High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5

First Published: March 31, 2021

Cisco Systems, Inc. www.cisco.com

Table of Contents

Introduc)on 5

Overview ....

Cisco Confidential

5 Feature Descrip)on and Func)onal Behavior ....

5 Pla;orms Supported ....

6 SSO Pre-requisites 6

SSO on Cisco Catalyst C9800-40-K9 and C9800-80-K9 Wireless Controllers 6

Physical Connec)vity for C9800-L, C9800-40 and C9800-80 Wireless Controller HA SSO 7

Connec&ng C9800-L Wireless Controllers using RJ-45 RP Port for SSO ....

7 Connec&ng C9800-40 and 9800-80 Wireless Controllers using RJ-45 RP Port for SSO

.... 8

Connec&ng C9800-40 and 9800-80 Wireless Controllers using SFP Gigabit RP Port for SSO

.. 8

Connec&ng a C9800 wireless controller HA pair to upstream switches ....

8 Op&on 1: Single VSS switch (or stack/VSL pair/modular switch) with RP back-to-back 9

Op&on 2: Single VSS switch (or stack/VSL pair/modular switch) with RP via upstream ...

9

Op&on 3: Dual Distributed switches with HSRP 10

Connec)ng a C9800 wireless controller HA pair to upstream switches with Release 17.1 and above ....

10 SSO on Cisco Catalyst C9800-CL running on ESXi, KVM, Hyper-V ....

11 Configuring High Availability SSO using GUI ....

11 Configuring High Availability SSO using CLI ....

12 Mobility MAC

Cisco Confidential

.. 13 Ac)ve and Standby Elec)on Process .... 14 State Transi)on for HA SSO Pair forma)on 14

Monitoring the HA Pair 16

Monitoring HA Pair from CLI 19

Verifying Redundancy States 19

Accessing standby wireless controller console 21

Switchover Func)onality 22

Process Failure Switchover .... 22 Power-fail Switchover 22

Manual Switchover 22

Failover Process 23

Ac&ve wireless controller 23

Standby wireless controller 23

Verifying AP and Client SSO State Sync 24

SSO Failover Time Metrics 24

Redundancy Management Interface 24

Redundancy Management Interface Configura&on using WebUI 25

Programma&c configura&on of RMI IPs 25

Dual Stack support with RMI IPv4 26

Dual Stack Support with RMI IPv6 26

Peer Timeout Configura&on 26

Redundancy Management Interface Configura&on using CLI 27

Verifying RMI and RP configura&on 28

Cisco Confidential

RMI and RP pairing combina&ons 28

Upgrade and HA Pairing with no previous HA config 28

Upgrade already Paired controllers 29

Downgrade 29

Default Gateway Check 30

Configuring Gateway Failure Detec)on Interval 31

Default Gateway Check WebUI Configura&on 33

Default Gateway Check CLI Configura&on 33

System and Network Fault Handling 34

HA Unpairing Behavior 38

LACP, PAGP support in SSO Pair 40

Supported LACP, PAGP topologies 40

Mul)-chassis Link Aggrega)on group 40

Supported Mul&-chassis LAG topologies 41

Supported Pla]orms: 41

Supported LAG Port Grouping 42

Sample LAG Configura)on for HA SSO pair connec)ng to a VSS Pair with Split Links 42

On the wireless Controller 42

On the VSS 46

Replacing a controller in an HA setup 49

N+1 with SSO Hybrid deployment 50

Standby Monitoring using RMI 50

Standby Monitoring CLIs 50

Standby Monitoring Programma&c Interfaces 52

Steps to monitor the standby controller using SSH to RMI IPv4 53

Command for Standby Monitoring using RESTCONF 54

Standby Monitoring in release 17.5 54

Cisco Confidential

Cisco Confiden+al

Introduction

High availability has been a requirement on wireless controllers to minimize downtime in live networks. This document provides information on the theory of operation and configuration for the Catalyst 9800 Wireless Controller as it pertains to supporting stateful switchover of access points and clients (AP and Client SSO). Catalyst 9800 Wireless Controller is the next generation wireless controller that can run on multiple platforms with different scalability goals from low to high scale. AP and Client SSO is supported on the physical appliances and the virtual cloud platforms of the Catalyst 9800 Wireless Controller, namely C9800-L, C9800-40, C9800-80 and C9800-CL. The underlying SSO functionality is the same on all platforms with some differences in the setup process.

Overview

The High availability SSO capability on wireless controller allows the access point to establish a CAPWAP tunnel with the Active wireless controller and the Active wireless controller to share a mirror copy of the AP and client database with the Standby wireless controller. The APs do not go into the Discovery state and clients do not disconnect when the Active wireless controller fails and the Standby wireless controller takes over the network as the Active wireless controller. There is only one CAPWAP tunnel maintained at a time between the APs and the wireless controller that is in an Active state.

Release 16.10 supports full access point and Client Stateful Switch Over. Client SSO is supported for clients which have already completed the authentication and DHCP phase and have started passing traffic. With Client SSO, a client's information is synced to the Standby wireless controller when the client associates to the wireless controller or the client’s parameters change. Fully authenticated clients, i.e. the ones in Run state, are synced to the Standby and thus, client reassociation is avoided on switchover making the failover seamless for the APs as well as for the clients, resulting in zero client service downtime and zero SSID outage. The overall goal for the addition of AP and client SSO support to the Catalyst 9800 Wireless controller is to reduce major downtime in wireless networks due to failure conditions that may occur due to box failover, network failover or power outage on the primary site.

Feature Description and Functional Behavior

All the control plane activities are centralized and synchronized between the active and standby units. The Active Controller centrally manages all the control and management communication. The network control data traffic is transparently switched from the standby unit to the active unit for centralized processing.

Bulk and Incremental configuration is synced between the two controllers at run-time and both controllers share the same IP address on the management interface. The CAPWAP state of the Access Points that are in Run State is also synched from the active wireless controller to the Hot-Standby wireless controller allowing the Access Points to be state-fully switched over when the Active wireless controller fails. The APs do not go to the Discovery state when Active wireless controller fails, and Standby wireless controller takes over as the Active wireless controller to serve the network.

The two units form a peer connection through a dedicated RP port (this can be a physical copper or fiber port) or a virtual interface for the VM. The Active/Standby election happens at boot time and it’s either based on the highest priority (priority range is <1-2>) or the lowest MAC if the priority is the same. By default the C9800 has a priority of 1. Once the HA pair is formed, all the configuration and AP and client databases are synched between Active and standby. Any configuration is done on the Active is automatically synch to the Standby. The standby is continuously monitoring the Active via keepalives over the RP link. If the Active becomes unavailable, the standby assumes the role of Active. It does that by sending a Gratuitous ARP message advertising to the network that it now owns that wireless management IP address. All the configurations and databases are already in synch, so the standby can take over without service disruption.

Cisco Confidential

There is no pre-empt funcMonality with SSO meaning that when the previous AcMve wireless controller resumes operaMon, it will not take back the role as an AcMve wireless controller but will negoMate its state with the current AcMve wireless controller and transiMon to Hot-Standby state.

Pla9orms Supported

- Cisco Catalyst C9800-40 Wireless Controller
- Cisco Catalyst C9800-80 Wireless Controller
- Cisco Catalyst C9800-CL Wireless Controller
- Cisco Catalyst C9800-L Wireless Controller

SSO Pre-requisites

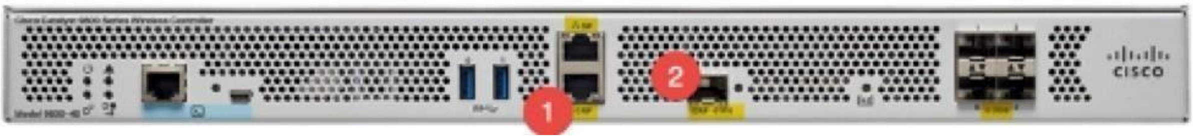
- HA Pair can only be form between two wireless controllers of the same form factor
- HA between 9800-L-C and 9800-L-F cannot be formed
- HA between Copper RP and Fiber RP cannot be formed
- Both controllers must be running the same sohware version in order to form the HA Pair

- Maximum RP link latency = 80 ms RTT, minimum bandwidth = 60 Mbps and minimum MTU = 1500

- Connect RPs via switches to enable controller HA. Ensure that the round-trip time between the two controllers is less than 80 milliseconds.

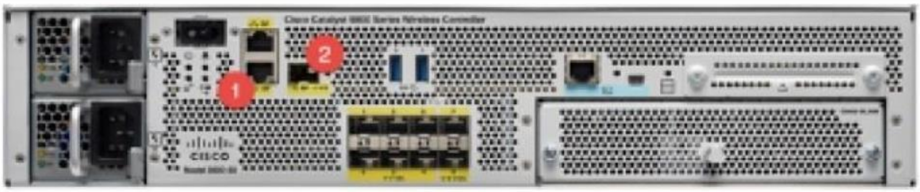
SSO on Cisco Catalyst C9800-40-K9 and C9800-80-K9 Wireless Controllers

The Cisco C9800-40-K9 wireless controller is an extensible and high performing wireless controller, which can scale up to 2000 access points and 32000 clients. The controller has four 10G data ports and a throughput of 40G.



1	RP— RJ-45 1G redundancy Ethernet port.	2	Gigabit SFP RP port

The Cisco C9800-80-K9 Wireless Controller is a 100G wireless controller that occupies two rack unit space and supports a pluggable Module slot, and eight built-in 10GE/1GE interfaces.



High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5

Physical ConnecMvity for C9800-L, C9800-40 and C9800-80 Wireless Controller HA SSO

1	RP— RJ-45 1G redundancy Ethernet port.	2	Gigabit SFP RP port

Both C9800-40-K9 and C9800-80-K9 Wireless controllers have two RP Ports as shown in the figures above:

■ RJ-45 Ethernet Redundancy port

■ SFP Gigabit Redundancy Port

If both the Redundancy Ports are connected:

■ SFP Gigabit Ethernet port takes precedence if they are connected at same Mme.

■ HA between RJ-45 and SFP Gigabit RP ports is not supported.

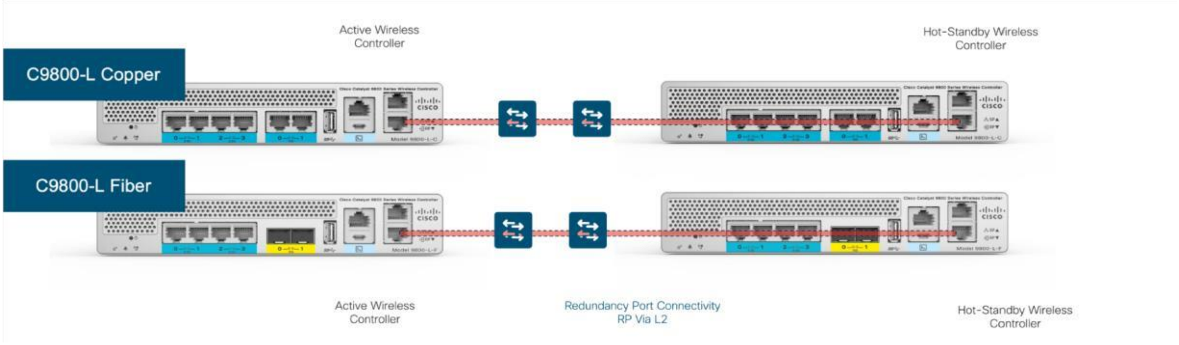
■ Only Cisco supported SFPs (GLC-LH-SMD and GLC-SX-MMD) are supported for RP port ■ 10G SFP-10G-SR is not supported on the RP port.

■ When HA link is up via RJ-45, SFPs on HA port should not be inserted even if there is no link between them. As it is a physical level detecMon, this would cause the HA to go down as precedence is given to SFP

Physical Connec)vity for C9800-L, C9800-40 and C9800-80 Wireless Controller HA SSO

The HA Pair always has one acMve controller and one standby controller. If the acMve controller becomes unavailable, the standby assumes the role of the acMve. The AcMve wireless controller creates and updates all the wireless informaMon and constantly synchronizes that informaMon with the standby controller. If the acMve wireless controller fails, the standby wireless controller assumes the role of the acMve wireless controller and conMnues to the keep the HA Pair operaMonal. Access Points and clients conMnue to remain connected during an acMve-to-standby switchover.

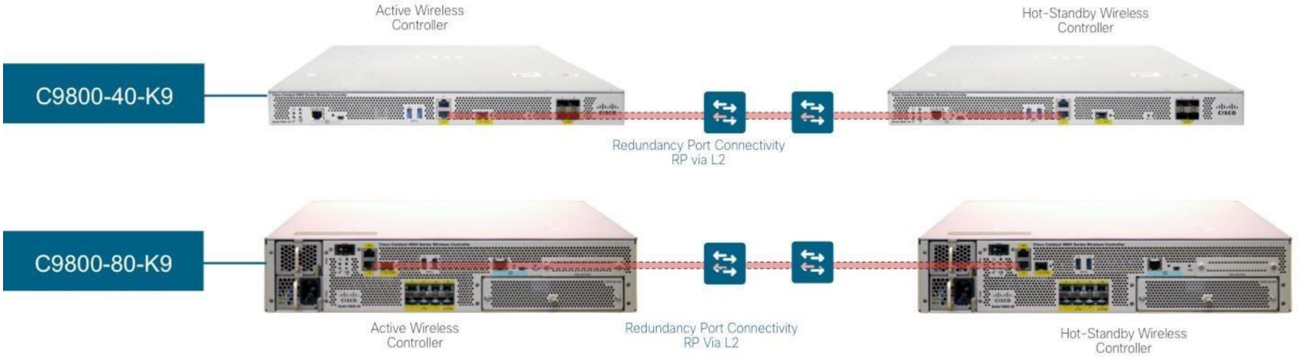
Connec&ng C9800-L Wireless Controllers using RJ-45 RP Port for SSO


Active Wireless Controller
Hot-Standby Wireless Controller
C9800-L Copper
C9800-L Fiber
Active Wireless Controller
Redundancy Port Connectivity RP Via L2
Hot-Standby Wireless Controller

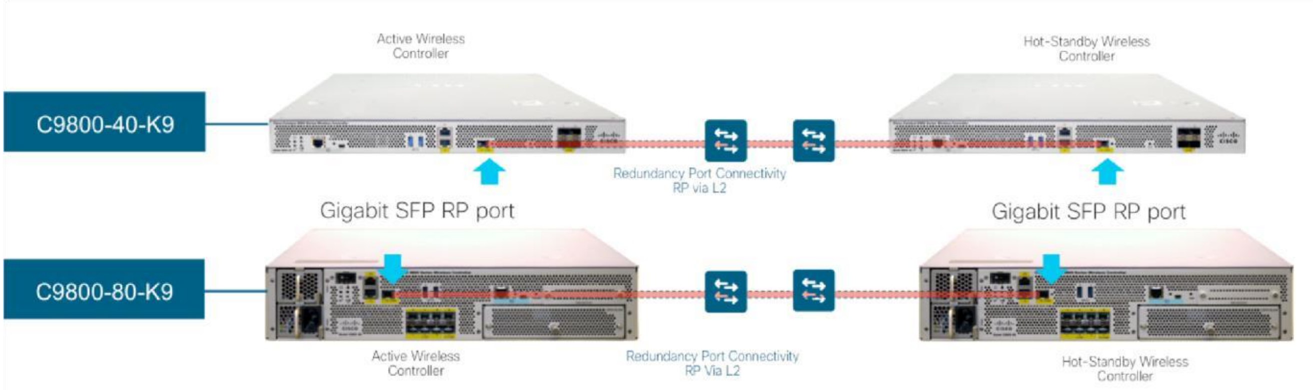
High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5

Physical ConnecMvity for C9800-L, C9800-40 and C9800-80 Wireless Controller HA SSO

Connec&ng C9800-40 and 9800-80 Wireless Controllers using RJ-45 RP Port for SSO


Active Wireless Controller
Hot-Standby Wireless Controller
C9800-40-K9
Redundancy Port Connectivity RP via L2
C9800-80-K9
Active Wireless Controller
Redundancy Port Connectivity RP Via L2
Hot-Standby Wireless Controller

Connec&ng C9800-40 and 9800-80 Wireless Controllers using SFP Gigabit RP Port for SSO


Active Wireless Controller
Hot-Standby Wireless Controller
C9800-40-K9
Redundancy Port Connectivity RP via L2
Gigabit SFP RP port
Gigabit SFP RP port
C9800-80-K9
Active Wireless Controller
Redundancy Port Connectivity RP Via L2
Hot-Standby Wireless Controller

Connec&ng a C9800 wireless controller HA pair to upstream switches

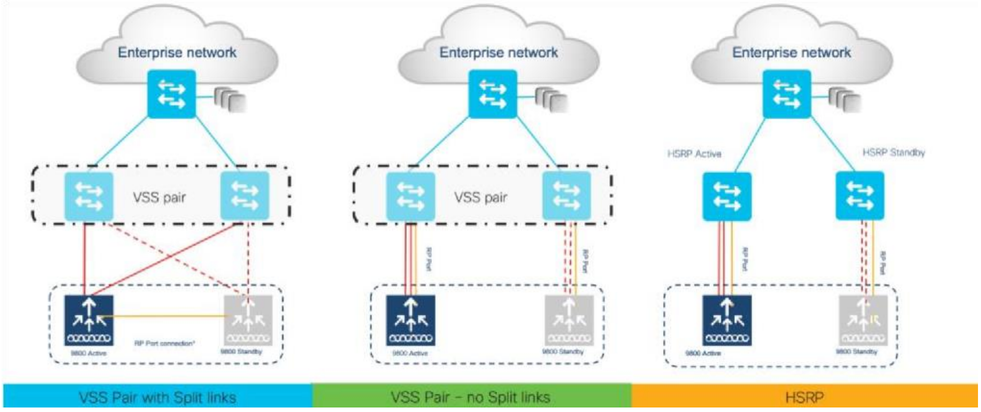
Prior to 17.1 following topologies were supported in terms of upstream connecMvity to the network:

1. SSO pair connected to upstream VSS pair with split links and RP connected back to back.
2. SSO pair connected to upstream VSS pair with RP connected via the upstream set of switches in order to detect gateway down scenario.

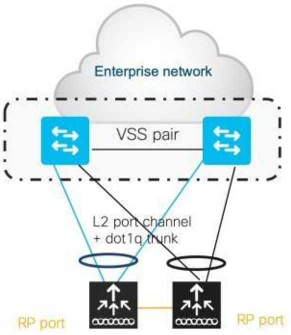
3. SSO pair connected to upstream HSRP acMve and standby and RP connected via upstream set of switches in order to detect gateway down scenario.

High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5

Physical ConnecMvity for C9800-L, C9800-40 and C9800-80 Wireless Controller HA SSO



Op&on 1: Single VSS switch (or stack/VSL pair/modular switch) with RP backtoback

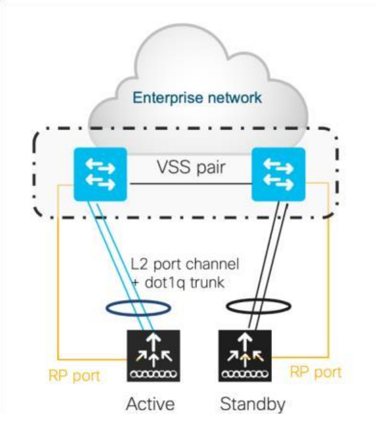


Single L2 port-channel on each box and enable dot1q to carry mulMple VLANs. Spread the uplinks of the HA pair across the VSS pair and connect the RP back to back (no L2 network in between). Make sure that switch can scale in terms of ARP and MAC table entries.

This is a recommended topology.

Note: In HA SSO topology only LAG with mode ON is supported.

Op&on 2: Single VSS switch (or stack/VSL pair/modular switch) with RP via upstream

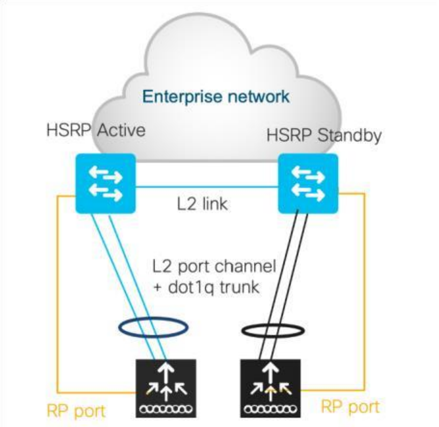


With this topology a single L2 port-channel is created on each box. Enable dot1q to carry mulMple VLANs and connect the standby in the same manner. Make sure that switch can scale in terms of ARP and MAC table entries

IMPORTANT: In this topology the links are not spread across the VSS stack. Connect RP port to the same VSS/stack member as the uplinks and not back to back

Note: In HA SSO topology only LAG with mode ON is supported.

Op&on 3: Dual Distributed switches with HSRP



With this topology a single L2 port-channel is created on each box. Enable dot1q to carry mulMple VLANs and connect the standby in the same manner. Make sure that switch can scale in terms of ARP and MAC table entries.

