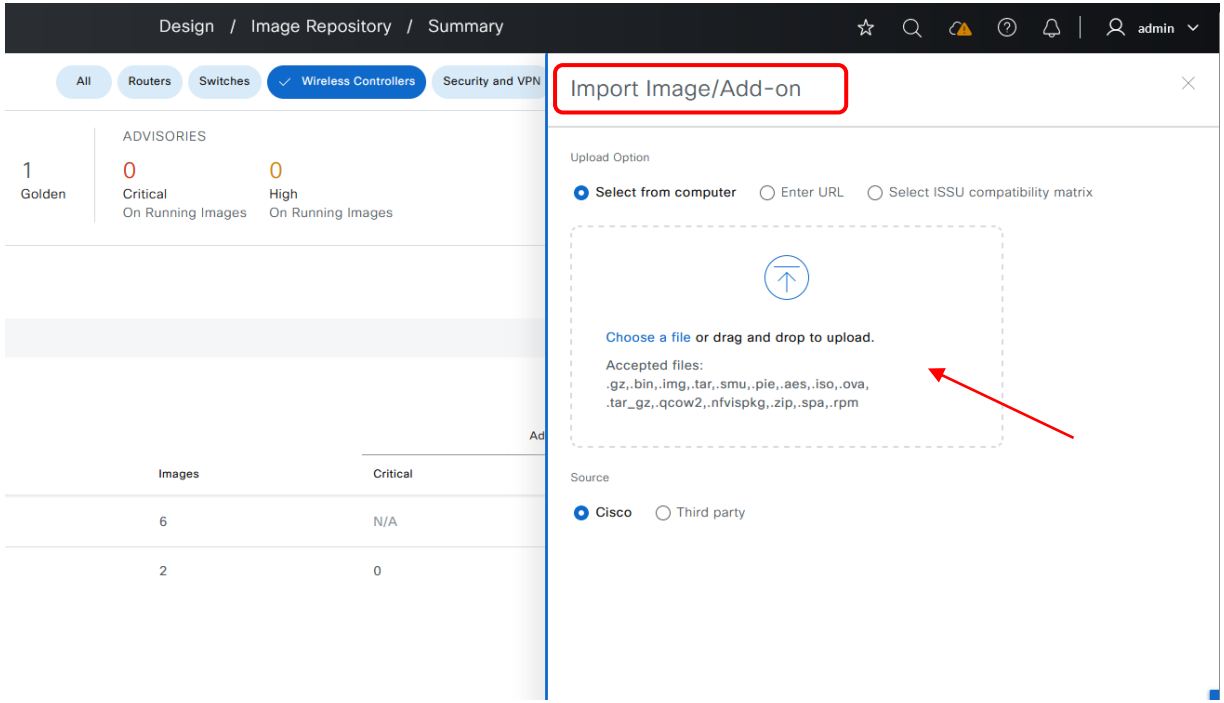


AP Device Pack (APDP)

