#CiscoLive

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 Live!

#CiscoLive

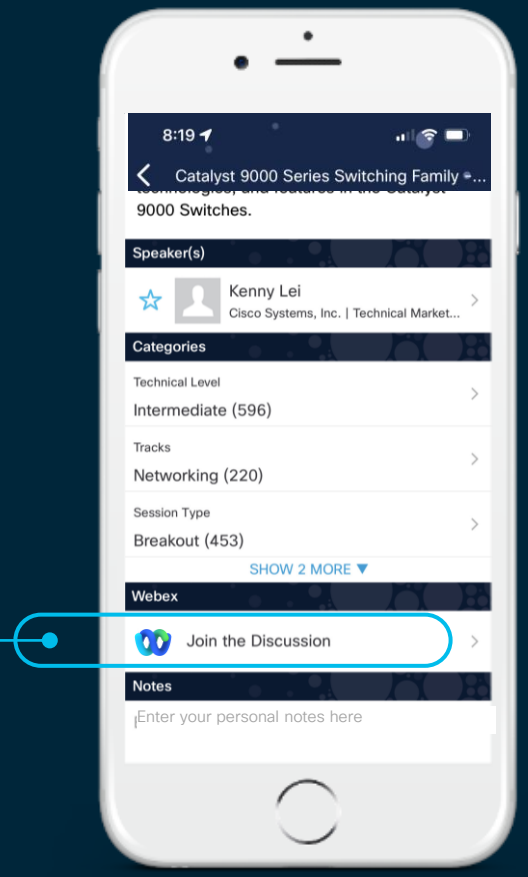
Cisco Webex app

Questions?

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

How

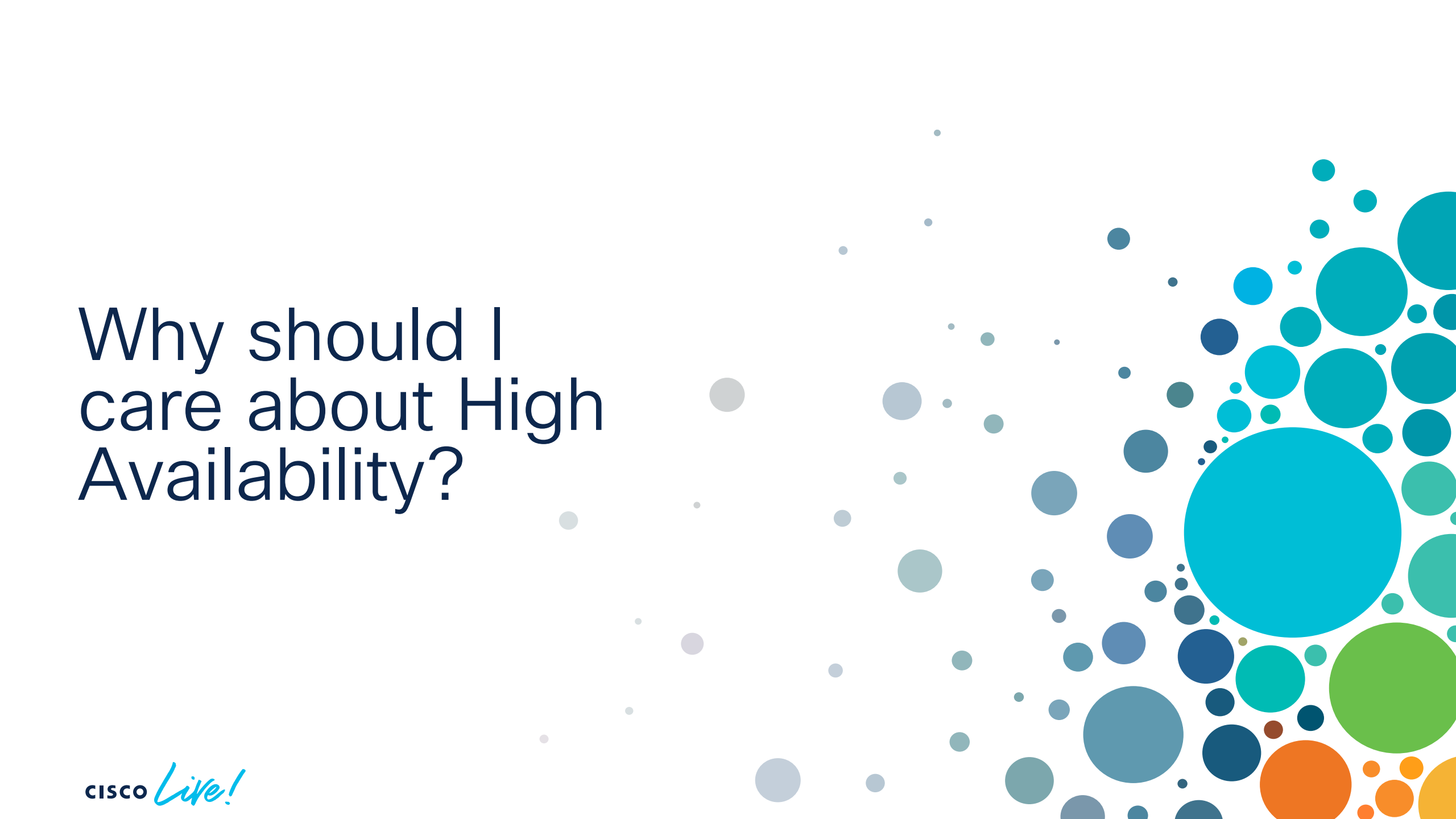
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



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

Webex spaces will be moderated by the speaker until June 17, 2022.

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. Software Patching Capabilities
   - Software Maintenance Updates, AP Service Packs and Device Packs
6. Controller Software Upgrades
   - N+1 Site Based Hitless Upgrade
   - In Service Software Upgrade (ISSU)

Cisco's Next-gen Wireless Stack

Enabling next-generation mobility powered for Wi-Fi 6

Cisco Catalyst 9800
Wireless Controllers

Cisco Catalyst 9100
Access Points

Managed by

Cisco DNA Center

Translate business intent into network policy
and capture actionable insights

Digitized by

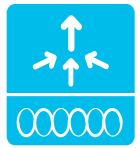
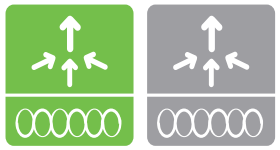
Cisco DNA Spaces

Digitize people, spaces and things

Resilient | Secure | Intelligent

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 Clients • 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

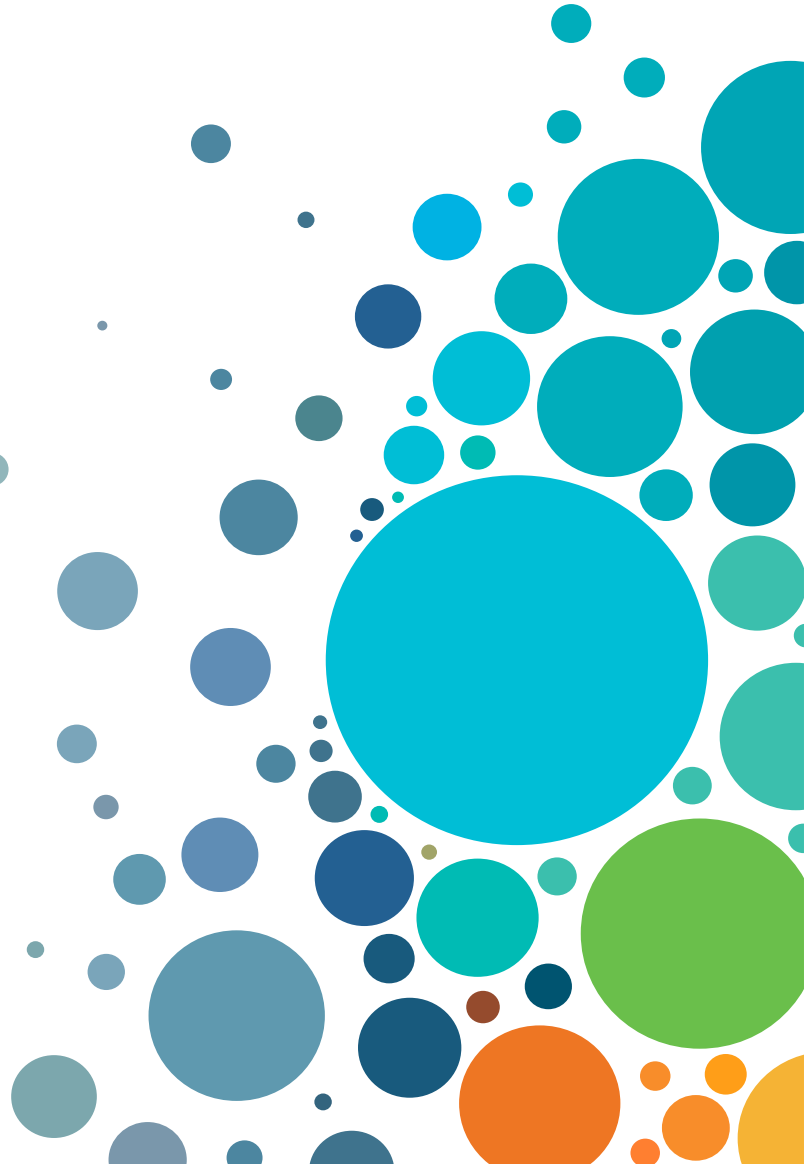
Functionality	AireOS	9800
SSO	Yes	Yes
N+1	Yes	Yes
RMI	Yes	Yes
Dual Active Detection	Yes	Yes
Recovery Mode	Yes	Yes
Default GW Check	Yes	Yes
LACP, PAGP with SSO	No	Yes
SMU for controller patching	No	Yes
APSP for AP Patching	No	Yes
Per-site, per-model AP Patching	No	Yes
AP device pack	No	Yes
ISSU	No	Yes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

For your reference

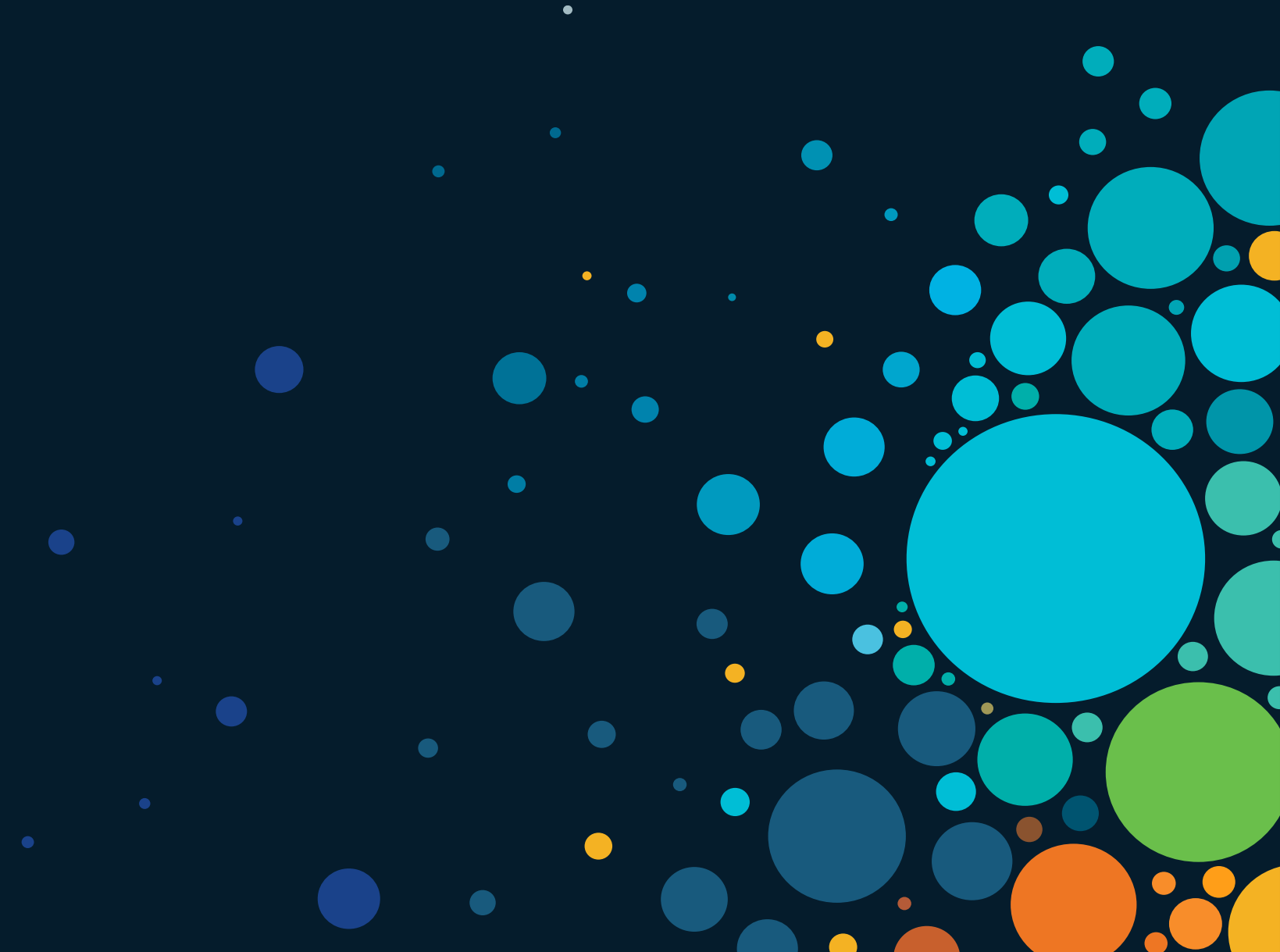
Resiliency Feature Matrix

	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

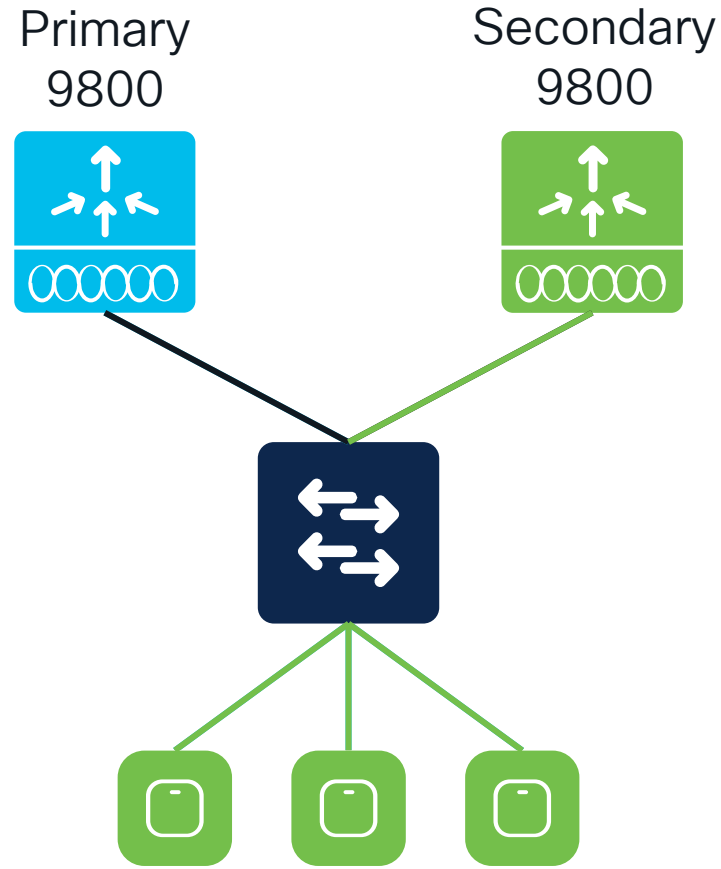


cisco Live!

N+1 Redundancy

N+1 Redundancy

- Single 9800 serve 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



AP failover takes ~45-60 seconds

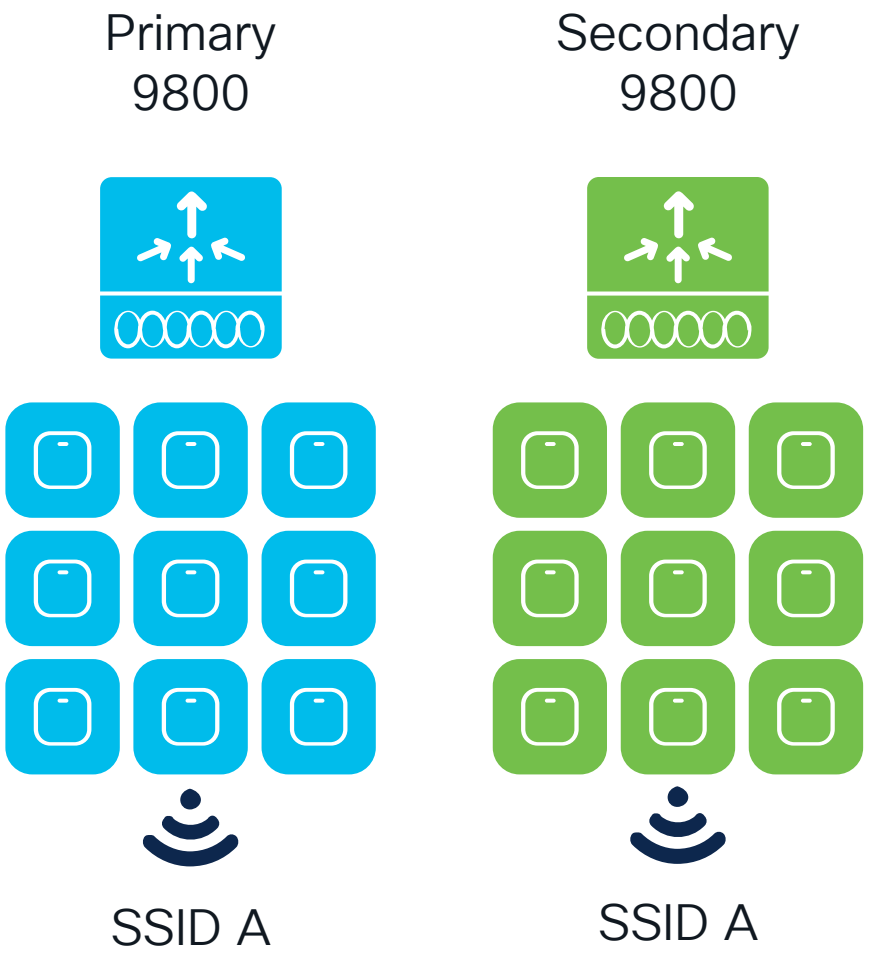
N+1 best practices

Primary and Secondary WLC should run the same software version

Configurations should be consistent across the Primary, Secondary, and Tertiary controllers

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

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

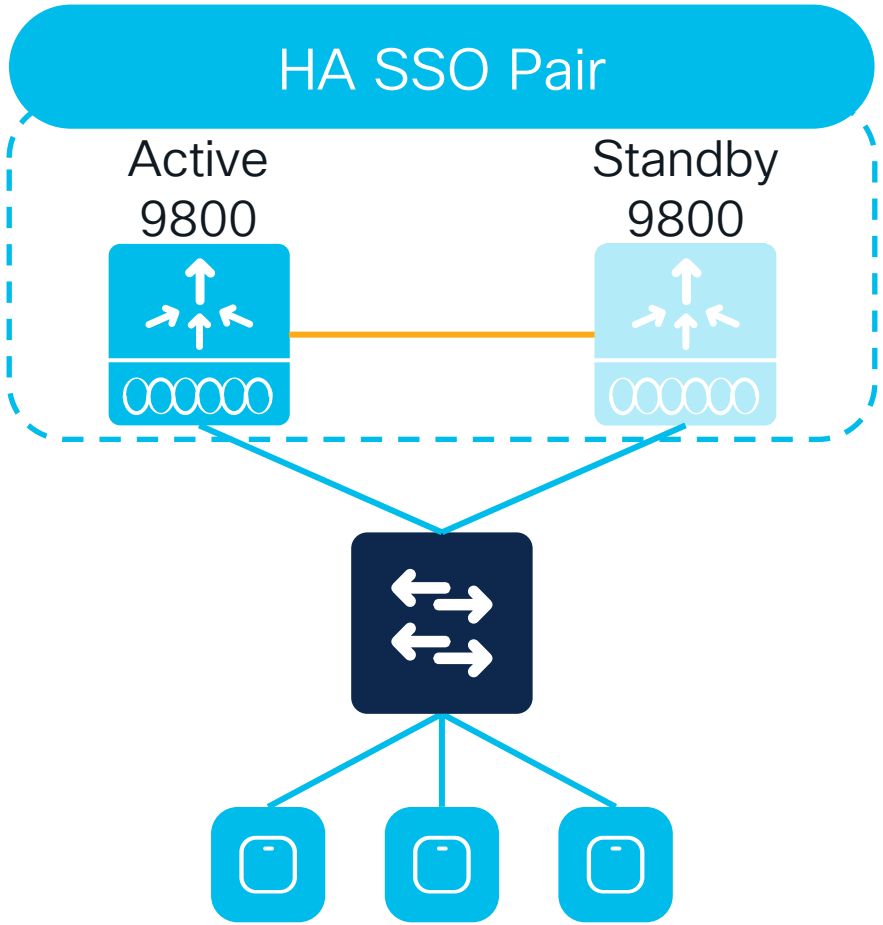
Pre-17.6.1: Manually write the tags to each AP