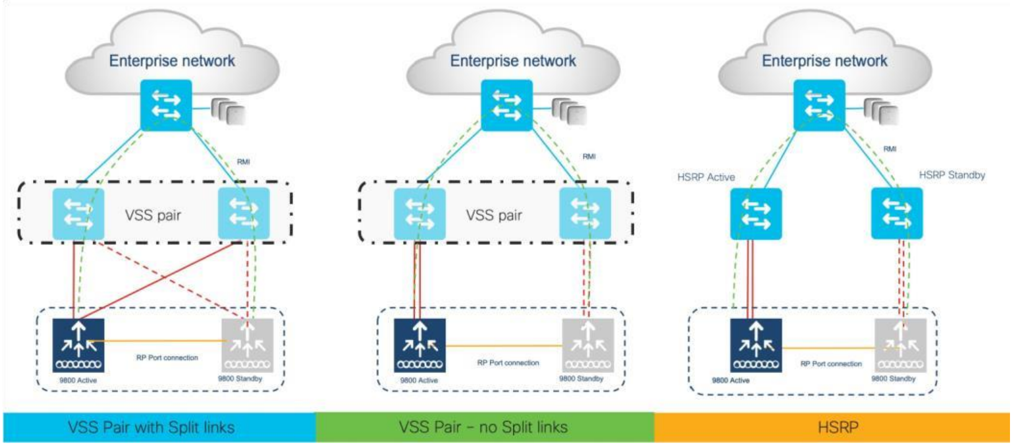
IMPORTANT: Connect RP port to the same distribuMon switch as the uplinks and not back to back

Note: In HA SSO topology only LAG with mode ON is supported prior to release 17.1. With 17.1, we addiMonally support LACP and PAGP. See the LACP, PAGP support in SSO Pair secMon for more details

Connec)ng a C9800 wireless controller HA pair to upstream switches with Release 17.1 and above

With the opMon of RMI and default gateway check feature available in release 17.1, the following topologies are now supported and recommended:

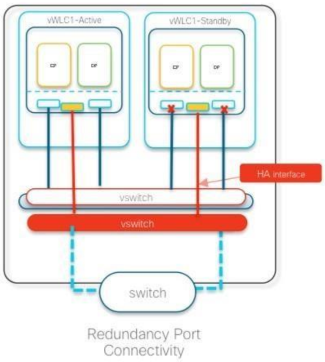
1. SSO pair connected to upstream VSS pair with split links and RP connected back to back.
2. SSO pair connected to upstream VSS pair and RP connected back to back.
3. SSO pair connected to upstream HSRP acMve and standby and RP connected back to back.

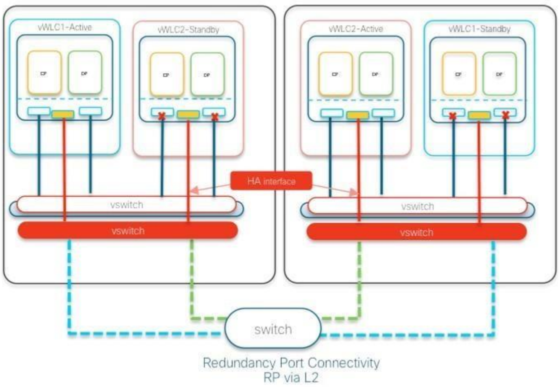


Note: It is recommended to configure porXast trunk in uplink switches for faster convergence using CLI "spanning-tree port type edge trunk" or "spanning-tree porXast trunk"

SSO on Cisco Catalyst C9800-CL running on ESXi, KVM, Hyper-V

The Virtual Catalyst 9800 Wireless controller can be deployed as an HA Pair in a single or dual server setup.





The figure on the leh shows Redundant port connected on the same server.

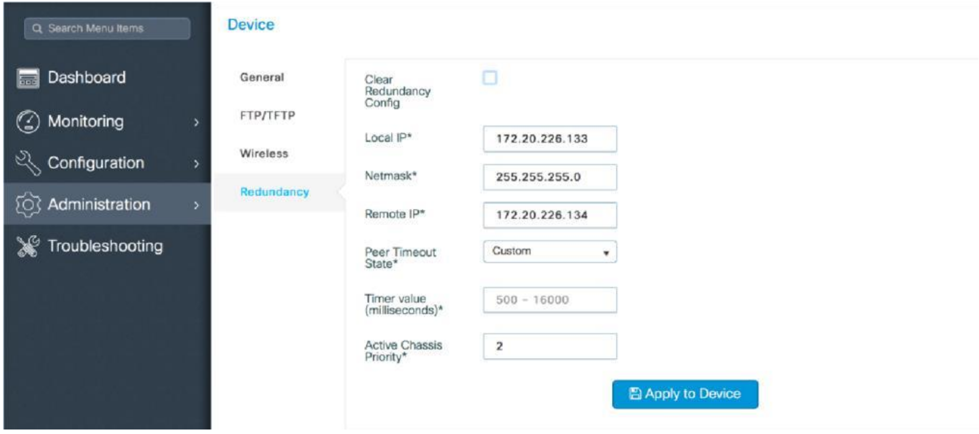
The figure on the right shows Redundant port L2 connected to a separate server.

The same interface number (for example Gig3) must be used to form the HA pair on 9800-CL. The scale of templates must also match. We support SSO across 9800-CL on HyperV, VMware ESXi and KVM.

Configuring High Availability SSO using GUI

Device redundancy can be configured from **the Administra?on > Device > Redundancy** page.

On the AcMve controller, the priority is set to a higher value than the standby controller. The wireless controller with the higher priority value is selected as the acMve during the acMve-standby elecMon process. The Remote IP is the IP address of the standby controller’s redundancy port IP.



Device

Clear Redundancy Config ☐

Local IP* 172.20.226.133

Netmask* 255.255.255.0

Remote IP* 172.20.226.134

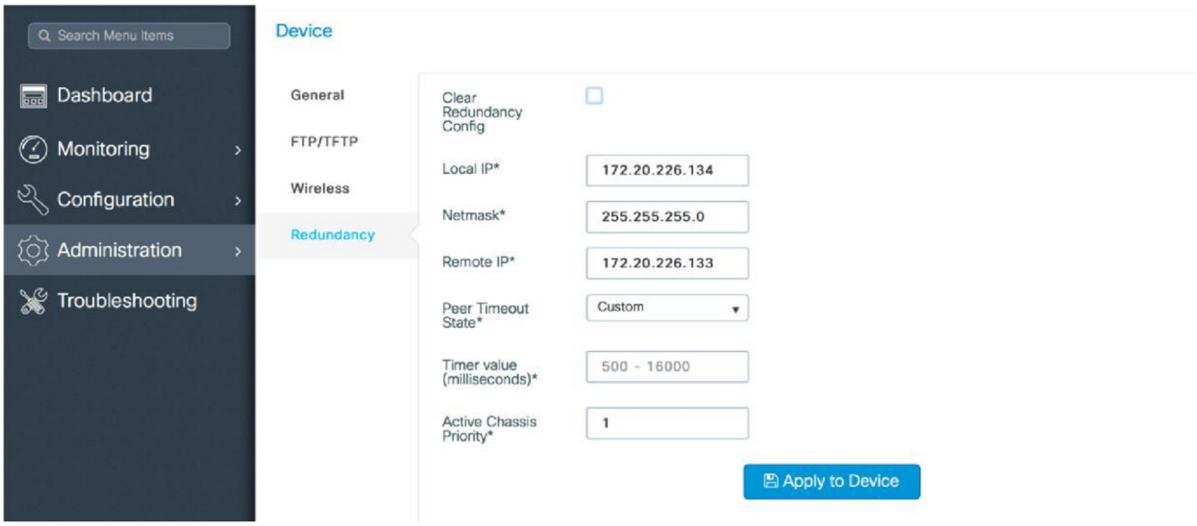
Peer Timeout State* Custom

Timer value (milliseconds)* 500 - 16000

Active Chassis Priority* 2

Note: This page has changed starting release 17.1 to include an option to configure the HA pair using RMI. Please refer to the Redundancy Management Interface section to see the updated screens for configuration.

On the standby controller, the remote IP is set to the Active controller’s redundancy port IP



Device

Clear Redundancy Config ☐

Local IP* 172.20.226.134

Netmask* 255.255.255.0

Remote IP* 172.20.226.133

Peer Timeout State* Custom

Timer value (milliseconds)* 500 - 16000

Active Chassis Priority* 1

1) Both IP address for the Local and Remote IP must be in the same subnet.

2) It is suggested to use the 169.254.X.X/16 subnet. The last two octets can be derived from last two octets of the management interface.

3) Avoid using 10.10.10.x/24 subnet for the RP port due to defect in 9800 WLC.

Clear Redundancy config clears the SSO configuration and returns the controller to standalone mode.

Note: It is recommended to configure HA using the Redundancy Management Interface (RMI) starting Release 17.1. To see configuration using RMI please see the Redundancy Management Interface section.

Configuring High Availability SSO using CLI

■ **On Virtual Catalyst 9800 Wireless controller**, enable High Availability SSO using the following command on each of the two virtual Catalyst 9800 Wireless controller instances

High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5 Mobility MAC

```
chassis redundancy ha-interface <RP interface> local-ip <local IP> <local IP subnet>
```

```
        remote-ip  <remote IP>
```

e.g.

On Virtual Catalyst 9800 Wireless controller instance-1:

```
chassis redundancy ha-interface Gig 3 local-ip 172.23.174.85 /24 remoteip  172.23.174.86
```

On Virtual Catalyst 9800 Wireless controller instance-2:

```
chassis redundancy ha-interface Gig 3 local-ip 172.23.174.86 /24 remoteip  172.23.174.85
```

■ **On C9800-40 and C9800-80 wireless controller,** enable High Availability SSO using the following command on each of the two wireless controller units

```
     chassis redundancy ha-interface local-ip <local IP> <local IP subnet> remoteip  <remote
    IP>
```

Reload both wireless controllers by execuMng the command reload from the CLI

Note: It is recommended to configure HA using the Redundancy Management Interface (RMI) starMng Release 17.1. To see configuraMon using RMI please see the Redundancy Management Interface secMon.

Note: These commands are not supported on these models:

- Cisco Catalyst CW9800H1 Wireless Controller.

- Cisco Catalyst CW9800H2 Wireless Controller.

- Cisco Catalyst CW9800M Wireless Controller.

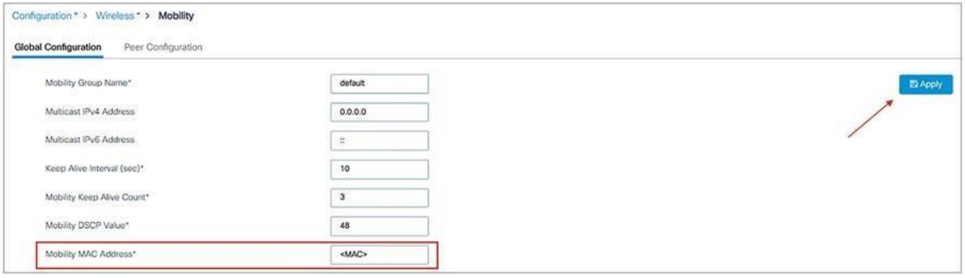
RMI-based High Availability is mandatory in the Cisco Catalyst CW9800H1 Wireless Controller, Cisco Catalyst CW9800H2 Wireless Controller and Cisco Catalyst CW9800M Wireless Controller.

Mobility MAC

The wireless mobility MAC is the MAC address used for mobility communicaMon. In an SSO scenario, ensure that you explicitly configure the wireless mobility MAC address; otherwise, the mobility tunnel will go down aher SSO. The mobility MAC address for the SSO pair can be configured either:

- Before forming the SSO pair on each standalone controller. This is recommended before sohware release 16.12.3.
- On the acMve controller once the SSO pair is formed.

To configure the mobility MAC address, you can use the GUI:



Mobility Group Name*: default

Multicast IPv4 Address: 0.0.0.0

Multicast IPv6 Address: ::

Keep Alive Interval (sec)*: 10

Mobility Keep Alive Count*: 3

Mobility DSCP Value*: 48

Mobility MAC Address*: <MAC>

Once you've entered the address, click Apply.

Note: The MAC address on the GUI is automaMcally derived from the wireless management interface, but you can use any other valid MAC address.

In the CLI, use the following command:

```
C9800#wireless mobility mac-address <MAC>
```

High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5

AcMve and Standby ElecMon Process

Ac)ve and Standby Elec)on Process

An acMve C9800 wireless controller retains its role as an AcMve Controller unless one of the following events occur:

- The wireless controller HA pair is reset.
- The acMve wireless controller is removed from the HA pair.
- The acMve wireless controller is reset or powered off.
- The acMve wireless controller fails.

The acMve wireless controller is elected or re-elected based on one of these factors and in the order listed below:

1. The wireless controller that is currently the acMve wireless controller.
2. The wireless controller with the highest priority value.

   Note: We recommend assigning the highest priority value to the wireless controller C9800 you prefer to be the acMve controller. This ensures that the controller is re-elected as acMve controller if a re-elecMon occurs.

   SeMng the Switch Priority Value `chassis chassis -number priority new-priority-number`

   Chassis-number Specifies the chassis number and the new priority for the chassis. The chassis number range is 1 to 2. Please note that the chassis renumbering command will require a reboot.

   The priority value range is <1-2>. Stack Priority 2 will be Primary while Priority 1 will be standby.

   Example

   ```
       wireless controller#chassis 1 priority 2
   ```

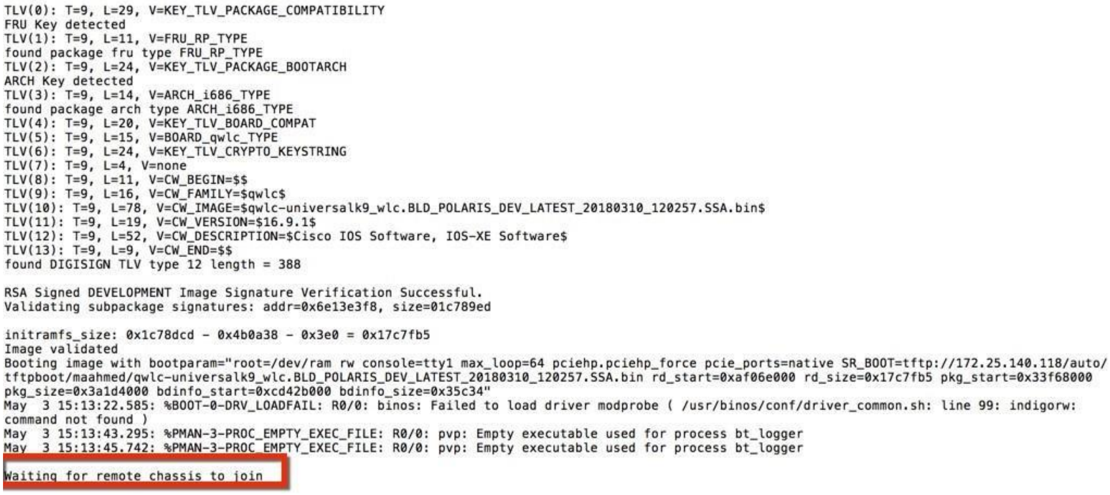
   You can display the current priority value by using the **show chassis** user EXEC command. The new priority value takes effect immediately but does not affect the current AcMve Controller. The new priority value helps determine which controller is elected as the new AcMve Controller when the current acMve wireless controller or HA redundant pair reloads.
3. The wireless controller with the shortest start-up Mme.

4. The wireless controller with the lowest MAC Address.

The HA LED on the chassis can be used to idenMfy the current AcMve Controller.

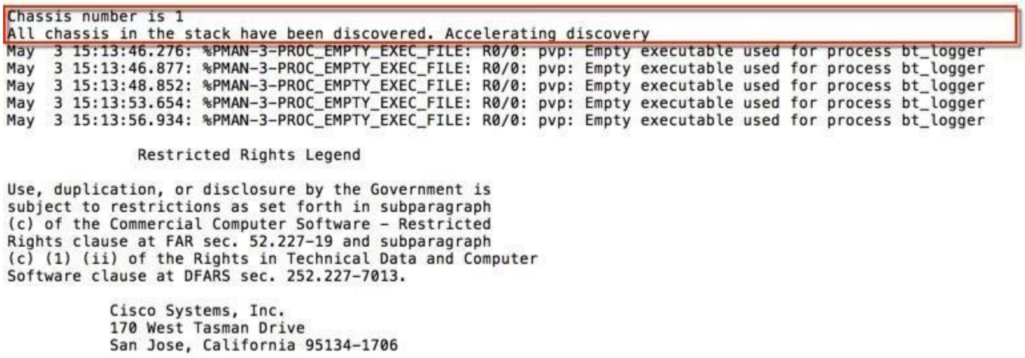
State Transi)on for HA SSO Pair forma)on

1. AcMve wireless controller in Non Redundant mode



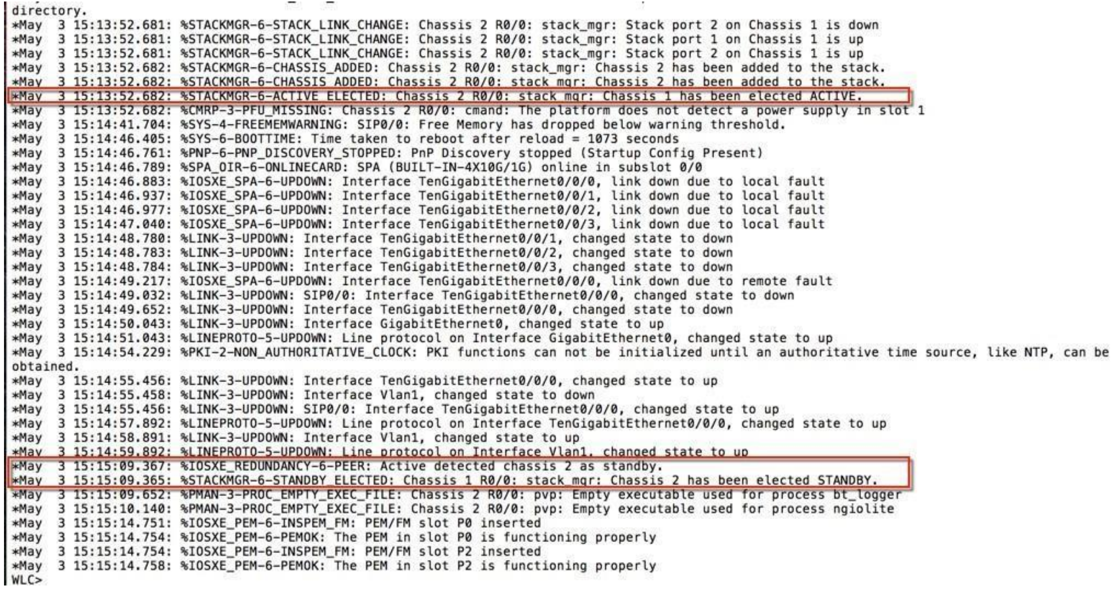
```
TLV(0): T=9, L=29, V=KEY_TLV_PACKAGE_COMPATIBILITY
FRU Key detected
TLV(1): T=9, L=11, V=FRU_RP_TYPE
found package fru type FRU_RP_TYPE
TLV(2): T=9, L=24, V=KEY_TLV_PACKAGE_BOOTARCH
ARCH Key detected
TLV(3): T=9, L=14, V=ARCH_i686_TYPE
found package arch type ARCH_i686_TYPE
TLV(4): T=9, L=20, V=KEY_TLV_BOARD_COMPAT
TLV(5): T=9, L=15, V=BOARD_qwlc_TYPE
TLV(6): T=9, L=24, V=KEY_TLV_CRYPTO_KEYSTRING
TLV(7): T=9, L=4, V=none
TLV(8): T=9, L=11, V=CW_BEGIN=$$
TLV(9): T=9, L=16, V=CW_FAMILY=$qwlc$
TLV(10): T=9, L=78, V=CW_IMAGE=$qwlc-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20180310_120257.SSA.bin$
TLV(11): T=9, L=19, V=CW_VERSION=$16.9.1$
TLV(12): T=9, L=52, V=CW_DESCRIPTION=$Cisco IOS Software, IOS-XE Software$
TLV(13): T=9, L=9, V=CW_END=$$
found DIGISIGN TLV type 12 length = 388

RSA Signed DEVELOPMENT Image Signature Verification Successful.
Validating subpackage signatures: addr=0x6e13e3f8, size=01c789ed

initramfs_size: 0x1c78dcd - 0x4b0a38 - 0x3e0 = 0x17c7fb5
Image validated
Booting image with bootparam="root=/dev/ram rw console=tty1 max_loop=64 pciehp.pciehp_force pcie_ports=native SR_BOOT=tftp://172.25.140.118/auto/
tftpboot/maahmed/qwlc-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20180310_120257.SSA.bin rd_start=0xaf06e000 rd_size=0x17c7fb5 pkg_start=0x33f68000
pkg_size=0x3a1d4000 bdinfo_start=0xcd42b000 bdinfo_size=0x35c34"
May  3 15:13:22.585: %BOOT-0-DRV_LOADFAIL: R0/0: binos: Failed to load driver modprobe ( /usr/binos/conf/driver_common.sh: line 99: indigorw:
command not found )
May  3 15:13:43.295: %PMAN-3-PROC_EMPTY_EXEC_FILE: R0/0: pvp: Empty executable used for process bt_logger
May  3 15:13:45.742: %PMAN-3-PROC_EMPTY_EXEC_FILE: R0/0: pvp: Empty executable used for process bt_logger

Waiting for remote chassis to join
```