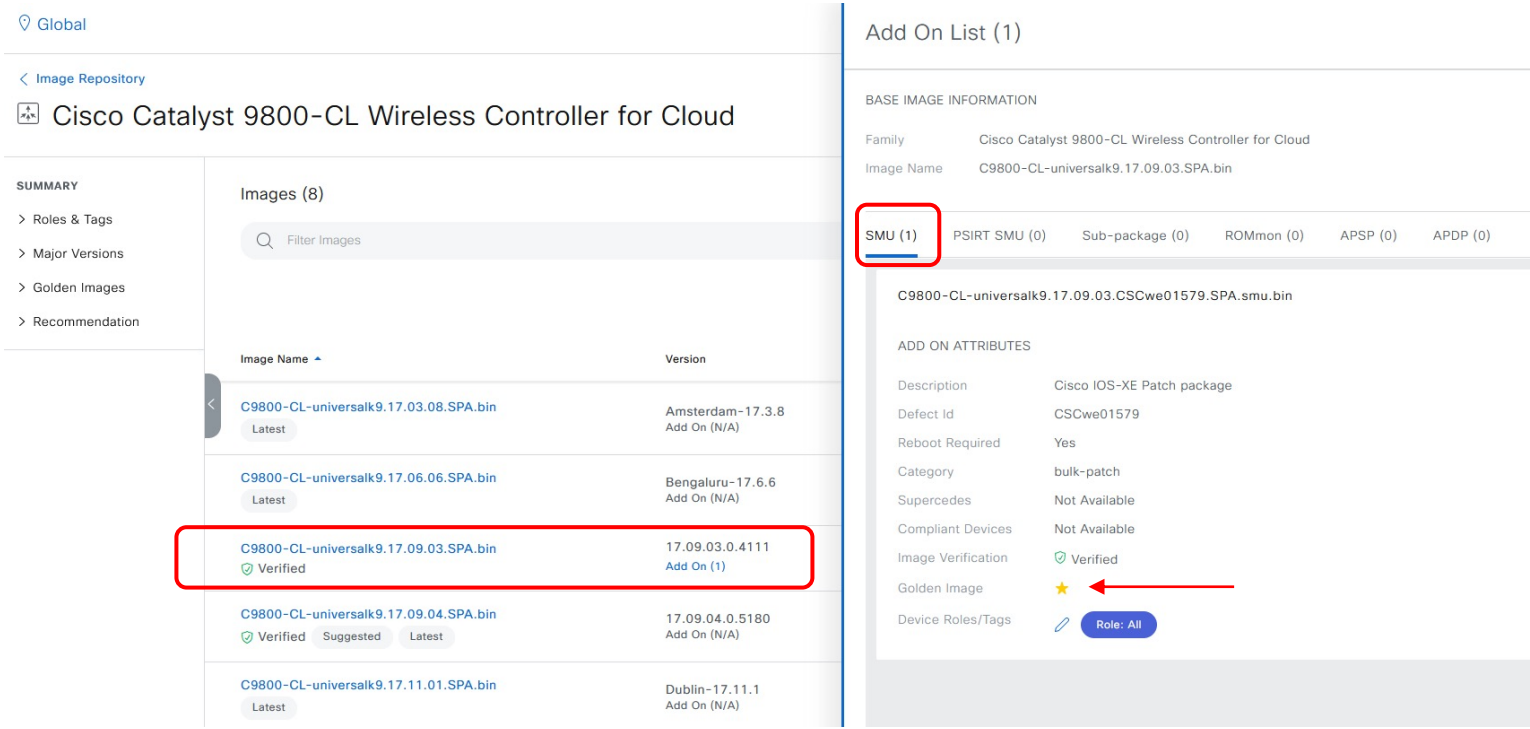
Verification

```
WLC-001#sh install summary
[ Chassis 1/R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.03.04.0.5557
SMU   C    bootflash:C9800-CL-universalk9.17.03.04.CSCvz30708.SPA.smu.bin
APSP   C    bootflash:C9800-CL-universalk9.17.03.04.CSCvz58821.SPA.apsp.bin
APDP   C    bootflash:C9800-CL-universalk9.17.03.04.CSCvz10726.SPA.apdp.bin

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------


WLC-001#
```

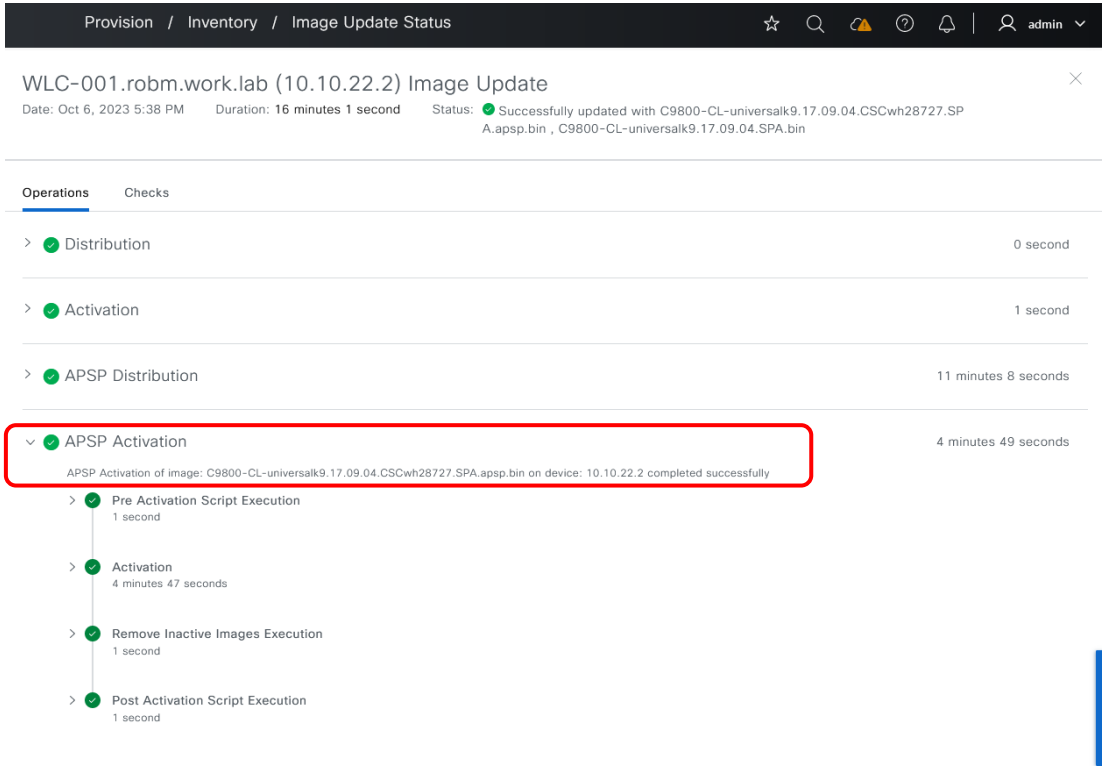
Software Patching using Catalyst Center



Software Patching using Catalyst Center



Software Patching in Catalyst Center



Extra Content..!

