

CISCO *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

High Availability Design with Cisco Catalyst 9800 Wireless Controller

Robert Moretti
Technical Solutions Specialist
BRKEWN-2846

CISCO *Live!*

#CiscoLiveAPJC



“Reconciliation” - Dustin Koa Art

CISCO *Live!*

Cisco Webex App

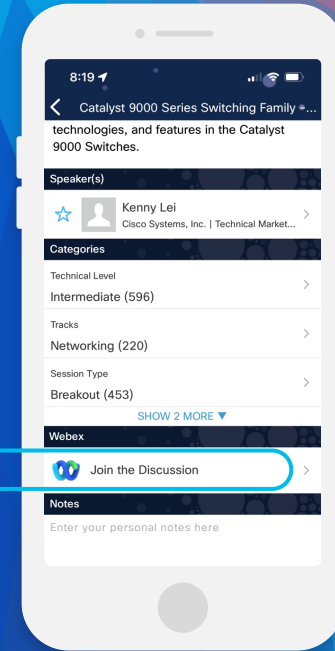
Questions?

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.

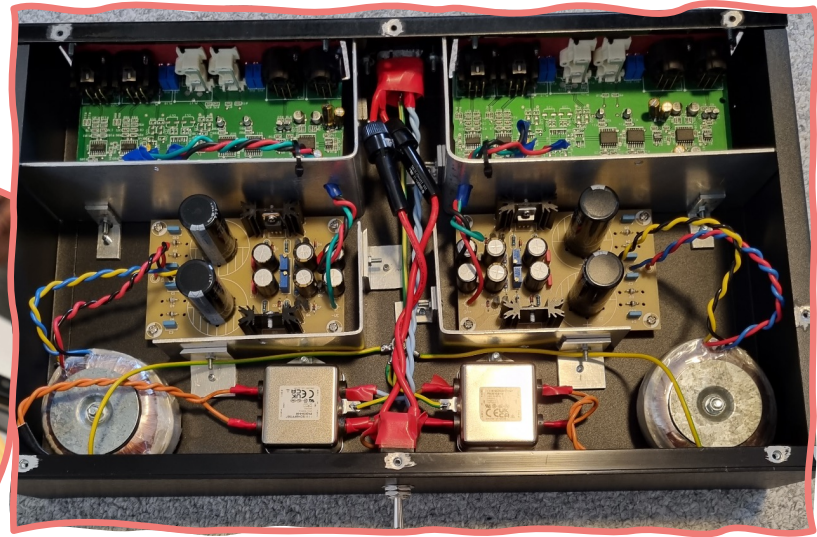


<https://cislolive.ciscoevents.com/cislolivebot/#BRKEWN-2846>

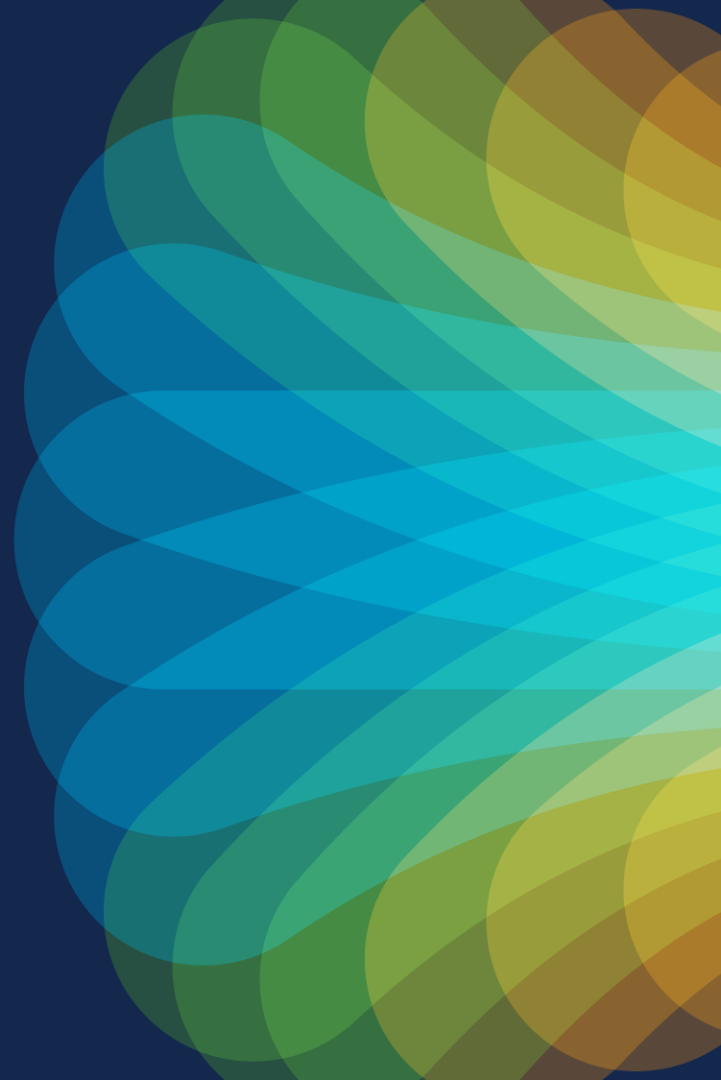
Agenda

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

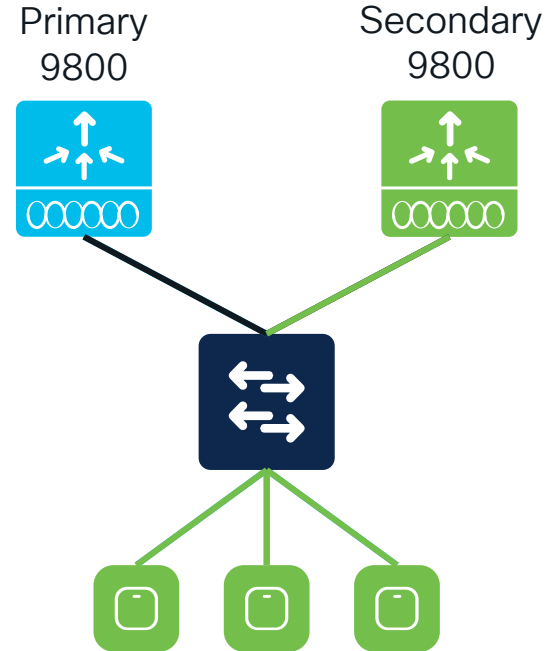
- Image Upgrade
- Network Upgrade

- 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



AP failover takes ~45-60 seconds

N+1 Redundancy Configuration

Configuration > Wireless > Access Points

▼ All Access Points

Total APs : 4

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address
APF4BD.9E9A.0574	C9120AXI-Z	2	✓	0 days 0 hrs 7 mins 49 secs	172.16.1
AP0CD0.F894.391C	C9117AXI-Z	2	✓	0 days 0 hrs 8 mins 3 secs	172.16.1
AP0CD0.F894.3C64	C9117AXI-Z	2	✓	0 days 0 hrs 8 mins 2 secs	172.16.1
APF4DB.E618.1E7C	AIR-AP3802I-Z-K9	2	✓	0 days 0 hrs 8 mins 6 secs	172.16.1

1 / 10

Edit AP




General Interfaces **High Availability** Inventory Geolocation ICap Advanced Support Bundle

	Name	Management IP Address (IPv4/IPv6)
Primary Controller	<input type="text" value="WLC-001"/>	<input type="text" value="10.10.10.10"/>
Secondary Controller	<input type="text" value="WLC-002"/>	<input type="text" value="10.10.20.10"/>
Tertiary Controller	<input type="text"/>	<input type="text"/>
AP failover priority	<input type="text" value="Low"/>	

N+1 Redundancy

Bulk AP Provisioning

Configuration > Wireless > Bulk AP Provisioning

 Select APs  Select Parameters  Summary

General

Admin Status: Location:

Geolocation

Height (meters): Height Uncertainty (meters):
Cable Length (meters): Floor:

High Availability

	Name	Management IP Address (IPv4/IPv6)
Primary Controller	<input type="text" value="WLC-001"/>	<input type="text" value="10.10.10.10"/>
Secondary Controller	<input type="text" value="WLC-002"/>	<input type="text" value="10.10.20.10"/>
Tertiary Controller	<input type="text"/>	<input type="text"/>

CLI Preview

```
ap name <ap-name> controller secondary WLC-002 10.10.20.10
ap name <ap-name> controller primary WLC-001 10.10.10.10
```

N+1 Redundancy

Bulk AP Provisioning

Task Details

Task Name: Test-1
Start Time: 09/14/2023 08:39:05
End Time: 09/14/2023 08:43:54
Status: Completed

Applied Configuration

Parameter	Value	Applied CLI
Primary Controller Name	WLC-001	ap name <ap-name> controller primary WLC-001 10.10.10.10
Primary Controller IP	10.10.10.10	ap name <ap-name> controller primary WLC-001 10.10.10.10
Secondary Controller Name	WLC-002	ap name <ap-name> controller secondary WLC-002 10.10.20.10
Secondary Controller IP	10.10.20.10	ap name <ap-name> controller secondary WLC-002 10.10.20.10

AP Provision Results

All configuration applied: 2 Some configuration applied: 0 None of the configuration applied: 0

AP Name	AP Status
AP0CD0.F894.391C	All configuration applied

Configuration

Configuration	Configuration Status
Primary Controller Name	✓ Applied Successfully
Primary Controller IP	✓ Applied Successfully
Secondary Controller Name	✓ Applied Successfully
Secondary Controller IP	✓ Applied Successfully

N+1 Redundancy Configuration

Edit AP Join Profile

General Client **CAPWAP** AP Management Security ICap QoS Geolocation

High Availability Advanced

CAPWAP Timers

Fast Heartbeat Timeout(sec)*	<input type="text" value="3"/>
Heartbeat Timeout(sec)*	<input type="text" value="30"/>
Discovery Timeout(sec)*	<input type="text" value="10"/>
Primary Discovery Timeout(sec)*	<input type="text" value="120"/>
Primed Join Timeout(sec)*	<input type="text" value="0"/>

Retransmit Timers

Count*	<input type="text" value="5"/>
Interval (sec)*	<input type="text" value="3"/>

AP Fallback to Primary ⓘ

Enable

Backup Primary Controller

Name	<input type="text" value="WLC-002"/>
IPv4/IPv6 Address	<input type="text" value="10.10.20.10"/>

Backup Secondary Controller

Name	<input type="text" value="Enter Name"/>
IPv4/IPv6 Address	<input type="text"/>

N+1 Redundancy Configuration

The screenshot displays the 'Edit AP Join Profile' configuration page. The 'CAPWAP' tab is active, and the 'High Availability' sub-tab is selected. The 'CAPWAP Timers' section is expanded, showing the 'AP Fallback to Primary' option enabled with a checkmark. Below this, the 'Backup Primary Controller' is configured with Name 'WLC-002' and IPv4/IPv6 Address '10.10.20.10'. The 'Backup Secondary Controller' section is also visible with a name input field set to 'Enter Name' and an empty IPv4/IPv6 address field. At the bottom, the 'Interval (sec)*' is set to 3. A red box highlights the 'AP Fallback to Primary' section, and a red arrow points from this box to the 'Primary Controller' entry in the 'Edit AP' window.