2. Standby InserMon for HA Pairing



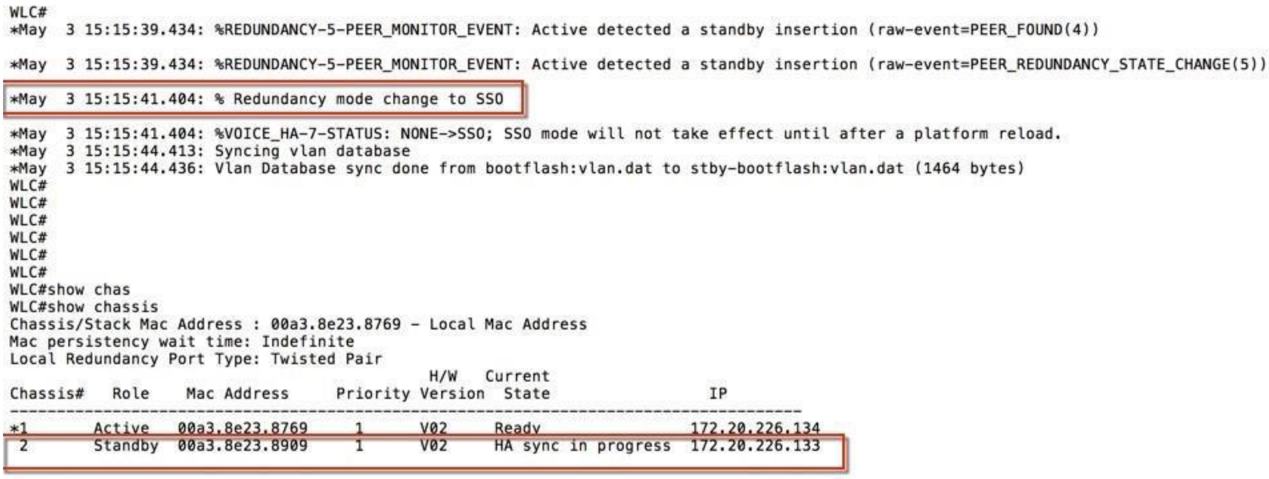
```
Chassis number is 1
All chassis in the stack have been discovered. Accelerating discovery
May  3 15:13:46.276: %PMAN-3-PROC_EMPTY_EXEC_FILE: R0/0: pvp: Empty executable used for process bt_logger
May  3 15:13:46.877: %PMAN-3-PROC_EMPTY_EXEC_FILE: R0/0: pvp: Empty executable used for process bt_logger
May  3 15:13:48.852: %PMAN-3-PROC_EMPTY_EXEC_FILE: R0/0: pvp: Empty executable used for process bt_logger
May  3 15:13:53.654: %PMAN-3-PROC_EMPTY_EXEC_FILE: R0/0: pvp: Empty executable used for process bt_logger
May  3 15:13:56.934: %PMAN-3-PROC_EMPTY_EXEC_FILE: R0/0: pvp: Empty executable used for process bt_logger

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706
```

3. HA Sync in Progress



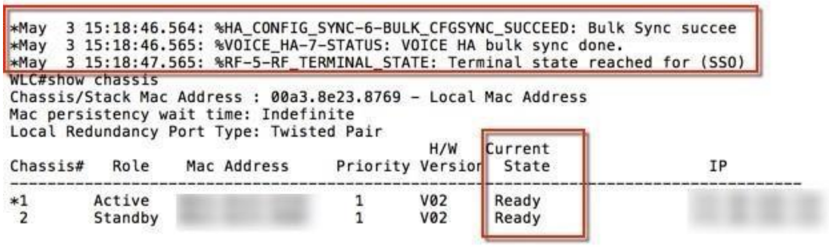
```
directory.
*May  3 15:13:52.681: %STACKMGR-6-STACK_LINK_CHANGE: Chassis 2 R0/0: stack_mgr: Stack port 2 on Chassis 1 is down
*May  3 15:13:52.681: %STACKMGR-6-STACK_LINK_CHANGE: Chassis 2 R0/0: stack_mgr: Stack port 1 on Chassis 1 is up
*May  3 15:13:52.681: %STACKMGR-6-STACK_LINK_CHANGE: Chassis 2 R0/0: stack_mgr: Stack port 2 on Chassis 1 is up
*May  3 15:13:52.682: %STACKMGR-6-CHASSIS_ADDED: Chassis 2 R0/0: stack_mgr: Chassis 2 has been added to the stack.
*May  3 15:13:52.682: %STACKMGR-6-CHASSIS_ADDED: Chassis 2 R0/0: stack_mgr: Chassis 2 has been added to the stack.
*May  3 15:13:52.682: %STACKMGR-6-ACTIVE_ELECTED: Chassis 2 R0/0: stack_mgr: Chassis 1 has been elected ACTIVE.
*May  3 15:13:52.682: %CMRP-3-PFU_MISSING: Chassis 2 R0/0: cmand: The platform does not detect a power supply in slot 1
*May  3 15:14:41.704: %SYS-4-FREEMEMWARNING: SIP0/0: Free Memory has dropped below warning threshold.
*May  3 15:14:46.405: %SYS-6-BOOTTIME: Time taken to reboot after reload = 1073 seconds
*May  3 15:14:46.761: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Startup Config Present)
*May  3 15:14:46.789: %SPA_OIR-6-ONLINECARD: SPA (BUILT-IN-4X10G/1G) online in subslot 0/0
*May  3 15:14:46.883: %IOSXE_SPA-6-UPDOWN: Interface TenGigabitEthernet0/0/0, link down due to local fault
*May  3 15:14:46.937: %IOSXE_SPA-6-UPDOWN: Interface TenGigabitEthernet0/0/1, link down due to local fault
*May  3 15:14:46.977: %IOSXE_SPA-6-UPDOWN: Interface TenGigabitEthernet0/0/2, link down due to local fault
*May  3 15:14:47.040: %IOSXE_SPA-6-UPDOWN: Interface TenGigabitEthernet0/0/3, link down due to local fault
*May  3 15:14:48.780: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/1, changed state to down
*May  3 15:14:48.783: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/2, changed state to down
*May  3 15:14:48.784: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/3, changed state to down
*May  3 15:14:49.217: %IOSXE_SPA-6-UPDOWN: Interface TenGigabitEthernet0/0/0, link down due to remote fault
*May  3 15:14:49.032: %LINK-3-UPDOWN: SIP0/0: Interface TenGigabitEthernet0/0/0, changed state to down
*May  3 15:14:49.652: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/0, changed state to down
*May  3 15:14:50.043: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to up
*May  3 15:14:51.043: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to up
*May  3 15:14:54.229: %PKI-2-NON_AUTHORITATIVE_CLOCK: PKI functions can not be initialized until an authoritative time source, like NTP, can be
obtained.
*May  3 15:14:55.456: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/0, changed state to up
*May  3 15:14:55.458: %LINK-3-UPDOWN: Interface Vlan1, changed state to down
*May  3 15:14:55.456: %LINK-3-UPDOWN: SIP0/0: Interface TenGigabitEthernet0/0/0, changed state to up
*May  3 15:14:57.892: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/0/0, changed state to up
*May  3 15:14:58.891: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*May  3 15:14:59.892: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
*May  3 15:15:09.367: %IOSXE_REDUNDANCY-6-PEER: Active detected chassis 2 as standby.
*May  3 15:15:09.365: %STACKMGR-6-STANDBY_ELECTED: Chassis 1 R0/0: stack_mgr: Chassis 2 has been elected STANDBY.
*May  3 15:15:09.652: %PMAN-3-PROC_EMPTY_EXEC_FILE: Chassis 2 R0/0: pvp: Empty executable used for process bt_logger
*May  3 15:15:10.140: %PMAN-3-PROC_EMPTY_EXEC_FILE: Chassis 2 R0/0: pvp: Empty executable used for process ngiolite
*May  3 15:15:14.751: %IOSXE_PEM-6-INSPEM_FM: PEM/FM slot P0 inserted
*May  3 15:15:14.754: %IOSXE_PEM-6-PEMOK: The PEM in slot P0 is functioning properly
*May  3 15:15:14.754: %IOSXE_PEM-6-INSPEM_FM: PEM/FM slot P2 inserted
*May  3 15:15:14.758: %IOSXE_PEM-6-PEMOK: The PEM in slot P2 is functioning properly
WLC>
```

Monitoring the HA Pair



```
WLC#
*May  3 15:15:39.434: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion (raw-event=PEER_FOUND(4))

*May  3 15:15:39.434: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

*May  3 15:15:41.404: % Redundancy mode change to SSO

*May  3 15:15:41.404: %VOICE_HA-7-STATUS: NONE->SSO; SSO mode will not take effect until after a platform reload.
*May  3 15:15:44.413: Syncing vlan database
*May  3 15:15:44.436: Vlan Database sync done from bootflash:vlan.dat to stby-bootflash:vlan.dat (1464 bytes)
WLC#
WLC#
WLC#
WLC#
WLC#
WLC#
WLC#show chas
WLC#show chassis
Chassis/Stack Mac Address : 00a3.8e23.8769 - 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
---------------------------------------------------------------------------------------------
*1       Active   00a3.8e23.8769     1      V02     Ready                 172.20.226.134
 2       Standby  00a3.8e23.8909     1      V02     HA sync in progress   172.20.226.133
```

4. Terminal State for SSO

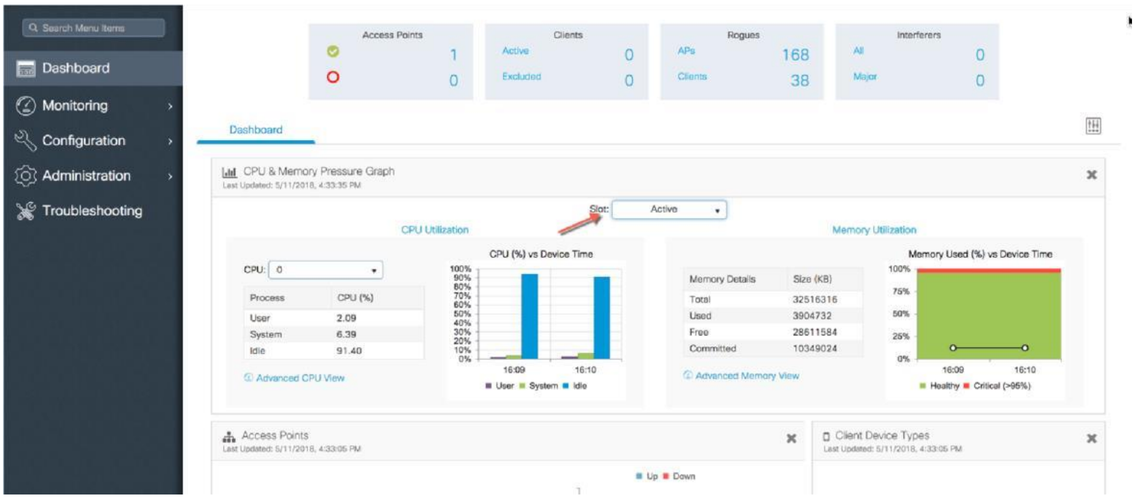


```
*May  3 15:18:46.564: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succee
*May  3 15:18:46.565: %VOICE_HA-7-STATUS: VOICE HA bulk sync done.
*May  3 15:18:47.565: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
WLC#show chassis
Chassis/Stack Mac Address : 00a3.8e23.8769 - Local Mac Address
Mac persistency wait time: Indefinite
Local Redundancy Port Type: Twisted Pair
                                           H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                  IP
---------------------------------------------------------------------------------------------
*1       Active   [redacted]         1      V02     Ready                 [redacted]
 2       Standby                     1      V02     Ready
```

Note: Breaking the HA Pair : The HA configuraMon can be disabled by using the chassis clear command followed by a reload

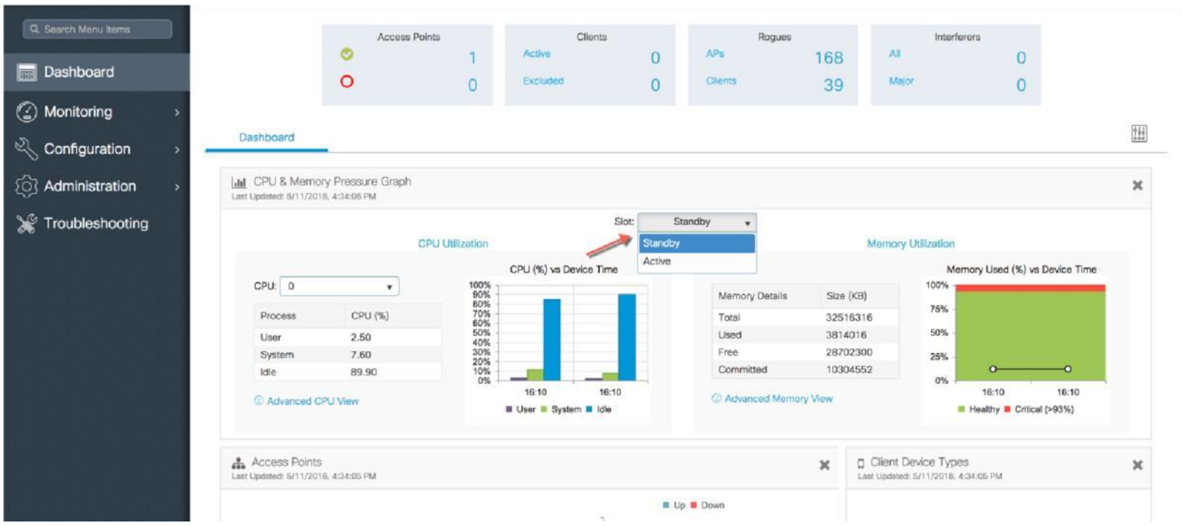
Monitoring the HA Pair

Both AcMve and Standby System can be monitored from the Management UI of the AcMve wireless controller. This includes informaMon about CPU and memory uMlizaMon as well and advanced CPU and memory views.



Process	CPU (%)
User	2.09
System	6.39
Idle	91.40

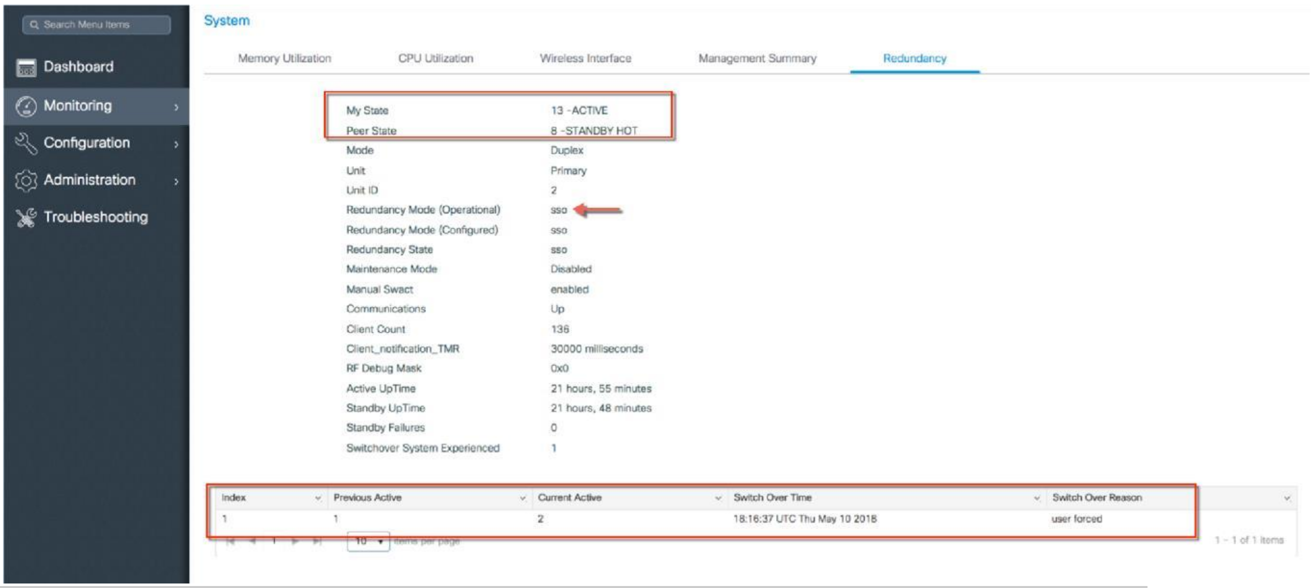
Memory Details	Size (KB)
Total	32516316
Used	3904732
Free	28611584
Committed	10349024



Process	CPU (%)
User	2.50
System	7.60
Idle	89.90

Memory Details	Size (KB)
Total	32516316
Used	3814016
Free	28702300
Committed	10304552

Navigate to Monitoring > System > Redundancy on the controller Web UI. The Redundancy States page is displayed:



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
Maintenance Mode	Disabled
Manual Swact	enabled
Communications	Up
Client Count	136
Client_notification_TMR	30000 milliseconds
RF Debug Mask	0x0
Active UpTime	21 hours, 55 minutes
Standby UpTime	21 hours, 48 minutes
Standby Failures	0
Switchover System Experienced	1

Index	Previous Active	Current Active	Switch Over Time	Switch Over Reason
1	1	2	18:16:37 UTC Thu May 10 2018	user forced

Parameter	Descrip?on

My State	Shows the state of the acMve CPU controller module. Values are as follows: AcMve Standby HOT Disable
Peer State	Displays the state of the peer (or standby) CPU controller module. Values are as follows: Standby HOT Disable
Mode	Displays the current state of the redundancy peer. Values are as follows: Simplex— Single CPU controller module. Duplex— Two CPU controller modules.

Unit ID	Displays the unit ID of the CPU controller module.
Redundancy Mode (OperaMonal)	Displays the current operaMonal redundancy mode supported on the unit.
Redundancy Mode (Configured)	Displays the current configured redundancy mode supported on the unit.
Redundancy State	Displays the current funcMoning redundancy state of the unit. Values are as follows: SSO Not Redundant

Cisco Confidential

Manual Swact	Displays whether manual switchovers have been enabled.
CommunicaMons	Displays whether communicaMons are up or down between the two controllers.

The same page displays Switchover history. The descripMon for the following parameters are displayed in the table below:

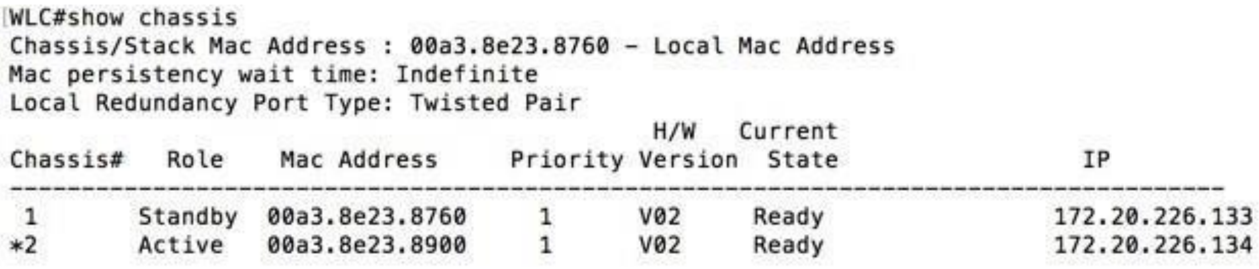
Parameter	**Descrip?on**
Index	Displays the index number of the redundant unit.
Previous AcMve	Displays the controller that was acMve prior to switchover.
Current AcMve	Displays the controller that is currently acMve.
Switch Over Time	Displays the system Mme when the switchover occurred.

Verifying Redundancy States

Switch Over Reason	Displays the cause of the switchover.