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

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

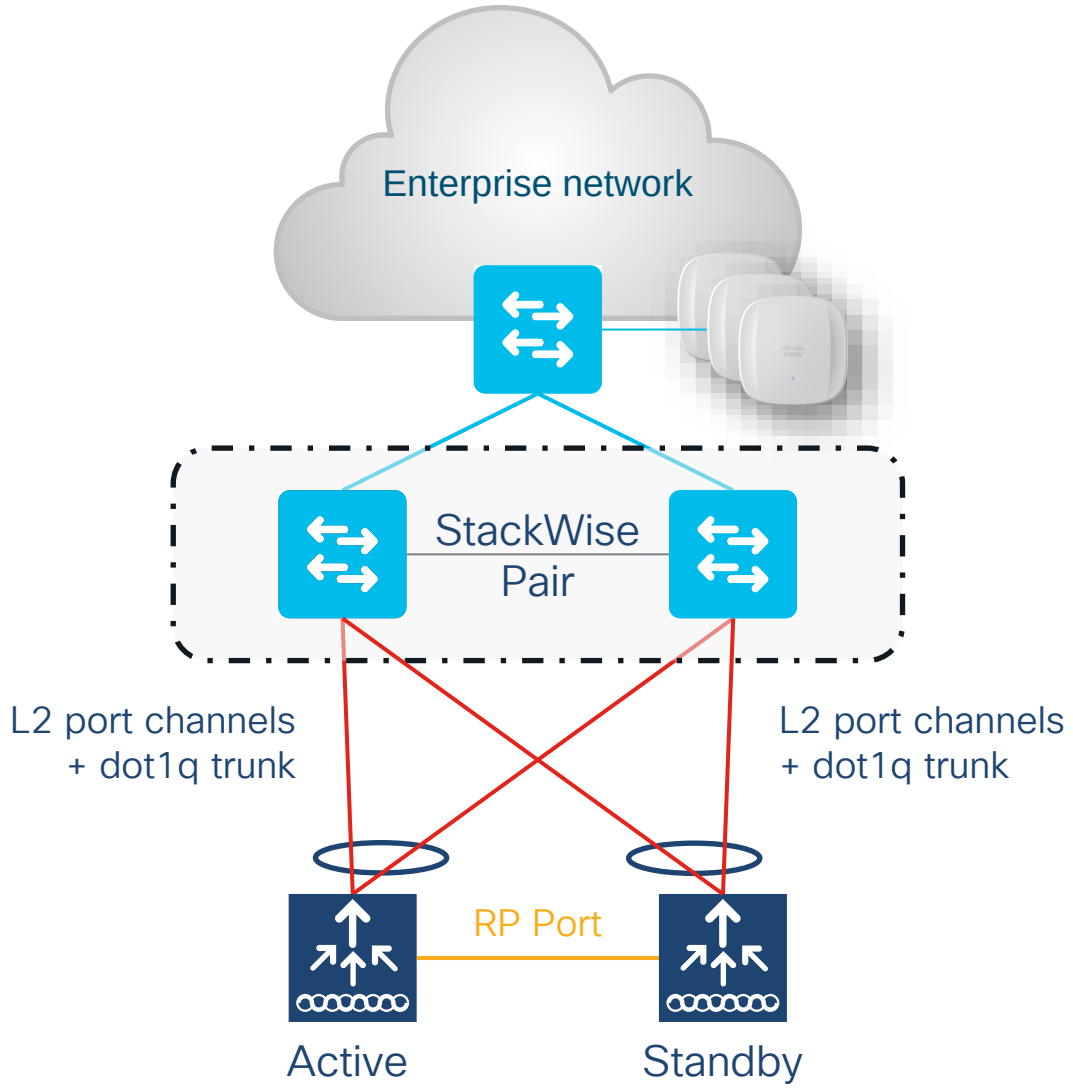


AP failover takes order of sub seconds

HA SSO behavior
Redundancy Port (RP)

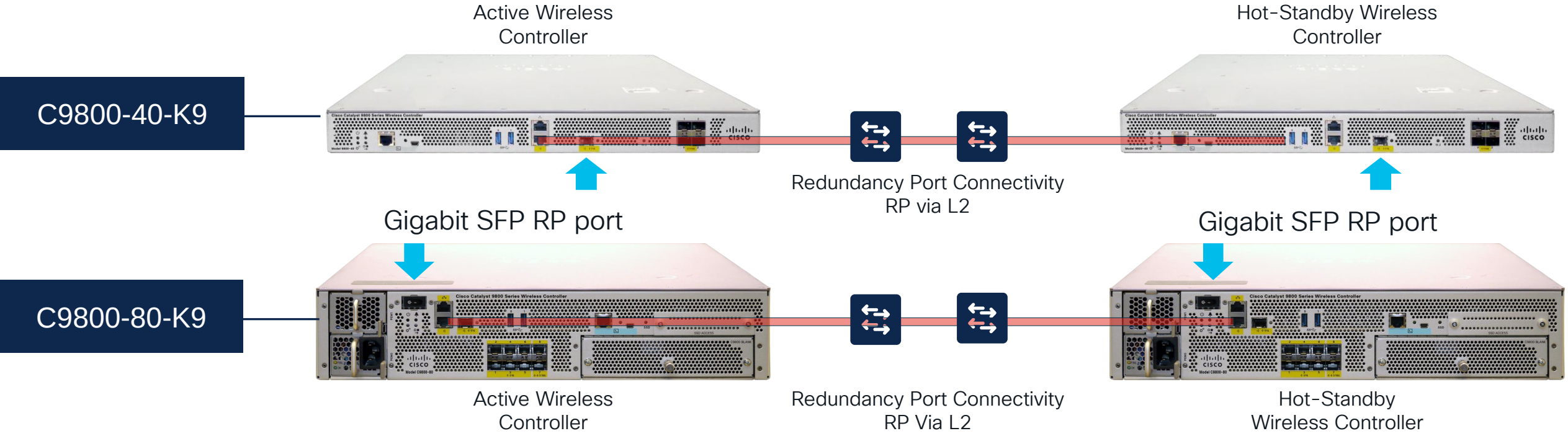
Redundancy Port (RP)

- 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



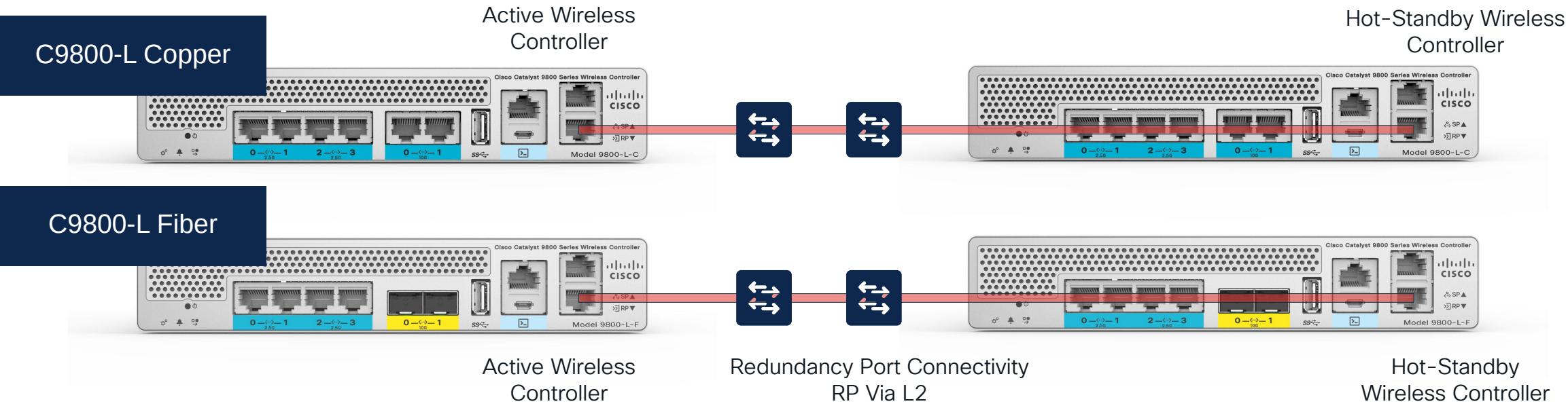
Sub-second failover and zero SSID outage

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.

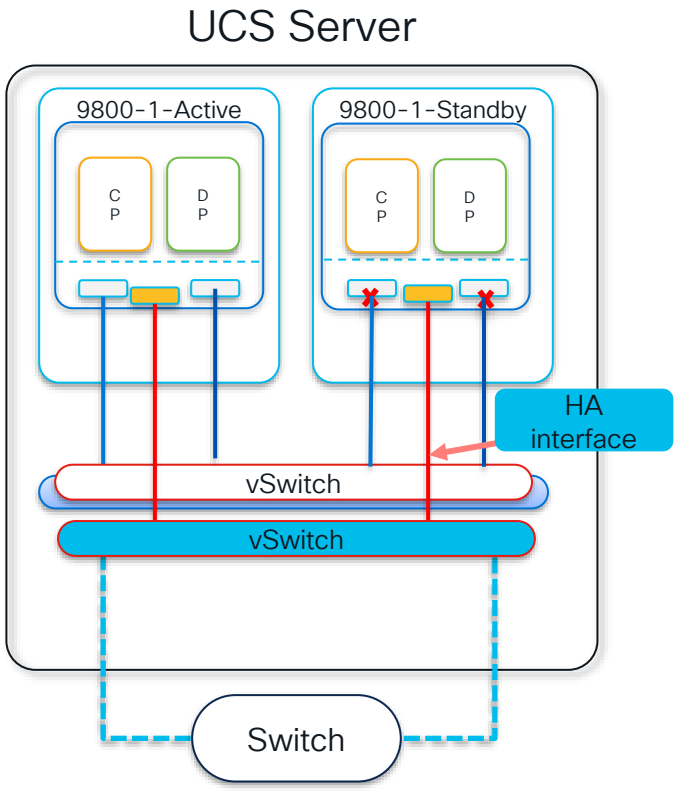
Note: There is no Fiber RP Port on 9800-L.



Sub-second failover and zero SSID outage

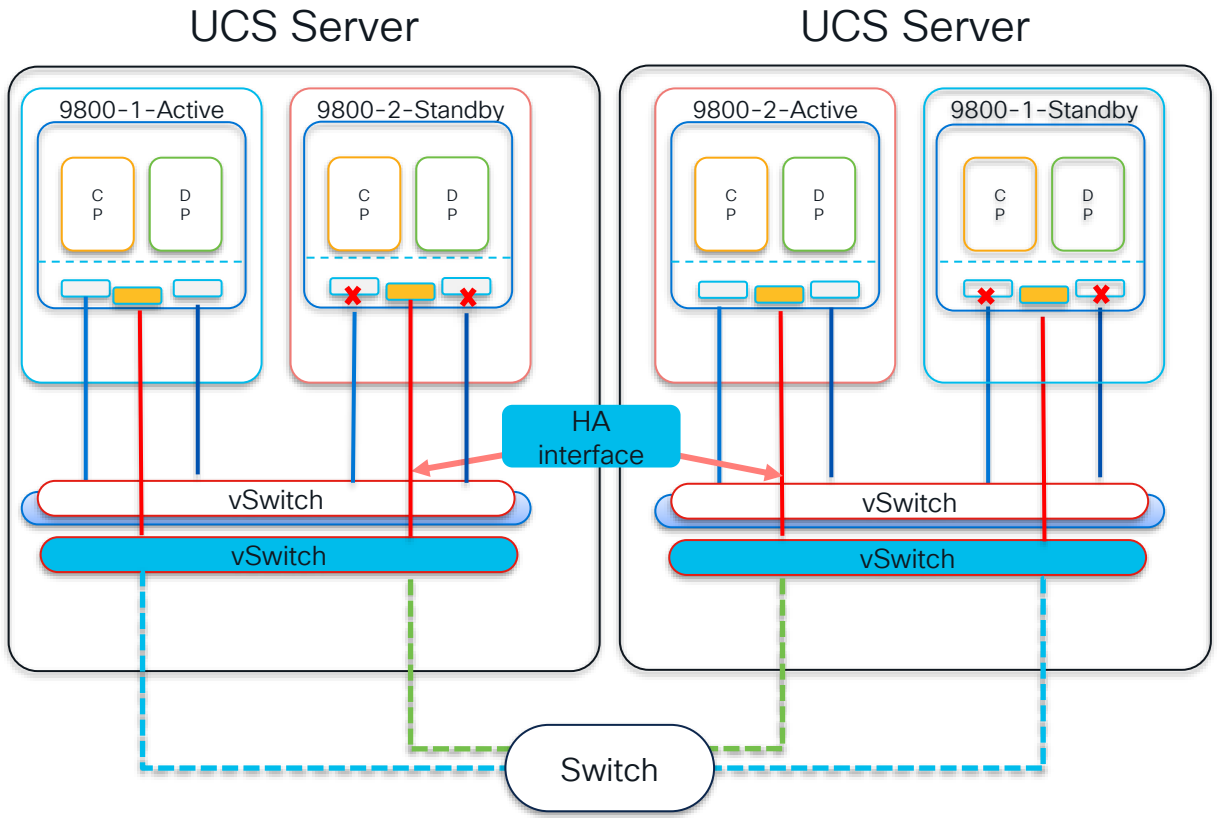
High Availability (SSO) on Catalyst 9800-CL