Name	Management IP Address (IPv4/IPv6)
Primary Controller	WLC-001 10.10.10.10
Secondary Controller	
Tertiary Controller	

AP Fallback to Primary *i*
Enable

Backup Primary Controller
Name: WLC-002
IPv4/IPv6 Address: 10.10.20.10

Backup Secondary Controller
Name: Enter Name
IPv4/IPv6 Address:

Interval (sec)*: 3

The 'Edit AP' window shows the 'High Availability' tab. It contains a table for controller configuration and an 'AP failover priority' dropdown set to 'Low'. A red box highlights the 'Primary Controller' row, and a red arrow points from this box to the 'AP Fallback to Primary' section in the main configuration window.

Name	Management IP Address (IPv4/IPv6)
Primary Controller	WLC-001 10.10.10.10
Secondary Controller	
Tertiary Controller	

AP failover priority: Low

N+1 Redundancy Configuration

Edit AP Join Profile

General Client **CAPWAP** AP Management Security ICap QoS Geolocation

High Availability Advanced

CAPWAP Timers

Fast Heartbeat Timeout(sec)*	<input type="text" value="3"/>
Heartbeat Timeout(sec)*	<input type="text" value="30"/>
Discovery Timeout(sec)*	<input type="text" value="10"/>
Primary Discovery Timeout(sec)*	<input type="text" value="120"/>
Primed Join Timeout(sec)*	<input type="text" value="0"/>

Retransmit Timers

Count*	<input type="text" value="5"/>
Interval (sec)*	<input type="text" value="3"/>

AP Fallback to Primary ⓘ

Enable

Backup Primary Controller

Name

IPv4/IPv6 Address

Backup Secondary Controller

Name

IPv4/IPv6 Address

N+1 Redundancy Configuration

The screenshot displays the 'Edit AP Join Profile' configuration page, specifically the 'CAPWAP' tab. The 'High Availability' sub-tab is active. The 'CAPWAP Timers' section contains several input fields: 'Fast Heartbeat Timeout(sec)*' is set to 0 and is highlighted with a red box; 'Heartbeat Timeout(sec)*' is 30; 'Discovery Timeout(sec)*' is 10; 'Primary Discovery Timeout(sec)*' is 120; and 'Primed Join Timeout(sec)*' is 0. The 'Retransmit Timers' section shows 'Count*' as 5 and 'Interval (sec)*' as 3. On the right, the 'AP Fallback to Primary' section has an 'Enable' checkbox that is unchecked. Below it, the 'Backup Primary Controller' section has a warning icon and a tooltip that reads: 'Backup primary/secondary controller requires 'Fast Heartbeat Timeout' to be enabled. To enable 'Fast Heartbeat Timeout' configure a value other than zero second.' The 'Name' field is empty, and the 'IPv4/IPv6 Address' field contains '10.10.20.10'. The 'Backup Secondary Controller' section has a 'Name' field with the placeholder 'Enter Name' and an empty 'IPv4/IPv6 Address' field.

Fast Heartbeat Timeout(sec)* 0

Heartbeat Timeout(sec)* 30

Discovery Timeout(sec)* 10

Primary Discovery Timeout(sec)* 120

Primed Join Timeout(sec)* 0

Count* 5

Interval (sec)* 3

AP Fallback to Primary (i)

Enable

Backup Primary Controller (A)

Name

IPv4/IPv6 Address 10.10.20.10

Backup Secondary Controller

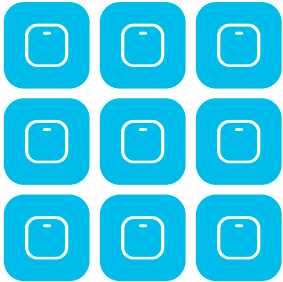
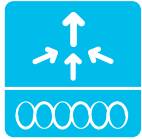
Name Enter Name

IPv4/IPv6 Address

Backup primary/secondary controller requires 'Fast Heartbeat Timeout' to be enabled. To enable 'Fast Heartbeat Timeout' configure a value other than zero second.

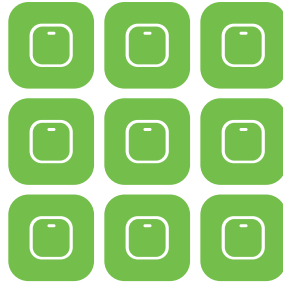
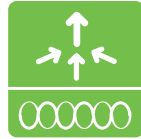
AP to Tag Mappings

Primary
9800



SSID A

Secondary
9800



SSID A

Define tag mappings via static mappings

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

AP to Tag Mappings

Configuration

Configuration > Tags & Profiles > Tags

Policy Site RF **AP**

Tag Source Static Location Filter

Priority	Tag Source	Status
0	Static	<input checked="" type="checkbox"/>
1	Location	<input checked="" type="checkbox"/>
2	Filter	<input checked="" type="checkbox"/>
3	AP	<input checked="" type="checkbox"/>

i Drag and Drop Tag Sources to change priorities

Revalidate Tag Sources on APs

Enable AP Tag Persistency

 Apply

N+1 Redundancy

Using Catalyst Center; Primary WLC

Provision / Network Devices / Provision Devices

Network Devices / Provision Devices

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

WLC-001.robm.work.lab

Serial Number: 9IAUZM8QJ9V
Devices: WLC-001.robm.work.lab

WLC Role: Active Main WLC Anchor

Managed AP location(s) **Managing 2 Primary location(s)** Select Secondary Managed AP Locations

Skip AP Provision

Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
Corp-Users	-	3			
Guest-users	-	4			

Search Hierarchy

- Global (2)
- Melbourne
 - 101-Collins
 - 03-Storeroom
 - 11-Reception
 - 12-Corp
 - 14-DataCenter

N+1 Redundancy

Using Catalyst Center; Secondary WLC

Network Devices / Provision Devices

Provision / Network Devices / Provision Devices

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

WLC-002.robm.work.lab

Serial Number: 905LRS91OR1
Devices: WLC-002.robm.work.lab

WLC Role: Active Main WLC Anchor

Managed AP location(s): **Managing 2 Secondary location(s)**

Skip AP Provision

In case of update in associated Wireless profile(s), Re-provisioning of HA-paired controller(s) is/are required.

Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
Corp-Users	-	3			
Guest-users	-	4			

Search Hierarchy

- Global (2)
- Melbourne
 - 101-Collins
 - 03-Storeroom
 - 11-Reception
 - 12-Corp
 - 14-DataCenter

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

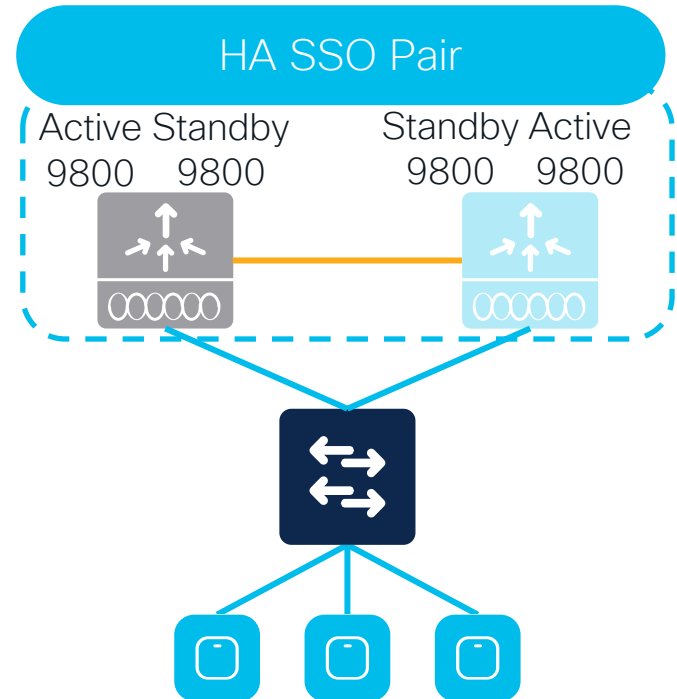
RF Tag

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

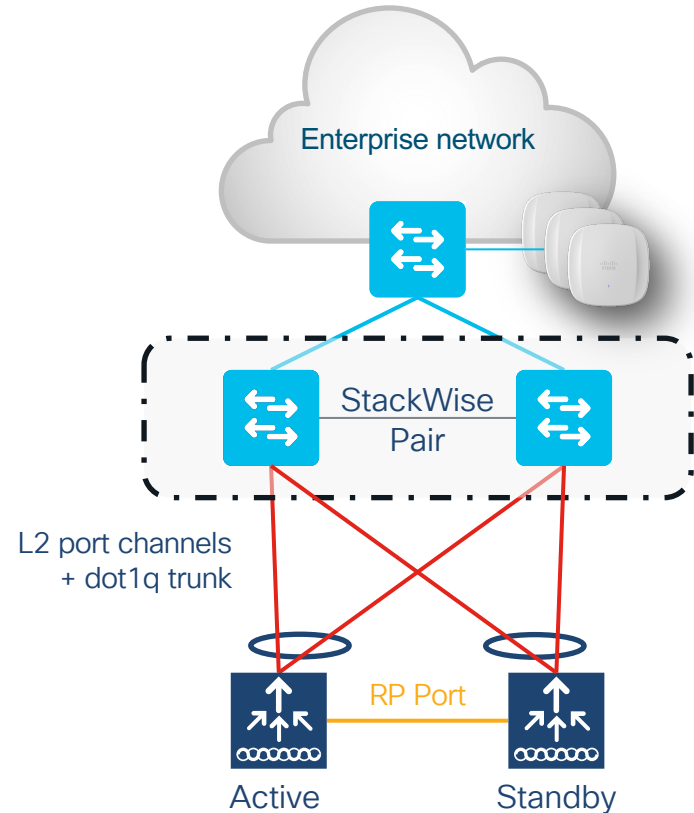


AP failover takes order of sub seconds

Stateful Switchover (SSO)

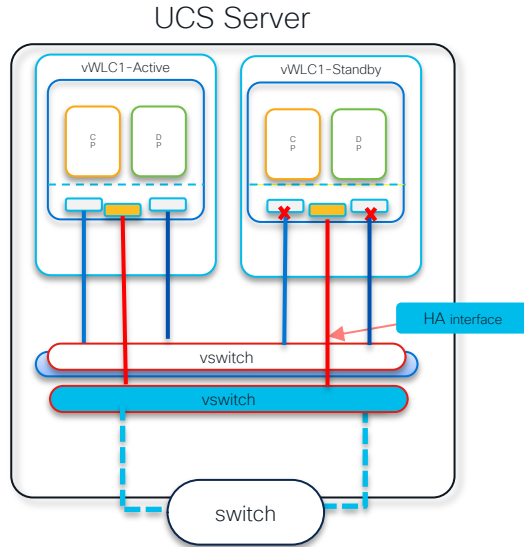
Redundancy Port (RP)