Monitoring HA Pair from CLI

The command `show chassis` displays summary informaMon about the HA Pair, including the MAC address, role, switch priority, and current state of each wireless controller in the redundant HA pair. By default, the Local MAC Address of the HA Pair is the MAC address of the first elected AcMve Controller.



```
WLC#show chassis
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
-----------------------------------------------------------------------------------------------
 1       Standby  00a3.8e23.8760     1       V02      Ready                172.20.226.133
*2       Active   00a3.8e23.8900     1       V02      Ready                172.20.226.134
```

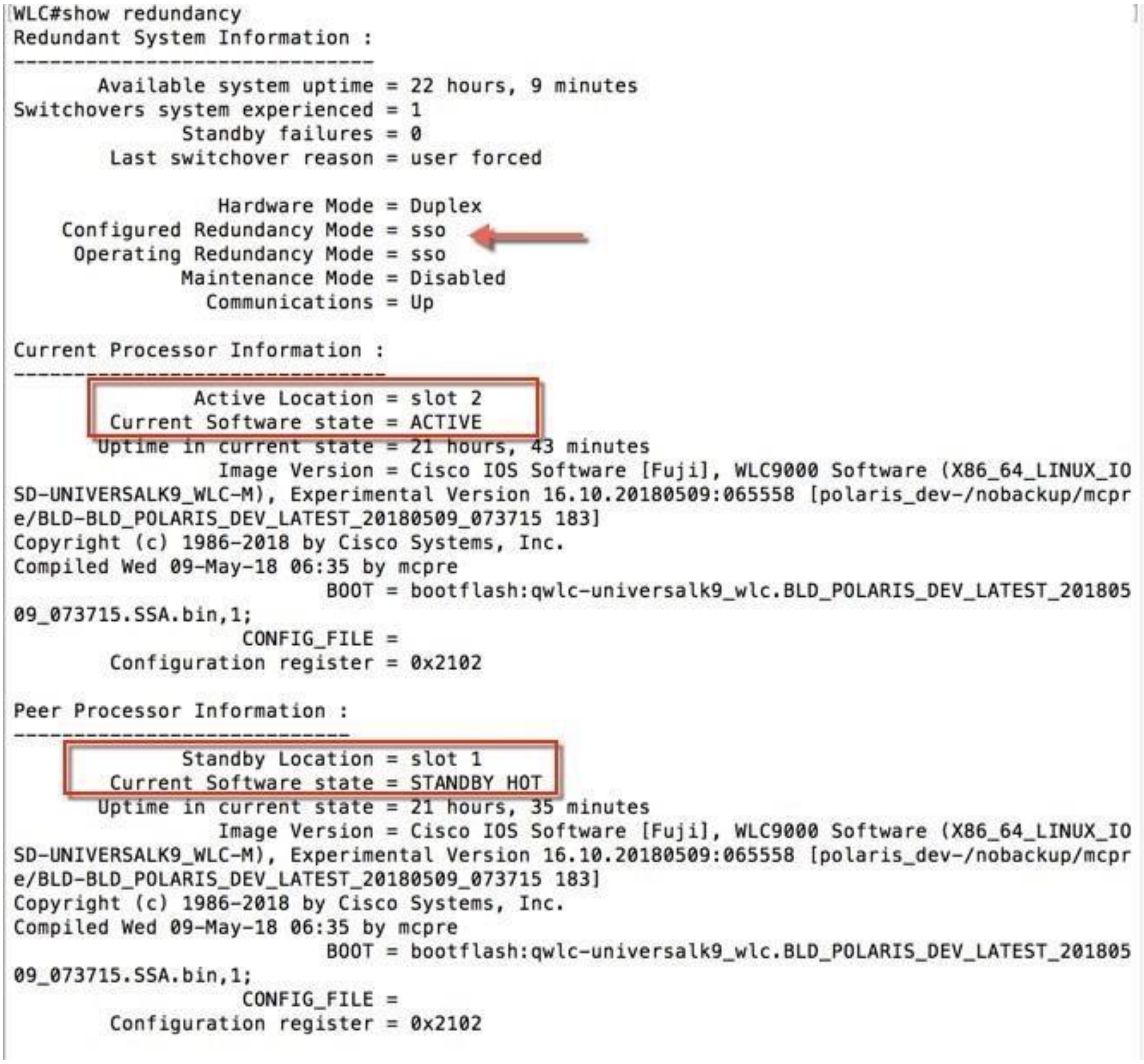
The `show chassis` command points to the current C9800 wireless controller on the console using the (*) symbol against the chassis number as shown above.

Verifying Redundancy States

■ The command **show redundancy** can be used to monitor the state of the two units

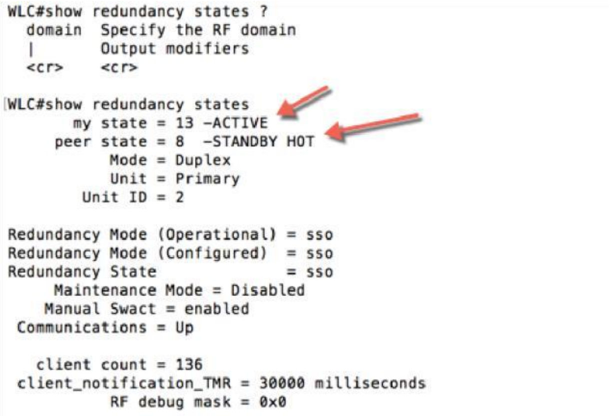
```
wireless controller#show redundancy ?    application       box 2
box application information   clients
Redundancy Facility (RF) client list   config-sync        Show
Redundancy Config Sync status   counters           Redundancy
 Facility (RF) operational counters   domain           Specify
 the RF domain   history            Redundancy Facility (RF)
 history   idb-sync-history  Redundancy Facility (RF) IDB sync
 history   linecard-group    Line card redundancy group
 information
   rii                Display the redundancy interface identifier for Box to
Box   states              Redundancy Facility (RF) states    switchover
Redundancy Facility (RF) switchover   trace             Redundancy Facility
(RF) trace
   |                  Output modifiers
   <cr>               <cr>
```

■ The command **show redundancy** displays the redundant system and the current processor informaMon. The redundant system informaMon includes the system upMme, standby failures, switchover reason, hardware mode, and configured and operaMng redundancy mode. The current processor informaMon displayed includes the image version, acMve locaMon, sohware state, BOOT variable, configuraMon register value, and upMme in the current state, and so on. The Peer Processor informaMon is only available from the AcMve Controller. Verifying Redundancy States



```
WLC#show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 22 hours, 9 minutes
Switchovers system experienced = 1
              Standby failures = 0
        Last switchover reason = user forced

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 2
        Current Software state = ACTIVE
       Uptime in current state = 21 hours, 43 minutes
                 Image Version = Cisco IOS Software [Fuji], WLC9000 Software (X86_64_LINUX_IO
SD-UNIVERSALK9_WLC-M), Experimental Version 16.10.20180509:065558 [polaris_dev-/nobackup/mcpr
e/BLD-BLD_POLARIS_DEV_LATEST_20180509_073715 183]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 09-May-18 06:35 by mcpre
                          BOOT = bootflash:qwlc-universalk9_wlc.BLD_POLARIS_DEV_LATEST_201805
09_073715.SSA.bin,1;
                   CONFIG_FILE =
        Configuration register = 0x2102

Peer Processor Information :
----------------------------
              Standby Location = slot 1
        Current Software state = STANDBY HOT
       Uptime in current state = 21 hours, 35 minutes
                 Image Version = Cisco IOS Software [Fuji], WLC9000 Software (X86_64_LINUX_IO
SD-UNIVERSALK9_WLC-M), Experimental Version 16.10.20180509:065558 [polaris_dev-/nobackup/mcpr
e/BLD-BLD_POLARIS_DEV_LATEST_20180509_073715 183]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 09-May-18 06:35 by mcpre
                          BOOT = bootflash:qwlc-universalk9_wlc.BLD_POLARIS_DEV_LATEST_201805
09_073715.SSA.bin,1;
                   CONFIG_FILE =
        Configuration register = 0x2102
```

- The command show redundancy states displays all the redundancy states of the acMve and standby controllers.

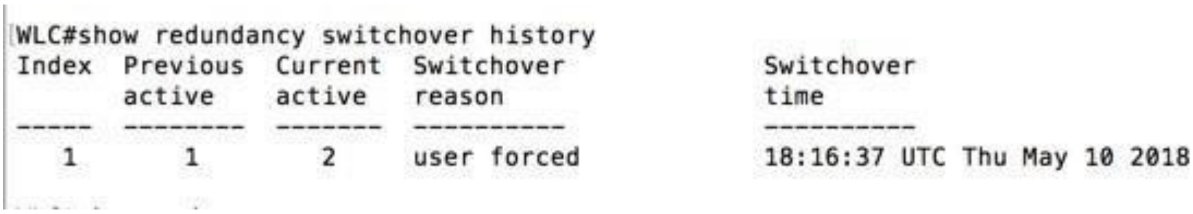


```
WLC#show redundancy states ?
  domain  Specify the RF domain
  |       Output modifiers
  <cr>    <cr>

WLC#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
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 136
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
```

Accessing standby wireless controller console

- Manual Switchover Action (Manual Swact) i.e. the command redundancy force-switchover cannot be executed on the Standby wireless controller and is enabled only on the Active Controller.

- Switchover History can be viewed using the following command

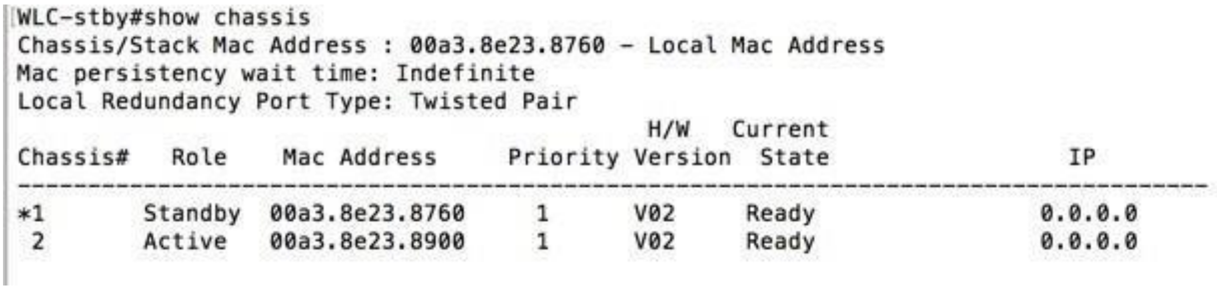


```
WLC#show redundancy switchover history
Index  Previous  Current  Switchover                 Switchover
       active    active   reason                     time
-----  --------- -------- -----------                -----------
   1       1        2     user forced                18:16:37 UTC Thu May 10 2018
```

Accessing standby wireless controller console

The active controller can be accessed through a console connection, Telnet, an SSH, or a Web Browser by using the Management IP address. To use the console on the standby wireless controller, execute the following commands from the active Catalyst 9800 Wireless controller `conf t redundancy main-cpu standby console enable`

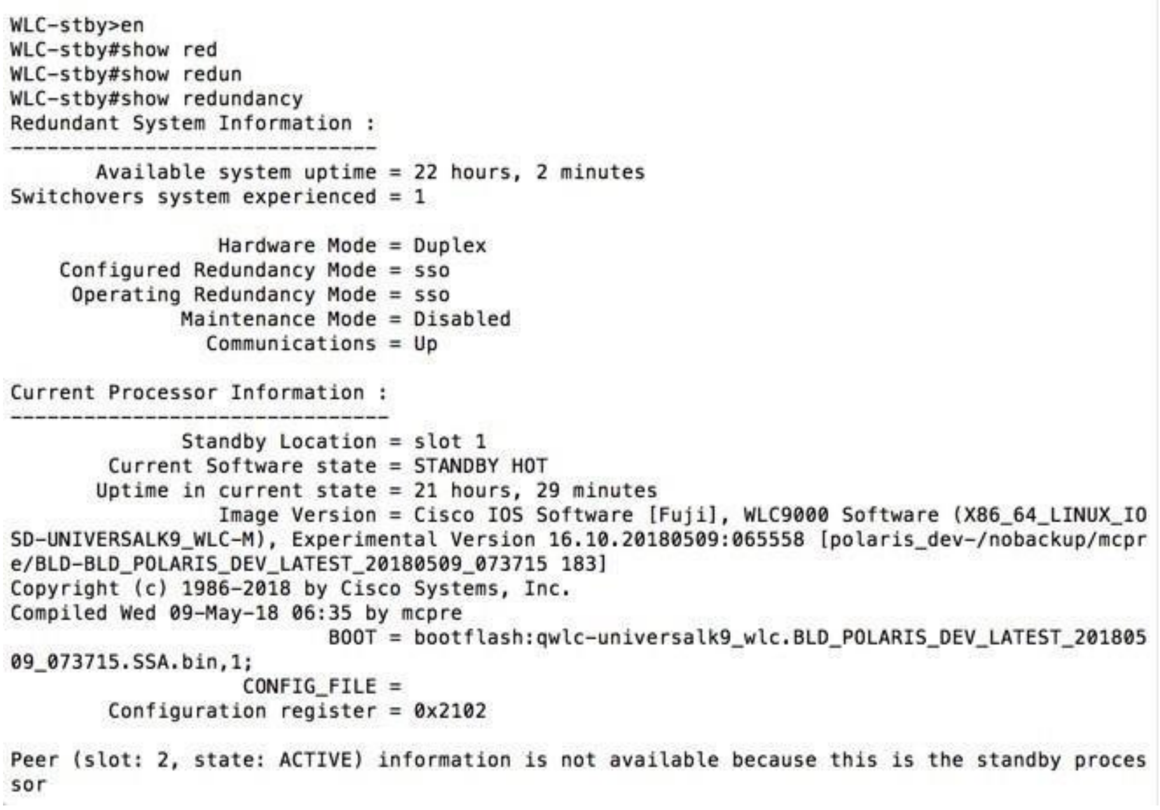
The prompt on the Standby console is appended with "-stby" to reflect the Standby wireless controller console as shown below.



```
WLC-stby#show chassis
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
-------------------------------------------------------------------------------------
*1       Standby  00a3.8e23.8760      1        V02     Ready                 0.0.0.0
 2       Active   00a3.8e23.8900      1        V02     Ready                 0.0.0.0
```

Note: The `show chassis` command points to the current C9800 wireless controller on the console using the (*) symbol against the chassis number as shown above. In this case it is the console of the standby Unit.

Cisco Confidential



```
WLC-stby>en
WLC-stby#show red
WLC-stby#show redun
WLC-stby#show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 22 hours, 2 minutes
Switchovers system experienced = 1

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
              Standby Location = slot 1
        Current Software state = STANDBY HOT
       Uptime in current state = 21 hours, 29 minutes
                 Image Version = Cisco IOS Software [Fuji], WLC9000 Software (X86_64_LINUX_IO
SD-UNIVERSALK9_WLC-M), Experimental Version 16.10.20180509:065558 [polaris_dev-/nobackup/mcpr
e/BLD-BLD_POLARIS_DEV_LATEST_20180509_073715 183]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 09-May-18 06:35 by mcpre
                          BOOT = bootflash:qwlc-universalk9_wlc.BLD_POLARIS_DEV_LATEST_201805
09_073715.SSA.bin,1;
                   CONFIG_FILE =
        Configuration register = 0x2102

Peer (slot: 2, state: ACTIVE) information is not available because this is the standby proces
sor
```

Switchover Func)onality

Process Failure Switchover

This type of switch over occurs when any of the key processes running on the AcMve unit fails or crashes. Upon such a failure, the AcMve unit reloads and the hot Standby takes over and becomes the new AcMve unit. When the failed system boots up, it will transiMon to Hot-Standby state. If the Standby unit is not yet in Hot Standby State, both units are reloaded and there will be no SSO. A process failure on the standby (hot or not) will cause it to reload.

Power-fail Switchover

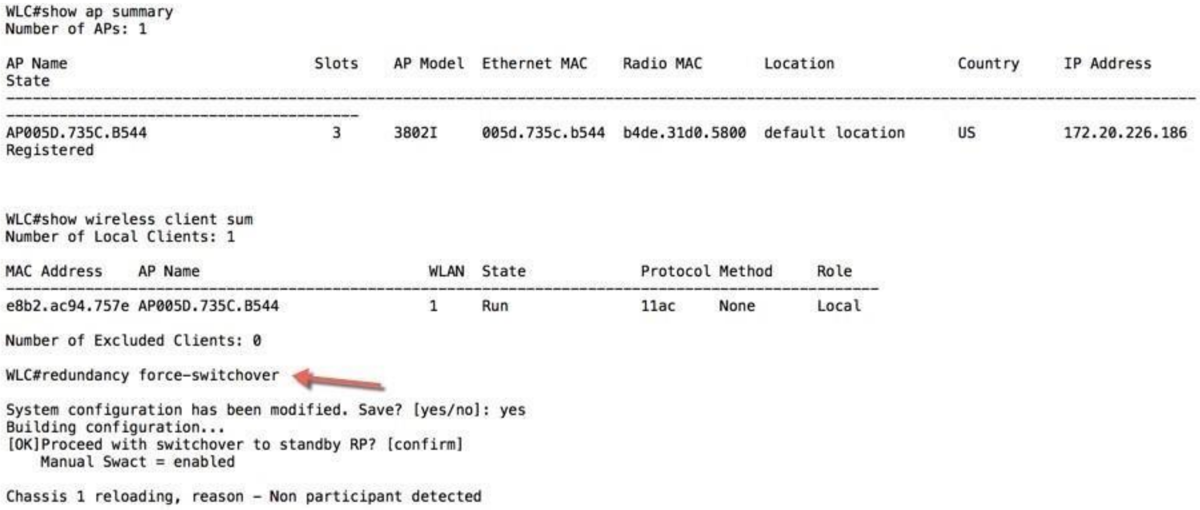
This switchover from the AcMve to Standby unit is caused due to power failure of the current AcMve unit. The current Standby unit becomes the new AcMve unit and when the failed system boots up, it will transiMon to Hot-Standby state.

Manual Switchover

This is a user iniMated forced switchover between the AcMve and Standby unit. The current Standby unit becomes the new AcMve unit and when the failed system boots up, it will transiMon to Hot-Standby state. To perform a manual switchover, execute the redundancy force-switchover command. This command iniMates a graceful switchover from the acMve to the standby controller. The acMve controller reloads and the standby takes over as the New AcMve controller.

Failover Process

Ac&ve wireless controller

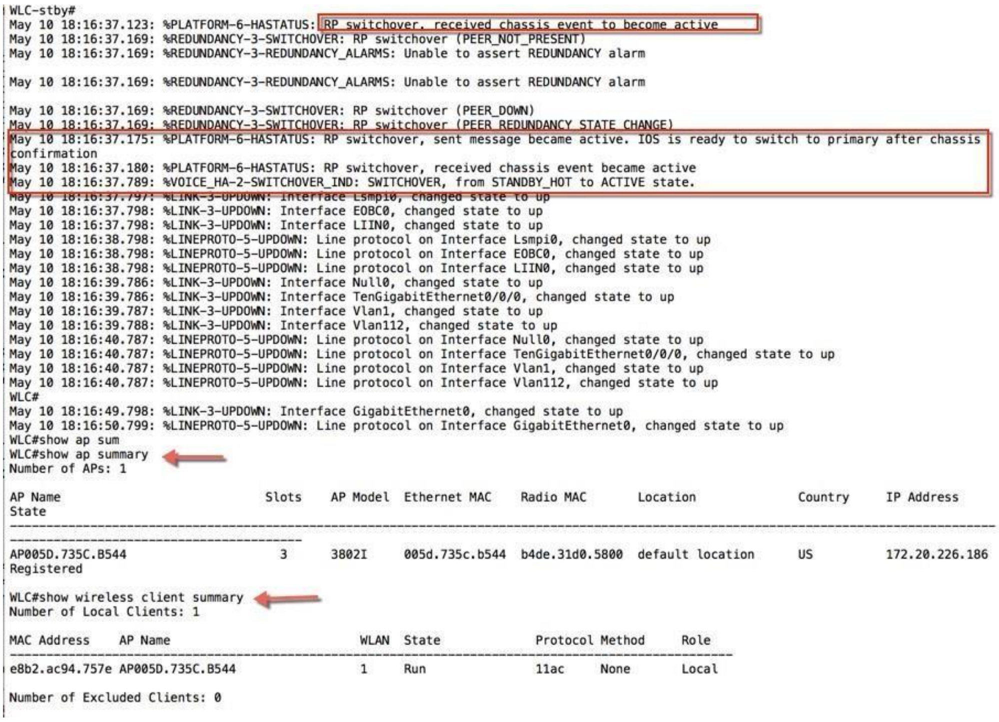


```
WLC#show ap summary
Number of APs: 1

AP Name                          Slots   AP Model  Ethernet MAC    Radio MAC       Location              Country     IP Address
State
-------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------
AP005D.735C.B544                   3     3802I     005d.735c.b544  b4de.31d0.5800  default location      US          172.20.226.186
Registered


WLC#show wireless client sum
Number of Local Clients: 1

MAC Address    AP Name                             WLAN  State              Protocol Method     Role
-------------------------------------------------------------------------------------------------------------
e8b2.ac94.757e AP005D.735C.B544                     1    Run                11ac     None       Local

Number of Excluded Clients: 0

WLC#redundancy force-switchover

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]Proceed with switchover to standby RP? [confirm]
    Manual Swact = enabled

Chassis 1 reloading, reason - Non participant detected
```

Standby wireless controller

An Access Point and client Stateful Switch Over (SSO) implies that all the Access Point and client sessions are switched over state-fully and conMnue to operate in a network with no loss of sessions, providing improved network availability and reducing service downMme.

Once a redundancy pair is formed, HA is enabled, which means that Access Points and clients conMnue to remain connected during an acMve-to-standby switchover.