Intra-Host Redundancy



Redundancy Port Connectivity

Inter-Host Redundancy



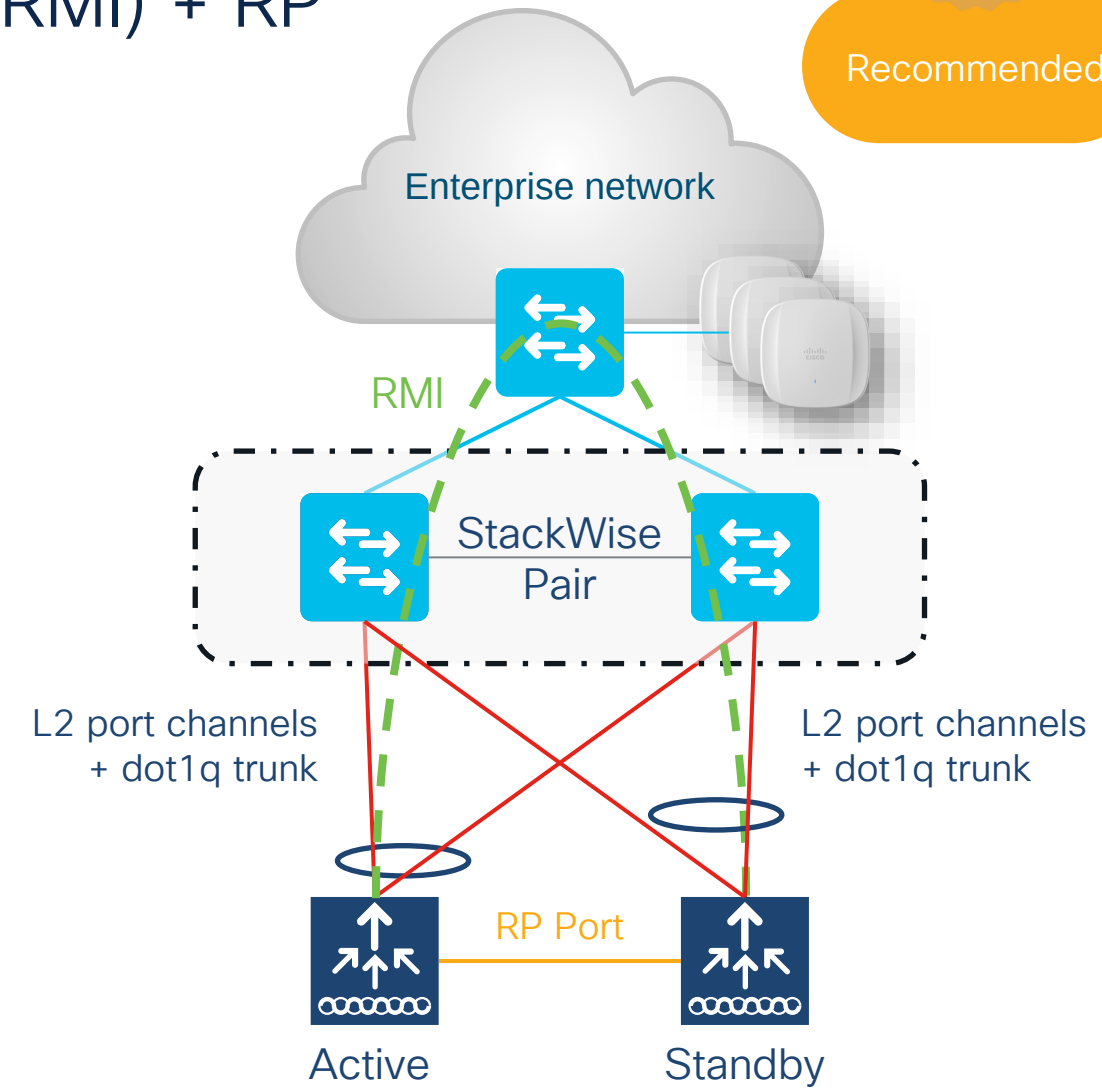
Redundancy Port Connectivity
RP via L2

HA SSO behavior
Redundancy Management Interface (RMI) + RP

Recommended

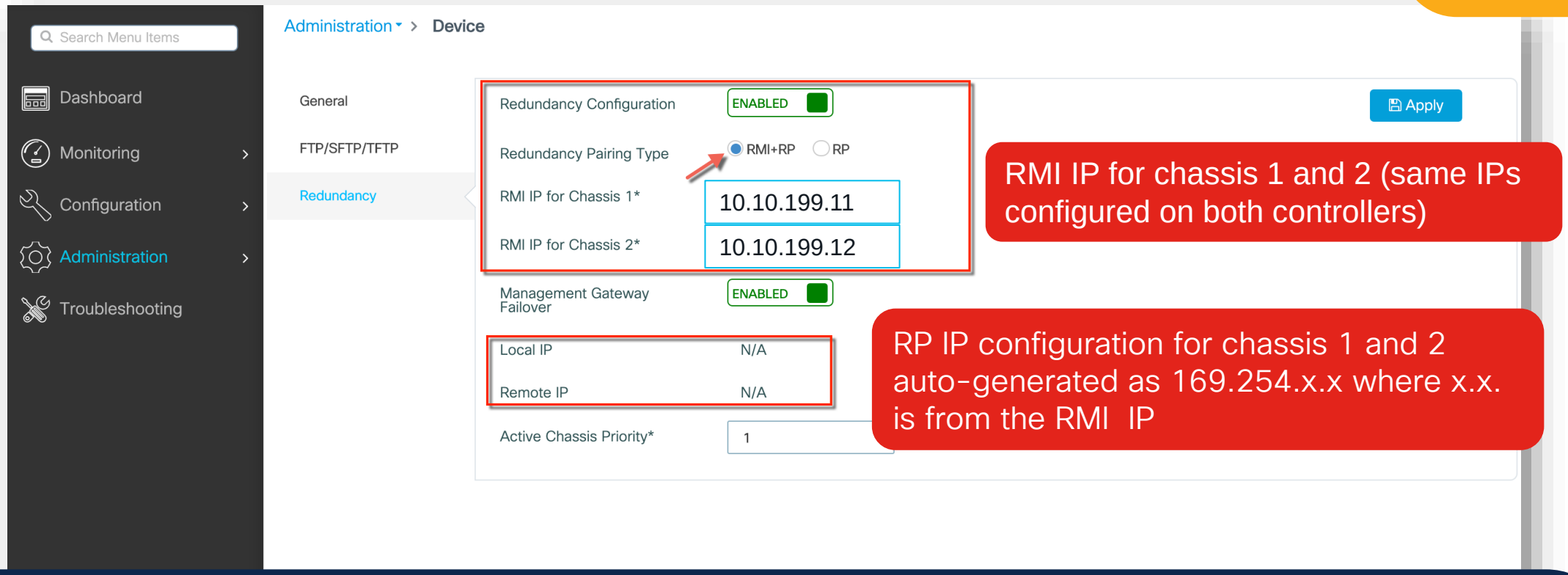
RMI + RP

- 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



SSO configuration using RMI+RP option

Recommended



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

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>
```

- Executed in CLI config mode
- 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.

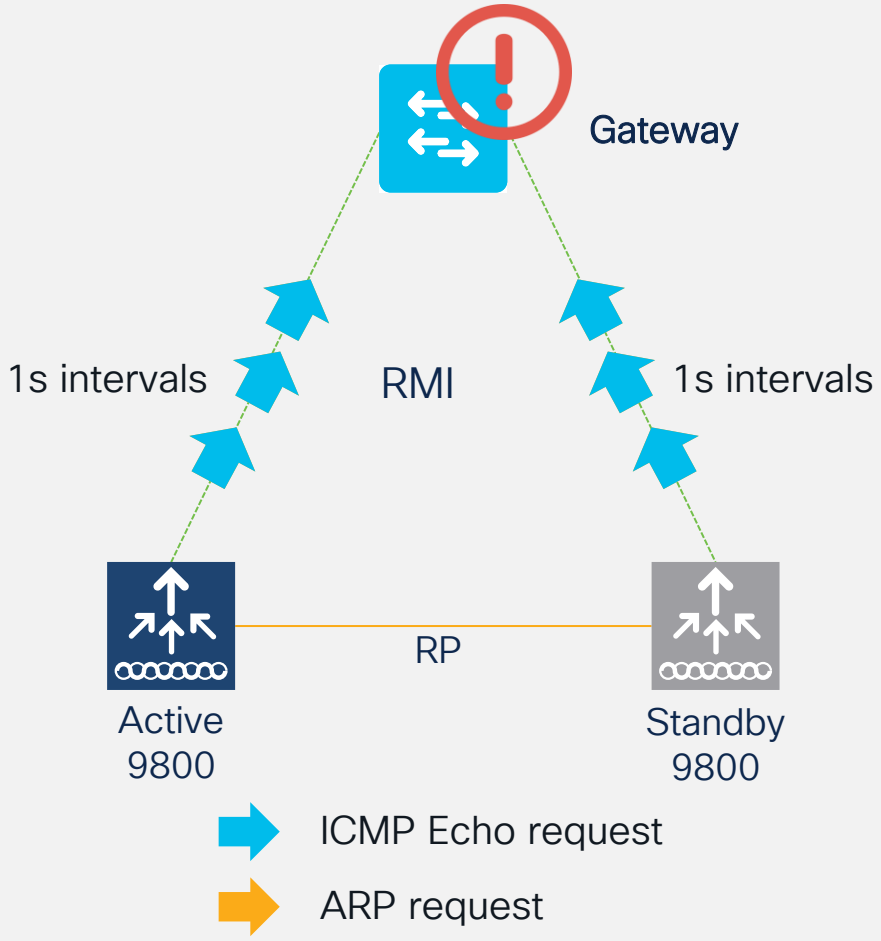
RMI Default Gateway Check

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>

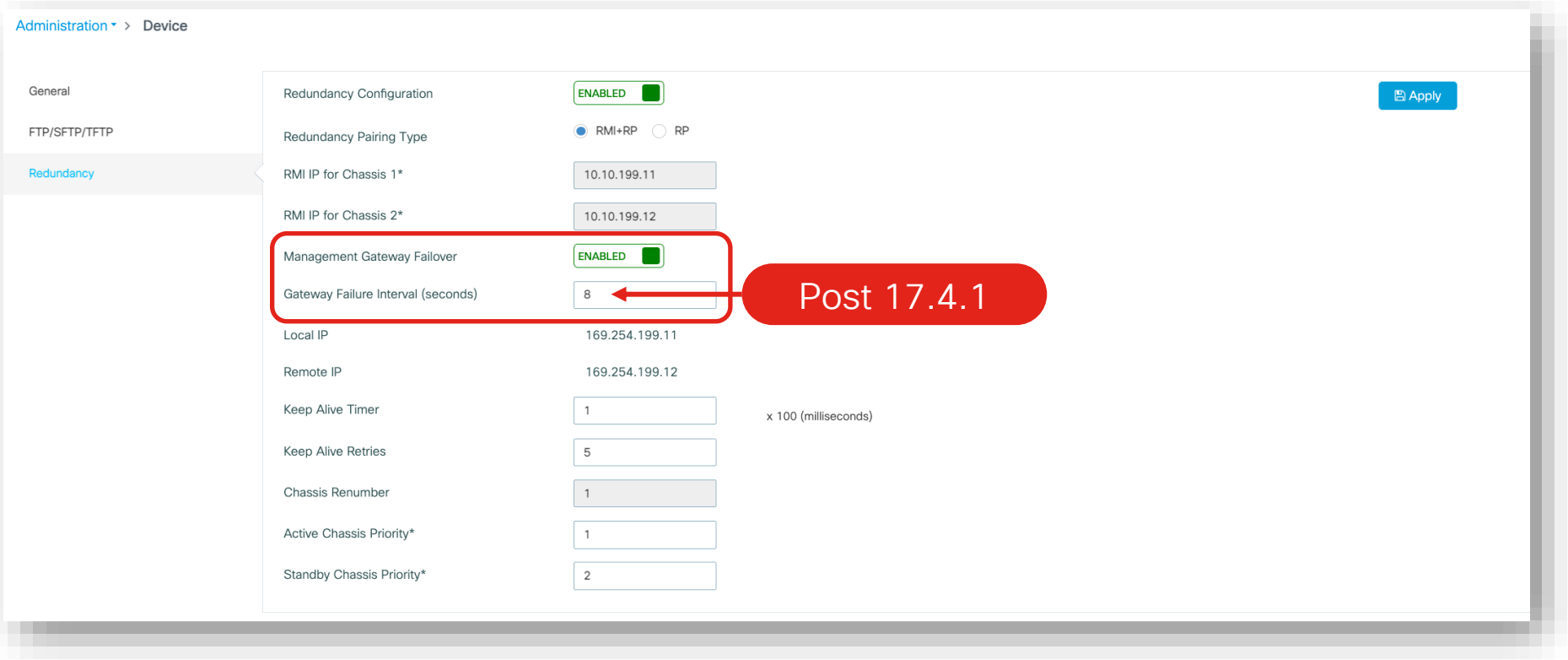
- GW failure interval is configurable – 6 to 20 seconds (Default is 8 sec)
- IPv6 only uses ICMP Echo Requests



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

```
WLC-9800#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
```

YANG Models

- Cisco-IOS-XE-native:management
- Cisco-IOS-XE-rmi-dad:gateway-failover
- Sample json:

```
{
    "Cisco-IOS-XE-native:management": {
        "Cisco-IOS-XE-rmi-dad:gateway-failover": {
            "enable": true,
            "interval": 10
        }
    }
}
```

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.

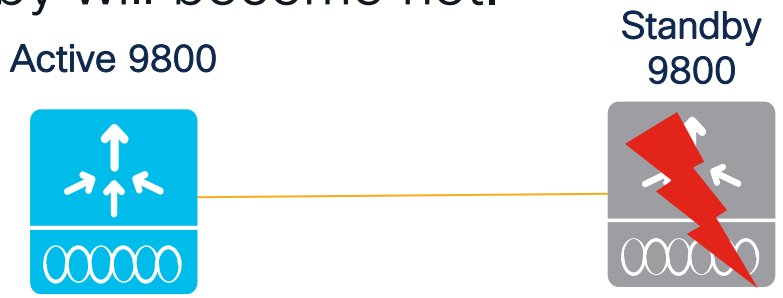
Software and network failover scenarios

Recovery Modes: Active-Recovery and Standby-Recovery

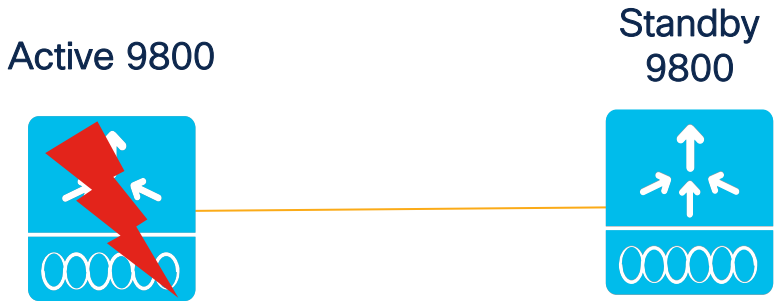
- **Recovery mode** logically means a state where the controller does not have all "resources" available to provide the service. At present, RP, RMI and Gateway are the resources. Ports will be in admin down in recovery mode, so no traffic goes through
- **Standby-Recovery:** If Gateway goes down, standby 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.

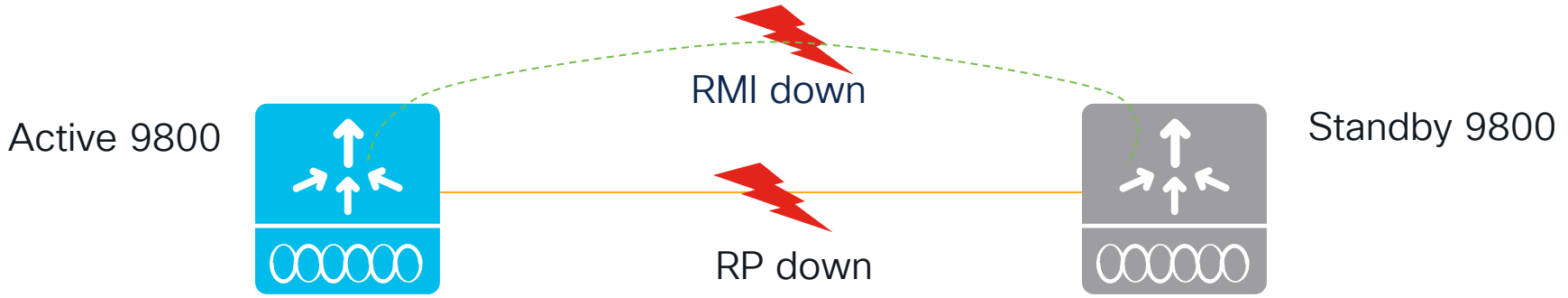
RP Link	Peer reachability through RMI	Gateway From Active	Gateway from Standby	Switchover	Result
Down	Up	Reachable	Reachable	Yes	Standby will become active with (old) active going to active-recovery. Config mode is disabled in active-recovery mode. All interfaces will be ADMIN DOWN with the wireless 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

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

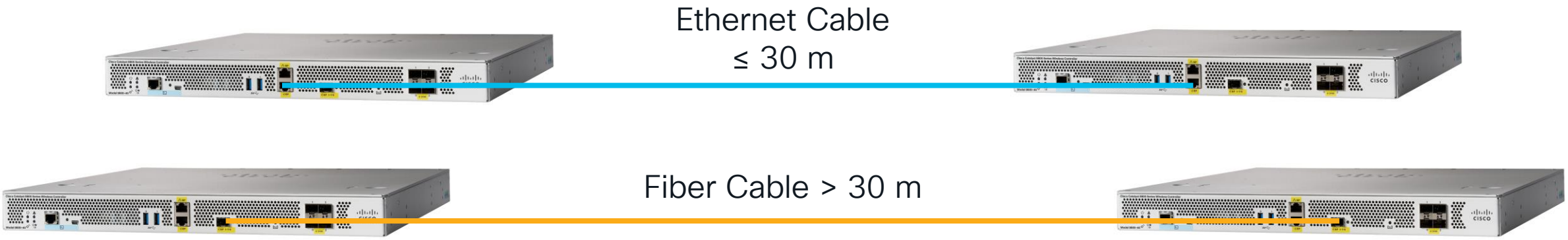
- Both boxes are running the same software and in the same boot mode
- Install mode is recommend

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

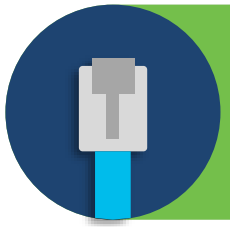


SSO best practices
C9800-CL Private Cloud with vMotion

vMotion is supported for C9800-CL with caveats

vMotion

- Do not run vMotion on both active and standby simultaneously



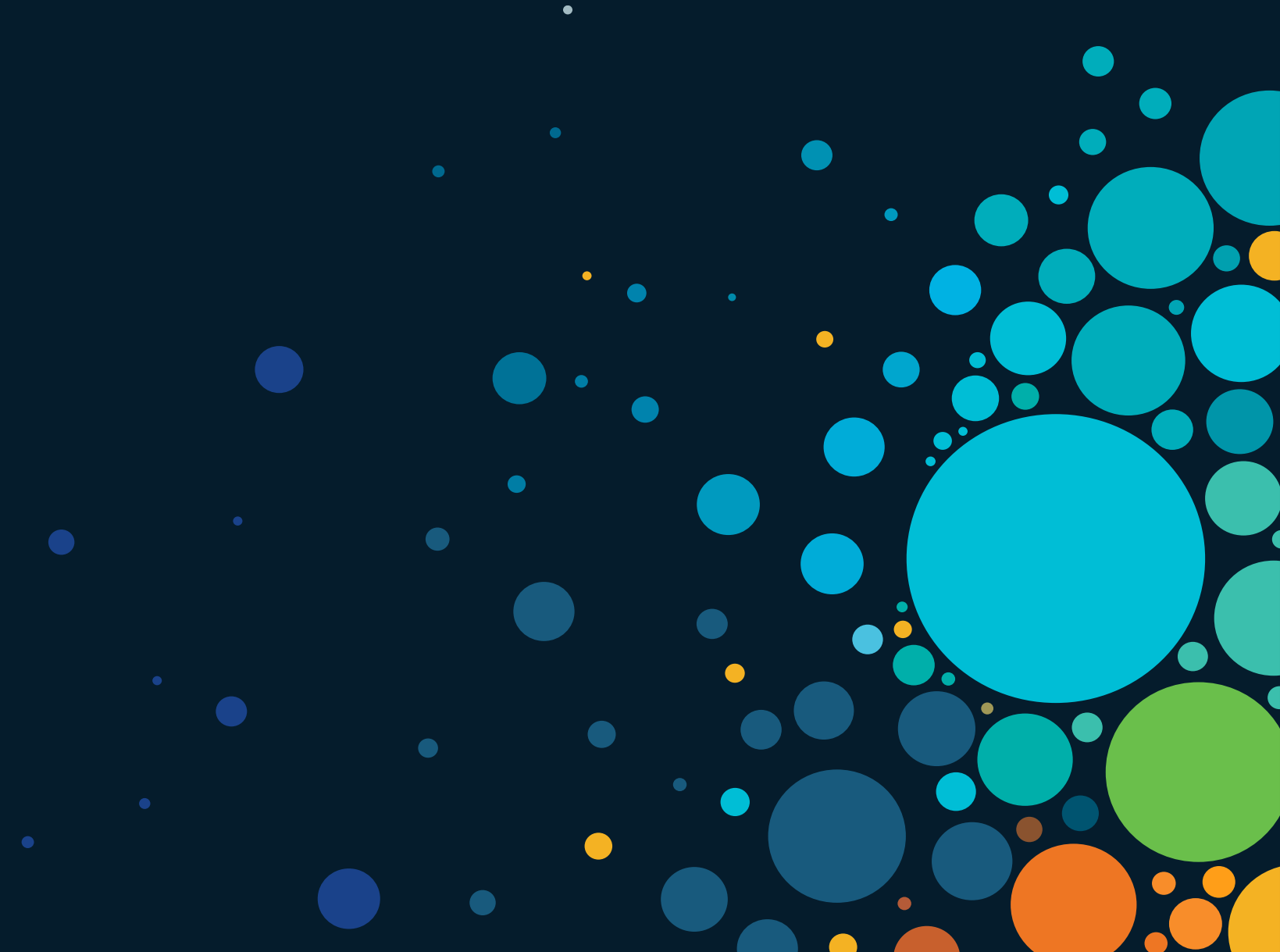
Networking

- 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

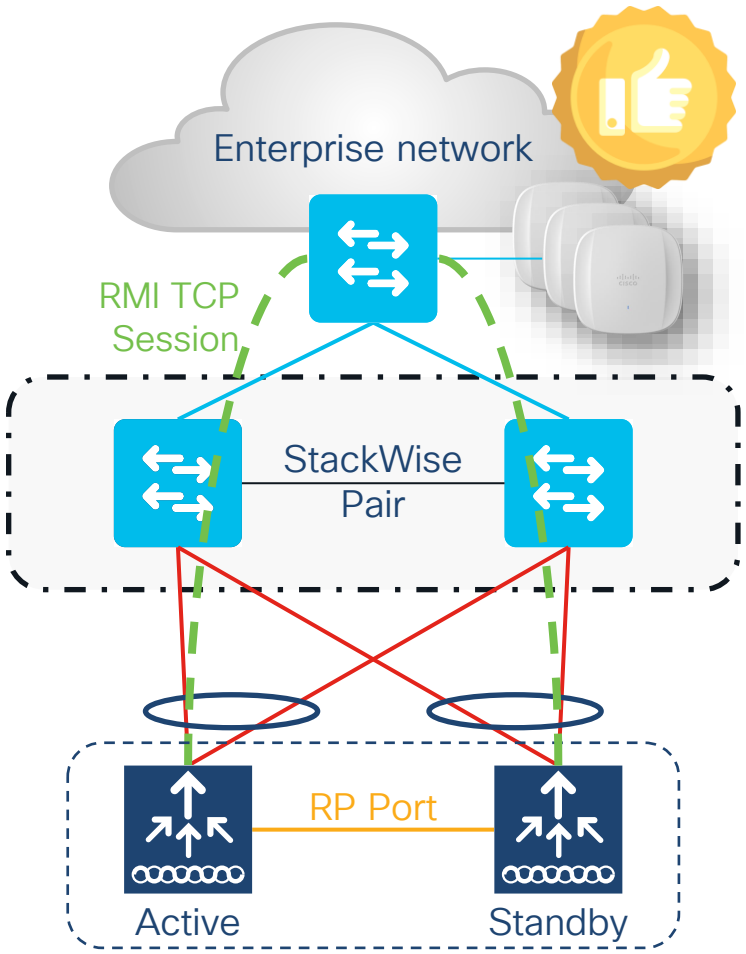
- Local Storage: RAID 0
- Remote Storage: Less than 10ms latency and 10G link

2. Upstream Switch Redundancy

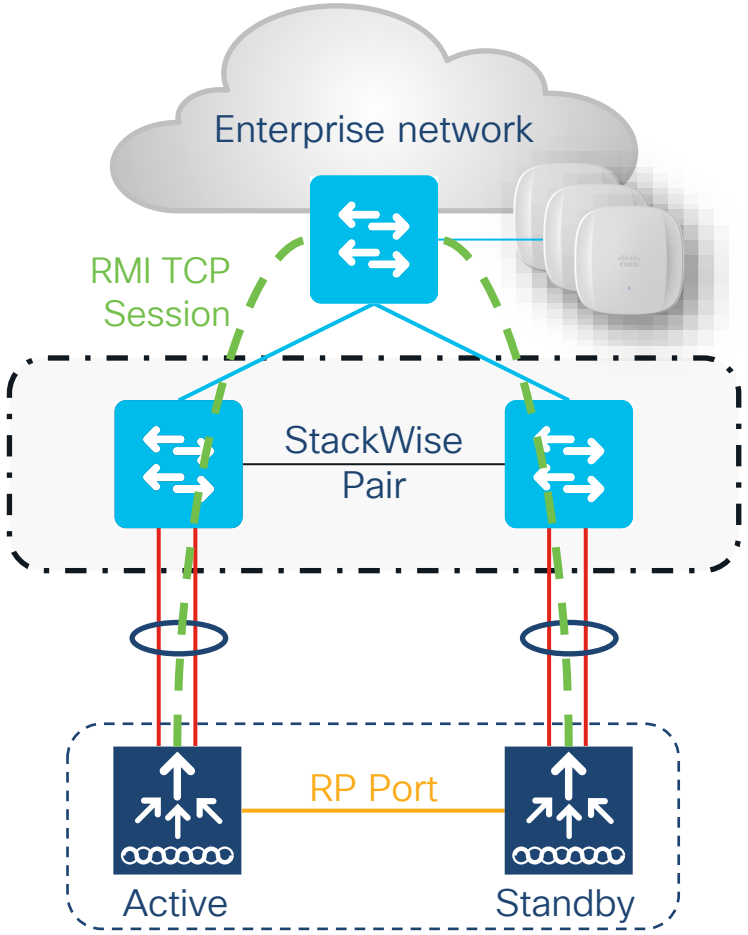


Supported SSO topologies

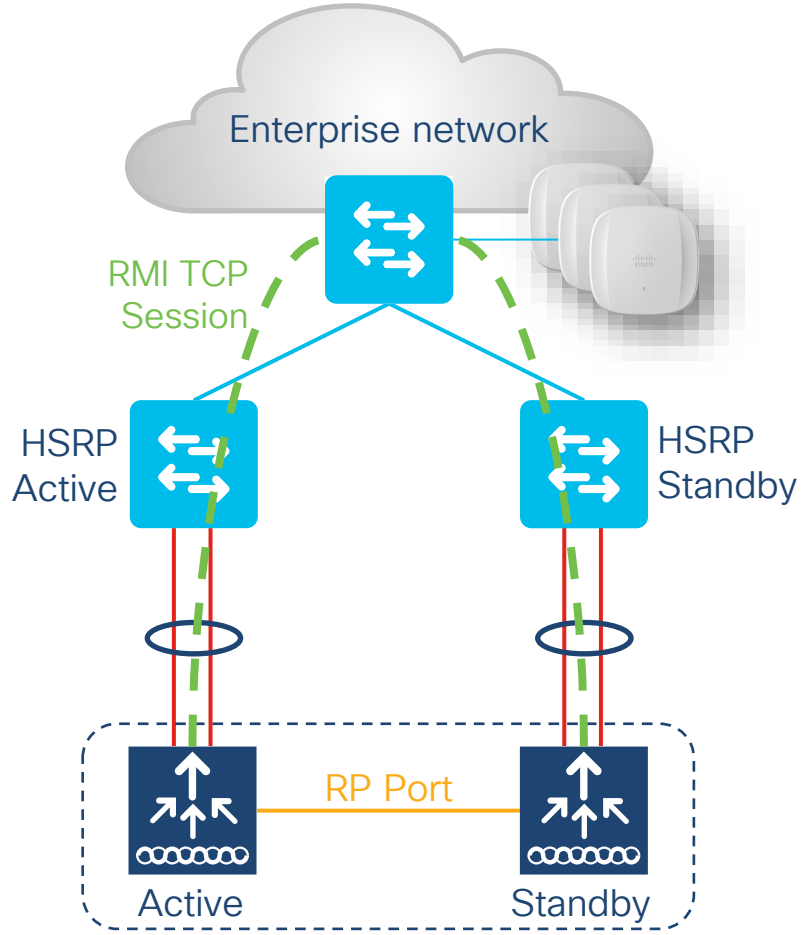
Supported topologies