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

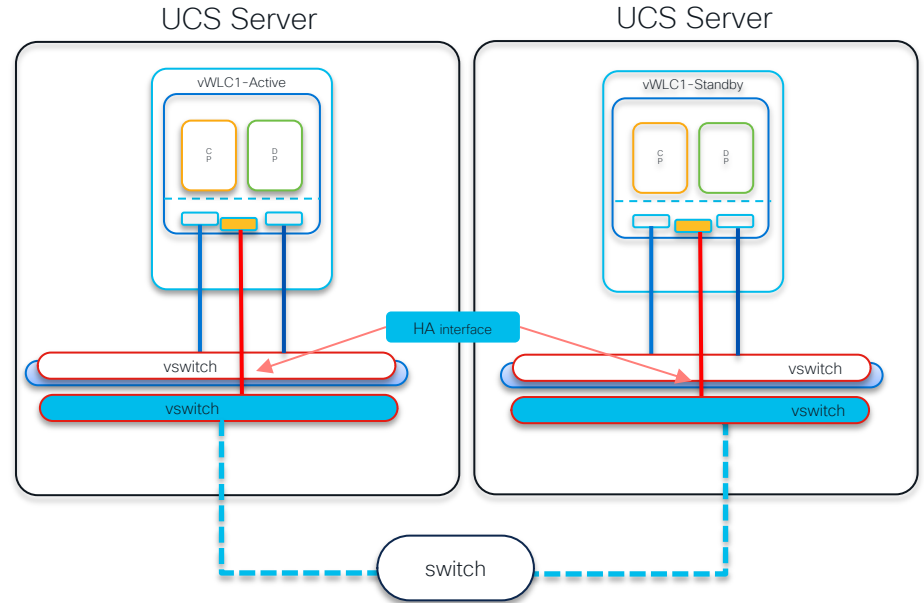


Stateful Switchover (SSO)

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



Intra-Host Redundancy



Inter-Host Redundancy

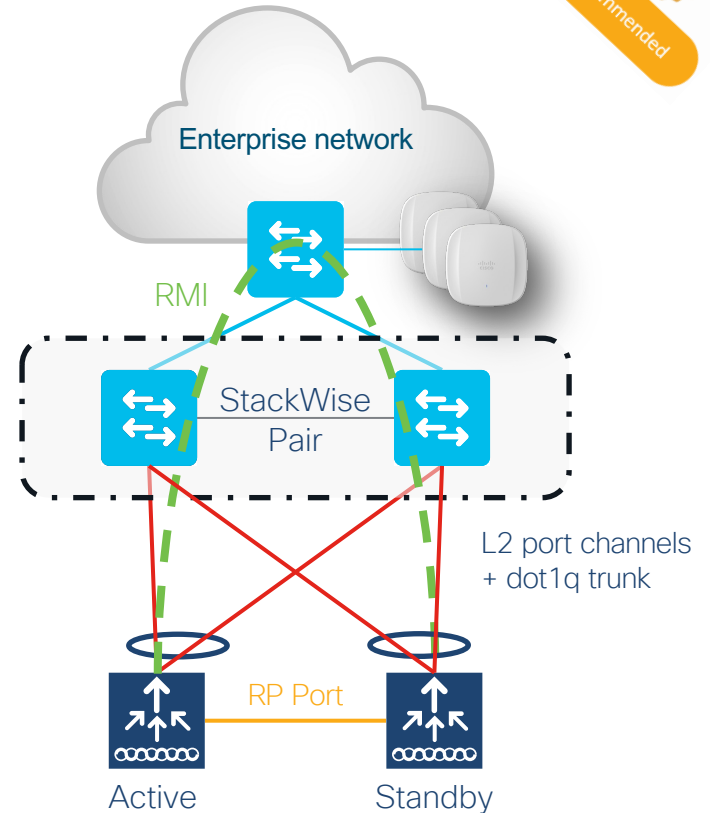
Stateful Switchover (SSO)

Redundancy Management Interface (RMI)



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



Administration > Device

General

FTP/SFTP/TFTP

Redundancy

Redundancy Configuration **ENABLED**

Redundancy Pairing Type RMI+RP RP

RMI IP for Chassis 1* 10.10.10.11

RMI IP for Chassis 2* 10.10.10.22

HA Interface GigabitEthernet3

Management Gateway Failover **ENABLED**

Gateway Failure Interval (seconds) 8

Local IP NA

Remote IP NA

Wireless Management Interface Vlan10

Keep Alive Timer 1 x 100 (milliseconds)

Keep Alive Retries 5

Chassis Renumber 1

Active Chassis Priority* 2

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

Monitoring > General > System

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	2	Standby Failures	0
Redundant Mode (Operational)	sso	Switchovers System Experienced	3
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	Device Uptime
1	Standby	000c.29e0.4466	2	V02	Ready	169.254.10.11	10.10.10.11	0000.0000.0000	17.12.1	0 minutes
*2	Active	000c.29a9.5a2e	1	V02	Ready	169.254.10.22	10.10.10.22	001e.bd1a.52ff	17.12.1	4 minutes

Switchover Details

Index	Previous Active	Current Active	Switch Over Time	Switch Over Reason
1	1	2	11:03:06 AEST Mon Oct 2 2023	user forced
2	2	1	11:14:57 AEST Mon Oct 2 2023	user forced
3	1	2	11:23:40 AEST Mon Oct 2 2023	Active lost GW

Stateful Switchover (SSO)

Using Catalyst Center

The screenshot shows the 'Provision / Inventory' page in Cisco Catalyst Center. At the top, there are navigation tabs for 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. Below this, a search bar and a 'Devices (14)' header are visible. A table lists several devices, with 'WLC-001.robm.work.lab' selected. A context menu is open over this device, showing options like 'Inventory', 'Software Image', 'Provision', 'Telemetry', 'Device Replacement', 'Compliance', and 'More'. The 'Provision' option is expanded, showing sub-options: 'Assign Device to Site', 'Provision Device', 'Configure WLC HA' (highlighted with a red box), 'Configure WLC Mobility', and 'Manage LED Flash Status'. The table columns include 'Device Name', 'IP Address', 'Inventory', 'EoX Status', and 'Manageability'.

Device Name	IP Address	Inventory	EoX Status	Manageability
WLC-Chassis-2-SSO.robm.work.lab	10.10.22.2			Managed
WLC-002.robm.work.lab	10.10.12.2			Managed
WLC-001.robm.work.lab	10.10.22.2			Managed
RobM-Lab-Backbone.robm.work.lab	10.67.53.194	Cisco	Ready	Managed

Stateful Switchover (SSO)

Using Catalyst Center

The screenshot shows the 'High Availability' configuration page in Cisco Catalyst Center. The page is titled 'Provision / Inventory' and includes a user profile 'admin'. A left-hand navigation pane shows a list of 14 devices, with 'WLC-001.robm.work.lab' selected. The main configuration area is for a 'Primary C9800' (WLC-001.robm.work.lab) and a 'Secondary C9800' (WLC-Chassis-2-SSO.robm.work.lab). The configuration includes fields for 'Select Primary Interface' (GigabitEthernet3), 'Select Secondary Interface' (GigabitEthernet3), 'Redundancy Management IP*' (10.10.22.11), and 'Peer Redundancy Management IP*' (10.10.22.12). A 'Netmask*' field is set to /24 (255.255.255.0). A red box highlights the 'Select Secondary C9800' dropdown menu, which shows 'WLC-Chassis-2-SSO.robm.work.lab' and 'Device IP: 10.10.22.22'. A warning message at the top states: 'Please make sure the Redundancy Management IP and Peer Redundancy Management IP are not assigned to any other network entities. If used, kindly change the IP accordingly and configure.'

Stateful Switchover (SSO)

Using Catalyst Center

The screenshot shows the Catalyst Center Provisioning interface. At the top, there is a 'Provision' header and navigation tabs for 'All', 'Routers', and 'Switches'. Below this, a 'Devices (13)' section is visible with a search bar and filter options. A table lists the devices, with 'WLC-001.robm.work.lab' highlighted in a red box. A red arrow points from this device to a 'Redundancy Summary' modal window on the right. The modal window displays the following details:

Property	Value
Primary WLC:	WLC-001.robm.work.lab
Secondary WLC:	WLC-Chassis-2-SSO.robm.work.lab
Unit MAC:	00:50:56:82:c2:0f
Redundancy State:	SSO
Mobility MAC:	00:1e:bd:76:a2:ff
Sync Status:	Duplex
Primary Chassis Serial No:	94LWEF9XQ66
Secondary Chassis Serial No:	9ZIYWSBRI8Q
Active RMI IP:	10.10.22.11
Standby RMI IP:	10.10.22.12
Gateway Monitoring:	Enabled
Recovery mode:	Not Applicable