- Resiliency Feature Matrix
- Failure Scenarios for SSO
- Official Support Matrix for ISSUs
- Reference Documentation
- Additional Technical notes

The New Normal: Zero Downtime




Unplanned Events

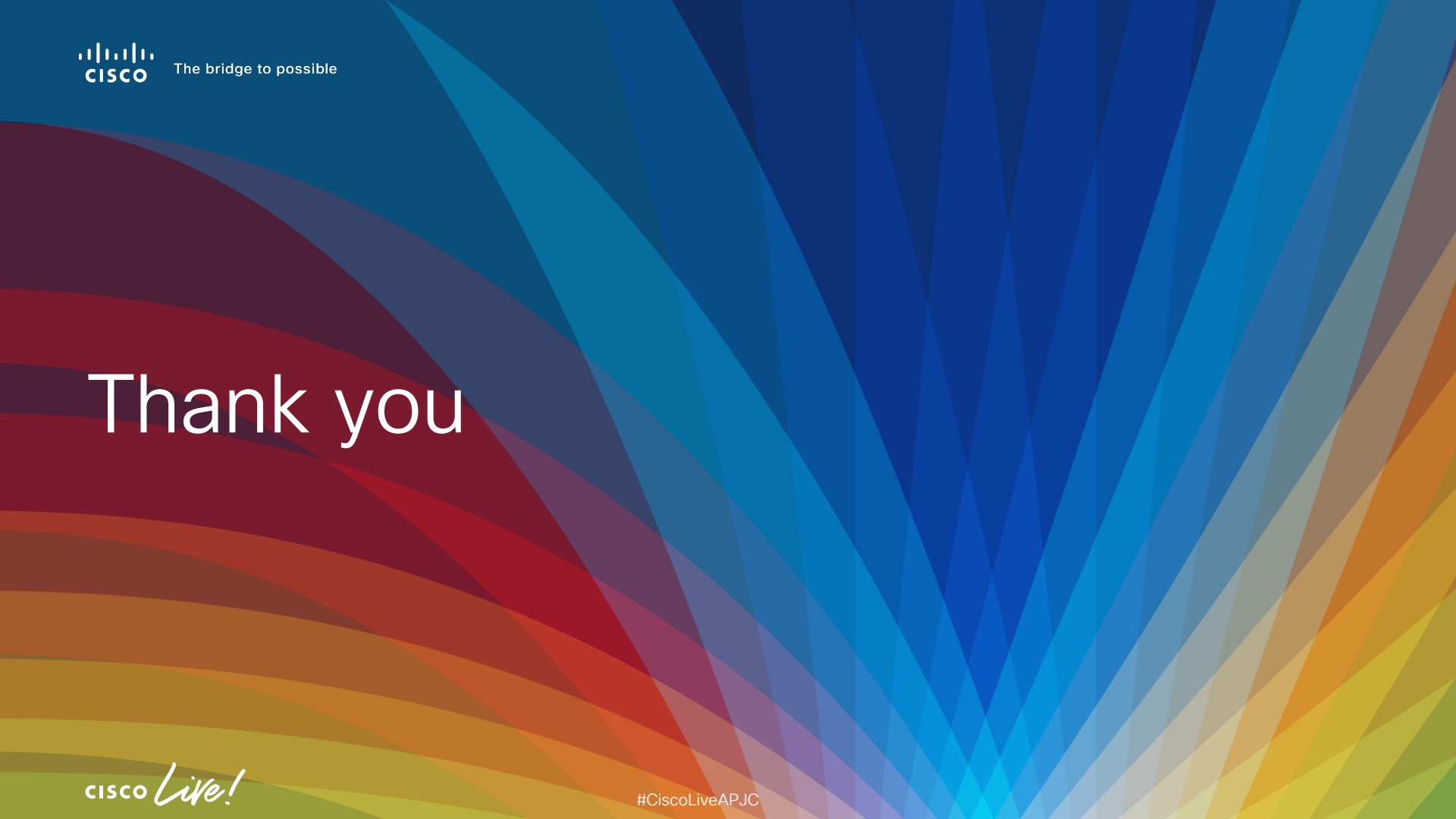
- ✓ Link Level redundancy
- ✓ N+1 redundancy for always-on wireless network
- ✓ SSO leveraging Active & Hot Standby

Image Upgrades

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

Infrastructure Updates

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


cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLiveAPJC

cisco Live!

Let's go

#CiscoLiveAPJC