StackWise Pair with Split links



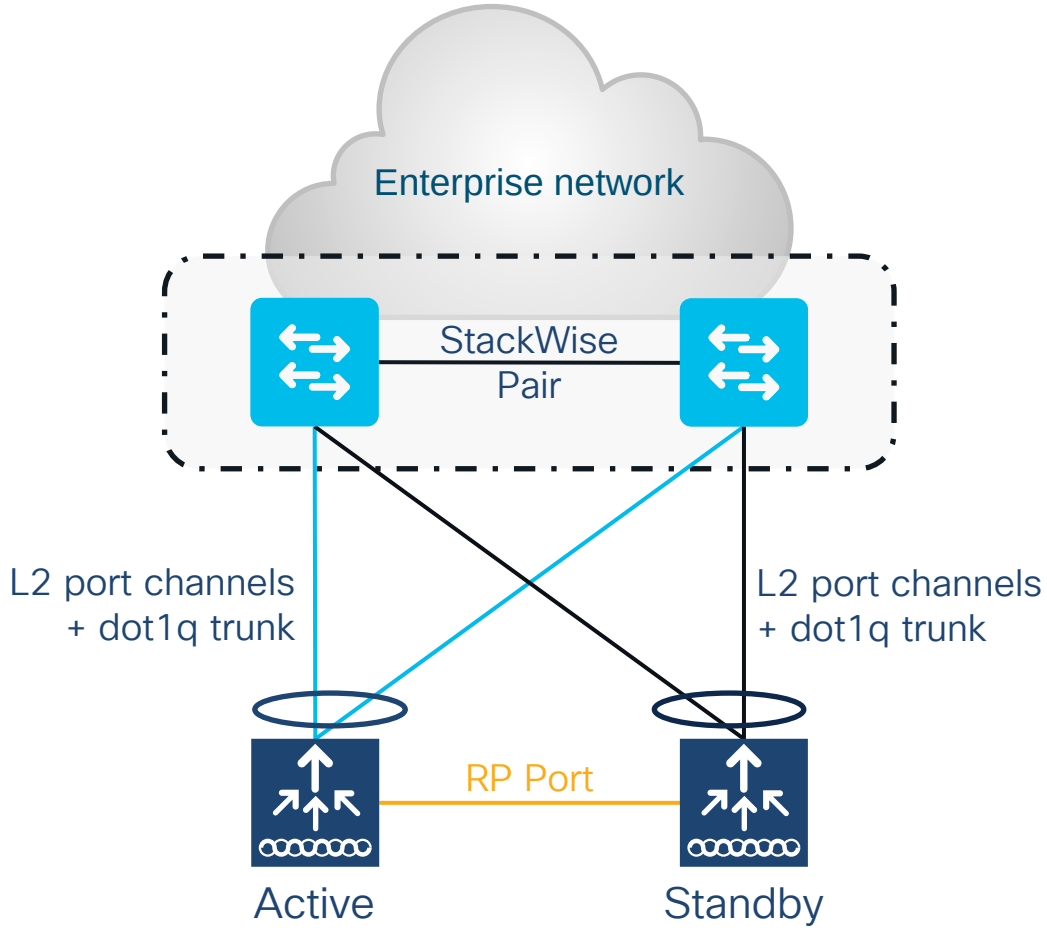
StackWise Pair without Split links



HSRP

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

StackWise Pair with split links
SSO HA Pair

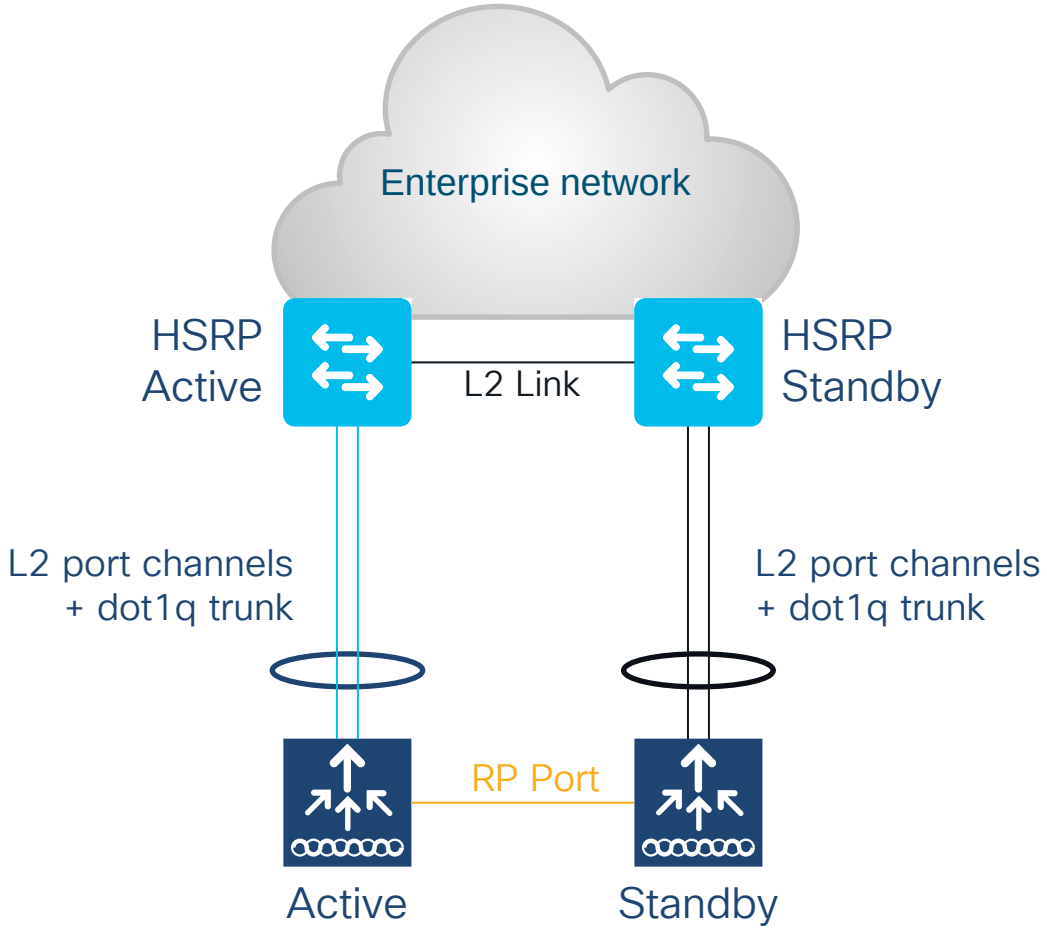


Recommended

- 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

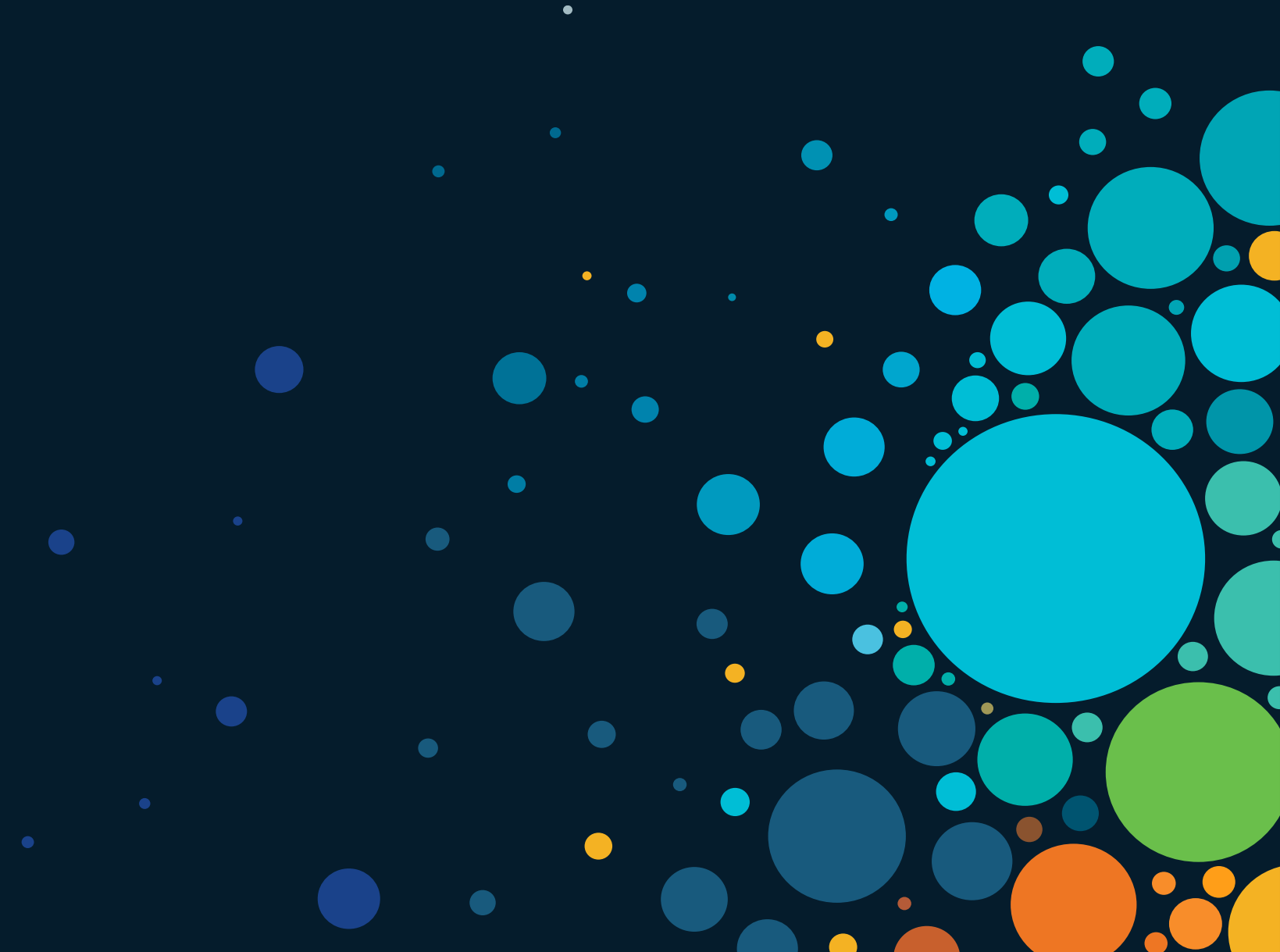
Note: Spread the uplinks across the StackWise pair and connect the RP back-to-back (no L2 network in between)

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
- This is a Recommended topology

3. Link Level Redundancy



LAG support with LACP and PAGP

LACP, PAGP support in SSO Pair

cisco Live!

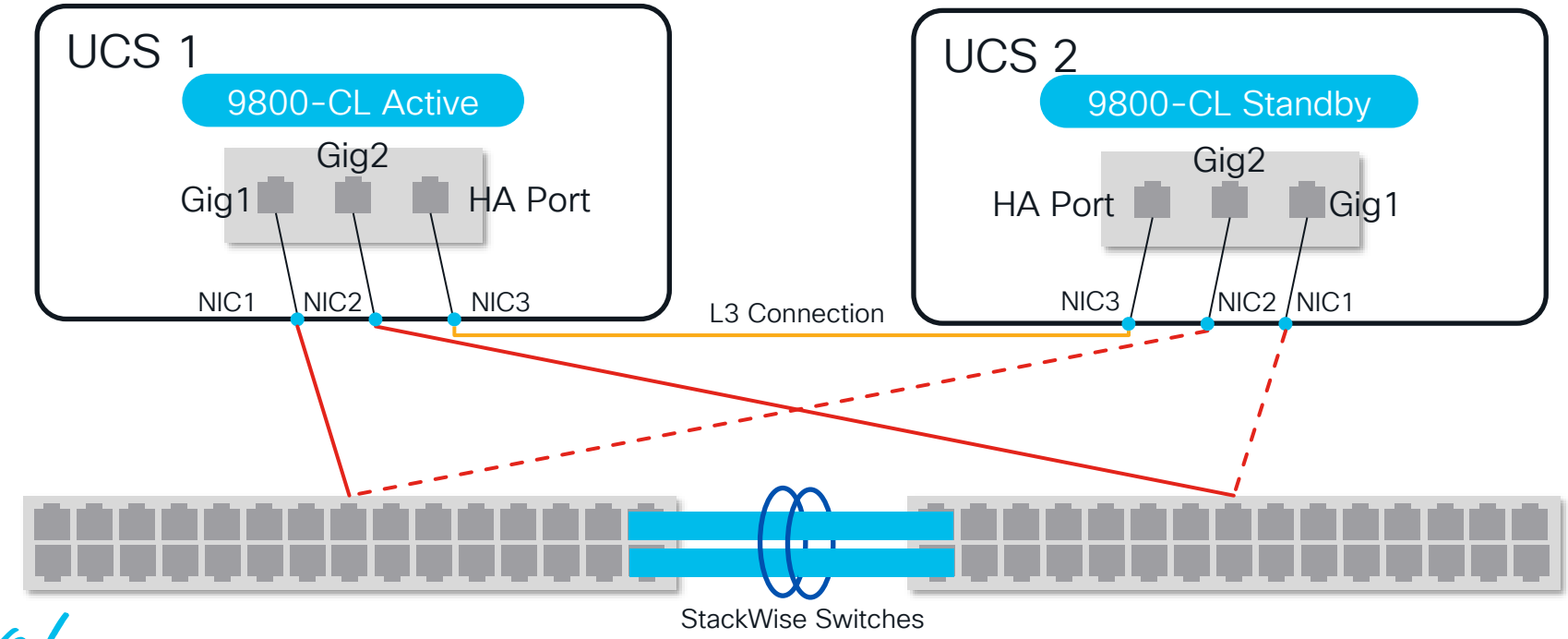
LAGP, PAGP support in SSO Pair

- 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)

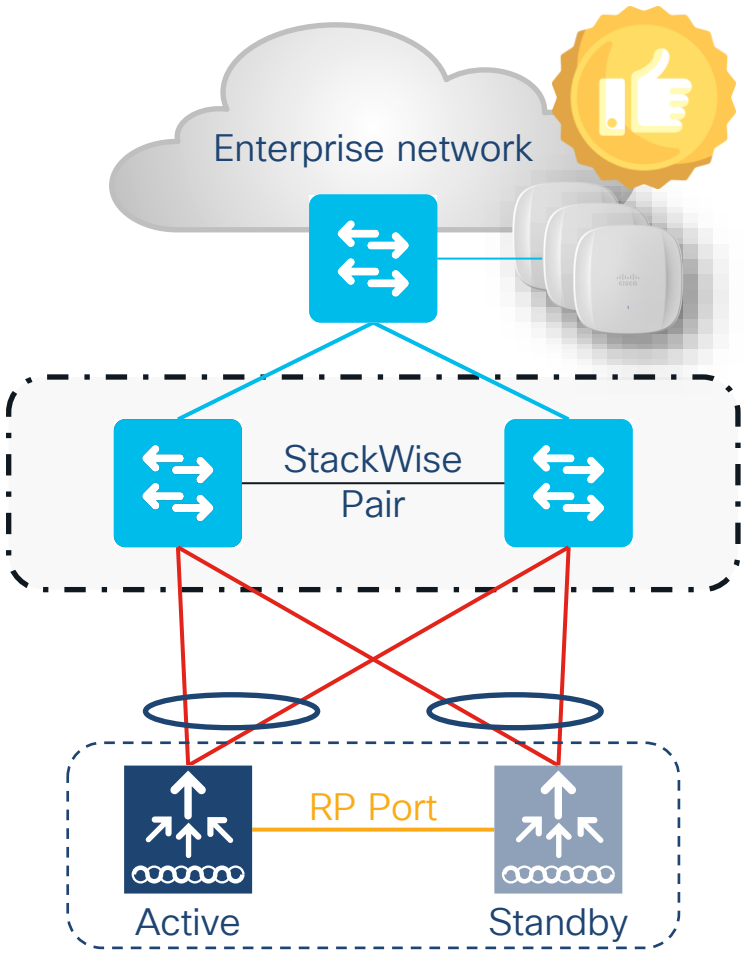
Platforms supported

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

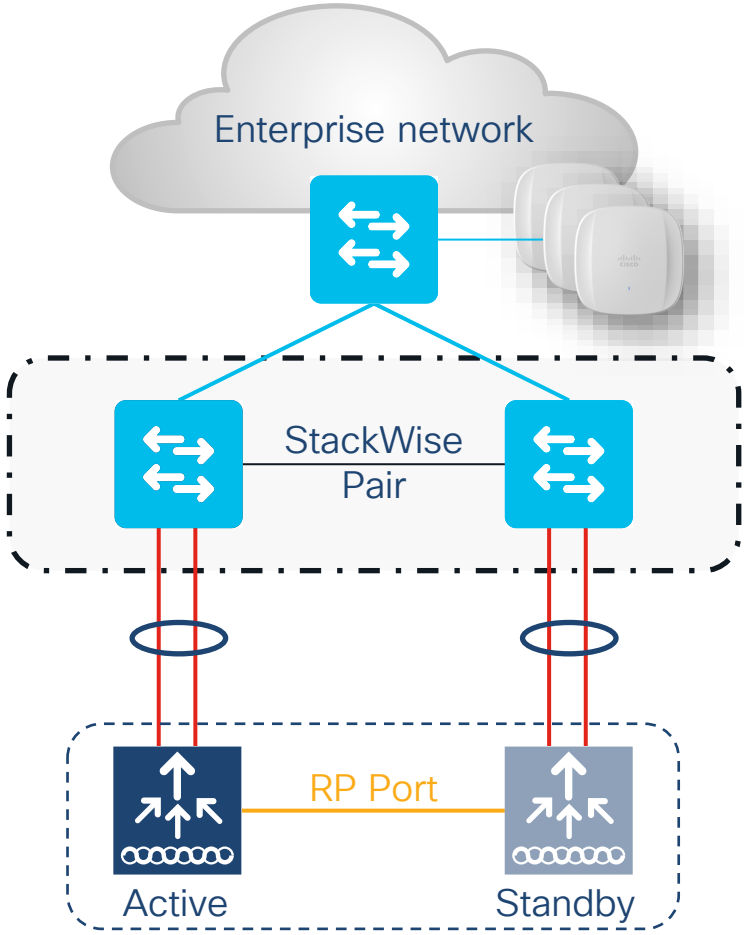
- Cisco Catalyst 9800-CL Private Cloud (Release 17.5.1 and later) - SR-IOV only



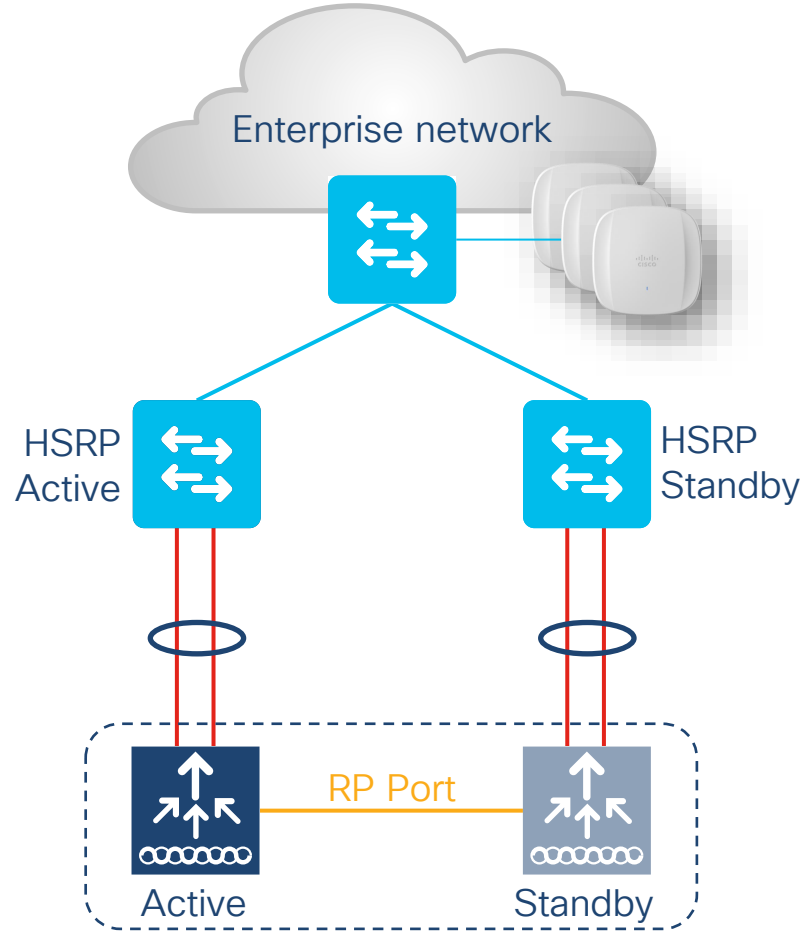
Supported LACP, PAGP topologies



StackWise Pair with Split links



StackWise Pair without Split links



HSRP

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 supported.

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.

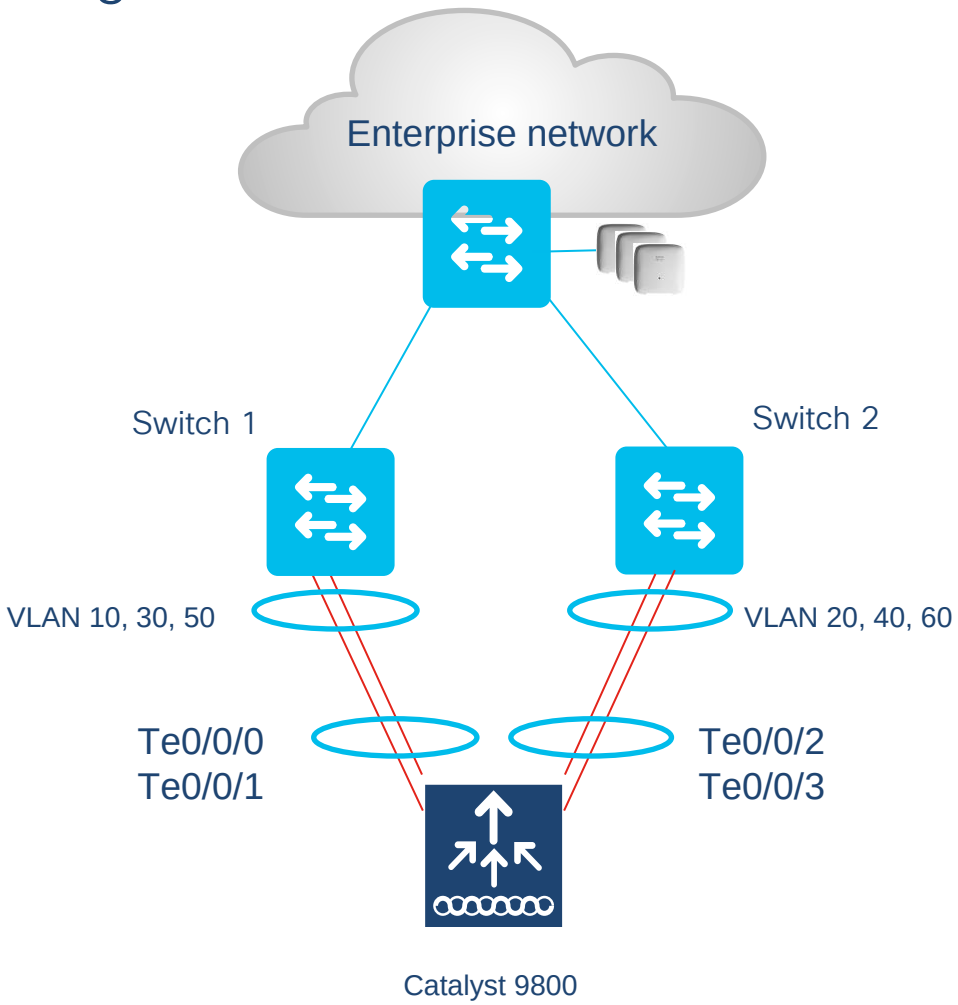
Catalyst 9800-L

Catalyst 9800-40

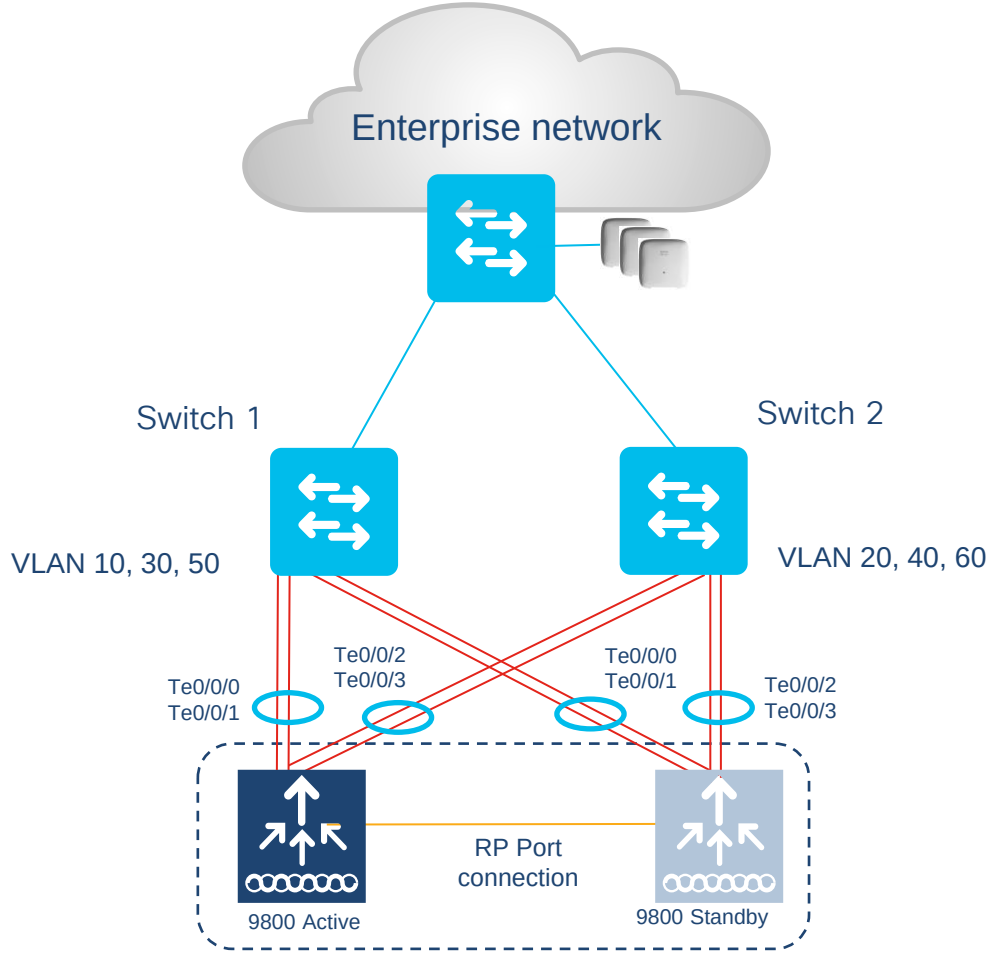
Catalyst 9800-80

Supported topologies

Single controller w/ Multi-chassis LAG

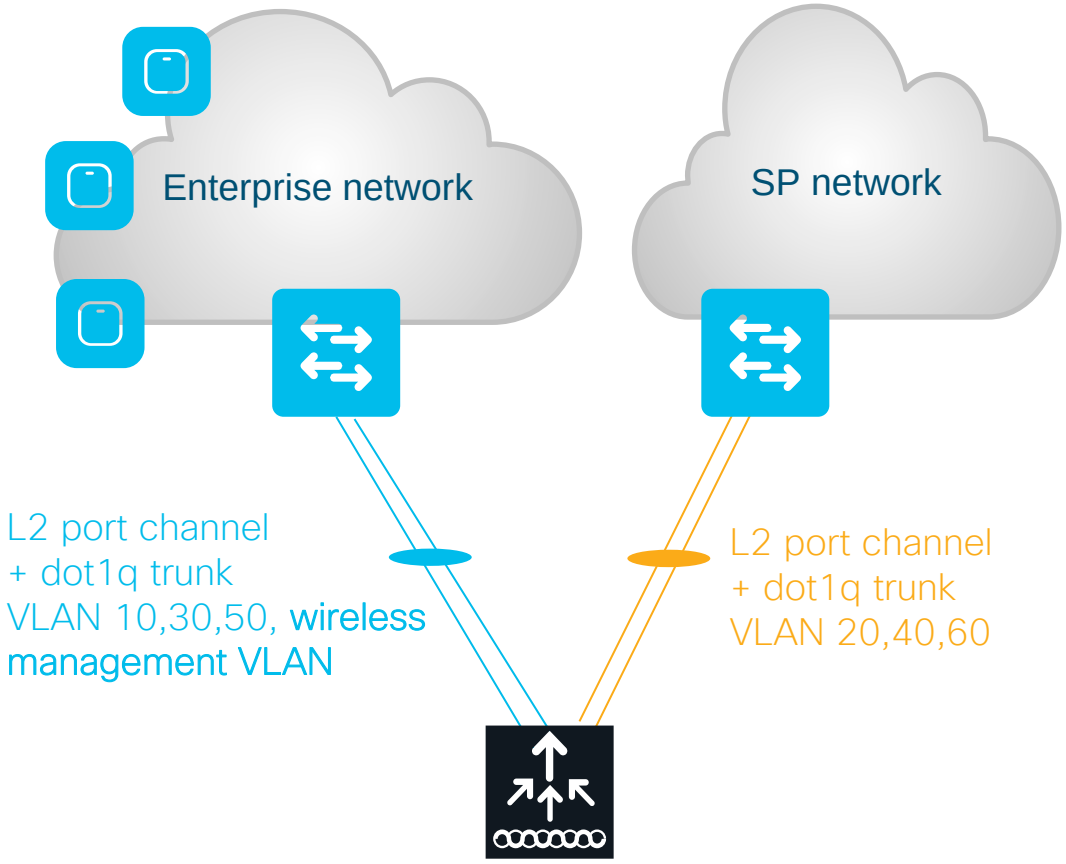


SSO Pair w/ Multi-chassis LAG



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

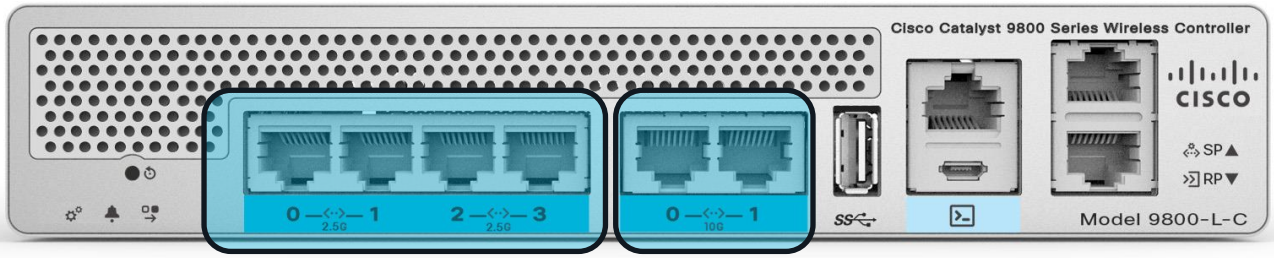
Multi-chassis LAG with separated VLANs



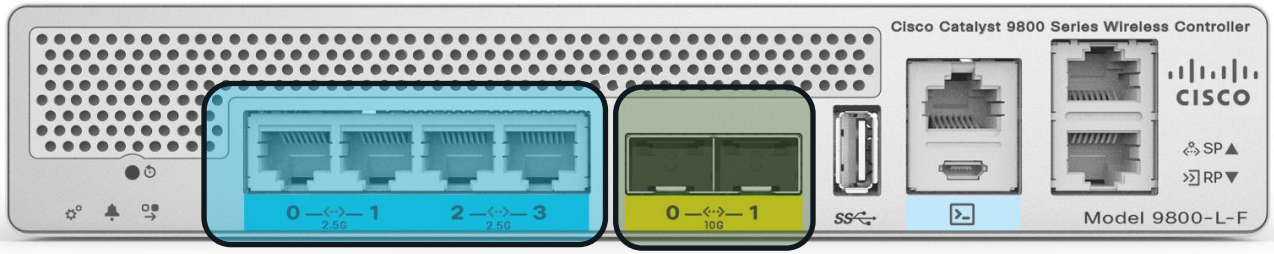
- Use case: map SSIDs to different separated wired network (e.g. Guest traffic to a separated switch/network)
- Dual uplink (port-channel or single link), each with different VLANs.
- Each LAG must be connected to a single switch.
- Different VLANs must be assigned to different LAGs.