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

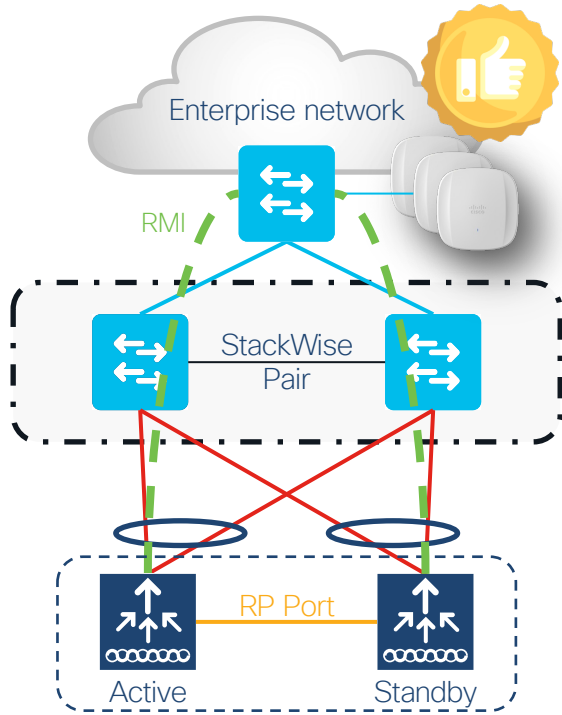
Configurations

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

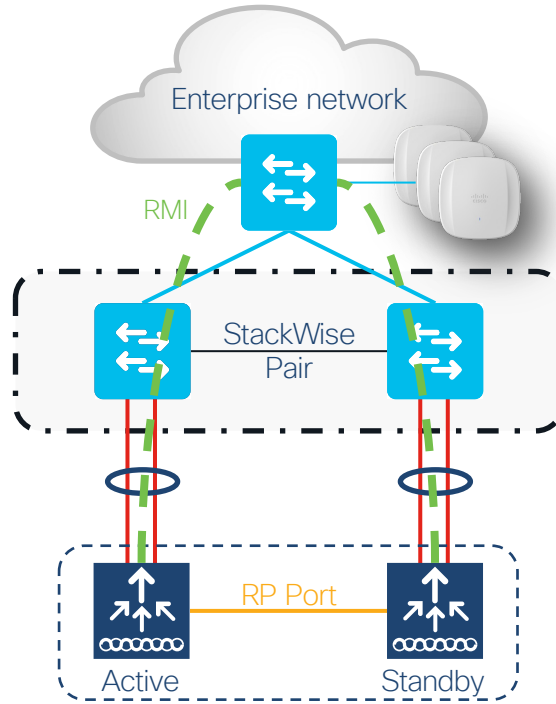
Upstream Switch & Link Level Redundancy



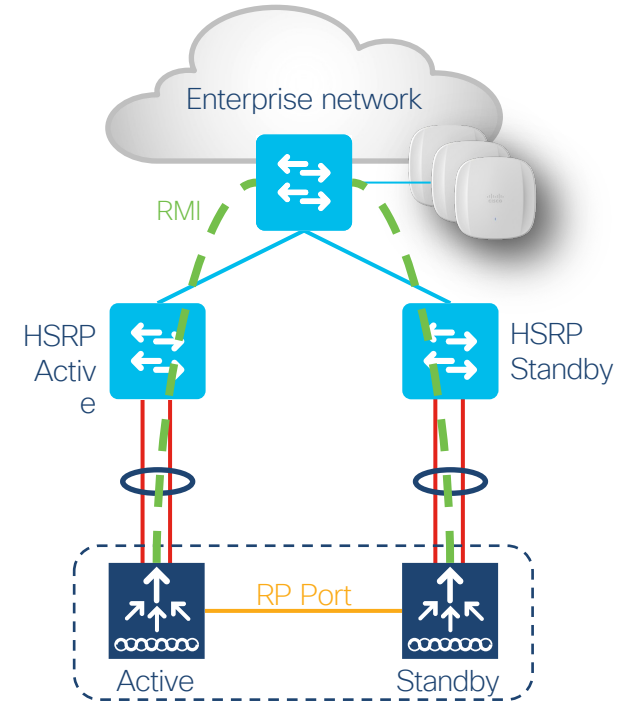
Supported Topologies



StackWise Pair with Split links



StackWise Pair without Split links

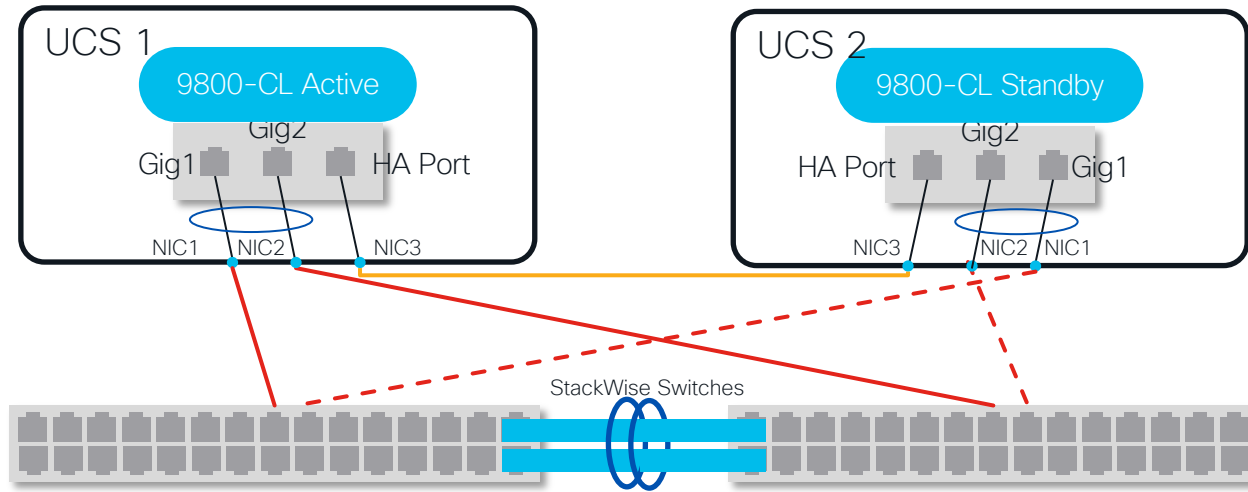


HSRP

9800-CL Port Channel

Link Level Connections

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



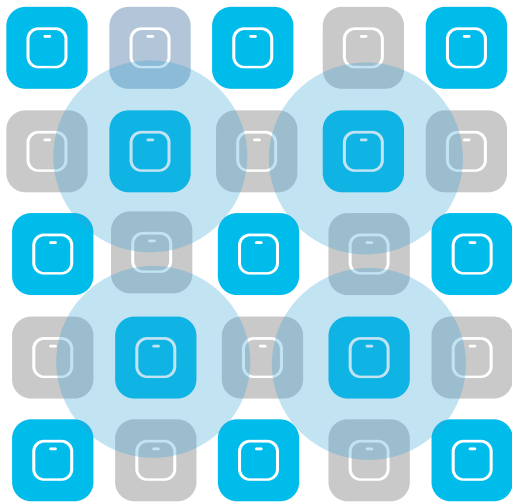
Software Upgrades; ISSU & N+1 Hitless

Rolling AP Upgrades

Rolling AP Upgrade

Neighbor Marking

25%



Rolling AP Upgrades

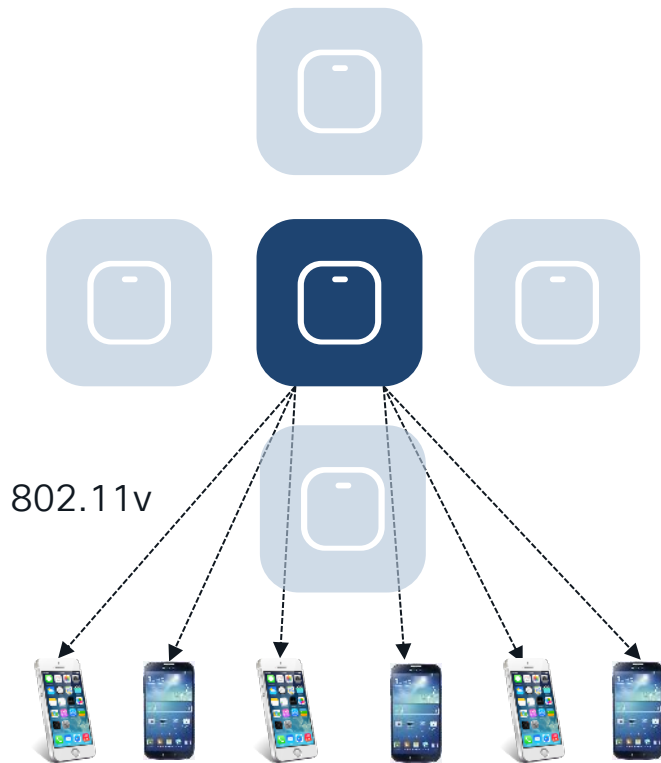
Client Steering

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

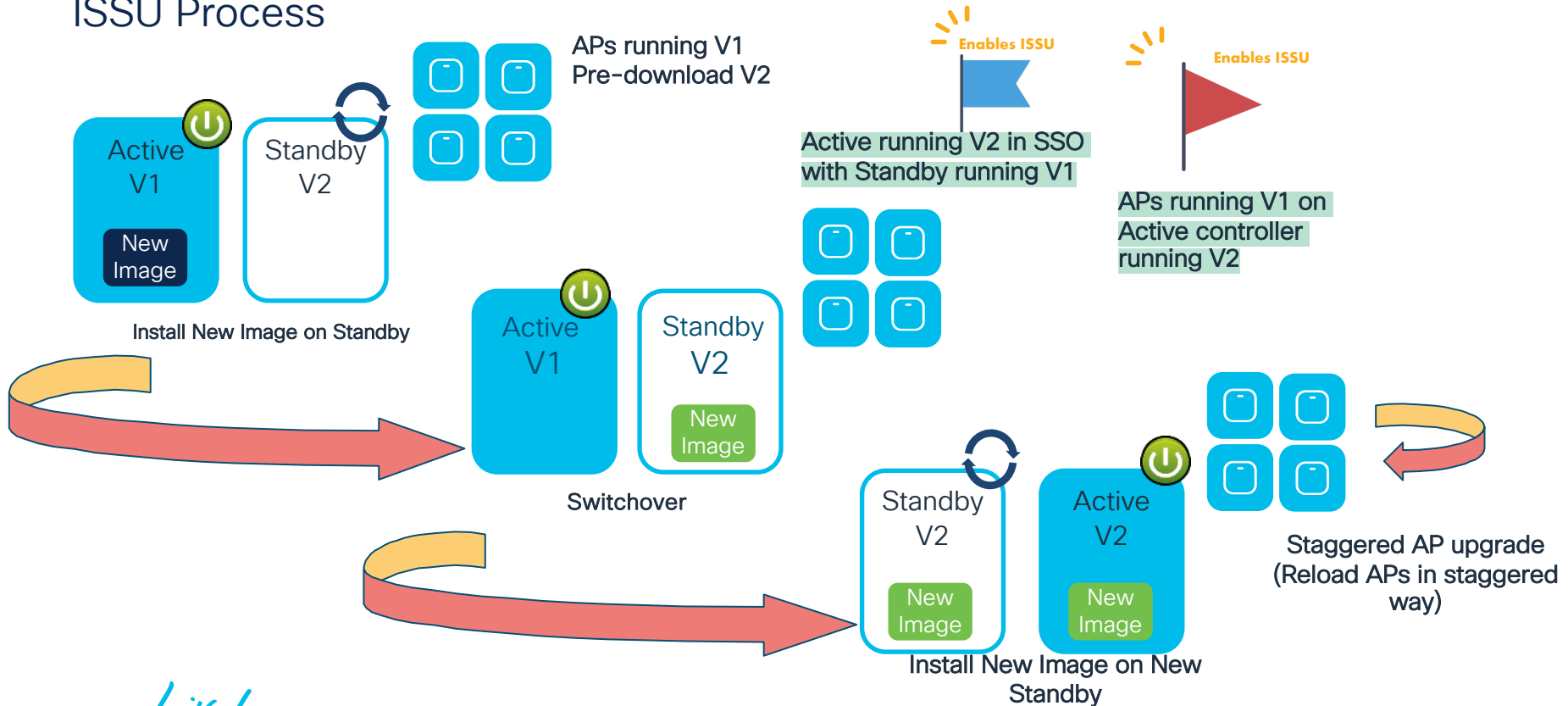


Pre-requisites:

- ✓ 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

Administration > Software Management

Software Upgrade

Software Maintenance Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

Upgrade Mode: INSTALL (Current Mode (until next reload): INSTALL)