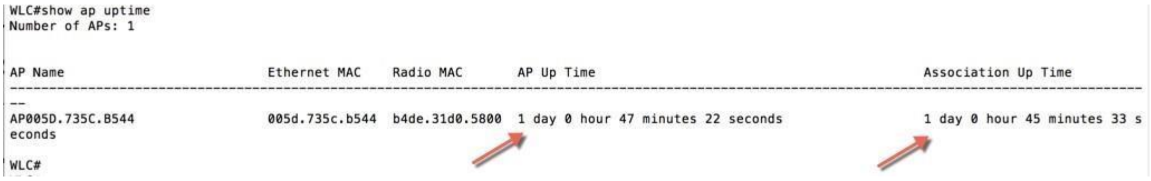
```
WLC-stby#
May 10 18:16:37.123: %PLATFORM-6-HASTATUS: RP switchover, received chassis event to become active
May 10 18:16:37.169: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_NOT_PRESENT)
May 10 18:16:37.169: %REDUNDANCY-3-REDUNDANCY_ALARMS: Unable to assert REDUNDANCY alarm

May 10 18:16:37.169: %REDUNDANCY-3-REDUNDANCY_ALARMS: Unable to assert REDUNDANCY alarm

May 10 18:16:37.169: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_DOWN)
May 10 18:16:37.169: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_REDUNDANCY_STATE_CHANGE)
May 10 18:16:37.175: %PLATFORM-6-HASTATUS: RP switchover, sent message became active. IOS is ready to switch to primary after chassis
confirmation
May 10 18:16:37.180: %PLATFORM-6-HASTATUS: RP switchover, received chassis event became active
May 10 18:16:37.789: %VOICE_HA-2-SWITCHOVER_IND: SWITCHOVER, from STANDBY_HOT to ACTIVE state.
May 10 18:16:37.797: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
May 10 18:16:37.798: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
May 10 18:16:37.798: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
May 10 18:16:38.798: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state to up
May 10 18:16:38.798: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state to up
May 10 18:16:38.798: %LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state to up
May 10 18:16:39.786: %LINK-3-UPDOWN: Interface Null0, changed state to up
May 10 18:16:39.786: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/0, changed state to up
May 10 18:16:39.787: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
May 10 18:16:39.788: %LINK-3-UPDOWN: Interface Vlan112, changed state to up
May 10 18:16:40.787: %LINEPROTO-5-UPDOWN: Line protocol on Interface Null0, changed state to up
May 10 18:16:40.787: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/0/0, changed state to up
May 10 18:16:40.787: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
May 10 18:16:40.787: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan112, changed state to up
WLC#
May 10 18:16:49.798: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to up
May 10 18:16:50.799: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to up
WLC#show ap sum
WLC#show ap summary
Number of APs: 1

AP Name                            Slots   AP Model  Ethernet MAC    Radio MAC       Location              Country     IP Address
State
-------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------
AP005D.735C.B544                     3     3802I     005d.735c.b544  b4de.31d0.5800  default location      US          172.20.226.186
Registered

WLC#show wireless client summary
Number of Local Clients: 1

MAC Address    AP Name                             WLAN  State              Protocol Method     Role
-------------------------------------------------------------------------------------------------------------
e8b2.ac94.757e AP005D.735C.B544                     1    Run                11ac     None       Local

Number of Excluded Clients: 0
```

Verifying AP and Client SSO State Sync

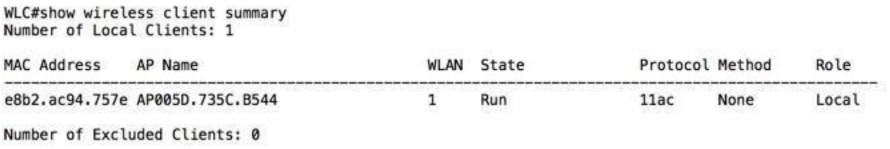
On successful switchover of the standby wireless controller as acMve, all access points and clients connected to the previously acMve wireless controller must remain connected to the new AcMve controller.

This can be verified by execuMng the commands:

- **show ap up3me** : Verifies that the upMme of the access point aher the switchover is not reset.
- **show wireless client summary**: Displays the clients connected to the new AcMve controller.



```
WLC#show ap uptime
Number of APs: 1

AP Name                          Ethernet MAC    Radio MAC       AP Up Time                                           Association Up Time
-----------------------------------------------------------------------------------------------------------------------------------------------------
--
AP005D.735C.B544                 005d.735c.b544  b4de.31d0.5800  1 day 0 hour 47 minutes 22 seconds                   1 day 0 hour 45 minutes 33 s
econds

WLC#
```



```
WLC#show wireless client summary
Number of Local Clients: 1

MAC Address    AP Name                          WLAN  State            Protocol Method     Role
-------------------------------------------------------------------------------------------------
e8b2.ac94.757e AP005D.735C.B544                 1     Run              11ac     None       Local

Number of Excluded Clients: 0
```

SSO Failover Time Metrics

Metrics	**Time**
Failure DetecMon	In the order of 500-1000ms

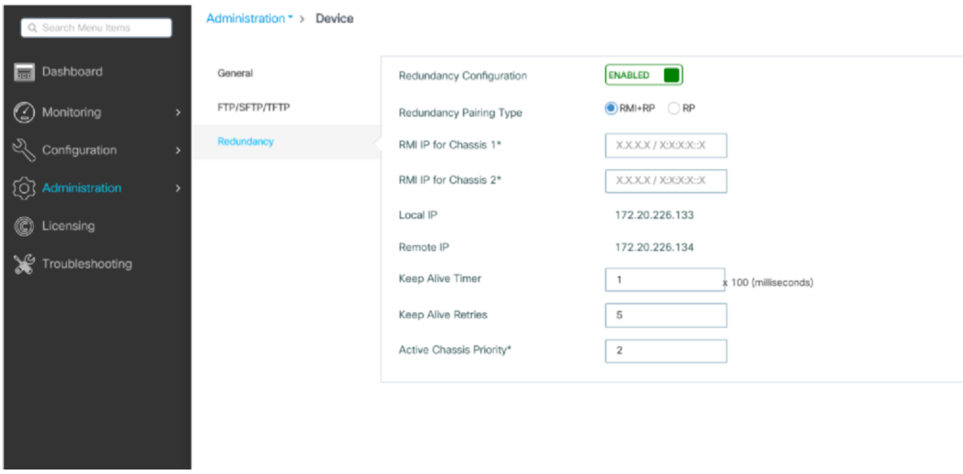
Redundancy Management Interface

With a single RP link between the SSO pair, if the heartbeat on RP fails, there is no way find out if the failure is limited to the link or if the other controller has failed. Redundancy Port (RP link) that handles state sync traffic between the active and the standby is a single point of failure.

Release 17.1 introduces the Redundancy Management Interface (RMI) as a secondary link between the active and the standby controllers. This release also introduces the support for default gateway check which is done using the redundancy management interface.

Release 17.4 introduces IPv6 Support for RMI interfaces. One management IPv6 address and one RMI IPv6 address is supported on the wireless management interface. Either RMI IPv4 or RMI IPv6 is supported and there is no simultaneous support for RMI IPv4 and RMI IPv6. The format of the CLI is same for IPv6 except that the IPv4 address is replaced with IPv6 address.

Redundancy Management Interface Configura&on using WebUI



Administration > Device

Redundancy Configuration: ENABLED

Redundancy Pairing Type: ● RMI+RP ○ RP

RMI IP for Chassis 1*: X.X.X.X / X:X:X:X::X

RMI IP for Chassis 2*: X.X.X.X / X:X:X:X::X

Local IP: 172.20.226.133

Remote IP: 172.20.226.134

Keep Alive Timer: 1 x 100 (milliseconds)

Keep Alive Retries: 5

Active Chassis Priority*: 2

- RMI IP for chassis 1 and 2 is same across both acMve and standby controllers
- RP IP configuraMon for chassis 1 and 2 auto-generated as 169.254.x.x where x.x. is from the RMI IP
- The netmask for RMI is picked up from the netmask configured on the Wireless Management VLAN.
- WebUI has RMI IPv6 support in Release 17.4

Programma&c configura&on of RMI IPs

On the Ac?ve controller:

Secondary address on the management VLAN is the RMI for the acMve. The primary address on the acMve is the management IP. It is possible to have mulMple "secondary" addresses on the interface as shown below. For the purpose of RMI, only one secondary IP will be defined. The secondary IP shall be configured programmaMcally.

There is no concept of "secondary" address in case of IPv6. The wireless management IP and the RMI IP will appear as 2 disMnct IPs in case of IPv6.

For eg, if the following CLI is configured: redun-management interface Vlan52 chassis 1 address

2020:0:0:1::211 chassis 2 address 2020:0:0:1::212 The acMve controller will be configured as follows:

Redundancy Management Interface `interface`

```
Vlan52
```

```
 ip address 10.100.0.1 255.252.0.0
 ipv6 address 2020:0:0:1::1/64  ipv6
address   2020:0:0:1::211/64    ipv6
enable
 ipv6 nd na glean  no
mop enabled  no
mop sysid end
```

On the Standby controller:

It cannot have the management IP as the address is claimed by the acMve. Therefore, on the standby controller, the RMI IP shall be configured as the primary address programmaMcally. When the standby becomes acMve, the management IP needs to be programmed as primary and the RMI IP as secondary.

The “secondary” IP concept is relevant for IPv4 only.

```
interface Vlan52  no
ip address
 ipv6 address 2020:0:0:1::212/64  ipv6
enable  ipv6 nd na glean  no mop
enabled  no mop sysid end
```

Dual Stack support with RMI IPv4

When RMI IPv4 is configured, it is possible to an IPv6 IP configured on the wireless management interface. This address shall be explicitly configured. With RMI enabled, the IPv6 address configured shall be programmaMcally removed in the standby and configured back when the standby transiMons to acMve. The address shall be removed when the controller is in acMverecovery mode. This would avoid Duplicate Address DetecMon.

Dual Stack Support with RMI IPv6

This case arises in release 17.4. In 17.4, the wireless management IP can be IPv6 with an RMI IPv6 configured. In addiMon, the wireless management interface can have an IPv4 IP configured. When the standby RMI interface is brought UP, the IPv6 and IPv4 management IPs will be unconfigured and IPv6 RMI configured. Upon transiMon from standby to acMve, the management IPs shall be restored.

Peer Timeout Configura&on

- AcMve and standby chassis send keepalives messages to each other to ensure both sMll available. Peer Mmeout is used to determine peer chassis is lost if it does not receive any keep alive message from peer chassis in the configured peer Mmeout.

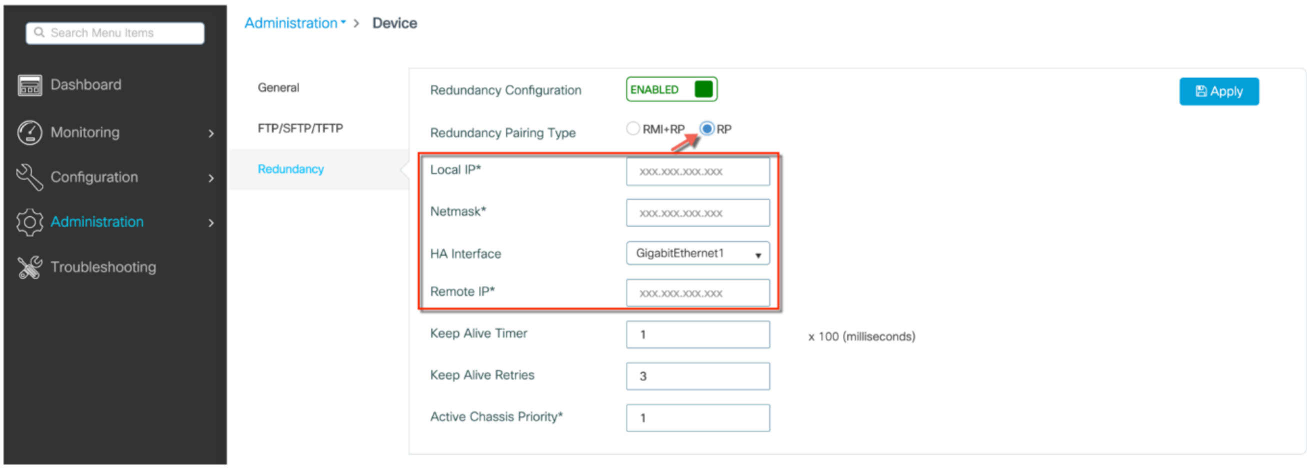
Cisco Confidential

- Default Mmeout is 100ms but is configurable up to 1000 ms. The keepalive retries are 5 by default but can be configured all the way to 10.

- CLI commands:

```
WLC#chassis redundancy keep-alive timer ?
        <1-10>  Chassis peer keep-alive time interval in multiple of 100 ms (enter 1 for

        default)
WLC#chassis redundancy keep-alive retries ?
        <5-10>  Chassis peer keep-alive retries before claiming peer is down (enter 5

for default)
```

For backward compaMbility, RP based SSO configuraMon will also be supported, but keep in mind that this will not support default gateway check and hence is not preferred.



Redundancy Configuration ENABLED

Redundancy Pairing Type ○ RMI+RP ● RP

Local IP* xxx.xxx.xxx.xxx

Netmask* xxx.xxx.xxx.xxx

HA Interface GigabitEthernet1

Remote IP* xxx.xxx.xxx.xxx

Keep Alive Timer 1 x 100 (milliseconds)

Keep Alive Retries 3

Active Chassis Priority* 1

Redundancy Management Interface Configura&on using CLI

UnMl 17.1, only RP-based SSO configuraMon was supported, i.e., chassis redundancy ha-interface <RP interface> local-ip <local IP> <local IP subnet> remote-ip <remote IP>.

17.1 and beyond, the user can use either RMI+RP or RP-based configuraMon. Once an HA pair is formed using RMI+RP configuraMon, the exec CLI for RP-based method of clearing and forming the HA pair shall not be allowed.

Note: Chassis re-number needs to be configured while bringing up HA with RMI from scratch using RMI in 17.x release.

The **chassis redundancy ha-interface GigabitEthernet** *interface-number* command needs to be defined in Cisco Catalyst 9800-CL Cloud Wireless Controller before pairing the controllers. This step is applicable only for Cisco Catalyst 9800-CL Series Wireless Controllers. The chosen interface is used as the dedicated interface for HA communicaMon between the 2 controllers.

By default, chassis number is 1. IP addresses of RP ports are derived from RMI. If the chassis number is the same on both controllers, local RP port IP derivaMon will be same and discovery will fail. This will result in AcMve-AcMve case.

To avoid this scenario, execute the following CLI:

Cisco Confidential
Cisco Confiden+al

```
    WLC#chassis 1 renumber ?
      <1-2>  Renumber local chassis id assignment
```

```
    WLC(config)# redun-management interface <VLAN> chassis 1 address <RMI IP of chassis 1>
chassis 2 address <RMI IP of chassis 2>
```

ConfiguraMon example:

Cisco Confidential

On WLC 1:

```
WLC(config)# redun-management interface Vlan112 chassis 1 address 172.20.226.148 chassis 2
address 172.20.226.149
```

On WLC 2: (Same CLI)

```
WLC(config)# redun-management interface Vlan112 chassis 1 address 172.20.226.148 chassis 2
address 172.20.226.149
```

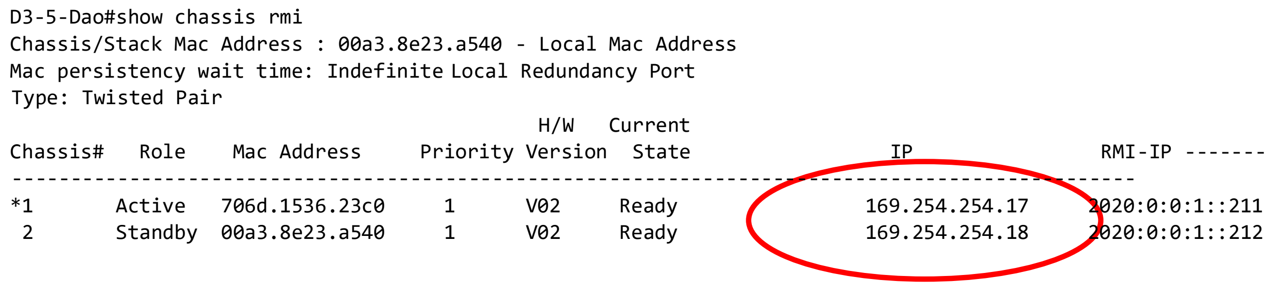
Chassis numbers idenMfy the individual controllers and must be configured before configuring the RMI IPs. It is mandatory to execute the same CLI on both controllers before forming the pair. The RMI IP configuraMon triggers HA pairing and forms the SSO pair.

Verifying RMI and RP configura&on

```
WLC-9800#show chassis rmi
Sep 20 21:26:13.024: %SYS-5-CONFIG_I: Configured from console by console
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  169.254.226.149 172.20.226.149
*2       Active   00a3.8e23.8900     1      V02     Ready  169.254.226.148 172.20.226.148
```

```
WLC-9800#show romvar   ROMMON
variables:
 SWITCH_NUMBER = 1
LICENSE_BOOT_LEVEL =
…
 RANDOM_NUM = 842430634
 SWITCH_PRIORITY = 1
 RMI_INTERFACE_NAME = Vlan112
 RMI_CHASSIS_LOCAL_IP = 172.20.226.148
RMI_CHASSIS_REMOTE_IP = 172.20.226.149  CHASSIS_HA_LOCAL_IP =
169.254.226.148
 CHASSIS_HA_REMOTE_IP = 169.254.226.149
CHASSIS_HA_LOCAL_MASK = 255.255.255.0
```

The following shows the scenario where the RP IP is derived from RMI IPv6 address:



```
D3-5-Dao#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
```

Cisco Confidential

RMI and RP pairing combina&ons

Upgrade and HA Pairing with no previous HA config

The user shall be presented with an opMon to choose the exisMng mechanism (exec RP-based CLIs) or the RMI IP based mechanism.

High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5

Redundancy Management Interface

If the user chooses the exec CLI based method, the RP IPs shall be configured as it happens Mll 16.12.

When the RMI configuraMon is done, it shall:

Generate the RP IPs with IPs derived from the RMI IPs and will also be used for sexng RMI IPs and pair the Controllers (while pairing only standby reloads in hardware plaXorms. Both acMve and standby reload in case of 9800-CL VM). Exec RPbased CLIs are blocked in this case. OpMon 1: RMI Based ConfiguraMon (Preferred)

1. Upgrade to 17.1 and connect the RPs
2. Configure RMI+RP
3. RP IPs are derived from the RMI IPs
4. RP-based exec commands are blocked
5. ROMMON RP and RMI variables are set OpMon 2: RP Based ConfiguraMon

1. Upgrade to 17.1 and connect RPs
2. Configure RP via GUI/CLI
3. RP-based configuraMon sets the local and remote IP
4. ROMMON RP Variables are set to the local and remote IP

Upgrade already Paired controllers

If the controllers are already in an HA pair, the exisMng exec RP CLIs can be conMnued to be used.

Those who would like to migrate to the RMI based HA pairing (preferred) can enable RMI.

This will overwrite the RP IPs with RMI derived IPs. The HA pair will not be immediately disturbed, but the controllers will pick up the new IP when they reload next.

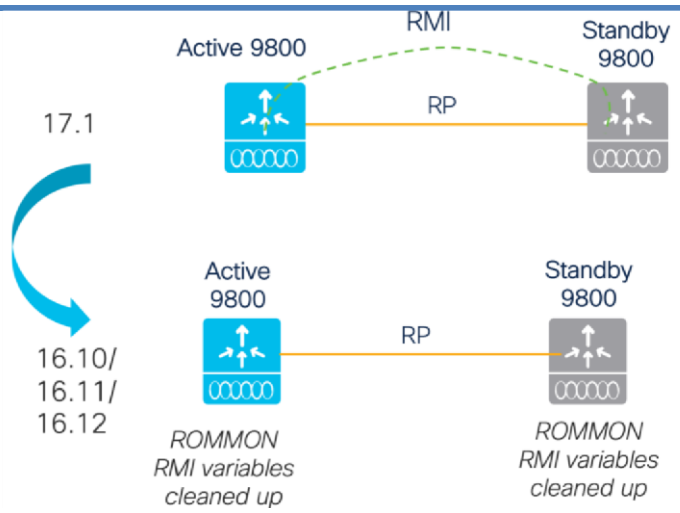
RMI feature mandates a reload for the feature to take effect.

When the controllers reload, they would come up as a pair with the new RMI-derived-RP-IPs. Exec RPbased CLIs will be blocked

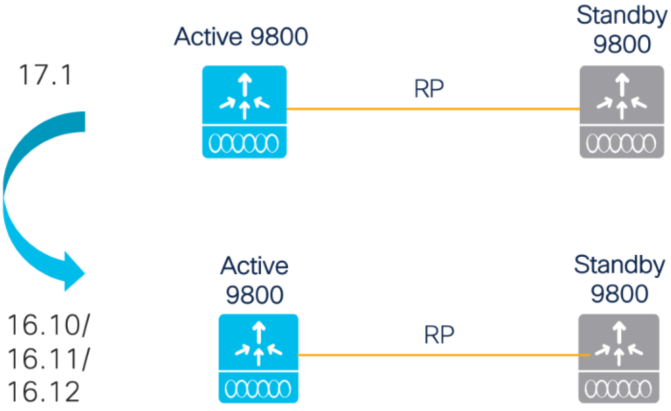
Downgrade

If RMI based configuraMon was used, aher downgrade the system will fall back to the RP-based configuraMon

High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5 Default Gateway Check



If RP based configuraMon was used, aher downgrade the system will conMnue to use RP-based configuraMon

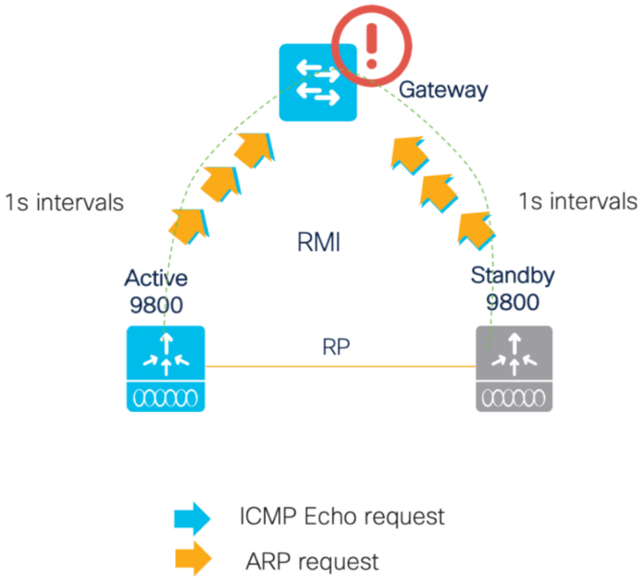


Default Gateway Check

Default Gateway check is done by periodically sending Internet Control Message Protocol (ICMP) ping to the gateway. Both the acMve and the standby controllers use the RMI IP as the source IP. These messages are sent at 1 second interval. If there are 8 consecuMve failures in reaching the gateway, the controller will declare the gateway as non-reachable.