- Note: user configuration 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**



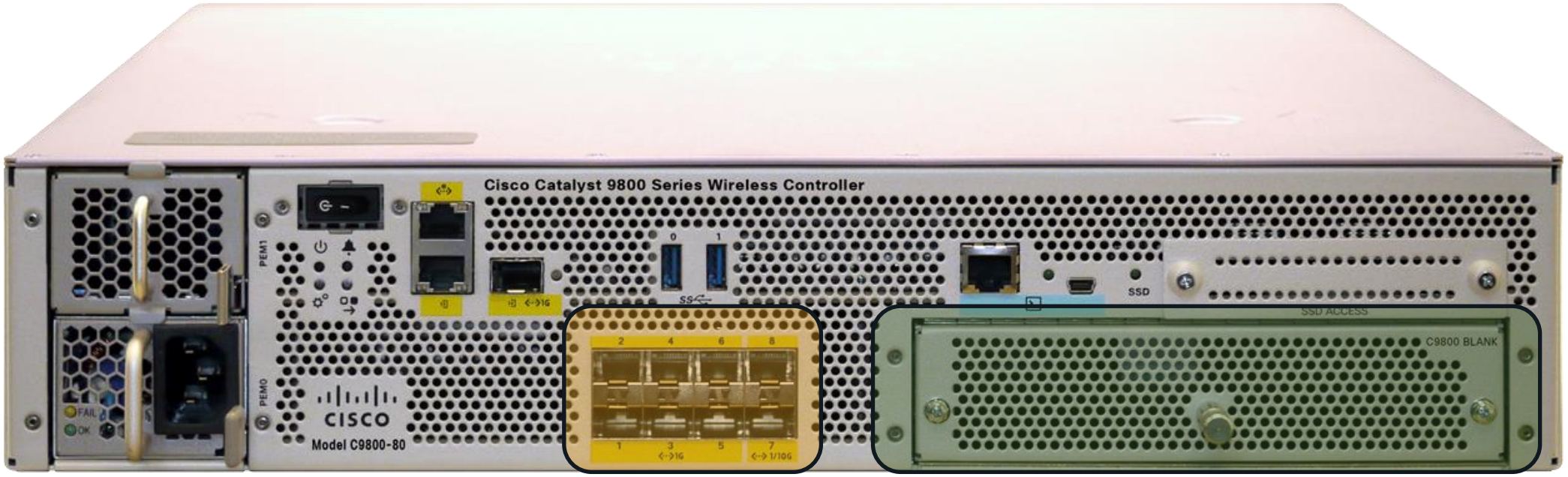
9800-L-C with 2.5G/1G and 10G/mGig ports in different port channels



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 **ports of same slot in the port channel**



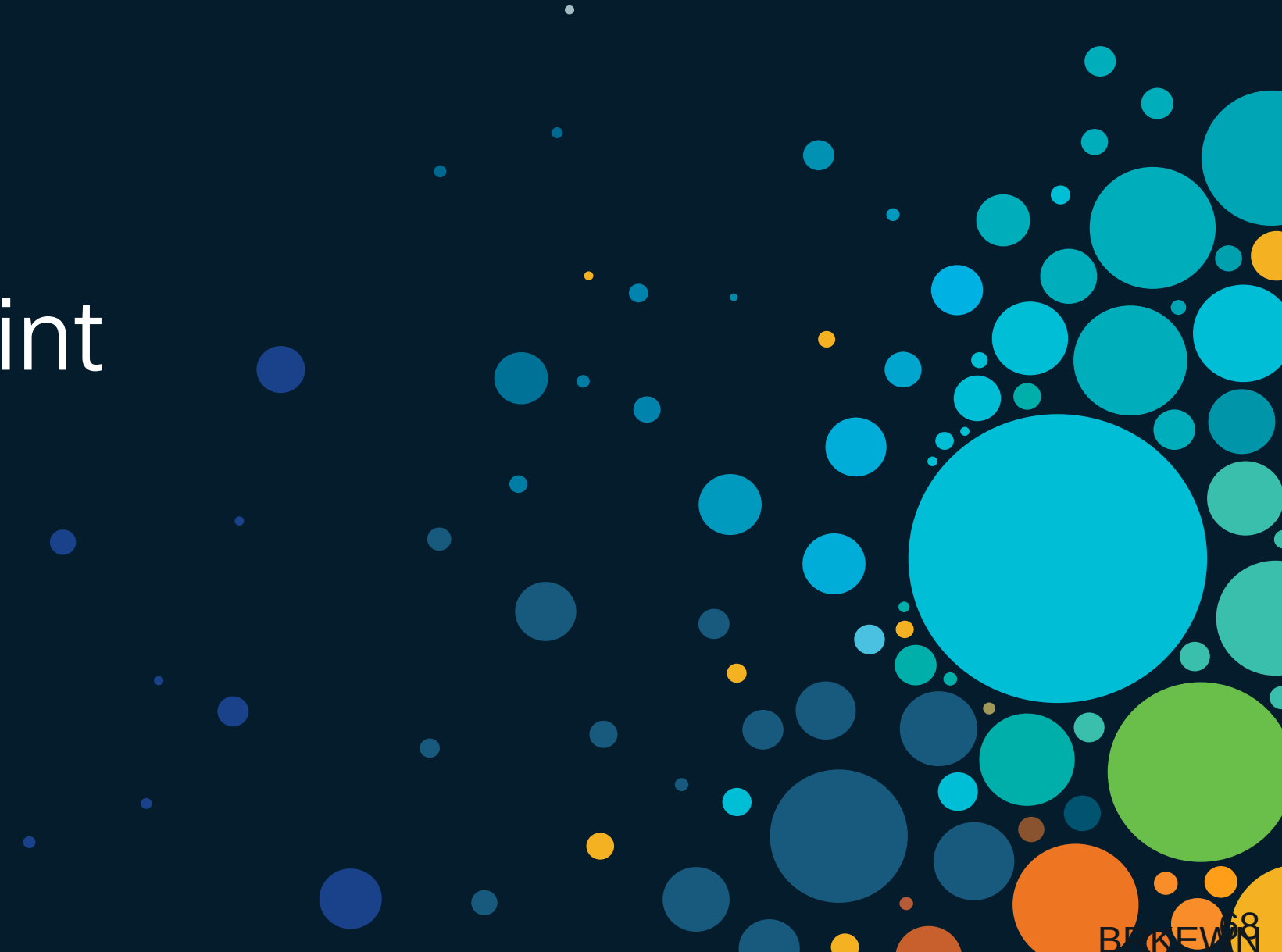
For your reference

SSO feature matrix

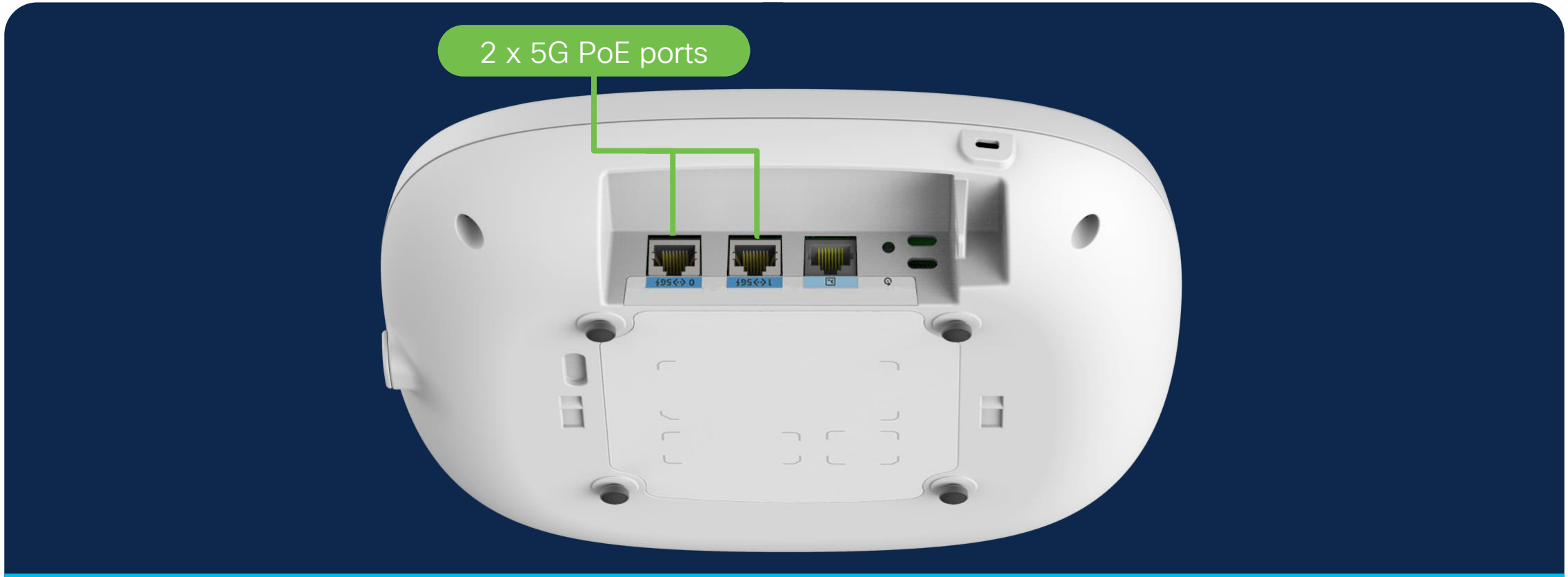
Functionality	Release	Embedded controller on 9K	9800-L	9800-40	9800-80	9800-CL PVT Cloud
RMI interface with config CLI (IPv4)	17.1	Supported	Supported	Supported	Supported	Supported
Dual Active Detection	17.1	Supported	Supported	Supported	Supported	Supported
Recovery Mode	17.1	Supported	Supported	Supported	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

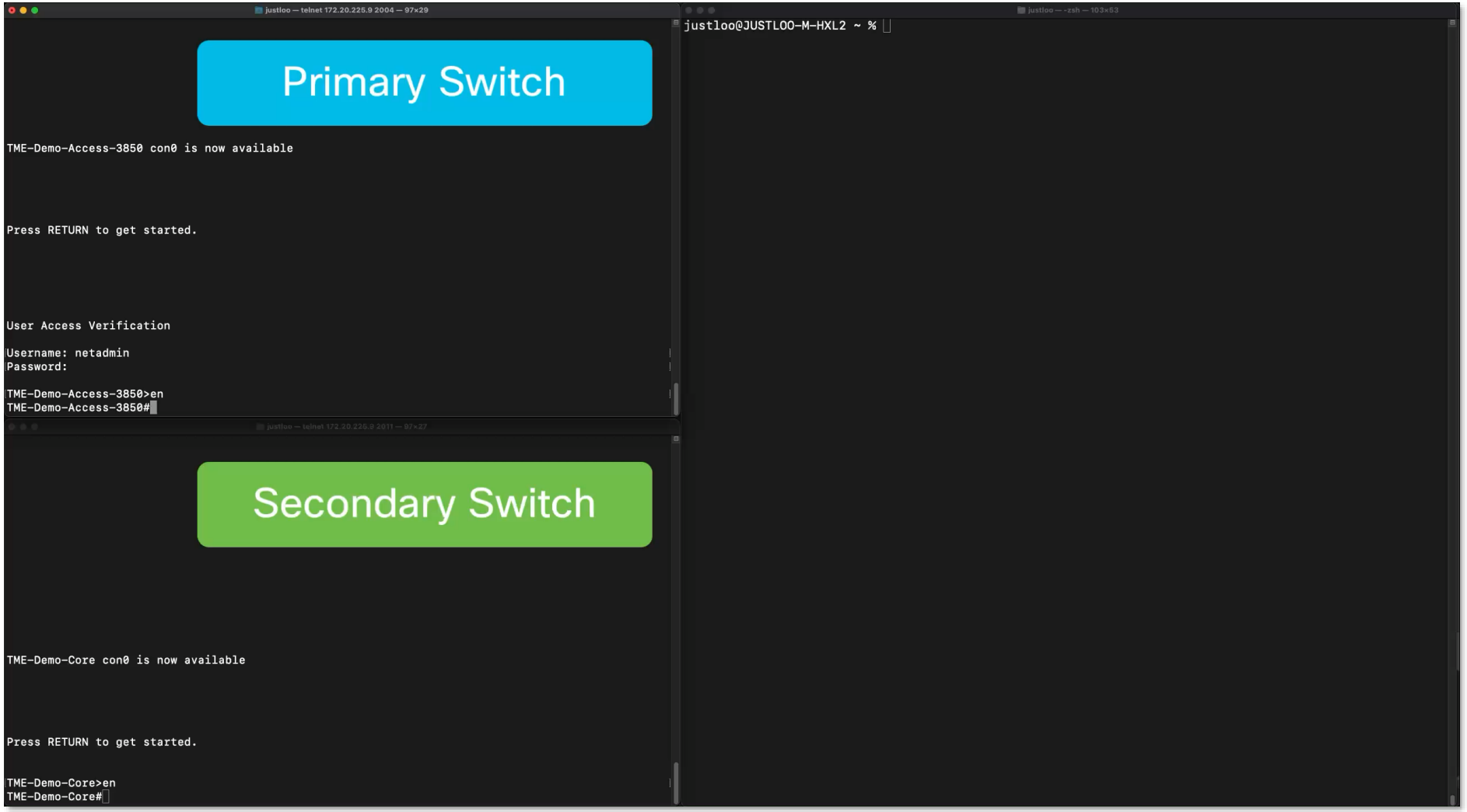
Uplink ports support:
802.3 link aggregation for increased throughput resiliency

PoE Redundancy with Catalyst 9136

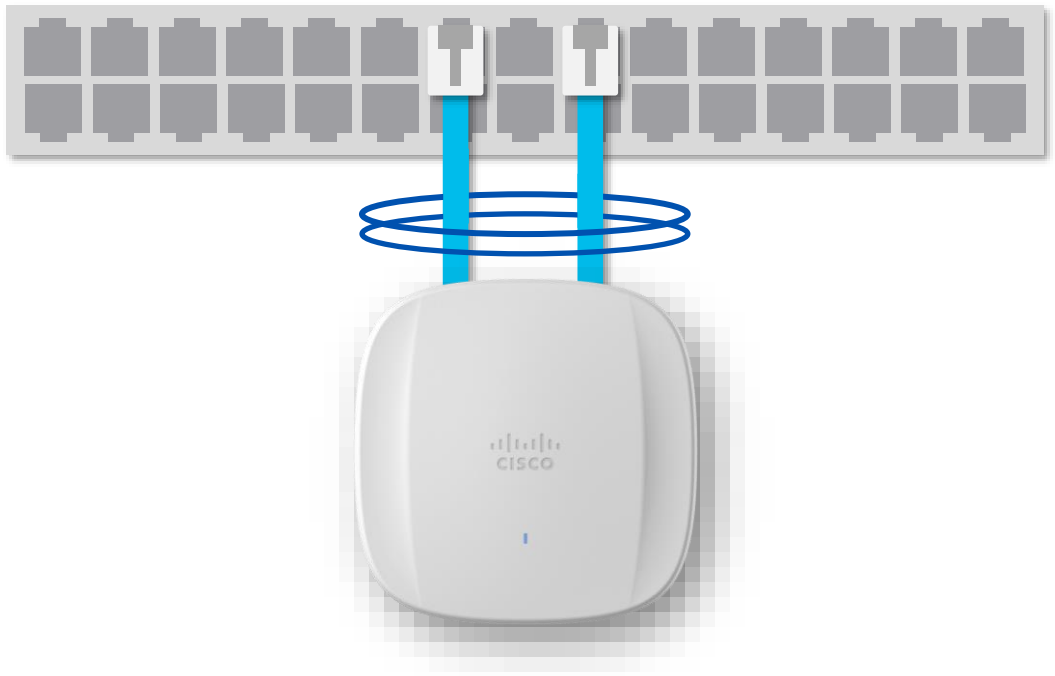
Note: Ensure both switches provide the same power level and have connectivity to the WLC.

*Can also be done with a single switch

Quick demo!



LAG on the Catalyst 9136

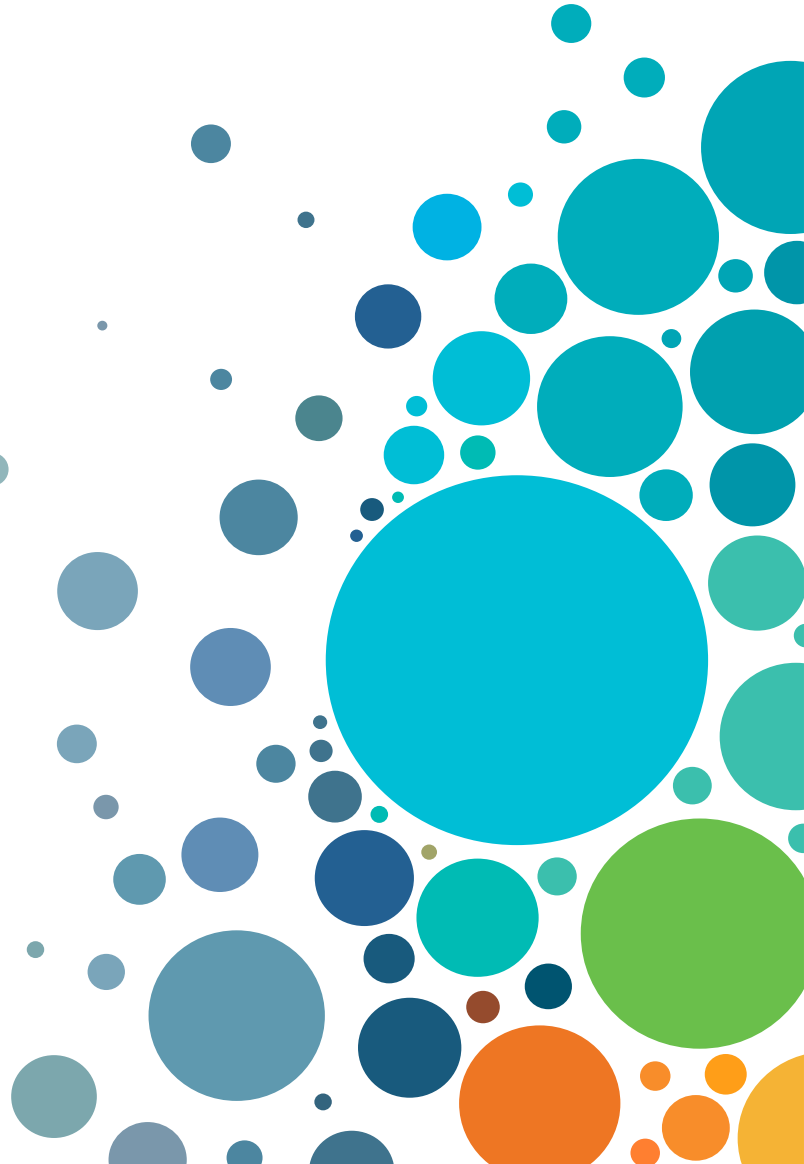


Overview

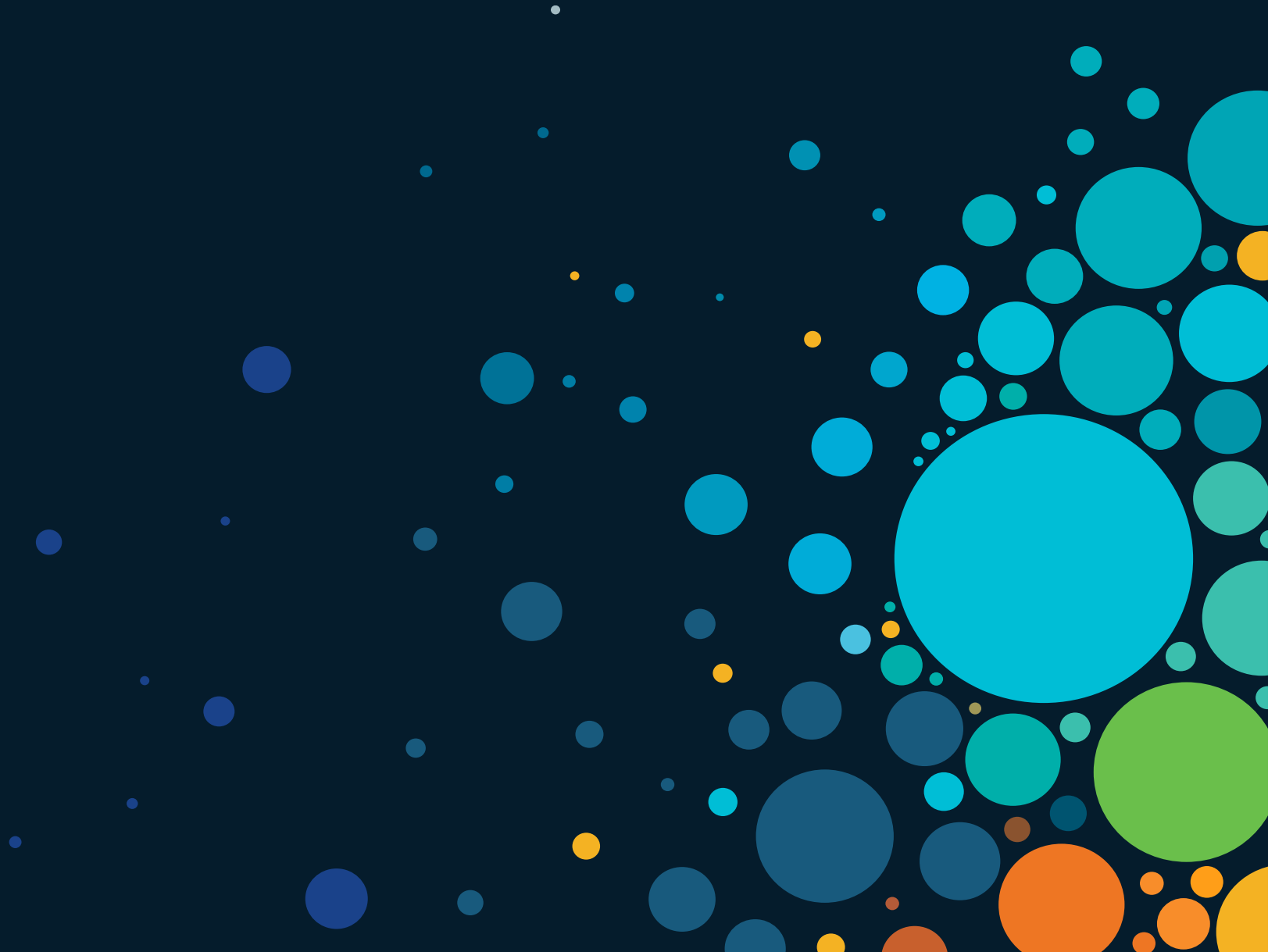
- Allows for uplink redundancy to the upstream switch
- Combined throughput of up to 5Gbps
- Supports LAG, LACP, and PAGP

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

Infrastructure updates



5. 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

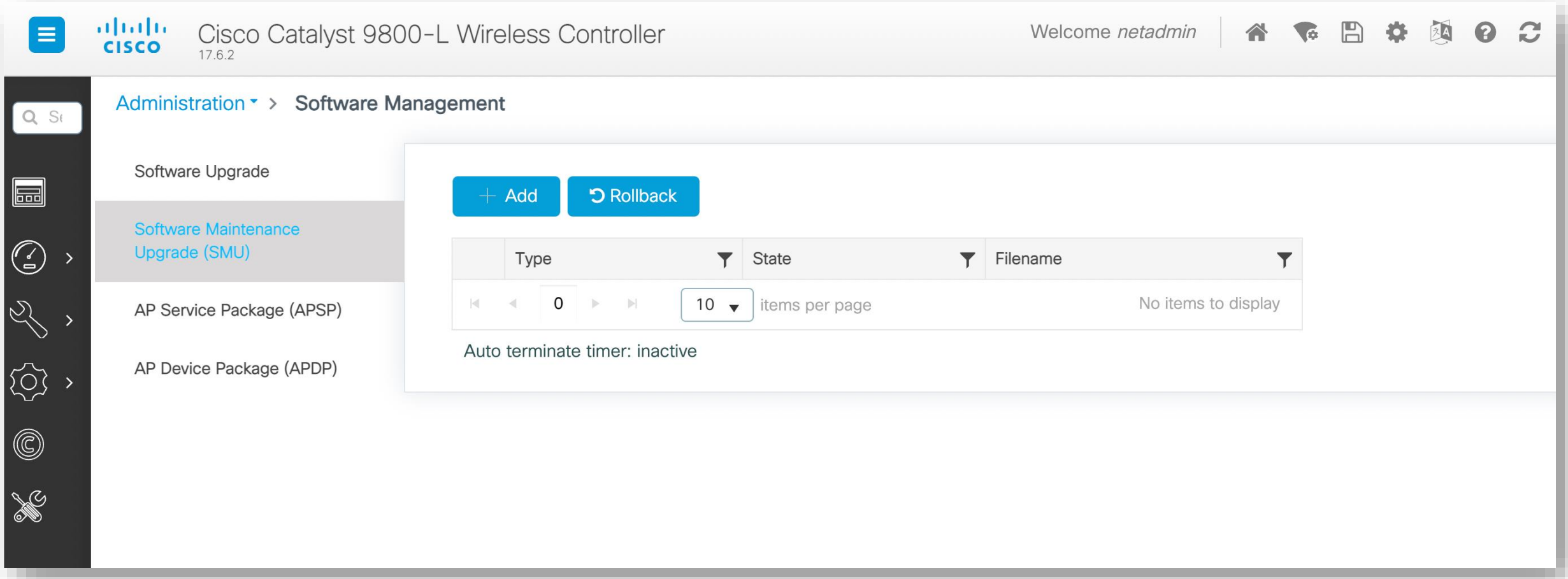
On SSO systems, SMU updates can be installed on the HA Pair with zero downtime

Controller SMU

Standalone vs Redundant Wireless Controller

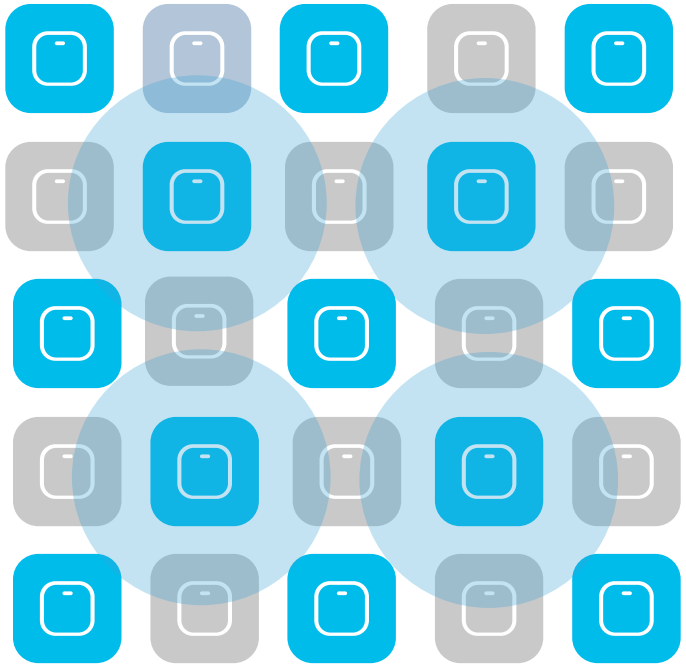
	Hot Patch (No Wireless Controller reboot) Auto Install on Standby	Cold Patch Wireless Controller Reboot
Standalone box	 No reload of Controller. AP & Client session won't be affected.	 Reload controller. AP & Client sessions would be affected.