Transport Type: My Desktop

File System: bootflash (Free Space: 9253.40 MB)

Source File Path*: C9800-CL-universalk9.17.12.01.SPA.bin

ISSU Upgrade (HA Upgrade)

Override ISSU Compatibility Check

Auto terminate timer (hours): 06:00

AP Upgrade Configuration

AP Upgrade per Iteration: 25 %

Client Steering

Client Deauthentication

Download & Install

Manage

[Remove Inactive Files](#)

[Rollback](#)

In Service Software Upgrades (ISSU)

ISSU; Monitoring the Process

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: Current Mode (until next reload): INSTALL

Transport Type:

File System: Free Space: 6780.36 MB

Source File Path*:

ISSU Upgrade (HA Upgrade)

Override ISSU Compatibility Check

Auto terminate timer: 05:38:03

AP Upgrade Configuration

AP Upgrade per Iteration:

Client Steering

Client Deauthentication

Status

- ✓ Download Image/Package
- ✓ Install Image/Package
- ✓ AP Image Predownload
 - Total: 4
 - 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: 25

[Show Logs](#)
[AP Upgrade Statistics](#)

In Service Software Upgrades (ISSU)

ISSU; Monitoring the Process

Software Upgrade

Software Maintenance Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

Upgrade M

Transport T

File System

Source File

ISSU Upgra
(Upgrade)

Override IS
Compatibili

Auto termin

AP Upgra

AP Upgra

Client Steer

Client Deau

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

AP Upgrade Statistics

Upgrade Status : In Progress
Percentage Complete : 50

From Version : 17.11.0.155
To Version : 17.12.1.5
Started at : 10/03/2023 19:47:46 AEDT
Expected time of completion : 10/03/2023 19:53:46 AEDT

Client Steering : Enabled
Client Deauthentication : Enabled

Number of APs
Upgraded : 2
In Progress : 1
Remaining : 1

AP Name	Radio MAC	Status
AP0CD0.F894.3C64	0cd0.f896.afe0	Upgraded and Joined
APF4DB.E618.1E7C	f4db.e615.8c20	Upgraded and Joined
AP0CD0.F894.391C	0cd0.f896.95a0	In-Progress
APF4BD.9E9A.0574	084f.f983.e540	Remaining

10 1 - 4 of 4 items

Download & Install Commit ISSU Terminate

Status

- ✓ Download Image/Package
- ✓ Install Image/Package
- ✓ AP Image Predownload
Total: 4
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: 50
- Commit

[Show Logs](#)
[AP Upgrade Statistics](#)

In Service Software Upgrades (ISSU)

Using Catalyst Center

The screenshot shows the 'Provision / Inventory' page in Cisco Catalyst Center. At the top, there are navigation tabs for 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. Below this, the page displays 'Devices (12)' with a 'Focus: Inventory' dropdown. A search bar is present with the text 'Click here to apply basic or advanced filters or view recently applied filters'. Below the search bar, there are action buttons: '1 Selected', 'Tag', '+ Add Device', 'Edit Device', 'Delete Device', and 'Actions'. The 'Actions' menu is open, showing options like 'Inventory', 'Software Image', 'Provision', 'Telemetry', 'Device Replacement', 'Compliance', and 'More'. The 'Software Image' option is selected, and its sub-menu is open, with 'Image Update' highlighted by a red box. Other sub-menu items include 'Image Update Status', 'Download Update Readiness Report', and 'Check Image Update Readiness'. The background shows a table of devices with columns for 'Device Name', 'IP Address', and 'Manageability'. The first device, 'WLC-001.robm.work.lab', is selected.

Device Name	IP Address	Manageability
WLC-001.robm.work.lab	10.10.22...	Managed
RobM-Lab-Backbone.robm.work.lab	10.67.53...	Managed
DNAC-Router.robm.work.lab	10.10.10...	Managed
AP4-9117	10.10.20...	Not Scanned

In Service Software Upgrades (ISSU)

Using Catalyst Center

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** ^

<input checked="" type="checkbox"/>	Device Name ^	IP Address	Enable ISSU Update	Device Series	Device Role	Current Image	Update Image ●	Comment
<input checked="" type="checkbox"/>	WLC-001.robm.work.lab	10.10.22.2	Disable ISSU Update	01-C...	Cisco Catalyst 9800 Wire...	Access	C9800-CL-universalk9.17.0... ISSU	✔ ISSU Validation Successful Update Readiness Report

In Service Software Upgrades (ISSU)

Using Catalyst Center

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** ▼

<input checked="" type="checkbox"/>	Device Name ▲	IP Address	Site	Device Series	Device Role	Current Image	Update Image ●	Comment
<input checked="" type="checkbox"/>	WLC-001.robm.work.lab	10.10.22.2	Global/Melbourne/101-C...	Cisco Catalyst 9800 Wire...	Access	C9800-CL-universalk9.17.0...	C9800-CL-universalk9.17.0... ISSU	● ISSU Validation Successful Update Readiness Report

ISSU Enabled. Device will be updated using ISSU.

In Service Software Upgrades (ISSU) Using Catalyst Center

The screenshot displays the Catalyst Center interface for an ISSU operation. The breadcrumb navigation at the top reads "Provision / Inventory / Image Update Status". The main header shows the device "WLC-001.robm.work.lab (10.10.22.2) Image Update" with a close button. Below this, the operation details are: "Date: Oct 4, 2023 3:58 PM", "Duration: 56 minutes 41 seconds", and "Status: Successfully updated with C9800-CL-universalk9.17.09.04.SPA.bin".

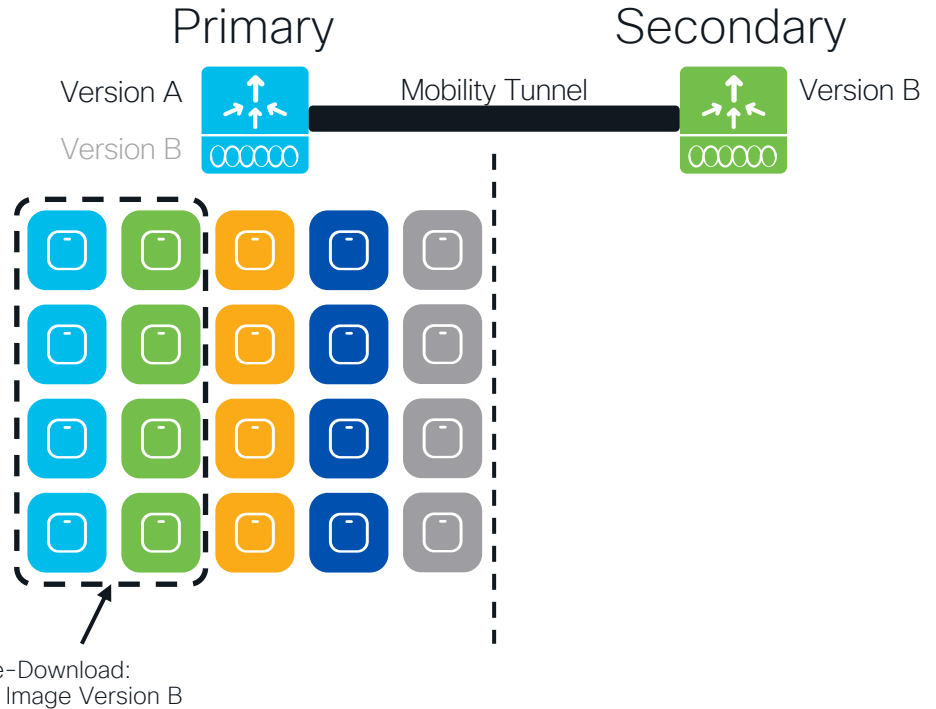
The "Operations" tab is active, showing a vertical timeline of steps. The "Activation" step is expanded and highlighted with a red box, indicating it is the current focus. The "Activation" step is completed and took 41 minutes 22 seconds. The steps in the timeline are:

- Pre Activation Operation (1 second)
- Image Activation (18 minutes 17 seconds)
- Staggered AP Upgrade (22 minutes 1 second)
- Install Commit (45 seconds)
- Remove Inactive Images (7 seconds)
- Collect Running Image Details (8 seconds)
- Verify Image Activation (1 second)
- Post Activation Operation

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:

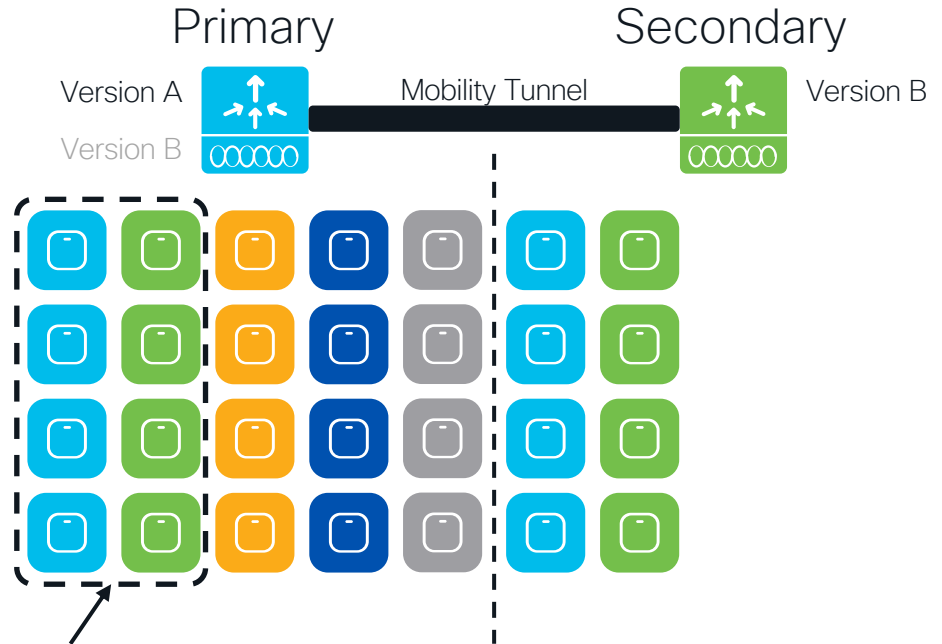


N+1 Site Based Hitless Upgrade

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.