Aher 4 ICMP Echo requests fail to get ICMP Echo responses, ARP requests are ayempted. If there is no response for 8 seconds (4 ICMP Echo Requests followed by 4 ARP Requests), the gateway is assumed to be non-reachable.

IPv6 default gateway detecMon is supported starMng release 17.4. Instead of ICMP and ARP in IPv4, IPv6 shall use ICMP to detect gateway failure.



The Catalyst 9800 Wireless controller has two recovery states to prevent an acMve-acMve scenario.

Recovery mode logically means a state where the controller does not have all "resources" available to provide the service. Currently, 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 acMve. But since it does not have the other resource (Gateway) it goes to Standby-Recovery. The standby shall not be in a posiMon to take over the acMve funcMonality 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.

- AcMve-Recovery is when the RP goes down. AcMve-Recovery does not have its internal state in sync with the AcMve. AcMveRecovery will reload when the RP link comes up so that it can come up as Standby with bulk sync.

Switchover history will show switchover reason as Gateway down in the event of a switchover triggered as a result of the gateway going down.

Configuring Gateway Failure Detec)on Interval

The gateway failure detecMon interval is configurable starMng release 17.4 using the following CLI:

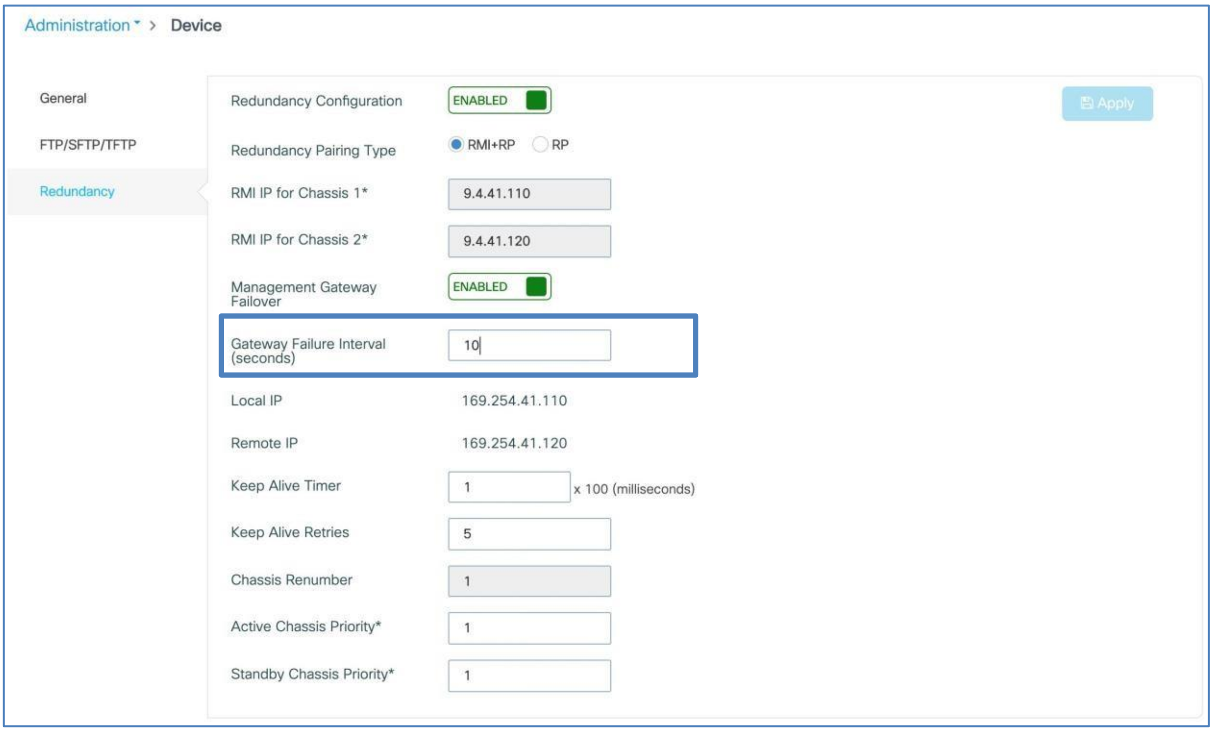
```
WLC(config)#management gateway-failover interval <6 - 12>
```

The default is 8.

This parameter can be configured through YANG, SNMP and WebUI as well. The configuraMon parameter is applicable for IPv6 gateway monitoring also.

Cisco Confidential

Configuring Gateway Failure Detection Interval



Redundancy Configuration: ENABLED

Redundancy Pairing Type: ● RMI+RP ○ RP

RMI IP for Chassis 1*: 9.4.41.110

RMI IP for Chassis 2*: 9.4.41.120

Management Gateway Failover: ENABLED

Gateway Failure Interval (seconds): 10

Local IP: 169.254.41.110

Remote IP: 169.254.41.120

Keep Alive Timer: 1 x 100 (milliseconds)

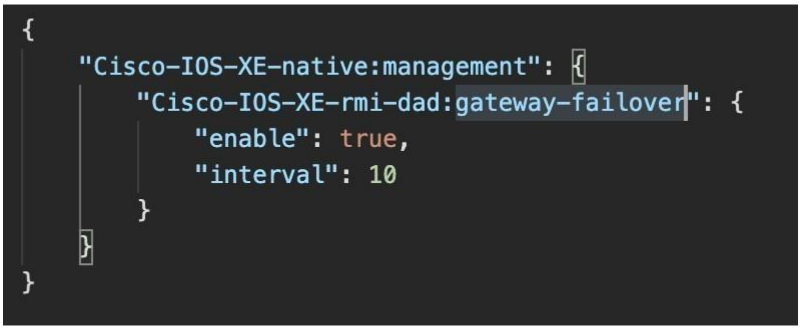
Keep Alive Retries: 5

Chassis Renumber: 1

Active Chassis Priority*: 1

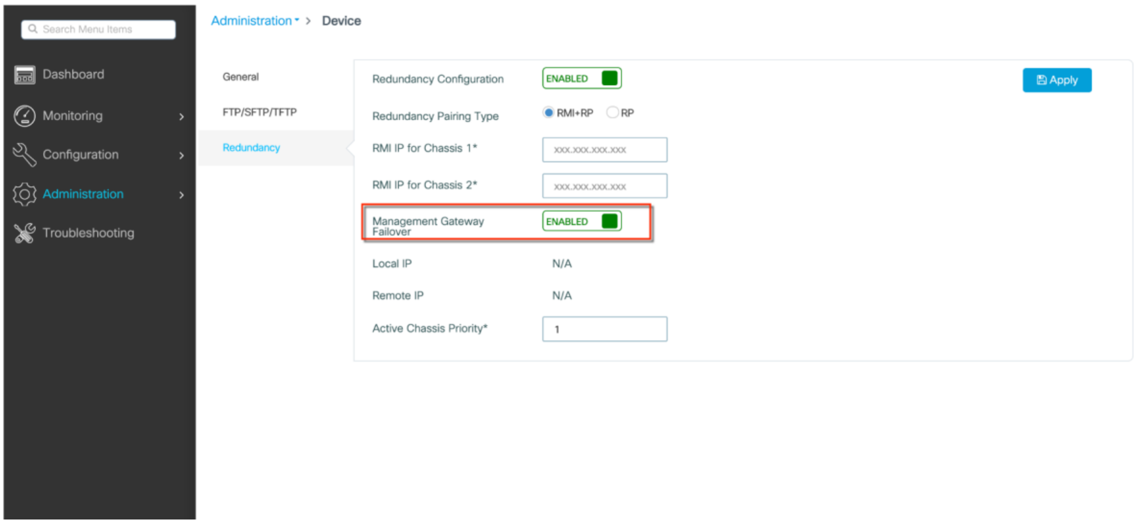
Standby Chassis Priority*: 1

Sample json for NETCONF/YANG support



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

Cisco Confidential



Redundancy Configuration ENABLED

Redundancy Pairing Type ● RMI+RP ○ RP

RMI IP for Chassis 1* xxx.xxx.xxx.xxx

RMI IP for Chassis 2* xxx.xxx.xxx.xxx

Management Gateway Failover ENABLED

Local IP N/A

Remote IP N/A

Active Chassis Priority* 1

Default Gateway Check CLI Configura&on

The following CLIs need to be configured for the gateway check funcMonality to be enabled and to specify the default gateway IP used by this feature

```
WLC-9800(config)#management gateway-failover enable   WLC-9800#ip
default-gateway <IP>
```

To verify if gateway check is enabled, use the CLI show redundancy state

```
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
```

With 17.2, usage of “ip default-gateway <IP>” shall be removed . Gateway IP will be picked up from the staMc IP routes configured. The HA infrastructure will choose the staMc route IP that matches the RMI network. If there are mulMple staMc routes configured, the route configured for the broadest network scope shall be selected. It is possible to configure mulMple gateways for the same network scope. If there are mulMple gateways for the same network, broadest mask and least gateway IP is chosen. The gateway IP shall be reevaluated, if necessary, when config update to staMc routes happens.

The above mechanism of selecMng the gateway IP from the set of staMc routes is applicable to IPv6 in Release 17.4.

Note:

•Physical port down scenario takes 8 seconds to be detected as it is detected via GW check mechanism prior to release

17.3.2. StarMng release 17.3.2, if the port state goes down all acMons associated with gateway going down will be triggered. A new reason code will be used to indicate SSO due to detecMon of port going down. “AcMve RMI Port Down” shall be used in place of “AcMve GW Lost”.

•Physical port status is synced from the acMve to standby controller in release 17.1. This has been fixed in release 17.2 and the acMve and standby controllers maintain their own port status.

System and Network 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 acMve controller crashes, the standby becomes acMve. The new acMve shall assume the role of master and try to detect a dual acMve.

These matrices provide a clear picture of what condiMon the WLC Switchover will trigger:

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

Cisco Confidential

Forced switchover	Down	Unreachable	N/A	Double fault – as menMoned in Network Error handling

RP Link	Peer reachability through RMI	Gateway From AcMve	Gateway from Standby	Switchover	Result
Up	Up	Reachable	Reachable	No	No acMon
Up	Up	Reachable	Unreachable	No	No AcMon. Standby is not ready for SSO in this state as it does not have gateway reachability. The standby shall be shown to be in standbyrecovery mode. If the RP goes down, standby (in recovery mode) shall become acMve.
Up	Up	Unreachable	Reachable	Yes	Gateway reachability message is exchanged over the RMI + RP links. AcMve shall reboot so that standby becomes acMve.

Cisco Confidential

Up	Up	Unreachable	Unreachable	No	Standby is not ready for SSO in this state as it does not have gateway reachability. Standby shall be shown to be in standby-recovery mode.
Up	Down	Reachable	Reachable	No	No AcMon
Up	Down	Reachable	Unreachable	No	No AcMon. 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.
Up	Down	Unreachable	Reachable	Yes	Gateway reachability message is exchanged over RP link also. AcMve shall reboot so that standby becomes acMve.

Up	Down	Unreachable	Unreachable	No	Standby is not ready for SSO in this state as it does not have gateway reachability. Standby shall be shown to be in standby-recovery mode.

Cisco Confidential

Down	Up	Reachable	Reachable	No	Standby shall go to Standby-Recovery mode as RP is not available.
Down	Up	Reachable	Unreachable	No	Standby is not ready for SSO in this state as it does not have gateway reachability. Standby shall be shown to be in standby-recovery mode.

Down	Up	Unreachable	Reachable	Yes	Gateway reachability message is exchanged over RP + RMI links. Old-AcMve goes to AcMve-Recovery mode. Config mode is disabled in acMverecovery mode. All interfaces will be ADMIN DOWN with the wireless management interface having RMI IP. The controller in AcMve Recovery will reload to become standby (or Standby-Recovery if Gateway Reachability is sMll not available) when the RP link comes UP.
Down	Up	Unreachable	Unreachable	No	Standby goes to Standby-Recovery.
Down	Down	Reachable	Reachable	Yes	Double fault – this may result in a network conflict as there will be 2 acMve controllers.

Cisco Confidential

Cisco Confiden+al

					Standby becomes acMve. Old acMve also exists. Role negoMaMon has to happen once the connecMvity is restored and keep the acMve that came up last
Down	Down	Reachable	Unreachable	No	Double fault - this may result in a network conflict as there will be 2 acMve controllers. Old AcMve conMnues to be AcMve. The Standby may become AcMve if network connecMvity is not restored with in a sMpulated Mme. Role negoMaMon has to happen once the connecMvity is restored and keep the acMve that came up last.
Down	Down	Unreachable	Reachable	Yes	Double fault – this may result in a network conflict as there will be 2 acMve controllers. Standby becomes acMve. Old acMve also may exist. Role negoMaMon has to happen once the connecMvity is restored and keep the acMve that came up last.

Down	Down	Unreachable	Unreachable	No	Double fault - this may result in a network conflict as there will be 2 active controllers. Old Active continues to be Active. The Standby may become Active if network connectivity is not restored with in a stipulated time. Role negotiation has to happen once the connectivity is restored and keep the active that came up last.

HA Unpairing Behavior

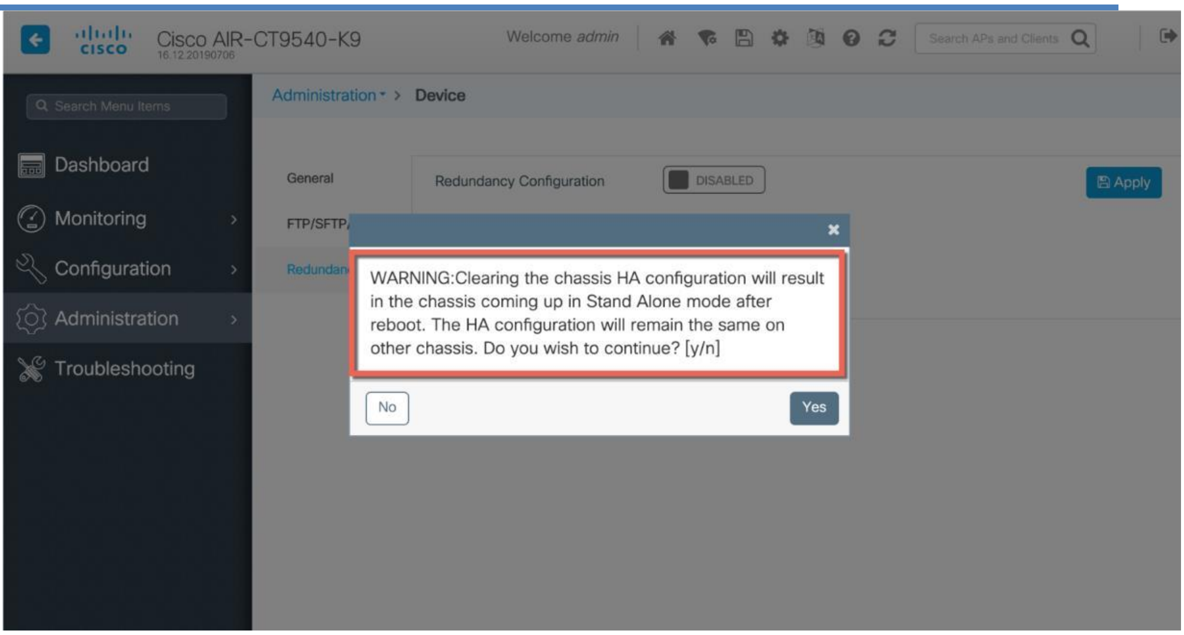
In release 16.10 and 16.11, when disjoining an HA pair by issuing the command 'clear chassis redundancy', the standby controller reboots and comes up with exactly the same configuration as the active controller, causing duplicate IP address error leading to the following messages:

```
WLC#sh log | i DUP
Mar 21 21:53:46.307 CET: %IP-4-DUPADDR: Duplicate address 120.0.0.1 on Vlan120, sourced by
d4c9.3ccc.f98b
Mar 21 21:54:16.947 CET: %IP-4-DUPADDR: Duplicate address 172.18.50.60 on
GigabitEthernet0, sourced by d4c9.3ccc.f981
```

The solution implemented in 16.12 and 17.1 is that after HA unpairing, the standby controller startup config and HA config will be cleared and standby will go to Day 0.

Before the command is executed, the user is prompted with the following warning on the active controller:

High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5 HA Unpairing Behavior



Redundancy Configuration DISABLED

WARNING:Clearing the chassis HA configuration will result in the chassis coming up in Stand Alone mode after reboot. The HA configuration will remain the same on other chassis. Do you wish to continue? [y/n]

The same is seen on the CLI as well.

```
WLC#clear chassis redundancy
WARNING: Clearing the chassis HA configuration will result in both the chassis move into Stand
Alone mode. This involves reloading the standby chassis after clearing its HA configuration and
startup configuration which results in standby chassis coming up as a totally clean after
reboot. Do you wish to continue? [y/n]? [yes]:
*Apr  3 23:42:22.985: received clear chassis.. ha_supported:1yes  WLC#
*Apr  3 23:42:25.042: clearing peer startup config
*Apr  3 23:42:25.042: chkpt send: sent msg type 2 to peer..
*Apr  3 23:42:25.043: chkpt send: sent msg type 1 to peer..
*Apr  3 23:42:25.043: Clearing HA configurations
*Apr  3 23:42:26.183:  Successfully sent Set chassis mode msg for chassis 1.chasfs file
updated  *Apr  3 23:42:26.359: %IOSXE_REDUNDANCY-6-PEER_LOST: Active detected chassis 2 is
no longer standby
```

On the standby controller, the following messages indicate that the configuraMon is being cleared:

```
WLC-stby#
*Apr  3 23:40:40.537: mcprp_handle_spa_oir_tsm_event: subslot 0/0 event=2
*Apr  3 23:40:40.537:     spa_oir_tsm subslot 0/0 TSM: during state ready, got event
3(ready)
*Apr  3 23:40:40.537: @@@ spa_oir_tsm subslot 0/0 TSM: ready -> ready
*Apr  3 23:42:25.041: Removing the startup config file on standby
*Apr  3 23:42:26.466: Calling HA configs clear on standby
*Apr  3 23:42:26.466: Clearing HA configurations
*Apr  3 23:42:27.499:  Successfully sent Set chassis mode msg for chassis 2.chasfs file
updated
```

Note: To unpair the SSO pair when using RMI based config, use the "no" version of the RMI configuraMon followed command by reload:

```
WLC(config)# no redun-management interface <VLAN> chassis 1 address <RMI IP of chassis 1>
chassis 2 address <RMI IP of chassis 2>
```

High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5

LACP, PAGP support in SSO Pair

LACP, PAGP support in SSO Pair

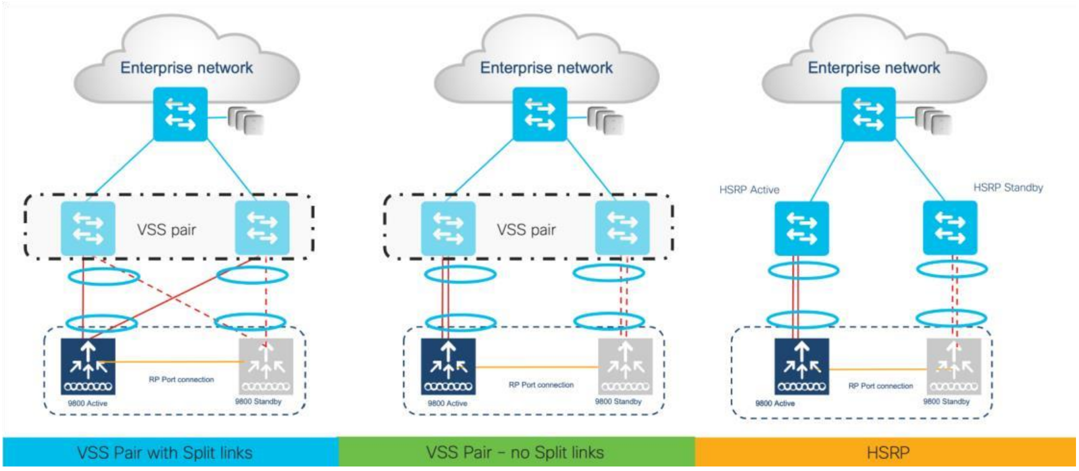
LACP protocol (IEEE 802.3ad) aggregates physical Ethernet interfaces by exchanging the Link AggregaMon Control Protocol Data Units (LACPDUs) between two devices.

LACP, PAGP support is needed on SSO pair in order to have the ability to detect and monitor the link/connecMvity failures on the standby controller and to have seamless transfer of client data traffic upon switchover (SSO). Prior to 17.1 only LAG mode

ON was supported in SSO mode. With 17.1 both LACP (acMve and passive) and PAGP will be supported in SSO mode. This feature is supported on Cisco Catalyst 9800-L, Cisco Catalyst 9800-40and Cisco Catalyst 9800-80 (including module ports).