Redundant box	 SMU activation applies patch on Active & Standby. 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.

SMU WebUI



Rolling AP Update/Upgrade Infrastructure

Neighbor marking for Rolling AP Upgrade



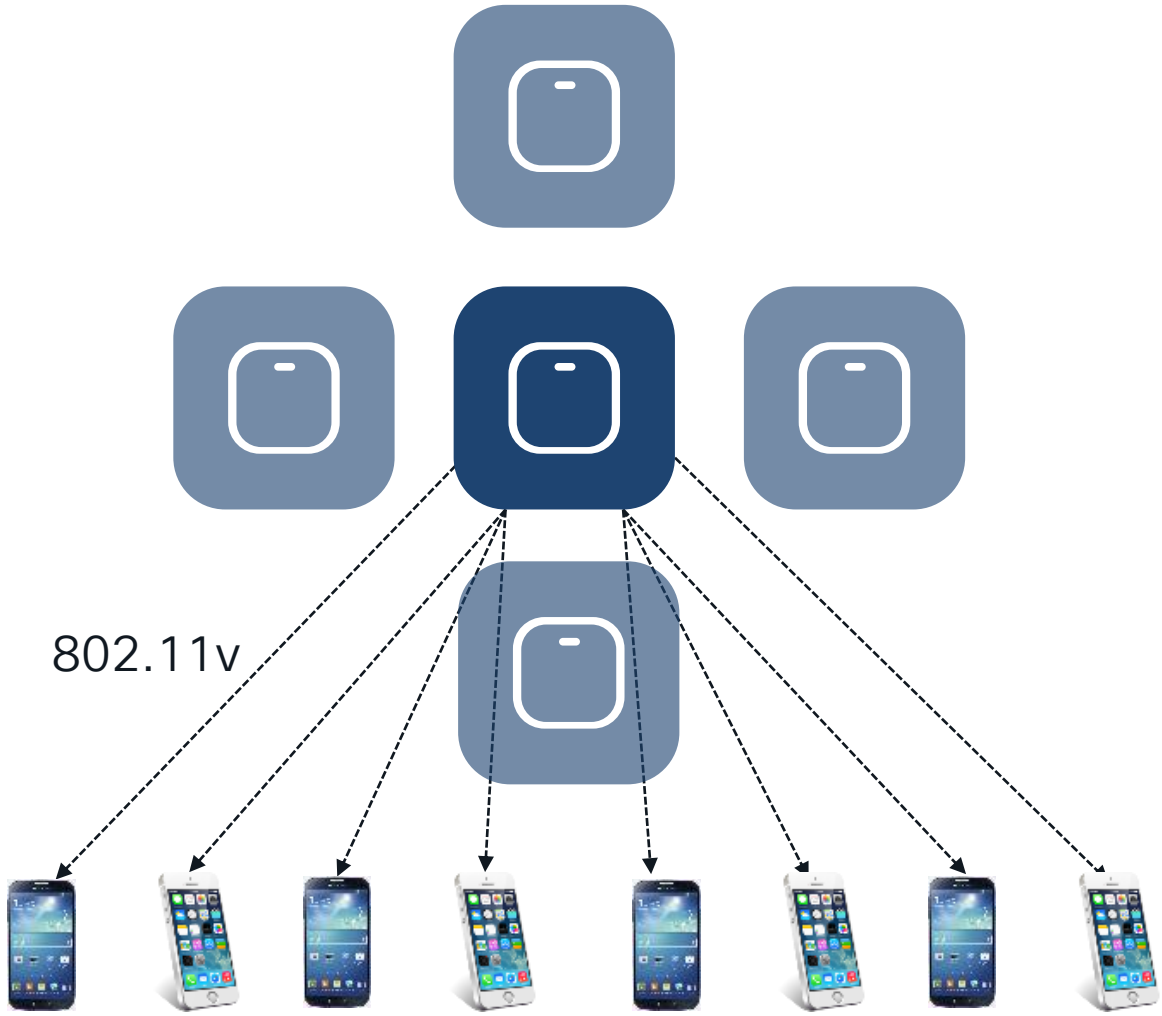
User selects % of APs to upgrade in one go [5, 15, 25]
For 25%, Neighbors marked = 6 [Expected number of iterations ~ 5]
For 15%, Neighbors marked = 12 [Expected number of iterations ~ 12]
For 5%, Neighbors marked = 24 [Expected number of iterations ~ 22]

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



Per-site & Per-AP Model AP Service Pack

cisco Live!

Per-site / Per-model AP Service Pack

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

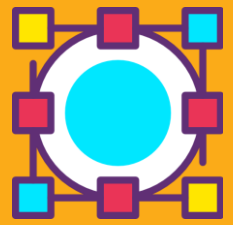
Per-model APSP works in conjunction with site-specific rollout

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

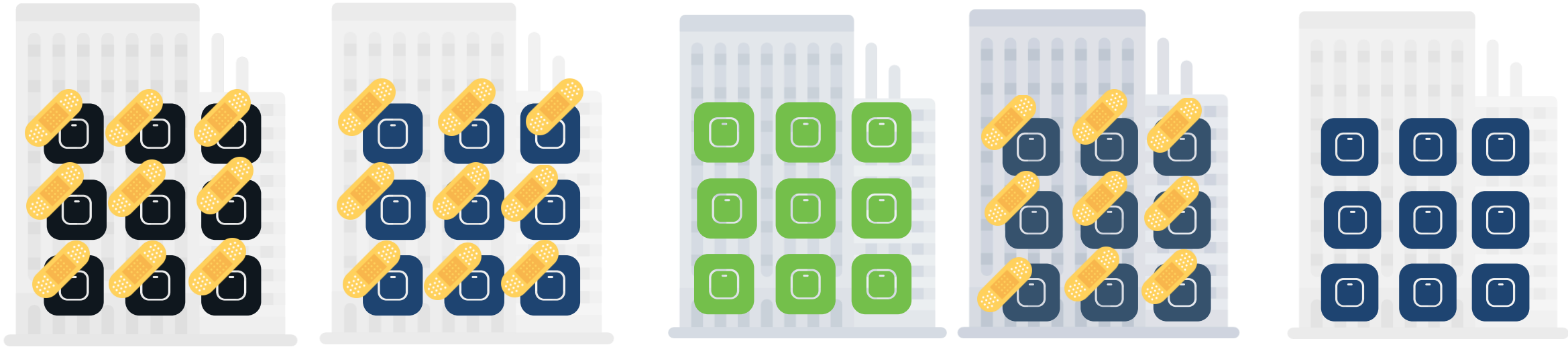
Applying APSP for 9115/9120 APs on per-site and per-model basis

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



9120AX APs 9115AX APs

SiteA

9130AX APs 9120AX APs

SiteB

9115AX APs

SiteC

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

Contain Impact within release

Deploy new hardware without need to requalify a new controller release

Reduce Lifecycle delays

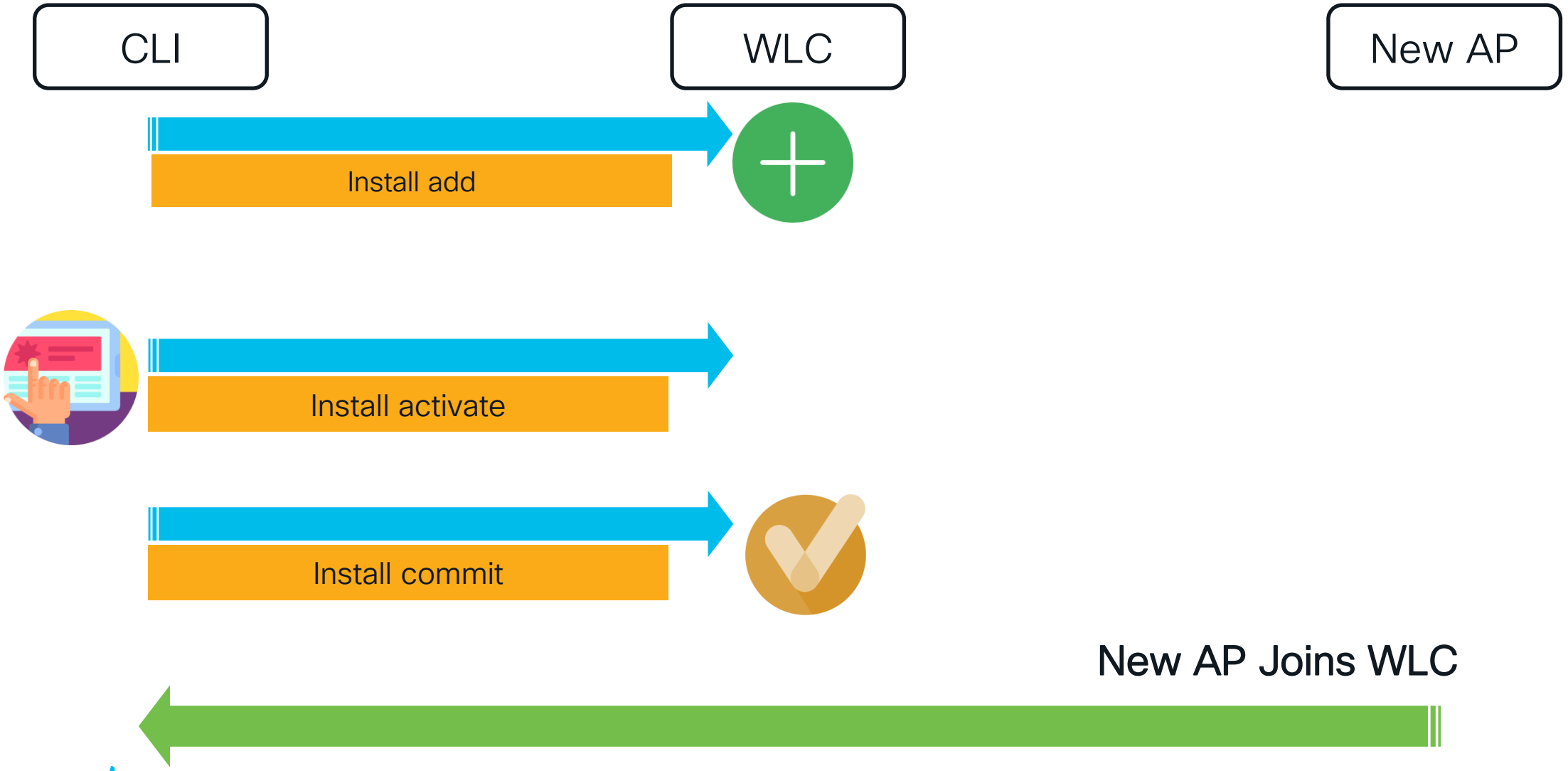
Faster deployment of latest AP hardware and technology

Zero Network Downtime

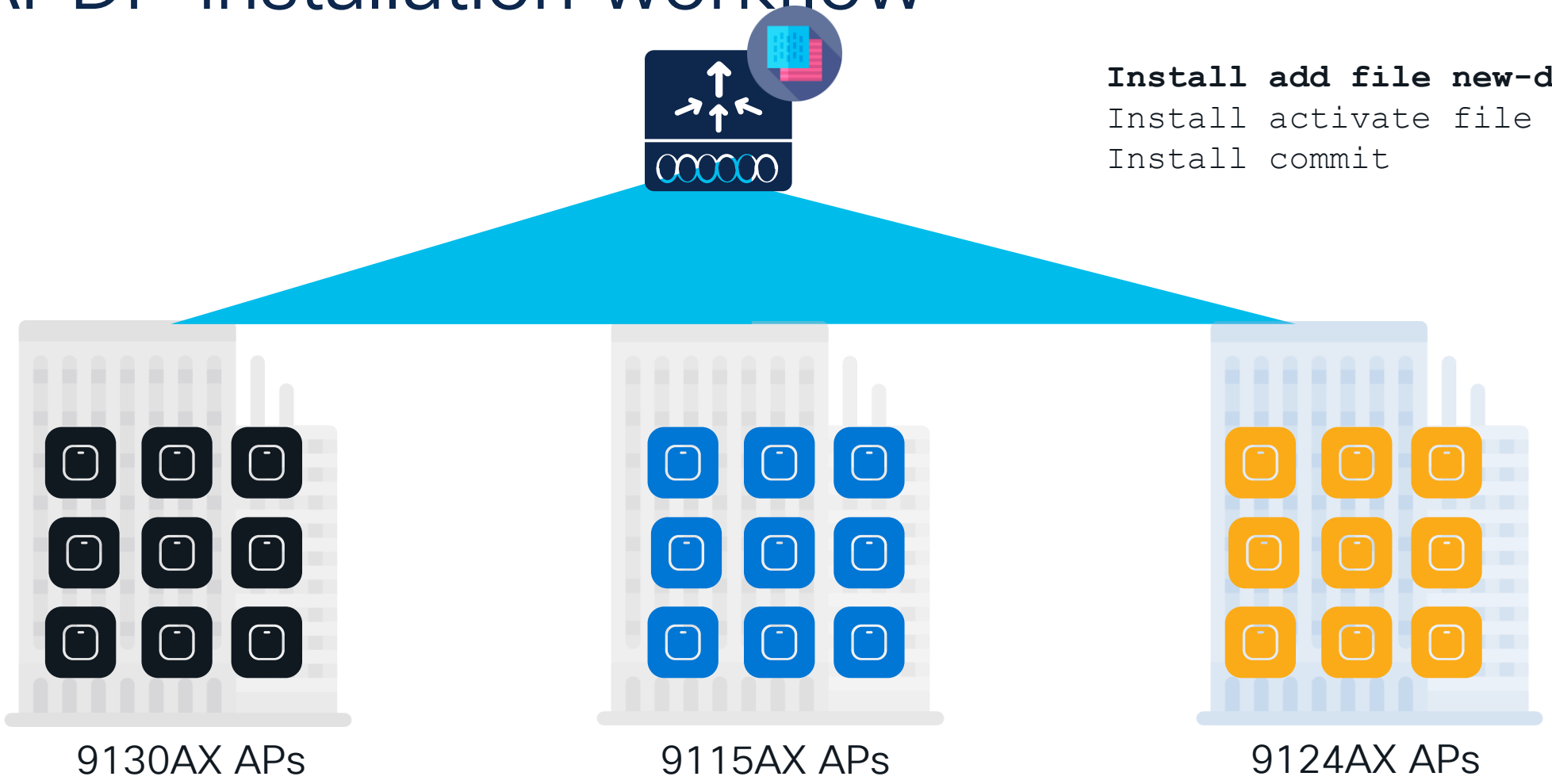
Applied as HOT patch on the controller with no service impact for APs and Clients

With AP Device Packs

APDP installation workflow



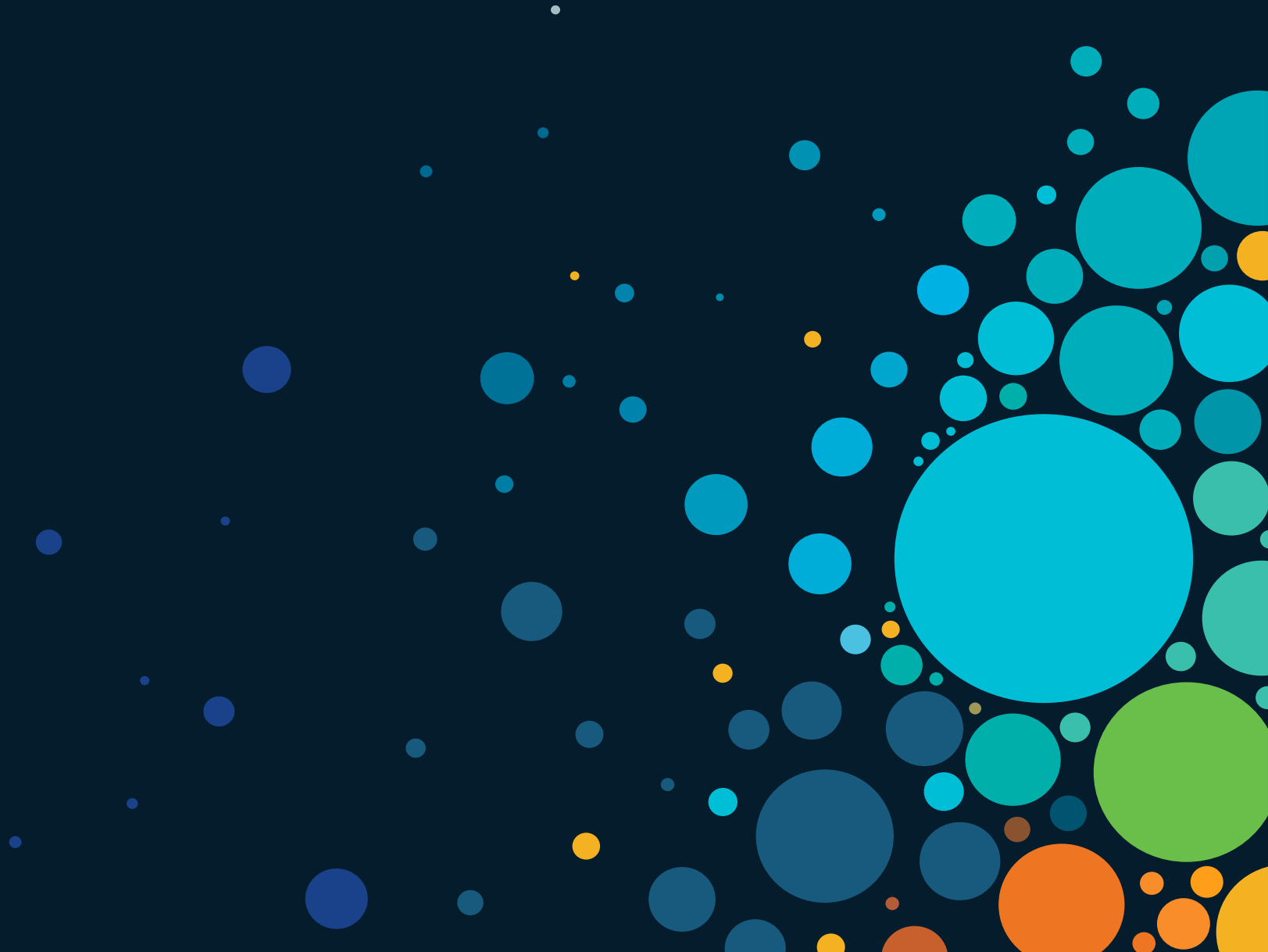
APDP installation workflow



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

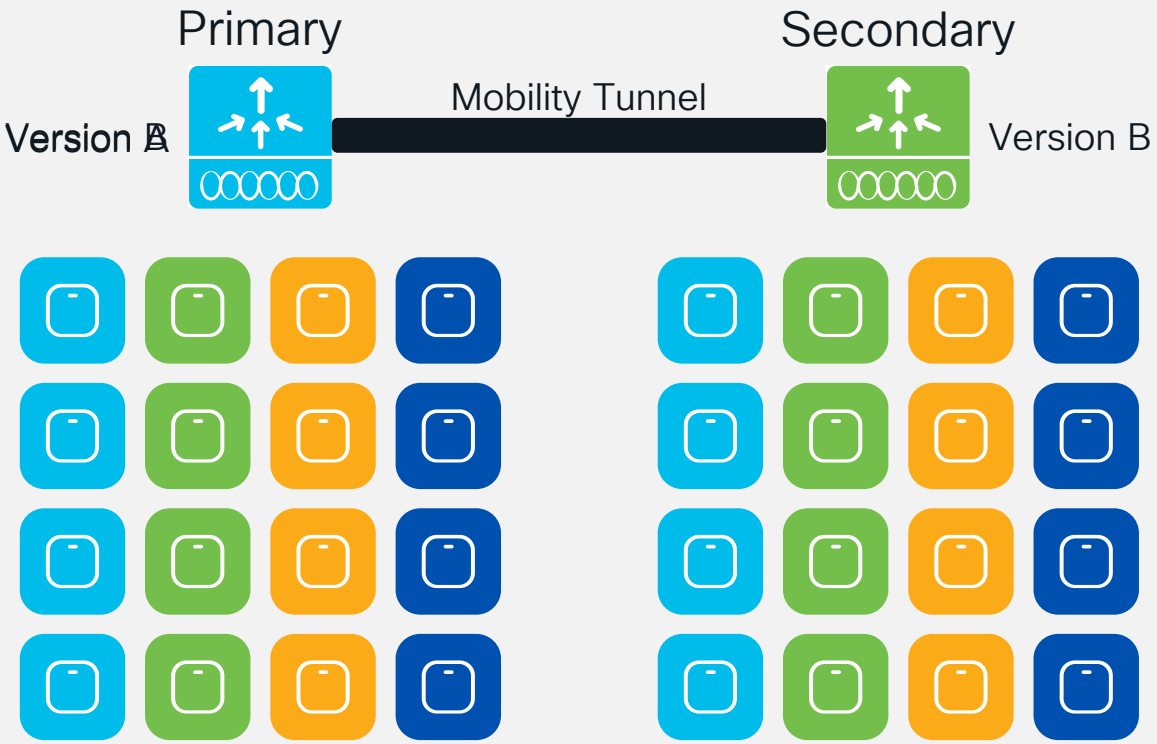
Note: Fixes for the AP installed via APDP will be via AP Service packs like a baseline supported AP.

6. Controller Software Upgrade



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

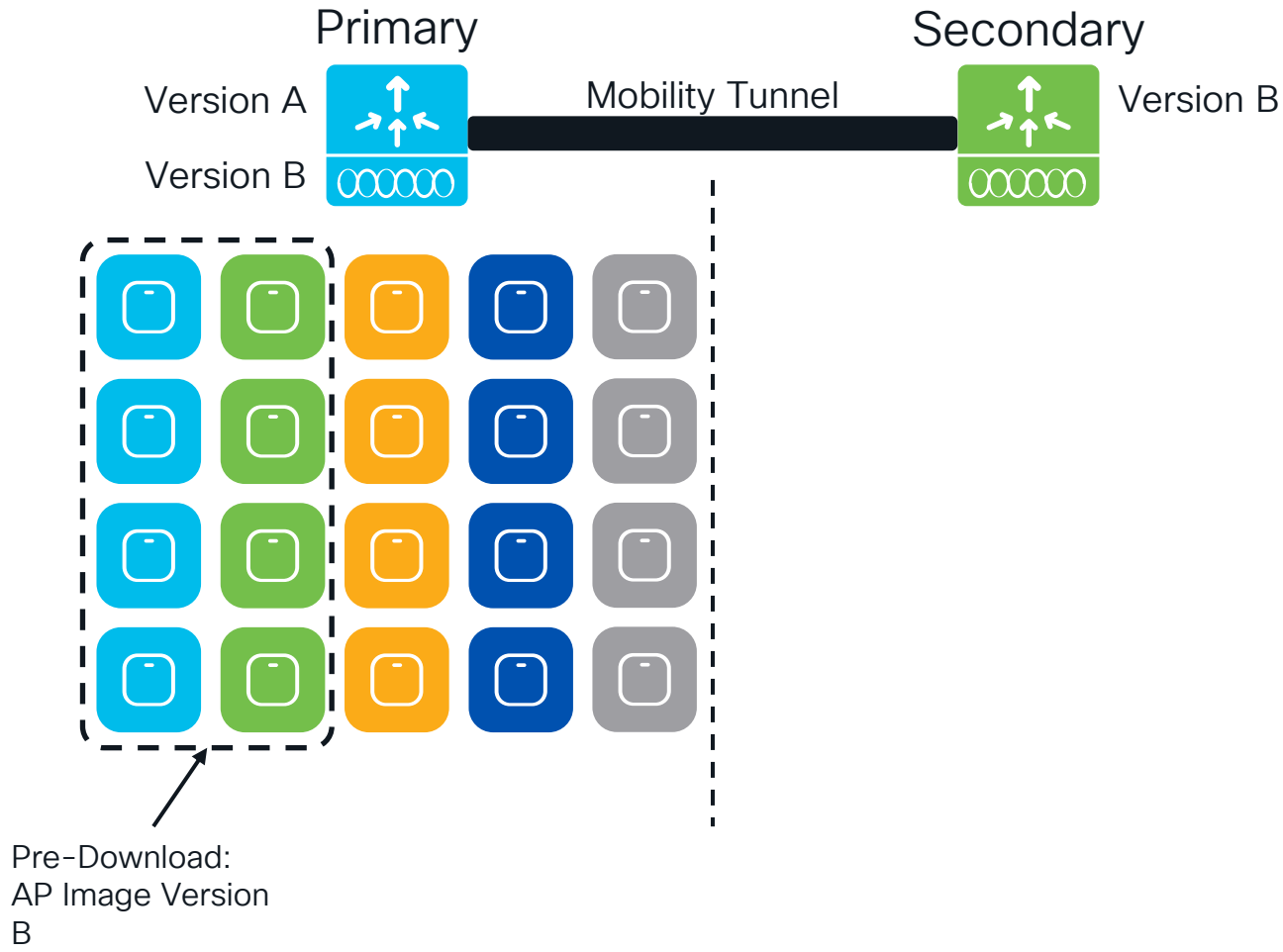
1. Add the new IOS XE image to the controller:
   `install add file <Path to Image>`