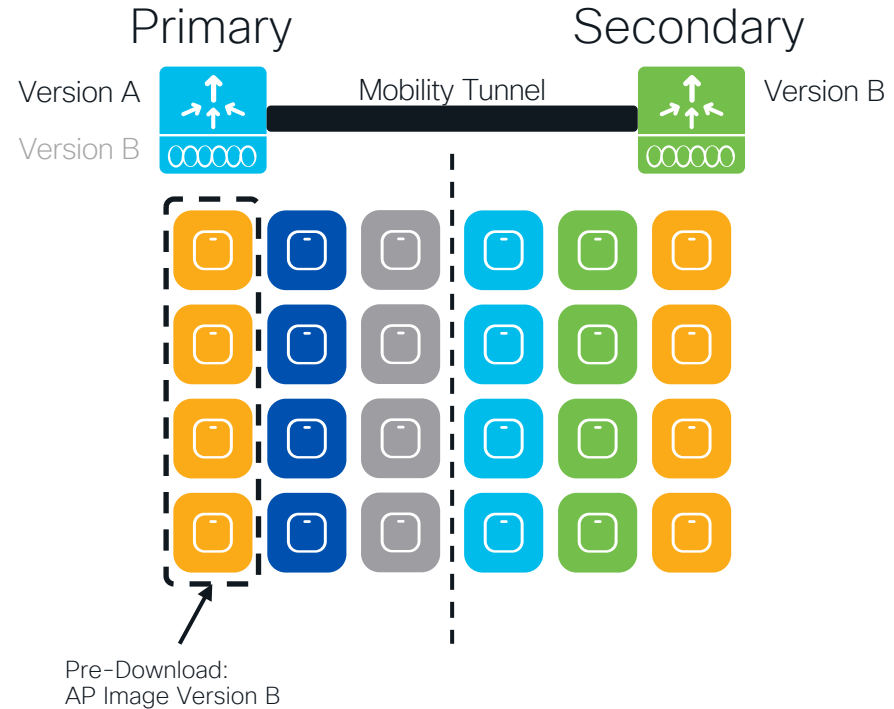
Pre-Download:
AP Image Version
B

N+1 Site Based Hitless Upgrade

7 Add further sites to the site filter:

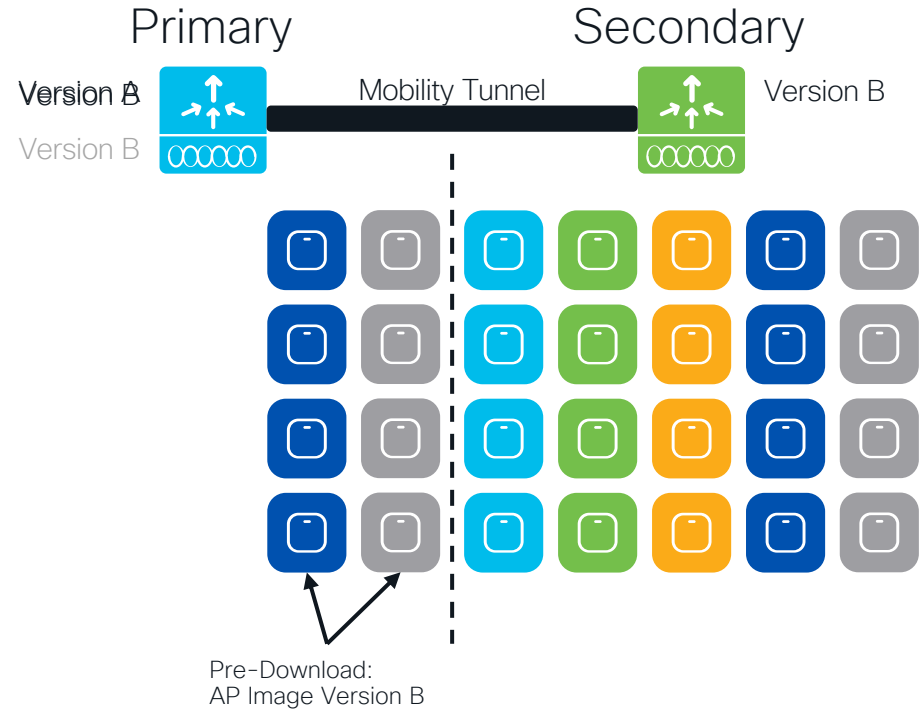
8 Initiate the AP image pre-download, reload with the new image, and join to the Secondary WLC in rolling fashion

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

Administration > Software Management

Software Upgrade

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

Upgrade Mode: Current Mode (until next reload): INSTALL

One-Shot Install Upgrade

Transport Type:

File System: Free Space: 6667.79 MB

Source File Path*

AP Image Predownload

Hitless Software Upgrade (N + 1 Upgrade)

Enable Hitless Upgrade

[Download & Install](#) [Save Configuration & Activate](#)

Manage

- [Remove Inactive Files](#)
- [Rollback](#)

N+1 Site Based Hitless Upgrade Configuration

Administration > Software Management

Software Upgrade

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

Upgrade Mode: Current Mode (until next reload): INSTALL

Transport Type:

File System: Free Space: 6667.79 MB

Source File Path*

Hitless Software Upgrade (N + 1 Upgrade)

Enable Hitless Upgrade

Site Filter:

Site Tags*:

Controller IP Address (IPv4/IPv6)*:

Controller Name*:

AP Upgrade Configuration

AP Upgrade per Iteration:

Client Steering

Client Deauthentication

Accounting Percentage:

Accounting Action:

Iteration Expiry:

[Manage](#)

[Remove Inactive Files](#)

[Rollback](#)

N+1 Site Based Hitless Upgrade Verification

Administration > Software Management

Software Upgrade

Software Maintenance Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

Upgrade Mode: INSTALL (Current Mode (until next reload): INSTALL)

Transport Type: My Desktop

File System: bootflash (Free Space: 7895.16 MB)

Source File Path*: C9800-CL-universalk9.17.12.01.SPA.bin

Hitless Software Upgrade (N + 1 Upgrade)

Enable Hitless Upgrade:

Site Filter: Custom

Site Tags*: Site-1, Site-2

Controller IP Address (IPv4/IPv6)*: 10.10.20.10

Controller Name*: WLC-002

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

Status

- ✓ Download Image/Package
C9800-CL-universalk9.17.12.01.SPA.bin
- ✓ Install Image/Package
- ✓ Update Site Filter
- ✓ AP Image Predownload
Total: 1
Initiated: 0
Predownloading: 0
Completed predownloading: 2
Failed to predownload: 0
- ⚙️ AP Image Upgrade and Move...
Percentage complete: 0
- Activate Image/Package
- Commit

[Show Logs](#)
[AP Upgrade Statistics](#)

N+1 Site Based Hitless Upgrade Verification

The screenshot displays a network management interface with several sections:

- Upgrade Mode:** INSTALL (Current Mode until next reload): INSTALL
- Transport Type:** My Desktop
- File System:** bootflash (Free Space: 7895.16 MB)
- Source File:** AP Upgrade Statistics (modal window)
- Hitless Section:** Includes fields for Enable Hitless Upgrade, Site Filter, Site Tags*, and Controller (IPv4/IPv6).
- AP Upgrade Table:** A table listing APs with columns for AP Name, Radio MAC, and Status.
- Status Panel:** Shows progress for Download Image/Package, Install Image/Package, Update Site Filter, and AP Image Predownload. Includes a link for AP Upgrade Statistics.

AP Upgrade Statistics Modal Window:

Upgrade Status : In Progress
Percentage Complete : 50

From Version : 17.9.4.27
To Version : 17.12.1.5

Started at : 09/25/2023 10:55:14 AEST
Expected time of completion : 09/25/2023 11:01:14 AEST

Number of APs

Upgraded	: 1
In Progress	: 1
Remaining	: 0

AP Upgrade Table:

AP Name	Radio MAC	Status
AP0CD0.F894.3C64	0cd0.f896.afe0	Upgraded and Joined Member
APF4DB.E618.1E7C	f4db.e615.8c20	In-Progress

1 - 2 of 2 Items

Status Panel:

- Download Image/Package
C9800-CL-universalk9.17.12.01.SPA.bin
- Install Image/Package
- Update Site Filter
- AP Image Predownload
Total: 1
Initiated: 0
Predownloading: 0
Completed predownloading: 2
Failed to predownload: 0

AP Image Upgrade and Move...
Percentage complete: 50

Activate Image/Package
Commit

[Show Logs](#)
[AP Upgrade Statistics](#)


N+1 Site Based Hitless Upgrade

Verification

Hitless Software Upgrade (N + 1 Upgrade)

Enable Hitless Upgrade

Site Filter

Site Tags* 

Controller IP Address (IPv4/IPv6)*

Controller Name*

AP Upgrade Configuration

AP Upgrade per Iteration

Client Steering

Accounting Percentage

Accounting Action

Iteration Expiry

N+1 Hitless Upgrade

Using Catalyst Center

Devices (13) Focus: [Inventory](#) ▾

🔍 Click here to apply basic or advanced filters or view recently applied filters

1 Selected Tag [+](#) Add Device [✎](#) Edit Device [🗑](#) Delete Device **Actions** [^](#) [ⓘ](#)

<input type="checkbox"/>	<input type="checkbox"/>	Device Name ▾	IP Address	Inventory	Provisionability ⓘ	EoX Status ⓘ
<input type="checkbox"/>	<input type="checkbox"/>	WLC-002.robm.work.lab	10.10.12...			
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WLC-001.robm.work.lab	10.10.22...			
<input type="checkbox"/>	<input type="checkbox"/>	RobM-Lab-Backbone.robm.work.lab	10.67.53...			
<input type="checkbox"/>	<input type="checkbox"/>	DNAC-Router.robm.work.lab	10.10.10...	Cisco	🟢	Rea

- Inventory >
- Software Image >
- Provision >**
 - Assign Device to Site
 - Provision Device
 - Configure WLC HA
 - Configure WLC Mobility**
 - Manage LED Flash Status
- Telemetry >
- Device Replacement >
- Compliance >
- More >

N+1 Hitless Upgrade

Using Catalyst Center

Configure Mobility Group

Mobility Group Name* **CL-Test-1** RF Group Name* **default** Data Link Encryption

DTLS High Cipher Only Restart for DTLS Ciphers to take effect

Mobility Peers + Add

Search

Delete 0 Selected As of: Sep 26, 2023 9:17 PM

Device Name	IP Address	MAC Address	Manageability	Hash	Mobility Group Name
<input type="checkbox"/> WLC-002.robm.work.lab	10.10.12.2	00:1e:49:eb:2c:ff	Managed		CL-Test-1

Devices (13) Focus: Inventory

1 Selected Tag + Add Device

Device Name

- WLC-002.robm.work
- WLC-001.robm.work
- RobM-Lab-Backbon
- DNAC-Router.robm.v

N+1 Hitless Upgrade

Using Catalyst Center

Network Devices / Provision Devices

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

[Select Secondary Managed AP Locations](#)

Skip AP Provision ⓘ

Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
Corp-Users ⓘ	-	3			
Guest-users ⓘ	-	4			

2 Record(s) Show Records: 25 ▾ 1 - 2 < ⓘ >

Rolling AP Upgrade

AP Reboot Percentage

Enable 25 ▾ ⓘ

N+1 Hitless Upgrade

Using Catalyst Center

The screenshot displays the Cisco Catalyst Center interface for managing devices. At the top, there are navigation tabs: All (selected), Routers, Switches, Wireless Controllers, Access Points, and Sensors. Below this, the 'Devices (13)' section is shown with a 'Focus: Inventory' dropdown. A search bar is present with the text 'Click here to apply basic or advanced filters or view recently applied filters'. Below the search bar, there are action buttons: '1 Selected', 'Tag', '+ Add Device', 'Edit Device', 'Delete Device', and 'Actions'. The 'Actions' menu is open, showing options: Inventory, Software Image (highlighted), Provision, Telemetry, Device Replacement, Compliance, and More. The 'Software Image' sub-menu is also open, showing options: Image Update (highlighted with a red box), Image Update Status, Download Update Readiness Report, and Check Image Update Readiness. In the background, a table lists devices with columns for Device Name, IP Address, and others. The device 'WLC-001.robm.work.lab' is selected, and a red arrow points to it.