Supported LACP, PAGP topologies

The following topologies are supported with SSO and LACP/PAGP



The following are not supported with LACP, PAGP topologies:

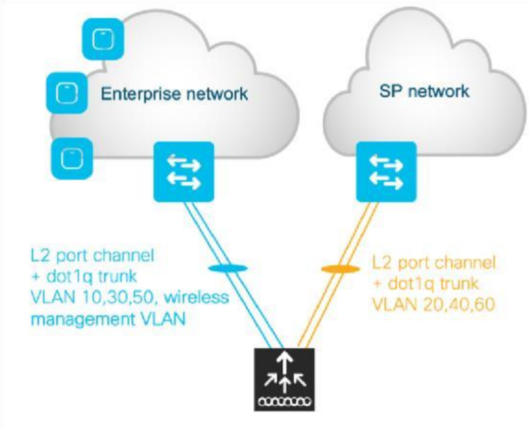
- Auto-LAG is not supported.
- C9800-CL and EWC on AP is not supported.
- L3 port-channel is not supported.

Mul$-chassis Link Aggrega$on group

StarMng with Release 17.2.1, MulM-chassis Link AggregaMon Group is supported on a standalone as well as HA Pair of controllers. MulM-chassis LAG provides the capability to connect mulMple uplinks from controller to separate uplink switches.

This enables flexibility in connecMng controller(s) to switch infrastructure and VLAN-based traffic splixng when connected to a mulM-switch topology, for e.g., to isolate Guest traffic on completely different switch/network from Enterprise traffic. Each LAG must be connected to a single switch and different VLANs must be assigned to different LAGs.

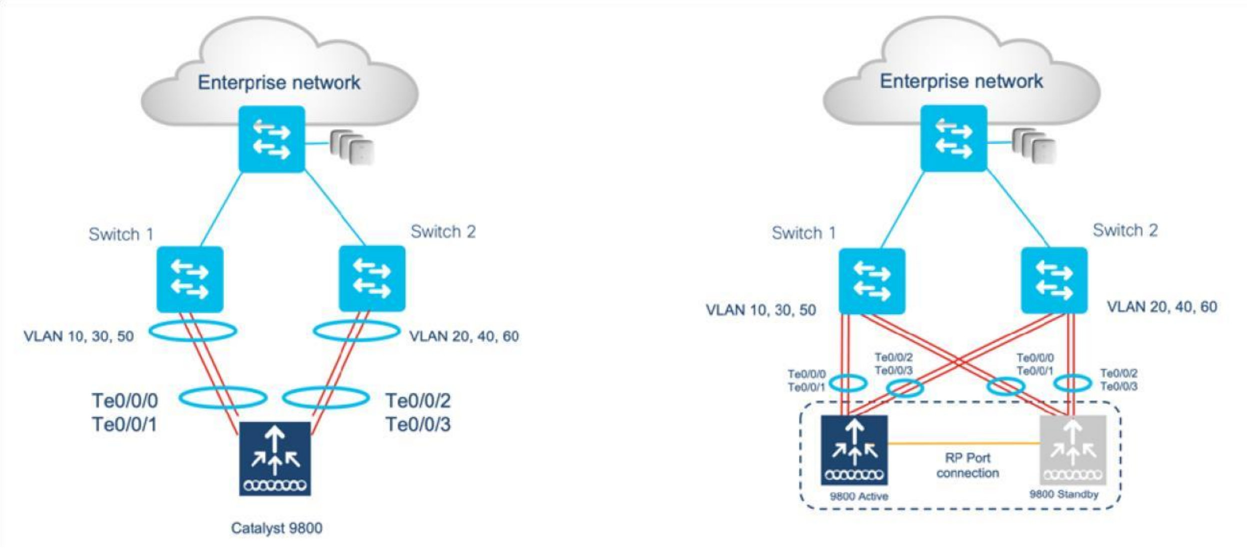
Cisco Confidential
Cisco Confiden+al



Note: It is the user's configuraOon responsibility not to create a loop.

Supported Mul)-chassis LAG topologies

- MulM-chassis LAG is supported with LAG mode ON and dynamic LAG (LACP and PAGP) • MulMchassis LAG is supported with a standalone controller as well as an HA pair as depicted below.



Note: Controller with mulOple LAGs can be connected to a single switch, However, different VLANs must be connected to different LAGs

Supported Pla9orms:

MulM-chassis LAG is supported on the following plaXorms:

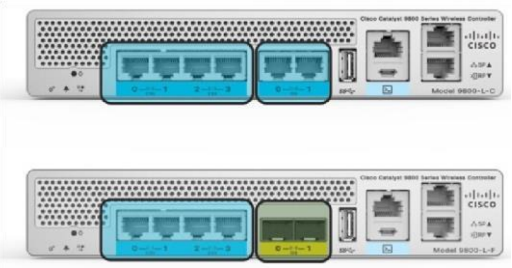
- Catalyst 9800-L Wireless Controllers
- Catalyst 9800-40 Wireless Controllers

- Catalyst 9800-80 Wireless Controllers

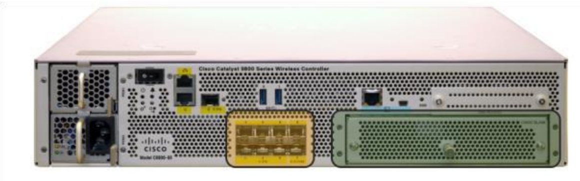
Supported LAG Port Grouping

Best pracMce 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



On the 9800-80 ports on Bay 0 and Bay 1 (modular slots) cannot be combined into the same port channel group. Best pracMce is to have ports of same slot in the port channel.



Sample LAG Configura)on for HA SSO pair connec)ng to a VSS Pair with Split Links

On the wireless Controller ACTIVE

WLC:

```
WLC#sh etherchannel summary

Flags:  D - down        P - bundled in port-channel

        I - stand-alone s - suspended

        H - Hot-standby (LACP only)

        R - Layer3      S - Layer2

        U - in use      f - failed to allocate aggregator
```

Cisco Confidential

Cisco Confiden+al

```
       M - not in use, minimum links not met        u -
unsuitable for bundling        w - waiting to be
aggregated
```

```
       d - default port


       A - formed by Auto LAG




Number of channel-groups in use: 1

Number of aggregators:          1


Group  Port-channel  Protocol    Ports

------+-------------+-----------+-----------------------------------------------

2      Po2(SU)        LACP        Te0/0/0(P)      Te0/0/3(P)


WLC#sh run int po2

Building configuration...


Current configuration : 54 bytes

!

interface Port-channel2  switchport

mode trunk end


WLC#sh run int te0/0/0

Building configuration...


Current configuration : 114 bytes

!

interface TenGigabitEthernet0/0/0
```

Cisco Confidential
Cisco Confiden+al

```
switchport mode trunk no negotiation auto

channel-group 2 mode active end
```

```
WLC#sh run int te0/0/3

Building configuration...


Current configuration : 114 bytes

!

interface TenGigabitEthernet0/0/3

switchport mode trunk no negotiation

auto channel-group 2 mode active end
```

STANDBY WLC:

```
WLC-stby#sh etherchannel summary

Flags:  D - down        P - bundled in port-channel

        I - stand-alone s - suspended

        H - Hot-standby (LACP only)

        R - Layer3      S - Layer2

        U - in use      f - failed to allocate aggregator


        M - not in use, minimum links not met         u -

unsuitable for bundling           w - waiting to be

aggregated        d - default port


        A - formed by Auto LAG




Number of channel-groups in use: 1    Number

of aggregators:          1    Group  Port-channel

Protocol    Ports
```

```
------+-------------+-----------+-----------------------------------------------
2     Po2(SU)       LACP      Te0/0/0(P)     Te0/0/3(P)


WLC-stby#sh run int po2 Building configuraMon...


Current configuraMon : 54 bytes
!
interface Port-channel2  switchport
mode trunk end


WLC-stby#sh run int te0/0/0 Building configuraMon...


Current configuraMon : 114 bytes
!
interface TenGigabitEthernet0/0/0
switchport mode trunk no negoMaMon
auto channel-group 2 mode acMve end


WLC-stby#sh run int te0/0/3 Building configuraMon...


Current configuraMon : 114 bytes
!
interface TenGigabitEthernet0/0/3
switchport mode trunk no negoMaMon
auto channel-group 2 mode acMve
```

Cisco Confidential
Cisco Confiden+al

end

```
WLC-stby#
```

On the VSS

```
Router#sh etherchannel summary

Flags:  D - down        P - bundled in port-channel

        I - stand-alone s - suspended

        H - Hot-standby (LACP only)

        R - Layer3      S - Layer2

        U - in use      N - not in use, no aggregaMon        f -
failed to allocate aggregator


        M - not in use, no aggregaMon due to minimum links not met         m - not in
use, port not aggregated due to minimum links not met          u - unsuitable for
bundling         d - default port


        w - waiMng to be aggregated

Number of channel-groups in use: 9

Number of aggregators:          9


Group  Port-channel  Protocol    Ports    ------+-------------+-----------+-----------------------------------------------

6      Po6(RD)          -

10     Po10(RU)         -        Te1/5/4(P)

20     Po20(RU)         -        Te2/5/4(P)
```

Cisco Confidential

```
30    Po30(SU)       LACP     Gi1/4/1(P)    Gi2/4/1(P)

40    Po40(SD)       -
```

Sample LAG ConfiguraMon for HA SSO pair connecMng to a VSS Pair with Split Links

```
60      Po60(SU)       LACP     Gi1/4/3(P)    Gi2/4/4(P)

61      Po61(SU)       LACP     Gi1/4/4(P)    Gi2/4/3(P)

833   Po833(SU)       -       Te1/1/1(P)    Te1/1/2(P) 865    Po865(SU)

-       Te2/1/1(P)    Te2/1/2(P)




Router#sh run int po60

Building configuraMon...



Current configuraMon : 67 bytes

!

interface Port-channel60 switchport

switchport mode trunk end



Router#sh run int po61

Building configuraMon...



Current configuraMon : 67 bytes

!

interface Port-channel61 switchport

switchport mode trunk end




Router#sh run int gi1/4/3 Building

configuraMon...
```

Cisco Confidential

```
Current configuraMon : 103 bytes

!
interface GigabitEthernet1/4/3 switchport

switchport mode trunk channel-group 60

mode acMve end


Router#sh run int gi2/4/4 Building

configuraMon...


Current configuraMon : 103 bytes

!
interface GigabitEthernet2/4/4 switchport

switchport mode trunk channel-group 60

mode acMve end


Router#sh run int Gi1/4/4 Building

configuraMon...


Current configuraMon : 103 bytes

!
interface GigabitEthernet1/4/4 switchport

switchport mode trunk channel-group 61

mode acMve end
```

Replacing a controller in an HA setup

```
Router#sh
run int Gi2/4/3 Building configuraMon...


Current configuraMon : 103 bytes

!
```

Cisco Confidential

```
interface GigabitEthernet2/4/3 switchport

switchport mode trunk channel-group 61

mode active end
```

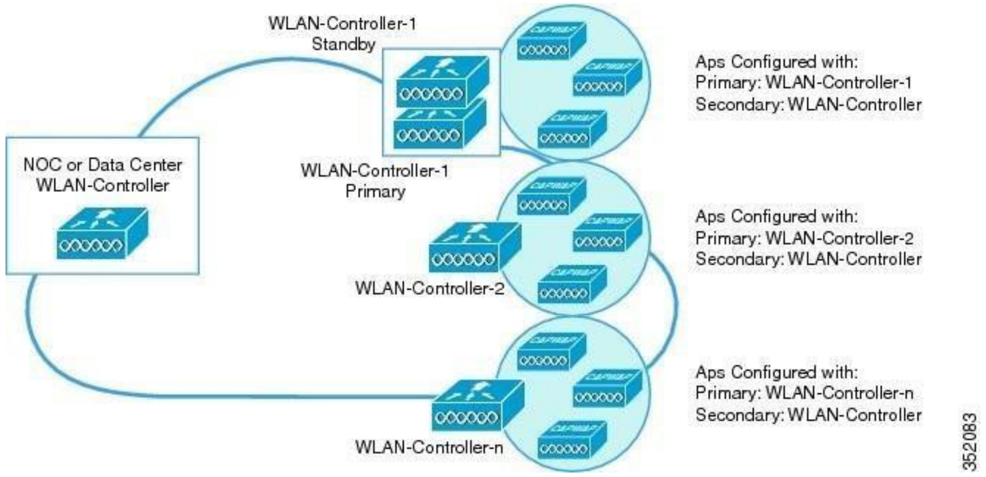
Replacing a controller in an HA setup

- Remove the active controller from the HA pair without breaking the pair. As a result of active controller going away, the standby controller will take over the role of Active.
- Prepare the new 9800 controller with the same configuration as the previous active controller. This means the same software version, licensing level, IP addresses WMI, RMI and mobility MAC.
- Configure a higher priority on the current Active controller to make sure that the current active remains the active even in the unlikely event of the active controller rebooting before the new controller is paired in SSO.
- Physically connect the new 9800 controller using the redundancy ports (RP)
- Enable SSO configuration on the new 9800 controller
- The new 9800 controller will reboot and come up as Standby paired with the current Active controller.

N+1 with SSO Hybrid deployment

Cisco Confidential

N+1 with SSO Hybrid deployment



A hybrid topology of SSO redundant pair and N+1 primary, secondary and terMary model is supported as shown above. The secondary controller at the DR site can be a Catalyst C9800-L, C9800-40 C9800-80 or C9800-CL Wireless controller. Access points failing back from Catalyst 9800 Wireless controller to CUWN controllers will re-download the code before joining the CUWN wireless controller and vice versa.

Standby Monitoring using RMI

This feature enables monitoring the health of the system on standby controller in an HA pair using programmaMc interfaces (NETCONF/YANG, RESTCONF) and CLIs without going through the acMve controller. This includes monitoring parameters such as CPU, memory, interface status, PSU (Power Supply Unit) failure, fan failure and temperature. This feature is supported on the Cisco Catalyst 9800-CL Private cloud, 9800-L, 9800-40, and 9800-80 wireless controller.

Using the RMI interface, the user can:

- Connect to the IOS SSH server on port 22 to execute a select set of show CLIs.
- Connect to the NETCONF SSH server on port 830 and use programmaMc interfaces to access NETCONF/YANG. • Connect on the HTTPS port 443 and use programmaMc interfaces using RESTCONF.

The user credenMals can be configured locally for Local AuthenMcaMon and External AAA server using RADIUS. SSH authenMcaMon shall be through user name and password. The standby controller does not run the PKI infrastructure to be able to handle cerMficate based authenMcaMon. External AAA servers shall be reachable through the default route which can be staMcally configured on the standby controller.

Syslog is supported on the standby controller as console logs.

Standby Monitoring using RMI IPv6 is supported starMng release 17.4

Standby Monitoring CLIs

Standby Monitoring using RMI

- To see power supply, fan and temperature status, the below CLI can be used on physical appliances. This output will be empty for virtual plaXorms.

```
Show environment
```

Cisco Confidential

```
9800-stby#show environment summary

Number of Critical alarms:  0
Number of Major alarms:     0
Number of Minor alarms:     0

 Slot         Sensor           Current State    Reading
Threshold(Minor,Major,Critical,Shutdown)
 ----------   --------------   --------------- ------------   -----------------------
-------------
 P0           Vin              Normal           218  V AC           na
 P0           Iin              Normal           1    A              na
 P0           Vout             Normal           12   V DC           na
 P0           Iout             Normal           20   A              na
P0           Temp1            Normal           31   Celsius        (na ,na ,na ,na
)(Celsius)
 P0           Temp2            Normal           42   Celsius        (na ,na ,na ,na
)(Celsius)
 P0           Temp3            Normal           43   Celsius        (na ,na ,na ,na
)(Celsius)
 P1           Vin              Normal           0    V AC           na
 P1           Iin              Normal           0    A              na
 P1              Vout                Normal               0     V  DC             na
P1              Iout                Normal               1     A                  na
P1           Temp1            Normal           28   Celsius        (na ,na ,na ,na
)(Celsius)
 P1           Temp2            Normal           29   Celsius        (na ,na ,na ,na
)(Celsius)
 P1           Temp3            Normal           0    Celsius        (na ,na ,na ,na
)(Celsius)
 R0           VRRX1: VX1       Normal           751  mV             na
 R0           VRRX1: VX2       Normal           6937 mV             na
 R0           VRRX1: VX3       Normal           1217 mV             na
 R0           VRRX1: VX5       Normal           1222 mV             na
 R0           VRRX1: VP1       Normal           1705 mV             na
 R0           VRRX1: VP2       Normal           2489 mV             na

 R0           VRRX1: VP3       Normal           1300 mV             na
 R0           VRRX1: VP4       Normal           5070 mV             na
 R0           VRRX1: VH        Normal           11993mV             na
 R0           VRRX2: VX1       Normal           853  mV             na
 R0           VRRX2: VX4       Normal           1016 mV             na
 R0           VRRX2: VX5       Normal           1019 mV             na
 R0           VRRX2: VP1       Normal           3325 mV             na
 R0           VRRX2: VP3       Normal           1826 mV             na
 R0           VRRX2: VP4       Normal           1050 mV             na
 R0           VRRX2: VH        Normal           11987mV             na
 R0           VRRX3: VX1       Normal           994  mV             na
 R0           VRRX3: VX2       Normal           1002 mV             na
 R0           VRRX3: VX4       Normal           750  mV             na
```

Cisco Confidential

```
 R0          VRRX3: VX5      Normal          751  mV             na
 R0          VRRX3: VP1      Normal          2477 mV             na
 R0          VRRX3: VP2      Normal          1197 mV             na
 R0          VRRX3: VP3      Normal          1517 mV             na
 R0          VRRX3: VP4      Normal          1514 mV             na
 R0          VRRX3: VH       Normal          11987mV             na
 R0          Temp: RCRX IN   Normal          26   Celsius        (52 ,57 ,62 ,73
)(Celsius)
 R0          Temp: RCRX OUT  Normal          41   Celsius        (62 ,67 ,72 ,80  )(Celsius)
 R0          Temp: Yoda      Normal          47   Celsius        (71 ,76 ,81 ,90 )(Celsius)
 R0          Temp: XEPhy     Normal          49   Celsius
(110,120,130,140)(Celsius)
```

```
 R0          Temp: CPU Die   Normal          47   Celsius        (61 ,66 ,71 ,80 )(Celsius)
R0          Temp: FC FANS   Fan Speed 40%   26   Celsius        (36 ,44 ,0   )(Celsius)
```

- To get interface status on Standby controller, the below CLI can be used:

```
show ip interface brief Eg.  9800-stby#show
ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES unset  down                  down
GigabitEthernet0       unassigned      YES NVRAM  administratively down down
Capwap1                unassigned      YES unset  up                    up
Capwap2                unassigned      YES unset  up                    up
Capwap3                unassigned      YES unset  up                    up
Capwap4                unassigned      YES unset  up                    up
Capwap5                unassigned      YES unset  up                    up
Capwap6                unassigned      YES unset  up                    up
Capwap7                unassigned      YES unset  up                    up
Capwap8                unassigned      YES unset  up                    up
Capwap9                unassigned      YES unset  up                    up
Capwap10               unassigned      YES unset  up                    up
Vlan1                  unassigned      YES NVRAM  down                  down      Vlan56
unassigned       YES unset  down                  down
Vlan111                111.1.1.85      YES NVRAM  up                    up
```

1. To see IOS task CPU on the standby, the CLI **show processes** can be used

```
9800-stby#show processes ?              <1-2147483647>
```

```
IOS(d) Process Number   cpu              Show CPU usage per IOS(d)
process   heapcheck       Show IOS(d) scheduler heapcheck
configuration   history          Show ordered IOS(d)
```

```
process history   memory           Show memory usage per IOS(d) process
platform        Show information per IOS-XE process
  timercheck      Show IOS(d) processes configured for timercheck
  |               Output modifiers
  <cr>            <cr>
```

Standby Monitoring Programma&c Interfaces

The CPU, memory and interface status on standby controller can be monitored programmaMc interfaces. Here is the list of operaMonal models required for this purpose:

- **Cisco-IOS-XE-device-hardware-oper.yang**: This has serial number for all FRUs in the device, including chassis. It also has informaMon about all hardware in the system.
- **Cisco-IOS-XE-process-cpu-oper.yang**: This has CPU uMlizaMon averages over intervals of past 1 min, 5 min, 5 seconds, and also per process CPU stats for IOS tasks.
- **Cisco-IOS-XE-plaYorm-soZware-oper.yang**: This gives Average CPU uMlizaMon of 5-second interval and allocated memory for the processes.

2. **Cisco-IOS-XE-process-memory-oper.yang**: This gives per process memory uMlizaMon.

- **Cisco-IOS-XE-interfaces-oper.yang**: This has interface operaMonal data including state and stats. It has a lot of other operaMonal data about interfaces also.