```
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`



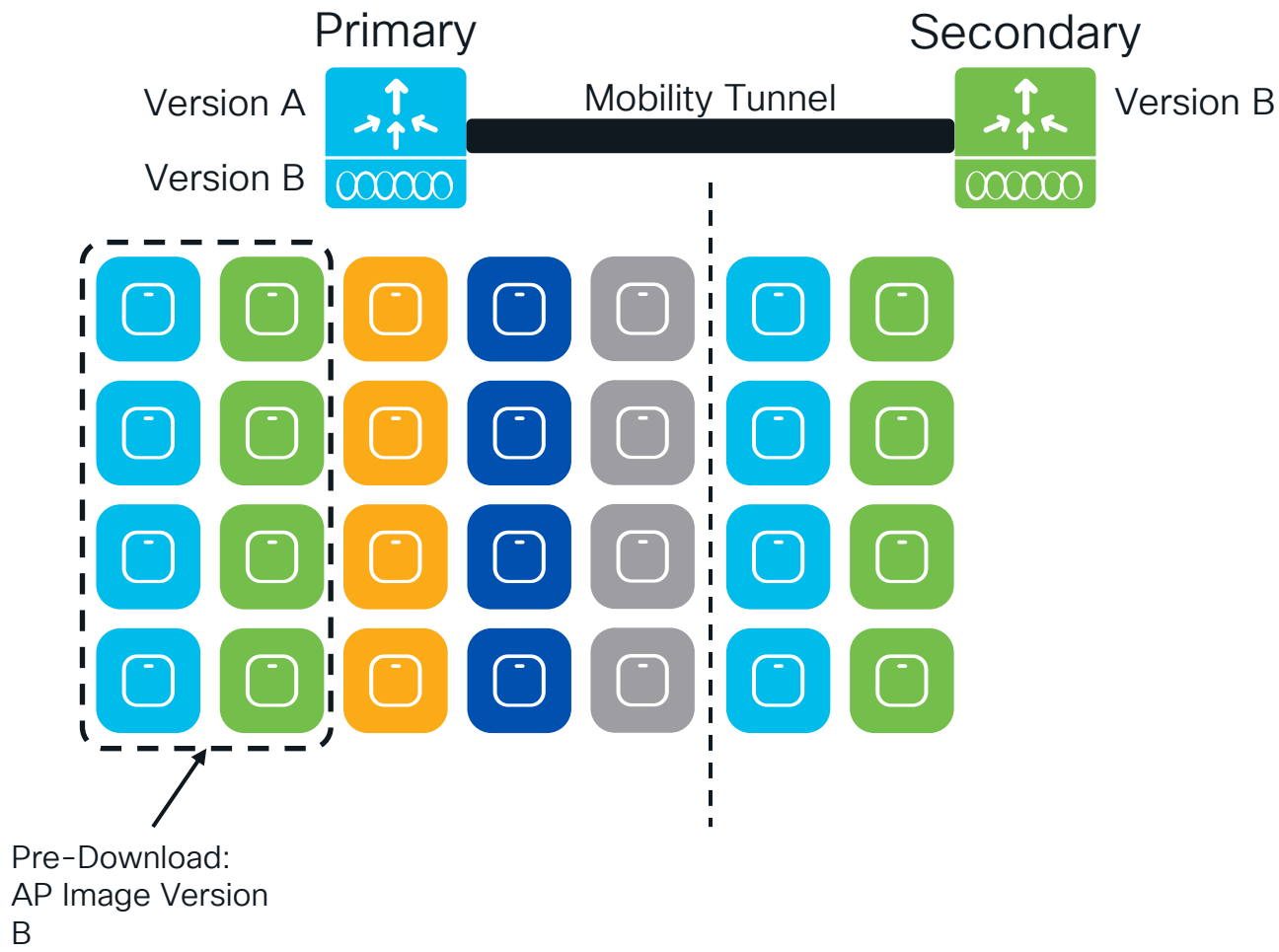
AP upgrade workflow

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.



AP upgrade workflow

Site Filter

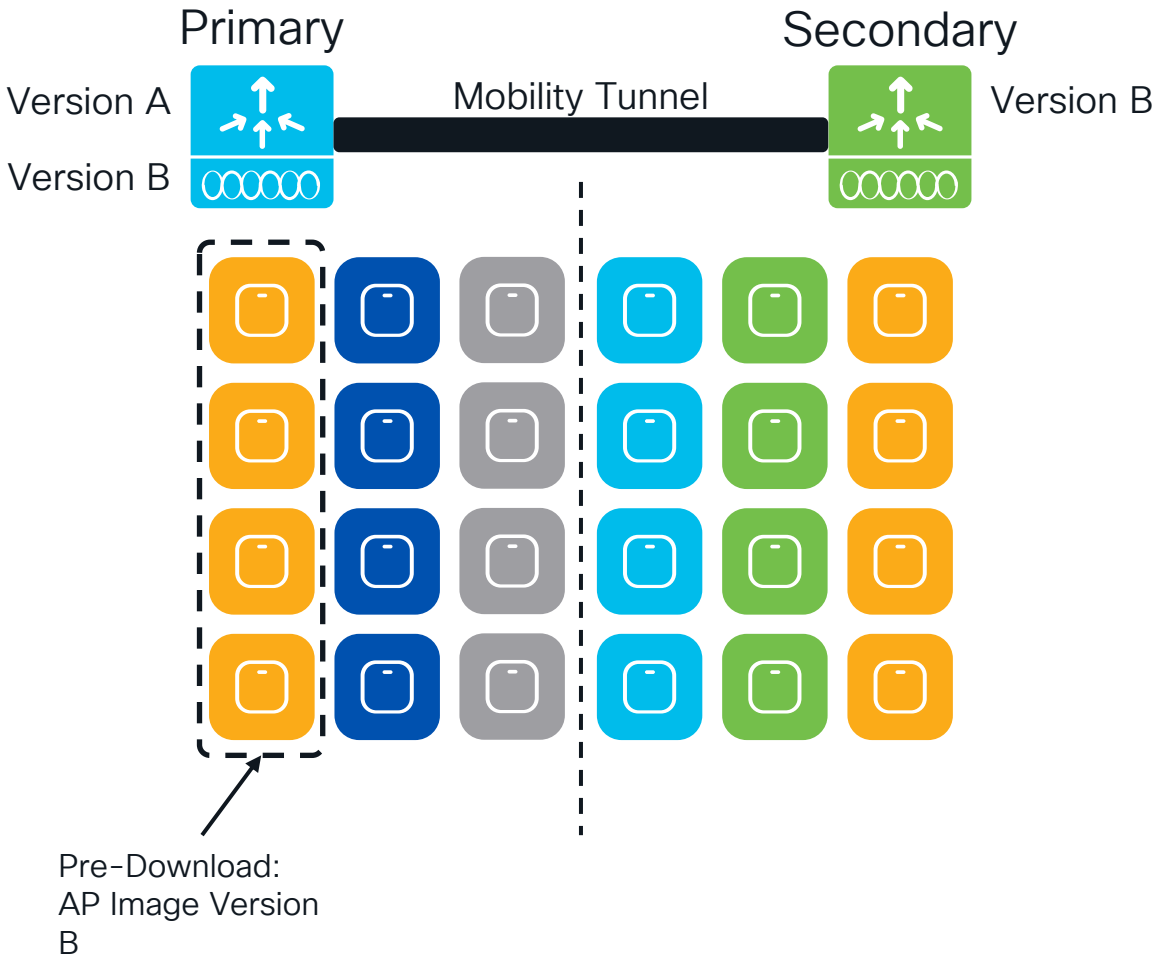
- Site 1
- Site 2
- Site 3

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

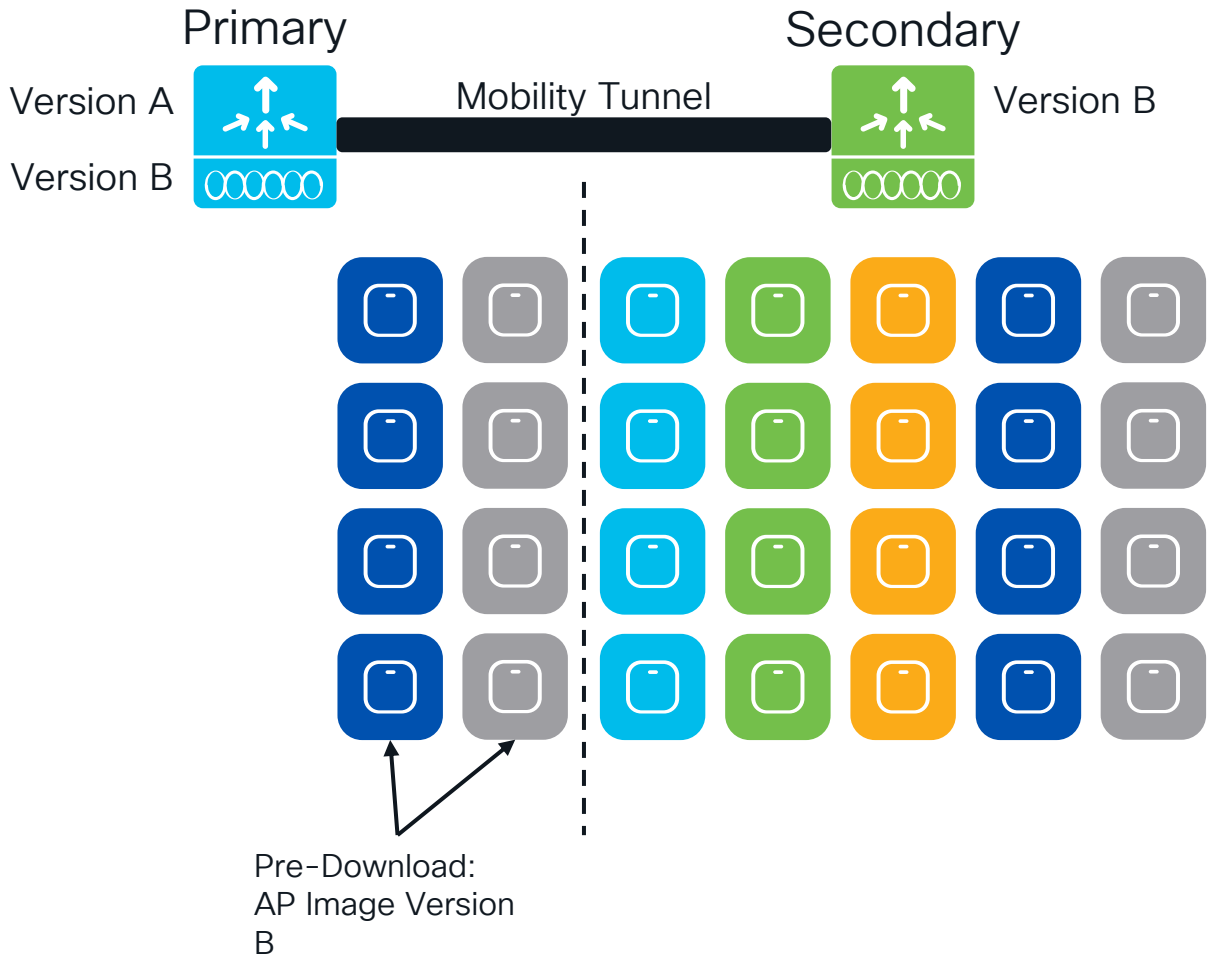
- Site 1
- Site 2
- Site 3

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.



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

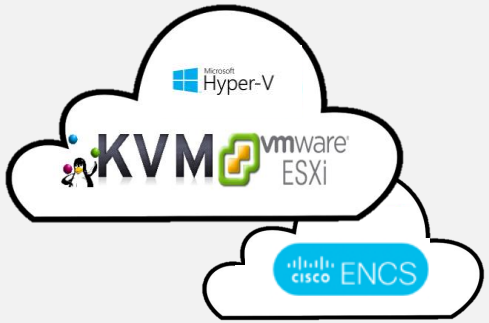
All AP/Client sessions are retained during upgrade process

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

9115, 9117, 9120, 9130, 9136 11ax APs

1815W

1815I, 1815M

1832

1842

1852

2802

3802

1700, 2700, 3700,
1570 Wave 1 APs

1540

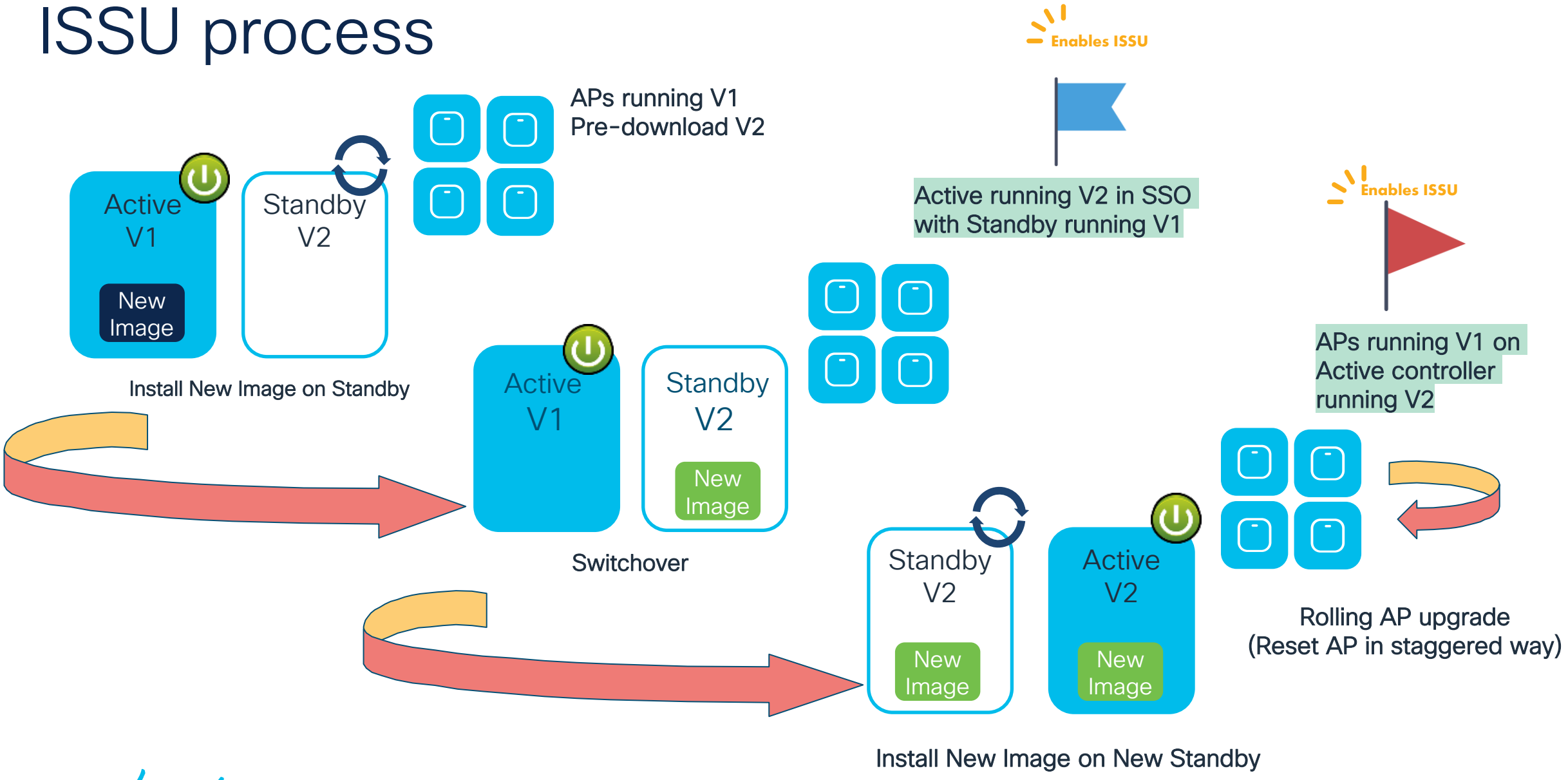
1560

4800

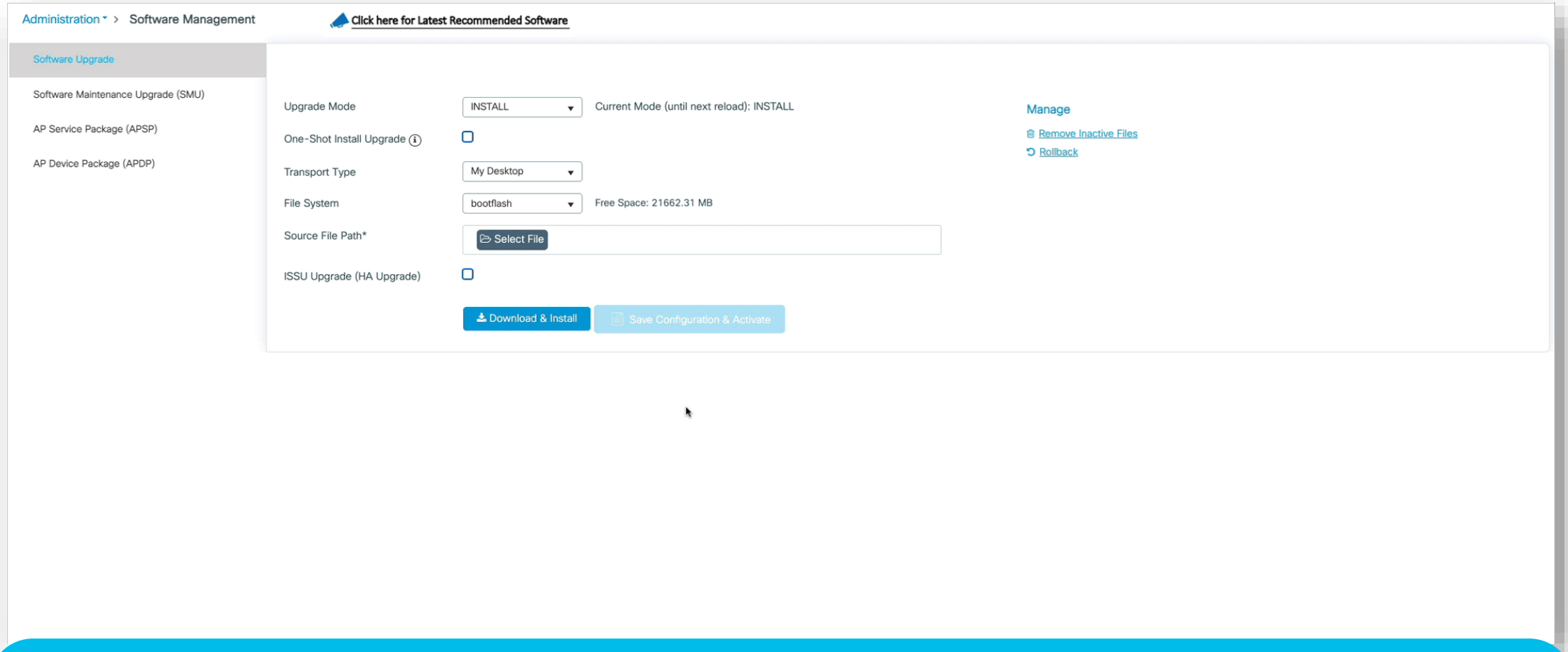
Wave 2 indoor and outdoor APs

Ensure APs are supported by target software version.

ISSU process

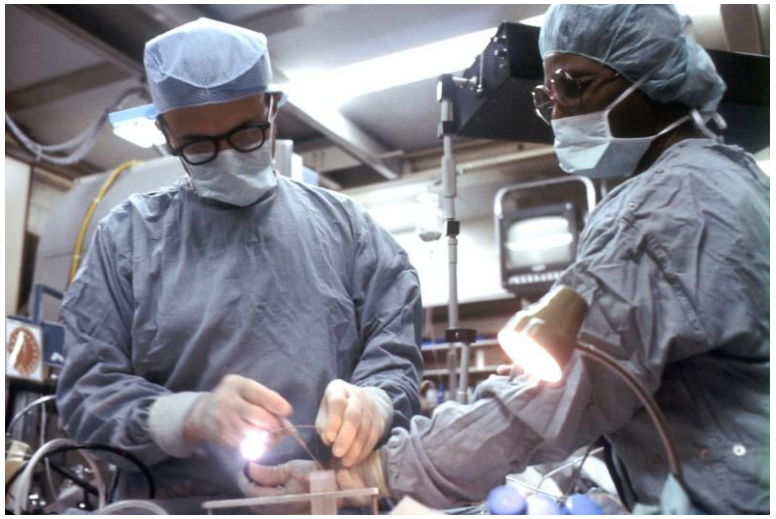


Easy ISSU upgrade with WebUI!



Few Clicks Only! : Load image → ISSU Upgrade → Click Download & Install

Achieving the zero downtime win!

Unplanned Events

- ✓ Stateful switchover with an active standby
- ✓ N+1 redundancy for always-on network, services, and clients
- ✓ Access Point link redundancy

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

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

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

cisco Live!


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

#CiscoLive