Device Name	IP Address	Inventory	Provisionability	EoX Status	Manageability
WLC-002.robm.work.lab	10.10.12...				
WLC-001.robm.work.lab	10.10.22...				
RobM-Lab-Backbone.robm.work.lab	10.67.53...				

N+1 Hitless Upgrade

Using Catalyst Center

Navigation tabs: All (selected), Routers, Switches, Wireless Controllers, Security and VPN, Sensors

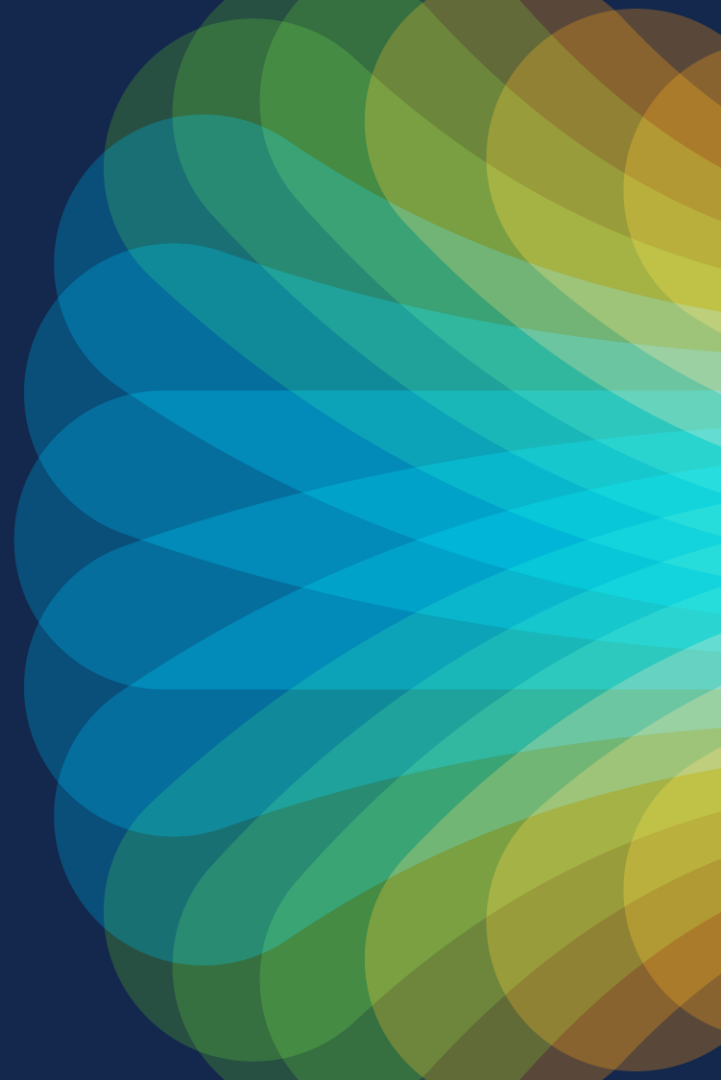
Devices Updates

Update Status: All (15) | In Progress (1) | Waiting (0) | Terminated (0) | Success (13) | Failure (1)

0 Selected | [Retry](#) | [Upcoming Tasks](#) | As of: Sep 26, 2023 9:36 PM [Refresh](#)

<input type="checkbox"/>	Device Name	Device Family	Date Updated	Duration	Image Version	Task Name	Status	Actions
<input type="checkbox"/>	WLC-001.robm.wor k.lab (10.10.22.2) Refresh	Wireless Controller	Sep 26, 2023	13 minutes 43 seconds	17.12.01.0.80	WLC-001-Image-Upgrade	<div style="border: 2px solid red; padding: 5px;"><div style="display: flex; align-items: center;"><div style="width: 50%; height: 10px; background-color: #0070C0; margin-right: 5px;"></div><div style="margin-left: 5px;">50%</div></div><p>Activating C9800-CL-Univers...</p></div>	Retry

Software Patching Capabilities



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



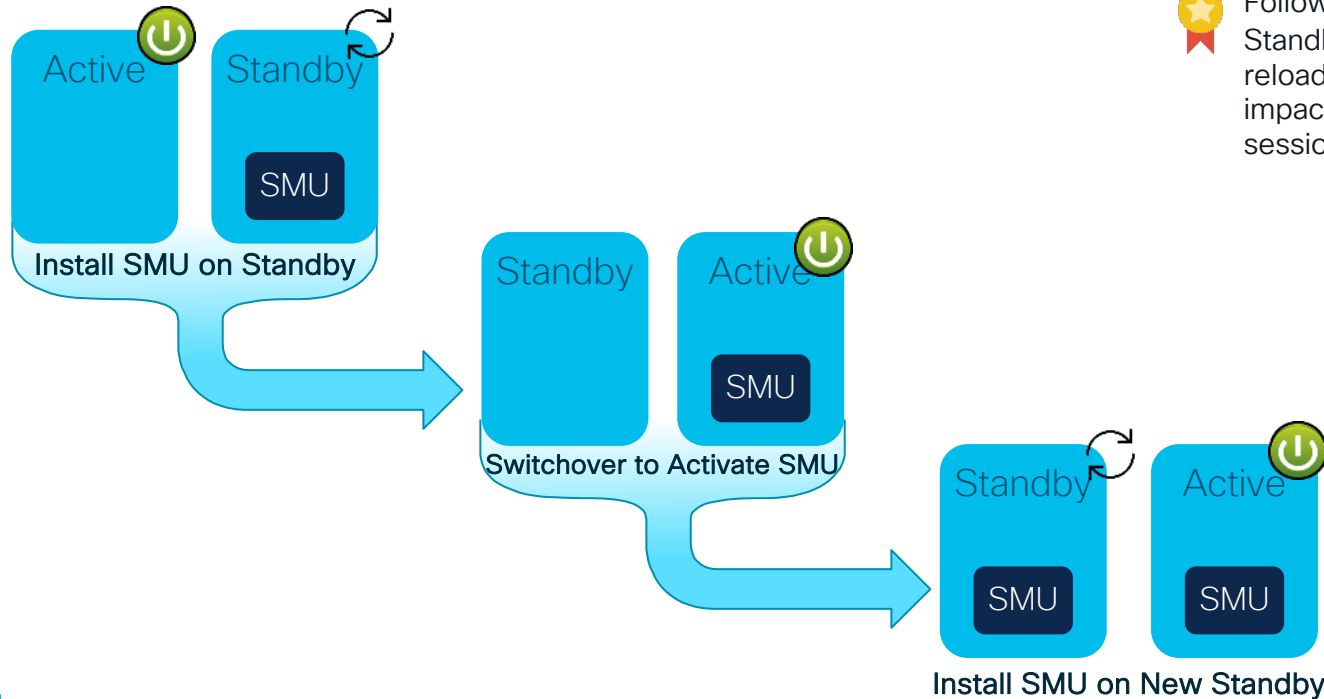
SMU activation applies patch on Active & Standby. There is no controller reload and there is no impact to AP and Client sessions.



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

Administration > Software Management

Software Upgrade

Software Maintenance Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

+ Add

Rollback

Type	State	Filename
No items to display		

Auto terminate timer: inactive

Software Maintenance Update (SMU)

SSO

Administration > Software Management

Software Upgrade

Software Maintenance Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

[+ Add](#) [Rollback](#)

Type	State	Filename
<input type="radio"/> SMU	Activated and Committed	bootflash:C9800-CL-universalk9.17.09.01.CSCwc60273.SPA.smu.bin

1 - 1 of 1 items

Auto terminate timer: inactive

```
INSTALL COMMIT OPERATION:
Initiating INSTALL_COMMIT operation
install_commit: START Thu Oct 5 11:29:46 AEDT 2023
install_commit: Committing SMU
Executing pre scripts....
Executing pre scripts 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-CL-universalk9.17.09.01.CSCwc6027
3.SPA.smu.bin Thu Oct 5 11:29:54 AEDT 2023
```

AP Service Pack (APSP)



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



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



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



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



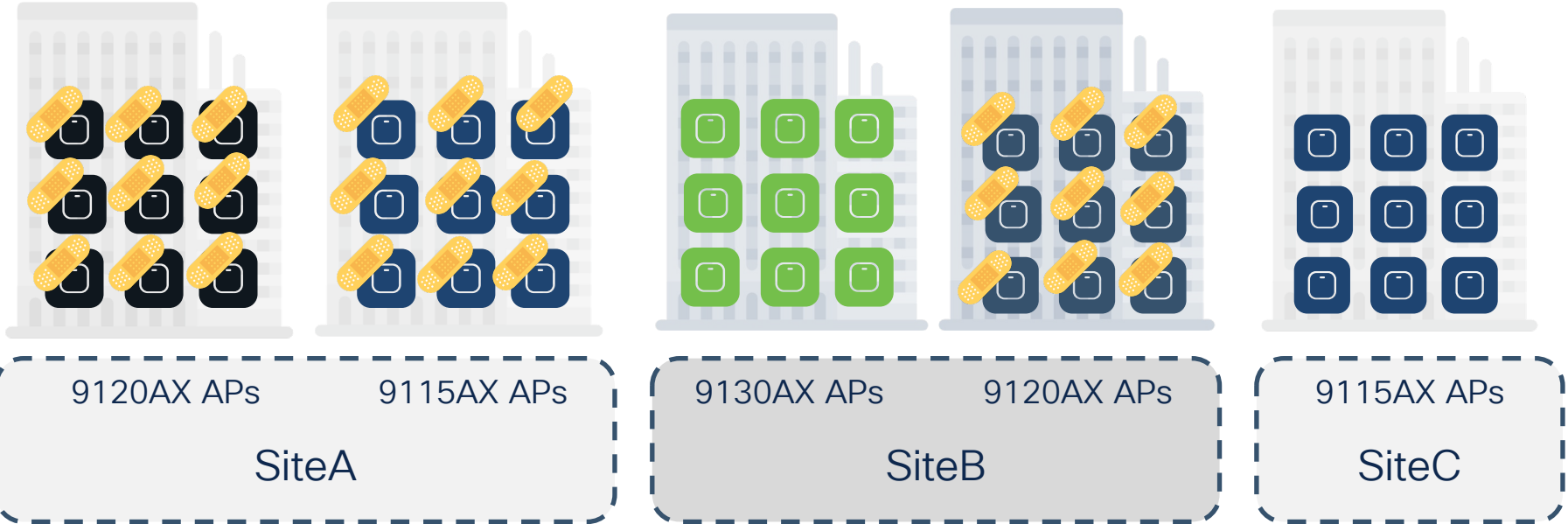
Controlled Propagation
Enables user to control the propagation of APSP in the network