Steps to monitor the standby controller using SSH to RMI IPv4

1. Enable SSH on the acMve controller. In order to do that, it is required to generate rsa key

```
9800(config)#crypto key generate rsa
% You already have RSA keys defined named ak_vewlc_small.cisco.com.
% Do you really want to replace them? [yes/no]: yes
Choose the size of the key modulus in the range of 2048 to 4096 for your   General
Purpose Keys. Choosing a key modulus greater than 512 may take   a few minutes.


How many bits in the modulus [2048]: 2048
```

```
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
9800(config)#
```

Configure Local AAA or External AAA (RADIUS) with local AAA fallback as shown below.

```
line vty 0 4   password
Cisco
 authorization exec DEVICE_ADMIN
login authentication DEVICE_ADMIN  length
0
 transport input ssh
line vty 5 15
password Cisco
 authorization exec DEVICE_ADMIN   login
authentication DEVICE_ADMIN  transport
input telnet ssh  transport output telnet
ssh
  aaa authentication login DEVICE_ADMIN group AAA_GROUP_ISE1 local
aaa authorization exec DEVICE_ADMIN group AAA_GROUP_ISE1 local
aaa group server radius AAA_GROUP_ISE1  server name ISE1 radius
server ISE1
 address ipv4 <RMI IP> auth-port 1812 acct-port 1813   key
<key>
```

Note: TACACS is not supported for standby. Make sure “LOCAL” is added in the method list. So user will be authenMcated locally for standby.

```
aaa authentication login VTY_authen_tacacs group tacacs_ise_group local  aaa
authentication login VTY_authen_tacacs group tacacs_ise_group local
```

2. Make sure default route is configured for management VLAN.

```
ip route <Destination prefix> <Destination prefix mask> <Forwarding router's address>
```

3. Login to the standby controller using the standby controller’s RMI IP address

```
ssh <username>@<RMI IP> Password:
```

High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Bengaluru 17.5

Standby Monitoring using RMI

Note: To use Netconf-YANG SSH use the command:

ssh *<username>@<RMI IP>* -p 830

Only the default port of 830 can be used for Netconf-YANG SSH

4. Execute the commands **show environment summary, show processes, show ip interface brief** to view the CPU, memory, interface status, PSU (Power Supply Unit) failure, fan failure and temperature.

Command for Standby Monitoring using RESTCONF

GET request:

```
curl --
request GET --url https://<Standby RMI IP>:443/restconf/data/Cisco-IOS-
XEnative:native/hostname --header 'accept: application/yang-data+json' --header
'cachecontrol: no-cache' --header 'content-type: application/yang-data+json' -k -u
username:password
```

eg.

```
$curl --request GET --url https://<Standby RMI IP>:443/restconf/data/Cisco-IOS-
XEnative:native/hostname --header 'accept: application/yang-data+json' --header
'cachecontrol: no-cache' --header 'content-type: application/yang-data+json' -k -u
username:password
```

```
{
"Cisco-IOS-XE-native:hostname": "Catalyst 9800 HA2"
}
```

PUT request is not supported for the standby and will return an access-denied error.

Standby Monitoring in release 17.5

The following enhancements are part of this release

1. Monitoring directly on the standby controller
2. Monitoring for Standby parameters from the ac;ve controller

We will look at both of these in detail in the following sec;ons

Monitoring directly on the standby controller

1. Support for **IF-MIB** - This MIB is used to monitor Interface sta;s;cs HA-stby#snmp get-bulk v2c *<ip address>* public n 0 m 1000 oid ifMIB

Cisco Confidential

```
SNMP Response: reqid 1, errstat 0, erridx 0  ifName.1
= Gi1  ifName.2 = Gi0    ifName.3
= Vo0
ifName.4 = Nu0  ifName.5
= Vl1  ifName.6 = Vl84
ifName.7 = Vl111
ifName.8 = Vl184
```

```
umang_ha-stby#$lk v2c <ip address> public n 0 m 1000 oid ifAdminStatus
SNMP Response: reqid 2, errstat 0, erridx 0  ifAdminStatus.1 = 1
ifAdminStatus.2 = 2  ifAdminStatus.3 = 1  ifAdminStatus.4 = 1
ifAdminStatus.5 = 2  ifAdminStatus.6 = 1  ifAdminStatus.7 = 1
ifAdminStatus.8 = 1
ifOperStatus.1 = 2  ifOperStatus.2 = 2  ifOperStatus.3
= 1  ifOperStatus.4 = 2  ifOperStatus.5 = 2
ifOperStatus.6 = 2  ifOperStatus.7 = 2  ifOperStatus.8
= 1
```

Note: Please note that traps from the standby are not supported.

2. Support to list all the sensors using **show env all** on the standby chassis.

   a) Load image on an HA system.
   b) Run show env all on the standby a[er ac;ve and standby are up and running.

```
HA-stby#sh env all
Sensor List: Environmental Monitoring
Sensor Loca;on State Reading
Temp: BRDTEMP1 R0 Normal 35 Celsius
Temp: BRDTEMP2 R0 Normal 33 Celsius   Temp:
CPU Die R0 Normal 45 Celsius
```

3. **Standby Syslog to external server**

   Standby is able to send syslogs to external syslog server independently whenever user logs in via ios SSH or NETCONF

   a) Bring up an HA Pair
   b) configure external logging server   (config)#logging host <ip>

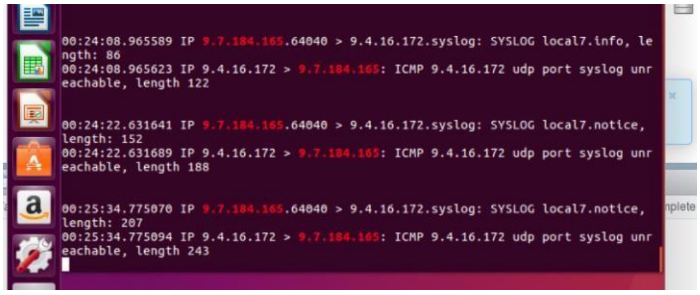
c) In logging server check if we are able to recieve syslogs from standby IP whenever user login in to standby via ssh or netconf SSH

Netconf:

Sep 28 10:52:43.263: %DMI-5-AUTH_PASSED: Chassis 2 R0/0: dmiauthd: User 'asomesul' authenticated successfully from 64.104.149.222:58970 and was authorized for netconf over ssh. External groups: PRIV15

IOS SSH:

Sep 28 10:56:02.163: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: asomesul] [Source: 9.4.16.172] [localport: 22] at 10:56:02 UTC Mon Sep 28 2020
Sep 28 10:56:04.183: %SYS-6-LOGOUT: User asomesul has exited tty session 1(9.4.16.172)



```
00:24:08.965589 IP 9.7.184.165.64040 > 9.4.16.172.syslog: SYSLOG local7.info, le
ngth: 86
00:24:08.965623 IP 9.4.16.172 > 9.7.184.165: ICMP 9.4.16.172 udp port syslog unr
eachable, length 122


00:24:22.631641 IP 9.7.184.165.64040 > 9.4.16.172.syslog: SYSLOG local7.notice,
length: 152
00:24:22.631689 IP 9.4.16.172 > 9.7.184.165: ICMP 9.4.16.172 udp port syslog unr
eachable, length 188


00:25:34.775070 IP 9.7.184.165.64040 > 9.4.16.172.syslog: SYSLOG local7.notice,
length: 207
00:25:34.775094 IP 9.4.16.172 > 9.7.184.165: ICMP 9.4.16.172 udp port syslog unr
eachable, length 243
```

Monitoring for Standby parameters from the active controller

1. Support for **CISCO-PROCESS-MIB** - This MIB is used to monitor CPU and process sta;s;cs.This is for CPU/Memory informa;on

In the sample output below, index 5 is chassis 1 and index 6 is chassis 2

#$lk v2c *<ip address>* public n 0 m 1000 oid cpmProcessEntry.2
SNMP Response: reqid 16, errstat 0, erridx 0
cpmProcessEntry.2.5.2890 = linux_iosd-imag
cpmProcessEntry.2.5.10111 = vman
cpmProcessEntry.2.5.11712 = lman cpmProcessEntry.2.5.13447
= cmand cpmProcessEntry.2.5.17443 = cli_agent

```
cpmProcessEntry.2.5.21398 = psd  cpmProcessEntry.2.5.22986
= smand  cpmProcessEntry.2.5.23265 = fman_fp_image
cpmProcessEntry.2.5.23936 = repm
cpmProcessEntry.2.5.24412 = plogd
```

```
cpmProcessEntry.2.5.25914 = cman_fp
cpmProcessEntry.2.5.26655 = hman
cpmProcessEntry.2.5.26981 = fman_rp
cpmProcessEntry.2.5.27625 = dbm
cpmProcessEntry.2.6.10140 = vman
cpmProcessEntry.2.6.11662 = lman
cpmProcessEntry.2.6.13007 = cmand
cpmProcessEntry.2.6.21071 = fman_fp_image
cpmProcessEntry.2.6.23341 = psd  cpmProcessEntry.2.6.23731
= cman_fp  cpmProcessEntry.2.6.25148 = repm
cpmProcessEntry.2.6.25424 = plogd
cpmProcessEntry.2.6.26475 = hman
cpmProcessEntry.2.6.26796 = fman_rp
cpmProcessEntry.2.6.27369 = dbm
cpmProcessEntry.2.6.27660 = cli_agent
cpmProcessEntry.2.6.28153 = linux_iosd-imag
cpmProcessEntry.2.6.30537 = smand
cpmProcessEntry.4.5.2890 = 1  cpmProcessEntry.4.5.10111
= 1  cpmProcessEntry.4.5.11712 = 3
cpmProcessEntry.4.5.13447 = 0
cpmProcessEntry.4.5.17443 = 1
cpmProcessEntry.4.5.21398 = 2
cpmProcessEntry.4.5.22986 = 2
cpmProcessEntry.4.5.23265 = 2
cpmProcessEntry.4.5.23936 = 0
cpmProcessEntry.4.5.24412 = 3
cpmProcessEntry.4.5.25914 = 0
cpmProcessEntry.4.5.26655 = 3
cpmProcessEntry.4.5.26981 = 1
cpmProcessEntry.4.5.27625 = 3
cpmProcessEntry.4.6.10140 = 2
```

```
cpmProcessEntry.4.6.11662 = 2  cpmProcessEntry.4.6.13007
= 2  cpmProcessEntry.4.6.21071 = 3   cpmProcessEntry.4.6.23341
= 3  cpmProcessEntry.4.6.23731
= 2  cpmProcessEntry.4.6.25148 = 3  cpmProcessEntry.4.6.25424
= 1
cpmProcessEntry.4.6.26475 = 1
```

Cisco Confidential
Cisco Confiden+al

2. Support for **CISCO-LWAPP-HA-MIB** – This MIB is used to monitor the HA parameters related to SSO

Supported fields:

9800-HA#$lk v2c 1.1.1.1 public n 0 m 1000 oid ciscoLwappHaMIB

```
SNMP Response: reqid 62, errstat 0, erridx 0
cLMcHaPortName.0 = GigabitEthernet2
cLMcHaPortLocIpAddrType.0 = 1  cLMcHaPortLocIp.0
= A9 FE B8 4E  cLMcHaPortMask.0 = FF FF FF 00
cLMcHaPortRemoteIpAddrType.0 = 1
cLMcHaPortRemIp.0 = A9 FE B8 4F
cLMcHaKeepAliveTimeOut.0 = 100
cLMcHaChassisPriority.0 = 1  cLMcHaClearConfig.0
= 2  cLMcHaKeepAliveRetryCount.0 = 5
cLMcRmiConfigAc;on.0 = 1  cLMcRmiInterface.0 =
Vlan184  cLMcRmiChassisANum.0 = 1
cLMcRmiChassisAIpAddrType.0 = 1
cLMcRmiChassisAIp.0 = 09 07 B8 4E
cLMcRmiChassisBNum.0 = 2
cLMcRmiChassisBIpAddrType.0 = 1
cLMcRmiChassisBIp.0 = 09 07 B8 4F
cLMcRmiGatewayFailover.0 = 1
cLMcRmiGatewayFailoverInterval.0 = 8
```

3. Support for **cLHaPeerHotStandbyEvent** - This object represents that the peer has turned hotstandby. a)

Bring up the HA pair

b) Reload the standby
c) From ac;ve: snmp get v2c *<ip address>* public oid cLHaPeerHotStandbyEvent.0
d) Ac;ve should return 0 as standby is not hot
e) A[er standby reloads and standby becomes HOT it must again changed to 1

A"er Reload of standby

#snmp get v2c *<ip address>* public oid cLHaPeerHotStandbyEvent.0
SNMP Response: reqid 31, errstat 0, erridx 0 **cLHaPeerHotStandbyEvent.0 = 0**

A"er reload to STANDBY HOT

```
#snmp get v2c <ip address> public oid cLHaPeerHotStandbyEvent.0
SNMP Response: reqid 33, errstat 0, erridx 0  cLHaPeerHotStandbyEvent.0
= 1
```

4. Support for **cLHaBulkSyncCompleteEvent** - This object represents the ;me when the bulk sync was complete.

   a) Bring up the HA pair
   b) Reload standby.
   c) From Ac;ve: snmp get *<ip address>* public oid cLHaBulkSyncCompleteEvent.0
   d) Ac;ve should return 0 as standby is not hot
   e) A[er standby reloads and standby becomes HOT bulk sync must again update

A"er Standby Reload

```
#snmp get <ip address> public oid cLHaBulkSyncCompleteEvent.0
SNMP Response: reqid 30, errstat 0, erridx 0  cLHaBulkSyncCompleteEvent.0
= 0
```

Standby to Standby HOT

```
#snmp get v2c <ip address> public oid cLHaBulkSyncCompleteEvent.0   SNMP
Response: reqid 32, errstat 0, erridx 0  cLHaBulkSyncCompleteEvent.0 =
1601288785
```

5. List ac;ve and standby sensors using **show env** command.

   a) Load image on an HA system.
   b) Run show env all on ac;ve a[er ac;ve and standby are up and running.

```
#sh env all
Sensor List:  Environmental Monitoring
 Sensor                 Loca;on       State         Reading
 Temp: BRDTEMP1         R0            Normal        39 Celsius
 Temp: BRDTEMP2         R0            Normal        36 Celsius   Temp:
CPU Die          R0            Normal        47 Celsius
 Stby Temp: BRDTEMP1     R0            Normal        36 Celsius
 Stby Temp: BRDTEMP2     R0           Normal        33 Celsius
 Stby Temp: CPU Die      R0           Normal        46 Celsius
```

Cisco Confidential

6. List standby sensors using the ‘show env chassis <standby chassis num> r0’ command.

   a) Load image on an HA system.

   b) Run **show env chassis <standby chassis num> r0** on ac;ve a[er ac;ve and standby are up and running. To see sensors on ac;ve controller from standby use the same command with the chassis number of the ac;ve chassis.

```
#sh env cha 2 r0
Sensor List: Environmental Monitoring
Sensor Loca;on State Reading
Stby Temp: BRDTEMP1 R0 Normal 35 Celsius
Stby Temp: BRDTEMP2 R0 Normal 33 Celsius  Stby
Temp: CPU Die R0 Normal 45 Celsius
```

7. Fetch ac;ve and standby sensors using YANG

   a) Load image on an HA system.
   b) Run NETCONF on the CISCO-IOS-XE-environmen-oper

Bellow is the xpath module use to get this informa:on.

Module   Cisco-IOS-XE-environment-oper
Revision   2019-05-01
Revision Info   Added seman,c version
Descrip,on   This module contains a collec,on of YANG defini,ons for monitoring Environment of a Network Element.
Copyright (c) 2016-2019 by Cisco Systems, Inc.
All rights reserved.
Organiza,on   Cisco Systems, Inc.
Imports
"cisco-semver"
Namespace   hZp://cisco.com/ns/yang/Cisco-IOS-XE-environment-oper   Prefix
environment-ios-xe-oper Namespace Prefixes   cisco-semver
hZp://cisco.com/ns/yang/cisco-semver environment-ios-xe-oper
hZp://cisco.com/ns/yang/Cisco-IOS-XE-
environmentoper
Modtype   module
Opera,ons
"get"

Below is the output of yang for reference:

```
Table Record Index 0 = {
[0] state = Normal
[1] current_reading = 35
```

```
[2] sensor_units = SENSOR_UNIT_CELSIUS
[3] low_cri;cal_threshold = 60
[4] low_normal_threshold = -2147483647
[5] high_normal_threshold = 53
[6] high_cri;cal_threshold = 60
[7] sensor_name = SENSOR_TYPE_TEMPERATURE
```

```
[8] name = Temp: BRDTEMP1
[9] loca;on = R0
}
Table Record Index 1 = {  [0]
state = Normal
[1] current_reading = 33
[2] sensor_units = SENSOR_UNIT_CELSIUS
[3] low_cri;cal_threshold = 64
[4] low_normal_threshold = -2147483647
[5] high_normal_threshold = 57
[6] high_cri;cal_threshold = 64
[7] sensor_name = SENSOR_TYPE_TEMPERATURE
[8] name = Temp: BRDTEMP2
[9] loca;on = R0
}
Table Record Index 2 = {
[0] state = Normal
[1] current_reading = 45
[2] sensor_units = SENSOR_UNIT_CELSIUS
[3] low_cri;cal_threshold = 104
[4] low_normal_threshold = -2147483647
[5] high_normal_threshold = 93
[6] high_cri;cal_threshold = 104
[7] sensor_name = SENSOR_TYPE_TEMPERATURE
[8] name = Temp: CPU Die
[9] loca;on = R0
}
Table Record Index 3 = {
[0] state = Normal
[1] current_reading = 39
[2] sensor_units = SENSOR_UNIT_CELSIUS
[3] low_cri;cal_threshold = 60
[4] low_normal_threshold = -2147483647

[5] high_normal_threshold = 53

[6] high_cri;cal_threshold = 60
[7] sensor_name = SENSOR_TYPE_TEMPERATURE
[8] name = Stby Temp: BRDTEMP1
[9] loca;on = R0
}
```

```
Table Record Index 4 = {
[0] state = Normal
[1] current_reading = 36
[2] sensor_units = SENSOR_UNIT_CELSIUS
[3] low_cri;cal_threshold = 64
[4] low_normal_threshold = -2147483647
[5] high_normal_threshold = 57
[6] high_cri;cal_threshold = 64
[7] sensor_name = SENSOR_TYPE_TEMPERATURE
[8] name = Stby Temp: BRDTEMP2
[9] loca;on = R0
}
```

Cisco Confidential

```
Table Record Index 5 = {
[0] state = Normal
[1] current_reading = 47
[2] sensor_units = SENSOR_UNIT_CELSIUS
[3] low_cri;cal_threshold = 104
[4] low_normal_threshold = -2147483647
[5] high_normal_threshold = 93
[6] high_cri;cal_threshold = 104
[7] sensor_name = SENSOR_TYPE_TEMPERATURE
[8] name = Stby Temp: CPU Die
[9] loca;on = R0
}
```

8. Get the ac;ve and standby power, fan and RP sensor informa;on using **snmpwalk**

    a) Load the Image on HA system.
    b) Run the snmpwalk from any Linux machine once standby joined.
    c) Run the CLI **show inventory raw** and check the sensors of standby and ac;ve
    d) Do snmpwalk on the en;ty mib and sensor mib check the power, fan and RP sensor are aligned with the values from the CLI output.

Below is the output of snmpwalk for reference

```
SNMPv2-SMI::mib-2.47.1.1.1.1.7.1 = STRING: "Mul; Chassis System"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.2 = STRING: "Chassis 1"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.3 = STRING: "Chassis 1 Power Supply Bay 0"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.4 = STRING: "Chassis 1 Power Supply Module 0"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.5 = STRING: "Vin  P0/0"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.6 = STRING: "Iin  P0/1"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.7 = STRING: "Vout P0/2"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.8 = STRING: "Iout P0/3"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.9 = STRING: "Temp1    P0/4"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.10 = STRING: "Temp2    P0/5"   SNMPv2-SMI::mib-
2.47.1.1.1.1.7.11 = STRING: "Temp3    P0/6"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.14 = STRING: "Chassis 1 Power Supply 0"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.23 = STRING: "Chassis 1 Power Supply Bay 1"   SNMPv2-
SMI::mib-2.47.1.1.1.1.7.44 = STRING: "Chassis 1 Fan Tray"

SNMPv2-SMI::mib-2.47.1.1.1.1.7.55 = STRING: "Chassis 1 Fan 2/0"
```

```
SNMPv2-SMI::mib-2.47.1.1.1.1.7.56 = STRING: "Chassis 1 Fan 2/1"
```

```
SNMPv2-SMI::mib-2.47.1.1.1.1.7.57 = STRING: "Chassis 1 Fan 2/2"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.58 = STRING: "Chassis 1 Fan 2/3" SNMPv2-SMI::mib-
2.47.1.1.1.1.7.500 = STRING: "Chassis 2"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.501 = STRING: "Chassis 2 Power Supply Bay 0"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.502 = STRING: "Chassis 2 Power Supply Module 0"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.503 = STRING: "Stby Vin  P0/0"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.504 = STRING: "Stby Iin  P0/1"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.505 = STRING: "Stby Vout P0/2"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.506 = STRING: "Stby Iout P0/3"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.507 = STRING: "Stby Temp1    P0/4"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.508 = STRING: "Stby Temp2    P0/5"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.509 = STRING: "Stby Temp3    P0/6"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.512 = STRING: "Chassis 2 Power Supply 0"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.521 = STRING: "Chassis 2 Power Supply Bay 1"
```

Legal InformaMon THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS

MANUAL ARE SUBJECT

TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementaMon of TCP header compression is an adaptaMon of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operaMng system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustraMve purposes only. Any use of actual IP addresses or phone numbers in illustraMve content is unintenMonal and coincidental.

All printed copies and duplicate soh copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices. **Cisco Trademark**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks menMoned are the property of their respecMve owners. The use of the word partner does not imply a partnership relaMonship between Cisco and any other company. (1110R)

Cisco Copyright