AP Service Pack (APSP)

Per-Site / Per-Model Workflow

Apply on Site A in rolling AP fashion

Not applicable for building with 9130AX



AP Service Pack (APSP) Configuration

Administration > Software Management

Software Upgrade

Software Maintenance Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

+ Add

Type	State	Filename	Site
APSP	Inactive	bootflash:C9800-CL-universalk9.17.09.04.CSCwh28727.SPA.apsp.bin	Not

Auto terminate timer: inactive

AP Upgrade Configuration

AP Upgrade per Iteration: 25 %

Apply

Edit Site Filters

Filename* bootflash:C9800-CL-universalk9.17.09.04.CSCwh28727.SPA.apsp.bin

State* Inactive

Site Filter: Custom

Site Tags*: SiteTag-1, SiteTag-2

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 - 4 of 4 items

AP Service Pack (APSP)

Verification

Administration > Software Management

Software Upgrade

Software Maintenance Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

+ Add Commit Rollback Terminate

Type	State	Filename	Site Filter
<input checked="" type="radio"/> APSP	Activated and Uncommitted	bootflash:C9800-CL-universalk9.17.09.04.CSCwh28727.SPA.apsp.bin	All Sites

1 - 1 of 1 items

Auto terminate timer: active , time before rollback - 05:59:52

AP Upgrade Configuration

AP Upgrade per Iteration

25 %

Apply

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

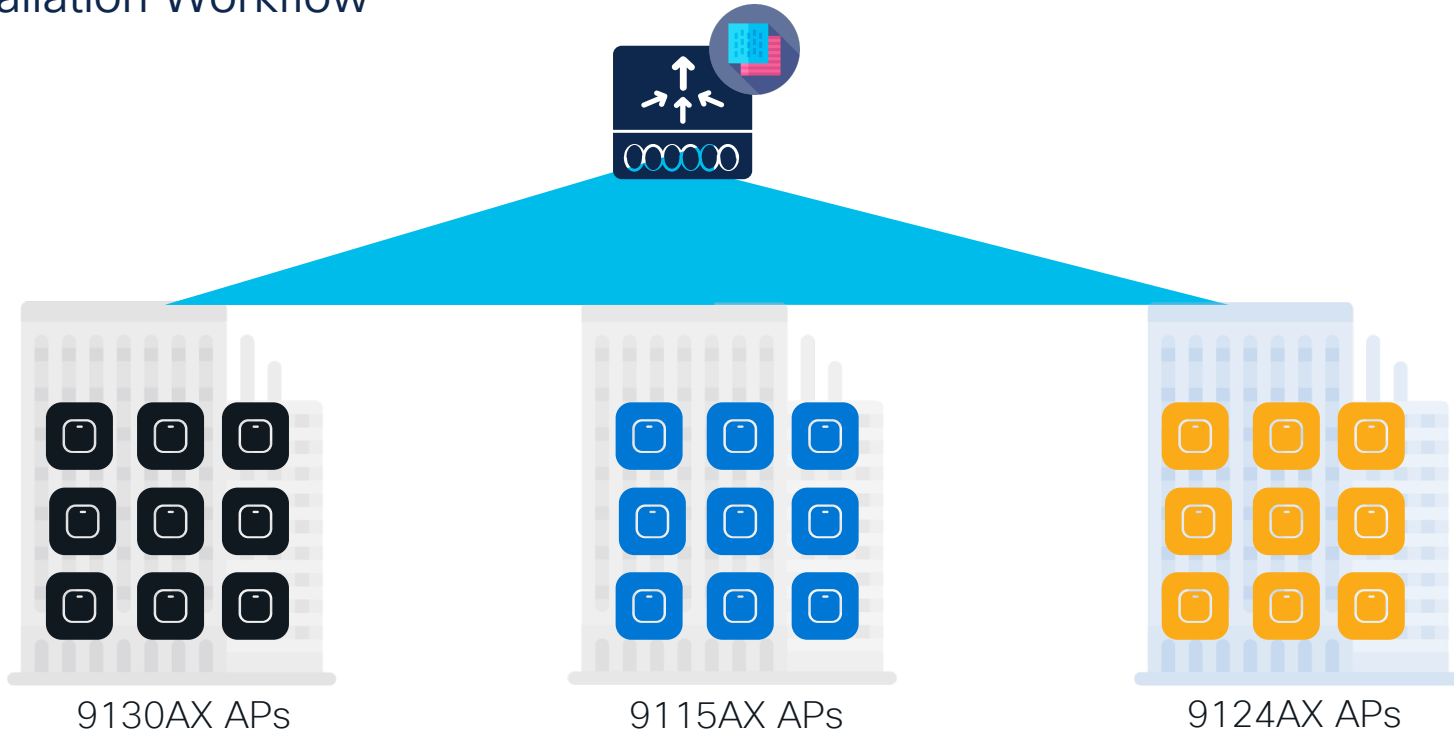


Zero Network Downtime
Applied as HOT patch on the controller with no service impact for APs and Clients

With AP Device Packs

AP Device Pack (APDP)

Installation Workflow



AP Device Pack (APDP)

Configuration

Administration > Software Management

Software Upgrade

Software Maintenance
Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

+ Add

	Type	State	Filename
<input type="radio"/>	APDP	Inactive	bootflash:C9800-CL-universalk9.17.03.04.CSCvz10726.SPA.apdp.bin

1 10 items per page

Auto terminate timer: inactive

AP Upgrade Configuration

AP Upgrade per Iteration

25 %

Apply

AP Device Pack (APDP)

Verification

Administration > Software Management

Software Upgrade

Software Maintenance Upgrade (SMU)

AP Service Package (APSP)

AP Device Package (APDP)

+ Add Rollback

Type	State	Filename	Site Filter
<input type="radio"/> APDP	Activated and Committed	bootflash:C9800-CL-universalk9.17.03.04.CSCvz10726.SPA.apdp.bin	All Sites

1 10 items per page 1 - 1 of 1 items

Auto terminate timer: inactive

AP Upgrade Configuration

AP Upgrade per Iteration

25 %

Apply

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

The screenshot displays the Cisco Catalyst Center interface for managing software images. The main navigation bar shows 'Design / Image Repository / Summary'. The left sidebar has tabs for 'All', 'Routers', 'Switches', 'Wireless Controllers', and 'Security and VPN'. The 'Wireless Controllers' tab is active. The main content area is divided into two sections. The top section, titled 'ADVISORIES', shows a summary of advisory counts: 1 Golden, 0 Critical, and 0 High. Below this is a table with columns for 'Images' and 'Critical'. The table contains two rows of data: the first row shows 6 images with a critical status of N/A, and the second row shows 2 images with a critical status of 0. The bottom section is the 'Import Image/Add-on' dialog box, which is highlighted with a red rectangle. This dialog box has a title bar with the text 'Import Image/Add-on' and a close button. It contains an 'Upload Option' section with three radio buttons: 'Select from computer' (selected), 'Enter URL', and 'Select ISSU compatibility matrix'. Below this is a large dashed box containing an upload icon and the text 'Choose a file or drag and drop to upload.' A red arrow points to this dashed box. Underneath the dashed box is a 'Source' section with two radio buttons: 'Cisco' (selected) and 'Third party'.

Design / Image Repository / Summary

All Routers Switches **Wireless Controllers** Security and VPN

ADVISORIES

1 Golden 0 Critical 0 High
On Running Images On Running Images

Images	Critical
6	N/A
2	0

Import Image/Add-on

Upload Option

Select from computer Enter URL Select ISSU compatibility matrix

Choose a file or drag and drop to upload.

Accepted files:
.gz,.bin,.img,.tar,.smu,.pie,.aes,.iso,.ova,
.tar_gz,.qcow2,.nfvspkg,.zip,.spa,.rpm

Source

Cisco Third party

Software Patching using Catalyst Center

Global

< Image Repository

Cisco Catalyst 9800-CL Wireless Controller for Cloud

SUMMARY

- > Roles & Tags
- > Major Versions
- > Golden Images
- > Recommendation

Images (8)

Filter Images

Image Name	Version
C9800-CL-universalk9.17.03.08.SPA.bin Latest	Amsterdam-17.3.8 Add On (N/A)
C9800-CL-universalk9.17.06.06.SPA.bin Latest	Bengaluru-17.6.6 Add On (N/A)
C9800-CL-universalk9.17.09.03.SPA.bin Verified	17.09.03.0.4111 Add On (1)
C9800-CL-universalk9.17.09.04.SPA.bin Verified Suggested Latest	17.09.04.0.5180 Add On (N/A)
C9800-CL-universalk9.17.11.01.SPA.bin Latest	Dublin-17.11.1 Add On (N/A)

Add On List (1)




BASE IMAGE INFORMATION

Family Cisco Catalyst 9800-CL Wireless Controller for Cloud
Image Name C9800-CL-universalk9.17.09.03.SPA.bin

SMU (1) PSIRT SMU (0) Sub-package (0) ROMmon (0) APSP (0) APDP (0)

C9800-CL-universalk9.17.09.03.CSCwe01579.SPA.smu.bin

ADD ON ATTRIBUTES

Description Cisco IOS-XE Patch package
Defect Id CSCwe01579
Reboot Required Yes
Category bulk-patch
Supercedes Not Available
Compliant Devices Not Available
Image Verification Verified
Golden Image  
Device Roles/Tags  Role: All

Software Patching in Catalyst Center

Provision / Inventory / Image Update Status

WLC-001.robm.work.lab (10.10.22.2) Image Update ✕

Date: Oct 6, 2023 5:38 PM Duration: 16 minutes 1 second Status: ● Successfully updated with C9800-CL-universalk9.17.09.04.CSCwh28727.SP A.apsp.bin , C9800-CL-universalk9.17.09.04.SPA.bin

Operations Checks

- > ● Distribution 0 second
- > ● Activation 1 second
- > ● APSP Distribution 11 minutes 8 seconds
- > ● APSP Activation 4 minutes 49 seconds
 - APSP Activation of image: C9800-CL-universalk9.17.09.04.CSCwh28727.SPA.apsp.bin on device: 10.10.22.2 completed successfully
 - > ● Pre Activation Script Execution 1 second
 - > ● Activation 4 minutes 47 seconds
 - > ● Remove Inactive Images Execution 1 second
 - > ● Post Activation Script Execution 1 second

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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire slide is a vibrant, multi-colored abstract pattern of overlapping, wavy lines in shades of red, orange, yellow, green, and blue, creating a sense of motion and energy.

CISCO *Live!*

Let's go

#CiscoLiveAPJC